Lecture Notes
on
Discrete Structures and Theory of Logic

Dharmendra Kumar

February 16, 2021

Contents

Chapter 1

Set Theory

1.1 Set

1.1.1 Definition

A well-defined collection of distinct objects can be considered to be a set.

Elements of a set can be just about anything from real physical objects to abstract mathematical objects. An important feature of a set is that its elements are distinct or uniquely identifiable.

A set is typically expressed by curly braces, {} enclosing its elements. If A is a set and a is an element of it, then we write a $\in$ A. The fact that a is not an element of A is written as a $\notin$ A. For instance, if A is the set {1, 2, 4, 9}, then 1 $\in$ A; 4 $\in$ A; 2 $\in$ A and 9 $\in$ A. But 7 $\notin$ A; 10 $\notin$ A, the English word 'four' is not in A, etc.

1.1.2 Representation of sets

We can represent sets in two ways.
1. Tabular form or roster form: Listing the elements of a set inside a pair of braces { } is called the roster form.
2. Set builder form: In the set builder form, all the elements of the set, must possess a single property to become the member of that set.

1.1.3 Examples

1. Let X = {apple, tomato, orange}. Here, orange $\in$ X, but potato $\notin$ X.
2. X = $\{a_1, a_2, ..., a_{100}\}$. Then, $a_{100} \in$ X.
3. Observe that the sets {1, 2, 3} and {3, 1, 2} are equal.
4. Let X = {1, 2, 3, 4, 5, 6, 7, 8, 9, 10}. Then X is the set of first 10 natural numbers. Or equivalently, X is the set of integers between 0 and 11.
5. X = {x : x is a prime number}.
6. X = {x : $0 < x \leq 10$ and x is an even integer }

Clearly examples 1, 2, 3, and 4 are in roster form, but 5 and 6 are in set builder form.

1.2 Types of set

1.2.1 Finite and Infinite sets

A set is said to be finite if the number of elements in the set is finite otherwise it is said to be infinite.

For example, a set of days in a week, set of months in a year, and a set of integer lie between 1 and 100 are finite sets. But set of integers, set of real numbers, and set of stars in sky are infinite sets.

1.2.2 Null or Empty set

A set which does not contain any element, is said to be null set. It is denoted by ϕ.
Example: set A = {a ! a is an integer lie between 4 and 5}

1.2.3 Singleton set

A set is said to be singleton set if it contains only one element.

1.2.4 Universal set

A universal set is the set of all elements under consideration, denoted by capital U or sometimes capital E.
Example: If we consider the elements are integers, then universal set will be the set of integer numbers. Similarly, if the elements are days of a week, then the set of all days in a week will be the universal set.

1.2.5 Subset

Consider two sets A and B. Set B is said to be subset of A if all the elements of B belong into A. It is denoted by $\subseteq$ symbol. That is, B $\subseteq$ A.
Example: Consider three sets A, B and C such that A= { 2, 3, 5, 8}, B= { 3, 5}, C={ 2, 9, 5, 8}. Clearly B is a subset of A but B is not a subset of C. Similarly, neither A is a subset of A nor C is a subset of A.
Note (1) Every set A is a subset of itself i.e. A $\subseteq$ A.
(2) The null set ϕ is a subset of any set.
(3) If A $\subseteq$ B and B $\subseteq$ C then A $\subseteq$ C.

1.2.6 Superset

Consider two sets A and B. Set A is said to be superset of B if all the elements of B belong into A. It is denoted by $\supseteq$ symbol. That is, A $\supseteq$ B.
Example: Consider three sets A, B and C such that A= { 2, 3, 5, 8}, B= { 3, 5}, C={ 2, 9, 5, 8}. Clearly A is a superset of B but C is not a superset of B. Similarly, neither A is a superset of A nor C is a superset of A.

1.2.7 Proper and Improper subsets

A set B is said to proper subset of set A if B is a subset of A and not equal to A that is B $\subseteq$ A and A $\neq$ B. It is denoted by $\supset$. Therefore, we can represent proper subset as B $\subset$ A.
A set B is said to improper subset of set A if B is a subset of A and equal to A that is B $\subseteq$ A and A = B.
Example: Consider four sets A, B, C and D such that A= { 2, 3, 5, 8}, B= { 3, 5}, C={ 2, 3, 5}, D={ 2, 3, 5, 8}. Clearly, B and C are the proper subsets and D is an improper subset.

1.2.8 Equal set

Two sets are said to be equal if both contains same elements. That is, if A $\subseteq$ B and B $\subseteq$ A then A = B.

1.2.9 Power set

The power set of a set A is the set of all the subsets of set A. It is denoted by P(A) or 2^A.
Example: (1) Consider set A = { a, b, c}. Then the power set of A is, P(A) = {ϕ ,{a},{b},{c},{a,b},{b,c},{a,c},{a,b,c}}.
(2) The power set of null or empty set will be {ϕ}.
Note If set A has n elements then number of elements in the power set of A will be 2^n.

1.3 Operations defined on set

1.3.1 Union operation

For any two sets A and B, the union of A and B is the set of all the elements which are belongs into A or B or both. It is denoted by A$\cup$B. Mathematically, it is defined as following:-
A$\cup$B = { x ! x $\in$ A or x $\in$ B}
Example: Let A = { a, b, c } and B = { d, e, c }. Then union of A and B will be, A$\cup$B = { a, b, c, d, e }.

1.3.2 Intersection operation

For any two sets A and B, the intersection of A and B is the set of all the elements which are belong into both A and B . It is denoted by A$\cap$B. Mathematically, it is defined as following:-
A$\cap$B = { x ! x $\in$ A and x $\in$ B}
Example: Let A = { a, b, c } and B = { d, e, c }. Then intersection of A and B will be, A$\cap$B = { c }.

1.3.3 Set difference operation

For any two sets A and B, the set difference of A and B is the set of all the elements which are belong into A but not belong into B . It is denoted by A-B. Mathematically, it

is defined as following:-
A-B = { x ! x ∈ A and x ∉ B}
Example: Let A = { a, b, c } and B = { d, e, c }. Then set difference of A and B will be, A-B = {a, b}.

1.3.4 Complement operation

Let U is the universal set. For any set A, the complement of A is the set of all the elements U, which are not belong into A. It is denoted by A^c or A'. Mathematically, it is defined as following:-
A'= U-A = { x ! x ∈ U and x ∉ A}
Example: Let A = { a, b, c } and U = { a, b, c, d, e, f, g }. Then complement of A will be, A' = { d, e, f, g}.

1.3.5 Symmetric difference operation

For any two sets A and B, the symmetric difference of A and B is denoted by A⨁B. Mathematically, it is defined as following:-
A⨁B = (A-B) ∪ (B-A)
Example: Let A = { a, b, c } and B = { d, e, c }. Then symmetric difference of A and B will be, A⨁B = {a, b, d, e }.

1.3.6 Disjoint sets

Two sets A and B are said to be disjoint if there is no common elements between A and B. That is, A and B are disjoint iff A∩B = ϕ.
Example: Let A = { a, b, c } and B = { d, e, f }. Here A and B are disjoint because A∩B = ϕ.

1.3.7 Mutually disjoint sets

A collection of sets S={ $A_1, A_2, ..., A_n$} is said to be mutually disjoint if each pair of A_i and A_j in S are disjoint. That is, S is mutually disjoint if $A_i \cap A_j = \phi$, ∀ i,j = 1,2,.....,n. and i≠j.
Example: Let A = { {1, 2}, { 3} }, B = { {1}, {2, 3}} and C = { {1, 2, 3}}. These sets A, B and C are mutually disjoint because A∩B = ϕ, B∩C = ϕ, and A∩C = ϕ.

1.3.8 Cardinality of a set

The number of elements in a set is said to be cardinality of a set. It is denoted by || symbol. That is, if A is a set then cardinality of set A is denoted by $|A|$.
Note:
(1) The number of elements in a set A is also represented by n(A).
(2) n(A∪B) = n(A) + n(B) - n(A∩B)
(3) n(A∪$B \cup C$) = n(A) + n(B) + n(C) - n(A∩B) - n(B∩C) - n(A∩C) + n(A∩$B \cap C$)

1.4 Some examples

Example: Show that $A \subseteq B \Leftrightarrow A \cap B = A$
Solution: In this question, we have to prove two parts.
First part: In this part, we have to show that if $A \subseteq B$ then $A \cap B = A$.
Suppose $A \subseteq B$.
Let $x \in A$. Since $A \subseteq B$ therefore $x \in B$. Clearly x is belong into both A and B. Therefore x also belongs into $A \cap B$. Therefore

$$A \subseteq A \cap B \text{ .....(1)}$$

Let $x \in A \cap B$. Therefore $x \in A$ and $x \in B$. Therefore we can say $x \in A$. Therefore

$$A \cap B \subseteq A \text{ .....(2)}$$

Using equations(1) and (2), $A \cap B = A$.

Second part: In this part we have to show that if $A \cap B = A$ then $A \subseteq B$.
Let $x \in A$. Since $A \cap B = A$ therefore $x \in A \cap B$. This imply that $x \in A$ and $x \in B$. Therefore we can say $x \in B$. Therefore

$$A \subseteq B.$$

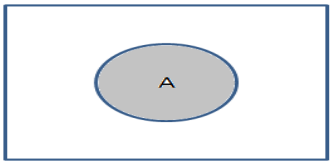
Example: Show that
(a) A-B = A∩B'
(b) $A \subseteq B \Leftrightarrow B' \subseteq A'$
Solution:
(a) Let $x \in A\text{-}B \Rightarrow x \in A$ and $x \notin B$
$\Rightarrow x \in A$ and $x \in B'$
$\Rightarrow x \in A \cap B'$
Therefore, $A\text{-}B \subseteq A \cap B'$ .....(1)
Now, let $x \in A \cap B' \Rightarrow x \in A$ and $x \in B'$
$\Rightarrow x \in A$ and $x \notin B$
$\Rightarrow x \in A\text{-}B$
Therefore, $A \cap B' \subseteq A\text{-}B$ .....(2)
Using equations (1) and (2), A-B = A∩B'
(b) First part: Suppose $A \subseteq B$.
Let let $x \in B' \Rightarrow x \notin B$
$\Rightarrow x \notin A$ (Since $A \subseteq B$)
$\Rightarrow x \in A'$
Therefore, $B' \subseteq A'$
Second part: Suppose $B' \subseteq A'$.
Let let $x \in A \Rightarrow x \notin A'$
$\Rightarrow x \notin B'$ (Since $B' \subseteq A'$)
$\Rightarrow x \in B$
Therefore, $A \subseteq B$
Using first and second parts, we can say that
$A \subseteq B \Leftrightarrow B' \subseteq A'$
Example: Show that for any two sets A and B,
A-(A∩B) = A-B
Solution: Let $x \in A\text{-}(A \cap B) \Leftrightarrow x \in A$ and $x \notin A \cap B$

$\Leftrightarrow$ x $\in$ A and x $\in$ (A$\cap$B)'
$\Leftrightarrow$ x $\in$ A and (x $\notin$ A or x $\notin$ B)
$\Leftrightarrow$ (x $\in$ A and x $\notin$ A) or (x $\in$ A and x $\notin$ B)
$\Leftrightarrow$ FALSE or (x $\in$ A and x $\notin$ B)
$\Leftrightarrow$ (x $\in$ A and x $\notin$ B)
$\Leftrightarrow$ x $\in$ A-B

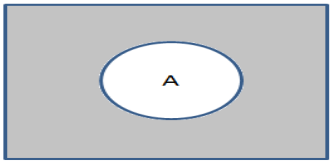
Therefore, A-(A$\cap$B) = A-B

1.5 Venn Diagram

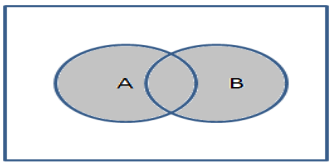
Venn Diagram is a diagram representing mathematical or logical sets pictorially as circles or closed curves within an enclosing rectangle (the universal set), common elements of the sets being represented by intersections of the circles.
The universal set U is represented by a set of points in a rectangle and a subset A of U is represented by a circle or some other closed curve inside the rectangle.



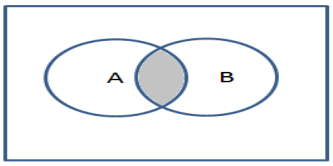
A



A′

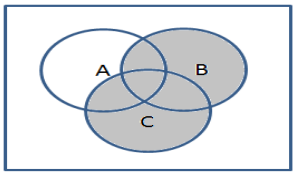


AUB

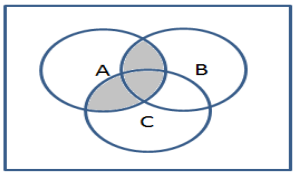


A∩B

Example: Using Venn diagram, show that
(a) A$\cap$(B$\cup$C) = (A$\cap$B) $\cup$ (A$\cap$C)
(b) A$\cup$(B$\cap$C) = (A$\cup$B) $\cap$ (A$\cup$C)
Solution:
(a)
LHS =

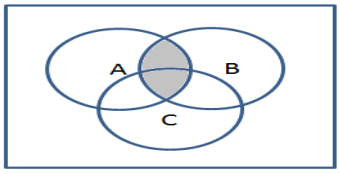


BUC

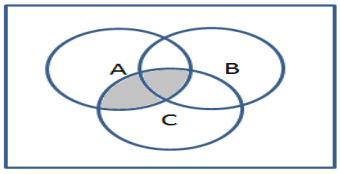


A ∩(BUC)

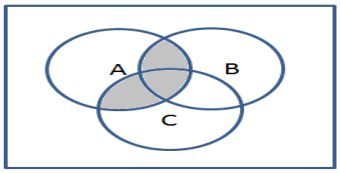
RHS =



A ∩B



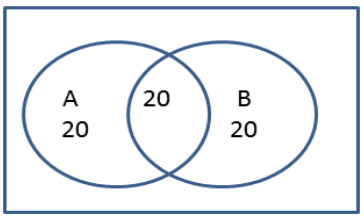
A ∩C



(A ∩B) U (A ∩C)

1.6 Some examples

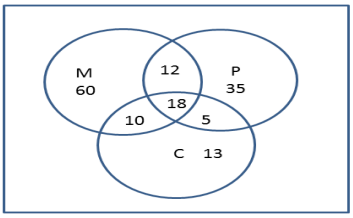
Example: In a group of 60 people, 40 speak Hindi, 20 speak both English and Hindi and all people speak at least one of the two languages. How many people speak only English and not Hindi? How many speak English?
Solution:
Total people = 60
Hindi speaking people = 40
Both English and Hindi speaking = 20
Let A = The set of Hindi speaking people
and B = The set of English speaking people
Therefore, n(A) = 40, n(A∪B) = 60, and n(A∩B) = 20.
Number of people that speak only English and not Hindi is
n(B-A) = n(A∪B)-n(A) = 60-40 = 20
Number of people that speak English is
n(B) = n(A∪B)-n(A) + n(A∩B) = 60-40+20 = 40
By Venn diagram, we can also compute these values.



From above diagram,
Number of people that speak only English and not Hindi = 20
Number of people that speak English = 40

Example: A class has 175 students. In which, the number of students studying subjects are the following:-
Mathematics: 100, Physics: 70, Chemistry: 46; Mathematics and Physics: 30, Mathematics and Chemistry: 28, Physics and Chemistry: 23, Mathematics, Physics and Chemistry: 18. Find the following:-
(1) How many students are enrolled in Mathematics alone; Physics alone and Chemistry

alone.
(2) The number of students who have not offered any of these subjects.
Solution:
Total students = 175
Let M, P, C denote the sets of students enrolled in Mathematics, Physics and Chemistry.
Therefore,
n(M) = 100, n(P) = 70, n(C) = 46, n(M∩P) = 30, n(P∩C) = 23,n(M∩C) = 28, n(M∩$P \cap C$) = 18.
Therefore, n(M∪$P \cup C$) = n(M)+n(P)+n(C)-n(M∩P)-n(P∩C)-n(M∩C)+n(M∩$P \cap C$)
= 100+70+46-30-23-28+18
= 153
(1) Number of students enrolled in Mathematics alone is
n(M)-n(M∩P)-n(M∩C)+ n(M∩$P \cap C$) = 100-30-28+18 = 60
Number of students enrolled in Physics alone is
n(P)-n(M∩P)-n(P∩C)+ n(M∩$P \cap C$) = 70-30-23+18 = 35
Number of students enrolled in Chemistry alone is
n(C)-n(P∩C)-n(M∩C)+ n(M∩$P \cap C$) = 46-23-28+18 = 13
(2) Number of students who have not offered any subjects is
Total students - n(M∪$P \cup C$) = 175 - 153 = 22
By Venn diagram:



From above diagram,
Number of students enrolled in Mathematics alone = 60
Number of students enrolled in Physics alone = 35
Number of students enrolled in Chemistry alone = 13
Number of students who have not offered any subjects = total students - (60+35+13+12+10+5+18)
= 175 - 153 = 22
Example: A total of 1232 student have taken a course in Spanish, 879 have taken a course in French, and 114 have taken a course in Russian. Further, 103 have taken courses in both Spanish and French, 23 have taken courses in both Spanish and Russian, and 14 have taken courses in both French and Russian. If 2092 students have taken at least one of Spanish, French, and Russian, how many students have taken a course in all three languages? AKTU(2018) **Solution:** Let S, F and R denotes the set of students have taken course Spanish, French and Russian. Therefore,
n(S) = 1232, n(F) = 879, n(R) = 114, n(S∩F) = 103, n(S∩R) = 23,n(F∩R) = 14, n(S∪$F \cup R$) = 2092
n(S∪$F \cup R$) = n(S)+n(F)+n(R)-n(S∩F)-n(S∩R)-n(F∩R)+n(S∩$F \cap R$)
2092 = 1232+879+114-103-23-13+n(S∩$F \cap R$)
n(S∩$F \cap R$) = 2231- 2225 = 6
Example: Find the number of integers between 1 and 250 that are not divisible by any of the integers 2, 3, and 5.

Solution: Let A, B and C denotes the set integers between 1 and 250 that are divisible by 2, 3 and 5 respectively. Therefore,

$n(A) = \left\lfloor \frac{250}{2} \right\rfloor = 125$, $n(B) = \left\lfloor \frac{250}{3} \right\rfloor = 83$

$n(C) = \left\lfloor \frac{250}{5} \right\rfloor = 50$, $n(A \cap B) = \left\lfloor \frac{250}{6} \right\rfloor = 41$

$n(A \cap C) = \left\lfloor \frac{250}{10} \right\rfloor = 25$, $n(B \cap C) = \left\lfloor \frac{250}{15} \right\rfloor = 16$

$n(A \cap B \cap C) = \left\lfloor \frac{250}{30} \right\rfloor = 8$

Number of integers divisible by any of 2,3, and 5 is

$= n(A \cup B \cup C)$

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

$= 125+83+50-41-25-16+8 = 266-82 = 184$

Therefore, number of integers not divisible by any of 2,3, and 5 is

= Total integers between 1 and 250 - $n(A \cup B \cup C)$

$= 250-184 = 66$

1.7 Equivalence laws in set theory

(1) Idempotent laws

(a) $A \cup A = A$

(b) $A \cap A = A$

(2) Associative laws

(a) $A \cup (B \cup C) = (A \cup B) \cup C$

(b) $A \cap (B \cap C) = (A \cap B) \cap C$

(3) Commutative laws

(a) $A \cup B = B \cup A$

(b) $A \cap B = B \cup A$

(4) Distributive laws

(a) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

(b) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

(5) Absorption laws

(a) $A \cup (A \cap B) = A$

(b) $A \cap (A \cup B) = A$

(6) Identity laws

(a) $A \cup \phi = A$ (b) $A \cap \phi = \phi$

(c) $A \cup U = U$ (d) $A \cap U = A$

(7) Complement laws

(a) $A \cup A' = U$ (b) $A \cap A' = \phi$

(c) $U' = \phi$ (d) $\phi' = U$

(8) DeMorgan's laws

(a) $(A \cup B)' = A' \cap B'$

(b) $(A \cap B)' = A' \cup B'$

1.8 Partition of a set

Let S be a given set and A = {A_1, A_2, A_3, ..., A_n}, where each A_i, for i = 1,2,3,.....,n, is a subset of S.

A is called the partition of set S if it satisfies the following two conditions:-
(1) $\cup_{i=1}^{n} A_i$ = S
(2) $A_i \cap A_j = \phi$, $\forall$ i,j = 1,2,3,.....,n and i≠j.
Example: Consider set S = { a, b, c, d } and A = {{a, b }, { c, d }}.
In this example, A is the partition of S because

{a, b }∪{ c, d } = S and {a, b }∩{ c, d } = ϕ.

1.9 Multiset

A multiset is an unordered collection of elements, in which the multiplicity of an element may be one or more than one or zero. The multiplicity of an element is the number of times the element repeated in the multiset. In other words, we can say that an element can appear any number of times in a set.
Example:
A = {l, l, m, m, n, n, n, n}
B = {a, a, a, a, a, c}

1.9.1 Operations defined on Multisets

Union of Multisets

The Union of two multisets A and B is a multiset such that the multiplicity of an element is equal to the maximum of the multiplicity of an element in A and B and is denoted by A∪B.
Example:
Let A = {l, l, m, m, n, n, n, n}
B = {l, m, m, m, n},
Therefore, A∪B = {l, l, m, m, m, n, n, n, n}

Intersection of Multisets

The intersection of two multisets A and B, is a multiset such that the multiplicity of an element is equal to the minimum of the multiplicity of an element in A and B and is denoted by A∩B.
Example:
Let A = {l, l, m, n, p, q, q, r}
B = {l, m, m, p, q, r, r, r, r}
Therefore, A∩B = {l, m, p, q, r}

Difference of Multisets

The difference of two multisets A and B, is a multiset such that the multiplicity of an element is equal to the multiplicity of the element in A minus the multiplicity of the element in B if the difference is +ve, and is equal to 0 if the difference is 0 or negative
Example:

Let A = {l, m, m, m, n, n, n, p, p, p}
B = {l, m, m, m, n, r, r, r}
A - B = {n, n, p, p, p}

Sum of Multisets

The sum of two multisets A and B, is a multiset such that the multiplicity of an element is equal to the sum of the multiplicity of an element in A and B **Example:**
Let A = {l, m, n, p, r}
B = {l, l, m, n, n, n, p, r, r}
A + B = {l, l, l, m, m, n, n, n, n, p, p, r, r, r}

1.10 Countable and Uncountable sets

A set is said to be countable if:
(1) It is finite, or
(2) It has the same cardinality (size) as the set of natural numbers.
Equivalently, a set is countable if it has the same cardinality as some subset of the set of natural numbers. Otherwise, it is uncountable.
For example, the set of integers, the set of rational numbers or the set of algebraic numbers are countable set. An uncountable set is the set of real numbers.
For example, the set of real numbers between 0 and 1 is an uncountable set because no matter what, you'll always have at least one number that is not included in the set. This set does not have a one-to-one correspondence with the set of natural numbers.

1.11 Exercise

1. Give another description of the following sets and indicate those which are infinite sets.
   (a) { x ! x is an integer and $5 \leq x \leq 12$}
   (b) { 2, 4, 8, ... }
   (c) All the countries of the world.
2. Given S = { 2, a, { 3 }, 4 } and R = { { a }, 3, 4, 1 }, indicate whether the following are true or false.
   (a) {a} $\in$ S
   (b) {a} $\in$ R
   (c) { a, 4, {3}} $\subseteq$ S
   (d) {{a}, 1, 3, 4 } $\subset$ R
   (e) R = S
   (f) {a} $\subseteq$ S
   (g) {a} $\subseteq$ R
   (h) $\phi \subset$ R

(i) $\phi \subseteq \{\{a\}\} \subseteq R \subseteq U$

(j) $\{\phi\} \subseteq S$

(k) $\{\phi\} \in R$

(l) $\{\phi\} \subseteq \{\{3\}, 4\}$

3. Show that
   $(R \subseteq S) \wedge (S \subset Q) \Rightarrow R \subset Q$
   Is it correct to replace $R \subset Q$ by $R \subseteq Q$? Explain your answer.

4. Determine the power sets of the followings:-

   (a) { a, { b } }

   (b) { 1, ϕ }

   (c) { 1, 2, 3, 4 }

5. What is the power set of the empty set? What is the power set of the set $\{\phi\}$?

6. Find the numbers between 1 to 500 that are not divisible by any of the integers 2 or 3 or 5 or 7. AKTU(2019)

7. Determine whether each of these statements is true or false.

   (a) $0 \in \phi$

   (b) $\phi \in 0$

   (c) $0 \subset \phi$

   (d) $\phi \subset 0$

   (e) $0 \in 0$

   (f) $0 \subset 0$

   (g) $\phi \subseteq \phi$

1.12 Ordered pairs and Cartesian products

1.12.1 Ordered pair

An ordered pair consists of two objects in a given fixed order. An ordered pair is not a set of two elements. The ordering of two objects is important. We denote ordered pair by (x,y).

The equality of two ordered pairs is defined by (x,y) = (u,v) $\Leftrightarrow$ x=u and y=v.

1.12.2 Cartesian products

Let A and B be any two sets. The set of all ordered pairs such that the first member of the ordered pair is an element of A and the second member is an element of B, is called the Cartesian product of A and B. It is denoted by A×B.

Mathematically, it is defined as

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

Example If A = {a, b} and B = { 1, 2 ,3}, then find A×B, B×A, A×A, B×B, and

(A×B)∩(B×A).
Solution:
A×B = { (a,1),(a,2),(a,3),(b,1),(b,2),(b,3)}
B×A = { (1,a),(1,b),(2,a),2,b),(3,a),(3,b)}
A×A = { (a,a),(a,b),(b,a),(b,b)}
B×B = { (1,1),(1,2),(1,3),(2,1),(2,2),(2,3),(3,1),(3,2),(3,3)}
(A×B)∩(B×A) = ϕ
Example If A = ϕ and B = { 1, 2 ,3}, then what are A×B, B×A?
Solution: A×B = ϕ and B×A = ϕ
Example Prove that
(a) A×(B∪C) = (A×B)∪(A×C)
(b) A×(B∩C) = (A×B)∩(A×C)
Solution:
(a) A×(B∪C) = {(x,y) ! x ∈ A and y ∈ (B∪C) }
= {(x,y) ! x ∈ A and (y ∈ B or y ∈ C) }
= {(x,y) ! (x ∈ A and y ∈ B) or (x ∈ A and y ∈ C) }
= {(x,y) ! (x,y) ∈ A×B or (x,y) ∈ A×C }
= {(x,y) ! (x,y) ∈ (A×B)∪(A×C) }
= (A×B)∪(A×C)
Therefore, A×(B∪C) = (A×B)∪(A×C).
(b) A×(B∩C) = {(x,y) ! x ∈ A and y ∈ (B∩C) }
= {(x,y) ! x ∈ A and (y ∈ B and y ∈ C) }
= {(x,y) ! (x ∈ A and y ∈ B) and (x ∈ A and y ∈ C) }
= {(x,y) ! (x,y) ∈ A×B and (x,y) ∈ A×C }
= {(x,y) ! (x,y) ∈ (A×B)∩(A×C) }
= (A×B)∩(A×C)
Therefore, A×(B∩C) = (A×B)∩(A×C).

1.13 Exercise

1. Determine the following:-
   (a) $\phi \cap \{\phi\}$
   (b) $\{\phi\} \cap \{\phi\}$
   (c) $\{\phi, \{\phi\}\} - \phi$
2. Determine A×B×C, B^2, A^3, $B^2 \times A$, where A = {1}, B = {a, b} and C = {2, 3}.
3. Prove that
   (a) (A∩B)∪(A∩B') = A
   (b) A∩(A'∪B) = A∩B
4. Show that (A∩B)∪C = A∩(B∪C) iff C ⊆ A
5. Draw Venn diagram for the following:-
   (a) B'

(b) (A∪B)'

(c) B-A'

(d) A'∪B

(e) A'∩B

6. Show that

   (a) (A-B)-C = (A-C)-(B-C)

   (b) (A∩B)×(C∩D) = (A×C)∩(B×D)

7. Let A and B be sets. Show that A×B ≠ B×A. Under what condition A×B = B×A?

Chapter 2

Relation

2.1 Relation

2.1.1 Definition

A relation is defined as the subset of Cartesian product. That is, if R is a relation defined from the set A to B, then

$$R \subseteq A \times B$$

Mathematically, R = {(x,y) ! x ∈ A and y ∈ B}
Element a related b by relation R if (a,b)∈ R. It is denoted by aRb.

2.1.2 Examples

1. R = {(x,y) ! x is the father of y}
2. R = {(a,2), (b,2), (c,3)}
3. Let A = {a, b, c, d}. Some relations R defined on set A are:
   (a) R = A×A
   (b) R = {(a, a), (b, b), (c, c), (d, d), (a, b), (a, c), (b, c)}
   (c) R = {(a, a), (b, b), (c, c)}
   (d) R = {(a, a), (b, b), (a, b), (b, a), (c, d)}
   (e) R = {(a, a), (a, c), (c, a), (a, b), (b, a), (c, c), (b, b)}

Note: Consider set A and B with m and n number of elements respectively. The number of relations which can be defined from set A to B will be 2^{mn}.

2.1.3 Domain of a relation

Domain of a relation R is the set of first element of all the ordered pairs belong into the relation R. Mathematically, it is defined as

Domain(R) = { a ! ∃ b, such that (a,b) ∈ R}

2.1.4 Range of a relation

Range of a relation R is the set of second element of all the ordered pairs belong into the relation R. Mathematically, it is defined as

Range(R) = { b ! ∃ a, such that (a,b) ∈ R}

2.2 Types of relation

2.2.1 Universal relation

A relation R defined from A to B is said to be universal relation if it contains all the ordered pairs defined from set A to B. That is, if R = A×B, then R is said to be universal set.

2.2.2 Void relation

If R does not contain any ordered pair, then it is said to be void or empty relation. That is, if R = ϕ then R is said to be empty relation.

2.2.3 Identity relation

A relation R defined on set A is said to be identity relation if
R = {(a,a) ! for all a ∈ A}

2.2.4 Inverse relation

A relation R' is said to be inverse relation of R defined on set A if
R' = {(a,b) ! (b,a) ∈ R}

2.3 Properties of binary relations in a set

There are following properties of which can be defined on a set. Consider the set is A.

2.3.1 Reflexive property

A binary relation R defined on set A is said to be satisfies reflexive property if every element of set A is related to itself. That is, aRa , ∀ a ∈ A. That is, (a,a) ∈ R, ∀ a ∈ A.

2.3.2 Symmetric property

A binary relation R defined on set A is said to be satisfies symmetric property if (a,b) ∈ R then (b,a) ∈ R, ∀ a,b ∈ A. That is, if aRb then bRa, ∀ a,b ∈ A.

2.3.3 Transitive property

A binary relation R defined on set A is said to be satisfies transitive property if (a,b) ∈ R and (b,c) ∈ R then (a,c) ∈ R, ∀ a,b,c ∈ A.

2.3.4 Irreflexive property

A binary relation R defined on set A is said to be satisfies irreflexive property if no element of set A is related to itself. That is, (a,a) $\notin$ R, $\forall$ a $\in$ A.

2.3.5 Anti-symmetric property

A binary relation R defined on set A is said to be satisfies anti-symmetric property if (a,b) $\in$ R and (b,a) $\in$ R then a=b, $\forall$ a,b $\in$ A.

2.3.6 Asymmetric property

A binary relation R defined on set A is said to be satisfies asymmetric property if (a,b) $\in$ R then (b,a) $\notin$ R, $\forall$ a,b $\in$ A.

Note: A relation which satisfies reflexive property is said to be reflexive relation. A relation which satisfies symmetric property is said to be symmetric relation. A relation which satisfies transitive property is said to be transitive relation. A relation which satisfies irreflexive property is said to be irreflexive relation. A relation which satisfies anti-symmetric property is said to be anti-symmetric relation. A relation which satisfies asymmetric property is said to be asymmetric relation.

Example: Consider the following relations defined on set A = {1,2,3,4}. Find out which of these satisfies which of the above properties i.e. reflexive, symmetric, transitive, irreflexive, anti-symmetric, and asymmetric.

1. {(2,2),(2,3),(2,4),(3,2),(3,3),(3,4)}
2. {(1,1),(2,2),(2,1),(1,2),(3,3),(4,4)}
3. {(2,4),(4,2)}
4. {(1,2),(2,3),(3,4)}
5. {(1,1),(2,2),(3,3),(4,4)}
6. {(1,3),(1,4),(2,3),(2,4),(3,1),(3,4)}

Solution:

1. Transitive.
2. Reflexive, symmetric, transitive.
3. Symmetric, irreflexive.
4. Irreflexive, anti-symmetric, asymmetric.
5. Reflexive, symmetric, transitive, anti-symmetric.
6. Irreflexive.

Example: Give an example of a relation which satisfies corresponding properties.

1. Neither reflexive nor irreflexive.

2. Both symmetric and anti-symmetric.

3. Reflexive, transitive but not symmetric.

4. Symmetric, transitive but not reflexive.

5. Reflexive, symmetric but not transitive.

6. Reflexive, transitive but neither symmetric nor anti-symmetric.

Example: Which of the following relations are transitive?
$R_1 = \{(1,1)\}$, $R_2 = \{(1,2),(2,2)\}$, $R_3 = \{(1,2),(2,3),(1,3),(2,1)\}$ **solution:** R_1 and R_2 are transitive but R_3 is not transitive. R_3 is not transitive because for pairs (1,2) and (2,1), its transitie Pair (1,1) not belong into R_3.

Example: Given S = {1,2,3,4}, and a relation R on S defined by
R = {(1,2),(4,3),(2,2),(2,1),(3,1)}
Show that R is not transitive. Find a relation $R_1 \supseteq R$ such that R_1 is transitive. Can you find another relation $R_2 \supseteq R$ which is also transitive?

