1. 1. Proportional Logic

Proposition:

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

Notations:

If a proposition is true then it's truth value is denoted by T.

If a proposition is false then it's truth value is denoted by F.

P, Q, R, S, . . . are used to denote propositions.

Connectives:

Connective is an operation which is used to connect two or more than two statements. Simply it is called sentential connectives. It is also known as Logical Connectives or Logical Operators.

Compound Statement:

Statements which contain one or more primary statements and some connectives are called compound or molecular or composite statements.

Example:

Let p: $5 + 10 = 20$ be the statement

$\neg p$: It is false that 5 + 10 = 20

Hence $\neg p$ is a compound statement with primary statement as p and connective as $\neg p$

Five Basic Connectives

	Logical Connectives	Name	Symbols	Type of Operator
1	Not	Negation	$\neg$	Unary
2	And	Conjunction	$\wedge$	Binary
3	Or	Disjunction	$\vee$	Binary
4	If . . . then	Conditional (or) Implication	$\rightarrow$	Binary
5	If and only if (iff)	Biconditional	$\leftrightarrow (or) \rightleftharpoons$	Binary

Statement Formula:

A statement formula is an expression which is a string consisting of variables (capital letters with or without subscripts), parenthesis and connective symbols.

Truth Tables:

The truth value of proposition is either true (T) or false (F).

A truth table is a table that shows the truth value of a compound proposition for all possible cases.

Negation:

If a statement is **TRUE**, then its negation is **FALSE**. (And if a statement is **FALSE**, then its negation is **TRUE**).

P	**¬p**
T	F
F	T

Conjunction:

A conjunction is a compound statement formed by joining two statements with the connector AND. The conjunction "p and q" is symbolized by p, q.

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

Disjunction:

A conjunction is a compound statement formed by joining two statements with the connector OR. The disjunction "p or q" is symbolized by p, q. A disjunction is FALSE if and only if (iff) both statements are FALSE; otherwise it is TRUE.

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

Conditional:

A conditional statement, symbolized by $p \rightarrow q$ is an if – then statement in which p is a hypothesis and q is a conclusion. The logical connector in a conditional statement is denoted by the symbol. The conditional is defined to be TRUE unless a TRUE hypothesis leads to a FALSE conclusion.

P	Q	$P \rightarrow Q$
T	T	T
T	F	F

F	T	T
F	F	T

Bi conditional:

A bi -conditional statement is defined to be TRUE whenever both parts have the same truth value. The bi-conditional operator is denoted by a double – headed arrow. The bi-conditional p↔ q represents "p if and only if", where p is a hypothesis and q is a conclusion.

P	Q	$P \leftrightarrow Q$
T	T	T
T	F	F
F	T	F
F	F	T

Problems under logical connectives

1.Write the following statements in symbolic form, "If either S.Pavithra takes calculus or S. Sharnika takes sociology, then Malathy will take English.

Solution:

P: S.Pavithra takes calculus.

Q: S.Sharnika takes sociology.

R: Malathy takes English.

∴ The logical expression is $(P \vee Q) \rightarrow R$

2. S. Pavithra can accesses the internet from campus only if she is a computer science major or she is not a fresh girl.

Solution:

P: S. Pavithra can accesses the internet from campus.

Q: S. Pavithra is a computer science major.

R: S. Pavithra is a fresh girl.

$\neg P$: S. Pavithra is not a fresh girl.

∴ The logical expression is $P \rightarrow (Q \vee \neg R)$

3. How can this English sentence be translated into logical expression.

"You can access the internet from campus only if you are computer science major or you are not a freshman".

Solution:

P: You can access the internet from campus.

Q: You are computer science major.

R: You are a freshman.

¬R: you are not a freshman.

∴ The logical expression is $P \rightarrow (Q \vee \neg R)$

4. Write the logical expression for "If tigers have wings then the earth travels round the sun."

Solution:

P: Tigers have wings. (F)

Q: Earth travels round the sun. (F)

The logical expression is $P \rightarrow Q$ (T)

5. Construct the truth table for a)$\neg (P \wedge Q)$ and b) $(\neg P) \vee (\neg Q)$

Solution:

To prove $\neg (P \wedge Q)$ and $(\neg P) \vee (\neg Q)$

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

F	T	F	T
F	F	F	T

P	Q	¬P	¬Q	(¬P) ∨ (¬Q)
T	T	F	F	F
T	F	F	T	T
F	T	T	F	T
F	F	T	T	T

6. Construct the truth table for (P ∨ Q) ∨ ¬Q.

Solution:

P	Q	P ∨ Q	¬Q	(P ∨ Q) ∨ ¬Q.
T	T	T	F	T
T	F	T	T	T
F	T	T	F	T
F	F	F	T	T

7. Construct the truth table for ¬(¬*P* ∨ ¬Q).

Solution:

P	Q	¬P	¬Q	$\neg P \vee \neg Q$	$\neg(\neg P \vee \neg Q)$
T	T	F	F	F	T
T	F	F	T	T	F
F	T	T	F	T	F
F	F	T	T	T	F

8. Construct the truth table for S: (P∧Q) ∨ (¬P∧Q) ∨ (P∧ ¬Q)

Solution:

P	Q	P ∧ Q	¬P	¬Q	¬P∧Q	P∧ ¬Q	(¬P∧Q) ∨ (P∧ ¬Q)	S
T	T	T	F	F	F	F	F	T
T	F	F	F	T	F	T	T	T
F	T	F	T	F	T	F	T	T
F	F	F	T	T	F	F	F	F

9. Construct the truth table for i) R: $\neg(\neg P \vee \neg Q)$. ii) $\neg(\neg P \wedge \neg Q)$.

Solution:

P	Q	¬P	¬Q	$\neg P \vee \neg Q$	$\neg P \wedge \neg Q$	R	S

T	T	F	F	F	F	T	T
T	F	F	T	T	F	F	T
F	T	T	F	T	F	F	T
F	F	T	T	T	T	F	F

10. Construct the truth table for $(P \rightarrow Q) \wedge (Q \rightarrow P)$.

Solution:

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

Tautology:

A Tautology is a statement that is always TRUE, no matter what. If you construct a truth table for a statement and all the column values for the statement are TRUE, then the statement is a Tautology because it's always TRUE.

Contradiction:

A statement that is always FALSE is known as a Contradiction.

i.e, The last column values contains all FALSE values.

Results:

Tautology	**Contradiction**
In the result column all the entries are T	In the result column all the entries are F
T	F
T	F
T	F
T	F

Problems under Tautology and contradiction

1.Show that the proposition P ∨ ¬ (P ∧ Q) is a tautology.

Solution:

P	Q	P ∧ Q	¬ (P ∧ Q)	P ∨ ¬ (P ∧ Q)
T	T	T	F	T
T	F	F	T	T
F	T	F	T	T
F	F	F	T	T

2.Show that (Q ∨ (P∧ ¬Q)) ∨ (¬P ∧ ¬Q) is a tautology.

Solution:

Let S = $(Q \vee (P \wedge \neg Q)) \vee (\neg P \wedge \neg Q)$

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

3. Show that $\neg P \rightarrow (P \rightarrow Q)$ is a tautology.

Solution:

P	Q	$\neg P$	$P \rightarrow Q$	$\neg P \rightarrow (P \rightarrow Q)$
T	T	F	T	T
T	F	F	F	T
F	T	T	T	T
F	F	T	T	T

4. Show that $(P \wedge Q) \wedge \neg (P \vee Q)$ is a contradiction.

Solution:

P	Q	P ∧ Q	P ∨ Q	¬ (P ∨ Q)	(P ∧ Q) ∧ ¬ (P ∨ 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

1. 2. Propositional Equivalences

Logical Equivalences or Equivalence Rules

Laws	**Formulae**
Idempotent Laws	$p \wedge p \Leftrightarrow p, p \vee p \Leftrightarrow p$
Associative Laws	$(p \wedge q) \wedge r \Leftrightarrow p \wedge (q \wedge r)$ $(p \vee q) \vee r \Leftrightarrow p \vee (q \vee r)$
Commutative Laws	$p \wedge q \Leftrightarrow q \wedge p$ $p \vee p \Leftrightarrow q \vee p$
DeMorgan's Laws	$\neg(p \wedge q) \Leftrightarrow (\neg p \vee \neg q)$ $\neg(p \vee q) \Leftrightarrow (\neg p \wedge \neg q)$
Distributive Laws	$p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$ $p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$
Complement Laws	$p \wedge \neg p \Leftrightarrow F, p \vee \neg p \Leftrightarrow T$
Dominance Laws	$p \vee T \Leftrightarrow T, p \wedge F \Leftrightarrow F$
Identity Laws	$p \wedge T \Leftrightarrow p, p \vee F \Leftrightarrow p$
Absorption Laws	$p \vee (p \wedge q) \Leftrightarrow p$ $p \wedge (p \vee q) \Leftrightarrow p$
Double Negation Laws	$\neg(\neg p) \Leftrightarrow p$
Contra Positive Laws	$p \rightarrow q \Leftrightarrow \neg q \rightarrow \neg p$

Conditional as Disjunction	$p \to q \Leftrightarrow \neg p \vee q$
Biconditional as Conditional	$p \to q \Leftrightarrow (p \to q) \wedge (q \to p)$
Exportations laws	$p \to (q \to r) \Leftrightarrow (p \wedge q) \to r$

1.Determine whether $(\neg Q \wedge (P \to Q)) \to \neg P$ is a tautology.

Solution:

$(\neg Q \wedge (P \to Q)) \to \neg P$	Reason
$\Rightarrow (\neg Q \wedge (\neg P \vee Q)) \vee \neg P$	$P \to Q \Leftrightarrow \neg P \vee Q$
$\Rightarrow \neg(\neg Q \wedge (\neg P \vee Q)) \vee \neg P$	$P \to Q \Leftrightarrow \neg P \vee Q$
$\Rightarrow (Q \vee (P \wedge \neg Q)) \vee \neg P$	(DeMorgan's law)
$\Rightarrow ((Q \vee P) \wedge (Q \vee \neg Q)) \vee \neg P$	(Distributive law)
$\Rightarrow ((Q \vee P) \wedge T) \vee \neg P$	$P \vee \neg P \Leftrightarrow T$
$\Rightarrow (Q \vee P) \vee \neg P$	$P \wedge T \Leftrightarrow P$
$\Rightarrow (Q \vee P \vee \neg P)$	(Associative law)
$\Rightarrow (Q \vee T)$	$P \vee \neg P \Leftrightarrow T$
$\Rightarrow T$	$P \vee T \Leftrightarrow T$

2. Show that the formula $Q \vee (P \wedge \neg Q) \vee (\neg P \wedge \neg Q)$ is a tautology.

Solution:

$Q \vee (P \wedge \neg Q) \vee (\neg P \wedge \neg Q)$	Reason
$\Rightarrow Q \vee (P \vee \neg P) \wedge \neg Q$	(Distributive law)
$\Rightarrow (\mathrm{Q} \vee (P \vee \neg P)) \vee (Q \vee \neg Q)$	(Distributive law)
$\Rightarrow (\mathrm{Q} \vee T) \wedge \mathrm{T}$	$P \vee \neg P \Leftrightarrow T$
$\Rightarrow T \wedge \mathrm{T}$	$P \vee T \Leftrightarrow P$

3. Show that the formula $(\boldsymbol{P} \wedge \boldsymbol{Q}) \rightarrow (\boldsymbol{P} \vee \boldsymbol{Q})$ is a tautology.

Solution:

$(P \wedge Q) \rightarrow (P \vee Q)$	Reason
$\Rightarrow \neg(P \wedge Q) \vee (P \vee Q)$	$P \rightarrow Q \Leftrightarrow \neg P \vee Q$
$\Rightarrow (\neg P \vee \neg Q) \vee (P \vee Q)$	(DeMorgan's law)
$\Rightarrow (P \vee \neg P) \vee (Q \vee \neg Q)$	(Associative law)
$\Rightarrow T \vee \mathrm{T} = \mathrm{T}$	(Negation law)

4. Show that the formula $\big(\neg \boldsymbol{P} \wedge (\neg \boldsymbol{Q} \wedge \boldsymbol{R})\big) \vee (\boldsymbol{Q} \wedge \boldsymbol{R}) \vee (\boldsymbol{P} \wedge \boldsymbol{R}) \Leftrightarrow \boldsymbol{R}$

Solution:

$\big(\neg P \wedge (\neg Q \wedge R)\big) \vee (Q \wedge R) \vee (P \wedge R)$	Reason
$\Rightarrow \big(\neg P \wedge (\neg Q \wedge R)\big) \vee \big((Q \vee P) \wedge R\big)$	(Distributive law)
$\Rightarrow ((\neg P \wedge \neg Q) \wedge R) \vee \big((Q \vee P) \wedge R\big)$	(Associative law)
$\Rightarrow [(P \vee \neg Q) \vee (Q \vee P)] \wedge R$	(Distributive law)
$\Rightarrow [\neg(P \vee Q) \vee (P \vee Q)] \wedge R$	(DeMorgan's law)
$\Rightarrow T \wedge$ R	$P \vee \neg P \Leftrightarrow T$
$\Rightarrow$ R	$P \wedge T \Leftrightarrow P$

Equivalence

Two statement formulas A and B are equivalent iff $A \leftrightarrow B$ or $A \leftrightharpoons B$ is a tautology. It is denoted by the symbol $A \Leftrightarrow B$ which is read as "A is equivalent to B."

Remark:

To prove two statement formulas A and B are equivalent, we can use any one of the following method:

(i) using Truth Table, we show that truth values of both statements formulas A and B are same for each 2^n combinations.

(ii) Assume A. By applying various equivalence rules try to derive B and vice versa.

(iii) Prove $A \leftrightharpoons B$ is a tautology.

1. Show that $\neg\big(\boldsymbol{P} \vee (\neg \boldsymbol{P} \wedge \boldsymbol{Q})\big)$ & $\neg \boldsymbol{P} \wedge \neg \boldsymbol{Q}$ are logically equivalent.

Solution:

$\neg\big(P \vee (\neg P \wedge Q)\big)$	Reason
$\Leftrightarrow \neg P \wedge \big(\neg(\neg P \wedge \neg Q)\big)$	(DeMorgan's law)
$\Leftrightarrow \neg P \wedge [\neg(\neg P) \vee \neg Q]$	(DeMorgan's law)
$\Leftrightarrow \neg P \wedge (P \vee \neg Q)$	(Double Negation law)
$\Leftrightarrow (\neg P \wedge P) \vee (\neg P \wedge \neg Q)$	(Distributive law)
$\Leftrightarrow F \vee (\neg P \wedge \neg Q)$	$\neg P \wedge P \Leftrightarrow F$
$\Leftrightarrow (\neg P \wedge \neg Q) \vee F$	(Commutative law)
$\Leftrightarrow \neg P \wedge \neg Q$	(identity law)

Hence $\neg\big(P \vee (\neg P \wedge Q)\big)$ & $\neg P \wedge \neg Q$ are logically equivalent.

2. Prove that $\boldsymbol{P} \rightarrow \boldsymbol{Q} \Leftrightarrow \boldsymbol{P} \rightarrow (\boldsymbol{P} \wedge \boldsymbol{Q})$

Solution:

$P \rightarrow (P \wedge Q)$	Reason

$\Leftrightarrow \neg P \vee (P \wedge Q)$	(Conditional as disjunction)
$\Leftrightarrow (\neg P \vee P) \wedge (\neg P \wedge Q)$	(Distributive law)
$\Leftrightarrow T \wedge (\neg P \wedge Q)$	$\neg P \wedge P \Leftrightarrow F$
$\Leftrightarrow \neg P \wedge Q$	(Identity law)
$\Leftrightarrow P \rightarrow Q$	(Conditional as disjunction)

3. Prove that $(P \rightarrow R) \wedge (Q \rightarrow R) \Leftrightarrow (P \vee Q) \rightarrow R$

Solution:

$(P \rightarrow R) \wedge (Q \rightarrow R)$	Reason
$\Leftrightarrow (\neg P \wedge R) \wedge (\neg Q \wedge R)$	(Conditional as disjunction)
$\Leftrightarrow (\neg P \wedge \neg Q) \vee R$	(Distributive law)
$\Leftrightarrow \neg(P \vee Q) \vee R$	(DeMorgan's law)
$\Leftrightarrow (P \vee Q) \rightarrow R$	(Conditional as disjunction)

4. Prove that $P \rightarrow (Q \rightarrow R) \Leftrightarrow (P \wedge Q) \rightarrow R$

Solution:

$P \rightarrow (Q \rightarrow R)$	Reason
$\Leftrightarrow \neg P \vee (Q \rightarrow R)$	(Conditional as disjunction)
$\Leftrightarrow \neg P \vee (\neg Q \vee R)$	(Conditional as disjunction)
$\Leftrightarrow \neg(\neg P \vee \neg Q) \vee R$	(Associative law)
$\Leftrightarrow \neg(P \wedge Q) \vee R$	(DeMorgan's law)
$\Leftrightarrow (P \wedge Q) \rightarrow R$	(Conditional as disjunction)

1. 3. Quantifiers

Normal Forms

Elementary Product

A product of the statement variables and their negations in the formula is called Elementary Product.

The possible elementary products are

$$P, Q, \neg P \wedge Q, \neg Q \wedge P, P \wedge \neg P, Q \wedge \neg Q, P \wedge \neg P \wedge Q$$

Elementary Sum

A sum of the two statement variables and their negations is called Elementary Sum.

The possible elementary sums are

$$P, Q, \neg P \vee Q, \neg Q \vee P, P \vee \neg P \vee Q, P \vee Q$$

Disjunctive Normal Forms (DNF)

A statement formula which is equivalent to a given formula and which consists of a sum of elementary products is called a disjunctive normal form of the given formula,

DNF = (Elementary product) ∨ (Elementary product) ∨ . . . ∨ (Elementary product)

Conjunctive Normal Forms (DNF)

A statement formula which is equivalent to a given formula and which consists of a sum of elementary products is called a disjunctive normal form of the given formula,

DNF = (Elementary product) ∨ (Elementary product) ∨ . . . ∨ (Elementary product)

Remark:

(i) Note that DNF and CNF of given statement formula need not be unique.

(ii) In DNF and CNF, the number of variables in each term need not be same.

1. Obtain a disjunctive Normal form $P \wedge (P \rightarrow Q)$

Solution:

$P \wedge (P \rightarrow Q)$	Reason
$\Rightarrow P \wedge (\neg P \vee Q)$ $\Rightarrow (P \wedge \neg P) \vee (P \wedge Q)$	$(P \rightarrow Q \Rightarrow \neg P \vee Q)$ (Distributive law)

Since the given statement formula is written in terms of sum of elementary product.

DNF of $P \wedge (P \rightarrow Q)$ is $(P \wedge \neg P) \vee (P \wedge Q)$

2. Obtain DNF of $\neg(\boldsymbol{P} \vee \boldsymbol{Q}) \rightleftharpoons (\boldsymbol{P} \wedge \boldsymbol{Q})$

Solution:

$\neg(P \vee Q) \rightleftharpoons (P \wedge Q)$	Reason
$\Rightarrow [\neg(P \vee Q) \wedge (P \wedge Q)]$ $\vee\ [(P \vee Q) \wedge \neg(P \wedge Q)]$	$\big(R \rightleftharpoons S \Leftrightarrow (R \wedge S) \vee (\neg R \wedge \neg S)\big)$
$\Rightarrow (\neg P \wedge \neg Q \wedge P \wedge Q) \vee [(P \vee Q) \wedge (\neg P \vee \neg Q)]$	(DeMorgan's law & Associative law)
$\Rightarrow (\neg P \wedge \neg Q \wedge P \wedge Q) \vee \big[P \wedge (\neg P \vee \neg Q) \vee \big(Q \wedge (\neg P \vee \neg Q)\big)\big]$	(Distributive law)
$\Rightarrow (P \wedge Q \wedge \neg P \wedge \neg Q) \vee (P \wedge \neg P) \vee (P \wedge \neg Q) \vee (Q \wedge \neg P) \vee (Q \wedge \neg Q)$	(Distributive law)

Which is the required DNF.

Principal Normal Forms:

Min terms:

Let P and Q be 2 statement variables. Let us construct all possible formulas which consist of conjunction of P or its negation and conjunction of Q or its negation.

None of the formulas should contain both a variable and its negation. Using commutative law, if any two terms are equivalent choose any one of the term. Collect the remaining terms. They are called minterms.

For example, let P and Q be two variables, then the minterms are

$$P \wedge Q, P \wedge \neg Q, \neg P \wedge Q, \neg P \wedge \neg Q$$

Remark: 1

1. If there are "n" variables then the number of minterms is 2^n.

2. In elementary product a variable and its negation exist. But in minterms such things does not exist.

3. Let P, Q and R be 3 variables. The possible minterms are

1. $P \wedge Q \wedge R$

2. $P \wedge Q \wedge \neg R$

3. $P \wedge \neg Q \wedge R$

4. $\neg P \wedge Q \wedge R$

5. $\neg P \wedge \neg Q \wedge R$

6. $\neg P \wedge Q \wedge \neg R$

7. $P \wedge \neg Q \wedge \neg R$

8. $\neg P \wedge \neg Q \wedge \neg R$

Max terms:

Let P and Q be 2 statement variables. Let us construct all possible conjunction of disjunction P or its negation and Q or its negation. None of the formulas should contain both a variable and its negation. Using commutative law, if any two terms are equivalent choose any one of the term. Collect the remaining terms. They are called maxterms.

The possible maxterms with 2 variables are

$$P \vee Q, P \vee \neg Q, \neg P \vee Q, \neg P \vee \neg Q$$

Principal Disjunctive Normal Forms (PDNF)

For a given statement formula, an equivalent formula consisting of disjunction of minterms only is known as its Principal Disjunctive Normal Forms (PDNF)

PDNF = (minterms) ∨ (minterms) ∨ . . . ∨ (minterms)

Principal Conjunctive Normal Forms (PCNF)

For a given statement formula, an equivalent formula consisting of conjunction of maxterms only is known as its Principal Conjunctive Normal Forms (PCNF)

PCNF = (maxterms) ∧ (maxterms) ∧ . . . ∧ (maxterms)

Note:

1. PDNF is also called sum –of – products canonical form. PCNF is also called product – of – sums canonical form.

2. PDNF and PCNF of a given statement formula need not be unique.

PDNF and PCNF using Truth table

Using truth table, we can easily find PDNF and PCNF of given statement formulas.

Working rule to find PDNF:

1. Construct truth table for the given statement formula.

2. Choose each and every row in which the final column value is “TRUE”

3. In the selected row, if the truth value of each individual variable value is TRUE select that variable and truth value is FALSE then select the negation of that variable. In such a way collect all possible minterms.

4. Sum of all minterms gives the required PDNF.

Working rule to find PCNF:

1. Construct truth table for the given statement formula.

2. Choose each and every row in which the final column value is “FALSE”

3. In the selected row, if the truth value of each individual variable value is FALSE select that variable and truth value is TRUE then select the negation of that variable. In such a way collect all possible maxterms.

4. Product of all maxterms gives the required PCNF.

Problems under PDNF and PCNF using Truth table

1. Obtain PDNF of $P \rightarrow Q$

Solution:

P	Q	$P \rightarrow Q$	Min term
T	T	T	$P \wedge Q$
T	F	F	-
F	T	T	$\neg P \wedge Q$
F	F	T	$\neg P \wedge \neg Q$

2. Obtain the PDNF of $(P \wedge Q) \vee (\neg P \wedge R) \vee (Q \wedge R)$

Solution:

P	Q	R	$P \wedge Q$	$\neg P \wedge R$	$Q \wedge R$	$(P \wedge Q) \vee (\neg P \wedge R) \vee (Q \wedge R)$	Min term
T	T	T	T	F	T	T	$P \wedge Q \wedge R$
T	T	F	T	F	F	T	$P \wedge Q \wedge \neg R$
T	F	T	F	F	F	F	
T	F	F	F	F	F	F	
F	T	T	F	T	T	T	$\neg P \wedge Q \wedge R$
F	T	F	F	F	F	F	
F	F	T	F	T	F	T	$\neg P \wedge \neg Q \wedge R$
F	F	F	F	F	F	F	

The PDNF is $(P \wedge Q \wedge R) \vee (P \wedge Q \wedge \neg R) \vee (\neg P \wedge Q \wedge R) \vee (\neg P \wedge \neg Q \wedge R)$

3. Find the PCNF and PDNF of the proposition $P \wedge (Q \rightarrow R)$

Solution:

P	Q	R	$Q \rightarrow R$	$P \wedge (Q \rightarrow R)$	Min term	Max term
T	T	T	T	F		$P \vee Q \vee R$
T	T	F	T	F		$P \vee Q \vee \neg R$
T	F	T	F	F		$P \vee \neg Q \vee R$

T	F	F	T	F		$P \vee \neg Q \vee \neg R$
F	T	T	T	T	$P \wedge \neg Q \wedge \neg R$	
F	T	F	T	T	$P \wedge \neg Q \wedge R$	
F	F	T	F	F		$\neg P \vee \neg Q \vee R$
F	F	F	T	T	$P \wedge Q \wedge R$	

The PDNF is $(P \wedge \neg Q \wedge \neg R) \vee (P \wedge \neg Q \wedge R) \vee (P \wedge Q \wedge R)$

The PCNF is $(P \vee Q \vee R) \wedge (P \vee Q \vee \neg R) \wedge (P \vee \neg Q \vee R) \wedge (P \vee \neg Q \vee \neg R) \wedge$

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

4. Find the Principal Conjunctive normal form of $(\boldsymbol{P \wedge A}) \wedge (\neg \boldsymbol{P \wedge R})$

Solution:

P	Q	R	$\neg P$	$P \wedge Q$	$\neg P \wedge R$	$(P \wedge Q) \vee (\neg P \wedge R)$	Min term
T	T	T	F	T	F	T	
T	T	F	F	T	F	T	
T	F	T	F	F	F	F	$\neg P \vee Q \vee \neg R$
T	F	F	F	F	F	F	$\neg P \vee Q \vee R$
F	T	T	T	F	T	T	
F	T	F	T	F	F	F	$P \vee \neg Q \vee R$

F	F	T	T	F	T	T	
F	F	F	T	F	T	T	

The required PCNF is $(\neg P \vee Q \vee \neg R) \wedge (\neg P \vee Q \vee R) \wedge (P \vee \neg Q \vee R)$

The Theory of Inference

The main aim of logic is to provide rules of inference, or principles of reasoning. Here, we are concerned with the inferring of a conclusion from given premises.

We are going to check the logical validity of the conclusion, from the given set of premises by making use of Equivalence rule and implication rule, the theory associated with such things is called inference theory.

Direct Method

When a conclusion is derived from a set of premises by using the accepted rules of reasoning, then such a process of derivation is called a direct proof.

