Fundamental Approach to

Discrete Mathematics

D.P. Acharjya
Sreekumar

NEW AGE INTERNATIONAL PUBLISHERS

Fundamental Approach to

Discrete Mathematics

THIS PAGE IS BLANK

Fundamental Approach to

Discrete Mathematics

D.P. Acharjya
Sreekumar

PUBLISHING FOR ONE WORLD

NEW AGE INTERNATIONAL (P) LIMITED, PUBLISHERS
New Delhi · Bangalore · Chennai · Cochin · Guwahati · Hyderabad
Jalandhar · Kolkata · Lucknow · Mumbai · Ranchi
Visit us at **www.newagepublishers.com**

Published by New Age International (P) Ltd., Publishers

ISBN (10) : 81-224-2304-3

ISBN (13) : 978-81-224-2304-4

PUBLISHING FOR ONE WORLD

NEW AGE INTERNATIONAL (P) LIMITED, PUBLISHERS
4835/24, Ansari Road, Daryaganj, New Delhi - 110002
Visit us at **www.newagepublishers.com**

Dedicated to my Beloved Parents

D. P. Acharjya

Dedicated to my Beloved Parents

Sreekumar

THIS PAGE IS BLANK

PREFACE

Discrete Mathematics, the study of finite systems, remains at the heart of any contemporary study of computer science, which is a need for every student to extend mathematical maturity and ability to deal with abstraction, algorithms and graphs. Our intention in writing this book is to offer fundamental concepts and methods of discrete mathematics in a precise and clear manner. In writing, the book our attempt is to provide the students of computer science and information technology the fundamental mathematical basis required to achieve in depth knowledge in the field of computer science. It will also help those students who have interest in mathematics to keep insight into mathematical techniques and their importance for application in real life.

This book is intended for one semester introductory course in discrete mathematics. The book is specially appropriate for the students of BE (Computer Science/IT), B.Tech. (Computer Science/IT), MCA and M.Sc. (Computer Science). The material in this book includes fundamental concepts, figures, tables, exercises and solved examples to help the reader master introductory discrete mathematics.

A discrete mathematics course has many objectives that students should learn the essentials of mathematics and how to think mathematically. To achieve these objectives we emphasized on mathematical reasoning and problem solving techniques in this book. Each chapter begins with a clear statement of definition, principles and theorems with illustrative and other descriptive materials. This is followed by sets of solved examples and exercises. The solved examples serve to illustrate and amplify the material. This has been done to make the book more flexible and to stimulate further interest in topics. Once basic mathematical concepts have been developed then more complex material and applications are presented.

The mathematical topics to be discussed are mathematical logic, set theory, binary relation, function, algebraic structure such as group theory and ring theory, Boolean algebra, graph theory and introduction to lattices. Although many excellent books exists in this area, we introduce this topic still keeping in mind that the reader will use them in practical applications related to computer science and information technology. It is hoped that the theoretical concepts present in this book will permit a student to understand most of the fundamental concepts. The text is designed that the students who do not have a strong background in discrete mathematics will find it very useful to begin with and the students with an exposure to discrete mathematics will also find the book very useful as some of exercises given are thought provoking and help them for application building.

We have the unique opportunity to express our deepest sense of gratitude to Prof. S. Nanda, NIT, Rourkela; Prof. B.K. Tripathy, Berhampur University, Prof. G.N. Patel, Sambalpur University and Dr. Md. N. Khan, IGIT, Sarang for their effective guidance, sincere advise and valuable suggestions during the project work and thus inspired us to take up an interesting and challenging project like this. We acknowledge to Prof. Sourya Pattnaik, Director, Rourkela Institute of Management Studies (RIMS), Rourkela who motivated and guided us in this project. We would like to acknowledge the contribution of many people, who have helped to bring this project successful.

No book-certainly no technical book is the product of its authors alone. We are pleased to acknowledge here the contributions of several colleagues who have had a major influence in this book and the course from which it arose. We shall be grateful to the readers for pointing out errors *and omissions that, in spite of all care might have crept in. We shall be delighted if this book* is accepted and appreciated by the scholars of today. You can **e-mail your comments to debi_69@rediffmail.com; debi_rims@yahoo.co.in or sreekumar42003@yahoo.com .**

At last but not the lest we express our heartfelt thanks to M/s New Age International (P) Ltd, Publishers, New Delhi, for the cooperation and publication with high accuracy.

D.P. Acharjya

Sreekumar

CONTENTS

THIS PAGE IS BLANK

1

Mathematical Logic

1.0 INTRODUCTION

Mathematics is considered to be a deductive science. We infer things from certain premises through logical reasoning. Consider an Example.

Three cap problem. A certain father had three sons: Sudeep, Sumeet and Ankeet. The father brought three caps of different colors; say Red, Blue and Black. He showed them the caps. After which they are blind folded. The father put three caps on the heads of three sons. Then the sons were taken away from his father to another room. Few minutes after father `called Ankeet and removed the blindfold of Ankeet and asked him to tell the color of his cap. Ankeet said he could not infer about the color of his own cap. Then he called Sumeet and removed the blindfold of Sumeet and asked him to tell the color of his cap by looking at the color of the cap of Ankeet. He too could not infer. Then he called Sudeep and asked him to tell the color of his cap without removing the blindfold of Sudeep. Sudeep replied he could tell the color of the cap on his own head.

How Sudeep come to that conclusion? Let us see. Sudeep asked two questions one to Ankeet and another to Sumeet. He asked to Ankeet about the color of Sumeet's cap and asked to Sumeet about the color of Ankeet's cap. By the way he got two colors of the cap. As a result Sudeep got the color of his own cap.

In the above reasoning we have certain premises and we conclude from them by a pure deductive reasoning. In the following passages we shall formalize the process of deduction.

1.1 STATEMENT (PROPOSITION)

A statement is a declarative sentence which is either true or false but not both. The statement is also known as proposition. The truth value True and False are denoted by the symbols **T** and **F** respectively. Some times it is also denoted by **1** and **0**, where **1** stands for true and **0** stands for false. As it depends on only two possible truth values, we call it as two-valued logic or bi-valued logic.

Consider the following examples

(*a*) Man is mortal.

(*b*) Sun rises in the east.
(*c*) Two is less then five.
(*d*) May God bless you!
(*e*) x is a Dog.
(*f*) Kittu is a nice Cat.
(*g*) It is too cold today.
(*h*) 6 is a composite number.

From the above example it is very clear that (*a*), (*b*), (*c*) and (*h*) are statements as they declare a definite truth value T or F. The other example (*d*), (*e*), (*f*), and (*g*) are not statements as they do not declare any truth value T or F.

Consider the sentence 111011 + 11 = 111110

The above sentence is a statement but its truth value depends on the context. If we consider the binary number system, the statement is True (T) but in decimal number system the statement is False (F).

■ 1.2 LOGICAL CONNECTIVES

Another important aspect is that logical connectives. We use some logical connectives to connect several statements into a single statement. The most basic and fundamental connectives are Negation, Composition and Disjunction.

1.2.1 Negation

It is observed that the negation of a statement is also a statement. We use the connective **Not** for negation. Usually the statements are denoted by single letters P, Q, R etc. If P be a statement, then the negation of P is denoted as $\neg$ P.

Consider the example of a statement.

P: Agra is the capital of India.
$\neg$ P: Agra is not the capital of India.

As we all know that New Delhi is the capital of India, the truth value for the statements P is False (F) and $\neg$ P is True (T). from the above it is clear that P and $\neg$ P has opposite truth values. $\neg$ P can also be written as

$\neg$ P: It is not true that Agra is the capital of India.

Rule: If P is True, then $\neg$ P is False and if P is false, then $\neg$ P is True.

Truth Table (Negation)

P	**$\neg$ P**
T	F
F	T

1.2.2 Conjunction

The conjunction of two statements P and Q is also a statement denoted by (P $\wedge$ Q). We use the connective **And** for conjunction.

Consider the example where P and Q are two statements.

P: $2 + 3 = 5$

Q: 5 is a composite number.

So, $(P \wedge Q)$: $2 + 3 = 5$ and 5 is a composite number.

As another example if P: Sudeep went to the college and Q: Aditi went to the college then $(P \wedge Q)$: Sudeep and Aditi went to the college.

It is clear that $(P \wedge Q)$ stand for P and Q. In order to make $(P \wedge Q)$ true, P and Q have to be simultaneously true.

Rule: $(P \wedge Q)$ is true if both P and Q are true, otherwise false.

Truth Table (Conjunction)

P	**Q**	**$(P \wedge Q)$**
T	T	T
T	F	F
F	T	F
F	F	F

1.2.3 Disjunction

The disjunction of two statements P and Q is also a statement denoted by $(P\vee Q)$. We use the connective **Or** for disjunction. Consider the example where P and Q are two statements

P: 2 + 3 is not equal to 5

Q: 5 is a prime number

So, $(P \vee Q)$: 2 + 3 is not equal to 5 or 5 is a prime number.

It is observed that $(P \vee Q)$ is true when P may be true or Q may be true and this also includes the case when both are true, that is the truth value of one statement is not assumed in exclusion of the truth value of the other statement. We call it as also inclusive or.

Rule: $(P \vee Q)$ is true if either P or Q is true and it is false when both P and Q are false.

Truth Table (Disjunction)

P	**Q**	**$(P \vee Q)$**
T	T	T
T	F	T
F	T	T
F	F	F

■ 1.3 CONDITIONAL

Let P and Q be any two statements. Then the statement $P \rightarrow Q$ is called a conditional statement. This can be put in any one of the following forms.

(*a*) If P, then Q

(*b*) P only if Q

(*c*) P implies Q

(*d*) Q if P

In an implication $P \rightarrow Q$, P is called the antecedent (hypothesis) and Q is called the consequent (conclusion). To explain the conditional statement, consider the example

A boy promises a girl "I will take you boating on Sunday if it is not raining".

Now if it is raining, then the boy would not be deemed to have broken his promise. The boy would be deemed to have broken his promise only when it is not raining and the boy did not take the girl for boating on Sunday.

Let us break the above conditional statement to symbolic from.

P: It is not raining

Q: I will take you boating on Sunday

So, the above statement reduces to $P \rightarrow Q$.

From the above discussion it is clear that if P is false then $P \rightarrow Q$ is true, whatever be the truth value of Q. The conditional $P \rightarrow Q$ is false if P is true and Q is false.

Rule: An implication (conditional) $P \rightarrow Q$ is False only when the hypothesis (P) is true and conclusion (Q) is false, otherwise True.

Truth Table (Conditional)

P	**Q**	**(P → Q)**
T	T	T
T	F	F
F	T	T
F	F	T

1.4 BI-CONDITIONAL

Let P and Q be any two statements. Then the statement $P \leftrightarrow Q$ is called a bi-conditional statement. This $P \leftrightarrow Q$ can be put in any one of the following forms.

(*a*) P if and only if Q (*b*) P is necessary and sufficient of Q

(*c*) P is necessary and sufficient for Q (*d*) P is implies and implied by Q

The bi-conditional (double implication) $P \leftrightarrow Q$ is defined as

$$\mathbf{(P \leftrightarrow Q): (P \rightarrow Q) \wedge (Q \rightarrow P)}$$

From the truth table discussed below it is clear that $P \leftrightarrow Q$ has the truth value T whenever both P and Q have identical truth values.

Truth Table (Bi-Conditional)

P	**Q**	**P → Q**	**Q → P**	**(P ↔ Q)**
T	T	T	T	T
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

Rule: $(P \leftrightarrow Q)$ is True only when both P and Q have identical truth Values, otherwise false.

■ 1.5 CONVERSE

Let P and Q be any two statements. The converse statement of the conditional P → Q is given as Q → P.

Consider the example "all concurrent triangles are similar". The above statement can also be written as "if triangles are concurrent, then they are similar".

Let P : Triangles are concurrent
Q : Triangles are similar

So, the statement becomes P → Q. The converse statement is given as "if triangles are similar, then they are concurrent" or all similar triangles are concurrent.

■ 1.6 INVERSE

Let P and Q be any two statements. The inverse statement of the conditional (P → Q) is given as (¬ P → ¬ Q).

Consider the Example "all concurrent triangles are similar". The above statement can also be written as "if triangles are concurrent, then they are similar".

Let P : Triangles are concurrent
Q : Triangles are similar

So, the statement becomes P → Q. The inverse statement is given as "if triangles are not concurrent, then they are not similar".

■ 1.7 CONTRA POSITIVE

Let P and Q be any two statements. The contra positive statement of the conditional (P → Q) is given as (¬ Q → ¬ P). Consider the Example "all concurrent triangles are similar". The above statement can also be written as "if triangles are concurrent, then they are similar".

Let P : Triangles are concurrent and
Q : Triangles are similar

So, the statement becomes P → Q. The contra positive statement is given as "if triangles are not similar, then they are not concurrent".

Truth Table (Contra positive)

P	**Q**	**P → Q**	**¬ Q**	**¬ P**	**(¬ Q → ¬ P)**
T	T	T	F	F	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

From the truth table it is observed that both conditional (P → Q) and contra positive (¬ Q → ¬ P) have same truth values.

■ 1.8 EXCLUSIVE OR

Let P and Q be any two statements. The exclusive OR of two statements P and Q is denoted by $(P \barvee Q)$. We use the connective XOR for exclusive OR. The exclusive OR $(P \barvee Q)$ is true if either P or Q is True but not both. The exclusive OR is also termed as exclusive disjunction.

Consider the example where P and Q be two statements such that $P \equiv 2 + 3 = 5$ and $Q \equiv 5 - 3 = 2$. Here both the statements are true. Therefore $(P \barvee Q)$ is false.

Rule : $(P \barvee Q)$ is true if either P or Q is True but not both, otherwise false.

Truth Table (Exclusive OR)

P	**Q**	**$(P \barvee Q)$**
T	T	F
T	F	T
F	T	T
F	F	F

■ 1.9 NAND

The word NAND stands for NOT and AND. The connective NAND is denoted by the symbol $\uparrow$. If P and Q be two statements, then NAND of P and Q is given as $(P \uparrow Q)$ defined by

$$(P \uparrow Q) \equiv \neg (P \wedge Q).$$

Rule : $(P \uparrow Q)$ is True if either P or Q is false, otherwise False.

Truth Table (NAND)

P	**Q**	**$(P \uparrow Q)$**
T	T	F
T	F	T
F	T	T
F	F	T

■ 1.10 NOR

The word NOR stands for NOT and OR. The connective NOR is denoted by the symbol $\downarrow$. If P and Q be two statements, then NOR of P and Q is given as $(P \downarrow Q)$ defined by

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

Rule : $(P \downarrow Q)$ is True only when both P and Q are false, otherwise false.

Truth Table (NOR)

P	**Q**	**$(P \downarrow Q)$**
T	T	F
T	F	F
F	T	F
F	F	T

■ 1.11 TAUTOLOGY

If the truth values of a composite statement are always true irrespective of the truth values of the atomic (individual) statements, then it is called a tautology.

For example the composite statement (P ∧ (P → Q)) → Q is a tautology. To verify this draw the truth table with composite statement as (P ∧ (P → Q)) → Q

Truth Table

P	**Q**	**(P → Q)**	**P ∧ (P → Q)**	**(P ∧ (P → Q)) → Q**
T	T	T	T	T
T	F	F	F	T
F	T	T	F	T
F	F	T	F	T

So, (P ∧ (P → Q)) → Q is a tautology.

■ 1.12 CONTRADICTION

If the truth values of a composite statement are always false irrespective of the truth values of the atomic statements, then it is called a contradiction or unsatisfiable.

For example the composite statement ¬ (P→ (Q → (P ∧ Q))) is a contradiction.

To verify this draw the truth table of ¬ (P → (Q → (P ∧ Q))). Let R ≡ P → (Q → (P ∧ Q))

Truth Table

P	**Q**	**(P ∧ Q)**	**Q → (P ∧ Q)**	**(P → (Q → (P ∧ Q))**	**¬ R**
T	T	T	T	T	F
T	F	F	T	T	F
F	T	F	F	T	F
F	F	F	T	T	F

So, ¬ R ≡ ¬ (P → (Q → (P ∧ Q))) is a contradiction.

■ 1.13 SATISFIABLE

If the truth values of a composite statement are some times true and some times false irrespective of the truth values of the atomic statements, then it is called a satisfiable.

Consider the composite statement (P → Q) → (Q → P). To verify this draw the truth table of (P → Q) → (Q → P).

Truth Table

P	**Q**	**P → Q**	**Q → P**	**(P → Q) → (Q → P)**
T	T	T	T	T
T	F	F	T	T
F	T	T	F	F
F	F	T	T	T

So, the composite statement (P → Q) → (Q → P) is satisfiable.

1.14 DUALITY LAW

Two formulae P and P* are said to be duals of each other if either one can be obtained from the other by interchanging $\wedge$ by $\vee$ and $\vee$ by $\wedge$. The two connectives $\wedge$ and $\vee$ are called dual to each other.

Consider the formulae $P \equiv (P \vee Q) \wedge R$ and $P^* \equiv (P \wedge Q) \vee R$ which are dual to each other.

1.15 ALGEBRA OF PROPOSITIONS

If P, Q and R be three statements, then the following laws hold good.

(*a*) Commutative Laws: $P \wedge Q \equiv Q \wedge P$ and
$P \vee Q \equiv Q \vee P$

(*b*) Associative Laws: $P \wedge (Q \wedge R) \equiv (P \wedge Q) \wedge R$ and
$P \vee (Q \vee R) \equiv (P \vee Q) \vee R$

(*c*) Distributive Laws: $P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$ and
$P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$

(*d*) Idempotent Laws: $P \wedge P \equiv P$ and
$P \vee P \equiv P$

(*e*) Absorption Laws: $P \vee (P \wedge Q) \equiv P$ and
$P \wedge (P \vee Q) \equiv P$

1.15.1 De Morgan's Laws

If P and Q be two statements, then

(*i*) $\neg (P \wedge Q) \Leftrightarrow (\neg P) \vee (\neg Q)$ and
(*ii*) $\neg (P \vee Q) \Leftrightarrow (\neg P) \wedge (\neg Q)$

1.16 MATHEMATICAL INDUCTION

Generally direct methods are adopted for proving theorems and propositions. Sometimes it is too difficult and tedious. As a result the other methods are developed for proving theorems and propositions. These are (*i*) method of contra positive, (*ii*) method of contradiction and (*iii*) method of induction. The method of induction is otherwise known as mathematical induction.

Suppose that n be a natural number. Our aim is to show that some statement P(n) involving n is true for any n. The following steps are used in mathematical induction.

1. Suppose that P(n) be a statement.
2. Show that P(1) and P(2) are true. *i.e*. P(n) is true for n = 1 and n = 2.
3. Assume that P(k) is true. *i.e*. P(n) is true for n = k.
4. Show that P(k + 1) follows from P(k).

Consider an example $1+ 2 + 3 + \ldots + n = \dfrac{n(n+1)}{2}$

Suppose that $P(n) \equiv 1+ 2 + 3 + \ldots + n = \dfrac{n(n+1)}{2}$

So, $$P(1) \equiv 1 = \frac{1(1+1)}{2}$$

and $$P(2) \equiv 1 + 2 = 3 = \frac{2(2+1)}{2}$$

So, P(1) and P(2) are true.

Assume that P(k) is true. So,

$$1 + 2 + 3 + \ldots + k = \frac{k(k+1)}{2}$$

So, $$P(k+1) \equiv 1 + 2 + 3 + \ldots + k + (k+1)$$

$$= \frac{k(k+1)}{2} + (k+1) \qquad [\because \ P(k) \text{ is true.}]$$

$$= \left(\frac{k+1}{2}\right)(k+2) = \frac{(k+1)(k+2)}{2}$$

Which shows that P(k + 1) is also true. Hence P(n) is true for all n.

SOLVED EXAMPLES

Example 1 *Find the negation of $P \to Q$.*

Solution : $P \to Q$ is equivalently written as $(\neg P \vee Q)$

So, negation of $$P \to Q \equiv \neg(\neg P \vee Q)$$
$$\equiv \neg(\neg P) \wedge (\neg Q), \text{ (By De-Morgan's Law)}$$
$$\equiv P \wedge (\neg Q)$$

Hence the negation of $P \to Q$ is $P \wedge (\neg Q)$.

Example 2 *Construct the truth table for $(P \to Q) \leftrightarrow (\neg P \vee Q)$.*

Solution : The given compound statement is $(P \to Q) \leftrightarrow (\neg P \vee Q)$ where P and Q are two atomic statements.

P	**Q**	**$\neg$ P**	**P$\to$ Q**	**$\neg$ P $\vee$ Q**	**(P $\to$ Q) $\leftrightarrow$ ($\neg$ P $\vee$ Q)**
T	T	F	T	T	T
T	F	F	F	F	T
F	T	T	T	T	T
F	F	T	T	T	T

Example 3 *Construct the truth table for $P \to (Q \leftrightarrow P \wedge Q)$.*

Solution : The given compound statement is $P \to (Q \leftrightarrow P \wedge Q)$, where P and Q are two atomic statements.

P	**Q**	**P $\wedge$ Q**	**Q $\leftrightarrow$ P $\wedge$ Q**	**P $\to$ (Q $\leftrightarrow$ P $\wedge$ Q)**
T	T	T	T	T
T	F	F	T	T
F	T	F	F	T
F	F	F	T	T

Example 4 *Find the negation of the following statement. " If Cows are Crows then Crows are four legged".*

Solution : Let P: Cows are Crows

Q : Crows are four legged

Given statement: If Cows are Crows then Crows are four legged.

$$\equiv P \to Q$$

So, the negation is given as $P \wedge (\neg Q)$ *i.e.* Cows are Crows and Crows are not four legged.

Example 5 *Find the negation of the following statement.*

He is rich and unhappy.

Solution : Let$P \equiv$ He is rich

$Q \equiv$ He is unhappy

Given statement: He is rich and unhappy

$$\equiv P \wedge Q$$

By De-Morgan's law $\neg (P \wedge Q) \equiv \neg P \vee \neg Q$

$\equiv$ He is neither rich nor unhappy.

Example 6 *Prove by constructing truth table*

$$P \to (Q \vee R) \equiv (P \to Q) \vee (P \to R)$$

Solution : Our aim to prove $P \to (Q \vee R) \equiv (P \to Q) \vee (P \to R)$

Let P, Q and R be three atomic statements.

P	**Q**	**R**	**$Q \vee R$**	**$P \to (Q \vee R)$**	**$P \to Q$**	**$P \to R$**	**$(P \to Q) \vee (P \to R)$**
T	T	T	T	T	T	T	T
T	F	F	F	F	F	F	F
F	T	F	T	T	T	T	T
F	F	T	T	T	T	T	T
F	T	T	T	T	T	T	T
T	F	T	T	T	F	T	T
T	T	F	T	T	T	F	T
F	F	F	F	T	T	T	T

From the truth table it is clear that $P \to (Q \vee R) \equiv (P \to Q) \vee (P \to R)$.

Example 7 *Find the negation of $P \leftrightarrow Q$.*

Solution : $P \leftrightarrow Q$ is equivalently written as $(P \to Q) \wedge (Q \to P)$

So, $\neg (P \leftrightarrow Q) \equiv \neg ((P \to Q) \wedge (Q \to P))$

$\equiv \neg (P \to Q) \vee \neg (Q \to P)$; (De-Morgan's law)

$\equiv \neg (\neg P \vee Q) \vee \neg (\neg Q \vee P)$

$\equiv (P \wedge \neg Q) \vee (Q \wedge \neg P)$; (De-Morgan's Law)

Hence $\neg (P \leftrightarrow Q) \equiv (P \wedge \neg Q) \vee (Q \wedge \neg P)$.

Example 8 *With the help of truth table prove that $\neg (P \wedge Q) \equiv \neg P \vee \neg Q$.*

Solution : Our claim is $\neg (P \wedge Q) \equiv \neg P \vee \neg Q$.

Let P and Q be two atomic statements.

P	**Q**	**P $\wedge$ Q**	**$\neg$ (P$\wedge$ Q)**	**$\neg$ P**	**$\neg$ Q**	**$\neg$ P $\vee$ $\neg$ Q**
T	T	T	F	F	F	F
T	F	F	T	F	T	T
F	T	F	T	T	F	T
F	F	F	T	T	T	T

From the truth table it is clear that $\neg$ (P $\wedge$ Q) $\equiv$ $\neg$ P $\vee$ $\neg$ Q.

Example 9 *Show that (P $\rightarrow$ Q) $\leftrightarrow$ ($\neg$P $\vee$Q) is a tautology.*

Solution : Let P and Q be two atomic statements. Our aim is to show (P $\rightarrow$ Q) $\leftrightarrow$ ($\neg$ P $\vee$ Q) is a tautology.

P	**Q**	**P $\rightarrow$ Q**	**$\neg$ P**	**$\neg$ P $\vee$ Q**	**(P $\rightarrow$ Q) $\leftrightarrow$ ($\neg$ P $\vee$ Q)**
T	T	T	F	T	T
T	F	F	F	F	T
F	T	T	T	T	T
F	F	T	T	T	T

Hence (P $\rightarrow$ Q) $\leftrightarrow$ ($\neg$ P $\vee$ Q) is a tautology.

Example 10 *Show that the following statements are equivalent.*

Statement 1 : Good food is not cheap

Statement 2 : Cheap food is not good.

Solution : Let P $\equiv$ Food is good and Q $\equiv$ Food is cheap

Statement 1 : Good food is not cheap

i.e. P $\rightarrow$ $\neg$ Q

Statement 2 : Cheap food is not good

i.e. Q $\rightarrow$ $\neg$ P

Truth Table

P	**Q**	**$\neg$ P**	**$\neg$ Q**	**P $\rightarrow$ $\neg$ Q**	**Q $\rightarrow$ $\neg$ P**
T	T	F	F	F	F
T	F	F	T	T	T
F	T	T	F	T	T
F	F	T	T	T	T

From truth table it is clear that both statements are equivalent.

Example 11 *Express P $\rightarrow$ Q using $\downarrow$ and $\uparrow$ only.*

Solution :

$$
\begin{aligned}
P \rightarrow Q &\equiv \neg P \vee Q \\
&\equiv \neg P \vee \neg\ (\neg Q) \\
&\equiv \neg (P \wedge \neg Q) \equiv P \uparrow \neg Q \\
&\equiv P \uparrow (\neg Q \vee \neg Q) \\
&\equiv P \uparrow \neg (Q \wedge Q) \equiv P \uparrow (Q \uparrow Q)
\end{aligned}
$$

i.e. $P \rightarrow Q \equiv P \uparrow (Q \uparrow Q)$

Example 12 *Prove that $(P \wedge Q) \wedge \neg(P \vee Q)$ is a contradiction.*

Solution : Truth table for $(P \wedge Q) \wedge \neg (P \vee Q)$

P	**Q**	**$(P \wedge Q)$**	**$(P \vee Q)$**	**$\neg (P \vee Q)$**	**$(P \wedge Q) \wedge \neg (P \vee Q)$**
T	T	T	T	F	F
T	F	F	T	F	F
F	T	F	T	F	F
F	F	F	F	T	F

Hence $(P \wedge Q) \wedge \neg (P \vee Q)$ is a contradiction.

Example 13 *Express $P \leftrightarrow Q$ using $\downarrow$ and $\uparrow$ only.*

Solution

$$\begin{aligned}
P \leftrightarrow Q &\equiv (P \to Q) \wedge (Q \to P)\\
&\equiv (\neg P \vee Q) \wedge (P \vee \neg Q)\\
&\equiv ((\neg P \vee Q) \wedge P) \vee ((\neg P \vee Q) \wedge \neg Q)\\
&\equiv \neg (\neg ((\neg P \vee Q) \wedge P) \wedge \neg ((\neg P \vee Q) \wedge \neg Q))\\
&\equiv \neg ((\neg P \vee Q) \wedge P) \uparrow \neg ((\neg P \vee Q) \wedge \neg Q)\\
&\equiv ((\neg P \vee Q) \uparrow P) \uparrow ((\neg P \vee Q) \uparrow \neg Q)\\
&\equiv (\neg (P \wedge \neg Q) \uparrow P) \uparrow (\neg (P \wedge \neg \ Q) \uparrow \neg Q)\\
&\equiv ((P \uparrow \neg Q) \uparrow P) \uparrow ((P \uparrow \neg Q) \uparrow \neg Q)\\
&\equiv ((P \uparrow (\neg Q \vee \neg Q) \uparrow P) \uparrow ((P \uparrow (\neg Q \vee \neg Q)) \uparrow (\neg Q \vee \neg Q))\\
&\equiv ((P \uparrow \neg (Q \wedge Q) \uparrow P) \uparrow ((P \uparrow \neg (Q \wedge Q)) \uparrow \neg (Q \wedge Q))\\
&\equiv ((P \uparrow (Q \uparrow Q) \uparrow P) \uparrow ((P \uparrow (Q \uparrow Q)) \uparrow (Q \uparrow Q))
\end{aligned}$$

Note: These expressions are not unique.

Alternative Solution :

$$\begin{aligned}
P \leftrightarrow Q &\equiv (P \to Q) \wedge (Q \to P)\\
&\equiv (\neg P \vee Q) \wedge (P \vee \neg Q)\\
&\equiv ((\neg P \vee Q) \wedge P) \vee ((\neg P \vee Q) \wedge \neg Q)\\
&\equiv ((\neg P \wedge P) \vee (Q \wedge P)) \vee ((\neg P \wedge \neg Q) \vee (Q \wedge \neg Q))\\
&\equiv (Q \wedge P) \vee (\neg P \wedge \neg Q)\\
&\equiv \neg (\neg (Q \wedge P)) \vee \neg (P \vee Q)\\
&\equiv \neg (\neg (Q \wedge P) \wedge (P \vee Q))\\
&\equiv \neg (Q \wedge P) \uparrow (P \vee Q)\\
&\equiv (Q \uparrow P) \uparrow \neg (\neg (P \vee Q))\\
&\equiv (Q \uparrow P) \uparrow \neg \ (\neg P \wedge \neg Q))\\
&\equiv (Q \uparrow P) \uparrow (\neg P \uparrow \neg Q)\\
&\equiv (Q \uparrow P) \uparrow ((\neg P \vee \neg P) \uparrow (\neg Q \vee \neg Q))\\
&\equiv (Q \uparrow P) \uparrow (\neg (P \wedge P) \uparrow \neg (Q \wedge Q))\\
&\equiv (Q \uparrow P) \uparrow ((P \uparrow P) \uparrow (Q \uparrow Q))
\end{aligned}$$

Example 14 *Prove that $n\ (n + 1)$ is an even natural number.*

Solution : Suppose that $P(n) \equiv n\ (n + 1)$ is even.

So, $P(1) \equiv 1(1 + 1) = 2$, which is even and

$P(2) \equiv 2\ (2 + 1) = 6$, which is also even.

Hence P(1) and P(2) are true.

Assume that $P(k) \equiv k\,(k+1)$ is even

i.e $k\,(k+1) = 2m;\ m \in N$

So, $P(k+1) \equiv (k+1)\,(k+2) = k\,(k+1) + 2\,(k+1)$

$= 2m + 2\,(k+1)$ [$\therefore$ P(k) is true.]

$= 2(m + k + 1)$, which is even

Which shows that P(k + 1) is also true.

So, P(n) is true for all n.

Example 15 *Show by truth table the following statements are equivalent.*

Statement 1 : Rich men are unhappy.

Statement 2 : Men are unhappy or poor.

Solution : Let $P \equiv$ Men are Rich and $Q \equiv$ Men are unhappy.

Statement 1 : Rich men are unhappy.

i.e. If men are rich then they are unhappy.

i.e. $P \rightarrow Q$.

Statement 2 : Men are unhappy or poor.

i.e $Q \vee \neg P$; (Here poor indicates not rich)

P	**Q**	**P → Q**	**¬ P**	**Q ∨ ¬ P**
T	T	T	F	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

So, it is clear that both statements are equivalent

Example 16 *A boy promises a girl "I will take you park on Monday if it is not raining". When the boy would be deemed to have broken his promise. Explain with the help of truth table.*

Solution Let P : I will take you park on Monday

Q : It is raining.

Given statement : I will take you park on Monday if it is not raining

i.e. P if $\neg$ Q

i.e. $\neg Q \rightarrow P$

Truth Table

P	**Q**	**¬ Q**	**¬ Q → P**
T	T	F	T
T	F	T	T
F	T	F	T
F	F	T	F

It indicates that if ¬ Q is true and P is false, then the boy is deemed to have broken his promise. *i.e.* When it is not raining and the boy does not take her park on Monday, Then the boy is deemed to have broken his promise.

Example 17 *Prove by method of induction*

$$1^3 + 2^3 + 3^3 + ... + n^3 = \left(\frac{n\,(n+1)}{2}\right)^2$$

Solution : Suppose that $P(n) \equiv 1^3 + 2^3 + 3^3 +.... + n^3 = \left(\frac{n\,(n+1)}{2}\right)^2$

So, $$P(1) = 1^3 = 1 = \left(\frac{1(1+1)}{2}\right)^2$$

and $$P(2) = 1^3 + 2^3 = 9 = \left(\frac{2\,(2+1)}{2}\right)^2$$

Hence P(1) and P(2) are true.

Assume that P(k) is true, so

$$P(k) \equiv 1^3 + 2^3 + 3^3 +.....+ k^3 = \left(\frac{k\,(k+1)}{2}\right)^2$$

$$P(k{+}1) \equiv 1^3 + 2^3 + 3^3 +.....+ k^3 + (k + 1)^3$$

$$= \left(\frac{k\,(k+1)}{2}\right)^2 + (k + 1)^3 \qquad [\because \; P(k) \text{ is true.}]$$

$$= (k + 1)^2\,(k^2 + 4\,(k + 1))\,/\,4$$

$$= \left(\frac{(k+1)\,(k+2)}{2}\right)^2$$

Which shows that P(k + 1) is also true.

So, P(n) is true for all n .

Example 18 *Show by method of induction*

$$\frac{1}{1*2} + \frac{1}{2*3} + \frac{1}{3*4} + ... + \frac{1}{n*(n+1)} = \frac{n}{n+1}$$

Solution : Suppose that

$$P(n) \equiv \frac{1}{1*2} + \frac{1}{2*3} + \frac{1}{3*4} + ... + \frac{1}{n*(n+1)} = \frac{n}{n+1}$$

So, $$P(1) \equiv \frac{1}{1*2} = \frac{1}{2} = \frac{1}{1+1} \text{ and}$$

$$P(2) \equiv \frac{1}{1*2} + \frac{1}{2*3} = \frac{1}{2} + \frac{1}{6} = \frac{2}{3} = \frac{2}{2+1}$$

Assume that P(k) is true . So,

$$P(k) \equiv \frac{1}{1*2} + \frac{1}{2*3} + \frac{1}{3*4} + \ldots + \frac{1}{k*(k+1)} = \frac{k}{k+1}$$

$$\therefore \qquad P(k+1) \equiv \frac{1}{1*2} + \frac{1}{2*3} + \frac{1}{3*4} + \ldots + \frac{1}{k*(k+1)} + \frac{1}{(k+1)*(k+2)}$$

$$= \frac{k}{k+1} + \frac{1}{(k+1)*(k+2)} \; ; \qquad [\because \quad P(k) \text{ is true}]$$

$$= \frac{1}{(k+1)}\left(k + \frac{1}{(k+2)}\right)$$

$$= \frac{1}{(k+1)}\left(\frac{k^2 + 2*k + 1}{(k+2)}\right)$$

$$= \frac{(k+1)^2}{(k+1)(k+2)} = \frac{k+1}{k+2}$$

Which shows that P(k + 1) is also true.

So, P(n) is true for all n.

EXERCISES

1. Find the negation of the following statements.

(*a*) Today is Sunday or Monday.

(*b*) If I am tired and busy, then I cannot study.

(*c*) Either it is raining or some one left the shower on.

(*d*) The moon rises in the west.

(*e*) The triangles are equilateral is necessary and sufficient for three equal sides.

(*f*) $2 + 3 \neq 18$.

2. Prove the following by using truth table.

(*a*) $P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$ (*b*) $P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$

(*c*) $\neg (P \vee Q) \equiv \neg P \wedge \neg Q$ (*d*) $P \rightarrow (Q \wedge R) \equiv (P \rightarrow Q) \wedge (P \rightarrow R)$

(*e*) $(P \wedge Q) \wedge R \equiv P \wedge (Q \wedge R)$ (*f*) $P \vee Q \equiv \neg (\neg P \wedge \neg Q)$

(*g*) $P \overline{\vee} Q \equiv (P \vee Q) \wedge \neg (P \wedge Q)$ (*h*) $(P \downarrow Q) \downarrow (P \downarrow Q) \equiv P \vee Q$

(*i*) $P \wedge Q \equiv (P \downarrow P) \downarrow (Q \downarrow Q)$ (*j*) $\neg (P \vee Q) \vee (\neg P \wedge Q) \equiv \neg P$

3. For each of the following formulas tell whether it is (*i*) tautology, (*ii*) satisfiable, or (*iii*) contradiction.

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

(*c*) $P \wedge \neg Q$ (*d*) $(P \vee Q) \rightarrow P$

(*e*) $\neg (P \rightarrow Q) \rightarrow (P \wedge \neg Q)$ (*f*) $(P \rightarrow Q) \rightarrow (Q \rightarrow P)$

(*g*) $((P \rightarrow Q) \leftrightarrow Q) \rightarrow P$ (*h*) $\neg P \wedge (P \vee Q) \rightarrow P$

(*i*) $P \rightarrow (P \wedge Q)$ (*j*) $P \rightarrow (Q \rightarrow (P \wedge Q))$

(*k*) $(P \vee Q) \leftrightarrow (Q \wedge P)$ (*l*) $(P \rightarrow (Q \rightarrow (P \wedge Q))) \leftrightarrow P$

4. Prove by using different laws.

(*a*) $\neg (P \vee Q) \vee (\neg P \wedge Q) \equiv \neg P$ (*b*) $P \vee (P \wedge Q) \equiv P$

(*c*) $(P \vee Q) \wedge \neg P \equiv \neg P \wedge Q$

5. Write each of the following in symbolic form by indicating statements.

(*a*) Ram is rich and unhappy.

(*b*) Sudeep speaks English or Oriya.

(*c*) I am hungry and I can study.

(*d*) I am tired if and only if I work hard.

(*e*) If Bhubaneswar is a city, then it is the capital of Orissa.

(*f*) $5 + 2 = 7$ if $7 - 2 = 5$.

6. Write the truth value of each of the following statements.

(*a*) Sun rises in the south.

(*b*) Man is mortal.

(*c*) Delhi is the capital of India.

(*d*) If three sides of a triangle are equal, then it is an equilateral triangle.

(*e*) $(11101)_2 + (1)_2 = (11110)_2$

(*f*) $(11101)_{10} + (1)_{10} = (11110)_{10}$

(*g*) $(11111)_2 + (1)_2 = (100000)_2$ and $(111)_2 = (7)_{10}$

(*h*) $(270)_8 + (5)_8 = (184)_{10}$ or $(11101)_2 + (111)_2 = (100101)_2$

(*i*) $2^2 = 9$ if and only if $2 \neq 3$

(*j*) $(111)_2 + (010)_2 = (1001)_2$ if and only if $(1001)_2 - (010)_2 = (111)_2$.

7. Write the converse, inverse and contra positive of the following statement by indicating the conditional statement.

(*a*) In binary number system $1 + 1 = 10$.

(*b*) Good food are not cheap.

(*c*) If $9x + 36 = 9$ then $x \neq 17$.

(*d*) If $\cos(x) = 1$ then $x = 0$.

(*e*) Two sets are similar if they contains equal number of elements.

8. Prove by using method of induction.

(*a*) $1^2 + 2^2 + 3^2 + \ldots\ldots + n^2 = \dfrac{n\,(n+1)\,(2n+1)}{6}$

(*b*) $1 + r + r^2 + \ldots\ldots + r^{n-1} = \dfrac{1-r^n}{1-r}; r \neq 1$

(*c*) $1 + r + r^2 + \ldots\ldots + r^n = \dfrac{1-r^{n+1}}{1-r}; r \neq 1$

(*d*) $a + ar + ar^2 + \ldots\ldots + ar^n = \dfrac{a\left(1-r^{n+1}\right)}{1-r}; r \neq 1$

(*e*) $a + (a + d) + (a + 2d) + \ldots. + (a + (n-1)d) = \dfrac{n\left(2a + (n-1)\,d\right)}{2}$

(*f*) $3 + 7 + 11 + \ldots + (4n - 1) = n\,(2n + 1)$

(*g*) $2 + 4 + 6 + \ldots. + 2n = n\,(n + 1)$

(*h*) $1^2 + 4^2 + 7^2 + \ldots. + (3n - 2)^2 = \dfrac{n\left(6n^2 - 3n - 1\right)}{2}$

(*i*) $3 * 6 + 6 * 9 + \ldots + 3n\,(3n + 3) = 3n\,(n + 1)\,(n + 2)$

(*j*) $1 * 2 + 2 * 3 + 3 * 4 + \ldots. + n(n + 1) = \dfrac{n\,(n+1)\,(n+2)}{3}$

(*k*) $1 * 2 * 3 + 2 * 3 * 4 + \ldots. + n(n + 1)\,(n + 2) = \dfrac{n\,(n+1)\,(n+2)\,(n+3)}{4}$

(*l*) $1 + 2 * 3 + 3 * 5 + \ldots + n(2n - 1) = \dfrac{n\,(n+1)\,(4n-1)}{6}$

(*m*) $1 * 3 * 5 + 3 * 5 * 7 + \ldots. + (2n - 1)\,(2n + 1)(2n + 3) = n\,(n + 2)(2n^2 + 4n - 1)$.

(*n*) $1^2 + (1^2 + 2^2) + (1^2 + 2^2 + 3^2) + \ldots. + (1^2 + 2^2 + \ldots + n^2) = \dfrac{n\,(n+1)^2\,(n+2)}{12}$

(*o*) $1 * 2^2 + 2 * 3^2 + \ldots + n\,(n + 1)^2 = \dfrac{n\,(n+1)\,(n+2)\,(3n+5)}{12}$

(*p*) $3 * 8 + 6 * 11 + \ldots + 3n\,(3n + 5) = 3n\,(n + 1)\,(n + 3)$

(*q*) $1 + (1 + 4) + (1 + 4 + 7) + \ldots. + (1 + 4 + 7 + \ldots + (3n - 2)) = \dfrac{n^2\,(n+1)}{2}$

(*r*) $2 + 6 + 12 + 20 + \ldots.. + \dfrac{n\,(2n+2)}{2} = \dfrac{n\,(n+1)\,(n+2)}{3}$

(*s*) $1 + \dfrac{1}{2} + \dfrac{1}{4} + \ldots + \dfrac{1}{2^{n-1}} = \dfrac{2^n - 1}{2^{n-1}}$

(*t*) $1 * 4 + 2 * 7 + 3 * 10 + \ldots. + n\,(3n + 1) = n\,(n + 1)^2$

2

Set Theory

2.0 INTRODUCTION

An ordinary understanding of a set is a collection of objects. In our day-to-day life we use phrases like a set of utensils, a bunch of flowers, a set of books, a herd of cattle, a set of birds and etc.. Which are all examples of sets.

In the 19th century the German Mathematician George Cantor developed the theory of sets to define numbers and to base mathematics on a solid logical foundation. In late 19th century, Frege developed these ideas further, but his work did not attract much attention. In 20th century Bertrand Russell rediscovered his analysis independently. His works in 1903 led to the monumental work with North Whitehead the principia Mathematica a land mark in the foundations of mathematics. It was observed in 1940s that all mathematics could develop from the idea of sets and mathematics was systematized.

In this chapter we try to impart fundamental concepts and approach to the problem. i.e. how to proceed for the expected solution as for as set theory is concerned. By the way we will study and learn about the basic concepts of sets, some of the operations on sets, Venn diagrams, Cartesian product of sets and its applications.

2.1 SETS

Collection of well defined objects is called a set. Well defined means distinct and distinguishable. The objects are called as elements of the set. The ordering of elements in a set does not change the set. *i.e.* the ordering of elements can not play a vital role in the set theory. For example

$$A = \{a, b, c, d\} \text{ and } B = \{b, a, d, c\} \text{ are equal sets.}$$

The symbol $\in$ stands for 'belongs to'. $x \in$ A means x is an element of the set A. It is observed that if A be a set and x is any object, then either $x \in$ A or $x \notin$ A but not both. Generally sets are denoted by capital letters A, B, C and etc.

Consider the examples of set:

$$A = \{2, 4, 6, 8, 10, 12, 14, 16, 18\}$$

$$B = \{x, y, z, u, v, w\}$$
$$N = \{1, 2, 3, ...\}$$
$$I = \{... -2, -1, 0, 1, 2, 3, ...\}$$

In general the set can be expressed in two ways. *i.e.* Tabular method (Roster method) and Set-builder method (Specification method).

2.1.1 Tabular Method

Expressing the elements of a set within a parenthesis where the elements are separated by commas is known as tabular method, roster method or method of extension.

Consider the example

$$A = \{1, 3, 5, 7, 9, 11, 13, 15\}$$

2.1.2 Set Builder Method

Expressing the elements of a set by a rule or formula is known as set-builder method, specification method or method of intension. Mathematically

$$S = \{x \mid P(x)\}$$

where P(x) is the property that describes the elements of the set. The symbol | stands for 'such that'. It is not possible to write every set in tabular form. Consider an example

$$S = \{x \mid x \text{ is an Italian}\}$$

The above set S can not be expressed in tabular form as it is impossible to list all Italians. Consider the examples

$$A = \{x \mid x = 2n + 1; 0 \le n \le 7; n \in I\}$$
$$= \{1, 3, 5, 7, 9, 11, 13, 15\}$$

and

$$B = \{x \mid x = 1, x = a, x = \text{Book}, x = \text{Pen}\}$$
$$= \{1, a, \text{Book}, \text{Pen}\}$$

From the second example given above it is clear that the elements of a set do not have any common property also.

■ 2.2 TYPES OF SETS

Here we will discuss the different types of sets.

2.2.1 Finite Set

A set which contains finite number of elements is known as finite set. Consider the example of finite set as

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

2.2.2 Infinite Set

A set which contains infinite number of elements is known as infinite set. Consider the example of infinite set as

$$N = \{1, 2, 3, 4, ...\}$$
$$I = \{... -3, -2, -1, 0, 1, 2, 3, ...\}$$

2.2.3 Singleton Set

A set which contains only one element is known as a singleton set. Consider the example

$$S = \{9\}$$

2.2.4 Pair Set

A set which contains only two elements is known as a pair set. Consider the examples

$$S = \{e, f\}$$
$$S = \{\{a\}, \{1, 3, 5\}\}$$

2.2.5 Empty Set

A set which contains no element is known as empty set. The empty set is also known as void set or null set. Generally denoted by ϕ. Consider the examples

(*i*) $\phi = \{x : x \neq x\}$

(*ii*) $\phi = \{x : x$ is a month of the year containing 368 days$\}$

2.2.6 Set of Sets

A set which contains sets is known as set of sets. Consider the example

$$A = \{\{a, b\}, \{1\}, \{1, 2, 3, 4\}, \{u, v\}, \{\text{Book, Pen}\}\}$$

2.2.7 Universal Set

A set which is superset of all the sets under consideration or particular discussion is known as universal set. Generally denoted by U or E or Ω.

Generally, the universal set can be chosen arbitrarily for discussion, but once chosen it is fixed for discussion. Consider the example

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

$B = \{a, e, i, o, u\}$

$C = \{p, q, r, s\}$

So, we can take the universal set U as $\{a, b, c, \ldots., z\}$

i.e. $U = \{a, b, c, d, e, \ldots., z\}$

■ 2.3 CARDINALITY OF A SET

If S be a set, then the number of elements present in the set S is known as cardinality of S and is denoted by $|S|$. Mathematically if $S = \{s_1, s_2, s_3, \ldots.., s_k\}$, then $|S| = k; k \in N$.

Consider the example

Let $A = \{2, 4, 8, 16, 32, 64, 128, 256\}$

So, $|A| = 8$

2.3.1 Equivalent Sets

Two sets A and B are said to be equivalent if they contains equal number of elements. In other words A and B are said to be equivalent if they have same cardinality, *i.e.* $|A| = |B|$. The equivalent sets are also known as similar sets and denoted by $A \approx B$.

Consider the example of two sets.

$$A = \{a, e, i, o, u\}$$
$$B = \{7, 9, 11, 13, 15\}$$

Here, $|A| = 5 = |B|$. Thus A and B are similar.

■ 2.4 SUBSET AND SUPERSET

Set A is said to be a subset of B or set B is said to be the superset of A if each element of A is also an element of the set B. We write $A \subseteq B$.

i.e. $A \subseteq B \leftrightarrow \{x \in A \rightarrow x \in B; \forall\, x \in A\}$

Consider the examples

(*i*) Let $A = \{1, 2, 3, 4, 5, 6\}$
$B = \{1, 2, 3, 4, 5, 6, 7, 8\}$
So $A \subseteq B$.

(ii) Let $A = \{a, b, c\}$
$B = \{b, c, a\}$
so, $A \subseteq B$ and $B \subseteq A$.

(iii) Let $A = \{\ \}$ and $B = \{1, 2, 3\}$
So, $A \subseteq B$.

2.4.1 Equal Sets

Two sets A and B are said to be equal if and only if every element of A is in B and every element of B is in A. *i.e.* $A \subseteq B$ and. $B \subseteq A$. Mathematically

$$A = B \leftrightarrow \{\ A \subseteq B \text{ and } B \subseteq A\}$$

i.e. $$A = B \leftrightarrow \{\ x \in A \leftrightarrow x \in B\}$$

Consider the example: Let $A = \{x, y, z, p, q, r\}$

$$B = \{p, q, r, x, y, z\}$$

So, $B \subseteq A$ and $A \subseteq B$. Thus $A = B$.

2.4.2 Proper Subset

Set A is said to be a proper subset of B if each element of A is also an element of B and set B has at least one element which is not an element of set A. We write $A \subset B$.

Mathematically

$$A \subset B \leftrightarrow \{x \in A \rightarrow x \in B \text{ and for at least one } y \in B \rightarrow y \notin A\}.$$

Consider an example

Let $$A = \{a, b, c, d\}$$
$$B = \{a, b, c, d, e, f, g\}$$

Here for $x \in A$ we have $x \in B$ and $y = e \in B$ such that $y = e \notin A$. Thus $A \subset B$.

Note

1. Every set is a subset of itself. *i.e.* $A \subseteq A$.
2. Empty set is a subset of every set. *i.e.* $\phi \subseteq A$.

2.5 COMPARABILITY OF SETS

Two sets A and B are said to be comparable if any one of the following relation holds.

i.e. (*i*) $A \subset B$ or (*ii*) $B \subset A$ or (*iii*) $A = B$.

Consider the following sets

$$A = \{a, b, c, d, e\};\ B = \{2, 3, 5\} \text{ and } C = \{c, d, e\}.$$

It is clear that $A \not\subset B$, $B \not\subset A$ and $A \neq B$. So, A and B are not comparable.

Similarly $B \not\subset C$, $C \not\subset B$ or $C \neq B$. So, B and C are also not comparable. Where as $C \subset A$, thus A and C are comparable.

2.6 POWER SET

If A be a set, then the set of all subsets of A is known as power set of A. Which is denoted by P(A).

Mathematically, $P(A) = \{X : X \subseteq A\}$

Consider the example

Let $A = \{a\}$

$\Rightarrow$ $P(A) = \{\Phi, \{a\}\}$

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

$\Rightarrow$ $P(A) = \{\{a\}, \{b\}, \{a, b\}, \Phi\}$

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

$\Rightarrow$ $P(A) = \{\{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{c, a\}, \{a, b, c\}, \Phi\}$

From the above examples it is clear that if a set A contains n elements then the power set of A *i.e.* P(A) contains 2^n elements.

i.e. $|A| = n \Rightarrow |P(A)|\ 2^n.$

2.7 OPERATIONS ON SETS

Here we will discuss certain operations such as union, intersection and difference in order to develop an algebra of sets.

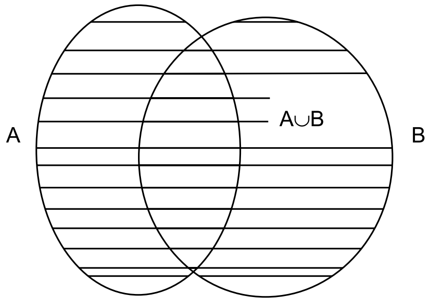
2.7.1 Union

If A and B be two sets, then the union $(A \cup B)$ is defined as a set of all those elements which are either in A or in B or in both.

Symbolically,

$$A \cup B = \{x : x \in A \text{ or } x \in B\}$$

Venn diagram



Consider the example

Let $A = \{a, b, c, d, e\}$

$B = \{a, e, i, o, u\}$

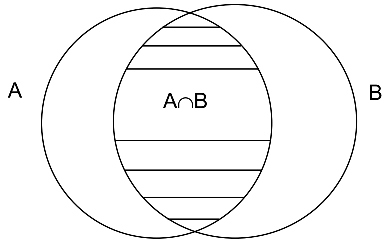
Therefore, $(A \cup B) = \{a, b, c, d, e, i, o, u\}$

2.7.2 Intersection

If A and B be two sets, then the intersection (A ∩ B) is defined as a set of all those elements which are common to both the sets. Symbolically

$$(A \cap B) = \{x : x \in A \text{ and } x \in B\}$$

Venn diagram



Consider the example

Let $A = \{a, b, c, d, e\}$

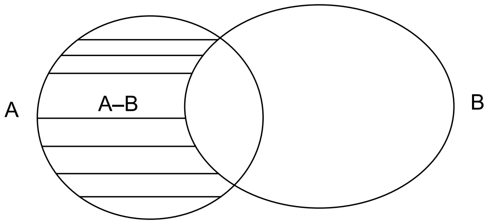
$B = \{a, e, i, o, u\}$

Therefore $(A \cap B) = \{a, e\}$

2.7.3 Difference

If A and B be two sets, then the difference (A – B) is defined as a set of all those elements of A which are not in B. Symbolically, $(A - B) = \{x \mid x \in A \text{ and } x \notin B\}$

Venn diagram



Consider the example

Let $A = \{a, b, c, d, e, f\}$

$B = \{a, c, i, o, u, k\}$

Therefore $(A - B) = \{b, d, e, f\}$

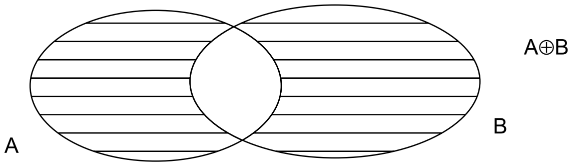
2.7.4 Symmetric Difference

If A and B be two sets, then the symmetric difference $(A \Delta B)$ or $(A \oplus B)$ is defined as a set of all those elements which are either in A or in B but not in both.

Symbolically,

$$(A \oplus B) = (A - B) \cup (B - A)$$

Venn diagram



Consider the example

Let $A = \{a, b, c, k, p, q, r, s\}$

$B = \{b, k, q, m, n, o, t\}$

So, $(A - B) = \{a, c, p, r, s\}$

and $(B - A) = \{m, n, o, t\}$

Therefore, $(A \oplus B) = (A - B) \cup (B - A)$

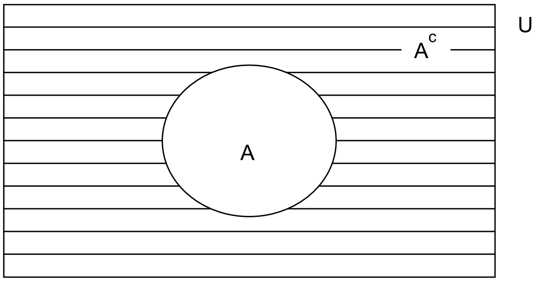
$= \{a, c, p, r, s, m, n, o, t\}$

2.7.5 Complement of a Set

If A be a set, then the complement of A is given as A^c, A' or $\overline{A}$ and is defined as a set of all those elements of the universal set U which are not in A. Symbolically,

$$A^c = \{x \mid x \in U \text{ and } x \notin A\}$$

Venn diagram



Consider the example:

Let $A = \{b, c, k, d, i, p, q, r, s, t\}$

So, we can take the universal set $U = \{a, b, c, \ldots, x, y, z\}$.

Therefore $A^c = U - A$

$= \{a, e, f, g, h, j, l, m, n, o, u, v, w, x, y, z\}$

2.7.6 Theorem

Let A, B and C be subsets of the universal set U. Then the following important laws hold.

(*a*) Commutative laws:
$(A \cup B) = (B \cup A)$; $(A \cap B) = (B \cap A)$

(*b*) Associative laws:
$A \cup (B \cup C) = (A \cup B) \cup C$; $A \cap (B \cap C) = (A \cap B) \cap C$

(*c*) Idempotent laws:
$(A \cup A) = A$; $(A \cap A) = A$

(*d*) Identity laws:
$(A \cup \phi) = A$; $(A \cap U) = A$

(*e*) Bound laws:
$(A \cup U) = U$; $(A \cap \phi) = \phi$

(*f*) Absorption laws:
$A \cup (A \cap B) = A$; $A \cap (A \cup B) = A$

(*g*) Complement laws:
$(A \cup A^c) = U$; $(A \cap A^c) = \phi$

(*h*) Involution law:
$(A^c)^c = A$

(*i*) Distributive laws :
(*i*) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
(*ii*) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Proof : Proofs of (*a*), (*b*), (*c*), (*d*), (*e*), (*f*), (*g*) and (*h*) are immediate consequences of the definitions. We prove only the distributive laws.

(*i*) $x \in A \cup (B \cap C)$
$\Leftrightarrow$ $x \in A$ or $x \in (B \cap C)$
$\Leftrightarrow$ $x \in A$ or ($x \in B$ and $x \in C$)
$\Leftrightarrow$ ($x \in A$ or $x \in B$) and ($x \in A$ or $x \in C$)
$\Leftrightarrow$ $x \in (A \cup B)$ and $x \in (A \cup C)$
$\Leftrightarrow$ $x \in (A \cup B) \cap (A \cup C)$
So, $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

(*ii*) $x \in A \cap (B \cup C)$
$\Leftrightarrow$ $x \in A$ and $x \in (B \cup C)$
$\Leftrightarrow$ $x \in A$ and ($x \in B$ or $x \in C$)
$\Leftrightarrow$ ($x \in A$ and $x \in B$) or ($x \in A$ and $x \in C$)
$\Leftrightarrow$ $x \in (A \cap B)$ or $x \in (A \cap C)$
$\Leftrightarrow$ $x \in (A \cap B) \cup (A \cap C)$
So, $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

2.7.7 Theorem

Let A, B and C be subsets of the universal set U. Then the following properties hold.

(*a*) $(A \Delta A) = \phi$ (*b*) $(A \Delta B) = (B \Delta A)$

(*c*) $A \cap (B \Delta C) = (A \cap B) \Delta (A \cap C)$ (*d*) $(A \Delta B) = (A \cup B) - (A \cap B)$

Proof : Proofs of (*a*) and (*b*) are immediate consequences of definitions. Here we prove (*c*) and (*d*).

(*c*) $x \in A \cap (B \Delta C)$

$\Leftrightarrow$ $x \in A$ and $x \in (B \Delta C)$

$\Leftrightarrow$ $x \in A$ and $x \in ((B - C) \cup (C - B))$

$\Leftrightarrow$ $x \in A$ and $(x \in (B - C)$ or $x \in (C - B))$

$\Leftrightarrow$ $(x \in A$ and $x \in (B - C))$ or$(x \in A$ and $x \in (C - B))$

$\Leftrightarrow$ $(x \in A$ and $(x \in B$ and $x \notin C))$

or $(x \in A$ and $(x \in C$ and $x \notin B))$

$\Leftrightarrow$ $((x \in A$ and $x \in B)$ and $(x \in A$ and $x \notin C))$

or $((x \in A$ and $x \in C)$ and $(x \in A$ and $x \notin B))$

$\Leftrightarrow$ $(x \in (A \cap B)$ and $x \notin (A \cap C))$ or

$(x \in (A \cap C)$ and $x \notin (A \cap B))$

$\Leftrightarrow$ $x \in ((A \cap B) - (A \cap C))$ or $x \in ((A \cap C) - (A \cap B))$

$\Leftrightarrow$ $x \in ((A \cap B) - (A \cap C)) \cup ((A \cap C) - (A \cap B))$

$\Leftrightarrow$ $x \in (A \cap B) \Delta (A \cap C)$

So, $A \cap (B \Delta C) = (A \cap B) \Delta (A \cap C)$.

(d) $x \in (A \cup B) - (A \cap B)$

$\Leftrightarrow$ $x \in (A \cup B)$ and $x \notin (A \cap B)$

$\Leftrightarrow$ $x \in (A \cup B)$ and $(x \notin A$ or $x \notin B)$

$\Leftrightarrow$ $(x \in (A \cup B)$ and $x \notin A)$ or $(x \in (A \cup B)$ and $x \notin B)$

$\Leftrightarrow$ $((x \in A$ or $x \in B)$ and $x \notin A)$

or $((x \in A$ or $x \in B)$ and $x \notin B)$

$\Leftrightarrow$ $((x \in A$ and $x \notin A)$ or $(x \in B$ and $x \notin A))$

or $((x \in A$ and $x \notin B)$ or $(x \in B$ and $x \notin B))$

$\Leftrightarrow$ $(x \in \phi$ or $x \in (B - A))$ or $(x \in (A - B)$ or $x \in \phi)$

$\Leftrightarrow$ $x \in (\phi \cup (B - A))$ or $x \in ((A - B) \cup \phi)$

$\Leftrightarrow$ $x \in (B - A) \cup (A - B)$ [By Identity law]

$\Leftrightarrow$ $x \in (B \Delta A)$

$\Leftrightarrow$ $x \in (A \Delta B)$ [By Commutative law]

So, $(A \Delta B) = (A \cup B) - (A \cap B)$

2.7.8 De-Morgan's Law

Let A and B be subsets of the universal set U. Then

(*a*) $(A \cup B)^c = (A^c \cap B^c)$

(*b*) $(A \cap B)^c = (A^c \cup B^c)$

Proof: (*a*) $x \in (A \cup B)^c$

$\Leftrightarrow$ $x \notin (A \cup B)$

$\Leftrightarrow$ $x \notin A$ and $x \notin B$

$\Leftrightarrow$ $x \in A^c$ and $x \in B^c$

$\Leftrightarrow$ $x \in A^c \cap B^c$

So, $(A \cup B)^c = (A^c \cap B^c)$

(*b*) $x \in (A \cap B)^c$

$\Leftrightarrow$ $x \notin (A \cap B)$

$\Leftrightarrow$ $x \notin A$ or $x \notin B$

$\Leftrightarrow$ $x \in A^c$ or $x \in B^c$

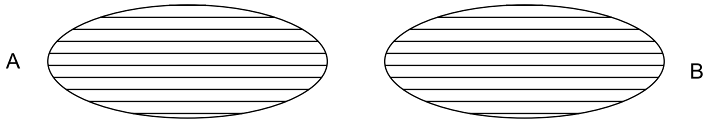
$\Leftrightarrow$ $x \in A^c \cup B^c$

So, $(A \cap B)^c = (A^c \cup B^c)$

■ 2.8 DISJOINT SETS

Two sets A and B are called disjoint or non-overlapping if both sets have no common element. Mathematically, $(A \cap B) = \phi$.

Venn diagram



■ 2.9 APPLICATION OF SET THEORY

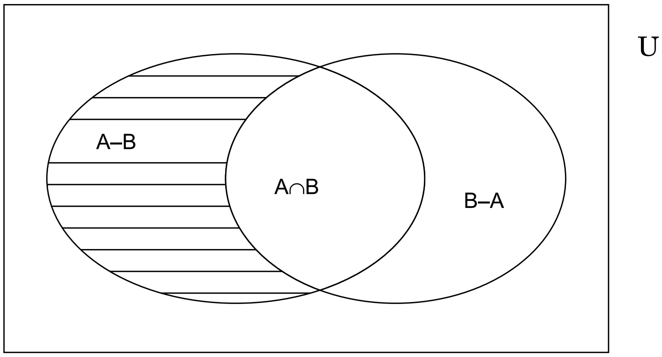
Let A and B be finite sets. Let $n(A)$ be the number of distinct elements of the set A. Then

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

Further if A and B are disjoint, then

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

Proof: A and B be finite sets and $n(A)$ represent the number of distinct elements of the set A.



From the above Venn diagram it is clear that

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

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

and $$\begin{aligned} n(A \cup B) &= n(A - B) + n(A \cap B) + n(B - A) \\ &= n(A) - n(A \cap B) + n(A \cap B) + n(B) - n(A \cap B) \\ &= n(A) + n(B) - n(A \cap B) \end{aligned}$$

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

If A and B are disjoint, then $(A \cap B) = \phi$ *i.e.* $n(A \cap B) = 0$

Therefore, $n(A \cup B) = n(A) + n(B)$.

■ 2.10 PRODUCT OF SETS

The product of sets is defined with the help of an order pair. An order pair is usually denoted by (x, y) such that $(x, y) \neq (y, x)$ whenever $x \neq y$. The product of two sets A and B is the set of all those order pairs whose first coordinate is an element of A and the second coordinate is an element of B. The set is denoted by $(A \times B)$. Mathematically,

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

Consider the example

Let $A = \{1, 2, 3, 5, 7\}$

$B = \{4, 9, 25\}$

So, $(A\times B) = \{(1,4), (1, 9), (1, 25), (2, 4), (2, 9), (2, 25), (3, 4), (3, 9), (3, 25), (5, 4), (5, 9), (5, 25), (7, 4), (7, 9), (7, 25)\}$

Note : The product of sets can be extendable for n sets $A_1, A_2, A_3, \ldots\ldots., A_n$. Thus $A_1 \times A_2 \times A_3 \times \ldots..\times A_n$ can be defined as

$A_1 \times A_2 \times A_3 \times \ldots..\times A_n = \{(x_1, x_2, x_3, \ldots., x_n) \mid x_1 \in A_1$ and $x_2 \in A_2$ and $x_3 \in A_3$ and ... and $x_n \in A_n\}$where $(x_1, x_2, x_3, \ldots., x_n)$ is called as n-tuple of $x_1, x_2, x_3, \ldots., x_n$. To explain this consider the example in which $A = \{a, b, c\}$; $B = \{1, 2\}$ and $C = \{\alpha, \beta\}$. Therefore

$A \times B \times C = \{(a, 1, \alpha), (a, 1, \beta), (a, 2, \alpha), (a, 2, \beta), (b, 1, \alpha), (b, 1, \beta), (b, 2, \alpha), (b, 2, \beta), (c, 1, \alpha), (c, 1, \beta), (c, 2, \alpha), (c, 2, \beta)\}$.

From the above example it is very clear that $|A \times B \times C| = |A| \times |B| \times |C|$. In general, $|A_1 \times A_2 \times A_3 \times \ldots..\times A_n| = |A_1| \times |A_2| \times |A_3| \times \ldots \times |A_n|$.

2.10.1 Theorem

Let A, B and C be three subsets of the universal set U. Then

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

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

Proof: (*a*) $(x, y) \in A \times (B \cup C)$

$\Leftrightarrow \quad x \in A$ and $y \in (B \cup C)$

$\Leftrightarrow \quad x \in A$ and $(y \in B$ or $y \in C)$

$\Leftrightarrow \quad (x \in A$ and $y \in B)$ or $(x \in A$ and $y \in C)$

$\Leftrightarrow (x, y) \in (A \times B)$ or $(x, y) \in (A \times C)$

$\Leftrightarrow (x, y) \in (A \times B) \cup (A \times C)$

Therefore, $A \times (B \cup C) = (A \times B) \cup (A \times C)$.

(*b*) $(x, y) \in A \times (B \cap C)$

$\Leftrightarrow \quad x \in A$ and $y \in (B \cap C)$

$\Leftrightarrow \quad x \in A$ and $(y \in B$ and $y \in C)$

$\Leftrightarrow \quad (x \in A$ and $y \in B)$ and $(x \in A$ and $y \in C)$

$\Leftrightarrow (x, y) \in (A \times B)$ and $(x, y) \in (A \times C)$

$\Leftrightarrow (x, y) \in (A \times B) \cap (A \times C)$

Therefore $A \times (B \cap C) = (A \times B) \cap (A \times C)$.

■ 2.11 FUNDAMENTAL PRODUCTS

Let $A_1, A_2, A_3, \ldots., A_n$ be n sets. A fundamental product of these n sets is an expression of the form $(B_1 \cap B_2 \cap B_3 \cap \ldots \cap B_n)$ where B_i is either A_i or A_i^c.

Consider an example with three sets A, B and C. The fundamental products of these three sets are as follows which are 2^3 in number.

i.e. $A \cap B \cap C$; $A^c \cap B \cap C$; $A \cap B^c \cap C$; $A \cap B \cap C^c$;
$A^c \cap B^c \cap C$; $A \cap B^c \cap C^c$; $A^c \cap B \cap C^c$; $A^c \cap B^c \cap C^c$.

SOLVED EXAMPLE

Example 1 *Let A, B and C be any three subsets of the universal set U. Then prove that*

(a) $A-(B \cup C) = (A-B) \cap (A-C)$
(b) $A-(B \cup C) = (A-B) - C$
(c) $(A \cap B) - C = A \cap (B - C)$

Solution: (*a*) $x \in A - (B \cup C)$

$\Leftrightarrow$ $x \in A$ and $x \notin (B \cup C)$
$\Leftrightarrow$ $x \in A$ and $(x \notin B$ and $x \notin C)$
$\Leftrightarrow$ $(x \in A$ and $x \notin B)$ and $(x \in A$ and $x \notin C)$
$\Leftrightarrow$ $x \in (A - B)$ and $x \in (A - C)$
$\Leftrightarrow$ $x \in (A - B) \cap (A - C)$

Therefore $A - (B \cup C) = (A - B) \cap (A - C)$

(*b*) $x \in A - (B \cup C)$

$\Leftrightarrow$ $x \in A$ and $x \notin (B \cup C)$
$\Leftrightarrow$ $x \in A$ and $(x \notin B$ and $x \notin C)$
$\Leftrightarrow$ $(x \in A$ and $x \notin B)$ and $x \notin C$
$\Leftrightarrow$ $x \in (A - B)$ and $x \notin C$
$\Leftrightarrow$ $x \in (A - B) - C$

Therefore $A - (B \cup C) = (A - B) - C$

(*c*) $x \in (A \cap B) - C$

$\Leftrightarrow$ $(x \in A$ and $x \in B)$ and $x \notin C$
$\Leftrightarrow$ $x \in A$ and $(x \in B$ and $x \notin C)$
$\Leftrightarrow$ $x \in A$ and $x \in (B - C)$
$\Leftrightarrow$ $x \in A \cap (B - C)$

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

Example 2 *Show that* $A - \bigcup_{i=1}^{n} B_i = \bigcap_{i=1}^{n} (A - B_i)$

Solution : $x \in A - \bigcup_{i=1}^{n} B_i$

$\Leftrightarrow$ $x \in A$ and $x \notin \bigcup_{i=1}^{n} B_i$
$\Leftrightarrow$ $x \in A$ and $x \notin (B_1 \cup B_2 \cup B_3 \cup \ldots \cup B_n)$
$\Leftrightarrow$ $x \in A$ and $(x \notin B_1$ and $x \notin B_2$ and $x \notin B_3$ and … and $x \notin B_n)$

$\Leftrightarrow \quad (x \in \text{A and } x \notin \text{B}_1) \text{ and } (x \in \text{A and } x \notin \text{B}_2) \text{ and .... and } (x \in \text{A and } x \notin \text{B}_n)$

$\Leftrightarrow \quad x \in (\text{A} - \text{B}_1) \text{ and } x \in (\text{A} - \text{B}_2) \text{ and ... and } x \in (\text{A} - \text{B}_n)$

$\Leftrightarrow \quad x \in (\text{A} - \text{B}_1) \cap (\text{A} - \text{B}_2) \cap \ldots \cap x \in (\text{A} - \text{B}_n)$

$$\Leftrightarrow \quad x \in \bigcap_{i=1}^{n} (\text{A} - \text{B}_i)$$

Therefore $\text{A} - \bigcup_{i=1}^{n} \text{B}_i = \bigcap_{i=1}^{n} (\text{A} - \text{B}_i)$

Example 3 *If A and B subsets of the universal set U, then show that*

(a) $(A^c)^c = A$

(b) $A - B = A \cap B^c$

(c) $(A - B) \cap B = \phi$

Solution : (*a*) $x \in (\text{A}^c)^c$

$\Leftrightarrow \quad x \notin \text{A}^c$

$\Leftrightarrow \quad x \in \text{A}$

So, $(\text{A}^c)^c = \text{A}$

(*b*) $x \in (\text{A} - \text{B})$

$\Leftrightarrow \quad x \in \text{A and } x \notin \text{B}$

$\Leftrightarrow \quad x \in \text{A and } x \in \text{B}^c$

$\Leftrightarrow \quad x \in (\text{A} \cap \text{B}^c)$

So, $(\text{A} - \text{B}) = (\text{A} \cap \text{B}^c)$

(*c*) $x \in (\text{A} - \text{B}) \cap \text{B}$

$\Leftrightarrow \quad x \in (\text{A} - \text{B}) \text{ and } x \in \text{B}$

$\Leftrightarrow \quad (x \in \text{A and } x \notin \text{B}) \text{ and } x \in \text{B}$

$\Leftrightarrow \quad x \in \text{A and } (x \notin \text{B and } x \in \text{B})$

$\Leftrightarrow \quad x \in \text{A and } x \in \phi$

$\Leftrightarrow \quad x \in (\text{A} \cap \phi)$

$\Leftrightarrow \quad x \in \phi$

So, $(\text{A} - \text{B}) \cap \text{B} = \phi$

Example 4 *Let A, B be the subsets of the universal set U, then prove that*

(a) $A - (A \cap B) = A \cap B^c$

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

Solution : (*a*) $x \in \text{A} - (\text{A} \cap \text{B})$

$\Leftrightarrow \quad x \in \text{A and } x \notin (\text{A} \cap \text{B})$

$\Leftrightarrow \quad x \in \text{A and } (x \notin \text{A or } x \notin \text{B})$

$\Leftrightarrow \quad (x \in \text{A and } x \notin \text{A}) \text{ or } (x \in \text{A and } x \notin \text{B})$

$\Leftrightarrow \quad x \in \phi \text{ or } (x \in \text{A and } x \in \text{B}^c)$

$\Leftrightarrow \quad x \in \phi \text{ or } x \in (\text{A} \cap \text{B}^c)$

$\Leftrightarrow \quad x \in \phi \cup (\text{A} \cap \text{B}^c)$

$\Leftrightarrow \quad x \in (\text{A} \cap \text{B}^c)$

So, $\text{A} - (\text{A} \cap \text{B}) = \text{A} \cap \text{B}^c$

(*b*) $x \in (A \cap B^c)^c$

$\Leftrightarrow$ $x \notin (A \cap B^c)$

$\Leftrightarrow$ $x \notin A$ or $x \notin B^c$

$\Leftrightarrow$ $x \in A^c$ or $x \in B$

$\Leftrightarrow$ $x \in (A^c \cup B)$

So, $(A \cap B^c)^c = (A^c \cup B)$

Example 5 *Let A, B and C be three subsets of the universal set U. Then show that*

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

Solution : Let $(B \cup C) = D$. So, we have

$$\begin{aligned} n(A \cup B \cup C) &= n(A \cup D) \\ &= n(A) + n(D) - n(A \cap D) \\ &= n(A) + n(B \cup C) - n(A \cap (B \cup C)) \\ &= n(A) + n(B) + n(C) - n(B \cap C) - n((A \cap B) \cup (A \cap C)) \\ &= n(A) + n(B) + n(C) - n(B \cap C) - n(A \cap B) - n(A \cap C) + n(A \cap B \cap C) \end{aligned}$$

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

Example 6 *In the CSI conference held at Delhi, 500 delegates attended. 200 of them could take tea, 350 could take coffee and 10 did not take either coffee or tea. Then answer the following questions.*

(a) How many can take both tea and coffee.
(b) How many can take tea only and
(c) How many can take coffee only.

Solution : Let T : Set of persons who take tea.
C : Set of persons who take coffee.
U : Total number of delegates.

Hence we have $n(U) = 500$; $n(T) = 200$; $n(C) = 350$

Number of delegates did not take either coffee or tea = 10

Therefore number of delegates who take either coffee or tea = 500 –10 = 490

i.e. $n(T \cup C) = 490$

i.e. $n(T) + n(C) - n(T \cap C) = 490$

i.e. $n(T \cap C) = n(T) + n(C) - 490 = 200 + 350 - 490 = 60$

So, the number of persons who take both coffee and tea = $n(T \cap C) = 60$

Number of persons take tea only = $n(T) - n(T \cap C) = 140$

Number of persons take coffee only = $n(C) - n(T \cap C) = 290$.

Example 7 *If 65% of students like apples where 75% like grapes then what percentage of students likes both apples and grapes?*

Solution : Let $n(S)$: Total number of students = 100
$n(A)$: Total number of students who like apples = 65
$n(B)$: Total number of students who like grapes = 75

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

i.e. $100 = 65 + 75 - n(A \cap B)$

i.e. $n(A \cap B) = 40$

So, 40% of students like both apples and grapes.

Example 8 *If $A = \{2, 3, 4, 5, 6\}$, $B = \{3, 4, 5, 6, 7\}$ and $C = \{4, 5, 6, 7, 8\}$ then find the followings.*

(i) $(A \cup B) \cap (A \cup C)$ *(ii)* $(A \cap B) \cup (A \cap C)$

(iii) $A - (B - C)$ *and* *(iv)* $(A \Delta B)$.

Solution : Given $A = \{2, 3, 4, 5, 6\}$, $B = \{3, 4, 5, 6, 7\}$ and $C = \{4, 5, 6, 7, 8\}$

(*i*) $(A \cup B) = \{2, 3, 4, 5, 6, 7\}$

$(A \cup C) = \{2, 3, 4, 5, 6, 7, 8\}$

Therefore $(A \cup B) \cap (A \cup C) = \{2, 3, 4, 5, 6, 7\}$

(*ii*) $(A \cap B) = \{3, 4, 5, 6\}$

$(A \cap C) = \{4, 5, 6\}$

Therefore $(A \cap B) \cup (A \cap C) = \{3, 4, 5, 6\}$

(*iii*) $(B - C) = \{3\}$

Therefore $A - (B - C) = \{2, 4, 5, 6\}$

(*iv*) $(A \cup B) = \{2, 3, 4, 5, 6, 7\}$

$(A \cap B) = \{3, 4, 5, 6\}$

Therefore $(A \Delta B) = (A \cup B) - (A \cap B) = \{2, 7\}$

Example 9 *Find the power sets of the following sets.*

(i) $\{0\}$

(ii) $\{1, \{1, 2\}\}$ *and*

(iii) $\{4, 1, 8\}$.

Solution : (*i*) Let $A = \{0\}$

Therefore $P(A) = \{\{0\}, \phi\}$

(*ii*) Let $A = \{1, \{1, 2\}\}$

So, $P(A) = \{\{1\}, \{\{1, 2\}\}, A, \phi\}$

(*iii*) Let $A = \{4, 1, 8\}$

So, $P(A) = \{\{4\}, \{1\}, \{8\}, \{4, 1\}, \{4, 8\}, \{1, 8\}, A, \phi\}$.

Example 10 *If $A = \{4, 5\}$, $B = \{7, 8\}$ and $C = \{9, 10\}$ then find the followings.*

(a) $(A \times B) \cup (B \times C)$ *and (b)* $A \times (B \cup C)$.

Solution : Given $A = \{4, 5\}$, $B = \{7, 8\}$ and $C = \{9, 10\}$

(*a*) $(A \times B) = \{(4, 7), (4, 8), (5, 7), (5,8)\}$

$(B \times C) = \{(7, 9), (7, 10), (8, 9), (8, 10)\}$

So, $(A \times B) \cup (B \times C) =\{(4, 7), (4, 8), (5, 7), (5,8), (7, 9), (7, 10), (8, 9), (8, 10)\}$

(*b*) $(B \cup C) = \{7, 8, 9, 10\}$

So, $A \times (B \cup C) = \{(4, 7), (4, 8), (4, 9), (4,10), (5,7), (5, 8), (5, 9), (5, 10)\}$.

Example 11 *If $A = \{1, 2, 3\}$, $B = \{2, 3, 4\}$ and $C = \{3, 4, 5\}$, then verify the product laws.*

Solution : Given $A = \{1, 2, 3\}$, $B = \{2, 3, 4\}$ and $C = \{3, 4, 5\}$

Therefore $(B \cup C) = \{2, 3, 4, 5\}$ and

$A \times (B \cup C) = \{(1, 2), (1, 3), (1, 4), (1, 5), (2, 2), (2, 3), (2, 4), (2, 5), (3, 2), (3, 3), (3, 4), (3, 5)\}$

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

$(A \times C) = \{(1, 3), (1, 4), (1, 5), (2, 3), (2, 4), (2, 5), (3, 3), (3, 4), (3, 5)\}$

Thus $(A \times B) \cup (A \times C) = \{(1, 2), (1, 3), (1, 4), (1, 5), (2, 2), (2, 3), (2, 4), (2, 5), (3, 2), (3, 3), (3, 4), (3, 5)\}$

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

Similarly the second product law $A \times (B \cap C) = (A \times B) \cap (A \times C)$ can be verified.

Example 12 *If P = {a, c, e}, Q ={100, 101, 102} and R = {m, c, e, 101} Compute ((Q ∪P) – (P ∩Q)) ×R. Where ∩, ∪, – and ×are well known set theoretic binary operations.*

Solution : Given $P = \{a, c, e\}$; $Q = \{100, 101, 102\}$ and $R = \{m, c, e, 101\}$.

So, $(Q \cup P) = \{100, 101, 102, a, c, e\}$ and $(P \cap Q) = \phi$

Therefore $((Q \cup P) - (P \cap Q)) = \{100, 101, 102, a, c, e\}$

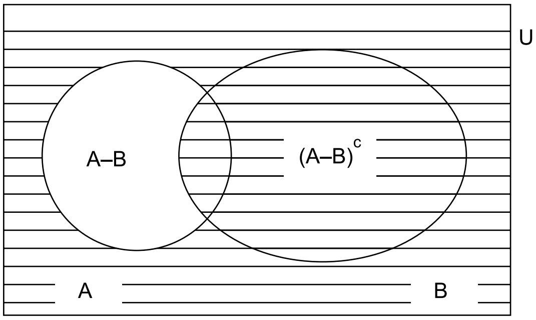
Thus $((Q \cup P) - (P \cap Q)) \times R = \{(100, m), (100, c), (100, e), (100, 101), (101, m), (101, c), (101, e), (101, 101), (102, m), (102, c), (102, e), (102, 101), (a, m), (a, c), (a, e), (a, 101), (c, m), (c, c), (c, e), (c, 101), (e, m), (e, c), (e, e), (e, 101)\}$

Example 13 *Show the following sets by Venn diagram.*

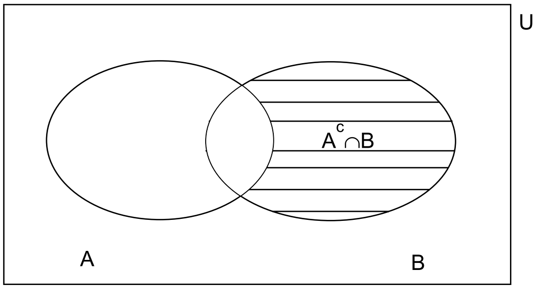
(a) $(A - B)^c$ *(b)* $A^c \cap B$ *(c)* $A \cap B \cap C$

Solution :

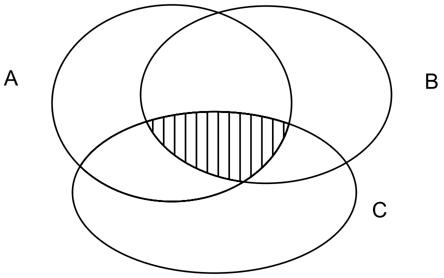
(*a*)



(*b*) $(A^c - B) = (B - A)$



(*c*) $A \cap B \cap C$



Example 14 *In a group of 64 students 26 can speak Hindi only, 14 can speak English only. How many can speak both Hindi and English.*

Solution : Let H : Set of students who can speak Hindi.

E : Set of students who can speak English.

Let n(S) : Total number of students = 64

i.e. $n(S) = n(H \cup E) = 64$

Given $n(H - E)$: Number of students speak Hindi only = 26

and $n(E - H)$: Number of students speak English only = 14

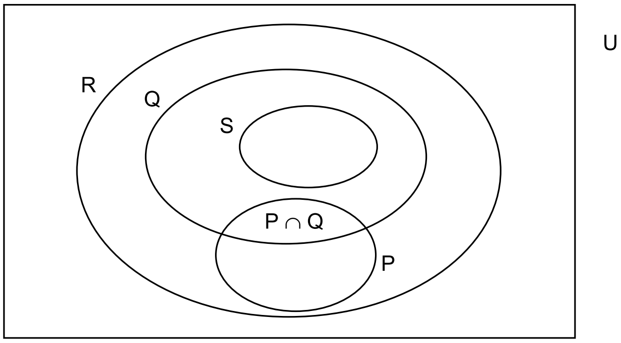
Therefore $n(H \cup E) = n(H - E) + n(E - H) + n(H \cap E)$

i.e. $n(H \cap E) = 64 - 26 - 14 = 24$

So, 24 students can speak both Hindi and English.

Example 15 *Draw a Venn diagram to represent the following facts for the sets P, Q, R and S. $(P \cap Q) \neq \phi$, $S \subseteq Q \subseteq R$ and $(P \cap S) = \phi$.*

Solution : Given conditions are $(P \cap Q) \neq \phi$, $S \subseteq Q \subseteq R$ and $(P \cap S) = \phi$. The Venn diagram for the above facts is given below.



Example 16 *If in a city 60% of the residents can speak Bengali and 50% can speak Kannada, What percentage of residents can speak both the languages, if 20% residents can not speak any of these two languages?*

Solution : Let n(S) : Total number of residents = 100

n(B) : Total number of residents who speak Bengali = 60

n(K) : Total number of residents who speak Kannada = 50

$n(B \cup K)^c$: Total number of residents who cannot speak any of these two languages = 20

So, $n(B \cup K) = n(S) - n(B \cup K)^c = 100 - 20 = 80$

i.e. $n(B) + n(K) - n(B \cap K) = 80$

i.e. $n(B \cap K) = 60 + 50 - 80 = 30$

Therefore 30% of the residents can speak both the languages Bengali and Kannada.

Example 17 *In a survey about liking for colours, it was found that everyone who was surveyed had a liking for at least one of the three colours namely Red, Green and Blue. Further 30% liked Red; 40% liked Green and 50% liked Blue. Further 10% people liked both Red and Green, 5% liked both Green and Blue and 10% liked both Red and Blue. Find the percentage of the surveyed people who like all the colours.*

Solution : Let R : Set of people who like Red colour

G : Set of people who like Green colour

B : Set of people who like Blue colour

and S : Set of all people who was surveyed.

Therefore $n(\mathrm{S}) = 100$; $n(\mathrm{R}) = 30; n(\mathrm{G}) = 40; n(\mathrm{B}) = 50; n(\mathrm{R} \cap \mathrm{G}) = 10; n(\mathrm{G} \cap \mathrm{B}) = 5; n(\mathrm{R} \cap \mathrm{B}) = 10.$

Thus $\quad n(\mathrm{S}) = n(\mathrm{R} \cup \mathrm{G} \cup \mathrm{B}) = 100$

i.e. $\quad n(\mathrm{R}) + n(\mathrm{G}) + n(\mathrm{B}) - n(\mathrm{R} \cap \mathrm{G}) - n(\mathrm{G} \cap \mathrm{B}) - n(\mathrm{R} \cap \mathrm{B}) + n(\mathrm{R} \cap \mathrm{G} \cap \mathrm{B})$
$= 100$

i.e. $\quad n(\mathrm{R} \cap \mathrm{G} \cap \mathrm{B}) = 100 - 30 - 40 - 50 + 10 + 5 + 10 = 5$

So, 5% of the surveyed people like all the colours, i.e. Red, Green and Blue.