Example: Given S = {1,2,3,.....,10}, and a relation R on S defined by
R = { (a,b) ! a+b = 10}
Which of the properties of a relation satisfy R?

Example: If R and S are both reflexive then show that R∪S and R∩S are also reflexive.
Solution: Since R and s are reflexive, therefore (a,a) ∈ R and (a,a) ∈ S, ∀ a. Since (a,a) ∈ R and (a,a) ∈ S, ∀ a, therefore (a,a) ∈ R∪S and (a,a) ∈ R∩S, ∀ a. Therefore, R∪S and R∩S are also reflexive.

Example: If R and S are both reflexive, symmetric, and transitive then show that R∪S and R∩S are also reflexive, symmetric, and transitive.
Solution:
For reflexive Since R and s are reflexive, therefore (a,a) ∈ R and (a,a) ∈ S, ∀ a. Since (a,a) ∈ R and (a,a) ∈ S, ∀ a, therefore (a,a) ∈ R∩S, ∀ a. Therefore, R∩S is also reflexive.
For symmetric Since R is symmetric, therefore if (a,b) ∈ R then (b,a) ∈ R. Similarly, since S is symmetric, therefore if (a,b) ∈ S then (b,a) ∈ S.
Let (a,b) ∈ R∩S. It imply that (a,b) ∈ R and (a,b) ∈ S. Since R and s are symmetric therefore (b,a) ∈ R and (b,a) ∈ S. It imply that (b,a) ∈ R∩S. Therefore R∩S is symmetric.
For transitive
Let (a,b) and (b,c) ∈ R∩S. ⇒ (a,b) and (b,c) ∈ R and (a,b) and (b,c) ∈ S
⇒ (a,c) ∈ R and (a,c) ∈ S (Since R and S are transitive)
⇒ (a,c) ∈ R∩S.
Therefore, R∩S is also transitive.

2.4 Equivalence relation

2.4.1 Definition

A relation R defined on set A is said to be an equivalence relation if it satisfies reflexive, symmetric, and transitive properties.

2.4.2 Some examples

Example: Let A = {1,2,3,4} and R = {(1,1),(1,4),(4,1),(4,4),(2,2),(2,3),(3,2),(3,3)}. Is this relation an equivalence relation?
Solution: Since (1,1),(2,2),(3,3), and (4,4) are belongs into R, therefore R is reflexive.
Clearly in R if (a,b) $\in$ R then (b,a) $\in$ R. Here both (1,4) and (4,1) $\in$ R and both (3,2) and (2,3) $\in$ R. Therefore R is symmetric.
Clearly in R if (a,b) $\in$ R and (b,c) $\in$ R then (a,c) $\in$ R. Here, for pair (1,4) and (4,1), its transitive pair (1,1) and (4,4) are also belong into R. Similarly, or pair (2,3) and (3,2), its transitive pair (2,2) and (3,3) are also belong into R. Therefore R is transitive.
Clearly, R satisfies all the three properties. Therefore, R is an equivalence relation.

Example: Let A = {1,2,3,4,5,6} and R = {(a,b) ! (a-b) is divisible by 3 }. Show that R is an equivalence relation.
Solution: In this example R will be

R = {(1,1),(2,2),(3,3),(4,4),(5,5),(6,6),(1,4),(4,1),(2,5),(5,2),(3,6),(6,3)}

Clearly R satisfies reflexive, symmetric and transitive, therefore R is an equivalence relation.

Example: Let S be the set of lines on a plane. Define a relation R on set S as following:- aRb if line a is parallel to line b, $\forall$ a,b $\in$ S. Is relation R an equivalence relation.
Solution: Since each line in a plane is parallel to itself, therefore R satisfies reflexive property.
We know that if line a is parallel to line b then line b is also parallel to line a. Therefore R satisfies symmetric property.
We know that if line a is parallel to line b and line b is parallel to line c, then line a is also parallel to line c. Therefore R satisfies transitive property.
Since R satisfies all the three properties, therefore R is an equivalence relation.

2.4.3 Exercise

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

2. Given a set S = {1,2, 3, 4,5}. Find the equivalence relation defined on S which generates the partition { $\overline{1,2}, \overline{3}, \overline{4,5}$ }.

3. Prove that the relation "congruence modulo m" defined as
   $\cong$ = { (a,b) ! (a-b) is divisible by m }
   over the set of positive integers is an equivalence relation. Show that if a $\cong$ b and c $\cong$ d, then (a+c) $\cong$ (b+d).

4. Let R_1 be a relation defined on R, the set of real numbers, such that R_1 = {(x,y) ! $|x - y| < 1$ }. Is R_1 an equivalence relation ? Justify. AKTU(2019)

5. Let R be a binary relation on the set of all positive integers such that:
   R = {(a,b) ! a-b is an odd positive integers}
   Is R reflexive ? Symmetric? Transitive?

2.5 Equivalence class

Let R is an equivalence relation defined on set S. For any a $\in$ S, the equivalence class of a is the set of all the elements of set S which are related from a. It is denoted by [a]. Mathematically it is defined as [a] = { b $\in$ S ! aRb i.e. (a,b) $\in$ R}.

Example: Let Z be the set of integers and let R be the relation called " Congruence modulo 3 ". Determine the equivalence classes generated by the elements of Z. That is, R = { (a,b) ! a,b $\in$ Z and (a-b) is divisible by 3 }.
Solution: The equivalence classes for this relation are the followings:-
[0] = {.....,-12,-9,-6,-3,0,3,6,9,12,.....}
[1] = {.....,-11,-8,-5,-2,1,4,7,10,13,.....}
[2] = {.....,-10,-7,-4,-1,2,5,8,11,14,.....}

2.6 Matrix and Graph representation of the relations

2.6.1 Matrix representation

Let A = $\{a_1, a_2, ..., a_m\}$, B = $\{b_1, b_2, ..., b_n\}$, and R be a relation from A to B. Then the relation matrix corresponding to relation R will be m×n order matrix. Let this matrix is M. Then

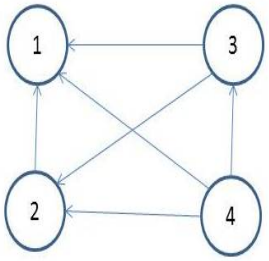
$$D_{it} = \begin{cases} 1 & \text{if } (a_i, b_j) \in R \\ 0 & \text{if } (a_i, b_j) \notin R \end{cases} \tag{2.1}$$

where m_{ij} is the element of matrix in i^{th} row and in j^{th} column.
Example: Consider a relation R = $\{(a_1, b_1), (a_2, b_1), (a_3, b_2), (a_2, b_2)\}$, and A = $\{a_1, a_2, a_3\}$, B = $\{b_1, b_2\}$. Find the relation matrix for R.
Solution:

	b_1	b_2
a_1	1	0
a_2	1	1
a_3	0	1

2.6.2 Graph representation

Let R be a relation defined in a set A = $\{a_1, a_2, ..., a_m\}$. The nodes in the graph corresponds to the elements in set a. Therefore, the number of nodes in the graph will be equal to number of elements in the set A. This graph will be directed graph. If $(a_i, a_j) \in$ R, then the directed edge will be from a_i to a_j in the graph.
Example: Let A = {1,2,3,4} and R = {(a,b) ! a > b}. Draw the graph of R and also give its matrix.
Solution:



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

2.7 Composition of binary relations

Let R be a relation from A to B and S be a relation from B to C. Then a relation RoS is called composition of relation R and S. It is defined as:-

RoS = {(a,c) ! a ∈ A and c ∈ C and ∃ b ∈ B such that (a,b) ∈ R and (b,c) ∈ S }

Example: Let R = {(1,2),(3,4),(2,2)} and S = {(4,2),(2,5),(3,1),(1,3)}. Find RoS, SoR and Ro(SoR).
Solution:
RoS = {(1,5),(3,2),(2,5)}
SoR = {(4,2),(3,2),(1,4)}
Ro(SoR) = {(3,2)}

Example: Let R and S be two relations on a set of positive integers I such that R = {(a, 2a) ! a ∈ I } and S = {(a, 7a) ! a ∈ I }. Find RoS, RoR, RoRoR and RoSoR.
Solution:
RoS = {(a,14a) ! a ∈ I }
RoR = {(a,4a) ! a ∈ I }
RoRoR = {(a,8a) ! a ∈ I }
RoSoR = {(a,28a) ! a ∈ I }

2.8 Closure of a relation

Consider R be relation defined on a set S.

2.8.1 Reflexive closure

The reflexive closure of a relation R is the smallest reflexive relation that contains R as a subset. It is denoted by r(R). Mathematically, it is defined as :-
r(R) = R$\cup I_S$
Where I_S is the identity relation defined on set S.

2.8.2 Symmetric closure

The symmetric closure of a relation R is the smallest symmetric relation that contains R as a subset. It is denoted by s(R). Mathematically, it is defined as :-
s(R) = R$\cup R^{-1}$
Where R^{-1} is the inverse relation of R.

2.8.3 Transitive closure

The transitive closure of a relation R is the smallest transitive relation that contains R as a subset. It is denoted by t(R). **Example:** Let S= {1,2,3,4}. Consider the following relation defined on the set S:-
R = { (1,1),(2,2),(1,2),(1,3),(3,1),(4,2)}
Find reflexive, symmetric and transitive closure of R.
Solution:
Reflexive closure r(R) = R $\cup$ I_S
= { (1,1),(2,2),(1,2),(1,3),(3,1),(4,2)}$\cup$ { (1,1),(2,2),(3,3),(4,4)}
= { (1,1),(2,2),(1,2),(1,3),(3,1),(4,2),(3,3),(4,4)}
Symmetric closure s(R) = R $\cup R^{-1}$
= { (1,1),(2,2),(1,2),(1,3),(3,1),(4,2)}$\cup${ (1,1),(2,2),(2,1),(1,3),(3,1),(2,4)}
= { (1,1),(2,2),(1,2),(2,1),(1,3),(3,1),(4,2),(2,4)}
Transitive closure t(R) = R $\cup$ The set of ordered pairs to satisfy the transitive property
= { (1,1),(2,2),(1,2),(1,3),(3,1),(4,2)}$\cup$ { (3,3),(3,2)}
= { (1,1),(2,2),(1,2),(1,3),(3,1),(4,2),(3,3),(3,2)}

Example: How many reflexive relations are defined on the set with n elements? AKTU(2019)
Solution: According to reflexive property, each reflexive relation contains all the pairs like (a,a), where a belongs into the set. Total number of ordered pairs defined in the set with n elements is n^2. The number of ordered pairs like (a,a) will be n. Therefore, the remaining elements like (a,b) and a$\neq$b will be n^2 - n. Since the relation is a subset of set of ordered pairs, therefore total number of reflexive relations will be $2^{(n^2-n)}$.

Example: How many symmetric relations are defined on the set with n elements? AKTU(2019)
Solution: Consider the set is S with n elements. Relation is defined on the set S. The total number of relations defined on set S will be n^2, because relation is the subset of S$\times$S.
Now, if relation satisfies the symmetric property, then (a,b) and (b,a) belongs into the relation together. Therefore, the set whose all the subsets are reflexive relation contains $\frac{(n^2-n)}{2} + n = \frac{(n^2+n)}{2}$. Here, n is the number of ordered pairs like (a,a).

Therefore the total number of symmetric relations = $2^{\frac{(n^2+n)}{2}}$.

Example: How many anti-symmetric relations are defined on the set with n elements?
Solution: Consider the set is S with n elements. Relation is defined on the set S. The total number of relations defined on set S will be n^2, because relation is the subset of S×S.
The total number of ordered pairs related to itself = n. Clearly, all the subsets of these ordered pairs are anti-symmetric. Therefore, the total anti-symmetric relations defined on these ordered pairs = 2^n.
The remaining ordered pairs which are not related to itself = $n^2 - n$
Since both (a,b) and (b,a) can not belong into any anti-symmetric relations, Therefore, we consider only orederd pair = $\frac{(n^2-n)}{2}$.
Therefore, there are three possibilities for ordered pairs (a,b) and (b,a).
First possibility: (a,b) and (b,a) both not belong.
Second possibility: (a,b) belong but (b,a) not belong.
Third possibility: (a,b) not belong but (b,a) belong.
Therefore, total number of anti-symmetric relations for these types of ordered pairs = $3^{\frac{(n^2-n)}{2}}$.
Therefore, total number of anti-symmetric relations for the set S = $2^n * 3^{\frac{(n^2-n)}{2}}$.

2.9 Exercise

1. Is the "divides" relation on the set of positive integers transitive? What is the reflexive and symmetric closure of the relation R = {(a, b) — a > b} on the set of positive integers? AKTU(2019)

Chapter 3

Function

3.1 Function

3.1.1 Definition

Let X and Y are any two sets. A relation f from X to Y is called a function if for every x∈X, there is a unique element y∈Y such that (x,y) ∈ f. It is denoted by f: X→Y.

3.1.2 Some examples

example: Let X = {1,2,3,4} and Y = {x,y,w,z} and f = {(1,x), (2,y),(3,w),(4,x)}. Is f a function?
Solution: Clearly in function f, each element of set X has an image in set Y and that image has an unique. Therefore, f is a function.

example: Let X = Y = R. Also let, f = { (x, x^2) ! x∈R } and g = { (x^2, x) ! x∈R }. Find out f and g is functions or not.
Solution: Here R is a set of real numbers. Clearly for f, each real number has a unique square because square of 2 is 4, 3 is 9, 4 is 16 etc. Therefore, f is a function.
For relation g, element 4 has two images 2 and -2. Similarly, 9 has two images 3 and -3. Therefore, g is not a function.

3.1.3 Domain, Range, and Co-domain

Consider a function f : X→Y.
Domain of a function f is X. Co-domain of function f is Y. And range of f will be the set of second elements of all the ordered pairs in f i.e. range ⊆ Y.

3.2 Types of function

3.2.1 Onto function (Surjective function)

A function f: X→Y is said to be onto function if every element of Y is the image of some element of X. That is, if range(f) = Y, then f is onto.

3.2.2 Into function

A function f: X→Y is said to be into function iff there exists at least one element in Y which is not the image of any element in X. That is, range(f) $\subset$ Y.

3.2.3 One-one function (Injective function)

A function f: X→Y is said to be one-one function if for all elements x_1, x_2 in X such that f(x_1) = f(x_2) then $x_1 = x_2$.

3.2.4 Many-one function

A function f: X→Y is said to be many-one function iff two or more elements of X have same image in Y.

3.2.5 Bijective function)

A function f: X→Y is said to be bijective function if f is both one-one and onto.

3.2.6 Exercise

1. Let N be the set of natural numbers including zero. Determine which of the following functions are one-one, onto and bijective.

   (a) f: N→N, f(j) = j^2+2

   (b) f: N→N, f(j) = j mod 3

   (c) f: N→N, f(j) = 1 , if j is odd
   = 0 , if j is even

   (d) f: N→{0,1}, f(j) = 0 , if j is odd
   = 1 , if j is even

2. Let I be the set of integers, I_+ the set of positive integers, and I_p = {0,1,2,3,. . . . . ,(p-1)}. Determine which of the following functions are one-one, onto and bijective.

   (a) f: I→I, f(j) = (j-1)/2 , if j is odd
   = j/2 , if j is even

   (b) f: $I_+ \to I_+$, f(x) = greatest integer $\leq \sqrt{(x)}$

   (c) $I_7 \to I_7$, f(x) = 3x mod 7

   (d) $I_4 \to I_4$, f(x) = 3x mod 4

3. List all possible functions from X = {a,b,c} to Y = {0,1} and indicate in each case whether the function is one-one, onto and bijective.

4. Show that the functions f and g which both are from N×N to N given by f(x,y) = x+y and g(x,y) = xy are onto but not one-one.

3.2.7 Composition of functions

Let f: X→Y and g: Y→Z be two functions. Then composition of f and g is denoted by gof. It is defined as gof : X →Z.
(gof)(x) = g(f(x))
Note: gof ≠ fog.

Example: Let X ={1,2,3}, Y = {p,q}, and Z = {a,b}. Also let f is a function from X to Y such that f = {(1,p), (2,p), (3,q)} and g is a function from Y to Z such that g = {(p,b), (q,b)}. Find gof.
Solution: gof = { (1,b), (2,b), (3,b)}

Example: Let X ={1,2,3}, and f, g, h and s be functions from X to X given by
f = {(1,2),(2,3),(3,1)}, g = {(1,2), (2,1), (3,3)}, h = {(1,1), (2,2), (3,1)}, and s = {(1,1), (2,2),(3,3)}
Find fog, gof, fohog, sog, gos, sos and fos.
Solution:
fog = {((1,3),(2,2),(3,1)}
gof = {((1,1),(2,3),(3,2)}
fohog = {((1,1),(2,2),(3,2)}
Similarly, we can calculate others.

Example: Let f(x) = x+2, g(x) = x-2, and h(x) = 3x, ∀ x∈ R, where R is the set of real numbers. Find gof, fog, fof, hog and fohog.
Solution:
gof(x) = g(f(x)) = g(x+2) = x+2-2 = x
fog(x) = f(g(x)) = f(x-2) = x-2+2 = x
fohog(x) = f(h(g(x))) = f(h(x-2)) = f(3(x-2)) = 3(x-2)+2 = 3x-4
Similarly, we can calculate others.

Example: Let f: R→R be given by f(x) = -x^2 and g: $R_+ \to R_+$ be given by g(x) = $\sqrt{(x)}$, where R_+ is the set of positive real numbers and R is the set of real numbers. Find fog. Is gof defined?
Solution:
fog(x) = f(g(x)) = f($\sqrt{(x)}$) = -($\sqrt{(x)}$)^2 = -x
gof can not be defined because square root of negative real number can not be a real number.

3.2.8 Inverse function

Let f: X→Y is a function. If f is a bijective function then we can define the inverse function of f. It is denoted by f^{-1}. It is defined as f^{-1}: Y→ X. If f(a) = b then f^{-1}(b) = a.

Example: Let X = {1,2,3} and Y = {p,q,r}. f: X→ Y be given by
f = {(1,p), (2,q), (3,q)}
Is inverse of this function possible?
Solution: Inverse of this function is not possible because this function is not bijective. This function is not bijective because f is not onto function.

Example: Let R be the set of real numbers and let f: R→ R be given by
f = {(x, x^2) ! x ∈ R}
Is inverse of this function possible?
Solution: Inverse of this function is not possible because this function is not bijective. This function is not bijective because f is not onto function.
Example: Let R be the set of real numbers and let f: R→ R be given by
f = {(x, x+2) ! x ∈ R}
Is inverse of this function possible?
Solution: Inverse of this function is possible because this function is bijective.

3.2.9 Identity function

A function I_X: X→ X is called an identity function if I_X(x) = x, ∀ x ∈ X.

3.2.10 Invertible function

A function f is said to be invertible function if there exists an inverse function of this function.

Note: (1) If f: X→Y is invertible then $f^{-1}$of = I_X and fof^{-1} = I_Y
(2) Let f: X→ Y and g: Y→ X are two functions. The function g is equal to f^{-1} only if gof = I_X and fog = I_Y.

Example: Show that the functions f(x) = x^3 and g(x) = $x^{1/3}$, for x ∈ R are inverses of one another.
Solution: These functions will be inverse of each other if gof = I = fog.
gof(x) = g(f(x)) = g(x^3) = $(x^3)^{1/3}$ = $x^{3/3}$ = x = I(x).
fog(x) = f(g(x)) = f($x^{1/3}$) = $(x^{1/3})^3$ = $x^{3/3}$ = x = I(x).
Therefore these functions are inverses of each others.

Example: Let F_X be the set of all bijective functions from X to X, where X = {1,2,3}. Find all the elements of F_X and also find the inverse of each element.
Solution: Since the number of elements in set X is 3, therefore the number of bijective functions will be 3! = 6. These functions are:-
f_1 = {(1,1),(2,2),(3,3)} f_2 = {(1,1),(2,3),(3,2)}
f_3 = {(1,2),(2,1),(3,3)} f_4 = {(1,2),(2,3),(3,1)}
f_5 = {(1,3),(2,2),(3,1)} f_6 = {(1,3),(2,1),(3,2)}
Inverse of these functions is determined by interchanging values in each ordered pairs of corresponding functions.

Note: If a set X has n elements, then the number of bijective functions from X to X is n!.

3.2.11 Exercise

1. Let f: R →R and g: R →R are two functions such that f(x) = x^2 – 2 and g(x) = x+4, where R is the set real numbers. Find fog and gof. State whetheher these

functions are injective, surjective and bijective.

2. If f: X →Y and g: Y→ Z and both f and g are onto, show that gof is also onto. Is gof one-one if both g and f are one-one?
3. Let f: R →R be given by f(x) = x^2-2. Find f^{-1}.
4. How many functions are there from X to Y for the sets given below? Find also the number of functions which are one-one, onto and bijective.
   (a) X = {1,2,3}, Y = {1,2,3}
   (b) X = {1,2,3,4}, Y = {1,2,3}
   (c) X = {1,2,3}, Y = {1,2,3,4}
   (d) X = {1,2,3,4,5}, Y = {1,2,3}
   (e) X = {1,2,3}, Y = {1,2,3,4,5}
5. Let X = {1,2,3,4}. Define a function f: X →X such that f≠ I_X an is one-one. Find f^2, f^3, f^{-1} and fof^{-1}. Can you find another one-one function g: X →X such that g ≠ I_X but gog = I_X?
6. Let f: X→Y and X=Y=R, the set of real numbers. Find f^{-1} if
   (a) f(x) = x^2
   (b) f(x) = $\frac{(2x-1)}{5}$
7. Let f and g be the functions from the set of integers to the set of integers defined by f (x) = 2x + 3 and g(x) = 3x + 2. What is the composition of f and g? What is the composition of g and f?

3.3 Peano's Axioms and Principle of Mathematical Induction

3.3.1 Peano's Axioms

These axioms are
(1) 0 ∈ N (where 0 = ϕ)
(2) If n ∈ N, then n^+ ∈ N, where n^+ = n∪{n}
(3) If a subset S ⊆ N possesses the properties
   (a) 0 ∈ S, and
   (b) If n ∈ S, then n^+ ∈ S
Then S = N.

3.3.2 Principle of Mathematical Induction

Definition

Mathematical Induction is a mathematical technique which is used to prove a statement, a formula or a theorem is true for every natural number.

The technique involves two steps to prove a statement, as stated below:-
Step 1(Base step): It proves that a statement is true for the initial value.
Step 2(Inductive step): It proves that if the statement is true for the number n, then it is also true for the number n+1.

Some examples

Example: Show that n $< 2^n$, by principle of induction method.
Solution:
Base step: For n = 0.
$0 < 2^0 \Leftrightarrow 0 < 1$
This is true. Therefore, the given statement is true for n = 0.
Now, for n=1.
$1 < 2^1 \Leftrightarrow 1 < 2$
This is true. Therefore, the given statement is also true for n = 1.
Therefore, the statement is true for base step.
Inductive Step: Now suppose the statement is true for n=k. We shall prove it for n=k+1.
Since statement is true for n=k, therefore k $< 2^k$ .....(1)
For n = k+1.

$$\begin{aligned} k+1 &< 2^k + 1 && \text{Using equation (1)} \\ &< 2^k + 2^k \\ &= 2.2^k \\ &= 2^{k+1} \end{aligned}$$

Therefore, k+1 $< 2^{k+1}$.
Therefore, statement is also true for inductive step.
Hence the given statement is proved.

Example: Show that $2^n <$ n!, $\forall$ n ≥ 4 by principle of induction method.
Solution:
Base step: For n = 4.
$2^0 < 4! \Leftrightarrow 16 < 24$
This is true. Therefore, the given statement is true for n = 4.
Now, for n=5.
$2^5 < 5! \Leftrightarrow 32 < 120$
This is true. Therefore, the given statement is also true for n = 5.
Therefore, the statement is true for base step.
Inductive Step: Now suppose the statement is true for n=k. We shall prove it for n=k+1.
Since statement is true for n=k, therefore $2^k <$k! .....(1)
For n = k+1.

$$\begin{aligned} 2^{k+1} &= 2.2^k \\ &< 2.k! && \text{Using equation (1)} \\ &< (k+1).k! \\ &= (k+1)! \end{aligned}$$

Therefore $2^{k+1} <$ (k+1)!
Therefore, statement is also true for inductive step.
Hence the given statement is proved.

Example: Show that n^3 + 2n is divisible by 3, by principle of induction method.
Solution:
Base step: For n = 1.
n^3 + 2n = 1^3 + 2x1 = 1+2 = 3
Clearly n^3 + 2n is divisible by 3, therefore it is true for n = 1.
For n = 2.
n^3 + 2n = 2^3 + 2x2 = 8+4 = 12
Clearly n^3 + 2n is divisible by 3. Therefore it is also true for n = 2.
Therefore, the statement is true for base step.
Inductive Step: Now suppose the statement is true for n = k. We shall prove it for n = k+1.
Since statement is true for n = k, therefore k^3 + 2k is divisible by 3. It can be written as k^3 + 2k = 3m. . . ..(1)
For n = k+1.

$$\begin{aligned}(k+1)^3 + 2(\text{k+1}) &= k^3 + 3k^2 + 3k + 1 + 2(k+1) \\ &= (k^3 + 2k) + 3(k^2 + k + 1) \\ &= 3\text{m} + 3(k^2 + k + 1) \qquad \text{Using equation (1)} \\ &= 3(\text{m} + (k^2 + k + 1)\ )\end{aligned}$$

Clearly it is divisible by 3. Therefore it is also true for n = (k+1).
Therefore, statement is also true for inductive step.
Hence the given statement is proved.

Exercise

1. Show that S(n) = 1+2+3+.....+n = $\frac{n(n+1)}{2}$
2. Prove that $\frac{1}{1.2} + \frac{1}{2.3} + \frac{1}{3.4} + \ldots\ldots\ldots\ldots\ldots + \frac{1}{n.(n+1)} = \frac{n}{(n+1)}$
3. Show that 2+2^2+2^3+.....+ 2^n = 2^{n+1} - 2
4. Show that 3^n - 1 is a multiple of 2, for n = 1, 2, 3,.....
5. Show that 1+3+5+.....+(2n - 1) = n^2, for n = 1,2, 3, ...
6. Prove that $\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \ldots\ldots\ldots\ldots\ldots + \frac{1}{\sqrt{n}} > \sqrt{n}$, for n $\geq$ 2 using principle of mathematical induction. AKTU(2019)
7. Prove by using mathematical induction that
   7+77+777+.....+777.....7 = $\frac{7}{81}[10^{n+1}$ - 9n - 10] $\forall$ n $\in$ N. AKTU(2019)

Chapter 4

Group

4.1 Group

Binary operation
Let G be a non empty set. If f:$G \times G \to$ G, then f is said to be binary operation defined on set G.
Thus, a binary operation on G is a function that assign each ordered pairs of elements of G to an element of G.
Algebraic structure
A non-empty set together with one or more than one binary operations is called an algebraic structure.
Example: (N,+), (Z,+), (R,+) and (R,+,*) are all the algebraic structures.

4.1.1 Definition of group

An algebraic structure (G,o), where G is a set and o is a binary operator defined on the set G, is called a group if it satisfies following properties:-
(1) Closure property:
For all a,b $\in$ G, aob $\in$ G.
(2) Associative property:
For all a,b,c $\in$ G, ao(boc) = (aob)oc.
(3) Existence of identity property:
For all a $\in$ G, $\exists$ e $\in$ G, such that aoe = eoa = a.
Element e is said to be identity element of the group G.
(4) Existence of inverse property:
For all a $\in$ G, $\exists$ b $\in$ G, such that aob = e = boa.
Element b is said to be inverse of an element a.

4.1.2 Abelian group

A group (G,o) is said to be an abelian group if it satisfies the following property:-
aob = boa, $\forall$ a,b $\in$ G.
Note: If aob = boa, $\forall$ a,b $\in$ G, then this is known as commutative property.

4.1.3 Groupoid

An algebraic structure (G,o) is said to be groupoid if it satisfies only closure property.

4.1.4 Semigroup

An algebraic structure (G,o) is said to be semigroup if it satisfies closure and associative property.

4.1.5 Monoid

An algebraic structure (G,o) is said to be monoid if it satisfies closure, associative and existence of identity property.

4.1.6 Some examples

Example: Is (R,+) a group, where R is a set of real numbers?
Solution: (R,+) will be a group if it satisfies all the four properties of the group.
Closure property
Consider any two real numbers a and b. Clearly a+b will also be a real number. Therefore, (R,+) satisfies closure property.
Associative property
Consider three real numbers 10, 15, 2/3.
10+(20+(2/3)) = 10+(62/3) = 92/3.
(10+20)+2/3 = 30+2/3 = 92/3. Clearly, 10+(20+(2/3)) = (10+20)+2/3. Therefore, a+(b+c) = (a+b)+c, for all a,b,c $\in$ R. Therefore, (R,+) satisfies associative property.
Identity property
Clearly, 0 is a real number such that 0+a = a, $\forall$ a $\in$ R.
Therefore, 0 is the identity element. Therefore, (R,+) satisfies identity property.
Inverse property
Consider an element a $\in$ R. Clearly, a+(-a) = 0, therefore inverse of a is -a. Similarly, for any real number a, -a will be its inverse. Therefore, (R,+) satisfies inverse property.
Since (R,+) satisfies all the four properties of the group, therefore (R,+) is a group.

Example: Is (R',*) a group, where R' = R-{0} ?
Solution:
Closure property
Consider any two non-zero real numbers a and b. Clearly a*b will also be a real number. Therefore, (R',*) satisfies closure property.
Associative property
Consider three real numbers 10, 0.5, 2.
10*(0.5*2) = 10*1 = 10.
(10*0.5)*2 = 5*2 = 10. Clearly, 10*(0.5*2) = (10*0.5)*2 . Therefore, a*(b*c) = (a*b)*c, for all a,b,c $\in$ R'. Therefore, (R',*) satisfies associative property.
Identity property
Clearly, 1 is a real number such that 1*a = a, $\forall$ a $\in$ R'.
Therefore, 1 is the identity element. Therefore, (R',*) satisfies identity property.
Inverse property
Consider an element a $\in$ R'. Clearly, there exists a non-zero real number 1/a such that

a*(1/a) = 1, therefore inverse of a is 1/a. Similarly, for any real number a, 1/a will be its inverse. Therefore, (R',*) satisfies inverse property.
Since (R',*) satisfies all the four properties of the group, therefore (R',*) is a group.

Example: Is $(Z^+,+)$ a group, where Z^+ denotes set of positive integers?
Solution:
Since the sum of any two positive integers is also a positive integers, therefore it satisfies closure property.
Similarly, the sum of any three positive integers in any way will be same. therefore it satisfies associative property.
Since the operation is addition, therefore identity element is 0. Clearly $0 \in Z^+$, therefore it satisfies identity property.
But the inverse of any positive integer a will be -a. and -a $\notin Z^+$. Therefore, inverse property is not satisfied. Hence, $(Z^+,+)$ is not a group.

Example: Prove that the four roots of unity 1, -1, i, , -i form an abelian multiplicative group.
Solution: First we construct composition table of it. The composition table of it is the following:-
From table, all entries in this table are belong into the given set. Therefore, closure

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

property is satisfied.
Clearly, associative operation is also satisfied, because the operation is multiplication.
In the table, row 1 indicate that element 1 is identity element.
Clearly, $(1)^{-1} = 1$, $(-1)^{-1}$ = -1, $(i)^{-1}$ = -i, $(-i)^{-1}$ = i. Since each element has inverse, therefore inverse property is satisfied.
Clearly, a*b = b*a, therefore commutative property is also satisfied. Since all the five properties of abelian group is satisfied, therefore this is a multiplicative group.

Example: Show that the set of all positive rational numbers form an abelian group under the operation defined by aob = (ab)/2.
Solution:
Closure property
Consider any two positive rational numbers a and b.
Since aob = (ab)/2. Clearly (ab)/2 will be a positive rational number. Therefore, it satisfies closure property.
Associative property
Consider three positive rational numbers a, b, c.
ao(boc) = ao(bc/2) = (abc)/4
(aob)oc = ((ab)/2)oc = (abc)/4
Clearly, ao(boc) = (aob)oc, for all a,b,c $\in$ R. Therefore, it satisfies associative property.
Identity property
Let e the identity element. Therefore, aoe = a $\Rightarrow$ (ae)/2 = a $\Rightarrow$ e = 2. Therefore, 2 is

an identity element. Therefore, (it satisfies identity property.
Inverse property
Consider, a is positive rational number. Let b is an inverse of a.
Therefore, aob = e = 2 ⇒ (ab)/2 = 2 ⇒ b = 4/a. Therefore inverse of a is 4/a. Therefore, it satisfies inverse property.
Now, aob = (ab)/2 = (ba)/2 = boa. Therefore, it satisfies commutative property.
Since it satisfies all the five properties of an abelian group, therefore it is an abelian group.

4.1.7 Order of a group

The order of a group(G,o) is the number of elements of G, when G is finite. If G is infinite, then the order will be infinite.
Example: Show that the set {1,2,3,4,5} is not a group under addition and multiplication modulo 6 operation.
Solution: The composition tables under addition and multiplication modulo 6 operations are the following:-

$+_6$	1	2	3	4	5
1	2	3	4	5	0
2	3	4	5	0	1
3	4	5	0	1	2
4	5	0	1	2	3
5	0	1	2	3	4

Table 4.1: Composition table under $+_6$ operation

$\times_6$	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

Table 4.2: Composition table under $\times_6$ operation

Closure property is not satisfied under both operation, because 0 entry belongs into table which is not the element of set. Therefore, the set {1,2,3,4,5} is not a group under addition and multiplication modulo 6 operation.