Indirect method of proof:

(i) Method of Contradiction:

In order to show that a conclusion C follows logically from the premises

$H_1,\ H_2,\ldots,H_m$, we assume that C is false and consider $\neg C$ as an additional premises. If the new set of premises gives contradict value, then the assumption $\neg C$ is true does not hold simultaneously with $H_1 \wedge\ H_2,\wedge \ldots \wedge\ H_m$.

Therefore, C is true whenever $H_1 \wedge\ H_2,\wedge \ldots \wedge\ H_m$ ids true. Thus C follows logically from the premises $H_1,\ H_2,\ldots,H_m$.

(ii) Method of contrapositive:

In order to prove $H_1 \wedge H_2, \wedge \ldots \wedge H_m \Rightarrow C$, if we prove

$\neg C \Rightarrow \neg(H_1 \wedge H_2, \wedge \ldots \wedge H_m)$ then the original problem follows. This method is called contrapositive method.

Rules of Inference

Rule P: A premise may be introduced at any point in the derivation.

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

Rule CP: If S can be derived from R and set of premises, then $R \rightarrow S$ can be derived from the set of premises alone.

Remark:

(i) Rule CP means Rule of Conditional Proof.

(ii) Rule CP is also called the deduction theorem.

Implication Rule:

$P, P \rightarrow Q \Rightarrow Q$	Modus Phones
$\neg Q, P \rightarrow Q \Rightarrow \neg P$	Modus Tollens
$\neg P, P \vee Q \Rightarrow Q$	Disjunctive syllogism
$P \rightarrow Q, Q \rightarrow R \Rightarrow P \rightarrow R$	Hypothetical syllogism (or) chain rule

$P, Q \Rightarrow P \wedge Q$	Simplification rule
$P, Q \Rightarrow P \vee Q$	Addition rule
$P \wedge \neg Q \Rightarrow \neg(P \rightarrow Q)$	Equivalence rule

Note:

In the derivation, we should use all the rules but exactly once. Also, the order is immaterial.

1.Demonstrate that R is a valid inference from the premises $P \rightarrow Q, Q \rightarrow R$ & P

Solution:

$\{1\}$	1)$P \rightarrow Q$	Rule P
$\{2\}$	2)$Q \rightarrow R$	Rule P
$\{1, 2\}$	3)$P \rightarrow R$	Rule T $(P \rightarrow Q, Q \rightarrow R \Rightarrow P \rightarrow R)$
$\{4\}$	4)P	Rule P
$\{1, 2, 4\}$	5)R	Rule T $(P, P \rightarrow Q \Rightarrow Q)$

2. Show that $\neg P$ follows logically from the premises $\neg(P \wedge \neg Q), (\neg Q \vee R)$ &$\neg R$

Solution:

Given premises are $\neg(P \wedge \neg Q), (\neg Q \vee R), \neg R$

Conclusion: &$\neg R$

$\{1\}$	1)$\neg(P \wedge \neg Q)$	Rule P
$\{2\}$	2))$\neg P \vee Q$	Rule T (Demorgan's law)
$\{1\}$	3)$P \rightarrow Q$	Rule T ($P \rightarrow Q \Leftrightarrow \neg P \vee R$)
$\{4\}$	4)$\neg Q \vee R$	Rule P
$\{4\}$	5)$Q \rightarrow R$	Rule T ($P \rightarrow Q \Leftrightarrow \neg P \vee R$)
$\{1,4\}$	6) $P \rightarrow R$	Rule T ($P \rightarrow Q, Q \rightarrow R \Rightarrow P \rightarrow R$)
$\{7\}$	7) $\neg R$	Rule P
$\{1,4,7\}$	8) $\neg P$	Rule T $\neg Q, P \rightarrow Q \Rightarrow \neg P$

Consistency and Inconsistency of Premises

A set of formulae $H_1, H_2, \ldots, H_m$ is said to be inconsistent if their conjunction implies contradiction.

i.e., $H_1 \wedge H_2 \wedge \ldots \wedge H_m \Rightarrow R \wedge \neg R$ for some formulae R.

Note:$R \wedge \neg R \Leftrightarrow F$

Consistent:

A set of formulae $H_1, H_2, \ldots, H_m$ is said to be consistent if their conjunction implies tautology.

Inconsistent:

A set of formula $H_1, H_2, \ldots, H_m$ is said to be consistent if it is not inconsistent.

1.Show that $P \to Q, P \to R, Q \to \neg R$ & P are inconsistent.

Solution:

$\{1\}$	1)$P \to Q$	Rule P
$\{2\}$	2)$Q \to \neg R$	Rule P
$\{1, 2\}$	3)$P \to \neg R$	Rule T
$\{4\}$	4)P	Rule P
$\{1, 2, 4\}$	5)$\neg R$	Rule T
$\{6\}$	6)$P \to R$	Rule P
$\{1, 2, 4, 6\}$	7)$\neg P$	Rule T
$\{1, 2, 4, 6\}$	8)$P \wedge \neg P$	Rule T

Which is nothing but false value.

Hence given set of premises are inconsistent.

2. Prove that $P \to Q, Q \to R, S \to \neg R$ & $P \wedge S$ are inconsistent.

Solution:

$\{1\}$	1)$P \to Q$	Rule P
$\{2\}$	2)$Q \to R$	Rule P
$\{1,2\}$	3)$P \to R$	Rule T
$\{4\}$	4)$S \to \neg R$	Rule P
$\{4\}$	5)$R \to \neg S$	Rule T
$\{1,2,4\}$	6)$P \to \neg S$	Rule T
$\{1,2,4\}$	7)$\neg P \vee \neg S$	Rule T
$\{1,2,4\}$	8)$\neg(P \wedge S)$	Rule T
$\{9\}$	9)$P \wedge S$	Rule P
$\{1,2,4,9\}$	10)$(P \wedge S) \wedge \neg(P \wedge S)$	Rule T

Which is nothing but false value.

Hence given set of premises are inconsistent.

3. Prove that $a \to (b \to c), d \to (b \wedge \neg c)$, & $a \wedge d$ are inconsistent.

Solution:

$\{1\}$	1)$a \wedge d$	Rule P
$\{1\}$	2)a, d	Rule T

$\{3\}$	3)$a \rightarrow (b \rightarrow c)$	Rule P
$\{1,3\}$	4)$b \rightarrow c$	Rule T
$\{1,3\}$	5)$\neg b \vee c$	Rule T
$\{6\}$	6)$d \rightarrow (b \wedge \neg c)$	Rule P
$\{6\}$	7)$\neg(b \wedge \neg c) \rightarrow \neg d$	Rule T
$\{6\}$	8))$\neg b \vee c \rightarrow \neg d$	Rule T
$\{1,3,6\}$	9) $\neg d$	Rule T
$\{1,3,6\}$	10) $d \wedge \neg d$	Rule T

Which is nothing but false value.

Hence given set of premises are inconsistent.

1.6 The Predicate Calculus

The predicate calculus deals with the study of predicates.

Consider the following statement.

"Ram is a boy"

In the above statement, **"is a boy"** is the predicate and the name **"Ram"** is the subject.

If we denote **"is a boy"** by B and subject **"Ram"** by r, then the statement **"Ram is a boy"** can be represented as B(r).

Some examples

1." x is a man"

Here, Predicate is **"is a man"** and it is denoted by M. Subject is **"x"** and it is denoted by x.

Hence the given statement **"x is a man"** can be denoted by **M(x).**

2. "Sam is poor and Ram is intelligent"

The statement **"Sam is poor"** can be represented by **P(s)** where P represents predicate **"is poor"** and s represents subject **"Sam"**

The statement "Ram is intelligent" can be represented by I(r) where I represents predicate **"is intelligent"** and r represents subject **"Ram".**

Hence the given statement **"Sam is poor and Ram is intelligent"** can be symbolized as $\boldsymbol{P(s) \wedge I(r)}$.

The Theory of Inference for Predicate Calculus

Universal Specification (UG): $A(y) \Rightarrow (x)A(x)$

Existential Generalization (EG): $A(y) \Rightarrow (\exists x)A(x)$

Universal Specification (US): $(x)A(x) \Rightarrow A(y)$

Existential Specification (ES): $(\exists x)A(x) \Rightarrow A(y)$

Problems:

1.Show that $\boldsymbol{(x)\big(H(x) \rightarrow M(x)\big) \wedge H(s) \Rightarrow M(s)}$

Solution:

$\{1\}$	1) $(x)\big(H(x) \rightarrow M(x)\big)$	Rule P
$\{1\}$	2)$H(s) \rightarrow M(s)$	Rule US
$\{3\}$	3 $H(s)$	Rule P
$\{1,3\}$	4)$M(s)$	Rule T $(P, P \rightarrow Q \Rightarrow Q)$

2. Show that $(x)\big(P(x) \to Q(x)\big) \wedge (x)\big(Q(x) \to R(x)\big) \Rightarrow (x)\big(P(x) \to R(x)\big)$

Solution:

$\{1\}$	1) $(x)\big(P(x) \to Q(x)\big)$	Rule P
$\{1\}$	2)$P(y) \to Q(y)$	Rule US
$\{3\}$	3 $(x)\big(Q(x) \to R(x)\big)$	Rule P
$\{1,3\}$	4)$Q(y) \to R(y)$	Rule US
$\{1,3\}$	5) $P(y) \to R(y)$	Rule T $(P \to Q, Q \to R \Rightarrow P \to R)$
$\{1,3\}$	6)$(x)\big(P(x) \to R(x)\big)$	Rule UG

3. Show that $(\exists x)\big(P(x) \wedge Q(x)\big) \Rightarrow (\exists x)P(x) \wedge (\exists x)Q(x)$

Solution:

$\{1\}$	1) $(\exists x)\big(P(x) \wedge Q(x)\big)$	Rule P
$\{1\}$	2)$P(y) \wedge Q(y)$	Rule ES
$\{3\}$	3 $P(y)$	Rule T $(P \wedge Q \Rightarrow P)$
$\{1,3\}$	4)$Q(y)$	Rule T $(P \wedge Q \Rightarrow P)$
$\{1,3\}$	5) $(\exists x)P(x)$	Rule EG
$\{1,3\}$	6)$(\exists x)Q(x)$	Rule EG
$\{1\}$	7)$(\exists x)P(x) \wedge (\exists x)Q(x)$	Rule T$(P, Q \Rightarrow P \wedge Q)$

4.Show that $(x)\big(P(x) \vee Q(x)\big) \Rightarrow (x)P(x) \vee (\exists x)Q(x)$

Solution:

We shall use the indirect method of proof.

Method of contradiction:

Assume $\neg\big((x)P(x) \vee (\exists x)Q(x)\big)$ **as an additional premises.**

{1}	1) $\neg\big((x)P(x) \vee (\exists x)Q(x)\big)$	Assumed Premises
{1}	2) $(\exists x)\neg P(x) \wedge (x)Q(x)$	Rule T (D'Morgan's law)
{1}	3) $(\exists x)\neg P(x)$	Rule T ($P \wedge Q \Rightarrow P$)
{1}	4) $(x)Q(x)$	Rule T ($P \wedge Q \Rightarrow P$)
{1}	5) $\neg P(y)$	Rule ES
{1}	6) $\neg Q(y)$	Rule US
{1}	7) $\neg P(y) \wedge \neg Q(y)$	Rule T($P, Q \Rightarrow P \wedge Q$)
{1}	8) $\neg\big(P(y) \vee Q(y)\big)$	Rule T (D'Morgan's law)
{1}	9) $(x)\big(P(x) \vee Q(x)\big)$	Rule P
{1}	10) $P(y) \vee Q(y)$	Rule US
{1}	11) $\big(P(y) \vee Q(y)\big) \wedge \neg\big(P(y) \vee Q(y)\big)$	Rule T($P, Q \Rightarrow P \wedge Q$)

which is nothing but false value.

5.Show that $(x)\big(P(x) \to Q(x)\big) \Rightarrow (x)P(x) \to (x)Q(x)$

Solution:

Assume $\neg\big((x)P(x) \to (x)Q(x)\big)$

{1}	1) $\neg\big((x)P(x) \to (x)Q(x)\big)$	Assumed Premises
{1}	2) $(x)P(x) \wedge \neg(x)Q(x)$	Rule T ($P \to Q \Rightarrow \neg P \vee Q$)
{1}	3) $(x)P(x)$	Rule T ($P \wedge Q \Rightarrow P$)
{1}	4) $\neg\big((x)Q(x)\big)$	Rule T ($P \wedge Q \Rightarrow P$)
{1}	5) $(\exists x)\neg Q(x)$	Rule T(Taking $\neg$)
{1}	6) $P(y)$	Rule US
{1}	7) $\neg Q(y)$	Rule ES
{1}	8) $P(y) \wedge \neg Q(y)$	Rule T ($P, Q \Rightarrow P \wedge Q$)
{9}	9) $\neg\big(P(y) \to Q(y)\big)$	Rule T($(P \wedge \neg Q) \Leftrightarrow \neg(P \to Q)$)
{9}	10) $(\exists x)\neg\big(P(x) \to Q(x)\big)$	Rule EG
{1, 9}	11) $\neg\big((x)P(x) \to Q(x)\big)$	Rule T(Taking $\neg$)

2.1 Mathematical induction:

Statement of the principle of Mathematical Induction

Let $P(n)$be statement involving the natural number "n".

If P(1) is true.

Under the assumption that when P(k) is true, P(k+1) is true, then we conclude that a statement P(n) is true for all natural number "n".

Steps to prove that a statement P(n) is true for all natural numbers

Step:1 We must prove that P(1) is true.

Step:2 By assuming P(k) is true, we must prove that P(k+1) is also true.

NOTE:

Step:1 is known as the basic step.

Step:2 is known as inductive step.

Problems on Mathematical Induction:

1. Show that $1 + 2 + \ldots + n = \frac{n(n+1)}{2}$ using mathematical induction.

Solution:

Let S be the set of positive integers.

To prove $p(1)$ is true.

When $n = 1$

RHS $\Rightarrow \frac{n(n+1)}{2} = \frac{1(1+1)}{2} = 1 =$ LHS

Hence $p(1)$ is true.

Assume that $p(k)$ is true.

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

To prove $p(k+1)$ is true.

Adding $k + 1$ on both sides

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

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

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

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

Hence $p(k+1)$ is true.

2. Show that $1^2 + 2^2 + 3^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}$

Solution:

Let S be the set of positive integers.

To prove $p(1)$ is true.

When $n = 1$

RHS $\Rightarrow \frac{n(n+1)(2n+1)}{6} = \frac{1(1+1)(2+1)}{6} = 1 =$ LHS

Hence $p(1)$ is true.

Assume that $p(k)$ is true.

$$1^2 + 2^2 + 3^2 + \ldots + k^2 = \frac{k(k+1)(2k+1)}{6} \quad \ldots (1)$$

To prove $p(k+1)$ is true.

$$1^2 + 2^2 + 3^2 + \ldots + k^2 + (k+1)^2 = \frac{(k+1)(k+2)(2k+3)}{6}$$

Adding $(k+1)^2$ on both sides

$$\Rightarrow 1^2 + 2^2 + 3^2 + \ldots + k^2 + (k+1)^2 = \frac{k(k+1)(2k+1)}{6} + (k+1)^2$$

$$= (k+1)\left[\frac{k(2k+1)}{6} + (k+1)\right]$$

$$= \frac{(k+1)}{6}[k(2k+1) + 6(k+1)]$$

$$= \frac{(k+1)}{6}[2k^2 + k + 6k + 6]$$

$$= \frac{(k+1)}{6}[2k^2 + 7k + 6]$$

$$= \frac{(k+1)}{6}[2k^2 + 4k + 3k + 6]$$

$$= \frac{(k+1)}{6}[2k(k+2) + 3(k+2)]$$

$$= \frac{(k+1)}{6}[(k+2) + (2k+3)]$$

Hence $p(k+1)$ is true.

3. Show that $1^3 + 2^3 + 3^3 + \ldots + n^3 = \frac{n^2(n+1)^2}{4}$

Solution:

Let S be the set of positive integers.

To prove $p(1)$ is true.

When $n = 1$

RHS $\Rightarrow \frac{n^2(n+1)^2}{4} = \frac{1^2(1+1)^2}{4} = 1 =$ LHS

Hence $p(1)$ is true.

Assume that $p(k)$ is true.

$$1^3 + 2^3 + 3^3 + \ldots + k^3 = \frac{k^2(k+1)^2}{4} \qquad \ldots (1)$$

To prove $p(k+1)$ is true.

$$1^3 + 2^3 + 3^3 + \ldots + k^3 + (k+1)^3 = \frac{(k+1)^2(k+2)^2}{4}$$

Adding $(k+1)^3$ on both sides

$$\Rightarrow 1^3 + 2^3 + 3^3 + \ldots + k^3 + (k+1)^3 = \frac{k^2(k+1)^2}{4} + (k+1)^3$$

$$= \frac{k^2(k+1)^2 + 4(k+1)^3}{4}$$

$$= \frac{(k+1)^2}{4}[k^2 + 4(k+1)]$$

$$= \frac{(k+1)^2}{4}[k^2 + 4k + 4]$$

$$= \frac{(k+1)^2}{4}[k^2 + 2k + 2k + 4]$$

$$= \frac{(k+1)^2}{4}[k(k+2) + 2(k+2)]$$

$$= \frac{(k+1)^2}{4}[(k+2) + (k+2)]$$

$$= \frac{(k+1)^2(k+2)^2}{4}$$

Hence $p(k+1)$ is true.

4.Prove that $n^3 - n$ is divisible by 3, using mathematical induction .

Solution:

Let S be the set of positive integers.

To prove $p(1)$ is true.

When $n = 1$

RHS $\Rightarrow n^3 - n = 1^3 - 1 = 0$ is divisible by 3.

Hence $p(1)$ is true.

Assume that $p(k)$ is true.

$k^3 - k$ is divisible by 3.

$\Rightarrow k^3 - k = 3m$

$\Rightarrow k^3 = 3m + k \ \ldots (1)$

To prove $p(k+1)$ is true.

$(k+1)^3 - (k+1)$ is divisible by 3.

$$\Rightarrow k^3 + 1 + 3k^2 + 3k - k - 1$$

$$\Rightarrow k^3 + 3k^2 + 2k$$

$$\Rightarrow (3m + k\ ) + 3k^2 + 2k$$

$$\Rightarrow 3m + 3k^2 + 3k$$

$\Rightarrow 3(m + k^2 + k)$ is divisible by 3.

Hence $p(k+1)$ is true.

5. Prove that $8^n - 3^n$ is a multiple of 5. .

Solution:

Let S be the set of positive integers.

To prove $p(1)$ is true.

When $n = 1$

RHS $\Rightarrow 8^n - 3^n = 8^1 - 3^1 = 5$ is a multiple of 5 which is true.

Hence $p(1)$ is true.

Assume that $p(k)$ is true.

$8^k - 3^k$ is a multiple of 5.

$\Rightarrow 8^k - 3^k = 5m$

$\Rightarrow 8^k = 5m + 3^k \ldots (1)$

To prove $p(k+1)$ is true.

$8^{k+1} - 3^{k+1}$ is a multiple of 5.

$$\Rightarrow 8 \cdot 8^k - 3 \cdot 3^k$$

$$\Rightarrow (5m + 3^k) \cdot 8 - 3 \cdot 3^k$$

$$\Rightarrow 5 \cdot 8m + 8 \cdot 3^k - 3 \cdot 3k$$

$$\Rightarrow 5 \cdot 8m + 5 \cdot 3^k$$

$\Rightarrow 5(8m + 3^k)$ is a multiple of 5.

Hence $p(k+1)$ is true.

6. State and prove Handshaking theorem.

Suppose there are "n" people in a room, $n \geq 1$ and that they all shake hands with one another, prove that $\frac{n(n-1)}{2}$ handshakes will have accured.

Solution:

Let S be the set of positive integers.

To prove $p(1)$ is true.

When $n = 1$

$p(1) = \frac{n(n-1)}{2} = \frac{1(1-1)}{2} = 0$

$\Rightarrow$ there is no handshake accured which means there is only one person.

Hence $p(1)$ is true.

Assume that $p(k)$ is true.

$p(k) = \frac{k(k-1)}{2}$ . . . (1)

To prove $p(k+1)$ is true.

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

Suppose if one person entered into the room then he will shake his hand with "k" other person whenever $p(k)$ is true.

Hence $p(k+1)$ is true by mathematical induction.

The Well – Ordering Property:

The validity of mathematical induction follows from the following fundamental axioms about the set of integers.

Every non – empty set of non – negative integers has a least element.

The well ordering property can often be used directly in the proof.

2.2 Pigeon Hole Principle and Generalized Pigeon Hole Principle

Pigeonhole Principle:

The pigeonhole principle in its simplest incarnation, states the following

If you have more pigeons than pigeonholes, and you try to stuff the pigeons into the holes, then Atleast one hole must contain at least two pigeons.

Basic Pigeonhole Principle:

If $k + 1$ or more objects are placed into k boxes, then there is Atleast one box containing two or more of the objects.

Pigeonhole Principle:

If $(n + 1)$ Pigeon occupies "n" holes then atleast one hole has more than one pigeon.

Proof:

Assume $(n + 1)$ pigeon occupies "n" holes.

Claim: Atleast one hole has more than one pigeon.

Suppose not,

Atleast one hole has not more than one pigeon.

Therefore each and every hole has exactly one pigeon.

Since, there are "n" hole, which implies, we have totally "n" pigeon.

Which is a contradiction to our assumption that there are $(n+1)$ pigeon.

Therefore atleast one hole has more than one pigeon.

Hence the proof.

Generalized Pigeon Hole Principle

If m pigeon occupies "n" holes $(m > n)$ then atleast one hole has more than $\left[\frac{m-1}{n}\right] + 1$ pigeon.Here $[x]$ denotes the greatest integer less than or equal to x, which is a real number.

Proof:

Assume "m" pigeon occupy "n" holes $(m > n)$

Claim: Atleast on hole has more than $\left[\frac{m-1}{n}\right] + 1$ pigeon.

Suppose not, i.e., Atleast one hole has not more than $\left[\frac{m-1}{n}\right] + 1$ pigeon.

Each and every hole has exactly $\left[\frac{m-1}{n}\right] + 1$ pigeon.

Since we have n holes, totally there are $n\left[\left[\frac{m-1}{n}\right] + 1\right]$ pigeon.

$\Rightarrow m - 1 + n$ pigeons

$\Rightarrow m + n - 1$ pigeons

Which is a contradiction to the assumption, that there are m pigeons.

Therefore, Atleast one hole has more than $\left[\frac{m-1}{n}\right] + 1$ pigeon.

Problems under Pigeonhole and Generalized pigeonhole principle

1. Show that, among 100 people, atleast 9 of them were born in the same month.

Solution:

Here, Number of Pigeon = Number of people = 100

Number of holes = Number of month = 12

Then by generalized pigeon hole principle,

$$\left[\frac{m-1}{n}\right] + 1 = \left[\frac{100-1}{12}\right] + 1 = 9$$

Were born in the same month.

2. Show that, if seven colors are used to paint 50 bicycles, atleast 8 bicycles will be the same.

Solution:

Here, Number of Pigeon = Number of bicycle = 50

Number of holes = Number of colors = 7

Then by generalized pigeon hole principle,

$$\left[\frac{m-1}{n}\right] + 1 = \left[\frac{50-1}{7}\right] + 1 = 8$$

Therefore atleast 8 bicycles will have the same color.

3. Show that, if 25 dictionaries in a library contain a total of 40,325 pages, then one of the dictionaries must have atleast 1614 pages.

Solution:

Here, Number of Pigeon = Number of bicycle = 40325

Number of holes = Number of colors = 25

Then by generalized pigeon hole principle,

$$\left[\frac{m-1}{n}\right]+1=\left[\frac{40325-1}{25}\right]+1=1614$$

Here, Number of Pigeon = Number of grades $= \ n \ = 5$

Let k be number of students (pigeon) in discrete mathematics class.

$$\Rightarrow k+1=6$$

$$\Rightarrow k=5$$

The total number of students $= kn+1$

$$=5\times 5+1=26$$

Minimum number of students = 26.

2.3 Permutation and Combination

The process of selecting things is called combination and that of arranging things is called permutation.

Examples of combinations and permutations:

(i) Formation of a team from a number of players.

(ii) Formation of a 3 member committee from 10members.

(iii) Arrangement of books on a shelf.

(iv) Formation of word with the given letters.

Permutation:

Each of the different arrangements which can be made by taking some or all of a number of things at a time is called a permutation.

The number of permutations of "n" things taken "r" at a time is denoted by nP_r

Examples:

$6P_2$ means the number of permutations of 6 things taken 2 at a time.

Formulae:

(i) $nP_r = \mathrm{n}(n-1)(n-2)\ldots(n-r+1)$

(ii) The number of permutations of "n" things taken all at a time is

$nP_n = \mathrm{n}(n-1)(n-2)\ldots 3 \cdot 2 \cdot 1$

$\Rightarrow nP_n = \mathrm{n}!$

Problems based on Permutations:

1. In how many ways can 6 persons occupy 3 vacant seats?

Solution:

Given $n = 6, r = 3$

Total number of ways = $nP_r = 6P_3$ ways

$= 6 \times 5 \times 4 = 120$ ways

2. How many permutations of the letters ABCDEFGH contain the string ABC.

Solution:

Given $n = 6$

No of arrangements = $nP_r = 6P_6 = 6!$ Ways

$= 720$ ways

3. In how many ways can letters of the word "INDIA" be arranged.

Solution:

The word INDIA contains 5 letters of which 2 are I's.

The number of word possible $= \frac{5!}{2!} = \frac{5\times4\times3\times2\times1}{2\times1}$

$= 60$ ways

4. There are 6 books on Economics, 3 on Commerce and 2 on History. In how many ways can these be placed on a shelf if books on the same subject are to be together.

Solution:

6 Economics books can be arranged in $6P_6$ ways or 6! Ways.

3 Commerce books can be arranged in $3P_3$ ways or 3! Ways.

2 History books can be arranged in $2P_2$ ways or 2! Ways.

The three books can be arranged in $3P_3$ ways

The total number of required arrangements

$= 6! \times 3! \times 2! \times 3!$ Ways

$= 51840$ ways

5. Out of 7 consonants and 4 vowels, how many words of 3 consonants and 2 vowels can be formed?

Solution:

Number of ways of selecting 3 consonants from 7 $= {}^{7}C_{3}$

Number of ways of selecting 2 vowels from 4 $= {}^{4}C_{2}$

Number of ways of selecting 3 consonants from 7 and 2 vowels from 4

$= {}^{7}C_{3} \times {}^{4}C_{2}$

$$= \frac{7 \times 6 \times 5}{3 \times 2 \times 1} \times \frac{4 \times 3}{2 \times 1} = 210$$

6. Find the number of distinct permutations that can be formed from all the letters of each word (i) RADAR (ii) UNUSUAL

Solution:

The word contains 5 letters of which 2 are A's and 2 are R's.