Example 18 *If $A \subset B$ and $B \subset C$, then show that $A \subset C$.*

Solution : Given $\mathrm{B} \subset \mathrm{C}$ *i.e.* $x \in \mathrm{B} \Rightarrow x \in \mathrm{C}$

Again $\mathrm{A} \subset \mathrm{B}$ *i.e.* $x \in \mathrm{A} \Rightarrow x \in \mathrm{B} \qquad \forall x \in \mathrm{A}$

i.e. $\quad x \in \mathrm{A} \Rightarrow x \in \mathrm{B} \Rightarrow x \in \mathrm{C}$

i.e. $\quad x \in \mathrm{A} \Rightarrow x \in \mathrm{C}$

Therefore $\mathrm{A} \subset \mathrm{C}$.

Example 19 *For all sets A and B prove that $\overline{A \times B} = \overline{A} \times \overline{B}$.*

Solution : $\quad (x, y) \in \overline{\mathrm{A} \times \mathrm{B}}$

$\Leftrightarrow \quad (x, y) \notin \mathrm{A} \times \mathrm{B}$

$\Leftrightarrow \quad x \notin \mathrm{A}$ and $y \notin \mathrm{B}$

$\Leftrightarrow \quad x \in \overline{\mathrm{A}}$ and $y \in \overline{\mathrm{B}}$

$\Leftrightarrow \quad (x, y) \in \overline{\mathrm{A}} \times \overline{\mathrm{B}}$

So, $\quad (x, y) \in \overline{\mathrm{A} \times \mathrm{B}} \Leftrightarrow (x, y) \in \overline{\mathrm{A}} \times \overline{\mathrm{B}}$

Therefore $\quad \overline{\mathrm{A} \times \mathrm{B}} = \overline{\mathrm{A}} \times \overline{\mathrm{B}}$

Example 20 *For all sets A, B and C prove that $A \times (B - C) = (A \times B) - (A \times C)$.*

Solution : $(x, y) \in \mathrm{A} \times (\mathrm{B} - \mathrm{C})$

$\Leftrightarrow \quad x \in \mathrm{A}$ and $y \in (\mathrm{B} - \mathrm{C})$

$\Leftrightarrow \quad x \in \mathrm{A}$ and ($y \in \mathrm{B}$ and $y \notin \mathrm{C}$)

$\Leftrightarrow \quad$ ($x \in \mathrm{A}$ and $y \in \mathrm{B}$) and ($x \in \mathrm{A}$ and $y \notin \mathrm{C}$)

$\Leftrightarrow \quad (x, y) \in (\mathrm{A} \times \mathrm{B})$ and $(x, y) \notin (\mathrm{A} \times \mathrm{C})$

$\Leftrightarrow \quad (x, y) \in (\mathrm{A} \times \mathrm{B}) - (\mathrm{A} \times \mathrm{C})$

Therefore $\mathrm{A} \times (\mathrm{B} - \mathrm{C}) = (\mathrm{A} \times \mathrm{B}) - (\mathrm{A} \times \mathrm{C})$.

Example 21 *In a group of 191 students, 10 are taking English, Computer Science and Music; 36 are taking English and Computer Science; 20 are taking English and Music; 18 are taking Computer Science and Music; 65 are taking English; 76 are taking Computer Science and 63 are taking Music. Then answer the followings*

(a) How many are taking English and Music but not Computer Science.
(b) How many are taking Computer Science and Music but not English.
(c) How many are taking Computer Science and neither English nor Music.
(d) How many are taking none of the three subjects.

Solution : Let S : Set of students
E : Set of students taking English
C : Set of students taking Computer Science
M : Set of students taking Music.

Given that $n(\mathrm{S}) = 191; n(\mathrm{E}) = 65; n(\mathrm{C}) = 76; n(\mathrm{M}) = 63; n(\mathrm{E} \cap \mathrm{C} \cap \mathrm{M}) = 10; n(\mathrm{E} \cap \mathrm{C}) = 36;$ $n(\mathrm{E} \cap \mathrm{M}) = 20; n(\mathrm{C} \cap \mathrm{M}) = 18$

(*a*) Number of students taking English and Music but not Computer Science

$$= n(\mathrm{E} \cap \mathrm{M}) - n(\mathrm{E} \cap \mathrm{C} \cap \mathrm{M}) = 20 - 10 = 10$$

(*b*) Number of students taking Computer Science and Music but not English

$$= n(\mathrm{C} \cap \mathrm{M}) - n(\mathrm{E} \cap \mathrm{C} \cap \mathrm{M}) = 18 - 10 = 8$$

(*c*) Number of students taking Computer Science and neither English nor Music = $n(\mathrm{C}) - n(\mathrm{E} \cap \mathrm{C}) - n(\mathrm{C} \cap \mathrm{M}) + n(\mathrm{E} \cap \mathrm{C} \cap \mathrm{M}) = 76 - 36 - 18 + 10 = 32$

(*d*) Number of students taking none of the three subjects

$$\begin{aligned}
&= n(\mathrm{E} \cup \mathrm{C} \cup \mathrm{M})^c \\
&= n(\mathrm{S}) - n(\mathrm{E} \cup \mathrm{C} \cup \mathrm{M}) \\
&= n(\mathrm{S}) - \{n(\mathrm{E}) + n(\mathrm{C}) + n(\mathrm{M}) - n(\mathrm{E} \cap \mathrm{C}) - n(\mathrm{C} \cap \mathrm{M}) - n(\mathrm{E} \cap \mathrm{M}) + n(\mathrm{E} \cap \mathrm{C} \cap \mathrm{M})\} \\
&= 191 - (65 + 63 + 76 - 20 - 36 - 18 + 10) \\
&= 51.
\end{aligned}$$

Example 22 *Examine whether the following sets are equivalent or not.*

(a) $A = \{ x \mid x^2 - 7x + 12 = 0; x \in N\}$ *(b)* $B = \{x \mid x = a \text{ and } x = b\}$

(c) $C = \{a, b, c, d, e\}$ *(d)* $D = \{x \mid x^2 - 4 = 0; x \in I\}$

Solution : Given that $\mathrm{A} = \{x \mid x^2 - 7x + 12 = 0; x \in \mathrm{N}\}$

Therefore $\mathrm{A} = \{3, 4\}$

i.e. $|\mathrm{A}| = 2$

Similarly $\mathrm{B} = \{x \mid x = a \text{ and } x = b\}$

$= \{a, b\}$

i.e. $|\mathrm{B}| = 2$

Also $\mathrm{C} = \{a, b, c, d, e\}$

i.e. $|\mathrm{C}| = 5$

Again $\mathrm{D} = \{x \mid x^2 - 4 = 0; x \in \mathrm{I}\} = \{2, -2\}$

i.e. $|\mathrm{D}| = 2$

Therefore $|\mathrm{A}| = |\mathrm{B}| = |\mathrm{D}| = 2 \neq |\mathrm{C}| = 5$; So A, B and D are equivalent.

Example 23 *For all Sets A and B prove that* $(A \cap B) \cup (B - A) = B$.

Solution :

$$\begin{aligned}
(\mathrm{A} \cap \mathrm{B}) \cup (\mathrm{B} - \mathrm{A}) &= (\mathrm{A} \cap \mathrm{B}) \cup (\mathrm{B} \cap \mathrm{A}^c) \\
&= ((\mathrm{A} \cap \mathrm{B}) \cup \mathrm{B}) \cap ((\mathrm{A} \cap \mathrm{B}) \cup \mathrm{A}^c) && \text{[Distributive law]} \\
&= \mathrm{B} \cap ((\mathrm{A} \cap \mathrm{B}) \cup \mathrm{A}^c) && \text{[Absorption law]} \\
&= \mathrm{B} \cap ((\mathrm{A} \cup \mathrm{A}^c) \cap (\mathrm{B} \cup \mathrm{A}^c)) && \text{[Distributive law]} \\
&= \mathrm{B} \cap (\mathrm{U} \cap (\mathrm{B} \cup \mathrm{A}^c)) && \text{[Complement law]} \\
&= \mathrm{B} \cap (\mathrm{B} \cup \mathrm{A}^c) \\
&= \mathrm{B} && \text{[Absorption law]}
\end{aligned}$$

Example 24 *By applying properties of sets prove that* $(A - B) \cap (B - A) = \phi$ *for all sets A and B.*

Solution :

$$\begin{aligned}
(\mathrm{A} - \mathrm{B}) \cap (\mathrm{B} - \mathrm{A}) &= (\mathrm{A} \cap \mathrm{B}^c) \cap (\mathrm{B} \cap \mathrm{A}^c) \\
&= \mathrm{A} \cap (\mathrm{B}^c \cap (\mathrm{B} \cap \mathrm{A}^c)) && \text{[Associative law]} \\
&= \mathrm{A} \cap ((\mathrm{B}^c \cap \mathrm{B}) \cap \mathrm{A}^c) && \text{[Associative law]} \\
&= \mathrm{A} \cap (\phi \cap \mathrm{A}^c) && \text{[Complement law]} \\
&= (\mathrm{A} \cap \phi) && \text{[Bound law]} \\
&= \phi && \text{[Bound law]}
\end{aligned}$$

Example 25 *For all sets X, Y and Z prove that $X \cap (Y - Z) = (X \cap Y) - (X \cap Z)$.*

Solution : $x \in X \cap (Y - Z)$

$\Leftrightarrow$ $x \in X$ and $x \in (Y - Z)$

$\Leftrightarrow$ $x \in X$ and ($x \in Y$ and $x \notin Z$)

$\Leftrightarrow$ ($x \in X$ and $x \in Y$) and ($x \in X$ and $x \notin Z$)

$\Leftrightarrow$ $x \in (X \cap Y)$ and $x \notin (X \cap Z)$

$\Leftrightarrow$ $x \in (X \cap Y) - (X \cap Z)$

Therefore $X \cap (Y - Z) = (X \cap Y) - (X \cap Z)$

Example 26 *For all sets X, Y and Z prove that $X - (Y \cup Z) = (X - Y) \cap Z^c$.*

Solution : $x \in X - (Y \cup Z)$

$\Leftrightarrow$ $x \in X$ and $x \notin (Y \cup Z)$

$\Leftrightarrow$ $x \in X$ and ($x \notin Y$ and $x \notin Z$)

$\Leftrightarrow$ ($x \in X$ and $x \notin Y$) and $x \notin Z$

$\Leftrightarrow$ $x \in (X - Y)$ and $x \in Z^c$

$\Leftrightarrow$ $x \in (X - Y) \cap Z^c$

Therefore $X - (Y \cup Z) = (X - Y) \cap Z^c$.

Example 27 *Determine the equality for the following pair of sets.*

$A = \{1, 2, 3\}$ and $B = \{x \mid x \in N;\ x^3 - 6x^2 + 11x - 6 = 0\}$

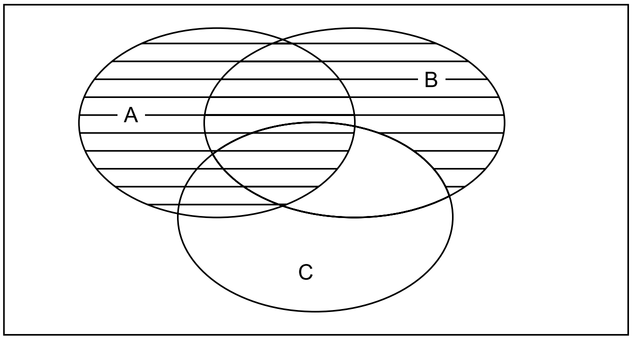
Solution : Given $A = \{1, 2, 3\}$ and

$$B = \{x \mid x \in N;\ x^3 - 6x^2 + 11x - 6 = 0\}$$
$$= \{x \mid x \in N;\ (x - 1)(x - 2)(x - 3) = 0\}$$
$$= \{1, 2, 3\}$$

Therefore sets A and B are equal as $A \subseteq B$ and $B \subseteq A$.

Example 28 *Express $A \cup (B - C)$ as the union of fundamental products.*

Solution : The figure given below represents the Venn diagram for $A \cup (B - C)$. From this it is clear that $A \cup (B - C)$ consists of the five areas of the Venn diagram corresponding to the fundamental products $(A \cap B \cap C)$, $(A \cap B \cap C^c)$, $(A \cap B^c \cap C)$, $(A^c \cap B \cap C^c)$ and $(A \cap B^c \cap C^c)$.



$A \cup (B - C)$ is shaded

Thus $A \cup (B - C) = (A \cap B \cap C) \cup (A \cap B \cap C^c) \cup (A \cap B^c \cap C) \cup (A^c \cap B \cap C^c) \cup (A \cap B^c \cap C^c)$.

EXERCISES

1. Express the following sets in tabular form.

(*a*) $A = \{x \mid x \text{ is a letter in the word MATHEMATICS}\}$

(*b*) $B = \{x \mid x = 2n + 1;\ 1 \leq n < 5;\ n \in N\}$

(*c*) $C = \{x \mid x = \text{Book and } x = 1 \text{ and } x = a \text{ and } x = \text{pen}\}$

(*d*) $D = \{x \mid x \text{ is an even integer and } 1 \leq x \leq 15\}$

(*e*) $E = \{x \mid x \in I \text{ and } x^2 + x - 20 = 0\}$

2. Express the following sets in set builder form.

(*a*) $A = \{1, 8, 27, 64, 125\}$ (*b*) $B = \{a, e, i, o, u\}$

(*c*) $C = \{2, 9, 28, 65, 126\}$ (*d*) $D = \{a, b, 2, 4, 6, \text{Book}\}$

(*e*) $E = \{1, 2, 3, 4, 5, 6, 7, \ldots\ldots\}$ (*f*) $F = \{1, 3\}$

3. Find the power sets of the following sets.

(*a*) $\{\phi\}$ (*b*) $\{k, l, m, n\}$

(c) $\{x \mid x \in N \text{ and } x^2 - 4x + 3 = 0\}$ (*d*) $\{1, \{1, 2\}, \{1, 2, 3\}\}$

(*e*) $\{x \mid x \text{ is a letter of the word wolf}\}$

4. Let the universal set $U = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, Let $A = \{1, 2, 3, 4, 5\}$, $B = \{2, 4, 6, 8\}$ and $C = \{1, 4, 7, 10\}$, then find the followings.

(*i*) $(A \cup B)$ (*ii*) $(A \cup B) \cap C$

(*iii*) $(A \cup B) \cap (A \cup C)$ (*iv*) $(A \cap B) \cup (A \cap C)$

(*v*) $A - (B \cup C)$ (*vi*) $(A \cap B) - C$

(*vii*) $B^c - (C - A)$ (*viii*) $A^c \cap B^c$

(*ix*) AB (*x*) A^c

(*xi*) $C - B$ (*xii*) $(A \cup B) - (C - B)$

5. Draw the Venn diagram and indicate the region for the given sets.

(*a*) $A \cup (B \cap C)$ (*b*) $A \cap (B \cup C)$

(*c*) $A^c - B$ (*d*) $(A \cup B) - B$

(*e*) $(A^c \cup B) \cap (C^c - A)$ (*f*) $B \cap (C \cup A)^c$

(*g*) $(B \cup C) - A$ (*h*) $(A \cup B \cup C)^c$

6. In a group of 1000 people, there are 800 people who can speak English and 500 people who can speak German. Except 100 people in the group, each person speaks at least one of English and German. Find how many people can speak both English and German.

7. If $P = \{a, c, e\}$, $Q = \{100, 101, 102\}$ and $R = \{m, c, e, 101\}$, then compute $((P \cup R) - (P \cap R)) \times Q$.

8. If $G = \{p, q, r\}$, $H = \{20, 70, 90\}$ and $K = \{r, 70, s\}$, then compute $(G - K) \times (K - H)$.

9. Let $X = \{a, b, c\}$ and $Y = \{1, 2\}$, then compute the followings.

(*a*) $X \times Y$ (*b*) $Y \times X$

(*c*) $Y \times Y$ (*d*) $X \times X$

(*e*) $(X \Delta Y) \times Y$

10. If $B_1, B_2, \ldots.., B_n$ and A are sets, then prove that $A - \bigcap_{i=1}^{n} B_i = \bigcup_{i=1}^{n} (A - B_i$

11. If $B_1, B_2, \ldots.., B_n$ are sets, then prove the following De-Morgan's laws.

(*a*) $\left(\bigcup_{i=1}^{n}\right)' = \bigcap_{i=1}^{n} B_i'$ (*b*) $\left(\bigcap_{i=1}^{n} B_i\right)' = \bigcup_{i=1}^{n} B_i'$

12. Let X, Y and Z be three sets. Show that $X - (Y \cap Z) = (X - Y) \cup (X - Z)$.

13. In a class of 120 students, 80 students study Mathematics, 45 study history and 20 students neither study History nor study Mathematics. What is the number of students who study both Mathematics and History.

14. Let A = {1, 2}, B = {α} and C = {α, β} then compute the followings.

(*a*) $A \times B \times C$ (*b*) $A \times B \times B$

(*c*) $B \times A \times C$ (*d*) $A \times A \times A$

(*e*) $(A - B) \times C$.

15. Examine the comparability with the following sets.

(*i*) A = {*a*, *b*, *c*} (*ii*) B = {*a*, *e*, *i*, *o*, *u*}

(*iii*) C = {*b*, *c*, *o*, *u*} (*iv*) D = {*b*, *c*, *i*, *o*, *u*, *k*}.

16. In a class containing 100 students, 30 play tennis; 40 play cricket; 40 do athletics; 6 play tennis and cricket; 12 play cricket and do athletics; and 10 play tennis and do athletics; while 14 play no game or do athletics at all. How many play cricket, tennis and do athletics.

17. If in a city 70% of the residents can speak Tamil and 50% can speak Kannada, what percentage of residents can speak both the languages, if 10% residents cannot speak any of these two languages?

18. Let X, Y, Z and T be four sets. Then Prove that $(X \cap Z) \times (Y \cap T) = (X \times Y) \cap (Z \times T)$

19. Write the following sets as the union of fundamental products.

(*a*) $A \cap (B \cup C)$ (b) $A^c \cap (B \cup C)$

(*c*) $A \cup (B \cap C)$ (d) $A \cup (B - C)$.

20. Identify the smallest set X containing the sets.
{Book, Pen}; {Pen, Pencil, Box}; {Book, Box, Ball}.

21. One hundred students were asked whether they had taken courses in any of the three subjects, Mathematics, Computer Science and Information Technology. The results were given below. 45 had taken Mathematics; 18 had taken Mathematics and Computer Science; 38 had taken Computer Science; 21 had taken Information Technology; 9 had taken Mathematics and Information Technology.; 4 had taken Computer Science and Information Technology and 23 had taken no courses in any of the subjects. Draw a Venn diagram that will show the results of the survey.

3

Binary Relation

■ 3.0 INTRODUCTION

After the development of set theory we shall try to develop another concept based on it. In this chapter we will introduce an important modeling in mathematics known as relation. This has tremendous application in Computer Science. The relations which are used in Mathematics and Computer Science are "less then", "is a subset of", "is perpendicular to", "is equal to", and so on.

Table 3.0.1

Student Names	***Subjects Taken***
Aditi	Computer Science
Sudeep	Mathematics
Lipsa	Computer Science
Aparupa	Human Resource
Ashirbad	Marketing
Srimant	Mathematics
Aditi	Mathematics

A relation can be thought of as a table. Consider the Table 3.0.1 given above in which the first column represent the student names and the second column represent the subject taken by the students. From the table it is clear that Aditi is taking Computer Science and Mathematics, Lipsa is taking Computer Science and Sudeep is taking Mathematics. This is nothing but a set of ordered pairs. We define a relation to be a set of ordered pairs.

Mostly the relations we come across are defined with two entities. We call such relation as binary relation or simply relation.

■ 3.1 BINARY RELATION

Let A and B be two sets. Then any subset R of the Cartesian product (A × B) is a relation (binary relation) from the set A to the set B. Symbolically $R \subseteq (A \times B)$.

i.e. $$R = \{(x, y) \mid x \in A \text{ and } y \in B\}$$

If $(x, y) \in$ R, then we write x R y and say that x is related to y. If $(x, y) \notin$ R, then we write $x \not{R}\, y$ and say that x is not related to y. If A = B, then R is a relation (binary relation) on A.

Consider the example A = {1, 2, 3, 4, 5} and B = {5, 6, 7, 8, 9} and let the relation R from the set A to the set B as

$$R = \{(x, y) \mid x \in A \text{ and } y = 2x + 3 \in B\}$$

i.e. $$R = \{(1, 5), (2, 7), (3, 9), (4, 11), (5, 13)\}$$

i.e. $$R \subseteq A \times B$$

3.1.1 Domain of a Relation

Let R be a relation from the set A to the set B. Then the set of all first constituents of the ordered pairs present in the relation R is known as domain of R . Denoted by dom. R or D(R). Mathematically,

$$D(R) = \{x \mid (x, y) \in R, \text{ for } x \in A\}$$

i.e. $$D(R) \subseteq A.$$

3.1.2 Range of a Relation

Let R be a relation from the set A to the set B. Then the set of all second constituents of the ordered pairs present in the relation R is known as range of R. Denoted by rng.R or R(R). Mathematically,

$$R(R) = \{y \mid (x, y) \in R, \text{ for } y \in B\}$$

i.e. $$R(R) \subseteq B.$$

Consider the example: Let A = $\{a, b, c, d\}$ and B = {5, 6, 7}. Let us define a relation R from the set A to the set B as below.

$$R = \{(a, 5), (a, 6), (c, 6), (d, 6)\}$$

So, $$D(R) = \{a, c, d\} \text{ and } R(R) = \{5, 6\}$$

■ 3.2 INVERSE RELATION

Let R be a relation from the set A to the set B. Then the inverse of the relation R is a relation from the set B to the set A. Which is denoted by $R^{-1}$and is defined as

$$R^{-1} = \{(y, x) \mid (x, y) \in R\}$$

Consider the example: Let A = {1, 2, 3, 4, 5}

and B = {4, 9, 16, 17, 25}

Let us consider the relation R from the set A to the set B as R = {(2, 4), (3, 9), (4, 16), (3, 17)}.

Therefore R^{-1}= {(4, 2), (9, 3), (16, 4), (17, 3)}.

3.2.1 Theorem

If R be a relation from the set A to the set B, then (*i*) $D(R) = R(R^{-1})$ and (*ii*) $R(R) = D(R^{-1})$.

Proof: Given that R be a relation from the set A to the set B. *i.e.* $R \subseteq (A \times B)$. Thus

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

Let $x \in D(R)$. Then there exists $x \in A$ and $y \in B$ such that

$(x, y) \in R$

This implies $(y, x) \in R^{-1}$

i.e. $x \in R(R^{-1})$

So, $x \in D(R) \Rightarrow x \in R(R^{-1})$

Thus, $D(R) \subseteq R(R^{-1})$ ...(1)

Again let $x \in R(R^{-1})$. Then there exists $x \in A$ and $y \in B$ such that $(y, x) \in R^{-1}$.

This implies $(x, y) \in R$

i.e. $x \in D(R)$

So, $x \in R(R^{-1}) \Rightarrow x \in D(R)$

Thus $R(R^{-1}) \subseteq D(R)$ ...(2)

Therefore from equations (1) and (2) it is clear that $D(R) = R(R^{-1})$

Similarly, let $y \in R(R)$, Then there exists $x \in A$ and $y \in B$ such that $(x, y) \in R$

This implies $(y, x) \in R^{-1}$

i.e. $y \in D(R^{-1})$

So, $y \in R(R) \Rightarrow y \in D(R^{-1})$

Thus $R(R) \subseteq D(R^{-1})$ ...(3)

Again let $y \in D(R^{-1})$, Then there exists $x \in A$ and $y \in B$ such that $(y, x) \in R^{-1}$

This implies $(x, y) \in R$

i.e. $y \in R(R)$.

So, $y \in D(R^{-1}) \Rightarrow y \in R(R)$

Thus $D(R^{-1}) \subseteq R(R)$ ...(4)

Therefore from equations (3) and (4) it is clear that $R(R) = D(R^{-1})$.

Note: Let R be a relation from the set A to the set B . Then $(R^{-1})^{-1} = R$.

Proof: Given that R be a relation from the set A to the set B. *i.e.* $R \subseteq (A \times B)$.

Let $(x, y) \in (R^{-1})^{-1}$

$\Leftrightarrow$ $(y, x) \in R^{-1}$

$\Leftrightarrow$ $(x, y) \in R$

So, $(x, y) \in (R^{-1})^{-1} \Leftrightarrow (x, y) \in R$

Therefore $(R^{-1})^{-1} = R$

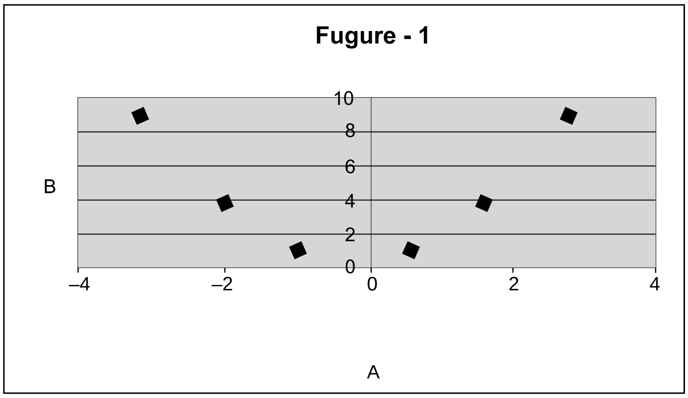
■ 3.3 GRAPH OF RELATION

Let R be a relation from the set A to the set B; that is R is a subset of $(A \times B)$. Since $(A \times B)$ can be represented by the set of points on the coordinate diagram of $(A \times B)$, we can picture R by emphasizing those points in the plane which belong to R. The pictorial representation of the relation R on the coordinate diagram of $(A \times B)$ is known as graph of the relation.

Consider the example: Let A = { – 3, – 2, – 1, 1, 2, 3 } and B = {1, 2, 3, 4, 5, 6, 7, 8, 9} and x R y such that $y = x^2$. Thus we have

$$R = \{(-1, 1), (1, 1), (-2, 4), (2, 4), (-3, 9), (3,9)\}.$$

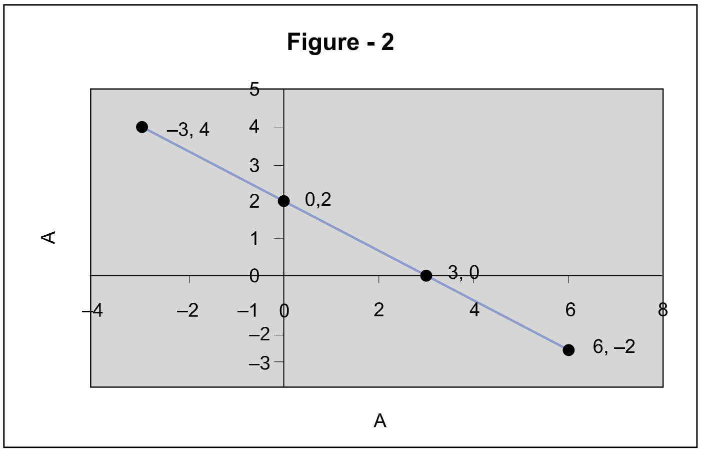
So, the graph of R is represented on the coordinate diagram of (A × B) as shown in the following fig. 1.



Consider another example: Let A = {x | x is a real number} and x R y such that $2x + 3y \le 6$.

Thus we have R = $\{(x, y) \mid 2x + 3y \le 6 \text{ and } x, y \in A\}$.

So, the graph of R is represented on the coordinate diagram of (A × A) as shown in the following Fig. 2.



■ 3.4 KINDS OF RELATION

A relation R from a set A to a set B may be of four kinds.

(*a*) One – One	(*b*) One – Many
(*c*) Many – One	(*d*) Many – Many .

The relation R from the set A to the set B is said to be One – One relation if $(x_1, y_1) \in$ R, $(x_2, y_2) \in$ R then $y_1 = y_2 \Rightarrow x_1 = x_2$.

The relation R from the set A to the set B is said to be One – Many relation if $(x_1, y_1) \in$ R, $(x_1, y_2) \in$ R for some $x_1 \in$ A and y_1 , $y_2 \in$ B with $y_1 \ne y_2$.

The relation R from the set A to the set B is said to be Many – One relation if $(x_1, y_1) \in$ R, $(x_2, y_1) \in$ R for some $y_1 \in$ B and x_1 , $x_2 \in$ A with $x_1 \ne x_2$.

The relation R from the set A to the set B is said to be Many – Many relation if $(x_1, y_1) \in$ R, $(x_1, y_2) \in$ R, $(x_{2\,,} y_1) \in$ R, and $(x_2, y_2) \in$ R for some $x_1, x_2 \in$ A and $y_1, y_2 \in$ B with $x_1 \ne x_2$ and $y_1 \ne y_2$.

■ 3.5 ARROW DIAGRAM

We use arrow diagrams to represent relations. Write down the elements of the set A and the elements of the set B in two disjoint sets, and then draw an arrow from $x \in$ A to $y \in$ B whenever xRy.

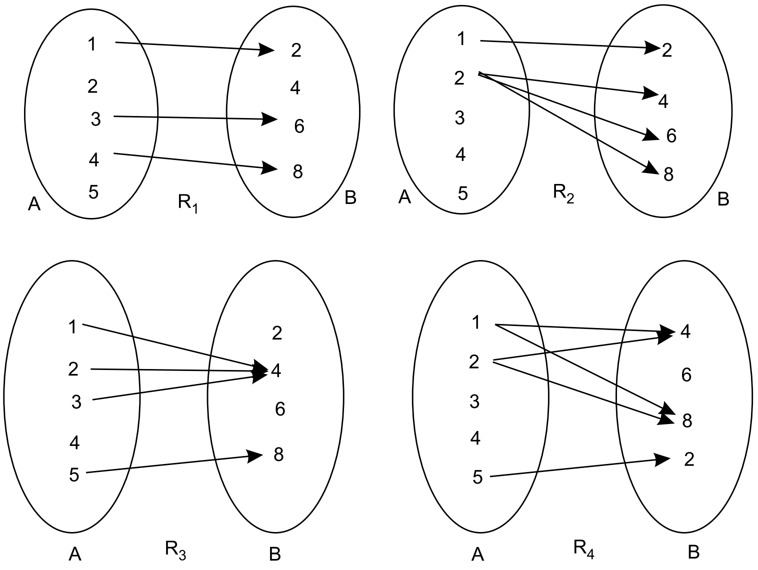
Consider the example: Let A = {1, 2, 3, 4, 5} and B = {2, 4, 6, 8}. Let us define the relations from the set A to the set B as

$$R_1 = \{(1, 2), (3, 6), (4, 8)\}$$

$$R_2 = \{(2, 4), (2, 6), (2, 8), (1, 2)\}$$

$$R_3 = \{(1, 4), (2, 4), (3,4), (5, 8)\}$$

and $$R_4 = \{(1, 4), (2, 4), (1, 8), (2, 8), (5, 2)\}$$



The arrow diagrams for the above relations are given above. From the above diagrams it is clear that R_1, R_2, R_3 and R_4 are One–One, One–Many, Many–One and Many–Many relations respectively.

■ 3.6 VOID RELATION

A relation R from a set A to a set B is said to be a void relation or empty relation if R = ϕ.

Consider the example: Let A = {3, 5, 7}; B = {2, 4, 8}; R $\subseteq$ A × B and x R y | x divides y; $x \in$ A, $y \in$ B. Hence we observe that R = $\phi \subseteq$ A × B is a void relation from the set A to the set B.

■ 3.7 IDENTITY RELATION

Let R be a relation on a set A; that is R is a subset of (A × A). Then the relation R is said to be an identity relation if $(x, x) \in$ R. Generally denoted by I_A. Mathematically,

$$I_A = \{(x, x) \mid x \in A\}$$

Consider the example: Let A = $\{a, b, c\}$ and I_A be a relation on A such that $I_A = \{(a, a), (b, b), (c, c)\}$. This is an identity relation on A.

■ 3.8 UNIVERSAL RELATION

A relation R from a set A to a set B is said to be an universal relation if R is equal to (A × B). That is R = (A × B).

Let A = {1, 2, 3} and B = $\{a, b\}$. Therefore the universal relation R from the set A to the set B is given as

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

■ 3.9 RELATION MATRIX (MATRIX OF THE RELATION)

A matrix is a convenient way to represent a relation R. Such a representation can be used by a computer to analyze the relation.

Let $\quad A = \{a_1, a_2, a_3, \ldots, a_i, \ldots\ldots, a_k\}$

and $\quad B = \{b_1, b_2, b_3, \ldots, b_j, \ldots, b_l\}$

be two finite sets and R be a relation from the set A to the set B. Then the matrix of the relation R, i.e. M(R) is defined as

$$M(R) = [m_{Ij}] \text{ of order } (k \times l)$$

where
$$m_{Ij} = \begin{cases} 1; & \text{if } a_i \, R \, b_j \\ 0; & \text{if } a_i \, \not{R} \, b_j \end{cases}$$

In other words label the rows of rectangular array by the elements of A and the columns by the elements of B. Each position of the array is to be filled with a 1 (one) or 0 (zero) according as $a \in$ A is related or not related to $b \in$ B. Consider the example

Let A = {1, 2, 3}; B = $\{a, b, c, d, e\}$ and R ⊆ (A × B) such that R = $\{(1, a), (1, d), (2, b), (3, c), (3, d)\}$.

So the matrix of the above relation R is given as

$$M(R) = \begin{array}{c} \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{ccccc} a & b & c & d & e \end{array} \\ \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix} \end{array}$$

■ 3.10 COMPOSITION OF RELATIONS

Let R_1 be a relation from the set A to the set B and R_2 be a relation from the set B to the set C. That is R_1 is a subset of (A × B) and R_2 is a subset of (B × C). Then the composition of R_1 and R_2 is given by R_1R_2 and is defined by

$$R_1R_2 = \{(x, z) \in (A \times C) \mid \text{for some } y \in B, (x, y) \in R_1 \text{ and } (y, z) \in R_2\}$$

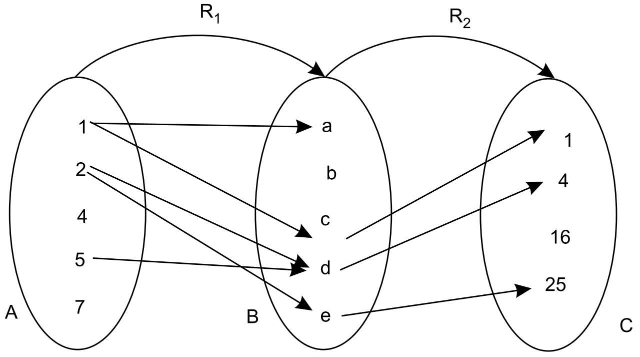
Consider the example: Let A = {1, 2, 4, 5, 7};

$\quad B = \{a, b, c, d, e\}$

and $\quad C = \{1, 4, 16, 25\}$.

Consider the relations R_1: A → B and R_2: B → C as

$R_1 = \{(1, a), (1, c), (2, d), (2, e), (5, d)\}$ and $R_2 = \{(c, 1), (d, 4), (e, 25)\}$. The arrow diagram is given as



So, $\qquad R_1R_2 = \{(1, 1), (2, 4), (2, 25), (5, 4)\}$

3.10.1 Composition of Relations and Relation Matrix

Let R_1 be a relation from the set A to the set B and R_2 be a relation from the set B to the set C. That is R_1 is a subset of $(A \times B)$ and R_2 is a subset of $(B \times C)$. Then the composition of R_1 and R_2 is given by R_1R_2 and the matrix of the composition R_1R_2 is defined as

$$M(R_1R_2) = M(R_1)\,M(R_2)$$

And replace all nonzero entries by 1 in M (R_1R_2) where M (R_1) is the matrix of the relation R_1 and M (R_2) is the matrix of the relation R_2.

Consider the same example stated above; we have

$$M(R_1) = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \text{ and } M(R_2) = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

So, $\qquad M(R_1R_2) = M(R_1)\,M(R_2)$

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

Therefore $R_1R_2 = \{(1, 1), (2, 4), (2, 25), (5, 4)\}$.

3.10.2 Theorem

Let R_1 and R_2 are relations from the set A to the set B. Let R_3 and R_4 are relations from the set B to the set C. If $R_1 \subseteq R_2$ and $R_3 \subseteq R_4$ then $R_1R_3 \subseteq R_2R_4$.

Proof: Given R_1 and R_2 are relations from the set A to the set B. R_3 and R_4 are relations from the set B to the set C.

Suppose that $R_1 \subseteq R_2$ and $R_3 \subseteq R_4$.

Let $(x, z) \in R_1 R_3$

Then for some $y \in$ B, we have $(x, y) \in R_1$ and $(y, z) \in R_3$. Therefore we have $(x, y) \in R_1 \subseteq R_2$ and $(y, z) \in R_3 \subseteq R_4$.

i.e. $(x, y) \in R_2$ and $(y, z) \in R_4$.

This implies $(x, z) \in R_2 R_4$.

Hence $(x, z) \in R_1R_3 \Rightarrow (x, z) \in R_2 R_4$

i.e. $R_1R_3 \subseteq R_2R_4$.

3.10.3 Theorem

Let R_1 be relation from the set A to the set B and R_2 be a relation from the set B to the set C. Then.

$$(R_1R_2)^{-1} = R_2^{-1}R_1^{-1}.$$

Proof: Let R_1 be a relation from the set A to the set B and R_2 be a relation from the set B to the set C.

Our claim: $(R_1R_2)^{-1} = R_2^{-1}R_1^{-1}$.

i.e. $(R_1R_2)^{-1} \subseteq R_2^{-1}R_1^{-1}$ and $R_2^{-1}R_1^{-1} \subseteq (R_1R_2)^{-1}$

Let $(x, z) \in (R_1R_2)^{-1}$

This implies $(z, x) \in R_1R_2$. Then for some $y \in$ B we have

$(z, y) \in R_1$ and $(y, x) \in R_2$

$\Rightarrow$ $(y, z) \in R_1^{-1}$ and $(x, y) \in R_2^{-1}$

i.e. $(x, y) \in R_2^{-1}$ and $(y, z) \in R_1^{-1}$

This implies $(x, z) \in R_2^{-1}R_1^{-1}$

Therefore $(x, z) \in (R_1R_2)^{-1} \Rightarrow (x, z) \in R_2^{-1}R_1^{-1}$

i.e. $(R_1R_2)^{-1} \subseteq R_2^{-1}R_1^{-1}$ ... (*i*)

Again let $(x, z) \in R_2^{-1}R_1^{-1}$. Then for some $y \in$ B we have

$(x, y) \in R_2^{-1}$ and $(y, z) \in R_1^{-1}$

$\Rightarrow$ $(y, x) \in R_2$ and $(z, y) \in R_1$

i.e. $(z, y) \in R_1$ and $(y, x) \in R_2$

This implies $(z, x) \in R_1R_2$

i.e. $(x, z) \in (R_1R_2)^{-1}$

Therefore $(x, z) \in R_2^{-1}R_1^{-1} \Rightarrow (x, z) \in (R_1R_2)^{-1}$

i.e. $R_2^{-1}R_1^{-1} \subseteq (R_1R_2)^{-1}$ ... (*ii*)

Thus from equations (*i*) and (*ii*) we get $(R_1R_2)^{-1} = R_2^{-1}R_1^{-1}$.

■ 3.11 TYPES OF RELATIONS

This section discusses a number of different important types of relations on a set A.

3.11.1 Reflexive Relations

A relation R defined on a set A is said to be reflexive if $(x, x) \in$ R for every element $x \in$ A.

i.e. $x\,Rx \quad \forall\, x \in A$

Consider the following relations on the set A = {1, 3, 5, 7}

$$R_1 = \{(1, 1), (1, 3), (1, 5), (5, 5), (5, 7)\}$$

$$R_2 = \{(1, 3), (1, 5), (5, 7), (3, 7)\}$$
$$R_3 = \{(1, 1), (1, 3), (3, 3), (5, 5), (5, 7), (1, 7), (7, 7)\}$$

From the above relations it is clear that R_3 is a reflexive relation. R_1 is not a reflexive relation as $(3, 3) \notin R_1$ and $(7, 7) \notin R_1$. Similarly R_2 is also not reflexive.

3.11.2 Symmetric Relations

A relation R defined on a set A is said to be symmetric if $(x, y) \in R$ then $(y, x) \in R$.

i.e. $x\,R\,y \Rightarrow y\,R\,x$.

Consider the following relations on the set A = {1, 3, 5, 7}

$$R_1 = \{(1, 1), (1, 3), (3, 5), (3, 1), (5, 3), (5, 5)\}$$
$$R_2 = \{(1, 1), (1, 3), (3, 1), (3, 5), (5, 3), (5, 7), (7, 7)\}$$

From the above relations it is clear that R_1 is a symmetric relation, but R_2 is not a symmetric relation as $(5, 7) \in R_2 \Rightarrow (7, 5) \notin R_2$.

3.11.3 Transitive Relations

A relation R defined on a set A is said to be transitive if $(x, y) \in R$ and $(y, z) \in R$ then $(x, z) \in R$.

i.e. $x\,R\,y$ and $y\,R\,z \Rightarrow x\,R\,z$

Consider the following relations on the set A = {1, 3, 5, 7}.

$$R_1 = \{(1, 1), (1, 3), (1, 5), (1, 7), (3, 3), (3, 5), (3, 7), (5, 3), (5, 5), (5, 7)\}$$
$$R_2 = \{(1, 1), (1, 3), (3, 5), (5, 5), (7, 7)\}$$

From the above relations it is clear that R_1 is a transitive relation. The relation R_2 is not transitive as $(1,3) \in R_2$, $(3, 5) \in R_2 \Rightarrow (1,5) \notin R_2$.

3.11.4 Anti-Reflexive Relations

A relation R defined on a set A is said to be anti-reflexive or irreflexive if $(x, x) \notin R$ for every element $x \in A$.

i.e. $x \not{R}\, x \quad \forall\, x \in A$

Consider the following relations on the set A = {1, 3, 5, 7}

$$R_1 = \{(1, 1), (1, 3), (1, 7), (3, 3), (5, 5), (5, 7), (7, 7)\}$$
$$R_2 = \{(1, 3), (1, 5), (5, 7), (3, 7)\}$$
$$R_3 = \{(1, 1), (1, 3), (1, 5), (7, 7)\}$$

From the above relations it is clear that R_2 is an anti-reflexive relation. R_3 is not an anti reflexive relation as $(1, 1) \in R_3$ and $(7, 7) \in R_3$. Similarly R_1 is not anti-reflexive relation.

3.11.5 Asymmetric Relations

A relation R defined on a set A is said to be asymmetric if $(x, y) \in R$ then $(y, x) \notin R$.

i.e. $x\,R\,y \Rightarrow y \not{R}\, x$

Consider the following relations on the set A = {1, 3, 5, 7}

$$R_1 = \{(1, 3), (3, 5), (3, 7), (5, 7)\}$$
$$R_2 = \{(1, 3), (3, 5), (3, 7), (5, 3), (5, 7)\}$$

From the above relations it is clear that R_1 is an asymmetric relation. R_2 is not an asymmetric relation as $(3, 5) \in R_2 \Rightarrow (5, 3) \in R_2$.

3.11.6 Anti-Symmetric Relations

A relation R defined on a set A is said to be anti-symmetric relation if $(x, y) \in$ R and $(y, x) \in$ R, then $x = y$.

i.e. $x \mathrm{R} y$ and $y \mathrm{R} x \Rightarrow x = y$.

Consider the following relations on the set A = {1, 3, 5, 7}

$$\mathrm{R}_1 = \{(1,1), (1, 3), (3, 5), (5, 5), (5, 7)\}$$
$$\mathrm{R}_2 = \{(1, 1), (3, 3), (7, 7)\}$$
$$\mathrm{R}_3 = \{(3, 3), (3, 5), (5, 3), (5, 7), (7, 5), (7, 7)\}$$

From the above relations it is clear that R_1 and R_2 are anti-symmetric. R_3 is not an anti-symmetric relation as $(3, 5) \in$ R and $(5, 3) \in$ R, but $3 \neq 5$. Similarly $(5, 7) \in$ R and $(7, 5) \in$ R, but $5 \neq 7$.

3.12 TYPES OF RELATIONS AND RELATION MATRIX

Let A = $\{a_1, a_2, \ldots, a_i, \ldots., a_j, \ldots\ldots, a_n\}$ be a non-empty set and R be a relation defined on the set A. Hence the matrix of the relation R relative to the ordering $a_1, a_2, \ldots, a_i, \ldots., a_j, \ldots\ldots, a_n$ is defined as

$$\mathrm{M(R)} = [\, m_{ij} \,]_{n\, x\, n}$$

where
$$m_{ij} = \begin{cases} 1 & \text{If } a_i \mathrel{\mathrm{R}} a_j \\ 0 & \text{If } a_i \not\mathrel{\mathrm{R}} a_j \end{cases}$$

3.12.1 Reflexive Relations

The relation R is said to be reflexive if $m_{ii} = 1 \; \forall \; 1 \leq i \leq n$

i.e. all elements of the main diagonal in relation matrix M(R) are 1.

3.12.2 Symmetric Relations

The relation R is said to be symmetric if $m_{ij} = m_{ji} \; \forall \; 1 \leq i \leq n$ and $1 \leq j \leq n$.

In other words the relation R is said to be symmetric if $\mathrm{M(R)} = [\,\mathrm{M(R)}]^{\mathrm{T}}$. where $[\mathrm{M(R)}]^{\mathrm{T}}$ represents the transpose of the relation matrix M(R).

3.12.3 Transitive Relation

The relation R is said to be transitive if $m_{ij} = 1$ and $m_{jk} = 1$, then $m_{ik} = 1$ for $1 \leq i \leq n$; $1 \leq j \leq n$ and $1 \leq k \leq n$.

In other words the relation R is said to be transitive if and only if $\mathrm{R}^2 \subseteq \mathrm{R}$. *i.e.* Whenever entry i, j in $[\mathrm{M(R)}]^2$ is non-zero, entry i, j in M(R) is also non-zero.

Let R be a relation on the set A and R is transitive.

Let $(x, z) \in \mathrm{R}^2 = \mathrm{R.R}$.

So, there exists $y \in$ A such that $(x, y) \in$ R and $(y, z) \in$ R

Thus $(x, z) \in$ R [$\because$ R is transitive]

i.e. $(x, z) \in \mathrm{R}^2 \Rightarrow (x, z) \in \mathrm{R}$

Therefore $\mathrm{R}^2 \subseteq \mathrm{R}$.

Conversely,Suppose that $R^2 \subseteq R$.

Let $(x, y) \in R$ and $(y, z) \in R$

This implies $(x, z) \in R$. $R = R^2$

i.e. $(x, z) \in R^2 \subseteq R$

i.e. $(x, z) \in R$

Therefore R is transitive.

3.12.4 Anti-Reflexive Relations

The relation R is said to be anti-reflexive if $m_{ii} = 0 \; \forall \; 1 \leq i \leq n$
i.e. All elements of the main diagonal in relation matrix M(R) are 0 (zero).

3.12.5 Asymmetric Relations

The relation R is said to be asymmetric if $m_{ij} = 1$, then $m_{ji} = 0$ and $m_{ii} = 0$.

3.12.6 Anti-Symmetric Relations

The relation R is said to be anti-symmetric if $a_i \neq a_j$ then either $m_{ij} = 0$ or $m_{ji} = 0$ and $m_{ij} = 1 = m_{ji}$ implies $a_i = a_j$.

Consider the following relations on the set A = {1, 3, 5, 7}

$$R_1 = \{(1, 1), (1, 3), (1, 7), (3, 3), (3, 7), (5, 5), (5, 7), (7, 7)\}$$
$$R_2 = \{(1, 1), (1, 5), (1, 7), (3, 5), (3, 7), (5, 1), (5, 3), (7, 1), (7, 3)\}$$
$$R_3 = \{(1, 1), (1, 3), (1, 5), (1, 7), (3, 1), (3, 3), (3, 5), (3, 7), (5, 7)\}$$
$$R_4 = \{(1, 3), (1, 7), (3, 7), (5, 7), (7, 1)\}$$
$$R_5 = \{(1, 3), (3, 5), (5, 7), (7, 1), (7, 3)\}$$
$$R_6 = \{(1,1), (1, 7), (7, 5), (7, 3), (5, 3)\}$$

Relative to the ordering 1, 3, 5, 7 we get

$$M(R_1) = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}; \quad M(R_2) = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix};$$

$$M(R_3) = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}; \quad M(R_4) = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix};$$

$$M(R_5) = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}; \quad M(R_6) = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix};$$

From the above matrices it is clear that $m_{ii} = 1$ in $M(R_1)$ and $m_{ii} = 0$ in $M(R_4)$ and $M(R_5)$. Thus the relation R_1 is reflexive where as the relations R_4 and R_5 are anti-reflexive. Again

$$[M(R_2)]^T = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix} = M(R_2)$$

So, the relation R_2 is symmetric. Also $[M(R_1)]^T \neq M(R_1)$, and hence the relation R_1 is not symmetric. Similarly it can be shown that the relations R_3, R_4, R_5 and R_6 are not symmetric.

Now in $M(R_1)$, $M(R_2)$, $M(R_3)$ and $M(R_6)$, we see that $m_{ii} \neq 0$, so the relations R_1, R_2, R_3 and R_6 are not asymmetric. In $M(R_4)$ we see that $m_{ii} = 0$, but $m_{14} = 1 = m_{41}$. This violate the conditions of asymmetric relation hence not asymmetric. It is also observed that in $M(R_5)$, $m_{ii} = 0$; $m_{12} = 1$, $m_{21} = 0$; $m_{23} = 1$, $m_{32} = 0$; $m_{34} = 1$, $m_{43} = 0$; $m_{41} = 1$, $m_{14} = 0$ and $m_{42} = 1$, $m_{24} = 0$. Thus the relation R_5 is asymmetric. Again

$$[M(R_3)]^2 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 2 & 2 & 2 & 3 \\ 2 & 2 & 2 & 3 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

We see that whenever i, j in $[M(R_3)]^2$ is non-zero, entry i, j in $M(R_3)$ is also non-zero. So the relation R_3 is transitive. It is also cleared that $[M(R_i)]^2 \not\subset M(R_i)$ for $i = 1, 2, 4, 5, 6$. Thus the relations R_1, R_2, R_4, R_5 and R_6 are not transitive. Also it can be shown that the relation R_6 is anti-symmetric.

■ 3.13 EQUIVALENCE RELATION

A relation R defined on a set A is said to be an equivalence relation in A if and only if R is reflexive, symmetric and transitive.

Consider the relation R in the real numbers defined by $x = y$, *i.e.* $x \; R \; y : x = y$

Reflexive: For all $x \in R$

$x = x$

i.e. $x \; R \; x$

i.e. R is reflexive.

Symmetric: Suppose $x \; R \; y$

i.e. $x = y$

i.e. $y = x$

i.e. $y \; R \; x$

i.e. R is symmetric.

Transitive: Suppose $x \; R \; y$ and $y \; R \; z$

i.e. $x = y$ and $y = z$

This implies $x = z$

i.e. $x \; R \; z$

i.e. R is transitive.

So, the relation R in the real numbers defined by $x = y$ is an equivalence relation.

3.13.1 Theorem

If R be an equivalence relation defined in a set A, then R^{-1} is also an equivalence relation in the set A.

Proof : Let R be an equivalence relation defined in a set A. Thus R is reflexive, symmetric and transitive.

Our claim : R^{-1} is an equivalence relation in the set A.

Reflexive : For all $x \in A$

$(x, x) \in R$ [$\because$ R is reflexive]

$\Rightarrow$ $(x, x) \in R^{-1}$

So, $(x, x) \in R^{-1}\ \forall\ x \in A$

Symmetric: Suppose $(x, y) \in R^{-1}$

$\Rightarrow$ $(y, x) \in R$

$\Rightarrow$ $(x, y) \in R$ [$\because$ R is symmetric]

$\Rightarrow$ $(y, x) \in R^{-1}$

i.e. R^{-1} is symmetric.

Transitive: Suppose $(x, y) \in R^{-1}$ and $(y, z) \in R^{-1}$

$\Rightarrow$ $(y, x) \in R$ and $(z, y) \in R$

i.e. $(z, y) \in R$ and $(y, x) \in R$

$\Rightarrow$ $(z, x) \in R$ [$\because$ R is transitive]

$\Rightarrow$ $(x, z) \in R^{-1}$

i.e. R^{-1} is transitive.

Therefore, R^{-1} is an equivalence relation in the set A.

■ 3.14 PARTIAL ORDER RELATION

Let R be a relation defined on a set A. Then the relation R is said to be a partial order relation in A if R is reflexive, transitive and anti-symmetric.

Consider the relation R in the real numbers defined by $x \le y$. *i.e.* $x\,R\,y : x \le y$

Reflexive: For all $x \in R$, $x \le x$

i.e. $x\,R\,x$

i.e. R is reflexive.

Transitive: Suppose that $x\,R\,y$ and $y\,R\,z$

i.e. $x \le y$ and $y \le z$

This implies $x \le z$

i.e. $x\,R\,z$

i.e. R is transitive.

Anti-Symmetric: Suppose that $x\,R\,y$ and $y\,R\,x$

i.e. $x \le$ y and $y \le x$

This implies $x = y$

i.e. R is anti-symmetric.

So, the relation R in the real numbers defined by $x \le y$ is a partial order relation.

3.14.1 Theorem

Let A be a set and R be a partial order relation on A. Then R^{-1} is also a partial order relation on A.

Proof : Let R be a partial order relation defined in a set A. Therefore R is reflexive, transitive and anti-symmetric.

Our claim: R^{-1} is a partial order relation.

Reflexive: For all $x \in A$

$(x, x) \in R$ [$\because$ R is reflexive]

This implies $(x, x) \in R^{-1}$

i.e. R^{-1} is reflexive.

Transitive: Suppose that $(x, y) \in R^{-1}$ and $(y, z) \in R^{-1}$

This implies$(y, x) \in R$ and $(z, y) \in R$

i.e. $(z, y) \in R$ and $(y, x) \in R$

This implies $(z, x) \in R$ [$\because$ R is transitive]

i.e. $(x, z) \in R^{-1}$

i.e. R^{-1} is transitive.

Anti-symmetric: Suppose that $(x, y) \in R^{-1}$ and $(y, x) \in R^{-1}$

This implies$(y, x) \in R$ and $(x, y) \in R$

This implies $x = y$ [$\because$ R is anti-symmetric]

i.e. R^{-1} is anti-symmetric.

Therefore R^{-1} is a partial order relation in the set A.

■ 3.15 TOTAL ORDER RELATION

Let R be a relation defined on a set A. Then the relation R is said to be a total order relation in A if R is a partial order relation and for any two elements x, y in A either $x < y$, $x = y$ or $x > y$ holds.

Consider the relation R in D(6) defined by$x \leq y$, where D(6) is the set of all positive divisors of 6.

Therefore D(6) = {1, 2, 3, 6} and $x \, R \, y : x \leq y$

i.e. R = {(1, 1), (1, 2), (1, 3), (1, 6), (2, 2), (2, 3), (2, 6), (3, 3), (3, 6), (6, 6)}

So, R is reflexive, transitive and anti-symmetric. *i.e.* R is a partial order relation in D(6).

Besides this for any two elementsx, y belongs D(6), one of the relations$x \leq y$ or$y \leq x$ holds. Thus the relation R in D(6) defined by $x \leq y$ is a total order relation.

Consider another relation R in A = {1, 2, 3, …. , 10} defined by x is a multiple of y.

i.e. $x \, R \, y$: x is a multiple of y

Reflexive: For all $x \in A$

x is a multiple of x

i.e. $x \, R \, x$

i.e. R is reflexive.

Transitive:Suppose $x \, R \, y$ and $y \, R \, z$

i.e.x is a multiple of y and y is a multiple of z

$\Rightarrow$ $x = K_1 y$ and $y = K_2$ z for $K_1, K_2 \in I$; $K_1, K_2 \neq 0$

$\Rightarrow$ $x = K_1K_2 \, z$; $K_1, K_2 \in I$; $K_1K_2 \neq 0$

i.e. x is a multiple of z

i.e. x R z

i.e. R is transitive.

Anti-symmetric: Suppose x R y and y R x

i.e.x is a multiple of y and y is a multiple of x

$\Rightarrow \quad x = K_1 y$ and $y = K_2 x$ for $K_1, K_2 \in I$; $K_1, K_2 \neq 0$

$\Rightarrow \quad x = K_1K_2 x$

$\Rightarrow \quad K_1K_2 = 1$

$\Rightarrow \quad K_1 = K_2 = 1 \qquad [\because \; K_1, K_2 \neq 0$ and $K_1, K_2 \in I]$

So, $x = y$, *i.e.* R is anti-symmetric. Therefore the relation in A defined by x is a multiple of y is a partial order relation.

Now R = {(1, 1), (1, 2), (1, 3), (1, 4), (1, 5), (1, 6), (1, 7), (1, 8), (1, 9), (1, 10), (2, 2), (2, 4), (2, 6), (2, 8), (2, 10), (3, 3), (3, 6), (3, 9), (4, 8), (5, 10)}

Again for 2 and 5 belongs to A either of the relations $2 \leq 5$ or $2 \geq 5$ do not hold because 2 is not a multiple of 5. Therefore R is not a total order relation.

■ 3.16 CLOSURES OF RELATIONS

If R be a relation defined on A, then the closure of the relation R is the smallest relation R′ that includes all the pairs of R and possesses the required properties of the closure.

3.16.1 Reflexive Closure

Let R be a relation defined on the set A. Then the reflexive closure r(R) is defined by

(*i*) if $(x, y) \in$ R then $(x, y) \in r$(R)

(*ii*) If $x \in$ A, then $(x, x) \in r$(R)

(*iii*) Nothing is in r(R) unless it is so follows from (*i*) and (*ii*).

Consider the following relation on the set A = {2, 4, 6, 8}

R = {(2, 2), (2, 4), (6, 8), (6, 6), (6, 4)}

Therefore r(R) = {(2, 2), (2, 4), (6, 8), (6, 6), (6, 4), (4, 4), (8, 8)}

3.16. 2 Symmetric Closure

Let R be a relation defined on the set A. Then the symmetric closure s(R) is defined by

(*i*) if $(x, y) \in$ R then $(x, y) \in s$(R)

(*ii*) If $(x, y) \in$ R, then $(y, x) \in s$(R)

(*iii*) Nothing is in s(R) unless it is so follows from (*i*) and (*ii*).

Consider the following relation on the set A = {2, 4, 6, 8}

R = {(2, 2), (2, 4), (2, 6), (4, 2), (4, 6), (6, 4), (6, 8), (8, 2)}

Therefore s(R) = {(2, 2), (2, 4), (2, 6), (4, 2), (4, 6), (6, 4), (6, 8), (8, 2), (6, 2), (8, 6), (2, 8)}

3.16.3 Transitive Closure

Let R be a relation defined on the set A. Then the transitive closure t(R) is defined by

(*i*) if $(x, y) \in$ R then $(x, y) \in t$(R) (*ii*) If $(x, y) \in$ R, $(y, z) \in$ R then $(x, z) \in t$(R)

(*iii*) Nothing is in t(R) unless it is so follows from (*i*) and (*ii*).

Consider the following relation on the set A = {2, 4, 6, 8}

$$R = \{(2, 2), (2, 4), (4, 6), (4, 8), (2, 8)\}$$

Therefore t(R) = {(2, 2), (2, 4), (4, 6), (4, 8), (2, 8), (2, 6)}

3.17 EQUIVALENCE CLASSES

Let A be a non empty set. R be an equivalence relation in A. For each $x \in$ A, the sets $[x]$ are called equivalence classes of A given by the relation R defined as

$$[x] = \{y \in A \mid y\,R\,x\}$$

Consider the equivalence relation R defined on the set A = {1, 3, 5, 7, 9} as

R = {(1, 1), (1, 3), (1, 5), (3, 1), (3, 3), (3, 5), (5, 1), (5, 3), (5, 5), (7, 7), (7, 9), (9, 7), (9, 9)}

So, the equivalence classes are given as

$$[1] = [3] = [5] = \{1, 3, 5\}$$
$$[7] = [9] = \{7, 9\}$$

3.17.1 Theorem

Let R be an equivalence relation defined on a non-empty set A and x, y be arbitrary elements in A. Then

(*i*) $x \in [x]$ and (*ii*) If $y \in [x]$, then $[x] = [y]$

Proof: Let R be an equivalence relation defined on a non-empty set A.

(*i*) Let $x \in$ A. Therefore $[x] = \{y \in A \mid y\,R\,x\}$

As R is reflexive in A, we have $x\,R\,x$. *i.e.* $x \in [x]$

(*ii*) Suppose that $y \in [x]$

$\Rightarrow$ $y\,R\,x$ [by definition]

$\Rightarrow$ $x\,R\,y$ [$\because$ R is symmetric]

Let $a \in [x]$; this implies $a\,R\,x$

So, $a\,R\,x$ and $x\,R\,y$

This implies $a\,R\,y$ [$\because$ R is transitive]

i.e. $a \in [y]$

Therefore $a \in [x] \Rightarrow a \in [y]$ *i.e.* $[x] \subseteq [y]$ ...(*i*)

Similarly, Let $b \in [y]$

This implies $b\,R\,y$ [by definition]

So, $b\,R\,y$ and $y\,R\,x$.

$\Rightarrow$ $b\,R\,x$ [$\because$ R is transitive]

i.e. $b \in [x]$.

Therefore $b \in [y] \Rightarrow b \in [x]$ *i.e.* $[y] \subseteq [x]$ ...(*ii*)

Therefore from equations (*i*) and (*ii*) we have $[x] = [y]$.

3.17.2 Theorem

Let A be a non-empty set and R be an equivalence relation defined in A. Let x, y be two arbitrary elements of A. Then $[x] = [y]$ if and only if $x \text{ R } y$.

Proof: Let R be an equivalence relation defined in A, and let $x, y \in$ A. Assume that $[x] = [y]$. Our claim is $x \text{ R } y$.

As R is reflexive, we have $x \text{ R } x$

i.e. $x \in [x]$

$\Rightarrow$ $x \in [x] = [y]$

$\Rightarrow$ $x \in [y]$

i.e. $x \text{ R } y$

Conversely, suppose that $x \text{ R } y$,

i.e. $y \text{ R } x$ [$\because$ R is symmetric]

Our claim is $[x] = [y]$

Let $a \in [x]$ this implies $a \text{ R } x$

i.e. $a \text{ R } x$ and $x \text{ R } y$

This implies $a \text{ R } y$ [$\because$ R is transitive]

i.e. $a \in [y]$

Therefore $a \in [x]$ implies $a \in [y]$, *i.e.* $[x] \subseteq [y]$ ... (i)

Again $a \in [y]$ this implies $a \text{ R } y$

i.e. $a \text{ R } y$ and $y \text{ R } x$

This implies $a \text{ R } x$ [$\because$ R is transitive]

i.e. $a \in [x]$

Therefore $a \in [y]$ implies $a \in [x]$. *i.e* $[y] \subseteq [x]$ ... (ii)

Thus from equations (i) and (ii) we get $[x] = [y]$.

3.17.3 Theorem

Let A be a non-empty set and R be an equivalence relation in A, Let $x, y \in$ A. Then the equivalence classes $[x]$ and $[y]$ are either equal or disjoint.

Proof: Let A be a non empty set and R be an equivalence relation defined in A. Let $x, y \in$ A

Assume that the equivalence classes $[x]$ and $[y]$ are not disjoint, *i.e.* $[x] \cap [y] \neq \phi$

Thus there exists at least one element a in $[x] \cap [y]$.

i.e. $a \in [x] \cap [y]$

i.e. $a \text{ R } x$ and $a \text{ R } y$

i.e. $x \text{ R } a$ and $a \text{ R } y$ [$\because$ R is symmetric]

This implies $x \text{ R } y$ [$\because$ R is transitive]

Hence by previous theorem 3.17.2 it is clear that $[x] = [y]$. Therefore it is clear that if two equivalence classes [x] and [y] are either disjoint or equal.

■ 3.18 PARTITIONS

Let A be a non-empty set. A partition P of A is a collection $\{A_i\}$ of non-empty subsets of A with the following two properties.

(*i*) $\bigcup_i A_i = A$ and

(*ii*) $A_i \cap A_j = \phi$ for $A_i \neq A_j$

In other words a partition of A is a collection of non-empty disjoint subset of A whose union is A.

Consider the relation $x \equiv y \pmod 3$ defined on the set of integers I. The above relation is an equivalence relation in I. The set of three equivalence classes are [0], [1] and [2]. Where

$$[0] = \{\ldots, -6, -3, 0, 3, 6, 9, \ldots\ldots\}$$
$$[1] = \{\ldots\ldots, -5, -2, 1, 4, 7, 10, \ldots\}$$
$$[2] = \{\ldots\ldots, -4, -1, 2, 5, 8, 11, \ldots\ldots\}$$

It is clear that [0], [1] and [2] are non empty subsets of I with $[0] \cup [1] \cup [2] = I$, and [0], [1] and [2] are pair-wise disjoint. Thus {[0], [1], [2]} is a partition of I.

SOLVED EXAMPLES

Example 1 *Show that the relation $x \equiv y \pmod 5$ defined on the set of integers I is an equivalence relation.*

Solution : Given that the relation is $x \equiv y \pmod 5$

i.e. $(x - y)$ is divisible by 5

i.e. $(x - y) = 5k; k \in I$

i.e. $x \,R\, y : (x - y) = 5k; k \in I$

Reflexive: For all $x \in I$ we have $(x - x) = 0$

i.e. $(x - x) = 5k; k = 0 \in I$

i.e. $x \,R\, x$

i.e. R is reflexive.

Symmetric: Suppose that $x \,R\, y$

i.e. $(x - y) = 5k$

$\Rightarrow$ $(y - x) = -5k$

i.e. $(y - x) = 5(-k)$

i.e. $y \,R\, x$

So, $x \,R\, y$ implies $y \,R\, x$.

i.e. R is symmetric.

Transitive: Suppose that $x \,R\, y$ and $y \,R\, z$

i.e. $(x - y) = 5k_1$ and $(y - z) = 5k_2$; $k_1, k_2 \in I$

$\Rightarrow$ $(x - y) + (y - z) = 5\,(k_1 + k_2); (k_1 + k_2) \in I$

$\Rightarrow$ $(x - z) = 5\,(k_1 + k_2)$

i.e. $x \,R\, z$

i.e. R is transitive.

So, the relation R on I defined by $x \equiv y \pmod 5$ is an equivalence relation.

Example 2 *Is every relation which is symmetric and transitive on a set A, always reflexive? Why or why not ?*

Solution : Let R be a symmetric and transitive relation on A.

Let $x, y \in$ R and x R y

As R is symmetric, x R $y \Rightarrow y$ R x

Again x R y and y R $x \Rightarrow x$ R x [$\because$ R is transitive]

Therefore R is reflexive, but the argument is not true.

Consider an example: A = {1, 2, 3, 4, 5}

Let R be a relation defined on A such that

R = {(2, 3), (3, 4), (2, 4), (3, 2), (4, 3), (4, 2), (2, 2), (3, 3), (4, 4)}

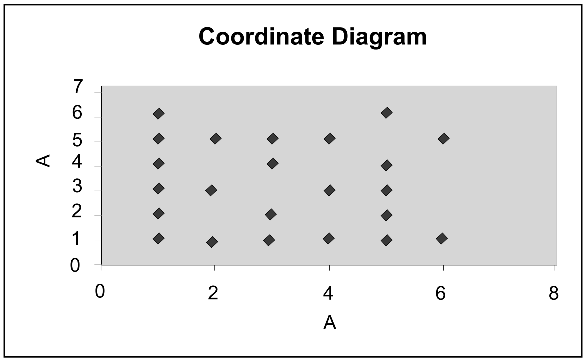
Which is symmetric and transitive but not reflexive. Therefore every relation which is symmetric and transitive on a set A is not always reflexive.

Example 3 *Let R be the relation in A = {1, 2, 3, 4, 5, 6} defined by 'x and y are relative prime'. Find the relation R and draw R on a coordinate diagram of (A ×A).*

Solution: Given A = {1, 2, 3, 4, 5, 6} and R $\subseteq$ (A $\times$ A) defined by x R y : x and y are relative prime.

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

The coordinate diagram of *R* is given below.



Example 4 *Prove that a relation R on a set A is symmetric if and only if $R^{-1} = R$.*

Solution: Suppose that a relation R on a set A is symmetric. Our claim is $R^{-1} = R$.

Let $(x, y) \in R^{-1}$

$\Rightarrow$ $(y, x) \in R$

$\Rightarrow$ $(x, y) \in R$ [$\because$ R is symmetric]

i.e. $(x, y) \in R^{-1} \Rightarrow (x, y) \in R$

i.e. $R^{-1} \subseteq R$ ... (*i*)

Again let $(x, y) \in R$

$\Rightarrow$ $(y, x) \in R$ [$\because$ R is symmetric]

$\Rightarrow$ $(x, y) \in R^{-1}$

i.e. $(x, y) \in R \Rightarrow (x, y) \in R^{-1}$

i.e. $R \subseteq R^{-1}$ ... (*ii*)

Hence we have $\qquad R = R^{-1}$

Conversely, suppose that $R = R^{-1}$.

Our claim isR on A is symmetric.

Let $(x, y) \in R \Rightarrow (y, x) \in R^{-1} = R$

i.e. R is symmetric.

Example 5 *Let N be the set of all natural numbers. R be a relation in N defined by x R y if and only if x + 3y = 12. Examine the relation for (i) reflexive, (ii) symmetric and (iii) transitive.*

Solution: Let R be a relation in N defined by

$$x \, R \, y : x + 3y = 12$$

Reflexive: Assume that $x + 3y = 12$ for $y = x$.

This implies $\qquad 4x = 12$

i.e. $\qquad x = 3$

i.e. $x \, R \, x$ for $x = 3$ only.

i.e. $\qquad x \not{R} \, x \; \forall \, x \in N$

Hence R is not reflexive.

Symmetric: Assume that $x \, R \, y$

i.e. $\qquad x + 3y = 12$

i.e.$y + 3x$ may or may not equal to 12.

i.e. $\qquad y \not{R} \, x$.

Hence R is not symmetric.

Transitive: Assume that $x \, R \, y$ and $y \, R \, z$.

i.e. $\qquad x + 3y = 12$ and $y + 3z = 12$

This holds only when $x = y = z = 3 \in N$

i.e. $\qquad x + 3z = 12$

i.e. $\qquad x \, R \, z$

So, R is transitive.

Example 6 *For a relation R on a set A = {1, 2, 3, 4, 5} given by R = {(1, 3), (1, 2), (2, 2), (3, 4)}, find reflexive closure, symmetric closure and transitive closure of R on the given set A.*

Solution: Given A = {1, 2, 3, 4, 5} and the relation

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

Therefore $\qquad r(R) = \{(1, 3),(1, 2), (1, 1), (2, 2), (3, 3),(3, 4), (4, 4),(5, 5)\}$

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

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

Example 7 *Let N be the set of all natural numbers. R be a relation in N defined by x R y if and only if x + y = 18. Show that R is symmetric but neither reflexive nor transitive.*

Solution: Let R be a relation in N defined by

$$x \, R \, y : x + y = 18$$

Reflexive: Assume that $x + y = 18$ for $y = x$

$\Rightarrow \qquad 2x = 18$

$\Rightarrow \qquad x = 9$

i.e. $x \, R \, x$ for $x = 9$ only. So, R is not reflexive.

Symmetric: Suppose that x R y

i.e. $x + y = 18$

$\Rightarrow$ $y + x = 18$

i.e. y R x, *i.e.* R is symmetric.

Transitive: Assume that x R y and y R z

i.e. $x + y = 18$ and $y + z = 18$

i.e. $(x + z)$ may or may not equal to 18.

For example let $x = 4$, $y = 14$ and $z = 4$. Hence we have $(x + y) = 18$ and $(y + z) = 18$, but $(x + z) = 8 \neq 18$

Therefore $x \not\mathrel{R} z$, *i.e.* R is not transitive.

Example 8 *A relation R defined on the set of natural numbers N by x R y if and only if (x . y) > 0 for x, y ∈ N is an equivalence relation.*

Solution: Given R be a relation in N defined by

$$x \text{ R } y : (x.\, y) > 0 \text{ for } x, y \in \text{N}$$

Reflexive: For all $x \in$ N we have

$$(x.\, x) = x^2 > 0$$

i.e. x R x. Thus R is reflexive.

Symmetric: Suppose that x R y

$\Rightarrow$ $(x\, .y) > 0$

$\Rightarrow$ $(y.\, x) > 0$

i.e. y R x

Thus R is symmetric.

Transitive: Suppose that x R y and y R z

i.e. $(x\, .y) > 0$ and $(y.\, z) > 0$

This implies $(x\, .y)\,(y.\, z) > 0$

i.e. $(x.\, z)\, y^2 > 0$

As $y^2 > 0$ for all $y \in$ N we have $(x.\, z) > 0$.

i.e. x R z

Hence x R y and y R $z \Rightarrow x$ R z

Thus R is transitive.

Therefore, the relation R in N defined by $(x.\, y) > 0$ is an equivalence relation.

Example 9 *Let A = {2, 4, 6, 8}; B = {1, 5, 7, 9} and Let R be a relation from A to B defined as x R y if and only if x ≤ y. Find the domain, range and inverse of the relation R.*

Solution: Given that A = {2, 4, 6, 8}; B = {1, 5, 7, 9} and R be a relation from A to B defined as x R y if and only if $x \leq y$.

Therefore, R = {(2, 5), (2, 7), (2, 9), (4, 5), (4, 7), (4, 9), (6, 7), (6, 9), (8, 9)}

Thus, D(R) = {2, 4, 6, 8}; R(R) = {5, 7, 9} and R^{-1} = {(5, 2), (7, 2), (9, 2), (5, 4), (7, 4), (9, 4), (7, 6), (9, 6), (9, 8)}

Example 10 *Let I be the set of all integers and R be a relation defined on I such that x R y if and only if x ≥ y. show that R is reflexive, transitive but not symmetric.*

Solution: Given R be a relation in I defined by

$$x \text{ R } y : x \geq y \text{ for } x, y \in \text{I}$$

Reflexive: For all $x \in$ I we have

$$x \geq x$$

i.e. $\quad x \text{ R } x.$

Thus R is reflexive.

Transitive:Suppose that x R y and y R z

i.e. $\quad x \geq y$ and $y \geq z$

This implies $\quad x \geq z$

i.e. $\quad x \text{ R } z$

Thus R is transitive.

Symmetric: Suppose that x R y

i.e. $\quad x \geq y$

This implies $y \not\geq x$

i.e. $\quad y \not\text{R} x$

Thus R is not symmetric.

Therefore the relation $x \geq y$ defined in I is reflexive, transitive but not symmetric.

Example 11 *Show that the relation $x \leq y$ defined on the set of integers is a partial order relation.*

Solution: Let R be a relation in I defined by

$$x \text{ R } y : x \leq y \text{ for } x, y \in \text{I}$$

Reflexive: For all $x \in$ I we have

$$x \leq x$$

i.e. $\quad x \text{ R } x.$

Thus R is reflexive.

Transitive: Suppose that x R y and y R z

i.e. $\quad x \leq y$ and $y \leq z$

This implies $\quad x \leq z$

i.e. $\quad x \text{ R } z$

Thus R is transitive.

Anti-symmetric: Suppose that x R y and y R x

i.e. $\quad x \leq y$ and $y \leq x$

This implies $x = y$

Thus R is anti-symmetric.

Therefore the relation $x \leq y$ defined in I is reflexive, transitive and anti-symmetric. So, $x \leq y$ is a partial order relation.

Example 12 *Let R be the relation on the set {1, 2, 3, 4, 5} defined by the rule (x, y) $\in$ R if $x + y \leq 6$. Find the followings.*

(*a*) List the elements of R

(*b*) List the elements of R $^{-1}$

(*c*) Domain of R

(*d*) Range of R

(*e*) Range of R $^{-1}$

(*f*) Domain of R $^{-1}$

Check that domain of R is equal to range of R $^{-1}$ and range of R is equal to domain of R $^{-1}$.

Solution: Let A = {1, 2, 3, 4, 5} and R = $\{(x, y) \in R \mid x + y \leq 6 ; x, y \in A\}$

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

(*b*) R^{-1} = {(1, 1), (2, 1), (3, 1), (4, 1), (5, 1), (1, 2), (2, 2), (3, 2), (4, 2), (1, 3), (2, 3), (3, 3), (1, 4), (2, 4), (1, 5)}

(*c*) Domain of R *i.e.* D(R) = {1, 2, 3, 4, 5}

(*d*) Range of R *i.e.* R(R) = {1, 2, 3, 4, 5}

(*e*) Range of R^{-1} *i.e.* $R(R^{-1})$ = {1, 2, 3, 4, 5}

(*f*) Domain of R^{-1} *i.e.* $D(R^{-1})$ = {1, 2, 3, 4, 5}

From this it is clear that D(R) = $R(R^{-1})$ and R(R) = $D(R^{-1})$.

Example 13 *Consider a relation R on {1, 2, 3, 4} as R = {(1, 3), (1, 4), (2, 2), (3, 3), (4, 1)}. Examine the relation for reflexive, symmetric and transitive with the help of relation matrix.*

Solution: Given that the relation R = {(1, 3), (1, 4), (2, 2), (3, 3), (4, 1)}. Relative to the ordering 1, 2, 3, 4 we get

$$M(R) = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

From the above matrix it is clear that $m_{11} \neq 1$ and $m_{44} \neq 1$. So, the relation R is not reflexive. Again R is not symmetric because

$$[M(R)]^T = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \neq M(R)$$

Also we have

$$[M(R)]^2 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

From this it is clear that the 1st row and 1st column entry in $[M(R)]^2$ is non-zero where as the 1st row and 1st column entry in M(R) is zero. Therefore the relation R is not transitive. Hence the relation R is neither reflexive nor symmetric and transitive.

Example 14 *Let A = {1, 2, 3, 4, 5}; B = {a, b, c, d} and C = {1, 4, 9, 16, 25}. Consider the relations R_1 from A to B and R_2 from B to C as R_1 = {(1, a), (1, b), (2, c), (2, d), (3, b), (5, d)} and R_2 = {(a, 1), (d, 4), (b, 9), (d, 25)}. Find the composition R_1R_2 with the help of relation matrix.*

Solution: Let A = {1, 2, 3, 4, 5}; B = {*a*, *b*, *c*, *d*} and C = {1, 4, 9, 16, 25}. Given $R_1 \subseteq (A \times B)$ and $R_2 \subseteq (B \times C)$ with

$$R_1 = \{(1, a), (1, b), (2, c), (2, d), (3, b), (5, d)\}$$

and $$R_2 = \{(a, 1), (d, 4), (b, 9), (d, 25)\}.$$

Therefore we get

$$M(R_1) = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \text{ and } M(R_2) = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

So, $$M(R_1R_2) = M(R_1)M(R_2)$$

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

Thus R_1R_2 = {(1, 1), (1, 9), (2, 4), (2, 25), (3, 9), (5, 4), (5, 25)}

Example 15 *Let R_1 and R_2 be the relations on {1, 2, 3, 4} given by R_1={(1, 1), (1, 2), (3, 4), (4, 2)}and R_2 = {(1, 1), (2, 1), (3, 1), (4, 4), (2, 2)} List the elements of R_1R_2 and R_2R_1. Show that $R_1R_2 \neq R_2R_1$.*

Solution: Given R_1 and R_2 be relations on {1, 2, 3, 4} as

R_1 = {(1, 1), (1, 2), (3, 4), (4, 2)} and R_2 ={(1, 1), (2, 1), (3, 1), (4, 4), (2, 2)} Relative to the ordering {1, 2, 3, 4} we have

$$M(R_1) = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix} \text{and } M(R_2) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Therefore $M(R_1R_2) = M(R_1)\, M(R_2)$

$$= \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}$$

Replacing all non-zero entries by 1 in $M(R_1R_2)$ we have $M(R_1R_2) = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}$

i.e. R_1R_2 = {(1, 1), (1, 2), (3, 4), (4, 1), (4, 2)}

Similarly, $M(R_2R_1) = M(R_2)\, M(R_1)$

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

i.e. R_2R_1 = {(1, 1), (1, 2), (2, 1), (2, 2), (3, 1), (3, 2), (4, 2)}

Therefore $R_1R_2 \neq R_2R_1$

Example 16 *Let R be the relation on the set {1, 2, 3, 4, 5} defined by the rule (x, y) ∈ R if x = y – 1. Find R in terms of relation matrix. Check the relation R for symmetric and irreflexive.*

Solution: Let A = {1, 2, 3, 4, 5}

and R = {(x, y): $x = y - 1$ $x, y \in$ A}

i.e. R = {(1, 2), (2, 3), (3, 4), (4, 5)}

Relative to the ordering {1, 2, 3, 4, 5} we have

$$M(R) = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Now,
$$[\mathrm{M(R)}]^{\mathrm{T}} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix} \neq \mathrm{M(R)}$$

So, R is not symmetric. It is clear that R is irreflexive as $m_{ii} = 0$ for all $1 \leq i = 5$. Therefore, R is irreflexive but not symmetric.

Example 17 *Let R and S be the following relations on A = {2, 4, 5, 6}. R = {(2, 4), (2, 5), (2, 6), (4, 2), (4, 4)} and S = {(5, 4), (5, 5), (5, 6), (6, 2), (6, 4)}. Find $(R \cup S)^c$ and R^2.*

Solution: Given R = {(2, 4), (2, 5), (2, 6), (4, 2), (4, 4)} and S = {(5, 4), (5, 5), (5, 6), (6, 2), (6, 4)}

(*i*) $(R \cup S)$ = {(2, 4), (2, 5), (2, 6), (4, 2), (4, 4), (5, 4), (5, 5), (5, 6), (6, 2), (6, 4)}
This implies $(R \cup S)^c$ = {(2, 2), (4, 5), (4, 6), (5, 2), (6, 5), (6, 6)}

(*ii*) Relative to the ordering 2, 4, 5, 6 we have

$$\mathrm{M(R)} = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

So, $\mathrm{M(R^2)} = \mathrm{M(R)\,M(R)}$

$$= \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 2 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Replacing all non-zero entries by 1 in $\mathrm{M(R^2)}$ we get

$$\mathrm{M(R^2)} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

So, R^2 = {(2, 2), (2, 4), (4, 2), (4, 4), (4, 5), (4, 6)}

Example 18 *Let R be the relation on the set {2, 3, 4, 5, 6} defined by the rule (x, y) ∈ R if $x + 2y \leq 12$. Find the relation R. Also find the reflexive, symmetric and transitive closure of R.*

Solution: Let A = {2, 3, 4, 5, 6} and R = {$(x, y) \in$ R if $x + 2y \leq 12$; $x, y \in$ A}

i.e. R = {(2, 2), (2, 3), (2, 4), (2, 5), (3, 2), (3, 3), (3, 4), (4, 2), (4, 3), (4, 4), (5, 2), (5, 3), (6, 2), (6, 3)}

The reflexive closure of R *i.e.* r(R) = {(2, 2), (2, 3), (2, 4), (2, 5), (3, 2), (3, 3), (3, 4), (4, 2), (4, 3), (4, 4), (5, 2), (5, 3), (5, 5), (6, 2), (6, 3), (6, 6)}

The symmetric closure of R *i.e.* s(R) = {(2, 2), (2, 3), (2, 4), (2, 5), (2, 6), (3, 2), (3, 3), (3, 4), (3, 5), (3, 6), (4, 2), (4, 3), (4, 4), (5, 2), (5, 3), (6, 2), (6, 3)}

The transitive closure of R *i.e.* t(R) = {(2, 2), (2, 3), (2, 4), (2, 5), (3, 2), (3, 3), (3, 4), (4, 2), (4, 3), (4, 4), (5, 2), (5, 3), (6, 2), (6, 3), (3, 5), (4, 5), (5, 4), (5, 5), (6, 4), (6, 5)}

Example 19 *Let R be the relation in the integers I defined by (x – y) is an even integer. Prove that R is an equivalence relation and find the disjoint equivalence classes.*

Solution: Let R be the relation in the integers I defined by $(x - y)$ is an even integer. *i.e.* $(x - y)$ is divisible by 2.

Reflexive: For all $x \in$ I we have $(x - x) = 0$

i.e. $(x - x) = 2k;\ k = 0 \in \mathrm{I}$

i.e. $x \,\mathrm{R}\, x \ \forall\, x \in \mathrm{I}$

i.e. R is reflexive.

Symmetric: Suppose that x R y

i.e. $(x - y)$ is divisible by 2

i.e. $(x - y) = 2k; k \in \mathrm{I}$

$\Rightarrow$ $(y - x) = 2(-k); -k \in \mathrm{I}$

i.e. y R x

Thus R is symmetric.

Transitive: Suppose that x R y and y R z

i.e.$(x - y)$ and $(y - z)$ are even integer.

i.e. $(x - y) = 2k_1$ and $(y - z) = 2k_2$; $k_1, k_2 \in \mathrm{I}$.

$\Rightarrow$ $(x - y) + (y - z) = 2(k_1 + k_2); (k_1 + k_2) \in \mathrm{I}$

i.e. $(x - z)$ is an even integer.

i.e. x R z

Thus R is transitive.

Therefore the relation R on I defined by $(x - y)$ is even integer is an equivalence relation. The disjoint equivalence classes are

$$[0] = \{\ldots.. , -4, -2, 0, 2, 4, 6, \ldots.\}$$
$$[1] = \{\ldots.. , -3, -1, 1, 3, 5, 7, \ldots\ldots\}$$

Example 20 *Let R be a relation defined in A = {1, 2, 3, 5, 7, 9} as R = {(1, 1), (1, 3), (1, 5), (1, 7), (3, 1), (3, 3), (3, 5), (3, 7), (5, 1), (5, 3), (5, 5), (5, 7), (7, 1), (7, 3), (7, 5), (7, 7), (9, 9), (2, 2)}. Find the partitions of A based on the equivalence relation R.*

Solution: Given A = {1, 2, 3, 5, 7, 9} and

R = {(1, 1), (1, 3), (1, 5), (1, 7), (3, 1), (3, 3), (3, 5), (3, 7), (5, 1), (5, 3), (5, 5), (5, 7), (7, 1), (7, 3), (7, 5), (7, 7), (9, 9), (2, 2)}

The disjoint equivalence classes are

$$[1] = \{1, 3, 5, 7\}; [9] = \{9\} \text{ and } [2] = \{2\}.$$

Obviously

(*i*) The sets [1], [2] and [9] are non-empty

(*ii*) $[1] \cap [2] = \phi$; $[1] \cap [9] = \phi$ and $[2] \cap [9] = \phi$

(*iii*) $[1] \cup [2] \cup [9] = \mathrm{A}$

Hence { [1], [2], [9]} is a partition of A.

Example 21 *Find the number of relations from the set A to the set B if* $|A| = m$ *and* $|B| = n$.

Solution: Given $|\mathrm{A}| = m$ and $|\mathrm{B}| = n$

Therefore $|\mathrm{A} \times \mathrm{B}| = mn$.

A relation R from the set A to the set B is a subset of (A × B). So, the number of subsets of (A × B) is equal to 2^{mn}. Therefore total number of relations from the set A to the set B is 2^{mn}.

EXERCISES

1. Let A = $\{p, q, r, s\}$ and R be an universal relation on A. Write down the relation R. Find out the smallest and largest subset of the universal relation which is an equivalence relation.

2. Let A = {1, 2, 3, 4, 5} and B = {1, 2, 4, 6, 7}. Find the relation from A to B defined by

(*a*) Greater then (*b*) Less then

(*c*) Greater then equal to (*d*) Less then equal to

(*e*) Equal to.