Example: Prove that the set {0,1,2,3,4} is a finite abelian group of order 5 under addition modulo 5 operation.
Solution: The composition tables under addition and multiplication modulo 6 operations are the following:-

$+_5$	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

From table, closure property is satisfied, because all entries of table belongs into set {0,1,2,3,4}. Since operation is addition, therefore associative property is satisfied. Clearly

from table, identity element is 0. And each element has a inverse i.e. $(0)^{-1} = 0$, $(1)^{-1} = 4$, $(2)^{-1} = 3$, $(3)^{-1} = 2$, $(4)^{-1} = 1$. Commutative property is also satisfied because aob = boa, for all a,b.
Therefore, this set is an abelian group under operation $+_5$.

4.1.8 Left cancellation law

For a,b,c ∈ G, aob = aoc ⇔ b = c.

4.1.9 Right cancellation law

For a,b,c ∈ G, boa = coa ⇔ b = c.

4.1.10 Some examples

Example: In a group (G,o), prove the following:-
(a) $(a^{-1})^{-1} = a$
(b) $(aob)^{-1} = b^{-1}oa^{-1}$
Solution:
(a) Since a^{-1} is the inverse of a, therefore $aoa^{-1} = e$ .....(1)
Since a ∈ G, therefore a^{-1} is also belong into G. Since $a^{-1} \in G$, therefore inverse of it will also belong.
Using inverse property, $(a^{-1})^{-1}oa^{-1} = e$ .....(2)
Using (1) and (2), $(a^{-1})^{-1}oa^{-1} = aoa^{-1}$
By right cancellation law, we get $(a^{-1})^{-1} = a$
It is proved.
(b) Consider a,b ∈ G. Therefore, its inverses are a^{-1} and b^{-1}.
Since a,b ∈ G, therefore aob also belong into G.
Now, $b^{-1}oa^{-1}$ will be inverse of aob if (aob)o $(b^{-1}oa^{-1}) = e$.
Now, (aob)o $(b^{-1}oa^{-1})$ = ao(bo$(b^{-1}oa^{-1})$) using associative property
= ao((bob^{-1})oa^{-1})) using associative property
= ao(eoa^{-1}) since b^{-1} is the inverse of b
= aoa^{-1} using identity property
= e since a^{-1} is the inverse of a
Therefore, $(aob)^{-1} = b^{-1}oa^{-1}$

Example: Prove that in a group (G,o), if $a^2 = a$, then a = e, for a ∈ G and e is the identity element of G.
Solution:
Since $a^2 = a \Rightarrow$ aoa = aoe
$\Rightarrow$ a = e using left cancellation law.

Example: Show that if every element of a group (G,o) be its own inverse, then it is an abelian group. Is the converse true?
Solution:
First part:
Consider two elements a,b ∈ G. Since each element has its own inverse, therefore $a^{-1} = a$ and $b^{-1} = b$.

To show that the group (G,o) is abelian, we have to show that aob = boa.
Since a,b ∈ G, therefore aob also belong into G. Since each element has its own inverse, therefore $(aob)^{-1} = aob$
We know that $(aob)^{-1} = b^{-1}oa^{-1}$, therefore $b^{-1}oa^{-1}$ = aob ⇒ boa = aob (Since $a^{-1} = a$ and $b^{-1} = b$)
Therefore the group is abelian.
Second part:
In this part, we have to check if a group is abelian then each element has its own inverse. This part is not true. We are giving justification of it below.
Consider an abelian group (Z,+). Clearly in this group, inverse of any element a will be -a, which is not equal to a. Therefore, converse part not true.

4.1.11 Exercise

1. If (G,o) is an abelian group, then for all a,b ∈ G, show that $(aob)^n = a^n o b^n$.

2. Write down the composition tables for $(Z_7, +_7)$ and $(Z_7^*, \times_7)$, where $Z_7^* = Z_7 - \{0\}$.

4.1.12 Order of an element

The order of an element **a** in a group (G,o) is the smallest positive integer n such that a^n = e, where e is the identity element of G.
If no such integer exists, then we say a has infinite order.

Example: Let G = {1,-1,i,-i} be a multiplicative group. Find the order of every element.
Solution: In this group, the identity element, e = 1. Therefore,
$(1)^1$ = 1 (That is e.), therefore order of 1 = 1.
$(-1)^1$ = -1, $(-1)^2$ = 1, therefore order of -1 = 2.
$(i)^1$ = i, $(i)^2$ = -1, $(i)^3$ = -i, $(i)^4$ = 1, therefore order of i = 4.
$(-i)^1$ = -i, $(-i)^2$ = -1, $(-i)^3$ = i, $(-i)^4$ = 1, therefore order of -i = 4.

Example: Find the order of every element in the multiplicative group G=$\{a, a^2, a^3, a^4, a^5, a^6 = e\}$.
Solution: In this group, the identity element, e = a^6. Therefore,
$(a)^6$ = e, therefore order of a = 6.
$(a^2)^1 = a^2$, $(a^2)^2 = a^4$, $(a^2)^3 = a^6$ = e, therefore order of a^2 = 3.
$(a^3)^1 = a^3$, $(a^3)^2 = a^6$ = e, therefore order of a^3 = 2.
$(a^4)^1 = a^4$, $(a^4)^2 = a^8 = a^6oa^2 = eoa^2 = a^2$,
$(a^4)^3 = a^12 = a^6oa^6$ = eoe = e, therefore order of a^4 = 3.
$(a^5)^1 = a^5$, $(a^5)^2 = a^10 = a^6oa^4 = eoa^4 = a^4$,
$(a^5)^3 = a^15 = a^6oa^6oa^3 = eoeoa^3 = a^3$
$(a^5)^4 = a^20 = a^6oa^6oa^6oa^2 = eoeoeoa^2 = a^2$
$(a^5)^5 = a^25 = a^6oa^6oa^6oa^6oa = eoeoeoeoa$ = a
$(a^5)^6 = a^30 = a^6oa^6oa^6oa^6oa^6 = eoeoeoeoe$ = e
Therefore, the order of a^5 = 6.
$(a^6)^1 = a^6$ = e, therefore order of a^6 = 1.

4.1.13 Cyclic group

A group (G,o) is said to be a cyclic group if there exists an element a∈G such that every element of G can be written as some power of a, that is a^n for some integer n. a is said to be the generator of G.
Example: Show that the set of integers with respect to + operation is cyclic group.
Solution: A group will be cyclic if there exists a generator in the group.
Consider an element 1 of this group.
$(1)^1 = 1$
$(1)^2 = 1+1 = 2$
$(1)^3 = 1+1+1 = 3$
$(1)^4 = 1+1+1+1 = 4$
Clearly 1, 2, 3, 4 are expressed in the power of 1. Similarly, we can expressed all the positive integers in the power of 1.
Now, $(1)^{-1}$ = -1
$(1)^{-2} = (1^{-1})^2 = (-1)^2$ = -1+(-1) = -2
$(1)^{-3} = (1^{-1})^3 = (-1)^3$ = -1+(-1)+(-1) = -3
$(1)^{-4} = (1^{-1})^4 = (-1)^4$ = -1+(-1)+(-1)+(-1) = -4
Clearly -1, -2, -3, -4 are expressed in the power of 1. Similarly, we can expressed all the negative integers in the power of 1.
Now, $(1)^0 = 0$
Clearly, all the integers are expressed in the powers of 1. Therefore, 1 is the generator of this group. Since generator exists, therefore the group is cyclic.

Example: Is $(G,+_6)$ a cyclic group, where G = {0,1,2,3,4,5}.
Solution: We have to find generator in this group.
Consider an element 1 of this group.
Now, $(1)^1 = 1$
$(1)^2 = 1+_61 = 2$
$(1)^3 = 1+_61+_61 = 3$
$(1)^4 = 1+_61+_61+_61 = 4$
$(1)^5 = 1+_61+_61+_61+_61 = 5$
$(1)^6 = 1+_61+_61+_61+_61+_61 = 0$
Clearly all the elements of G are expressed in the power of 1, therefore 1 is a generator of G. Since generator exists, therefore the group is cyclic.

Example: Is the multiplicative group $\{1, \omega, \omega^2\}$, a cyclic group?
Solution: Consider an element ω of G.
Now, $(\omega)^1 = \omega$
$(\omega)^2 = \omega^2$
$(\omega)^3 = \omega^3 = 1$
Clearly all the elements of G are expressed in the power of ω, therefore ω is a generator of G. Since generator exists, therefore the group is cyclic.

Example: Show that every cyclic group is an abelian group.

Solution: Consider (G,o) is a cyclic group. Since (G,o) is cyclic, therefore generator exists. Let it's generator is a.
Consider two elements b,c ∈ G. It can be expressed in the power of a. Let b = a^i and c = a^j.
Now, boc = $a^i o a^j$
= a^{i+j}
= a^{j+i} (since set of integers with respect to addition operation is an abelian)
= $a^j o a^i$
= cob
That is, boc = cob
Therefore group (G,o) is an abelian. Now, we can say, every cyclic group is an abelian group.

Example: Show that if a is a generator of a cyclic group G, then a^{-1} is also a generator of G.
Solution: Since a is a generator of G, therefore each elements of G can be epressed in the power of a.
Consider any element b ∈ G such that b = a^i. If we can epressed b in the power of a^{-1}, then a^{-1} will be also generator of G.
Now, b = $a^i = (a^{-1})^{-i}$. Clearly b is expressed in the power of a^{-1}, therefore a^{-1} is also generator of G.

Example: How many generators are there of the cyclic group G of order 8?
Solution: Since the group is cyclic, therefore there exists generator in this group. Let a is a generator.
Therefore, G=$\{a, a^2, a^3, a^4, a^5, a^6, a^7, a^8 = e\}$.
Now, consider an element a^2.
$(a^2)^1 = a^2$
$(a^2)^2 = a^4$
$(a^2)^3 = a^6$
$(a^2)^4 = a^8$ = e
$(a^2)^5 = a^10 = a^2$
Clearly elements a^1, a^3, a^5, a^7 are not expressed in the power of a^2. Therefore a^2 is not generator.
Now, consider an element a^3.
$(a^3)^1 = a^3$
$(a^3)^2 = a^6$
$(a^3)^3 = a^9$ = a
$(a^3)^4 = a^12 = a^4$
$(a^3)^5 = a^15 = a^7$
$(a^3)^6 = a^18 = a^2$
$(a^3)^7 = a^21 = a^5$
$(a^3)^8 = a^24 = a^8$ = e
Clearly all the elements of G are expressed in the power of a^3, therefore a^3 is a generator of G.
Now, consider an element a^4.
$(a^4)^1 = a^4$
$(a^4)^2 = a^8$ = e

$(a^4)^3 = a^12 = a^4$
Clearly elements a^1,a^2, a^3, a^5,a^6, a^7 are not expressed in the power of a^4. Therefore a^4 is not a generator.
Now, consider an element a^5.
$(a^5)^1 = a^5$
$(a^5)^2 = a^10 = a^2$
$(a^5)^3 = a^15 = a^7$
$(a^5)^4 = a^20 = a^4$
$(a^5)^5 = a^25 = a$
$(a^5)^6 = a^30 = a^6$
$(a^5)^7 = a^35 = a^3$
$(a^5)^8 = a^40 = a^8 = e$
Clearly all the elements of G are expressed in the power of a^5, therefore a^5 is a generator of G.
Similarly, we can show that a^7 is a generator and a^6 is not generator.
Therefore the generators of this group are a, a^3, a^5, a^7. Total number of generators is 4.

Example: Show that the group ({ 1,2,3,4,5,6}, $\times_7$) is cyclic. How many generators of this group?
Solution:
Consider the element 3 of this group.
$(3)^1 = 3$
$(3)^2 = 3\times_7 3 = 2$
$(3)^3 = 3\times_7 3\times_7 3 = 6$
$(3)^4 = 3\times_7 3\times_7 3\times_7 3 = 4$
$(3)^5 = 3\times_7 3\times_7 3\times_7 3\times_7 3 = 5$
$(3)^6 = 3\times_7 3\times_7 3\times_7 3\times_7 3\times_7 3 = 1$
Clearly all the elements of G are expressed in the power of 3, therefore 3 is a generator of G.
Since generator exists, therefore the group is cyclic.
Another generator will be 5. Because,
$(5)^1 = 5$
$(5)^2 = 5\times_7 5 = 4$
$(5)^3 = 5\times_7 5\times_7 5 = 6$
$(5)^4 = 5\times_7 5\times_7 5\times_7 5 = 2$
$(5)^5 = 5\times_7 5\times_7 5\times_7 5\times_7 5 = 3$
$(5)^6 = 5\times_7 5\times_7 5\times_7 5\times_7 5\times_7 5 = 1$
No other elements will be generator. Therefore number of generators is 2 i.e. 3 and 5.

4.1.14 Subgroup

Let (G,o) be a group and H is a subset of G. (H,o) is said to be a subgroup of (G,o) if (H,o) is also a group by itself.

Note: (G,o) and ({e},o) are the improper subgroups or trivial subgroups of (G,o).

Example: Is the subset {1,-1} a subgroup of multiplicative group {1, -1, i, -i}?
Solution: We have to check all the properties of group is satisfied with in set {1,-1}

under multiplication operation.
Now, 1*1 = 1, 1*-1 = -1, and -1*(-1) = 1. Clearly the results of these operation are 1 and -1. And both elements belong in to given subset {1,-1}. Therefore closure property is satisfied.
Since {1,-1} is subset of set {1,-1,i,-i}, therefore associative property is satisfied with in {1,-1}.
Clearly 1 is identity element and it is belong into {1,-1} , therefore existence of identity property is also satisfied.
Now, 1*1 = 1, and -1*(-1) = 1. Therefore, inverse of 1 is 1 and inverse of -1 is -1. Since each element has its inverse, therefore subset {1,-1} is satisfied inverse property.
Clearly, this subset satisfies all the property, therefore this is group. And it will also be subgroup of {1,-1,i,-i}.

Example: Is the set of even integers a subgroup of additive group of integers?
Solution: Let I be the set of integers and H be the set of even integers.
If we add any two even integers, then we get also an integer. Therefore, addition operation satisfies closure property with in H.
Since H is a subset of I, therefore associative property is also satisfied in H.
Clearly 0 is an identity element and it also belong into H, therefore, identity property is also satisfied in H.
Consider an element a∈H. Clearly, a+(-a) = 0, therefore -a is the inverse of a. And -a is also belong into H. Therefore, inverse property is satisfied in H.
Clearly, this subset satisfies all the property, therefore this subset H is group. And it will also be subgroup of I.

4.1.15 Some theorems

Theorem: The identity of a subgroup is the same as that of the group.
Proof: Let H be the subgroup of G and e and e' are the identity elements of G and H respectively.
Let a ∈ H. Then
aoe' = a .....(1)
Since a ∈ H ⇒ a∈ G, therefore
aoe = a .....(2)
from (1) and (2), aoe' = aoe
⇒ e' = e (using left cancellation law)
Therefore, the identity of a subgroup is the same as that of the group.

Theorem: The inverse of an element of a subgroup is the same as the inverse of the same regarded as an element of the group.
Proof: Let H be a subgroup of G..
Let a ∈ H. Let b and c are the inverses of element a in H and g respectively. Therefore,
aob = e' .....(1)
and aoc = e .....(2)
From previous theorem, e' = e
Therefore, aob = aoc

$\Rightarrow$ b = c (using left cancellation law)
Therefore, the inverse of an element of a subgroup is the same as the inverse of the same regarded as an element of the group.

Theorem: A non-empty subset H of a group G is a subgroup of G iff
(a) a $\in$ H, b $\in$ H $\Rightarrow$ aob $\in$ H.
(b) a $\in$ H $\Rightarrow$ $a^{-1} \in$ H, where a^{-1} is the inverse of a in G.
Proof:
Necessary part:
Suppose H is a subgroup of G.
Since H is a subgroup of G, therefore closure property is satisfied within H.
So, a $\in$ H, b $\in$ H $\Rightarrow$ aob $\in$ H. Clearly part (a) is proved.
Let a $\in$ H. Since H $\subseteq$ G, therefore a $\in$ G. Let a^{-1} is the inverse of a in G. Since the inverse of an element in subgroup and group is same, therefore $a^{-1} \in$ H. Clearly, part (b) is also proved.
Sufficient part:
Suppose given two statements (a) and (b) are true.
Using statement (a), closure property is satisfied within H.
Since H is a subset of G and G is a group, therefore associative property is also satisfied within H.
Using statement (b), if a $\in$ H then $a^{-1} \in$ H. therefore inverse property is also satisfied within H.
Now, consider a $\in$ H $\Rightarrow$ a $\in$ H and $a^{-1} \in$ H (since inesr property is satisfied)
$\Rightarrow$ ao$a^{-1} \in$ H (using statement (a))
$\Rightarrow$ e $\in$ H, where e is an identity element.
Therefore, identity property is also satisfied within H. Clearly, all the four properties of group is satisfied within H. Therefore, H is a subgroup of G.

Theorem: The necessary and sufficient condition for a non-empty subset H of a group (G,o) to be a subgroup is
a$\in$H, b$\in$H $\Rightarrow$ ao$b^{-1} \in H$
Where b^{-1} is the inverse of b in G.
Proof:
Necessary part:
Suppose H is a subgroup of G.
Let a$\in$ H and b $\in$ H. Since H is subgroup, therefore $b^{-1} \in$ H using inverse property.
Now, a$\in$ H and $b^{-1} \in$ H. By using closure property, ao$b^{-1} \in H$. Therefore the given statement is proved.
Sufficient part:
Suppose a$\in$H, b$\in$H $\Rightarrow$ ao$b^{-1} \in H$ .....(1)
Now, we have to show that H is a subgroup of G.
Identity property:
a$\in$H , a$\in$H $\Rightarrow$ ao$a^{-1} \in H$ (using statement (1))
$\Rightarrow$ e $\in H$
Here, e is the identity element. Therefore, identity property is satisfied within H.
Inverse property:
Now, e $\in H$, a$\in$H $\Rightarrow$ eo$a^{-1} \in H$ (using statement (1))

$\Rightarrow a^{-1} \in H$

Therefore, inverse property is satisfied within H.

Associative property:

Since H $\subseteq$ G, therefore associative property is also satisfied within H, because G is a group.

Closure property:

consider a$\in$H, b$\in$H $\Rightarrow$ a$\in$H, $b^{-1} \in$H

$\Rightarrow$ ao$(b^{-1})^{-1} \in H$ (using statement (1))

$\Rightarrow$ aob $\in$ H

Therefore, closure property is satisfied within H.

Clearly all the four properties are satisfied within H, therefore H is a subgroup of G.

It is proved.

Example: Let G = { .....,$3^{-2}, 3^{-1}, 1, 3, 3^2, 3^3$,.....} be the multiplicative group. Let H = {1,3,$3^2, 3^3$,.....}. Is H a subgroup of G.

Solution: Clearly H is a subset of G, therefore it may be subgroup.

If a$\in$H, b$\in$H $\Rightarrow$ a$ob^{-1} \in H$ is satisfied for each elements a,b $\in$ H, then H will be subgroup.

Consider a = 3 and b= 3^3.

Now, aob^{-1} = 3o$(3^3)^{-1}$

= 3o3^{-3}

= 3^{-2}

Clearly this element i.e. $3^{-2} \notin$ H, therefore H is not subgroup of G.

Theorem: The intersection of any two subgroups of a group (G,o) is again a subgroup of (G,o).

Proof: Let (H_1,o) and (H_2,o) are the two subgroups of (G,o).

Let a $\in H_1 \cap H_2$ and b $\in H_1 \cap H_2$

$\Rightarrow$ (a $\in H_1$ and a $\in H_2$) and (b $\in H_1$ and b $\in H_2$)

$\Rightarrow$ (a $\in H_1$ and b $\in H_1$) and (a $\in H_2$ and b $\in H_2$)

$\Rightarrow$ a$ob^{-1} \in H_1$ and a$ob^{-1} \in H_2$ (Since H_1 and H_2 are subgroups.)

$\Rightarrow$ a$ob^{-1} \in H_1 \cap H_2$

Therefore, $H_1 \cap H_2$ is also a subgroup.

Example: The union of two subgroups is not necessarily a subgroup.

Solution: Let G be the additive group of integers.

H_1 = { .....,-6,-4,-2,0,2,4,6,.....} and H_2 = { .....,-9,-6,-3,0,3,6,9,.....} are both subgroups of G. But $H_1 \cup H_2$ is not subgroup.

4.1.16 Coset

Let H be subgroup of G and let a $\in$ G. Then set {aoh ! h $\in$ H} is called the left coset generated by a and H and is denoted by aH. And right coset is denoted by Ha = {hoa ! h $\in$ H}.

4.1.17 Index of a subgroup in a group

If H is a subgroup of a group G, then the number of distinct right(or left) cosets of H in G is called the index of H in G and it is denoted by [G:H].

Example: Let G be the additive group of integers i.e. G = { .....-3,-2,-1,0,1,2,3,4,.....}. Let H = { .....,-9,-6,-3,0,3,6,9,.....} be the subgroup of G. Determine the index of H in G.
Solution: The index of H in G = The number of left cosets of H in G.
Now, we calculate all distinct left cosets.
0+H = H = { .....,-9,-6,-3,0,3,6,9,.....}.
1+H = {.....,-8,-5,-2,1,4,7,10,.....}
2+H = {....., -7,-4,-1,2,5,8,11,.....}
3+H = { .....,-9,-6,-3,0,3,6,9,.....}.
4+H = {.....,-8,-5,-2,1,4,7,10,.....}
Clearly the number of distinct left cosets is 3. Therefore, the index of H in G = 3.

4.1.18 Normal Subgroup

A subgroup H of G is said to be normal subgroup of G if Ha = aH, $\forall$ a $\in$ G.

Theorem: A subgroup H of G is normal iff $g^{-1}hg \in$ H, $\forall$ h $\in$ H, g$\in$ G.
Proof:
First part: Let H be a normal subgroup of G.
Let h $\in$ H, $g \in$ G. Since H is normal subgroup, therefore $gH = Hg$.
Now,$hg \in Hg \Rightarrow$ hg $\in gH$ (since $gH = Hg$)
$\Rightarrow g^{-1}hg \in (g^{-1}g)H$
$\Rightarrow g^{-1}hg \in$ eH
$\Rightarrow g^{-1}hg \in$ H
Now, it is proved.
Second part: Suppose $g^{-1}hg \in$ H, $\forall$ h $\in$ H, $g \in$ G .....(1)
Now, we have to show that $gH = Hg$.
Let $hg \in Hg$. $\Rightarrow (gg^{-1})hg \in Hg$
$\Rightarrow g(g^{-1}hg) \in Hg$
$\Rightarrow gh' \in$ Hg (using (1))
$\Rightarrow gh' \in$ gH
$\Rightarrow g(g^{-1}hg) \in gH$
$\Rightarrow hg \in gH$
Therefore, $Hg \subseteq gH$ .....(2)
Now, let $gh \in gH$. $\Rightarrow (g^{-1})^{-1})hg^{-1}g \in gH$
$\Rightarrow h'g \in gH$ (using (1))
$\Rightarrow h'g \in Hg$
$\Rightarrow (g^{-1})^{-1})hg^{-1}g \in Hg$
$\Rightarrow gh \in Hg$
Therefore, $gH \subseteq Hg$ .....(3)
From (2) and (3), $gH = Hg$, $\forall$ $g \in$ G.
Therefore, H is normal subgroup of G. Now, it is proved.

Example: If H is a subgroup of G such that $a^2 \in$ H for every a$\in$ G, then prove that H is a normal subgroup of G.
Solution: Let a $\in$ G. Then $a^2 \in$ H.
We know that if $a^{-1}ba \in$ H, then H is normal subgroup, for b $\in$ H.
Here, b = a^2, therefore, $a^{-1}ba = a^{-1}a^2a = a^2$ = b
Since, b $\in$ H, therefore $a^{-1}ba \in$ H. Hence, H is a normal subgroup.

4.1.19 Lagrange's theorem

Statement: The order of each subgroup of a finite group G is a divisor of the order of the group.

Proof: Let H be any subgroup of order m of a finite group G of order n.
Consider all the left cosets of H in G.
Let H = $\{h_1, h_2, h_3, ..., h_m\}$. Then the left cosets of H i.e aH also consists of m elements i.e. aH = $\{ah_i \ ! \ 1 \leq i \leq m\}$.
Clearly, each cosets of H in G consists of m distinct elements. Since G is a finite group, therefore the number of distinct left cosets is also finite. Let this be k. Therefore,

km = n
$\Rightarrow$ m is a divisor of n.

It is proved.

4.1.20 Exercise

1. Consider the group G = {1, 2, 3, 4, 5, 6} under multiplication modulo 7.
   (a) Find the multiplication table of G.
   (b) Find $2^{-1}, 3^{-1}, 6^{-1}$.
   (c) Find the orders and subgroups generated by 2 and 3.
   (d) Is G cyclic?
2. Let Z be the group of integers with binary operation $*$ defined by $a * b$ = a + b - 2 , for all a,b $\in$ Z . Find the identity element of the group $(Z, *)$.
3. What do you mean by cosets of a subgroup? Consider the group Z of integers under addition and the subgroup H = {. . . ., -12, -6, 0, 6 12, ... } considering of multiple of 6.
   (a) Find the cosets of H in Z.
   (b) What is the index of H in Z.
4. Prove or disprove that intersection of two normal subgroups of a group G is again a normal subgroup of G.
5. Let $(A, *)$ be a monoid such that for every x in A , $x * x$ = e, where e is the identity element . Show that $(A, *)$ is an abelian group.
6. Let H be a subgroup of a finite group G. Prove that order of H is a divisor of order of G.
7. Prove that every group of prime order is cyclic.

4.2 Permutation group

4.2.1 Permutation

Let A be a finite set. Then a function f: A $\rightarrow$ A is said to be a permutation of A if f is bijective.

Degree of permutation The number of distinct elements in the finite set A is called the degree of the permutation.

Suppose A = $\{a_1, a_2, a_3, ..., a_n\}$. Then the notation of permutation will be of the following type:-

$$f = \begin{pmatrix} a_1 & a_2 & a_3 & ..... & a_n \\ f(a_1) & f(a_2) & f(a_3) & ..... & f(a_n) \end{pmatrix}$$

4.2.2 Equality of two permutations

Let f and g be two permutations defined on the set A.

f = g iff f(a) = g(a), $\forall$ a $\in$ A.

Example: f = $\begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}$, g = $\begin{pmatrix} b & a & c \\ a & c & b \end{pmatrix}$

Clearly f = g because image of each element is same.

4.2.3 Identity permutation

If each element of a permutation is replaced by itself, then it is called an identity permutation.

Example: Identity permutation defined on set A = {a,b,c} is

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

4.2.4 Product of permutations or Composition of permutations

The product of two permutations f and g of same degree is denoted by fog or fg, meaning first perform f and then perform g.

Example: If f = $\begin{pmatrix} a_1 & a_2 & ..... & a_n \\ b_1 & b_2 & ..... & b_n \end{pmatrix}$, g = $\begin{pmatrix} b_1 & b_2 & ..... & b_n \\ c_1 & c_2 & ..... & c_n \end{pmatrix}$

Then fg = $\begin{pmatrix} a_1 & a_2 & ..... & a_n \\ c_1 & c_2 & ..... & c_n \end{pmatrix}$

Note 1: fg $\neq$ gf.

Therefore, the product of two permutations is not commutative.

Note 2: The product of permutations is associative.

4.2.5 Inverse permutation

Consider a permutation $f = \begin{pmatrix} a_1 & a_2 & ..... & a_n \\ b_1 & b_2 & ..... & b_n \end{pmatrix}$

Then the inverse of this permutation will be $f^{-1} = \begin{pmatrix} b_1 & b_2 & ..... & b_n \\ a_1 & a_2 & ..... & a_n \end{pmatrix}$

Total number of permutations
If n is the degree of the permutation, then the number of permutations of degree n is n!. If S_n be the set of all permutations of degree n, then S_n is said to be symmetric set of permutations of degree n.

4.2.6 Permutation group or symmetric group

An algebraic structure $(S_n, *)$ is said to be permutation group, where the operation * is the composition or product of permutations and set S_n is symmetric set of permutations of degree n. This group is also called symmetric group.

4.2.7 Cyclic permutation

A permutation which replaces n objects or elements cyclically is called a cyclic permutation of degree n.

Example: Permutation f = $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$
It is written as (1 2 3 4) = (2 3 4 1) = (3 4 1 2) = (4 1 2 3)
The number of elements in a cycle is said to be its length.

Disjoint cycle; Two cycles are said to be disjoint if there is no common element in both the cycles.
Every permutation of a finite set can be expressed as a cycle or as a product of disjoint cycles.

Example: Permutation f = $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 6 & 5 & 3 \end{pmatrix}$

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

Transposition A cyclic permutation with length 2 is said to be transposition.
Ex.: (1 2), (4 5) are transpositions.

Even or odd permutation
A permutation is said to be even or odd according as it can be expressed as a product of even or odd number of transpositions.

Example: Find out following permutations are even or odd.
(1) f = $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 2 & 4 & 1 & 3 \end{pmatrix}$, (2) f = $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 4 & 5 & 2 & 1 \end{pmatrix}$
Solution:
(1) f = $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 2 & 4 & 1 & 3 \end{pmatrix}$

= (1 5) (2 6 3) (4)
= (1 5) (2 6) (2 3)
Clearly, this permutation is expressed as 3 number of transpositions, therefore this permutation is odd permutation.

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

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

Clearly, this permutation is expressed as 4 number of transpositions, therefore this permutation is even permutation.

4.3 Homomorphism and Isomorphism of groups

4.3.1 Group homomorphism

Let (G_1, o_1) and (G_2, o_2) be the two groups and f is function from G_1 to G_2. f is said to be group homomorphism from G_1 to G_2 if $\forall$ a,b$\in G_1$,

f(ao_1b)= f(a)o_2f(b).

4.3.2 Group Isomorphism

A group homomorphism f is said to be group isomorphism if f is bijective.

4.3.3 Group automorphism

An isomorphism is said to be automorphism if both groups are same i.e. $G_1 = G_2$.

4.3.4 Kernel of homomorphism

The kernel of homomorphism f of a group G_1 to G_2 is the set of all elements of G_1 mapped on the identity element of G_2 by f. That is,
ker(f) = { a$\in G_1$! f(a) = e_2, where e_2 is the identity element of G_2}

Example: Let (G_1, o_1) = (Z,+) and (G_2, o_2) = ({1,-1},$\times$) are two groups.
f: Z $\rightarrow$ {1,-1} such that

$$f(x) = \begin{cases} 1 & , \ if\ n\ is\ even \\ -1 & , \ if\ n\ is\ odd \end{cases}$$

Find out f is a group homomprphism and isomorphism. And also find kernel of f.
Solution: Consider two integers a and b belong into Z. There will be four case for the sum a+b.
Case 1: when both a and b are even.
f(a+b) = 1 = 1 $\times$ 1 = f(a)$\times$f(b)
Case 2: when both a and b are odd.
f(a+b) = 1 = (-1) $\times$ (-1) = f(a)$\times$f(b)
Case 3: when a is even and b is odd.
f(a+b) = -1 = 1 $\times$ (-1) = f(a)$\times$f(b)
Case 4: when a is odd and b is even.
f(a+b) = -1 = (-1) $\times$ 1 = f(a)$\times$f(b)
Clearly, in all the four cases, f(a+b) = f(a)$\times$f(b)
Therefore, f is homomorphism.
Now, we have to check function is bijective or not.

Clearly, function not one-one. Because all even numbers mapped to 1 and all odd numbers mapped to -1. Therefore, this function is not bijective.
Hence the function is not isomorphism.
Now, ker(f) = The set of all even integers. Because all even integers are mapped on to identity element 1 of G_2.

Example: Let (G_1, o_1) = (R,+) and $(G_2, o_2) = (R^+,\times)$ are two groups.
f: $G_1 \to G_2$ defined by f(x) = 2^x.
Find out f is a group homomorphism and isomorphism.
Solution: Consider any two elements a and b of R.
Now, f(a+b) = $2^{(a+b)}$
$= 2^a \times 2^b$
= f(a)×f(b)
Clearly, f(a+b) = f(a)×f(b). Therefore f is homomorphism.
Clearly, for each distinct real number a, there will be distinct positive real number 2^a. Therefore the function is one-one.
Clearly, the function is onto because each element of R^+ is the image of some element of R.
Therefore the function f is bijective. Hence the function is isomorphism.

Theorem: Let (G_1, o_1) and (G_2, o_2) are two groups and let f be a homomorphism from G_1 to G_2. Then, prove the following:-
(1) f(e_1) = e_2, where e_1 is the identity of G_1 and e_2 is the identity of G_2.
(2) f(a^{-1}) = $(f(a))^{-1}$, $\forall a \in G_1$
(3) If H is a subgroup of G_1, then f(H) = {f(h) ! h ∈ H} is a subgroup of G_2.
Proof: (1) f(e_1) = f(e_1 o_1 e_1) = f(e_1) o_2 f(e_1)
⇒ f(e_1) = f(e_1) o_2 f(e_1) .....(1)
Since f(e_1) is the element of G_2, therefore using identity property
e_2 o_2 $f(e_1)$ = f(e_1) .....(2)
From (1) and (2), f(e_1)o_2f(e_1) = $e_2 o_2 f(e_1)$
⇒ f(e_1) = e_2 (using right cancellation law)
It is proved.
(2) f(e_1) = f(a o_1 a^{-1}) = $f(a)$ o_2 $f(a^{-1})$
⇒ f(e_1) = $f(a)$ o_2 $f(a^{-1})$ .....(3)
Now, $f(a)$ o_2 $(f(a))^{-1} = e_2$ .....(4)
From part (1), we know that f(e_1) = e_2 , therefore from (3) and (4)
$f(a)$ o_2 $f(a^{-1}) = f(a)$ o_2 $(f(a))^{-1}$
⇒ f(a^{-1}) = $(f(a))^{-1}$ (using left cancellation law)
It is proved.
(3) Let h is subgroup of G_1.
a∈H, b∈H ⇒ ao_1b^{-1} ∈ H
Now, we have to show that f(H) is a subgroup of G_2.
Since a,b∈ H, therefore f(a), f(b) ∈ f(H).
f(a)∈ f(H), f(b)∈ f(H) ⇒ a∈H, b∈H

$\Rightarrow a\ o_1\ b^{-1} \in$ H
$\Rightarrow$ f($a\ o_1\ b^{-1}$) $\in$ f(H)
$\Rightarrow f(a)\ o_2\ f(b^{-1}) \in$ f(H)
$\Rightarrow f(a)\ o_2\ (f(b))^{-1} \in$ f(H) (using part (2),f(a^{-1}) = $(f(a))^{-1}$)
Therefore, f(H) is a subgroup of G_2.
It is proved.