The number of possible words $= \frac{5!}{2!2!} = 30$

(ii) The word contains 7 letters of which 3 U's are there

The number of possible words $= \frac{7!}{3!} = 40$

7. Find the value of n if $nP_2 = 20$

Solution:

We know that $nP_r = \frac{n!}{(n-r)!}$

$$nP_2 = \frac{n!}{(n-2)!} = \frac{n(n-1)(n-2)!}{(n-2)!}$$

$$\Rightarrow n(n-1) = 20$$

$$\Rightarrow n = 20 \ (or) \ n-1 = 20$$

$$\Rightarrow n = 21$$

Combinations:

Each of the different groups or selections which can be made by taking some or all of a number of things at a time is called a combination.

The number of combinations of "n" things taken "r" at a time is denoted by nC_r.

Formula:

$$nC_r = \frac{n!}{r! \ (n-r)!}$$

Problems based on Combinations:

1. In how many ways can 5 persons be selected from amongst 10 persons?

Solution:

The selection can be done in $10C_5$ ways.

$$= \frac{10 \times 9 \times 8 \times 7 \times 6}{1 \times 2 \times 3 \times 4 \times 5}$$

$$= 252 \text{ ways}$$

2. How many ways are there to select five players from 10 member tennis team to make a trip to match to another school.

Solution:

5 members can be selected from 10 members in $10C_5$ ways.

Now $10C_5 = \frac{10\times9\times8\times7\times6\times5\times4\times3\times2\times1}{5\times4\times3\times2\times1}$

$= 252$ ways

3. Find the number of diagonals that can be drawn by joining the angular points of a heptagon.

Solution:

A heptagon has seven angular points and seven sides.

The join of two angular points is either a side or a diagonal.

The number of lines joining the angular points

$= 7C_2$

$= \frac{7\times6}{2\times1} = 21$

But the number of sides = 7

Hence the number of diagonals $= 21 - 7 = 14$

4. A team of 11 players is to be chosen from 15members. In how many ways can this be done if (i)one particular player is always included? (ii) Two such players have always to be included?

Solution:

(i) Let one player be fixed.

The remaining players are 14.

Out of these 14 players, we have to select 10 players in $14C_{10}$ ways.

$$14C_{10} = \frac{n!}{r!\,(n-r)!} = \frac{14!}{10!\,(14-10)!} = 1001 \text{ ways.}$$

(ii) Let 2 players be fixed.

The remaining players are 13.

Out of 13 players, we have to select 9 players in $13C_9$ ways.

$$13C_9 = \frac{n!}{r!\,(n-r)!} = \frac{13!}{9!\,(13-9)!} = 715 \text{ ways.}$$

5. If $nC_5 = 20nC_4$, find the value of n.

Solution:

Given $nC_5 = 20nC_4$

$$\frac{n!}{5!\,(n-5)!} = \frac{20n!}{4!\,(n-4)!}$$

$\Rightarrow (n-4)!\,4! = 20 \times (n-5)!\,5!$

$\Rightarrow (n-4-1)!\,(n-4)4! = 20 \times (n-5)!\,5!$

$\Rightarrow (n-5)!\,(n-4)4! = 20 \times (n-5)!\,4! \times 5$

$\Rightarrow (n-4) = 100$

$\Rightarrow n = 100 + 4 = 104$

$\Rightarrow n = 104$

6. A question paper has 3 parts, Part A, Part B and Part C having 12, 4 and 4 questions respectively. A student has to answer 10 questions from Part A and 5 questions from Part B and Part C put together selecting atleast 2 from each one of these two parts. In how many ways the selection of questions can be done.

Solution:

12	4	4
Part A	Part B	Part C
10	2	3
10	3	2

The selection of questions can be done in

$$12C_{10} \times 4C_2 \times 4C_3 + 12C_{10} \times 4C_3 \times 4C_2$$

$$= 3168 \text{ ways}$$

2.4 Recurrence Relations:

An equation that expresses a_n, the general term of the sequence $\{a_n\}$ in terms of one or more of the previous terms of the sequence, namely $a_0, a_1, \ldots, a_{n-1}$, for all integers n with $n \geq n_0$, where n_0 is a non – negative integer is called a recurrence relation for $\{a_n\}$ or a difference equation.

If the terms of a sequence satisfies a recurrence relation, then the sequence is called a solution of the recurrence relation.

For example, we consider the famous Fibonacci sequence

0, 1, 1, 2, 3, 5, 8, 13, 21, . . .

Which can be represented by the recurrence relation.

$$F_n = F_{n-1} + F_{n-2}, n \geq 2$$

and $F_0 = 0, F_1 = 1$

Here, $F_0 = 0, F_1 = 1$ are called initial conditions.

It is a second order recurrence relation.

Definition:

A linear homogeneous recurrence relation of degree k with constant coefficients is a recurrence relation of the form

$$a_n = C_1 a_{n-1} + C_2 a_{n-2} + \ldots + C_K k a_{n-k}$$

Where $C_1, C_2, \ldots, C_k$ are real numbers, and $C_k \neq 0$.

The recurrence relation in the definition is linear since the right – hand side is a sum of multiplies of the previous terms of the sequence.

The recurrence relation is homogeneous, since no terms occur that are not multiplies of the a_j's.

The coefficients of the terms of the sequence are all constants, rather than function that depend on "n".

The degree is k because a_n is expressed in terms of the previous k terms of the sequence.

Solving Linear Homogeneous Recurrence Relations With Constant Coefficients:

Step: 1 Write down the characteristic equation for the given recurrence relation. Here, the degree of character equation is 1 less than the number of terms in recurrence relation.

Step: 2 By solving the characteristic equation find out the characteristic roots.

Step: 3 Depends upon the nature of roots, find out the solution a_n as follows:

Case (i) Let the roots be real and distinct say $r_1, r_2, \ldots, r_n$.

Then $a_n = \alpha_1 {r_1}^n + \alpha_2 {r_2}^n + \alpha_3 {r_3}^n + \ldots + \alpha_n {r_n}^n$ where $\alpha_1, \alpha_2, \ldots, \alpha_n$ are arbitrary constants.

Case (ii) Let the roots be real and equal say $r_1 = r_2 = \ldots = r_n$.

Then $a_n = \alpha_1 {r_1}^n + n\alpha_2 {r_2}^n + n^2\alpha_3 {r_3}^n + \ldots + n^n\alpha_n {r_n}^n$ where $\alpha_1, \alpha_2, \ldots, \alpha_n$ are arbitrary constants.

Case (iii) When the roots are complex conjugate, then

$a_n = r^n(\alpha_1 \cos n\theta + \alpha_2 \sin n\theta)$

Step: 4 Apply initial conditions and find out arbitrary constants.

Note:

There is no single method or technique to solve all recurrence relations. There exist some recurrence relations which cannot be solved. The recurrence relation

$S(k) = 2[S(k-1)]^2 - kS(k-3)$ cannot be solved.

1. If the sequence $a_n = 3 \cdot 2^n, n \geq 1$, then find the corresponding recurrence relation.

Solution:

Given $a_n = 3 \cdot 2^n$

$\Rightarrow a_{n-1} = 3 \cdot 2^{n-1}$

$= 3 \cdot \frac{2^n}{2}$

$\Rightarrow a_{n-1} = \frac{a^n}{2}$

$\Rightarrow a_n = 2(a_{n-1})$

Hence $a_n = 2a_{n-1}, n \geq 1$ with $a_0 = 3$

2. Find the recurrence relation for $S(n) = 6(-5)^n, n \geq 0$

Solution:

Given $S(n) = 6(-5)^n$

$\Rightarrow S(n-1) = 6(-5)^{n-1}$

$= 6\frac{(-5)^n}{-5}$

$= \frac{S(n)}{-5}$

$\Rightarrow S(n) = -5 \cdot S(n-1), n \geq 0$ with $S(0) = 6$

3. Find the recurrence relation from $y_k = A \cdot 2^k + B \cdot 3^k$

Solution:

Given $y_k = A \cdot 2^k + B \cdot 3^k$ . . . (1)

$\Rightarrow y_{k+1} = A \cdot 2^{k+1} + B \cdot 3^{k+1}$

$= A \cdot 2^k \cdot 2 + B \cdot 3^k \cdot 3$

$= 2A \cdot 2^k + 3B \cdot 3^k \quad \ldots (2)$

$\Rightarrow y_{k+2} = 4A \cdot 2^k + 9B \cdot 3^k \quad \ldots (3)$

$(3) - 5(2) + 6(1)$

$\Rightarrow y_{k+2} - 5y_{k+1} + 6y_k = 4A \cdot 2^k + 9B \cdot 3^k - 10A \cdot 2^k - 15B \cdot 3^k + 6A \cdot 2^k + 6B \cdot 3^k = 0$

$\Rightarrow y_{k+2} - 5y_{k+1} + 6y_k = 0$

4. Find the recurrence relation from $y_n = A3^n + B(-4)^n$

Solution:

Given $y_n = A3^n + B(-4)^n \quad \ldots (1)$

$\Rightarrow y_{n+1} = y_n = A3^{n+1} + B(-4)^{n+1}$

$= A3^n \cdot 3 + B(-4)^n \cdot (-4)$

$= 3A \cdot 3^n - 4B \cdot (-4)^n \quad \ldots (2)$

$\Rightarrow y_{n+2} = 9A \cdot 3^n + 16B \cdot (-4)^n \quad \ldots (3)$

$(3) + (2) - 12(1)$

$\Rightarrow y_{n+2} + y_{n+1} - 12y_n = 9A3^n + 16B(-4)^n + 3A3^n - 4B(-4)^n - 12A3^n - 12B(-4)^n = 0$

$\Rightarrow y_{n+2} + y_{n+1} - y_n = 0$

5. Find the solution to the recurrence relation $a_n = 6a_{n-1} - 11a_{n-2} + 6a_{n-3}$ with the initial conditions $a_0 = 2, a_1 = 5, a_2 = 15$

Solution:

The recurrence relation can be written as $a_n - 6a_{n-1} + 11a_{n-2} - 6a_{n-3} = 0$

The characteristic equation is $r^3 - 6r^2 + 11r - 6 = 0$

By solving, we get the characteristic roots, $r = 1, 2, 3$

Solution is $a_n = \alpha_1 \cdot 1^n + \alpha_2 2^n + \alpha_3 3^n \quad \ldots$ (A)

Given $a_0 = 2$, Put $n = 0$ in (A)

$$a_0 = \alpha_1 \cdot (1)^0 + \alpha_2 (2)^0 + \alpha_3 (3)^0$$

(A) $\Rightarrow \alpha_1 + \alpha_2 + \alpha_3 = 2 \quad \ldots (1)$

Given $a_1 = 5$, Put $n = 1$ in (A)

$$a_1 = \alpha_1 \cdot (1)^1 + \alpha_2 (2)^1 + \alpha_3 (3)^1$$

(A) $\Rightarrow \alpha_1 + 2\alpha_2 + 3\alpha_3 = 5 \quad \ldots (2)$

Given $a_2 = 15$, Put $n = 2$ in (A)

$$a_2 = \alpha_1 \cdot (1)^2 + \alpha_2(2)^2 + \alpha_3(3)^2$$

(A) $\Rightarrow \alpha_1 + 4\alpha_2 + 9\alpha_3 = 15 \quad \ldots (3)$

To solve (1), (2) and (3)

$(1) \Rightarrow \alpha_3 = 2 - \alpha_1 - \alpha_2 \quad \ldots (4)$

Using (4) in (2)

$(2) \Rightarrow 2\alpha_1 + \alpha_2 = 1 \quad \ldots (5)$

Using (4) in (3)

$(3) \Rightarrow 8\alpha_1 + 5\alpha_3 = 3 \quad \ldots (6)$

Solving (5) and (6), we get $\alpha_1 = 1$ and $\alpha_2 = -1$

Using $\alpha_1 = 1$ and $\alpha_2 = -1$ in (1) we get $\alpha_3 = 2$

Substituting $\alpha_1 = 1$ and $\alpha_2 = -1$ and $\alpha_3 = 2$ in (A), we get

Solution is $a_n = 1 \cdot 1^n - 1 \cdot 2^n + 2 \cdot 3^n$

2.5 Generating Function:

The generating function for the sequence "s" with terms $a_0, a_1, \ldots, a_n$ of real numbers is the infinite sum.

$$G(x) = G(s,x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n + \ldots$$

$$= \sum_{n=0}^{\infty} a_n x^n$$

For example, (i) The generating function for the sequence "s" with the terms $1, 1, 1, \ldots$ is given by

$$G(x) = G(s,x) = \sum_{n=0}^{\infty} x^n = \frac{1}{1-x}$$

(ii) The generating function for the sequence "s" with terms $1, 2, 3, 4, \ldots$ is given by

$$G(x) = G(s,x) = \sum_{n=0}^{\infty} (n+1)x^n$$

$$= 1 + 2x + 3x^2 + \ldots$$

$$= (1-x)^{-2}$$

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

Problems:

1. Write the generating function for the sequence $1, a, a^2, a^3, a^4, \ldots$

Solution:

Generating function $G(x) = 1 + a + a^2 + a^3 + a^4 + \ldots$

$$= \frac{1}{1-ax} \text{ for } |ax| < 1$$

Solution for Recurrence Relations using Generating Functions:

Procedure for solving Recurrence Relation using Generating Function:

Step: 1 Rewrite the recurrence relation as an equation on RHS

Step: 2 Multiply the equation in step: 1 by x^n and summing it from 1 to ∞ or

(0 to ∞) or (2 to ∞)

Step: 3 Put $G(x) = \sum_{n=0}^{\infty} a_n x^n$ and write $G(x)$ as a function of x.

Step: 4 Decompose $G(x)$ into partial fraction.

Step: 5 Express $G(x)$ as a sum of familiar series.

Step: 6 Express a_n as the coefficient of x^n in $G(x)$.

The following table represents some sequences and their generating functions.

S. no	Sequence	Generating Function
1	1	$\frac{1}{1-z}$
2	$(-1)^n$	$\frac{1}{1+z}$
3	a^n	$\frac{1}{1-az}$
4	$(-a)^n$	$\frac{1}{1+az}$
5	$n+1$	$\frac{1}{1-(z)^2}$
6	n	$\frac{1}{(1-z)^2}$
7	n^2	$\frac{z(1+2)}{(1-z)^3}$
8	na^n	$\frac{az}{(1-za)^2}$

1. Using generating function solve the recurrence relation $a_n = 3a_{n-1}$ for $n \geq 1$ with $a_0 = 2$

Solution:

Let $G(x) = \sum_{n=0}^{\infty} a_n x^n$

Given $a_n - 3a_{n-1} = 0$

Multiply the above equation by x^n and summing from 1 to ∞, we get

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

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

$\Rightarrow (G(x) - a_0) - 3xG(x) = 0$

$\Rightarrow G(x)(1 - 3x) = a_0$

$\Rightarrow G(x)(1 - 3x) = 2$

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

$= 2(1 + 3x + (3x)^2 + \ldots)$

$= 2\sum_{n=0}^{\infty} 3^n x^n$

Consequently, $a_n = 2$. coefficient of x^n in $G(x)$

$$a_n = 2 \cdot 3^n$$

2. Solve the recurrence relation $a_n - 7a_{n-1} + 10a_{n-2} = 0$ for $n \geq 2$ given that $a_0 = 10, a_1 = 41$ using generating function.

Solution:

The given recurrence relation is $a_n - 7a_{n-1} + 10a_{n-2} = 0$

Multiply the above equation by x^n and summing from 2 to ∞, we get

$$\Rightarrow \sum_{n=2}^{\infty} a_n x^n - 7\sum_{n=2}^{\infty} a_{n-1}x^n + 10\sum_{n=2}^{\infty} a_{n-2}x^n = 0$$

$$\Rightarrow \sum_{n=2}^{\infty} a_n x^n - 7x\sum_{n=2}^{\infty} a_{n-1}x^{n-1} + 10x^2\sum_{n=2}^{\infty} a_{n-2}x^{n-2} = 0$$

$\Rightarrow [G(x) - a_0 - a_1 x] - 7x[G(x) - a_0] + 10x^2 G(x) = 0$

$\Rightarrow G(x) - 10 - 41x - 7x[G(x) - 10] + 10x^2 G(x) = 0$

$\Rightarrow G(x)(1 - 7x + 10x^2) + 29x - 10 = 0$

$\Rightarrow G(x) = \frac{10-29x}{10x^2-7x+1}$

$\Rightarrow G(x) = \frac{10-29x}{(1-2x)(1-5x)}$

$\Rightarrow G(x) = \frac{A}{(1-2x)} + \frac{B}{(1-5x)}$

$= A(1-2x)^{-1} + B(1-5x)^{-1}$

$= A[1 + 2x + (2x)^2 + \ldots] + B[1 + 5x + (5x)^2 + \ldots]$

$= A\sum_{n=2}^{\infty} 2^n x^n + B\sum_{n=2}^{\infty} 5^n x^n$

a_n = coefficient of x^n in $G(x)$

$a_n = A2^n + B5^n, n \geq 2 \quad \ldots$ (A)

Given $a_0 = 10$, Put $n = 0$ in (A), we get

$\Rightarrow a_0 = A2^0 + B5^0$

$\Rightarrow 10 = A + B \quad \ldots (1)$

Given $a_1 = 41$, Put $n = 1$ in (A), we get

$\Rightarrow a_1 = A2^1 + B5^1$

$\Rightarrow 41 = 2A + 5B \quad \ldots (2)$

Solving (1) and (2) we get $A = 3, B = 7$

Hence $a_n = 3 \cdot 2^n + 7 \cdot 5^n$

3. Using generating function solve the recurrence relation corresponding to the Fibonacci sequence $a_n = a_{n-1} + a_{n-2}, n \geq 2$ with $a_0 = 1, a_1 = 1$

Solution:

Given recurrence relation $a_n - a_{n-1} - a_{n-2} = 0$

Multiply the above recurrence relation by x^n and summing from 2 to ∞, we get

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

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

$$\Rightarrow [G(x) - a_0 - a_1 x] - x[G(x) - a_0] - x^2 G(x) = 0$$

$$\Rightarrow G(x) - 10 - 41x - 7x[G(x) - 10] + 10x^2 G(x) = 0$$

$$\Rightarrow G(x)(1 - x - x^2) = a_0 - a_0 x + a_1 x$$

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

$$= \frac{1}{\left(1-\frac{1+\sqrt{5}}{2}x\right)\left(1-\frac{1-\sqrt{5}}{2}x\right)}$$

$$= \frac{A}{\left(1-\frac{1+\sqrt{5}}{2}x\right)} + \frac{B}{\left(1-\frac{1-\sqrt{5}}{2}x\right)}$$

Now $\frac{1}{1-x-x^2} = \frac{A}{\left(1-\frac{1+\sqrt{5}}{2}x\right)} + \frac{B}{\left(1-\frac{1-\sqrt{5}}{2}x\right)}$ ... (1)

$$1 = A\left(1 - \frac{1-\sqrt{5}}{2}x\right) + B\left(1 - \frac{1+\sqrt{5}}{2}x\right) \quad \ldots (2)$$

Put $x = 0$ in (2)

$(2) \Rightarrow A + B = 1$ ... (3)

Put $x = \frac{2}{1-\sqrt{5}}$ in (2)

$$(2) \Rightarrow 1 = B\left(1 - \frac{1+\sqrt{5}}{1-\sqrt{5}}\right)$$

$$\Rightarrow 1 = B\left(\frac{1-\sqrt{5}-1-\sqrt{5}}{1-\sqrt{5}}\right)$$

$$\Rightarrow 1 = B\left(\frac{-2\sqrt{5}}{1-\sqrt{5}}\right) \quad \text{(Using B value in (3))}$$

$$\Rightarrow B = \frac{1-\sqrt{5}}{-2\sqrt{5}}$$

$$(3) \Rightarrow A = \frac{1}{2\sqrt{5}}\left(1+\sqrt{5}\right)$$

Sub A and B in (1), we get

$$G(x) = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)\left(1-\left(\frac{1+\sqrt{5}}{2}\right)x\right)^{-1} - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)\left(1-\left(\frac{1-\sqrt{5}}{2}\right)x\right)^{-1}$$

$$= \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)\left[1+\frac{1+\sqrt{5}}{2}x+\left(\frac{1+\sqrt{5}}{2}\right)^{2}+\ldots\right]$$

$$-\frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)\left[1+\frac{1-\sqrt{5}}{2}x+\left\{\left(\frac{1-\sqrt{5}}{2}\right)x\right\}^{2}+\ldots\right]$$

a_n = coefficient of x^n in $G(x)$

Solving, we get

$$a_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{n+1}$$

4. Identify the sequence having the expression $\frac{5+2x}{1-4x^2}$ as a generating function.

Solution:

Given $G(x) = \frac{5+2x}{1-4x^2}$ . . . (1)

$= \frac{5+2x}{(1+2x)(1-2x)}$

Now, $\frac{5+2x}{(1+2x)(1-2x)} = \frac{A}{(1+2x)} + \frac{B}{(1-2x)}$ . . . (2)

Put $x = \frac{1}{2}$

$\Rightarrow 5 + 1 = 2B$

$\Rightarrow B = 3$

Put $x = -\frac{1}{2}$

$\Rightarrow 5 - 1 = 2A$

$\Rightarrow A = 2$

(2) $\Rightarrow \frac{5+2x}{(1+2x)(1-2x)} = \frac{2}{(1+2x)} + \frac{3}{(1-2x)}$

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

$= A[1 - 2x - (2x)^2 + \ldots] + B[1 + 2x + (2x)^2 + \ldots]$

$= 2\sum_{n=2}^{\infty}(-1)^n 2^n x^n + 3\sum_{n=2}^{\infty} 2^n x^n$

$= 2\sum_{n=2}^{\infty}(-2)^n x^n + 3\sum_{n=2}^{\infty} 2^n x^n$

The required sequence is the coefficient of x^n in $G(x)$

Hence $S(n) = 2(-2)^n + 3(2)^n$

5. Identify the sequence having the expression $\frac{3-5x}{1-2x-3x^2}$ as a generating function.

Solution:

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

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

Now, $\frac{3-5x}{(1+2x)(1-2x)} = \frac{A}{(1-3x)} + \frac{B}{(1+x)}$ . . . (2)

$3 - 5x = A(1 + x) + B(1 - 3x)$

Put $x = -1$

$\Rightarrow 3 + 5 = 4B$

$\Rightarrow B = 2$

Put $x = \frac{1}{3}$

$\Rightarrow 3 - \frac{5}{3} = A\left(1 + \frac{1}{3}\right)$

$\Rightarrow \frac{4}{3} = \frac{4}{3}A$

$\Rightarrow A = 1$

$$(2) \Rightarrow \frac{3-5x}{(1+2x)(1-2x)} = \frac{1}{(1-3x)} + \frac{2}{(1+x)}$$

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

$$= A[1 + 3x + (3x)^2 + \dots] + B[1 - x + (x)^2 + \dots]$$

$$= \sum_{n=2}^{\infty} 3^n x^n + 3\sum_{n=2}^{\infty} (-1)^n x^n$$

The required sequence is the coefficient of x^n in $G(x)$

Hence $S(n) = 3^n + 2(-1)^n$

2.6 The Principle of Inclusion – Exclusion:

Formula

$$|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| + |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|$$

$$|A_1 \cup A_2 \cup A_3 \cup A_4| = |A_1| + |A_2| + |A_3| + |A_4| + |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| - |A_1 \cap A_4| - |A_2 \cap A_4| - |A_3 \cap A_4| + |A_1 \cap A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3| + |A_1 \cap A_2 \cap A_4| + |A_1 \cap A_3 \cap A_4| - |A_1 \cap A_2 \cap A_3 \cap A_4|$$

Problems under Inclusion and Exclusion:

1. How many positive integers not exceeding 1000 are divisible by 7 or 11?

Solution:

Let A denote the set of positive integers not exceeding 1000 that are divisible by 7.

Let B denote the set of positive integers not exceeding 1000 that are divisible by 11.

Then, $|A| = \left[\frac{1000}{7}\right] = [142.8] = 142$

$|B| = \left[\frac{1000}{11}\right] = [90.9] = 90$

$$|A \cap B| = \left[\frac{1000}{7\times11}\right] = [12.9] = 12$$

The number of positive integer not exceeding 1000 that are divisible either 7 or 77 is $|A \cup B|$

By principle of inclusion – exclusion,

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

$$= 142 + 90 - 12 = 220$$

There are 220 positive integer not exceeding 1000 divisible by either 7 or 11.

2. Determine n such that $1 \leq n \leq 100$ which are not divisible by 5 or by 7.

Solution:

Let A denote the number n, $1 \leq n \leq 100$ which is divisible by 5.

Let B denote the number n, $1 \leq n \leq 100$ which is divisible by 7.

Then, $|A| = \left[\frac{100}{5}\right] = [20] = 20$

$$|B| = \left[\frac{100}{7}\right] = [14.3] = 14$$

$$|A \cap B| = \left[\frac{1000}{5\times7}\right] = [2.8] = 2$$

Now, the number n, $1 \leq n \leq 100$ which is divisible by either 5 or 7 is $|A \cup B|$

By principle of inclusion – exclusion,

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

$$= 20 + 14 - 2 = 32$$

The number $n,\ 1 \leq n \leq 100$ which is divisible by either 5 or 7 is

$$= 100 - 32 = 68$$

There are 68 number not exceeding 100 that are not divisible by either 5 or 7.

3. Find the number of integers between 1 to 250 that are not divisible by any of the integers 2, 3, 5 and 7

Solution:

Let A denote the integer from 1 to 250 that are divisible by 2.

Let B denote the integer from 1 to 250 that are divisible by 3.

Let C denote the integer from 1 to 250 that are divisible by 5.

Let D denote the integer from 1 to 250 that are divisible by 7.

Then, $|A| = \left[\frac{250}{2}\right] = 125$

$|B| = \left[\frac{250}{3}\right] = 83$

$|C| = \left[\frac{250}{5}\right] = 50$

$$|D| = \left[\frac{250}{7}\right] = 35$$

The number of integer between 1 – 250 that are divisible by 2 & 3

$$|A \cap B| = \left[\frac{250}{2\times3}\right] = 41$$

$$|A \cap C| = \left[\frac{250}{2\times5}\right] = 25$$

$$|A \cap D| = \left[\frac{250}{2\times7}\right] = 17$$

$$|B \cap C| = \left[\frac{250}{3\times5}\right] = 16$$

$$|B \cap D| = \left[\frac{250}{3\times7}\right] = 11$$

$$|C \cap D| = \left[\frac{250}{5\times7}\right] = 7$$

The number of integer between 1 – 250 that are divisible by 2, 3 & 5

$$|A \cap B \cap C| = \left[\frac{250}{2\times3\times5}\right] = 8$$

$$|A \cap B \cap D| = \left[\frac{250}{2\times3\times7}\right] = 5$$

$$|A \cap C \cap D| = \left[\frac{250}{2\times5\times7}\right] = 3$$

$$|B \cap C \cap D| = \left[\frac{250}{3\times5\times7}\right] = 2$$

$$|A \cap B \cap C \cap D| = \left[\frac{250}{2\times3\times5\times7}\right] = 1$$

The number of integer between 1 – 250 that are divisible by 2, 3, 5 & 7 is

$|A \cap B \cap C \cap D|$

By principle of inclusion and exclusion,

$$|A \cup B \cup C \cup D|$$

$$= |A| + |B| + |C| + |D| - |A \cap B| - |A \cap C| - |A \cap D| - |B \cap C|$$

$$- |B \cap D| - |C \cap D| + |A \cap B \cap C| + |A \cap B \cap D| + |A \cap C \cap D|$$

$$+ |B \cap C \cap D| - |A \cap B \cap C \cap D|$$

$$= (125 + 83 + 50 + 35) - (41 + 25 + 17 + 16 + 11 + 7) + (8 + 5 + 3 + 2)$$

$$- 1$$

$$= 293 - 117 + 18 - 1 = 193$$

Now, the number of integer not divisible by any of 2, 3, 5 and 7

$$= 250 - 193 = 57$$

4. How many integers between 1 to 100 that are (i) not divisible by 7, 11 or 13 (ii) divisible by 3 but not by 7.

Solution:

Let A, B and C denote respectively the number of integer between 1 to 100 that are divisible by 7, 11 and 13 respectively.