3. For the above No. 2, determine the domains and ranges of each of the cases.

4. For the above No. 2, determine the inverse relation in each of the above cases.

5. Prove that the relation $x \equiv y$ mod(3) on the set of integers Z is an equivalence relation.

6. Give an example of a relation which is

(*a*) Reflexive, Symmetric but not Transitive.

(*b*) Reflexive, Transitive but not Symmetric.

(*c*) Symmetric, Transitive but not Reflexive.

(*d*) Reflexive but not Symmetric and Transitive.

(*e*) Symmetric but not Reflexive and Transitive.

(*f*) Transitive but not Reflexive and Symmetric.

(*g*) Neither Reflexive nor Symmetric and Transitive.

(*h*) Reflexive, Symmetric and Transitive.

(*i*) Symmetric and Anti-symmetric.

(*j*) Anti-symmetric but not Reflexive.

7. Prove that the relation on the set of natural numbers N determined by x R y if and only if x divides y is reflexive, transitive but not symmetric.

8. Consider the relations R_1 and R_2 on $\{a, b, c, d, e\}$ as $R_1 = \{(a, b), (a, c), (b, b), (c, d), (c, c), (c, e)\}$ and $R_2 = \{(a, a), (a, d), (d, b), (d, e), (d, d), (e, c)\}$. Find the reflexive, symmetric and transitive closures of R_1 and R_2.

9 Write the following relations as a table

(*a*) $R_1 = \{(1, 1), (2, 4), (3, 9), (4, 16), (6, 36), (7, 49)\}$

(*b*) $R_2 = \{(2, 5), (5, 8), (8, 11), (11, 14)\}$

(*c*) $R_3 = \{(8, i), (1, l), (4, o), (1, v), (4, e), (0, u)\}$

(*d*) R_4 = {(Bapa, Comp. Sc.), (Megha, Math), (Suni, Math)}

10. Let R be the relation in the natural numbers N defined by $(a - b)$ is divisible by 8. Show that R is an equivalence relation.

11. Let L be the set of lines in the Euclidean plane and let R be the relation in L defined by l_1 R l_2 if and only if l_1 is parallel to l_2. Show that R is an equivalence relation.

12. Write the following relations as a set of order pairs.

(*a*)

Cloth Material	*Price in Rupees*
Cotton	55
Teri cot	60
Woolen	50
Fancy	45

(*b*)

Names	*Course*
Aditi	Comp. Sc.
Sudeep	Math
Sudeep	Comp. Sc.
Amita	Chemistry
Ashima	Economics

(*c*)

Number	*Square*
5	25
4	16
3	9
2	4
1	1

(*d*)

Alphabet	*Number*
a	1
c	3
e	5
z	26
m	13

13. Let A = {5, 6, 7, 8, 9}; B = {x, y, z, p, q, r}; C = {5, 7, 25, 36, 81} and let R_1 = {(5, p), (5, r), (6, z), (7, y), (9, x), (9, z)} and R_2 = { (p, 25), (x, 81), (z, 36), (y, 7), (r, 5)}. Find the composition R_1R_2 with the help of relation matrix.

14. For the relation R on the set {5, 6, 7, ,8, 9} defined by the rule (x, y) if $x + 2y \leq 20$. Find the followings.

(*a*) Elements of R (*b*) Elements of R^{-1}

(*c*) Domain of R (*d*) Range of R

15. Let S = {1, 2, 3, 4, 5} and let R be a relation defined by a rule (x, y) if $(x - y)$ is an even natural number. Find the followings.

(*a*) Elements of R (*b*) Inverse relation of R

(*c*) Domain of R (*d*) Range of R^{-1}.

16. Let R be a relation defined on the set S = {1, 2, 3, 4, 5} by a rule (x, y) if $x^2 + y^2 \leq 16$. Find the reflexive, symmetric and transitive closures of R.

17. Let R be a relation on {a, b, c, d} defined as R = {(a, a), (a, b), (a, c), (b, a), (b, b), (b, c), (c, a), (c, b), (c, c), (d, d)}. Show that the relation R is an equivalence relation using relation matrix.

18. Let N be the set of all natural numbers. Define a relation R in N by x R y if and only if $(x - y) = 34$. Show that R is anti-symmetric.

19. Let R be a relation defined by a rule A R B if and only if $A \subseteq B$. Show that R is a partial order relation.

20. Test the following relations on N for being reflexive, symmetric and transitive. Let $x, y \in$ N.

(*a*) $x + y$ is even (*b*) $\frac{x}{y}$ is a power of 2.

(*c*) $x + y \leq 20$

21. Examine the following relations on the set of integers I for partial order relations. Let $(x, y) \in$ R if and only if

(*a*) $x = y$ (*b*) $x \geq y$

(*c*) $x = y^2$ (*d*) $x < y$.

22. Let R_1 and R_2 be relations on the set S. Show that $(R_1 \cup R_2)$ is reflexive if both R_1 and R_2 are reflexive.

23. Let R_1 be an anti-symmetric relation on the set S. Prove that R^{-1} is also an anti-symmetric relation on the set S.

24. Show that if R_1 and R_2 be transitive relations on a set A, then $(R_1 \cup R_2)$ is not necessarily transitive on A.

25. Find the equivalence classes determined by the equivalence relation R on Z defined by a R b if and only if $a \equiv b$ mod (5) for $a, b \in$ Z.

26. Sketch each of the following relations on R.

(*a*) $x^2 + y^2 < 25$ (*b*) $x^2 + 4y^2 = 16$

(*c*) $x^2 - 4y^2 = 16$ (*d*) $3x + 2y \geq 6$

27. Let R be a relation in the natural number N defined by a R b if and only if 'a is a multiple of b' for $a, b \in$ N. Examine the above relation for reflexive, symmetric, anti-symmetric, transitive and anti-reflexive.

28. Let R be a relation in the natural number N defined by x R y if and only if '$x^2 = y^2$' for x, $y \in$ N. Examine the above relation for reflexive, symmetric, anti-symmetric, transitive and partial order.

29. Let A be the set of non zero integers and R be a relation in A defined by (a, b) R (c, d) if and only if $a + d = b + c$. Prove that R is an equivalence relation.

30. Let A be the set of non-zero integers and R be a relation in A defined by (a, b) R (c, d) if and only if $ad = bc$. Show that R is an equivalence relation.

4

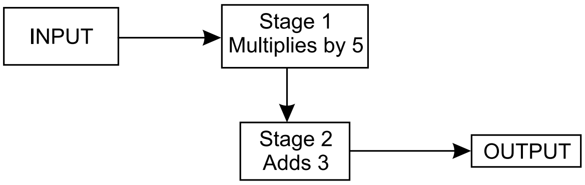
Function

■ 4.0 INTRODUCTION

One of the most important concepts in mathematics is that of a function. It is being used in our day- to-day life. At every moment by knowingly or unknowingly.

German Mathematician Leibniz was first to use the term function (1646 –1716). The terms mapping, map and transformation mean the same thing. Computer Science has many applications of function. Hashing function is one of that.

Consider a computing device that accepts any real number, multiplies it by 5 and adds 3 with the product, and gives the output.



(Computing Devise)

If the input is 1, then the out put is 8. If the input is $\frac{1}{5}$, then the output is 4. If the input is 10, then the out put is $(10 \times 5 + 3) = 53$. This clear indicates that if the input is x, $x \in$ R, then the out put is $(5x + 3)$. As a result the computing device pairs off the element $x \in$ R as $(x, 5x + 3)$ in a definite way or principle. This is nothing but a function.

■ 4.1 FUNCTION

Let A and B be two non-empty sets. A relation f from the set A to the set B is said to be a function if it satisfies the following two conditions.

(*i*) $D(f) = A$ and

(*ii*) if $(x_1, y_1) \in f$ and $(x_2, y_2) \in f$ then $y_1 = y_2$.

In other words a relation f from the set A to the set B is said to be a function if for each element x in A there exists unique element y in B. A function from A to B is some times denoted as $f : \text{A} \to \text{B}$.

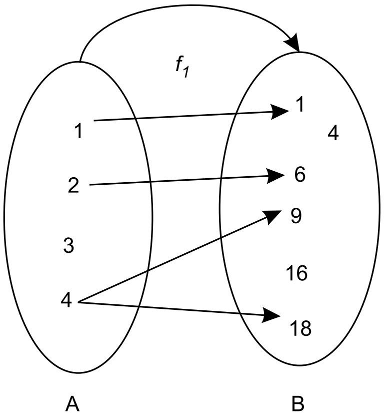
Consider the following relations from the set A = {1, 2, 3, 4} to the set B = {1, 4, 6, 9, 16, 18}.

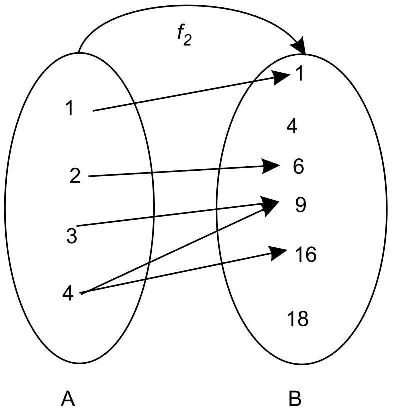
$$f_1 = \{(1, 1), (2, 6), (4, 9), (4, 18)\}$$
$$f_2 = \{(1, 1), (2, 6), (3, 9), (4, 9), (4, 16)\}$$
$$f_3 = \{(1, 1), (2, 4), (3, 9), (4, 16)\}$$
and $$f_4 = \{(1, 1), (2, 4), (3, 9), (4, 9)\}$$

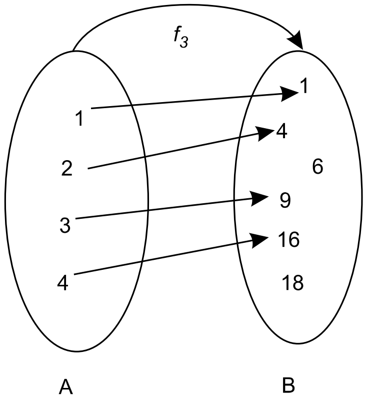
Now, $D(f_1) = \{1, 2, 4\} \neq A$. Therefore f_1 is not a function from the set A to the set B. Further $D(f_2) = \{1, 2, 3, 4\} = A$; but $(4, 9) \in f_2$ and $(4, 16) \in f_2$ with $9 \neq 16$. This implies f_2 can not be a function from the set A to the set B.

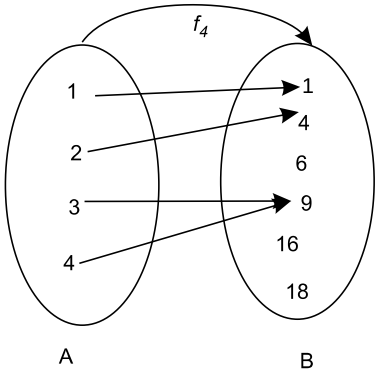
Again $D(f_3) = \{1, 2, 3, 4\} = A$ and for every element $x \in A$ there exists unique $y \in B$. Therefore f_3 is a function from the set A to the set B. Similarly f_4 is also a function. The arrow diagrams are given below.

Note: From the above discussions it is clear that One-Many and Many-Many relations are not functions.









4.1.1 Domain and Co-domain of a Function

Suppose that f be a function from the set A to the set B. The set A is called the domain of the function f where as the set B is called the co-domain of the function f.

Consider the function f from the set A = $\{a, b, c, d\}$ to the set B = $\{1, 2, 3, 4\}$ as

$$f = \{(a, 1), (b, 2), (c, 2), (d, 4)\}$$

Therefore, domain of $f = \{a, b, c, d\}$ and co-domain of $f = \{1, 2, 3, 4\}$. *i.e.* $D(f) = \{a, b, c, d\}$ and Co-domain $f = \{1, 2, 3, 4\}$.

4.1.2 Range of a Function

Let f be a function from the set A to the set B. The element $y \in$ B which the function f associates to an element $x \in$ A is called the image of x or the value of the function f for x. From the definition of function it is clear that each element of A has an unique image on B. Therefore the range of a function $f : A \to B$ is defined as the image of its domain A. Mathematically,

$$R(f) \text{ or rng } (f) = \{y = f(x) : x \in A\}$$

It is clear that $R(f) \subseteq B$.

Consider the function f from A = $\{a, b, c\}$ to B = $\{1, 3, 5, 7, 9\}$ as $f = \{(a, 3), (b, 5), (c, 5)\}$. Therefore $R(f) = \{3, 5\}$.

4.2 EQUALITY OF FUNCTIONS

If f and g are functions from A to B, then they are said to be equal *i.e.* $f = g$ if the following conditions hold.

(*a*) $D(f) = D(g)$

(*b*) $R(f) = R(g)$

(*c*) $f(x) \neq g(x)\ \forall\, x \in A$.

Consider $f(x) = 3x^2 + 6 : R \to R$ and $g(x) = 3x^2 + 6 : C \to C$, where R and C are the set of real numbers and complex numbers respectively. Now it is clear that $D(f) \neq D(g)$. Therefore $f(x) \neq g(x)$.

Let us consider A = $\{1, 2, 3, 4\}$; B = $\{1, 2, 7, 8, 17, 18, 31, 32\}$ and the function $f : A \to B$ defined by $f = \{(1, 2), (2, 8), (3, 18), (4, 32)\}$. Consider another function $g : A \to N$ defined by $g(x) = 2x^2$. Now it is clear that $D(f) = \{1, 2, 3, 4\}$ with $f(1) = 2, f(2) = 8, f(3) = 18, f(4) = 32$. Similarly $D(g) = A = \{1, 2, 3, 4\}$ with $g(1) = 2, g(2) = 8, g(3) = 18, g(4) = 32$. Therefore, we get

(*a*) $D(f) = \{1, 2, 3, 4\} = D(g)$

(*b*) $R(f) = \{2, 8, 18, 32\} = R(g)$ and

(*c*) $f(x) = g(x)\ \forall\, x \in \{1, 2, 3, 4\}$.

This implies f and g are equal. *i.e.* $f = g$.

4.3 TYPES OF FUNCTION

In this section we will discuss different types of function.

4.3.1 One-One Function

A function $f : A \to B$ is said to be an One–One function or Injective if $f(x_1) = f(x_2)$, then $x_1 = x_2$ for $x_1, x_2 \in$ A. *i.e.* $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$

Consider a function $f : Q \to Q$ defined by $f(x) = 4x + 3; x \in Q$.

Suppose that $f(x_1) = f(x_2)$ for $x_1, x_2 \in$ Q.

$$\Rightarrow \quad 4x_1 + 3 = 4x_2 + 3$$

$$\Rightarrow \quad 4x_1 = 4x_2$$

$$\Rightarrow \quad x_1 = x_2$$

i.e. $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$. So, $f(x) = (4x + 3) : \mathrm{Q} \to \mathrm{Q}$ is One-One.

Consider another function $f : \mathrm{R} \to \mathrm{R}$ defined by $f(x) = x^2$; $x \in$ R. Suppose that $f(x_1) = f(x_2)$

$$\Rightarrow \quad {x_1}^2 = {x_2}^2$$

$$\Rightarrow \quad x_1 = \pm x_2$$

$$\Rightarrow \quad x_1 \neq x_2$$

i.e. $f(x_1) = f(x_2) \Rightarrow x_1 \neq x_2$. It is also clear that $f(1) = 1 = f(-1)$; but $1 \neq -1$. Therefore $f(x) = x^2$: $\mathrm{R} \to \mathrm{R}$; $x \in$ R is not One-One.

4.3.2 Onto Function

A function f: $\mathrm{A} \to \mathrm{B}$ is said to be an onto function or Surjective if for every $y \in$ B there exists at least one element $x \in$ A such that $f(x) = y$.

In other words a function $f : \mathrm{A} \to \mathrm{B}$ is said to be an Onto function if $f(\mathrm{A}) = \mathrm{B}$. *i.e.* range of f is equal to co-domain of f.

Consider a function f: $\mathrm{Q} \to \mathrm{Q}$ defined by $f(x) = 4x + 3, x \in$ Q. Then for every $y \in$ co-domain set Q there exists $x = \dfrac{y-3}{4}$ belongs to domain set Q. Therefore $f(x) = 4x + 3$ is an Onto function.

4.3.3 One-One Onto Function

A function $f : \mathrm{A} \to \mathrm{B}$ is said to be an One-One Onto function or Bijective if f is both One-One and Onto function.

Consider a function f : $\mathrm{Q} \to \mathrm{Q}$ defined by $f(x) = 4x + 3, x \in$ Q. From the above discussions it is clear that $f(x) = 4x + 3$, $x \in$ Q is an One-One Onto function.

4.3.4 Into Function

A function $f : \mathrm{A} \to \mathrm{B}$ is said to be an into function if for at least one $y \in$ B there exists no element $x \in$ A such that $f(x) = y$. In other words

A function $f : \mathrm{A} \to \mathrm{B}$ is said to be an into function if $f(\mathrm{A}) \subset \mathrm{B}$, *i.e.* range of f is a proper subset of co-domain of f.

Consider a function f : $\mathrm{Q} \to \mathrm{R}$ defined by $f(x) = x + 4, x \in$ Q. Hence it is clear that for $y = \sqrt{3} \in$ R there exists no element $x = \sqrt{3} - 4 \in$ Q. Therefore, $f(x) = x + 4 : \mathrm{Q} \to \mathrm{R}$ is an into function.

■ 4.4 GRAPH OF FUNCTION

Let f be a function from A to B, *i.e.* for every $x \in$ A there exists unique $y \in$ B such that $y = f(x)$. Further note that using the functional notation, f can be expressed as

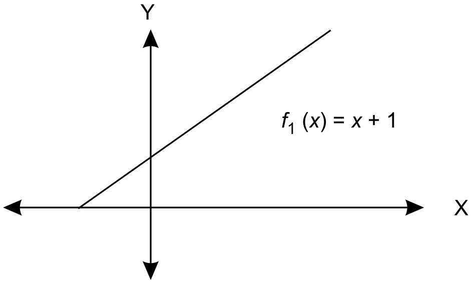
$$f = \{(x, f(x)) : x \in \mathrm{A}\}.$$

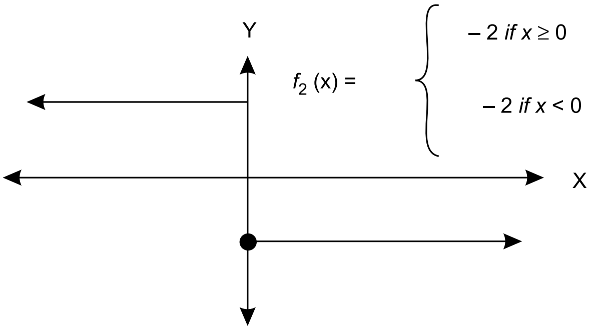
This representation is known as the graph of the function f .

Consider the functions $f_1 : \mathrm{R} \to \mathrm{R}$ defined by $f_1(x) = x + 1$; and

$f_2 : \text{R} \rightarrow \{-2, 2\}$ defined by $f_2(x) = \begin{cases} -2 & \text{if } x > 0 \\ 2 & \text{if } x < 0 \end{cases}$

The graphs of above functions are given below.





Now consider the relations $f_1 : [-4, 4] \rightarrow [-4, 4]$ defined by $[f_1(x)]^2 = 16 - x^2$; $x \in [-4, 4]$ and $f_2 : \text{R} \rightarrow \text{R}$ defined by $[f_2(x)]^2 = 16x$; $x \in \text{R}$. The graphs of above relations are given below.

These are nothing but a circle and parabola respectively. Where in figure – 1, $y = f_1(x)$ and in figure – 2, $y = f_2(x)$.

From the graph it is clear that for one value of x in the domain set leads to two values in the range set. Hence these relations are not functions.

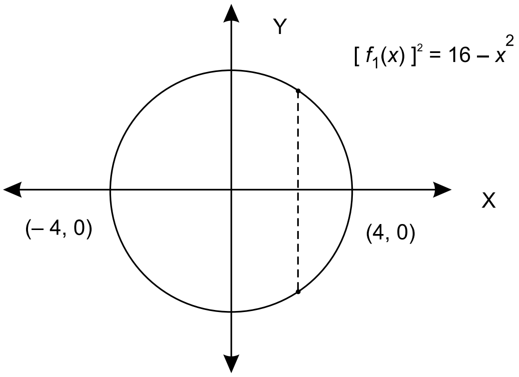
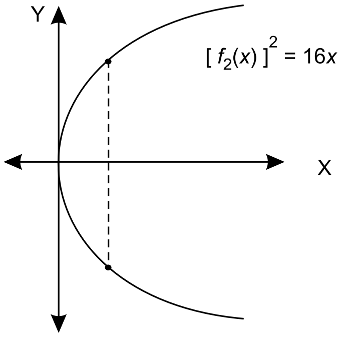
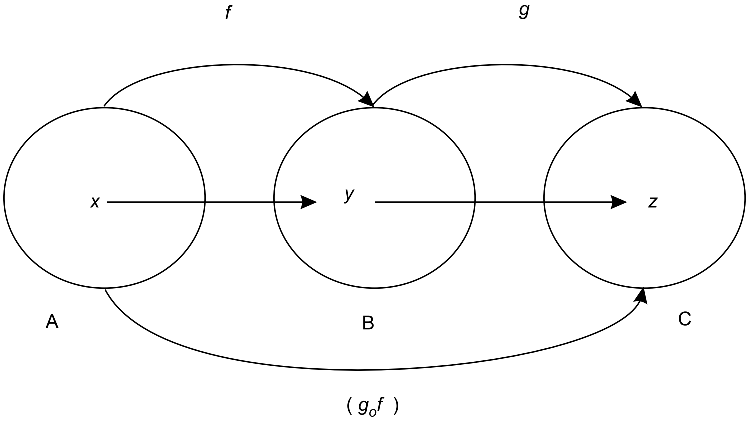


Figure – 1



■ 4.5 COMPOSITION OF FUNCTIONS

Let f be a function from the set A to the set B and g be a function from the set B to the set C. Then the composition of the functions f and g is given as $(g_{\,0} f)$ or gf. This is a function from the set A to the set C. It may also be noted that domain of g is equal to co-domain of f.



As f is a function from the set A to the set B, then for every $x \in$ A there exists unique $y \in$ B such that $y = f(x)$. Similarly g is a function from the set B to the set C, then for every $y \in$ B there exists unique $z \in$ C such that $z = g(y)$. Again $(g_{\,0} f)$ is a function from the set A to the set C, so we get $(g_{\,0} f)(x) = z$ for all $x \in$ A.

i.e. $(g_{\,0} f)(x) = g(y)$

i.e. $(g_{\,0} f)(x) = g(f(x))$

Consider two functions $f(x) = 2x + 5$ and $g(x) = 3x$.

Therefore $(g_{\,0} f)(x) = g(f(x))$

$$= g(2x + 5)$$
$$= 3(2x + 5)$$

i.e. $(g_{\,0} f)(x) = 6x + 15$

Similarly, $(f_{\,0} g)(x) = f(g(x))$

$$= f(3x)$$

$$= 2(3x) + 5$$

i.e. $(f\ {}_o g)\ (x) = 6x + 5$

4.5.1 Theorem

Let $f : \text{A} \to \text{B}$ and $g : \text{B} \to \text{C}$ be two functions. Then $(g\ {}_o f)$ is one-one if both f and g are one-one and $(g\ {}_o f)$ is onto if both f and g are onto.

Proof : Let $f : \text{A} \to \text{B}$ and $g : \text{B} \to \text{C}$ be two functions. Since f is a function from the set A to the set B, then for every $x \in \text{A}$ there exists unique $y \in \text{B}$ such that $y = f(x)$. Similarly g is a function from the set B to the set C, then for every $y \in \text{B}$ there exists unique $z \in \text{C}$ such that $z = g(y)$.

Suppose the f and g are both one-one. Our claim is $(g\ {}_o f)$ is one-one. Since $f : \text{A} \to \text{B}$ and $g : \text{B} \to \text{C}$ we have $(g\ {}_o f) : \text{A} \to \text{C}$.

Let $x_1, x_2 \in \text{A}$ and $(g\ {}_o f)\ (x_1) = (g\ {}_o f)\ (x_2)$

This implies $g(f(x_1)) = g(f(x_2))$

i.e. $f(x_1) = f(x_2)$ [$\because$ g is one-one]

i.e. $x_1 = x_2$ [$\because f$ is one-one]

Therefore $g(f(x_1)) = g(f(x_2))$ implies $x_1 = x_2$. So $(g\ {}_o f)$ is one-one.

Suppose that both f and g are onto. Since g is onto, for every $z \in \text{C}$ there is at least one $y \in \text{B}$ such that $g(y) = z$. Again as f is onto, for every $y \in \text{B}$ there exists at least one $x \in \text{A}$ such that $f(x) = y$.

As a result for every $z \in \text{C}$ there is at least one $x \in \text{A}$ such that $(g\ {}_o f)\ (x) = z$. Therefore $(g\ {}_o f)$ is onto.

4.5.2 Theorem

If $f : \text{A} \to \text{B}$; $g : \text{B} \to \text{C}$ and $h : \text{C} \to \text{D}$, then $h\ {}_o (g\ {}_o f) = (h\ {}_o g)\ {}_o f$, *i.e.* composition of functions holds the associative law.

Proof : Let $f : \text{A} \to \text{B}$, $g : \text{B} \to \text{C}$ and $h : \text{C} \to \text{D}$ be three functions. So, $(g\ {}_o f) : \text{A} \to \text{C}$. Therefore $h\ {}_o (g\ {}_o f) : \text{A} \to \text{D}$.

Further $(h\ {}_o g) : \text{B} \to \text{D}$. So, $(h\ {}_o g)\ {}_o f : \text{A} \to \text{D}$. Therefore both $h\ {}_o (g\ {}_o f)$ and $(h\ {}_o g)\ {}_o f$ are functions from $\text{A} \to \text{D}$.

Since $f : \text{A} \to \text{B}$, then for every $x \in \text{A}$ there exists unique $y \in \text{B}$ such that $f(x) = y$. Further $g : \text{B} \to \text{C}$, then for every $y \in \text{B}$ there exists unique $z \in \text{C}$ such that $g(y) = z$. Again $h : \text{C} \to \text{D}$, then for every $z \in \text{C}$ there exists unique $t \in \text{D}$ such that $h(z) = t$.

Then $h\ {}_o (g\ {}_o f)\ (x) = h\ (g\ {}_o f(x))$

$$= h\ (g\ (f(x)))$$

$$= h\ (g\ (y)) = h\ (z) = t.$$

Further, $(h\ {}_o g)\ {}_o f(x) = (h\ {}_o g)(f(x))$

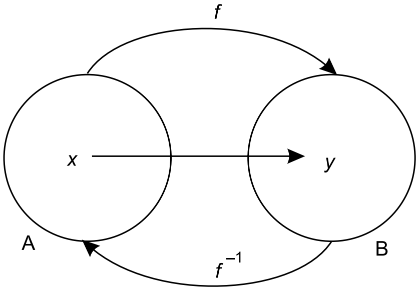
$$= (h\ {}_o g)\ (y)$$

$$= h\ (g\ (y)) = h\ (z) = t.$$

Therefore for $x \in \text{A}$ we have $h\ {}_o (g\ {}_o f)\ (x) = (h\ {}_o g)\ {}_o f(x)$ for all $x \in \text{A}$. *i.e.* $h\ {}_o (g\ {}_o f) = (h\ {}_o g)\ {}_o f$.

■ 4.6 INVERSE FUNCTION

Let $f : A \to B$ be a bijective function. Then the inverse of f, *i.e.* f^{-1} be a function from B to A. Since f is a function from A to B, for every $x \in A$, there exists unique $y \in B$ such that $f(x) = y$.



Since $f^{-1} : B \to A$ for every $y \in B$ there exists unique $x \in A$ such that $f^{-1}(y) = x$, *i.e.* $f^{-1}(f(x)) = x$.

4.6.1 Theorem

If $f : A \to B$ is bijective, then the function f posses inverse mapping.

Proof : Suppose that $f : A \to B$ is not bijective and posses an inverse mapping, *i.e.* (*i*) f is onto but not one-one. (*ii*) f is one-one but not onto or (*iii*) f is neither one-one nor onto.

Case (*i*) Suppose that f is onto but not one-one.

As f is onto, so for every $y_1 \in B$ there exists at least one $x_1 \in A$ such that $f(x_1) = y_1$ and $R(f) = B$. Again as f is not one-one we have $x_1 \neq x_2$, $x_1, x_2 \in A$ implies $y_1 = f(x_1) = f(x_2) = y_2$.

Since $f^{-1} : B \to A$, so $D(f^{-1}) = R(f) = B$, *i.e.* $D(f^{-1}) = B$. Also (x_1, y_1), $(x_2, y_2) \in f$ implies (y_1, x_1), $(y_2, x_2) \in f^{-1}$ with $x_1 \neq x_2$ as $y_1 = y_2$. Hence f^{-1} can not be a function.

Case (*ii*) Suppose that f is one-one but not onto.

As f is not onto, so for at least one $y_1 \in B$ there exists no $x_1 \in A$ such that $f(x_1) = y_1$ and $R(f) \neq B$. Since, $f^{-1} : B \to A$, so

$D(f^{-1}) = R(f) \neq B$, *i.e.* $D(f^{-1}) \neq B$. Hence f^{-1} can not be a function.

Case (*iii*) Similarly it can be proved that f^{-1} can not be a function if f is neither onto nor one-one.

Therefore, it is a contradiction. So our supposition is wrong. Hence $f : B \to A$ must be bijective to posses a inverse mapping.

4.6.2 Theorem

Let $f : A \to B$ and $g : B \to C$ be two functions. If both f and g are invertible, then $(g \,_0 f)^{-1} = f^{-1} \,_0 g^{-1}$.

Proof : Suppose that both f and g are invertible. This indicates that both f and g are bijective functions. So by theorem 4.5.1, $(g \,_0 f)$ is also bijective and hence invertible.

As $f : A \to B$ and $g : B \to C$ we have $(g \,_0 f) : A \to C$ *i.e.* $(g \,_0 f)^{-1} : C \to A$. Also $f^{-1} : B \to A$ and $g^{-1} : C \to B$ we have $f^{-1} \,_0 g^{-1} : C \to A$.

Hence first of all it is evident that both $(g \,_0 f)^{-1}$ are $f^{-1} \,_0 g^{-1}$ are functions from the set C to the set A and $(g \,_0 f)^{-1}(z) = x$ for $z \in C$ and $x \in A$.

Again g^{-1} : C → B, so for every $z \in$ C there exists unique $y \in$ B such that $g^{-1}(z) = y$. Similarly f^{-1} : B → A, so for every $y \in$ B there exists $x \in$ A such that $f^{-1}(y) = x$. Further

$$f^{-1} {}_{o} g^{-1}(z) = f^{-1} (g^{-1}(z)) = f^{-1}(y) = x.$$

i.e. $f^{-1} {}_{o} g^{-1}(z) = x = (g {}_{o} f)^{-1}(z)$. Therefore $(g {}_{o} f)^{-1} = f^{-1} {}_{o} g^{-1}$.

4.6.3 Theorem

If f : A → B is a bijective function, then f^{-1} : B → A is also a bijective function.

Proof : Let f : A → B is a bijective function, *i.e.* f is one-one and onto function. Since f is one-one and onto, for every $y \in$ B there exists unique $x \in$ A such that $f(x) = y$. Again f^{-1} : B → A such that $f^{-1}(y) = x$.

Let $y_1, y_2 \in$ B with $f^{-1}(y_1) = f^{-1}(y_2)$

This implies $x_1 = x_2$

i.e. $f(x_1) = f(x_2)$ [∵ f is one-one]

i.e. $y_1 = y_2$

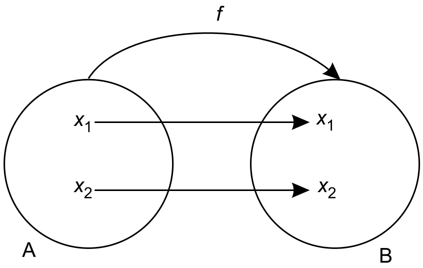
i.e. $f^{-1}(y_1) = f^{-1}(y_2) \Rightarrow y_1 = y_2$. Thus f^{-1} is one-one. Besides this R(f^{-1}) = D(f) = A. *i.e.* R(f^{-1}) = A. This indicates that f^{-1} is onto. Therefore f^{-1} is both one-one and onto. *i.e.* f^{-1} is bijective.

■ 4.7 SOME IMPORTANT FUNCTIONS

In this section we will discuss some important functions.

4.7.1 Identity Function

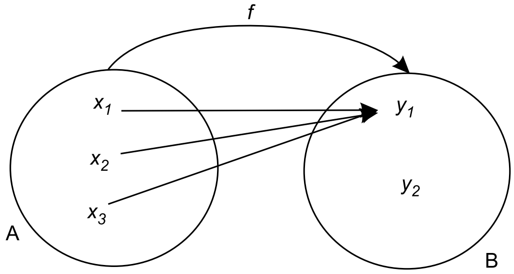
Let A be a set. The function f : A → A is said to be an identity function if for every $x \in$ A, $f(x) = x$. Mathematically $f(x) = x \ \forall \ x \in$ A.



4.7.2 Constant Function

The function f : A → B is said to be a constant function if for every $x \in$ A there exists unique $y \in$ B such that $f(x) = y$. Mathematically,

$$f(x) = y \ \ \forall \ x \in \text{A}$$



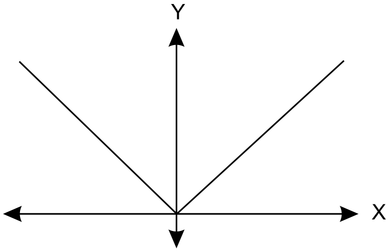
Consider a function $f : R \to I$ defined by $f(x) = 2$ for $x \in R$. Which is a constant function.

4.7.3 Absolute Function

The absolute function or absolute value function $f(x) = [x]$ is defined as

$$|x| = \begin{cases} x; & \text{if } x \geq 0 \\ -x; & \text{if } x < 0 \end{cases}$$

The graph of $f = \{(x, |x|) : x \in R\}$ is shown in the following figure.



4.7.4 Greatest Integer Function

The greatest integer function $f(x) = [x]$ is defined as the greatest integer less than or equal to x. The value of $f(x) = [x]$ is equal to n if $n \leq x < (n + 1)$; $n \in Z$.

Consider the examples $[5] = 5$; $[5.7] = 5$; $[-3.9] = -4$; $[-2.2] = -3$ and $[6.1] = 6$.

4.7.5 Floor and Ceiling Function

The floor function $f(x) = \lfloor x \rfloor$ is defined as the greatest integer less than or equal to x. The ceiling function $f(x) = \lfloor x \rfloor$ is defined as the least integer greater than or equal to x.

Let x be any real number, then x lies between two integers called floor of x and ceiling of x.

Consider the following examples. $\lfloor 3.5 \rfloor = 3$; $\lfloor 5 \rfloor = 5$; $\lfloor -7.2 \rfloor = -8$; $\lceil 3.5 \rceil = 4$; $\lceil 5 \rceil = 5$; $\lceil -7.2 \rceil = -7$.

Note: From the above discussion it is clear that $\lceil x \rceil = \lfloor x \rfloor + 1$ if x is not an integer otherwise $\lceil x \rceil = \lfloor x \rfloor$.

4.7.6 Even and Odd Functions

A real function $y = f(x)$ is said to be even if $f(-x) = f(x)$ and odd if $f(-x) = -f(x)$.

Consider the function $f(x) = 5x^6 + 2x^4 - x^2$.

Therefore $f(-x) = 5(-x)^6 + 2(-x)^4 - (-x)^2 = 5x^6 + 2x^4 - x^2 = f(x)$. Hence $f(x) = 5x^6 + 2x^4 - x^2$ is an even function.

Similarly consider another function $f(x) = \sin x - 5x^3$. Therefore $f(-x) = \sin(-x) - 5(-x)^3 = -\sin x + 5x^3 = -(\sin x - 5x^3) = -f(x)$.

Hence $f(x) = \sin x - 5x^3$ is an odd function.

Note: It is to be noted that a function can neither be even nor odd. Consider the example $f(x) = x^4 + x^3 + x^2 - x$.

Therefore $f(-x) = (-x)^4 + (-x)^3 + (-x)^2 - (-x) = x^4 - x^3 + x^2 + x$. This implies neither $f(-x) = f(x)$ nor $f(-x) = -f(x)$.

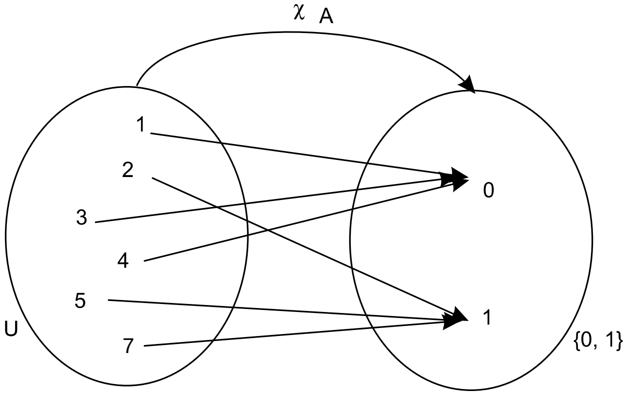
Therefore, $f(x) = x^4 + x^3 + x^2 - x$ is neither even nor odd function.

4.7.7 Characteristic Function

Suppose A be any subset of the universal set U. The characteristic function of A *i.e.* χ_A is a real valued function $\chi_A : U \to \{0, 1\}$ defined by

$$\chi_A(x) = \begin{cases} 1; & \text{if } x \in A \\ 0; & \text{if } x \notin A \end{cases}$$

Consider the example where A = {2, 5, 7} and U = {1, 2, 3, 4, 5,7}. Then we have $\chi_A(1) = 0$, $\chi_A(2) = 1$, $\chi_A(3) = 0$, $\chi_A(4) = 0$, $\chi_A(5) = 1$, $\chi_A(7) = 1$. The arrow diagram is given below.



4.7.8 Remainder Function

Let x be a non-negative integer and y be a positive integer. We define x mod y or $R_y(x)$ to be the remainder when x is divided by y. Thus R_y is a function on Z.

Consider the following examples

8 mod 2 = 0,	15 mod 4 = 3,	251 mod 2 = 1,	177 mod 3 = 0
i.e. $R_2(8) = 0$,	$R_4(15) = 3$,	$R_2(251) = 1$,	$R_3(177) = 0$.

4.7.9 Signum Function

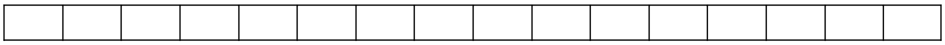
The signum function sgn(x) on R is defined as

$$\text{sgn}(x) = \begin{cases} 0 & \text{if } x = 0 \\ \dfrac{x}{|x|} & \text{if } x \neq 0 \end{cases}$$

The range of this function is {–1, 0, 1}.

4.8 HASH FUNCTION

Suppose that we have cells in a computer memory indexed from 0 to 16. This is given in the following figure.



We wish to store and retrieve arbitrary positive integers in these empty cells. One way is to use a hash function. A hash function takes a data item to be stored or retrieved and computes the first choice for a location for the data item by the relation

$$H(n) = n \bmod k.$$

Where n is the data item (number) to be stored or retrieved. k is the size of the computer memory (preferably prime). If the first choice for a location is already occupied, then we say that a collision has occurred. To handle collisions, a collision resolution policy is required. One simple policy is to find the next highest unoccupied cell.

If we want to locate a stored value n, compute $m = H(n)$ and begin looking at location m. If n is not at this location, move forward in the next highest location. In this context we used one collision resolution policy. Besides this there are several other methods to handle collision, which is beyond the scope of this Book.

Consider an example in which the data item 15, 286, 77, 18, 5, 572, 102, 257 and 55 are to be stored in order in a computer memory indexed from 0 to 16. Here $k = 17$. It is clear that

H(15) = 15 mod 17 = 15, H(286) = 286 mod 17 = 14. Similarly H(77) = 9, H(18) = 1, H(5) = 5, H(572) = 11, H(102) = 0, H(257) = 2, H(55) = 4. Thus the allocation in the computer memory is given in the following figure.

102	18	257		55	5	89			77		572			286	15	
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Now suppose we want to store 89. Since H(89) = 89 mod 17 = 4, 89 should be stored at location 4; but this position is already occupied. If we use the collision resolution policy discussed earlier, we would store 89 at location 6, which is as shown in the above figure.

SOLVED EXAMPLES

Example 1 *Let A = {a, b, c, d} and B = {7, 8, 9}. Find whether the following subsets of (A ×B) are functions from A to B.*

(i) $f_1 = \{(a, 7), (b, 8), (c, 8)\}$

(ii) $f_2 = \{(a, 7), (a, 8), (b, 9), (c, 9), (d, 9)\}$

(iii) $f_3 = \{(a, 7), (b, 8), (c, 9), (d, 9)\}$

(iv) $f_4 = \{(a, 7), (b, 7), (c, 9), (d, 8)\}$

Solution: Given that A = $\{a, b, c, d\}$ and B = {7, 8, 9}.

(*i*) Given $f_1 = \{(a, 7), (b, 8), (c, 8)\}$
This implies $D(f_1) = \{a, b, c\} \neq A$. Hence f_1 can not be a function.

(*ii*) Given $f_2 = \{(a, 7), (a, 8), (b, 9), (c, 9), (d, 9)\}$
This implies $D(f_2) = \{a, b, c, d\} = A$ and $(a, 7) \in f_2$, $(a, 8) \in f_2$ with $7 \neq 8$. Thus f_2 can not be a function.

(*iii*) Given $f_3 = \{(a, 7), (b, 8), (c, 9), (d, 9)\}$
This implies $D(f_3) = \{a, b, c, d\} = A$ and there is no such order pair $(x, y) \in f_3$, $(x, z) \in f_3$ such that $y = z$. So f_3 is a function.

(*iv*) Given $f_4 = \{(a, 7), (b, 7), (c, 9), (d, 8)\}$
This implies $D(f_4) = \{a, b, c, d\} = A$ and there is no such order pair $(x, y) \in f_4$, $(x, z) \in f_4$ such that $y = z$. So f_4 is a function.

Example 2 *Give an example of a function which is*

(a) Injective but not surjective. *(b) Surjective but not Injective.*

(c) Bijective *(d) Neither Injective nor Surjective.*

(e) Constant.

Explain with the help of arrow diagrams.

Solution: (*a*) Let A = {a, b, c, d, e}and B = {1, 2, 3, 4, 5, 6}. Consider a function f_1 from A to B as

$$f_1 = \{(a, 1), (b, 2), (c, 3), (d, 4), (e, 5)\}$$

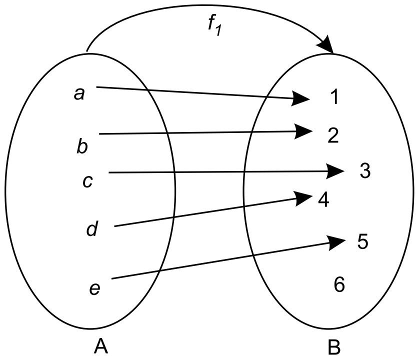
Now R (f_1) = {1, 2, 3, 4, 5} ≠ B. Hence f_1 is not a surjective function but injective. The arrow diagram is given below.

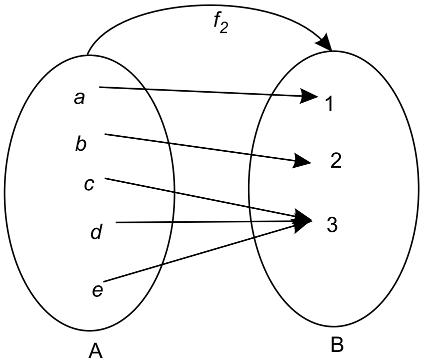
(*b*) Let A = {a, b, c, d, e} and B = {1, 2, 3}
Consider a function f_2 from A to B as $f_2 = \{(a, 1), (b, 2), (c, 3), (d, 3), (e, 3)\}$
Here R(f_2) = {1, 2, 3} = B and $(c, 3) \in f_2$, $(d, 3) \in f_2$, $(e, 3) \in f_2$ such that $c \neq d \neq e$. Thus f_2 is surjective but not injective. The arrow diagram is given below.

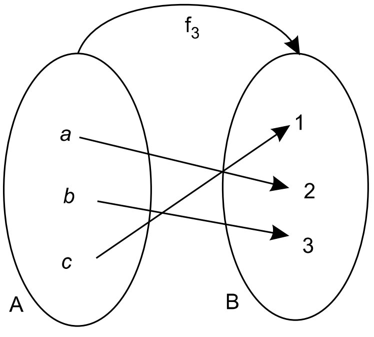
(*c*) Let A = {a, b, c} and B = {1, 2, 3}
Consider a function f_3 from A to B as $f_3 = \{(a, 2), (b, 3), (c, 1)\}$. Here R ($f_3$) = {1, 2, 3} = B. Therefore f_3 is bijective. The arrow diagram is given below.

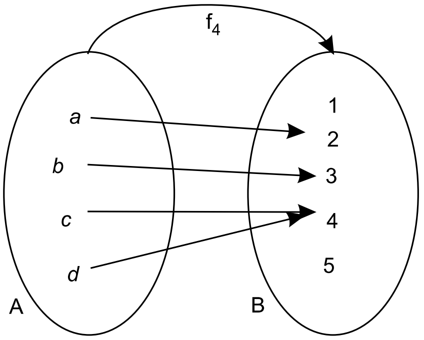
(*d*) Let A = {a, b, c, d} and B = {1, 2, 3, 4, 5}.
Consider a function f_4 from A to B as $f_4 = \{(a, 2), (b, 3), (c, 4), (d, 4)\}$. Here R($f_4$) = {2, 3, 4} ≠ B and $(c, 4) \in f_4$, $(d, 4) \in f_4$ such that $c \neq d$. Therefore f_4 is neither injective nor surjective. The arrow diagram is given below.

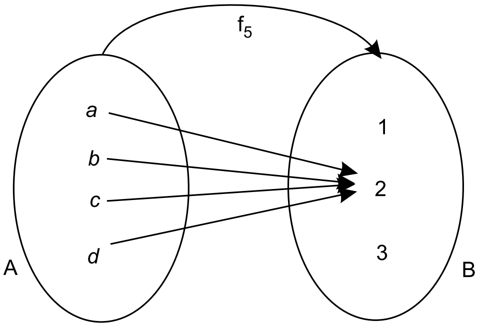
(*e*) Let A = {a, b, c, d} and B = {1, 2, 3}
Consider a function f_5 from A to B as $f_5 = \{(a, 2), (b, 2), (c, 2), (d, 2)\}$. This implies f_5 (x) = 2 for every $x \in$ A. Therefore f_5 is constant. The arrow diagram is given below.











Example 3 *If $f : x \to 2x$; $g : x \to x^2$ and $h : x \to (x + 1)$, then find $(f_o g)_o h$ and $f_o (g_o h)$. Show that $(f_o g)_o h = f_o (g_o h)$.*

Solution: Let $f : x \to 2x$; $g : x \to x^2$ and $h : x \to (x + 1)$.

i.e. $f(x) = 2x, g(x) = x^2$ and $h(x) = x + 1$.

So, $(f_o g)(x) = f(g(x))$

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

Therefore, $(f_o g)_o h(x) = (f_o g)(h(x)) = (f_o g)(x + 1) = 2(x + 1)^2$.

Again $(g_o h)(x) = g(h(x))$

$= g(x + 1) = (x + 1)^2$

Therefore $f_o (g_o h)(x) = f(x + 1)^2 = 2(x + 1)^2$.

Hence $(f_o g)_o h = f_o (g_o h)$.

Example 4 *Let f(x) be any real function. Show that $g_1(x) = \frac{f(x)+f(-x)}{2}$ is always an even function where as $g_2(x) = \frac{f(x)-f(-x)}{2}$ is always an odd function.*

Solution: Let $g_1(x) = \dfrac{f(x)+f(-x)}{2}$

Therefore $g_1(-x) = \dfrac{f(x)+f(-x)}{2} = g_1(x)$, *i.e.* $g_1(-x) = g_1(x)$.

Also let $g_2(x) = \dfrac{f(x)-f(-x)}{2}$.

Therefore $g_2(-x) = \dfrac{f(-x)-f(x)}{2} = -\dfrac{f(x)-f(-x)}{2} = -g_2(x)$. This implies $g_1(x)$ is an even function where as $g_2(x)$ is an odd function.

Example 5 *Find the composition $(f_o g)$ and $(g_o f)$ in the following cases.*

(i) $f(x) = \sin^2 x$ and $g(x) = x^2 + 1$
(ii) $f(x) = e^x$ and $g(x) = x^3$
(iii) $f(x) = 2x^2 + x$ and $g(x) = x^2 + 1$

Hence show that $(f_o g) \neq (g_o f)$.

Solution: (*i*) Let $f(x) = \sin^2 x$ and $g(x) = x^2 + 1$

Therefore $(f_o g)(x) = f(g(x))$

$= f(x^2 + 1) = \sin^2(x^2 + 1)$

Similarly $(g_0 f)(x) = g(f(x)) = g(\sin^2 x) = \sin^4 x + 1$

So, $(f_0 g) \neq (g_0 f)$.

(*ii*) Let $f(x) = e^x$ and $g(x) = x^3$

Therefore $(f_0 g)(x) = f(g(x)) = f(x^3) = e^{x^3}$

Similarly $(g_0 f)(x) = g(f(x)) = g(e^x) = (e^x)^3 = e^{3x}$.

So, $(f_0 g) \neq (g_0 f)$.

(*iii*) Let $f(x) = 2x^2 + x$ and $g(x) = x^2 + 1$

Therefore $(f_0 g)(x) = f(g(x)) = f(x^2 + 1)$

$= 2(x^2 + 1)^2 + (x^2 + 1) = 2x^4 + 5x^2 + 3$

$(g_0 f)(x) = g(f(x)) = g(2x^2 + x) = (2x^2 + x)^2 + 1$

$= 4x^4 + 4x^3 + x^2 + 1$

So, $(f_0 g)(x) \neq (g_0 f)(x)$.

Example 6 *Determine whether the given functions are one-one, onto or bijective.*

(*a*) *$f : R^+ \rightarrow R^+$ defined by $f(x) = |x|$*

(*b*) *$f: I \rightarrow R^+$ defined by $f(x) = 2x + 7$*

(*c*) *$f: R \rightarrow R$ defined by $f(x) = |x|$*

Solution: (*a*) Given $f : R^+ \rightarrow R^+$ defined by $f(x) = |x|$.

Suppose that $f(x_1) = f(x_2)$

$\Rightarrow |x_1| = |x_2|$; *i.e.* $x_1 = x_2$

So, $f : R^+ \rightarrow R^+$ defined by $f(x) = |x|$ is one-one. Again $f(x) = |x|$; $x \in R^+$

This implies $y = |x| = x$ [$\because x \in R^+$]. This indicates that for every $y \in R^+$ there exists $x \in R^+$ such that $y = f(x) = |x|$. Hence, $f : R^+ \rightarrow R^+$ defined by $f(x) = |x|$ is onto. Therefore, bijective.

(*b*) f: I $\rightarrow$ R$^+$ defined by $f(x) = 2x + 7$

Assume that $f(x_1) = f(x_2)$

This implies $2x_1 + 7 = 2x_2 + 7$; *i.e.* $x_1 = x_2$.

So, $f(x) = 2x + 7$; $x \in$ I, is One-One.

Again $f(x) = 2x + 7; x \in I$

$\Rightarrow$ $y = 2x + 7$ [$\because y = f(x)$]

$$\Rightarrow \quad x = \frac{y-7}{2}$$

It is clear that for $y = 5$ we get $x = -1 \notin$ I (Set of positive integers). Hence $f(x) = 2x + 7$ is not onto. Thus $f(x) = 2x + 7$ is One-One only.

(*c*) Given f: R $\rightarrow$ R defined by $f(x) = |x|$

Suppose that $f(x_1) = f(x_2)$

$\Rightarrow$ $|x_1| = |x_2|$

$\Rightarrow$ $\pm x_1 = x_2$

$\Rightarrow$ $x_1 \neq x_2$.

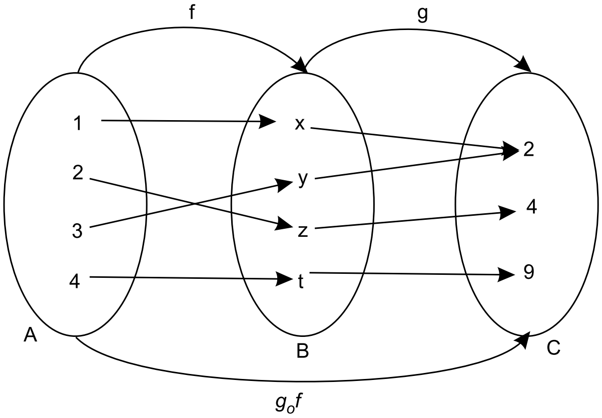
So, f: R $\rightarrow$ R defined by $f(x) = |x|$ is not One-One. Again for $f(x) = y = -5$ in the co-domain R there exists no element x *i*n the domain R. Hence f : R $\rightarrow$ R defined by $f(x) = |x|$ is neither One-One nor onto.

Example 7 *Let A = {1, 2, 3, 4}, B = {x, y, z, t} and C = {2, 4, 9}. Let f = {(1, x), (2, z), (3, y), (4, t)} and g = {(x, 2), (y, 2), (z, 4), (t, 9)} be two functions from A $\rightarrow$ B and B $\rightarrow$ C respectively. Find the composition $(g_0 f)$.*

Solution: Let A = {1, 2, 3, 4}, B = $\{x, y, z, t\}$ and C = {2, 4, 9}. Let $f = \{(1, x), (2, z), (3, y), (4, t)\}$ and

$$g = \{(x, 2), (y, 2), (z, 4), (t, 9)\}$$

Therefore $g\ _o f = \{(1, 2), (3, 2), (2, 4), (4, 9)\}$. Which is a function from A → C . The arrow diagram is given below.



Example 8 *Let Q be the set of rational numbers. Show that the function $f : Q \to Q$ defined by $f(x) = 2x + 7$, $x \in Q$ is a bijective function. Find $f^{-1}(0)$, $f^{-1}(1)$ and $f^{-1}(2)$.*

Solution: f: Q → Q defined by $f(x) = 2x + 7; x \in$ Q

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

$\Rightarrow \qquad 2x_1 + 7 = 2x_2 + 7$

$\Rightarrow \qquad x_1 = x_2.$

i.e. $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$. So, $f(x) = 2x + 7; x \in$ Q is One-One. Again for every $y \in$ Q (co-domain set) there exists $x = \frac{y-7}{2}$ in the domain set Q such that $y = f(x) = 2x + 7$. Hence $f(x) = 2x + 7$ is onto. Therefore $f(x) = 2x + 7$, $x \in$ Q is a bijective function.

To compute the inverse we have $f^{-1}(y) = x$

i.e. $\qquad f^{-1}(y) = \frac{y-7}{2}$

In general $f^{-1}(x) = \frac{x-7}{2}$; $x \in$ Q. Hence we have $f^{-1}(0) = \frac{-7}{2}$, $f^{-1}(1) = -3$ and $f^{-1}(2) = \frac{-5}{2}$.

Example 9 *Let A = R – {3} and B = R – {1}, where R is the set of real numbers. Let $f : A \to B$ defined by $f(x) = \frac{x-2}{x-3}$, $x \in A$. Show that f is One-One and onto. Find the inverse function of f.*

Solution: Let A = R – {3} and B = R – {1}, where R is the set of real numbers. Let f : A → B defined by $f(x) = \frac{x-2}{x-3}$, $x \in$ A. Let $x_1, x_2 \in$ A such that $f(x_1) = f(x_2)$

$\Rightarrow \qquad \frac{x_1 - 2}{x_1 - 3} = \frac{x_2 - 2}{x_2 - 3}$

$\Rightarrow \qquad x_1x_2 - 2x_2 - 3x_1 + 6 = x_1x_2 - 3x_2 - 2x_1 + 6$

$\Rightarrow \qquad -2x_2 - 3x_1 = -3x_2 - 2x_1$

$\Rightarrow \qquad x_1 = x_2$

i.e. $\qquad f(x_1) = f(x_2)$

$\Rightarrow \qquad x_1 = x_2.$

So, $f(x)$ is One-One.

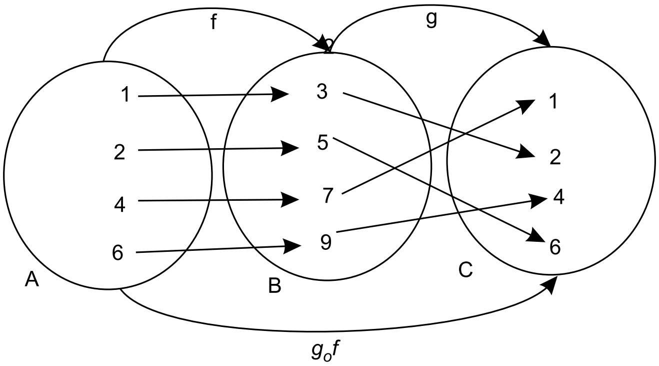
Again for every $y \in$ B, there exists $x = \dfrac{3y-2}{y-1}$ in A such that $y = f(x) = \dfrac{x-2}{x-3}$. Hence $f(x) = \dfrac{x-2}{x-3}$ is onto.

Therefore $f(x) = \dfrac{x-2}{x-3}$, $x \in$ A is a bijective function. To compute inverse we have $f^{-1}(y) = x$.

i.e. $f^{-1}(y) = \dfrac{3y-2}{y-1}$. In general $f^{-1}(x) = \dfrac{3x-2}{x-1}$; $x \in$ B.

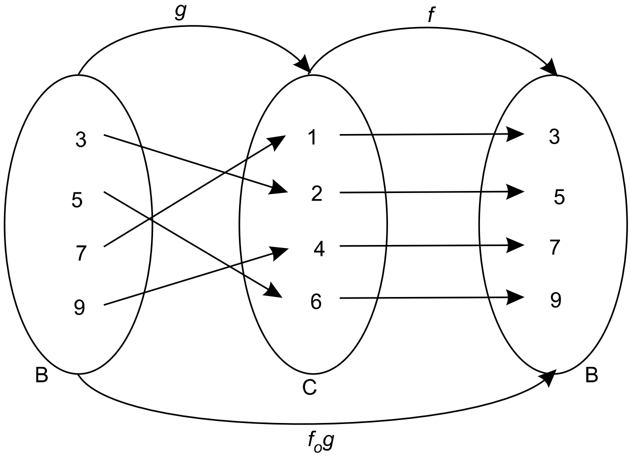
Example 10 *Let A = {1, 2, 4, 6}; B = {3, 5, 7, 9}, C = {1, 2, 4, 6} and f : A → B defined by f = {(1, 3), (2, 5), (4, 7), (6, 9)}; g : B → C defined by g = {(5, 6), (3, 2), (7, 1), (9, 4)} be two functions. Find the compositions ($f_o g$) and ($g_o f$). Show that ($f_o g$) ≠ ($g_o f$).*

Solution: Let A = {1, 2, 4, 6}; B = {3, 5, 7, 9}and C = {1, 2, 4, 6}. Also given f = {(1, 3), (2, 5), (4, 7), (6, 9)} with g = {(5, 6), (3, 2), (7, 1), (9, 4)}. Consider the arrow diagram to compute ($g_o f$).



Therefore, ($g_o f$) = {(1, 2), (2, 6), (4, 1), (6, 4)}.

Similarly, to compute ($f_o g$) the arrow diagram becomes



Therefore, ($f_o g$) = {(5, 9), (3, 5), (7, 3), (9, 7)}. Hence, it is clear that ($f_o g$) ≠ ($g_o f$).

Example 11 *Let $f : R \to (-1, 1)$ defined by $f(x) = \dfrac{x}{1+x^2}$, $x \in R$. Find the inverse of above function if exists, where R is the set of real numbers.*

Solution: Let $f : \mathrm{R} \to (-1, 1)$ defined by $f(x) = \dfrac{x}{1+x^2}$, $x \in$ R. Let $x_1, x_2 \in$ R such that $f(x_1) = f(x_2)$

$$\Rightarrow \qquad \frac{x_1}{1+x_1^2} = \frac{x_2}{1+x_2^2}$$

$$\Rightarrow \qquad x_1 + x_1x_2^2 - x_2 - x_2x_1^2 = 0$$

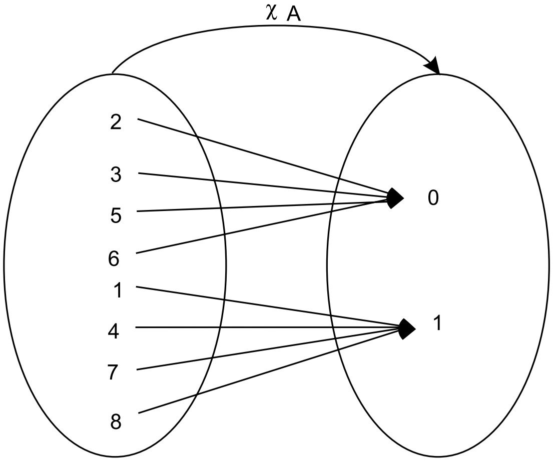
$$\Rightarrow \qquad (x_1 - x_2)(1 - x_1x_2) = 0$$

$$\Rightarrow \qquad x_1 = x_2 \text{ or } (1/x_2)$$

So, $f(x) = \dfrac{x}{1+x^2}$, $x \in$ R is not One-One, hence not bijective. Therefore inverse does not exists.

Example 12 *Find the characteristic function for the set A. Where the Universal set U = {1, 2, 3, 4, 5, 6, 7, 8} and A = {1, 4, 7, 8}.*

Solution: Given Universal set U = {1, 2, 3, 4, 5, 6, 7, 8} and A = {1, 4, 7, 8}. The characteristic function for the set A is given as $\chi_A(1) = 1, \chi_A(2) = 0, \chi_A(3) = 0, \chi_A(4) = 1, \chi_A(5) = 0, \chi_A(6) = 0, \chi_A(7) = 1, \chi_A(8) = 1$. The arrow diagram is given below.



Example 13 *If f(x) and g(x) are both even or both odd, then prove that f(x) g(x) is even.*

Solution: Suppose that $f(x)$ and $g(x)$ are both even.

i.e. $\qquad f(-x) = f(x)$ and $g(-x) = g(x)$.

Let $\qquad h(x) = f(x)\,g(x)$

Therefore $\qquad h(-x) = f(-x)\,g(-x) = f(x)g(x) = h(x)$.

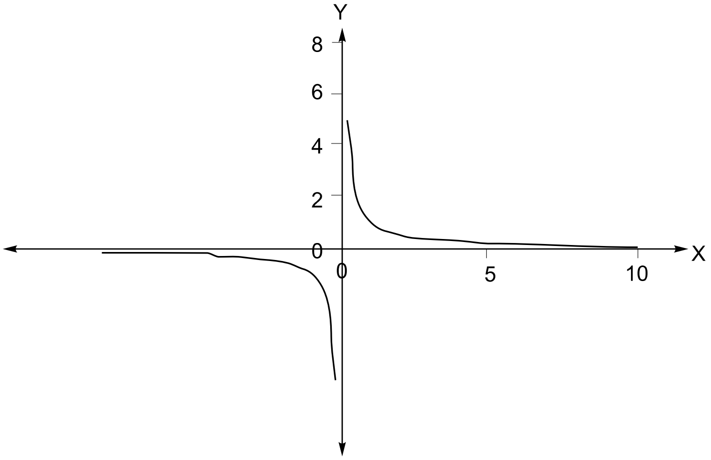
This indicates that $f(x)\,g(x)$ is even. Similarly it can be proved that if both $f(x)$ and $g(x)$ are odd, then $f(x)\,g(x)$ is even.

Example 14 *Sketch the graph of*

$$f(x) = \begin{cases} \dfrac{1}{x}; & \text{if } x \neq 0 \\ 0; & \text{if } x = 0 \end{cases}$$

Solution: Given that $f(x) = \begin{cases} \frac{1}{x}; & \text{if } x \neq 0 \\ 0; & \text{if } x = 0 \end{cases};$

It is clear that if x is very large, then $f(x)$ is nearly equals to 0 and $f(x)$ is very large when x is nearly equals to zero. The graph is given below.



Example 15 *Let f(x) and g(x) are both even functions. Prove that $(f_0 g)$ is also an even function.*

Solution: Suppose that $f(x)$ and $g(x)$ are both even.

i.e. $f(-x) = f(x)$ and $g(-x) = g(x)$.

Now $(f_0 g)(-x) = f(g(-x)) = f(g(x)) = (f_0 g)(x)$

i.e. $(f_0 g)(-x) = (f_0 g)(x)$. Therefore $(f_0 g)(x)$ is an even function.

Example 16 *Prove that $(f_0 g)(x)$ is an odd function if both f(x) and g(x) are odd functions.*

Solution: Suppose that $f(x)$ and $g(x)$ are odd functions.

i.e. $f(-x) = -f(x)$ and $g(-x) = -g(x)$

Now $(f_0 g)(-x) = f(g(-x))$

$= f(-g(x))$ [$\because$ $g(x)$ is an odd function]

$= -f(g(x))$ [$\because$ $f(x)$ is an odd function]

$= -(f_0 g)(x)$

i.e. $(f_0 g)(-x) = -(f_0 g)(x)$. Therefore $(f_0 g)(x)$ is an odd function.

Example 17 *If $g(x) = e^x$ and $(f_0 g)$ is an identity function, prove that f(x) = ln x.*

Solution: Let $g(x) = e^x$ and $(f_0 g)$ is an identity function. *i.e.* $(f_0 g)(x) = x$

i.e. $f(g(x)) = x$

i.e. $f(e^x) = x = \ln(e^x)$

Therefore in general $f(x) = \ln x$.

Example 18 *Let $f(x) = 2x + 1$ and $g(x) = x^2 + 2$. Find the values of $(g_o f)$ (4) and $(f_o g)$ (4). Show that they are not equal.*

Solution: Given that $f(x) = 2x + 1$ and $g(x) = x^2 + 2$

Therefore $(g_o f)(4) = g(f(4)) = g(9)$ [∵ $f(4) = 2(4) + 1 = 9$]

$= 83$ [∵ $g(9) = 9^2 + 2 = 83$]

Again $(f_o g)(4) = f(g(4)) = f(18)$ [∵ $g(4) = 4^2 + 2 = 18$]

$= 37$ [∵ $f(18) = 2(18) + 1 = 37$]

Therefore $(f_o g)(4) \neq (g_o f)(4)$

Example 19 *Let $f : R \to R$ be defined as $f(x) = x^2 - 3x$, if $x < 2$ and $x + 2$, if $x \geq 2$. Find $f(5)$, $f(2)$, $f(0)$ and $f(- 2)$.*

Solution:

Given that
$$f(x) = \begin{cases} x^2 - 3x; & \text{if } x < 2 \\ x + 2; & \text{if } x \geq 2 \end{cases}$$

So,
$$f(5) = 5 + 2 = 7$$
$$f(0) = 0 - 0 = 0$$
$$f(-2) = (-2)^2 - 3(-2) = 10$$
$$f(2) = 2 + 2 = 4.$$

Example 20 *Find the domain D(f) of each of the following functions. (i) $f(x) = \sqrt{16 - x^2}$;*

(ii) $f(x) = \dfrac{1}{x-4}$; (iii) $f(x) = x^2 - 5x + 6$

Solution: (*i*) Given $f(x) = \sqrt{16 - x^2}$; it is clear that $f(x)$ is not defined for $16 - x^2 \leq 0$. *i.e.* $-4 \leq x \leq 4$. So, $f(x)$ is not defined for $x \in [-4, 4]$. Therefore D(f) = R – [– 4, 4].

(*ii*) Given $f(x) = \dfrac{1}{(x-4)}$; it is clear that $f(x)$ is not defined for $(x - 4) = 0$, *i.e.* $f(x)$ is not defined at $x = 4$. Therefore D(f) = R – {4}.

(*iii*) Given $f(x) = x^2 - 5x + 6$. It is clear that $f(x)$ is defined for every real number R. Therefore D (f) = R.

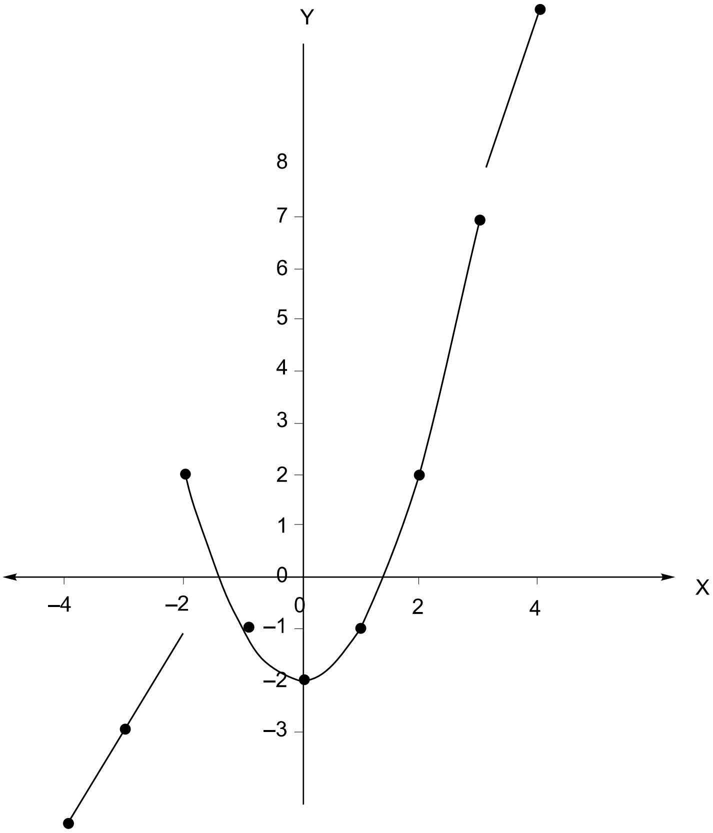
Example 21 *Find the graph of the following functions.*

(*a*) $f(x) = \begin{cases} 3x - 1 & \text{if } x > 3 \\ x^2 - 2 & \text{if } -2 \leq x \leq 3 \\ 2x + 3 & \text{if } x < -2 \end{cases}$ (*b*) $f(x) = \begin{cases} x + 6 & \text{if } x \leq -1 \\ 5 - x & \text{if } x > -1 \end{cases}$

Solution: (*a*) Given that

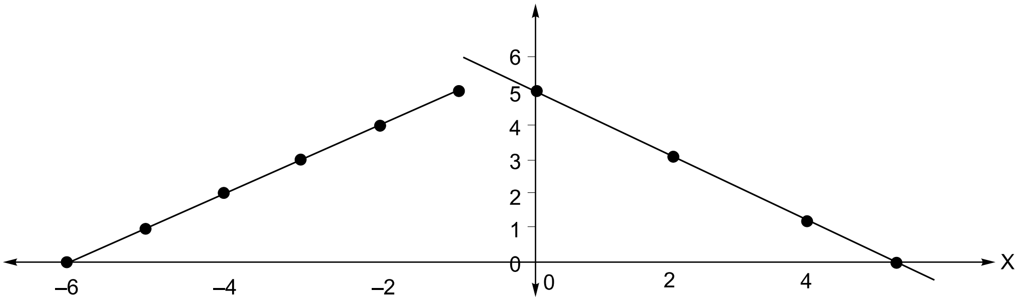
$$f(x) = \begin{cases} 3x - 1 & \text{if } x > 3 \\ x^2 - 2 & \text{if } -2 \leq x \leq 3 \\ 2x + 3 & \text{if } x < -2 \end{cases}$$

The graph of above function is given below.



(*b*) Given that $f(x) = \begin{cases} x + 6 & \text{if } x \leq -1 \\ 5 - x & \text{if } x > -1 \end{cases}$

The graph is given below.



EXERCISES

1. Let A = {1, 2, 3, 4, 5, 6} and B = {*a*, *b*, *c*, *d*, *e*, *f*}. Determine whether each relation given below is a function from A to B. If it is a function, find domain, range. Draw the arrow diagram of each relation.

(*a*) $\{(1, d), (1, e), (2, a), (3, b), (4, e), (5, e), (6, f)\}$

(*b*) $\{(3, d), (4, e), (5, e)\}$

(*c*) $\{(1, b), (2, b), (3, c), (4, c), (5, f), (6, f)\}$

(*d*) $\{(1, c), (2, c), (3, c), (4, c), (5, c), (6, c)\}$

(*e*) $\{(1, a), (2, b), (3, c), (4, d), (5, e), (6, f)\}$

(*f*) $\{(1, a), (2, b), (3, c), (3, d), (3, f)\}$

(*g*) $\{(1, e), (4, e), (5, e), (6, e)\}$

2. Let f be a function from the set R to the set R, where R is a set of real numbers. Determine whether the following are One-One, Onto or both.

(*a*) $f(x) = \cos(x)$ (*b*) $f(x) = 7x + 3$

(*c*) $f(x) = x^3 + 27$ (*d*) $f(x) = 3x^2 - 3x + 1$

(*e*) $f(x) = 3^x + 2$ (*f*) $f(x) = e^x - 4$

(*g*) $f(x) = \dfrac{2x+3}{2x-4}$

3. Let f and g be functions from I to I, where I is the set of positive integers. Find the compositions $(f_0 g)$ and $(g_0 f)$.

(*a*) $f(x) = 2x + 7; g(x) = \cos(x)$ (*b*) $f(x) = x^2 + 2; g(x) = 3^x + 5$

(*c*) $f(x) = \log(x); g(x) = 5x + 2$ *d*) $f(x) = x + 4; g(x) = |x|$

(*e*) $f(x) = 2^x + 2; g(x) = x^2$

4. Let A = $\{a, b, c, d\}$, B = $\{1, 2, 3\}$, C = $\{4, 5, 6\}$ and $f : A \rightarrow B$ defined by $f = \{(a, 1), (b, 1), (c, 2), (d, 2)\}$; g: B $\rightarrow$ C defined by $g = \{(1, 4), (2, 5), (3, 6)\}$ be two functions. Find $(g_0 f)$. Is $(f_0 g)$ defined?

5. Let A = $\{1, 8, 27, 64\}$; B = $\{a, b, c, d, e\}$; C = $\{1, 8, 27, 64\}$ and $f : A \rightarrow B$ defined by $f = \{(1, a), (8, d), (27, b), (64, e)\}$; $g : B \rightarrow C$ defined by $g = \{(a, 1), (b, 64), (c, 8), (d, 27), (e, 8)\}$ be two functions. Find both $(f_0 g)$ and $(g_0 f)$. Show that $(f_0 g) \neq (g_0 f)$.

6. Let U = $\{a, e, I, o, u\}$ be the universal set. Find the characteristic function for the set A = $\{e, o, u\}$.

7. Sketch the functions given below on R $\rightarrow$ R.

(*a*) $f(x) = [x]; -2 \leq x \leq 3$ (*b*) $f(x) = 3^x$

(*c*) $f(x) = 3x + 2$ (*d*) $f(x) = \begin{cases} x^2 \text{ if } x \geq 0 \\ 6 \text{ if } x < 0 \end{cases}$

(*e*) $f(x) = \begin{cases} 2x + 1 & \text{if } 0 < x < 2 \\ -2 & \text{if } x \leq 0 \\ x + 4 & \text{if } x \geq 2 \end{cases}$

8. Find the domain of each of the following functions.

(*a*) $f(x) = \dfrac{1}{(x-2)(x-3)}$ (*b*) $f(x) = \dfrac{1}{x^2 - 7x + 12}$

(*c*) $f(x) = x^2 - 7x + 12$ (*d*) $f(x) = x^2 ; 0 \leq x \leq 2$

(*e*) $f(x) = \sqrt{36 - x^2}$

9. Let $f : R \rightarrow R$ defined by $f(x) = x^2 + x - 6$. Find $f^{-1}(14)$ and $f^{-1}(-8)$.

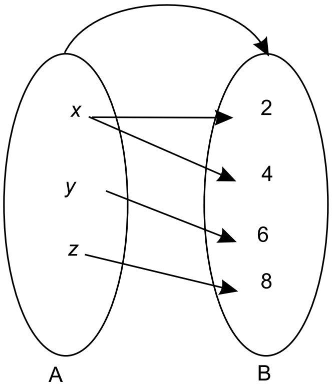
10. Draw the graph of following functions.

(*a*) $f(x) = x^3 - 3x + 2$ (*b*) $f(x) = x^4 - 10x^2 + 9$

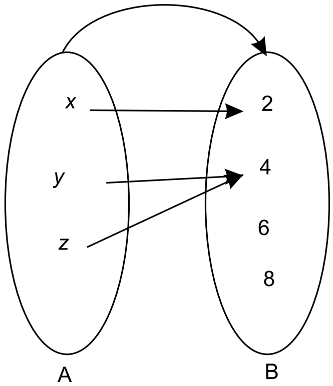
(*c*) $f(x) = \dfrac{x}{2} + 1$

11. If $f(x) = 2x - 3$ and $g(x) = x^2 + 3x + 5$, find $(f_o g)(5)$ and $(g_o f)(5)$. Show that they are not equal.
12. If $f(x) = 2x - 3$ and $g(x) = x^2 + 2x + 1$. Find the compositions $(f_o g)$ and $(g_o f)$. Find $(f_o g)(2)$ and $(g_o f)(2)$.
13. If $f(x) = 5x + 1$. Find a formula for the composition function f^3 . [**Hint :** $f^3 = (f_o f_o f)$]
14. Let A = $\{x, y, z\}$ and B = $\{2, 4, 6, 8\}$. State whether or not each diagram given below defines a function from A into B.

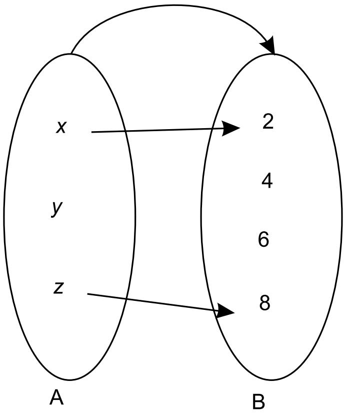
(*a*)



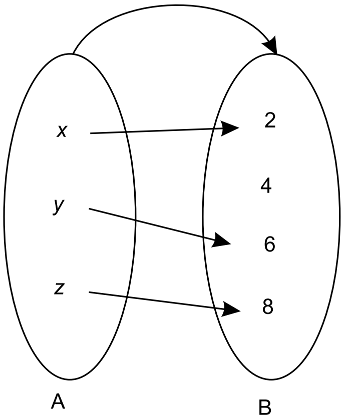
(*b*)



(*c*)



(*d*)



15. Let $f: R \to R$ defined by $f(x) = 2x + 5$. Show that $f(x)$ is invertible. Find the values of $f^{-1}(2)$, $f^{-1}(4)$ and $f^{-1}(5\ )$.
16. Let f and g be functions from the positive integers to the positive integers defined by $f(x) = 3x + 1$, and $g(x) = 2x + 1$. Find the compositions $(f_o f)$, $(f_o g)$, $(g_o f)$ and $(g_o g)$.
17. Let A = R – {2} and B = R $- \left\{\frac{3}{5}\right\}$, where R is the set of real numbers. Let $f: A \to B$ defined by $f(x) = \dfrac{3x - 9}{5x - 10}$; $x \in$ R. Show that f is bijective and hence find the inverse of f.
18. For each Hash function, show how the data would be inserted in the order given in initially empty cells. Use collision resolution policy if required.
    (*a*) $h(n) = n \bmod 11$; cells indexed 0 to 10; data 55, 15, 285, 743, 375, 22, 10, 800.
    (*b*) $h(n) = n \bmod 13$; cells indexed 0 to 12; data 714, 635, 26, 775, 42, 30, 10, 136, 509.

19. Show that the inverse of $f(x) = x^2 - 1$ does not exists in general, but f : $[0, \infty) \to [-1, \infty)$ has an inverse given by $f^{-1}(x) = \sqrt{x+1}$ and $f^{-1} : [-1, \infty) \to [0, \infty)$.
20. Let f be a function from $X \to X$; $X = \{1, 2, 3, 4, 5, 6\}$ defined by $f(x) = 3x$ mod 5. Write the function and draw the arrow diagram.
21. Let $f : X \to X$; $X = \{0, 1, 2, 3, 4, 5, 6\}$ defined by $f(x) = 4x$ mod 5. Write the function f as a set of order pairs. With the help of arrow diagram check whether or not f is one-to-one or onto.
22. Let $f : A \to B$ be a function . Show that f is injective if and only if $f^{-1}(f(X)) = X$ for all $X \subseteq A$.
23. Let $f : R - \{0\} \to R - \{0\}$ defined by $f(x) = \dfrac{1}{x}$. Show that f is bijective and its inverse is given by $f^{-1}(x) = \dfrac{1}{x}$.
24. Show that the function $f(x) = \dfrac{x}{x^2+1}$: $R \to R$ is neither one-one nor onto.

5

Group Theory

■ 5.0 INTRODUCTION

In this chapter we will study the algebraic structure known as group which is the building block of "Abstract Algebra". Group is a one operational system. *i.e.* it has one binary operation using which we can combine two elements of a set to get the third element. In this chapter we will discuss definition of group, subgroup, cyclic group, group homomorphism and etc. Group theory has also wide application in the areas of Computer Science specially in the field of binary coding.

■ 5.1 BINARY OPERATION ON A SET

Let A be a non-empty set. If f be a function from $(A \times A) \to A$, then f is said to be a binary operation on the set A. So the binary operation must satisfy the following two conditions, *i.e.* f assigns an element $f(a, b)$ of A to every ordered pair (a, b) in $(A \times A)$ and only one element of A is assigned to each ordered pair; as the operation is a function.

Generally we use the symbols +, ×, *, o etc. for representing the binary operation on a set. So o will be the binary operation in A if and only if

(*a*) $(a\ _0\, b) \in A \quad \forall\, a, b \in A$

(*b*) $(a\ _0\, b)$ is unique.

We will use the symbol $(_0)$ to represent the binary operation in place of f and the element assigned to (a, b) by $(a\ _0\, b)$. It is clear that binary operation function is a special case of Binary Operation.

Let us consider the operation addition in the set of Natural numbers N.

Let $a, b \in N$; *i.e.* a and b are two natural numbers. But we know that sum of any two natural numbers is again a natural number and is unique, *i.e.* $(a + b) \in N$ for all $a, b \in N$. Hence + is a binary operation.

■ 5.2 ALGEBRAIC STRUCTURE

A non-empty set A along with one or more binary operations is called an algebraic structure. So if A is a non empty set & o is a binary operation then (A, o) is a algebraic Structure. Consider the examples of algebraic structures as (N, +), (R, X) and (I, +).

5.2.1 Semi Group

A algebraic structure (G, o) is said to be a semi group if the binary operation (o) is associative in G.

i.e. $a_0 (b_0 c) = (a_0 b) \text{ o } c\ ;\ a, b, c \in$ G.

Let us consider the algebraic Structure (N, o), where o is a usual product. We know that for any three natural numbers $a, b, c \in$ N, we have $a_0 (b_0 c) = (a_0 b)_0 c$, as product is associative in N. This implies that (N, o) is a semi group.

5.2.2 Monoid

A algebraic structure (G, o) is said to be a monoid if the binary operation (o) is associative in G with an identity element e in G.

i.e. $a_0 (b_0 c) = (a_0 b)_0 c$ and $a_0 e = e_0 a = a\ \forall\ a, b, c \in$ G, where e is the identity element of G.

Let us consider the algebraic structure (Z, +), where Z is the set of positive integers and the binary operation is an addition. It will become monoid if there exists an identity element e in Z such that

$$a + e = a\ \forall\ a \in \text{Z}$$

This implies that $e = 0$, but $0 \notin$ Z. Hence (Z, +) is not a monoid.

■ 5.3 GROUP

A non empty set G is said to be a Group under the binary operation o if the following conditions are satisfied. It is also to be noted that a Group is a monoid with unit element e.

(*a*) Closure Law: For all $a, b \in$ G ; $(a_0 b) \in$ G
(*b*) Associative Law: For all $a, b, c \in$ G, $a_0 (b_0 c) = (a_0 b)_0 c$
(*c*) Identity: For all $a \in$ G, there exists an identity element $e \in$ G such that $(a_0 e) = a = (e_0 a)$, where e is called the identity element.
(*d*) Inverse: For all $a \in$ G, there exists an element $a^{-1} \in$ G such that $(a_0 a^{-1}) = e = (a^{-1}{}_0 a)$.

5.3.1 Commutative Group

A group G is said to be a commutative group or abelian group if the commutative law holds. *i.e.*

$$(a_0 b) = (b_0 a)\ \forall\ a, b \in \text{G}$$

5.3.2 Finite and Infinite Group

If the number of elements in a group G is finite, then it is called a finite group. Otherwise it is called an infinite group.

5.3.3 Order of a Group

The number of elements in a finite group G is called the order of the group and is denoted by O(G).

Let us consider the group G ={a, e}, then O(G)= 2, *i.e.* G is a group of order 2.

5.3.4 Order of an element

Let G be a group and $a \in$ G, then the order of an element a is the least positive integer n such that $a^n = e$. If there exists no such n, then the order of a is infinity or zero.

Let us consider the set of integers G with the binary operation addition.

(*a*) *Closure Law:* We know that the sum of two integers is also an integer,

i.e. $(a+b) \in G \; \forall \; a, b \in G.$

(*b*) *Associative Law:* We know that the addition of integers is associative,

i.e. $a + (b + c) = (a + b) + c \; \forall \; a, b, c \; G.$

(*c*) *Existence of Identity:* For every integer $a \in$ G there exists identity element $0 \in$ G such that

$$a + 0 = 0 + a = a$$

(*d*) *Existence of Inverse:* For every integer $a \in$ G, there exists inverse element $-a \in$ G such that $a + (-a) = (-a) + a = 0$. So every element of G has an additive inverse.

This implies that the set of integers G together with the binary operation addition (+) is a group.

Note

1. Since addition of Integers is Commutative *i.e.* $(a + b) = (b + a)$ for all $a, b \in$ G, the group G is an abelian or commutative group.
2. Since G Contains infinite element, So G is a commutative group of infinite order.

5.3.5 Theorem

If G be a group, then

(*a*) The identity element is unique.

(*b*) Every $a \in$ G has an unique inverse in G.

(*c*) For every $a \in$ G; $(a^{-1})^{-1} = a$

(*d*) For all $a, b \in$ G; $(a \,_o\, b)^{-1} = b^{-1} \,_o\, a^{-1}$

Proof: (*a*) If not and if possible let e and f be the two identity elements of group G. Thus we have

$$e \,_o\, f = f \text{ (Taking } e \text{ as identity)}$$

and $$e \,_o\, f = e \text{ (Taking } f \text{ as identity).}$$

Now $(e \,_o\, f)$ is an unique element of G as G is a group. Therefore $f = e$, *i.e.* Identity element is unique.

(*b*) Let $a \in$ G and $e \in$ G be the identity element of G. If not and if possible let $a_1 \in$ G and $a_2 \in$ G be two inverses of $a \in$ G. Therefore

$$(a \,_o\, a_1) = (a_1 \,_o\, a) = e \text{ and } (a \,_o\, a_2) = (a_2 \,_o\, a) = e.$$

Now; $a_2 \,_o\, (a \,_o\, a_1) = a_2 \,_o\, e = a_2$ ... (*i*)

And $(a_2 \,_o\, a) \,_o\, a_1 = e \,_o\, a_1 = a_1$ ... (*ii*)

Again by associative property $a_2 \,_o\, (a \,_o\, a_1) = (a_2 \,_o\, a) \,_o\, a_1$. Therefore from equations (*i*) and (*ii*) we get $a_1 = a_2$. This implies that the inverse of an element is unique.