4.3.5 Factor or Quotient group

If H is a normal subgroup of group G, then the set of all left cosets of G forms a group with respect to the multiplication of left coset defined as (aH)(bH) = (ab)H, called the factor group of G by H. It is denoted by G/H.
G/H = { gH ! g $\in$ G }

4.4 Exercise

1. In the symmetric group S_3, find all those elements a and b such that
   (a) $(a * b)^2 \neq a^2 * b^2$
   (b) $a^2 =$ e
   (c) $a^3 =$ e
2. Show that in a group (G,o), if for any a,b $\in$ G, $(aob)^2 = a^2ob^2$, then (G,o) must be abelian.
3. Show that every cyclic group of order n is isomorphic to the group $(Z_n,\ +_n)$.
4. Find all the subgroups of following groups:-
   (a) $(Z_{12},\ +_{12})$
   (b) $(Z_5,\ +_5)$
   (c) $(Z_7^*,\ \times_7)$
   (d) $(Z_{11}^*,\ \times_{11})$

4.5 Exercise's solution

1. Let $p_1, p_2, p_3, p_4, p_5, p_6$ are the elements of S_3.

$$p_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, p_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$
$$p_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, p_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, p_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

   The composition table for S_3 with respect to multiplication operation is the following:-

$*$	p_1	p_2	p_3	p_4	p_5	p_6
p_1	p_1	p_2	p_3	p_4	p_5	p_6
p_2	p_2	p_1	p_5	p_6	p_3	p_4
p_3	p_3	p_6	p_1	p_5	p_4	p_2
p_4	p_14	p_5	p_6	p_1	p_2	p_3
p_5	p_5	p_4	p_2	p_3	p_6	p_1
p_6	p_6	p_3	p_4	p_2	p_1	p_5

(a) In this part, we have to find elements a and b of S_3 which satisfy equation (1).
$(a*b)^2 \neq a^2 * b^2$ ..... (1)
Consider, a = p_2 and b = p_3.
Now, LHS = $(a*b)^2 = (p_2 * p_3)^2 = p_5^2 = p_6$
RHS = $a^2 * b^2 = p_2^2 * p_3^2 = p_1 * p_1 = p_1$
Clearly, $(a*b)^2 \neq a^2 * b^2$ for a = p_2 and b = p_3.

Similarly, Consider, a = p_2 and b = p_4.
Now, LHS = $(a*b)^2 = (p_2 * p_4)^2 = p_6^2 = p_5$
RHS = $a^2 * b^2 = p_2^2 * p_4^2 = p_1 * p_1 = p_1$
Clearly, $(a*b)^2 \neq a^2 * b^2$ for a = p_2 and b = p_4.

Similarly, following pairs of a and b are also satisfied.
a = p_2 and b = p_5
a = p_2 and b = p_6
a = p_3 and b = p_4
a = p_3 and b = p_5
a = p_3 and b = p_6
a = p_4 and b = p_5
a = p_4 and b = p_6

(b) In this part, we have to find element a of S_3 which satisfy equation (2).
a^2 = e .....(2)
Here, the identity element is e = p_1.
Consider, a = p_1
$a^2 = p_1^2 = p_1$ = e
Therefore, a = p_1 satisfy the equation (2).
Similarly, a = p_2, p_3, p_4 also satisfy the equation (2).

(c) In this part, we have to find element a of S_3 which satisfy equation (3).
a^3 = e .....(3)
Here, the identity element is e = p_1.
Consider, a = p_1
$a^3 = p_1^3 = p_1$ = e
Therefore, a = p_1 satisfy the equation (3).
Similarly, a = p_5, p_6 also satisfy the equation (3).

2. Given $(aob)^2 = a^2ob^2$, for a,b $\in$ G.
It imply that (aob)o(aob) = (aoa)o(bob)
$\Rightarrow$ ao(bo(aob)) = ao(ao(bob)) (using associative law)
$\Rightarrow$(bo(aob)) = (ao(bob)) (using left cancellation law)

$\Rightarrow$(boa)ob = (aob)ob (using associative law)
$\Rightarrow$ (boa) = (aob)(using right cancellation law)
Therefore, the group (G,o) is an abelian group.

3. Let cyclic group(G,o) of order n be generated by an element a $\in$ G. So the elements of G are $a, a^2, a^3, ..., a^n = e$.
Define g : $Z_n \to G$ such that g([1]) = a. [1] is the generator of $(Z_n, +_n)$. Then g([j]) = a^j, for all j = 0,1,2,3,.....,n-1.
Clearly this function is bijective because each element j is mapped to unique element a^j.
Now, g([j]+[k]) = $a^{[j]+[k]}$
$= a^{[j]} o a^{[k]}$
= g[j] o g[k]
Clearly, g([j]+[k]) = g[j] o g[k]
Therefore, g is homoomorphism. Since g is bijective and homomorphism, so g is isomorphism.
Therefore, every cyclic group of order n is isomorphic to the group $(Z_n, +_n)$.

4. In this question, we have to find all the subgroups of given groups. In these questions, Z_n = {0,1,2,3,4,.....,n-1} and $+_n$ and $\times_n$ are addition and multiplication modulo n operations.
According to Lagrange's theorem, order of each subgroup is the divisor of the order of the group. We will use this theorem to find all the subgroups.

   (a) Here group is $(Z_{12}, +_{12})$. Therefore Z_{12} = {0,1,2,3,4,5,6,7,8,9,10,11}. Clearly, the order of this group is 12. Using Lagrange's theorem, the number of subgroups of Z_{12} = number of positive divisors of 12.
   The positive divisors of 12 are 1,2,3,4,6,12. Since the number of divisors is 6, therefore number of subgroups will be 6 with orders 1,2,3,4,6,12. These subgroups are the following:-
   Now, H_1 = {0}, this is a subgroup with order 1.
   H_2 = {0,6}, this is a subgroup with order 2.
   H_3 = {0,4,8}, this is a subgroup with order 3.
   H_4 = {0,3,6,9}, this is a subgroup with order 4.
   H_5 = {0,2,4,6,8,10}, this is a subgroup with order 6.
   H_6 = {0,1,2,3,4,5,6,7,8,9,10,11}, this is a subgroup with order 12.

   (b) Here group is $(Z_5, +_5)$. Therefore Z_5 = {0,1,2,3,4}. Clearly, the order of this group is 5. The positive divisors of 5 are 1,5. Since the number of divisors is 2, therefore number of subgroups will be 2 with orders 1,5. These subgroups are the following:-
   H_1 = {0}, this is a subgroup with order 1.
   H_2 = {0,1,2,3,4}, this is a subgroup with order 5.

   (c) Here group is $(Z_7^*, \times_7)$. Therefore Z_7^* = {1,2,3,4,5,6}. Clearly, the order of this group is 6. The positive divisors of 6 are 1,2,3,6. Since the number of divisors is 4, therefore number of subgroups will be 4 with orders 1,2,3,6. These subgroups are the following:-
   H_1 = {1}, this is a subgroup with order 1.

$H_2 = \{1,6\}$, this is a subgroup with order 2.
$H_3 = \{1,2,4\}$, this is a subgroup with order 3.
$H_4 = \{1,2,3,4,5,6\}$, this is a subgroup with order 6.

(d) Here group is $(Z_{11}^*, \times_{11})$. Therefore $Z_{11}^* = \{1,2,3,4,5,6,7,8,9,10\}$. Clearly, the order of this group is 10. The positive divisors of 10 are 1,2,5,10. Since the number of divisors is 4, therefore number of subgroups will be 4 with orders 1,2,5,10. These subgroups are the following:-
$H_1 = \{1\}$, this is a subgroup with order 1.
$H_2 = \{1,10\}$, this is a subgroup with order 2.
$H_3 = \{1,3,4,5,9\}$, this is a subgroup with order 5.
$H_4 = \{1,2,3,4,5,6,7,8,9,10\}$, this is a subgroup with order 10.

Chapter 5

Ring and Field

5.1 Ring

5.1.1 Definition

An algebraic structure (R, +, .), where R is a set and + and . are two binary operators defined on set R, is said to be ring if it satisfies following properties:-
(1) (R, +) is an abelian group.
(2) (R, .) is a semigroup.
(3) Distributive property must hold i.e. a.(b+c) = a.b + a.c and (b+c).a = b.a + c.a, $\forall$ a,b,c $\in$ R.

5.1.2 Commutative ring

A ring R is said to be commutative ring if it satisfies commutative property with respect second operation i.e.
a.b = b.a, $\forall$ a,b $\in$ R.

5.1.3 Ring with unity

A ring R is said to be ring with unity if it contains identity element with respect to second operation that is . operation.
Note: We will denote here identity element with respect to first operation by 0 and identity element with respect to second operation by 1.

Example: Show that the set Z of integers under addition and multiplication is commutative ring with unity.
Solution: (Z, +, .) is a ring if it satisfies all the properties of ring.
First we have to show that (Z,+) is an abelian group.
Closure property: We know that the addition of any two integers is also an integers. So, Z is closed under addition operation.
Associative property: We know that the addition of any three integers in any way is equal, therefore we can say, a+(b+c) = (a+b)+c, $\forall$ a,b,c $\in$ Z.
Therefore, Z satisfies associative property.
Existence of identity property: Let a $\in$ Z. Clearly, 0 $\in$ Z such that a+0 = a = 0+a. Therefore, 0 is an identity element. So, it satisfies identity property.

Existence of inverse property: Let a ∈ Z. Clearly, -a ∈ Z such that a+(-a) = 0. Therefore, -a is an additive inverse of any element a. So, it satisfies inverse property under addition operation.
Commutative property: Clearly, a+b = b+a, ∀ a,b ∈ Z. So, Z satisfies commutative property with respect to addition operation.
Therefore, (Z,+) is an abelian group.
Now, we have to show that (Z, .) is a semigroup.
Closure property: We know that the multiplication of any two integers is also an integers. So, Z is closed under multiplication operation.
Associative property: We know that the multiplication of any three integers in any way is equal, therefore we can say, a.(b.c) = (a.b).c, ∀ a,b,c ∈ Z.
Therefore, Z satisfies associative property.
Therefore, (Z, .) is a semigroup.
Now, we have to show **distributive property** is satisfied.
Clearly, for any three integers a,b,c; followings are satisfied:-
(i) a.(b+c) = a.b + a.c
(ii) (b+c).a = b.a + c.a
Therefore, distributive property is satisfied in (Z, +, .).
Therefore, (Z, +, .) is a ring.

Example: The set Z_n = {0,1,2,3,.....,n-1} under addition and multiplication modulo n is a commutative ring with unity.
Solution: $(Z_n, +_n, \times_n)$ is a ring if it satisfies all the properties of ring.
First we have to show that $(Z, +_n)$ is an abelian group.
Closure property: Consider a,b ∈ Z_n. Clearly, a$+_n$b = c ∈ Z_n. Therefore, Z_n is closed under addition modulo n operation.
Associative property: Clearly, if we compute $a +_n (b +_n c)$ and $(a +_n b) +_n c)$ then both value will be same. Therefore we can say, $a +_n (b +_n c) = (a +_n b) +_n c)$, ∀ a,b,c ∈ Z_n).
Therefore, Z_n satisfies associative property.
Existence of identity property: Let a ∈ Z_n. Clearly, 0 ∈ Z_n such that a$+_n$0 = a = 0$+_n$a. Therefore, 0 is an identity element. So, it satisfies identity property.
Existence of inverse property: Let a ∈ Z_n. Clearly, n-a ∈ Z_n such that a$+_n$(n-a) = 0. Therefore, n-a is an additive modulo n inverse of any element a. So, it satisfies inverse property under addition operation.
Commutative property: Clearly, a$+_n$b = b$+_n$a, ∀ a,b ∈ Z_n. So, Z_n satisfies commutative property with respect to addition modulo n operation.
Therefore, $(Z_n, +_n)$ is an abelian group.
Now, we have to show that $(Z_n, \times_n)$ is a semigroup.
Closure property: Consider a,b ∈ Z_n. Clearly, a$\times_n$b = c ∈ Z_n. Therefore, Z_n is closed under multiplication modulo n operation.
Associative property: Clearly, if we compute $a \times_n (b \times_n c)$ and $(a \times_n b) \times_n c)$ then both value will be same. Therefore we can say, $a \times_n (b \times_n c) = (a \times_n b) \times_n c)$, ∀ a,b,c ∈ Z_n).
Therefore, Z_n satisfies associative property.
Therefore, $(Z_n, \times_n)$ is a semigroup.
Now, we have to show **distributive property** is satisfied.
Clearly, for any three elements a,b,c Z_n; followings are satisfied:-

(i) $a\times_n(b+_nc) = a\times_nb +_n a\times_nc$
(ii) $(b+_nc)\times_na = b\times_na +_n c\times_na$
Therefore, distributive property is satisfied in $(Z_n, +_n, \times_n)$.
Therefore, $(Z_n, +_n, \times_n)$ is a ring.
Now, if this ring satisfies commutative property and identity property with respect to multiplication modulo n operation, then it is said to be commutative ring with unity.
Commutative property: Clearly, $a\times_nb = b\times_na$, $\forall$ a,b $\in Z_n$. So, Z_n satisfies commutative property with respect to multiplication modulo n operation.
Existence of identity property: Let $a \in Z_n$. Clearly, $1 \in Z_n$ such that $a\times_n1 = a = 1\times_na$. Therefore, 1 is an identity element. So, it satisfies identity property with respect to multiplication modulo n operation.
Therefore, this ring $(Z_n, +_n, \times_n)$ is commutative ring with unity.

5.1.4 Elementary properties of a ring

Let a,b,c $\in$ R, then

1. a.0 = 0.a = 0
2. a.(-b) = (-a).b = -(a.b)
3. (-a).(-b) = a.b
4. a.(b-c) = a.b - a.c and (b-c).a = b.a - c.a

Proof: (1) a.0 +a.a = a.(0+a)
= a.a
= 0 + a.a
using right cancellation law, a.0 = 0
Similarly, 0.a +a.a = (0+a).a
= a.a
= 0 + a.a
using right cancellation law, 0.a = 0
Therefore, a.0 = 0.a = 0
(2) a.(-b) + a.b = a.(-b+b)
= a.0
= 0
therefore, a.(-b) = -(a.b)
Similarly, (-a).b + a.b = (-a+a).b
= 0.b
= 0
Therefore, (-a).b = -(a.b)
Therefore, a.(-b) = (-a).b = -(a.b)
(3) (-a).(-b) = -((-a).b) = -(-(a.b)) = a.b
(4) a.(b-c) = a.(b+(-c))
= a.b + a.(-c)
= a.b - a.c
Similarly, (b-c).a = (b+(-c)).a

= b.a + (-c).a
= b.a - c.a

Example: If R is a ring such that a^2 = a, ∀ a ∈ R, prove that
(1) a+a = 0 , ∀ a ∈ R i.e. each element of R is its own additive inverse.
(2) a+b = 0 ⇒ a = b
(3) R is a commutative ring.
Solution:
(1) $(a+a)^2$ = a+a
⇒ $a^2 + a^2 + a^2 + a^2$ = a+a
⇒ a+a+a+a = a+a
⇒ a+a = 0 using cancellation law
It is proved.
(2) a+b = 0 ⇒ a+b = a+a (using part (1))
⇒ b = a (using cancellation law)
It is proved.
(3) $(a+b)^2$ = a+b
⇒ $a^2 + ab + ba + b^2$ = a+b
⇒ a + ab + ba + b = a + b
⇒ ab + ba = 0 (using cancellation law)
⇒ ab = ba (using part (2))
Therefore, R is commutative ring. Now, It is proved.

5.2 Field

5.2.1 Definition

An algebraic structure (F, +, .), where F is a set and + and . are two binary operators defined on set F, is said to be field if it satisfies following properties:-
(1) (R, +) is an abelian group.
(2) (R' , .) is an abelian group, where R' = R-{0}.
(3) Distributive property must hold i.e. a.(b+c) = a.b + a.c and (b+c).a = b.a + c.a, ∀ a,b,c ∈ F.

Example: The ring of rational numbers (Q , +, .) is a field.
Solution: Since (Q , +, .) is a ring therefore we have to show only second property of field i.e. (Q',.) is an abelian.
Since (Q , +, .) is ring therefore (Q',.) is a semigroup. Now, we hae to find identity element and inverse.
Clearly 1 is an identity element.
Consider an element a ∈ Q'. clearly the inverse of a is 1/a. Therefore inverse property is also satisfied.
If a,b ∈ Q' then a.b = b.a, therefore commutative property is satisfied. Since all the properties of an abelian group is satisfied within Q'. Therefore, (Q',.) is an abelian group.
Therefore, (Q , +, .) is a field.

Example: (R,+,.) is a field.

5.2.2 Ring with zero divisors

If a and b are two non-zero elements of a ring R such that a.b = 0, then a and b are divisors of 0(or o divisors). In particular, a is a left divisor of 0 and b is right divisor of 0.

Example: The ring of integers do not have zero divisors. Because there exist no two non-zero integers such that their product is zero.

5.2.3 Ring homomorphism

Let (R, +, .) and (S, $\oplus, \odot$) be rings. A mapping f: R $\rightarrow$ S is called a ring homomorphism from (R, +, .) to (S, $\oplus, \odot$) if for any a,b $\in$ R,
f(a+b) = f(a)$\oplus$ f(b) and f(a.b) = f(a)$\odot$ f(b)

5.2.4 Boolean ring

A ring R is said to be boolean ring if a^2 = a, $\forall$ a $\in$ R. **Example:** Show that a Boolean ring is always commutative.

Solution: It is proved in the previous example.

Example: If (R, +, .) is a ring with unity, then show that, for all a $\in$ R,
(i) (-1).a = -a
(ii) (-1).(-1) = 1
Solution:
(i) a + (-1).a = 1.a + (-1).a
= (1+(-1)).a
= 0.a
= 0
$\Rightarrow$ -a = (-1).a
(ii) (-1).(-1) = -((-1).1) = -(-(1.1)) = -(-(1)) = 1 (since $(a^{-1})^{-1}$ = a)

Example: Explain Boolean ring with suitable example.
Solution: A ring R is said to be boolean ring if a^2 = a, $\forall$ a $\in$ R.
Example of Boolean ring is $(Z_2, +_2, \times_2)$ because
Z_2 = {0,1} and $0^2 = 0 \times_2 0 = 0$, $1^2 = 1 \times_2 1 = 1$.

Note: $(Z_n, +_n, \times_n)$ is a field iff n is prime number.

Example: Determine all values of x from the given field which satisfies the given equation:-
(i) x + 1 = -1 over Z_2, Z_3, Z_5 *and* Z_7
(ii) 2x + 1 = 2 over Z_3, *and* Z_5
(iii) 5x + 1 = 2 over Z_5
Solution:

(i) Consider field Z_2. Z_2 = {0,1}. Now, we have to find which values of Z_2 satisfies following x + 1 = -1.
Here, -1 indicate the additive inverse of 1.Clearly, in this field, additive inverse of 1 is 1, therefore the given equation is modified as x + 1 = 1.
Clearly x = 0 satisfies this equation.
Consider field Z_3. Z_3 = {0,1,2}. In this field, additive inverse of 1 is 2, therefore the given equation is modified as x + 1 = 2.
Clearly x = 1 satisfies this equation.
Consider field Z_5. Z_5 = {0,1,2,3,4}. In this field, additive inverse of 1 is 4, therefore the given equation is modified as x + 1 = 4.
Clearly x = 3 satisfies this equation.
Consider field Z_7. Z_7 = {0,1,2,3,4,5,6}. In this field, additive inverse of 1 is 6, therefore the given equation is modified as x + 1 = 6.
Clearly x = 5 satisfies this equation.
(ii) Consider field Z_3. Z_3 = {0,1,2}. Now, we have to find which values of Z_3 satisfies following 2x + 1 = 2.
Clearly x = 2 satisfies this equation.
Consider field Z_5. Z_5 = {0,1,2,3,4}. Now, we have to find which values of Z_5 satisfies following 2x + 1 = 2.
Clearly x = 3 satisfies this equation.
(iii) Consider field Z_5. Z_5 = {0,1,2,3,4}. Now, we have to find which values of Z_5 satisfies following 5x + 1 = 2.
Clearly there is no x in Z_5 which satisfies this equation.

5.2.5 Exercise

1. Show that $(Z_7, +_7, \times_7)$ is a commutative ring with identity.

2. We are given the ring ({a,b,c,d}, +, .), whose operations are given by the following table:-

+	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

.	a	b	c	d
a	a	a	a	a
b	a	c	a	c
c	a	a	a	a
d	a	c	a	a

   Is it commutative ring? Does it have an identity? what is the zero of this ring? Find the additive inverse pf each of its elements.

3. Show that $(I, \oplus, \odot)$ is a commutative ring with identity, where the operations $\oplus$ and $\odot$ are defined, for any a,b $\in$ I as a$\oplus$b = a+b-1 and a$\odot$b = a+b-ab.

4. Prove that $(R, +, *)$ is a ring with zero divisors, where R is 2x2 matrix and + and $*$ are usual addition and multiplication operations.

Chapter 6

Partial ordered set and Hasse diagram

6.1 Partial ordered relation and Partial ordered set

6.1.1 Partial ordered relation

Consider a relation R defined on set S. Relation R is said to be partial ordered relation if R satisfies following properties:-
(1) R is reflexive, i.e., xRx for every x ∈ S.
(2) R is anti-symmetric, i.e., if xRy and yRx, then x = y.
(3) R is transitive, i.e., xRy and yRz, then xRz.

6.1.2 Partial ordered set (POSET)

Consider a relation R defined on set S. If R is a partial order relation, then the combination of set S and partial order relation R is said to be partial ordered set i.e. POSET. We denote POSET by $< S, \preceq >$, where $\preceq$ denotes partial ordered relation.

6.1.3 Totally ordered relation and set

Let $< S, \preceq >$ bea partially ordered set. If for eery a,b ∈ S, we hae either a$\preceq$b or b$\preceq$a, then $\preceq$ is called a totally ordered relation defined on set P.
And the ordered pair $< S, \preceq >$ is called a totally ordered set.

6.1.4 Some examples

Example: Let R be the set of real numbers and relation $\preceq$ is less than or equal i.e. a$\preceq$b iff a≤b. Is $< R, \preceq >$ a POSET?
Solution: $< R, \preceq >$ will be a POSET if $\preceq$ is partial ordered relation. $\preceq$ will be partial ordered relation if this relation satisfies reflexive, anti-symmetric and transitive.
Here, the relation is less than or equal.
Each real number will be related to itself because each real number is equal to itself. Therefore, this relation is reflexive.
a is less than or equal to b and b is less than or equal to a , this is only possible iff a=b.

Therefore this relation is anti-symmetric.
Consider a$\preceq$b and b$\preceq$c. It imply that a$\leq$b and b$\leq$c. It imply that a$\leq$c. Therefore R is transitive.
Since all the three properties are satisfies, therefore, this relation is partial ordered relation.

Example: Let A = {1,2,3}. Show that ¡P(A),$\subseteq$¿ is POSET, P(A) is power set o A.
Solution: Here P(A) = {ϕ, {1},{2},{3},{1,2},{1,3},{2,3},{1,2,3}} and relation is subset i.e. set B related set C iff B$\subseteq$C.
For reflexive: Since each set is subset of itself, therefore this relation is reflexive.
For anti-symmetric: Consider B and C are two elements of P(A) such that B$\subseteq$C and C$\subseteq$B. Clearly it will be only true when B=C, otherwise it will be false. Therefore this relation is anti-symmetric.
For transitive: Consider B, C and D are three elements of P(A) such that B$\subseteq$C, C$\subseteq$D. It will imply that B$\subseteq$D. Therefore this relation is transitive.
Since all the three properties are satisfies, therefore, this relation is partial ordered relation. And the ordered pair $< P(A), \subseteq >$ is POSET.

Example: Let D(n) is the set of all positive divisors of n. And relation $\preceq$ is defined as:- a $\preceq$ b iff a divides b. Is $< D(n), \preceq >$ POSET?
Solution: Two elements a and b of D(n) will be related iff a divides b.
For reflexive: Since each element divides to itself, therefore this relation is reflexive.
For anti-symmetric: Consider a and b are two elements of D(n) such that a$\preceq$b and b$\preceq$c. Clearly it will be only true when a=b, otherwise it will be false. Therefore this relation is anti-symmetric.
For transitive: Consider a, b and c are three elements of D(n) such that a$\preceq$b, b$\preceq$c. It will imply that a$\preceq$c. Therefore this relation is transitive.
Since all the three properties are satisfies, therefore, this relation is partial ordered relation. And the ordered pair $< D(n), \preceq >$ is POSET.

6.1.5 Cover, Successor, Predecessor

In a partially ordered set $< S, \preceq >$, an element b $\in$ S is said to be cover of element a $\in$ S if a $\preceq$ b and if there does not exist any element c $\in$ S such that a $\preceq$ c $\preceq$ b.
a is the immediate predecessor of b and b is the immediate successor of a.

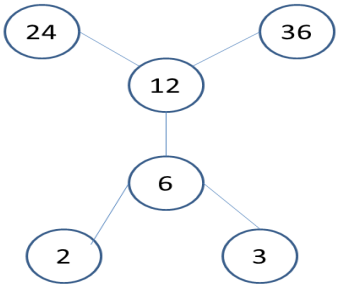
6.2 Hasse diagram

It is the graphical representation of POSET.

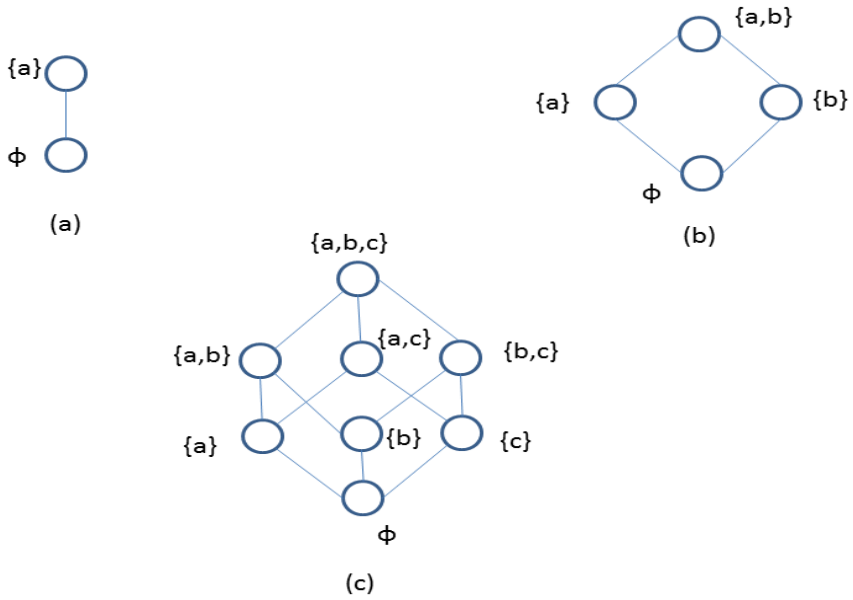
In this diagram, we make nodes corresponding to each elements in the POSET, that is the number of nodes is equal to the number of elements in the POSET. Edges will undirected. These edges will link elements a and b if b is cover of a such that a will be at lower side of b and b will be at upper side from a. In other words, two elements will be connected by an edge if one element is an immediate successor of another element.

6.2.1 Some examples

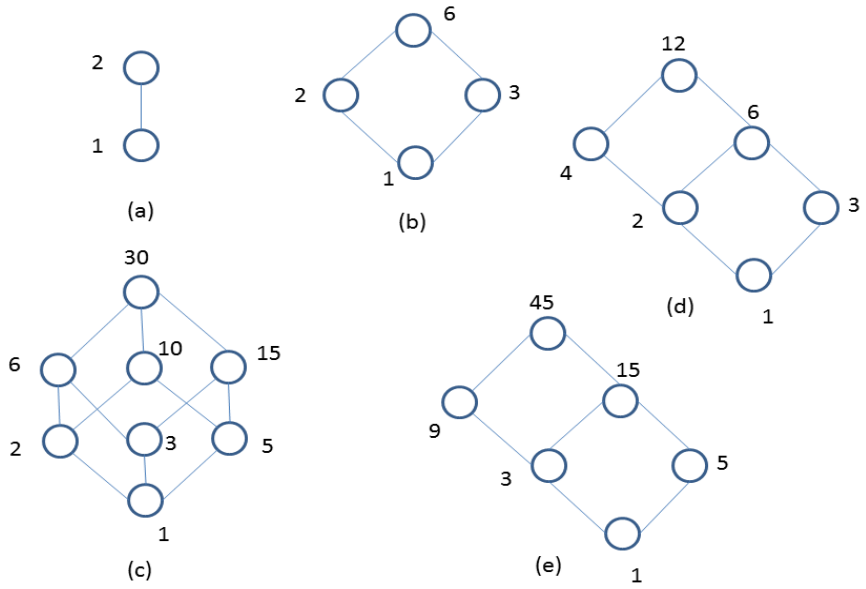
Example: Let S = {2,3,6,12,24,36} and the relation $\preceq$ be such that a $\preceq$ b if a divides b. Draw the Hasse diagram of this POSET $< S, \preceq >$.
Solution:



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



Example: Let A be the set of factors of a particular positive integer m and let $\preceq$ be the relation divides, i.e.
$\preceq$ = {(a,b) ! a divides b}
Draw Hasse diagram for (a) m = 2 (b) m = 6 (c) m = 30 (d) m = 12 (e) m = 45
Solution: Since A be the set of factors of a particular positive integer m, therefore A will be for each case:-
(a) A = {1,2} (b) A = {1,2,3,6} (c) A = {1,2,3,5,6,10,15,30}
(d) A = {1,2,3,4,6,12} (e) A = {1,3,5,9,15,45}



6.2.2 Least and Greatest element

An element a ∈ S is said to be the least element of the POSET $< S, \preceq >$, if a$\preceq$b, ∀ b ∈ S.
An element b ∈ S is said to be the greatest element of the POSET $< S, \preceq >$, if a$\preceq$b, ∀ a ∈ S.

6.2.3 Minimal and Maximal element

An element a ∈ S is said to be the minimal element of the POSET $< S, \preceq >$, if there is no element b ∈ S such that b$\preceq$a.
An element b ∈ S is said to be the maximal element of the POSET $< S, \preceq >$, if there is no element a ∈ S such that b$\preceq$a.

6.2.4 Upper bound and Lower bound

Let $< S, \preceq >$ be a POSET and let A⊆S.
An element u∈S is said to be upper bound of set A if a$\preceq$u, ∀ a∈ A.
An element l∈S is said to be lower bound of set A if l$\preceq$a, ∀ a∈ A.

6.2.5 Least upper and Greatest lower bound

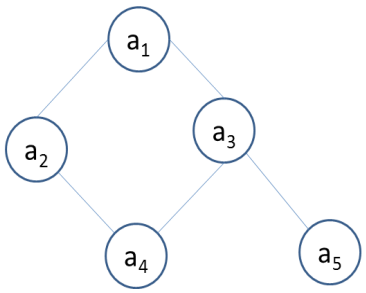
An upper bound u of the set A is said to be least upper bound of set A if u$\preceq$u', ∀ upper bound u' of A.
An upper bound l of the set A is said to be greatest lower bound of set A if l'$\preceq$l, ∀ lower bound l' of A.

6.2.6 Well ordered set

A POSET is said to be well-ordered set if for every non-empty subset of it has a least element.