Then, $|A| = \left[\frac{100}{7}\right] = 14$

$|B| = \left[\frac{100}{11}\right] = 9$

$|C| = \left[\frac{100}{13}\right] = 7$

$|A \cap B| = \left[\frac{100}{7\times11}\right] = 1$

$|A \cap C| = \left[\frac{100}{7\times13}\right] = 1$

$|B \cap C| = \left[\frac{100}{11\times13}\right] = 0$

$|A \cap B \cap C| = \left[\frac{100}{7\times11\times13}\right] = 0$

The number of integers between 1 – 100 that are divisible by 7, 11 and 13 is

$|A \cup B \cup C \cup D|$

By principle of inclusion and exclusion,

$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| - |B \cap D| +$

$|A \cap B \cap C| - |A \cap B \cap C|$

$= (14 + 9 + 7) - (1 + 1 + 0) + (0)$

$$= 30 - 2 = 28$$

Now, the number of integer not divisible by any of 7, 11 and 13

$$= 100 - 28 = 72$$

Let A and B denote the number between 1 – 100that are divisible by 3 and 7 respectively.

Then, $|A| = \left[\frac{100}{3}\right] = 33$

$|B| = \left[\frac{100}{7}\right] = 14$

$|A \cap B| = \left[\frac{100}{3\times7}\right] = 4$

The number of integers divisible by 3 but not by 7.

$$= |A| - |A \cap B| = 33 - 4 = 29$$

5. Find the number of integers between 1 to 100 that are divisible by (i) 2, 3, 5 and 7 (ii) 2, 3, 5 but not by 7

Solution:

Let A, B, C and D denote the number of positive integers between 1 to 100 that are divisible by 2, 3, 5 and 7 respectively.

Then, $|A| = \left[\frac{100}{2}\right] = 50$

$|B| = \left[\frac{100}{3}\right] = 33$

$|C| = \left[\frac{100}{5}\right] = 20$

$|D| = \left[\frac{100}{7}\right] = 14$

$|A \cap B| = \left[\frac{100}{2\times3}\right] = 16$

$|A \cap C| = \left[\frac{100}{2\times5}\right] = 10$

$|A \cap D| = \left[\frac{100}{2\times7}\right] = 7$

$|B \cap C| = \left[\frac{100}{3\times5}\right] = 6$

$|B \cap D| = \left[\frac{100}{3\times7}\right] = 4$

$|C \cap D| = \left[\frac{100}{5\times7}\right] = 2$

$|A \cap B \cap C| = \left[\frac{100}{7\times11\times13}\right] = 3$

$|A \cap B \cap D| = \left[\frac{100}{2\times3\times7}\right] = 2$

$|A \cap C \cap D| = \left[\frac{100}{2\times5\times7}\right] = 1$

$|B \cap C \cap D| = \left[\frac{100}{3\times5\times7}\right] = 0$

$$|A \cap B \cap C \cap D| = \left[\frac{100}{2\times3\times7\times11}\right] = 0$$

By principle of inclusion and exclusion,

$$|A \cup B \cup C \cup D|$$

$$= |A| + |B| + |C| + |D| - |A \cap B| - |A \cap C| - |A \cap D| - |B \cap C|$$

$$- |B \cap D| - |C \cap D| + |A \cap B \cap C| + |A \cap B \cap D| + |A \cap C \cap D|$$

$$+ |B \cap C \cap D| - |A \cap B \cap C \cap D|$$

$$= (50 + 33 + 20 + 14) - (16 + 10 + 7 + 6 + 4 + 2) + (3 + 2 + 1 + 0) - 0$$

$$= 117 - 45 + 6 = 78$$

(ii) The number of integers between 1 – 100 that are divisible by 2, 3, 5 but not by 7 $= |A \cap B \cap C| - |A \cap B \cap C \cap D|$

$$= 3 - 0 = 3$$

6. Determine the number of positive integers n, $1 \leq n \leq 1000$, that are not divisible by 2, 3 or 5 but are divisible by 7.

Solution:

Let A, B, C and D denote the number of positive integers between 1 to 1000 that are divisible by 2, 3, 5 and 7 respectively.

$$|D| = \left[\frac{1000}{7}\right] = [142.8] = 142$$

$$|A \cap B \cap C \cap D| = \left[\frac{1000}{2\times3\times5\times7}\right] = [4.7] = 4$$

The number between 1 – 1000 that are divisible by 7 but not divisible by 2, 3, 5 and $7 = |D| - |A \cap B \cap C \cap D|$

$$= 42 - 4 = 138$$

7. In a survey of 100 students, it was found that 30 studied Mathematics, 54 studied Statistics, 25 studied Operation research, 1 studied all the three subjects. 20 studied Mathematics and Statistics, 3 studied Mathematics and Operation Research and 15 studied Statistics and Operations Research, (i) How many students studied none of these subjects?(ii) How many students studied only Mathematics.

Solution:

Let A denote the students who studied Mathematics.

Let B denote the students who studied Statistics.

Let B denote the students who studied Operations Research.

It is given that $|A| = 30, |B| = 54,\ |C| = 25, |A \cap B| = 20, |A \cap C| = 3,$ $|B \cap C| = 15, |A \cap B \cap C| = 1$

By principle of inclusion – exclusion, the number of students playing either volleyball or hockey is

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

$$= 30 + 54 + 25 - 20 - 3 - 15 + 1$$

Students who studied none of these 3 subjects $= 100 - 72 = 28$

The number of students only studied Mathematics and Statistics $= 20 - 1 = 19$

The number of students only studied Mathematics and Operations Research

$= 3 - 1 = 2$

The number of students only studied Mathematics $= 30 - 19 - 2 - 1 = 8$

8. A survey of 500 from a school produced the following information. 200 play volleyball, 120 play hockey, 60 play both volleyball and hockey. How many are not playing either volleyball or hockey?

Solution:

Let A denote the students who play volleyball.

Let B denote the students who play hockey.

It is given that $n = 500, |A| = 200, |B| = 120, |A \cap B| = 60$

By principle of inclusion – exclusion, the number of students playing either volleyball or hockey is

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

$$= 200 + 120 - 60 = 260$$

The number of students not playing either volleyball or hockey is

$$= 500 - 260 = 240$$

9. Out of 100 students in a college, 38 play tennis, 57 play cricket and 31 play hockey, 9 play cricket and hockey, 10 play hockey and tennis, 12 play tennis and cricket. How many play (i) all three games (ii) just one game (iii) tennis and cricket but not hockey. (Assume that each student plays atleast one game)

Solution:

Let T, C and H denote the set of students playing Tennis, Cricket and Hockey respectively.

Given that $|T| = 38, |C| = 57,\ |H| = 31, |T \cap C| = 12, |T \cap H| = 10,$

$|C \cap H| = 9, |T \cup C \cup H| = 100$

Now, the number of integer who play all three games $= |T \cap C \cap H|$

By principle of inclusion – exclusion,

$$|T \cup C \cup H| = |T| + |C| + |H| - |T \cap C| - |T \cap H| - |C \cap H| + |T \cap C \cap H|$$

$$100 = 38 + 5 + 31 - 103 - 12 - 10 + 9 + |T \cap C \cap H|$$

$$|T \cap C \cap H| = 100 - 126 + 31 = 5$$

Number of students who play all 3 games = 5

Number of students playing just one game = number of students Tennis only + number of students playing cricket only + number of students playing Hockey only

$$= 21 + 41 + 17 = 79$$

The number of students playing Tennis and Cricket but not Hockey

$$= |T \cap C| - |T \cap C \cap H|$$

$$= 12 - 5 = 7$$

10. A survey of 500 television watchers produced the following information. 285 watch Hockey games. 195 watch Football games. 115 watch basketball games.70 watch football and hockey games. 50 watch hockey and basketball games and 30 watch football and basketball games. 50 do not watch any of the three games. How many people watch exactly one of the three games.

Solution:

Let H denotes the television watchers who watch Hockey.

Let F denotes the television watchers who watch Football.

Let B denotes the television watchers who watch Basket Ball.

Given that $|H| = 285, |F| = 195,\ |B| = 115, |H \cap F| = 70, |H \cap B| = 50,$

$|F \cap B| = 30$

Let x be the number of television watchers who watch all three games.

Now, we have

Given 50 members does not watch any of the three games.

Hence, $(165 + x) + (95 + x) + (35 + x) + (70 - x) + (50 - x) + (30 - x) + x = 500$

$\Rightarrow 445 + x = 500$

$\Rightarrow x = 55$

Number of students who watches exactly one game is

$= 165 + x + 95 + x + 35 + x$

$= 295 + 3 \times 55 = 295 + 165 = 460$

11. A total of 1232 have taken a course in Tamil, 879 have taken a course in Telugu, and 114 have taken a course in Hindi. Further 103 have taken a course in both Tamil and Telugu, 23 have taken a course in Tamil and Hindi, and 14 have taken a course in Telugu and Hindi. If 2092 students have taken

atleast one of the Tamil, Telugu and Hindi, how many students have taken a course in all three languages.

Solution:

Let A denote the students who have taken a course in Tamil.

Let B denote the students who have taken a course in Telugu.

Let C denote the students who have taken a course in Hindi.

It is given that $|A| = 1232, |B| = 879,\ |C| = 114, |A \cap B| = 103, |A \cap C| = 23,$ $|B \cap C| = 14, |A \cup B \cup C| = 2092$

By principle of inclusion – exclusion, the number of students playing either volleyball or hockey is

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

$$2092 = 1232 + 879 + 114 - 103 - 23 - 14 + |A \cap B \cap C|$$

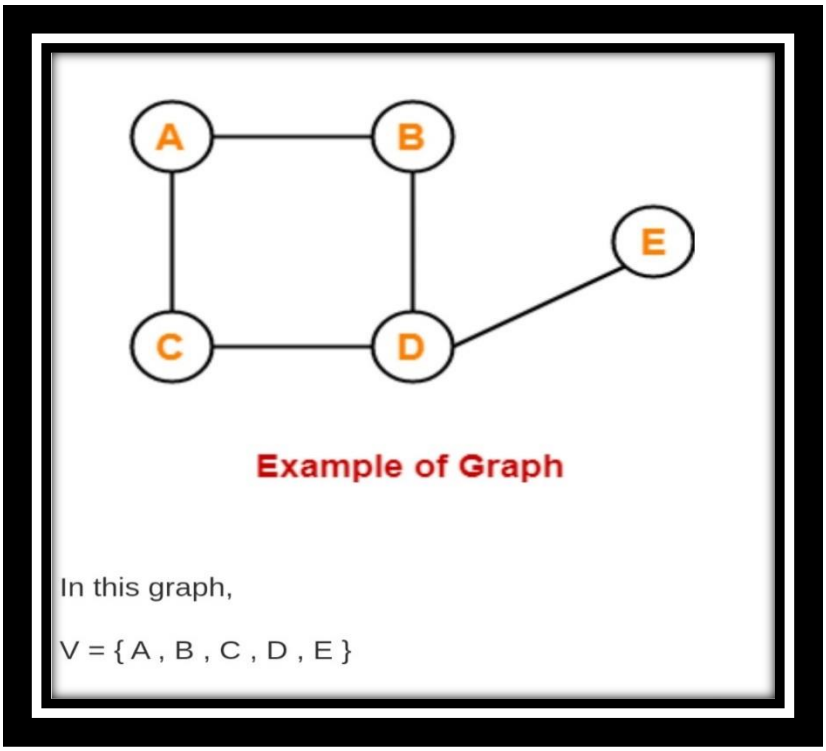
$$|A \cap B \cap C| = 2232 - 2225 = 7$$

Therefore, there are 7 students who have taken the course in Tamil, Telugu and Hindi.

Graph:

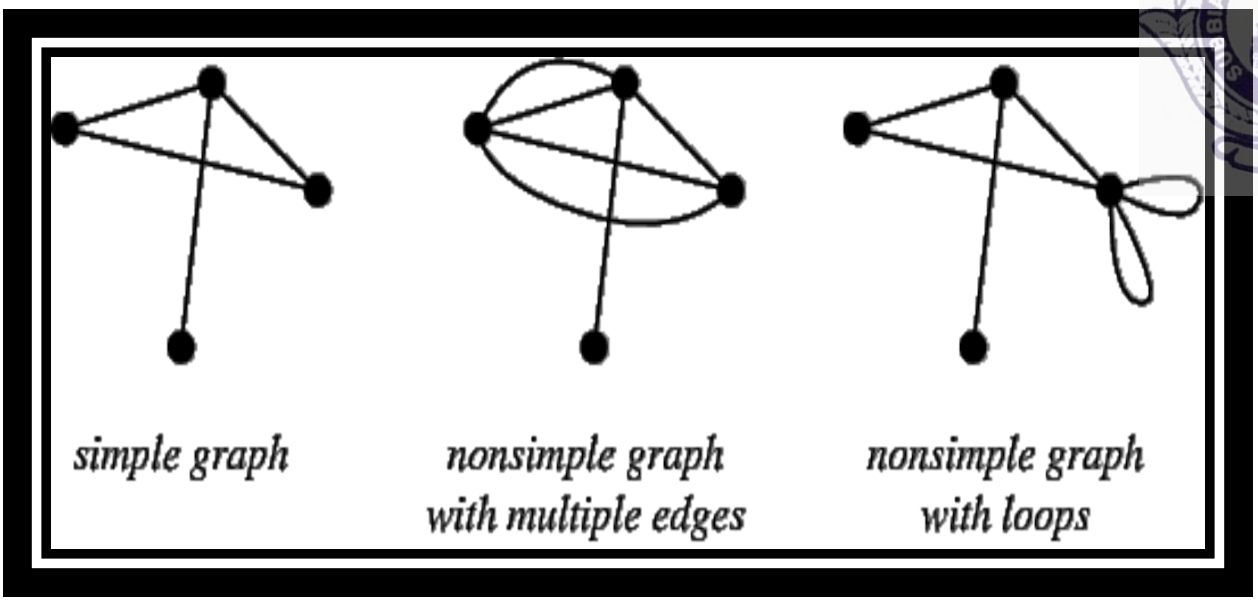
A graph $G = (V, E, \phi)$ consists of a non – empty set $V = \{V_1, V_2, \ldots\}$ called the set of nodes (Points, Vertices) of the graph, $E = \{e_1, e_2, \ldots\}$ is said to be the set of edges of the graph, and , ϕ is a mapping from the set of edges E to set of ordered or unordered pairs of elements of V.

The vertices are represented by points and each edge is represented by a line digrammatically.



Self Loop:

If there is an edge from v_i to v_i then that edge is called self loop or simply loop.



Parallel edges:

If two edges have same end points then the edges are called parallel edges.

Incident:

If the vertex v_i is an end vertex of some edge e_k then e_k is said to be incident with v_i.

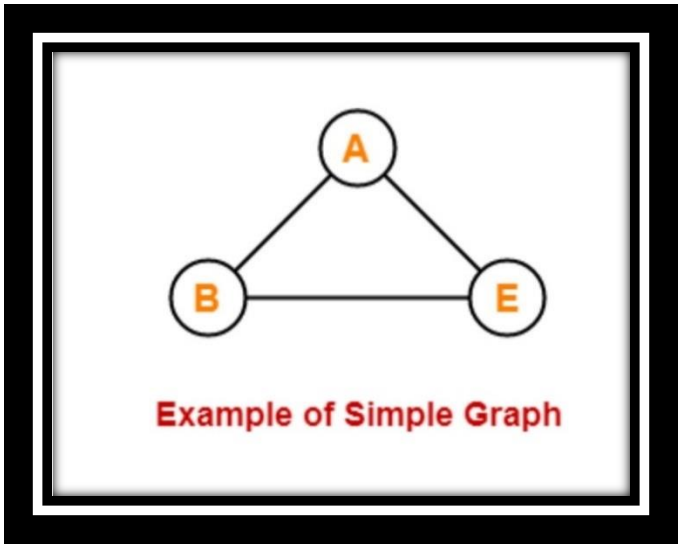
Adjacent edges and vertices:

Two edges are said to be adjacent if they are incident on a common vertex.

Two vertices v_i and v_j are said to be adjacent if $v_i v_j$ is an edge of the graph.

Simple Graph:

A graph which has neither self loops nor parallel edges is called a simple graph.



Isolated vertex:

A vertex having no edge incident on it is called an isolated vertex. It is obvious that for an isolated vertex degree is zero.

Pendent vertex:

If the degree of any vertex is one, then that vertex is called pendent vertex

Directed edges:

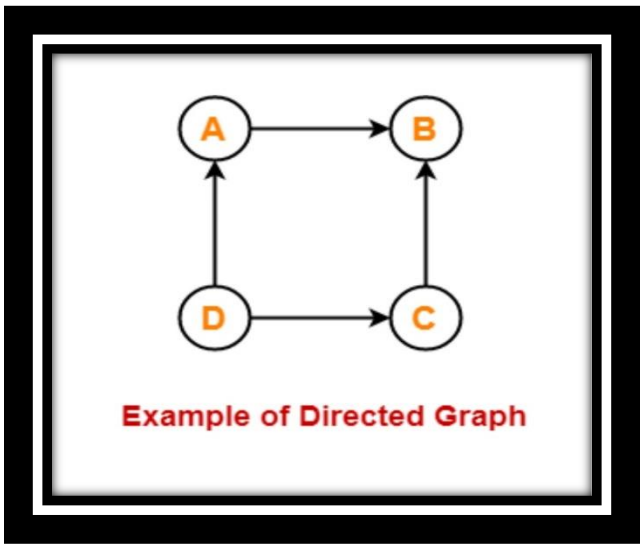
In a graph $G = (V, E)$, on edge which is associated with an ordered pair of $V \times V$ is called a directed edge of G.

Undirected edge:

If an edge which is associated with an unordered pair of nodes is called an undirected edge.

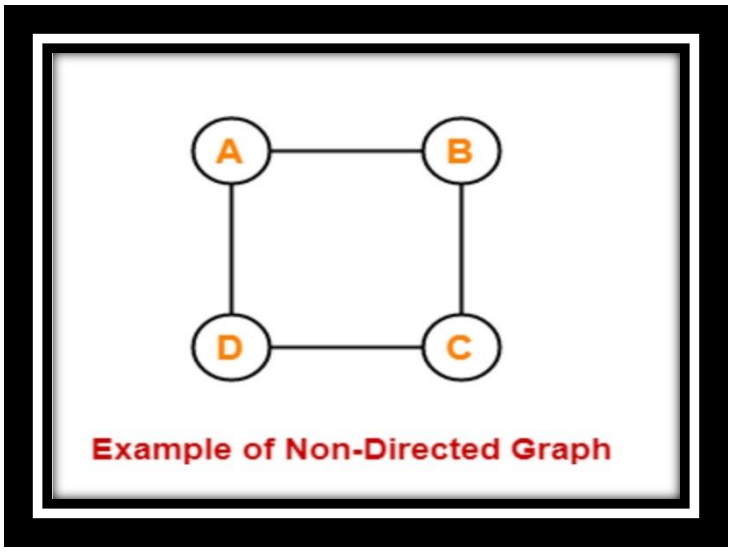
Digraph:

A graph in which every edge is directed edge is called a digraph or directed graph.



Undirected graph:

A graph in which every edge is undirected is called an undirected graph.

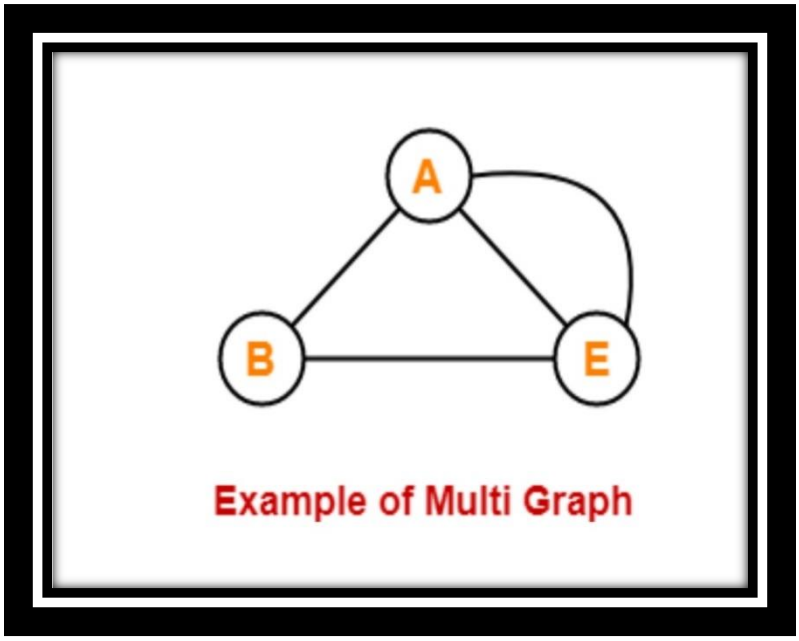


Mixed graph:

If some edges are directed and some are undirected in a graph, the graph is called mixed graph.

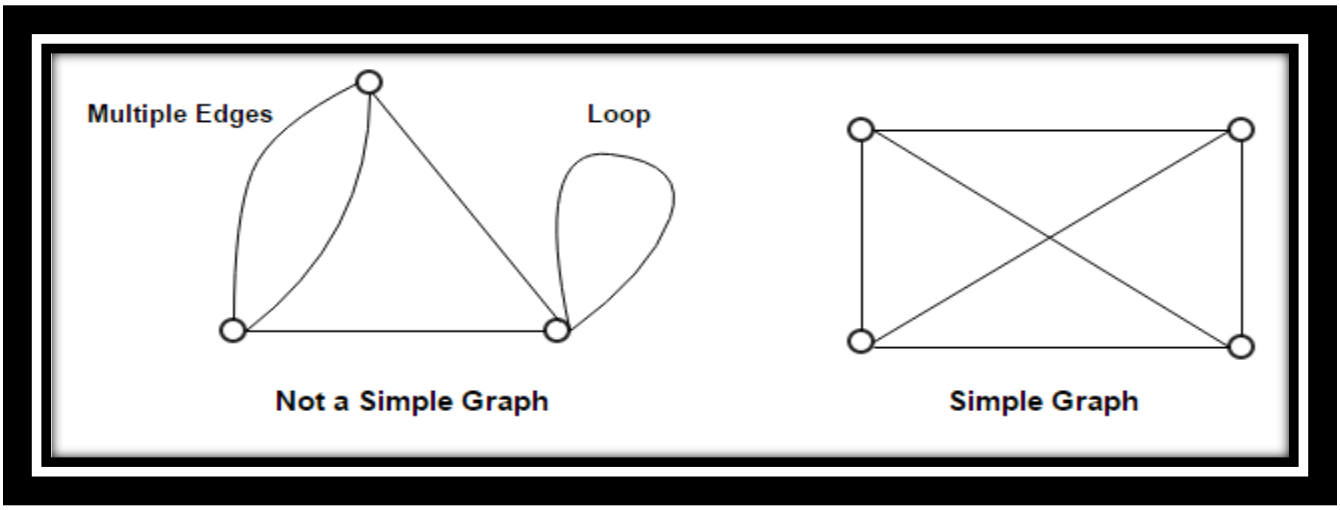
Multigraph:

A graph which contains some parallel edges is called a multigraph.



Pseudograph:

A graph in which loops are parallel edges are allowed is called a Pseudo graph.

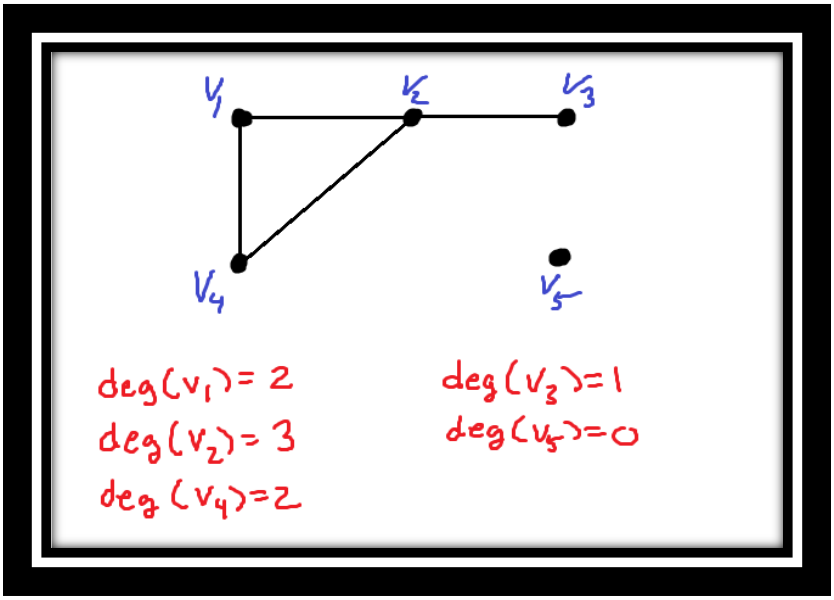


Graph Terminology:

Degree of a vertex:

The number of edges incident at the vertex v_i is called the degree of the vertex with self loops counted twice and it is denoted by $d(v_i)$.