(*c*) Given that G is a group. Let $a \in$ G, this implies $a^{-1} \in$ G. Similarly $(a^{-1})^{-1} \in$ G. Let e be the identity element of G. Hence we have $(a^{-1} \,_o\, a) = e$

$\Rightarrow$ $(a^{-1})^{-1} \,_o\, (a^{-1} \,_o\, a) = (a^{-1})^{-1} \,_o\, e$

$\Rightarrow$ $((a^{-1})^{-1} \,_o\, a^{-1}) \,_o\, a = (a^{-1})^{-1}$ [Using associative and identity law]

$\Rightarrow$ $e \,_o\, a = (a^{-1})^{-1}$ [Using identity law]

$\Rightarrow$ $a = (a^{-1})^{-1}$ [Using inverse law]

So, $(a^{-1})^{-1} = a.$

(*d*) Given that G is a group. Let $a, b \in$ G

Now $(a \,_0\, b)(b^{-1}\,_0 a^{-1}) = ((a \,_0\, b)\, b^{-1})\,_0\, a^{-1}$ [Associative law]

$= (a \,_0\, (b \,_0\, b^{-1}))\,_0\, a^{-1}$ [Associative law]

$= (a \,_0\, e)\,_0\, a^{-1}$ [Inverse law]

$= a \,_0\, a^{-1}$ [Identity law]

$= e$ [Inverse law]

So, $(a \,_0\, b)(b^{-1}\,_0 a^{-1}) = e$

Similarly it can be shown that $(b^{-1}\,_0\, a^{-1})(a \,_0\, b) = e$.

Thus it is clear that $(b^{-1}\,_0\, a^{-1})$ is the inverse of $(a \,_0\, b)$.

i.e. $(a \,_0\, b)^{-1} = b^{-1}\,_0\, a^{-1}$.

5.3.6 Theorem

Let G be a group and for all $a, b, c \in$ G

(*i*) if $(a \,_0\, b) = (a \,_0\, c)$ then $b = c$ [Left cancellation law]

(*ii*) if $(b \,_0\, a) = (c \,_0\, a)$ then $b = c$ [Right cancellation law]

Proof: (*i*) Let G be a group and $a, b, c \in$ G

Assume that $(a \,_0\, b) = (a \,_0\, c)$

$\Rightarrow$ $a^{-1}\,_0\, (a \,_0\, b) = a^{-1}\,_0\, (a \,_0\, c)$

$\Rightarrow$ $(a^{-1}\,_0\, a)\,_0\, b = (a^{-1}\,_0\, a)\,_0\, c$ [Associative law]

$\Rightarrow$ $e \,_0\, b = e \,_0\, c$ [Existence of inverse]

$\Rightarrow$ $b = c$ [Existence of identity]

So, if $(a \,_0\, b) = (a \,_0\, c)$ then $b = c$. This is called the left cancellation law.

(*ii*) Let G be a group and $a, b, c \in$ G

Assume that $(b \,_0\, a) = (c \,_0\, a)$

$\Rightarrow$ $(b \,_0\, a)\,_0\, a^{-1} = (c \,_0\, a)\,_0\, a^{-1}$

$\Rightarrow$ $b \,_0\, (a \,_0\, a^{-1}) = c \,_0\, (a \,_0\, a^{-1})$ [Associative law]

$\Rightarrow$ $b \,_0\, e = c \,_0\, e$ [Existence of inverse]

$\Rightarrow$ $b = c$ [Existence of identity]

So,if $(b \,_0\, a) = (c \,_0\, a)$ then $b = c$. This is called the right cancellation law.

5.3.7 Theorem

Let G be a group and a, b be the elements of G, then

(*i*) The equation $ax = b$ has unique solution in G.

(*ii*) The equation $ya = b$ has unique solution in G.

Proof: (*i*) Let G be a group and let $a, b \in$ G.

According to closure law $(a^{-1}\, b) \in$ G, as $a^{-1} \in$ G and $b \in$ G. Let $x = a^{-1}\, b$. Now

$$ax = a(a^{-1}\, b) = (a \,_0\, a^{-1})\, b = e \,_0\, b = b$$

Therefore $x = a^{-1}\, b$ is the solution to the equation $ax = b$.

Let us assume that x_1 and x_2 be two solutions to the equation $ax = b$. Hence we have

$$ax_1 = b \text{ and } ax_2 = b.$$

This implies that $ax_1 = ax_2$. Therefore by left cancellation law $x_1 = x_2$. Hence the solution is unique.

(*ii*) Let G be a group and let $a, b \in$ G.

According to closure law $(ba^{-1}) \in$ G, as $a^{-1} \in$ G and $b \in$ G. Let $y = ba^{-1}$. Now

$$ya = (ba^{-1})\,a = b\,(a^{-1}{}_{o}\,a) = b\,{}_{o}\,e = b$$

Therefore $y = b\,a^{-1}$ is the solution to the equation $ya = b$.

Let us assume that y_1 and y_2 be two solutions to the equation $ya = b$. Hence we have

$$y_1a = b \text{ and } y_2a = b.$$

This implies that $y_1a = y_2a$. Therefore by right cancellation law $y_1 = y_2$. Hence, the solution is unique.

5.3.8 Theorem

The order of all the elements of a finite group is finite and is less than or equal to the order of the group.

Proof : Let G be a finite group and the composition being multiplication.

Let $\qquad a \in$ G.

This implies $\qquad (a * a) = a^2 \in$ G.

$\Rightarrow \qquad (a * a^2) = a^3 \in$ G.

$\Rightarrow \qquad (a * a^3) = a^4 \in$ G and so on.

i.e. $a, a^2, a^3, a^4, a^5, \ldots.$ are the elements of G. This implies that G has infinite order.

But it is given that G is of finite order. So there must exist two integers j and k such that

$$a^j = a^k \text{ for } j > k.$$

$\Rightarrow \qquad a^j\,a^{-k} = a^{\,k}\,a^{-k} = e$

$\Rightarrow \qquad a^{\,j-k} = e$

$\Rightarrow \qquad a^l = e$; Where $l = (j - k) \in$ I$^+$ (Set of positive integers)

Now the set of all these positive integers l satisfying $a^l = e$ will have a least member say m. So, $a^m = e$.

Therefore O(a) is finite. Let O(a) = n.

Now we have to show that O(a) ≤ O(G), *i.e.* $n \le$ O(G). If not and if possible let us assume that $n >$ O(G).

Let $a \in$ G. Therefore by closure property we have $a, a^2, a^3, a^4, a^5, \ldots.\ a^n \in$ G. If they are not distinct then there exists two integers r and s such that $a^r = a^s$, $\quad 1 \le s < r \le n$

$\Rightarrow \qquad a^{r-s} = e.$

Thus $\qquad$ O(a) = $(r - s)$ as $(r - s) < n$.

This contradicts to the fact that O(a) = n. Hence our supposition is wrong. Similarly this is not possible if $n >$ O(G).

Therefore O(a) ≤ O(G).

5.3.9 Theorem

The order of any integral power of an element a can not exceed the order of a.

Proof : Let G be a group and $a \in$ G. Let us assume that the order of the element a is n, *i.e.* O(a) = n. This implies that $a^n = e$, where e is the identity element of G.

Suppose that a^m be the integral power of a.

Again $\quad a^n = e$

$\Rightarrow \quad (a^n)^m = e^m = e$

$\Rightarrow \quad (a^{nm}) = e$

$\Rightarrow \quad (a^m)^n = e$

This implies that the order of the element a^m can not exceed the order of a, *i.e.* O(a^m) $\leq n$.

5.3.10 Theorem

The order of an element a of a group G is the same as the order of its a^{-1}, *i.e.* If G is a group and $a \in$ G, then O(a) = O(a^{-1}).

Proof : Let the order of an element a of a group G be m and that of a^{-1} be n. *i.e.* O(a) = m and O(a^{-1}) = n.

Now $\quad$ O(a) = m.

This implies that $\quad a^m = e$.

$\Rightarrow \quad (a^m)^{-1} = e$

$\Rightarrow \quad (a^{-1})^m = e$

Therefore order of a^{-1} is less than or equal to m, *i.e.* O(a^{-1}) $\leq m$. Thus we have $n \leq m$ ... (i)

Again $\quad$ O(a^{-1}) = n

This implies that $\quad (a^{-1})^n = e$

$\Rightarrow \quad (a^n)^{-1} = e$

$\Rightarrow \quad (a^n) = e \qquad [\because \ a^{-1} = e$ implies $a = e$]

Therefore order of a is less than or equal to n, *i.e.* $\leq$ O(na). Thus we have $m \leq n$. ... (ii)

Hence from equations (i) and (ii) it is clear that $m = n$. Therefore, the order of an element a of a group G is the same as the order of its inverse a^{-1}.

■ 5.4 SUBGROUP

A non-empty subset H of a group G is said to be subgroup of G if H forms the group under the binary operation defined on G.

As every set is subset of itself, so G is subset of itself and hence G is subgroup of G.

5.4.1 Theorem

A non empty subset H of a group G is said to be subgroup of G if and only if

(i) $a, b \in$ H implies $(a \,_0\, b) \in$ H [Closure Law] and

(ii) $a \in$ H implies $a^{-1} \in$ H [Inverse Law]

Proof : Let H be a subgroup of G. Therefore H satisfies all properties of a group. Thus closure law and existence of inverse holds.

Conversely, suppose that

(i) $a, b \in$ H implies $(a \,_0\, b) \in$ H [Closure Law] and

(ii) $a \in$ H implies $a^{-1} \in$ H [Inverse Law]

Now we have to show that H is a subgroup of G, *i.e.* Existence of identity and associative law holds in H.

Associative Law : Let $a, b, c \in$ H. This implies that $a, b, c \in$ G as H $\subseteq$ G. Thus we get $a \,_0 (b \,_0 c) = (a \,_0 b) \,_0 c$. Therefore associative law holds in H.

Existence of Identity: Given that $a \in$ H implies $a^{-1} \in$ H. So, by closure law $(a \,_0 a^{-1}) \in$ H. *i.e.* $e \in$ H. Therefore identity element exists in H. Thus H is a subgroup of G.

5.4.2 Theorem

A non empty subset H of a group G is the subgroup of G if and only if $(a \,_0 b^{-1}) \in$ H for $a, b \in$ H.

Proof : Let H be a subgroup of G. Therefore H satisfies all properties of a group G. Thus closure law and existence of inverse holds.

Let $a, b \in$ H. Again by existence of inverse we have $b^{-1} \in$ H. Therefore by closure property $(a \,_0 b^{-1}) \in$ H as $a \in$ H, $b^{-1} \in$ H.

Conversely, Suppose that $(a \,_0 b^{-1}) \in$ H for $a, b \in$ H.

Now we have to show that H is a subgroup of G, *i.e.* H satisfies all the four properties of the group G.

Given that $(a \,_0 b^{-1}) \in$ H for $a, b \in$ H. Hence we have $(b \,_0 b^{-1}) \in$ H. This implies that $e \in$ H. So, identity element exists in H. Again $e \in$ H and $a \in$ H implies that $(e \,_0 a^{-1}) \in$ H. *i.e.* $a^{-1} \in$ H. Thus inverse element for every element exist in H.

Also $a \in$ H, $b^{-1} \in$ H implies that $(a \,_0 (b^{-1})^{-1}) \in$ H. *i.e.* $(a \,_0 b) \in$ H. So, closure law holds in H. As H is a subset of G and G is a group, so associative law also holds in H.

Therefore H is a subgroup of G.

5.4.3 Theorem

Intersection of two subgroups of a group G is also a subgroup of G.

Proof : Let H and K be two subgroups of group G. So, H $\subseteq$ G and K $\subseteq$ G. This implies that (H $\cap$ K) is also a subset of G.

Now our claim is to show that (H $\cap$ K) is a subgroup of G, *i.e.* Closure law and existence of inverse holds in (H $\cap$ K).

Closure Law: Let $a, b \in$ (H $\cap$ K)

$\Rightarrow$ $a, b \in$ H and $a, b \in$ K

$\Rightarrow$ $(a \,_0 b) \in$ H and $(a \,_0 b) \in$ K [$\because$ H and K are subgroups]

$\Rightarrow$ $(a \,_0 b) \in$ (H $\cap$ K).

Existence of Inverse: Let $a \in$ (H $\cap$ K).

$\Rightarrow$ $a \in$ H and $a \in$ K.

$\Rightarrow$ $a^{-1} \in$ H and $a^{-1} \in$ K [$\because$ H and K are subgroups]

$\Rightarrow$ $a^{-1} \in$ (H $\cap$ K)

Therefore (H $\cap$ K) satisfies both closure law and inverse axiom. Hence (H $\cap$ K) is a subgroup of G.

5.4.4 Theorem

If H is a non empty finite subset of a group G, then H is a subgroup of G if and only if H is closed under multiplication.

Proof : (Necessary Part). Let H be a multiplicative subgroup of the group G.

As H is a subgroup G so it satisfies all the properties of group, hence the closure properties.

i.e. $a, b \in$ H implies $(a \,_0\, b) \in$ H.

(Sufficient Part) Let H be non-empty finite subset of group G and H is closed under multiplication.

i.e. $a, b \in$ H implies $(a \,_0\, b) \in$ H.

Now we have to show that every element of H has an inverse element in H, *i.e.* $a \in$ H implies $a^{-1} \in$ H.

Let $a \in$ H. This implies that $(a \,_0\, a) = a^2 \in$ H. Similarly $a^3 = (a^2 \,_0\, a) \in$ H and so on. Therefore we get

$$\text{H} = \{a, a^2, a^3, a^4, \ldots, a^m, \ldots\}$$

This indicates that H is an infinite set. But, it is given that H is a finite set. So, all the elements of H listed above are not distinct. Thus there exists two integers j and k such that $a^j = a^k$ for $j > k > 0$.

This implies that $a^j a^{-k} = a^k a^{-k} = e$

i.e. $a^{j-k} = e \ldots.$ $\ldots.(i)$

Now as $j > k > 0$ are two positive integers we have $(j - k) \geq 1$. *i.e.* $(j - k - 1) \geq 0$.

So, $a^{(j-k-1)} \in$ H, as H contains elements of type a^m.

Again $a \in$ H and $a^{(j-k-1)} \in$ H implies that

$(a \,_0\, a^{(j-k-1)}) \in$ H [By closure law]

i.e. $a^{j-k} = e \in$ H.

Therefore $(a \text{ o } a^{(j-k-1)}) = e \ \ldots(ii)$

From equation it is clear that $a^{(j-k-1)}$ is the inverse element of a. *i.e.* $a^{-1} = a^{(j-k-1)}$. So, inverse element exists in H. Therefore H is a subgroup of G.

5.4.5 Definition

Let G be a group and H is subgroup of G. Now for $a, b \in$ G we say "a is congruent to b mod H" written as $a \equiv b$ mod H if $a\, b^{-1} \in$ H.

5.4.6 Theorem

Let G be a group and H is a subgroup of G. Then show that relation $a \equiv b$ mod H is an equivalence relation.

Proof : Given G be a group and H be a subgroup of G. We have to show that the relation $a \equiv b$ mod H is an equivalence relation.

Reflexive : Let $a \in$ H. This implies that $a^{-1} \in$ H.

Hence by closure axiom we have $(a \,_0\, a^{-1}) \in$ H.

i.e. $a \equiv a$ mod H.

Symmetric : Suppose that $a \equiv b$ mod H.

This implies that $ab^{-1} \in$ H

$\Rightarrow$ $(ab^{-1})^{-1} \in$ H [By Existence of inverse]

$\Rightarrow$ $(b^{-1})^{-1} a^{-1} \in$ H [By Theorem]

$\Rightarrow \qquad ba^{-1} \in \mathrm{H}$

$\Rightarrow \qquad b \equiv a \bmod \mathrm{H}.$

Transitive: Suppose that $a \equiv b \bmod \mathrm{H}$ and $b \equiv c \bmod \mathrm{H}$

This implies that $ab^{-1} \in \mathrm{H}$ and $b\,c^{-1} \in \mathrm{H}$

$\Rightarrow \qquad (ab^{-1})\,(b\,c^{-1}) \in \mathrm{H}$ [By Closure law]

$\Rightarrow \qquad a(b^{-1}\,b)\,c^{-1} \in \mathrm{H}$ [By Associative law]

$\Rightarrow \qquad (ae)\,c^{-1} \in \mathrm{H}$ [By Existence of Inverse]

$\Rightarrow \qquad ac^{-1} \in \mathrm{H}$ [By Existence of Identity]

i.e. $\qquad a \equiv c \bmod \mathrm{H}$

Therefore the relation $a \equiv b \bmod \mathrm{H}$ is an equivalence relation.

■ 5.5 CYCLIC GROUP

A group G is called the cyclic group if for any $a \in$ G all other elements are of type a^n, where n is any integer. 'a' is called the generator of G. A cyclic group may have more than one generator and the generator is denoted by (a). Therefore a cyclic group G is of the type

$$\mathrm{G} = \{x \mid x = a^n \text{ ; } n \text{ is any integer}\}$$

The elements of G is of the form $\ldots, a^{-3}, a^{-2}, a^{-1}, a^0 = e, a, a^2, a^3, \ldots$

5.5.1 Theorem

Every cyclic group is an abelian group.

Proof : Let G be a cyclic group with generator a. Let a^m and a^n be two elements of G, *i.e.* a^m, $a^n \in$ G.

Now $\qquad (a^m\,_0\,a^n) = a^{m+n} = a^{n+m} = (a^n\,_0\,a^m).$

Therefore G is an abelian group.

5.5.2 Theorem

G be a cyclic group with generator a, then a^{-1} is also the generator.

Proof : Let G be a cyclic group with generator a. So, $a^n \in$ G, where n is some integer.

Now $\qquad a^n = (a^{-1})^{-n}\,;\, -n \in \mathrm{I}$

This indicates that every element can be expressed as some powers of a^{-1}. Therefore a^{-1} is also the generator of G.

5.5.3 Theorem

The order of cyclic group is same as the order of its generator.

Proof: Let G be a cyclic group with generator a and let the order of a be n, *i.e.* $a^n = e$.

Now we have to show that the order of cyclic group G is n, *i.e.* G contains exactly n elements.

Let m be an integer; $m > n$ and $a^m \in$ G.

As $m > n$, we have by division algorithm $m = nk + r\,;\, 0 \le r < n$.

Therefore $a^m = a^{nk+r} = a^{nk}\,a^r = (a^n)^k\,a^r = e^k\,a^r = a^r$. This implies that $a^m = a^r$, *i.e.* a^m is one of the element from $a, a^2, a^3, \ldots, a^n$. Therefore G can not have more than n elements.

Now we have to show G contains exactly n elements, *i.e.* all the elements $a, a^2, a^3, \dots, a^n$ are distinct.

If not and if possible, let there be repetition. *i.e.* $a^m = a^r$; $0 < r < m$. Thus we have

$$a^m a^{-r} = a^r a^{-r} = e, \text{ i.e. } a^{m-r} = e \text{ with } 0 < (m-r) < n.$$

This contradicts to the fact that the order of a is n. So, our supposition is wrong. Hence all elements are distinct. Therefore G contains exactly n elements.

5.5.4 Theorem

A finite group G of order n containing an element of order n must be cyclic.

Proof : Let us consider G be a finite group of order n. Let a be an element of G with order n.

This implies that

$$a^n = e.$$

Let us construct an cyclic group G_1 with generator a. Thus we have $G_1 = \{a, a^2, a^3, \dots, a^n = e\}$

But we know that order of group and order of its generator is same. This implies that

$$O(G_1) = O(a) = O(G).$$

i.e. $$O(G_1) = O(G)$$

Again let $$a \in G_1$$

$$\Rightarrow \quad a^n \in G_1$$

$$\Rightarrow \quad a^n \in G$$

This implies that $G_1 \subseteq G$; but $O(G_1) = O(G)$. Therefore $G = G_1$. Hence G is a cyclic group.

5.5.5 Theorem

Subgroup of a cyclic group is itself a cyclic group.

Proof : Let G be a cyclic group with generator a and let H be the subgroup of G.

Now as H is contained in G, the elements of H are of the type a^k. Let m be the least positive integer such that

$$a^m \in H$$

Let $a^k \in H$, where k is an integer greater than m, *i.e.* $k > m$.

This implies that $$k = mn + r;\ 0 \le r \le m\ a^{-mn} \qquad \dots(i)$$

But we know that the elements of H are in the form of integral power of a. Therefore $a^{mn} \in H$. This implies that $a^{-mn} \in H$.

Now $a^k \in H$ and $a^{-mn} \in H$. So by closure property we have $a^k \,.\, a^{-mn} \in H$

$$\Rightarrow \quad a^{k-mn} \in H$$

$$\Rightarrow \quad a^{mn+r-mn} \in H$$

$$\Rightarrow \quad a^r \in H$$

This contradicts to the assumption that m is the least positive integer for which $a^m \in H$. So $a^r \in H$ is possible only if $r = 0$. Thus we have from equation (i) $k = mn$.

Thus $$a^k = a^{mn} = (a^m)^n.$$

Therefore H is a cyclic group with generator a^m.

■ 5.6 COSETS

Associated with any subgroup there are two cosets namely left coset and right coset. Let G be a group and H be any subgroup of G and let $a \in$ G. The left coset of H in G is the set aH given by

$$a\text{H} = \{x \mid x = ah, \forall\, h \in \text{H}\}$$

The Right coset of H in G is the set Ha given by

$$\text{H}a = \{x \mid x = ha, \forall\, h \in \text{H}\}$$

The cosets are not necessarily subgroup of G. If G is an abelian group, then the left coset of H in G is equal to the right coset of H in G.

5.6.1 Theorem

If H is subgroup of a group G and $h \in$ H, then Hh = H = hH.

Proof : Given that H is a subgroup of group G and $h \in$ H.

Our claim is Hh = H, *i.e*. H$h \subseteq$ H and H $\subseteq$ Hh.

Let $h_1 \in$ H. Again $h_1 \in$ H and $h \in$ H implies that $(h_1\, h) \in$ H.

But we know that being the right coset $(h_1\, h) \in$ Hh.

Thus $\qquad (h_1\, h) \in \text{H}h \Rightarrow (h_1\, h) \in \text{H}.$

Therefore $\qquad \text{H}h \subseteq \text{H}$ ...(*i*)

Now $\qquad h_1 \in \text{H}$

and
$$\begin{aligned} h_1 &= h_1 e \\ &= h_1(h^{-1}\, h) && \text{[By existence of identity]} \\ &= (h_1\, h^{-1})\, h && \text{[By associative law]} \end{aligned}$$

Therefore, $\qquad h_1 = (h_1\, h^{-1})\, h \in \text{H}h$

Hence, we get $h_1 \in \text{H} \Rightarrow h_1 \in \text{H}h$. Thus we get

$$\text{H} \subseteq \text{H}h \qquad \text{... }(ii)$$

Therefore on combining equations (*i*) and (*ii*) we get Hh = H.

Similarly it can be shown that hH = H.

Therefore we have $\qquad$ Hh = H = hH.

■ 5.7 HOMOMORPHISM

A mapping ϕ defined from a group G_1 with binary operation (o) to the group G_2 with binary operation (*) is said to be homomorphism if

$$\phi\,(x\,{}_o\,y) = \phi(x) * \phi(y)\ \forall\, x, y \in G_1$$

5.7.1 Theorem

If ϕ is a homomorphism defined from G_1 to G_2, then

(*i*) $\phi\,(e_1) = e_2$; e_1 is the identity element of G_1 and e_2 is the identity element of G_2.

(*ii*) $\phi\,(x^{-1}) = (\phi\,(x))^{-1}$; $\forall\, x \in G_1$

Proof: (*i*) Given that ϕ is a homomorphism from G_1 to G_2. Also given that e_1 is the identity element of G_1 and e_2 is the identity element of G_2.

Let $x \in G_1$. This implies that $\phi\,(x) \in G_2$. Now $e_1 \in G_1$ such that $x\, e_1 = x$.

Therefore $\qquad \phi\,(x) = \phi\,(x\, e_1)$

$$= \phi(x)\,\phi(e_1) \qquad [\because \ \phi \text{ is a homomorphism}]$$

i.e. $$\phi(x) = \phi(x)\,\phi(e_1) \qquad \ldots(i)$$

Again as e_2 is the identity element of G_2 we have

$$\phi(x) = \phi(x)\,e_2 \qquad \ldots(ii)$$

Hence from equations (*i*) and (*ii*) it is clear that

$$\phi(x)\,\phi(e_1) = \phi(x) = \phi(x)\,e_2$$

$$\Rightarrow \quad \phi(e_1) = e_2 \qquad [\text{Left cancellation law}]$$

(*ii*) Given that ϕ is a homomorphism from G_1 to G_2. Also given that e_1 is the identity element of G_1 and e_2 is the identity element of G_2.

Let $x \in G_1$ such that $(x\,x^{-1}) = e_1$

$$\Rightarrow \quad \phi((x\,x^{-1})) = \phi(e_1)$$

$$\Rightarrow \quad \phi(x)\,\phi(x^{-1}) = \phi(e_1) \qquad [\phi \text{ is a homomorphism}]$$

$$\Rightarrow \quad \phi(x)\,\phi(x^{-1}) = e_2$$

Hence it is clear that $\phi(x^{-1})$ is the inverse element of $\phi(x)$.

Thus we have $\phi(x^{-1}) = (\phi(x))^{-1}$; $\forall\, x \in G_1$

i.e. Inverse element corresponds to the inverse element.

5.7.2 Theorem

If $\phi : G_1 \to G_2$ is a homomorphism, then $\phi(G_1)$ is a subgroup of G_2.

Proof : Given $\phi : G_1 \to G_2$ is a homomorphism. Then for $x, y \in G_1$ we have $\phi(x\,y) = \phi(x)\,\phi(y)$.

Again $\phi(x) \in \phi(G_1), \phi(y) \in \phi(G_1)$ such that

$$\phi(x)\,\phi(y) = \phi(x\,y) \in \phi(G_1).$$

Therefore the closure property is satisfied.

Also $y \in G_1$ implies $y^{-1} \in G_1$ such that $(y\,y^{-1}) = e_1$, where e_1 is the identity element of G_1. Thus we have

$$\phi(y\,y^{-1}) = \phi(e_1)$$

$$\Rightarrow \quad \phi(y)\,\phi(y^{-1}) = \phi(e_1) \qquad [\because \phi \text{ is a homomorphism}]$$

$$\Rightarrow \quad \phi(y)\,\phi(y^{-1}) = e_2 \text{ ; where } e_2 \text{ identity element of } \phi(G_1).$$

Therefore, $(\phi(y))^{-1} = \phi(y^{-1})$.

This indicates that for every element $\phi(y) \in \phi(G_1)$ there exist inverse element $\phi(y^{-1})$ in $\phi(G_1)$.

Hence $\phi(G_1)$ is a subgroup of G_2.

SOLVED EXAMPLES

Example 1 *Show that the subtraction is not a binary operation on the set of natural numbers N.*

Solution: We know that o will be a binary operation in N if and only if $(a \,_o\, b) \in N \ \forall\, a, b \in N$ and $(a \,_o\, b)$ is unique. Here the binary operation is subtraction (–). It is clear that for $a, b \in N$, $(a - b)$ may or may not belongs to N. Let us take $a = 5$ and $b = 10$, so $(a - b) = -5 \notin N$. Hence the subtraction is not a binary operation.

Example 2 *The operation o defined by the relation* $(a \,_o\, b) = \dfrac{a}{b}$ *is not a binary operation in the set of real number R.*

Solution: We know that o will be a binary operation in R if and only if $(a\ _o\, b) \in$ R $\forall\, a, b \in$ R and $(a\ _o\, b)$ is unique. Here the binary operation o defined by the relation $(a\ _o\, b) = \frac{a}{b}$. It is clear that $\frac{a}{b}$ is not defined for $b = 0$. Let us take $a = 5$ and $b = 0$, but $\frac{5}{0}$ is not defined. Hence the operation o defined by the relation $(a\ _o\, b) = \frac{a}{b}$ is not a binary operation on R.

Example 3 *Is the following a valid definition of binary operation.*

(a) $(a\ _o\, b) = a\, b + 2b$ *on R*
(b) $(a\ _o\, b) = a^b$ *on* I^+
(c) $(a\ _o\, b) = \text{Min}\ (a, b)$ *on R*

Solution: (*a*) Let $a, b \in$ R

$\Rightarrow$ $(a\, b) \in$ R [Product of two real numbers is also a real number]

Again $b \in$ R implies that $2b \in$ R.

We know that addition of two real numbers is also a real number, so $(ab + 2b) \in$ R and it is unique. Hence the operation $(a\ _o\, b) = a\, b + 2b$ on R satisfies the definition of binary operation.

(*b*) Let $a, b \in$ I $^+$ (Set of positive integers)

Given that $(a\ _o\, b) = a^b$. We know that a positive integer raised to the power by a positive integer will always result on a positive integer and it is unique also.

This implies that a^b is a unique positive integer. Hence $(a\ _o\, b) = a^b$ is a binary operation.

(*d*) Let $a, b \in$ R (Set of real numbers)

Given that $(a\ _o\, b)$ = Min (a, b). Which is equal to either a or $b \in$ R. This implies that $(a\ _o\, b)$ = Min (a, b) is a binary operation in R.

Example 4 *Let A = {0, 1}, then define the binary operations for and* ($\wedge$) *and or* ($\vee$).

Solution: Given that A = {0, 1}. The binary operations for and ($\wedge$) and or ($\vee$) is given as below.

$\vee$	1	0
1	1	1
0	1	0

$\wedge$	1	0
1	1	0
0	0	0

Example 5 *Complete the following table so that the binary operation (o) is commutative.*

o	*a*	*b*	*c*
a	*b*		
b	*c*	*b*	*a*
c	*a*		*c*

Solution: *A binary operation (o) in set G is said to be commutative if* $(a\ _o\, b) = (b\ _o\, a)$. *Since binary operation (o) is commutative we have the followings.*

$$(a\ _o\, b) = (b\ _o\, a) = c$$
$$(a\ _o\, c) = (c\ _o\, a) = a$$
$$(c\ _o\, b) = (b\ _o\, c) = a$$

Thus the complete table is given below.

o	a	b	c
a	b	c	a
b	c	b	a
c	a	a	c

Example 6 *For the algebraic structure (G, o), defined by* $(a\ _0\ b) = a + b - ab$*;* $a, b \in G$*. Show that G is a semi group, monoid and also show that commutative property holds.*

Solution: Given that for all $a, b \in$ G, $(a\ _0\ b) = a + b - ab$.

Semi group: Let $a, b, c \in$ G

Now $a\ _0\ (b\ _0\ c) = a\ _0\ (b + c - bc)$

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

Again $(a\ _0\ b)\ _0\ c = (a + b - ab)\ _0\ c$

$$= (a + b - ab) + c - c\,(a + b - ab)$$
$$= a + b + c - ab - ca - bc + abc$$

Comparing the above two we see $a\ _0\ (b\ _0\ c) = (a\ _0\ b)\ _0\ c$. This implies that (G, o) is a semi group.

Monoid : We know that the algebraic structure (G, o) is monoid if it is a semi group and has an identity element. We have already shown that (G, o) is a semi group.

Let us now try to find the unit element $e \in$ G such that $(a\ _0\ e) = a$. *i.e.* $a + e - ae = a$

$\Rightarrow$ $a + e\,(1 - a) = a$

$\Rightarrow$ $e\,(1 - a) = a - a = 0$

$\Rightarrow$ $e = 0$

So, the unit element 0 (Zero) exist in G.

Commutative Law: G is said to be commutative if $(a\ _0\ b) = (b\ _0\ a)$.

Now $(a\ _0\ b) = a + b - ab$ and $(b\ _0\ a) = b + a - ba$. This implies that $(a\ _0\ b) = (b\ _0\ a)$, hence commutative.

Example 7 *A set G = {a, b, c, d}, the binary operation (o) on this set is defined by the following figure. Find the followings.*

(a) $(a\ _0\ b)$ *and* $(b\ _0\ a)$

(b) Is binary operation (o) commutative.

(c) Is binary operation (o) associative.

o	a	b	c	d
a	a	c	b	d
b	d	a	b	c
c	a	d	a	a
d	d	b	a	c

Solution: Given that G = $\{a, b, c, d\}$. The binary operation (o) on this set is defined by the following figure.

o	a	b	c	d
a	a	c	b	d
b	d	a	b	c
c	c	d	a	a
d	d	b	a	c

(a) $(a\,_o\,b) = c$ and $(b\,_o\,a) = d$

(b) As $(a\,_o\,b) \neq (b\,_o\,a)$, so the binary operation as defined is not commutative.

(c) Now $a\,_o\,(b\,_o\,c) = a\,_o\,(b) = c$ and

$$(a\,_o\,b)\,_o\,c = c\,_o\,c = a$$

So, $$a\,_o\,(b\,_o\,c) \neq (a\,_o\,b)\,_o\,c.$$

This implies that the binary operation defined above is not associative.

Example 8 *Given the algebraic structure (G, o), defined by the following table. Show that G is a semi group, monoid and find the unit element.*

o	a	b	c
a	c	b	a
b	b	c	b
c	a	b	c

Solution: Given the algebraic structure (G, o), defined by the following table as

o	a	b	c
a	c	b	a
b	b	c	b
c	a	b	c

Semi group: Let $a, b, c \in$ G

Now $$a\,_o\,(b\,_o\,c) = a\,_o\,b = b \text{ and } (a\,_o\,b)\,_o\,c = b\,_o\,c = b$$
$$b\,_o\,(a\,_o\,c) = b\,_o\,a = b \text{ and } (b\,_o\,a)\,_o\,c = b\,_o\,c = b$$
$$c\,_o\,(a\,_o\,b) = c\,_o\,b = b \text{ and } (c\,_o\,a)\,_o\,b = a\,_o\,b = b$$

Therefore, the algebraic structure (G, o) is a semi group.

Monoid: We know that the algebraic structure (G, o) is monoid if it is a semi group and has an identity element.

We have already shown that (G, o) is a semi group.

Let us now try to find the unit element $e \in$ G. It is very clear from the table that

$$(a\,_o\,c) = a = (c\,_o\,a)$$
$$(b\,_o\,c) = b = (c\,_o\,b) \text{ and}$$
$$(c\,_o\,c) = c = (c\,_o\,c)$$

Therefore the identity element is given as $e = c$.

Thus the algebraic structure (G, o) is a monoid.

Example 9 *G contains real numbers 1, – 1 under the usual multiplication. Then show that G is a commutative group of order 2.*

Solution: Given G = {1, –1} and the binary operation (o) is multiplication (*). Let us construct the table.

*	1	–1
1	1	–1
–1	–1	1

Closure Law: From the above table it is clear that the binary operation with any two element results either 1 or –1. So the closure property is satisfied.

Associative Law: From the above table it is clear that the associative property is also satisfied.

Existence of Identity: From the above table it is clear that the identity element is 1 ∈ G.

Existence of Inverse: From the above table it is clear that (1 * 1) = 1 and (–1 * –1) = 1. Therefore 1 and – 1 are their own inverses.

Commutative Law: From the table it is clear that 1 * (–1) = (–1) * 1. So, commutative property is also satisfied.

Therefore G is an abelian group of order 2.

Example 10 *Show that the set G = {1, ω, ω²} is a group with respect to binary operation multiplication, where ω is the cube root of unity.*

Solution: Given ω is the cube root of unity. Thus us have $\omega^3 = 1$ and $1 + \omega + \omega^2 = 0$. It is also given that the binary operation (o) is also a multiplication. Let us construct the table.

*	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

Closure Law : As seen from the table all the elements belongs to the Set G. So, Closure law is satisfied.

Associative Law : The elements of G are complex numbers and we know that complex number multiplication is associative. Thus associative law is satisfied.

Existence of Identity: From the table it is clear that 1 ∈ G is the identity element.

Existence of Inverse: From the table it is also clear that 1 * 1 = 1; $\omega * \omega^2 = \omega^3 = 1$ and $\omega^2 * \omega = \omega^3 = 1$.

Hence it is clear that ω is the inverse element of ω^2, ω^2 is the inverse element of ω and 1 is the inverse element of 1. So, every element of G has its inverse in G.

Therefore the set G = {1, ω, ω^2 }is a group with respect to binary operation multiplication.

Example 11 *Give an example of a group of second order such that every element is its own inverse.*

Solution: Let us consider the set G = {1, –1} and the binary operation (o) is multiplication (*). Let us construct the table.

*	1	–1
1	1	–1
–1	–1	1

Closure Law: From the above table it is clear that the binary operation with any two element results either 1 or – 1. So the closure property is satisfied.

Associative Law: From the above table it is clear that the associative property is also satisfied.

Existence of Identity: From the above table it is clear that the identity element is 1 ∈ G.

Existence of Inverse: From the above table it is clear that (1 * 1) = 1 and (– 1 * – 1) = 1. Therefore 1 and – 1 are their own inverses.

Therefore, G is a group of second order. *i.e.* O(G) = 2.

Example 12 *G is a set of all non-zero real numbers and let* $(a\,_{0}\,b) = \dfrac{ab}{2}$. *Show that (G, o) is an abelian group.*

Solution: Given that G is a set of real numbers.

Closure Law: Let $a, b \in$ G. We know that product of any two real numbers is a real number. This implies that $(ab) \in$ G. Similarly $\dfrac{ab}{2} \in$ G. Therefore $(a\,_{0}\,b) \in$ G.

Associative Law: Let $a, b, c \in$ G.

Now $a\,_{0}\,(b\,_{0}\,c) = a\,_{0}\left(\dfrac{bc}{2}\right) = \dfrac{abc}{4}$ and $(a\,_{0}\,b)\,_{0}\,c = \left(\dfrac{ab}{2}\right)_{0}c = \dfrac{abc}{4}$. Therefore $a\,_{0}\,(b\,_{0}\,c) = (a\,_{0}\,b)\,_{0}\,c$

Existence of Identity: Let $a \in$ G and $e \in$ G be the identity element such that $(a\,_{0}\,e) = a$. *i.e.* $\dfrac{ae}{2} = a$. This implies that $e = 2 \in$ G. So every element of G has 2 as the identity element.

Existence of Inverse: Let $a \in$ G and $a^{-1} \in$ G be the inverse element of a.

Thus we have $(a\,_{0}\,a^{-1}) = e = 2$. This implies that $a^{-1} = \dfrac{4}{a} \in$ G as $4 \in$ G, $a \in$ G and ratio of two non zero real number is a real number.

Commutative Law: Now $(a\,_{0}\,b) = \dfrac{ab}{2} = \dfrac{ba}{2} = (b\,_{0}\,a)$. This implies that $(a\,_{0}\,b) = (b\,_{0}\,a)$. Therefore commutative law also holds in G.

Thus (G, o) is an abelian group.

Example 13 *Let G be the set of all (2 ×2) real matrices* $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *where (ad – bc) ≠0 is a rational number. Prove that G forms a group under multiplication.*

Solution: Let us consider G be the set of all (2 × 2) real matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where $(ad - bc) \neq 0$ is a rational number.

Closure Law: Let A, B $\in$ G. *i.e.* A and B are two matrices of order (2 × 2). This implies that (A × B) is also a real matrix of order (2 × 2).

From the definition it is clear that $|A| \neq 0$ and $|B| \neq 0$, Hence $|A \times B| = |A| \times |B| \neq 0$. Thus (A × B) is a matrix of order (2 × 2) and $|A \times B| \neq 0$. So, (A × B) $\in$ G. Therefore closure law is satisfied.

Associative Law: We know that matrix multiplication is associative. So, for A, B, C $\in$ G we have A × (B × C) = (A × B) × C. Therefore associative law is satisfied.

Existence of Inverse: The matrix I = $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in$ G, since $|I| = 1 \neq 0$, will act as the identity element since

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Existence of Inverse: For every A $\in$ G, there exists inverse $A^{-1} \in$ G such that $(A \times A^{-1}) = I$, where

$$A^{-1} = \frac{\text{Adj(A)}}{|A|} = \frac{1}{|A|}\begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix}$$; c_{ij} is the cofactor of a_{ij} .

Therefore G forms a group under multiplication.

Example 14 *Let G be the set {a_0, a_1, a_2, …. , a_6}.The binary operation (o) is defined as below. Check whether (G, o) is a group or not.*

$$(a_{i\ o}\, a_j) = \begin{cases} a_{i+j} & \textit{if } (i+j) < 7 \\ a_{i+j-7} & \textit{if } (i+j) \geq 7 \end{cases}$$

Solution: Let G = {a_0 , a_1 , a_2 , …. , a_6 }. The binary operation (o) is defined as

$$(a_{i\ o}\, a_j) = \begin{cases} a_{i+j} & \text{if } (i+j) < 7 \\ a_{i+j-7} & \text{if } (i+j) \geq 7 \end{cases}$$

Based on the binary operation defined above we have

$$(a_{0\ o}\, a_0) = a_0 \text{ ; } (a_{0\ o}\, a_1) = a_1\text{; } (a_{5\ o}\, a_1) = a_6\text{;}$$

$(a_{5\ o}\, a_2) = a_{\ 7-7} = a_0$;$(a_{6\ o}\, a_3) = a_{\ 9-7} = a_2$; and so on. Thus we have the following table.

0	a_0	a_1	a_2	a_3	a_4	a_5	a_6
a_0	a_0	a_1	a_2	a_3	a_4	a_5	a_6
a_1	a_1	a_2	a_3	a_4	a_5	a_6	a_0
a_2	a_2	a_3	a_4	a_5	a_6	a_0	a_1
a_3	a_3	a_4	a_5	a_6	a_0	a_1	a_2
a_4	a_4	a_5	a_6	a_0	a_1	a_2	a_3
a_5	a_5	a_6	a_0	a_1	a_2	a_3	a_4
a_6	a_6	a_0	a_1	a_2	a_3	a_4	a_5

Closure Law: From the table it is clear that all the elements are in G. So, closure property is satisfied.

Associative Law: Let a_i, a_j , $a_k \in$ G. Now it is evident from the table that

$$a_{i\ o}(a_{j\ o}\, a_k) = \begin{cases} a_{(i+j+k)} & \text{if } (i+j+k) < 7 \\ a_{(i+j+k-7)} & \text{if } 7 < (i+j+k) < 14 \\ a_{(i+j+k-14)} & \text{if } (i+j+k) \geq 14 \end{cases}$$

Same definition holds for $(a_{i\ o}\, a_j)\ o\ a_k$. So, associative property is satisfied.

Existence of Identity: From the first row of the table it is clear that $a_0 \in$ G is the identity element as $(a_{0\ o}\, a_j) = a_j$ for all j = 0, 1, 2, 3, 4, 5, 6.

Existence of Inverse: From the table it is clear that a_0 is the inverse of a_0 and a_j is the inverse element of $a_{\ (7-j)}$ for J = 1, 2, 3, 4, 5, 6. So, every element has its inverse in G.

Therefore, G is a group under the binary operation defined above.

Example 15 *If G is a group of even order then there exists an element $a \neq e$ such that $a^2 = e$.*

Solution: Given G is a group of even order.

Let there be n elements and its n number of inverses. So altogether there are $2n$ number of elements. Again in this $2n$ number of elements there is an identity element $e \in$ G and $e^{-1} = e$.

This implies G contains $(2n - 1)$ number of elements, but it is given that G is of even order. So there must exist at-least one element which is its own inverse.

i.e. $a \in G \Rightarrow a^{-1} = a$

$\Rightarrow$ $(a\ _o\ a^{-1}) = (a\ _o\ a)$

$\Rightarrow$ $e = a^2$

i.e. $a^2 = e$.

Example 16 *Suppose that G is a group and $a^2 = a$, $a \in G$. Prove that $a = e$.*

Solution: Given that $a^2 = a$

$\Rightarrow$ $(a\ _o\ a) = (a\ _o\ e)$. So, by left cancellation law $a = e$.

Example 17 *If every element of the group G is its own inverse, then it is an abelian group.*

Solution: Given every element of group G is its own inverse.

Let $a, b \in$ G implies that $a^{-1} = a$ and $b^{-1} = b$.

Again by closure law $a, b \in$ G implies that $(a\ _o\ b) \in$ G and $(a\ _o\ b)^{-1} = (a\ _o\ b)$.

$\Rightarrow$ $(b^{-1}\ _o\ a^{-1}) = (a\ _o\ b)$ [By Theorem]

$\Rightarrow$ $(b\ _o\ a) = (a\ _o\ b)$ $[a^{-1} = a$ and $b^{-1} = b]$

Therefore G is an abelian group.

Example 18 *If G is a group with $(a\ _o\ b)^n = a^n\ b^n$ for three consecutive integers, then G is an abelian group.*

Solution: Given G is a group and $(a\ _o\ b)^n = a^n\ b^n$ for three consecutive integers.

Let the three consecutive integers be n, $(n + 1)$ and $(n + 2)$. So, by definition we have

$(a\ _o\ b)^n = a^n\ b^n$; $(a\ _o\ b)^{n+1} = a^{n+1} b^{n+1}$ and

$(a\ _o\ b)^{n+2} = a^{n+2} b^{n+2}$

Now $(a\ _o\ b)^{n+2} = (a\ _o\ b)^{n+1}\ (a\ _o\ b)$

$\Rightarrow$ $a^{n+2}\ b^{n+2} = (a^{n+1}\ b^{n+1})\ (a\ _o\ b)$

$\Rightarrow$ $(a^{n+1}\ a)\ b^{n+2} = (a^{n+1})\ (b^{n+1}\ a)\ _o\ b$

$\Rightarrow$ $(a^{n+1})\ (a\ b^{n+2}) = (a^{n+1})\ (b^{n+1}\ a)\ _o\ b$

$\Rightarrow$ $(ab^{n+2}) = (b^{n+1}\ a)\ _o\ b$ [Left cancellation law]

$\Rightarrow$ $(ab^{n+1})\ b = (b^{n+1}\ a)\ _o\ b$

$\Rightarrow$ $(ab^{n+1}) = (b^{n+1}\ a)$ [Right cancellation law]

$\Rightarrow$ $a^n\ (ab^{n+1}) = a^n\ (b^{n+1}\ a)$

$\Rightarrow$ $(a^{n+1}\ b^{n+1}) = (a^n\ b^n)\ (b\ _o\ a)$

$\Rightarrow$ $(a\ _o\ b)^{n+1} = (a\ _o\ b)^n\ (b\ _o\ a)$

$\Rightarrow$ $(a\ _o\ b)^n\ (a\ _o\ b) = (a\ _o\ b)^n\ (b\ _o\ a)$

$\Rightarrow$ $(a\ _o\ b) = (b\ _o\ a)$ [Left cancellation law]

This implies that G is an abelian group.

Example 19 *G is the set of all integers and the binary operation (o) is defined by $(a\ _o\ b) = a - b$. Test whether G is a group.*

Solution: Given that G is the set of all integers and the binary operation (o) is defined by $(a\ _o\ b) = a - b$.

Closure Law : We know that difference of two integers is an integer. So, for $a, b \in$ G, we have $(a - b) \in$ G. Thus $(a\ _o\ b) \in$ G. Therefore closure law is satisfied.

Associative Law: Let $a, b, c \in$ G.

Now $a\ _o\ (b\ _o\ c) = a\ _o\ (b - c)$

$= a - (b - c)$

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

Again $(a\ _o\ b)\ _o\ c = (a - b)\ _o\ c$

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

$$= a - b - c \qquad \ldots (ii)$$

From the equations (i) and (ii) it is clear that $a \,_o (b \,_o c) \neq (a \,_o b) \,_o c$. Therefore associative law is not satisfied. Hence G is not a group.

Example 20 *Let G = {1, – 1, i, – i } be a group under the binary operation multiplication. Find the order of elements.*

Solution: Given G = {1, – 1, i, – i } be a group under the binary operation multiplication. Therefore the identity element is 1.

Now $O(1) = 1 \qquad [\because \quad (1)^1 = 1]$

$O(-1) = 2 \qquad [\because \quad (1)^2 = 1]$

$O(i) = 4 \qquad [\because \quad (i)^4 = (i^2)^2 = (-1)^2 = 1]$

$O(-i) = 4 \qquad [\because \quad (-i)^4 = (i)^4 = (i^2)^2 = (-1)^2 = 1]$

Example 21 *G is the set of positive integers and the binary operation (o) is defined by $(a \,_o b) = ab$. Test whether G is a group.*

Solution: G is the set of positive integers and the binary operation (o) is defined by

$$(a \,_o b) = (a\, b).$$

Closure Law: We know that product of two positive integers is a positive integer. So, for $a, b \in$ G, we have $(a\, b) \in$ G. Thus $(a \,_o b) \in$ G.

Therefore, closure law is satisfied.

Associative Law: Let $a, b, c \in$ G.

Now $a \,_o (b \,_o c) = (a\, b\, c) = (a \,_o b) \,_o c$. Therefore associative law is satisfied.

Existence of Identity: G is the set of positive integer. This implies that $1 \in$ G and $(1_o\, a) = (a \,_o 1) =$ a for all $a \in$ G. Therefore 1 is the identity element of G.

Existence of Inverse : Let $a \in$ G and let b be the inverse of a. Thus we have $(a \,_o b) = 1$. This implies that $b = \frac{1}{a} \notin$ G. Since $\frac{1}{a}$ is not a positive integer. So, inverse element does not exist in G.

Therefore, G is not a group.

Example 22 *Let G = {a, a^2, a^3, a^4, a^5, a^6 = e } be a group under the binary operation multiplication. Find the order of elements.*

Solution: Let G = {$a, a^2, a^3, a^4, a^5, a^6 = e$ } be a group under the binary operation multiplication.

Now $O(a) = 6 \qquad [\because a^6 = e]$

$O(a^2) = 3 \qquad [\because (a^2)^3 = a^6 = e]$

$O(a^3) = 2 \qquad [\because (a^3)^2 = a^6 = e]$

$O(a^4) = 3 \qquad [\because (a^4)^3 = a^{12} = (a^6)^2 = e]$

$O(a^5) = 6 \qquad [\because (a^5)^6 = a^{30} = (a^6)^5 = e]$

$O(a^6) = 1 \qquad [\because (a^6)^1 = e]$

Example 23 *Let G = {0, 1, 2, 3, 4, 5} be a group under the binary operation addition modulo 6. Find the order of elements of the group.*

Solution: Given G = {0, 1, 2, 3, 4, 5} be a group under the binary operation addition modulo 6. Here the identity element is 0 (Zero). *i.e.* O(0) = 1 as $0^1 = 0$. Let us now find out the order of 1.

$$1^1 = 1$$

$$1^2 = 1 \oplus_6 1 = 2$$

$$1^3 = 1 \oplus_6 1^2 = 1 \oplus_6 2 = 3$$

$1^4 = 1 \oplus_6 1^3 = 1 \oplus_6 3 = 4$

$1^5 = 1 \oplus_6 1^4 = 1 \oplus_6 4 = 5$

$1^6 = 1 \oplus_6 1^5 = 1 \oplus_6 5 = 0$

Therefore $O(1) = 6$

Similarly $O(2) = 3; O(3) = 2; O(4) = 3; O(5) = 6.$

Example 24 *Let G is a group and order of every element $a \neq e$ of the group G is two. Show that G is an abelian group.*

Solution: Given G is a group and order of every element $a \neq e$ of the group G is two.

Let $a \in$ G. This implies that $O(a) = 2$. *i.e.* $a^2 = e$

$\Rightarrow \quad (a\,_{o}\,a) = e$

$\Rightarrow \quad (a\,_{o}\,a)\,_{o}\,a^{-1} = e\,_{o}\,a^{-1} = a^{-1}$ [Existence of Identity]

$\Rightarrow \quad a\,_{o}\,(a\,_{o}\,a^{-1}) = a^{-1}$ [Associative Law]

$\Rightarrow \quad a\,_{o}\,e = a^{-1}$ [Existence of Inverse]

$\Rightarrow \quad a = a^{-1}$ [Existence of Identity]

So, every element of G is its own inverse. *i.e.* For $a, b \in$ G we have $a = a^{-1}$ and $b = b^{-1}$.

Again by closure law $(a\,_{o}\,b) \in$ G and $(a\,_{o}\,b)^{-1} = (a\,_{o}\,b)$. This implies that $(b^{-1}\,_{o}\,a^{-1}) = (a\,_{o}\,b)$

i.e. $(b\,_{o}\,a) = (a\,_{o}\,b)$.

Therefore, G is an abelian group.

Example 25 *Show that in a additive group of integers G the order of every element except 0 (zero) is infinite.*

Solution: Given G is the additive group of integers. The identity element in case of additive group of integers is 0 (zero). This implies that $O(0) = 1$ as $0^1 = 0$. Let us consider the next element 1.

Now $1^1 = 1$

$1^2 = 1 + 1 = 2$

$1^3 = 1 + 1 + 1 = 3$

and so on …. . From this it is clear that there exists no such n for which $1^n = 0$. This implies that order of 1 is infinite. The same argument also holds for other integers.

Example 26 *Let G be a group and the order of a, b and $(a\,_{o}\,b)$ be two. Show that G is an abelian group.*

Solution: Given G be a group and the order of a, b and $(a\,_{o}\,b)$ be two. *i.e.* $a^2 = e$; $b^2 = e$ and $(a\,_{o}\,b)^2 = e$.

Now $(a\,_{o}\,b)^2 = e$

$\Rightarrow \quad (a\,_{o}\,b)\,(a\,_{o}\,b) = e$

$\Rightarrow \quad (a\,_{o}\,b)\,(a\,_{o}\,b) = e\,_{o}\,e = a^2\,_{o}\,b^2$

$\Rightarrow \quad a\,_{o}\,(b\,_{o}\,a)\,_{o}\,b = (a\,_{o}\,a)\,_{o}\,(b\,_{o}\,b)$

$\Rightarrow \quad a\,_{o}\,(b\,_{o}\,a)\,_{o}\,b = a\,_{o}\,(a\,_{o}\,b)\,_{o}\,b$ [Associative Law]

$\Rightarrow \quad (b\,_{o}\,a) = (a\,_{o}\,b)$ [Cancellation Law]

Therefore, G is an abelian group.

Example 27 *Is union of two subgroups of a group G is a subgroup of G? If no then explain with the help of a counter example.*

Solution: The union of two subgroups of a group G is not a subgroup of G.

Let us consider the group G = {... – 3, – 2, – 1, 0, 1, 2, 3, ...} with the binary operation addition. Let us define two subgroups H_1 and H_2 of G as

$H_1 = \{0, \pm 2, \pm 4, \pm 6, ... \}$ and $H_2 = \{0, \pm 3, \pm 6, \pm 9, ...\}$. Hence $(H_1 \cup H_2) = \{0, \pm 2, \pm 3, \pm 4, \pm 6, ...\}$. From this it is clear that $2, 3 \in (H_1 \cup H_2)$ implies that $(2 + 3) = 5 \notin (H_1 \cup H_2)$. Therefore closure law is not satisfied.

Hence, $(H_1 \cup H_2)$ is not a subgroup of G.

Example 28 *Suppose G = {... , 2^{-3}, 2^{-2}, 2^{-1}, 1, 2, 2^2, 2^3, ... } is the multiplicative group. Let H = {1, 2, 2^2, 2^3, ...} be the subset of G. Test whether H is a subgroup of G or not.*

Solution: Given G = {... , 2^{-3}, 2^{-2}, 2^{-1}, 1, 2, 2^2, 2^3, ... } is the multiplicative group. Let H = {1, 2, 2^2, 2^3, ...} be the non empty subset of G and $a, b \in$ H implies that $(a\ {}_0\ b) \in$ H. So, H is closed under multiplication.

Again $2 \in$ H implies $2^{-1} \notin$ H. Thus inverse axiom is not satisfied. Therefore H is not the subgroup of G.

Example 29 *Let G be a group of integers under addition and H is the subset of G consisting of all multiples of $n \in N$. Show that H is a subgroup for every value of n.*

Solution: Given G be a group of integers under addition and H is the subset of G consisting of all multiples of $n \in$ N.

Let $a, b \in$ H. This implies that a and b are both multiples of n. Therefore $(a + b)$ is also a multiple of n. So, $(a\ {}_0\ b) = (a + b) \in$ H. Again $a \in$ H implies $-a \in$ H. Therefore H is a subgroup of G.

Example 30 *Suppose that G be the set of all ordered pairs (a, b) of Real numbers; a ≠ 0. The binary operation (o) is defined by (a, b) ${}_o$ (c, d) = (ac, bc + d). Show that (G, o) is a non abelian group. Let H be a subset of G containing elements of the form (1, b). Does H is a subgroup of G.*

Solution: Given G be the set of all ordered pairs (a, b); $a, b \in$ R, $a \neq 0$. The binary operation is defined as $(a, b)\ {}_0\ (c, d) = (ac, bc + d)$.

We have to show that G is a group. *i.e.* G satisfies all the four properties of the group.

Closure Law: Let $(a, b), (c, d) \in$ G; This implies that $a \neq 0$ and $c \neq 0$.

Now $(a, b)\ {}_0\ (c, d) = (ac, bc + d) \in$ G $[ac \neq 0; ac, bc + d \in \text{R}]$

Associative Law: Let $(a, b), (c, d), (e, f) \in$ G.

Now $(a, b)\ {}_0\ [(c, d)\ {}_0\ (e, f)] = (a, b)\ {}_0\ (ce, de + f)$

$= (ace, bce + de + f)$ ... (*i*)

Again $[(a, b)\ {}_0\ (c, d)]\ {}_0\ (e, f) = (ac, bc + d)\ {}_0\ (e, f)$

$= (ace, bce + de + f)$ ... (*ii*)

So, from equations (*i*) and (*ii*) we have

$$(a, b)\ {}_0\ [(c, d)\ {}_0\ (e, f)] = [(a, b)\ {}_0\ (c, d)]\ {}_0\ (e, f)$$

Existence of Identity: Let $(a, b) \in$ G. Let (u, v) be the identity element. Thus we have

$$(a, b)\ {}_0\ (u, v) = (a, b)$$

i.e. $(au, bu + v) = (a, b)$

This implies that $au = a$ and $bu + v = b$. *i.e.* $u = 1$ and $v = 0$. So, the identity element $(u, v) = (1, 0) \in$ G.

Existence of Inverse: Let $(a, b) \in$ G and let (u, v) be the inverse element of (a, b). Thus, we have

$(a, b)\ {}_0\ (u, v) = (1, 0)$ [∵ (1, 0) is the identity element]

i.e. $(au, bu + v) = (1, 0)$

This implies that $au = 1$ and $bu + v = 0$ *i.e.* $u = \frac{1}{a}$ and $v = \frac{-b}{a}$. So, the inverse element of (a, b) is $\left(\frac{1}{a}, \frac{-b}{a}\right) \in$ G. Thus G satisfies all the four properties of group and hence G is a group.

Commutative Law: Let $(a, b), (c, d) \in$ G.

Thus we have $(a, b)\ _{0}\ (c, d) = (ac, bc + d)$ and

$(c, d)\ _{0}\ (a, b) = (ca, da + b)$.

Hence it is clear that $(a, b)\ _{0}\ (c, d) \neq (c, d)\ _{0}\ (a, b)$. Therefore G is not an abelian group.

Let H be a subset of G containing elements of the form $(1, b)$. Now we have check whether H is subgroup or not.

Let $(1, b), (1, c) \in$ H. Such that $(1, b)\ _{0}\ (1, c) = (1, b + c) \in$ H. Hence closure law holds in H.

Let $(1, b) \in$ H. The inverse of $(1, b)$ is $(1, -b) \in$ H. Hence every element of H has an inverse element.

Therefore H is a subgroup of G.

Example 31 *The set of all integers under addition is a cyclic group with generator 1.*

Solution: Let G be the set of all integers.

Now $1^0 = 0$ $[\because \ 10 = e = 0]$ $1^1 = 1$; $1^2 = 1 + 1 = 2$; $1^3 = 1 + 1 + 1 = 3$ and so on ..... $1^{-1} = -1$; $1^{-2} = (1^2)^{-1} = -2$; $1^{-3} = (1^3)^{-1} = -3$ and so on..... So, all the elements of G can be expressed as some powers of 1.

Example 32 *Let G = {0, 1, 2, 3, 4, 5}. Show that G is the cyclic group with generator 1 under addition modulo 6.*

Solution: Given that G = {0, 1, 2, 3, 4, 5}. Here the generator is 1. Again $1^1 = 1$

$$1^2 = 1 \oplus_6 1 = 2$$
$$1^3 = 1 \oplus_6 1^2 = 1 \oplus_6 2 = 3$$
$$1^4 = 1 \oplus_6 1^3 = 1 \oplus_6 3 = 4$$
$$1^5 = 1 \oplus_6 1^4 = 1 \oplus_6 4 = 5$$
$$1^6 = 1 \oplus_6 1^5 = 1 \oplus_6 5 = 0$$
$$1^7 = 1 \oplus_6 1^6 = 1 \oplus_6 0 = 1$$

Therefore we get G = $\{1, 1^2, 1^3, 1^4, 1^5, 1^6 = 0\}$. This indicates that G is the cyclic group with generator 1.

Example 33 *Prove that any group of order 3 is cyclic.*

Solution: Given G is a group of order 3. So G contains 3 elements and one of this element is e where as the other two are distinct elements. Let the distinct elements of G be a and b.

i.e. G = $\{a, b, e\}$

Now by closure property $a \in$ G, $b \in$ G implies $(a\ .\ b) \in$ G. As G has only three elements, we have the following possibilities.

(*i*) $(a\ .\ b) = a$; (*ii*) $(a\ .\ b) = b$ or (*iii*) $(a\ .\ b) = e$.

Suppose that $(a\ .\ b) = a$

$\Rightarrow$ $(a\ .\ b) = a\ .\ e$

$\Rightarrow$ $b = e$ [Left cancellation law]

Suppose that $(a\ .\ b) = b$

$\Rightarrow$ $(a\ .\ b) = b\ .\ e = e.\ b$ [Existence of identity]

$\Rightarrow$ $a = e$ [Right cancellation law]

We have taken that a and b are two distinct elements other then e. Hence both $(a\ .\ b) = a$ and $(a\ .\ b) = b$ are not possible. Thus we must have $(a\ .\ b) = e$.

Similarly $a \in$ G implies $a^2 \in$ G. Hence there arises three cases. *i.e.* (*i*) $a^2 = e$; (*ii*) $a^2 = a$ or (*iii*) $a^2 = b$.

Suppose that $a^2 = e$

$\Rightarrow$ $a^2 = (a\ .\ b)$ $[(a\ .\ b) = e]$

This implies that $a = b$. This is not possible as a and b are distinct.

Suppose that $\quad a^2 = a$

$\Rightarrow \quad (a \,.\, a) = a \,.\, e$

This implies that $a = e$. This is also not possible as a is other than e. Hence we must have $a^2 = b$. Thus we get

$$G = \{e, a, b\} = \{e, a, a^2\}$$

Therefore, G is a cyclic group with generator a.

Example 34 *Let G be the additive group of integers. i.e. G = {... , –3, – 2, – 1, 0, 1, 2, 3, ...}. Let H be the subgroup of G given by H = { ... , – 9, – 6, –3, 0, 3, 6, 9, ... }. Form the right cosets and left cosets.*

Solution: Given that G = {... , – 3, – 2, – 1, 0, 1, 2, 3, ...}.

$$H = \{ \ldots, -9, -6, -3, 0, 3, 6, 9, \ldots \}$$

Let us now form the Right cosets.

Now $0 \in$ G, so

$$H = H + 0 = \{ \ldots, -9 + 0, -6 + 0, -3 + 0, 0 + 0, 3 + 0, 6 + 0, \ldots \}$$
$$= \{ \ldots, -9, -6, -3, 0, 3, 6, 9, \ldots \}$$

Again $1 \in$ G, so

$$H + 1 = \{ \ldots, -9 + 1, -6 + 1, -3 + 1, 0 + 1, 3 + 1, 6 + 1, \ldots \}$$
$$= \{ \ldots, -8, -5, -2, 1, 4, 7, 10, \ldots \}$$

Similarly $2 \in$ G, so

$$H + 2 = \{ \ldots, -9 + 2, -6 + 2, -3 + 2, 0 + 2, 3 + 2, 6 + 2, \ldots \}$$
$$= \{ \ldots, -7, -4, -1, 2, 5, 8, 11, \ldots \}$$

Example 35 *Let $\phi : G \to G$ defined by $\phi(x) = e$, for all $x \in G$, where e is the identity element. Show that ϕ is a homomorphism.*

Solution: Given that $\phi : G \to G$ defined by $\phi(x) = e \ \forall \ x \in G$, where e is the identity element.

Let $\quad x, y \in G$

$\Rightarrow \quad \phi(x) = e$ and $\phi(y) = e$

Now $x, y \in$ G implies that $(x y) \in$ G

Therefore $\quad \phi(x y) = e$

$$= e \,.\, e = \phi(x)\, \phi(y)$$

i.e. $\quad \phi(x y) = \phi(x)\, \phi(y)$

Hence ϕ is a homomorphism.

In this way we can form the right cosets and the left cosets.

Example 36 *Let $\phi : G_1 \to G_2$ defined by $\phi(x) = 2^x$, where G_1 is a group of Real numbers under addition and G_2 is a group of non-zero Real numbers under multiplication. Show that ϕ is a homomorphism.*

Proof : Given that G_1 is a group of Real numbers under addition and G_2 is a group of non-zero Real numbers under multiplication. Let $x, y \in G_1$

This implies $\quad \phi(x) = 2^x \in G_2$ and $\phi(y) = 2^y \in G_2$

Now $x, y \in G_1$ implies that $(x + y) \in G_1$

Therefore $\quad \phi(x + y) = 2^{x+y}$

$$= 2^x\, 2^y = \phi(x)\, \phi(y)$$

i.e. $\quad \phi(x + y) = \phi(x)\, \phi(y)$

Hence ϕ is a homomorphism.

EXERCISES

1. Define the binary operation. Show that the binary operation multiplication is closed on the set A = {1, – 1}.
2. Show that the addition and multiplication are associative binary operation in the set of rational numbers.
3. Show that (I, +) and (R, +) are semi group.
4. Show that the set of integers and real numbers are abelian group under ordinary addition but is not a group under ordinary multiplication.
5. Show that $G = \{\ldots, 3^{-3}, 3^{-2}, 3^{-1}, 1, 3, 3^2, 3^3, \ldots\}$forms an infinite abelian group under ordinary multiplication.
6. Is the set of all even natural numbers forms a group
   (*i*) under addition (*ii*) under multiplication.
7. Distinguish between abelian and non-abelian group. Explain with the help of examples.
8. Let G is a semi group and for any $a, b \in G$; $a^2 b = b = b a^2$. Show that G is an abelian group.
9. Distinguish between the order of an element of a group and order of the group.
10. Show that every finite group of order less than six (6) must be abelian.
11. If G be a cyclic group of order 10, then find out how many generators are there in G.
12. Show that a cyclic group is abelian. Show by an example that the converse is not true.
13. G is a group of all real numbers under addition and H is the set of all integers. Then show that H is a subgroup of G.
14. Can an abelian group have non-abelian subgroup?
15. Can a non-abelian group have an abelian subgroup?
16. Can a non-abelian group have a non-abelian subgroup?
17. Show that homomorphic image of an abelian group is abelian.
18. Show that $G = \{1, \omega, \omega^2\}$ is the cyclic group under multiplication , where ω is the cube root of unity.
19. Show that $G = \{1, -1, i, -i\}$ is the cyclic group under multiplication, where i is the imaginary quantity such that $i^2 = -1$.
20. Form two cyclic subgroups of a cyclic group $G = \{a, a^2, a^3, \ldots, a^8 = e\}$and how many generators are there for G.
21. Let G_1 be a group of non zero Real numbers under multiplication and $G_2 = \{-1, 1\}$be a group under multiplication. Let $\phi : G_1 \to G_2$ defined by
$$\phi(x) = \begin{cases} 1 & \text{if } x > 0 \\ -1 & \text{if } x < 0 \end{cases}$$
   Show that φ is a homomorphism.
22. Let $\phi: G_1 \to G_2$ defined by $\phi(x) = \log_{10}(x)$, where G_1 is a group of positive Real numbers under multiplication and G_2 is a group of all Real numbers under addition. Show that φ is homomorphism.
23. Let $\phi: G_1 \to G_2$ defined by $\phi\begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$, where G_1 be a group of all (2 × 2) matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$: $ad - bc \neq 0$ under matrix multiplication and G_2 be a group of non zero Real numbers under multiplication. Show that φ is a homomorphism.
24. Show that homomorphic image of an abelian group is abelian.

6

Codes and Group Codes

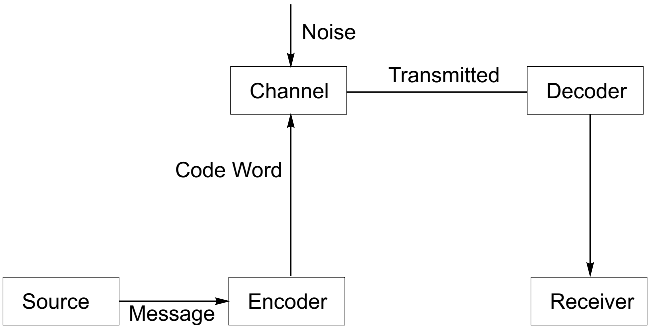
6.0 INTRODUCTION

When we want to send a message to someone, we send it through some communication channel. This transmission of message over a channel entails some chances of undesirable interference in the channel some times deliberate and sometimes due to random defects in the channel.

The coding problem is to represent distinct messages by distinct sequence of letters from a given alphabet set.

For example, in a Morse code we represent a message by dots and dashes. Similarly over alphabet can be {0, 1) *i.e.*, binary alphabet.

When a message is to be transmitted then the message is first given by the source to the encoder, the encoder converts the message into the code word. The encoded message is then sent through the channel, where noise may occur and change the message. When this message arrives at the decoder at the receivers end, it is equated to most likely code word.



Communication Channel with Noise

6.1 TERMINOLOGIES

We will use the following terms in our discussion.

Word: A word is the sequence of letters drawn from the alphabet set.

Code: Code is the collection of words to represent a distinct message.

Code word: A word represented by a code is called the code word.

Block Code: A code consisting of words that are of same length is called Block code. One of the advantages of using the Block Code is its ability to correct errors.

■ 6.2 ERROR CORRECTION

When we transmit a message from the source to the destination, due to the presence of noise in the communication channel the message may get altered, *i.e.* some of the 1's transmitted may be received as 0's and some of the 0's may be received as 1's. So the received message is no more is the transmitted message. Now we would want to recover the transmitted message from the received message. This is called error correction.

■ 6.3 GROUP CODES

Let A be the Set of all binary sequence of length n. Let us define a binary operation ⊕ in A such that X, Y ∈ A implies (X ⊕ Y) ∈ A *i.e.*, a sequence of length n. Where

$$(X \oplus Y) = \begin{cases} 1 & \text{if X, Y differs in position} \\ 0 & \text{if X, Y are same in position} \end{cases}$$

The set A together with the binary operation ⊕, *i.e.* (A, ⊕) forms a Group and a subset G of A is called the group code if (G, ⊕) is a subgroup of (A, ⊕).

Let us consider X = 1 0 0 1 0 0 1 and Y = 0 1 0 1 0 0 1. Therefore we have (X ⊕ Y) = 1 1 0 0 0 0 0.

■ 6.4 WEIGHT OF CODE WORD

Let A be the set of all binary sequence of length n. Let X be a code word in A, the weight of X denoted by ω(X) is the number of 1's in X.

Let us consider the code words X = 10101 and Y = 00011. The number of 1's present in X are three where as the number of 1's present in Y are two. So, the weight of X is 3 and the weight of Y is 2.

i.e., $\omega(X) = 3$ and $\omega(Y) = 2$.

■ 6.5 DISTANCE BETWEEN THE CODE WORDS

Let A be the set of all binary sequence of length n. Let X and Y be two code words in A, the distance between X and Y denoted by d (X, Y) and is defined as the weight of ω (X ⊕ Y).

i.e., $d(X, Y) = \omega(X \oplus Y)$

The distance between the two code words gives the number of positions in which they differ.

Let us consider code words X = 01011 and Y = 10101. Now the distance between X and Y is defined as ω (X ⊕ Y). Now

$$\begin{array}{r} X = 01011 \\ Y = 10101 \\ \hline (X \oplus Y) = 11110 \end{array}$$

Therefore, $d(X, Y) = \omega\,(X \oplus Y) = 4$

6.5.1 Theorem

Let A be the set of all binary sequence of length n. The distance between two code words X and Y satisfies the following properties.

(a) Commutative law *i.e.* $d(X, Y) = d(Y, X)$

(b) Triangle's inequality *i.e.* $d(X, Y) \le d\,(X, Z) + d(Z, Y)$.

Proof : (a) Let A be the set of all binary sequence of length n. Let X and Y be two code words in A.

Therefore $X \oplus Y = Y \oplus X$

This implies that $\omega\,(X \oplus Y) = \omega\,(Y \oplus X)$

Thus, $d(X, Y) = d(Y, X)$

(b) Let A be the set of all binary sequence of length n. Let X ,Y and Z be three code words in A.

We know that ω (X) is the number of 1's in X and $(X \oplus X) = 0$. This implies that $\omega\,(U \oplus V) \le \omega\,(U) + w\,(V)$ ... (1)

Now, $\omega\,(X \oplus Y) = \omega\,(X \oplus Z \oplus Z \oplus Y)$ $[\because\ (Z \oplus Z) = 0]$

$\le \omega\,(X \oplus Z) + \omega\,(Z \oplus Y)$ [By Equation (1)]

Therefore, $d(X, Y) \le d(X, Z) + d(Z, Y)$.

■ 6.6 ERROR CORRECTION FOR BLOCK CODE

We know that block code is a code consisting of words that are of same length. The advantage of using block code is its ability to correct the errors.

Let G be a Block code, the distance of G is defined as the minimum distance between any pair of distinct code words in G. The ability of Block codes to correct the errors depends on its distance.

Let a word has been transmitted and we received a word Y (say). Now there is a likelihood of received word containing an error. Now we will like to have the transmitted word corresponding to the received word Y.

We can use two methods. *i.e.* Maximum likelihood decoding criterion and Minimum distance decoding criterion.

6.6.1 Maximum Likelihood Criterion

Let $X_1, X_2, \ldots\ldots \ldots\ldots, X_n$ be the code words in G. One of this is transmitted and we have received the code word Y. The received word may contain error and we are interested to find the word transmitted. Maximum likelihood criterion says that compute the conditional probabilities $P(X_1 \mid Y), P(X_2 \mid Y), \ldots P(X_n \mid Y)$. Where $P(X_i \mid Y)$ means the probability that X_i is transmitted when the received word is Y. Let

$$P(X_k \mid Y) = \underset{i}{\text{Max}}\,\{P(X_i|Y)\};\ i = 1, 2, \ldots\ldots\ldots\ldots, n$$

Then X_k is the transmitted word.

6.6.2 Minimum Distance Decoding Criterion

In the minimum distance decoding criterion we compute d (X_1, Y), d (X_2, Y), d (X_3, Y), ..., d (X_n ,Y). Let us define

$$d(X_k, Y) = \operatorname*{Min}_i \{d(X_i, Y)\};\ i = 1, 2, 3, ..., n$$

Then, X_k is taken as the transmitted word when the received word is y.

■ 6.7 COSETS

Let (G, ⊕) be a group code. Let a word y is received. Then the coset with respect to y denoted by (G ⊕ y) is defined as

$$(G \oplus y) = \{X_i \oplus y \mid X_i \in G, i \in N\}$$

Again $d(X_i , Y) = \omega\,(X_i \oplus y)$. So the weights of the words in the coset (G ⊕ y) are the distances between the code words in G and y.

The decoding procedure includes the followings:

1. Determine all cosets of G.
2. For each coset, choose the coset leader., *i.e.*, the word of smallest weight.
3. For the received word y, ($e \oplus y$) is the transmitted word.

SOLVED EXAMPLES

Example 1 *Let X = 0101011 and Y = 1010101. Find (X ⊕Y).*

Solution: Given that X = 0101011 and Y = 1010101

$$\begin{array}{lr} \text{Now} & X = 0101011 \\ & Y = 1010101 \\ \hline & (X \oplus Y) = 1111110 \end{array}$$

Therefore, (X ⊕ Y) = 1111110.

Example 2 *A is a set of all binary sequence of length n. Show that (A, ⊕) forms a group.*

Solution: Given that is a set of all binary sequence of length n, say for our convenience we take the length to be 5.

Closure Law: Let X = 01011 and Y = 10101

Now X ⊕ Y = 01011 ⊕ 10101 = 11110

This is again a code word of length 5.

Therefore, X, Y ∈ A implies (X ⊕ Y) ∈ A. So, closure law holds.

Associative Law: Let X = 10101, Y = 10000 and Z = 01010

Now (Y ⊕ Z) = 10000 ⊕ 01010 = 11010

Therefore, X ⊕ (Y ⊕ Z) = 10101 ⊕ 11010 = 01111

So, X ⊕ (Y ⊕ Z) = 01111 ... (1)

Again (X ⊕ Y) = 10101 ⊕ 10000 = 00101

Therefore, (X ⊕ Y) ⊕ Z = 00101 ⊕ 01010 = 01111

So, (X ⊕ Y) ⊕ Z = 01111 ... (2)

Therefore from equations (1) and (2) we get $(X \oplus Y) \oplus Z = X \oplus (Y \oplus Z)$. So, associative law holds.

Existence of Identity: A code word with all zeros of specified length will act as the identity element.

Let $X = 10101$ and $Y = e = 00000$ such that

$$X \oplus Y = 10101 \oplus 00000 = 10101 = X$$

Therefore, $(X \oplus Y) = X$

So, $Y = 00000 \in A$ acts as an identity element.

Existence of Inverse: A code word itself is inverse of its own.

Let $X = 10101$ such that $(X \oplus X) = 10101 \oplus 10101 = 00000 = e$. Therefore, $(X \oplus X) = e$. This implies that every code word is its own inverse. So, $(A, \oplus)$ satisfies all the properties of group and hence called group codes.

Example 3 *Illustrate by example distance function satisfies the commutative and triangle's inequality.*

Solution: Commutative Law: Let $X = 101010$ and $Y = 010101$

So, $(X \oplus Y) = 101010 \oplus 010101 = 111111$

Therefore, $d(X, Y) = \omega\,(X \oplus Y) = 6$ ....(*i*)

Again, $(Y \oplus X) = 010101 \oplus 101010 = 111111$

Therefore, $d(Y, X) = \omega\,(Y \oplus X) = 6$ ...(*ii*)

So, from equations (*i*) and (*ii*) it is clear that $d\,(X, Y) = d(Y, X)$.

Triangle's inequality: Let us take $X = 101010$, $Y = 100010$ and $Z = 101000$. Now

$$\begin{aligned}
(X \oplus Y) &= 101010 \oplus 100010 = 001000\\
(X \oplus Z) &= 101010 \oplus 101000 = 000010\\
(Z \oplus Y) &= 101000 \oplus 100010 = 001010
\end{aligned}$$

Therefore,
$$\begin{aligned}
d(X, Y) &= \omega\,(X \oplus Y) = 1\\
d(X, Z) &= \omega\,(X \oplus Z) = 1\\
d(Z, Y) &= \omega\,(Z \oplus Y) = 2
\end{aligned}$$

Thus we have $d(X, Z) + d(Z, Y) = 1 + 2 = 3 \geq d\,(X, Y) = 1$

i.e. $d\,(X, Y) \leq d(X, Z) + d(Z, Y)$

Example 4 *In the minimum distance criterion, a code of distance (2t + 1) can correct t or fewer transmission errors.*

Solution: Let X be the transmitted word and Y be the received word.

Now if t or less number of errors has occurred during the transmission we will have

$$d(X, Y) \leq t \quad \text{...}(i)$$

Now since the distance is $(2t + 1)$, so for any code word X_1 we have

$$d(X, X_1) \geq 2\,t + 1 \quad \text{...}(ii)$$

Since the distance means the minimum distance between any pairs of distinct code words. Again from triangle's inequality we have

$$d\,(X, X_1) \leq d\,(X, Y) + d\,(Y, X_1)$$

$$\Rightarrow \quad 2t + 1 \leq d(X, X_1) \leq t + d\,(Y, X_1)$$

$$\Rightarrow \quad 2t + 1 \leq t + d\,(Y, X_1)$$

$$\Rightarrow \quad d(Y, X_1) \geq (t + 1) \qquad \ldots (iii)$$

So, we have $d(X, Y) \leq t$ and $d(Y, X_1) \geq (t + 1)$

From the minimum distance decoding criterion X will be selected as the transmitted word.

EXERCISES

1. Let X and Y be two code words. Find (X ⊕ Y) in each of the following cases.

(*a*) X = 11111 and Y = 11111

(*b*) X = 11111 and Y = 00000

(*c*) X = 1010101 and Y = 0101010

(*d*) X = 00101101 and Y = 11101100

(*e*) X = 1100110 and Y = 0011101

2. Find the weight of the following code words.

(*a*) X = 11111 (*b*) X = 11111

(*c*) X = 1010101 (*d*) X = 00101101

(*e*) X = 1100110

3. Find the distance between the code words in each of the following cases.

(*a*) X = 10011 and Y = 00000

(*b*) X = 01101 and Y = 10110

(*c*) X = 0011101 and Y = 0101010

(*d*) X = 11101101 and Y = 10011101

(*e*) X = 1100110 and Y = 1110110

4. Illustrate by example distance function satisfies the associative law and triangle's inequality.

5. Illustrate by example (A, ⊕) forms a group. Where A is a set of all binary sequence of length 7.

7

Ring Theory

■ 7.0 INTRODUCTION

As we have discussed group as an algebraic structure, in this chapter we will discuss about "Ring" which is quite different from the Group in a way that it is two operational systems viz; Addition and multiplication where as the Group is a one operational system. In Ring theory many of the notions of Group theory will be extended to the system with two operations.

■ 7.1 RING

A non empty set R with two binary operations addition (+) and multiplication (.) defined in it is said to be associative Ring if it satisfies the following properties.

Under Addition:

(*a*) Closure Axiom: For $a, b \in$ R; $a + b \in$ R

(*b*) Associative Axiom: For $a, b, c \in$ R; $(a + b) + c = a + (b + c)$

(*c*) Existence of Identity: For every element $a \in$ R, there exist an identity element $0 \in$ R such that

$$a + 0 = 0 + a = a \;\forall\; a \in \text{R}.$$

(*d*) Existence of Inverse: For every element $a \in$ R there exist an inverse element $-a \in$ R such that

$$a + (-a) = 0$$

(*e*) Commutative Axiom: For $a, b \in$ R; $(a + b) = (b + a)$

Under Multiplication

(*a*) Closure Axiom : For $a, b \in$ R; $(a \,.\, b) \in$ R

(*b*) Associative Axiom : For $a, b, c \in$ R; $(a \,.\, b) \,.\, c = a \,.\, (b \,.\, c)$

(*c*) Distributive Axiom : For $a, b, c \in$ R we have

(*i*) $a \,.\, (b + c) = a \,.\, b + a \,.\, c$ [Left distributive Law]

(*ii*) $(b + c) \,.\, a = b \,.\, a + c \,.\, a$ [Right distributive Law]

7.1.1 Theorem

If R is a Ring, then for all $a, b, c \in$ R (*i*) $a \,.\, 0 = 0 \,.\, a = 0$

(*ii*) $a\,(-b) = (-a)\,b = -(ab)$

(*iii*) $(-a)\,(-b) = a\,b$

(*iv*) $a \,.\, (b - c) = a \,.\, b - a \,.\, c$

(*v*) $(b - c) \,.\, a = b \,.\, a - c \,.\, a$

Proof: (*i*) We know that $0 = 0 + 0$

This implies that $a \,.\, 0 = a \,.\, (0 + 0)$

$= a \,.\, 0 + a \,.\, 0$ [Distributive Law]

So, $a \,.\, 0 = a \,.\, 0 + a \,.\, 0$ ... (1)

Again, $a \,.\, 0 = a \,.\, 0 + 0$ ... (2) [Additive Identity Law]

Therefore from equations (1) and (2) we have

$$a \,.\, 0 + 0 = a \,.\, 0 + a \,.\, 0$$

$\Rightarrow$ $0 = a \,.\, 0$ [Left Cancellation law]

Thus, $a \,.\, 0 = 0$ ....(3)

Similarly $0 = 0 + 0$

This implies that $0 \,.\, a = (0 + 0) \,.\, a$

$= 0 \,.\, a + 0 \,.\, a$ [Distributive Law]

So, $0 \,.\, a = 0 \,.\, a + 0 \,.\, a$ ...(4)

Again, $0 \,.\, a + 0 = 0 \,.\, a$ ...(5) [Additive Identity Law]

Therefore from equations (4) and (5) we have

$$0 \,.\, a + 0 = 0 \,.\, a + 0 \,.\, a$$

$\Rightarrow$ $0 = 0 \,.\, a$ ...(6) [Left Cancellation Law]

Combining equations (3) and (6) we get

$$a \,.\, 0 = 0 \,.\, a = 0$$

(*ii*) Given $b \in$ R, so by existence of additive inverse $(-b) \in$ R such that $b + (-b) = 0$

$\Rightarrow$ $a \,.\, (b + (-b)) = a \,.\, 0$

$\Rightarrow$ $a \,.\, b + a \,.\, (-b) = 0$ [By previous (*i*)]

$\Rightarrow$ $a \,.\, (-b) = -(a\,b)$ ...(1)

Again $a \in$ R implies that $-a \in$ R such that

$$a + (-a) = 0$$

$\Rightarrow$ $(a + (-a)) \,.\, b = 0 \,.\, b$

$\Rightarrow$ $a \,.\, b + (-a) \,.\, b = 0$ [By previous (*i*)]

$\Rightarrow$ $(-a) \,.\, b = -(a\,b)$ ...(2)

Combining equations (1) and (2) we get

$$a \,.\, (-b) = -(a \,.\, b) = (-a) \,.\, b$$

(*iii*) Given $a, b \in$ R implies that $-a, -b \in$ R.

Now, $(-a)\,(-b) = (-a) \,.\, x; \quad x = -b$

$= -(a \,.\, x)$ [By previous (*ii*)]

$= -(a \,.\, (-b))$

$= -(-(a \,.\, b))$ [By previous (*ii*)]

$= a \,.\, b$

Therefore, $(-a)\,.\,(-b) = a \,.\, b$

(*iv*) $a \,.\, (b - c) = a \,.\, (b + (-c))$

$= a \,.\, b + a \,.\, (-c)$ [Left distributive Law]

$= a \,.\, b + (-(a \,.\, c))$

$= a \,.\, b - a \,.\, c$

Therefore, $a \,.\, (b - c) = a \,.\, b - a \,.\, c$

(*v*) $(b - c)\,.\, a = (b + (-c))\,.\, a$

$= b \,.\, a + (-c)\,.\, a$ [Right distributive Law]

$= b \,.\, a + (-(c \,.\, a))$

$= b \,.\, a - c \,.\, a$

Therefore, $(b - c)\,.\, a = b \,.\, a - c \,.\, a$

7.1.2 Theorem

If R is a ring with unit element then

(*i*) $(-1)\,.\, a = -a$

(*ii*) $(-1)(-1) = 1$

Proof: (*i*) Given R is a ring with unit element *i.e.* $1 \in$ R.

Now $0 = 0 \,.\, a$

$= (1 + (-1))\,.\, a$

$= 1 \,.\, a + (-1)\,.\, a$

$= a + (-1)\,.\, \text{a}$

i.e. $a + (-1)\,.\, a = 0$

Therefore, $(-1)\,.\, a = -a$

(*ii*) In the previous we have proved that $(-1).\, a = -a$.

Let $a = -1$

So, $(-1)(-1) = -(-1) = 1$

Therefore, $(-1)(-1) = 1$

7.2 SPECIAL TYPES OF RING

In this section we will discuss special types of ring.

7.2.1 Commutative Ring

A ring R is said to be commutative ring if under multiplication

$$(a \,.\, b) = (b \,.\, a) \;\forall\; a, b \in \text{R}.$$

7.2.2 Ring with Unit Element

A ring R is said to be ring with unit element if there exist an element $1 \in$ R such that

$$(1.\, a) = (a \,.\, 1) = a \;\forall\; a \in \text{R}$$

7.2.3 Null Ring

The singleton set {0} with binary operation + and . defined as

$$0 + 0 = 0 \quad \text{and} \quad 0 \,.\, 0 = 0$$

is called a Null Ring or zero Ring.

7.2.4 Boolean Ring

A ring R is said to be Boolean ring if $a^2 = a$ for all $a \in$ R.