6.2.7 Some examples

Example: Consider the following Hasse diagram:-



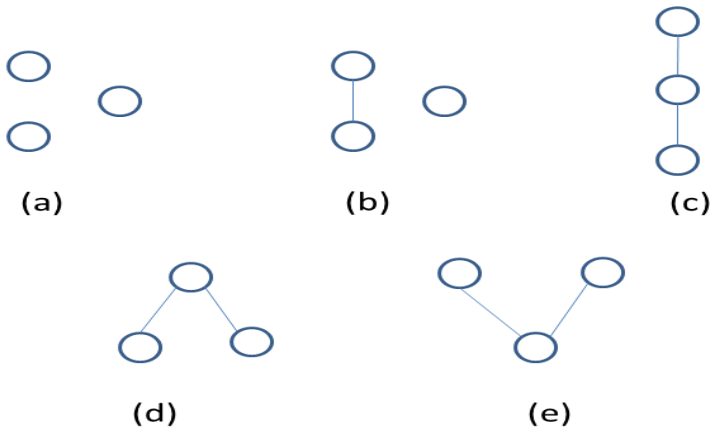
Find the least and greatest element of this POSET if they exist. Also find minimal and maximal elements. Find the upper and lower bounds of $\{a_2, a_3, a_4\}$, $\{a_3, a_4, a_5\}$, $\{a_1, a_2, a_3\}$. Also indicate the least upper bound and greatest lower bound of these subsets if they exists.
Solution:
Least element = does not exists because no element in this POSET is related to all the elements.
Greatest element = a_1 because all the elements of the POSET is related to a_1
Minimal elements = a_4, a_5
Maximal elements = a_1

Consider the set $\{a_2, a_3, a_4\}$.
lower bounds = a_4, because a_4 is related to all the elements of the set $\{a_2, a_3, a_4\}$
upper bounds = a_1, because all the elements of the set $\{a_2, a_3, a_4\}$ is related to a_1.
greatest lower bound = a_4
least upper bound = a_1

Consider the set $\{a_3, a_4, a_5\}$.
lower bounds = does not exists because no element is related to all the elements of the set $\{a_3, a_4, a_4\}$
upper bounds = a_1, a_3, because all the elements of the set $\{a_3, a_4, a_5\}$ is related to a_1, a_3.
greatest lower bound = does not exists
least upper bound = a_3

Consider the set $\{a_1, a_2, a_3\}$.
lower bounds = a_4, because a_4 is related to all the elements of the set $\{a_1, a_2, a_3\}$
upper bounds = a_1, because all the elements of the set $\{a_1, a_2, a_3\}$ is related to a_1.
greatest lower bound = a_4
least upper bound = a_1

Example: Show that there are only five distinct Hasse diagrams for partial ordered sets that contain three elements.
Solution: All the distinct Hasse diagrams corresponding to three elements are the followings:-



Clearly no other Hasse diagrams can be drawn for three elements. If we make any other diagram for three elements then it will be equivalent to any one of the above. Therefore, Hasse diagram corresponding to three elements will be five.

6.2.8 Exercise

1. Draw the Hasse diagram of the following sets under the partial ordering relation "divides" and indicate those which are totally ordered.
   (a) {2,6,24}
   (b) {3,5,15}
   (c) {1,2,3,6,12}
   (d) {2,4,8,16}
   (e) {3,9,27,54}
2. Give an example of a set A such that $< P(A), \subseteq >$ is a totally ordered set.
3. Give a relation which is both partial ordering and an equivalence on a set.
4. Draw all the Hasse diagrams corresponding to four elements.

Chapter 7

Lattice

7.1 Lattice

7.1.1 Definition

A POSET $< L, \subseteq >$ is said to be lattice if for every pair of elements a,b $\in$ L, its greatest lower bound and least upper bound exists.
Greatest lower bound is denoted by a$\wedge$b and least upper bound is denoted by a$\vee$b.

7.1.2 Some examples

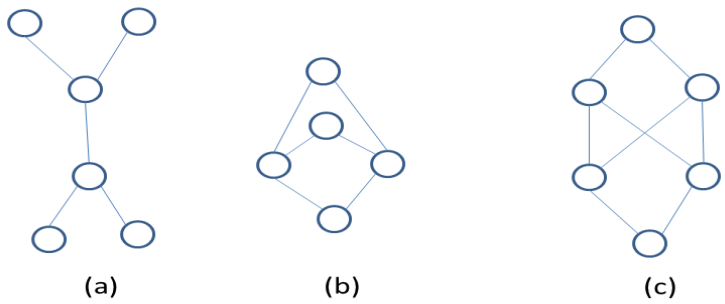
Example: Is POSET $< P(A), \subseteq >$ a lattice, where A = {1,2,3}?
Solution: In this POSET, greatest lower bound of two elements of P(A) is equivalent to intersection of those elements and least upper bound of two elements of P(A) is equivalent to union of those elements.
Clearly, intersection and union of any two elements of P(A) always exists in P(A). Therefore this POSET is lattice.

Example: Let I_+ be the set of all positive integers and D denote the relation of division in I_+ such that for any a,b $\in I_+$, aDb iff a divides b. Is (I_+,D) a lattice?
Solution: In this example, first we have to check this set is POSET or Not. After this, we have to check for lattice.
Clearly, this set is POSET because it satisfies all the three properties.
Clearly, for each pair of integers, its least upper bound and greatest lower bound exists because the operation is division and set is set of all positive integers. For example, consider two elements 4 and 6. Its lub = 12 and glb = 2. Both 2 and 12 belongs into I_+. Similarly for elements 3 and 4, lub = 12 and glb = 1. Here 1 and 12 both belong into I_+. Therefore this set is lattice.

Example: Let n be a positive integer and S_n be the set of all positive divisors of n. And D is a division relation. Is (S_6,D), (S_8,D), (S_{24},D), and(S_{30},D) lattices?
Solution: All these are lattices.

7.1.3 Exercise

1. Find out the following POSETs are lattices or not.



2. Draw the diagram of lattices $< S_n, D >$ for n = 4, 6, 10, 12, 15, 45, 60, 75 and 210. For what values of n, do you expect $< S_n, D >$ to be a chain?

3. Let R be the set of real numbers in [0,1] and $\preceq$ be the usual operation of "less than or equal" on R. Show that $< R, \preceq >$ is a lattice. What are the operations of meet and join on this lattice?

4. Let the sets $S_0, S_1, S_2, S_3, S_4, S_5, S_6, S_7$ be given by
   S_0 = {a,b,c,d,e,f} S_1 = {a,b,c,d,e} S_2 = {a,b,c,e,f} S_3 = {a,b,c,e}
   S_4 = {a,b,c} S_5 = {a,b} S_6 = {a,c} S_7 = {a}
   Draw the diagram of $< L, \subseteq >$, where L = $\{S_0, S_1, S_2, S_3, S_4, S_5, S_6, S_7\}$.

7.1.4 Principle of Duality

Any statement about lattices involving the operations $\wedge$ and $\vee$ remains true if $\wedge$ is replaced by $\vee$ and $\vee$ is replaced by $\wedge$.
The operations $\wedge$ and $\vee$ are said to be dual of each other. For example a$\wedge$b is the dual of a$\vee$b.

7.1.5 Properties of lattices

(1) Idempotent law
a$\wedge$a = a , a$\vee$a = a
(2) Commutative law
a$\wedge$b = b$\wedge$a , a$\vee$b = b$\vee$a
(3) Associative law
a$\wedge$(b$\wedge$c) = (a$\wedge$b)$\wedge$c , a$\vee$(b$\vee$c) = (a$\vee$b)$\vee$c
(4) Absorption law
a$\wedge$(a$\vee$b) = a , a$\vee$(a$\wedge$b) = a

Theorem: Let $< L, \preceq >$ be a lattice. For any a,b $\in$ L,
a $\preceq$ b $\Leftrightarrow$ a$\wedge$b = a $\Leftrightarrow$ a$\vee$b = b
Proof: In this theorem,we have to prove many parts.
First part: In this part, we will prove a $\preceq$ b $\Leftrightarrow$ a$\wedge$b = a.

Suppose a $\preceq$ b. Since a $\preceq$ a, therefore a = lower bound(l.b.) of a and b.
Since a is lower bound therefore, a$\preceq$ greatest lower bound(g.l.b.) of a and b.
hence a $\preceq$ a$\wedge$b .....(1)
By the definition of glb, a$\wedge$b $\preceq$ a .....(2)
from (1) and (2),
a$\wedge$b = a.
Conversely, suppose a$\wedge$b = a.
By the definition of glb,
a$\wedge$b $\preceq$ b
Since a$\wedge$b = a, therefore a $\preceq$ b.

Second part: In this part, we will prove a $\preceq$ b $\Leftrightarrow$ a$\vee$b = b.
Suppose a $\preceq$ b. Since b $\preceq$ b, therefore b = upper bound(u.b.) of a and b.
Since b is an upper bound therefore, least upper bound(l.u.b.) of a and b $\preceq$ b.
hence a$\vee$b $\preceq$ b .....(1)
By the definition of lub, b $\preceq$ a$\vee$b .....(2)
from (1) and (2),
a$\vee$b = b.
Conversely, suppose a$\vee$b = b.
By the definition of lub,
a $\preceq$ a$\vee$b
Since a$\vee$b = b, therefore a $\preceq$ b.

Third part: In this part, we will prove a$\wedge$b = a $\Leftrightarrow$ a$\vee$b = b.
Suppose a $\wedge$ b = a.
Now, a$\vee$b = (a$\wedge$b)$\vee$b = b , by absorption law.
Suppose a $\vee$ b = b.
Now, a$\wedge$b = a$\wedge$(a$\vee$b) = a , by absorption law.

Theorem: Let $< L, \preceq >$ be a lattice. For any a,b,c $\in$ L,
(1) a$\vee$(b$\wedge$c) $\preceq$ (a$\vee$b)$\wedge$ (a$\vee$c)
(2) a$\wedge$(b$\vee$c) $\succeq$ (a$\wedge$b)$\vee$ (a$\wedge$c)

Proof:
(1) Using definition of least upper bound, a $\preceq$ (a$\vee$b).....(1)
Using definition of greatest lower bound, b$\wedge$c $\preceq$ b .....(2)
Using definition of least upper bound, b $\preceq$ (a$\vee$b).....(3)
From (2) and (3), b$\wedge$c $\preceq$ b $\preceq$ (a$\vee$b)
Therefore, b$\wedge$c $\preceq$ (a$\vee$b).....(4)
From (1) and (4), (a$\vee$b) is the upper bound of a and b$\wedge$c, therefore
lub{a , b$\wedge$c} $\preceq$ (a$\vee$b) i.e.
a$\vee$(b$\wedge$c) $\preceq$ (a$\vee$b) .....(5)
Similarly, using definition of least upper bound, a $\preceq$ (a$\vee$c).....(6)
Using definition of greatest lower bound, b$\wedge$c $\preceq$ c .....(7)
Using definition of least upper bound, c $\preceq$ (a$\vee$c).....(8)
From (7) and (8), b$\wedge$c $\preceq$ c $\preceq$ (a$\vee$c)
Therefore, b$\wedge$c $\preceq$ (a$\vee$c).....(9)
From (6) and (9), (a$\vee$c) is the upper bound of a and b$\wedge$c, therefore

lub{a , b∧c} ⪯ (a∨c) i.e.
a∨(b∧c) ⪯ (a∨c) .....(10)
From (5) and (10), a∨(b∧c) is lower bound of (a∨b) and (a∨c), therefore
a∨(b∧c) ⪯ glb{(a∨b), (a∨c)} i.e.
a∨(b∧c) ⪯ (a∨b)∧(a∨c)
Now, it is proved.

(2) Using definition of greatest lower bound, (a∧b)⪯ a .....(1)
Using definition of least upper bound, b ⪯ (b∨c).....(2)
Using definition of greatest lower bound, (a∧b)⪯ b.....(3)
From (2) and (3), (a∧b)⪯ b ⪯ (b∨c)
Therefore, (a∧b) ⪯ b∨c.....(4)
From (1) and (4), (a∧b) is the lower bound of a and b∨c, therefore
(a∧b)⪯ glb{a , b∨c} i.e.
(a∧b)⪯ a∧(b∨c) .....(5)
Similarly, using definition of greatest lower bound, (a∧c)⪯ a .....(6)
Using definition of least upper bound, c ⪯ (b∨c).....(7)
Using definition of greatest lower bound, (a∧c)⪯ c.....(8)
From (7) and (8), (a∧c)⪯ c ⪯ (b∨c)
Therefore, (a∧c) ⪯ (b∨c).....(9)
From (6) and (9), (a∧c) is the lower bound of a and (b∨c), therefore
(a∧c)⪯ glb{a , b∨c} i.e.
(a∧c)⪯ a∧(b∨c) .....(10)
From (5) and (10), a∧(b∨c) is upper bound of (a∧b) and (a∧c), therefore
lub{(a∧b), (a∧c)} ⪯ a∧(b∨c) i.e.
(a∧b)∨(a∧c)} ⪯ a∧(b∨c)
Now, it is proved.

Theorem: Let $< L, \preceq >$ be a lattice. For any a,b,c ∈ L,
a ⪯ c ⇔ a∨(b∧c) ⪯ (a∨b)∧c
Proof:
First part: In this part, we will prove that if a ⪯ c then a∨(b∧c) ⪯ (a∨b)∧c
Suppose a ⪯ c.
Using definition of least upper bound, a ⪯ (a∨b).....(1)
Using definition of greatest lower bound, (b∧c) ⪯ b .....(2)
Using definition of least upper bound, b ⪯ (a∨b) .....(3)
Therefore, from (2) and (3), (b∧c) ⪯ b ⪯ (a∨b)
Therefore, (b∧c) ⪯ (a∨b) .....(4)
From (1) and (4), (a∨b) is the upper bound of a and b∧c, therefore
lub{a , b∧c} ⪯ (a∨b) i.e.
a∨(b∧c) ⪯ (a∨b) .....(5)
Now, using definition of greatest lower bound, (b∧c) ⪯ c .....(6)
Since a ⪯ c, therefore using (6), c is an upper bound of a and (b∧c). Therefore
a∨(b∧c) ⪯ c .....(7)
from (5) and (7), a∨(b∧c) is lower bound of (a∨b) and c. Therefore,
a∨(b∧c) ⪯ (a∨b)∧c
Second part: In this part, we will prove that if a∨(b∧c) ⪯ (a∨b)∧c then a ⪯ c.
Now, a ⪯ a∨(b∧c) ⪯ (a∨b)∧c ⪯ c

Therefore, a $\preceq$ c.
Since both parts are proved. Therefore, it is proved.

7.1.6 Exercise

1. Show that in a lattice if a $\preceq$ b $\preceq$ c, then
   a$\vee$b = b$\wedge$c and (a$\wedge$b)$\vee$(b$\wedge$c) = b = (a$\vee$b)$\wedge$(a$\vee$c)
2. Show that in a lattice if a $\preceq$ b and c $\preceq$ d, then
   (a$\wedge$c) $\preceq$ (b$\wedge$d)
3. In a lattice, show that
   (a) (a$\wedge$b)$\vee$ (c$\wedge$d) $\preceq$ (a$\vee$c)$\wedge$ (b$\vee$d)
   (b) (a$\wedge$b)$\vee$ (b$\wedge$c) $\vee$ (c$\wedge$a) $\preceq$ (a$\vee$b)$\wedge$ (b$\vee$c) $\wedge$ (c$\vee$a)
4. Show that a lattice with three or fewer elements is a chain.

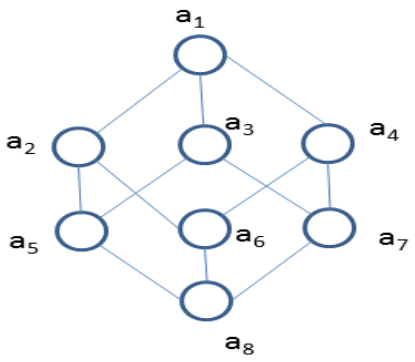
7.1.7 Lattices as algebraic system

A lattice is an algebraic system $< L, \wedge, \vee >$ with two binary operations $\wedge$ and $\vee$ on L which are satisfy commutative, associative, absorption and idempotent properties.

7.1.8 Sublattice

Let $< L, \wedge, \vee >$ be a lattice and let S $\subseteq$ L be a subset of L. Then $< S, \wedge, \vee >$ is said to be sublattice of $< L, \wedge, \vee >$ iff $< S, \wedge, \vee >$ is also a lattice.

Example: Consider the following lattice L = $\{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8\}$.
Let $S_1 = \{a_1, a_2, a_4, a_6\}$, $S_2 = \{a_3, a_5, a_7, a_8\}$, and $S_3 = \{a_1, a_2, a_4, a_8\}$.



Find out $< S_1, \prec >, < S_2, \prec >, and < S_3, \prec >$ sublattices or not.

7.2 Types of morphism in lattice

7.2.1 Lattice Homomorphism

Let $< L, \otimes, \oplus >$ and $< S, \wedge, \vee >$ be two lattices. A mapping f: L $\rightarrow$ S is called lattice homomorphism from the lattice $< L, \otimes, \oplus >$ to $< S, \wedge, \vee >$ if for any (a,b) $\in$ L,
f(a$\otimes$b) = f(a)$\wedge$f(b) and f(a$\oplus$b) = f(a)$\vee$f(b)

7.2.2 Lattice Isomorphism

A homomorphism f: L $\rightarrow$ S is said to be isomorphism if f is bijective.
If there exists isomorphism between two lattices, then the lattices are called isomorphic.

7.2.3 Lattice Endomorphism

A homomorphism is said to be endomorphism if both lattices are same.

7.2.4 Lattice Automorphism

An isomorphism is said to be autoomorphism if both lattices are same.

7.2.5 Order-preserving

Let $< P, \preceq >$ and $< Q, \preceq' >$ be two POSETs. A mapping f: P$\rightarrow$Q is said to be order-preserving relatie to the ordering $\prec$ in P and $\prec$' in Q iff for any a,b $\in$ P such that a $\prec$ b, f(a) $\prec$' f(b).
Note: If f is homomorphism, then f is order-preserving.

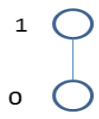
7.2.6 Order-isomorphic

Two POSETs $< P, \preceq >$ and $< Q, \preceq' >$ are called order-isomorphic if there exists a mapping f: P$\rightarrow$Q which is bijective and if both f and f^1 are order-preserving.
Note: It may happen that a mapping f: P$\rightarrow$Q is bijective and order-preserving, but that f^1 is not order-preserving.

7.2.7 Direct product or Cartesian product

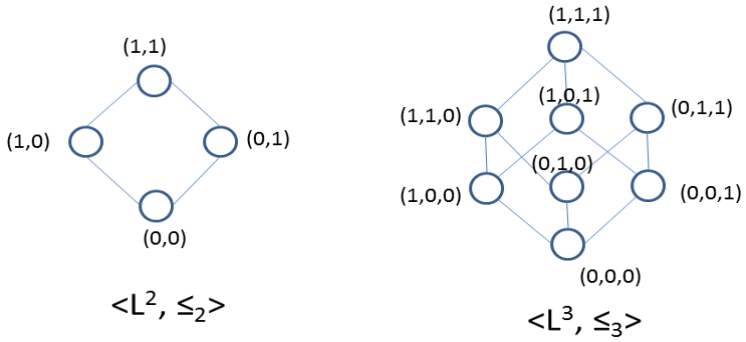
Let $< L, \otimes, \oplus >$ and $< S, \wedge, \vee >$ be two lattices. The algebraic system $< L \times S, *, + >$ in which the binary operations + and * on L$\times$S are such that for any (a_1, b_1) and (a_2, b_2) in L$\times$S
(a_1, b_1) * $(a_2, b_2) = (a_1 \otimes a_2, b_1 \wedge b_2)$
(a_1, b_1) + $(a_2, b_2) = (a_1 \oplus a_2, b_1 \vee b_2)$
is called the direct product of the lattices $< L, \otimes, \oplus >$ and $< S, \wedge, \vee >$.
Note: L^2 = L$\times$L and L^3 = L$\times$L$\times$L

Example: Let L = {0,1} and the lattice $< L, \prec >$ is



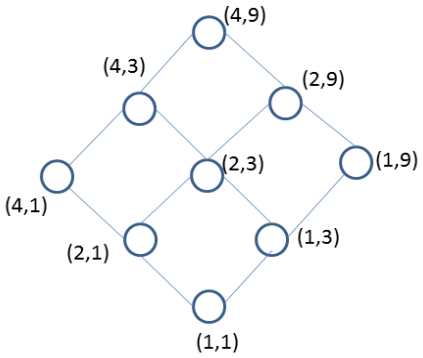
Find the lattices $< L^2, \prec_2 >$ and $< L^3, \prec_3 >$.
Solution: Lattices $< L^2, \prec_2 >$ and $< L^3, \prec_3 >$ are drawn as following:-

Note: The partial ordering relation $\preceq^n$ on L^n can be defined for any a,b $\in L^n$, where



a = $(a_1, a_2, ..., a_n)$ and $(b_1, b_2, ..., b_n)$, as
a$\prec_n$b $\Leftrightarrow$ $a_i \preceq b_i$, $\forall$ i.
Where $\preceq$ means the relation of "less than or equal to" on {0,1}.

Example: Consider the chains of divisors of 4 and 9, that is L_1 = {1,2,4} and L_2 = {1,3,9}, and the partial order relation of "division" on L_1 and L_2. Draw the Hasse diagram for $L_1 \times L_2$.
Solution: Hasse diagram for this lattice can be drawn as following:-

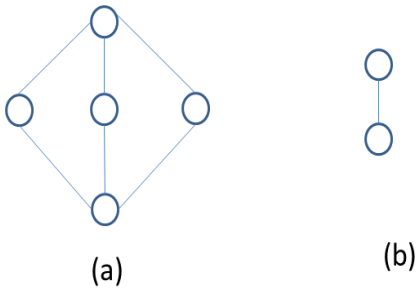


This diagram is same as the lattice of divisors of 36, where (a, b) is replaced by the product ab.
Example: Let S be any set containing n elements and P(S) be its power set. Then the lattice $< P(S), \cap, \cup >$ or $< P(S), \subseteq >$ is isomorphic to the lattice $< L^n, \prec_n >$.

7.2.8 Exercise

1. Find all the sublattices of the lattice $< D(n), / >$, for n = 12.

2. Draw the diagram of a lattice which is the direct product of the five element lattice and a two element lattice.



7.3 Types of lattice

7.3.1 Complete lattice

A lattice is called complete if each of its non-empty subsets has a least upper bound and a greatest lower bound.

7.3.2 Bounded lattice

Bounds: The least and greatest elements of a lattice, if they exists, are called the bounds of the lattice and are denoted by 0 and 1 respectively.
Definition: A lattice which has both least and greatest elements i.e. 0 and 1, is called a bounded lattice.
Note: The bounds 0 and 1 of a lattice satisfy the following identities:-
For any a $\in$ L, a$\wedge$0 = 0, a$\wedge$1 = a
a$\vee$0 = a, a$\vee$1 = 1.

7.3.3 Complemented lattice

In a bounded lattice, an element b $\in$ L is said to be complement of an element a $\in$ L if a$\wedge$b = 0 and a$\vee$b = 1.
A lattice $< L, \wedge, \vee, 0, 1 >$ is said to be a complemented lattice if every element of L has at least one complement.

7.3.4 Some examples

Example: Is the lattice $< P(\{a, b, c\}), \subseteq >$ a complemented?
Solution: This lattice will be complemented if eery element has complement in this lattice.
P({a,b,c}) = {ϕ,{a},{b},{c},{a,b},{b,c},{a,c},{a,b,c}}
In this lattice, least element i.e. 0 = ϕ and greatest element i.e. 1 = {a,b,c}
The complement of ϕ will be {a,b,c}, because $\phi\wedge${a,b,c} = ϕ and $\phi\vee${a,b,c} = {a,b,c}.
Similarly, the complement of {a,b,c} will be ϕ.
Similarly, {a}' = {b,c}, {b}' = {a,c}, {c}' = {a,b}.
{a,b}' = {c}, {a,c}' = {b}, and {b,c}' = {a}
Clearly each element has a complement, therefore this lattice is complemented.

Example: Is the lattice $< D(30), / >$ a complemented?
Solution: Here, D(30) = {1,2,3,5,6,10,15,30}

Two elements a and b will be complement of each other iff a∧b = 0 and a∨b = 1.
In this eample, 0(least element) = 1 and 1(greatest element) = 30.
Since 2∧15 = 1 and 2∨15 = 30, therefore 2 and 15 are complement of each other.
Since 3∧10 = 1 and 3∨10 = 30, therefore 3 and 10 are complement of each other.
Since 5∧6 = 1 and 5∨6 = 30, therefore 5 and 6 are complement of each other.
Since 1∧30 = 1 and 1∨30 = 30, therefore 1 and 30 are complement of each other.
Clearly each element has a complement, therefore this lattice is complemented.

Example: Is the lattice $< D(12), / >$ a complete?
Solution: Here, D(12) = {1,2,3,4,6,12}
Since this lattice is finite, therefore every subset of this set has a least upper bound and greatest lower bound. Clearly, consider the set {2,3,4}. The least upper bound of this set is 12 because each elements of this set divides 12 and no other elements in this. The greatest lower bound will be 1 because 1 diides to each elements of this set. Similarly, we can check for any subset of the given lattice.
Therefore this lattice is complete.

7.3.5 Distributive lattice

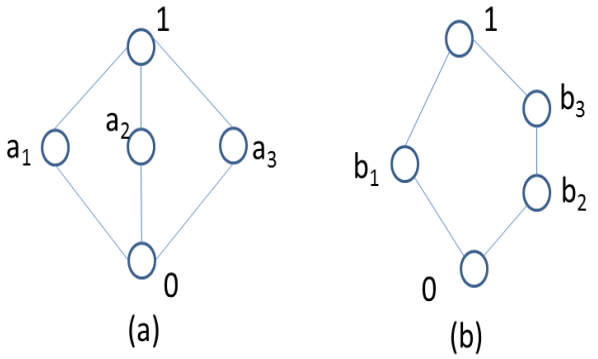
A lattice $< L, \wedge, \vee >$ is called a distributive lattice if for any a,b,c ∈ L,
$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$
and $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$

7.3.6 Modular lattice

A lattice $< L, \wedge, \vee >$ is called a modular lattice if for any a,b,c ∈ L,
a$\preceq$c $\Rightarrow a \vee (b \wedge c) = (a \vee b) \wedge c$.

7.3.7 Some examples

Example: Check the following lattices to be modular or distributive.



Solution:
(a) For modular lattice:
Consider three elements a,b,c belongs into the lattice such that a$\preceq$c.
Let a = a_1, b = a_2, and c = 1.
Therefore, $a \vee (b \wedge c) = a_1 \vee (a_2 \wedge 1) = a_1 \vee a_2 = 1$

and $(a \vee b) \wedge c = (a_1 \vee a_2) \wedge 1 = 1 \wedge 1 = 1$
Therefore, a$\preceq$c $\Rightarrow a \vee (b \wedge c) = (a \vee b) \wedge c$ for a = a_1, b = a_2, and c = 1.
Similarly, we can show that a$\preceq$c $\Rightarrow a \vee (b \wedge c) = (a \vee b) \wedge c$ for any a,b,c belongs into lattice such that a$\preceq$c. Therefore, this lattice is modular lattice.
For distributive lattice:
Consider three elements a,b,c belongs into the lattice.
Let a = a_1, b = a_2, and c = a_3.
Therefore, $a \wedge (b \vee c) = a_1 \wedge (a_2 \vee a_3) = a_1 \wedge 1 = a_1$
and $(a \wedge b) \vee (a \wedge c) = (a_1 \wedge a_2) \vee (a_1 \wedge a_3) = 0 \vee 0 = 0$
Clearly, $a \wedge (b \vee c) \neq (a \wedge b) \vee (a \wedge c)$ for a = a_1, b = a_2, and c = a_3. Therefore this lattice is not distributive.

Example: Show that every chain is a distributive lattice.
Solution: Consider any three elements a,b,c of a chain. There will be six different relations exist between these elements.
Case-1: $(a \preceq b \preceq c)$**:**
In this case, $a \wedge (b \vee c) = a \wedge c =$ a
and $(a \wedge b) \vee (a \wedge c) = a \vee a =$ a
Therefore, $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$
Similarly, $a \vee (b \wedge c) = a \vee b =$ b
and $(a \vee b) \wedge (a \vee c) = b \wedge c =$ b
Therefore, $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$
Clearly, both properties of distributive lattice are satisfied for this case.

Case-2: $(a \preceq c \preceq b)$**:**
In this case, $a \wedge (b \vee c) = a \wedge b =$ a
and $(a \wedge b) \vee (a \wedge c) = a \vee a =$ a
Therefore, $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$
Similarly, $a \vee (b \wedge c) = a \vee c =$ c
and $(a \vee b) \wedge (a \vee c) = b \wedge c =$ c
Therefore, $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$
Clearly, both properties of distributive lattice are satisfied for this case.

Similarly, we can show for other four cases that properties of distributive lattice are satisfied. Other four case are (3) $(b \preceq a \preceq c)$ (4) $(b \preceq c \preceq a)$ (5) $(c \preceq a \preceq b)$ (6) $(c \preceq b \preceq a)$.
Since, in all the cases, properties of distributive lattice are satisfied, therefore a chain is distributive lattice.

Example: Let $< L, \wedge, \vee >$ be a distributive lattice. For any a,b,c $\in$ L,
a$\wedge$b = a$\wedge$c and a$\vee$b = a$\vee$c $\Rightarrow$ b = c.
Solution:
LHS = b = $b \wedge (b \vee a)$ (using absorption law)

$= b \wedge (a \vee b)$ (using commutative law)
$= b \wedge (a \vee c)$ (using given equality a∨b = a∨c)
$= (b \wedge a) \vee (b \wedge c)$ (using distributive law)
$= (a \wedge b) \vee (b \wedge c)$ (using commutative law)
$= (a \wedge c) \vee (b \wedge c)$ (using given equality a∧b = a∧c)
$= (a \wedge b) \vee c)$ (using distributive law)
$= (a \wedge c) \vee c)$ (using given equality a∧b = a∧c)
= c (using absorption law)
= RHS
Therefore, b = c

Example: In a distributive lattice, every element has a unique complement.
Solution: Consider an element a belong into given lattice L. Suppose b and c are two complements of a in L. Therefore,
a∧b = 0, a∨b = 1 , and a∧c = 0, a∨c = 1. .....(1)
Now, we have to show that b and c will be equal.
b = b∧1 (using identity law)
= b∧(a∨c) (using equation (1))
$= (b \wedge a) \vee (b \wedge c)$ using distributive law)
$= 0 \vee (b \wedge c)$ (using equation (1))
$= (a \wedge c) \vee (b \wedge c)$ (using equation (1))
$= (a \wedge b) \vee c$ (using distributive law)
$= 0 \vee c$ (using equation (1))
= c (using identity law)
Therefore, b = c. That is, we can say, every element has a unique complement.

7.3.8 Exercise

1. Find the complements of every elements of the lattice $< D(n), / >$ for n = 75.
2. Show that in a lattice with two or more elements, no element is its own complement.
3. Show that a chain of three or more elements is not complemented.
4. Which of the two lattices $< D(n), / >$ for n = 30 and n = 45 are complemented? Are these lattices are distributive?
5. Show that De-Morgan's law given by
(a∧b)' = a'∨b' and (a∨b)' = a'∧b'
hold in complemented and distributive lattice.
6. Show that in a complemented, distributive lattice,
a⪯b ⇔ a∧b' = 0 ⇔ a'∨b = 1 ⇔ b'⪯a'
7. Show that every distributive lattice is modular, but not conversely.

Chapter 8

Boolean algebra

8.1 Boolean algebra

8.1.1 Definition

A lattice is said to be boolean algebra if it is both complemented and distributive. It is denoted by $< B, \wedge, \vee, ', 0, 1 >$.

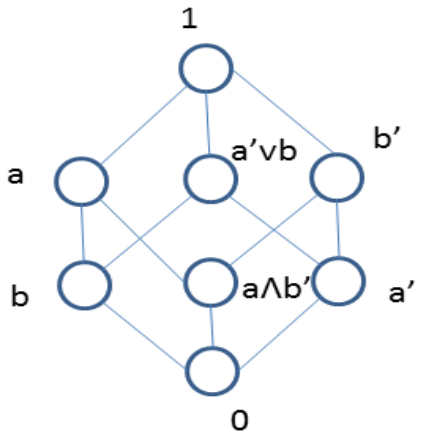
8.1.2 Some examples

Example: $< P(S), \cap, \cup, ', \phi, S >$ is a boolean algebra. Because it is complemented and distributive both. In this lattice, 0 is ϕ and 1 is S. Each elements of P(S) has a complement.

Example: $< D(30), gcd, lcm, ', 1, 30 >$ is a boolean algebra.

8.1.3 Sub-boolean algebra

Let $< B, \wedge, \vee, ', 0, 1 >$ be a boolean algebra and S $\subseteq$ B. If S contains the elements 0 and 1 and is closed under the operations $\wedge, \vee$ and ', then $< S, \wedge, \vee, ', 0, 1 >$ is called a sub-boolean algebra.
Example: Consider the following boolean algebra.



Let the subsets of this boolean algebra are:-
S_1 = {a,a',0,1} S_2 = {a'∨b ,a∧b',0,1} S_3 = {a∧b' ,b',a,1}
S_4 = {b' ,a∧b',a',0} S_5 = {a,b',0,1}
Find out which are sub-boolean algebra.
Solution: Consider the subset S_1. Since S_1 is subset of B, therefore it satisfies distributive property. Now, 0 and 1 are also belongs into this subset. Complement of each element is also belong into S_1. Since a and a' are complement of each other. we know 0 and 1 are complement of each other. Therefore, S_1 is sub-boolean algebra.
Consider the subset S_2. Since S_1 is subset of B, therefore it satisfies distributive property. Now, 0 and 1 are also belongs into this subset.
Clearly from diagram, complement of a'∨b = a∧b'. complement of 0 = 1. Therefore, S_2 is sub-boolean algebra.
Consider the subset S_3. In this subset 0 is not belong, therefore this subset is not a boolean algebra.
Consider the subset S_4. In this subset 1 is not belong, therefore this subset is not a boolean algebra.
Consider the subset S_5. In this subset, complement of a and b' do not exists, therefore this subset is also not a boolean algebra.

8.2 Boolean expression

8.2.1 Boolean expression

Definition: A Boolean expression always produces a Boolean value. A Boolean expression is composed of a combination of the Boolean constants (True or False), Boolean variables and logical connectives. Each Boolean expression represents a Boolean function. A Boolean expression in n variables $x_1, x_2, ..., x_n$ is any finite string of symbols formed in the following manner:-
(1) 0 and 1 are Boolean expressions.
(2) $x_1, x_2, ..., x_n$ are Boolean expressions.
(3) If α_1 and α_2 are Boolean expressions, then $\alpha_1 \wedge \alpha_2$ and $\alpha_1 \vee \alpha_2$ are also Boolean expressions.
(4) If α is a Boolean expression then α' is also a Boolean expression.
(5) All the expressions formed by step 1 to 4, are also Boolean expressions.
Example: x_1, $x_1' \vee x_2$, $(x_2' \vee x_1)' \wedge (x_3 \vee x_1)$, and $(x_1' \vee x_1) \wedge x_2 \wedge x_3'$ are all Boolean expressions.