Example:



(i) $d(v_1) = 2$

(ii) $d(v_2) = 3$

(iii) $d(v_3) = 1$

(iv) $d(v_4) = 2$

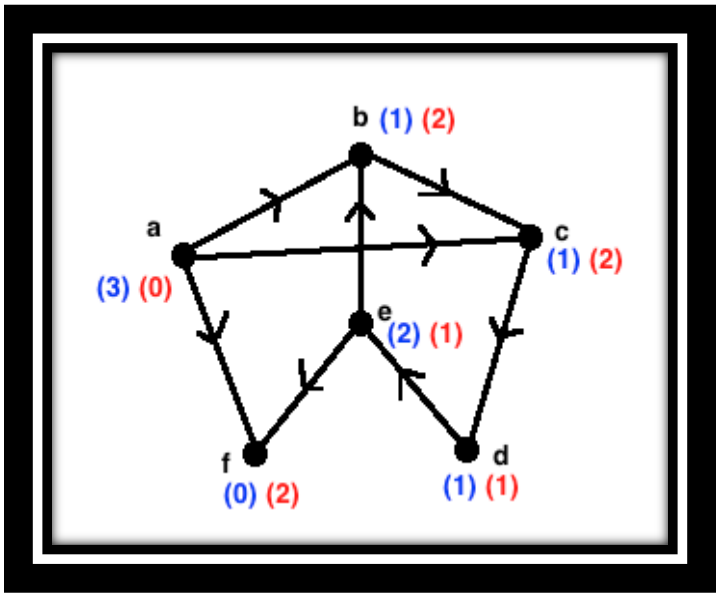
(v) $d(v_5) = 0$

In – degree and out – degree of a directed graph:

In a directed graph, the in – degree of a vertex V, denoted by $deg^-(V)$and defined by the number of edges with V as their terminal vertex.

The out – degree of V, denoted by $deg^+(V)$, is the number of edges with V as their initial vertex.

Example:



In – degree	Out – degree	Total degree
$deg^-(a) = 0$	$deg^+(a) = 3$	$deg(a) = 3$
$deg^-(b) = 2$	$deg^+(b) = 1$	$deg(b) = 3$
$deg^-(c) = 2$	$deg^+(c) = 1$	$deg(c) = 3$

$deg^-(d) = 1$	$deg^+(d) = 1$	$deg(d) = 2$
$deg^-(e) = 1$	$deg^+(e) = 2$	$deg(e) = 3$
$deg^-(f) = 2$	$deg^+(f) = 0$	$deg(f) = 2$

Note:

A loop at a vertex contributes 1 to both the in – degree and the out – degree of this vertex.

Theorem: 1(The Handshaking Theorem)

Let $G = (V, E)$ be an undirected graph with e edges then $\sum_{v \in V} deg(v) = 2e$.

The sum of degrees of all the vertices of an undirected graph is twice the number of edges of the graph and hence even.

Proof:

Since every edge is incident with exactly two vertices, every edge contributes 2 to the sum of the degree of the vertices.

All the 'e' edges contribute $(2e)$ to the sum of the degrees of vertices.

Hence $\sum_{v \in V} deg(v) = 2e$

Hence the proof.

Theorem: 2

In a undirected graph, the number of odd degree vertices are even.

Proof:

Let V_1 and V_2 be the set of all vertices of even degree and set of all vertices of odd degree, respectively, in a graph $G = (V, E)$.

$\Rightarrow \sum d(v) = \sum_{v_i \in V_1} d(v_i) + \sum_{v_j \in V_2} d(v_j)$

By Handshaking theorem, we have

$$\Rightarrow 2e = \sum_{v_i \in V_1} d(v_i) + \sum_{v_j \in V_2} d(v_j)$$

Since each $\deg(v_i)$ is even, $\sum_{v_i \in V_1} d(v_i)$ is even

As left hand side of equation (1) is even and the first expression of the RHS of (1) is even, we have the second expression on the RHS must be even.

$\sum_{v_j \in V_2} d(v_j)$ is even.

Since each $d(v_j)$ is odd, the number of terms contained in $\sum_{v_j \in V_2} d(v_j)$ is even.

i.e., The number of vertices of odd degree is even.

Hence the proof.

Theorem: 3

The maximum number of edges in a simple graph with "n" vertices is $\frac{n(n-1)}{2}$

Proof:

We prove this theorem by the principle of Mathematical induction.

For $n = 1$, a graph with one vertex has no edges.

The result is true for $n = 1$.

For $n = 2$, a graph with 2 vertices may have atmost one edge.

$\Rightarrow \frac{2(2-1)}{2} = 1$

The result is true for $n = 2$.

Assume that the result is true for $n = k$.

i.e., a graph with k vertices has atmost $\frac{k(k-1)}{2}$ edges.

When $n = k + 1$, let G be a graph having "n" vertices and G' be the graph obtained from G by deleting one vertex say $v \in V(G)$.

Since G' has k vertices, then by the hypothesis G' has atmost $\frac{k(k-1)}{2}$ edges.

Now add the vertex "v" to G'. Such that "v" may be adjacent to all the k vertices of G'.

The total number of edges in G are,

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

$$= \frac{k^2+k}{2}$$

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

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

The result is true for $n = k + 1$

Hence the maximum number of edges in a simple graph with "n" vertices is $\frac{n(n-1)}{2}$.

Hence the proof.

Theorem: 4

If all the vertices of an undirected graph are each of degree k, show that the number of edges of the graph is a multiple of k.

Proof:

Let $2n$ be the number of vertices of the given graph. . . . (1)

Let n_e be the number of edges of the given graph.

By Handshaking theorem, we have $\sum_{i=1}^{2n} \deg V_i = 2\, n_e$

$\Rightarrow 2nk = 2n_e$ using (1)

$\Rightarrow nk = n_e$

$\Rightarrow$ number of edges = multiple of k.

The number of edges of the given graph is a multiple of k.

Example:1

How many edges are there in a graph with ten vertices each of degree six.

Solution:

Let e be the number of edges of the graph.

$\Rightarrow 2e$ = Sum of all degrees

$= 10\ X\ 6 = 60$

$\Rightarrow 2e = 60$

$\Rightarrow e = 30$

There are 30 edges.

Example: 2

Can a simple graph exist with 15 vertices of degree 5.

Solution:

$\Rightarrow 2e = \sum d(v)$

$\Rightarrow 2e = 15X\ 5 = 75$

$\Rightarrow e = \frac{75}{2}$

Which is not an integer.

Such a graph does not exist.

(or) By theorem (2) in a graph the number of odd degree vertices is even.

Therefore, it is not possible to have 15 vertices, which is of odd degree.

Such a graph does not exist.

Example: 3

For the following degree sequences 4, 4, 4, 3, 2 find if there exist a graph or not.

Solution:

Sum of the degree of all vertices $= 4 + 4 + 4 + 3 + 2 = 17$

Which is an odd number.

Such a graph does not exist.

Example: 4

Does there exist a simple graph with five vertices of the following degrees? If so draw such graph (a) 1, 1, 1, 1, 1 (b) 3, 3, 3, 3, 2

Solution:

We know that in any graph the number of odd degree vertices is always a even.

In case (a) number of odd degree vertices is 5 (not an even)

Such graph does not exist.

For case (b)

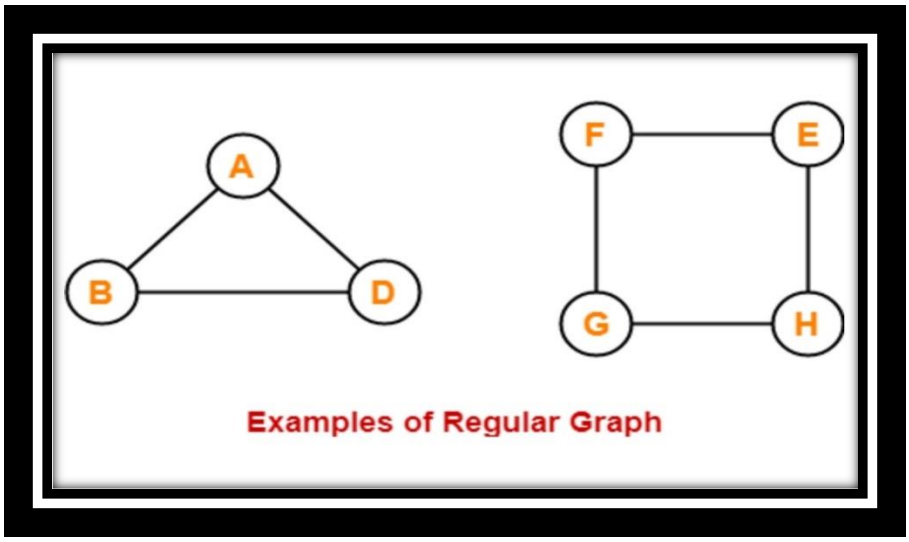
Sum of degree = 14 = even

The graph exist.

Special Types of Graphs

Regular Graph

If every vertex of a simple graph has the same degree, then the graph is called a regular graph.



If every vertex in a regular graph has degree k, then the graph is called k – regular.

Complete Graph

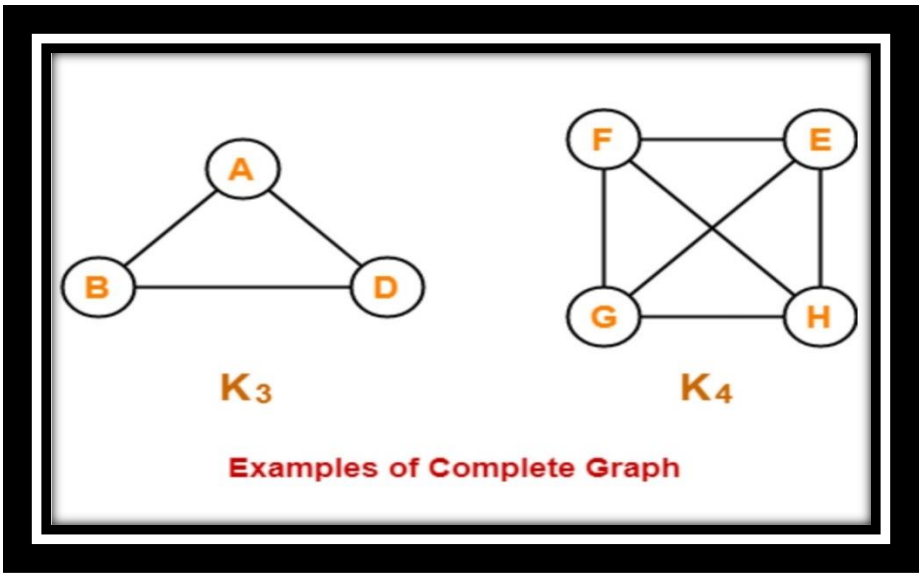
In a graph, if there exist an edge between every pair of vertices, then such a graph is called complete graph.

In a graph if every pair of vertices are adjacent then such a graph is called complete graph.

If is noted that, every complete graph is a regular graph. In fact every complete graph with n vertices is a $(n - 1)$ regular graph.

The complete graph on n vertices is denoted by k_n. The graphs k_n for

$n = 1, 2, 3, 4, 5$ are



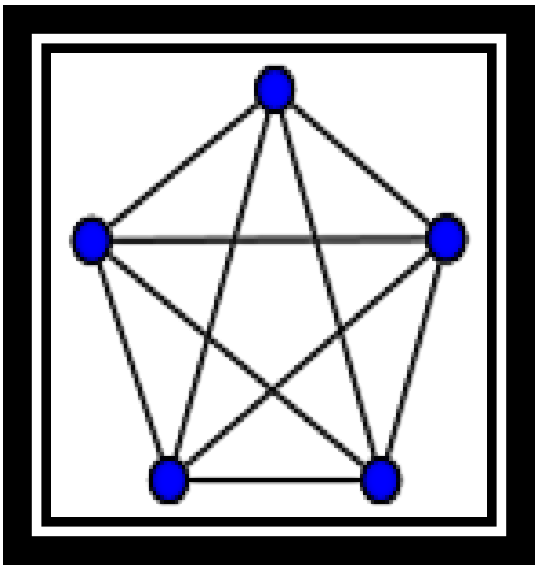
Example: 1

Draw the complete graph k_5 with vertices A, B, C, D, E. Draw all complete sub graph of k_5 with 4 vertices.

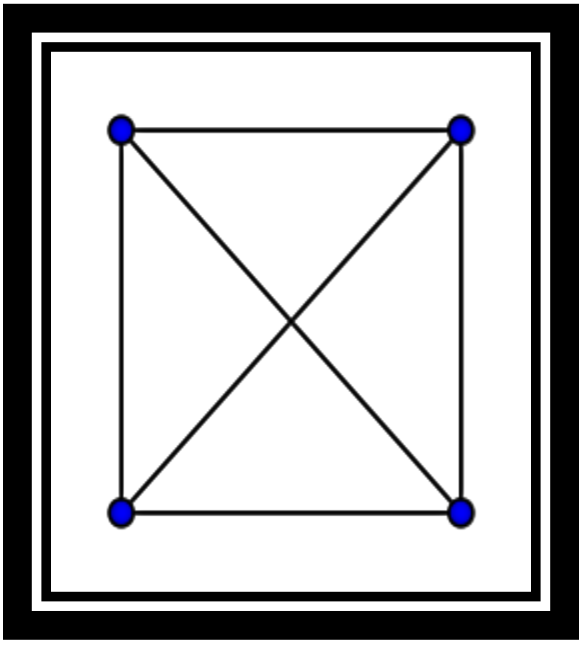
Solution:

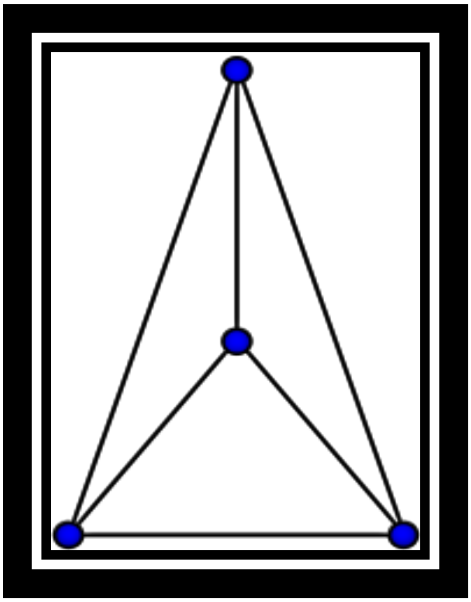
In a graph, if there exist an edge between every pair of vertices, then such a graph is called complete graph.

i.e., In a graph if every pair of vertices are adjacent, then such a graph is called complete graph. Complete graph k_5 is



Now, complete subgraph of k_5 with 4 vertices are





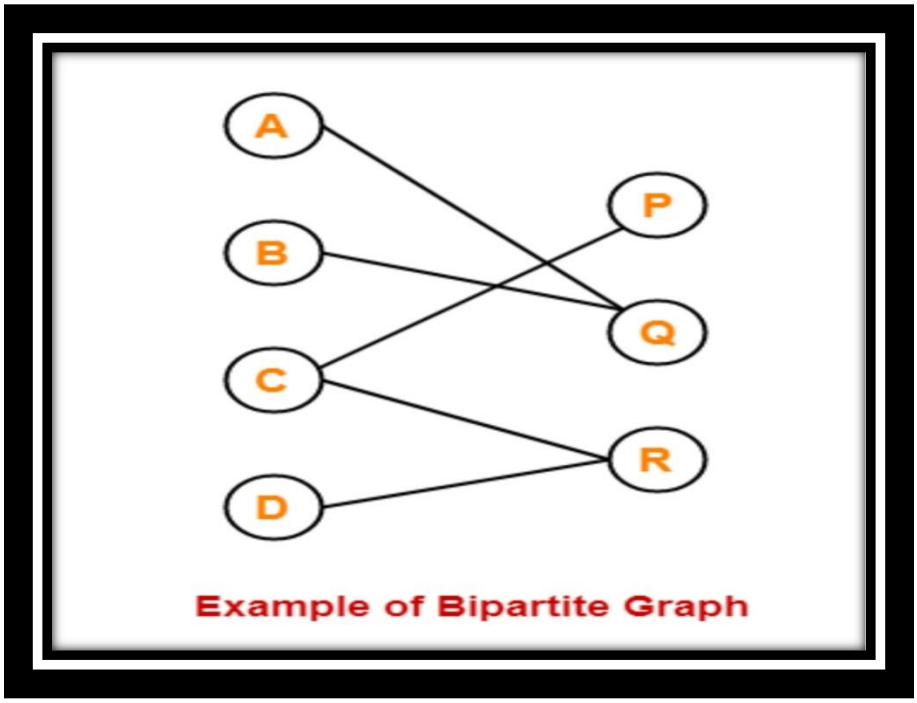
Bipartite Graph

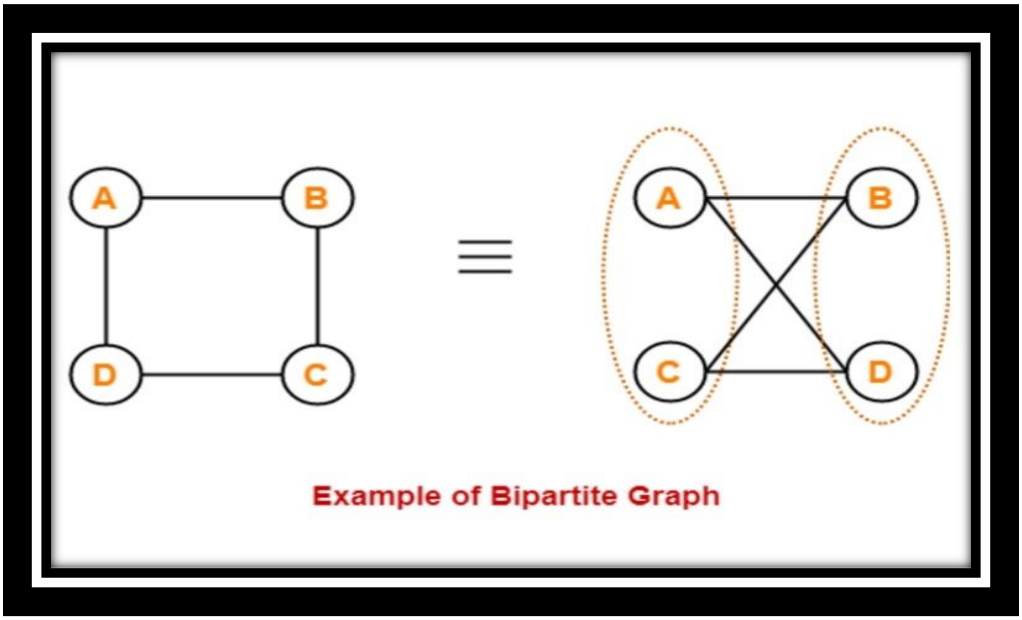
A graph G is said to be bipartite if its vertex set $V(G)$ can be partitioned into two disjoint non empty sets V_1 and V_2, $V_1 \cup V_2 = V(G)$, such that every edge in $E(G)$

has one end vertex in V_1 and another end vertex in V_2 . (So that no edges in , connects either two vertices in V_1 or two vertices in V_2.)

For example, consider the graph G

Then G is a Bipartite graph.



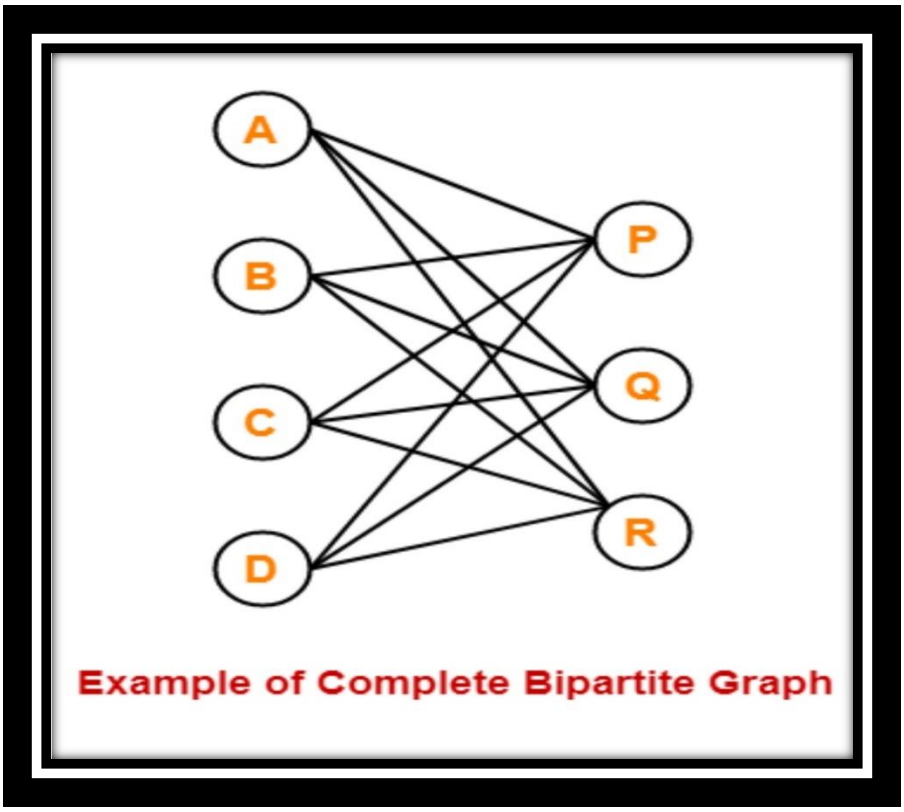


Example of Bipartite Graph

Complete Bipartite Graph:

A bipartite graph G, with the partition V_1 and V_2, is called complete bipartite graph, if every vertex in V_1 is adjacent to every vertex in V_2. Clearly, every vertex in V_2 is adjacent to every vertex in V_1.

A complete bipartite graph with 'm' and 'n' vertices in the bipartition is denoted by $k_{m,n}$.



Subgraph:

A graph $H = (V', E')$ is called a subgraph of $G = (V, E)$, if $V' \subseteq V$ and $E' \subseteq E$.

In other words, a graph H is said to be a subgraph is said to be a subgraph of G, if all the vertices and all the edges of H are in G and if the adjacency is preserved in H exactly as in G.

Hence, we have the following

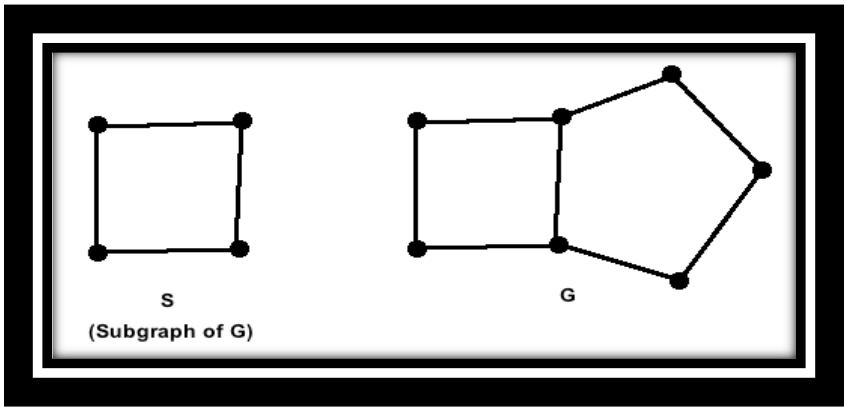
(i)Each graph has its own subgraph.

(ii)A single vertex in a graph G is a subgraph of G.

(iii)A single edge in G, together with its end vertices is also a subgraph of G.

(iv)A subgraph of a subgraph of G is also a subgraph of G.

(v)H is a proper subgraph of G if $H \neq G$.



Graph representation:

Adjacency Matrix of a simple graph:

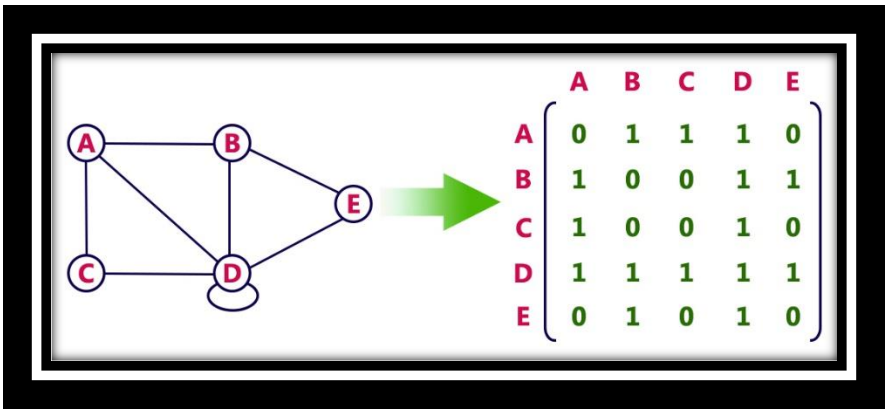
Let $G = (V, E)$ be a simple graph with n – vertices $\{v_1, v_2, \ldots, v_n\}$. Its adjacency matrix is denoted by $A = [a_{ij}]$ and defined by

$$A = [a_{ij}] = \begin{cases} 1, if\ there\ exist\ an\ edge\ between\ v_i\ and\ v_j \\ 0, otherwise \end{cases}$$

Example: 1

Find adjacency matrix of the graph given below.

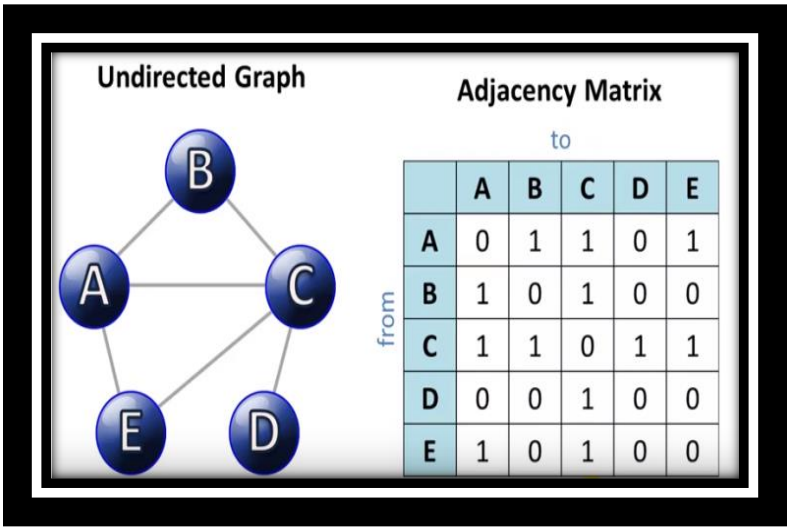
Solution:



Example: 2

Find adjacency matrix of the graph given below.