7.2.5 Division Ring

A ring R is said to be division ring if the non zero elements of R forms a group under multiplication.

7.2.6 Zero Divisor

Let R be a commutative ring, a element $a \neq 0 \in$ R is said to be zero divisor if there exists $b \neq 0$ such that

$$(a \,.\, b) = 0 \,; \quad a, b \in \text{R}$$

7.2.7 Integral Domain

An integral domain is a commutative ring that has no zero divisors.

Let us consider a set R of integers. From the discussion given below it is clear that R is a commutative ring with unit element.

Under Addition

(*i*) Closure Axiom: We know that the addition of two integer is again an integer.

i.e. $$a, b \in \text{R} \Rightarrow (a + b) \in \text{R}$$

(*ii*) Associative Axiom: We know that addition of integers is associative.

i.e. $$a + (b + c) = (a + b) + c \,; \quad \forall \quad a, b, c \in \text{R}$$

(*iii*) Existence of Identity : For all $a \in$ R, there exists $0 \in$ R such that

$$(a + 0) = (0 + a) = a$$

(*iv*) Existence of Inverse: For every $a \in$ R there exists $-a \in$ R such that

$$a + (-a) = (-a) + a = 0.$$

(*v*) Commutative Axiom: For any $a, b \in$ R we know that the addition of integers is commutative.

i.e. $$(a + b) = (b + a)$$

Under Multiplication

(*i*) Closure Axiom: We know that multiplication of two integers is again an integer.

i.e. $$(a \,.\, b) \in \text{R} \quad \forall \quad a, b \in \text{R}.$$

(*ii*) Associative Axiom: We know that integer multiplication is associative.

i.e. $$a \,.\, (b \,.\, c) = (a \,.\, b) \,.\, c \quad \forall \quad a, b, c \in \text{R}.$$

(*iii*) Distributive Laws: Set of integers follow both left distributive and right distributive property *i.e.* $a.(b+c) = (a \,.\, b) + (a \,.\, c)$

and $(b+c) \,.\, a = (b \,.\, a) + (c \,.\, a) \quad \forall\, a, b, c \in \mathrm{R}$

(*iv*) Commutative Law: We know that multiplication of integers is commutative,

i.e. $(a \,.\, b) = (b \,.\, a)$ for all $a, b \in \mathrm{R}$.

(*v*) Unit Element: As R contains integers, so $1 \in \mathrm{R}$.

Again $(a \,.\, 1) = (1 \,.\, a) = a \;\forall\, a \in \mathrm{R}$

Therefore, R is a commutative ring with unit element.

■ 7.3 RING WITHOUT ZERO DIVISOR

A commutative ring R is said to be without zero divisor if for $a, b \in \mathrm{R}$

$$a \cdot b = 0 \text{ implies } a = 0 \text{ or } b = 0 \text{ or both } a \text{ and } b \text{ are zero.}$$

Set of integers I is a ring without zero divisor as product of integers is zero only if any one of them is zero.

7.3.1 Theorem

A commutative ring R is without zero divisor if and only if the cancellation law holds.

Proof: (*Necessary part*) Let the commutative ring R does not have zero divisor.

Let $a, b, c \in \mathrm{R}, a \neq 0$ and $ab = ac$

$\Rightarrow$ $ab - a\,c = 0$

$\Rightarrow$ $a\,(b - c) = 0$

As $a \neq 0$ and R does not have zero divisor, so we must have $(b - c) = 0$. This implies that $b = c$.

Hence left cancellation law holds.

Similarly it can be shown that right cancellation also holds.

(*Sufficient part*) Let the cancellation law holds in the ring R. We have to show that R has no zero divisor.

If possible, let $(a \,.\, b) = 0$ with $a \neq 0$ and $b \neq 0$

$\Rightarrow$ $(a \,.\, b) = (a \,.\, 0)$ $[\because \; a \,.\, 0 = 0]$

Hence by left cancellation $b = 0$. This contradicts to the fact that $b \neq 0$.

Therefore, R is a ring without zero divisor.

■ 7.4 INTEGRAL DOMAIN

A commutative ring without zero divisors is an integral domain.

Set of integers is an integral domain since it forms a commutative ring but does not have zero divisors.

■ 7.5 DIVISION RING

If the non-zero elements of a ring R form a group under multiplication then the ring R is said to be a division ring.

7.6 FIELD

A ring F is said to be a field if the non-zero elements form a multiplicative abelian group. It is defined also as a commutative division ring. Besides this if, every element $a \neq 0$ of an integral domain has a multiplicative inverse a^{-1}, then the integral domain is called as a field.

7.6.1 Theorem

Every field is an integral domain.

Proof: Suppose that F be a field. This indicates that F is a commutative division ring. *i.e.* The non-zero elements of F forms a group under multiplication.

Our claim is to show F is an integral domain. *i.e.* F does not have the zero divisor.

Let $a, b \in \mathrm{F}$ and $a \neq 0$ such that

$$a \,.\, b = 0$$

$\Rightarrow$ $a^{-1}.\,(a\,.\,b) = a^{-1}.\,0$ $[\because a \neq 0 \Rightarrow a^{-1} \in \mathrm{F}]$

$\Rightarrow$ $(a^{-1}.\,a)\,.\,b = 0$ [Associative Law]

$\Rightarrow$ $1\,.\,b = 0$

$\Rightarrow$ $b = 0$

Thus, we get $(a\,.\,b) = 0, a \neq 0 \Rightarrow b = 0$

Similarly we can show that $(a\,.\,b) = 0, b \neq 0 \Rightarrow a = 0$

So, the field F does not have a zero divisor. Hence, F is an integral domain.

7.6.2 Theorem

A finite integral domain is a field.

Proof : Let R be a finite integral domain.

Let $\mathrm{R} = \{x_1, x_2, \ldots\ldots, x_n\}$; where the elements of R are distinct.

i.e. $x_\mathrm{i} \neq x_j$ for all $i \neq j$; where $i, j = 1, 2, \ldots., n$.

Now since R is an integral domain, so R is a commutative ring without zero divisors.

Our claim is to prove R is a field. *i.e.* It is sufficient to prove that R contains the unit element and every non-zero element has multiplicative inverse.

(*Existence of unity*) Let $a \neq 0 \in \mathrm{R}$

Now, $ax_1, ax_2, ax_3, \ldots., ax_n \in \mathrm{R}$ and all these elements are distinct. If not,

let $ax_i = a\,x_j$ for $i \neq j$

$\Rightarrow$ $(a\,x_i - a\,x_j) = 0$

$\Rightarrow$ $a\,(x_i - x_j) = 0$

$\Rightarrow$ $(x_i - x_j) = 0$ $[\because a \neq 0$ is the additive Identity]

$\Rightarrow$ $x_i = x_j$

This contradicts to the statement $x_1, x_2, \ldots, x_n$ are all distinct.

So, $ax_1, ax_2, ax_3, \ldots, ax_n \in \mathrm{R}$ and are distinct. Therefore one of these elements must be equal to 'a' since $a \in \mathrm{R}$.

Let $a = ax_k$

i.e. $ax_k = a = x_k a$ [R is commutative]

Let us take any element $x_m \in$ R. Now x_m must be equal to $(a\, x_r)$ for some value of r. $1 \le r \le n$.

i.e., $\quad a\, x_r = x_m = x_r .\times a$

Now, $\quad x_k \,.\, x_m = x_k\,(a\, x_r)$

$= (x_k \,.\, a) \,.\, x_r$ [Associative Law]

$= a \,.\, x_r = x_m$

So, $x_k \,.\, x_m = x_m$. This implies that 'x_k' is the identity element and is denoted by 1. Thus, we have the unit element in R.

(*Multiplicative Inverse*)

We have proved that 1$\in$ R. So 1 must be equal to 'ax_i' for some i.

i.e. $\quad ax_i = 1$. Therefore there is some $b \in$ R such that

$$a \,.\, b = 1 = b \,.\, a$$

Hence, b is the multiplicative inverse of the non-zero element a.

7.6.3 Theorem

The commutative ring $Z_p = \{0, 1, 2, ..., p - 1\}$ under the operation $\oplus_p$ and $\otimes_p$ is a field if and only if p is a prime number.

Proof: Given $Z_p = \{0, 1, 2, ..., p - 1\}$ is a commutative ring under addition and multiplication modulo p.

Suppose that p is a prime number.

Let $\quad a, b \in Z_p$ and $a \neq 0, b \neq 0$ and let $(a \,.\, b) \equiv 0 \bmod p$.

This implies $p \mid ab$. *i.e.* $p \mid a$ or $p \mid b$. Therefore, we get

$$a \equiv 0 \bmod p \quad \text{or } b \equiv 0 \bmod p.$$

This contradicts to the fact p is a prime number. Hence, Z_p does not have zero divisors.

Therefore, Z $_p$ is a field.

Conversely, Suppose that Z_p is a field. We have to show that p is a prime number.

Suppose that p is not a prime number.

$\Rightarrow \quad p = m \,.\, n \quad (1 < m, n < p)$

$\Rightarrow \quad m \,.\, n \equiv 0 \bmod p$ ... (1)

Now $\quad n = 1 \,.\, n \bmod p$

$= (m^{-1}.\, m)\, n \bmod p$ $[\because m^{-1}.\, m = 1]$

$= m^{-1}\,(m\, n) \bmod p$

$= m^{-1}.\, 0 = 0$

Thus, we get $n = 0$. This is a contradiction.

Therefore, p is a prime number.

■ 7.7 THE PIGEONHOLE PRINCIPLE

If n objects are distributed over m places and if $(n > m)$ then some places will receive at least two objects. So if n objects are distributed over m places in such a way that no place receives more than one object, then each place will receive exactly one object. This principle is known as Pigeonhole principle.

■ 7.8 CHARACTERISTICS OF A RING

Let (R, + , .) be a ring with 0 as zero element. If there exist a positive integer 'n' such that

$$n \,.\, a = a + a + a + \ldots + a \ (n \text{ times}) = 0 \ \forall \ a \in \text{R}.$$

Then such smallest positive integer 'n' is called the characteristic of the ring. Thus, the characteristic of a ring R is defined as

$$\text{Ch(R)} = \begin{cases} \text{Smallest positive integer } n \text{ such that } n\,a \ = \ 0, \forall\, a \in \text{R} \\ 0 \quad \text{otherwise} \end{cases}$$

If no such 'n' exist then the ring R is said to have a characteristic zero or infinite.

Let us consider the ring $\text{I}_6 = \{0, 1, 2, 3, 4, 5\}$ with the binary operations $\oplus_6$, $\otimes_6$. Then the characteristic of this ring R will be 6 since $6 \,.\, a = 0$ for all $a \in \text{I}_6$.

7.8.1 Theorem

The characteristic of a ring with unity is 0 or $n > 0$ depending on whether unity element is regarded as the member of additive group has the order 0 or 'n' respectively.

Proof: Let R be a ring with unity 1. Hence, there arises two cases.

Case 1 : If the order of 1 is zero then obviously the characteristic of ring is zero.

Case 2 : If the order of 1 is n (finite), then

$$\underbrace{1 + 1 + 1 \,.....\, + 1}_{n - \text{times}} = 0 \quad \forall\, a \in \text{R}$$

$$\Rightarrow \qquad n \,.1 = 0$$

Now for any $a \in$ R we have

$$\begin{aligned} na &= a + a + \text{--------} + a \ (n \text{ terms}) \\ &= 1 \cdot a + 1 \cdot a + \text{--------} + 1 \cdot a \qquad [\because \ 1 \text{ is the unity}] \\ &= (1 + 1 + \text{------} +1) \cdot a \\ &= (n \,.\, 1) \,.\, a = (0 \,.\, a) = 0 \end{aligned}$$

i.e. $\qquad na = 0$

Therefore, the characteristic of R is n.

7.8.2 Theorem

The characteristic of an integral domain is either 0 or a prime number.

Proof : Let R be an integral domain. We have to show that the characteristic of R, *i.e.* Ch (R) is either 0 or a prime number.

Let $\qquad \text{Ch (R)} = n$

Let if possible assume that $n \neq 0$ and not a prime number. Therefore, $n = n_1 \,.\, n_2$ with n_1, n_2 less then n.

Now as the characteristic of R is n, we have the order of the unit element e is 'n'. *i.e.* $0(e) = n$

$$\Rightarrow \qquad n \,.\, e = 0$$

$$\Rightarrow \qquad (n_1 \,.\, n_2)\, e = 0$$

$\Rightarrow \quad n_1 . (n_2 . e) = 0$ [Associative Law]

$\Rightarrow \quad (n_1 . e)(n_2 . e) = 0$ $[\because (n_1 . e) = n_1]$

As R does not have zero divisor so $n_1 . e = 0$ or $n_2 . e = 0$. This indicates that the characteristic of R is either 'n_1' or 'n_2'.

This is a contradiction to the assumption that characteristic of R is 'n'. So, our assumption was wrong. Therefore, 'n' is zero or a prime number.

■ 7.9 SUB RING

For a ring (R, +, .), a nonempty subset S of R is called a sub ring of R if (S,+, .) forms a ring under the binary operations defined in R.

For the ring (I, +, .) the subset of even integers is a sub ring.

7.9.1 Theorem

The necessary and sufficient condition for (S, +, .) to be a sub ring of the ring (R, +, .) is

(*i*) $a - b \in \text{S} \quad \forall \quad a, b \in \text{S}$

(*ii*) $a . b \in \text{S} \quad \forall \quad a, b \in \text{S}$

Where S is the sub set of R.

Proof : (*Necessary part*) Suppose that (S, +, .) be the sub ring of the ring (R, +, .). This implies that S is a group with respect to addition.

Now, for $b \in \text{S}$ we have $(-b) \in \text{S}$.

Again since S is closed under addition so, $(a + (-b)) \in \text{S}$ for $a \in \text{S}$, and $(-b) \in \text{S}$. *i.e.* $(a - b) \in \text{S}$.

Similarly since S is closed under multiplication we have

$$a \in \text{S}, b \in \text{S}$$

$$\Rightarrow \quad a . b \in \text{S}$$

(*Sufficient part*) Suppose that

(*i*) $a - b \in \text{S} \quad \forall \quad a, b \in \text{S}$ and

(*ii*) $a . b \in \text{S} \quad \forall \quad a, b \in \text{S}$

Now $\quad a \in \text{S}, a \in \text{S}$

$\Rightarrow \quad (a - a) \in \text{S}$

$\Rightarrow \quad 0 \in \text{S}$ ... (*i*)

Again, $\quad 0 \in \text{S}, a \in \text{S}$

$\Rightarrow \quad (0 - a) \in \text{S}$

i.e. $\quad -a \in \text{S}$

Again, $\quad a \in \text{S}, -b \in \text{S}$

$\Rightarrow \quad a - (-b) \in \text{S}$

i.e. $\quad (a + b) \in \text{S}.$

The addition and commutative axiom under addition holds in R so it will hold in S. Therefore, (S, +, .) is an abelian group. The remaining postulates will hold in S as they hold in R.

■ 7.10 HOMOMORPHISM

Let R_1 and R_2 be two rings, then the mapping

$\phi: R_1 \to R_2$ is said to be homomorphism if it satisfies the following conditions.

(*a*) $\phi(a + b) = \phi(a) + \phi(b)$

(*b*) $\phi(a \,.\, b) = \phi(a) \,.\, \phi(b) \quad \forall \quad a, b \in R$

7.10.1 Theorem

If ϕ is homomorphism from ring R_1 into Ring R_2 then

(*i*) $\phi(0) = 0$

(*ii*) $\phi(-a) = -\phi(a)$

Proof : (*i*) Let $a \in R_1$. Then there exists an identity element $0 \in R_1$ such that $(a + 0) = a$

$$\begin{aligned}
\Rightarrow \quad & \phi(a + 0) = \phi(a) && \\
\Rightarrow \quad & \phi(a) + \phi(0) = \phi(a) && [\phi \text{ is a homomorphism}] \\
\Rightarrow \quad & \phi(a) + \phi(0) = \phi(a) + 0 && [0 \text{ is additive identity of } R_2] \\
\Rightarrow \quad & \phi(0) = 0 && [\text{Left cancellation Law}]
\end{aligned}$$

(*ii*) For the ring R_1, $a \in R_1$ implies $-a \in R_1$

Now, $a + (-a) = 0$

$$\begin{aligned}
\Rightarrow \quad & \phi(a + (-a)) = \phi(0) && \\
\Rightarrow \quad & \phi(a) + \phi(-a) = 0 && [\because \phi(0) = 0]
\end{aligned}$$

This indicates that $\phi(-a)$ is the additive inverse of $\phi(a)$ in R_2.

Therefore, $\phi(-a) = -\phi(a)$.

7.10.2 Theorem

Let R_1 is a ring with unit element 1 and ϕ is a homomorphism of R_1 into R_2, then $\phi(1)$ is the unit element of R_2.

Proof : Given that the mapping ϕ is homomorphism from ring R_1 into R_2.

i.e. $\phi : R_1 \to R_2$ is homomorphism.

Let $1 \in R_1$, this implies that $\phi(1) \in R_2$.

Now for any $a_1 \in R_2$, we have $a_1 = \phi(a)$ for some $a \in R_1$.

Therefore,
$$\begin{aligned}
\phi(1) \,.\, a_1 &= \phi(1) \,.\, \phi(a) && \\
&= \phi(1 \,.\, a) && [\phi \text{ is a homomorphism}] \\
&= \phi(a) && [\text{Existence of Identity}] \\
&= a_1 &&
\end{aligned}$$

Therefore, $\phi(1) \,.\, a_1 = a_1$. Hence, $\phi(1)$ is the unit element of R_2.

7.10.3 Theorem

Every homomorphic image of a commutative ring is commutative.

Proof : Let R be a commutative ring and ϕ is a homomorphic mapping from R into R′. *i.e.* R′ is the homomorphic image of the commutative ring R.

Our claim is R′ is commutative.

Let $a', b' \in R'$. Hence there exists $a, b \in R$ such that

$$a' = \phi(a), \quad \text{and} \quad b' = \phi(b),$$

Now,
$$\begin{aligned} a' . b' &= \phi(a) . \phi(b) \\ &= \phi(a . b) && [\phi \text{ is a homomorphism}] \\ &= \phi(b . a) && [R \text{ is commutative}] \\ &= \phi(b) . \phi(a) && [\phi \text{ is a homomorphism}] \end{aligned}$$

Therefore, $a' . b' = \phi(b) . \phi(a) = b' . a'$

Hence the homomorphic image R′ is commutative.

■ 7.11 KERNEL OF HOMOMORPHISM OF RING

If ϕ is a homomorphism from ring R into R′, then the kernel of homomorphism is a set denoted by I (ϕ) containing elements of R which are mapped to the additive identity element of R′.

i.e. $$I(\phi) = \{x \in R \mid \phi(x) = 0; 0 \in R'\}$$

7.11.1 Theorem

If ϕ is homomorphism from R into R′ with kernel I(ϕ) then

(*i*) I (ϕ) is a subgroup of R under addition

(*ii*) If $a \in I(\phi)$ and $x \in R$, then $(x . a)$ and $(a . x) \in I(\phi)$

Proof: (*i*) Given ϕ is homomorphism from R into R′ with kernel I(Φ)

Our claim is I(ϕ) is a subgroup of R under addition. *i.e.* I(ϕ) satisfies the closure and inverse axiom.

Let $a, b \in I(\phi)$.

This implies that $\phi(a) = 0$ and $\phi(b) = 0$

Now, $\phi(a + b) = \phi(a) + \phi(b) = 0 + 0 = 0$

Hence, $\phi(a + b) = 0$.

Therefore, $(a + b) \in I(\phi)$.

Again $\phi(-a) = -\phi(a) = 0$

Hence, $\phi(-a) = 0$

Therefore, $-a \in I(\phi)$

This implies that I (ϕ) is subgroup under addition.

(*ii*) Suppose that $a \in I(\phi)$ and $x \in R$.

Now,
$$\begin{aligned} \phi(a . x) &= \phi(a) . \phi(x) && [\phi \text{ is a homomorphism}] \\ &= 0 . \phi(x) && [a \in I(\phi) \Rightarrow \phi(a) = 0] \\ &= 0 \end{aligned}$$

So, $\phi(a . x) = 0$.

This implies that $(a . x) \in I(\phi)$.

Similarly it can be shown that $(x . a) \in I(\phi)$.

■ 7.12 ISOMORPHISM

A mapping ϕ from ring R into R′ is said to be isomorphism if

(*i*) ϕ is homomorphism

(*ii*) ϕ is one -one

i.e. A homomorphism ϕ of R into R′ is said to be isomorphism if it is one-to-one mapping.

7.12.1 Theorem

The homomorphism ϕ defined from the ring R into R′ is an isomorphism if and only if $I(\phi) = (0)$.

Proof : (*Necessary part*) Let ϕ: R → R′ is an isomorphism.

This implies that ϕ is a homomorphism and one-one.

Let $a \in I(\Phi) \Rightarrow \phi(a) = 0$

$\Rightarrow \phi(a) = \phi(0)$ [ϕ is homomorphism; $\phi(0) = 0$]

$\Rightarrow a = 0$ [ϕ is one-one]

So, $a \in I(\phi) \Rightarrow a = 0 \quad \forall\, a \in R$

Therefore, $I(\phi) = (0)$

(*Sufficient part*) Let $I(\phi) = (0)$

Let $x, y \in R$ and $\phi(x) = \phi(y)$

Now, $\phi(x) = \phi(y)$

$\Rightarrow \phi(x) - \phi(y) = 0$

$\Rightarrow \phi(x - y) = 0$

$\Rightarrow (x - y) \in I(\phi) = (0)$

Therefore, $x - y = 0$, hence $x = y$.

So, $\phi(x) = \phi(y) \Rightarrow x = y$

This implies that ϕ is one - one and hence ϕ is isomorphism.

SOLVED EXAMPLES

Example 1 *Show that the set of all square matrix of order (m × m) under the binary operations addition and multiplication is a non commutative ring.*

Solution Let R be a set of all square matrices of order $(m \times m)$.

We have to show that R is a ring, *i.e.* R satisfies all the eight properties of ring.

Under Addition

Closure Law : Let A and B be two square matrices of order $(m \times m)$.

So, (A + B) will be a square matrix of order $(m \times m)$

This implies $(A + B) \in R$

i.e. $A, B \in R \Rightarrow (A + B) \in R$

Associative Law : We know that matrix addition is associative. *i.e.* $A, B, C \in R$ implies that

$$A + (B + C) = (A + B) + C$$

Existence of Identity: For every square matrix $A \in R$, there exists null matrix $[0]_{m \times m} \in R$ such that

$$A + 0 = 0 + A = A$$

Existence of Inverse : For every A ∈ R there exist inverse element (– A) ∈ R such that

$$A + (-A) = 0$$

Commutative Law: We know that matrix addition is commutative, *i.e.* For A, B ∈ R we have

$$(A + B) = (B + A)$$

Under Multiplication

Closure Law : Let A, B ∈ R. *i.e.* A and B are two square matrices of order $(m \times m)$. Now multiplying A and B we will get a matrix of order $(m\times m)$.

i.e. $$A \,.\, B \in R$$

Associative Law : We know that matrix multiplication is associative.

i.e. $$A \,.\, (B \,.\, C) = (A \,.\, B) \,.\, C \quad \forall \quad A, B, C \in R$$

Distributive Laws : Let A, B, C ∈ R. *i.e.* A, B and C are three square matrices of order $(m\times m)$. Also we know that

$$A \,.\, (B + C) = A \,.\, B + A \,.\, C$$

Therefore, R satisfies all the properties of Ring. Hence R is a ring.

Example 2 *If R is a Boolean ring, then prove that*

(i) $a + a = 0 \quad \forall \quad a \in R$

(ii) $a + b = 0$ *implies* $a = b \ \forall a, b \in R$

(iii) R is a commutative ring.

Solution Given that R is Boolean ring.

i.e. $$a^2 = a \ \forall \ a \in R$$

(*i*) Let $a \in$ R, this implies that $(a + a) \in$ R

$$\begin{aligned}
\Rightarrow \quad (a+a)^2 &= (a+a) && [\because a^2 = a]\\
\Rightarrow \quad (a+a)\,.\,(a+a) &= a+a\\
\Rightarrow \quad a\,.\,(a+a) + a\,.\,(a+a) &= a+a && \text{[Distributive Law]}\\
\Rightarrow \quad (a\,.\,a + a\,.\,a) + (a\,.\,a + a\,.\,a) &= a+a && \text{[Distributive Law]}\\
\Rightarrow \quad (a^2 + a^2 + a^2 + a^2) &= a+a\\
\Rightarrow \quad a+a+a+a &= a+a\\
\Rightarrow \quad a+a &= 0 && \text{[Cancellation Law]}
\end{aligned}$$

(*ii*) Suppose that $a + b = 0 \ \forall\, a, b \in$ R

Again, we have proved that $a + a = 0$

Thus we have $a + b = a + a$

This implies that $b = a$ [Cancellation Law]

(*iii*)Let $a, b \in$ R, this implies that $(a + b) \in$ R. As R is a Boolean ring, so we have $(a + b)^2 = a + b$

$$\begin{aligned}
\Rightarrow \quad (a+b)\,.\,(a+b) &= a+b\\
\Rightarrow \quad a\,.\,(a+b) + b\,.\,(a+b) &= a+b && \text{[Distributive Law]}\\
\Rightarrow \quad (a\,.\,a + a\,.\,b) + (b\,.\,a + b\,.\,b) &= a+b && \text{[Distributive Law]}\\
\Rightarrow \quad a^2 + a\,.\,b + b\,.\,a + b^2 &= a+b\\
\Rightarrow \quad a + a\,.\,b + b\,.\,a + b &= (a+b)\\
\Rightarrow \quad a\,.\,b + b\,.\,a &= 0\\
\Rightarrow \quad a\,.\,b &= b\,.\,a && [a + b = 0 \text{ implies } a = b]
\end{aligned}$$

Therefore R is a commutative ring.

Example 3 *If R is a ring with unity 1 = 0; then show that R is a singleton set.*

Solution Given R is a ring with unity 1 = 0 and let $a \in$ R

Now $$a = 1 \,.\, a = 0 \,.\, a = 0$$

The above argument is true for all $a \in$ R

Therefore, $$\mathrm{R} = \{0\}$$

Hence R is a singleton set with 0 as its element.

Example 4 *Let R is a set satisfying all the properties of ring except the commutative axiom under addition. If R has the unit element, then prove that R is a ring.*

Solution Given that R is a set satisfying all the properties of ring except the commutative axiom under addition.

i.e. $$a + b = b + a$$

It is also given that R contains unit element, *i.e.* $1 \in$ R

Let $a, b \in \mathrm{R}$ implies that $(a + b) \in \mathrm{R}$ [Closure Law]

Again, $1 \in \mathrm{R} \Rightarrow (1 + 1) \in \mathrm{R}$

Now,
$$\begin{aligned}(a + b) \,.\, (1 + 1) &= a \,.\, (1 + 1) + b \,.\, (1 + 1) && \text{[Distributive Law]}\\ &= a \,.\, 1 + a \,.\, 1 + b \,.\, 1 + b \,.\, 1 && \text{[Distributive Law]}\\ &= (a + a) + (b + b) && \text{......}(i)\end{aligned}$$

Again,
$$\begin{aligned}(a + b) \,.\, (1 + 1) &= (a + b) \,.\, 1 + (a + b) \,.\, 1 && \text{[Distributive Law]}\\ &= (a + b) + (a + b) && \text{......}(ii)\end{aligned}$$

Combining equations (*i*) and (*ii*) we get

$$\begin{aligned} & (a + a) + (b + b) = (a + b) + (a + b) && \\ \Rightarrow\ & a + \{a + (b + b)\} = a + \{b + (a + b)\} && \text{[Associative Law]}\\ \Rightarrow\ & a + (b + b) = b + (a + b) && \text{[Cancellation Law]}\\ \Rightarrow\ & (a + b) + b = (b + a) + b && \text{[Associative Law]}\\ \Rightarrow\ & (a + b) = (b + a) && \text{[Cancellation Law]}\end{aligned}$$

Therefore, R is a ring.

Example 5 *Let R be a ring of all square matrices of order (2 ×2). Show that R has zero divisor.*

Solution Let us consider two square matrices A and B of the ring R as

$$\mathrm{A} = \begin{bmatrix} 5 & 0 \\ 0 & 0 \end{bmatrix} \text{and } \mathrm{B} = \begin{bmatrix} 0 & 0 \\ 5 & 0 \end{bmatrix}$$

Here A ≠ 0 and B ≠ 0, but

$$(\mathrm{A} \,.\, \mathrm{B}) = \begin{bmatrix} 5 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 5 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in \mathrm{R}$$

Therefore, R is a ring with zero divisor.

Example 6 *Let R is a ring with unity and* $(x \,.\, y)^2 = x^2 \,.\, y^2 \ \forall x, y \in$ *R. Show that R is a commutative ring.*

Solution Given R is a ring with unity, *i.e.* $1 \in$ R. Also given that $(x \,.\, y)^2 = x^2 \,.\, y^2 \ \forall\ x, y \in$ R.

Again, $(y + 1) \in$ R as $y \in$ R and $1 \in$ R

Therefore, $$(x \,.\, (y + 1))^2 = x^2 \,.\, (y + 1)^2$$

$\Rightarrow \quad (x\,y + x)^2 = x^2 \,.\, (y^2 + 2y + 1)$

$\Rightarrow \quad (x\,y + x) \,.\, (x\,y + x) = x^2 \,.\, (y^2 + 2y + 1)$

$\Rightarrow \quad x\,y \,.\, x\,y + x\,y \,.\, x + x \,.\, x\,y + x^2 = x^2y^2 + 2x^2y + x^2$

$\Rightarrow \quad (x\,y)^2 + x\,y \,.\, x + x \,.\, x\,y + x^2 = x^2y^2 + 2x^2y + x^2$

$\Rightarrow \quad x^2\,y^2 + (x\,y \,.\, x + x \,.\, x\,y) + x^2 = x^2y^2 + 2x^2y + x^2$

$\Rightarrow \quad x\,y\,x + x\,x\,y = 2x^2\,y$ [Left and Right Cancellation Law]

$\Rightarrow \quad x\,y\,x + x^2\,y = x^2\,y + x^2\,y$

$\Rightarrow \quad x\,y\,x = x^2\,y$ [Cancellation Law]

Now on replacing x by $(x + 1)$ we have

$(x + 1)\,y\,(x + 1) = (x + 1)^2\,y$

$\Rightarrow \quad (x\,y + y)\,(x + 1) = (x^2 + 2x + 1)\,y$

$\Rightarrow \quad x\,y\,x + x\,y + y\,x + y = x^2\,y + 2\,x\,y + y$

$\Rightarrow \quad x^2\,y + x\,y + y\,x + y = x^2\,y + 2\,x\,y + y$ $[\because\, xy\,x = x^2\,y]$

$\Rightarrow \quad x\,y + y\,x = 2xy$ [Left and Right Cancellation Law]

$\Rightarrow \quad y\,x = x\,y$

Therefore, R is commutative ring.

Example 7 *Let R = {0, 1, 2, 3, 4, 5} be a ring under binary operations* $\oplus_6$ *and* $\otimes_6$. *Show that R is a ring with zero divisor.*

Solution Given that R = {0, 1, 2, 3, 4, 5} be a ring under binary operations $\oplus_6$ and $\otimes_6$.

Here $2 \in$ R and $3 \in$ R are two non zero elements such that

$$2 \cdot 3 = 0$$

Therefore, R is a ring with zero divisor.

Example 8 *R is the set of integer mod 7 under addition and multiplication mod 7. Show that R is a commutative ring with unit element.*

Solution Given R is the set of integer mod 7 under addition and multiplication mod 7. The operation is defined as

(*i*) $a + b = c$ where c is the remainder of $a + b$ when divided by 7.

(*ii*) $a \,.\, b = c$ where c is the remainder of $a \,.\, b$ when divided by 7.

So, it is clear that R contains 7 elements. *i.e.* R = {0, 1, 2, 3, 4, 5, 6}.

Table for addition modulo 7

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

Table for multiplication modulo 7

.	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Under Addition

Closure Law : From the table for addition modulo 7 it is clear that for any

$$a, b \in \mathrm{R} \Rightarrow (a + b) \in \mathrm{R}$$

Associative Law : From the table for addition modulo 7 it is clear that for any

$$a + (b + c) = (a + b) + c \quad \forall \quad a, b, c \in \mathrm{R}.$$

Let $a = 1, b = 3, c = 5.$

Therefore, we have

$$a + (b + c) = 1 + (3 + 5) = 1 + 1 = 2$$

and $(a + b) + c = (1 + 3) + 5 = 4 + 5 = 2$

Therefore,. $a + (b + c) = (a + b) + c$

Existence of Identity : From first row of the table for addition modulo 7 it is clear that $0 \in \mathrm{R}$ is the identity element.

i.e. $0 + a = a \quad \forall \quad a \in \mathrm{R}$

Existence of Inverse : From the table for addition modulo 7 it is clear that the inverse elements of 0, 1, 2, 3, 4, 5, 6 are 0, 6, 5, 4, 3, 2, 1 $\in$ R respectively. The inverse element of 3 is 4 because 3 + 4 = 0.

i.e. For every $a \in \mathrm{R}$ there exists an $(-a) \in \mathrm{R}$ such that $a + (-a) = 0$.

Commutative Law : From the table for addition modulo 7 it is clear that

$$a + b = b + a \quad \forall \quad a, b \in \mathrm{R}$$

Under Multiplication

Closure Law : From the table for multiplication modulo 7 it is clear that for all

$$a, b \in \mathrm{R} \Rightarrow a \,.\, b \in \mathrm{R}$$

Associative Law : From the table for multiplication modulo 7 it is clear that

$$a \,.\, (b. c) = (a \,.\, b) \,.\, c \quad \forall \quad a, b, c \in \mathrm{R}$$

Let $a = 3, b = 4, c = 6.$

Therefore we have

$$a \,.\, (b \,.\, c) = 3 \,.\, (4 \,.\, 6) = 3 \,.\, 3 = 2 \text{ and}$$

$$(a \,.\, b) \,.\, c = (3 \,.\, 4) \,.\, 6 = 5 \,.\, 6 = 2$$

Therefore, we get $a \,.\, (b \,.\, c) = (a \,.\, b) \,.\, c$

Distributive Law :

Let $a = 1, b = 4, c = 2$.

Hence we have

$$a\,.\,(b + c) = 1\,.\,(4 + 2) = 1\,.\,6 = 6 \text{ and}$$

$$(a\,.\,b) + (a\,.\,c) = (1\,.\,4) + (1\,.\,2) = 6$$

Therefore, we get $a\,.\,(b + c) = a\,.\,b + a\,.\,c$

Commutative Law : From the table for multiplication modulo 7 it is clear that

$$a\,.\,b = b\,.\,a \quad \forall \quad a, b \in \text{R}$$

Unit Element : From the table for multiplication modulo 7, the 2nd row or column indicates that $1 \in$ R is the identity element for every element $a \in$ R. Hence for every $a \in$ R there exists unit element $1 \in$ R such that

$$(1\,.\,a) = a \quad \forall \quad a \in \text{R}.$$

Therefore, R is commutative ring with unit element.

Example 9 *Show that if R is a ring with unity, then any nonzero element with multiplicative inverse in R cannot be the zero divisor.*

Solution Given that R is a ring with unity.

Let $a \in$ R and $a \neq 0$.

Again a$\neq 0$ implies $a^{-1} \in$ R

Suppose that $(a\,.\,b) = 0$ with $b \neq 0 \in$ R

$$\begin{aligned}
\Rightarrow \quad & a^{-1}\,.\,(a\,.\,b) = a^{-1}\,.\,0 \\
\Rightarrow \quad & (a^{-1}\,.\,a)\,b = 0 \\
\Rightarrow \quad & b = 0 \quad [(a^{-1}.\,a) = 1]
\end{aligned}$$

This is a contradiction. This contradicts to the fact that $b \neq 0$. This indicates that a is not the zero divisor.

Example 10 *For the ring R = $M_{2\times 2}$(I), show that the subset S defined as*

$$S = \left\{\begin{pmatrix} x & x+y \\ x+y & x \end{pmatrix} : x, y \in I\right\} \textit{ is a sub string.}$$

Solution Given R = $\text{M}_{2\times 2}$(I) be a ring and

$$\text{S} = \left\{\begin{pmatrix} x & x+y \\ x+y & x \end{pmatrix} : x, y \in \text{I}\right\}$$

Putting $x = y = 0$ we have

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in \text{S} \Rightarrow \text{S is non-empty. } \textit{i.e. } \text{S} \neq \varphi.$$

To prove S is a sub ring we have to show that S satisfies two axioms

(*i*) A – B ∈ S; A, B ∈ S

(*ii*) A . B ∈ S; A, B ∈ S

Let $$\text{A} = \begin{pmatrix} x & x+y \\ x+y & x \end{pmatrix} \text{and B} = \begin{pmatrix} u & u+v \\ u+v & u \end{pmatrix}; \quad u, v, x, y \in \text{I}$$

Now, $$\text{A} - \text{B} = \begin{pmatrix} x-u & x+y-u-v \\ x+y-u-v & x-u \end{pmatrix} \in \text{S}$$

and $$\text{A . B} = \begin{pmatrix} x & x+y \\ x+y & x \end{pmatrix}\begin{pmatrix} u & u+w \\ u+w & u \end{pmatrix}$$

$$= \begin{pmatrix} xu+(x+y)(u+w) & (x)(u+w)+(x+y)u \\ (x+y)u+x(u+w) & (x+y)(u+w)+xu \end{pmatrix} \in \text{S}$$

This implies that all the entries of the matrices (A – B) and A.B are integers. Therefore, S is a sub ring.

Example 11 *Let R = {0, 1, 2, 3, 4} be a commutative ring with respect to the binary operations* $\oplus_5$ *and* $\otimes_5$*. Show that R is an integral domain.*

Solution Given that R = {0, 1, 2, 3, 4} be a commutative ring with respect to the binary operations $\oplus_5$ and $\otimes_5$.

It is also clear that there is no such nonzero element in R for which $(a \,.\, b) = 0$. Hence R is an integral domain.

Example 12 *Let R = {0, 1, 2, 3, 4, 5, 6, 7} be a commutative ring under the binary operations* $\oplus_8$ *and* $\otimes_8 \cdot$ *Show that R is not an integral domain.*

Solution Given that R = {0, 1, 2, 3, 4, 5, 6, 7} be a commutative ring under the binary operations $\oplus_8$ and $\otimes_8$

Now $2 \in \text{R}$ and $4 \in \text{R}$ such that $2 \otimes_8 4 = 0$

Therefore, R is not an integral domain.

Example 13 *R = {u, v, w, t} define the operations + and . in such a way that R will be a ring.*

+	*u*	*v*	*w*	*t*
u	*u*	*v*	*w*	*t*
v	*v*	*u*	*t*	*w*
w	*w*	*t*	*u*	*v*
t	*t*	*w*	*v*	*u*

.	*u*	*v*	*w*	*t*
u	*u*	*u*	*u*	*u*
v	*u*	*v*		
w	*u*	*v*		*t*
t	*u*		*u*	

(*a*) Using the associative and distributive law determine the entries in the blank space.

(*b*) Is it a commutative ring ?

(*c*) Does it have unity ? If yes, find the unit element.

(*d*) Is the ring an integral domain or a field.

Solution (*a*) Now, $(w \,.\, w) = w \,.\, (v + t)$ $[\because\ (v + t) = w]$

$= w \,.\, v + w \,.\, t$ [Distributive Law]

$= v + t = w$

Therefore, $w \,.\, w = w$

Again, $(t \,.\, v) = (w + v) \,.\, v$ $[\because\ (w + v) = t]$

$= w \,.\, v + v \,.\, v$ [Distributive Law]

$= v + v = u$

Therefore, $t \,.\, v = u$

Again, $(t \,.\, t) = t \,.\, (v + w)$ $[\because\ (w + v) = t]$

$= t \,.\ v + t \,.\, w$ [Distributive Law]

$= u + u = u$

Therefore, $(t \,.\, t) = u$

Similarly, $(v \,.\, w) = (t + w) \,.\, w$ [$\because$ $(t + w) = v$]

$= t \,.\, w + w \,.\, w$ [Distributive Law]

$= u + w = w$

Therefore, $(v \,.\, w) = w$

And $v \,.\, t = (t + w) \,.\, t$ [$\because$ $(w + t) = v$]

$= t \,.\, t + w \,.\, t$ [Distributive Law]

$= u + t = t$

So, the complete table is given as

.	u	v	w	t
u	u	u	u	u
v	u	v	w	t
w	u	v	w	t
t	u	v	u	u

(*b*) From the above table it is clear that $(v \,.\, w) = w$ and $(w \,.\, v) = v$. This implies $(v \,.\, w) \neq (w \,.\, v)$. Thus, R is not a commutative ring.

(*c*) As it is clear from the table, the ring does not contain unity and hence does not have unit element.

(*d*) Since R is not commutative, so it is neither integral domain nor field.

Example 14 *If a, b, c, d* $\in$ *R and R is a ring then evaluate (a + b).(c + d).*

Solution Given R is a ring and $a, b, c, d \in$ R

Now, $(a + b) \,.\, (c + d) = u \,.\, (c + d);$ [Let $u = a + b$]

$= u \,.\, c + u \,.\, d$ [Distributive Law]

$= (a + b) \,.\, c + (a + b) \,.\, d$

$= a \,.\, c + b \,.\, c + a \,.\, d + b \,.\, d$ [Distributive Law]

Example 15 *If R is a ring and* $(x + y)^2 = x^2 + 2xy + y^2$ *then prove that R is commutative for all* $x, y \in R$.

Solution Given R is a ring and $(x + y)^2 = x^2 + 2xy + y^2$ for $x, y \in$ R.

$\Rightarrow$ $(x + y)\,(x + y) = x^2 + 2xy + y^2$

$\Rightarrow$ $x\,(x + y) + y\,(x + y) = x^2 + 2xy + y^2$

$\Rightarrow$ $xx + x\,y + y\,x + y\,y = x^2 + 2xy + y^2$

$\Rightarrow$ $x^2 + x\,y + y\,x + y^2 = x^2 + 2xy + y^2$

$\Rightarrow$ $x\,y + y\,x = 2xy$ [Cancellation Law]

$\Rightarrow$ $x\,y + y\,x = x\,y + x\,y$

$\Rightarrow$ $y\,x = x\,y$ [Cancellation Law]

Therefore, R is commutative ring.

Example 16 *For a commutative ring R with characteristic 2 show that*

$$(a + b)^2 = a^2 + b^2 = (a - b)^2 \quad \forall \quad a, b \in \mathrm{R}$$

Solution Let R be a commutative ring with characteristic 2. This indicates that $(2 \,.\, a) = 0$ for all $a \in$ R.

$$\begin{aligned}
\text{Now,} \quad (a+b)^2 &= (a+b)\,.\,(a+b) \\
&= a\,a + a\,b + b\,a + b\,b \\
&= a^2 + a\,b + a\,b + b^2 && \text{[R is commutative]} \\
&= a^2 + 2ab + b^2 \\
&= a^2 + 0 + b^2 && [2a = 0] \\
&= a^2 + b^2 \\
\Rightarrow \quad (a+b)^2 &= a^2 + b^2 \\
\text{Similarly,} \quad (a-b)^2 &= a^2 - 2ab + b^2 \\
&= a^2 + 0 + b^2 = a^2 + b^2 \\
\Rightarrow \quad (a-b)^2 &= a^2 + b^2 \\
\text{Therefore,} \quad (a+b)^2 &= a^2 + b^2 = (a-b)^2
\end{aligned}$$

Example 17 *Show that a Boolean ring R is a commutative ring with characteristic 2.*

Solution Given R is a Boolean ring. This implies $a^2 = a$ for all $a \in$ R.

$$\begin{aligned}
\text{Let} \quad & a, b \in \text{R} \\
\Rightarrow \quad & (a+b) \in \text{R} \\
\Rightarrow \quad & (a+b)^2 = (a+b) && [\because a^2 = a] \\
\Rightarrow \quad & (a+b)\,.\,(a+b) = (a+b) \\
\Rightarrow \quad & a\,a + a\,b + b\,a + b\,b = a + b \\
\Rightarrow \quad & a^2 + a\,b + b\,a + b^2 = (a+b) + 0 \\
\Rightarrow \quad & a + a\,b + b\,a + b = (a+b) + 0 \\
\Rightarrow \quad & (a+b) + (a\,b + b\,a) = (a+b) + 0 && \text{[Associative Law]} \\
\Rightarrow \quad & a\,b + b\,a = 0 \\
\Rightarrow \quad & a\,b = b\,a && [\because \text{ In Boolean ring } (a+b) = 0 \Rightarrow a = b]
\end{aligned}$$

Therefore, R is a commutative ring.

$$\begin{aligned}
\text{Again,} \quad & (a+a)^2 = (a+a) \\
\Rightarrow \quad & a^2 + a^2 + a^2 + a^2 = a + a \\
\Rightarrow \quad & (a+a) + (a+a) = (a+a) + 0 \\
\Rightarrow \quad & a + a = 0 && \text{[Left Cancellation Law]} \\
\Rightarrow \quad & 2a = 0
\end{aligned}$$

Hence, R is a commutative ring with characteristic 2.

Example 18 *For the ring (I, $\oplus$, $\odot$) with binary operation defined as $x \oplus y = x + y - 1$ and $x \odot y = x + y - xy$, show that the subset S of all odd integers is a sub ring.*

Solution Suppose that S be the set of all odd integers. Let $a, b \in$ S. This implies a and b are odd integers.

$$\text{Now,} \quad a \oplus b = a + b - 1$$

Again $(a + b)$ is even as sum of odds is even.

$$\begin{aligned}
\Rightarrow \quad & a + b - 1 \text{ is odd} \\
\Rightarrow \quad & a + b - 1 \in \text{S}
\end{aligned}$$

$\Rightarrow \qquad a \oplus b \in \text{S}$

Similarly, $a \odot b = a + b - a\,b$. However, we know that $(a + b)$ is even and $(a\,b)$ is odd. Therefore $(a + b - a\,b)$ is odd.

$\Rightarrow \qquad a \odot b \in \text{S}$

Let a ∈ S, then the additive inverse is $-a$ which is odd hence belongs to S, *i.e.* $-a \in$ S.

Therefore, S is a sub ring.

Example 19 *Show that isomorphic image of a division ring is division ring.*

Solution Let R be a division ring. Therefore, the non zero elements of R forms a group under multiplication.

Let ϕ be a isomorphism defined from R into R′**.** *i.e.*$\phi : \text{R} \to \text{R}'$.

Let $a \neq 0 \in \text{R} \Rightarrow a^{-1} \neq 0 \in \text{R}$.

As ϕ is isomorphism, so $\phi\,(a) \neq 0$. We have to show that $\phi\,(a^{-1}) = \phi(a)^{-1}$.

Again, $\qquad \phi(a)\,.\,\phi(a^{-1}) = \phi\,(a\,.\,a^{-1}) = \phi\,(1) = 1' \in \text{R}'$

$\Rightarrow \qquad \phi(a)\,.\,\phi(a^{-1}) = 1'$

Therefore we get $\qquad \phi(a^{-1}) = \phi(a)^{-1}$.

This indicates that every non-zero element of R′ has an inverse. Thus R′ is a division ring.

Example 20 Show that the isomorphic image of an integral domain is an integral domain.

Solution Let R be an integral domain and ϕ be a isomorphism from R into R′, *i. e.* ϕ: R → R′.

Since R is an integral domain, so it is a commutative ring without zero divisors. Let a, $b \in$ R, $a \neq 0$ and $b \neq 0$ such that $(a\,.\,b) \neq 0$.

$\Rightarrow \qquad \phi(a\,.\,b) \neq 0$

$\Rightarrow \qquad \phi(a)\,.\,\phi(b) \neq \phi(0)$

$\Rightarrow \qquad \phi(a)\,.\,\phi(b) \neq 0$

Since ϕ is an isomorphism, $a \neq 0$, $b \neq 0$ implies that $\phi(a) \neq 0$, $\phi(b) \neq 0$.

Therefore we get $\phi(a) \neq 0$ and $\phi(b) \neq 0$ implies $\phi(a)\,.\,\phi(b) \neq 0$. Hence R′ is without zero divisor.

Again we know that isomorphic image of a commutative ring is a commutative ring.

This indicates that R′ is a commutative ring without zero divisor, thus is an integral domain.

EXERCISES

1. Prove that the set of Real numbers R forms a Ring under ordinary addition multiplication.
2. Show that the set of Rational numbers Q forms a commutative ring with unit element under ordinary addition and multiplication.
3. Let S = $\{a + b\sqrt{2} \mid a$ and b are integers$\}$ forms a Ring under addition and multiplication.
4. The set R = {0, 1, 2, 3, 4, 5} is a commutative ring with unit element under $\oplus_6$ and $\otimes_6$.
5. The operations $a \oplus b = (a + b + 1)$ and $a \otimes b = (a + b + ab)$ are defined on the set of integers. Show that I forms a commutative ring under the operations defined. Does it have unit element?
6. Show that set of Real numbers of the type $(a + b\,\sqrt{2})$; $a, b \in$ R is an integral domain.
7. Show that ring of integers (I, +) is an integral domain but not field.
8. R_P = {0, 1, 2, ... , P – 1}, where P is a prime. Show that R_P is an integral domain.

9. Show that the set of numbers given by $\{a + b\sqrt{2}; a, b \in \text{I}\}$ is a ring under ordinary addition and multiplication.

10. Let R = $\{a, b, c, d, e\}$. The operations + and . on R is defined as

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

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

(*a*) Show that (R, +, .) is a commutative ring.

(*b*) What is the additive identity and unity ?

(*c*) What are the inverse elements of a, b, c, d ?

11. Show that set of all rational numbers is a commutative ring with unity under ordinary addition and multiplication.

12. Do the following sets forms an integral domain with respect to ordinary addition and multiplication. If yes, then test whether they are field.

(*a*) $\text{I}\left(\sqrt{2}\right) = \{x \mid x = b\sqrt{2} : b \text{ is rational}\}$

(*b*) Set of even integers

(*c*) Set of positive integers.

13. Show that (I, +, .) is a sub ring of (Q, +, .) which is a sub ring of (R, +, .) which is a sub ring of (C, +, .). Where

I : Set of integers
Q : Set of rational numbers
R : Set of real numbers
C : Set of complex numbers

14. Give an example of each of the followings.

(*a*) A non-commutative ring

(*b*) Ring without zero divisor

(*c*) Division ring

(*d*) A ring which is not an integral domain.

15. Show that set of all square matrix of order $(n \times n)$ is a non-commutative ring with unity under the matrix addition and multiplication.

16. Show that set of even integers under ordinary addition and multiplication is a commutative ring without unit element.

17. The set of rational numbers under usual addition and multiplication is a field.

18. Let R be a ring. Prove that $(n\,a)\,(m\,b) = (n\,m)\,(a\,b)$ for all $a, b \in$ R and $m, n \in$ I.

19. Give an example of a ring which contains an element $a \neq 0$ such that $a^3 = 0$. Is it an integral domain.

20. Given a, b be two elements of a field F with characteristic 3. Show that $(a + b)^3 = a^3 + b^3$.

21. Prove that for a field

(*a*) $\dfrac{a}{b} = \dfrac{c}{d} \Leftrightarrow ad = bc$

(*b*) $(-a)^{-1} = -(a^{-1})$

(*c*) $\dfrac{a}{b} - \dfrac{c}{d} = \dfrac{ad - bc}{bd}$

(*d*) $\dfrac{-a}{-b} = \dfrac{a}{b}$

22. R is a ring with unit element 1 and ϕ is a homomorphism of R onto R_1. Then prove that $\phi\,(1)$ is the unit element of R_1.

8

Boolean Algebra

■ 8.0 INTRODUCTION

For centuries mathematicians felt there was a connection between mathematics and logic, but no one could find this missing link before George Boole. In 1854 he introduced symbolic logic known as Boolean Algebra, Boolean function, Boolean expression, Boolean ring and many more honor the nineteenth century mathematician George Boole. Each variable in Boolean algebra has either of two values: true or false. The purpose of this two - state algebra was to solve logic problems.

Almost after a century of Boole's work, it was observed by C.E. Shannon in 1938, that Boolean algebra could be used to analyze electrical circuits. This was developed by Shannon while he analyzed telephone switching circuits. Because of Shannon's work, engineers realized that Boolean algebra could be applied to Computer electronics.

This chapter introduces the Gate, Combinatorial Circuits, Boolean Expression, Boolean Algebra, Boolean Functions and Various Normal Forms.

■ 8.1 GATES

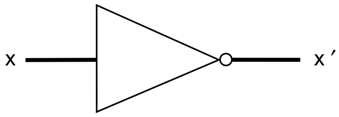
In logic we have discussed about the logical connectives ¬, ∧ and ∨. The connectives ∧ and ∨ can be considered as circuits connected in series and parallel respectively. A circuit with one or more input signals but only one output signal is known as a gate. Gates are digital circuits because of input and output signals, which are either low or high. Gates are also called logical circuits because they can be analyzed with Boolean algebra. In gates, the connectives ¬, ∧ and ∨ are usually denoted by the symbols ′, . and + respectively. The block diagrams for different gates are discussed below.

8.1.1 A NOT Gate

A NOT gate receives input x, where x is a bit (binary digit) and produces output x' where

$$x' = \begin{cases} 1 \text{ if } x = 0 \\ 0 \text{ if } x = 1 \end{cases}$$

The output state is always the opposite of the input state. The output is sometimes called the complement of the input. A NOT gate is drawn as shown in the following figure.

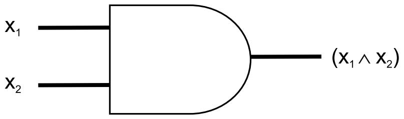


8.1.2 An AND Gate

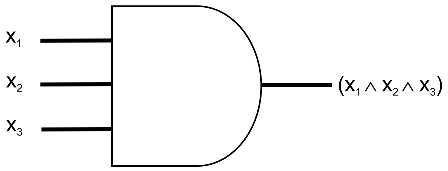
An AND gate receives inputs x_1 andx_2, wherex_1 andx_2 are bits, and produces output $(x_1 \wedge x_2)$, where

$$(x_1 \wedge x_2) = \begin{cases} 1 \text{ if } x_1 = x_2 = 1 \\ 0 \text{ Otherwise} \end{cases}$$

An AND gate may have more inputs also but the output is always one. An AND gate is drawn as shown in the following figure.



(2 input AND gate)



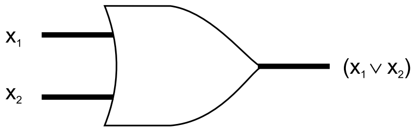
(3 input AND gate)

8.1.3 An OR Gate

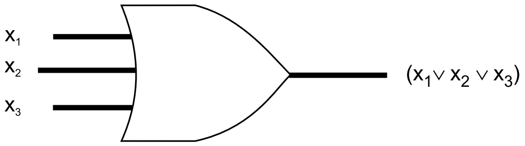
An OR gate receives inputs x_1 and x_2, wherex_1 andx_2 are bits, and produces output $(x_1 \vee x_2)$, where

$$(x_1 \vee x_2) = \begin{cases} 1 \text{ if } x_1 = 1 \text{ or } x_2 = 1 \\ 0 \text{ Otherwise} \end{cases}$$

An OR gate may have more inputs also but the output is always one. An OR gate is drawn as shown in the following figure.



(2 input OR gate)



(3 input OR gate)

The logic tables for the basic AND, OR and NOT gates are given below.

x_1	x_2	$(x_1 \wedge x_2)$
1	1	1
1	0	0
1	0	0
0	0	0

x_1	x_2	$(x_1 \vee x_2)$
1	1	1
1	0	1
0	1	1
0	0	0

x	x'
1	0
0	1

■ 8.2 MORE LOGIC GATES

There are some other types of gates which are useful and frequently used in Computer Science. These are called NAND, NOR, XOR and XNOR gates.

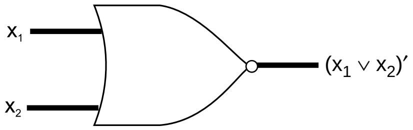
The block diagrams for these different gates are given below.

8.2.1 NOR Gate

A NOR gate receives inputs x_1 and x_2 where x_1 and x_2 are bits, and produces output $(x_1 \vee x_2)'$, where

$$(x_1 \vee x_2)' = \begin{cases} 1 \text{ if } x_1 = x_2 = 0 \\ 0 \text{ Otherwise} \end{cases}$$

A NOR gate may have more inputs also, but the output is always one. A NOR gate is drawn as shown in the following figure.



(2 input NOR gate)

According to De Morgan's first theorem we have

$$(x_1 \vee x_2)' = x_1' \wedge x_2' \quad i.e. \quad (x_1 + x_2)' = x_1' \,.\, x_2'$$

8.2.2 NAND Gate

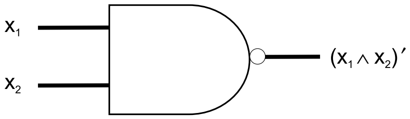
A NAND gate receives inputs x_1 and x_2, where x_1 and x_2 are bits, and produces output $(x_1 \wedge x_2)'$, where

$$(x_1 \wedge x_2)' = \begin{cases} 1 \text{ if } x_1 = 0 \text{ or } x_2 = 0 \\ 0 \text{ Otherwise} \end{cases}$$

A NAND gate may have more inputs also, but the output is always one. A NAND gate is drawn as shown in the following figure.

According to the De Morgan's second theorem we have

$$(x_1 \wedge x_2)' = x'_1 + x_2' \; i.e. \; (x_1 . x_2)' = x_1' + x_2'$$

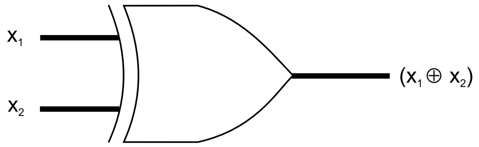


8.2.3 XOR Gate (Exclusive OR Gate)

A XOR gate receives inputs x_1 and x_2, where x_1 and x_2 are bits, and produces output $(x_1 \overline{\vee} x_2)$ or $(x_1 \oplus x_2)$, where

$$(x_1 \oplus x_2) = \begin{cases} 1 \text{ if } x_1 = 1 \text{ or } x_2 = 1 \text{ but not both} \\ 0 \text{ Otherwise} \end{cases}$$

From the definition, it is clear that, the Exclusive OR gate, *i.e.* XOR gate produces 1 that have an odd number of 1's. A XOR gate may have more inputs also, but the output is always one. A XOR gate is drawn as shown in the following figure.



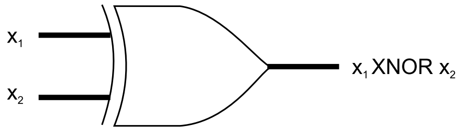
8.2.4 XNOR Gate (Exclusive NOR Gate)

A XNOR gate receives inputs x_1 and x_2, where x_1 and x_2 are bits, and produces output x_1 XNOR x_2 where

$$x_1 \text{ XNOR } x_2 = \begin{cases} 1 \text{ if } x_1 \text{and } x_2 \text{ are same bits} \\ 0 \text{ Otherwise} \end{cases}$$

XNOR gate may have more inputs also, but the output is always one. In this case it recognizes even-parity words. Even parity means a word has an even number of 1's. For example 11100111 has even parity because it contains six 1's. Odd parity means a word has an odd number of 1's. For example 1101 has odd parity because it contains three 1's.

A XNOR gate is drawn as shown in the following figure.



The logic tables for the above NOR, NAND, XOR and XNOR gates are given below.

x_1	x_2	$(x_1 \wedge x_2)'$
1	1	0
1	0	1
0	1	1
0	0	1

x_1	x_2	$(x_1 \vee x_2)'$
1	1	0
1	0	0
0	1	0
0	0	1

x_1	x_2	$(x_1 \oplus x_2)$
1	1	0
1	0	1
0	1	1
0	0	0

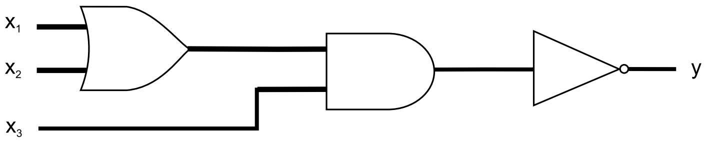
x_1	x_2	(x_1 XNOR x_2)
1	1	1
1	0	0
0	1	0
0	0	1

■ 8.3 COMBINATORIAL CIRCUIT

In digital computer electronics, there are only two possibilities, *i.e.* 0 and 1, for the smallest, indivisible object. These 0 and 1 are known as binary digits (bit). A bit in one part of a circuit is transmitted to another part of the circuit as a voltage. Thus two voltage levels are needed. *i.e.* high voltage level and low voltage level. A high voltage level communicates 1 where as a low voltage level communicates 0.

A combinatorial circuit is a circuit which produces an unique output for every combination of inputs. A combinatorial circuit has no memory, previous inputs and the state of the system do not affect the output of a combinatorial circuit. These circuits can be constructed using gates which we have already discussed.

Let us consider the circuit

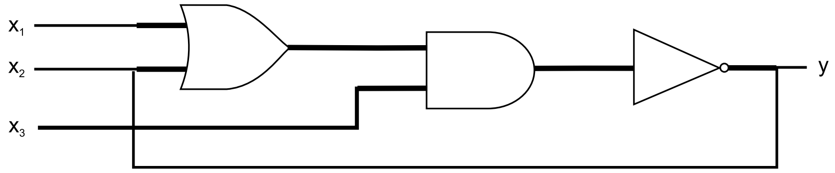


x_1	x_2	x_3	y
1	1	1	0
1	1	0	1
0	1	1	0
1	0	1	0
0	0	1	1
0	1	0	1
1	0	0	1
0	0	0	1

The logic table for the above circuit is given in the side table. From the table it is cleared that the output y is uniquely defined for each combination of inputs x_1, x_2 and x_3. Therefore, the circuit is a combinatorial circuit.

If $x_1 = 1$ and $x_2 = 1$, then the output of OR gate is 1. Now the input for AND gate is 1 and 0, so the output of AND gate is 0. Since the input to the Not gate is 0, the output $y = 1$.

Consider another circuit as

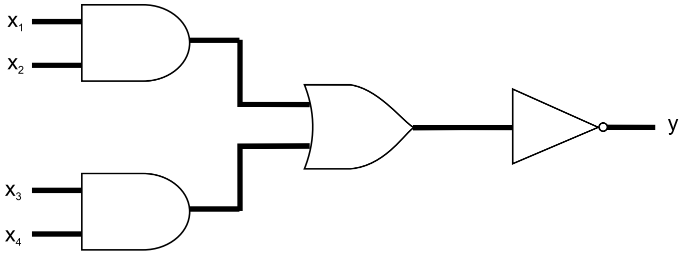


The above circuit is not a combinatorial circuit, as the output y is not defined uniquely for every combination of inputs x_1, x_2 and x_3 .

■ 8.4 BOOLEAN EXPRESSION

Any expression built up from the variables $x_1, y_1, z_1, x_2, y_2, z_2, \ldots$ by applying the operations $\wedge$, $\vee$ and $'$ a finite number of times. If X_1 and X_2 are Boolean expressions, then (X_1), X_2', $(X_1 \wedge X_2)$ and $(X_1 \vee X_2)$ are also Boolean expressions. The output of a combinatorial circuit is also a Boolean expression.

Let us consider the combinatorial circuit as



The Boolean expression to the above circuit is given as $((x_1 \wedge x_2) \vee (x_3 \wedge x_4))'$.

8.4.1 Theorem

If $\wedge$, $\vee$ and $'$ are connectives defined earlier, then the following properties hold.

(*i*) Associative Laws: For all $a, b, c \in \{0, 1\}$

$$(a \wedge b) \wedge c = a \wedge (b \wedge c) \text{ and}$$
$$(a \vee b) \vee c = a \vee (b \vee c)$$

(*ii*) Identity Laws: For all $a \in \{0, 1\}$

$$(a \wedge 1) = a \quad \text{and} \quad (a \vee 0) = a$$

(*iii*) Commutative Laws: For all $a, b \in \{0, 1\}$

$$(a \wedge b) = (b \wedge a) \quad \text{and}$$
$$(a \vee b) = (b \vee a)$$

(*iv*) Complement Laws: For all $a \in \{0, 1\}$

$$(a \wedge a') = 0 \quad \text{and}$$
$$(a \vee a') = 1$$

(*v*) Distributive Laws : For all $a, b, c \in \{0, 1\}$

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c) \quad \text{and}$$
$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$$

Proof: Proofs of (*i*), (*ii*), (*iii*) and (*iv*) are immediate consequences of the definitions. We prove only the first distributive law. Here we simply evaluate both sides of law for all possible values of $a, b, c \in \{0, 1\}$ and verify that in each case we obtain the same result.

We must show that $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$

a	b	c	$(b \wedge c)$	$a \vee (b \wedge c)$	$(a \vee b)$	$(a \vee c)$	$(a \vee b) \wedge (a \vee c)$
1	1	1	1	1	1	1	1
0	0	1	0	0	0	1	0
0	1	0	0	0	1	0	0
1	0	0	0	1	1	1	1
1	1	0	0	1	1	1	1
1	0	1	0	1	1	1	1
0	1	1	1	1	1	1	1
0	0	0	0	0	0	0	0

Therefore, $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$

8.4.2 De-Morgan's Laws

If x_1, x_2 are bits, *i.e.* $x_1, x_2 \in \{0, 1\}$, then

(*i*) $(x_1 \wedge x_2)' = x_1' \vee x_2'$

(*ii*) $(x_1 \vee x_2)' = x_1' \wedge x_2'$

Proof: We prove only the first De-Morgan's Law.

i.e. $(x_1 \wedge x_2)' = x_1' \vee x_2'$

Construct the logical table.

x_1	x_2	$(x_1 \wedge x_2)'$	x_1'	x_2'	$x_1' \vee x_2'$
1	1	0	0	0	0
1	0	1	0	1	1
0	1	1	1	0	1
0	0	1	1	1	1

Therefore, $(x_1 \wedge x_2)' = x_1' \vee x_2'$.

■ 8.5 EQUIVALENT COMBINATORIAL CIRCUITS

Two combinatorial circuits, each having inputs $x_1, x_2, \ldots, x_n$ are said to be equivalent if they produce the same outputs for same inputs, *i.e.*, the output for both the circuits remains same if the circuits receive same inputs.

Consider the following combinatorial circuits.

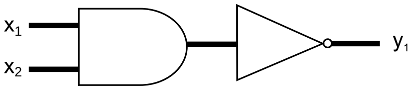


Figure 1

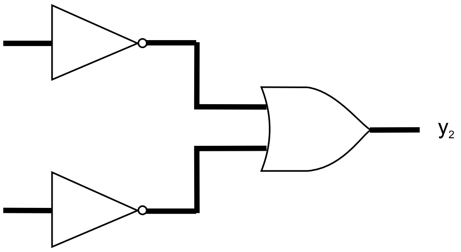


Figure 2

The logic tables for both the circuits are given below, which are identical.

x_1	x_2	y_1
1	1	0
1	0	1
0	1	1
0	0	1

x_1	x_2	y_2
1	1	0
1	0	1
0	1	1
0	0	1

From the logic tables it is clear that both the combinatorial circuits are equivalent.

■ 8.6 BOOLEAN ALGEBRA

A Boolean algebra B consists of a set S together with two binary operations $\wedge$ and $\vee$ on S, a singular operation $'$ on S and two specific elements 0 and 1 of S such that the following laws hold. We write B = {S, $\wedge$, $\vee$, $'$, 0, 1}.

(*a*) Associative Laws: For all $a, b, c \in$ S

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

and $$(a \vee b) \vee c = a \vee (b \vee c)$$

(*b*) Commutative Laws: For all $a, b \in$ S

$$(a \wedge b) = (b \wedge a)$$

and $$(a \vee b) = (b \vee a)$$

(*c*) Distributive Laws: For all $a, b, c \in$ S

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

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

(*d*) Identity Laws: For all $a \in$ S

$$(a \wedge 1) = a \quad \text{and} \quad (a \vee 0) = \text{a}$$

(*e*) Complement Laws: For all $a \in$ S

$$(a \wedge a') = 0 \quad \text{and} \quad (a \vee a') = 1$$

8.6.1 Theorem

In a Boolean algebra; if $(a \vee b) = 1$ and $(a \wedge b) = 0$, then $b = a'$, *i.e.* the complement is unique.

Proof: Suppose that $(a \vee b) = 1$ and $(a \wedge b) = 0$

Now $b = (b \vee 0)$ [Identity Law]

$= b \vee (a \wedge a')$ [Complement Law]

$= (b \vee a) \wedge (b \vee a')$ [Distributive Law]

$= (a \vee b) \wedge (b \vee a')$ [Commutative Law]

$= 1 \wedge (b \vee a')$ [Given condition]

$= (b \vee a')$ [Identity Law]

This implies $b = (b \vee a')$ ...(*i*)

Again $a' = (a' \vee 0)$ [Identity Law]

$= a' \vee (a \wedge b)$ [Given condition]

$= (a' \vee a) \wedge (a' \vee b)$ [Distributive Law]

$= 1 \wedge (a' \vee b)$ [Complement Law]

$= (a' \vee b)$ [Identity Law]

$= (b \vee a')$ [Commutative law]

This implies $a' = (b \vee a') = b$ [Equation 1]

8.6.2 Theorem

In a Boolean algebra B = (S, $\vee$, $\wedge$, $'$, 0, 1) ; the following properties hold.

(*a*) Idempotent Laws: For all $x \in$ S

$$(x \vee x) = x \quad \text{and} \quad (x \wedge x) = x$$

(*b*) Bound Laws: For all $x \in$ S

$$(x \vee 1) = 1 \quad \text{and} \quad (x \wedge 0) = 0$$

(*c*) Absorption Laws: For all $x, y \in$ S

$$x \wedge (x \vee y) = x \quad \text{and} \quad x \vee (x \wedge y) = x$$

(*d*) Involution Laws: For all $x \in$ S

$$(x')' = x$$

(*e*) 0 and 1 Laws: $0' = 1$ and $1' = 0$

(*f*) De Morgan's Laws: For all $x, y \in$ S

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

and $(x \vee y)' = x' \wedge y'$

Proof: (*a*) $x = x \vee 0$ [Identity Law]

$= x \vee (x \wedge x')$ [Complement Law]

$= (x \vee x) \wedge (x \vee x')$ [Distributive Law]

$= (x \vee x) \wedge 1$ [Complement Law]

$= (x \vee x)$ [Identity Law]

Therefore, $(x \vee x) = x$

Again $x = x \wedge 1$ [Identity Law]

$= x \wedge (x \vee x')$ [Complement Law]

$= (x \wedge x) \vee (x \wedge x')$ [Distributive Law]

$= (x \wedge x) \vee 0$ [Complement Law]

$= (x \wedge x)$ [Identity Law]

Therefore, $(x \wedge x) = x$

(*b*) $(x \vee 1) = (x \vee 1) \wedge 1$ [Identity Law]

$= (x \vee 1) \wedge (x \vee x')$ [Complement Law]

$= ((x \vee 1) \wedge x) \vee ((x \vee 1) \wedge x')$ [Distributive Law]

$= ((x \wedge x) \vee (1 \wedge x)) \vee ((x \wedge x') \vee (1 \wedge x'))$

$= (x \vee (1 \wedge x)) \vee ((x \wedge x') \vee (1 \wedge x'))$ [Idempotent Law]

$= (x \vee x) \vee ((x \wedge x') \vee x'))$ [Identity Law]

$= (x \vee x) \vee (0 \vee x')$ [Complement Law]

$= x \vee (0 \vee \mathrm{x}')$ [Idempotent Law]

$= (x \vee x')$ [Identity Law]

$= 1$ [Complement Law]

Therefore, $(x \vee 1) = 1$

Again, $(x \wedge 0) = (x \wedge 0) \vee 0$ [Identity Law]

$= (x \wedge 0) \vee (x \wedge x')$ [Complement Law]

$= ((x \wedge 0) \vee x) \wedge ((x \wedge 0) \vee x')$ [Distributive Law]

$= ((x \vee x) \wedge (0 \vee x)) \wedge ((x \vee x') \wedge (0 \vee x'))$

$= ((x \vee x) \wedge x) \wedge ((x \vee x') \wedge x')$ [Identity Law]

$= (x \wedge x) \wedge ((x \vee x') \wedge x')$ [Idempotent Law]

$= (x \wedge x) \wedge ((x \wedge x') \vee (x' \wedge x'))$ [Distributive Law]

$= x \wedge ((x \wedge x') \vee (x' \wedge x'))$ [Idempotent Law]

$= x \wedge (0 \vee (x' \wedge x'))$ [Complement Law]

$= x \wedge (0 \vee x')$ [Idempotent Law]

$= x \wedge x'$ [Identity Law]

$= 0$ [Complement law]

Therefore, $(x \wedge 0) = 0$

(*c*) $x \wedge (x \vee y) = (x \vee 0) \wedge (x \vee y)$ [Identity Law]

$= x \vee (0 \wedge y)$ [Distributive Law]

$= x \vee (y \wedge 0)$ [Commutative Law]

$= x \vee 0$ [Bound Law]

$= x$ [Identity Law]

Therefore, $x \wedge (x \vee y) = x$

Again, $x \vee (x \wedge y) = (x \wedge 1) \vee (x \wedge y)$ [Identity Law]

$= x \wedge (1 \vee y)$ [Distributive Law]

$= x \wedge (y \vee 1)$ [Commutative Law]

$= x \wedge 1$ [Bound Law]

$= x$ [Identity Law]

Therefore, $x \vee (x \wedge y) = x$

(*d*) $x' \vee x = x \vee x'$ [Commutative Law]

$= 1$ [Complement Law]

i.e. $x' \vee x = 1$

Also, $x' \wedge x = x \wedge x'$ [Commutative Law]

$= 0$ [Complement Law]

i.e., $x' \wedge x = 0$

Thus we have $x' \vee x = 1$ and $x' \wedge x = 0$

Therefore, $x = (x')'$ *i.e.* $(x')' = x$

(*e*) We know that $(0 \vee 1) = (1 \vee 0) = 1$

i.e. $(0 \vee 1) = 1$

Again by Theorem $(0 \wedge 1) = (1 \wedge 0) = 0$

Thus we have $(0 \vee 1) = 1$ and $(0 \wedge 1) = 0$

Therefore, $1 = 0'$ and $0' = 1$

Similarly we also have$(1 \vee 0) = 1$ and $(1 \wedge 0) = 0$

Therefore, $0 = 1'$ and $1' = 0$

(*f*) Let $a = (x \wedge y)$ and $b = (x' \vee y')$

Now

$$
\begin{aligned}
(a \vee b) &= (x \wedge y) \vee b \\
&= (x \vee b) \wedge (y \vee b) && \text{[Distributive Law]} \\
&= (x \vee (x' \vee y')) \wedge (y \vee (x' \vee y')) \\
&= ((x \vee x') \vee y') \wedge (y \vee (x' \vee y')) && \text{[Associative Law]} \\
&= (1 \vee y') \wedge (y \vee (x' \vee y')) && \text{[Complement Law]} \\
&= (1 \vee y') \wedge (y \vee (y' \vee x')) && \text{[Commutative Law]} \\
&= (1 \vee y') \wedge ((y \vee y') \vee x') && \text{[Associative Law]} \\
&= (1 \vee y') \wedge (1 \vee x') && \text{[Complement Law]} \\
&= 1 \wedge 1 && \text{[Bound Law]} \\
&= 1 && \text{[Idempotent Law]}
\end{aligned}
$$

Again,

$$
\begin{aligned}
(a \wedge b) &= (x \wedge y) \wedge (x' \vee y') \\
&= ((x \wedge y) \wedge x') \vee ((x \wedge y) \wedge y') && \text{[Distributive Law]} \\
&= ((y \wedge x) \wedge x') \vee ((x \wedge y) \wedge y') && \text{[Commutative Law]} \\
&= (y \wedge (x \wedge x')) \vee (x \wedge (y \wedge y')) && \text{[Associative Law]} \\
&= (y \wedge 0) \vee (x \wedge 0) && \text{[Complement Law]} \\
&= 0 \vee 0 && \text{[Bound Law]} \\
&= 0 && \text{[Idempotent Law]}
\end{aligned}
$$

Therefore, $(a \vee b) = 1$ and $(a \wedge b) = 0$

This implies that $b = a'$ *i.e.* $a' = b$

i.e. $(x \wedge y)' = (x' \vee y')$

Similarly the other De Morgan's law $(x \vee y)' = (x' \wedge y')$ can be proved.

■ 8.7 DUAL OF A STATEMENT

The dual of a statement involving Boolean expressions is obtained by replacing 0 by 1, 1 by 0, $\wedge$ by $\vee$, and $\vee$ by $\wedge$. Two Boolean expressions are said to be dual of each other if one expression is obtained from other by replacing 0 by 1, 1 by 0, $\wedge$ by $\vee$, and $\vee$ by $\wedge$.

Consider the statement $(x \wedge y)' = x' \vee y'$. The dual of above statement is $(x \vee y)' = x' \wedge y'$. Similarly the Boolean expressions $(x \wedge 1) = x$ and $(x \vee 0) = x$ are dual of each other.

8.7.1 Theorem

In Boolean algebra, the dual of a theorem is also a theorem.

Proof: Suppose that T is a theorem in Boolean algebra. Then there is a proof P of T involving definitions of a Boolean algebra. Let P_1 be the sequence of statements obtained by replacing 0 by 1, 1 by 0, $\wedge$ by $\vee$ and $\vee$ by $\wedge$. Then P_1 is a proof of the dual of T.

■ 8.8 BOOLEAN FUNCTION

Let B = (S, $\vee$, $\wedge$, $'$, 0, 1) be a Boolean algebra and let X $(x_1, x_2, x_3, \ldots., x_n)$ be a Boolean expression in 'n' variables. A function $f: B^n \to B$ is called a Boolean function if f is of the form

$$f(x_1, x_2, x_3, \ldots., x_n) = X(x_1, x_2, x_3, \ldots., x_n)$$

Let us consider the example of a Boolean function $f: B^3 \to B$; B = {0, 1} defined by

$$f(x_1, x_2, x_3) = x_1 \wedge (x_2 \vee \bar{x}_3)$$

The inputs and outputs are given in the following table.

x_1	x_2	x_3	$f(x_1, x_2, x_3)$
1	1	1	1
1	1	0	1
1	0	1	0
0	1	1	0
1	0	0	1
0	1	0	0
0	0	1	0
0	0	0	0

8.8.1 Representations of Boolean Functions

We have seen that Boolean functions are nothing but the evaluation functions of Boolean expressions. It is also to be noted that two Boolean expressions give rise to the same evaluation function if and only if they are equivalent. Therefore we identify a Boolean function with any of the equivalent Boolean expressions, whose evaluation function gives it.

This gives rise to the representation of a Boolean function. There are several ways for representing Boolean functions. These are

(*a*) Tabular Representation
(*b*) n Space Representation
(*c*) Cube Representation

Here we will discuss only tabular representation.

Tabular Representation : We know that, a Boolean function is completely determined by its evaluation over any Boolean algebra. In tabular representation, the procedure is very clear. We consider a row R of the table where the output is 1. We then form the combination $(x_1 \wedge x_2 \wedge x_3 \wedge \ldots. \wedge x_n)$ and place a bar over each x_i whose value is 0 in row R. The combination formed is 1 if and only if x_i have the values given in row R. We thus OR the terms to obtain the Boolean expression.

To clear the procedure let us consider the Boolean function given by the following table.

x_1	x_2	x_3	$f(x_1, x_2, x_3)$
1	1	1	1 ← Row 1
1	1	0	0
1	0	1	1 ← Row 3
0	1	1	0
1	0	0	0
0	1	0	1 ← Row 6
0	0	1	0
0	0	0	0

From the table it is clear that, the output is 1 for the rows 1, 3 and 6. Consider the first row of the table and the combination is $(x_1 \wedge x_2 \wedge x_3)$ as $x_1 = x_2 = x_3 = 1$. Similarly for third row of the table we may construct the combination $(x_1 \wedge \overline{x_2} \wedge x_3)$ as $x_1 = 1, x_2 = 0, x_3 = 1$. Thus for sixth row the combination is $(\overline{x_1} \wedge x_2 \wedge \overline{x_3})$.

Therefore, the Boolean function $f(x_1, x_2, x_3)$ is given as

$$f(x_1, x_2, x_3) = (x_1 \wedge x_2 \wedge x_3) \vee (x_1 \wedge \overline{x_2} \wedge x_3) \vee (\overline{x_1} \wedge x_2 \wedge \overline{x_3}).$$

■ 8.9 VARIOUS NORMAL FORMS

In this section we will discuss about two normal forms. *i.e.* Disjunctive normal form and Conjunctive normal form.

8.9.1 Disjunctive Normal Form

A Boolean function $f : B^n \to B$ which consists of a sum of elementary products is called the disjunctive normal form of the given function f.

Let $f : B^n \to B$ is a Boolean function. If f is not identically zero, let $A_1, A_2, A_3, \ldots, A_k$ denote the elements A_i of B_2^n, for which $f(A_i) = 1$,

where $A_i = (a_1, a_2, \ldots a_n)$.

For each A_i set $m_i = (y_1 \wedge y_2 \wedge y_3 \wedge \ldots \wedge y_n)$

where, $$y_i = \begin{cases} x_i & \text{if } a_i = 1 \\ x_i' & \text{if } a_i = 0 \end{cases}$$

Then $f(x_1, x_2, x_3, \ldots, x_n) = m_1 \vee m_2 \vee m_3 \vee \ldots \vee m_k$. This representation of a Boolean function is called the disjunctive normal form.

Let us consider the Boolean function $(x_1 \oplus x_2)$. The truth table for this function is given below.

x_1	x_1	$(x_1 \oplus x_2)$
1	1	0
1	0	1
0	1	1
0	0	0

The disjunctive normal form of this function is given as

$$(x_1 \oplus x_2) = (x_1 \wedge \bar{x}_2) \vee (\bar{x}_1 \wedge x_2)$$

8.9.2 Conjunctive Normal Form

A Boolean function $f : B^n \to B$ which consists of a product of elementary sums is called the conjunctive normal form of the given function f.

Let $f : B^n \to B$ is a Boolean function. If f is not identically one, let $A_1, A_2, A_3, \ldots, A_k$ denote the elements A_i of B_2^n, for which $f(A_i) = 0$,

where $A_i = (a_1, a_2, a_3, \ldots\ldots. a_n)$.

For each A_i set

$$M_i = (y_1 \vee y_2 \vee y_3 \vee \ldots. \vee y_n)$$

where, $$y_i = \begin{cases} x_i & \text{if } a_i = 0 \\ x_i' & \text{if } a_i = 1 \end{cases}$$

Then $f(x_1, x_2, x_3, \ldots, x_n) = M_1 \wedge M_2 \wedge M_3 \wedge \ldots. \wedge M_k$. This representation of a Boolean function is called the conjunctive normal form.

Let us consider the Boolean function $(x_1 \oplus x_2)$. The truth table for this function is given below.

x_1	x_1	$(x_1 \oplus x_2)$
1	1	0
1	0	1
0	1	1
0	0	0

From the table it is clear that, the output is 0 for the rows 1 and 4. Consider the first row of the table and the combination is $(\bar{x}_1 \vee \bar{x}_2)$. Similarly for the fourth row the combination is $(x_1 \vee x_2)$. So the conjunctive normal form for this function is given as

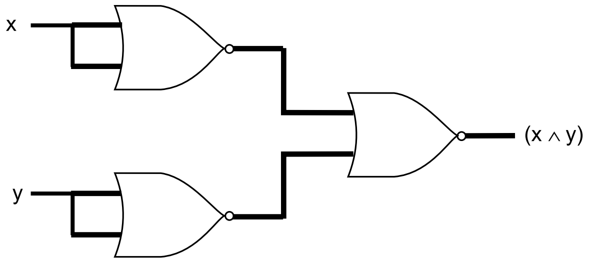
$$(x_1 \oplus x_2) = (\bar{x}_1 \vee \bar{x}_2) \wedge (x_1 \vee x_2)$$

Note: A term of the form $(y_1 \wedge y_2 \wedge y_3 \wedge \ldots. \wedge y_n)$, where each y_i is either x_i or $\bar{x}_i$ is called a minterm where as a term of the form $(y_1 \vee y_2 \vee y_3 \vee \ldots. \vee y_n)$, where each y_i is either x_i or $\bar{x}_i$ is called a maxterm.

SOLVED EXAMPLES

Example 1 *Construct an AND gate using three NOR gates.*

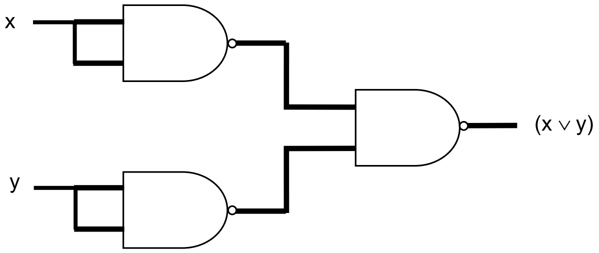
Solution : The output to an AND gate is $(x \wedge y)$, if the inputs are x and y. The output to a NOR gate is $\left(\overline{x \vee y}\right)$, if the inputs are x and y. The gating network is given below.



From the diagram given above it is clear that the output to the first NOR gate is $\left(\overline{x \vee x}\right) = \bar{x}$. Similarly the output to the second NOR gate is $\left(\overline{y \vee y}\right) = \bar{y}$. Therefore the output to the final NOR gate is $(x \wedge y)$.

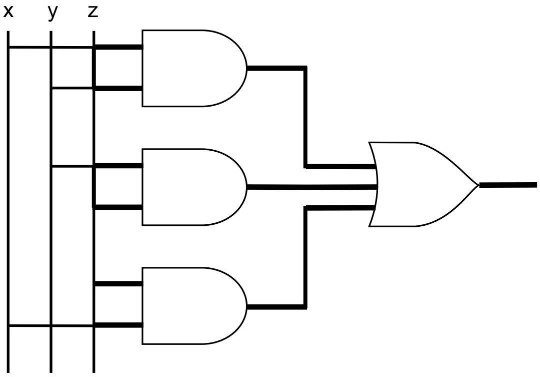
Example 2 *Construct an OR gate using three NAND gates.*

Solution : The output to an OR gate is $(x \vee y)$, if the inputs are x and y. The output to an NAND gate is $\left(\overline{x \wedge y}\right)$, if the inputs are x and y. The gating network is given as below.