Equivalent Boolean expressions: Two Boolean expressions α and β are said to be equivalent if one can be obtained from the other by a finite number of applications of the identities of a Boolean algebra.

Minterm: A Boolean expression of n variables in the following form is said to be minterm.

$$x_1^{\alpha_1} \wedge x_2^{\alpha_2} \wedge ..... \wedge x_n^{\alpha_n}$$

where α_i is either 0 or 1, x_i^0 stands for x_i' and x_i^1 stands for x_i.
Maxterm: A Boolean expression of n variables in the following form is said to be maxterm.

$x_1^{\alpha_1} \vee x_2^{\alpha_2} \vee \ldots\ldots\ldots\ldots \vee x_n^{\alpha_n}$
where α_i is either 0 or 1, x_i^0 stands for x_i' and x_i^1 stands for x_i.

Canonical sum of product form: A Boolean expression is said to be in canonical sum of product form if it is the join of only minterms.
For example, for three variables, Boolean expression $(x_1' \wedge x_2' \wedge x_3') \vee (x_1' \wedge x_2 \wedge x_3')$ is in canonical sum of product form.

Canonical product of sum form: A Boolean expression is said to be in canonical product of sum form if it is the meet of only maxterms.
For example, for three variables, Boolean expression $(x_1' \vee x_2' \vee x_3') \wedge (x_1' \vee x_2 \vee x_3')$ is in canonical product of sum form.

Example: Obtain the values of the Boolean expression (1) $x_1 \wedge (x_1' \vee x_2)$ (2) $x_1 \wedge x_2$ and (3) $x_1 \vee (x_1 \wedge x_2)$
over the ordered pairs of the two elements Boolean algebra.

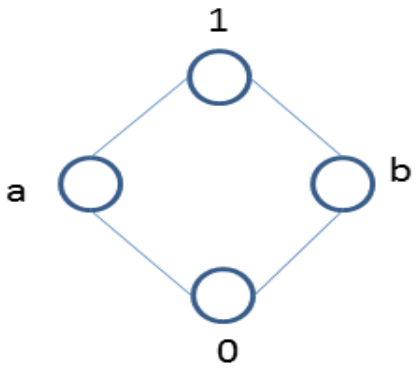
Solution: Let B = {0,1}. Consider $x_1 = 0$ and $x_2 = 1$.

(1) $x_1 \wedge (x_1' \vee x_2) = (x_1 \wedge x_1') \vee (x_1 \wedge x_2)$
$= 0 \vee (x_1 \wedge x_2)$
$= x_1 \wedge x_2$
$= 0 \wedge 1$ (putting the values of $x_1 = 0$ and $x_2 = 1$)
$= 0.$

(2) $x_1 \wedge x_2 = 0 \wedge 1$ (putting the values of $x_1 = 0$ and $x_2 = 1$)
$= 0.$

(3) $x_1 \vee (x_1 \wedge x_2) = 0 \vee (0 \wedge 1)$
$= 0 \vee 0 = 0.$

Example: Find the value of following Boolean expression
$x_1 \wedge x_2 \wedge [(x_1 \wedge x_4) \vee x_2' \vee (x_3 \wedge x_1')]$
for $x_1 = a$, $x_2 = 1$, $x_3 = b$, $x_4 = 1$, where 1,a,b $\in$ B and the Boolean algebra B is the following:-

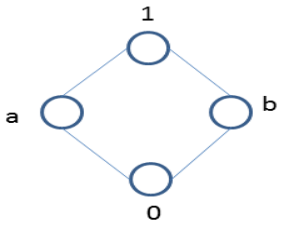


Solution:
$f(x_1, x_2, x_3) = x_1 \wedge x_2 \wedge [(x_1 \wedge x_4) \vee x_2' \vee (x_3 \wedge x_1')]$
$= a \wedge 1 \wedge [(a \wedge 1) \vee 1' \vee (b \wedge a')]$
$= a \wedge [a \vee 0 \vee (b \wedge b)]$
$= a \wedge [a \vee b]$
$= a \wedge 1$
$= a$

x_1	x_2	x_3	$\alpha(x_1, x_2, x_3)$
0	0	0	1
0	0	1	0
0	1	0	1
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	0

Note: Given a Boolean expression $\alpha(x_1, x_2, ..., x_n)$ and a Boolean algebra $< B, \wedge, \vee, ', 0, 1 >$, we can obtain the values of the Boolean expression for every n-tuple of B^n. Let us now consider a function $f_{\alpha,B} : B^n \to B$ such that for any n-tuple $< a_1, a_2, ..., a_n > \in B^n$, the value of $f_{\alpha,B}$ is equal to the value of the Boolean expression $\alpha(x_1, x_2, ..., x_n)$, that is,
$f_{\alpha,B}(a_1, a_2, ..., a_n) = \alpha(x_1, x_2, ..., x_n)$
for all $(a_1, a_2, ..., a_n) \in B^n$. We shall call $f_{\alpha,B}$ the function associated with the Boolean expression $\alpha(x_1, x_2, ..., x_n)$.

Example: Find the value of the function $f_{\alpha,B} : B^3 \to B$ for x_1 = a, x_2 = 1,and x_3 = b, where a,b,1 are the elements of the Boolean algebra is shown in the following figure:-



and $\alpha(x_1, x_2, ..., x_n)$ is the expression whose binary valuation is given in the following table:-

Solution: From the table,
$f_{\alpha,B}(x_1, x_2, x_3) = (x_1' \wedge x_2' \wedge x_3') \vee (x_1' \wedge x_2 \wedge x_3') \vee (x_1' \wedge x_2 \wedge x_3) \vee (x_1 \wedge x_2' \wedge x_3)$
$\alpha(a, 1, b) = (a' \wedge 1' \wedge b') \vee (a' \wedge 1 \wedge b') \vee (a' \wedge 1 \wedge b) \vee (a \wedge 1' \wedge b)$
$= (b \wedge 0 \wedge a) \vee (b \wedge 1 \wedge a) \vee (b \wedge 1 \wedge b) \vee (a \wedge 0 \wedge b)$
$= 0 \vee (b \wedge a) \vee b \vee 0$
$= (b \wedge a) \vee b$
$= 0 \vee b$
$= b$

8.2.2 Boolean function

Let $< B, \wedge, \vee, ', 0, 1 >$ ba Boolean algebra. A function f: $B^n \to$ B which is associated with a Boolean expression in n-variables is called a Boolean function.

Note: For a two elements Boolean algebra, the number of functions from B^n to B

is 2^{2^n}. Here, every function from B^n to B is Boolean function.

8.2.3 Symmetric Boolean expression

A Boolean expression in n variables is called symmetric if interchanging any two variables results in an equivalent expression.
Example: Following expressions are symmetric.
(a) $(x_1 \wedge x_2') \vee (x_1' \wedge x_2)$
(b) $(x_1 \wedge x_2 \wedge x_3') \vee (x_1 \wedge x_2' \wedge x_3) \vee (x_1' \wedge x_2 \wedge x_3)$

8.2.4 Exercise

1. Find the canonical sum of product form of the following Boolean expressions:-

   (a) $x_1 \vee x_2$

   (b) $x_1 \vee (x_2 \wedge x_3')$

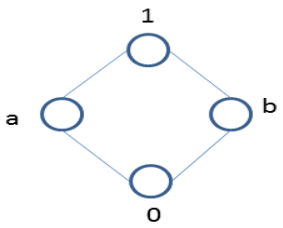
   (c) $(x_1 \vee x_2)' \vee (x_1' \wedge x_3)$

2. Show that

   (a) $(a \wedge (b' \vee c))' \wedge (b' \vee (a \wedge c')')' = (a \wedge b \wedge c')$

   (b) $a' \wedge ((b' \vee c)' \vee (b \wedge c)) \vee ((a \vee b')' \wedge c) = a' \wedge b$

3. Given an expression $\alpha(x_1, x_2, x_3)$ defined to be Σ 0,3,5,7, determine the value of $\alpha(a, b, 1)$, where a,b,1 $\in$ B and $< B, \wedge, \vee, ', 0, 1 >$ is the following Boolean algebra.

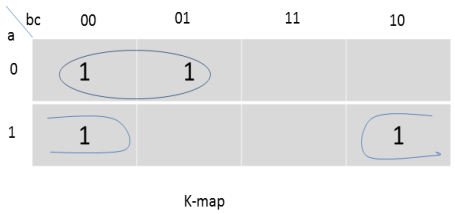


4. Obtain simplified Boolean expressions which are equivalent to these expressions:-

   (a) $m_0 + m_7$

   (b) $m_0 + m_1 + m_2 + m_3$

   (c) $m_5 + m_7 + m_9 + m_1 1 + m_1 3$
   Where m_j are the minterms in the variables x_1, x_2, x_3, and x_4.



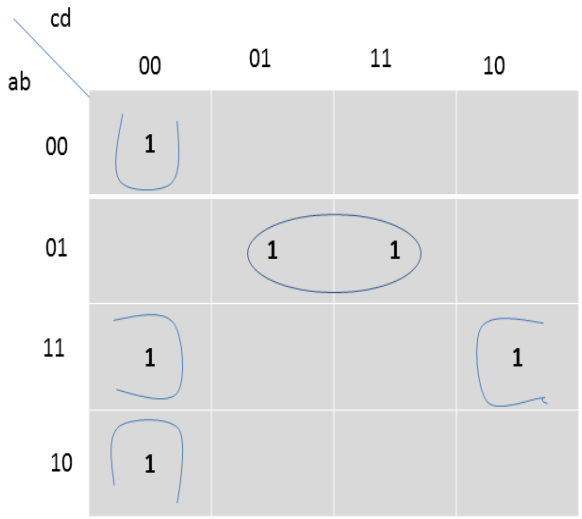
K-map

8.2.5 Minimization of Boolean function or expression

We shall minimize the Boolean function or expression using Karnaugh map.
Example: Minimize the following function using K-map.
f(a,b,c) = $\Sigma(0, 1, 4, 6)$
Solution:

The minimized function will be, f(a,b,c) = $(a' \wedge b') \vee (a \wedge c')$.

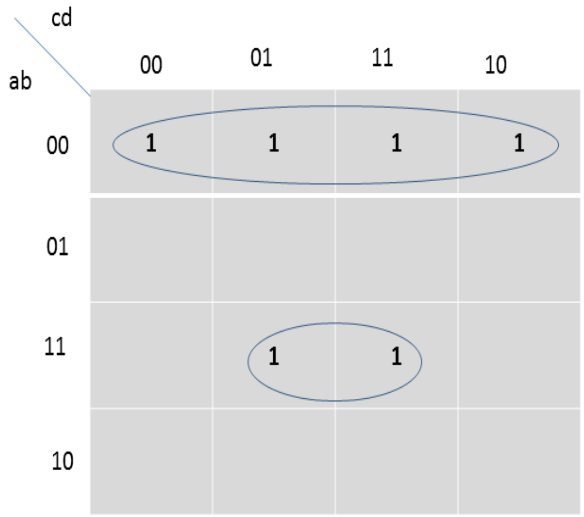
Example: Minimize the following function using K-map.
f(a,b,c,d) = $\Sigma(0, 5, 7, 8, 12, 14)$
Solution:



K-map

The minimized function will be, f(a,b,c,d) = $(a' \wedge b \wedge d') \vee (b' \wedge c' \wedge d') \vee (a \wedge b \wedge d')$.

Example: Minimize the following function using K-map.
f(a,b,c,d) = $\Sigma(0, 1, 2, 3, 13, 15)$
Solution:
The minimized function will be, f(a,b,c,d) = $(a' \wedge b') \vee (a \wedge b \wedge d)$.



K-map

Chapter 9

Mathematical Logic

9.1 Statement(Proposition)

All the declarative sentences to which it is possible to assign one and only one of the two possible truth values(True or False) are called statements.
There are two types of statements. (i) Primitive Statement (ii) Compound Statement

9.1.1 Primitive Statement

The statement which do not contain any of the connective is called primitive statement.

9.1.2 Compound Statement

The statement which contain more than one primitive statements is called compound statement.

Primitive statements are denoted by P, Q, R, S etc.

Example: Find out following sentences are statement or not.

1. Canada is a country.
2. Mumbai is the capital of India.
3. This statement is false.
4. 1+101 = 110
5. Close the door.
6. Toronto is an old city.
7. Please go from here.

Solution:
Sentences (1), (2), (4), (6) are the statements.

9.2 Connective

Connectives are used to make compound sentences. Following are the main connectives:-

1. Negation($\neg$)
2. Conjunction($\wedge$)
3. Disjunction($\vee$)
4. Conditional($\rightarrow$)
5. Biconditional($\leftrightarrow$)

9.2.1 Negation

If P denotes a statement, then the negation of P is written as $\neg P$ and read as "not P". Truth table of negation is the following:-
Example: Consider the statement

P	$\neg P$
T	F
F	T

(1) P: London is a city.
Then $\neg P$ will be
London is not a city.

(2) Q: I went to my class yesterday.
$\neg Q$: I did not go to to my class yesterday.

9.2.2 Conjunction

The conjunction of two statements P and Q is denoted by P$\wedge$Q which is read as "P and Q". Truth table for this is the following:-
Example: Form the conjunction of the following statements

P	Q	P$\wedge$Q
T	T	T
T	F	F
F	T	F
F	F	F

P: It is raining today.
Q: There are 20 tables in this room.
Solution:
P$\wedge$Q: It is raining today and there are 20 tables in this room.

Example: Translate the following statement in to symbolic form

Jack and Jill went up the hill.
Solution:
P: Jack went up the hill.
Q: Jill went up the hill.
Symbolic form is P∧Q.

Example: Consider the following statements
(1) Roses are red and violets are blue.
(2) He opened the book and started to read.
(3) Jack and Jill are cousins.
Statement (1) can be written in the form of ∧.
But (2) and (3) can not be written in the form of ∧.

9.2.3 Disjunction

The disjunction of two statements P and Q is denoted by P∨Q which is read as "P or Q". Truth table for this is the following:-
Example: Consider the following statements

P	Q	P∨Q
T	T	T
T	F	T
F	T	T
F	F	F

(1) I shall watch the game on television or go to the game.
(2) There is something wrong with the bulb or with the wiring.
(3) Twenty or thirty animals were killed in the fire today.
Statement (1) and (2)can be written in the form of ∨.
But(3) can not be written in the form of ∨.

Example: Using the following statements
R: Mark is rich.
H: Mark is happy.
Write the following statements in the symbolic form.
(a) Mark is poor but happy.
(b) Mark is rich but unhappy.
(c) Mark is neither rich nor happy.
(d) Mark is poor or he is both rich and unhappy.
Solution:
(a) $\neg R \wedge H$
(b) $R \wedge \neg H$
(c) $\neg R \wedge \neg H$
(d) $\neg R \vee (R \wedge \neg H)$

9.2.4 Conditional

If P and Q are two statements, then conditional of P and Q is denoted by 'P→Q'. It is read as "if P then Q".

Example: Write the following statements in the symbolic form.

P	Q	P→Q
T	T	T
T	F	F
F	T	T
F	F	T

If either Jerry takes Calculus or Ken takes Sociology, then Larry will take English.
Solution:
P: Jerry takes Calculus.
Q: Ken takes Sociology.
R: Larry takes English.
Then symbolic form of given statement is
$(P \vee Q) \rightarrow R$

Example: Write the following statements in the symbolic form.
The crop will be destroyed if there is a flood.
Solution:
P: There is a flood.
Q: The crop will be destroyed.
Then symbolic form of given statement is
$P \rightarrow Q$

Note: $P \rightarrow Q = \neg P \vee Q$ **Example:** Construct truth table for $(P \rightarrow Q) \wedge (Q \rightarrow P)$.

9.2.5 Biconditional

If P and Q are two statements, then biconditional of P and Q is denoted by 'P↔Q'. It is read as "P if and only if Q". **Note:** $P \leftrightarrow Q = (P \rightarrow Q) \wedge (Q \rightarrow P)$

P	Q	P↔Q
T	T	T
T	F	F
F	T	F
F	F	T

Example: Construct truth table for the following formula:-
$\neg(P \wedge Q) \leftrightarrow (\neg P \vee \neg Q)$

9.2.6 Exercise

1. Show that the truth values of the following formulas are independent of their components.

(a) $(P \wedge (P \rightarrow Q)) \rightarrow Q$
(b) $(P \rightarrow Q) \leftrightarrow (\neg P \vee Q)$
(c) $((P \rightarrow Q) \wedge (Q \rightarrow R) \rightarrow (P \rightarrow R)$
(d) $(P \leftrightarrow Q) \leftrightarrow ((P \wedge Q) \vee (\neg P \wedge \neg Q))$

2. Construct truth table for the following formulas:-

(a) $(Q \wedge (P \rightarrow Q)) \rightarrow P$
(b) $\neg(P \vee (Q \wedge R)) \leftrightarrow ((P \vee Q) \wedge (P \vee R))$

9.3 Well formed formulas

A well formed formulas are defined as following:

1. A statement variable standing alone is a well formed formula.
2. If A is a well formed formula, then $\neg A$ is also a well formed formula.
3. If A and B are well formed formulas, then (A$\wedge$ B), (A$\vee$ B), (A$\rightarrow$ B) and (A$\leftrightarrow$ B) are also well formed formulas.
4. A string of symbols containing the statement variables, connectives and parenthesis is a well formed formula iff it can be obtained by finitely many applications of the rules 1, 2 and 3.

Example: Some well-formed formulas are
$\neg(P \wedge Q)$, $\neg(P \vee Q)$, $(P \rightarrow (P \vee Q))$ etc.

Example: Following are not well-formed formulas
$\neg P \wedge Q$, $(P \rightarrow Q$, $(P \rightarrow Q) \rightarrow (\wedge Q))$ and $(P \wedge Q) \rightarrow Q)$

9.4 Tautology and Contradiction

9.4.1 Tautology

A statement formula which is always true, is called a tautology.

9.4.2 Contradiction

A statement formula which is always false, is called a contradiction.

Example: $(P \vee (\neg P))$, $\neg(P \wedge \neg P)$ are tautology.

9.4.3 Satisfiable

If a statement formula A has the truth value t for at least one combination of truth values assigned to $P_1, P_2, ..., P_n$, then A is said to be satisfiable.

9.4.4 Exercise:

From the formula given below, select those which are well-formed and indicate which ones are tautologies or contradictions.

1. $(P \to (P \vee Q))$
2. $((P \to (\neg P)) \to \neg P)$
3. $((\neg Q \wedge P) \wedge Q)$
4. $((P \to (Q \to R)) \to ((P \to Q) \to (P \to R)))$
5. $((\neg P \to Q) \to (Q \to P))$
6. $((P \wedge Q) \leftrightarrow P)$

9.5 Equivalence formulas

Let A and B be the two statement formulas and let $P_1, P_2, ..., P_n$ denote all the ariables occurring in both A and B.
If the truth value of A is equal to the truth value of B for every possible sets of truth values assigned to $P_1, P_2, ..., P_n$, then A and B are said to be equivalent.
The equivalence of two formulas are denoted by $A \Leftrightarrow B$.

Example:

1. $\neg\neg P$ is equivalent to P.
2. $P \vee P$ is equivalent to P.
3. $(P \wedge \neg P) \vee Q$ is equivalent to Q.
4. $P \vee \neg P$ is equivalent to $q \vee \neg q$.

Note: $(P \to Q) \Leftrightarrow (\neg P \vee Q)$

Equivalence formulas:

1. **Idempotent law**
   (i) $P \vee P \Leftrightarrow P$
   (ii) $P \wedge P \Leftrightarrow P$

2. **Associative law**
   (i) $P \vee (Q \vee R) \Leftrightarrow (P \vee Q) \vee R$
   (ii) $P \wedge (Q \wedge R) \Leftrightarrow (P \wedge Q) \wedge R$

3. **Commutative law**
   (i) $P \vee Q \Leftrightarrow Q \vee P$
   (ii)$P \wedge Q \Leftrightarrow Q \wedge P$

4. **Distributive law**
   (i) $P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$
   (ii) $P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$

5. **Identities law**
   (i) $P \vee F \Leftrightarrow P$, (ii) $P \wedge T \Leftrightarrow P$
   (iii) $P \vee T \Leftrightarrow T$, (iv) $P \wedge F \Leftrightarrow F$
   (v) $P \vee \neg P \Leftrightarrow T$, (vi) $P \wedge \neg P \Leftrightarrow F$

6. **Absorption law**
   (i) $P \vee (P \wedge Q) \Leftrightarrow P)$
   (ii) $P \wedge (P \vee Q) \Leftrightarrow P$

7. **DeMorgan's law**
   (i) $\neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q$
   (ii)$\neg(P \wedge Q) \Leftrightarrow \neg P \vee \neg Q$

Example: Show that

1. $P \to (Q \to R) \Leftrightarrow P \to (\neg Q \vee R) \Leftrightarrow (P \wedge Q) \to R$
2. $(\neg P \wedge (\neg Q \wedge R)) \vee (Q \wedge R) \vee (P \wedge R) \Leftrightarrow R$
3. $\neg(P \wedge Q) \to (\neg P \vee (\neg P \vee Q)) \Leftrightarrow (\neg P \vee Q)$
4. $(P \vee Q) \wedge (\neg P \wedge (\neg P \wedge Q)) \Leftrightarrow (\neg P \wedge Q)$
5. $((P \vee Q) \wedge \neg(\neg P \wedge (\neg Q \vee \neg R))) \vee (\neg P \wedge \neg Q) \vee (\neg P \wedge \neg R)$ are a tautology.

9.6 Duality law

Two formulas P and Q are said to be dual of each others if either one can be obtained from the other by replacing $\wedge$ by $\vee$ and $\vee$ by $\wedge$. The connectives $\wedge$ and $\vee$ are also called dual of each other. If the formula P contains the special symbols T or F, then Q, its dual, is obtained by replacing T by F and F by T.

Example: Dual of $(P \wedge Q) \vee T$ is $(P \vee Q) \wedge F$.

9.7 Converse, Inverse and Contrapositive

For any statement formula $P \to Q$, the statement formula $Q \to P$ is called the converse, $\neg P \to \neg Q$ is called its inverse and $\neg Q \to \neg P$ is called its contrapositive.

Note: $P \to Q \Leftrightarrow \neg Q \to \neg P$ and $Q \to P \Leftrightarrow \neg P \to \neg Q$

9.8 Tautological Implication

A statement A is said to be tautologically imply a statement B iff $A \to B$ is tautology. We shall denote this by $A \Rightarrow B$, which is read as "A implies B".

$A \Rightarrow B$ guarantees that B has the truth value T whenever A has the truth value T.

Exercise

1. Show the following implications.
   (a) $(P \wedge Q) \Rightarrow (P \to Q)$
   (b) $P \Rightarrow (Q \to P)$
   (c) $(P \to (Q \to R)) \Rightarrow (P \to Q) \to (P \to R)$
2. Show the following equivalences.
   (a) $P \to (Q \to P) \Leftrightarrow \neg P \to (P \to \neg Q)$
   (b) $P \to (Q \vee R) \Leftrightarrow (P \to Q) \vee (P \to R)$
   (c) $(P \to Q) \wedge (R \to Q) \Leftrightarrow (P \vee R) \to Q$
   (d) $\neg(P \leftrightarrow Q) \Leftrightarrow (P \vee Q) \wedge \neg(P \wedge Q)$
3. Show the following implications without constructing truth tables.
   (a) $(P \to Q) \Rightarrow P \to (P \wedge Q)$
   (b) $(P \to Q) \to Q)) \Rightarrow (P \vee Q)$
   (c) $((P \vee \neg P) \to Q) \to ((P \vee \neg P) \to R) \Rightarrow (Q \to R)$
   (d) $(Q \to (P \wedge \neg P)) \to (R \to (P \wedge \neg P)) \Leftrightarrow (R \to Q)$

9.8.1 Formulas with distinct truth tables

A statement formula containing n variables must have as its truth table one of the 2^{2^n} possible truth table, each of them having 2^n rows.

9.9 Functionally complete set of connectives

A set of connectives by which every formula can be expressed in terms of an equivalent formula containing the connectives from this set, is called a functionally complete set of connectives.

Minimal functionally complete set: A functional complete set is said to be minimal functionally complete set if its proper subset is not functionally complete.

Example:

1. Are the sets $\{\wedge, \vee, \neg\}, \{\wedge, \neg\}, and \{\vee, \neg\}$ functionally complete?
2. Is the set $\{\wedge, \vee, \neg\}$ minimal functionally complete?

3. Are the sets $\{\wedge, \neg\}$, and $\{\vee, \neg\}$ minimal functionally complete?

4. Are the sets $\{\neg\}, \{\wedge\}, \{\vee\} and \{\wedge, \vee\}$ functionally complete?

Example: Write the formulas which are equivalent to the formulas given below and which contain the connectives $\wedge$ and $\neg$.

1. $\neg(p \leftrightarrow (Q \rightarrow (R \vee P))$

2. $((P \vee Q) \wedge R) \rightarrow (P \vee R)$

9.10 Some other connectives

9.10.1 NAND Connective

It is denoted by $\uparrow$.

$$P \uparrow Q \Leftrightarrow \neg(P \wedge Q)$$

Truth table for this is the following

P	Q	$P \uparrow Q$
T	T	F
T	F	T
F	T	T
F	F	T

9.10.2 NOR Connective

It is denoted by $\downarrow$.

$$P \downarrow Q \Leftrightarrow \neg(P \vee Q)$$

Truth table for this is the following **Example:** Express the connectives $\neg, \wedge and \vee$ in the

P	Q	$P \downarrow Q$
T	T	F
T	F	F
F	T	F
F	F	T

terms of $\uparrow$ only.
Solution:

1. $\neg P \Leftrightarrow \neg P \vee \neg P \Leftrightarrow \neg(P \wedge P) \Leftrightarrow P \uparrow P$

2. $P \wedge Q \Leftrightarrow \neg\neg(P \wedge Q) \Leftrightarrow \neg(P \uparrow Q) \Leftrightarrow (P \uparrow Q) \uparrow (P \uparrow Q)$

3. $P \vee Q \Leftrightarrow \neg\neg(P \vee Q) \Leftrightarrow \neg(\neg P \wedge \neg Q) \Leftrightarrow (\neg P) \uparrow (\neg Q) \Leftrightarrow (P \uparrow P) \uparrow (Q \uparrow Q)$

Example: Express the connectives $\neg, \wedge and \vee$ in the terms of $\downarrow$ only.
Solution:

1. $\neg P \Leftrightarrow \neg P \wedge \neg P \Leftrightarrow \neg(P \vee P) \Leftrightarrow P \downarrow P$
2. $P \vee Q \Leftrightarrow \neg\neg(P \vee Q) \Leftrightarrow \neg(P \downarrow Q) \Leftrightarrow (P \downarrow Q) \downarrow (P \downarrow Q)$
3. $P \wedge Q \Leftrightarrow \neg\neg(P \wedge Q) \Leftrightarrow \neg(\neg P \vee \neg Q) \Leftrightarrow (\neg P) \downarrow (\neg Q) \Leftrightarrow (P \downarrow P) \downarrow (Q \downarrow Q)$

Note: NAND or NOR is functionally complete.

9.10.3 Exercise

1. Express $P \rightarrow (\neg P \rightarrow Q)$ in terms of $\uparrow$ only. Express same formula in terms of $\downarrow$ only.
2. Express $P \uparrow Q$ in terms of $\downarrow$ only.
3. Show the following:-
   (a) $\neg(P \uparrow Q) \Leftrightarrow \neg P \downarrow \neg Q$
   (b) $\neg(P \downarrow Q) \Leftrightarrow \neg P \uparrow \neg Q$
4. Write a formula which is equivalent to the formula
   $$P \wedge (Q \leftrightarrow R)$$
   and contains the connective NAND($\uparrow$) only. Obtain an equivalent formula which contains the connective NOR($\downarrow$) only.
5. Show the following equivalences.
   (a) $A \rightarrow (P \vee C) \Leftrightarrow (A \wedge \neg P) \rightarrow C$
   (b) $(P \rightarrow C) \wedge (Q \rightarrow C) \Leftrightarrow (P \vee Q) \rightarrow C$
   (c) $((Q \wedge A) \rightarrow C) \wedge (A \rightarrow (P \vee C)) \Leftrightarrow (A \wedge (P \rightarrow Q)) \rightarrow C$
   (d) $((P \wedge Q \wedge A) \rightarrow C) \wedge (A \rightarrow (P \vee Q \vee C)) \Leftrightarrow (A \wedge (P \leftrightarrow Q)) \rightarrow C$

9.11 Normal Form

There are following types of normal form.

9.11.1 Disjunctive normal form

A statement formula is said to be in disjunctive normal form if it is the disjunction of conjunction.
Example: $(P \wedge Q) \vee (\neg Q \wedge R)$

9.11.2 Conjunctive normal form

A statement formula is said to be in conjunctive normal form if it is the conjunction of disjunction.
Example: $(P \vee Q) \wedge (\neg Q \vee R)$

9.11.3 Principal disjunctive normal form

A statement formula is said to be in principal disjunctive normal form if it is the disjunction of minterms only.
Example: $(P \wedge Q) \vee (\neg P \wedge Q)$

9.11.4 Principal conjunctive normal form

A statement formula is said to be in principal conjunctive normal form if it is the conjunction of maxterms only.
Example: $(P \vee Q) \wedge (\neg P \vee Q)$

9.11.5 Exercise

1. Obtain disjunctive normal form of the followings:-
   (a) $P \wedge (P \rightarrow Q)$
   (b) $\neg(P \vee Q) \leftrightarrow (P \wedge Q)$

   Also find the conjunctive normal form of above formulas.

2. Obtain the principal disjunctive normal form of the followings:-
   (a) $\neg P \vee Q$
   (b) $(P \wedge Q) \vee (\neg P \wedge R) \vee (Q \wedge R)$
   (c) $P \rightarrow ((P \rightarrow Q) \wedge \neg(\neg Q \vee \neg P))$

3. Obtain the principal conjunctive normal form of the followings:-
   (a) $(P \wedge Q) \vee (\neg P \wedge R) \vee (Q \wedge R)$
   (b) $P \rightarrow ((P \rightarrow Q) \wedge \neg(\neg Q \vee \neg P))$
   (c) $(\neg P \rightarrow R) \wedge (Q \leftrightarrow P)$

9.12 Theory of inference for statement calculus

Let A and B be two statement formulas. We say that "B logically follows from A" or "B is a alid conclusion of the premise A" iff $A \rightarrow B$ is a tautology. That is, $A \Rightarrow B$.

A conclusion C follows from a set of premises $\{H_1, H_2, ..., H_m\}$ iff
$H_1 \wedge H_2 \wedge ..... \wedge H_m \Rightarrow C$

9.12.1 Exercise

1. Determine whether the conclusion C follows logically from the premises H_1 and H_2.
   (a) $H_1 : P \rightarrow Q$ $H_2 : P$ $C : Q$
   (b) $H_1 : P \rightarrow Q$ $H_2 : \neg P$ $C : Q$
   (c) $H_1 : P \rightarrow Q$ $H_2 : \neg(P \wedge Q)$ $C : \neg P$
   (d) $H_1 : \neg P$ $H_2 : P \leftrightarrow Q$ $C : \neg(P \wedge Q)$
   (e) $H_1 : P \rightarrow Q$ $H_2 : Q$ $C : P$

2. Show that the conclusion C follows from the premises $H_1, H_2, ...$ in the following cases:-

(a) $H_1 : P \to Q$	$C : P \to (P \wedge Q)$		
(b) $H_1 : \neg P \vee Q$	$H_2 : \neg(Q \wedge \neg R)$	$H_3 : \neg R$	$C : \neg P$
(c) $H_1 : \neg P$	$H_2 : P \vee Q$	$C : Q$	
(d) $H_1 : \neg Q$	$H_2 : P \to Q$	$C : \neg P$	
(e) $H_1 : P \to Q$	$H_2 : Q \to R$	$C : P \to R$	
(f) $H_1 : R$	$H_2 : P \vee \neg P$	$C : R$	

3. Determine whether the conclusion C is valid in the following, when $H_1, H_2, ...$ are the premises.

(a) $H_1 : P \to Q$	$H_2 : \neg Q$	$C : P$	
(b) $H_1 : P \vee Q$	$H_2 : P \to R$	$H_3 : Q \to R$	$C : R$
(c) $H_1 : P \to (Q \to R)$	$H_2 : P \wedge Q$	$C : R$	
(d) $H_1 : P \to (Q \to R)$	$H_2 : R$	$C : P$	
(e) $H_1 : \neg P$	$H_2 : P \vee Q$	$C : P \wedge Q$	

4. Without constructing a truth table, show that $A \wedge E$ is not a valid consequence of
   $A \leftrightarrow B, B \leftrightarrow (C \wedge D), C \leftrightarrow (A \vee E)$ *and* $A \vee E$
   Also show that $A \vee C$ is not a valid consequence of
   $A \leftrightarrow (B \to C), B \leftrightarrow (\neg A \vee \neg C), C \leftrightarrow (A \vee \neg B)$ *and* B

9.12.2 Implication rules

1. **Simplification**
   $P \wedge Q \Rightarrow P$, $P \wedge Q \Rightarrow Q$

2. **Addition**
   $P \Rightarrow P \vee Q$, $Q \Rightarrow P \vee Q$

3. **Disjunctive Syllogism**
   $\neg P, P \vee Q \Rightarrow Q$

4. **Modus Ponens**
   $P, P \to Q \Rightarrow Q$

5. **Modus Tollens**
   $\neg Q, P \to Q \Rightarrow \neg P$

6. **Hypothetical Syllogism**
   $P \to Q, Q \to R \Rightarrow P \to R$

7. **Dilemma**
   $P \vee Q, P \to R, Q \to R \Rightarrow R$

8. **Conjunction**
   $P, Q \Rightarrow P \wedge Q$

9.12.3 Rules of Inference

Rule P: A premise may be introduced at any point in the derivation.
Rule T: A formula S may be introduced in a derivation if S is tautology implied by any one or more of the preceding formulas in the derivation.