Solution:



Incidence matrices:

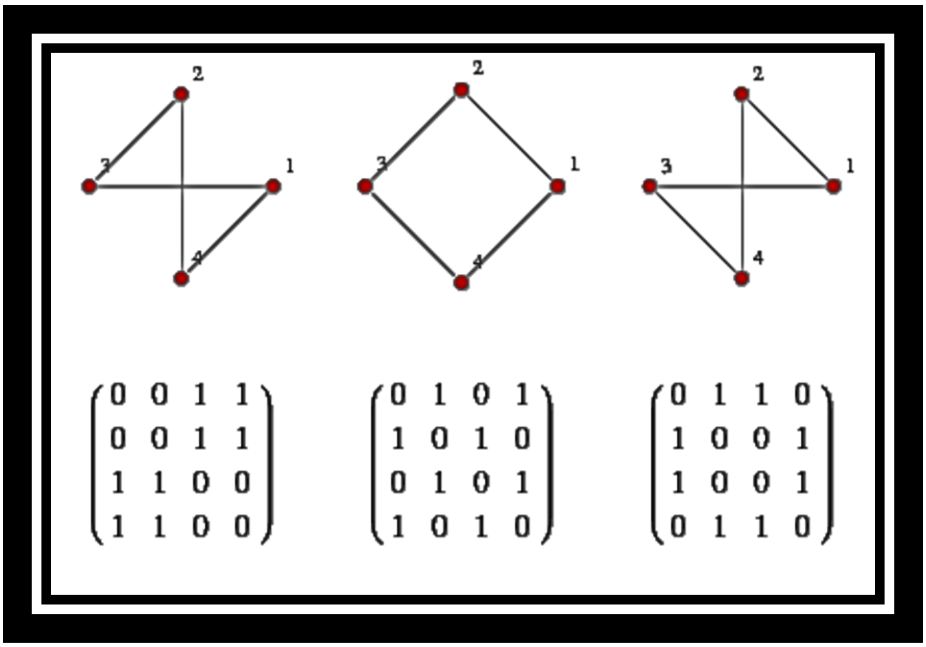
Let $G = (V, E)$ be an undirected graph with n vertices $\{V_1, V_2, \ldots, V_n\}$ and m edges $\{e_1, e, \ldots, e_m\}$. Then the $(n \times m)$ matrix $B = [b_{ij}]$, where

$$B = [b_{ij}] = \begin{cases} 1, when\ edge\ e_j\ incident\ on\ V_i \\ 0, otherwise \end{cases}$$

Example: 1

Find incidence matrix of the following graph and your observations regarding the entries of B.

Solution:



$$\begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$$

Path Matrix:

Let $G = (V, E)$ be a simple digraph in which $|V| = n$ and the nodes of g are assumed to be ordered. An $n \times n$ matrix P whose elements are given by

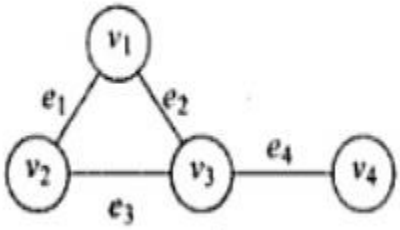
$$P_{ij} = \begin{cases} 1, If\ there\ exists\ a\ path\ from\ V_i\ to\ V_j \\ 0, otherwise \end{cases}$$

is called a path matrix (reachability matrix) of the graph G.

Example: 1

Find path matrix

Solution:



(a) Graph G_{16}

$$P(v_1, v_4) = \begin{array}{c} \\ 1 \\ 2 \end{array} \begin{array}{c} \begin{array}{cccc} e_1 & e_2 & e_3 & e_4 \end{array} \\ \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix} \end{array} \begin{array}{l} \text{Paths:} \\ 1: \{e_2, e_4\} \\ 2: \{e_1, e_3, e_4\} \end{array}$$

(b) Path matrix between v_1 v_4 of G_{16}

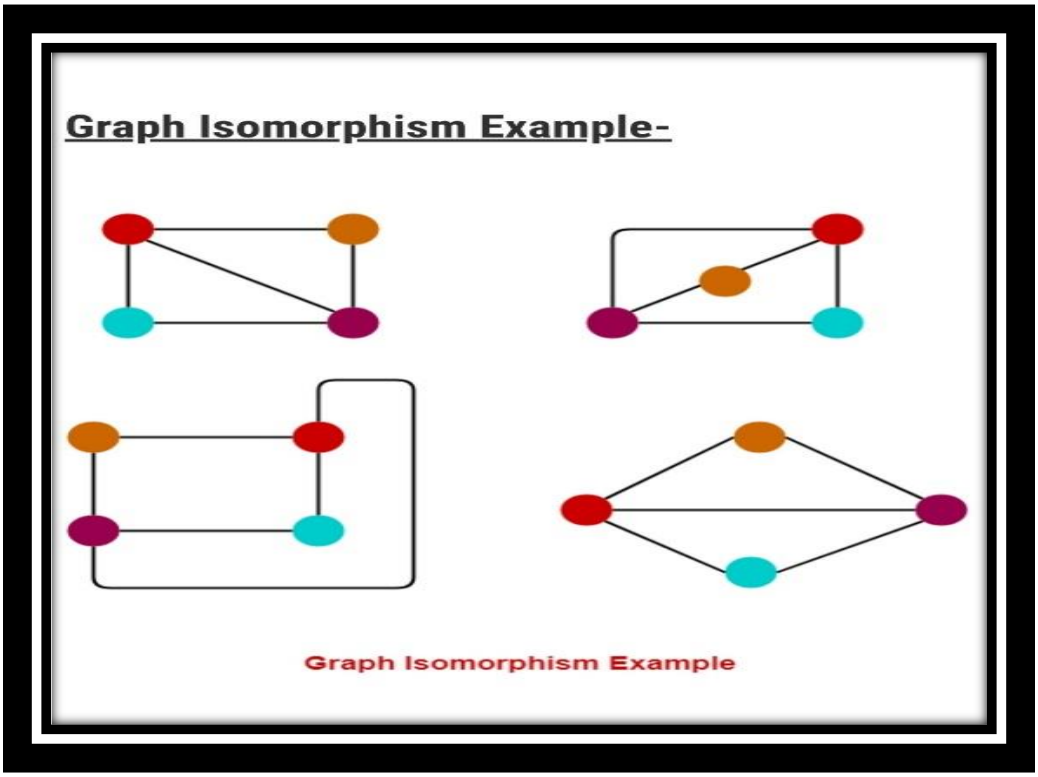
Note:

Path Matrix is very useful in communications and transportation networks.

Graph Isomorphism:

Two graphs G_1 and G_2 are said to be isomorphic to each other, if there exist a one – to –one correspondence between the vertex sets which preserves adjacency of the vertices.

The Graph $G_1 = (V_1, E_1)$ is isomorphic to the graph $G_2 = (V_2, E_2)$ if there is a one – to – one correspondence between the vertex sets V_1 and V_2 and the edge sets E_1 and E_2 in such a way that if e_1 is incident on u_1 and V_1 in G_1, then the corresponding edge e_2 in G_2 is incident on u_2 and V_2 which correspondence is called graph isomorphism.



However, the definition of isomorphism of two graphs were easy, but the given graph having "n" vertices itself has n! ways of one – to – one correspondence.

So, before going to isomorphism, we can verify whether they have the same number of vertices and edges and if the degree sequence of the graphs are same. If not, the we can say the graphs are not isomorphic.

Note:

If G_1 and G_2 are isomorphic then G_1 and G_2 have

(i)The same number of vertices.

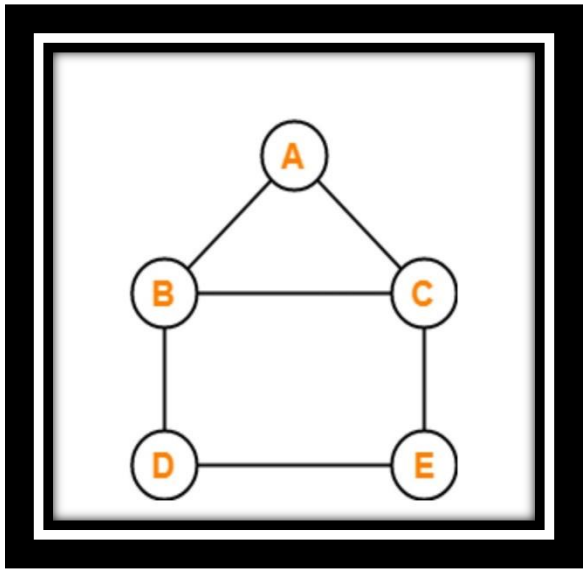
(ii)The same number of edges.

(iii)An equal number of vertices with a given degree.

However, these conditions are not sufficient for graph isomorphism.

Paths, Reachability and Connectedness:

A path is a graph is a sequence $v_1, v_2, v_3, \ldots, v_k$ of vertices each adjacent to the next. In other words, starting with the vertex v_1, one can travel along edges $(v_1, v_2), (v_2, v_3)$, ... and reach the vertex v_k.



Length of the path:

The number of edges appearing in the sequence of a path is called the length of path.

Cycle or Circuit:

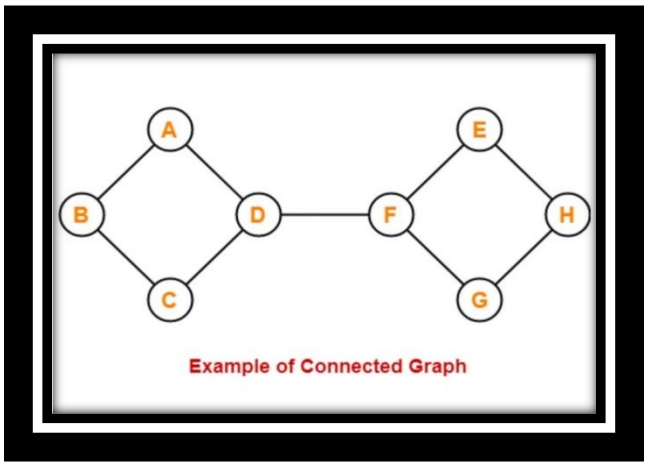
A path which originates and ends in the same node is called a cycle of circuit.

A path is said to be simple if all the edges in the path are distinct.

A path in which all the vertices are traversed only once is called an elementary path.

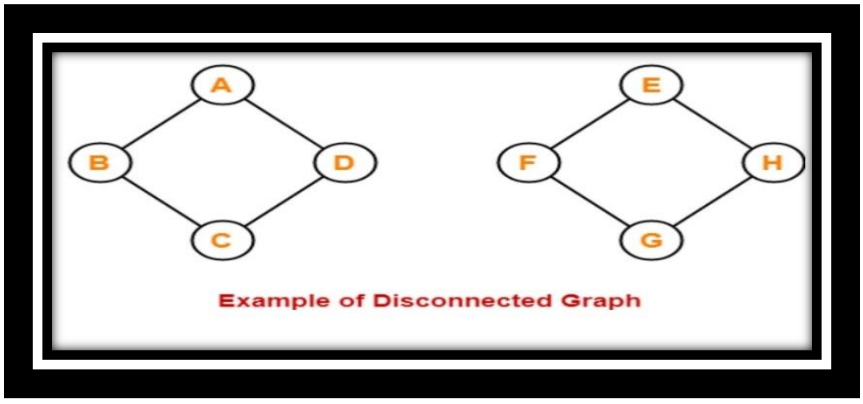
Connected Graph:

An directed graph is said to be connected if any pair of nodes are reachable from one another. That is, there is a path between any pair of nodes.



Disconnected graph:

A graph which is not connected is called disconnected graph.



Theorem: 1

If a graph has n vertices and a vertex v is connected to a vertex w, then there exists a path from v to w of length not more than $(n-1)$.

Proof:

Let $v, u_1, u_2, \ldots, u_{m-1}, w$ be a path in G from v to w.

By definition pf path, the vertices $v, u_1, u_2, \ldots, u_{m-1}$ and w all are distinct.

As G, contains only "n" vertices, it follows that $m + 1 \leq n$

$$\Rightarrow m \leq n - 1$$

Hence the proof.

Theorem: 2

Prove that a simple graph with n vertices must be connected if it has more than $\frac{(n-1)(n-2)}{2}$ edges.

Proof:

Let G be a simple graph with n vertices and more than $\frac{(n-1)(n-2)}{2}$ edges.

Suppose if G is not connected, then G must have atleast two components. Let it be $G_1$and G_2.

Let V_1 be the vertex set of G_1 with $|V_1| = m$. If V_2 is the vertex set of G_2, then $|V_2| = n - m$.

Then (i) $1 \leq m \leq n-1$

(ii) There is no edge joining a vertex of V_1 and a vertex of V_2.

(iii) $|V_2| = n - m \geq 1$

Now, $|E(G)| = |E(G_1 \cup G_2)|$

$$= |E(G_1)| + |E(G_2)|$$

$$\leq \frac{m(m-1)}{2} + \frac{(n-m)(n-m-1)}{2}$$

$$= \frac{1}{2}[m^2 - m + n(n-m-1) - m(n-m-1)]$$

$$= \frac{1}{2}[n(n-1) - nm - m(n-m-1) + m^2 - m]$$

$$= \frac{1}{2}[(n-1)(n-2) + 2(n-1) - 2nm + m^2 + m + m^2 - m]$$

Adding and Subtracting $2n-2$

$$= \frac{1}{2}[(n-1)(n-2) + 2n - 2 - 2nm + 2m^2]$$

$$= \frac{1}{2}[(n-1)(n-2) + 2n(1-m) + 2(m^2-1)]$$

$$= \frac{1}{2}[(n-1)(n-2) - 2n(m-1) + 2(m-1)(m+1)]$$

$$= \frac{1}{2}[(n-1)(n-2) - 2(m-1)(n-m-1)]$$

$|E(G)| \leq \frac{(n-1)(n-2)}{2}$, Since $(m-1)(n-m-1) \geq 0$ for $1 \leq m \leq n-1$

Which is a contradiction as G has more than $\frac{(n-1)(n-2)}{2}$ edges.

Hence G is a connected graph.

Hence the proof.

Theorem: 3

Let G be a simple graph with n vertices. Show that if $\delta(G) \geq \left[\frac{n}{2}\right]$, then G is connected where $\delta(G)$ is minimum degree of the graph G.

Proof:

Let u and v be any two distinct vertices in the graph G.

We claim that there is a $u - v$ path in G.

Suppose uv is not an edge of G. Then, X be the set of all vertices which are adjacent to u and Y be the set of all vertices which are adjacent to v.

Then $u, v \notin X \cup Y$. (Since G is a simple graph)

And hence $|X \cup Y| \leq n-2$

We have $|X| = deg(u) \geq \delta(G) \geq \left\lceil \frac{n}{2} \right\rceil$ and $|Y| = deg(v) \geq \delta(G) \geq \left\lceil \frac{n}{2} \right\rceil$

Now, $|X| + |Y| \geq \left\lceil \frac{n}{2} \right\rceil + \left\lceil \frac{n}{2} \right\rceil = n \geq n - 1$

We know that $|X \cup Y| = |X| + |Y| - |X \cap Y|$

$n - 2 \geq |X \cup Y| \geq n - 1 - |X \cap Y|$

We have, $|X \cap Y| \geq 1 \Rightarrow X \cap Y \neq \emptyset$

Now, take a vertex $w \in X \cap Y$. Then uvw is a $u - v$ path in G.

Thus for every pair of distinct vertices of G there is a path between them.

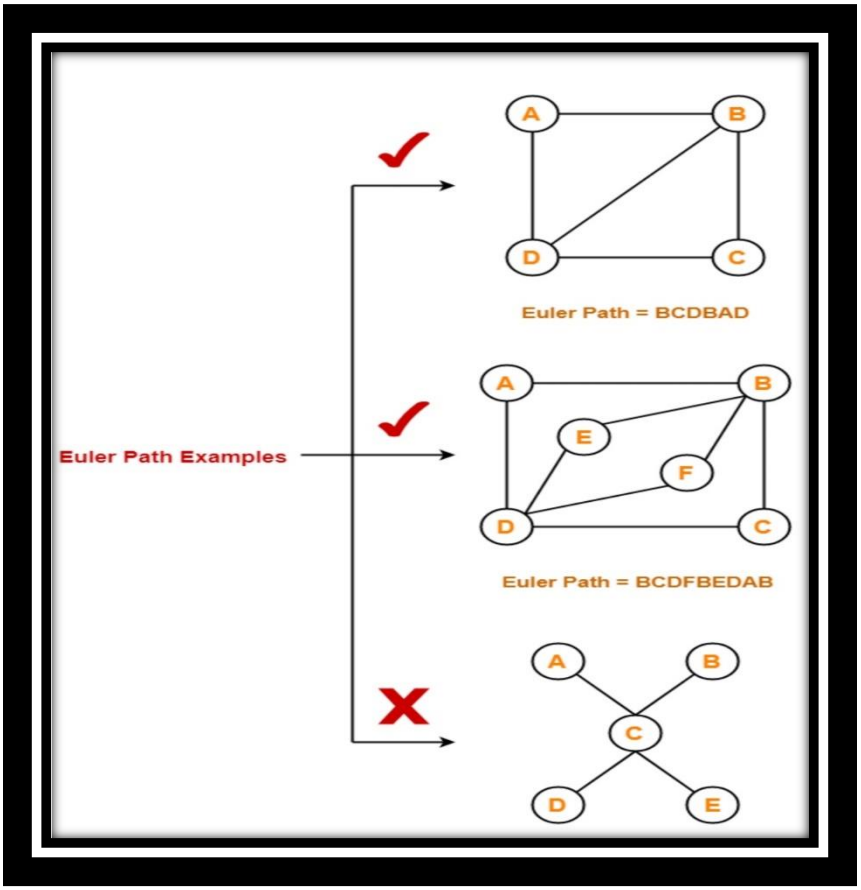
Hence G is connected.

Hence the proof.

Euler graph and Hamilton graph:

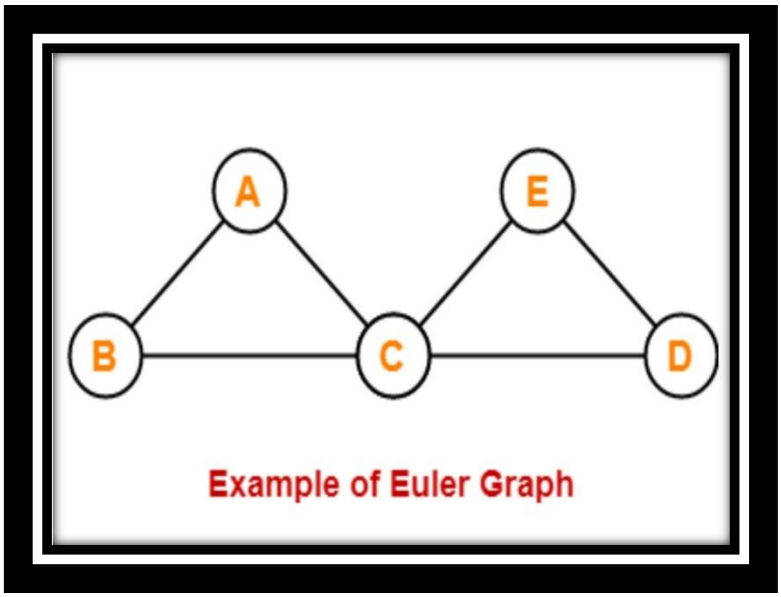
Euler path:

A path of a graph G is called an Eulerian path, if it contains each edge of the graph exactly once.



Euler graph:

A path of a graph G is called an Eulerian path, if it contains each edge of the graph exactly once.



Eulerian Circuit or Eulerian Cycle:

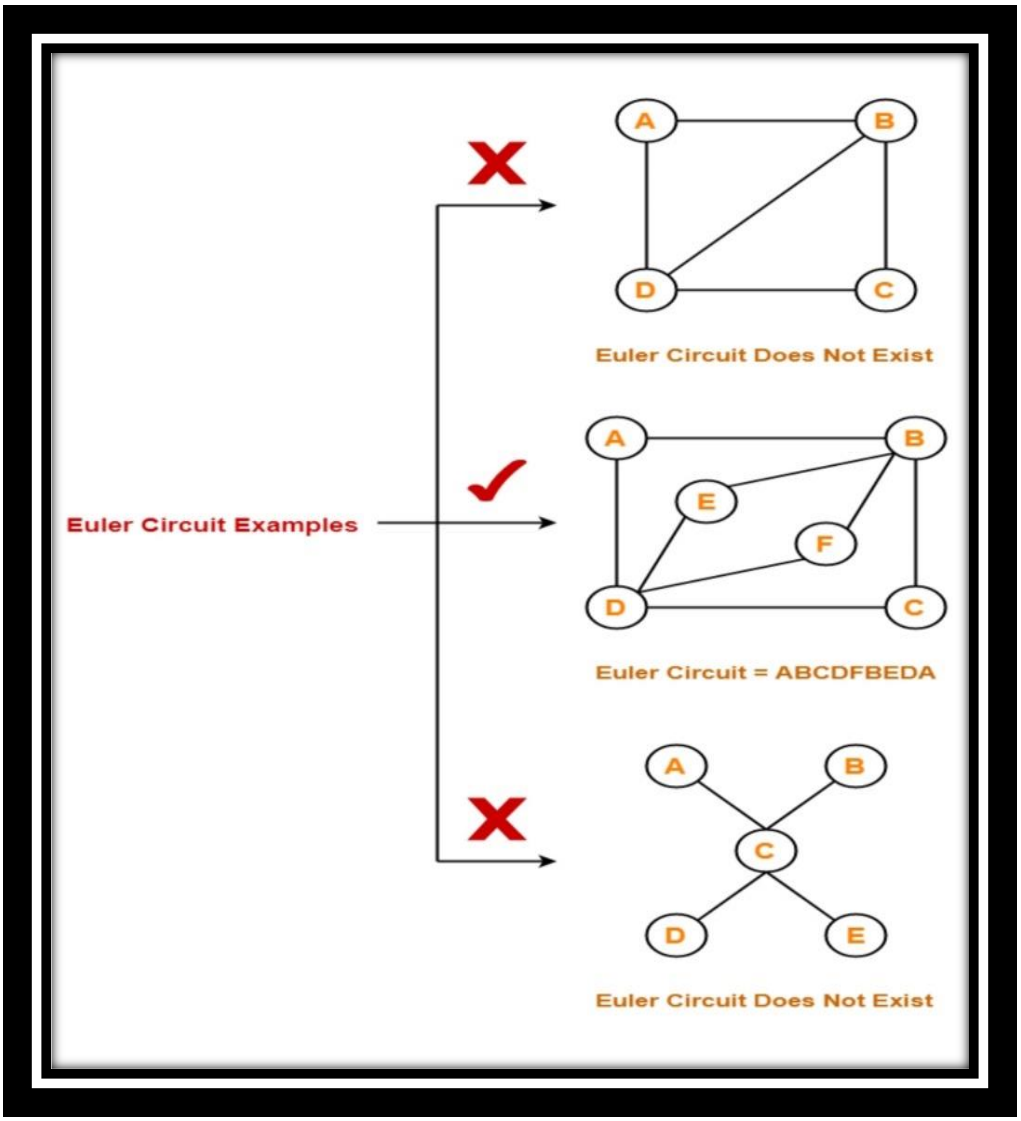
A circuit or cycle of a graph G is called Eulerian circuit or cycle, if it includes each edge of G exactly once.

Here starting and ending vertex are same.

An Eulerian circuit or cycle should satisfies the following conditions:

Starting and ending points (vertices) are same.

Cycle should contain all the edges of graph but exactly once.



Eulerian Graph or Euler graph:

Any graph containing an Eulerian circuit or cycle is called an Eulerian graph.

Theorem:1

A connected graph is Euler graph (contains Eulerian circuit) if and only if each of its vertices is of even degree.

Proof:

Let G be any graph having an Eulerian circuit and let "C" be an Eulerian circuit of G with origin vertex as u. Each time a vertex occurs as an internal vertex of C, then two of the edges incident with v are accounted for degree.

We, get, for internal vertex $v \in v(G)$

$d(v) = 2 \times$ number of times v occur inside the Euler circuit C

= even degree

And, since an Euler circuit C contains every edge of G and C starts and ends at u.

$d(u) = 2 + 2 + \times$ number of times u occur inside C.

= even degree Hence G has all the vertices of even degree.

Conversely, assume each of its vertices has an even degree.

Claim:

G has an Eulerian circuit.

Assume G be a connected graph which is not having an Euler circuit, with all vertices of even degree and less number of edges. That is, any graph having less number of edges than G, then it has an Eulerian circuit. Since each vertex of G has atleast two, therefore G contains closed path. Let C be a closed path of maximum

possible length in G. If C itself has all the edges of G, then G itself an Euler circuit in G.

By assumption, C is not an Euler circuit of G and $G - E(C)$ has some component G' with $|E(G')| > 0$. C has less number of edges than G, therefore C itself is an Eulerian, and C has all the vertices of even degree.

Since $|E(G')| < |E(G)|$, therefore G' has an Euler circuit C'. Because G is connected, there is a vertex v in both C and C'. Now join C and C' and traverse all the edges of C and C' with common vertex v, we get CC' is a closed path in G and $E(CC') > E(C)$ which is not possible choices of C.

Hence G has an Eulerian circuit.

Hence G is a Euler graph.

Hence the proof.

Theorem:2

Prove that if a graph G has not more than two vertices of odd degree, then there can be Euler path in G.

Proof:

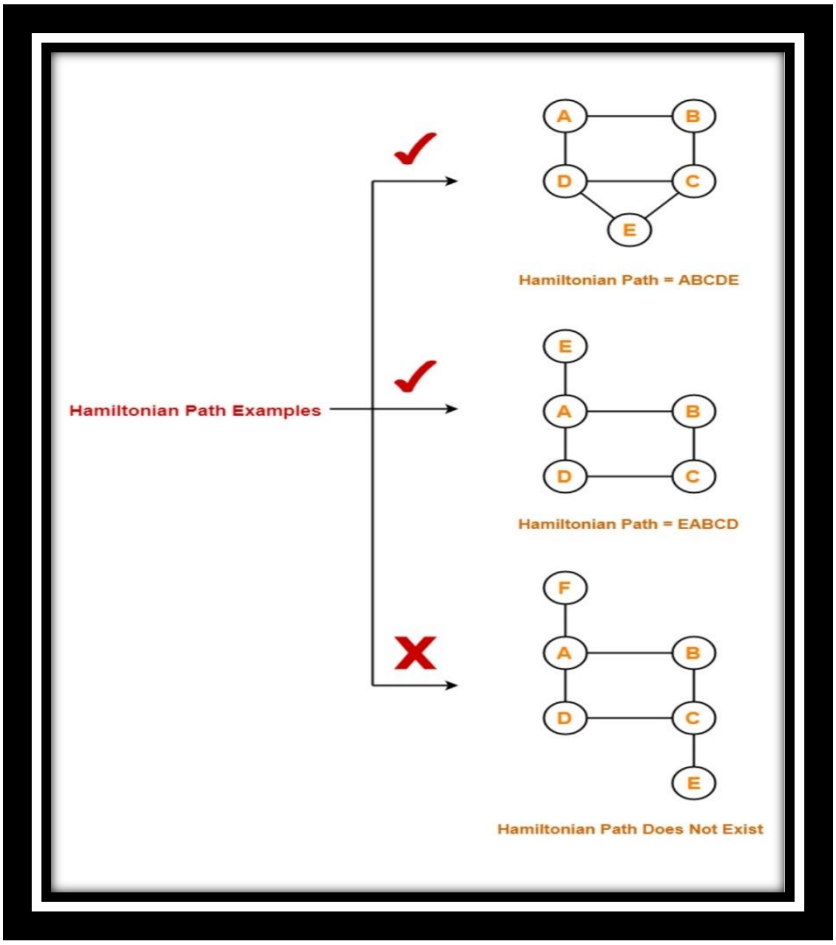
Let the odd degree vertices be labelled as V and W in any arbitrary order. Add an edge of G between the vertex pair (V, W) to form a new graph G'.