Example 3 *Describe a gating network corresponding to the statement (x . y) + (y . z) + (z . x).*

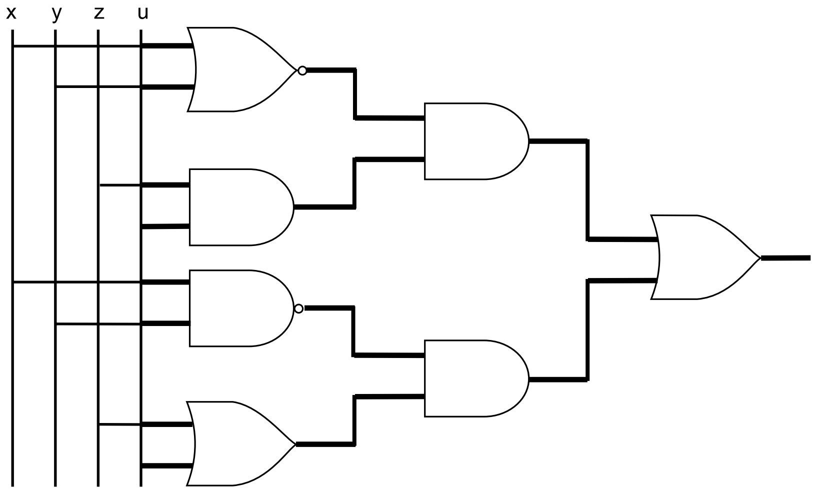
Solution: Given statement is $(x \cdot y) + (y \cdot z) + (z \cdot x)$. The gating network is given as



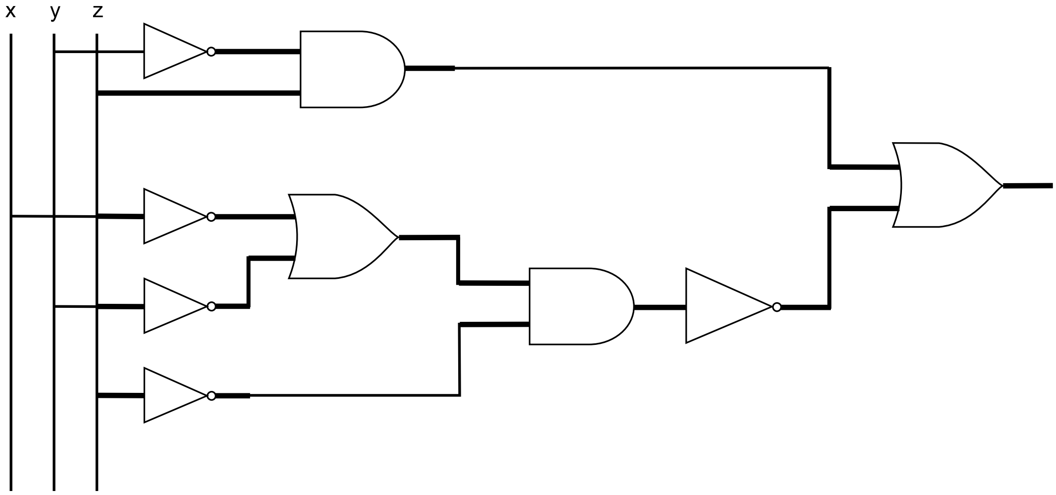
Example 4 *Describe a gating network corresponding to the statement*

$$\left(\overline{x+y}\right)(z \cdot u)+\left(\overline{x \cdot y}\right)(z+u)$$

Solution: Given statement is $\left(\overline{x+y}\right)(z \cdot u)+\left(\overline{x \cdot y}\right)(z+u)$. The gating network is given as below.



Example 5 *Describe the output of the following gating network.*



Solution : Consider the gating network given above. The output to the above gating network is given as

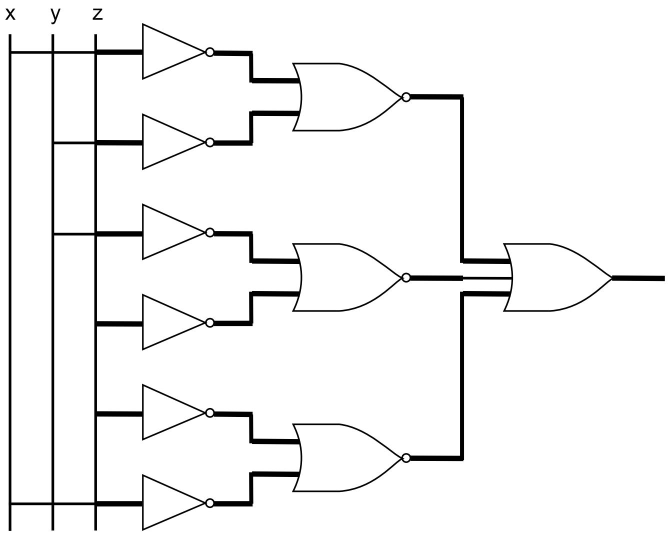
$$(\bar{y}\,.z)+((\overline{(\bar{x}+\bar{y}).\bar{z}}) = \bar{y}z+(\overline{\bar{x}+\bar{y}})+\bar{\bar{z}} \qquad \text{[De Morgan's Law]}$$

$$=\bar{y}z+\bar{\bar{x}}\,.\bar{\bar{y}}+z \qquad \text{[De Morgan's Law]}$$

$$=\bar{y}\,z+xy+z$$

Example 6 *Construct a gating network using inverter and OR gate corresponding to the statement (x . y) + (y . z) + (z . x).*

Solution : Given statement is $(x\,.\,y)+(y\,.\,z)+(z\,.\,x)$. The gating network is given below.



Example 7 *Find the value of the Boolean expression given below for x = 1, y = 1 and z = 0.*

$$(x\wedge(y\vee(x\wedge\overline{y})))\vee((x\wedge\overline{y})\vee(\overline{x\wedge\overline{z}}))$$

Solution : Given that the value of the inputs are $x = 1$, $y = 1$ and $z = 0$. Now,the value of $(x\wedge\overline{y})$ is 0

The value of $(y\vee(x\wedge\overline{y}))$ is 1

The value of $(x\wedge(y\vee(x\wedge\overline{y})))$ is 1

Similarly, the value of the $(\overline{x\wedge\overline{z}})$ is 0

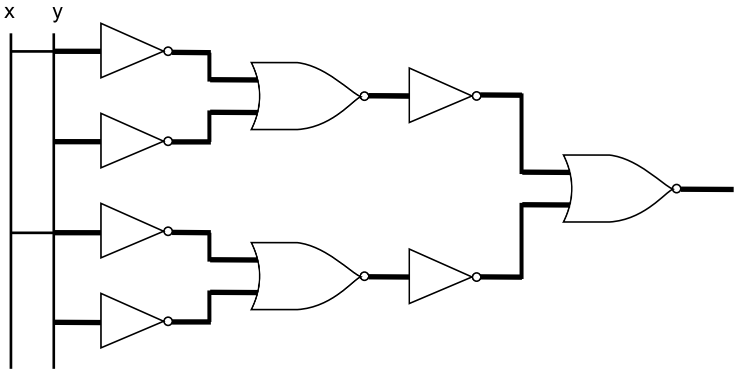
The value of $((x\wedge\overline{y})\vee(\overline{x\wedge\overline{z}}))$ is 0

So, the value of the Boolean expression

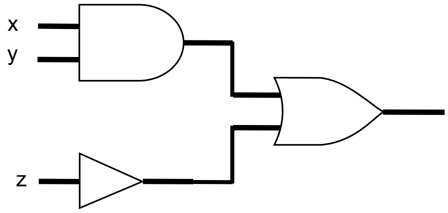
$(x\wedge(y\vee(x\wedge\overline{y})))\vee((x\wedge\overline{y})\vee(\overline{x\wedge\overline{z}}))$ is 1.

Example 8 *Construct an AND gate using inverters and three NOR gates.*

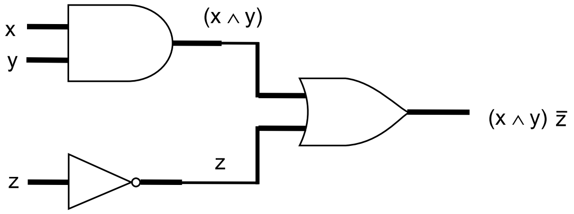
Solution : Output to an AND gate is $(x\wedge y)$ or xy, if the inputs are x and y. The output to a NOR gate is $(\overline{x\vee y})$, if the inputs are x and y. The gating network is given below.



Example 9 *Write the Boolean expression that represents the combinatorial circuit, write the logic table and write the output of each gate symbolically.*



Solution: Given the gating network as below.



The Boolean expression that represents the combinatorial circuit is $((x \wedge y) \vee \bar{z})$. The logic table is given as below.

x	y	z	$(x \wedge y)$	$(x \wedge y) \vee \bar{z}$
1	1	1	1	1
1	1	0	1	1
1	0	1	0	0
0	1	1	0	0
1	0	0	0	1
0	1	0	0	1
0	0	1	0	0
0	0	0	0	1

Example 10 *If $(x + y) = (x + z)$ and $(x' + y) = (x' + z)$, then $y = z$.*

Solution : Given that $(x + y) = (x + z)$ *i.e.* $(x \vee y) = (x \vee z)$

And $(x' + y) = (x' + z)$ *i.e.* $(x' \vee y) = (x' \vee z)$

Now,

$$
\begin{aligned}
y &= y \vee 0 && \text{[Identity Law]}\\
&= y \vee (x \wedge x') && \text{[Complement Law]}\\
&= (y \vee x) \wedge (y \vee x') && \text{[Distributive Law]}\\
&= (x \vee y) \wedge (x' \vee y) && \text{[Commutative Law]}\\
&= (x \vee z) \wedge (x' \vee \mathrm{z}) && \text{[Given Condition]}\\
&= (\mathrm{z} \vee x) \wedge (z \vee x') && \text{[Commutative Law]}\\
&= z \vee (x \wedge x') && \text{[Distributive Law]}\\
&= z \vee 0 && \text{[Complement Law]}\\
&= z && \text{[Identity Law]}
\end{aligned}
$$

Therefore, $y = z$.

Example 11 *Given the Boolean function f, write f in its disjunctive normal form.*

x	y	z	$f(x, y, z)$
1	1	1	1
1	1	0	1
1	0	1	0
0	1	1	0
1	0	0	0
0	1	0	1
0	0	1	0
0	0	0	1

Solution From the table given below it is clear that, the output is 1 for the rows 1, 2, 6 and 8. For the first row the combination is $(x \wedge y \wedge z)$. Similarly for rows 2, 6 and 8 the combinations are $(x \wedge y \wedge \bar{z})$, $(\bar{x} \wedge y \wedge \bar{z})$ and $(\bar{x} \wedge \bar{y} \wedge \bar{z})$ respectively.

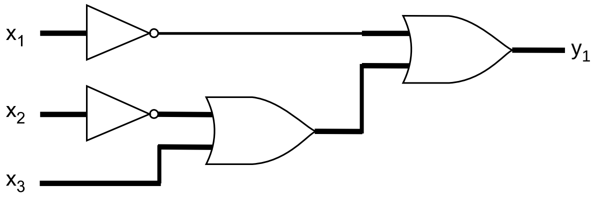
Thus, the disjunctive normal form to the above function *f* is given as

$$f(x, y, z) = (x \wedge y \wedge z) \vee (x \wedge y \wedge \bar{z}) \vee (\bar{x} \wedge y \wedge \bar{z}) \vee (\bar{x} \wedge \bar{y} \wedge \bar{z})$$

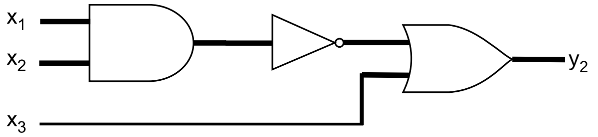
x	y	z	$f(x, y, z)$
1	1	1	1← Row 1
1	1	0	1 ← Row 2
1	0	1	0
0	1	1	0
1	0	0	0
0	1	0	1← Row 6
0	0	1	0
0	0	0	1← Row 8

Example 12. *Show that the combinatorial circuits (a) and (b) are equivalent.*

(*a*)

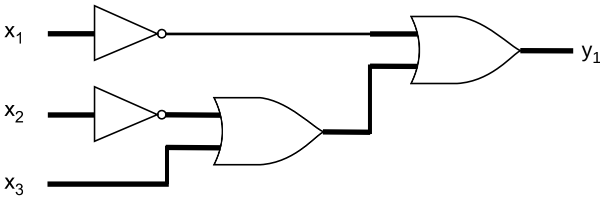


(*b*)

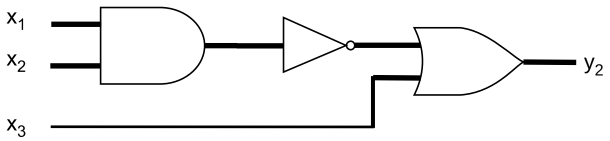


Solution: Given combinatorial circuits are

(*a*)



(*b*)



The output y_1 for combinatorial circuit (*a*) is given as

$$y_1 = \bar{x}_1 \vee (\bar{x}_2 \vee x_3) = (\bar{x}_1 \vee \bar{x}_2) \vee x_3 = \left(\overline{x_1 \wedge x_2}\right) \vee x_3$$

The output y_2 for combinatorial circuit (*b*) is given as $y_2 = \left(\overline{x_1 \wedge x_2}\right) \vee x_3$. Hence, the combinatorial circuits (*a*) and (*b*) are equivalent.

Example 13 *Reduce the following Boolean products to either 0 or a fundamental product.*

(*a*) $x\,y\,x'z$ (*b*) $x\,y\,z'y\,x$

Solution : (*a*) $x\,y\,x'z = x\,x'\,y\,z$ [Commutative Law]

$= 0\,y\,z$ [Complement Law]

$= 0$ [Bound Law]

i.e. $x\,y\,x'z = 0$

(*b*) $x\,y\,z'y\,x = x\,y\,y\,z'\,x$ [Commutative Law]

$= x\,y\,z'\,x$ [Idempotent Law]

$= x\,y\,x\,z'$ [Commutative Law]

$= x\,x\,y\,z'$ [Commutative Law]

$= x\,y\,z'$ [Idempotent law]

i.e. $x\,y\,z'y\,x = x\,y\,z'$

Example 14 *Given the Boolean function f, write f in its conjunctive normal form.*

x	*y*	*z*	*f(x, y, z)*
1	1	1	1
1	1	0	1
1	0	1	0
0	1	1	0
1	0	0	0
0	1	0	1
0	0	1	0
0	0	0	1

Solution Given the Boolean function *f* as below.

x	*y*	*z*	*f(x, y, z)*
1	1	1	1
1	1	0	1
1	0	1	0 ← Row 3
0	1	1	0 ← Row 4
1	0	0	0 ← Row 5
0	1	0	1
0	0	1	0 ← Row 7
0	0	0	1

From the table it is clear that, the output is 0 for the rows 3, 4, 5 and 7. For the third row the combination is $(\bar{x} \vee y \vee \bar{z})$. Similarly for rows 4, 5 and 7 the combinations are $(x \vee \bar{y} \vee \bar{z})$, $(\bar{x} \vee y \vee z)$ and $(x \vee y \vee \bar{z})$ respectively.

Thus, the conjunctive normal form to the above function is given as

$$f(x, y, z) = (\bar{x} \vee y \vee \bar{z}) \wedge (x \vee \bar{y} \vee \bar{z}) \wedge (\bar{x} \vee y \vee z) \wedge (x \vee y \vee \bar{z}).$$

Example 15 *Design a combinatorial circuit that computes exclusive OR; XOR of x and y.*

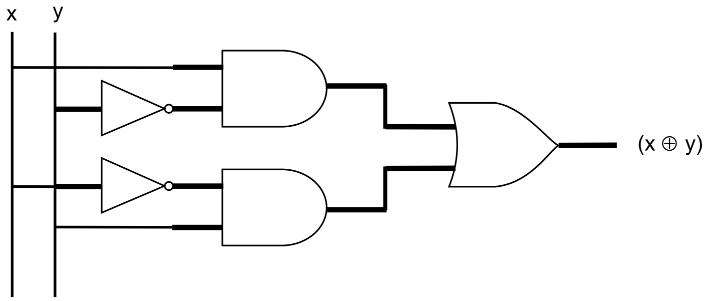
Solution : Let the inputs to the XOR gate be x and y. The logic table for XOR gate is given below.

x	y	$x \oplus y$
1	1	0
1	0	1
0	1	1
0	0	0

So, the disjunctive normal form of this function is given as

$$x \oplus y = (x \wedge y') \vee (x' \wedge y)$$

The combinatorial circuit corresponding to $(x \oplus y)$ is given below.



Example 16 *Find the disjunctive and conjunctive normal form of the given function and draw the combinatorial circuit corresponding to the disjunctive normal form.*

x	y	z	$f(x, y, z)$
1	1	1	0
1	1	0	0
1	0	1	0
0	1	1	1
1	0	0	1
0	1	0	1
0	0	1	1
0	0	0	0

Solution Given Boolean function is

x	y	z	$f(x, y, z)$
1	1	1	0
1	1	0	0
1	0	1	0
1	0	0	1← Row 4
0	1	1	1← Row 5
0	1	0	1← Row 6
0	0	1	1← Row 7
0	0	0	0

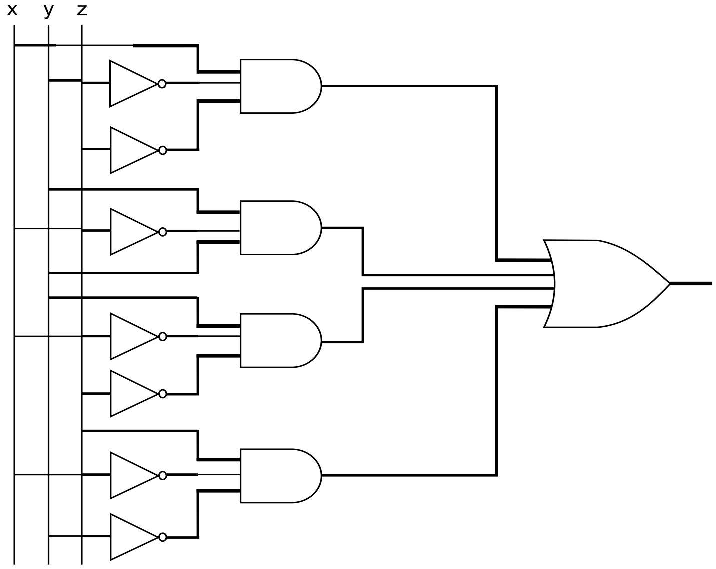
From the table it is clear that the output is 1 for rows 4, 5, 6 and 7. For the fourth row the combination is $(x \wedge y' \wedge z')$. Similarly the combinations $(x' \wedge y \wedge z)$, $(x' \wedge y \wedge z')$, and $(x' \wedge y' \wedge z)$ are for rows 5, 6 and 7 respectively. So, the disjunctive normal form to the above function is given as

$$f(x, y, z) = (x \wedge y' \wedge z') \vee (x' \wedge y \wedge z) \vee (x' \wedge y \wedge z') \vee (x' \wedge y' \wedge z).$$

Similarly, corresponding to the output 0 for rows 1, 2, 3 and 8, the conjunctive normal form to the above function is given as

$$f(x, y, z) = (x' \vee y' \vee z') \wedge (x' \vee y' \vee z) \wedge (x' \vee y \vee z') \wedge (x \vee y \vee z).$$

The combinatorial circuit corresponding to the disjunctive normal form is given below.



Example 17 *Find the disjunctive normal form of the function using algebraic technique.*

$$f(x, y) = (x \vee y) \wedge (x' \vee y')$$

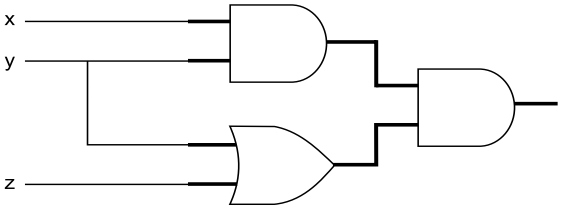
Solution :

$$\begin{aligned} f(x,y) &= (x \vee y) \wedge (x' \vee y') \\ &= (x \wedge (x' \vee y')) \vee (y \wedge (x' \vee y')) && \text{[Distributive Law]} \\ &= (x \wedge x') \vee (x \wedge y') \vee (y \wedge x') \vee (y \wedge y') && \text{[Distributive Law]} \\ &= 0 \vee (x \wedge y') \vee (y \wedge x') \vee 0 && \text{[Complement Law]} \\ &= (x \wedge y') \vee (y \wedge x') && \text{[Identity Law]} \end{aligned}$$

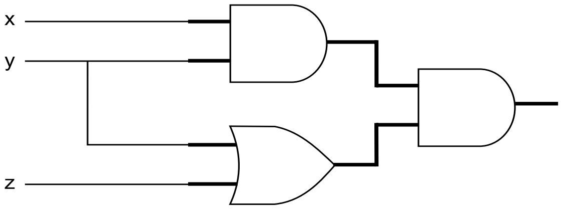
i.e. $f(x, y) = (x \wedge y') \vee (y \wedge x')$

Which is the disjunctive normal form of the function $f(x, y)$.

Example 18 *Find the disjunctive normal form for the following combinatorial circuit.*



Solution Given that the combinatorial circuit as



The output of the above combinatorial circuit is given as $f(x, y, z) = (x \wedge y) \wedge (y \vee z)$. The logic table for the above expression is given below. From the table it is clear that the function has output 1 for rows 1 and 2. For the first row the combination is $(x \wedge y \wedge z)$ where as for second row the combination is $(x \wedge y \wedge z')$. Thus, the disjunctive normal form for the above function is given as

$$f(x, y, z) = (x \wedge y \wedge z) \vee (x \wedge y \wedge z')$$

x	y	z	$(x \wedge y)$	$(y \vee z)$	$(x \wedge y) \wedge (y \vee z)$
1	1	1	1	1	1
1	1	0	1	1	1
1	0	1	0	1	0
0	1	1	0	1	0
1	0	0	0	0	0
0	1	0	0	1	0
0	0	1	0	1	0
0	0	0	0	0	0

EXERCISES

1. Find the disjunctive normal form of each function using algebraic technique.

(*a*) $f(x, y) = x \vee (x \wedge y)$

(*b*) $f(x, y, z) = x \vee y \wedge (x \vee z')$

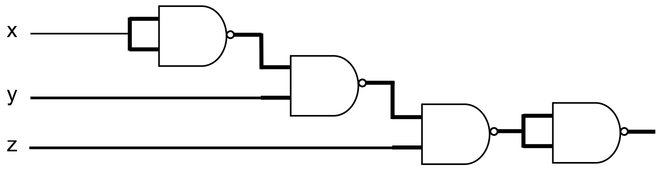
(*c*) $f(x, y, z) = x \vee (y' \vee (x\,y' \vee x\,z'))$

2. Reduce the following Boolean products to either 0 or a fundamental product.

(*a*) $x\,y\,z\,y$ (*b*) $x\,y\,z'\,y\,x'\,z'$ (*c*) $x\,y'\,z\,x\,y'$ (*d*) $x\,y\,z'\,t\,y'\,t$

(*e*) $x\,y'\,x\,z'\,t\,y'$

3. Write the logic table for the circuit given below.

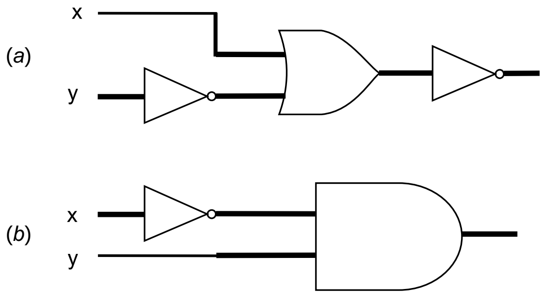


4. Find the disjunctive normal form of a Boolean expression having a logic table the same as the given table and draw the combinatorial circuit corresponding to the disjunctive normal form.

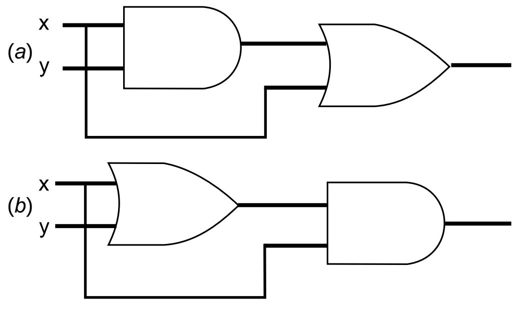
x	y	z	f
1	1	1	1
1	1	0	1
1	0	1	0
0	1	1	0
1	0	0	1
0	1	0	0
0	0	1	1
0	0	0	0

5. Are the combinatorial circuits equivalent? Explain.

(*i*)

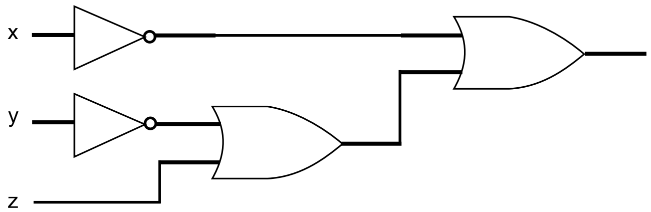


(*ii*)

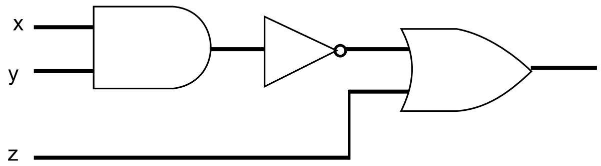


(*iii*)

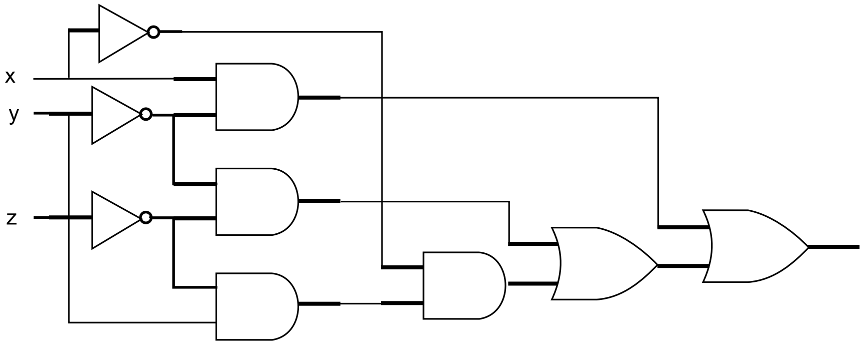
(*a*)



(*b*)



6. Find the Boolean expression in disjunctive normal form for the circuit given below.



7. Find the disjunctive normal form of each function corresponding to the logic tables given below.

(*a*)

x	*y*	*f* (*x*, *y*)
1	1	1
1	0	0
0	1	1
0	0	1

(*b*)

x	*y*	*f* (*x*, *y*)
1	1	0
1	0	1
0	1	0
0	0	1

(*c*)

x	y	z	$f(x, y, z)$
1	1	1	1
1	1	0	0
1	0	1	1
0	1	1	1
1	0	0	0
0	1	0	0
0	0	1	0
0	0	0	1

(*d*)

x	y	z	$f(x, y, z)$
1	1	1	0
1	1	0	0
1	0	1	1
0	1	1	0
1	0	0	1
0	1	0	1
0	0	1	1
0	0	0	1

8. Find the conjunctive normal form of each function given in question 7.

9. Draw the logic circuit (Combinatorial circuit) with inputs x, y, z and output Y which corresponds to each Boolean expression.

(*i*) $Y = x'y\,z + x'y\,z' + x\,y\,z'$

(*ii*) $Y = x\,y'\,z + x\,z' + y'\,z$

10. Construct a combinatorial circuit that represents the following Boolean function.

x	y	z	$f(x, y, z)$
1	1	1	0
1	1	0	1
1	0	1	1
0	1	1	1
1	0	0	1
0	1	0	1
0	0	1	1
0	0	0	0

11. Write the dual of each Boolean equation.

(*a*) $(a \wedge 1) \vee (0 \vee a') = 0$

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

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

(*d*) $(a \vee 1) \wedge (a \vee 0) = a$

(*e*) $(a \wedge a') \vee (a \wedge 0) = a$

(*f*) $(a \vee b) \wedge (b \vee c) = (a \wedge c) \vee b$

[**Hint:** To obtain the dual equation, interchange $\vee$ and $\wedge$, and interchange 0 and 1]

12. Discuss a XOR gate with four inputs x, y, z and t.

13. Express the following Boolean expression $f(x, y, z)$ as a sum of products and then in its complete sum- of- products form.

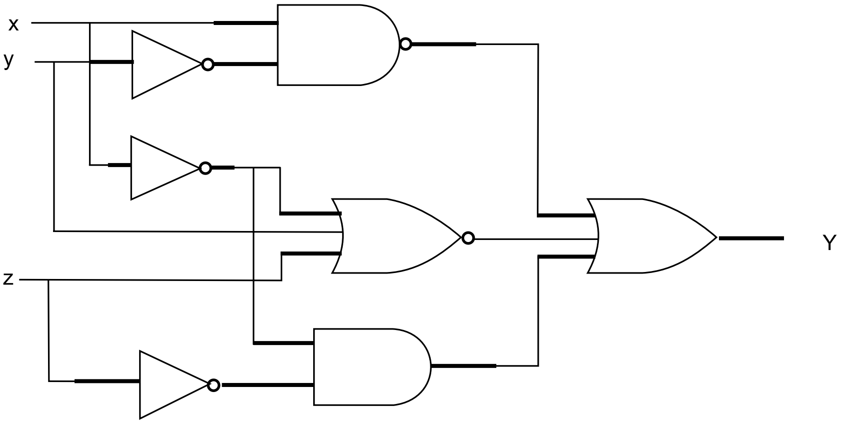
(*a*) $f(x, y, z) = x\ (x\ y' + x'y + y'\ z)$

(*b*) $f(x, y, z) = (x'+ y)' + y'\ z$

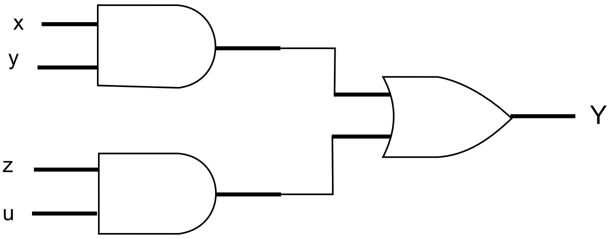
(*c*) $f(x, y, z) = (x + y'\ z)\ (y +\ z')$

14. Express the output Y as a Boolean expression in the inputs x, y, z, t and u for the logic circuits given below.

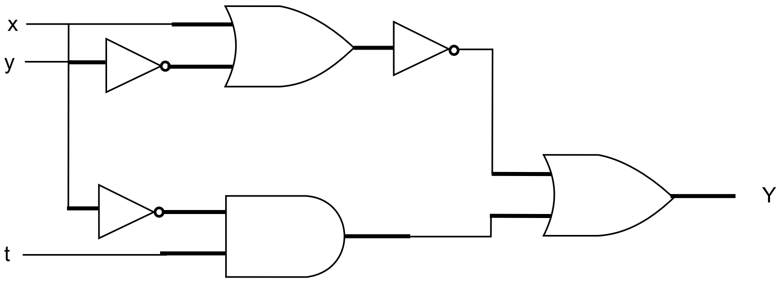
(*a*)



(*b*)



(*c*)



9

Introduction to Lattices

9.0 INTRODUCTION

In this chapter, we shall introduce the fundamental concepts of Lattices. After defining them as particular kind of poset (partial ordered sets) we shall show that they could be introduced as algebraic systems possessing some specific properties. Here we will discuss Lattices, Duality principle, Distributed lattices, Bounded lattices, Complemented lattices and some special kind of lattices.

9.1 LATTICES

Lattices is a partially ordered set (poset) in which every two elements have a unique least upper bound (L.U.B.) and a unique greatest lower bound (G.L.B.) *i.e.* a lattice is a poset $\langle$ L , $\leq\rangle$ in which every subset $\{a, b\}$ has a least upper bound and greatest lower bound. Where

L.U.B $(\{a, b\}) = a \vee b$ (join of a and b)

G.L.B $(\{a , b\}) = a \wedge b$ (meet of a and b)

Let us consider the poset (N, $\leq$); where N is a set of natural numbers and $\leq$ is the ordinary less than or equal to relation. To show (N , $\leq$) is a lattice, it is sufficient to define the L.U.B.and G.L.B. in N.

Now, Let $a, b \in$ N

L.U.B. $(\{a, b\}) = (a \vee b) =$ Max (a, b) and

G.L.B. $(\{a, b\}) = (a \wedge b) =$ Min (a, b)

Therefore, (N, $\leq$) is a lattice.

9.1.1 Theorem

For a lattice (B , $\leq$); a , $b \in$ B

$$a \leq (a \vee b) \text{ and } (a \wedge b) \leq a.$$

Proof : Given (B , $\leq$) is a lattice and a , $b \in$ B

Now, $(a \vee b) =$ L.U.B. $(\{a, b\})$

i.e., $(a \vee b)$ is an upper bound of both a and b.

This implies that $a \leq (a \vee b)$.

Again, $$(a \wedge b) = \text{G.L.B. } (\{a, b\})$$

i.e., $(a \wedge b)$ is the lower bound of both a and b.

This implies that $(a \wedge b) \leq a$.

■ 9.2 HASSE DIAGRAM

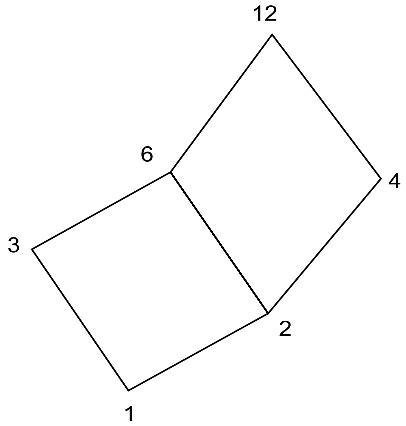
In principle, it is possible to draw a diagram which shows the order relation on a finite poset. Let (B, ≤) be a poset. Define the relation ≤ on B by x R y if and only if $x \leq y$ but $x \neq y$ for $x, y \in$ B. Given a partial order ≤ on B, 'y' is said to cover 'x' if $x < y$ and there is no element 'z' in B such that x R z and z R y.

A Hasse diagram of a poset (B, ≤) is a graphical representation consisting of points labeled by the members of B, with a line segment directed generally upward from x to wherever y covers x.

Let us consider B = D(12); set of all positive divisors of 12. Therefore, B = {1, 2, 3, 4, 6, 12}. Let us define the relation x R y means x is a divisor of y for $x, y \in$ B. Thus we get

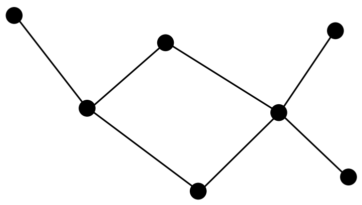
R = {(1, 2), (1, 3), (1,4), (1, 6), (1, 12), (2, 4), (2, 6), (2, 12), (3, 6), (3, 12), (4, 12), (6, 12)}

From the above relation it is clear that 4 does not cover 1 because there exists 2 such that 1 R 2 and 2 R 4. Similarly 6 does not cover 1, 12 does not cover 1, 12 does not cover 2 and 12 does not cover 3. Again it is also clear that 2 covers 1, 3 covers 1, 6 covers both 2 and 3 and 12 covers both 4 and 6. Therefore, the Hasse diagram is given below.

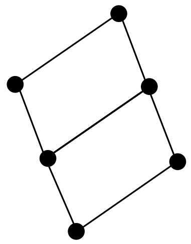


Note: We can distinguish lattices by looking at their Hasse diagrams. Because any two elements have a common predecessor and a common successor, the Hasse diagram of a lattice always is made up as a combination of closed polygons and thus its name lattice. A poset which has polygons open above or below is not a lattice because of lack of supremum or infimum.

Consider the following Hasse diagram.



(Figure 1)



(Figure 2)

The above Hasse diagrams are posets, but figure 1 which is open above as well as open below is not a lattice where as figure 2 is a lattice.

■ 9.3 PRINCIPLE OF DUALITY

Given a valid statement for a Lattice we can obtain another valid statement by replacing the relation ≤ with ≥, join with meet and meet with join operation. This is known as the principles of duality in lattices.

9.3.1 Theorem

Let B be a Lattice with $a, b, c \in$ B, then following properties holds.

1. **Idempotent Properties**

   (a) $(a \vee a) = a$

   (b) $(a \wedge a) = a$

2. **Commutative Properties**

   (a) $(a \vee b) = (b \vee a)$

   (b) $(a \wedge b) = (b \wedge a)$

3. **Associative Properties**

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

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

4. **Absorption Properties**

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

   (b) $a \wedge (a \vee b) = \mathrm{a}$

Proof :

1. **Idempotent Properties**

   (a) We know that $(a \vee b) =$ L.U.B. $(\{a , b\})$

This implies that $a \leq (a \vee a)$ … (i)

Again, $a \leq a$

This implies $(a \vee a) \leq a$ … (ii)

Combining (i) and (ii) we will get

$$(a \vee a) = a$$

(b) Applying the principle of duality, we have,

$$(a \wedge a) = a$$

2. Commutative Properties

(*a*) We know that $(a \vee b) = \text{L.U.B.}(\{a, b\})$

and $(b \vee a) = \text{L.U.B.}(\{b, a\})$

$= \text{L.U.B.}(\{a, b\})$

$= (a \vee b)$

Therefore, $(a \vee b) = (b \vee a)$

(*b*) Applying the principle of duality, we have

$$(a \wedge b) = (b \wedge a)$$

3. Associative Properties

(*a*) Let $a \vee (b \vee c) = d$

and $(a \vee b) \vee c = e$

This implies that $a \leq d$ and $(b \vee c) \leq d$ $[\because a \leq (a \vee b); b \leq (a \vee b)]$

$\Rightarrow$ $a \leq d, b \leq d, c \leq d$

$\Rightarrow$ $(a \vee b) \leq d$ and $c \leq d$

$\Rightarrow$ $(a \vee b) \vee c \leq d$

i.e. $e \leq d$ ...(*i*)

Again, $(a \vee b) \vee c = e$

$\Rightarrow$ $(a \vee b) \leq e, c \leq e$

$\Rightarrow$ $a \leq e, b \leq e, c \leq e$

$\Rightarrow$ $a \leq e, (b \vee c) \leq e$

$\Rightarrow$ $a \vee (b \vee c) \leq e$

$\Rightarrow$ $d \leq e$ ...(*ii*)

Therefore from equations (*i*) and (*ii*) we have $d = e$

i.e. $a \vee (b \vee c) = (a \vee b) \vee c$

(*b*) Applying the principle of duality, we have

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

4. Absorption Properties

(*a*) We know that $a \vee (a \wedge b) = \text{L.U.B.}(\{a, a \wedge b\})$

This implies that $a \leq a \vee (a \wedge b)$ ...(*i*)

Again, $a \leq a$ and $(a \wedge b) \leq a$ $[\because (a \wedge b) = \text{G.L.B.}(\{a, b\})]$

$\Rightarrow$ $a \vee (a \wedge b) \leq (a \vee a) = a$

$\Rightarrow$ $a \vee (a \wedge b) \leq a$ ...(*ii*)

Combining equations (*i*) and (*ii*) we get

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

(*b*) Applying the principle of duality, we have

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

9.3.2 Theorem

Let (B, ≤) be a lattice. For any a, b, c, d in Lattice B if $a \leq b$ and $c \leq d$, then $(a \vee c) \leq (b \vee d)$ and $(a \wedge c) \leq (b \wedge d)$.

Proof : Given (B, ≤) is a lattice and a, b, c, $d \in$ B.

Suppose that, $a \leq b$ and $c \leq d$

We know that $(b \vee d)$ = L.U.B. ($\{b, d\}$)

This implies that $b \leq (b \vee d)$ and $d \leq (b \vee d)$

⇒ $a \leq (b \vee d)$ and $c \leq (b \vee d)$ [∵ $a \leq b$ and $c \leq d$]

So, $(b \vee d)$ is an upper bound of a and c. Again $(a \vee c)$ is the least upper bound of a and c. Therefore,

$$(a \vee c) \leq (b \vee d)$$

Again, we know that $(a \wedge c)$ = G.L.B. ($\{a, c\}$)

This implies that $(a \wedge c) \leq a$ and $(a \wedge c) \leq c$

⇒ $(a \wedge c) \leq b$ and $(a \wedge c) \leq d$ [∵ $a \leq b$ and $c \leq d$]

Therefore, $(a \wedge c)$ is the lower bound of b and d. Again $(b \wedge d)$ is the greatest lower bound of b and d. Hence, we get

$$(a \wedge c) \leq (b \wedge d)$$

9.3.3 Theorem

Let (B, ≤) be a lattice. For any a, b, $c \in$ B we have

(*a*) If $a \leq b, a \leq c$,

then $a \leq (b \vee c)$ and $a \leq (b \wedge c)$

(*b*) If $a \geq b, a \geq c$,

then $a \geq (b \wedge c)$ and $a \geq (b \vee c)$

Proof: (*a*) Given that (B, ≤) be a lattice and a, b, $c \in$ B.

Suppose that $a \leq b$, $a \leq c$. This indicates that a is a lower bound of $\{b, c\}$.

Therefore, $a \leq$ G.L.B. ($\{b, c\}$) $= (b \wedge c)$

i.e. $a \leq (b \wedge c)$

Again, $(b \vee c)$ = L.U.B. ($\{b, c\}$)

This implies that $b \leq (b \vee c)$.

Also by hypothesis $a \leq b$.

Therefore, we have $a \leq b \leq (b \vee c)$.

i.e. $a \leq (b \vee c)$.

i.e. $a \leq b, a \leq c$,

⇒ $a \leq (b \vee c)$ and $a \leq (b \wedge c)$.

(*b*) On applying the principle of duality we can prove that if $a \geq b, a \geq c$,

then $a \geq (b \wedge c)$ and $a \geq (b \vee c)$.

■ 9.4 DISTRIBUTIVE LATTICE

A lattice B is said to be distributive lattice if for a , b, $c \in$ B we have (*a*) $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$

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

If a lattice is not distributive then it is called "non distributive" lattice.

9.4.1 Theorem

If the meet operation is distributive over the join operation in a Lattice, then the join operation is also distributive over the meet operation and vice versa.

Proof : Let (B, ≤) be a Lattice and the meet operation is distributive over the joint operation.

i.e $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c);\ a\ ,\ b\ ,\ c \in \mathrm{B}$

Now, $(a \vee b) \wedge (a \vee c) = [(a \vee b) \wedge a\ ] \vee [(a \vee b) \wedge c]$

$= a \vee [(a \vee b) \wedge c]$ [Absorption Law]

$= a \vee [(a \wedge c) \vee (b \wedge c)]$

$= [a \vee (a \wedge c)] \vee (b \wedge c)$ [Associative Law]

$= a \vee (b \wedge c)$ [Absorption Law]

Therefore, $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$

9.4.2 Theorem

In any distributive lattice (B, ≤), the joint cancellation law holds.

i.e. If $(a \vee b) = (a \vee c)$ and $(a \wedge b) = (a \wedge c)$

then $b = c$.

Proof: Suppose that $(a \vee b) = (a \vee c)$ and $(a \wedge b) = (a \wedge c)$

Now, $b = b \vee (a \wedge b)$ [Absorption Law]

$= b \vee (a \wedge c)$ [Hypothesis]

$= (b \vee a) \wedge (b \vee c)$ [Distributive Law]

$= (a \vee b) \wedge (b \vee c)$ [Commutative Law]

$= (a \vee c) \wedge (b \vee c)$ [Hypothesis]

$= (a \wedge b) \vee c$ [Distributive Law]

$= (a \wedge c) \vee c$ [Hypothesis]

$= c$ [Absorption Law]

Therefore, $b = c$.

9.4.3 Theorem

In a distributed lattice (B, ≤) the following equality holds for all $a, b, c \in \mathrm{B}$

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

Proof: Suppose that B be a distributive lattice with $a, b, c \in$ B.

Now, $(a \wedge b) \vee (b \wedge c) \vee (c \wedge a) = [\{(a \wedge b) \vee b\} \wedge \{(a \wedge b) \vee c\}] \vee (c \wedge a)$

$= [\,b \wedge \{(a \wedge b) \vee c\}] \vee (c \wedge a)$ [Absorption Law]

$$= [\,b \wedge \{(a \vee c) \wedge (b \vee c)\}] \vee (c \wedge a) \qquad \text{[Distributive Law]}$$
$$= [(a \vee c) \wedge \{b \wedge (b \vee c)\}] \vee (c \wedge a) \qquad \text{[Associative Law]}$$
$$= [(a \vee c) \wedge b] \vee (c \wedge a) \qquad \text{[Absorption Law]}$$
$$= \{(a \vee c) \vee (c \wedge a)\} \wedge \{b \vee (c \wedge a)\} \qquad \text{[Distributive Law]}$$
$$= (c \vee a) \wedge (b \vee c) \wedge (b \vee a) \qquad \text{[Distributive Law]}$$
$$= (a \vee b) \wedge (b \vee c) \wedge (c \vee a)$$

Therefore,

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

■ 9.5 BOUNDED LATTICE

A lattice B is said to be bounded if it has a lower bound and an upper bound. The universal lower bound and the universal upper bound are denoted by 0 and 1 respectively.

9.5.1 Universal Lower Bound

Let (B, ≤) be a lattice. An element $a \in$ B is said to be universal lower bound if

$$a \le b \;\forall\; b \in \text{B}.$$

9.5.2 Universal Upper Bound

Let (B, ≤) be a lattice. An element $a \in$ B is said to be universal upper bound if

$$b \le a \;\forall\; b \in \text{B}.$$

9.5.3 Theorem

The universal lower bound and the universal upper bound are unique.

Proof: Let us first show that the universal lower bound is unique. Suppose two the contrary there exists two universal lower bound a and b of the lattice (B, ≤).

Therefore, $a, b \in$ B.

Now as 'a' is the universal lower bound we have

$$a \le b \qquad \ldots (i)$$

Similarly, as 'b' is the universal lower bound we have

$$b \le a. \qquad \ldots (ii)$$

Hence, from equations (i) and (ii) we get

$$a = b$$

Therefore, our supposition is wrong. Thus, the universal lower bound is unique.

Similarly, it can be shown that the universal upper bound is also unique.

9.5.4 Theorem

In a bounded lattice (B, ≤), the universal upper and lower bounds 1 and 0 clearly satisfy the followings for any element $a \in$ B.

(i) $a \vee 1 = 1$ (ii) $a \wedge 1 = a$

(iii) $a \vee 0 = a$ (iv) $a \wedge 0 = 0$

Proof: (*i*) We know that for any lattice (B , ≤)

$$a \le (a \vee b) \text{ for } a\ ,\, b \in \mathrm{B}$$

So, $$1 \le (a \vee 1) \qquad \ldots (i)$$

Again, since 1 is the universal upper bound

$$(a \vee 1) \le 1 \qquad \ldots (ii)$$

Combining (*i*) and (*ii*) we get $(a \vee 1) = 1$

(*ii*) We know that for any lattice (B, ≤)

$$(a \wedge b) \le a \text{ for } a, b \in \mathrm{B}$$

So, $$(a \wedge 1) \le a \qquad \ldots(i)$$

Again, since 1 is the universal upper bound we have $a \le 1$. Also we know that $a \le a$. Therefore,

$$(a \wedge a) \le (a \wedge 1)$$

i.e. $$a \le (a \wedge 1) \qquad \ldots (ii)$$

Combining (*i*) and (*ii*) we get $(a \wedge 1) = a$

Similarly, (*iii*) and (*iv*) can be proved.

■ 9.6 COMPLEMENTED LATTICE

A lattice (B, ≤) is said to be complemented lattice if every element in the lattice has a complement.

9.6.1 Complement of an Element

Let (B, ≤) be a lattice with 0 and 1 as its universal lower bound and upper bound respectively. An element b is said to be complement of $a \in \mathrm{B}$ if

$$(a \vee b) = 1 \text{ and } (a \wedge b) = 0$$

From the commutative property, if '*b*' is complement of '*a*' then '*a*' is also complement of '*b*'.

9.6.2 Theorem

In a bounded distributive lattice, if a complement exists then it is unique.

Proof : Let (B, ≤) be a bounded distributive lattice.

Let $a \in \mathrm{B}$ and a_1, a_2 are two complements of a. Hence by definition we have

$$a \vee a_1 = 1; \qquad a \vee a_2 = 1$$
$$a \wedge a_1 = 0\ ; \qquad a \wedge a_2 = 0$$

Now, $$a_1 = (a_1 \vee 0) = a_1 \vee (a \wedge a_2) \qquad [\because (a \wedge a_2) = 0]$$
$$= (a_1 \vee a) \wedge (a_1 \vee a_2) \qquad [\text{Distributive Law}]$$
$$= 1 \wedge (a_1 \vee a_2)$$
$$= (a_1 \vee a_2)$$

So, $$a_1 = (a_1 \vee a_2) \qquad \ldots (i)$$

Similarly, $$a_2 = (a_2 \vee 0) = a_2 \vee (a \wedge a_1) \qquad [\because (a \wedge a_1) = 0]$$
$$= (a_2 \vee a) \wedge (a_2 \vee a_1) \qquad [\text{Distributive Law}]$$

$$= (a \vee a_2) \wedge (a_1 \vee a_2)$$
$$= 1 \wedge (a_1 \vee a_2)$$
$$= (a_1 \vee a_2)$$

So, $\quad a_2 = (a_1 \vee a_2) \quad \ldots (ii)$

Therefore, from equations (*i*) and (*ii*) we get

$$a_1 = a_2$$

Thus, in a bounded distributive lattice, if a complement exists then it is unique.

■ 9.7 SOME SPECIAL LATTICES

Here we will discuss some special type of lattices.

9.7.1 Boolean Lattice

A complemented and distributive Lattice is called a Boolean Lattice.

9.7.2 Sublattice

Let (B, ≤) be a Lattice. Then any nonempty subset L of B is called a sub lattice of B if

$$(a \vee b) \in \text{L and } (a \wedge b) \in \text{L}; \forall\, a, b \in \text{L}$$

In general if D(n) be a lattice and if m divides n, D(m) is a sublattice of D(n).

9.7.3 Isomorphic Lattices

Let (B_1, ≤) and (B_2, ≤) be two Lattices, then $f : B_1 \rightarrow B_2$ is an isomorphism if

$$f(a \wedge b) = f(a) \wedge f(b) \text{ and } f(a \vee b) = f(a) \vee f(b) \text{ for all } a, b \in \text{A}$$

If two lattices are isomorphic as posets then they are said to be isomorphic lattices.

SOLVED EXAMPLES

Example 1 *Show that (I , /) is a lattice ; where I is the set of positive integers and the relation | is defined as a | b if and only if a divides b.*

Solution : To show (I, |) is lattice, first of all we have to show that (I, |) is a poset. Here the relation is defined as

$a\,\text{R}\,b \quad : \quad a \mid b\,; \quad a, b \in \text{I}$

i.e. $\quad a\,\text{R}\,b \quad : \quad a$ divides b

Reflexive: It is clear that for every $a \in$ I, a divides a, *i.e.* $a \mid a$ for every $a \in$ I.

Anti Symmetric: Suppose that a R b and b R a.

i.e. $\quad a$ divides b and b divides a.

This implies that $\quad a = b$.

i.e. a R b and b R a implies that $a = b$.

Transitive: Suppose that a R b and b R c

i.e. $\quad a$ divides b and b divides c.

This implies $\quad b = a\,k_1$ and $c = b\,k_2$; k_1 and $k_2 \in$ I

Now, $c = b\,k_2 = a\,(k_1\,k_2)$.

This indicates that a divides c.

i.e. $a \text{ R } b$ and $b \text{ R } c$ implies $a \text{ R } c$.

Therefore, (I, |) is a poset. To show it is a lattice, it is sufficient to define the L.U.B. and G.L.B. in I.

Now, let a, $b \in$ I

$$\text{L.U.B. } (\{a\ , b\}) = (a \vee b) = \text{L.C.M. } (a\ , b) \text{ and}$$
$$\text{G.L.B. } (\{a\ , b\}) = (a \wedge b) = \text{G.C.D. } (a\ , b)$$

Therefore, (I, |) is a lattice.

Example 2 *For a Lattice B ; a , b ∈ B prove the following*

(i) $(a \vee b) = b$ *if and only if* $a \leq b$

(ii) $(a \wedge b) = a$ *if and only if* $a \leq b$

(iii) $(a \wedge b) = a$ *if and only if* $(a \vee b) = b$

Solution Given B is a Lattice and $a, b \in$ B

(*i*) Suppose that $(a \vee b) = b$.

Our claim is that $a \leq b$.

Now, $(a \vee b) = \text{L.U.B. } (\{a\ , b\})$

i.e. $a \leq (\text{a} \vee b)$

i.e. $a \leq b$ $[\because b = (a \vee b)]$

Conversely, suppose that $a \leq b$.

Our claim is that $(a \vee b) = b$

Given that $a \leq b$. Also we know that $b \leq b$. Hence it is clear that b is an upper bound of a and b. Again $(a \vee b)$ is the least upper bound, so

$$(a \vee b) \leq b \qquad \dots (1)$$

Again since $(a \vee b)$ is an upper bound of a and b. So,

$$b \leq (a \vee b) \qquad \dots (2)$$

Hence, from equations (1) and (2) we get

$$(a \vee b) = b.$$

(*ii*) Suppose that $(a \wedge b) = a$

Our claim is $a \leq b$

We know that $(a \wedge b) = \text{G.L.B. } (\{a, b\})$

i.e. $(a \wedge b) \leq b$

This implies that $a \leq b$ $[\because (a \wedge b) = a\ ]$

Conversely, Suppose that $a \leq b$

Our Claim is $(a \wedge b) = a$.

Given $a \leq b$, also we know that $a \leq a$.

Hence it is clear that 'a' is the lower bound of both a and b. Again $(a \wedge b)$ is the G.L.B. of both a and b. Therefore,

$$a \leq (a \wedge b) \qquad \dots (i)$$

Also, $(a \wedge b)$ is the lower bound of a and b. Therefore,

$$(a \wedge b) \leq a \qquad \ldots (ii)$$

Combining (i) and (ii) we get $(a \wedge b) = a$.

(iii) On combining the proofs of (i) and (ii) we can get

$$(a \wedge b) = a \text{ if and only if } (a \vee b) = b$$

Example 3 *Let B be the power set of S = {1, 2, 3} and (B, ⊴) be a poset defined by X ≤ Y if X ⊆ Y for X, Y ∈ B. Draw the Hasse diagram of the poset (B, ⊴).*

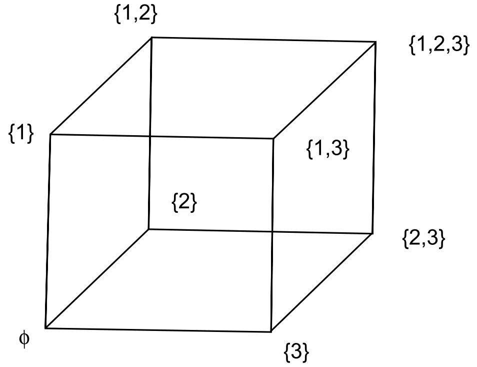
Solution : Given that B be the power set of S = {1, 2, 3}.

Therefore, B = {ϕ, {1}, {2}, {3}, {1, 2}, {1, 3}, {2, 3}, {1, 2, 3}}.

Given that (B, ≤) be a poset. Where the relation ≤ is defined as

XRY : X ⊆ Y for X, Y ∈ B

Therefore, the Hasse diagram is given as



Example 4 *Set of all positive divisors of 30 i.e. D(30), forms a poset under the relation x ≤ y means x divides y for x, y ∈ D(30). Draw the Hasse diagram.*

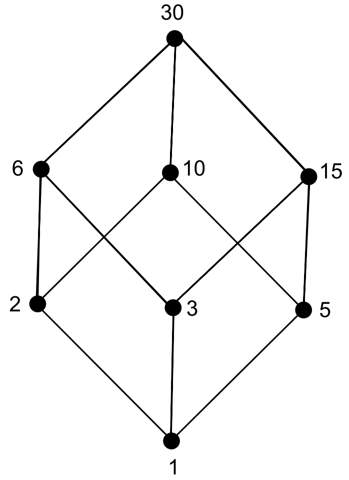
Solution : D(30) = {1, 2, 3, 5, 6, 10, 15, 30}.

Let us define the relation x R y means x is a divisor of y for $x, y \in$ D(30). Thus we get

R = {(1, 2), (1, 3), (1, 5), (1, 6), (1, 10), (1, 15), (1, 30), (2, 6), (2, 10), (2, 30), (3, 6), (3, 15), (3, 30), (5, 10), (5, 15), (5, 30), (6, 30), (10, 30), (15, 30)}

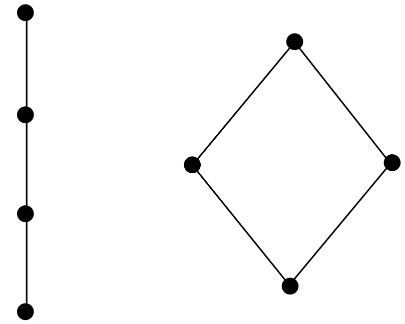
From the above relation it is clear that 6 does not cover 1 because there exists 2 such that 1 R 2 and 2 R 6. Similarly 10 does not cover 1, 15 does not cover 1 and 30 does not cover 1, 2, 3, 5. Again it is also clear that 2 covers 1, 3 covers 1, 5 covers 1 and so on.

Therefore, the Hasse diagram is given below.



Example 5 *Draw Hasse diagrams of all lattices with four elements.*

Solution: Hasse diagrams of all lattices with four elements are given below.

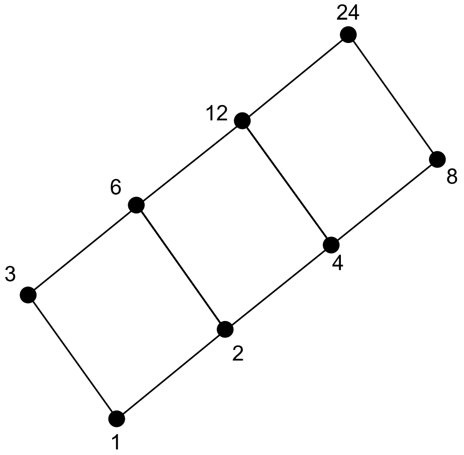


Example 6 *If B = D(24) be a lattice, then find all the sublattices of D(24). Also draw the Hasse diagram.*

Solution : Given that B = D(24) be a lattice. Where D(24) is the set of all positive divisors of 24. Therefore,

D(24) = {1, 2, 3, 4, 6, 8, 12, 24}

The Hasse diagram for the above lattice is given below.

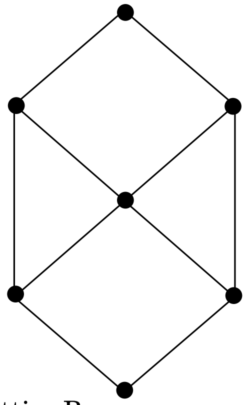


The sublattices of D(24) are D(6) = {1, 2, 3, 6}, {2, 4, 6, 12} and {4, 8, 12, 24}. Another sublattice is D(12) = {1, 2, 3, 4, 6, 12} as 12 divides 24.

EXERCISES

1. Let n be the positive integer and D(n) be the set of all positive divisor of n, then show that D(n) is a lattice under the relation of divisibility.
2. Let A = {1, 2, 3, 4, 5, 6}. We define x R y as $x \leq y$ if x divides y. Draw the Hasse diagram of the poset (A, ≤).
3. Draw the Hasse diagram of (P(A), ⊆). Where A = {1, 2} and P(A) is the power set of A.
4. Draw the Hasse diagram of (P(A), ⊆). Where A = {0, 1, 2, 3} and P(A) is the power set of A.
5. Draw the Hasse diagram of (D(n), |) for n = 6, 16, 24, 32, 100.

6. Draw Hasse diagrams of all lattices with five elements.
7. Show that set of all positive divisors of 105 *i.e.* D(105), forms a poset under the relation $x \leq y$ means x divides y for $x, y \in$ D(105). Draw the Hasse diagram.
8. Show that the poset with the Hasse diagram given below is not a lattice.



9. Prove that for all a, b, c in a lattice B,

$$[(a \wedge b) \vee (a \wedge c)] \wedge [(a \wedge b) \vee (b \wedge c)]$$

10. If B = D(30) be a lattice, then find all the sublattices of D(30). Also draw the Hasse diagram.

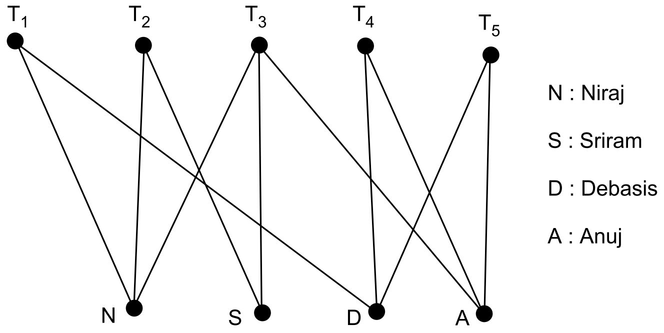
10

Graph Theory

■ 10.0 INTRODUCTION

Graph theory has applications in many areas like Mathematics, Computer Science, Engineering, Communication Science etc. Oystein Ore, the prominent graph theorist and author of the first graph theory book said in that "the theory of graphs is one of the few fields of mathematics with a definite birth date". Graph theory is considered to have begun in 1736 with the publication of Euler's solution of the Konigsberg Bridge problem. In 1936, Denes Konig wrote the first book on graph theory. The major developments of graph theory occurred by the ever growing importance of Computer Science and its connection with graph theory.

Now the question arises "what is a graph"? Consider the example. Suppose there are four sales persons Niraj, Sriram, Debasis, Anuj and five territories T_1, T_2, T_3, T_4, T_5. Niraj is interested to work in the territories T_1, T_2, T_3. Sriram is interested to work in the territories T_2, T_3. Debasis is interested to work in the territories T_1, T_4, T_5 where as Anuj is interested for the territories T_3, T_4, T_5. This is explained in the following figure. This is nothing but a graph, a concept which we are about to study extensively.



In this chapter, we will study the basic components of graph theory.

■ 10.1 GRAPH

A graph G consists of a finite set of vertices V and a finite set of edges E. Mathematically,

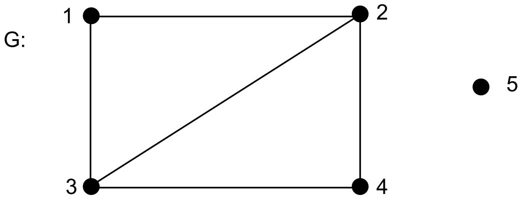
$$G = (V, E)$$

Where, $E = \{(v_i, v_j) \mid v_i, v_j \in V\}$

Let us consider $V = \{1, 2, 3, 4, 5\}$

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

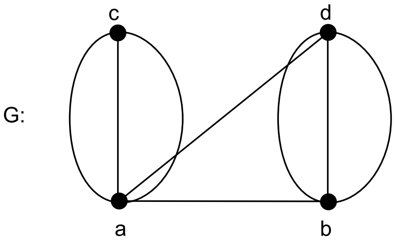
Hence the graph $G = (V, E)$ becomes



■ 10.1.1 Order and Size

The number of vertices in a graph G(V, E) is called its order, and the number of edges is its size. That is the order of G is |V| and its size |E|

Consider the following graph G



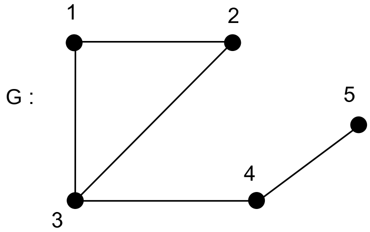
The order of G *i.e.* |V| = 4

The size of G *i.e.* |E| = 8

■ 10.1.2 Adjacent Vertices

Two vertices v_i and v_j are said to be adjacent if there exists an edge (v_i, v_j) in the graph G(V, E).

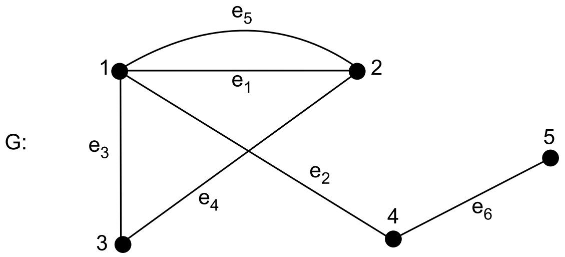
Consider the graph G as



Here the vertices 1 and 2 are adjacent. Similarly, the vertices 1 and 3 are also adjacent.

■ 10.1.3 Parallel edges

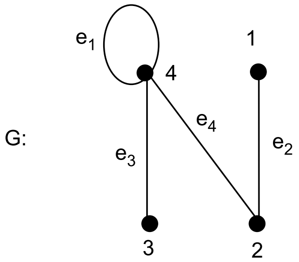
If there is more than one edge between the same pair of vertices, then the edges are termed as parallel edges. Consider the graph G as



Here the edges e_1 and e_5 are parallel edges.

■ 10.1.4 Loop

An edge whose starting and ending vertex are same is known as a loop. Mathematically $e = (v_i , v_i)$. Consider the graph G as



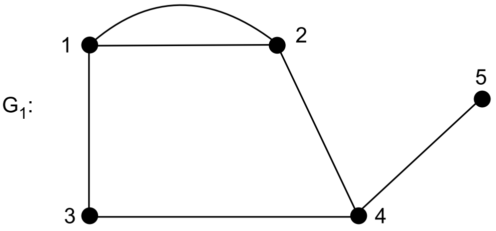
From the graph, it is clear that the edge e_1 is a loop.

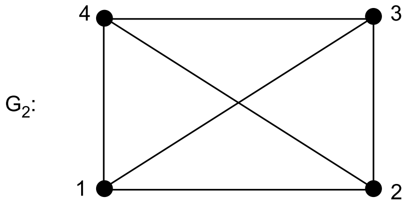
■ 10.2 KINDS OF GRAPH

In this section, we will discuss different kinds of graph.

■ 10.2.1 Simple Graph

A graph G(V, E) that has no self-loop or parallel edges is called a simple graph. Consider the graphs G_1 and G_2 as

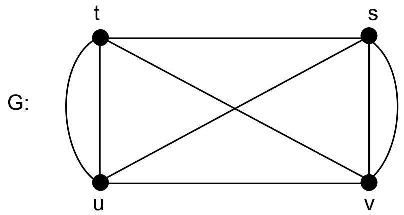




The graph G_1 is not a simple graph because there exists parallel edges between the vertices 1 and 2 whereas the graph G_2 is a simple graph.

■ 10.2.2 Multi Graph

A graph G(V, E) is known as a multi graph if it contains parallel edges, *i.e.* two or more edges between a pair of vertices. It is to be noted that every simple graph is a multi graph but the converse is not true. Consider the graph G as

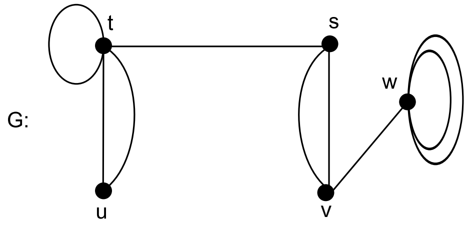


The above graph is a multi graph because there are parallel edges between the vertices u, t and v, s.

■ 10.2.3 Pseudo Graph

A graph G(V,E) is known as a pseudo graph if we allow both parallel edges and loops. It is to be noted that every simple graph and multi graph are pseudo graph but the converse is not true.

Consider the graph G as

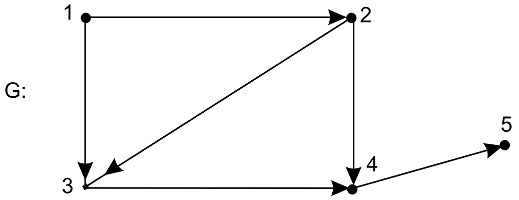


■ 10.3 DIGRAPH

A graph G(V, E) where V is the set of nodes or vertices and E is the set of edges having direction. If (v_i, v_j) is an edge, then there is an edge from the vertex v_i to the vertex v_j. A digraph is also called a directed graph. Let us consider

$$V = \{1, 2, 3, 4, 5\} \text{ and } E = \{(1, 2), (1, 3), (2, 3), (2, 4), (3, 4), (4, 5)\}$$

Hence, the digraph G becomes



■ 10.4 WEIGHTED GRAPH

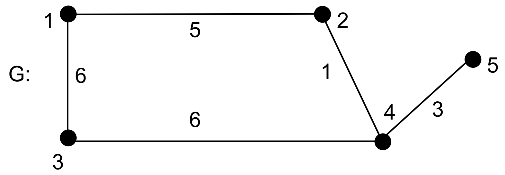
A graph (or digraph) is known as a weighted graph (or digraph) if each edge of the graph has some weights. Let us consider

$$V = \{1, 2, 3, 4, 5\} \text{ and } E = \{e_1, e_2, e_3, e_4, e_5\}$$

Where $e_1 = (1, 2), e_2 = (1, 3), e_3 = (2, 4), e_4 = (3, 4), e_5 = (4, 5)$

and $w(e_1) = 5, w(e_2) = 6, w(e_3) = 1, w(e_4) = 6, w(e_5) = 3$

Hence, the weighted graph G becomes



■ 10.5 DEGREE OF A VERTEX

The number of edges connected to the vertex 'v' is known as degree of vertex 'v', generally denoted by degree (v). In case of a digraph, there are two degrees *i.e.* indegree and outdegree.

The number of edges coming to the vertex 'v' is known as indegree of 'v' where as the number of edges emanating from the vertex 'v' is known as outdegree of 'v'. Generally, the indegree is denoted by indegree (v) and the outdegree is denoted by outdegree (v).

Note: In case of a loop, it contributes 2 to the degree of a vertex.

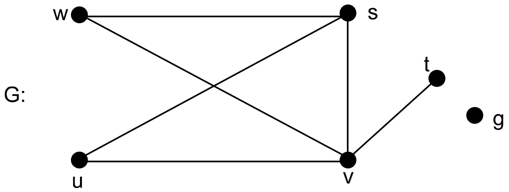
■ 10.5.1 Isolated Vertex

A vertex is said to be an isolated vertex if there is no edge connected from any other vertex to the vertex.

In other words a vertex is said to be an isolated vertex if the degree of that vertex is zero.

i.e. If degree (v) = 0, then v is isolated.

Consider the graph G as



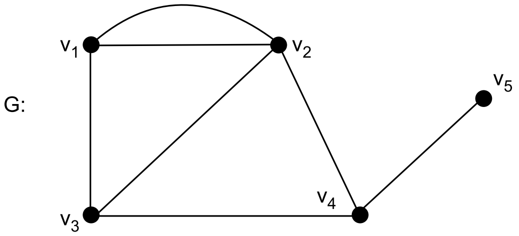
Now, degree (u) = 2; degree (v) = 4; degree (t) = 1
degree (g) = 0; degree (s) = 3; degree (w) = 2

Therefore, it is clear that 'g' is an isolated vertex.

■ 10.6 PATH

A path in a graph is a sequence $v_1, v_2, \ldots, v_k$ of vertices each adjacent to the next, and a choice of an edge between each 'v_i' to 'v_{i+1}' so that no edge is chosen more than once.

Consider the graph G as

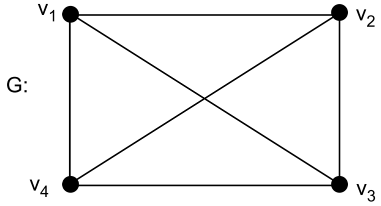


Here one path is $v_1\, v_2\, v_1\, v_3\, v_4\, v_5$.

■ 10.7 COMPLETE GRAPH

A graph (digraph) G is said to be complete if each vertex 'u' is adjacent to every other vertex 'v' in G.

In other words, there are edges from any vertex to all other vertices. Consider the graph G as



The above graph G is a complete graph.

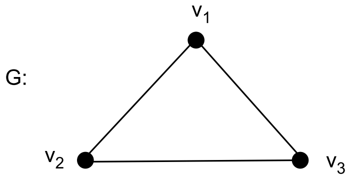
■ 10.8 REGULAR GRAPH

A graph G (V, E) is said to be regular if the degree of every vertex are equal. Mathematically, G is denoted as regular if

$$\text{degree }(v_i) = \text{degree }(v_j)\ \forall\ i, j.$$

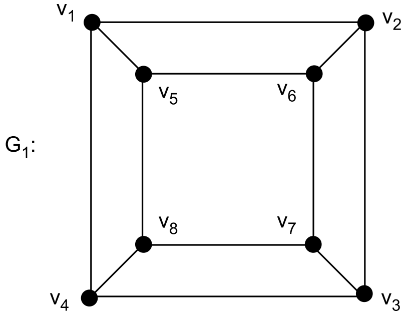
Where, $v_i, v_j \in$ G (V, E).

Consider the graph G as



In the above graph, degree (v_1) = degree (v_2) = degree (v_3) = 2. Therefore, the graph G is regular (2 regular). The above graph is also complete.

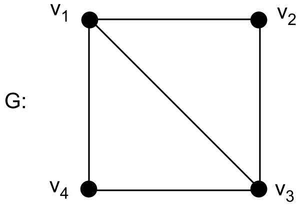
Consider another example G_1 as



Here the degree of every vertex is 3. So, the above graph is 3-regular but not complete.

■ 10.9 CYCLE

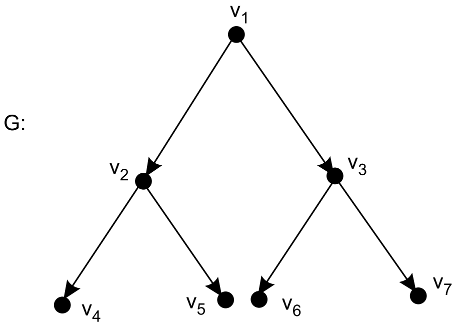
If there is a path containing one or more edges which starts from a vertex 'v' and terminates into the same vertex, then the path is known as a cycle. Consider the graph G as



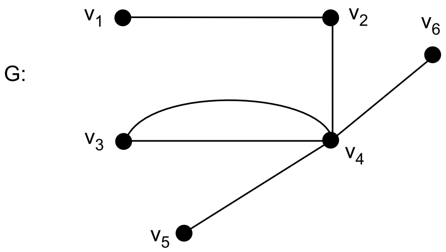
In the above graph G, one cycle is $v_1v_2\, v_3\, v_1$. Similarly, another cycle is $v_1\, v_2\, v_3\, v_4\, v_1$.

■ 10.10 PENDANT VERTEX

A vertex 'v' in a graph G is said to be a pendant vertex if the degree (v) =1. In case of a digraph, a vertex 'v' is said to be a pendant vertex if the indegree (v) = 1 and outdegree (v) = 0. In the graph 'G(figure 1)' given below, indegree of the vertices v_4 , v_5 , v_6 and v_7 is equal to 1 and the outdegree is equal to 0. Therefore, these vertices are pendant vertices. Similarly, in the graph 'G(figure 2) given below the vertices v_1, v_5 and v_6 are pendent vertices.



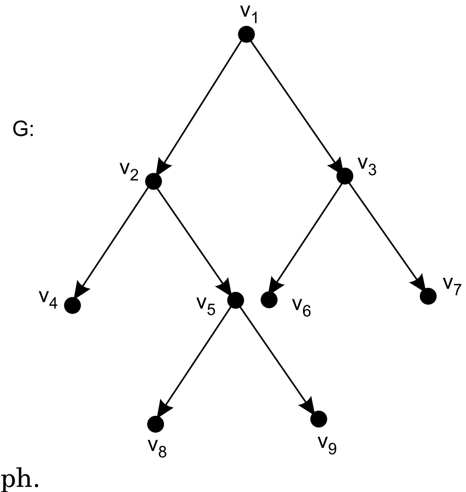
(Figure 1)



(Figure 2)

■ 10.11 ACYCLIC GRAPH

A graph (digraph) which does not have any cycle is known as an acyclic graph (digraph). Consider the graph G as



Here, G is an acyclic graph.

■ 10.12 MATRIX REPRESENTATION OF GRAPHS

A matrix is a convenient way to represent a graph. A computer to analyze them can use such a representation.

■ 10.12.1 Adjacency Matrix

The most useful way of representing any graph is the matrix representation. It is a square matrix of order $(n \times n)$ where n is the number of vertices in the graph G. Generally denoted by A $[a_{ij}]$ where a_{ij} is the ith row and jth column element. The general form of adjacency matrix is given as below.

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} & . \; . \; . & a_{1n} \\ a_{21} & a_{22} & a_{23} & . \; . \; . & a_{2n} \\ a_{31} & a_{32} & a_{33} & . \; . \; . & a_{3n} \\ . & . & . & . \; . \; . & . \\ . & . & . & . \; . \; . & . \\ . & . & . & . \; . \; . & . \\ a_{n1} & a_{n2} & a_{n3} & . \; . \; . & a_{nn} \end{bmatrix}$$

where, $$a_{ij} = \begin{cases} 1; & \text{if there is an edge from '}v_i\text{' to '}v_j\text{'} \\ 0; & \text{Otherwise} \end{cases}$$

This matrix is termed as adjacency matrix, because an entry stores the information whether two vertices are adjacent or not. This is also known as bit matrix or Boolean matrix as each entry is either 1 or 0.

Note 1. In the adjacency matrix if the main diagonal elements are zero, then the graph is said to be a simple graph.

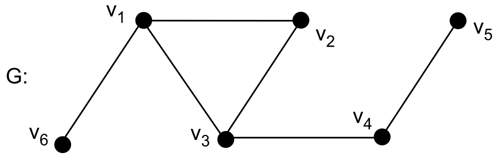
2. In case of a multi graph the adjacency matrix can be found out with the relation.

$$a_{ij} = \begin{cases} n; & n \text{ be the number of edges from '}v_i\text{' to '}v_j\text{'} \\ 0; & \text{Otherwise} \end{cases}$$

3. In case of a weighted graph the adjacency matrix can be found out with the relation

$$a_{ij} = \begin{cases} n; & w \text{ is the weight of the edges from '}v_i\text{' to '}v_j\text{'} \\ 0; & \text{Otherwise} \end{cases}$$

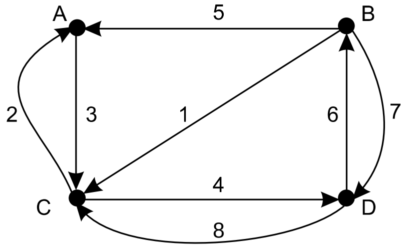
Consider the graph G as



Hence, the adjacency matrix is given as

$$A = \begin{array}{c|cccccc|} & v_1 & v_2 & v_3 & v_4 & v_5 & v_6 \\ \hline v_1 & 0 & 1 & 1 & 0 & 0 & 1 \\ v_2 & 1 & 0 & 1 & 0 & 0 & 0 \\ v_3 & 1 & 1 & 0 & 1 & 0 & 0 \\ v_4 & 0 & 0 & 1 & 0 & 1 & 0 \\ v_5 & 0 & 0 & 0 & 1 & 0 & 0 \\ v_6 & 1 & 0 & 0 & 0 & 0 & 0 \end{array}$$

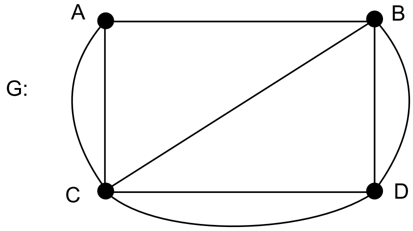
Consider the graph G as



The adjacency matrix of the above graph with respect to the ordering A, B, C and D is given below.

$$A = \begin{bmatrix} 0 & 0 & 3 & 0 \\ 5 & 0 & 1 & 7 \\ 2 & 0 & 0 & 4 \\ 0 & 6 & 8 & 0 \end{bmatrix}$$

Consider the graph G as



The adjacency matrix of the above graph with respect to the ordering A, B, C and D is given below.

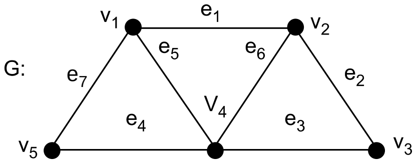
$$A = \begin{bmatrix} 0 & 1 & 2 & 0 \\ 1 & 0 & 1 & 2 \\ 2 & 1 & 0 & 2 \\ 0 & 2 & 2 & 0 \end{bmatrix}$$

■ 10.12.2 Incidence Matrix

Suppose that G be a simple undirected graph with m vertices and n edges, then the incidence matrix is a matrix of order $(m \times n)$ where the element a_{ij} is defined as

$$a_{ij} = \begin{cases} 1; & \text{If vertex } i \text{ belongs to edges } j. \\ 0; & \text{Otherwise} \end{cases}$$

Consider the graph G as



Hence, the incidence matrix of the graph G is of order (5 × 7). The incidence matrix relative to the ordering v_1, v_2, v_3, v_4, v_5 and e_1, e_2, e_3, e_4, e_5, e_6, e_7 is given as below.

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

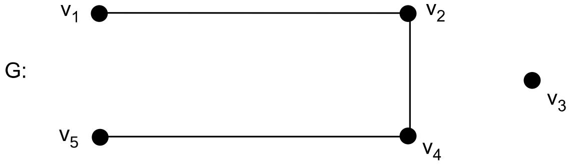
■ 10.12.3 Path Matrix

Suppose that G be simple graph with n-vertices. Then the $(n \times n)$ matrix P = $[P_{ij}](n \times n)$ defined by

$$P_{ij} = \begin{cases} 1; & \text{if there is a path from } v_i \text{ to } v_j \\ 0; & \text{Otherwise} \end{cases}$$

is known as the path matrix or reachability matrix.

Consider the graph G as



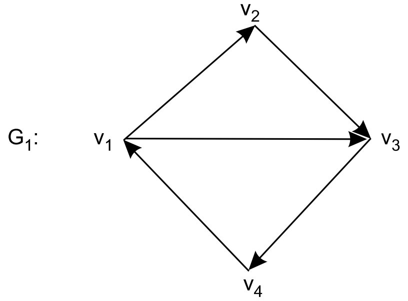
Therefore, the path matrix of the above graph relative to the ordering v_1, v_2, v_3 , v_4 , v_5 is given as

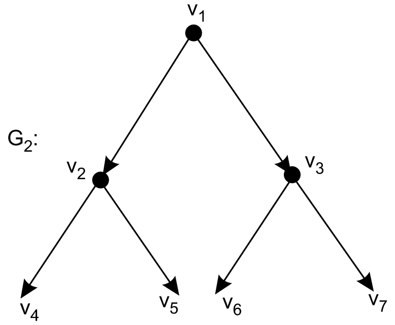
$$P = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \end{bmatrix}$$

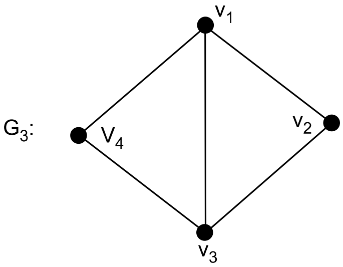
■ 10.13 CONNECTED GRAPH

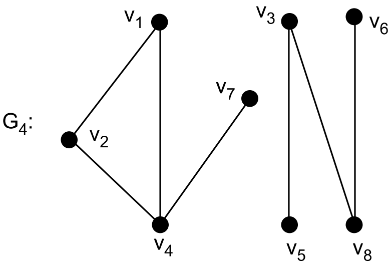
A graph (not digraph) G (V, E) is said to be connected if for every pair of distinct vertices 'u' and 'v' in G, there is a path. A directed graph is said to be strongly connected if for every pair of distinct vertices 'u' and 'v' in G, there is a directed path from 'u' to 'v' and also from 'v' to 'u'. A directed graph is said to be weakly connected if for every pair of distinct vertices, there is a path without taking the direction.

Consider the following graphs









From the above graphs, it is clear that

G_1 : Strongly Connected; G_2: Weakly Connected

G_3 : Connected; G_4: Disconnected

■ 10.13.1 Theorem

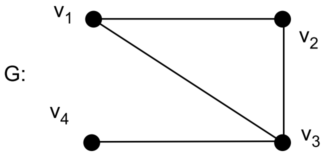
Suppose that G be a graph with n-vertices $v_1, v_2, ..., v_n$ and let A be the adjacency matrix of G. Let us define $B = [b_{ij}]$ such that

$$B = A + A^2 + A^3 + ... + A^{n-1}.$$

If for every pair of distinct indices i and j, $b_{ij} \neq 0$, then the graph is said to be connected.

The proof of the above theorem is beyond the scope of this book.

Consider the graph G as



Hence, the adjacency matrix A is given as

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

Here, number of vertices (n) = 4. Therefore, $B = A + A^2 + A^3$

Now, $$A^2 = \begin{pmatrix} 2 & 1 & 1 & 1 \\ 1 & 2 & 1 & 1 \\ 1 & 1 & 3 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix}; A^3 = A^2\,A = \begin{pmatrix} 2 & 3 & 4 & 1 \\ 3 & 2 & 4 & 1 \\ 4 & 4 & 2 & 3 \\ 1 & 1 & 3 & 0 \end{pmatrix}$$

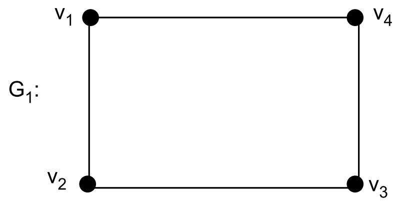
Therefore, $$B = A + A^2 + A^3 = \begin{pmatrix} 4 & 5 & 6 & 2 \\ 5 & 4 & 6 & 2 \\ 6 & 6 & 5 & 4 \\ 2 & 2 & 4 & 1 \end{pmatrix}$$

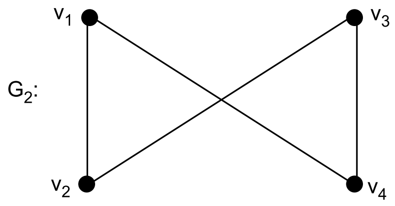
Since, all $b_{ij} \neq 0$ for $i \neq j$; the graph G is connected. All elements except the diagonal elements must not be zero for connected graph.

■ 10.14 GRAPH ISOMORPHISM

Suppose $G_1 : (V_1, E_1)$ and $G_2 : (V_2, E_2)$ be two graphs. Then the two graphs G_1 and G_2 are said to be isomorphic if there is one to one correspondence between the edges E_1 of G_1 and E_2 of G_2 which indicates that if $(u_1, v_1) \in G_1$ then $(u_1, v_1) \in G_2$.

Such a pair of correspondence is known as graph isomorphism. The different way of representing the same graph is known as graph isomorphism. Consider graph G_1 and G_2 as



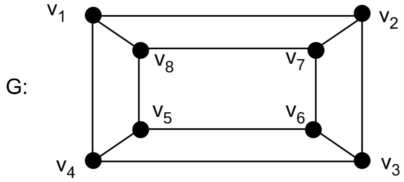


Therefore, the graphs G_1 and G_2 are isomorphic to each other.

■ 10.15 BIPARTITE GRAPH

Suppose that G: (V, E) be the graph. If the vertex set V can be partitioned into two non empty disjoint sets V_1 and V_2 such that each edge of the graph G has one end in V_1 and other end in V_2, then the graph is said to be bipartite graph.

Consider the graph G as



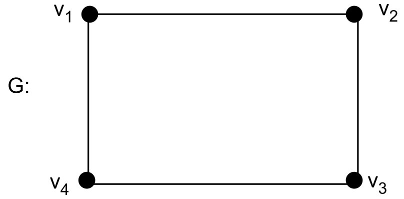
Let $V_1 = \{v_1, v_3 , v_5 , v_7\}$ and $V_2 = \{v_4, v_2, v_6, v_8\}$

Now, $(V_1 \cap V_2) = \phi$ and each edge of G has one vertex in V_1 and other vertex at V_2 . So, G is said to be a bipartite graph.

■ 10.15.1 Complete Bipartite Graph

Suppose that G: (V, E) be the graph. If the vertex set $V = (V_1 \cup V_2)$ and $V_1, V_2 \neq \phi$, $(V_1 \cap V_2) = \phi$, such that each edge of the graph G has one end in V_1 and other end in V_2 , then the graph G is termed as bipartite.

If every vertex of V_1 is joined to every vertex of V_2, then the graph G is termed as complete bipartite graph. Consider the graph G as



Let $V_1 = \{v_1, v_3\}$ and $V_2 =\{v_2, v_4\}$.

Therefore, $V = (V_1 \cup V_2)$; $V_1, V_2 \neq \phi$, and $(V_1 \cap V_2) = \phi$.

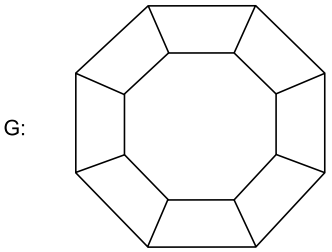
Also, every vertex of V_1 is joined to every vertex of V_2. So, G is a complete bipartite graph.