Example: Demonstrate that R is a valid inference from the premises $P \to Q$, $Q \to R$ and P.
Solution:
(1) $P \to Q$ By rule P
(2) $Q \to R$ By rule P
(3) $P \to R$ By rule T, (1), (2) and hypothetical syllogism
(4) P By rule P
(5) R By rule T, (3), (4) and modus ponens

Example: Show that $R \vee S$ follows logically from the premises $C \vee D$, $(C \vee D) \to \neg H$, $\neg H \to (A \wedge \neg B)$ and $(A \wedge \neg B) \to (R \vee S)$.
Solution:
(1) $(C \vee D) \to \neg H$ By rule P
(2) $\neg H \to (A \wedge \neg B)$ By rule P
(3) $C \vee D \to (A \wedge \neg B)$ By rule T, (1), (2) and hypothetical syllogism
(4) $(A \wedge \neg B) \to (R \vee S)$ By rule P
(5) $C \vee D \to (R \wedge S)$ By rule T, (3), (4) and hypothetical syllogism
(6) $C \vee D$ By rule P
(7) $R \vee S$ By rule T, (5), (6) and modus ponens

Example: Show that $R \vee S$ is tautologically implied by $(P \vee Q) \wedge (P \to R) \wedge (Q \to S)$.
Solution:
(1) $P \vee Q$ By rule P
(2) $\neg P \to Q$ By rule T, (1) and $(P \to Q \Leftrightarrow \neg P \vee Q)$
(3) $Q \to S$ By rule P
(4) $\neg P \to S$ By rule T, (2), (3) and hypothetical syllogism
(5) $\neg S \to P$ By rule T, (4) and $(\neg P \to S \Leftrightarrow \neg S \to P)$
(6) $P \to R$ By rule P
(7) $\neg S \to R$ By rule T, (5), (6) and hypothetical syllogism
(8) $R \vee S$ By rule T, (7)and $(P \to Q \Leftrightarrow \neg P \vee Q)$

Example: Show that $R \wedge (P \vee Q)$ is a valid conclusion from the premises $P \vee Q$, $Q \to R$, $P \to M$ and $\neg M$.
Solution:
(1) $P \to M$ By rule P
(2) $\neg M$ By rule P
(3) $\neg P$ By rule T, (1), (2) and modus tollens
(4) $P \vee Q$ By rule P
(5) Q By rule T, (3), (4) and disjunctive syllogism
(6) $Q \to R$ By rule P
(7) R By rule T, (3), (4) and modus ponens
(8) $R \wedge (P \vee Q)$ By rule T, (4), (7) and conjunction

Example: Show that $R \to S$ can be derived from the premises $\neg R \vee P$, $P \to (Q \to S)$, and Q.
Solution:
(1) $P \to (Q \to S)$
(2) $\neg R \vee P$
(3) $R \to P$
(4) $R \to (Q \to S)$
(5) $\neg R \vee \neg Q \vee S$
(6) $Q \to (\neg R \vee S)$
(4) Q
(5) $\neg R \vee S$
(9) $R \to S$

Example: "If there was a ball game, then traveling was difficult. If they arrived on time, then traveling was not difficult. They arrived on time. Therefore there was no ball game." Show that these statements constitute a valid argument.
Solution:
Let
P: There was a ball game.
Q: Traveling was difficult.
R: They arrived on time.
Therefore sentences in symbolic form will be:
Premises: $P \to Q$, $R \to \neg Q$, R and Conclusion: $\neg P$
(1) $R \to \neg Q$
(2) R
(3) $\neg Q$
(4) $P \to Q$
(5)$\neg P$

Rule CP: If we can derive S from r and a set of premises, then we can derive $R \to S$ from the set of premises alone.

Example: If A works hard, then either B or C will enjoy themselves. If B enjoy himself, then A will not work hard. If D enjoys himself, then C will not. Therefore, if A works hard, then D will not enjoy himself.
Solution:
Let
A: A works hard.
B: B will enjoy himself.
C: C will enjoy himself.
D: D will enjoy himself.
Therefore sentences in symbolic form will be:
Premises: $A \to (B \vee C)$, $B \to \neg A$, $D \to \neg C$ and Conclusion: $A \to \neg D$
(1) A
(2) $A \to B \vee C$
(3) $B \vee C$ (4) $\neg C \to B$
(5) $D \to \neg C$

(6) $D \to B$
(7) $B \to \neg A$
(8) $D \to \neg A$
(9) $A \to \neg D$
(10)$\neg D$

9.12.4 Consistency of premises and Indirect method of proof

Consistency of premises

- A set of premises $H_1, H_2, ..., H_m$ is said to be consistent if their conjunction has the truth value T for some assignment of the truth values of the atomic variables appearing in $H_1, H_2, ..., H_m$.
- If for every assignment of the truth values to the atomic variables, at least one of the formulas $H_1, H_2, ..., H_m$ is false, so that their conjunction is identically false, then the formulas $H_1, H_2, ..., H_m$ are called inconsistent.
- Alternatively, a set of formulas $H_1, H_2, ..., H_m$ is inconsistent if their conjunction implies a contradiction, that is,
  $H_1 \wedge H_2 \wedge ..... \wedge H_m \Rightarrow R \wedge \neg R$
  Where R is any formula.

Indirect method of proof

- In order to show that a conclusion C follows logically from the premises $H_1, H_2, ..., H_m$, we assume that C is false and $\neg C$ as an additional premises.
- If the new set of premises is inconsistent, then the assumption that $\neg C$ is true does not hold simultaneously with $H_1, H_2, ..., H_m$ being true. Therefore, C is true whenever $H_1, H_2, ..., H_m$ is true. Thus, C follows logically from the premises $H_1, H_2, ..., H_m$.

Example: Show that the following premises are inconsistent.
(1) If Jack misses many classes through illness, then he fails high school.
(2) If Jack fails high school, then he is uneducated.
(3) If Jack reads a lot of books, then he is not uneducated.
(4) Jack misses many classes through illness and reads a lot of books.
Solution:
E: Jack misses many classes.
S: Jack fails high school.
A: Jack reads a lot of books.
H: Jack is uneducated.
The premises are $E \to S$, $S \to H$, $A \to \neg H$, and $E \wedge A$.
(1) $E \to S$
(2) $S \to H$
(3) $E \to H$ (4) $A \to \neg H$
(5) $H \to \neg A$
(6) $E \to \neg A$

(7) $\neg E \vee \neg A$
(8) $\neg(E \wedge A)$
(9) $E \wedge A$
(10)$\neg(E \wedge A) \wedge (E \wedge A)$ Contradiction

9.12.5 Exercise

1. Show the validity of the following arguments, for which the premises are given on the left and the conclusion on the right.

   (a) $\neg(P \wedge \neg Q)$, $\neg Q \vee R$, $\neg R$ C: $\neg P$

   (b) $(A \to B) \wedge (A \to C)$, $\neg(B \wedge C)$, $D \vee A$ C: D

   (c) $\neg J \to (M \vee N)$, $(H \vee G) \to \neg J$, $H \vee G$ C: $M \vee N$

   (d) $(P \to Q)$, $(\neg Q \vee R) \wedge \neg R$, $\neg(\neg P \wedge S)$ C: $\neg S$

2. Derive the following using rule CP if necessary.

   (a) $\neg P \vee Q$, $\neg Q \vee R$, $R \to S \Rightarrow P \to S$

   (b) P, $P \to (Q \to (R \wedge S)) \Rightarrow Q \to S$

   (c) $(P \vee Q) \to R \Rightarrow (P \wedge Q) \to R$

   (d) $P \to (Q \to R)$, $Q \to (R \to S) \Rightarrow P \to (Q \to S)$

3. Show that the following sets of premises are inconsistent.

   (a) $P \to Q$, $P \to R$, $Q \to \neg R$, P

   (b) $A \to (B \to C)$, $D \to (B \wedge \neg C)$, $A \wedge D$

4. Show the following (use indirect method if needed).

   (a) $R \to \neg Q$, $R \vee S$, $S \to \neg Q$, $P \to Q \Rightarrow \neg P$

   (b) $S \to \neg Q$, $R \vee S$, $\neg R$, $\neg R \leftrightarrow Q \Rightarrow \neg P$

   (c) $\neg(P \to Q) \to \neg(R \vee S)$, $((Q \to P) \vee \neg R)$, $R \Rightarrow P \leftrightarrow Q$

9.13 Predicate Calculus

9.13.1 Predicate

Consider the statements.
John is a bachelor.
Smith is a bachelor.
The part "is a bachelor" is called a predicate.
Now, we denote the predicate as following:- B: is a bachelor.
Therefore the statement in predicate form will be:-
B(John), B(Smith).

Example: Write the following statements in predicate form.
(a) Jack is taller than Jill.
(b) Canada is to the north of the United States.
Solution:
(a) Let P: is taller than
Therefore, statement in predicate form will be
P(Jack, Jill)
(b)Let Q: is to the north of the
Therefore, statement in predicate form will be
Q(Canada, United States)

9.13.2 The statement function, variables and quantifiers

A simple statement function of one variable is defined to be an expression consisting of a predicate symbol and an individual variable. Such a statement function becomes a statement when the variable is replaced by the name of any object.
Let M(x) : x is a man.
H(x): x is a mortal.
The compound statement functions are
$M(x) \wedge H(x)$, $M(x) \rightarrow H(x)$, $\neg H(x)$, $M(x) \vee \neg H(x)$ etc.

Example: Consider the following statements
(a) All men are mortal.
(b) Every apple is red.
(c) Any integer is either positive or negative.
Write these statements in predicate form.
Solution:
(a) Let M(x) : x is a man.
H(x): x is a mortal.
Therefore, the predicate form of the statement will be
$(\forall x)(M(x) \rightarrow H(x))$
(b) Let A(x) : x is an apple.
R(x): x is a red.
Therefore, the predicate form of the statement will be
$(\forall x)(A(x) \rightarrow R(x))$
(c) Let I(x) : x is an integer.
P(x): x is either positive or negative integer.
Therefore, the predicate form of the statement will be
$(\forall x)(I(x) \rightarrow P(x))$

The symbol $(\forall x)$ or (x) is said to be universal quantifier. It is used in the statement which contains for all, every and for any.

Example: Find the predicate form of the following statement.
For any x and y, if x is taller than y, then y is not taller than x.
Solution:
$(\forall x)(\forall y)(G(x, y) \rightarrow \neg G(y, x))$

Example: Consider the following statements
(a)There exists a man.
(b)Some men are clever.
(c) Some real numbers are rational.
Write these statements in predicate form.
Solution:
Let M(x): x is a man.
C(x): x is clever.
R(x): x is real number.
Q(x): x is rational number.
(a) $(\exists x)M(x)$
(b) $(\exists x)(M(x) \wedge C(x))$
(c) $(\exists x)(R(x) \wedge Q(x))$

The symbol $(\exists x)$ is said to be existential quantifier. It is used in the statement which contains some or there exists.

9.13.3 Free and Bound variables

Given a formula containing a part of the form $(\forall$ x)P(x) or $(\exists$ x)P(x), such a part is called an x-bound part of the formula. Any occurrence of x in an x-bound part of a formula is called a bound occurrence of x , while any occurrence of x or of any variable that is not a bound occurrence is called a free occurrence.

Example:
(i) $(\forall x)P(x, y)$
(ii) $(\forall x)(A(x) \rightarrow R(x))$
(iii) $(\forall x)(A(x) \rightarrow (\exists y)R(x, y))$
(iv) $(\exists x)(A(x) \wedge R(x))$
(v) $(\exists x)A(x) \wedge R(x)$
Example: Let P(x): x is a person.
F(x,y): x is the father of y.
M(x,y): x is the mother of y.
Write the predicate form of the following statement
" x is the father of the mother of y."
Solution: Let z as the mother of y. Therefore, statement will be
$(\exists z)(P(z) \wedge F(x, z) \wedge M(z, y))$

9.13.4 Universe of discourse

The domain of a variable is known as the universe of discourse.
Example: If the discussion refers to human beings only, then the universe of discourse is the class of human beings.

Example: Consider the predicate

Q(x): x is less than 5.
and the statements $(\forall x)Q(x)$ and $(\exists x)Q(x)$. If the universe of discourse is given by the following sets, then find the truth value of statements $(\forall x)Q(x)$ and $(\exists x)Q(x)$.
(1) {-1, 0, 1, 2, 4}
(2) {3, -2, 7, 8, -5}
(3) {15, 20, 24}
Solution: $(\forall x)Q(x)$ is true for (1) and false for (2) and (3).
$(\exists x)Q(x)$ is true for (1) and (2) and false for (3).

9.14 Inference theory of the predicate calculus

9.14.1 Some equivalences

(i) $\neg((\forall x)A(x)) \Leftrightarrow (\exists x)\neg A(x)$
(ii) $\neg((\exists x)A(x)) \Leftrightarrow (\forall x)\neg A(x)$
(iii) $A(x) \rightarrow B(x) \Leftrightarrow \neg A(x) \vee B(x)$

9.14.2 Some rules

(1) Universal Specification rule (US rule)
$(\forall x)A(x) \Rightarrow A(x)$
(2) Universal Generalization rule (UG rule)
$A(x) \Rightarrow (\forall x)A(x)$
(3) Existential Specification rule (ES rule)
$(\exists x)A(x) \Rightarrow A(y)$
(4) Existential Generalization rule (EG rule)
$A(y) \Rightarrow (\exists x)A(x)$

9.14.3 Some implications and equivalences

(1) $(\exists x)(A(x) \vee B(x)) \Leftrightarrow (\exists x)A(x) \vee (\exists x)B(x)$
(2) $(\forall x)(A(x) \wedge B(x)) \Leftrightarrow (\forall x)A(x) \wedge (\forall x)B(x)$
(3) $\neg(\exists x)A(x) \Leftrightarrow (\forall x)\neg A(x)$
(4) $\neg(\forall x)A(x) \Leftrightarrow (\exists x)\neg A(x)$
(5) $(\forall x)A(x) \vee (\forall x)B(x) \Rightarrow (\forall x)(A(x) \vee B(x))$
(6) $(\exists x)(A(x) \wedge B(x)) \Rightarrow (\exists x)A(x) \wedge (\exists x)B(x)$

Note: If a formula does not depend upon the variable x, then $\forall x)A \Leftrightarrow A$ and $\exists x)A \Leftrightarrow A$

Example: Prove the following:-
(1) $(\exists x)(A(x) \rightarrow B(x)) \Leftrightarrow (\forall x)A(x) \rightarrow (\exists x)B(x)$
(2) $(\exists x)A(x) \rightarrow (\forall x)B(x)) \Leftrightarrow (\forall x)(A(x) \rightarrow B(x))$
Proof:
(1) $(\exists x)(A(x) \rightarrow B(x))$

$\Leftrightarrow (\exists x)(\neg A(x) \vee B(x))$
$\Leftrightarrow (\exists x)\neg A(x) \vee (\exists x)B(x)$
$\Leftrightarrow \neg(\forall x)A(x) \vee (\exists x)B(x)$
$\Leftrightarrow (\forall x)A(x) \rightarrow (\exists x)B(x)$

(2) $(\exists x)A(x) \rightarrow (\forall x)B(x)$
$\Leftrightarrow \neg(\exists x)A(x) \vee (\forall x)B(x)$
$\Leftrightarrow (\forall x)\neg A(x) \vee (\forall x)B(x)$
$\Leftrightarrow (\forall x)(\neg A(x) \vee B(x))$
$\Leftrightarrow (\forall x)(A(x) \rightarrow B(x))$

Example: Show that $(\forall x)(H(x) \rightarrow M(x)) \wedge H(s) \Rightarrow M(s)$.
Solution:
(1) $(\forall x)(H(x) \rightarrow M(x))$, By rule P
(2) $H(s) \rightarrow M(s)$, By rule US and (1)
(3) H(s) , By rule P
(4) M(s) , By rule T, (2), (3) and modus ponens

Example: Show that $(\forall x)(P(x) \rightarrow Q(x)) \wedge (\forall x)(Q(x) \rightarrow R(x)) \Rightarrow (\forall x)(P(x) \rightarrow R(x))$.
Solution:
(1) $(\forall x)(P(x) \rightarrow Q(x))$, By rule P
(2) $P(y) \rightarrow Q(y)$, By rule US and (1)
(3) $(\forall x)(Q(x) \rightarrow R(x))$, By rule P
(4) $Q(y) \rightarrow R(y)$, By rule US and (3)
(5) $P(y) \rightarrow R(y)$, By rule T, (2), (3) and hypothetical syllogism
(6) $(\forall x)(P(x) \rightarrow R(x))$, By rule UG and (5)

Example: Show that $(\exists x)M(x)$ follows logically from the premises.
$(\forall x)(H(x) \rightarrow M(x))$ and $(\exists x)H(x)$
Solution:
(1) $(\forall x)(H(x) \rightarrow M(x))$, By rule P
(2) $H(y) \rightarrow M(y)$, By rule US and (1)
(3) $(\exists x)H(x)$, By rule P
(4) H(y) , By rule ES and (3)
(5) M(y) , By rule T, (2), (4) and modus ponens
(6) $(\exists x)M(x)$, By rule EG and (5)

Example: Show that $(\exists x)(P(x) \wedge Q(x)) \Rightarrow (\exists x)P(x) \wedge (\exists x)Q(x)$
Solution:
(1) $(\exists x)(P(x) \wedge Q(x))$, By rule P
(2) $P(y) \wedge Q(y)$, By rule ES
(3) P(y)
(4) Q(y)
(5) $(\exists x)P(x)$, By rule EG
(6) $(\exists x)Q(x)$, By rule EG
(7) $(\exists x)P(x) \wedge (\exists x)Q(x)$

Example: Show that from
(a) $(\exists x)(F(x) \wedge S(x)) \rightarrow (\forall y)(M(y) \rightarrow W(y))$

(b) $(\exists y)(M(y) \wedge \neg W(y))$
the conclusion $(\forall x)(F(x) \rightarrow \neg S(x))$ follows.
Solution:
(1) $(\exists y)(M(y) \wedge \neg W(y))$, By rule P
(2) $(M(z) \wedge \neg W(z))$, By rule ES and (1)
(3) $\neg(M(z) \rightarrow W(z))$, By rule T and (2)
(4) $(\exists y)\neg(M(y) \rightarrow W(y))$, By rule EG
(5) $\neg(\forall y)\neg(M(y) \rightarrow W(y))$
(6) $(\exists x)(F(x) \wedge S(x)) \rightarrow (\forall y)(M(y) \rightarrow W(y))$
(7) $\neg(\exists x)(F(x) \wedge S(x))$, By rule T, (5), (6) and modus ponens
(8) $(\forall x)\neg(F(x) \wedge S(x))$
(9) $\neg(F(x) \wedge S(x))$, By rule US and (8)
(10) $(F(x) \rightarrow \neg S(x))$
(11) $(\forall x)(F(x) \rightarrow \neg S(x))$, By rule UG and (10)

Example: Show that $(\forall x)(P(x) \vee Q(x)) \Rightarrow (\forall x)P(x) \vee (\exists x)Q(x))$
Solution:
We shall use the indirect method of proof by assuming $\neg((\forall x)P(x) \vee (\exists x)Q(x))$ as an additional premise.
(1) $\neg((\forall x)P(x) \vee (\exists x)Q(x))$, By rule P(assumed)
(2) $\neg(\forall x)P(x) \wedge \neg(\exists x)Q(x))$, By rule T
(3) $\neg(\forall x)P(x)$
(4) $(\exists x)\neg P(x))$
(5) $\neg(\exists x)Q(x))$
(6) $(\forall x)\neg Q(x)$
(7) $\neg P(y)$, By rule ES and (4)
(8) $\neg Q(y)$, By rule US and (6)
(9) $\neg P(y) \wedge \neg Q(y)$
(10) $\neg(P(y) \vee Q(y))$
(11) $(\forall x)(P(x) \vee Q(x))$, By rule P
(12) $(P(y) \vee Q(y))$, By rule US and (11)
(13) $\neg(P(y) \vee Q(y)) \wedge (P(y) \vee Q(y))$, By rule T and (10),(12)
This is contradiction. Therefore the given statement is proved.

9.15 AKTU Examination Questions

1. Verify that the given propositions are tautology or not.

   (a) $p \vee \neg(p \wedge q)$

   (b) $\neg p \wedge q$

2. Write the contra positive of the implication: "if it is Sunday then it is a holiday".

3. Show that the propositions $p \rightarrow q$ and $\neg p \vee q$ are logically equivalent

4. Show that $((P \vee Q) \wedge \neg(\neg Q \vee \neg R)) \vee (\neg P \vee \neg Q) \vee (\neg P \vee \neg Q)$ is a tautology by using equivalences.

5. Obtain the principle disjunctive and conjunctive normal forms of the formula $(P \rightarrow R) \wedge (Q \leftrightarrow P)$.

6. Explain various Rules of Inference for Propositional Logic.

7. Prove the validity of the following argument "if the races are fixed so the casinos are crooked, then the tourist trade will decline. If the tourist trade decreases, then the police will be happy. The police force is never happy. Therefore, the races are not fixed."

8. Prove that $(P \vee Q) \rightarrow (P \wedge Q)$ is logically equivalent to $P \leftrightarrow Q$.

9. Express this statement using quantifiers:
"Every student in this class has taken some course in every department in the school of mathematical sciences".

10. Construct the truth table for the following statements:

    (a) $(P \rightarrow \neg Q) \rightarrow \neg P$

    (b) $P \leftrightarrow (\neg P \vee \neg Q)$

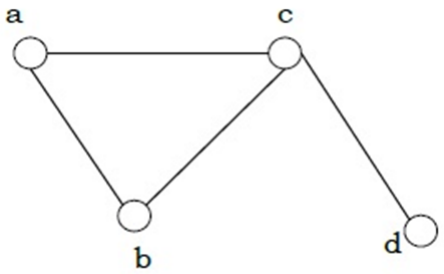
Chapter 10

Graph Theory

10.1 Graph definition

A graph is an ordered pair G=(V,E) consisting of a nonempty set V of vertices and a set E of edges.

Example:



10.1.1 Order of a graph

The number of vertices in a graph is said to be the order of the graph.

10.1.2 Degree of a Vertex

The degree of a vertex v of a graph G (denoted by deg (v)) is the number of edges incident with the vertex v.

In-degree: The number of incoming edges at a vertex is said to be in-degree of that vertex.

Out-degree: The number of out going edges from a vertex is said to be out-degree of that vertex.

10.1.3 Even and Odd Vertex

If the degree of a vertex is even, the vertex is called an even vertex and if the degree of a vertex is odd, the vertex is called an odd vertex.

10.1.4 Degree of a Graph

The degree of a graph is the largest vertex degree of that graph.

10.1.5 Isolated Vertex

A vertex with degree zero is called an isolated vertex.

10.1.6 Pendant Vertex

A vertex with degree one is called a pendent vertex.

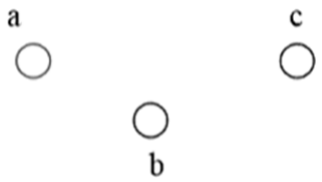
10.2 Types of Graph

There are different types of graphs.

10.2.1 Null Graph

A null graph is a graph in which there are no edges between its vertices. A null graph is also called empty graph.

Example:



10.2.2 Trivial Graph

A trivial graph is the graph which has only one vertex.

10.2.3 Directed and Undirected Graph

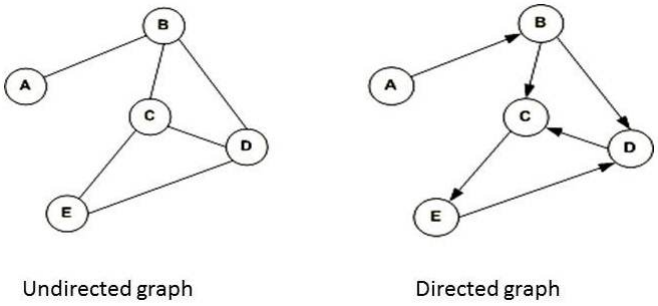
An undirected graph is a graph whose edges are not directed.

A directed graph is a graph in which the edges are directed by arrows.

Directed graph is also known as digraphs.

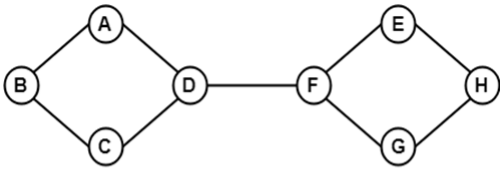
10.2.4 Connected and Disconnected Graph

A connected graph is a graph in which we can visit from any one vertex to any other vertex. In a connected graph, at least one edge or path exists between every pair of vertices.

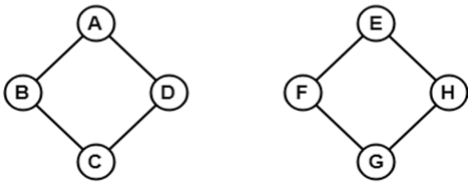


Undirected graph Directed graph

A disconnected graph is a graph in which any path does not exist between every pair of vertices.



Connected graph

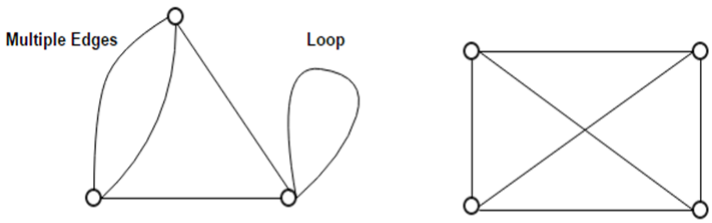


Disconnected graph

10.2.5 Simple graph

A simple graph is the undirected graph with no parallel edges and no loops.
A simple graph which has n vertices, the degree of every vertex is at most n -1.

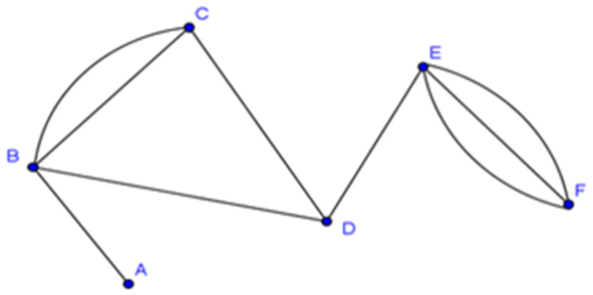
Example:



Not a Simple Graph Simple Graph

10.2.6 Multi-graph

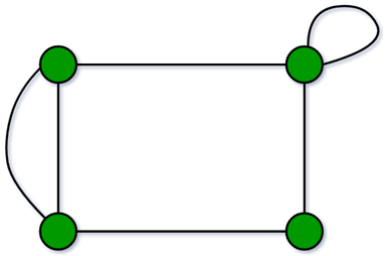
A graph having no self loops but having parallel edge(s) in it is called as a multi-graph.
Example:



10.2.7 Pseudo Graph

A graph in which loops and multiple edges are allowed is called psuedograph.

Example: Following graph is pseudo graph:-



Handshaking lemma
In any graph (simple) G, the sum of degree of all vertices is equal to 2e, where e is the number of edges that is
$\sum_{v \in V} deg_G(v)$= 2e.
Proof:
Since the degree of a vertex is the number of edges incident with that vertex, the sum of degree counts the number of times an edge is incident with a vertex. Since every edge is incident with exactly two vertices, so each edge gets counted twice , once at each end. Thus the sum of degree is equal twice the number of edges.

Theorem: The number of vertices of odd degree in a graph G is always even.
Proof: We know that, the sum of the degrees of all ertices in a graph G is twice the number of edges in G i.e. $\sum_{v \in V} deg_G(v)$= 2e
$\sum_{v \in EVEN} deg_G(v) + \sum_{v \in ODD} deg_G(v) = 2e$, where EVEN is the set of even degree vertices and ODD is the set odd degree vertices.
$\Rightarrow \sum_{v \in ODD} deg_G(v) = 2e - \sum_{v \in EVEN} deg_G(v)$
= even number - even number = even number
$\Rightarrow \sum_{v \in ODD} deg_G(v)$ = even number

Hence the number of vertices of odd degree in a graph is even.

Note: In a graph G with n≥2, there are two vertices of equal degree.

Example: Is there a simple graph with degree sequence (1,3,3,3,5,6,6)?

Example: Is there a simple graph with seven vertices having degree sequence (1,3,3,4,5,6,6)?

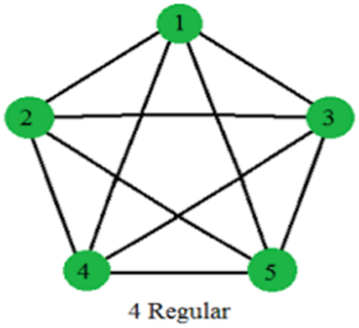
Example: Is there a simple graph with degree sequence (1,1,3,3,3,4,6,7)?

Example: Show that the maximum number of edges in a simple graph with n vertices is n(n-1)/2.

10.2.8 Regular Graph

A graph is called a regular if all the vertices of the graph have the same degree. If degree of each vertex is k, then the graph is called k-regular graph.

Example: Following graph is regular.



Regular graph

Example: Determine the number of edges in a graph with 6 vertices, 2 of degree 4 and 4 of degree 2. And also draw this graph.
Solution:
Let e is the number of edges in the graph. Since the sum of degree of all vertices is 2e, therefore
$2*4+4*2 = 2e \Rightarrow e = 8$
Hence the number of edges in the graph is 8.

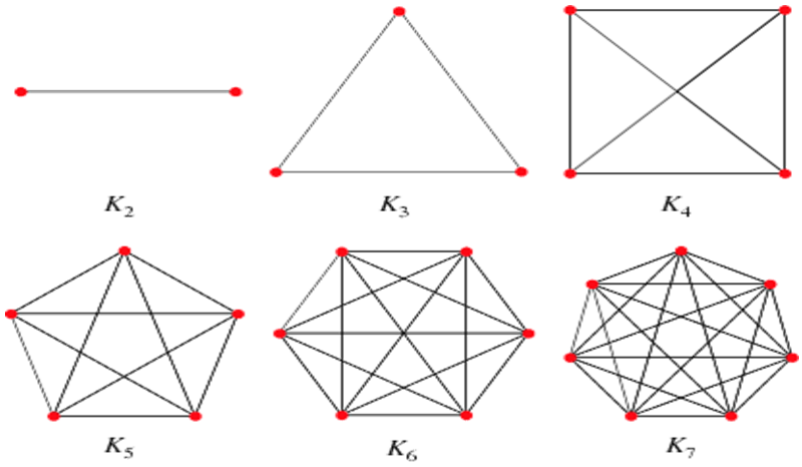
Example: Does there exists a 4-regular graph with 6 vertices? If so, construct a graph.
Solution:

10.2.9 Complete Graph

A graph G is said to be complete if every vertex in G is connected with every other vertex. A complete graph is denoted by K_n, where n is the number of vertex in G. Number of

edges in complete graph K_n is exactly n(n-1)/2 edges.

Example: Draw the complete graph for n=2 to 7.
Solution:

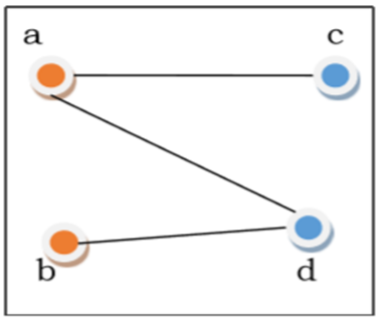


Complete graphs

10.2.10 Bipartite Graph

If the vertex-set of a graph G can be split into two disjoint sets, V_1 and V_2, in such a way that each edge in the graph joins a vertex in V_1 to a vertex in V_2, and there are no edges in G that connect two vertices in V_1 or two vertices in V_2, then the graph G is called a bipartite graph.

Example: Following graph is bipartite.



Bipartite graph

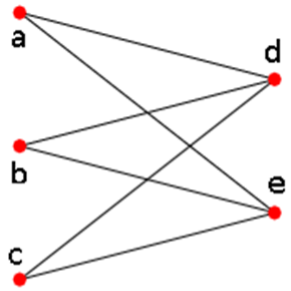
10.2.11 Complete Bipartite Graph

A complete bipartite graph is a bipartite graph in which each vertex in the first set is joined to every single vertex in the second set. The complete bipartite graph is denoted by $K_{m,n}$ where the graph G contains m vertices in the first set and n vertices in the

second set.

Example: Draw the complete bipartite graph for m=3 and n=2.

Note: Number of edges in complete bipartite graph $K_{m,n}$ is m*n and number of



Complete bipartite graph $K_{3,2}$

vertices is m+n.

10.2.12 Isomorphism of graph

Suppose G=(V,E) and G'=(V',E') are two graphs. A function f: V→ V' is called a graph isomorphism if

1. f is bijective.
2. For all a,b ∈ V, (a,b)∈ E iff (f(a),f(b))∈ E'.

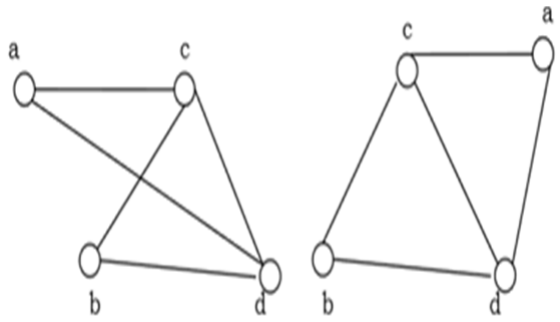
If such function exists then graph G and G' are said to be isomorphic to each other.