Now every vertex of G' is of even degree and hence G' has an Eulerian trial T. If the edge that we added to G is now removed from T, it will split into an open trail containing all edges of G which is nothing but an Euler path in G.

Hamiltonian Graph:

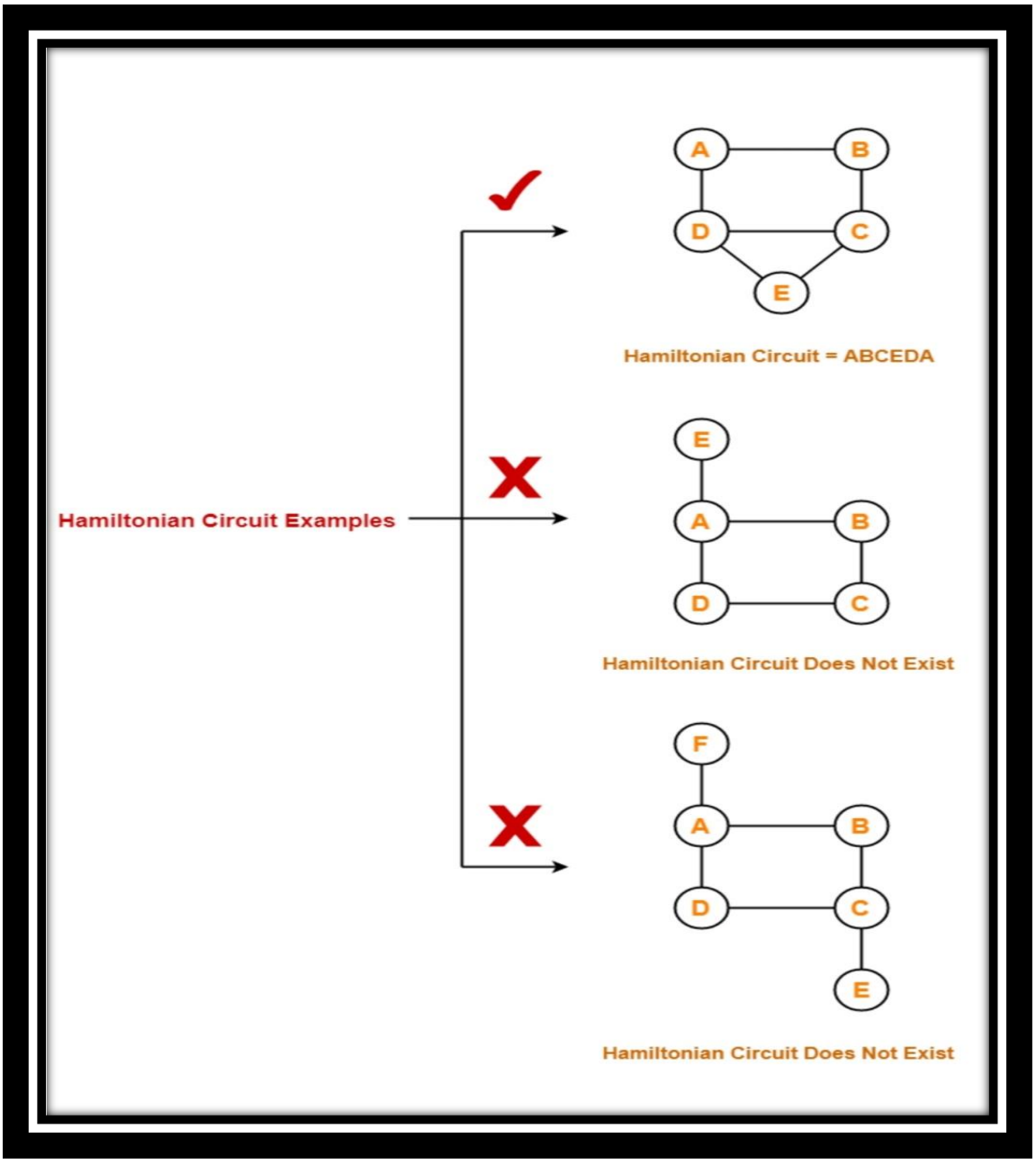
Hamiltonian Path:

A path of a graph G is called a Hamiltonian path, if it includes each vertex of G exactly once.



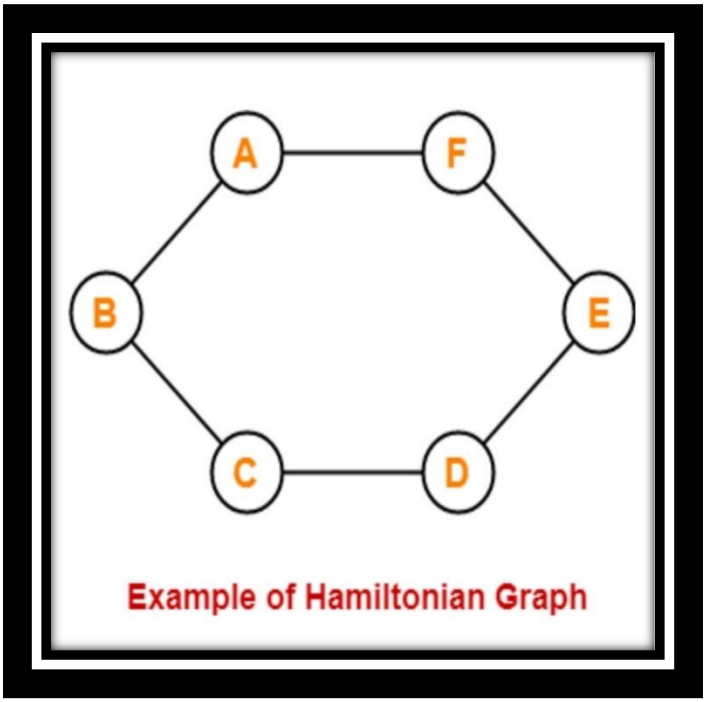
Hamiltonian Circuit or Cycle:

A circuit of a graph G is called a Hamiltonian circuit, if it includes each vertex of G exactly once, except the starting and ending vertices.



Hamiltonian graph:

Any graph containing a Hamiltonian circuit or cycle is called a Hamiltonian graph.



Properties:

(i) A Hamiltonian circuit contains a Hamiltonian path, but a graph containing a Hamiltonian path need not have a Hamiltonian cycle.

(ii) By deleting any one edge from Hamiltonian cycle, we can get Hamiltonian path.

(iii) A graph may contain more than one Hamiltonian cycle.

(iv) A complete graph k_n, will always have a Hamiltonian cycle, when $n \geq 3$.

(v) A graph with a vertex of degree one cannot have a Hamiltonian cycle.

Theorem: 1

Let G be a simple indirected graph with n vertices. Let u and v be two nonadjacent vertices in G such that $deg(u) + deg(v) \geq n$ in G. Show that G is Hamiltonian if and only if $G + uv$ is Hamiltonian.

Proof:

If G is Hamiltonian, then obviously $G + uv$ is Hamiltonian.

Conversely, suppose that $G + uv$ is Hamiltonian, but G is not.

Then by Dirac theorem, we have $deg(u) + deg(v) < n$

Which is a contradiction to our assumption.

Thus $G + uv$ is Hamiltonian implies G is Hamiltonian.

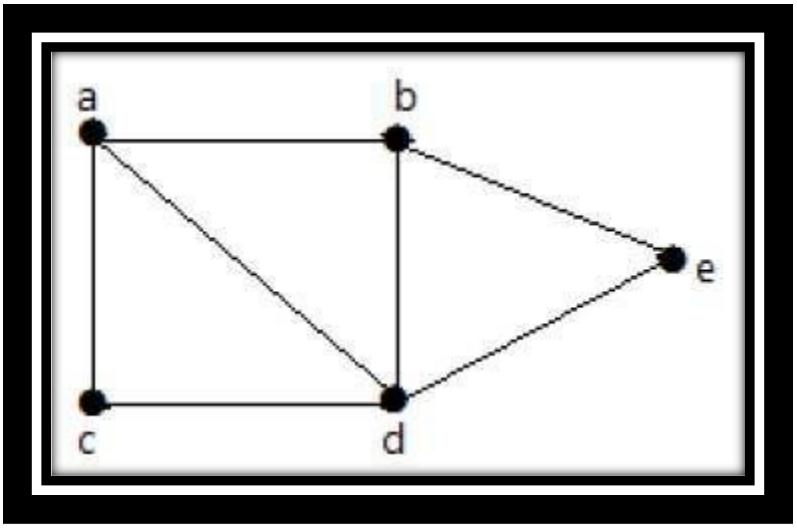
Hence the proof.

Connectivity:

A graph is said to be connected if there is a path between every pair of vertex. From every vertex to any other vertex, there should be some path to traverse. That is called the connectivity of a graph. A graph with multiple disconnected vertices and edges is said to be disconnected.

Example 1

In the following graph, it is possible to travel from one vertex to any other vertex. For example, one can traverse from vertex ‘a’ to vertex ‘e’ using the path ‘a-b-e’.



Theorem: 1

Show that graph G is disconnected if and only if its vertex set V can be partitioned into two nonempty subsets V_1 and V_2 such that there exists no edge in G whose one end vertex is in V_1 and the other in V_2.

Proof:

Suppose that such a partitioning exists. Consider two arbitrary vertices a and b of G such that $a \in V_1$ and $b \in V_2$.

No path can exist between vertices a and b.

Otherwise, there would be atleast one edge whose one end vertex be in V_1 and the other in V_2.

Hence if partition exists, G is not connected.

Conversely, let G be a disconnected graph.

Consider a vertex a in G.

Let V_1 be the set of all vertices that are joined by paths to a.

Since G is disconnected, V_1 does not include all vertices of G.

The remaining vertices will form a set V_2.

No vertex in V_1 is joined to any in V_2 by an edge.

Hence the partition.

Hence the proof.

Components of a graph:

The connected subgraphs of a graph G are called components of the graph G.

Theorem: 1

A simple graph with n vertices and k components can have atmost $\frac{(n-k)(n-k+1)}{2}$ edges.

Proof:

Let $n_1, n_2, \ldots, n_k$ be the number of vertices in each of k components of the graph G.

Then $n_1 + n_2 + \ldots + n_k = n = |V(G)|$

$\sum_{i=1}^{k} n_i = n \quad \ldots (1)$

Now, $\sum_{i=1}^{k}(n_i - 1) = (n_1 - 1) + (n_2 - 1) + \ldots + (n_k - 1)$

$= \sum_{i=1}^{k} n_i - k$

$\Rightarrow \sum_{i=1}^{k}(n_i - 1) = n - k$

Squaring on both sides

$\Rightarrow \left[\sum_{i=1}^{k}(n_i - 1)\right]^2 = (n-k)^2$

$\Rightarrow (n_1 - 1)^2 + (n_2 - 1)^2 + \ldots + (n_k - 1)^2 \leq n^2 + k^2 - 2nk$

$\Rightarrow {n_1}^2 + 1 - 2n_1 + {n_2}^2 + 1 - 2n_2 + \ldots + {n_k}^2 + 1 - 2n_k \leq n^2 + k^2 - 2nk$

$\Rightarrow \sum_{i=1}^{k} {n_i}^2 + k - 2n \leq n^2 + k^2 - 2nk$

$\Rightarrow \sum_{i=1}^{k} {n_i}^2 \leq n^2 + k^2 - 2nk + 2n - k$

$\Rightarrow \sum_{i=1}^{k} {n_i}^2 = n^2 + k^2 - k - 2nk + 2n$

$= n^2 + k(k-1) - 2n(k-1)$

$= n^2 + (k-1)(k-2n) \quad \ldots (2)$

Since, G is simple, the maximum number of edges of G in its components is $\frac{n_i(n_i-1)}{2}$.

Maximum number of edges of $G = \sum_{i=1}^{k} \frac{n_i(n_i-1)}{2}$

$= \sum_{i=1}^{k} \left[\frac{{n_i}^2 - n_i}{2}\right]$

$= \frac{1}{2}\sum_{i=1}^{k} {n_i}^2 - \frac{1}{2}\sum_{i=1}^{k} n_i$

$\leq \frac{1}{2}[n^2 + (k-1)(k-2n)] - \frac{n}{2}$ (Using (1) and (2))

$= \frac{1}{2}[n^2 - 2nk + k^2 + 2n - k - n]$

$= \frac{1}{2}[n^2 - 2nk + k^2 + n - k]$

$= \frac{1}{2}[(n-k)^2 + (n-k)]$

$$= \frac{1}{2}[(n-k)(n-k+1)]$$

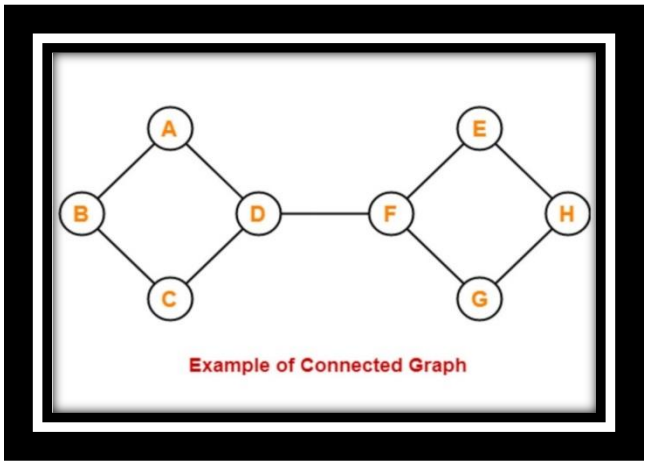
Maximum number of edges of $G \leq \frac{(n-k)(n-k+1)}{2}$

Hence the proof.

Directed Graphs:

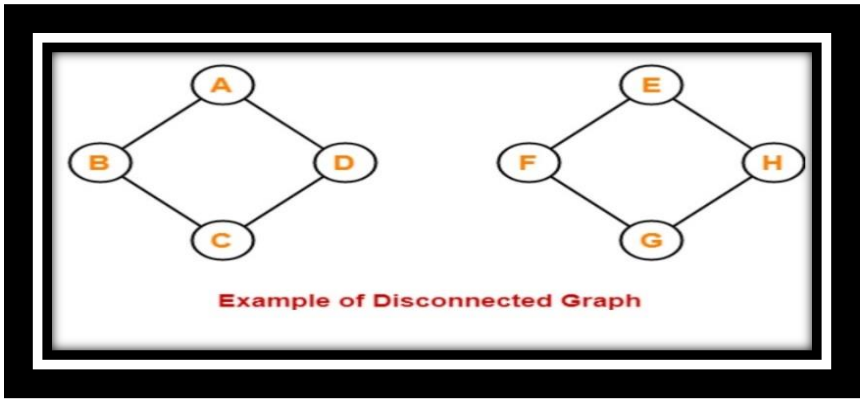
Connected Graph:

An directed graph is said to be connected if any pair of nodes are reachable from one another. That is, there is a path between any pair of nodes.



Disconnected graph:

A graph which is not connected is called disconnected graph.



Unilaterally connected:

A simple digraph is said to be unilaterally connected, if for any pair of nodes of the graph atleast one of the nodes of the pair is reachable from the other node.

Strongly connected:

A simple digraph is said to be strongly connected, if for any pair of nodes of the graph both the nodes of the pair are reachable from one to another.

Weakly connected:

A digraph is weakly connected, if it is connected as an undirected graph in which the direction of the edges is neglected.

Note:

A unilaterally connected digraph is weakly connected, but a weakly connected digraph is not necessarily unilaterally connected.

A strongly connected digraph is both unilaterally and weakly connected.

Theorem: 1

In a simple digraph $G = (V, E)$, every node of the digraph lies in exactly one strong component.

Proof:

Let $v \in V(G)$ and S be the set of all vertices of G which are mutually reachable with v.

Then $v \in S$, and S is a strong component of G. This shows that every vertex of G is contained in a strong component.

Assume that the vertex v is in two strong components S_1 and S_2.

Since $v \in S$, and any pair of vertices are mutually reachable with v, and also any pair of vertices of S_2

Are mutually reachable with v, we get any pair of vertices $S_1 \cup S_2$ are mutually reachable through v.

Therefore, $S_1 \cup S_2$ becomes one strong component of G.

This is impossible.

Therefore every vertex of G lies in exactly one strong component.

Hence the proof.

4.1 Semigroups and Monoids

Define Algebraic System:

- A non – empty set G together with one or more n – ary operations say $*$ (binary) is called an Algebraic System or Algebraic Structure or Algebra.
- We denoted it by $[G, *]$.
- Note: $+, -, \cdot, \times, *, \cup, \cap$ etc are some of binary operations.

Properties of Binary Operations

Let the binary operation be $* : G \times G \rightarrow G$.

Then we have the following properties:

Closure Property:

a $*$ b = $x \in$ G, for all $a, b \varepsilon G$.

Commutativity Property:

$a * b = b * a$, for all $a, b \varepsilon G$.

Associativity:

$(a * b) * c = a * (b * c)$, for all $a, b, c \varepsilon G$.

Identity Element:

$a * e = e * a = a$, for all $a \varepsilon G$.

'e' is called the identity element.

Inverse Element:

If $a * b = b * a = e$ (identity), then b is called the inverse of a and it is denoted by b = a^{-1}.

Left Cancellation law:

$a * b = a * c \Rightarrow b = c$

Right Cancellation law:

$b * a = c * a \Rightarrow b = c$

If the binary operation defined on G is + and X, then we have the following table.

For all a, b, c ε G	**(G, +)**	**(G,×)**
Commutativity	a + b = b + a	a× b = b × a
Associativity	(a + b) + c = a + (b + c)	(a× b)× c =a × (b × c)
Identity element	a + 0 = 0 + a = a (0 → identity)	a× 1 = 1 × a = a (1 →identity)
Inverse element	a + (-a) = 0 (-a→ additive inverse)	a× $\frac{1}{a}$ = $\frac{1}{a}$ × a = 1 ($\frac{1}{a}$ → multiplicative inverse)

NOTATIONS:

- Z - the set of all integers.
- Q - the set of all rational numbers.
- R - the set of all real numbers.
- C - the set of all complex numbers.
- R^+ - the set of all positive real numbers.
- Q^+ - the set of all positive rational numbers.

Semigroups and Monoids:

Define semigroup

If a non – empty set S together with the binary operation $*$ satisfying the following properties

Closure Property:

$a * b = b * a$, for all $a, b \, \varepsilon \, S$.

Associativity:

$(a * b) * c = a * (b * c)$, for all $a, b, c \, \varepsilon \, S$.

Then $(S,*)$ is called a semigroup.

Monoid:

A semigroup $(S,*)$ with an identity element with respect to $*$ is called Monoid. It is denoted by $(M,*)$.

In other words, a non – empty set 'M' with respect to $*$ is said to be a monoid, if $*$ satisfies the following properties

For $a, b \in M$

Closure Property:

$a * b = b * a$, for all a, b ε M.

Associativity:

$(a * b) * c = a * (b * c)$, for all a, b, c ε M.

Identity Element:

$a * e = e * a = a$, for all a ε M.

'e' is called the identity element.

4.2 Groups

Define Group

A non-empty set G together with the binary operation $*$,i.e., $(G,*)$ is called a group if $*$ satisfies the following conditions.

(i) Closure Property: $a * b = x \epsilon G$, for all $a, b \varepsilon G$.

(ii) Associativity: $(a * b) * c = a * (b * c)$ for all $a, b, c \varepsilon G$.

(iii) Identity: There exists an element $e \varepsilon G$ called the identity element such that

$a * e = e * a = a$, for all a ε G.

(iv) Inverse: There exists an element $a^{-1} \varepsilon$ G called the inverse of 'a' such that

$a * a^{-1} = a^{-1} * a = a$, for all a ε G.

Define Abelian Group

In a group (G, $*$), if a $*$ b = b $*$a, for all a, b ε G, then the group (G, $*$) is called an Abelian group.

Example: $(Z, +)$ is an Abelian group.

Define an Order of a Group

The number of elements in a group G is called the order of the group and is denoted by O(G).

It is denoted by O(G) or $|G|$.

Define Finite and Infinite Group

(i) If O(G) is finite, then G is said to be a finite group.

(ii) If O(G) is infinite, then G is said to be a infinite group.

Theorems on Abelian Groups

Theorem: 1

If every element of a group G has its own inverse, then G is abelian.

(OR)

For any group G, if $a^2 = e$ with $a \neq e$, then G is abelian.

Proof:

Let (G, $*$) be a group.

For a, b ε G, we have a $*$ b ϵ G

Given $a = a^{-1}$ and $b = b^{-1}$

$(a * b) = (a * b)^{-1}$

$= b^{-1} * a^{-1} = b * a (\because a = a^{-1} \& b = b^{-1})$

$\Longrightarrow a * b = b * a$

$\therefore G$ is abelian.

Hence the proof.

Theorem: 2

Prove that a group (G, $*$) is abelian iff $(a * b)^2 = a^2 * b^2$ for all $a, b \epsilon G$

Proof:

Assume that G is abelian.

$a * b = b * a$, a , b ϵ G $\rightarrow (1)$

Let $a^2 * b^2 = (a * a) * (b * b)$

$= a * [a * (b * b)]$ $\because$ ($*$ is Associative)

$= a * [(a * b) * b]$ $\because$ ($*$ is Associative)

$= a * [(b * a) * b]$ $\because (By\ (1))$

$= (a * b) * (a * b)$ $\because$ ($*$ is Associative)

$= (a * b)^2$

$\therefore (a * b)^2 = a^2 * b^2$

Conversely assume that $(a * b)^2 = a^2 * b^2$

To prove G is abelian.

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

$\Longrightarrow a * [b * (a * b)] = a * [a * (b * b)]$ $\because$ ($*$ is Associative)

$\Longrightarrow b * (a * b) = a * (b * b)$ (Left Cancellation law)

$\Longrightarrow (b * a) * b = (a * b) * b$ (Right Cancellation law)

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

$\therefore$ G is abelian.

Hence the proof.

Theorem: 3

If (G, $*$) is an abelian group, then for all a, b ε G then $(a * b)^n = a^n * b^n$

Proof:

Let (G, $*$) be an abelian group and a, b εG. Then for all n ε Z,

$$(a * b)^n = a^n * b^n$$

Case (i) Let $n = 0$

Then $a^0 = e,\ b^0 = e,\ (a * b)^0 = e$

$$\therefore\ (a * b)^0 = a^0 * b^0$$

Hence the result is true when n = 0

Case (ii) let $n = 1$

Let n be a positive integer

$$(a * b)^1 = a^1 * b^1$$

The result is true for $n = 1$

Assume that it is true for $n = k$, so that

$$(a * b)^k = a^k * b^k \rightarrow (1)$$

To prove it is true for $n = k + 1$

Now $(a * b)^{k+1} = (a * b)^k * (a * b)$

$$= a^k * b^k * a * b$$

$$= a^k * (b^k * a) * b$$

$$= a^k * (a * b^k) * b$$

$$= (a^k * a) * (b * b^k)$$

$$= a^{k+1} * b^{k+1}$$

*H*ence the result is true for $n = k + 1$.

Hence by induction, the result is true for positive integer values of n.

Hence the proof.

Problems on Groups:

1. Show that set $\mathbb{R}$ with the usual addition as a binary operation is an abelian group.

Solution: Let $a, b, c \in \mathbb{R}$

(i) Closure property: Clearly $a + b \in \mathbb{R}$

(ii) Associative property: $a + (b + c) = (a + b) + c$

(iii) Identity element: Since $0 \in \mathbb{R}$, we have

$\Rightarrow a + 0 = 0 + a = a$

(iv) Additive Inverse: For $a \in \mathbb{R}$, we have $-a \in \mathbb{R}$, such that

$$a + (-a) = 0 = (-a) + a$$

∴ The inverse of a is –a .

(v) Commutative property: $a + b = b + a \; for \; all \; a, b \in \mathbb{R}$

∴ $(\mathbb{R}, +)$ is an abelian group.

Since $\mathbb{R}$ contains infinite number of elements, $(\mathbb{R}, +)$ is an infinite abelian group

2. Show that $(\mathbb{R} - \{1\}, *)$ is an abelian group, where $*$ is defined by

$a * b = a + b + ab$, for all $a, b \in \mathbb{R}$.

Solution:

Here $\mathbb{R} - \{1\}$ means the set or real numbers except 1.

(i) Closure property:

Clearly $a * b = a + b + ab \in (\mathbb{R} - \{1\})$ $\quad [a \neq -1, b \neq -1]$

(ii) Associative property:

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

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

$$= a + b + ab + c + ac + bc + abc \quad \ldots. (A)$$

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

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

$$= a + b + c + bc + ab + ac + abc \qquad \text{….. (B)}$$

From (A) and (B), we get

$$(a * b) * c = a * (b * c), \quad \text{for all } a, b \in (\mathbb{R} - \{1\})$$

(iii) Identity element:

Let 'e' be the identity element.

Then, $a * e = a$

$\Rightarrow a + e + ae = a$

$\Rightarrow e(1 + a) = 0$

$\Rightarrow e = 0$

Here '0' is the identity element and $0 \in (\mathbb{R} - \{1\})$

(iv) Inverse:

Let the inverse of a be a^{-1}

Then, $a * a^{-1} = 0$ (identity)

$\Rightarrow a + a^{-1} + aa^{-1} = 0$

$\Rightarrow a^{-1}(1 + a) = -a$

$\Rightarrow a^{-1} = -\frac{a}{1+a} \in (\mathbb{R} - \{1\})$

$\therefore$ Inverse element is $-\frac{a}{1+a}$

(v) Commutative:

$\Rightarrow a * b = a + b + ab$

$= b + a + ba$

$= bb * a$

$\therefore a * b = b * a,$ for all $a, b \in (\mathbb{R} - \{1\})$

$\therefore (\mathbb{R} - \{1\})$ is an abelian group.

3. Show that $(\mathbb{Q}^+, *)$ is an abelian group where $*$is defined by

$$\boldsymbol{a * b = \frac{ab}{2}, for\ all\ a, b\ \in\ \mathbb{Q}^+}$$

Solution:

Let $\mathbb{Q}^+$be the set of all positive rational numbers.

(i) Closure property:

Clearly $a * b = \frac{ab}{2} \in \mathbb{Q}^+$

(ii) Associative property:

$$(a * b) * c = \frac{ab}{2} * c = \frac{\frac{abc}{2}}{2} = \frac{abc}{4} \quad \ldots (1)$$

$$a * (b * c) = a * \frac{bc}{2} = \frac{\frac{abc}{2}}{2} = \frac{abc}{4} \quad \ldots (2)$$

From (1) and (2) we get,

$$(a * b) * c = a * (b * c), for\ all\ a, b \in \mathbb{Q}^+$$

(iii) Identity element:

Let 'e' be the identity element.