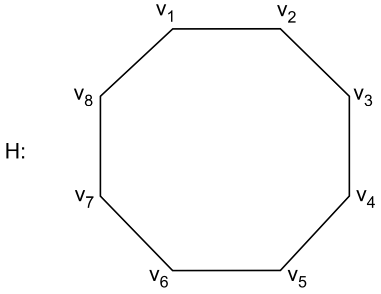
■ 10.16 SUBGRAPH

Suppose that G and H be two graphs with vertex sets V(G) and V(H). Let the edge sets be E(G) and E(H). Now H is said to be subgraph of G if

$$V(H) \subseteq V(G) \text{ and } E(H) \subseteq E(G)$$

Consider two graphs G and H as

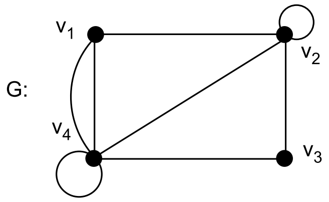




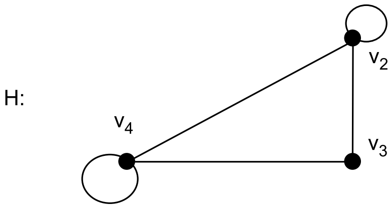
Therefore, it is clear that $V(H) \subseteq V(G)$ and $E(H) \subseteq E(G)$. So, H is a subgraph of G.

■ 10.16.1 Vertex Deleted Subgraph

Suppose that G(V, E) be a graph. If we delete a subset U of the set V and all the edges, which have a vertex in U as an end, then the resultant graph is termed as vertex deleted subgraph of G. Consider the graph G as

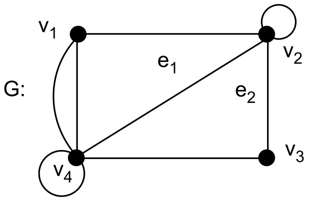


On deleting the vertex v_1, the vertex deleted subgraph H is given as

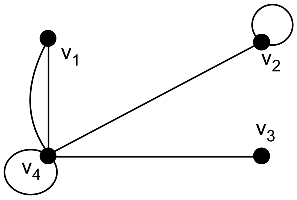


■ 10.16.2 Edge Deleted Subgraph

Suppose that G: (V, E) be a graph. If a subset F from the set of edges E is deleted from the graph G, then the resultant graph is edge deleted subgraph of G. Consider the graph G as



On deleting the edges e_1 and e_2, the edge deleted subgraph is given as



■ 10.17 WALKS

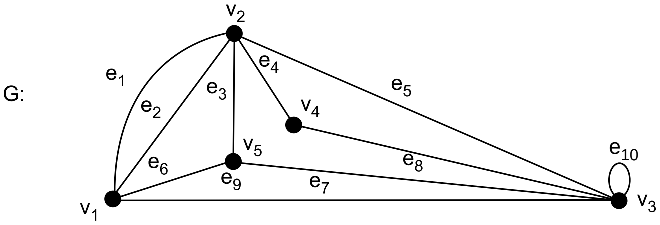
Let G be a graph, then a walk W in a graph G is a finite sequence W = $v_0\, e_1\, v_1 e_2\, v_2\, e_3$ .... $v_{i-1}\, e_i\, v_i$ ...... $v_{k-1}\, e_k\, v_k$. Whose terms are alternately vertices and edges such that for $1 \leq i \leq k$, the edge e_i has ends v_{i-1} and v_1 . The starting vertex v_o is the origin and the end vertex v_k is the terminus of the walk W. The vertices v_1, v_2, ... v_{k-1} are known as internal vertices. The walk is termed as $v_o - v_k$ walk.

The number of edges present in the walk W is known as the length of walk W. Note that in a walk W there may be repetition of vertices and edges. In a simple graph, a walk W = $v_0e_1\ v_1e_2$............. e_kv_k is determined by a sequence of vertices $v_0\ v_1\ v_2$ .... $v_{k-1}v_k$ because each pair of vertices $v_{i-1}\ v_i$ has one edge only. Even if a graph is not simple, a walk is often simply denoted by a sequence of vertices $v_0\ v_1\ v_2$ ...... $v_{k-1}v_k$ where the consecutive vertices are adjacent.

Note : 1. A walk containing no edges is known as a trivial walk.

2. A walk containing no repeated edges is termed as a trail.
3. A walk containing no repeated vertices is termed as a path. Which indicates that if the sequence of vertices $v_0\ v_1\ v_2$ ...... $v_{k-1}v_k$ of the walk W = $v_0\ e_1v_1\ e_2\ v_2$ .... $v_{k-1}\ e_k\ v_k$ are distinct, then the walk is a path.
4. Every path is a trail but the converse is not true always.

Consider the graph G as



Consider the following walks

$$W_1 = v_1e_1\ v_2e_2\ v_1e_6\ v_5e_7\ v_3e_{10}\ v_3e_8\ v_4$$

$$W_2 = v_1e_1\ v_2e_1\ v_1e_1\ v_2e_2\ v_1e_1\ v_2$$

$$W_3 = v_3e_{10}\ v_3e_9\ v_1e_1\ v_2e_2\ v_1$$

$$W_4 = v_1e_2\ v_2e_5\ v_3e_7\ v_5$$

The length of W_1 is 6. Similarly, the length of other walks can be found out. Here W_1 and W_2 are walks; W_3 is trail and W_4 is a path.

■ 10.17.1 Open and Closed Walk

Suppose that u and v be two vertices of a graph. An $u - v$ walk is said to be open or closed according to $u \neq v$ or $u = v$ respectively. In other words a walk is closed if the starting vertex (u) and the terminus (v) are same otherwise it is open.

■ 10.18 OPERATIONS ON GRAPHS

In this section we will discuss the different operations on graphs.

■10.18.1 Union

If G_1 and G_2 be two graphs, then their union ($G_1 \cup G_2$) is a graph with V ($G_1 \cup G_2$) = V (G_1) ∪ V (G_2) and E ($G_1 \cup G_2$) = E (G_1) ∪ E (G_2).

■ 10.18.2 Intersection

If G_1 and G_2 be two graphs with at least one vertex in common, then their intersection ($G_1 \cap G_2$) is a graph with

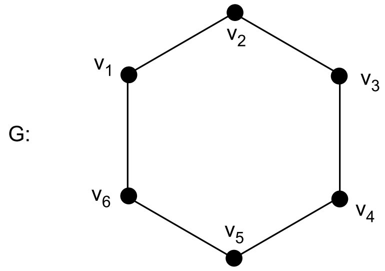
$$V(G_1 \cap G_2) = V(G_1) \cap V(G_2)$$

and

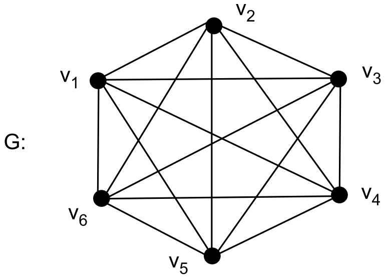
$$E(G_1 \cap G_2) = E(G_1) \cap E(G_2)$$

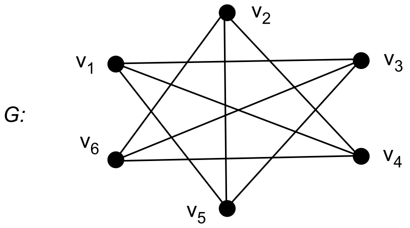
■ 10.18.3 Complement

Suppose that G be a simple graph with n-vertices. Then the complement of G is given by $\overline{G}$ and is defined to be the simple graph with the same vertices of G and where two vertices (u, v) are adjacent in $\overline{G}$, if u and v are not adjacent in G. In other words the complement of G can be obtained from the complete graph K_n by deleting all the edges of G. Consider the graph G as



To obtain the complement of G construct the complete graph with the same vertices and then delete the edges of the graph G. The complement graph of G *i.e.* $\overline{G}$ is given below.





■ 10.18.4 Product of Graphs

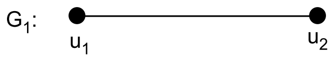
Suppose that G_1: (V_1, E_1) and G_2: (V_2, E_2) be two graphs. Then the product of graphs G_1 and G_2 is given as $(G_1 \times G_2)$ and is defined as $(G_1 \times G_2)$: (V, E). Where $V = (V_1 \times V_2)$ and the edge set E can be found out from the following relation.

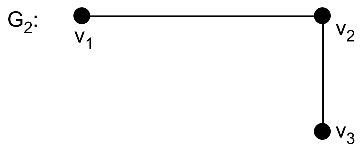
If (u_1, u_2) and (v_1, v_2) be two vertices of $(G_1 \times G_2)$, Then there is an edge between them if

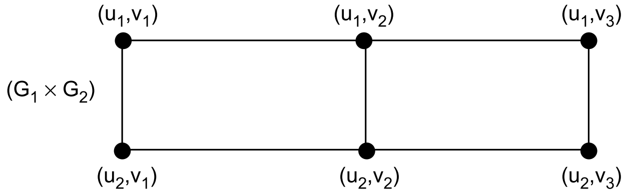
(*i*) ($u_1 = v_1$ and u_2 is adjacent to v_2) or

(*ii*) (u_1 is adjacent to v_1 and $u_2 = v_2$).

Consider the graphs G_1 and G_2 as







■ 10.18.5 Composition

Suppose that G_1: (V_1, E_1) and G_2: (V_2, E_2) be two graphs. Then the composition of $G_1[G_2]$ and is defined as

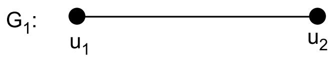
$$G_1[G_2] : (V, E)$$

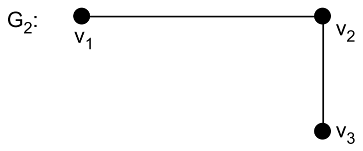
Where, $V = (V_1 \times V_2)$ and the edge set E can be found out from the following relation. If (u_1, u_2) and (v_1, v_2) be two vertices of $G_1[G_2]$, then there is an edge between them if

(*i*) u_1 is adjacent to v_1 or

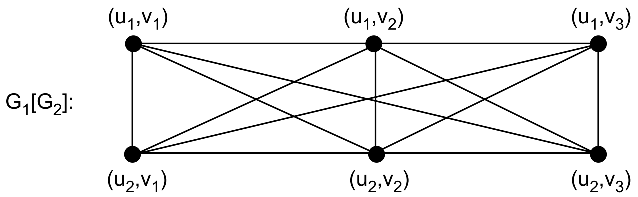
(*ii*) ($u_1 = v_1$ and u_2 is adjacent to v_2)

Consider the graphs G_1 and G_2 as





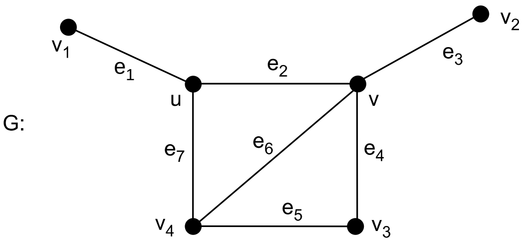
The composition $G_1[G_2]$ is defined as



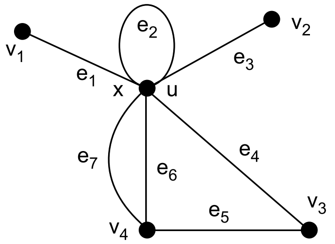
■ 10.19 FUSION OF GRAPHS

Let u and v be distinct vertices of a graph G, we can construct a new graph G_1 by fusing the two vertices. This means by replacing them by a single new vertex 'x' such that every edge that was incident with either 'u' or 'v' is now incident with x.

Consider the graph G as



On fusing the vertices '*u*' and '*v*' the graph becomes



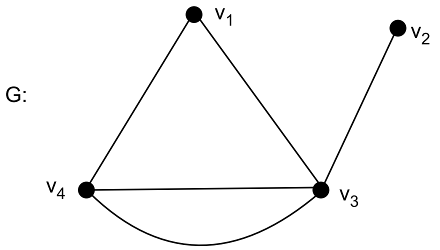
■ 10.19.1 Adjacency Matrix (After fusion of two adjacent vertices)

The following steps are used to find the new adjacency matrix after fusion of two adjacent vertices '*u*' and '*v*'.

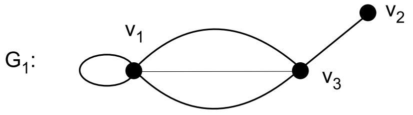
Step 1. Replace the *u*th row by the sum of *u*th row and *v*th row. Similarly, replace the *u*th column by the sum of *u*th column and *v*th column.

Step 2. Delete the row and column corresponding to the vertex *v*. The resulting matrix is the new adjacency matrix.

Consider the graph G as



After fusing v_1 and v_4 we have the new graph G_1 as



Relative to the ordering v_1, v_2, v_3 and v_4 we have $A(G) = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 2 \\ 1 & 0 & 2 & 0 \end{pmatrix}$

Now on replacing Row $(v_1) \leftarrow$ Row (v_1) + Row (v_4) and Col $(v_1) \leftarrow$ Col (v_1) + Col (v_4) we get

$$A(G) = \begin{pmatrix} 1 & 0 & 3 & 1 \\ 0 & 0 & 1 & 0 \\ 3 & 1 & 0 & 2 \\ 1 & 0 & 2 & 0 \end{pmatrix}$$

On deleting the row and column corresponding to v_4 the adjacency matrix of G_1 is given as

$$A(G_1) = \begin{pmatrix} 1 & 0 & 3 \\ 0 & 0 & 1 \\ 3 & 1 & 0 \end{pmatrix}$$

■ 10.19.2 Fusion Algorithm (Connectedness)

The following steps are used to check the connectedness of a graph G.

Step 1. Replace the graph G by its underlying simple graph. The adjacency matrix can be obtained by replacing all non zero entries off the diagonal by 1 and all entries on the diagonal by 0.

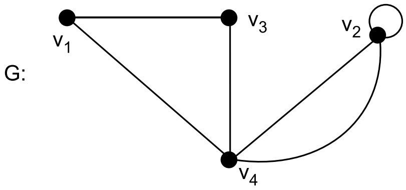
Step 2. Fuse vertex v_1 to the first of the vertices v_2, v_3 ...., v_n with which it is adjacent to give a new graph. Denote it by G in which the new vertex is also denoted by v_1.

Step 3. Carry out step1 on the new graph G.

Step 4. Carry out step 2 to step 3 repeatedly with v_1 until v_1 is not adjacent to any of the other vertices.

Step 5. Carry out steps 2 to 4 on the vertex v_2 of the latest graph and than on all the remaining vertices of the resulting graphs in turn. The final graph is empty and the number of its isolated vertices is the number of connected components of the initial graph G.

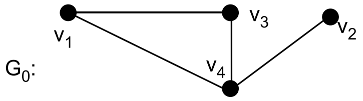
Consider the following graph G.



The adjacency matrix A (G) relative to the ordering v_1, v_2, v_3 and v_4 becomes

$$A(G) = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 2 \\ 1 & 0 & 0 & 1 \\ 1 & 2 & 1 & 0 \end{pmatrix}$$

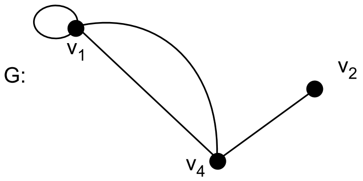
The underlying simple graph of G is given as



The adjacency matrix becomes

$$A(G_0) = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

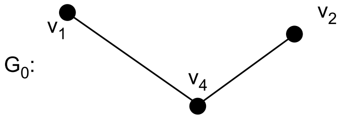
On fusing v_1 with v_3 we have the graph G as



Therefore, on replacing Row $(v_1) \leftarrow$ Row (v_1) + Row (v_3); Col $(v_1) \leftarrow$ Col. (v_1) + Col. (v_3) and on removing the row and column corresponding to v_3 the adjacency matrix relative to the ordering v_1, v_2 and v_4 becomes

$$A(G) = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 0 & 1 \\ 2 & 1 & 0 \end{pmatrix}$$

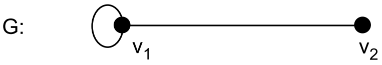
The underlying simple graph of G is given as



The adjacency matrix becomes

$$A(G_0) = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

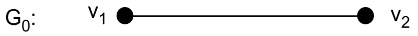
On fusing v_1 with v_4 we have the graph G as



Therefore, on replacing Row $(v_1) \leftarrow$ Row (v_1) + Row (v_4); Col $(v_1) \leftarrow$ Col (v_1) + Col. (v_4) and on removing the row and column corresponding to v_4, the adjacency matrix relative to the ordering v_1 and v_2 becomes

$$A(G) = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

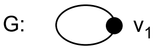
The underlying spanning graph of G is given as



The adjacency matrix becomes

$$A(G_0) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

On fusing v_1 with v_2 we have the graph G as



Therefore, on replacing Row $(v_1) \leftarrow$ Row (v_1) + Row (v_2); Col $(v_1) \leftarrow$ Col (v_1) + Col (v_2) and on removing the row and column corresponding to v_2, the adjacency matrix relative to v_1 becomes

$$A(G) = (1)$$

The underlying spanning graph of G is given as

The adjacency matrix becomes

$$A(G_0) = (0)$$

As the final graph is empty, the process terminates. Here the number of isolated point is one. So, the graph is said to be connected.

SOLVED EXAMPLES

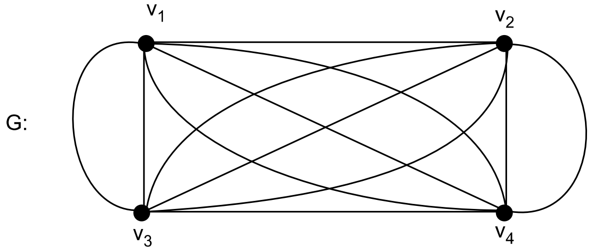
Example 1 *Draw the graph having the following matrix as its adjacency matrix*

$$\begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{pmatrix}$$

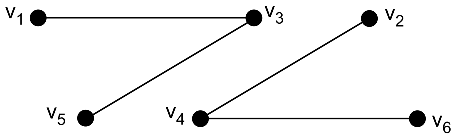
Solution : Given that the adjacency matrix is

$$\begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{pmatrix}$$

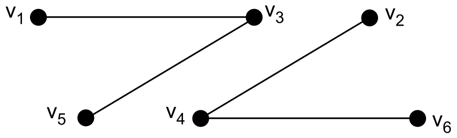
The order of the adjacency matrix is (4×4). So, the graph G has four vertices, say v_1, v_2, v_3 and v_4 . Relative to the ordering v_1, v_2, v_3 and v_4 the graph G is given below.



Example 2 *Write down the path matrix of the following graph.*



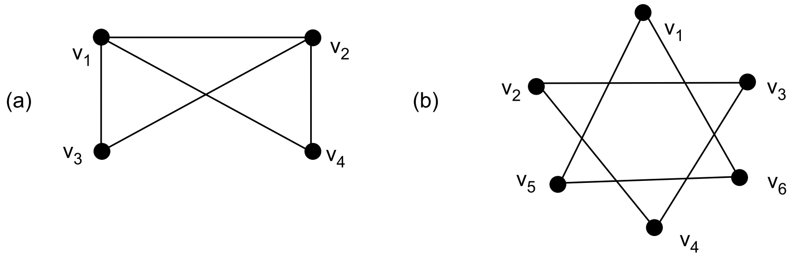
Solution : Given that the graph is



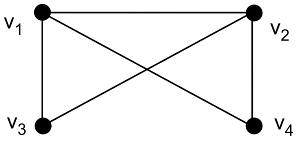
The path matrix relative to the ordering v_1, v_2, v_3, v_4, v_5 and v_6 is given as

$$P(G) = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \end{pmatrix}$$

Example 3 *Write the adjacency matrix of the following graphs*



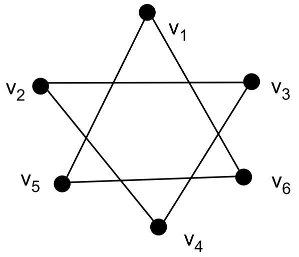
Solution : (a) Given graph is



The adjacency matrix relative to the ordering v_1, v_2, v_3 and v_4 is given as

$$A(G) = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}$$

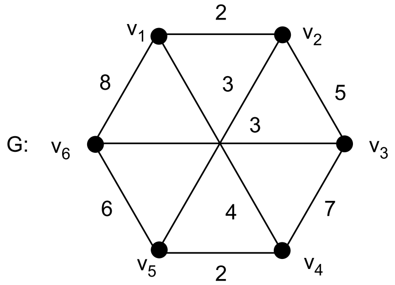
(*b*) Given graph is



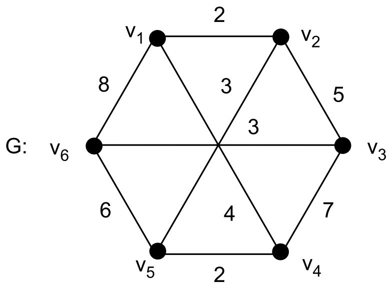
The adjacency matrix relative to the ordering v_1, v_2, v_3, v_4, v_5 and v_6 is given as

$$A(G) = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Example 4 *Write the adjacency matrix of the following weighted graph.*



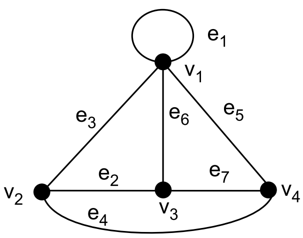
Solution : The weighted graph is



The adjacency matrix relative to the ordering v_1, v_2, v_3, v_4, v_5 and v_6 is given as

$$A(G) = \begin{pmatrix} 0 & 2 & 0 & 4 & 0 & 8 \\ 2 & 0 & 5 & 0 & 3 & 0 \\ 0 & 5 & 0 & 7 & 0 & 3 \\ 4 & 0 & 7 & 0 & 2 & 0 \\ 0 & 3 & 0 & 2 & 0 & 6 \\ 8 & 0 & 3 & 0 & 6 & 0 \end{pmatrix}$$

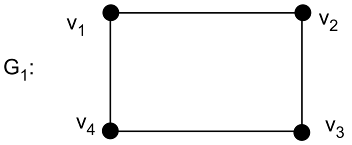
Example 5 *Write down the incidence matrix of the following graph G.*

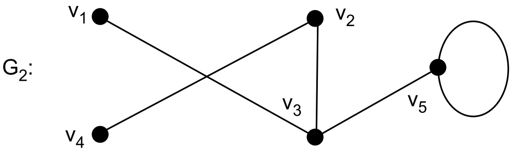


Solution : In the above graph G V = $\{v_1, v_2, v_3, v_4\}$ and E = $\{e_1, e_2, e_3, e_4, e_5, e_6, e_7\}$. Therefore the order of incidence matrix is (4 × 7). Relative to the ordering of V and E, the incidence matrix is given as

$$I(G) = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

Example 6 *Find the union of the following graphs.*





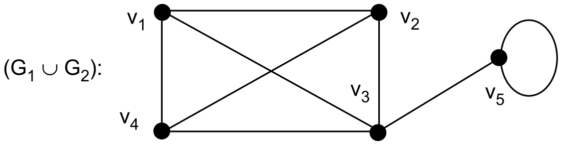
Solution : Here, $V(G_1) = \{v_1, v_2, v_3, v_4\}$

and $V(G_2) = \{v_1, v_2, v_3, v_4, v_5\}$.

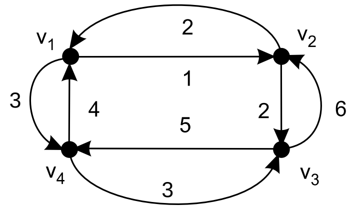
Therefore, $V(G_1 \cup G_2) = \{v_1, v_2, v_3, v_4, v_5\}$.

Similarly, $E(G_1 \cup G_2) = \{(v_1, v_2), (v_2, v_3), (v_3, v_4), (v_4, v_1), (v_1, v_3), (v_2, v_4), (v_3, v_5), (v_5, v_5)\}$.

Therefore, the graph $(G_1 \cup G_2)$ becomes



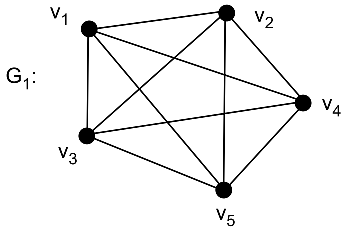
Example 7 *Write the adjacency matrix of the following directed weighted graph*

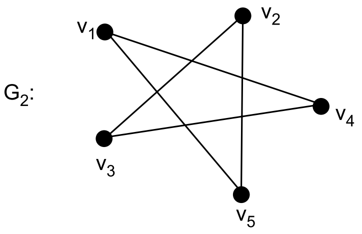


Solution : In the above directed weighted graph the total number of vertices are 4. So, the adjacency matrix is of order (4 × 4). The adjacency matrix relative to the ordering v_1, v_2, v_3 and v_4 is given as below.

$$A(G) = \begin{pmatrix} 0 & 1 & 0 & 3 \\ 2 & 0 & 2 & 0 \\ 0 & 6 & 0 & 5 \\ 4 & 0 & 3 & 0 \end{pmatrix}$$

Example 8 *Find the intersection of the following graphs.*





Solution Here, $V(G_1) = \{v_1, v_2, v_3, v_4, v_5\}$

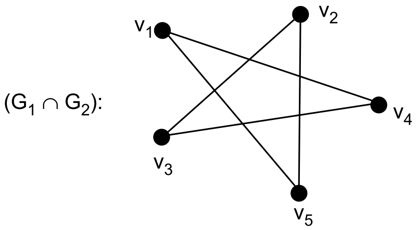
and $V(G_2) = \{v_1, v_2, v_3, v_4, v_5\}$.

Therefore, $V(G_1 \cap G_2) = \{v_1, v_2, v_3, v_4, v_5\}$.

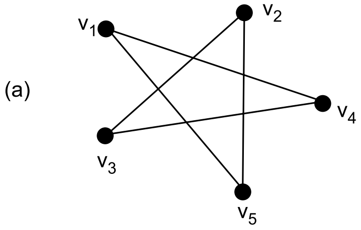
Similarly, $E(G_1 \cap G_2)$

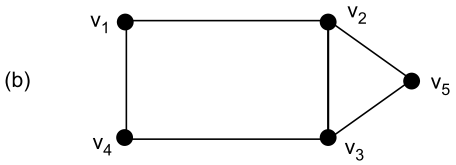
$$= \{(v_1, v_4), (v_4, v_3), (v_3, v_2), (v_2, v_5), (v_5, v_1)\}.$$

Therefore, the graph $(G_1 \cap G_2)$ becomes

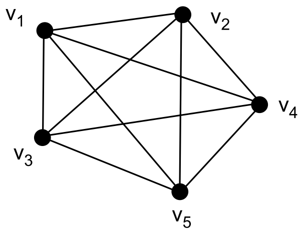


Example 9 *Find the complement of the following graphs.*

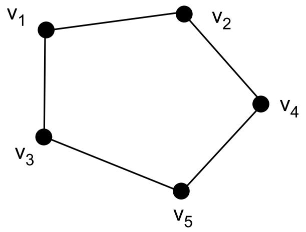




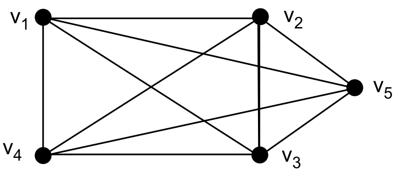
Solution (*a*) To obtain the complement of G, find the complete graph with the same vertices. This is given below.



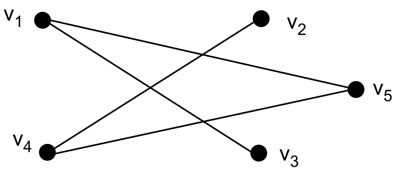
On deleting the edges of G, the complement $\overline{G}$ of G is given below.



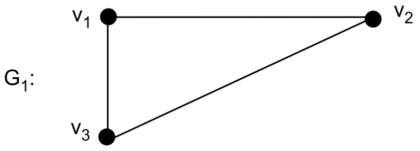
(*b*) To obtain the complement of G, find the complete graph with the same vertices. This is given below.

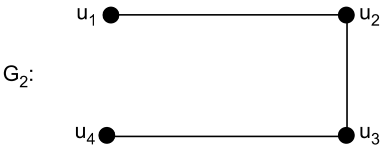


On deleting the edges of G, the complement $\overline{G}$ of G is given below.



Example 10 *If G_1 and G_2 be two graphs given below, then find the product of graphs ($G_1 \times G_2$). Where*

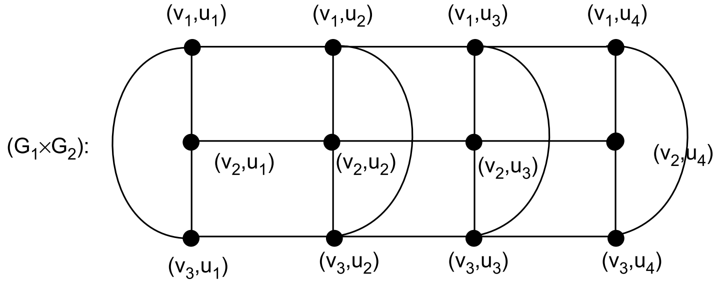




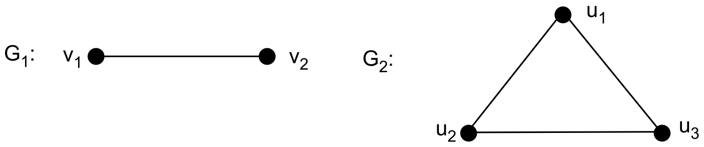
Solution : Here $V(G_1) = \{v_1, v_2, v_3\}$

and $V(G_2) = \{u_1, u_2, u_3, u_4\}$.

Therefore, $V(G_1 \times G_2) = \{(v_1, u_1), (v_1, u_2), (v_1, u_3), (v_1, u_4), (v_2, u_1), (v_2, u_2), (v_2, u_3), (v_2, u_4), (v_3, u_1), (v_3, u_2), (v_3, u_3), (v_3, u_4)\}$



Example 11 *Given G_1 and G_2 be two graphs. Find the composition $G_1[G_2]$ where*

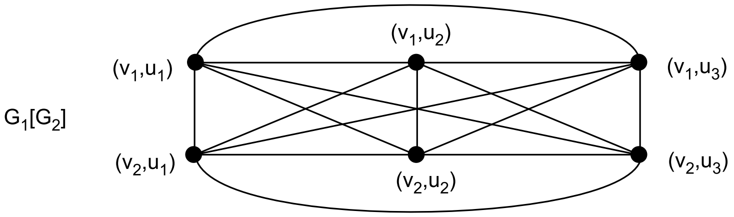


Solution : In the above graph

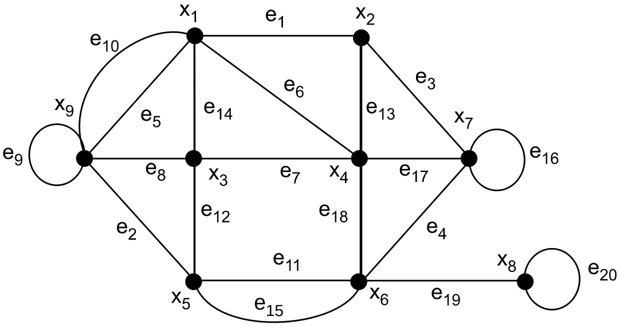
$$V(G_1) = \{v_1, v_2\}$$

and $$V(G_2) = \{u_1, u_2, u_3\}.$$

Therefore, the vertex set of $G_1[G_2]$ is $\{(v_1, u_1), (v_1, u_2), (v_1, u_3), (v_2, u_1), (v_2, u_2), (v_2, u_3)\}$. Thus the composition graph $G_1[G_2]$ is given below.



Example 12 *Let G be the graph given below.*



(*a*) *Find G – U; where* $U = \{x_1, x_3, x_5, x_7\}$

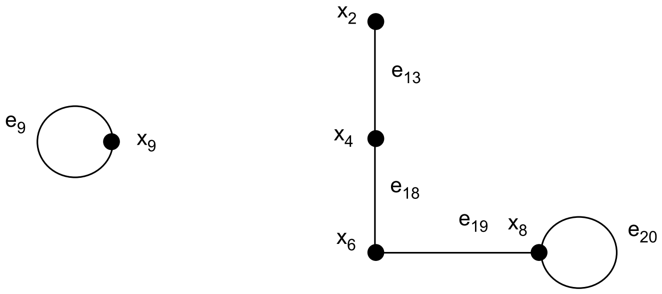
(b) Find G(U); where $U = \{x_1, x_3, x_4, x_9\}$

(c) Find G – V; where $V = \{e_2, e_5, e_8, e_{12}, e_{14}, e_1, e_6, e_{18}, e_4, e_{19}, e_{20}\}$

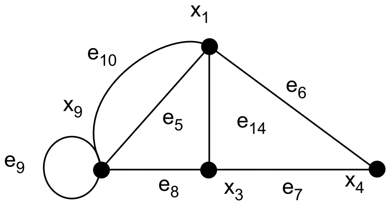
(d) Find G(V); where $V = \{e_1, e_6, e_7, e_{11}, e_{15}\}$

Solution (*a*) Given $U = \{x_1, x_3, x_5, x_7\}$.

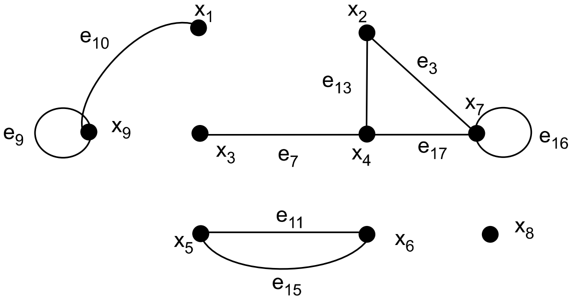
Therefore, G – U becomes



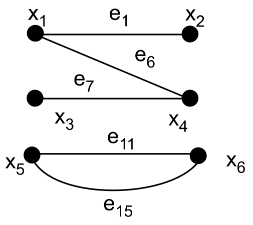
(*b*) Given $U = \{x_1, x_3, x_4, x_9\}$. Therefore, G(U) becomes



(*c*) Given $V = \{e_2, e_5, e_8, e_{12}, e_{14}, e_1, e_6, e_{18}, e_4, e_{19}, e_{20}\}$. Therefore, G – V becomes



(*d*) Given $V = \{e_1, e_6, e_7, e_{11}, e_{15}\}$. Therefore, G(V) becomes



Example 13 *Determine whether the graph given below by its adjacency matrix is connected or not.*

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

Solution : The adjacency matrix A is given as

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

Here, the number of vertices (n) = 4. Let $B = A + A^2 + A^3$

Now, $$A^2 = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 3 & 1 & 2 & 1 \\ 1 & 2 & 1 & 2 \\ 2 & 1 & 3 & 1 \\ 1 & 2 & 1 & 2 \end{pmatrix}$$

Again, $$A^3 = A^2A = \begin{pmatrix} 3 & 1 & 2 & 1 \\ 1 & 2 & 1 & 2 \\ 2 & 1 & 3 & 1 \\ 1 & 2 & 1 & 2 \end{pmatrix}\begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 4 & 5 & 5 & 5 \\ 5 & 2 & 5 & 2 \\ 5 & 5 & 4 & 5 \\ 5 & 2 & 5 & 2 \end{pmatrix}$$

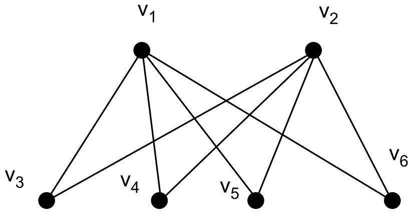
Therefore, $$B = A + A^2 + A^3 = \begin{pmatrix} 7 & 7 & 8 & 7 \\ 7 & 4 & 7 & 4 \\ 8 & 7 & 7 & 7 \\ 7 & 4 & 7 & 4 \end{pmatrix}$$

As all $b_{ij} \neq 0$ for $i \neq j$, the graph G is connected.

Example 14 *Draw a complete bipartite graph on two and four vertices.*

Solution : Complete bipartite graph on m and n is the simple graph whose vertex set is partitioned into sets V_1 and V_2 with m and n vertices respectively. Generally, denoted by K_{mn}.

The complete bipartite graph on two and four vertices is shown in the following figure.



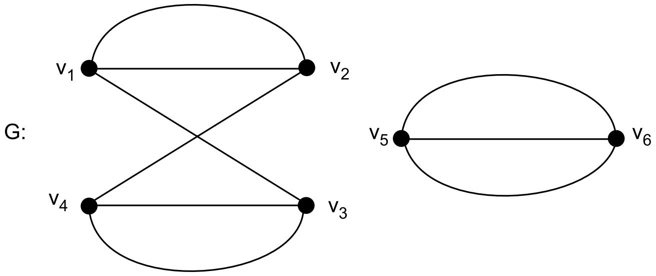
Example 15 *Use the fusion algorithm to determine whether the graph given below by its adjacency matrix is connected or not.*

$$\begin{pmatrix} 0 & 2 & 1 & 0 & 0 & 0 \\ 2 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 2 & 0 & 0 \\ 0 & 1 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 & 3 & 0 \end{pmatrix}$$

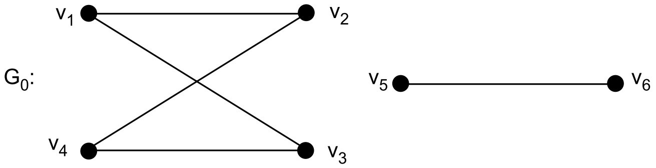
Solution : The adjacency matrix of the graph G is given as

$$A(G) = \begin{pmatrix} 0 & 2 & 1 & 0 & 0 & 0 \\ 2 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 2 & 0 & 0 \\ 0 & 1 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 & 3 & 0 \end{pmatrix}$$

Therefore, the graph G becomes



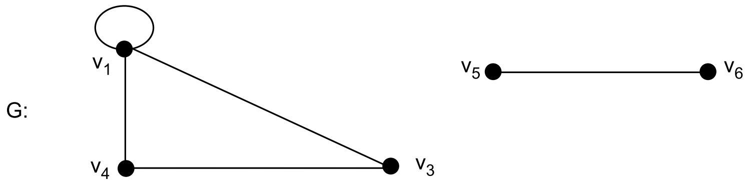
The underlying simple graph of G is given as



The adjacency matrix is given as

$$A(G_0) = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

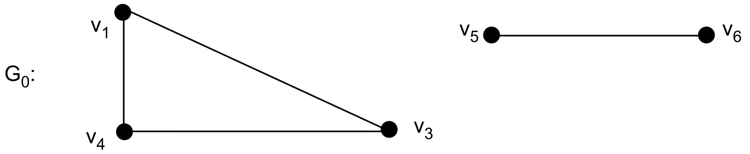
On fusing vertex v_1 with v_2 we have the graph G as



So, on replacing Row $(v_1) \leftarrow$ Row (v_1) + Row (v_2); Col $(v_1) \leftarrow$ Col (v_1) + Col (v_2) and on removing the row and column corresponding to v_2 the adjacency matrix becomes

$$A(G) = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

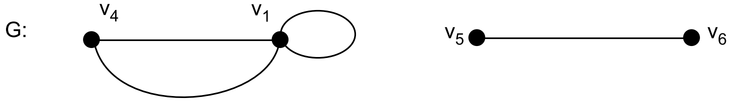
The underlying simple graph of G is given as



The adjacency matrix becomes

$$A(G_0) = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

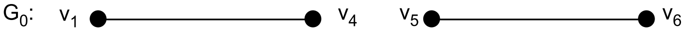
On fusing v_1 with v_3 we have the graph G as



So, on replacing Row $(v_1) \leftarrow$ Row (v_1) + Row (v_3); Col $(v_1) \leftarrow$ Col (v_1) + Col (v_3) and on removing the row and column corresponding to v_3 the adjacency matrix becomes

$$A(G) = \begin{pmatrix} 1 & 2 & 0 & 0 \\ 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

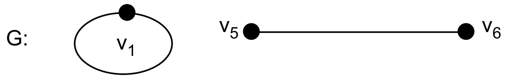
The underlying simple graph of G is given as



The adjacency matrix becomes

$$A(G_0) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

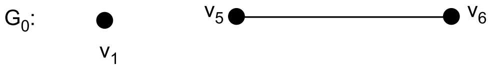
On fusing v_1 with v_4 we have the graph G as



So, on replacing Row $(v_1) \leftarrow$ Row (v_1) + Row (v_4); Col $(v_1) \leftarrow$ Col (v_1) + Col (v_4) and on removing the row and column corresponding to v_4 the adjacency matrix becomes

$$A(G) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

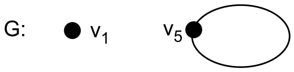
The underlying simple graph of G is given as



The adjacency matrix becomes

$$A(G_0) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

On fusing v_5 with v_6 we have the graph G as



So, on replacing Row $(v_5) \leftarrow$ Row (v_5) + Row (v_6); Col $(v_5) \leftarrow$ Col (v_5) + Col (v_6) and on removing the row and column corresponding to v_6 the adjacency matrix becomes

$$A(G) = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

The underlying simple graph of G is given as

The adjacency matrix becomes

$$A(G_0) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

As the final graph is empty, the process terminates. The number of isolated points is the order of the matrix *i.e.* two. So, the graph is not connected.

Example 16 *Draw the following graphs.*

(i) 3 regular but not complete

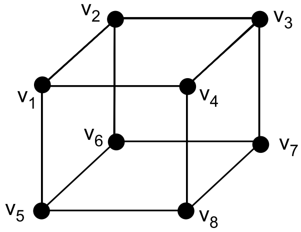
(ii) 3 regular and complete

(iii) 4 regular but not complete

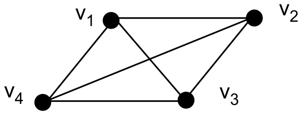
(iv) 2 regular but not complete.

Solution :

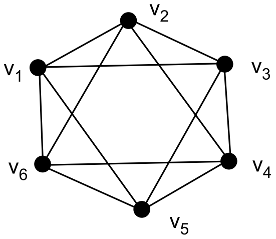
(*i*) In the graph given below, the degree of every vertex is 3 but for vertices v_1 and v_6 there is no edge. Hence the graph is 3 regular but not complete.



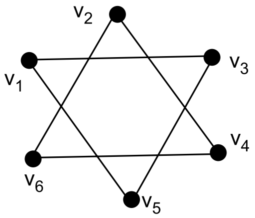
(*ii*) In the graph given below, the degree of every vertex is 3 and for any two vertices v_i and v_j there is an edge. Hence the graph is 3 regular and complete.



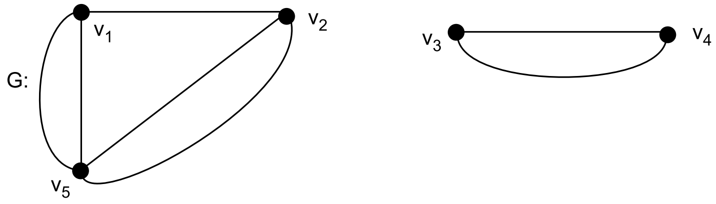
(*iii*) In the graph given below, the degree of every vertex is 4 and for the vertices v_2 and v_5 there exists no edge. Hence the graph is 4 regular but not complete.



(*iv*) In the graph given below, the degree of every vertex is 2 and for the vertices v_2 and v_5 there exists no edge. Hence the graph is 2 regular but not complete.



Example 17 *Find whether the graph given below is connected or not.*



Solution : The adjacency matrix A(G) of the above graph relative to the ordering v_1, v_2, v_3, v_4 and v_5 is given as

$$A(G) = \begin{pmatrix} 0 & 1 & 0 & 0 & 2 \\ 1 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 2 & 1 & 0 \\ 2 & 2 & 0 & 0 & 0 \end{pmatrix}$$

Here, the number of vertices (n) = 5. Let B = A + A^2 + A^3 + A^4. Therefore, we get

$$A^2 = AA = \begin{pmatrix} 5 & 4 & 0 & 0 & 2 \\ 4 & 5 & 0 & 0 & 2 \\ 0 & 0 & 4 & 2 & 0 \\ 0 & 0 & 2 & 5 & 0 \\ 2 & 2 & 0 & 0 & 8 \end{pmatrix}; A^3 = A^2 A = \begin{pmatrix} 8 & 9 & 0 & 0 & 18 \\ 9 & 8 & 0 & 0 & 18 \\ 0 & 0 & 4 & 10 & 0 \\ 0 & 0 & 10 & 9 & 0 \\ 18 & 18 & 0 & 0 & 8 \end{pmatrix}$$

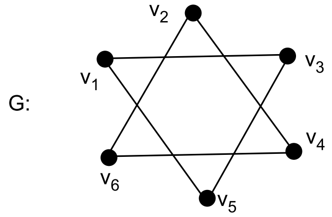
$$A^4 = A^3A = \begin{pmatrix} 45 & 44 & 0 & 0 & 34 \\ 44 & 45 & 0 & 0 & 34 \\ 0 & 0 & 20 & 18 & 0 \\ 0 & 0 & 18 & 29 & 0 \\ 34 & 34 & 0 & 0 & 72 \end{pmatrix}$$

Therefore, $B = A + A^2 + A^3 + A^4$

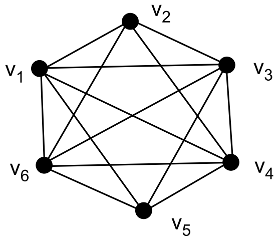
$$= \begin{pmatrix} 58 & 58 & 0 & 0 & 56 \\ 58 & 58 & 0 & 0 & 56 \\ 0 & 0 & 28 & 32 & 0 \\ 0 & 0 & 32 & 44 & 0 \\ 56 & 56 & 0 & 0 & 88 \end{pmatrix}$$

As some $b_{ij} = 0$ for $i \neq j$, the graph G is not connected.

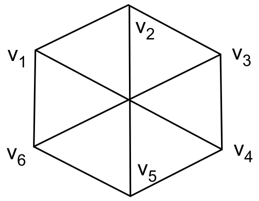
Example 18 *Find the complement graph of the following graph G, where*



Solution : On considering the above graph G, construct the complete graph with the same vertices as G. The graph is given below.

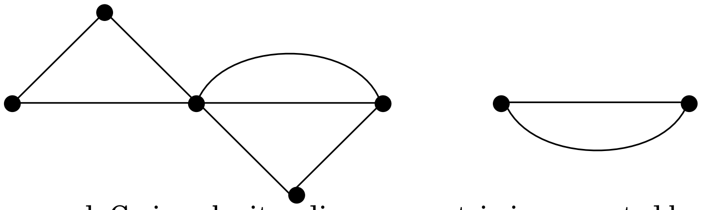


On deleting the edges of the graph G, the complement $\overline{G}$ of G is given below.



EXERCISES

1. Using fusion algorithm determine whether the graph given below is connected or not.

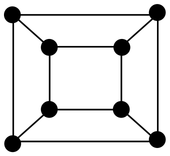


2. Show that the graph G given by its adjacency matrix is connected by using fusion algorithm.

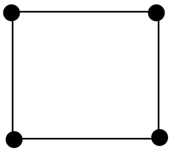
$$A(G) = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 2 \\ 0 & 0 & 1 & 1 \\ 1 & 2 & 1 & 0 \end{pmatrix}$$

3. Find the complement of the following graphs.

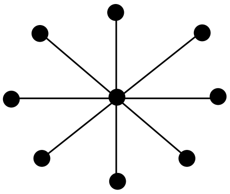
(a)



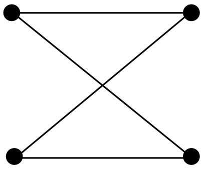
(b)



(c)

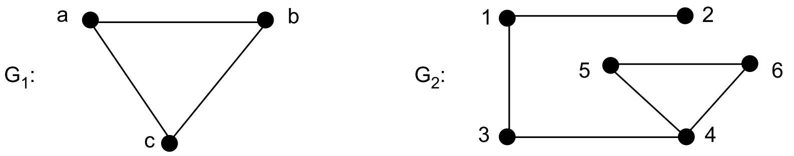


(d)

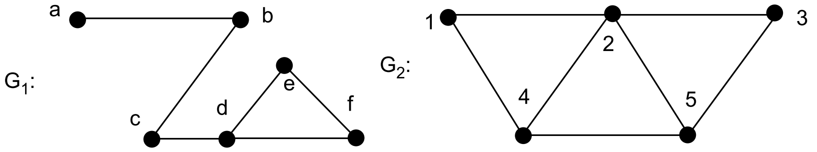


4. Find the product graph where G_1 and G_2 are given below.

(a)



(b)

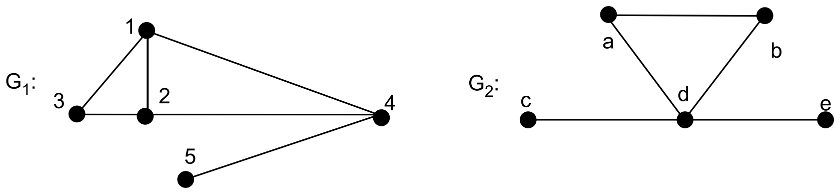


5. Construct a graph of order 5, whose vertices have degrees 1, 2, 2, 3 and 4. What is the size of this graph?

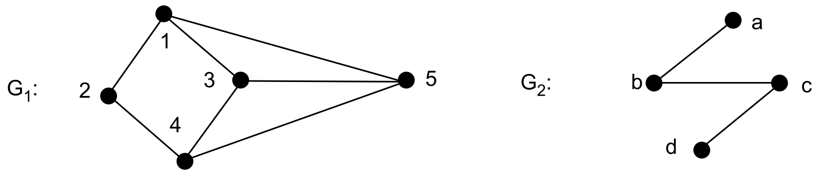
6. Construct a 3-regular graph G. Determine the complement of G. Show that $\overline{G}$ is also regular.

7. Write the graph which is the composition of the following graphs G_1 and G_2.

(a)

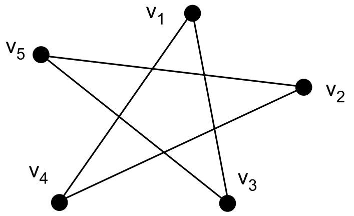


(b)

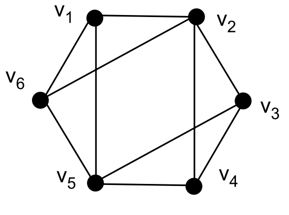


8. For the following graphs, find the adjacency matrix.

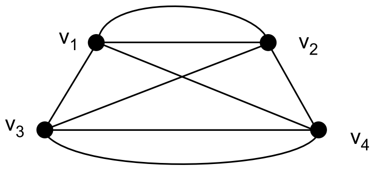
(a)



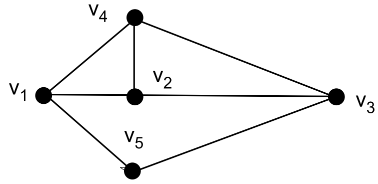
(b)



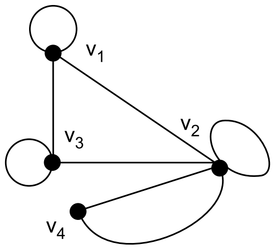
(c)



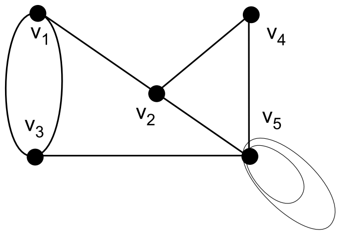
(d)



(e)

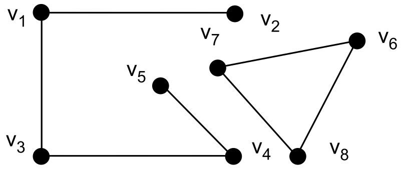


(f)

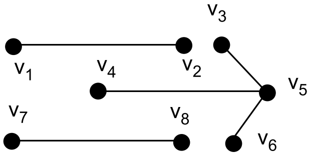


9. Find the path matrix of the following graphs.

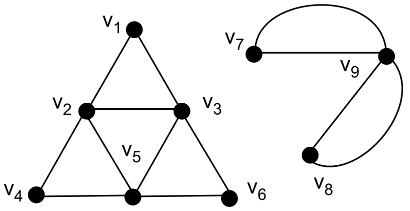
(a)



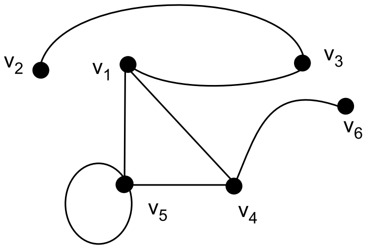
(b)



(c)

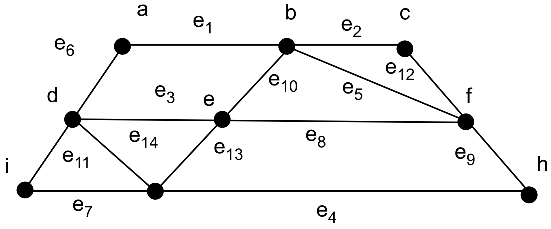


(d)

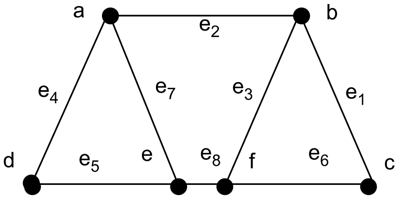


10. Write the incidence matrix of the following graphs.

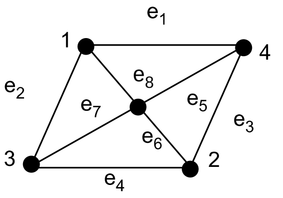
(a)



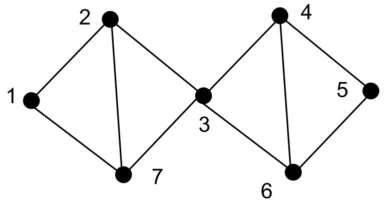
(b)



(c)

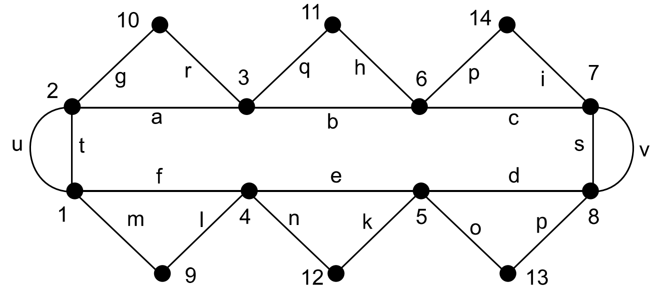


(d)



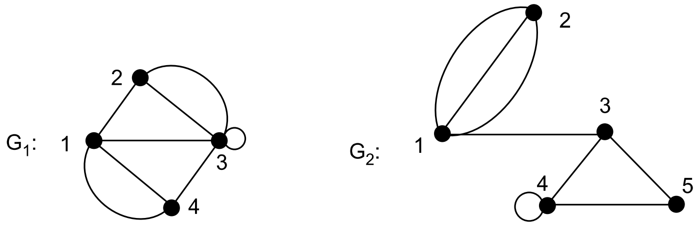
11. Let the graph G is given below. Find the followings.

(*a*) $G - V_1$; where $V_1 = \{1, 3, 5, 6, 7, 8\}$
(*b*) $G - E_1$; where $E_1 = \{a, c, d, f, g, i, j, m, n, q, r, t\}$
(*c*) $G - V_2$; where $V_2 = \{1, 3, 5, 7, 9, 11, 13\}$
(*d*) $G - E_2$; where $E_2 = \{m, l, n, k, o, j, f, e, d\}$
(*e*) G(U); where $U = \{1, 2, 3, 4\}$
(*f*) G(V); where $V = \{a, b, c, d, e, f\}$

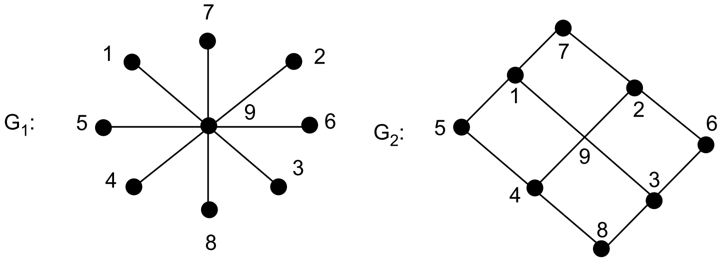


12. Write the union and intersection of the following graphs.

(a)



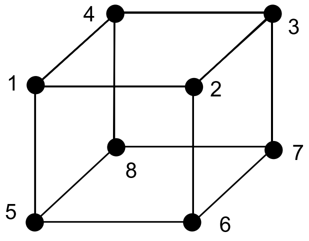
(b)



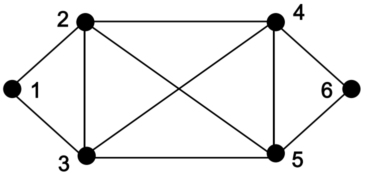
13. Let G be the set of all graphs. Show that the relation "is isomorphic" is an equivalence relation on the set G.

14. Find the degree of every vertex for the following graphs.

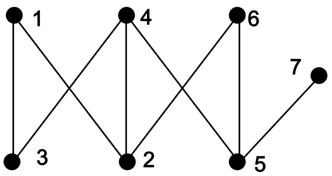
(a)



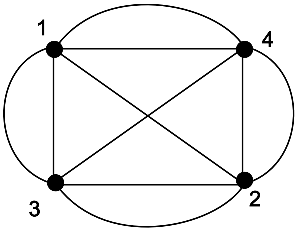
(b)



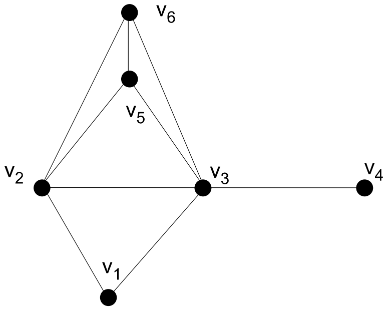
(c)



(d)

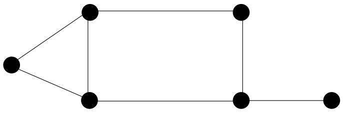


15. Determine the degrees of the vertices v_i ; I = 1, 2, 3, 4, 5 and 6 of the graph G shown below. Compute $\sum_i deg\,(v_i)$. Use this to determine the size of G.

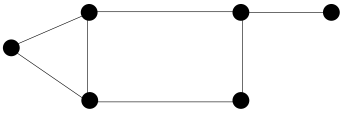


16. Determine which pairs of the graphs G_1, G_2 and G_3 are isomorphic.

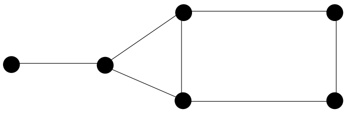
G_1:



G_2:

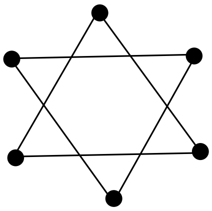


G_3:

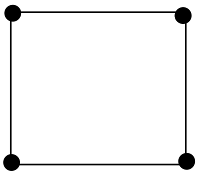


17. From the graphs given below identify
(*i*) Regular Graphs
(*ii*) Complete graphs and
(*iii*) Neither regular nor complete graphs.

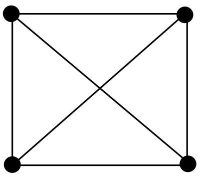
(a)



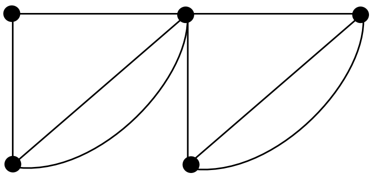
(b)



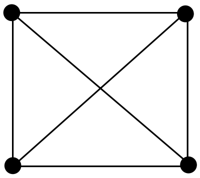
(c)



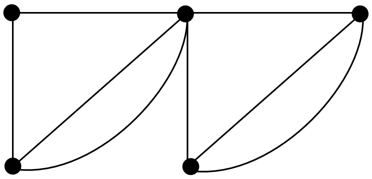
(d)



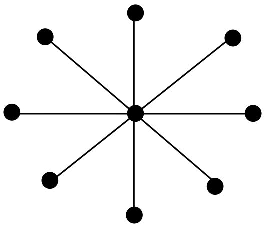
(c)



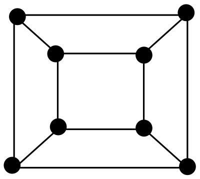
(d)



(e)

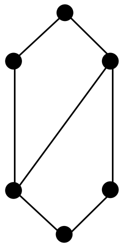


(f)

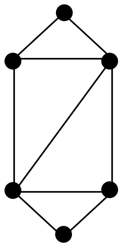


18. Determine whether the graphs G_1 and G_2 shown below are isomorphic.

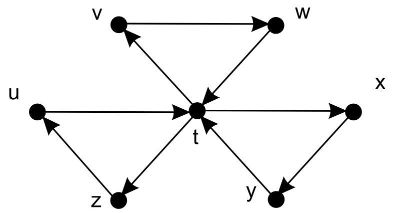
G_1:



G_2:

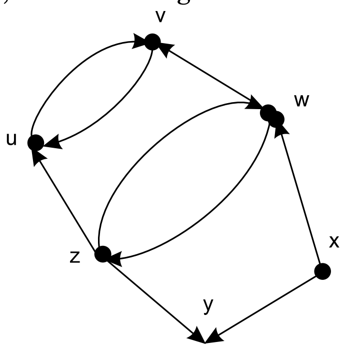


19. Determine whether the graph G shown below is strongly connected or weakly connected.



20. In the digraph G shown below, find the indegree and outdegree of every vertex.

G:

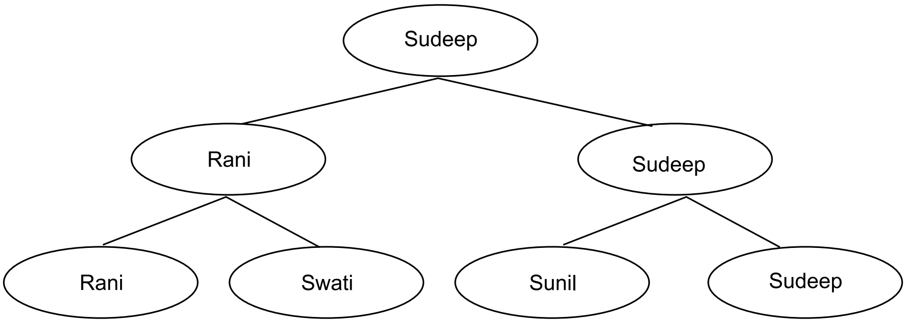


11

Tree

■ 11.0 INTRODUCTION

Another very simple and important graph is tree. Computer science makes extensive use of trees. Trees are useful in organizing and relating data in a database. These are interesting not only for their applications to computer science but also for their theoretical properties. Let us consider a single elimination tournament, which means when a player loses, he/she is out of the tournament. Winners continue to play until only one person, the champion, remains. The following figure shows that Rani defeated Swati and Sudeep defeated Sunil. The winners Rani and Sudeep, then played, and Sudeep defeated Rani. i.e. Sudeep became champion. This is nothing but a tree.



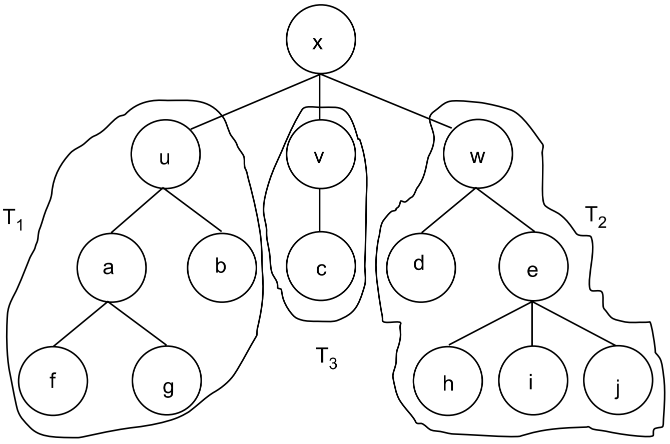
■ 11.1 TREE

A connected acyclic graph G is called a tree. A tree T is a finite set of one or more nodes such that

(*i*) There is a specially designated node called the root.

(*ii*) Remaining nodes are partitioned into k disjoint sets T_1, T_2, ..., T_k ; $k > 0$. Where each T_i for $i = 1, 2, \ldots, k$ is a tree. T_1, T_2, ... , T_k are called subtrees of the root.

In the example given below the tree T has 14 number of nodes. Which are partitioned into three sets T_1, T_2 and T_3 called the subtrees of T.



■ 11.2 FUNDAMENTAL TERMINOLOGIES

A tree has the following fundamental terminologies.

11.2.1 Node

The main component of a tree is the node. This stores the actual data and links to the other node.

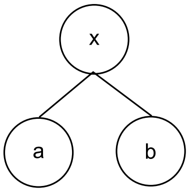
11.2.2 Child

Child of a node is the immediate successor of a node. Child, which is at the left side, is called left child and the child, which is at the right side, is called right child.

11.2.3 Parent

Parent of a node is the immediate predecessor of a node.

In the figure given below '*x*' is the parent of '*a*' and '*b*'. Where, '*a*' is the left child and '*b*' is the right child of '*x*'.



11.2.4 Root

A node that has no parent is termed as the root of the tree. In the above figure '*x*' is termed as the root.

11.2.5 Leaf

The node which is at the end and which does not have any child is called leaf node. Leaf node is also termed as terminal node and external node.

11.2.6 Level

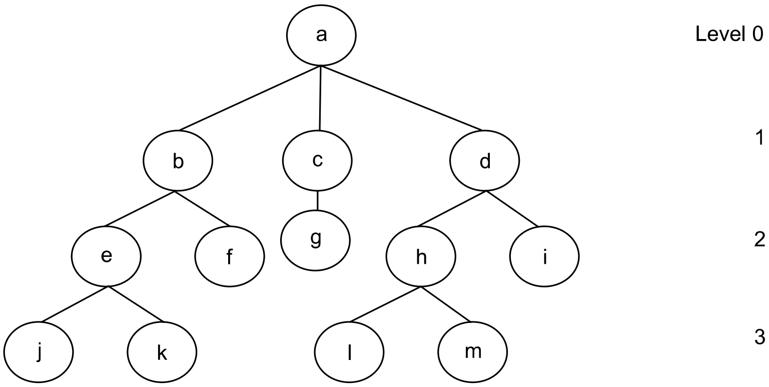
The rank of the hierarchy is known as level. The root node is termed as level 0. If a node is at level n, then its parent is at level $(n - 1)$ and child is at level $(n + 1)$.

11.2.7 Height

The height h of a tree T is defined as maximum number of nodes that is present in a path starting from root node to a leaf node. The height of a tree is also termed as depth of tree. Mathematically,

$$h = \text{Maximum level} + 1$$

Consider the example of a tree



Height of the tree = Maximum level + 1 = 3 + 1 = 4.

11.2.8 Sibling

The nodes, which have the same parent, are termed as siblings. In the above figure h and i are siblings. Similarly l and m are siblings.

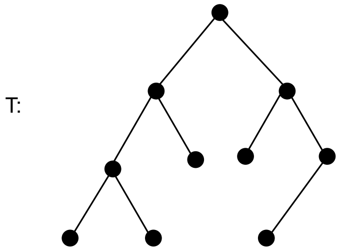
■ 11.3 BINARY TREE

A binary tree T is a finite set of nodes such that

(*i*) T is empty or

(*ii*) T contains a specially designed node called the root of T and the remaining nodes of T form two disjoint binary trees T_1 and T_2. This implies that in case of a binary tree a node may have at most two children.

Consider the following simple binary tree T as



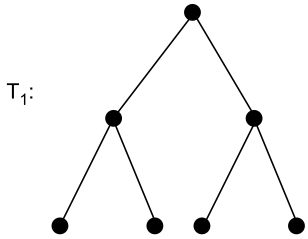
11.3.1 Full Binary Tree

A binary tree T is said to be a full binary tree if it contains maximum possible number of nodes in all level. This indicates that, for the level '*n*' of the tree it must contain 2^n number of nodes.

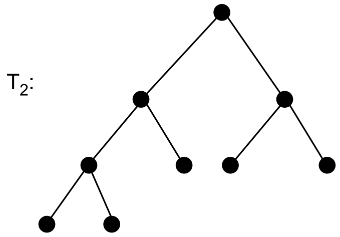
11.3.2 Complete Binary Tree

A binary tree T is said to be a complete binary tree if it contains maximum possible number of nodes in all levels except the last level.

Consider the following examples. In the figure given below T_1 is a full binary tree where as T_2 is a complete binary tree.



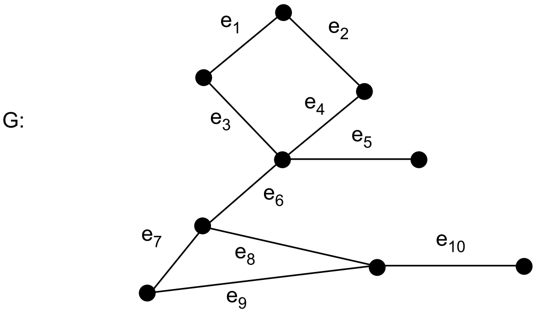
(Full Binary Tree)



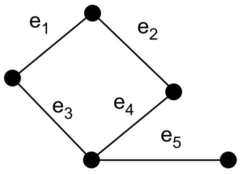
(Complete Binary Tree)

■ 11.4 BRIDGE

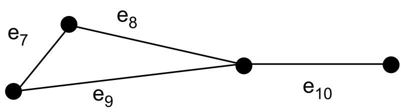
An edge of a graph G (V, E) is said to be a bridge if we remove the edge from the graph G, then the graph G has more connected components. Consider the graph G as



On removing the edge e_6 from the above graph G, the graph has two connected components such as



and



Hence, the edge e_6 is called as a bridge. In the above figure e_5 and e_{10} are also bridges. The bridge is also known as cut edge.

11.4.1 Theorem

A tree of order n has size $(n - 1)$.

Proof : We prove this by the method of induction.

For $n = 1$ we have a single vertex and hence size is 0.

For $n = 2$, the tree T contains two vertices, so size is 1.

Hence the result follows for $n = 1$ and 2. Assume that the result is true for all trees of order less than k. Let T be a tree of order $n = k$ and size q, and let e be an edge of T.

We have already observed that e is a bridge of T, so that $(T - e)$ is a forest. Let the two components of $(T - e)$ are T_1 and T_2, where T_i is a tree of order n_i and size q_i for $i = 1$ and 2.

As, $n_i < k$ for $i = 1$ and 2 so we have $q_1 = (n_1 - 1)$ and $q_2 = (n_2 - 1)$. Since, $n = (n_1 + n_2)$ and $q = (q_1 + q_2 + 1)$ we get

$$q = (n_1 - 1) + (n_2 - 1) + 1 = (n_1 + n_2) - 1 = (n - 1)$$

Therefore, by induction the size of a tree is $(n - 1)$, *i.e.* one less than its order.

11.4.2 Theorem

Every nontrivial tree contains at least two end vertices.

Proof : Suppose that T be a tree of order n and size q. Let $d_1, d_2, \ldots, d_n$ denote the degrees of its vertices, ordered so that $d_1 \le d_2 \le d_3 \le \ldots \le d_n$. Since T is connected and nontrivial, $d_i \ge 1$ for each i; $1 \le i \le n$.

Assume that T does not contain two end-vertices. Hence $d_1 \ge 1$ and $d_i \ge 2$ for $2 \le i \le n$. Thus,

$$\sum_{i=1}^{n} d_i = d_1 + d_2 + d_3 + \ldots. + d_n \ge 1 + 2(n - 1) = 2n - 1 \qquad \ldots (i)$$

But we know $$\sum_{i=1}^{n} d_i = 2q = 2\,(n - 1) = 2n - 2$$

This contradicts inequality (i). So our assumption is wrong. Hence, T contains at least two end-vertices.

■ 11.5 DISTANCE

Let u and v be two vertices of the graph G. The distance between u and v is denoted by $d(u, v)$ and is defined as the length of a shortest $u - v$ path. If there is no path between u and v, then $d\,(u, v) = \infty$.

■ 11.6 ECCENTRICITY

Let V be the vertex set of G. Let $v \in V$. The eccentricity of v is denoted as $e(v)$ and is defined as

$$e(v) = \text{Max}\,\{d\,(u, v) : u \in V \text{ and } u \ne v\}$$

■ 11.7 RADIUS

Let G be the graph, then the radius of G is denoted as rad (G) and is defined as

$$\text{rad}(G) = \text{Min}\,\{e(v) : v \in V\}.$$

■ 11.8 DIAMETER

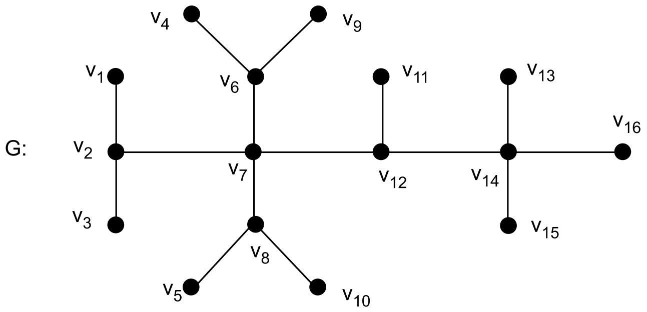
Let V be the vertex set of the graph G. The diameter of G is denoted as diam (G) and is defined as

$$\text{diam}(G) = \text{Max}\,\{e(v) : v \in V\}.$$

■ 11.9 CENTRAL POINT AND CENTRE

Let V be the vertex set of the graph G. Then $v \in V$ is said to be a central point if $e(v) = \text{rad}(G)$. The set of all central points of G is known as centre of G.

Consider the following graph G where each edge is of length 1.



Here $V = \{v_1, v_2, v_3, \ldots, v_{16}\}$. Now, we get

$d(v_1, v_2) = 1$; $d(v_1, v_3) = 2$; $d(v_1, v_4) = 4$; $d(v_1, v_5) = 4$; $d(v_1, v_6) = 3$;
$d(v_1, v_7) = 2$; $d(v_1, v_8) = 3$; $d(v_1, v_9) = 4$; $d(v_1, v_{10}) = 4$; $d(v_1, v_{11}) = 4$;
$d(v_1, v_{12}) = 3$; $d(v_1, v_{13}) = 5$; $d(v_1, v_{14}) = 4$; $d(v_1, v_{15}) = 5$; $d(v_1, v_{16}) = 3$.

Therefore, $e(v_1) = \text{Max}\,\{1, 2, 3, 4, 5\} = 5$.

$d(v_2, v_1) = 1$; $d(v_2, v_3) = 1$; $d(v_2, v_4) = 3$; $d(v_2, v_5) = 3$; $d(v_2, v_6) = 2$; $d(v_2, v_7) = 1$;
$d(v_2, v_8) = 2$; $d(v_2, v_9) = 3$; $d(v_2, v_{10}) = 3$; $d(v_2, v_{11}) = 3$; $d(v_2, v_{12}) = 2$; $d(v_2, v_{13}) = 4$;
$d(v_2, v_{14}) = 3$; $d(v_2, v_{15}) = 4$; $d(v_2, v_{16}) = 4$.

Therefore, $e(v_2) = \text{Max}\,\{1, 2, 3, 4\} = 4$. Proceeding in this manner, we will get

$e(v_3) = 5$; $e(v_4) = 5$; $e(v_5) = 5$; $e(v_6) = 4$; $e(v_7) = 3$;
$e(v_8) = 4$; $e(v_9) = 5$; $e(v_{10}) = 5$; $e(v_{11}) = 4$; $e(v_{12}) = 3$;
$e(v_{13}) = 5$; $e(v_{14}) = 4$; $e(v_{15}) = 5$; $e(v_{16}) = 5$.

Now, radius = rad (G) = Min $\{e(v), v \in V\}$ = Min $\{5, 4, 3\}$
= 3 and diameter = diam (G) = Max $\{e(v), v \in V\}$
= Max $\{5, 4, 3\} = 5$.

Therefore, the central points are v_7 and v_{12} and center = $\{v_7, v_{12}\}$.

■ 11.10 SPANNING TREE

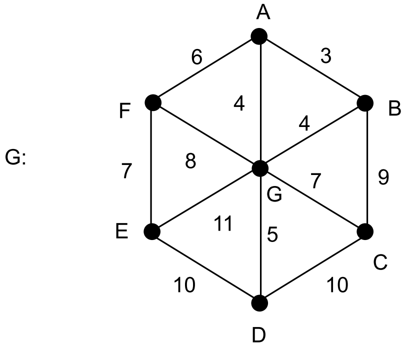
Suppose G = (V, E) be a graph. A sub graph H of G is said to be a spanning sub graph of G if both H and G has same vertex set. A spanning tree of a graph G is a tree which is a spanning sub graph of G. In this section we will discuss the algorithms for finding minimum spanning tree.

11.10.1 Prim's Algorithm

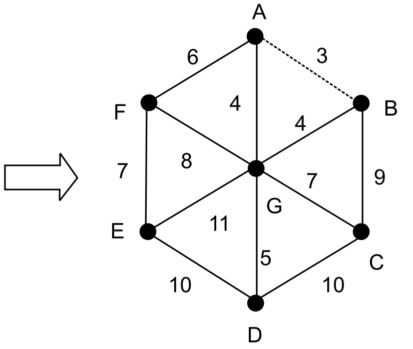
The following steps are used in Prim's algorithm for finding a minimum spanning tree of a graph G. Assume that the graph G has n vertices.

1. Choose any vertex v_1 of G
2. Choose an edge $e_1 = v_1 v_2$ of G such that $v_1 \neq v_2$ and e_1 has smallest weight among the edges of G incident with v_1.
3. If edges e_1, e_2 .... e_i have been chosen involving vertices $v_1, v_2, \ldots, v_{i+1}$, then choose an edge $e_{i+1} = u\ v$ with $u \in \{v_1, v_2, \ldots, v_{i+1}\}$ and $v \notin \{v_1, v_2, \ldots, v_{i+1}\}$ such that e_{i+1} has smallest weight among the edges of G.
4. The step 3 is to be repeated until we are getting the total $(n - 1)$ edges.

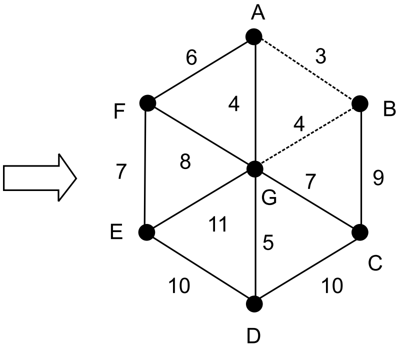
Consider the following connected weighted graph G. Here the number of vertices $n = 7$



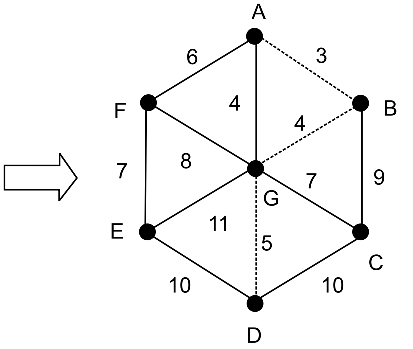
(V$_1$= A ; One can choose any other vertex)



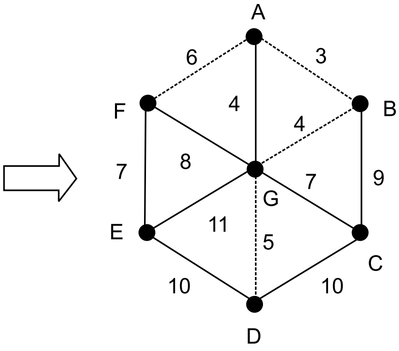
(e_1 = AB, So that v_2 = B)



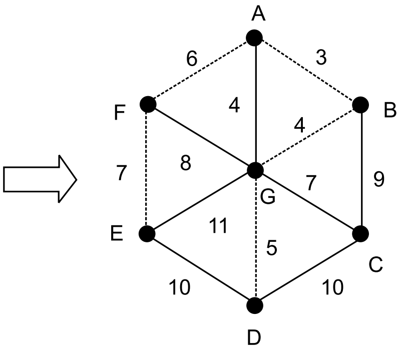
(e_2 = BG ; So that v_3 = G ; An alternative choice is AG)



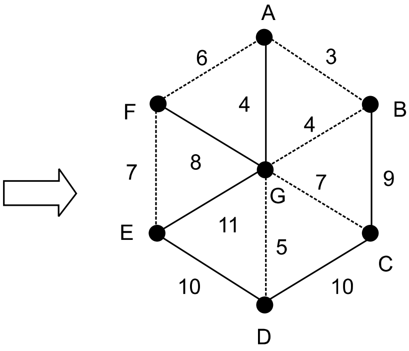
(e_3 = GD ; So that v_4 = D; No alternative choice)



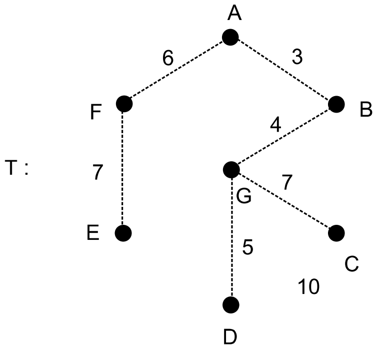
(e_4 = AF ; So that v_4 = F ; No altrative choice)



(e_5 = FE ; So that v_5 = E ; An alternative choice is GC)



(e_6 = GC ; So that v_6 = C; No alternative choice)



w(T) = 32

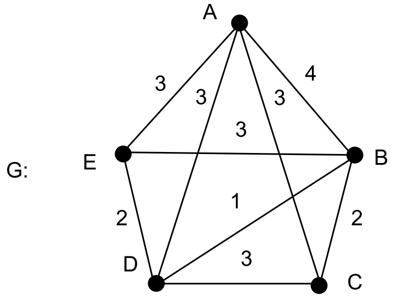
Since the total edges are 6 = (7 – 1), the process terminates. Hence, the minimum spanning tree T is given as shown in the above figure.

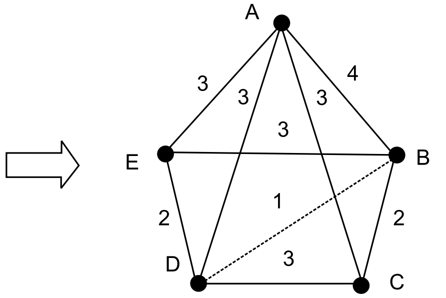
11.10.2 Kruskal's Algorithm

The following steps are used in Kruskal's algorithm for finding a minimum spanning tree of a graph G. Assume that the graph G has n vertices.

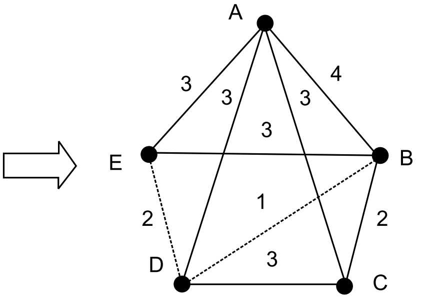
1. Choose an edge e_1 of G, which is as small as possible and e_1 must not be a loop.
2. Suppose the edges e_1, e_2, ..., e_k have been chosen. Then the edge e_{k+1} (not already chosen) can be chosen such that
   (*i*) The induced sub graph G[{e_1, e_2 ,.......... , e_{k+1}}] is acyclic and
   (*ii*) Weight of e_{k+1} is as small as possible.
3. The step 2 is to be repeated until we are getting the total (n – 1) edges.

Consider the following connected weighted graph G. Here the number of vertices n = 5. On applying Kruskal's algorithm we have the following stages.

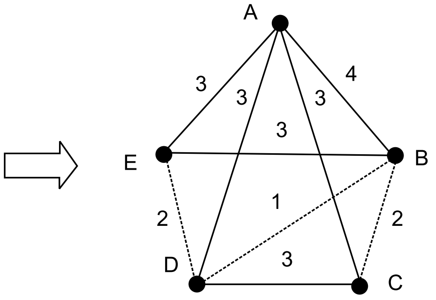




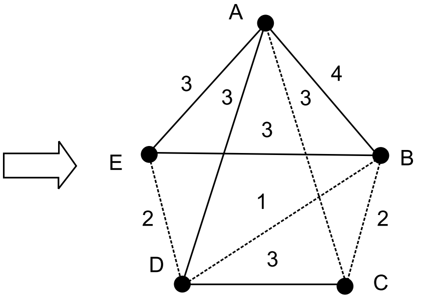
(e_1 = BD ; w (e_1) = 1 ; No alternative choice)



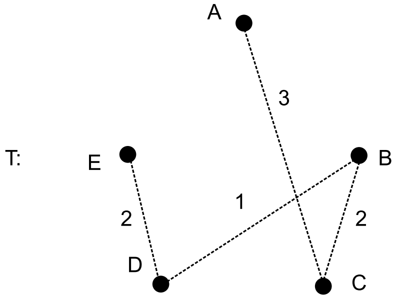
(e_2 = DE ; w (e_2) = 2; An alternative choice is BC)



(e_3 = BC; w (e_3) = 2 ; No alternative choice)



(e_4 = AC; w (e_4) = 3 ; Alternative choices are AE and AD)



w (T) = 1 + 2 + 2 + 3 = 8

Since the total edges are 4 = (5 – 1), the process terminates. Hence, the minimum spanning tree T is given as shown in the above figure.

■ 11.11 SEARCHING ALGORITHMS

This section presents methods for searching a graph. This means systematically following the edges of the graph so as to visit the vertices of the graph. The graph searching algorithms can discover much about the structure of a graph. Here we present two algorithms, depth first search and breadth first search. In addition, we will discuss to create a breadth first and depth first tree.

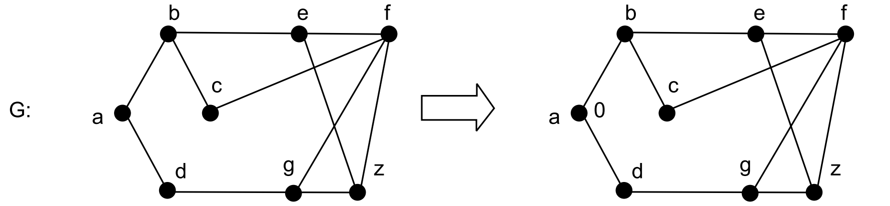
11.11.1 Breadth First Search

Breadth first search is one of the simplest algorithms for searching a graph. Given a graph G(V, E) and a distinguished source vertex s, breadth first search systematically explores the edges of G to discover every vertex that is reachable from s. It computes the distance (fewest number of edges) from s to all such reachable vertices. Breadth first search is so named because it expands the frontier between discovered and un discovered vertices uniformly across the breadth of the frontier. It constructs a breadth first tree, initially containing only its root, that is the source vertex s.

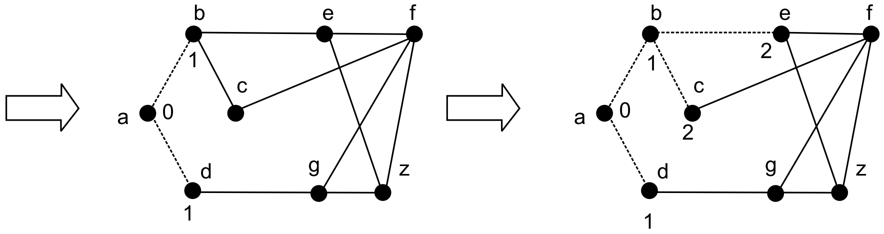
Suppose that v_i, v_j, be two specified vertices of G. We will now describe a method of finding a path from v_i to v_j which uses the least number of edges. Such a path is known as shortest path, if it exists. The method assigns labels 0, 1, 2, ... to the vertices of G and is called the Breadth First Search (BFS) technique. The BFS algorithm consists of the following steps.

1. Label the vertex v_i with 0. Set $i = 0$
2. Find all unlabelled vertices in G, which are adjacent to vertices, labeled i. If there are no such vertices, then v_i is not connected to v_j else label them by $(i + 1)$.
3. If v_j is labeled go to step 4, else replace i by $(i + 1)$ and go to step 2.
4. The length of shortest path from v_i to v_j is $(i + 1)$ then stop.