Conditions for Graph Isomorphism

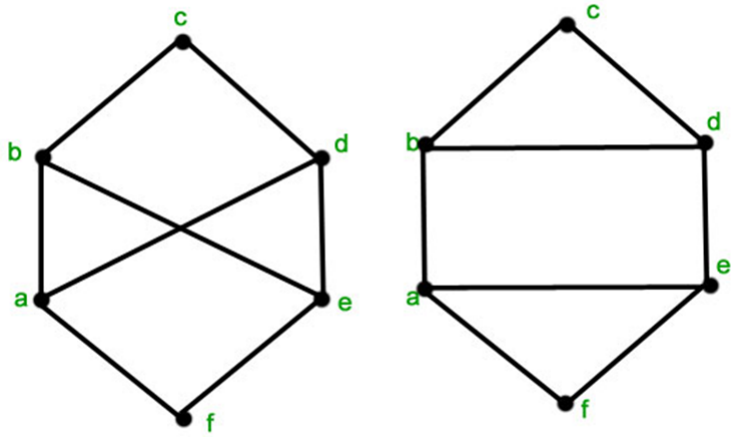
1. Both graphs G and G' must have the same number of vertices.
2. Both graphs G and G' must have the same number of edges.
3. Degree sequence of both graphs are same.

Example: Is the following graphs isomorphism?

Solution:



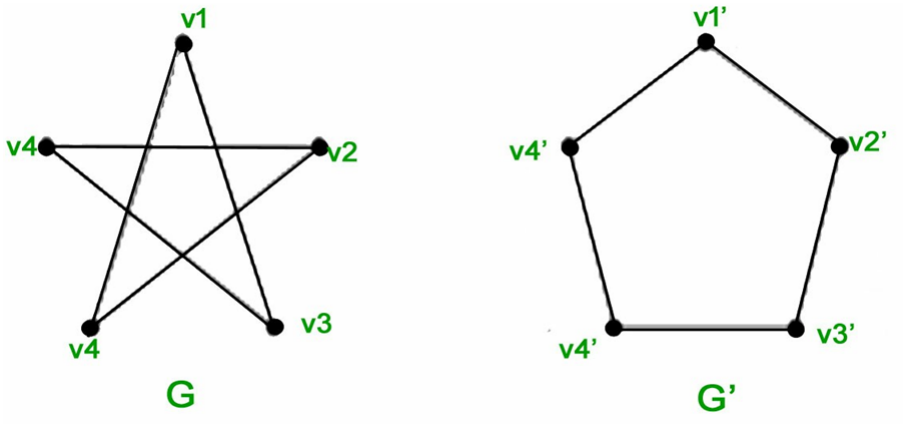
Example: Is the following graphs isomorphism?



Solution:

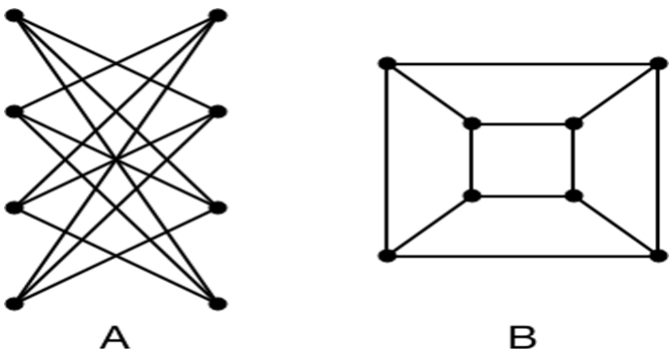
Example: Is the following graphs isomorphism?

Solution:



Example: Is the following graphs isomorphism?

Solution:



10.2.13 Homomorphism of graph

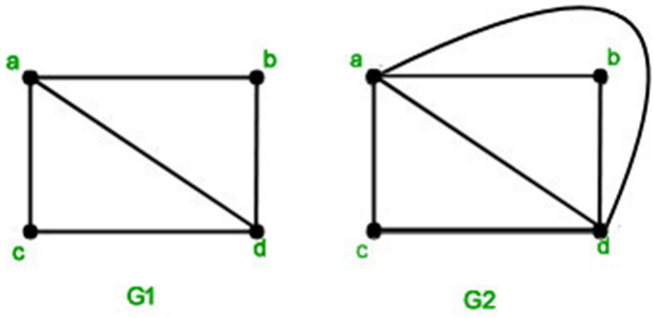
Suppose G=(V,E) and G'=(V',E') are two graphs. A function f: V$\rightarrow$ V' is called a graph homomorphism if for all a,b $\in$ V, if (a,b)$\in$ E then (f(a),f(b))$\in$ E'.

If such function exists then graph G and G' are said to be homomorphic to each other.

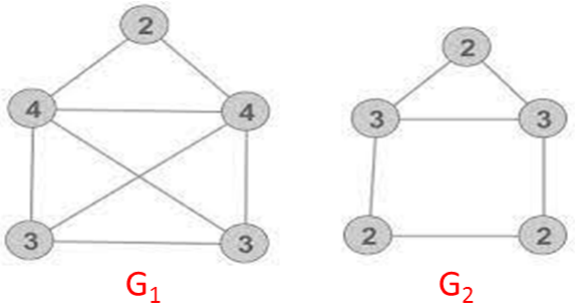
10.2.14 Euler Graphs

A graph G is called Euler graph if it contains an Euler cycle.
Euler cycle: An Euler cycle is a cycle which contains every edges of the graph and no edge is repeated.
Euler path: A path is called an Euler path if it contains every edges of the graph and no edge is repeated.

Example: Which graphs shown below an Euler?
Solution:



Example: Which graphs shown below an Euler?
Solution:

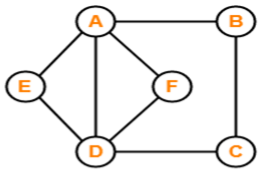


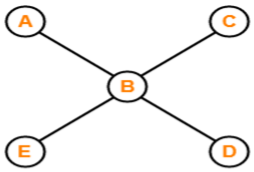
Note: A graph is an Euler iff every vertex has an even degree.

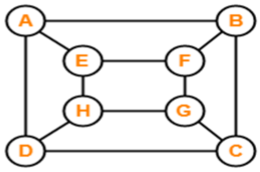
10.2.15 Hamiltonian Graphs

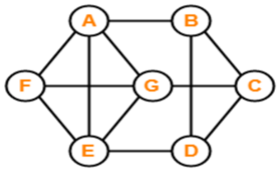
A graph G is called Hamiltonian graph if it contains an Hamiltonian cycle.
Hamiltonian cycle: An Hamiltonian cycle is a cycle which contains every vertex of the graph and no vettex is repeated.
Hamiltonian path: A path is called an Hamiltonian path if it contains every vertex of the graph and no vertex is repeated.

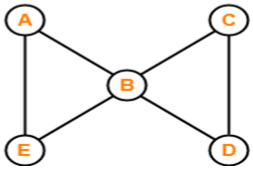
Example: Which graphs shown below a Hamiltonian?
Solution:

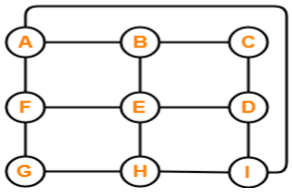
A) 

B) 

C) 

D) 

E) 

F) 

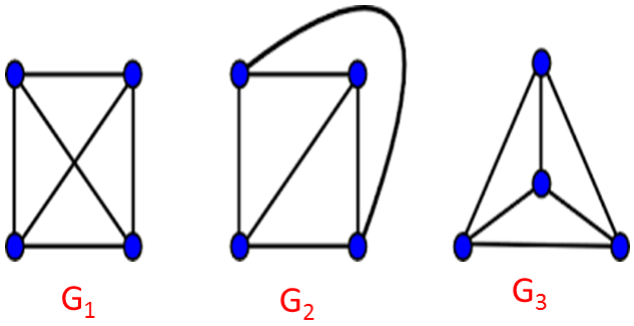
Note: A simple connected graph G of order n≥3 vertices is Hamiltonian if deg(v)≥ n/2 for every v in G.

Note: Let G be a simple graph with n vertices and m edges where m is atleast 3. If $m \geq \frac{(n-1)(n-2)}{2} + 2$, then G is Hamiltonian.

10.2.16 Planar Graph

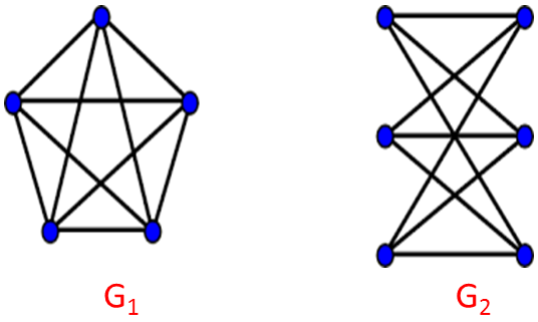
A graph is said to be planar if it can be drawn on a plane without crossing their edges.

Example: Are the following graphs planar?



Example: Are the following graphs planar?

Note: The complete graph of five vertices is not planar.



Properties of Planar Graphs:

1. If a connected planar graph G has e edges and r regions, then r $\geq$ (2/3)e.
2. If a connected planar graph G has e edges and v vertices, then 3v-e$\geq$6.
3. A complete graph K_n is a planar if and only if n<5.
4. A complete bipartite graph K_{mn} is planar if and only if m < 3 or n <3.

Example: Prove that complete graph K_4 is planar.
Solution: The complete graph K_4 contains 4 vertices and 6 edges.
We know that for a connected planar graph 3v-e$\geq$6.Hence for K_4, we have 3x4-6 = 6 which satisfies the property. Thus K_4 is a planar graph. Hence Proved.

Euler's Formula

Let G be a connected planar graph and let n, e and r denote respectively the number of vertices, edges and region in a plane representation of G, then n-e+r = 2.

10.3 Matrix representation of Graphs

There are two principal ways to represent a graph G with the matrix, i.e., adjacency matrix and incidence matrix representation.

10.3.1 Adjacency Matrix Representation

If an undirected Graph G consists of n vertices, then the adjacency matrix of a graph is an n x n matrix A = $[a_{ij}]$ and defined by
a_{ij} = 1, if there exists an edge between vertex v_i and v_j
= 0, otherwise

10.3.2 Incidence Matrix Representation

If an undirected Graph G consists of n vertices and m edges, then the incidence matrix is an n x m matrix C = $[c_{ij}]$ and defined by

$c_{ij} = 1$, if the vertex v_i incident by edge e_j
$= 0$, otherwise

Note: The number of ones in an incidence matrix of the undirected graph (without loops) is equal to the sum of the degrees of all the vertices in a graph.

10.4 Graph Coloring

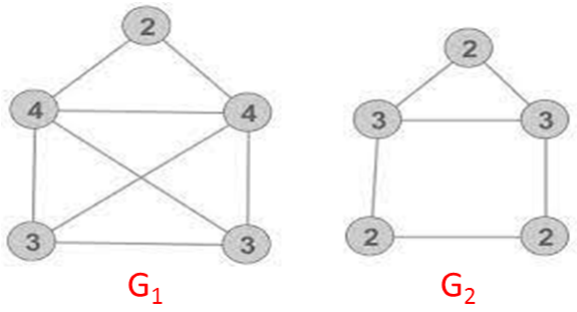
10.4.1 Vertex Coloring

Vertex coloring is an assignment of colors to the vertices of a graph 'G' such that no two adjacent vertices have the same color.

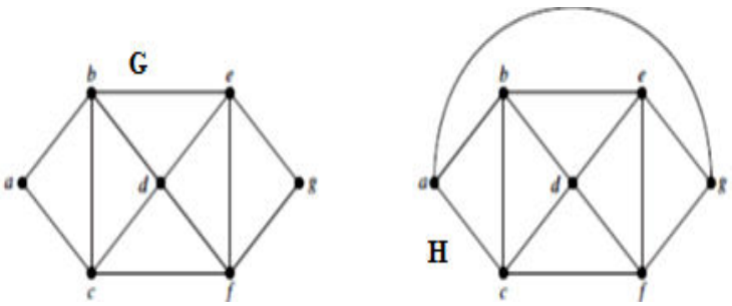
10.4.2 Chromatic Number

The minimum number of colors required for vertex coloring of graph 'G' is called as the chromatic number of G, denoted by X(G).

Example: Find the chromatic number of the following graphs



Example: Find the chromatic number of the following graphs



Note: $\chi(G) = 1$, if and only if 'G' is a null graph. If 'G' is not a null graph, then $\chi(G) \geq 2$.

Note: A graph 'G' is said to be n-coverable if there is a vertex coloring that uses

at most n colors, i.e., X(G) $\geq$ n.

Note: The chromatic number of K_n is n.

10.4.3 Region Coloring

Region coloring is an assignment of colors to the regions of a planar graph such that no two adjacent regions have the same color. Two regions are said to be adjacent if they have a common edge.

Chapter 11

Recurrence Relation and Generating Function

11.1 Recurrence Relation

A recurrence relation for the sequence $< a_n >$ is an equation that expresses a_n in terms of one or more of the previous terms of the sequence.

Example: Consider the following recurrence relation:-
$a_n = a_{n-1} - a_{n-2}$
for n=2,3,4,5,....., with the conditions $a_0 = 3$, $a_1 = 5$.

Example: The sequence 1,1,2,3,5,8,....., is defined by the recurrence relation
$a_n = a_{n-1} + a_{n-2}$
with initial conditions $a_0 = 1$, $a_1 = 1$.

11.1.1 Order of the Recurrence Relation

The order of a recurrence relation is the difference between the largest and the smallest subscript appearing in the the relation.

Example: Consider the following recurrence relation:-
$a_n = a_{n-1} + a_{n-2}$
The order of this relation = 2

Consider another recurrence relation:-
$a_{n+3} - a_{n+2} + a_{n+1} - a_n = 0$
The order of this relation = 3

11.1.2 Degree of the Recurrence Relation

The degree of a recurrence relation is the highest power of a_n occurring in that relation.

Example: Consider the following recurrence relation:-
${a_n}^3 + 3a_{n-1}^2 + 6a_{n-2}^2 + 4a_{n-3} = 0$
The degree of this relation = 3

Consider another recurrence relation:-
$a_{n+2}^2 + 4a_{n+1} + 5a_n = 0$
The degree of this relation = 2

11.1.3 Linear Recurrence Relation with Constant Coefficients

A recurrence relation of the form
$c_0a_n + c_1a_{n-1} + c_2a_{n-2} + \ldots\ldots\ldots\ldots + c_ka_{n-k} = f(n)$
where c_i's are constants, is called a linear recurrence relation with constant coefficients of k^{th} order, provided c_0 and c_k, both are non-zero. f(n) is the function of the independent variable 'n' only.

Example: (i) $3a_n + 6a_{n-1} = 2^n$
is the first order linear recurrence relation with constant coefficients.

(ii) $2a_n + 5a_{n-2} = n^2 + n$
is the second order linear recurrence relation with constant coefficients.

Note: A recurrence relation is said to be linear if its degree is one.

11.1.4 Homogeneous Linear Recurrence Relation

A linear recurrence realtion is said to be homogeneous if f(n) = 0.
If f(n)$\neq$ 0, then it is said to be non-homogeneous.

11.1.5 Solution of Linear Equation

The solution of linear equation consists of two parts (i) homogeneous solution (ii) particular solution. That is,
$a = a^h + a^p$

11.1.6 Solution of Homogeneous Linear Recurrence Equation

Example: Find the solution of the recurrence relation
$a_n = a_{n-1} + 2a_{n-2}$
with $a_0 = 2$, and $a_1 = 7$.
Solution:
Let the solution be $a_n = \alpha^n$.
Put $a_n = \alpha^n$ in the given recurrence relation.

$\alpha^n = \alpha^{n-1} + 2\alpha^{n-2}$
$\Rightarrow \alpha^2 - \alpha - 2 = 0$
$\Rightarrow (\alpha - 2)(\alpha + 1) = 0$
$\Rightarrow \alpha = 2, -1$
Therefore, the solution of recurrence equation will be
$a_n = c_1 2^n + c_2(-1)^n$ ..... (1)
Now, we find c_1 and c_2 by using initial values $a_0 = 2$, and $a_1 = 7$.
For n=0, equation (1) will be
$a_0 = c_1 2^0 + c_2(-1)^0$
therefore, $c_1 + c_2 = 2$ .....(2)
For n=1, equation (1) will be
$a_1 = c_1 2^1 + c_2(-1)^1$
therefore, $2c_1 - c_2 = 7$ .....(3)
After solving equations (2) and (3), we get $c_1 = 3$ and $c_2 = -1$.
Putting c_1 and c_2 in equation (1), we get the final solution
$a_n = 32^n - (-1)^n$

Example: Find the solution of the recurrence relation
$a_n - 6a_{n-1} + 9a_{n-2} = 0$
with $a_0 = 1$, and $a_1 = 6$.
Solution:
Let the solution be $a_n = \alpha^n$.
Put $a_n = \alpha^n$ in the given recurrence relation.
$\alpha^n - 6\alpha^{n-1} + 9\alpha^{n-2}=0$
$\Rightarrow \alpha^2 - 6\alpha + 9 = 0$
$\Rightarrow (\alpha - 3)^2 = 0$
$\Rightarrow \alpha = 3, 3$
Therefore, the solution of recurrence equation will be
$a_n = (c_1 + c_2 n)(3)^n$ ..... (1)
Now, we find c_1 and c_2 by using initial values $a_0 = 1$, and $a_1 = 6$.
For n=0, equation (1) will be
$a_0 = (c_1 + c_2.0)(3)^0$
therefore, $c_1 = 1$ .....(2)
For n=1, equation (1) will be
$a_1 = (c_1 + c_2.1)(3)^1$
therefore, $3c_1 + 3c_2 = 6$ .....(3)
After solving equations (2) and (3), we get $c_1 = 1$ and $c_2 = 1$.
Putting c_1 and c_2 in equation (1), we get the final solution
$a_n = (1 + n)(3)^n$

Example: Find the solution of the recurrence relation
$a_n - 5a_{n-1} + 8a_{n-2} - 4a_{n-3} = 0$
Solution:
Let the solution be $a_n = \alpha^n$.
Put $a_n = \alpha^n$ in the given recurrence relation.
$\alpha^n - 5\alpha^{n-1} + 8\alpha^{n-2} - 4\alpha^{n-3}=0$
$\Rightarrow \alpha^3 - 5\alpha^2 + 8\alpha - 4 = 0$
$\Rightarrow (\alpha - 1)(\alpha - 2)^2 = 0$

$\Rightarrow \alpha = 1, 2, 2$
Therefore, the solution of recurrence equation will be
$a_n = c_1(1)^n + (c_2 + c_3 n)(2)^n$

Example: Find the solution of the recurrence relation
$a_n + 6a_{n-1} + 12a_{n-2} + 8a_{n-3} = 0$
Solution:
Let the solution be $a_n = \alpha^n$.
Put $a_n = \alpha^n$ in the given recurrence relation.
$\alpha^n + 6\alpha^{n-1} + 12\alpha^{n-2} + 8\alpha^{n-3}$=0
$\Rightarrow \alpha^3 + 6\alpha^2 + 12\alpha + 8 = 0$
$\Rightarrow (\alpha + 2)^3 = 0$
$\Rightarrow \alpha$ = -2, -2, -2
Therefore, the solution of recurrence equation will be
$a_n = (c_1 + c_2 n + c_3 n^2)(-2)^n$

Example: Find the solution of the recurrence relation
$4a_n - 20a_{n-1} + 17a_{n-2} - 4a_{n-3} = 0$
Solution:
Let the solution be $a_n = \alpha^n$.
Put $a_n = \alpha^n$ in the given recurrence relation.
$4\alpha^n - 20\alpha^{n-1} + 17\alpha^{n-2} - 4\alpha^{n-3}$=0
$\Rightarrow 4\alpha^3 - 20\alpha^2 + 17\alpha - 4 = 0$
$\Rightarrow (\alpha - 4)(2\alpha - 1)^2 = 0$
$\Rightarrow \alpha = 4, 1/2, 1/2$
Therefore, the solution of recurrence equation will be
$a_n = c_1(4)^n + (c_2 + c_3 n)(1/2)^n$

11.1.7 Solution of Non-Homogeneous Linear Recurrence Equation

In this case, we find homogeneous and particular solution both. The final solution will be addition of both.
Here, f(n)≠0.

Method to find Particular Solution

The particular solution of a recurrence relation can be obtained by the method of inspection, since the particular solution depend on the form of f(n).
We guess the solution according to following table:-
The solution of non-homogeneous equation is
$a_n = a_n^{(h)} + a_n^{(p)}$

Example: Solve the recurrence relation
$a_n + 5a_{n-1} + 6a_{n-2} = 3n^2 - 2n + 1$ .....(1)

S. No.	f(n)	Guessing solution
1	b^n (If b is not a root of characteristic equation)	A b^n
2	Polynomial P(n) of degree m	$A_0 + A_1n + A_2n^2 + ... + A_mn^m$
3	c^nP(n)(If c is not a root of characteristic equation and Polynomial P(n) of degree m)	$c^n(A_0 + A_1n + A_2n^2 + ... + A_mn^m)$
4	b^n (If b is a root of characteristic equation of multiplicity s)	An^sb^n
5	c^nP(n) (If b is a root of characteristic equation of multiplicity t)	$n^t(A_0 + A_1n + A_2n^2 + ... + A_mn^m)b^n$

Solution: The homogeneous equation will be
$a_n + 5a_{n-1} + 6a_{n-2} = 0$
The characteristic equation will be
$\alpha^2 + 5\alpha + 6 = 0$
$\Rightarrow (\alpha + 2)(\alpha + 3) = 0$
$\Rightarrow \alpha$ = -2, -3
Therefore, the homogeneous solution of recurrence equation will be
$a_n^{(h)} = c_1(-2)^n + c_2(-3)^n$

For particular solution:
Here, f(n) = $3n^2 - 2n + 1$
Clearly, f(n) is the polynomial equation of degree 2. Therefore using above table, we guess the following solution:-
$a_n = A_0 + A_1n + A_2n^2$.....(2)
Put the value of a_n in equation (1),
$(A_0 + A_1n + A_2n^2) + 5(A_0 + A_1(n-1) + A_2(n-1)^2) + 6(A_0 + A_1(n-2) + A_2(n-2)^2)$
$= 3n^2 - 2n + 1$
$(A_0 + 5A_0 - 5A_1 + 5A_2 + 6A_0 - 12A_1 + 24A_2) + (A_1 + 5A_1 - 10A_2 + 6A_1 - 24A_2)n + (A_2 + 5A_2 + 6A_2)n^2 = 3n^2 - 2n + 1$
$(12A_0 - 17A_1 + 29A_2) + (12A_1 - 34A_2)n + 12A_2n^2 = 3n^2 - 2n + 1$
Comparing the coefficients of power of n on both sides
$12A_0 - 17A_1 + 29A_2 = 1$ .....(3)
$12A_1 - 34A_2$ = -2 .....(4)
$12A_2 = 3$.....(5)
After solving equations (3), (4) and (5), we get
$A_0 = 47/288$, $A_1 = 13/24$, $A_2 = 1/4$
Therefore, particular solution is
$a_n^{(p)} = (47/288) + (13/24)n + (1/4)n^2$
Therefore, the final solution of given recurrence relation will be the following:-
$a_n = a_n^{(h)} + a_n^{(p)}$
$= c_1(-2)^n + c_2(-3)^n + (47/288) + (13/24)n + (1/4)n^2$

11.1.8 Exercise:

Solve the following recurrence relations:-

1. $a_{n+2} - 5a_{n+1} + 6a_n = n^2$
2. $a_n - 6a_{n-1} + 8a_{n-2} = 3^n$
3. $a_n + 5a_{n-1} + 6a_{n-2} = 42(4)^n$
4. $a_n + a_{n-1} = 3n2^n$
5. $a_n - 2a_{n-1} = 32^n$
6. $a_n - 4a_{n-1} + 4a_{n-2} = (n+1)2^n$

Example: Solve the recurrence relation
$a_n - 5a_{n-1} + 6a_{n-2} = 2^n + n$ .....(1)
Solution: The homogeneous solution will be
$a_n^{(h)} = c_1(2)^n + c_2(3)^n$

For particular solution:
Here, f(n) = $2^n + n$
Therefore, we guess the solution as following:-
Let $a_n = A_0 n2^n + (A_1 + A_2 n)$
Put this in equation (1), we get
A_0 = -2, A_1 = 7/4, A_2 = 1/2
Therefore the solution will be
$a_n = c_1 2^n + c_2 3^n - 2n2^n + (7/4) + (1/2)n$

11.2 Generating Functions

The generating function of a sequence of numbers $a_0, a_1, a_2, ..., a_n, ...$ is defined as
G(x) = $a_0 + a_1 x + a_2 x^2 + ... + a_n x^n + ...$
= $\sum_{n=0}^{\infty} a_n x^n$

Example: Find the generating functions for the following sequences

1. 1,1,1,1,1,.....
2. 1,2,3,4,.....
3. 0,1,2,3,4,.....
4. 1,a,a^2,a^3,.....

Solution:

1. The generating function of this sequence will be the following:-
   G(x) = 1+x+x^2+ x^3+ x^4+.....
   = $\frac{1}{(1-x)}$

2. The generating function of this sequence will be the following:-
   G(x) = 1+2x+$3x^2$+$4x^3$+.....
   xG(x)= x+$2x^2$+$3x^3$+.....
   Subtracting from above, we get
   (1-x)G(x) = 1+x+x^2+ x^3+ x^4+.....
   (1-x)G(x) = $\frac{1}{(1-x)}$
   Therefore, G(x) = $\frac{1}{(1-x)^2}$

3. The generating function of this sequence will be the following:-
   G(x) = 0+x+$2x^2$+ $3x^3$+ $4x^4$+.....
   = x(1+2x+$3x^2$+$4x^3$+.....)
   Therefore, G(x) = $\frac{x}{(1-x)^2}$

4. The generating function of this sequence will be the following:-
   G(x) = 1+ax+a^2x^2+ a^3x^3+ a^4x^4+.....
   = 1+ax+$(ax)^2$+ $(ax)^3$+ $(ax)^4$+.....
   = $\frac{1}{(1-ax)}$

Example: Find the generating functions for the following sequences

1. 0,0,1,1,1,.....
2. 1,1,0,1,1,1,1,.....
3. 1,0,-1,0,1,0,-1,0,1,.....
4. 3,-3,3,-3,3,-3,.....

Solution:

Example: Find the generating function of a sequence $< a_k >$ if a_k = 2+3k.
Solution: The generating function of a sequence whose general term is 2, is
G1(x) = $\frac{2}{(1-x)}$

The generating function of a sequence whose general term is 3k, is

G2(x) = $\frac{3x}{(1-x)^2}$

Hence the required generating function is

G(x) = G1(x)+ G1(x)= $\frac{2}{(1-x)}$+$\frac{3x}{(1-x)^2}$

11.2.1 Solution of linear recurrence relation using generating function

Example: Solve the linear recurrence relation
$a_n - 3a_{n-1} + 2a_{n-2} = 0$, n $\geq$ 2
using the method of generating function with the initial conditions $a_0 = 2$, and $a_1 = 3$.
Solution:

$a_n - 3a_{n-1} + 2a_{n-2} = 0$

Multiply both sides by x^n and taking summation, we get

$\sum_{n=2}^{\infty} a_n x^n - 3\sum_{n=2}^{\infty} a_{n-1}x^n + 2\sum_{n=2}^{\infty} a_{n-2}x^n = 0$

Since G(x) = $\sum_{n=0}^{\infty} a_n x^n$, therefore

(G(x)-a_0-a_1x)- 3x(G(x)-a_0)+2x^2G(x) = 0

$\Rightarrow$ G(x)(1-3x+2x^2)-a_0-a_1x+3a_0x = 0

Put the value of $a_0 = 2$ and $a_1 = 3$,

G(x) = $\frac{2+3x-6x}{(1-3x+2x^2)} = \frac{2-3x}{(1-3x+2x^2)}$

$= \frac{2-3x}{(1-x)(1-2x)}$

$= \frac{1}{(1-x)} + \frac{1}{(1-2x)}$

Therefore, the solution of recurrence relation will be

$a_n = (1)^n + (2)^n$

This is the final answer.

Example: Solve the linear recurrence relation
$a_n - 2a_{n-1} - 3a_{n-2} = 0$, n $\geq$ 2
using the method of generating function with the initial conditions $a_0 = 3$, and $a_1 = 1$.
Solution:
$a_n - 2a_{n-1} - 3a_{n-2} = 0$

Multiply both sides by x^n and taking summation, we get

$\sum_{n=2}^{\infty} a_n x^n - 2\sum_{n=2}^{\infty} a_{n-1}x^n - 3\sum_{n=2}^{\infty} a_{n-2}x^n = 0$

Since G(x) = $\sum_{n=0}^{\infty} a_n x^n$, therefore

(G(x)-a_0-a_1x)- 2x(G(x)-a_0)- 3x^2G(x) = 0

$\Rightarrow$ G(x)(1-2x-3x^2)-a_0-a_1x+2a_0x = 0

Put the value of $a_0 = 3$ and $a_1 = 1$,

G(x) = $\frac{3+x-6x}{(1-2x-3x^2)} = \frac{3-5x}{(1-2x-3x^2)}$

$= \frac{3-5x}{(1-3x)(1+x)}$

$= \frac{2}{(1+x)} + \frac{1}{(1-3x)}$

Therefore, the solution of recurrence relation will be

$a_n = 2(-1)^n + (3)^n$

This is the final answer.

Example: Solve the linear recurrence relation
$a_n - 2a_{n-1} + a_{n-2} = 2^n$, n $\geq$ 2
using the method of generating function with the initial conditions $a_0 = 2$, and $a_1 = 1$.
Solution:
$a_n - 2a_{n-1} + a_{n-2} = 2^n$ Multiply both sides by x^n and taking summation, we get

$\sum_{n=2}^{\infty} a_n x^n - 2\sum_{n=2}^{\infty} a_{n-1}x^n + \sum_{n=2}^{\infty} a_{n-2}x^n = \sum_{n=2} \infty 2^n x^n$

Since G(x) = $\sum_{n=0}^{\infty} a_n x^n$, therefore

(G(x)-a_0-a_1x)- 2x(G(x)-a_0)+ x^2G(x) = $\frac{4x^2}{(1-2x)}$

G(x)(1-2x+x^2)-a_0-a_1x+2a_0x = $\frac{4x^2}{(1-2x)}$

Put the value of $a_0 = 2$ and $a_1 = 1$,

G(x)(1-2x+x^2) = 2+x-4x + $\frac{4x^2}{(1-2x)}$

G(x) = $\frac{2-7x+10x^2}{(1-2x+x^2)(1-2x)}$

G(x) = $\frac{2-7x+10x^2}{(1-x)^2(1-2x)}$

G(x) = $\frac{3}{(1-x)}$ - $\frac{5}{(1-x)^2}$ + $\frac{4}{(1-2x)}$

Therefore, the solution of recurrence relation will be

$a_n = 3(1)^n$ -5(n+1) + $4(2)^n$

This is the final answer.

Example: Solve the linear recurrence relation
$a_{n+2} - 2a_{n+1} + a_n = 2^n$, n $\geq$ 2
using the method of generating function with the initial conditions $a_0 = 2$, and $a_1 = 1$.
Solution:
$a_{n+2} - 2a_{n+1} + a_n = 2^n$

Multiply both sides by x^n and taking summation, we get

$\sum_{n=0}^{\infty} a_{n+2}x^n - 2\sum_{n=0}^{\infty} a_{n+1}x^n + \sum_{n=0}^{\infty} a_n x^n = \sum_{n=0} \infty 2^n x^n$

Since G(x) = $\sum_{n=0}^{\infty} a_n x^n$, therefore

$\frac{(G(x)-a_0-a_1x)}{x^2}$- 2 $\frac{(G(x)-a_0)}{x}$+ G(x) = $\sum_{n=0} \infty 2^n x^n$

$\Rightarrow$ G(x)(1-2x+x^2)-a_0-a_1x+2a_0x = $\frac{x^2}{(1-2x)}$

Put the value of $a_0 = 2$ and $a_1 = 1$,

G(x)(1-2x+x^2) = 2+x-4x + $\frac{4x^2}{(1-2x)}$

G(x) = $\frac{2-7x+7x^2}{(1-2x+x^2)(1-2x)}$

= $\frac{2-7x+7x^2}{(1-x)^2(1-2x)}$

G(x) = $\frac{3}{(1-x)}$ - $\frac{2}{(1-x)^2}$ + $\frac{1}{(1-2x)}$

Therefore, the solution of recurrence relation will be

$a_n = 3(1)^n$ -2(n+1) + $(2)^n$
= 1 - 2n + 2^n
This is the final answer.

11.3 AKTU Examination Question

1. Obtain the generating function for the sequence 4, 4, 4, 4, 4, 4, 4.
2. Solve the following recurrence equation using generating function
   G(K) -7G(K-1) + 10G(K-2) = 8K + 6
3. Solve the recurrence relation by the method of generating function
   $a_n - 7a_{n-1} + 10a_{n-2} = 0$, n $\geq$ 2, Given $a_0 = 3$ and $a_1 = 3$.
4. Find the recurrence relation from y_n = A2^n + B(–3)^n.
5. Solve the recurrence relation
   $y_{n+2} - 5y_{n+1} + 6y_n = 5^n$ subject to the condition $y_0 = 0$, $y_1 = 2$.
6. Solve the recurrence relation using generating function:
   $a_n - 7a_{n-1} + 10a_{n-2} = 0$ with $a_0 = 3$, and $a_1 = 3$.
7. Solve the recurrence relation
   $a_{r+2} - 5a_{r+1} + 6a_r = (r+1)^2$