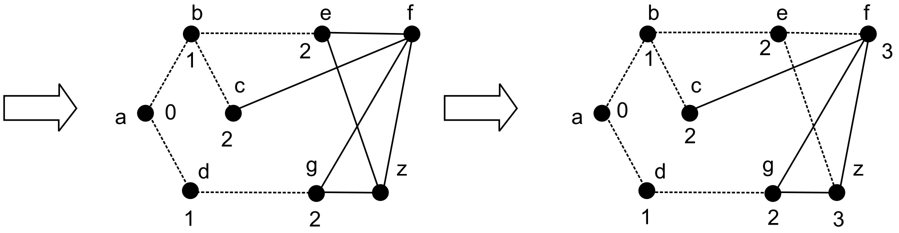
Consider the following graph G. Now we have to find out the shortest path from the source vertex a to the vertex z. On using the BFS technique, we get the following stages.



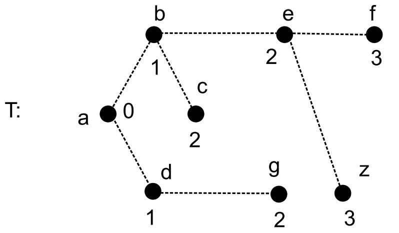
(Label (a) = 0 and set i = 0)



In the above figure the adjacent vertices of a are b and d. Therefore we get label (b) = i + 1 = 0 + 1 = 1 and label (d) = i + 1 = 0 + 1 = 1. Similarly, adjacent vertices of b are c and e. Therefore, label (c) = i + 1 = 1 + 1 = 2 and label (e) = i + 1 = 1 + 1 = 2.



In the above figure the adjacent vertices of d is g. Therefore we get label $(g) = i + 1 = 1 + 1 = 2$. Similarly, adjacent vertices of e are f and z. Therefore, label $(f) = i + 1 = 2 + 1 = 3$ and label $(z) = i + 1 = 2 + 1 = 3$. Hence, the breadth first tree T becomes

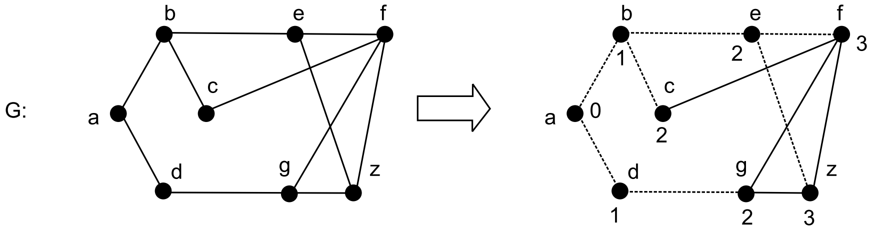


11.11.2 Back-Tracking Algorithm

The following steps are use in back-tracking algorithm.

1. Set $\lambda\ (t) = i$ and assign $v_i = t$, where 't' is the terminating node.
2. Find a vertex 'u' which is adjacent to v_i and with $\lambda\ (u) = (i - 1)$. Set $v_{i-1} = u$.
3. If $i = 1$, then stop else replace i by $(i - 1)$ and go to step 2.

Consider the following graph G. Now we have to find out the shortest path from the source vertex 'a' to the vertex 'z'. On using the BFS technique, we get.



On using back-tracking algorithm we have

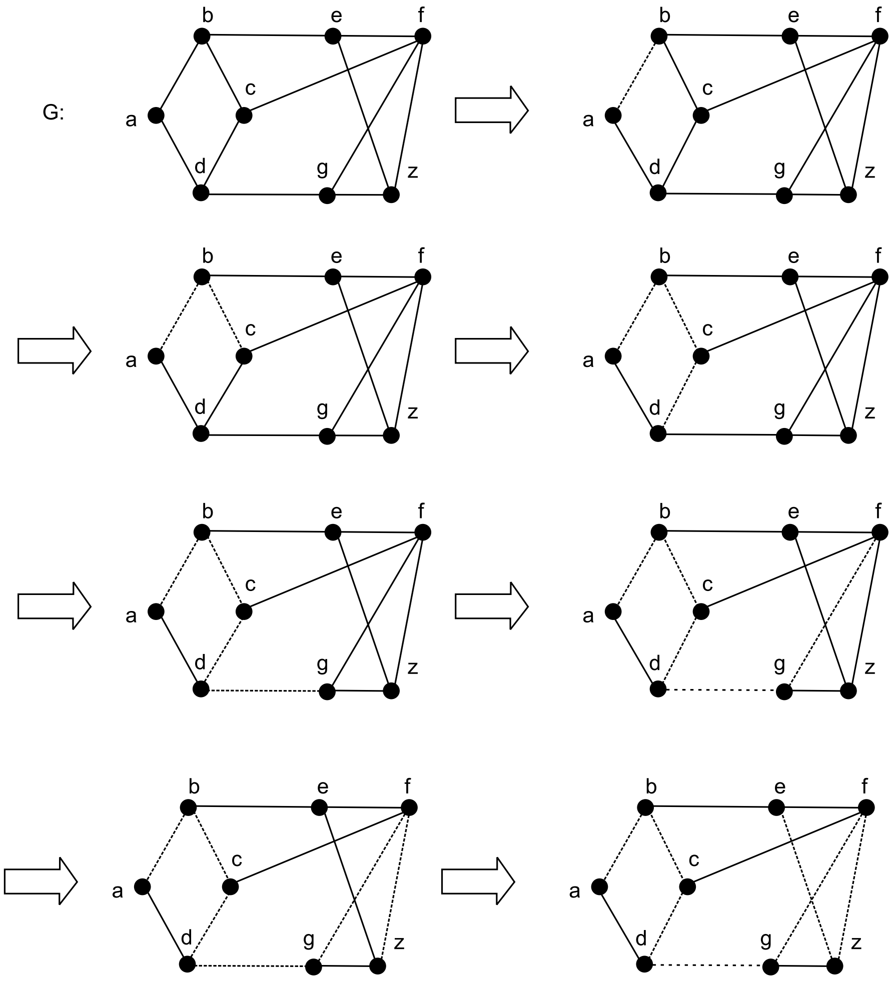
1. Set $i = \lambda(z) = 3$ and $v_i = v_3 = z$
2. The adjacent to $v_3 = z$ is e and $\lambda\ (e) = (i - 1) = 2$. Set $v_2 = e$.
3. As $i = 3 \neq 1$, so $i = (i - 1) = 2$, Go to step 2.
2. The adjacent to $v_2 = e$ is b and $\lambda\ (b) = (i - 1) = 1$. Set $v_1 = b$.
3. As $i = 2 \neq 1$, so $i = (i - 1) = 1$, Go to step 2.
2. The adjacent to $v_1 = b$ is a and $\lambda\ (a) = (i - 1) = 0$. Set $v_0 = a$.
3. As $i = 1$, so the process terminates.

Therefore, the shortest path from 'a' to z is given as '$a\ b\ e\ z$'. Besides that, there could be several paths from 'a' to 'z'.

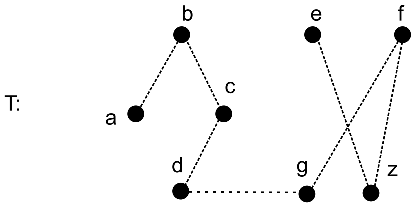
11.11.3 Depth First Search

Basic philosophy in depth first search is that first all vertices reachable from the vertex 'v' are searched before proceeding to see the siblings. In depth first search, edges are explored out of the most recently discovered vertex 'v' that still has unexplored edges leaving it. When all of v's edges have been explored, then the search "backtracks" to explore edges leaving the vertex from which 'v' was discovered. The process is being continued until we have discovered all the vertices that are reachable from the original source vertex. If any undiscovered vertices remain, then one of them is selected as a new source vertex and the search is repeated. This process is repeated until all vertices are discovered.

Consider the graph G as below. Let us consider the source vertex as '*a*'. On using the DFS technique, the order in which the vertices are being visited is described below by the sequence of graphs.



Therefore, the depth first tree T is given below. Besides that, there could be several depth first trees from the same vertex '*a*'. This indicates that the depth first tree is not unique.



■ 11.12 SHORTEST PATH ALGORITHMS

This section presents methods for finding shortest path from a source vertex to a terminating vertex in a graph G. This problem is a real life problem, where cities are connected through roads, rails and air routes and we want to find out the shortest path between the vertices. Here we present two algorithms Dijkastra's Algorithm and Floyd-Warshall Algorithm.

11.12.1 Dijkstra's Algorithm

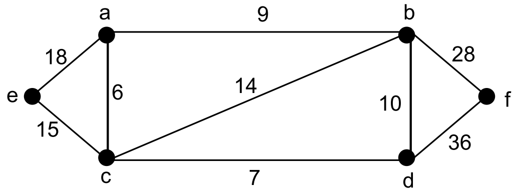
In a given graph G(V, E), we want to find a shortest path from a given source vertex 's ∈ V' to every vertex 'v ∈ V'. This is otherwise known as single source shortest path problem. Dijkastra's Algorithm solves the single source shortest path problems in weighted graphs that to non-negative weights. Therefore, we assume that $w(uv) \geq 0$ for each edge $(uv) \in$ E.

1. Set $\lambda\,(v_s) = 0$ and for all vertices $v_i \neq v_s\ \lambda\,(v_i) = \infty$. Set T = V; where V is the set of vertices of G and T is the set of uncolored vertices.
2. Let u be the vertex in T for which $\lambda\,(u)$ is minimum.
3. If $u = v_t$ (Terminating node), then stop. Else, go to step 4.
4. For every edge $e = uv$, incident with u, if $v \in$ T, then replace $\lambda\,(v)$ with Min $\{\lambda\,(v), \lambda\,(u) + w\,(uv)\}$.

i.e. $$\lambda\,(v) = \text{Min}\ \{\lambda\,(v), \lambda\,(u) + w\,(uv)\}$$

5. Change T by T – $\{u\}$ and go to step 2.

Consider the following graph G. Let us consider the source vertex as e and the terminating vertex as f. We have to find out the shortest distance between the vertices e and f.



In the above graph G, the source vertex is $v_s = e$ and $v_t = f$. Set $\lambda(e) = 0$ and $\lambda(a) = \lambda(b) = \lambda(c) = \lambda(d) = \lambda(f) = \infty$. T = V = $\{e, a, b, c, d, f\}$. Hence, we have the following table

Vertex	e	a	b	c	d	f
$\lambda(v)$	0	∞	∞	∞	∞	∞
T	e	a	b	c	d	f

Now, $u = e$ as $\lambda(u) = \lambda(e) = 0$ which is minimum. The edges incident on $u = e$ are ea and ec. Therefore,

$$\begin{aligned}\lambda(a) &= \text{Min}\ [\lambda(a), \lambda(e) + w(ea)]\\ &= \text{Min}\ [\infty, 18] = 18.\\ \lambda(c) &= \text{Min}\ [\lambda(c), \lambda(e) + w(ec)]\\ &= \text{Min}\ [\infty, 15\ ] = 15.\end{aligned}$$

Again, T = T – $\{u = e\}$ = $\{\,a, b, c, d, f\,\}$. Thus, we have the following table

Vertex	e	a	b	c	d	f
$\lambda(v)$	0	18	∞	15	∞	∞
T		a	b	c	d	f

Now, $u = c$ as $\lambda(u) = \lambda(c) = 15$ which is minimum. The edges incident with $u = c$ are ca, cb and cd. Therefore,

$$\begin{aligned}\lambda(a) &= \text{Min }[\lambda(a), \lambda(c) + w(ca)]\\ &= \text{Min }[18, 21] = 18.\\ \lambda(b) &= \text{Min }[\lambda(b), \lambda(c) + w(cb)]\\ &= \text{Min }[\infty, 29] = 29.\\ \lambda(d) &= \text{Min }[\lambda(d), \lambda(c) + w(cd)]\\ &= \text{Min }[\infty, 22] = 22.\end{aligned}$$

Again, $\quad T = T - \{u = c\} = \{a, b, d, f\}$. Thus, we have the following table

Vertex	e	a	b	c	d	f
$\lambda(v)$	0	18	29	15	22	∞
T		a	b		d	f

Now, $u = a$ as $\lambda(u) = \lambda(a) = 18$ which is minimum. The edges incident with $u = a$ is ab. Therefore,

$$\begin{aligned}\lambda(b) &= \text{Min }[\lambda(b), \lambda(a) + w(ab)]\\ &= \text{Min }[29, 27] = 27.\end{aligned}$$

Again, $\quad T = T - \{u = a\} = \{b, d, f\}$. Thus, we have the following table

Vertex	e	a	b	c	d	f
$\lambda(v)$	0	18	27	15	22	∞
T			b		d	f

Now, $u = d$ as $\lambda(u) = \lambda(d) = 22$ which is minimum. The edges incident with $u = d$ are db and df. Therefore,

$$\begin{aligned}\lambda(b) &= \text{Min }[\lambda(b), \lambda(d) + w(db)]\\ &= \text{Min }[27, 32] = 27.\\ \lambda(f) &= \text{Min }[\lambda(f), \lambda(d) + w(df)]\\ &= \text{Min }[\infty, 58] = 58.\end{aligned}$$

Again, $\quad T = T - \{u = d\} = \{b, f\}$. Thus, we have the following table.

Vertex	e	a	b	c	d	f
$\lambda(v)$	0	18	27	15	22	58
T			b			f

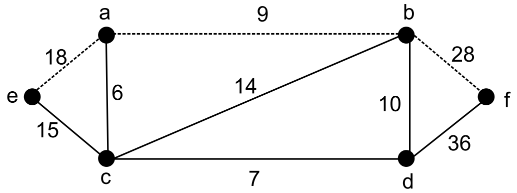
Now, $u = b$ as $\lambda(u) = \lambda(b) = 27$ which is minimum. The edges incident with $u = b$ is bf. Therefore,

$$\begin{aligned}\lambda(f) &= \text{Min }[\lambda(f), \lambda(b) + w(bf)]\\ &= \text{Min }[58, 55\ ] = 55.\end{aligned}$$

Again, $\quad T = T - \{u = b\} = \{f\}$. Thus, we have the following table

Vertex	e	a	b	c	d	f
$\lambda(v)$	0	18	27	15	22	55
T						f

Now, $u = f$ and f is the terminating node, so the process terminates. Hence the shortest distances from e to a, b, c, d and f are 18, 27, 15, 22, 55 respectively. The shortest distance between e and f is given in the following figure.



11.12.2 Floyd-Warshall Algorithm

Floyd-Warshall algorithm solves all-pairs shortest paths problem on a directed weighted graph G = (V, E). The weighted graph may contain negative weight edges, but we shall assume that there are no negative weight cycles. In this algorithm, we use the adjacency matrix of the graph to find out the shortest distance between any pair of vertices.

Suppose that G(V, E) be a graph. Let W be the adjacency matrix of the weighted directed graph G. The algorithm has the following steps.

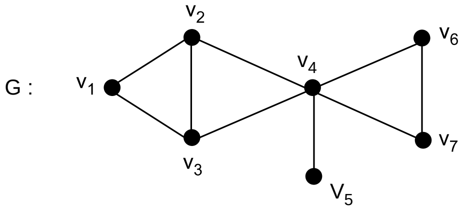
```
1. $n$ = Rows [W]
2. $D^{(0)} = W$
3. Fo $k = 1$ to $n$
4.         Do for $i = 1$ to $n$
5.             Do for $j = 1$ to $n$
6.                 $d_{ij}^{(k)} = \text{Min}\left(d_{ij}^{(k-1)}, d_{ik}^{(k-1)} + d_{kj}^{(k-1)}\right)$
7. Write $D^{(n)}$
```

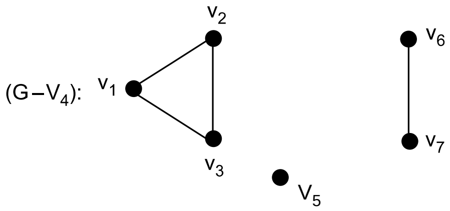
Where, $D^{(n)} = \left(d_{ij}^{n}\right)$.

■ 11.13 CUT VERTICES

Suppose that G(V, E) be the graph. A vertex 'v' of a graph G is called a cut vertex of G if the number of component of $(G - v)$ is greater than the number of components of G. *i.e.* $w(G - v) > w(g)$, where $w(G)$ represents number of component of G.

Consider the graph G as below. In the graph G, 'v_4' is a cut vertex as $w(G - v_4) = 3 > w(G) = 1$.





■ 11.14 EULER GRAPH

A tour is a closed walk of G, which include every edge of G at least once. An Euler tour is a closed walk of G, which include every edge of G exactly once. A graph G is said to be an Euler or Eulerian if the graph G has an Euler tour.

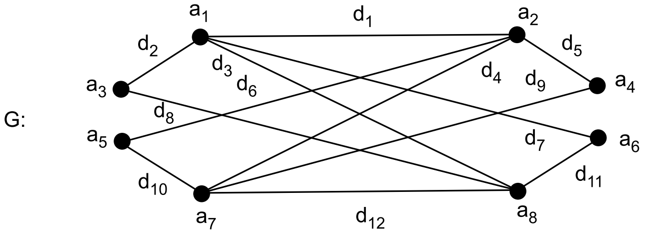
In this section, we will discuss two algorithms *i.e.* Fleury's algorithm and Hierholzer's algorithm to construct Euler tour in a Euler graph.

11.14.1 Fleury's Algorithm

This algorithm is generally developed to construct an Euler tour in a Euler graph. The following steps are used in this algorithm.

1. Choose any vertex v_0 in the Euler graph G and set $W_0 = v_0$.
2. If the trail $W_i = v_0\, e_1\, v_1\, e_2\, v_2$ .... $e_i\, v_i$ has been chosen, then choose an edge e_{i+1} different from $e_1, e_2, ..., e_i$ such that
   (*i*) e_{i+1} is incident with v_i and
   (*ii*) unless there is no alternative, e_{i+1} is not a bridge of the edge deleted subgraph $G - \{e_1, e_2, ..., e_i\}$
3. Stop if w_i contains every edge of G; otherwise go to step 2.

Consider the following Euler graph G. We have to find out the Euler tour using Fleury's algorithm for the Euler graph G.



1. Let us choose $v_0 = a_1$ and Set $w_0 = a_1$
2. Choose edge $e_1 = d_1$ such that $W_1 = v_0\, e_1 = a_1\, d_1\, a_2$
3. As W_1 contains only one edge, so go to step 2.
2. Choose edge $e_2 = d_6$ such that $W_2 = a_1\, d_1\, a_2\, d_6\, a_5$
3. As W_2 contains 2 edges, so go to step 2.
2. Choose edge $e_3 = d_{10}$ such that $W_3 = a_1\, d_1\, a_2\, d_6\, a_5\, d_{10}\, a_7$
3. As W_3 contains 3 edges, so go to step 2.
2. Choose edge $e_4 = d_9$ such that $W_4 = a_1\, d_1\, a_2\, d_6\, a_5\, d_{10}\, a_7\, d_9\, a_4$
3. As W_4 contains 4 edges, so go to step 2.
2. Choose edge $e_5 = d_5$ such that $W_5 = a_1\, d_1\, a_2\, d_6\, a_5\, d_{10}\, a_7\, d_9\, a_4\, d_5\, a_2$
3. As W_5 contains 5 edges, so go to step 2.

Proceeding in this manner, we will get

$$W_{12} = a_1\, d_1\, a_2\, d_6\, a_5\, d_{10}\, a_7\, d_9\, a_4\, d_5\, a_2\, d_4\, a_7\, d_{12}\, a_8\, d_8\, a_3\, d_2\, a_1\, d_3\, a_8\, d_{11}\, a_6\, d_7\, a_1$$

As W_{12} contains all the 12 edges once, so the process terminates. Thus the Euler tour produced is given as

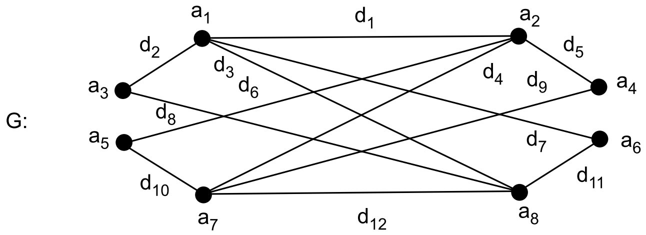
$$a_1\, d_1\, a_2\, d_6\, a_5\, d_{10}\, a_7\, d_9\, a_4\, d_5\, a_2\, d_4\, a_7\, d_{12}\, a_8\, d_8\, a_3\, d_2\, a_1\, d_3\, a_8\, d_{11}\, a_6\, d_7\, a_1$$

11.14.2 Hierholzer's Algorithm

Like Fleury's algorithm, this algorithm is also developed to construct an Euler tour in a Euler graph. The following steps are used in this algorithm.

1. Choose any vertex v in G and choose any closed trail W_0 in G. Set $i = 0$.
2. If $E(W_i) = E(G)$, then stop and W_i is an Euler tour of G; else chose a vertex v_i on W_i which is incident with an edge in G but not in W_i. Choose a closed trail W_i*in the subgraph G - $E(W_i)$, starting at the vertex v_i. Where W_i* is the detour trail.
3. Let W_{i+1} be the closed trail consisting of the edges of both W_i and W_i* obtained by starting at the vertex v, traversing the trail W_i until v_i is reached, then traversing the closed trail W_i* and returning to v_i , completing the rest of the trail W_i. Replace i by $(i + 1)$ and go to step 2.

Consider the graph G. We have to find out the Euler tour using Hierholzer's algorithm for the Euler graph G.



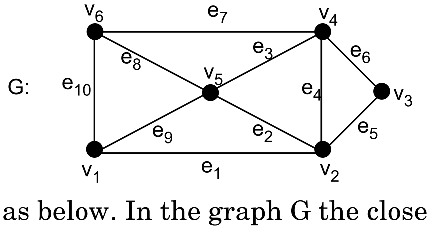
1. Let $v = a_1$ choose the closed trail W_0 as $W_0 = a_1\, d_1\, a_2\, d_5\, a_4\, d_9\, a_7\, d_{12}\, a_8\, d_3\, a_1$. Set $i = 0$.
2. As $E(W_0) \neq E(G)$, choose a_2 on W_0 incident with d_6 not in W_0. Choose $W_0{}^* = a_2\, d_6\, a_5\, d_{10}\, a_7\, d_4\, a_2$; where all $d_i \in G - E(W_0)$; i = 6, 4, 10.
3. Now, we have $W_1 = W_{0+1} = a_1\, d_1\, a_2\, d_6\, a_5\, d_{10}\, a_7\, d_4\, a_2\, d_5\, a_4\, d_9\, a_7\, d_{12}\, a_8\, d_3\, a_1$ and $i = (i + 1) = 0 + 1 = 1$. Go to step 2.
2. As $E(W_1) \neq E(G)$, choose a_1 on W_1 incident with d_2 not in W_1. Choose $W_1{}^* = a_1\, d_2\, a_3\, d_8\, a_8\, d_{11}\, a_6\, d_7\, a_1$; where all $d_i \in G - E(W_1)$; i = 2, 8, 11, 7.
3. Now, we get $W_2 = W_{1+1} = a_1\, d_2\, a_3\, d_8\, a_8\, d_{11}\, a_6\, d_7\, a_1\, d_1\, a_2\, d_6\, a_5\, d_{10}\, a_7\, d_4\, a_2\, d_5\, a_4\, d_9\, a_7\, d_{12}\, a_8\, d_3 a_1$ and $i = (i + 1) = 2$. Go to step 2. Since, $E(W_2) = E(G)$; the process terminates. Therefore, the Euler tour is given as
$$a_1\, d_2\, a_3\, d_8\, a_8\, d_{11}\, a_6\, d_7\, a_1\, d_1\, a_2\, d_6\, a_5\, d_{10}\, a_7\, d_4\, a_2\, d_5\, a_4\, d_9\, a_7\, d_{12}\, a_8\, d_3\, a_1.$$

11.14.3 Euler Trail

Suppose that G be the graph. A trail in G is said to be an Euler trail if it contains every edge of G exactly once. So every Euler tour is a closed Euler Trail.

Consider the graph G as below. One Euler trail in the graph G is given as

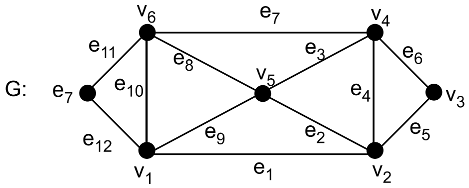
$$v_1\, e_1\, v_2\, e_2\, v_5\, e_3\, v_4\, e_4\, v_2\, e_5\, v_3\, e_6\, v_4\, e_7\, v_6\, e_8\, v_5\, e_9\, v_1\, e_{10}\, v_6\ .$$



Consider another graph G as below. In the graph G the closed Euler trail is given as

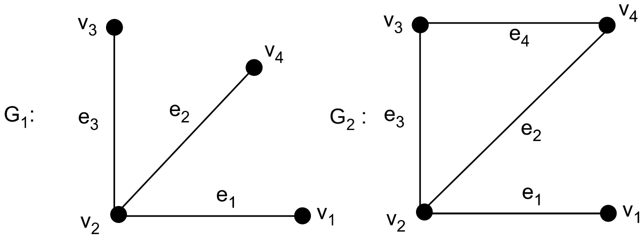
$$v_1\, e_1\, v_2\, e_2\, v_5\, e_3\, v_4\, e_6 v_3\, e_5\, v_2\, e_4\, v_4\, e_7\, v_6\, e_8\, v_5\, e_9\, v_1\, e_{10}\, v_6\, e_{11}\, v_7\, e_{12}\, v_1.$$

This is known as an Euler Tour.



■ 11.15 HAMILTONIAN PATH

A path of a graph G(V, E) which contains every vertex of G exactly once is known as Hamiltonian path. Consider the following graphs

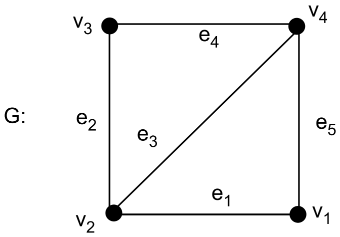


The graph G_1 has no Hamiltonian path where as G_2 has a Hamiltonian path, *i.e.*

$$v_1 \, e_1 \, v_2 \, e_3 \, v_3 \, e_4 \, v_4 \, .$$

11.15.1 Hamiltonian Graph

A cycle in a graph G, which contains every vertex of G only once, is known as a Hamiltonian cycle. It is to be noted that no vertex of a cycle is repeated apart from the final vertex, which is same as the starting vertex. A graph G is said to be Hamiltonian if it has a Hamiltonian cycle. Consider the graph G as

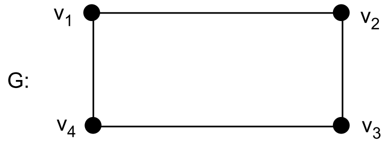


The Hamiltonian cycle is $v_1 \, e_1 \, v_2 \, e_2 \, v_3 \, e_4 \, v_4 \, e_5 \, v_1$. Therefore, the graph G is a Hamiltonian graph.

■ 11.16 CLOSURE OF A GRAPH

Let G be a simple graph. If there are two non-adjacent vertices u_1 and v_1 in G such that $d(u_1) + d(v_1) \geq n$ (number of vertices in G) then join u_1 and v_1 by an edge to get the super graph G_1 of G. Continue this process recursively joining pairs of non-adjacent vertices whose degree sum is at least n until no such pair remains. The final super graph thus obtained is called the closure of G denoted by C(G).

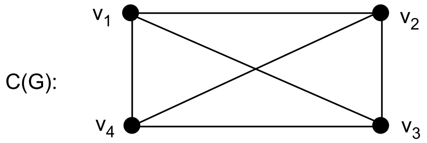
Consider the graph G as



Here, V = { v_1, v_2, v_3, v_4 } and $n = 4$ (number of vertices). Now for the non-adjacent vertices v_1 and v_3 we get

$$d(v_1) + d(v_3) = 2 + 2 = 4 \geq n = 4.$$

Therefore, there exists an edge between v_1 and v_3. Similarly, for the non adjacent vertices v_2 and v_4 we get $d(v_2) + d(v_4) = 2 + 2 = 4 \geq 4 = n$. So, there exists an edge between v_2 and v_4. Thus, the final super graph is given as below. This is nothing but the closure of G, *i.e.* C(G).



■ 11.17 TRAVELLING SALESMAN PROBLEM

The job of a travelling salesman is to visit all the towns linked with roads in a particular territory. He has to visit all the towns exactly once in such a manner that the total distance travelled by himself will be minimum.

In graph theory we denote nodes as towns joined by a weighted edge if and only if road connects them which does not pass through any of the other towns. In travelling salesman problem, we have to construct a minimum Hamiltonian cycle. The following algorithms provide minimum Hamiltonian cycle in case of a complete weighted graph.

(*i*) Two optimal Algorithm and
(*ii*) Closest insertion Algorithm

11.17.1 Two Optimal Algorithm

Suppose that G(V, E) be a complete weighted graph. Where V{$v_1, v_2, \ldots, v_n$}. Here we choose a Hamiltonian cycle C and perform a sequence of modifications to C to find a smaller weight. The following steps are used in two optimal algorithm.

1. Let C = $v_1 v_2 \ldots\ldots v_n v_1$ be a Hamiltonian cycle of the complete weighted graph G. Calculate the weight w of C by the relation

$$w = w(v_1, v_2) + w(v_2, v_3) + \ldots\ldots + w(v_n, v_1).$$

Where, $w(v_i, v_j)$ denote the weight of the edge joining v_i and v_j.

2. Set $i = 1$
3. Set $j = i + 2$
4. Let C_{ij} denote the Hamiltonian cycle as

$$C_{ij} = v_1 v_2 v_3 \ldots v_i v_j v_{j-1}\, v_{j-2} \ldots v_{i+1}\, v_{j+1} \ldots v_n v_1.$$

Calculate w_{ij} of C_{ij}, where $w_{ij} = w - w(v_i\, v_{i+1}) - w(v_j\, v_{j+1}) + w(v_i\, v_j) + w(v_{i+1}\, v_{j+1})$.

5. If $w_{ij} < w$, then replace C by C_{ij} and w by w_{ij}. Also relabel the vertices of C_{ij} in the order $v_1 v_2 v_3 \ldots\ldots v_n v_1$; else go to step 6.
6. Set $j = (j + 1)$. If $j \leq n$, go to step 4 else set $i = (i + 1)$.
7. If $i \leq (n - 2)$, go to step 3 else stop.

11.17.2 The Closest Insertion Algorithm

In this algorithm we gradually build up a sequence of cycles in the graph which involve more and more vertices until all the vertices are chosen up. In this case one more vertex is inserted into the cycle each time in cheapest possible way. The description uses the idea of the distance of a vertex v from a walk W. The following steps are used in this algorithm.

1. Choose any vertex v_1 as a starting vertex.
2. Choose the 2nd vertex v_2 which is closest to v_1 from the $(n - 1)$ vertices not chosen so far. Let $w_2 = v_1v_2v_1$ denote the walk.
3. Choose the 3rd vertex v_3 which is closest to the walk $w_2 = v_1v_2v_1$ from the $(n - 2)$ vertices not chosen so far. Let $w_3 = v_1v_2v_3v_1$ denote the walk.
4. Choose the 4th vertex v_4 which is closest to the walk $w_3 = v_1v_2v_3v_1$ from the $(n - 3)$ vertices not chosen so far. Find the shortest walk from the walks $v_1\, v_2\, v_3\, v_4\, v_1$; $v_1\, v_2\, v_4\, v_3\, v_1$; $v_1\, v_4\, v_2\, v_3\, v_1$. Let w_4 denote the shortest walk. Relabel the vertices as $v_1\, v_2\, v_3\, v_4\, v_1$ if necessary.
5. Choose the 5th vertex v_5 which is closest to the walk w_4 from the $(n - 4)$ vertices not chosen so far. Find the shortest walk from the walks $v_1\, v_2\, v_3\, v_4\, v_5\, v_1$; $v_1\, v_2\, v_3\, v_5\, v_4\, v_1$; $v_1\, v_2\, v_5\, v_3\, v_4\, v_1$; $v_1\, v_5\, v_2\, v_3\, v_4\, v_1$. Let w_5 denote the shortest walk. Relabel the vertices as $v_1\, v_2\, v_3\, v_4\, v_5\, v_1$ if necessary.
6. The process is being repeated until all the vertices are included in the cycle. Therefore the walk w_n is the Hamiltonian cycle of the graph G.

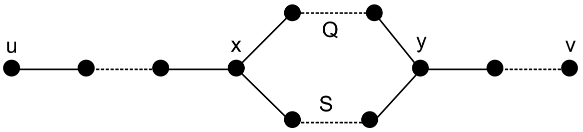
Note: Both the algorithms *i.e.* Two optimal algorithm and Closest insertion algorithm provide reasonably good solutions. Therefore, both are approximately optimal.

SOLVED EXAMPLES

Example 1 *If u and v are distinct vertices of a tree T, then T contains exactly one u – v path.*

Solution : Suppose, to the contrary, the tree T contains two $u - v$ paths. Let us assume that the two $u - v$ paths are Q and S.

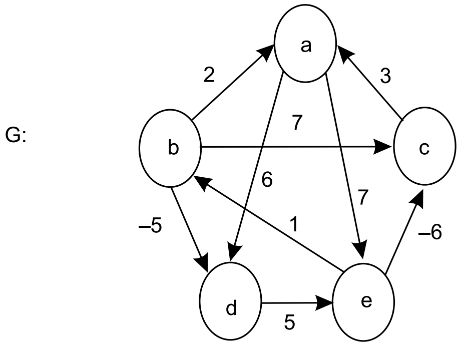
Since Q and S are different $u - v$ paths, there must exists a vertex x belonging to both Q and S such that the vertex immediately following x on Q is different from the vertex immediately following x on S. This can be easily understandable from the figure shown below.



Let us assume that y be the first vertex of Q following x, which also belongs to S. This implies that there exists two $x - y$ paths that have only x and y in common. It is clear that these two paths produce a cycle in T. This is a contradiction. This contradict to the fact that T is a tree.

Therefore, our supposition is wrong. Hence, T has only one $u - v$ path.

Example 2 *For the following weighted graph G apply Floyd-Warshall algorithm to find the shortest path between any pair of vertices a, b, c, d and e. Show at least one iteration in details.*



Solution : The adjacency matrix W with respect to the nodes b, a, c, e

and d is given as $\begin{pmatrix} 0 & 2 & 7 & \infty & -5 \\ \infty & 0 & \infty & 7 & 6 \\ \infty & 3 & 0 & \infty & \infty \\ 1 & \infty & -6 & 0 & \infty \\ \infty & \infty & \infty & 5 & 0 \end{pmatrix}$

Hence, $n = \text{Row}[\text{W}] = 5$

$$\text{D}^{(0)} = \left(d_{ij}^{(0)}\right) = \begin{pmatrix} 0 & 2 & 7 & \infty & -5 \\ \infty & 0 & \infty & 7 & 6 \\ \infty & 3 & 0 & \infty & \infty \\ 1 & \infty & -6 & 0 & \infty \\ \infty & \infty & \infty & 5 & 0 \end{pmatrix}$$

For $k = 1$, $i = 1$ and $j = 1$ to 5 we get

$$d_{11}^{1} = \text{Min}(d_{11}^{0}, d_{11}^{0} + d_{11}^{0}) = \text{Min}(0, 0+0) = 0$$
$$d_{12}^{1} = \text{Min}(d_{12}^{0}, d_{11}^{0} + d_{12}^{0}) = \text{Min}(2, 0+2) = 2$$
$$d_{13}^{1} = \text{Min}(d_{13}^{0}, d_{11}^{0} + d_{13}^{0}) = \text{Min}(7, 0+7) = 7$$
$$d_{14}^{1} = \text{Min}(d_{14}^{0}, d_{11}^{0} + d_{14}^{0}) = \text{Min}(\infty, 0+\infty) = \infty$$
$$d_{15}^{1} = \text{Min}(d_{15}^{0}, d_{11}^{0} + d_{15}^{0}) = \text{Min}(-5, 0-5) = -5$$

For $k = 1$, $i = 2$ and $j = 1$ to 5 we get

$$d_{21}^{1} = \text{Min}(d_{21}^{0}, d_{21}^{0} + d_{11}^{0}) = \text{Min}(\infty, \infty+0) = \infty$$
$$d_{22}^{1} = \text{Min}(d_{22}^{0}, d_{21}^{0} + d_{12}^{0}) = \text{Min}(0, \infty+2) = 0$$
$$d_{23}^{1} = \text{Min}(d_{23}^{0}, d_{21}^{0} + d_{13}^{0}) = \text{Min}(\infty, \infty+7) = \infty$$
$$d_{24}^{1} = \text{Min}(d_{24}^{0}, d_{21}^{0} + d_{14}^{0}) = \text{Min}(7, \infty+\infty) = 7$$
$$d_{25}^{1} = \text{Min}(d_{25}^{0}, d_{21}^{0} + d_{15}^{0}) = \text{Min}(6, \infty-5) = 6$$

For $k = 1$, $i = 3$ and $j = 1$ to 5 we get

$$d_{31}^{1} = \text{Min}(d_{31}^{0}, d_{31}^{0} + d_{11}^{0}) = \text{Min}(\infty, \infty + 0) = \infty$$

$$d_{32}^{1} = \text{Min}(d_{32}^{0}, d_{31}^{0} + d_{12}^{0}) = \text{Min}(3, \infty + 2) = 3$$

$$d_{33}^{1} = \text{Min}(d_{33}^{0}, d_{31}^{0} + d_{13}^{0}) = \text{Min}(0, \infty + 7) = 0$$

$$d_{34}^{1} = \text{Min}(d_{34}^{0}, d_{31}^{0} + d_{14}^{0}) = \text{Min}(\infty, \infty + \infty) = \infty$$

$$d_{35}^{1} = \text{Min}(d_{35}^{0}, d_{31}^{0} + d_{15}^{0}) = \text{Min}(\infty, \infty - 5) = \infty$$

For $k = 1$, $i = 4$ and $j = 1$ to 5 we get

$$d_{41}^{1} = \text{Min}(d_{41}^{0}, d_{41}^{0} + d_{11}^{0}) = \text{Min}(1, 1 + 0) = 1$$

$$d_{42}^{1} = \text{Min}(d_{42}^{0}, d_{41}^{0} + d_{12}^{0}) = \text{Min}(\infty, 1 + 2) = 3$$

$$d_{43}^{1} = \text{Min}(d_{43}^{0}, d_{41}^{0} + d_{13}^{0}) = \text{Min}(-6, 1 + 7) = -6$$

$$d_{44}^{1} = \text{Min}(d_{44}^{0}, d_{41}^{0} + d_{14}^{0}) = \text{Min}(0, 1 + \infty) = 0$$

$$d_{45}^{1} = \text{Min}(d_{45}^{0}, d_{41}^{0} + d_{15}^{0}) = \text{Min}(\infty, 1 - 5) = -4$$

For $k = 1$, $i = 5$ and $j = 1$ to 5 we get

$$d_{51}^{1} = \text{Min}(d_{51}^{0}, d_{51}^{0} + d_{11}^{0}) = \text{Min}(\infty, \infty + 0) = \infty$$

$$d_{52}^{1} = \text{Min}(d_{52}^{0}, d_{51}^{0} + d_{12}^{0}) = \text{Min}(\infty, \infty + 2) = \infty$$

$$d_{53}^{1} = \text{Min}(d_{53}^{0}, d_{51}^{0} + d_{13}^{0}) = \text{Min}(\infty, \infty + 7) = \infty$$

$$d_{54}^{1} = \text{Min}(d_{54}^{0}, d_{51}^{0} + d_{14}^{0}) = \text{Min}(5, \infty + \infty) = 5$$

$$d_{55}^{1} = \text{Min}(d_{55}^{0}, d_{51}^{0} + d_{15}^{0}) = \text{Min}(0, \infty - 5) = 0$$

Therefore, we have

$$D^{(1)} = \begin{pmatrix} 0 & 2 & 7 & \infty & -5 \\ \infty & 0 & \infty & 7 & 6 \\ \infty & 3 & 0 & \infty & \infty \\ 1 & 3 & -6 & 0 & -4 \\ \infty & \infty & \infty & 5 & 0 \end{pmatrix}$$

Similarly for $k = 2$, $i = 1$ to 5 and $j = 1$ to 5 we get

$$D^{(2)} = \begin{pmatrix} 0 & 2 & 7 & 9 & -5 \\ \infty & 0 & \infty & 7 & 6 \\ \infty & 3 & 0 & 10 & 9 \\ 1 & 3 & -6 & 0 & -4 \\ \infty & \infty & \infty & 5 & 0 \end{pmatrix}$$

Similarly for $k = 3$, $i = 1$ to 5 and $j = 1$ to 5 we get

$$D^{(3)} = \begin{pmatrix} 0 & 2 & 7 & 9 & -5 \\ \infty & 0 & \infty & 7 & 6 \\ \infty & 3 & 0 & 10 & 9 \\ 1 & -3 & -6 & 0 & -4 \\ \infty & \infty & \infty & 5 & 0 \end{pmatrix}$$

Similarly for $k = 4$, $i = 1$ to 5 and $j = 1$ to 5 we get

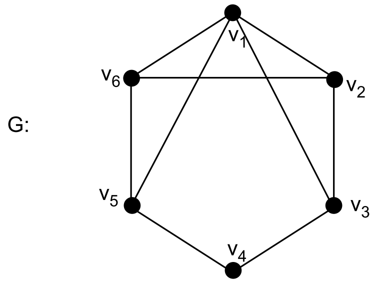
$$D^{(4)} = \begin{pmatrix} 0 & 2 & 3 & 9 & -5 \\ 8 & 0 & 1 & 7 & 3 \\ 11 & 3 & 0 & 10 & 6 \\ 1 & -3 & -6 & 0 & -4 \\ 6 & 2 & -1 & 5 & 0 \end{pmatrix}$$

Similarly for $k = 5$, $i = 1$ to 5 and $j = 1$ to 5 we get

$$D^{(5)} = \begin{pmatrix} 0 & -3 & -6 & 0 & -5 \\ 8 & 0 & 1 & 7 & 3 \\ 11 & 3 & 0 & 10 & 6 \\ 1 & -3 & -6 & 0 & -4 \\ 6 & 2 & -1 & 5 & 0 \end{pmatrix}$$

From the above matrix, the shortest distance for any pair of vertices can be found out.

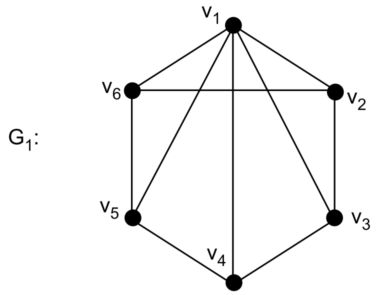
Example 3 *Find the closure of the graph G where*



Solution : In the above graph G we have V = $\{v_1, v_2, v_3, v_4, v_5, v_6\}$ and number of vertices $(n) = 6$. Now for the non adjacent vertices v_1 and v_4 we have

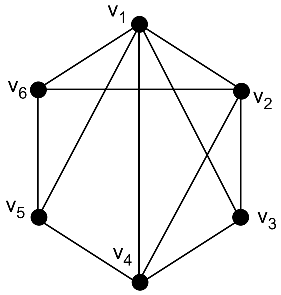
$$d(v_1) + d(v_4) = 4 + 2 = 6 \geq n = 6.$$

Therefore, there exists an edge between v_1 and v_4. Let the super graph G_1 be



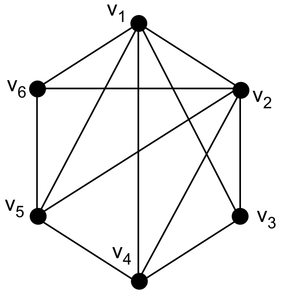
For the non-adjacent vertices v_2 and v_4 we have $d(v_2) + d(v_4) = 3 + 3 = 6 \geq n$. Therefore, there exists an edge between v_2 and v_4 . Let the super graph G_2 be

G$_2$:



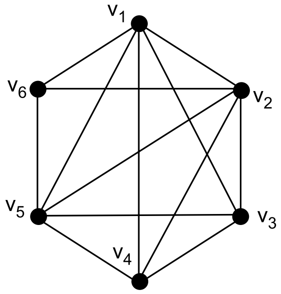
Again, v_2 and v_5 are non-adjacent such that $d(v_2) + d(v_5) = 4 + 3 = 7 \geq n = 6$. Therefore, there exists an edge between v_2 and v_5. Let the super graph G$_3$ be

G$_3$:



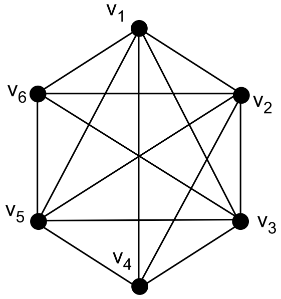
For the non-adjacent vertices v_3 and v_5 we have $d(v_3) + d(v_5) = 3 + 4 = 7 \geq n$. Therefore, there exists an edge between v_3 and v_5. Let the super graph G$_4$ be

G$_4$:

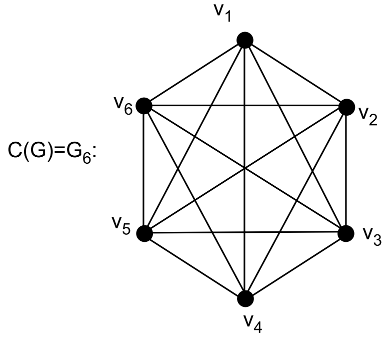


For the non-adjacent vertices v_3 and v_6 we have $d(v_3) + d(v_6) = 4 + 3 = 7 \geq n$. Therefore, there exists an edge between v_3 and v_6 . Let the super graph G$_5$ be.

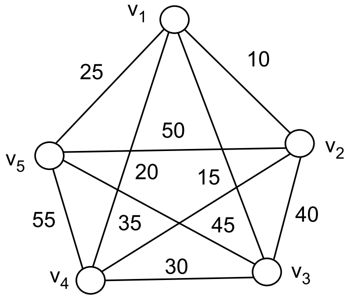
G$_5$:



For the non-adjacent vertices v_4 and v_6 we have $d(v_4) + d(v_6) = 4 + 4 = 8 \geq n$. Therefore, there exists an edge between v_4 and v_6 . Let the super graph be G$_6$. In the above graph, there is no two non-adjacent vertices. Thus, G$_6$ is the final super graph. Therefore, the closure of the graph G is given as



Example 4 *For the following travelling salesman problem, carry out the closest insertion algorithm.*



Solution : Given that the complete weighted graph G as

1. Choose the vertex v_1
2. Choose the vertex v_2, which is closest to v_1. So, $w_2 = v_1\, v_2\, v_1$
3. Choose the vertex v_3, which is close to w_2. So, $w_3 = v_1\, v_2\, v_3\, v_1$
4. Choose the vertex v_4, which is close to w_3. Hence, we have the following cases.

$$\begin{aligned} w_4 &= v_1\, v_2\, v_3\, v_4\, v_1 \text{ or} \\ &= v_1\, v_2\, v_4\, v_3\, v_1 \text{ or} \\ &= v_1\, v_4\, v_2\, v_3\, v_1 \end{aligned}$$

Now length of $v_1\, v_2\, v_3\, v_4\, v_1 = 10 + 40 + 30 + 20 = 100$

Length of $v_1\, v_2\, v_4\, v_3\, v_1 = 10 + 45 + 30 + 15 = 100$

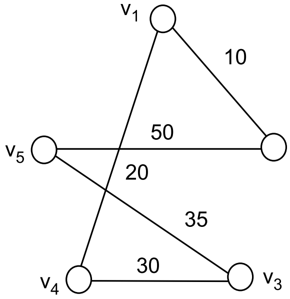
Length of $v_1\, v_4\, v_2\, v_3\, v_1 = 20 + 45 + 40 + 15 = 120$

Therefore, $w_4 = v_1\, v_2\, v_3\, v_4\, v_1$ is minimum.

5. Choose the vertex v_5, which is close to w_4. Hence, we have the following cases. The length of following cycles is given as below.

$$v_1\, v_2\, v_3\, v_4\, v_5\, v_1 = 10 + 40 + 30 + 55 + 25 = 160$$
$$v_1\, v_2\, v_3\, v_5\, v_4\, v_1 = 10 + 40 + 35 + 55 + 20 = 160$$
$$v_1\, v_2\, v_5\, v_3\, v_4\, v_1 = 10 + 50 + 35 + 30 + 20 = 145$$
$$v_1\, v_5\, v_2\, v_3\, v_4\, v_1 = 25 + 50 + 40 + 30 + 20 = 165$$

As all the vertices are included in the cycle, so the process terminates. Hence , the shortest Hamiltonian cycle is given as $v_1\, v_2\, v_5\, v_3\, v_4\, v_1$.



Example 5 *For the travelling salesman problem given in example 4, carry out the two optimal algorithm.*

Solution : For the complete weighted graph G given above, the number of vertices (n) = 5. According to the two optimal algorithm we have the following steps.

1. Let C = $v_1, v_2, v_3, v_4, v_5, v_1$ be a Hamiltonian cycle.
Therefore, we get

$$w = w(v_1v_2) + w(v_2v_3) + w(v_3v_4) + w(v_4v_5) + w(v_5v_1)$$
$$= 10 + 40 + 30 + 55 + 25 = 160$$

2. Set $i = 1$

3. Set $j = i + 2 = 3$

4. Set $C_{ij} = C_{13} = v_1\, v_3\, v_2\, v_4\, v_5\, v_1$

$$w_{13} = w - w(v_1v_2) - w(v_3v_4) + w(v_1v_3) + w(v_2v_4)$$
$$= 160 - 10 - 30 + 15 + 45 = 180$$

5. As $w_{13} \nless w$; Go to step 6.

6. Set $j = (j + 1) = 4$ and $4 \leq n = 5$. Go to step 4.

4. Set $C_{ij} = C_{14} = v_1\, v_4\, v_3\, v_2\, v_5\, v_1$

$$w_{14} = w - w(v_1v_2) - w(v_4v_5) + w(v_1v_4) + w(v_2v_5) = 165$$

5. As $w_{14} = 165 \nless 160 = w$; Go to step 6.

6. Set $j = (j + 1) = 5$ and $5 \leq n = 5$. Go to step 4.

4. Set $C_{ij} = C_{15} = v_1\, v_5\, v_4\, v_3\, v_2\, v_1$

$$w_{15} = w - w(v_1v_2) - w(v_5v_1) + w(v_1v_5) + w(v_2v_1) = 160$$

5. As $w_{15} = 160 \nless 160 = w$; Go to step 6

6. Set $j = (j + 1) = 6$ and $6 \nless n = 5$. Go to step 7 with $i = (i + 1) = 2$.

7. As $i = 2 \leq (n - 2) = 3$, Go to step 3.

3. Set $j = (i + 2) = 2 + 2 = 4$

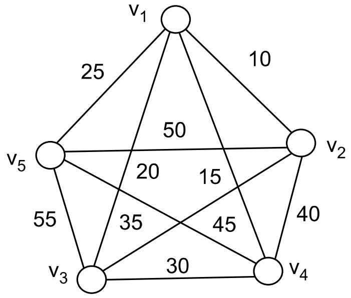
4. Set $C_{ij} = C_{24} = v_1\, v_2\, v_4\, v_3\, v_5\, v_1$

$$W_{24} = w - w(v_2\, v_3) - w(v_4\, v_5) + w(v_2\, v_4) + w(v_3\, v_5) = 145$$

5. As $w_{24} = 145 < 160 = w$; go to step 1

1. C = $C_{24} = v_1\, v_2\, v_4\, v_3\, v_5\, v_1$ with $w = w_{24} = 145$.
After re-labeling the vertices we have

$$C = C_{24} = v_1\, v_2\, v_3\, v_4\, v_5\, v_1.$$



2. Set $i = 1$

3. Set $j = (i + 2) = 3$

4. Set $C_{ij} = C_{13} = v_1\, v_3\, v_2\, v_4\, v_5\, v_1$
$$w_{13} = w - w(v_1 v_2) - w(v_3 v_4) + w(v_1 v_3) + w(v_2 v_4) = 165$$

5. As $w_{13} = 165 \nless 145 = w$; go to step 6

6. Set $j = (j + 1) = 4$ and $4 \le n = 5$. Go to step 4

4. Set $C_{ij} = C_{14} = v_1\, v_4\, v_3\, v_2\, v_5\, v_1$
$$w_{14} = w - w(v_1 v_2) - w(v_4 v_5) + w(v_1 v_4) + w(v_2 v_5) = 165$$

5. As $w_{14} = 165 \nless 145 = w$; go to step 6

6. Set $j = (j + 1) = 5$ and $5 \le n = 5$. Go to step 4

4. Set $C_{ij} = C_{15} = v_1\, v_5\, v_4\, v_3\, v_2\, v_1$
$$w_{15} = w - w(v_1 v_2) - w(v_5 v_1) + w(v_1 v_5) + w(v_2 v_1) = 145$$

5. As $w_{15} = 145 \nless 145 = w$; go to step 6

6. Set $j = (j + 1) = 6 \nless n = 5$ with $i = (i + 1) = 2$.

7. As $i = 2 \le (n - 2) = 3$, Go to step 3

3. Set $j = (i + 2) = 2 + 2 = 4$

4. Set $C_{ij} = C_{24} = v_1\, v_2\, v_4\, v_3\, v_5\, v_1$
$$w_{24} = w - w(v_2 v_3) - w(v_4 v_5) + w(v_2 v_4) + w(v_3 v_5) = 160$$

5. As $w_{24} = 160 \nless 145 = w$; go to step 6

6. Set $j = (j + 1) = 5 \le 5 = n$, go to step 4

4. Set $C_{ij} = C_{25} = v_1\, v_2\, v_5\, v_4\, v_3\, v_1$
$$w_{25} = w - w(v_2 v_3) - w(v_5 v_1) + w(v_2 v_5) + w(v_3 v_1) = 145$$

5. As $w_{25} = 145 \nless 145 = w$; go to step 6

6. Set $j = (j + 1) = 6 \nless n = 5$ with $i = (i + 1) = 3$. go to step 7

7. As $i = 3 \le (n - 2) = 3$, go to step 3

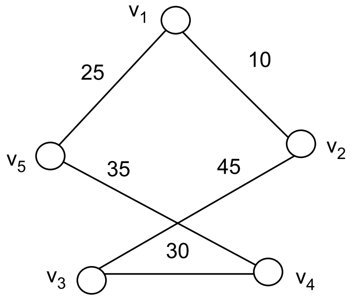
3. Set $j = (i + 2) = 5$

4. Set $C_{ij} = C_{35} = v_1\, v_2\, v_3\, v_5\, v_4\, v_1$
$$w_{35} = w - w(v_3 v_4) - w(v_5 v_1) + w(v_3 v_5) + w(v_4 v_1) = 160$$

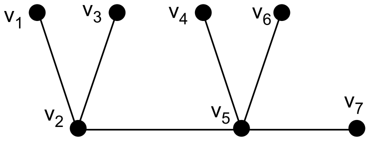
5. As $w_{35} = 160 \nless 145 = w$; go to step 6

6. Set $j = (j + 1) = 6 \nless n = 5$ with $i = (i + 1) = 4$, go to step 7

7. As $i = 4 \nless (n - 2) = 3$, therefore the process terminates. Hence, the minimum Hamiltonian path is given as $v_1\, v_2\, v_3\, v_4\, v_5\, v_1$. The path for travelling salesman is given below.



Example 6 *Find the eccentricity of all vertices, radius, diameter and centre of the graph given below. It is given that the distance between any two adjacent vertices is 1.*



Solution : In the graph given above V = $\{v_1, v_2, v_3, v_4, v_5, v_6, v_7\}$. It is also given that length of each edge is 1. Now,

$d(v_1, v_2) = 1$; $d(v_1, v_3) = 2$; $d(v_1, v_4) = 3$;
$d(v_1, v_5) = 2$; $d(v_1, v_6) = 3$; $d(v_1, v_7) = 3$;

Therefore, $e(v_1) = \text{Max } \{1, 2, 3\} = 3$.

Similarly, we get

$d(v_2, v_1) = 1$; $d(v_2, v_3) = 1$; $d(v_2, v_4) = 2$;
$d(v_2, v_5) = 1$; $d(v_2, v_6) = 2$; $d(v_2, v_7) = 2$;

Therefore, $e(v_2) = \text{Max } \{1, 2\} = 2$.

Proceeding in this way we get

$e(v_3) = 3; e(v_4) = 3;\ e(v_5) = 2;\ e(v_6) = 3;\ e(v_7) = 3.$

Now, radius = rad (G) = Min $\{e(v): v \in \text{V}\}$ = Min (2, 3) = 2.

Diameter = diam (G) = Max $\{e(v): v \in \text{V}\}$ = Max (2, 3) = 3.

So, the central points are v_2, v_5 and centre $\{v_2, v_5\}$.

Example 7 *Let T be a tree of order p and size q having p_i vertices of degree i (i = 1, 2, 3, ...).*

Let $$\sum_i p_i = p \text{ and } \sum_i ip_i = 2q = 2(p-1).$$

Show that $$p_1 = p_3 + 2p_4 + 3p_5 + 4p_6 + \ldots + 2.$$.

Solution : Given that T is a tree of order p and size q. It is also given that

$$\sum_i p_i = p \text{ and } \sum_i ip_i = 2(p-1)$$

i.e. $p_1 + 2p_2 + 3p_3 + 4p_4 + \ldots 2(p-1) = 2p - 2$

i.e. $$p_1 + 2p_2 + 3p_3 + 4p_4 + \ldots = 2\sum_i p_i - 2$$

i.e. $p_1 + 2p_2 + 3p_3 + 4p_4 + \ldots = 2(p_1 + p_2 + p_3 + \ldots) - 2$

i.e. $p_1 = p_3 + 2p_4 + 3p_5 + 4p_6 + \ldots + 2.$

Example 8 *If T is a binary tree of height h and order p, then*

$$(h + 1) \le p \le 2^{(h+1)} - 1$$

Solution : Let p_k denote the number of vertices of T at level k for $0 \le k \le h$.

Therefore, we get

$$\sum_{k=0}^{h} p_k = p$$

Since $p_k \ge 1$ for each k, and $p_k \le 2p_{(k-1)}$ for $1 \le k \le h$, it follows, inductively, that $p_k \le 2^k$. Again,

$$\sum_{k=0}^{h} 2^k = 1 + 2 + 2^2 + 2^3 + \ldots + 2^h = 2^{h+1} - 1$$

Again, $$\sum_{k=0}^{h} p_k \le \sum_{k=0}^{h} 2^k = 2^{h+1} - 1$$

i.e. $$p \le 2^{h+1} - 1 \qquad \ldots (i)$$

Also, $$\sum_{k=0}^{h} 1 \le \sum_{k=0}^{h} p_k = p$$

i.e. $$(h + 1) \le p \qquad \ldots (ii)$$

On combining equations (*i*) and (*ii*) we get

$$(h + 1) \le p \le 2^{h+1} - 1.$$

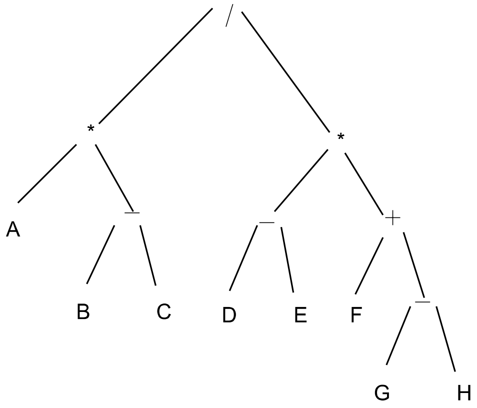
Example 9 *Construct the binary tree for the arithmetic expression*

(A(B – C))/((D – E)(F + G – H)).

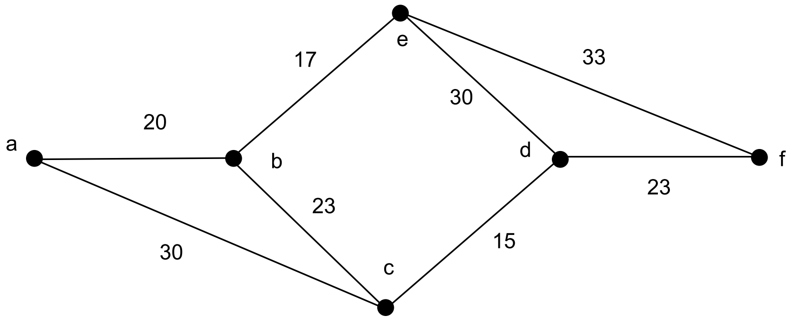
Solution : Given arithmetic expression is

(A(B – C))/((D – E)(F + G – H)).

The binary tree corresponding to the above expression is given below.



Example 10 *For the graph G shown below, use Dijkstra's algorithm to compute the shortest path between a and f.*



Solution : In the above graph G, the source vertex is

$v_s = a$ and $v_t = f$. Set $\lambda(a) = 0$

and $\lambda(b) = \lambda(c) = \lambda(d) = \lambda(e) = \lambda(f) = \infty$. T = V = $\{a, b, c, d, e, f\}$.

Hence, we have the following table

Vertex	a	b	c	d	e	f
$\lambda(v)$	0	∞	∞	∞	∞	∞
T	a	b	c	d	e	f

Now, $u = a$ as $\lambda(u) = \lambda(a) = 0$

which is minimum.

The edges incident on $u = a$ are ab and ac.

Therefore,
$$\lambda(b) = \text{Min } [\lambda(b), \lambda(a) + w(ab)]$$
$$= \text{Min } [\infty, 20] = 20.$$
$$\lambda(c) = \text{Min } [\lambda(c), \lambda(a) + w(ac)]$$
$$= \text{Min } [\infty, 30] = 30.$$

Again, T = T– $\{u = a\} = \{b, c, d, e, f\}$.

Therefore, we have the following table

Vertex	a	b	c	d	e	f
$\lambda(v)$	0	20	30	∞	∞	∞
T		b	c	d	e	f

Now, $u = b$ as $\lambda(u) = \lambda(b) = 20$

which is minimum.

The edges incident with $u = b$ are bc and be. Therefore,
$$\lambda(c) = \text{Min } [\lambda(c), \lambda(b) + w(bc)]$$
$$= \text{Min } [30, 43] = 30.$$
$$\lambda(e) = \text{Min } [\lambda(e), \lambda(b) + w(be)]$$
$$= \text{Min } [\infty, 37] = 37.$$

Again, T = T – $\{u = b\}$ =$\{c, d, e, f\}$.

Thus, we have the following table

Vertex	a	b	c	d	e	f
$\lambda(v)$	0	20	30	∞	37	∞
T			c	d	e	f

Now, $u = c$ as $\lambda(u) = \lambda(c) = 30$ which is minimum.

The edges incident with $u = c$ is cd.

Therefore,
$$\lambda(d) = \text{Min } [\lambda(d), \lambda(c) + w(cd)]$$
$$= \text{Min } [\infty, 45] = 45.$$

Again, $\text{T} = \text{T} - \{u = c\} = \{d, e, f\}$.

Thus, we have the following table

Vertex	a	b	c	d	e	f
$\lambda(v)$	0	20	30	45	37	∞
T				d	e	f

Now, $u = e$ as $\lambda(u) = \lambda(e) = 37$ which is minimum.

The edges incident with $u = e$ are ed and ef.

Therefore,
$$\lambda(d) = \text{Min } [\lambda(d), \lambda(e) + w(ed)]$$
$$= \text{Min } [45, 67] = 45.$$
$$\lambda(f) = \text{Min } [\lambda(f), \lambda(e) + w(ef)]$$
$$= \text{Min } [\infty, 70] = 70.$$

Again, $\text{T} = \text{T} - \{u = e\} = \{d, f\}$.

Thus, we have the following table

Vertex	a	b	c	d	e	f
$\lambda(v)$	0	20	30	45	37	70
T				d		f

Now, $u = d$ as $\lambda(u) = \lambda(d) = 45$ which is minimum.

The edges incident with $u = d$ is df. Therefore,
$$\lambda(f) = \text{Min } [\lambda(f), \lambda(d) + w(df)]$$
$$= \text{Min } [70, 68] = 68.$$

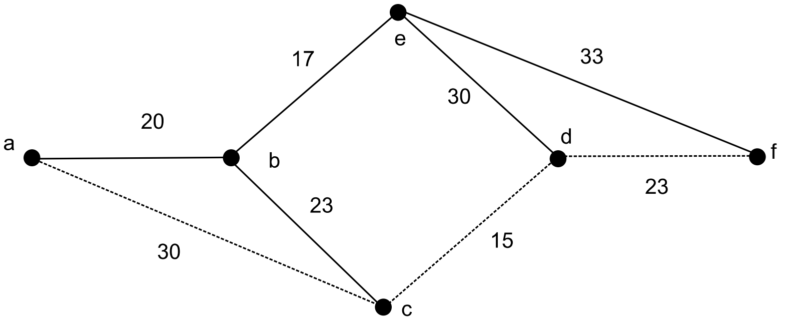
Again, $\text{T} = \text{T} - \{u = d\} = \{f\}$.

Thus, we have the following table

Vertex	a	b	c	d	e	f
$\lambda(v)$	0	20	30	45	37	68
T						f

Now, $u = f$ and f is the terminating node, so the process terminates.

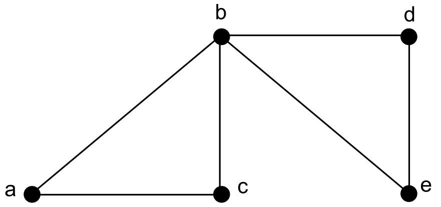
Hence the shortest distances from a to b, c, d, e and f are 20, 30, 45, 37, 68 respectively. The shortest distance between a and f is given in the figure below.



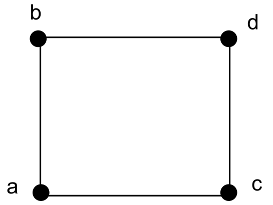
Example 11 *Construct the following graphs*

(a) Eulerian but not Hamiltonian *(b) Hamiltonian but not Eulerian*
(c) Neither Eulerian nor Hamiltonian *(d) Eulerian and Hamiltonian*

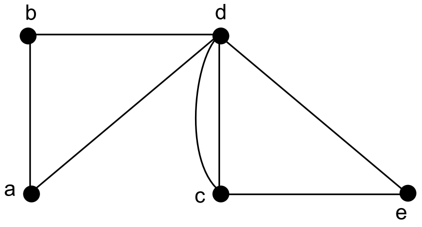
Solution : The different graphs are given below.



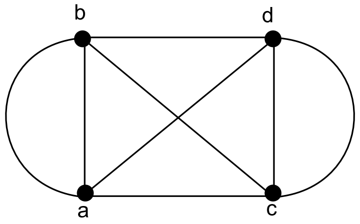
Eulrian but not Hamiltonian



Hamiltonian but not Eulerian

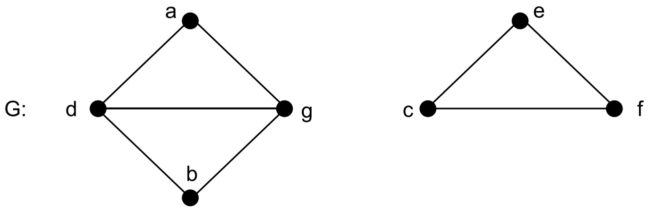


Neiher Eulerian not Hamiltonian

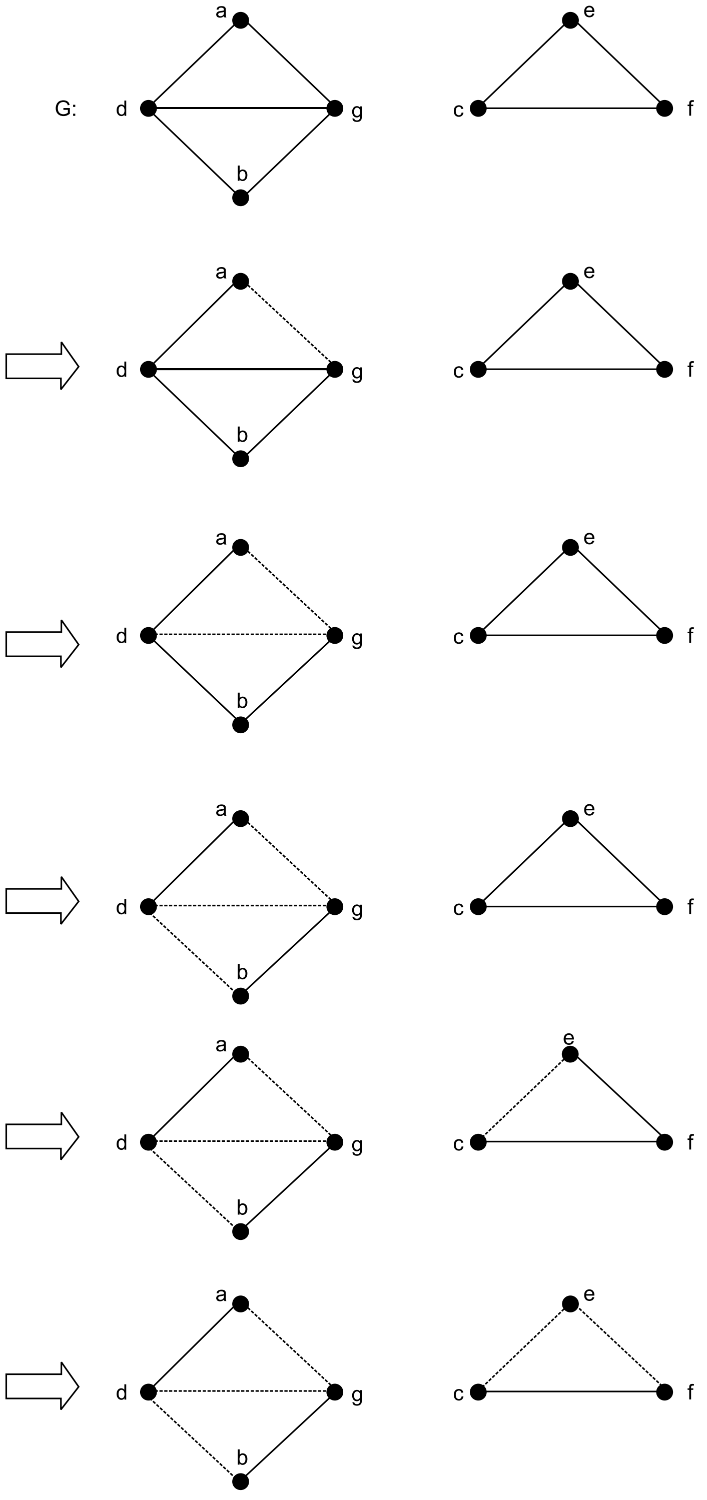


Hamiltonian and Eulerian

Example 12 *For the graph G shown below, find the depth first search forest.*

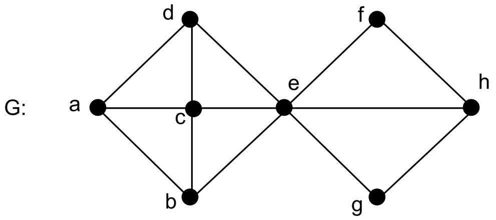


Solution : Let us consider the source vertex as '*a*' in the above graph G. On using the DFS technique, the order in which the vertices are being visited is described below by the sequence of graphs.

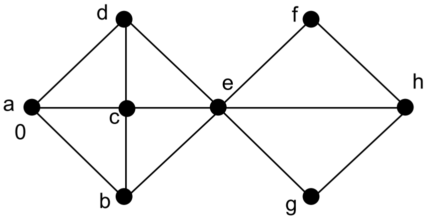


Therefore, the dotted graph shown above is the depth first forest T of the graph G. Besides that there could be several depth first forest from the same vertex '*a*'. This indicates that the depth first forest is not unique.

Example 13 *For the graph G shown below, find the breadth first search tree.*



Solution : Consider the graph G given above. Now we have to find out the shortest path from the source vertex a to the vertex h. On using the BFS technique, we get the following stages.



(Label $(a) = 0$ and set $i = 0$)

In the above figure the adjacent vertices of a are b, c and d. Therefore we get label

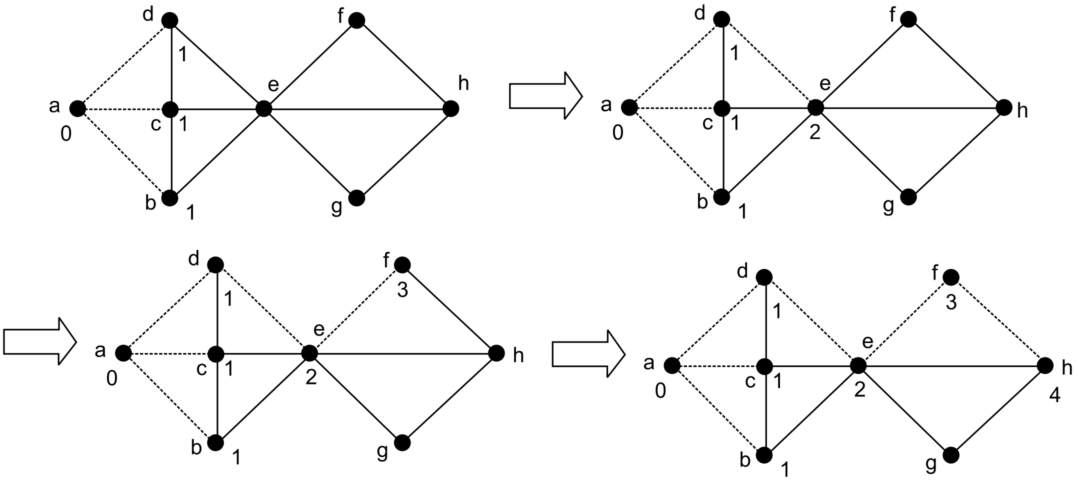
label $(b) = i + 1 = 0 + 1 = 1$;

label $(c) = i + 1 = 0 + 1 = 1$ and label $(d) = i + 1 = 0 + 1 = 1$.

Similarly, the adjacent vertex of d is e.

Therefore we get label $(e) = i + 1 = 1 + 1 = 2$.

Therefore, we have



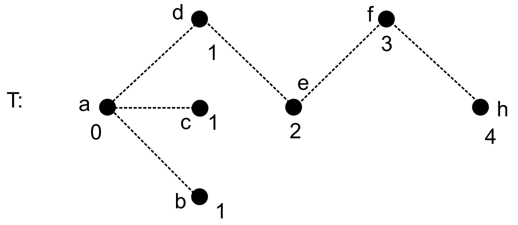
In the above figure, the adjacent vertex of e is f. Therefore we get

label $(f) = i + 1 = 2 + 1 = 3$.

Similarly, the adjacent vertex of f is h. So,

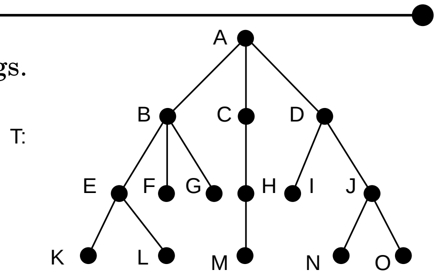
label $(h) = i + 1 = 3 + 1 = 4$.

Therefore, the breadth first search tree is given as below.

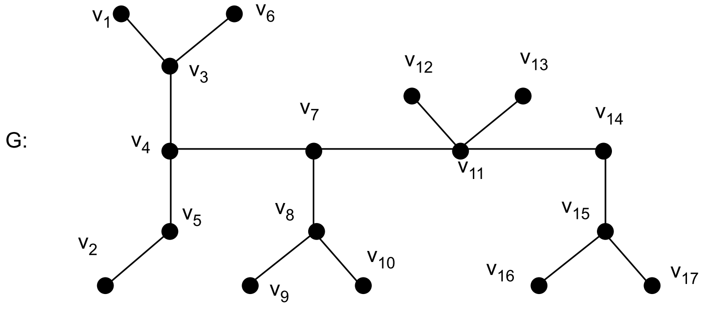


EXERCISES

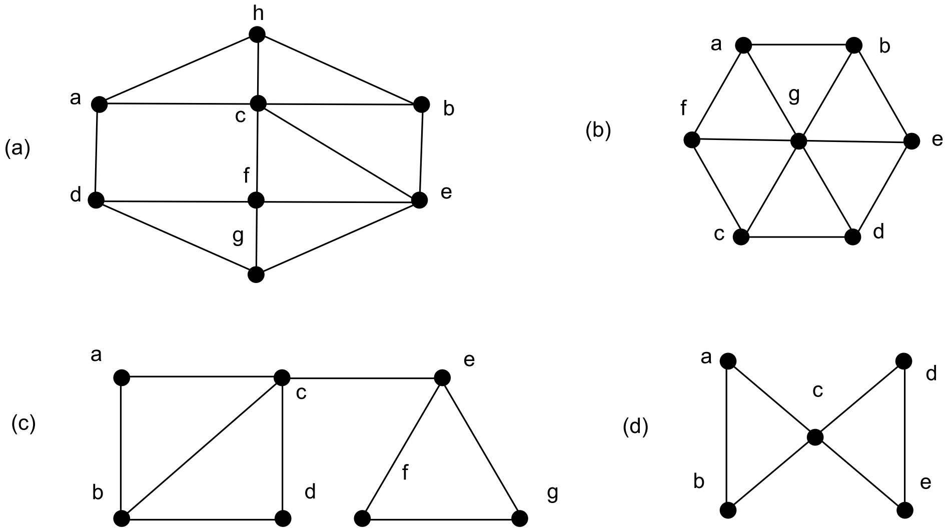
1. With reference to the given tree T find the followings.
   (*a*) Height of the tree
   (*b*) Degree of the tree
   (*c*) Longest path of the tree
   (*d*) Level (L); Level (H); Level (N)
   (*e*) Parent (M); Sibling (B); Child (D)



2. (*a*) Draw all trees of order 5
   (*b*) Draw all trees of order 7 and $\Delta(T) \geq 4$, where $\Delta(T)$ represents maximum degree of tree T.
3. In a binary tree of height h, there are at most 2^{h-1} leaf nodes.
4. If T is a binary tree of height h and order p, then $h \geq \lceil g\,((p+1)/2)\rceil$. The equality holds if T is a balanced complete binary tree.
5. Find the eccentricity of all vertices, radius, diameter and centre of the graph G given below. It is given that the distance between any two adjacent vertices is 1.



6. Construct the following graphs.
   (*a*) Eulerian but not Hamiltonian
   (*b*) Hamiltonian but not Eulerian
   (*c*) Neither Eulerian nor Hamiltonian
   (*d*) Eulerian and Hamiltonian.
7. For the graph G shown below, find the depth-first search tree.

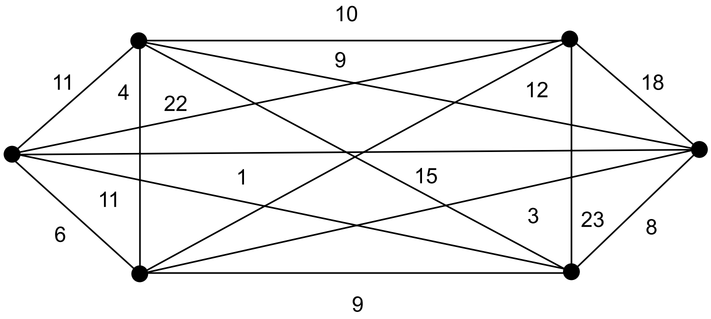


8. For the graphs given on No. 7, find the breadth first search tree.

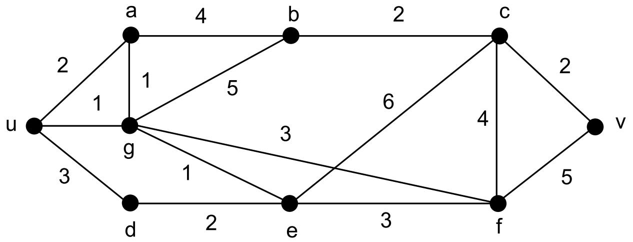
9. Solve the travelling salesman problem for the complete weighted graph G given below by using

(*a*) Closest Insertion algorithm and

(*b*) Two optimal algorithm.



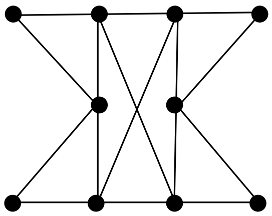
10. Let G be the weighted graph shown below. Use Dijkstra's algorithm to compute the shortest distance between *u* and *v*.



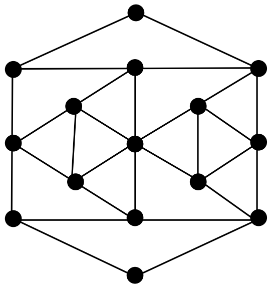
11. Determine which of the graphs given below are Euler graph by using the following algorithms.

(*a*) Fleury's algorithm and (*b*) Hierholzer's algorithm

(a)

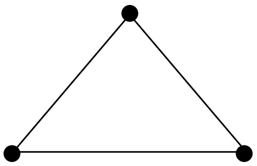


(b)

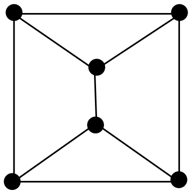


12. Find the closure graph C(G) for the graphs shown below.

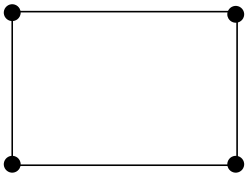
(a)



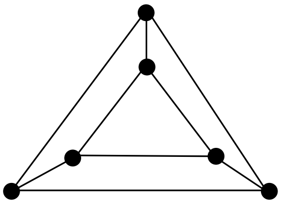
(b)



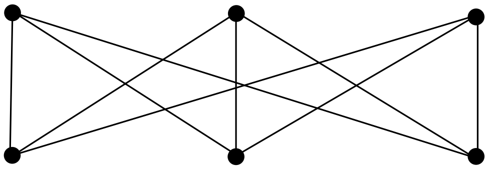
(c)



(d)



(e)

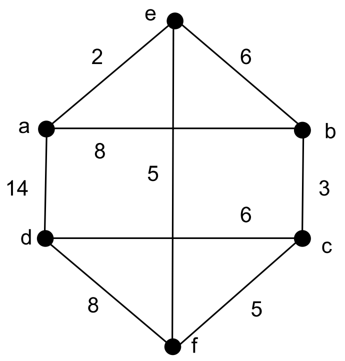


13. Find the binary tree representation of the followings.

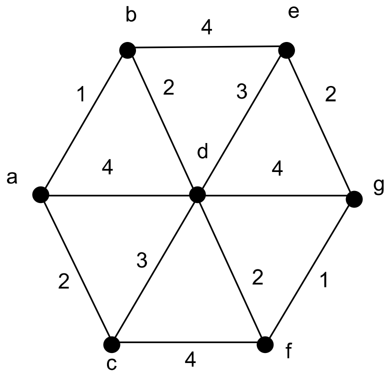
(*a*) $(4x + 2)(2x + xy)$ (*b*) $(x + 3y) - ((5x + y)/4)$

14. Let G be a connected weighted graph. Use Dijkstra's algorithms to find the length of shortest paths from the vertex a to each of the other vertices.

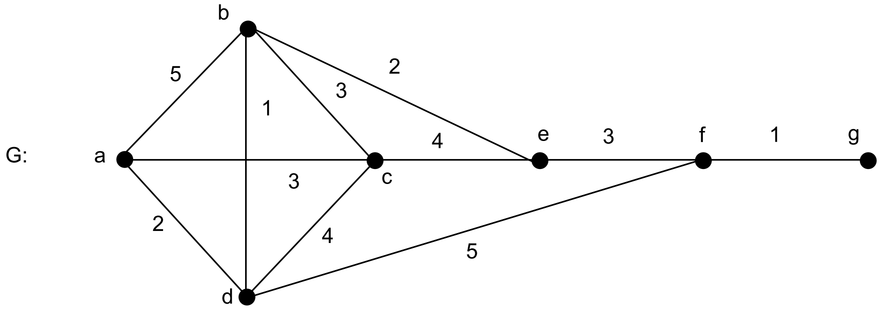
(a)



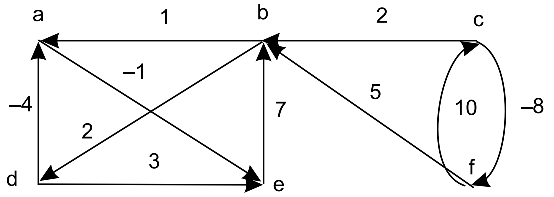
(b)



15. Apply Dijkstra's algorithm to the weighted graph G below to find the shortest distance for each vertex from the source vertex *a*.

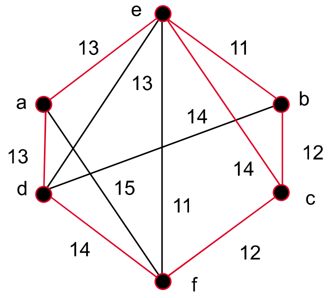


16. Use Floyd-Warshall algorithm on the weighted, directed graph G shown below to find out shortest path between any pair of vertices. Show the matrix D(*k*) that results for each iteration.

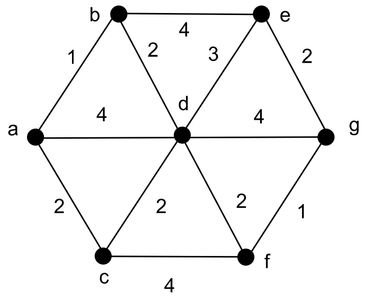


17. Find the minimum spanning tree of the graphs shown below by using
(*a*) Prim's algorithm and (*b*) Kruskal's algorithm.

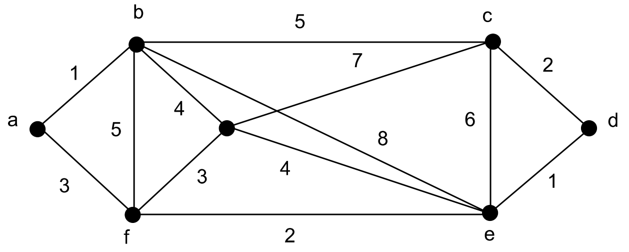
(a)



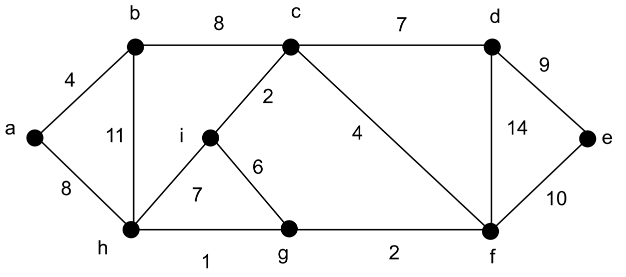
(b)



(C)



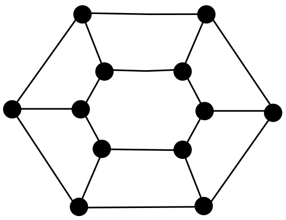
(d)



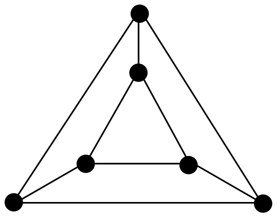
18. Find a maximal spanning tree for each of the graphs of No 17. using either Prim's algorithm or Kruskal's algorithm. [**Hint:** To get the maximal spanning tree replace the weight of each edge of the graph by M – $w(e)$, where M is any number greater than the weight $w(e)$ of every edge e of the graph. Then apply Prim's algorithm or Kruskal's algorithm. The corresponding spanning tree in the original weighted graph is a maximal spanning tree.]

19. Find the closure graph C(G) of the following graphs.

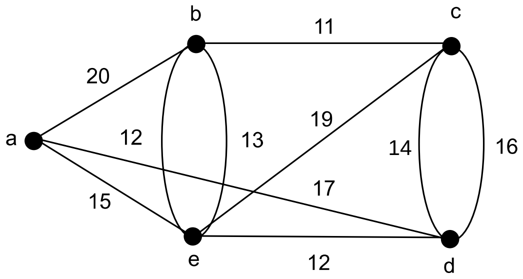
(a)



(b)



20. Let G be a connected weighted graph. Use Floyd-Warshall algorithm to find the length of shortest path between any pair of vertices.


b
11
c
20
19
a
12
13
14
16
17
15
e
12
d