Then, $a * e = a$

$\Rightarrow \frac{ae}{2} = a \quad \Rightarrow e = 2$

Here '2' is the identity element and $2 \in \mathbb{Q}^+$

iv) Inverse:

Let the inverse of a be a^{-1}

Then, $a * a^{-1} = 2$ (identity)

$$\Rightarrow \frac{aa^{-1}}{2} = 2$$

$$\Rightarrow a^{-1} = \frac{4}{a}$$

$\therefore$ Inverse element is $\frac{4}{a} \in \mathbb{Q}^+$

v) Commutative:

Now $a * b = \frac{ab}{2}$

$\therefore b * a = \frac{ba}{2} = \frac{ab}{2}$

$\therefore a * b = b * a,$ for all $a, b \in \mathbb{Q}^+$

Hence $(\mathbb{Q}^+, *)$ is an abelian group.

4. Let $G = \left\{\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}, \begin{bmatrix}-1 & 0\\0 & 1\end{bmatrix}, \begin{bmatrix}1 & 0\\0 & -1\end{bmatrix}, \begin{bmatrix}-1 & 0\\0 & -1\end{bmatrix}\right\}$ Show that G is a group under the operation of matrix multiplication.

Solution:

Let I = $\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}$, A = $\begin{bmatrix}-1 & 0\\0 & 1\end{bmatrix}$, B = $\begin{bmatrix}1 & 0\\0 & -1\end{bmatrix}$, C = $\begin{bmatrix}-1 & 0\\0 & -1\end{bmatrix}$

$\therefore G = \{I, A, B, C\}$. Since it is finite set we shall form Cayley table and verify the axioms of a Group.

I is the identity element.

$$A \cdot I = I \cdot A = A,\ B \cdot I = I \cdot B = B,\ C \cdot I = I \cdot C = C$$

$$A^2 = A \cdot A = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

$$AB = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = C$$

$$AC = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = B$$

$$B^2 = B \cdot B = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

$$C^2 = C \cdot C = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

$$BC = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} = A$$

$$CA = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = B$$

Similarly BA = C, CB = A

Cayley table:

·	I	A	B	C
I	I	A	B	C

A	A	I	C	B
B	B	C	I	A
C	C	B	A	I

(i) Closure property:

The first line of the table contains only all the elements of G. So G is closed under matrix multiplication.

(ii) Associative property:

Since matrix multiplication is associative it is true for G also. So Associative is satisfied.

(iii) Identity element:

I is the identity element.

(iv) Inverse:

Inverse of A is A, B is B and C is C.

So $(G, \cdot)$ is a group under matrix multiplication.

5. Check whether $H_1 = \{0, 5, 10\}$ and $H_2 = \{0, 4, 8, 12\}$ are subgroups of Z_{15} with respect to $+_{15}$.

Solution:

The addition tables (mod 15) for the sets H_1 and H_2 is given below:

For H_1

$+_{15}$	0	5	10
0	0	5	10
5	5	10	0
10	10	0	5

For H_2

$+_{15}$	0	4	8	12
0	0	4	8	12
4	4	8	12	1
8	8	12	1	5
12	12	1	5	9

Here all the entries in the addition table for H_1 are the elements of H_1.

$\therefore H_1$ is a subgroup of Z_{15}.

Also all the entries in the addition table for H_2 are not the elements of H_2.

$\therefore H_2$ is not closed under addition.

$\therefore H_2$ is not a subgroup of Z_{15}.

4.3 Subgroups

Define Subgroups

Let (G, $*$) be a group. Then (H, $*$) is said to be subgroup of (G, $*$) if $H \subseteq G$ and (H, $*$) itself is a group under the operation $*$

i.e., (H, $*$) is said to be a subgroup of (G, $*$) if

- $e \, \varepsilon \, H$, where e is the identity in G.
- For any $a \, \varepsilon \, H$, $a^{-1} \, \varepsilon \, H$
- For $a, \, b \, \varepsilon \, H$, $a * b \, \varepsilon \, H$

Define Trivial and Proper Subgroups

- $(\{e\}, *)$ and $(G, *)$ are trivial subgroups of $(G, *)$.
- All other subgroups of $(\boldsymbol{G}, *)$ are called proper subgroups.

Examples of Subgroups:

- (Z, +) is a Subgroup of (Q, +)
- (Q, +) is a Subgroup of (R, +)
- (R, +) is a Subgroup of(C,+)

Example of Subgroups

Find all the subgroups $(z_{12},+_{12})$

Solution:

z_{12} = {0, 1, 2, 3, 4, 5, 6, 7,8,9, 10, 11}

- Let S_1 = {0, 6}
- S_2 = {0, 4,8}
- S_3 = {0, 3, 6, 9}
- S_4 = {0, 2, 4, 6, 8}
- S_1, S_2, S_3, S_4 are proper subgroups of $(z_{12}, +_{12})$
- ({0}, $+_{12}$) and $(z_{12}, +_{12})$ *a*re its trivial subgroup

Theorems on Subgroups:

Theorem: 1

State and prove the necessary and sufficient condition for a subset of a group to be subgroup.

Statement:

Let (G, $*$) be a group. H is a nonempty subset of G, then H is a subgroup of G

if and only if whenever $a, b \in H \Rightarrow a * b^{-1} \in H$ for all

$a, b \in H$

(**Definition:** (G, $*$) be a group, H nonempty subset of G. H is a subgroup of G if

H itself is a group under the same binary operation $*$)

Proof:

Necessary Part

Let (G, $*$) be a group. H is a nonempty subset of G.

Assume that H is a subgroup of G.

By definition, (H, $*$) is a group.

So $a, b \in H \Rightarrow b^{-1} \in H$ by inverse property

$\Rightarrow a * b^{-1} \in H$ by closure property

Sufficient Part

Let (G, $*$) be a group. H is a nonempty subset of G.

Assume $a, b \in H \Rightarrow a * b^{-1} \in H \rightarrow$ (1)

Claim: H is a subgroup of

G i.e., (H, $*$) is a group.

H is nonempty so let $a \in H$

(iii) Identity

Now $a, a \in H$ by (1)

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

i.e., $e \in H$

Identity exists

(iv)Inverse

Let a $\in H$. Now by previous step $e \in H$

Now $e, a \in H$ by (1)

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

$\Rightarrow e \in H$

Hence Inverse exists.

(i) Closure

Let $a, b \in H$ by previous step $b^{-1} \in H$

Now $a, b^{-1} \in H$ by (1)

$\Rightarrow a * (b^{-1})^{-1} \in H$

$\Rightarrow a * b \in H$

Closure is verified.

(ii) Associative

$a, b, c \in H$, $\boldsymbol{H} \subseteq \boldsymbol{G}$, $a, b, c \in G$

In G $(a * b) * c = a * (b * c)$

$\therefore$ In H $(a * b) * c = a * (b * c)$

Associative is verified.

(H, $*$) be a group.

Hence H is a subgroup of G.

Hence the proof.

Theorem: 2

Prove that intersection of two subgroups of a group (G, $*$) is a subgroup of (G, $*$). Also, prove that union of subgroups need not be a group.

Proof:

Let (G, $*$) be a group. H and K are non – empty subgroups of (G, $*$). Both H and K satisfying the following necessary conditions

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

Let $a, b \in K \Rightarrow a * b^{-1} \in K$ . . . (1)

Consider the subset $H \cap K$ of G

(i) Since H is a subgroup of G, $e \in H$

Since K is a subgroup of G, $e \in K$

$\therefore e \in H \cap K$

so, $H \cap K$ is a non – empty subset of G.

(ii) Let a, b $\in H \cap K$

By Sufficient condition for aSubgroup

We need to prove $a * b^{-1} \in H \cap K$

$a, b \in H$ and $a, b \in K$

By (1) $a * b^{-1} \in H \cap K$

$\therefore H \cap K$ is a subgroup of (G, $*$)

Hence the proof.

Now we are going to Prove that Union of two Subgroups of a group need not be a Subgroup.

Let us prove the above fact by giving counter examples

Consider G = set of integers under addition $(Z, +)$

$= \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$

- H = 2Z = {. . . , − 6, − 4, − 2, 0, 2, 4, 6, . . . }
- K = 3Z = {. . . , − 9, − 6, − 3, 0, 3, 6, 9, . . . }

H and K are subgroups of $(Z, +)$

$H \cup K$ ={. . . , − 9, − 6, − 4, − 3, − 2, 0 , 2, 3 , 4, 6, 9, . . . }

$H \cup K$ is not closed under addition.

As 2,3 ∈ $H \cup K$ but 2 + 3 = 5 ∉ $H \cup K$

So $H \cup K$ is not a subgroup of $(Z, +)$.

Hence the proof.

Cyclic Group:

Define Cyclic Groups

A group (G, ∗) is said to be cyclic if there exists an element $a \in G$ such that every element of G can be written as some power of "a".

i.e., $a^n for\ some\ integer\ n.$

G is said to be generated by "a" (or) "a" is a generator ofG.

We write $G = \prec a \succ$

Examples:

The set of complex numbers $\{1, -1, i, -i\}$ under multiplication operation is a cyclic group.

There are two generators – i and i as $i^1 = 1$, $i^2 = -1$, $i^3 = -i$, $i^4 = 1$ and also $(-i)^1 = -i$, $(-i)^2 = -1$, $(-i)^3 = i$, $(-i)^4 = 1$ which covers all the elements of the group.

Hence it is a Cyclic Group.

However -1 is not a generator.

Theorem: 1

Every Subgroup of a Cyclic group is Cyclic.

Proof:

Let H be a cyclic group generated by an element $a \in G$.

∴ Every element in G can be expressed as a power of the element "a".

Let H be a subgroup of G.

If $H = \{e\}$, then H is a subgroup of G and it is cyclic.

∴ The result is trivial.

Suppose $H \neq \{e\}$ then there exists an element $x \in H$ with $x \neq e$.

$\therefore x = a^k$ for some integer k.

Let m be the least positive integer such that $a^m \epsilon H$.

Let $b \epsilon H$ then $b = a^n$ for some integer n.

Let $n = mq + r$ where $0 \leq r < m$

$\Rightarrow b = a^n$

$\Rightarrow b = a^{mq+r}$

$\Rightarrow b = a^{mq} * a^r$

$\Rightarrow b = (a^m)^q * a^r$

$\Rightarrow a^r = {}^{b}/_{(a^m)q}$

$\Rightarrow a^r = b * (a^m)^{-q}$

Now $b \epsilon H$, $(a^m)^q \epsilon H$ and H is closed in $*$.

$\therefore$ we have $b * (a^m)^{-q} \epsilon H$

This shows that there exists an integer "r" such that $o \leq r < m$ with $a^r \epsilon H$.

Since m is the least positive integer for which $a^m \epsilon H$, $a^r \epsilon H$ with $o \leq r < m$ is not possible.

$\therefore r = 0$ so $b = a^{mq}$

$\Rightarrow b = (a^m)^q$

Every element $b \in H$ is expressed as a power of a^m.

i.e., H is generated by the element $a^m \in H$

H is a cyclic group generated by a^m.

Hence, every subgroup of a cyclic group is

cyclic.

Hence the proof.

4.4 Cosets

Define Left Coset and Right Coset of H in G.

Let $(H, *)$ be a subgroup of $(G, *)$.

For any $a \in G$, the left coset of H, denoted by $a * H$, is the set

$a * H = \{a * h: h \in H\}$ for all $a \in G$

For any $a \in G$, the right coset of H, denoted by $H * a$, is the set

$H * a = \{h * a: h \in H\}$ for all $a \in G$

Theorem: 1

Let $(H, *)$ be a subgroup of $(G, *)$. Then any two left Cosets (right Cosets) of H of a group $(G, *)$ are either identical or disjoint and the union of distinct left Cosets of H is G (or) The set of all distinct left Cosets of the subgroup H of the group $(G, *)$ forms a partition of G.

Proof:

Let $a, b \in G$

Consider the Cosets $a * H$ and $b * H$

We shall prove that $a * H = b * H$ (or) $a * H \cap b * H = \emptyset$

Suppose $a * H \cap b * H \neq \emptyset$

Let c ϵ $a * H \cap b * H = \emptyset$

$\Rightarrow c \epsilon a * H$ and $c \epsilon b * H$

Let $c = a * h_1$ and $c = b * h_2$ for all $h_1, h_2 \epsilon H$

$\therefore a * h_1 = b * h_2$

Take ${h_1}^{-1}$ on both sides

$\Rightarrow (a * h_1) * {h_1}^{-1} = (b * h_2) * {h_1}^{-1}$

$\Rightarrow a * (h_1 * {h_1}^{-1}) = b * (h_2 * {h_1}^{-1})$

$\Rightarrow a * e = b * h_3$ where $h_3 = h_2 * {h_1}^{-1}$

$\Rightarrow a = b * h_3$

$\Rightarrow a \in b * h_3$

$\Rightarrow a * H \subseteq b * H$ . . . (1)

IIIrly $b * H \subseteq a * H$ . . .(2)

From (1) and (2) we have $a * H = b * H$

$\therefore$ Any two left cosets are either identical or distinct.

Each element of the left Coset $a * H$ is also an element of G.

$\therefore$ Every left coset of $a * H$ is a subset of G.

Hence $\bigcup_{a \in G} a * H \subseteq G$ . . . (3)

If $a \in G$, $a \in a * H$ then $a \in \bigcup_{a \in G} a * H$

$G \subseteq \bigcup_{a \in G} a * H$ . . . (4)

$\therefore$The set of all distinct left cosets of H is a partition "n' of the group G.

Hence the proof.

LAGRANGE'S THEOREM:

The order of a subgroup of a finite group is a divisor of the order of the group.

i.e., if H is a subgroup of a finite group $(G, *)$ then O(H) divides O(G).

Proof:

Let $(G, *)$ be a finite group of order n and H be a subgroup of G with order m.

$\Rightarrow O(H) = m$ & $O(G) = n$

We will prove that $O(H) / O(G)$

Since H contains m distinct elements, every left cost of H contains exactly m elements.

(Write the theorem: 1)

Let $a_1 * H, a_2 * H, \ldots, a_k * H$ be the distinct left cosets of

H. Let $G = a_1 * H \cup a_2 * H \cup \ldots \cup a_k * H$

$O(G) = O(a_1 * H) + O(a_2 * H) + \ldots + O(a_k * H)$

$= O(H) + O(H) + \ldots + O(H)$

$= m + m + \ldots + m$ (n times)

$\Rightarrow n = mk$

$\Longrightarrow n/m = k$

$\Longrightarrow$ m divides n.

This means that $O(H) / O(G)$.

Hence the proof.

Normal Subgroup

A subgroup $(H,*)$ of $(G,*)$ is said to be normal subgroup of G, for $x \in G$ and for $h \in H$, if $x * h = h * x$ (or) for all $x \in G, xH = Hx$

Note:

Consider H as a subgroup of G, then the subgroup H is said to be normal,

for all $x \in G, x * h * x^{-1} = H$(or) for all $x \in G, x * h * x^{-1} \in H$

Theorem: 1

Every subgroup of an abelian group is normal.

Proof:

Let $(G,*)$ be an abelian group and $(H,*)$ be a subgroup of G.

Let $x \in G$ be any element.

Then $xH = \{x * h \ / h \in H\}$

$= \{h * x \ / h \in H\}$ (G is abelian)

$= Hx$

Since "x" is arbitrary, $xH = Hx \ \forall \ x \in G$

Hence H is a normal subgroup of G.

Hence the proof.

Theorem: 2

Prove that intersection of two normal subgroup of $(G,*)$is a normal subgroup of $(G,*)$.

Proof:

Let $(H,*)$ and $(K,*)$are two normal subgroup.

$\Rightarrow$ H and K are subgroups of G.

$\Rightarrow H \cap K$ is a subgroup of G. (Already proved)

To prove $(H \cap K,\ *)$ is a normal subgroup of $(G,*)$.

Let $h \in\ H \cap K$ be any element and $x \in G$ be any element.

Then $x \in G$ and$h \in H$ and $h \in K$

Since H and K are normal, $x\ *h\ *x^{-1} \in\ H$ . . . (1)

and $x *\ h *\ x^{-1} \in\ K$ . . . (2)

From (1) and (2) we get,

$$x\ *h\ *x^{-1} \in\ H\ \cap K$$

Hence $H\ \cap K$ is a normal subgroup of G.

Hence the proof.

4.5 Homomorphism

Let $(G, \cdot)$ and $(G', *)$ be any two groups.

A mapping $f: G \rightarrow G'$ is said to be a homomorphism, if $f(a \cdot b) = f(a) * f(b)$ for any $a, b \in G$ is called a group homomorphism.

Example: (i)

Let $f: (Z, +) \rightarrow (Z, +)$ given by $f(x) = 2x \; \forall \; x \in Z$ is a homomorphism.

For, $x, y \in Z, f(x + y) = 2(x + y) = 2x + 2y = f(x) + f(y)$

Example: (ii)

Let $f: (R, +) \rightarrow (R^+, \cdot)$ given by $f(x) = e^x \; \forall \; x \in R$ is a homomorphism.

For, $x \in R, \; f(x + y) = e^{x+y} = e^x \cdot e^y = f(x) \cdot f(y)$

Isomorphism:

Let $(G, \cdot)$ and $(G', *)$ be any two groups. A mapping $f: G \rightarrow G'$ is said to be isomorphism if

(i) f is one – one

(ii) f is onto

(iii) f is homomorphism

Types of Homomorphism

(i) If f is one – to – one then f is monomorphism.

(ii) (ii) If f is onto then f is epimorphism.

Theorem: 1

Homomorphism preserves identities.

Proof:

Let $a \in G$

Let f be a homomorphism from $(G, *)$ and $(G', *)$

Clearly $f(a) \in G'$

$\Rightarrow f(a) * e' = f(a)$ $(e' - identity\ in\ G')$

$= f(a * e)$ (e – identity in G)

$= f(a) * f(e)$ (f – homomorphism)

$\Rightarrow\ e' = f(e)$ (Left cancellation law)

Hence f preserves identities.

Hence the proof.

Theorem: 2

Homomorphism preserves inverse.

Proof:

Let $a \in G$

Since G is a group, $a^{-1} \in G$

Since G is a group $a * a^{-1} = a^{-1} * a = e$

Consider $a * a^{-1} = e$

$$\Rightarrow f(a * a^{-1}) = f(e)$$

$$\Rightarrow f(a) * f(a^{-1}) = e' \because e' = f(e), f \text{ is homomorphism}$$

$\Rightarrow f(a^{-1})$ is the inverse of $f(a) \in G'$

Hence $[f(a)]^{-1} = f(a^{-1})$

Hence f preserves inverse.

Hence the proof.

Kernal of Homomorphism

Let $f: G \to G'$ be a group homomorphism. The set of elements of G which are mapped into e' (identity in G') is called the kernel of f and it is denoted by ker(f)

$$\ker(f) = \{x \in G / f(x) = e'\}$$

Theorem: 1

Kernel of a homomorphism of a group into another group is a normal subgroup.

Proof:

Let $(G,*)$ and $(G',\ \oplus)$ be two groups.

f: $(G,*) \rightarrow (G',\ \oplus)$ is a homomorphism.

Define ker$(f) = \{x\ \in G\ /f(x) = e'\}$

Claim: Ker f is a normal subgroup of G

We know that homomorphism preserves identity.

$i.e., f(e) =\ e'$, so $e \in kerf$

⇒Ker f is non empty.

(ii) $a, b\ \in$ ker $f \Rightarrow a * b^{-1} \in kerf$ then ker f is a subgroup.

$a \in kerf\ \Rightarrow f(a) = e'$ by definition of ker f

$b \in kerf\ \Rightarrow f(b) = e'$ by definition of ker f

Since homomorphism preserves inverse ⇒ $[f(a)]^{-1} = f(a^{-1})$

Now $f(a * b^{-1}) = f(a) \oplus f(b^{-1})$

$= f(a) \oplus [f(b)]^{-1}$

$= e' \oplus e'$

$= e'$

$\Rightarrow a * b^{-1} \in kerf$

Hence kerf is a subgroup of G.

(iii)Let $a \in kerf \Rightarrow f(a) = e'$ by definition of kerf

Homomorphism preserves inverses $\Rightarrow [f(a)]^{-1} = f(a^{-1})$

So $f(g^{-1} * a * g) = f(g^{-1}) \oplus f(a) \oplus f(g)$

$= [f(g)]^{-1} \oplus e' \oplus f(g)$

$= [f(g)]^{-1} \oplus f(g)$

$= e'$

Hence by definition, $g^{-1} * a * g \in kerf$

Hence kerf is a normal subgroup.

Hence the proof.

Theorem:2

Fundamental theorem of group homomorphism

Every homomorphic image of a group G is isomorphic to some quotient group of G.

(OR)

Let $f: G \to G'$ be a onto homomorphism of groups with kernel K, then $\frac{G}{K} \cong G'$

Proof:

Let f be the homomorphism $f: G \to G'$

Let G' be the homomorphic image of a group G.

Let K be the kernel of this homomorphism.

Clearly K is a normal subgroup of G.

Claim: $\frac{G}{K} \cong G'$

Define φ: $\frac{G}{K} \to G'$ by $\varphi(K * a) = f(a)$ for all $a \in G$

(i) φ is well defined.

We have $K * a = K * b$

$$\Rightarrow a * b^{-1} \in K$$

$\Rightarrow f(a * b^{-1}) = e'$ (e' is identity)

$\Rightarrow f(a) * f(b^{-1}) = e'$

$\Rightarrow f(a) * [f(b)]^{-1} = e'$

$\Rightarrow f(a) * [f(b)]^{-1} * f(b) = e' * f(b)$

$\Rightarrow f(a) = f(b)$

$\Rightarrow \varphi(K * a) = \varphi(K * b)$

Hence φ is well defined.

(ii) To prove φ is one – one.

To prove $\varphi(K * a) = \varphi(K * b) \Rightarrow K * a = K * b$

We know that $\varphi(K * a) = \varphi(K * b)$

$\Rightarrow f(a) = f(b)$

$\Rightarrow f(a) * f(b^{-1}) = f(b) * f(b^{-1})$

$= f(b * b^{-1})$

$= f(e)$

$\Rightarrow f(a) * f(b^{-1}) = e'$

$\Rightarrow f(a * b^{-1}) = e'$

$\Rightarrow a * b^{-1} \in K$

$\Rightarrow K * a * b^{-1} = K$

$\Rightarrow K * a = K * b$

Hence φ is one – one.

(iii) φ is onto.

Let $y \in G'$

Since f is onto, there exists $a \in G$ such that $f(a) = y$

Hence $\varphi(K * a) = f(a) = y$

Hence φ is onto.

(iv) φ is a homomorphism.

Now $\varphi(K * a \ * \ K * b) = \varphi(K * a \ * b)$

$$= f(a * b)$$

$$= f(a) * f(b)$$

$$= \varphi(K * a) * (K * b)$$

Hence φ is a homomorphism.

Since φ is one – one, onto, homomorphism φ is an isomorphism between $\frac{G}{K}$ and G'.

Hence $\frac{G}{K} \cong \ G'$

Hence the proof.

Hasse Diagram:

Pictorial representation of a Poset is called Hasse Diagram.

Example:

If $X = \{2, 3, 6, 12, 24, 36\}$ and the relation R defined on X by $R =$

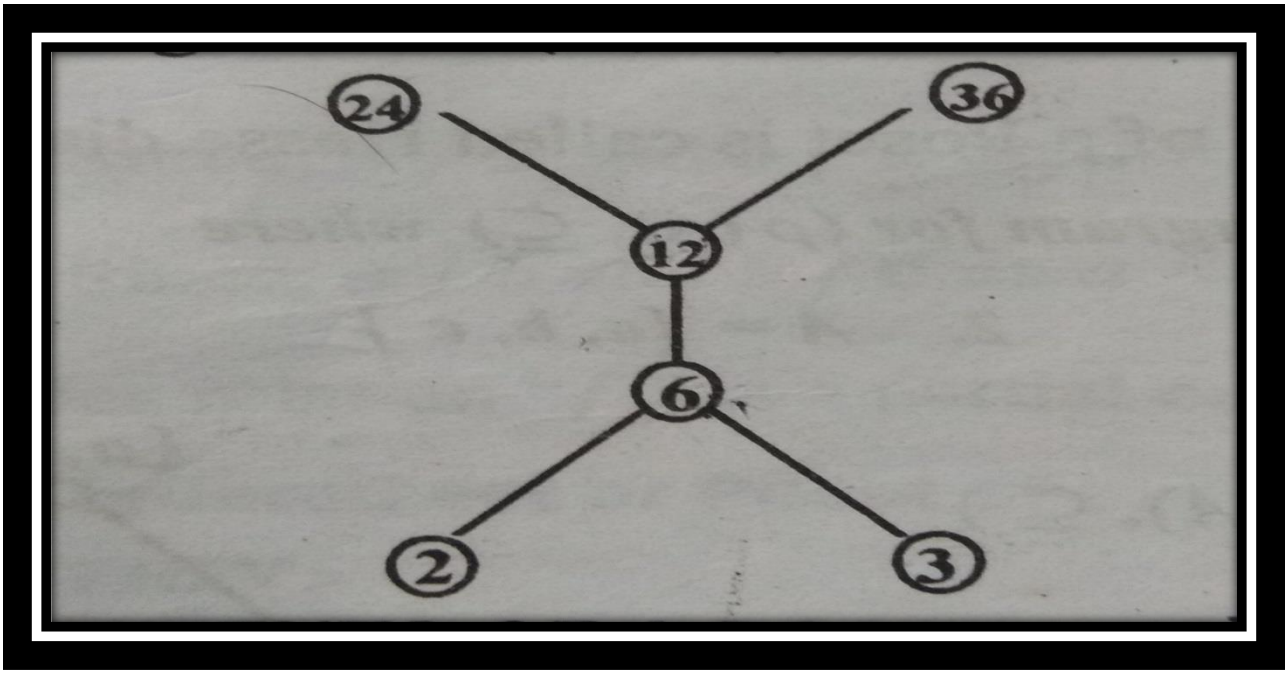
$\{\langle a, b\rangle / a / b\}$. Draw the Hasse diagram for (X, R).

Solution:

The relation

$$R = \{\langle 2,6\rangle\ \langle 2,12\rangle\ \langle 2,24\rangle\ \langle 2,36\rangle\ \langle 3,6\rangle\ \langle 3,12\rangle\ \langle 3,24\rangle\ \langle 3,36\rangle\ \langle 6,12\rangle\ \langle 6,24\rangle\ \langle 6,36\rangle\ \langle 12,24\rangle\ \langle 12,36\rangle\ \langle 2,36\rangle\}$$

The Hasse Diagram for (X, R) is



Special Elements of a Poset:

Let $(P, \leq)$ be a Poset. An element $a \in P$ is called least element in P, if $a \leq x$ for all $x \in P$.

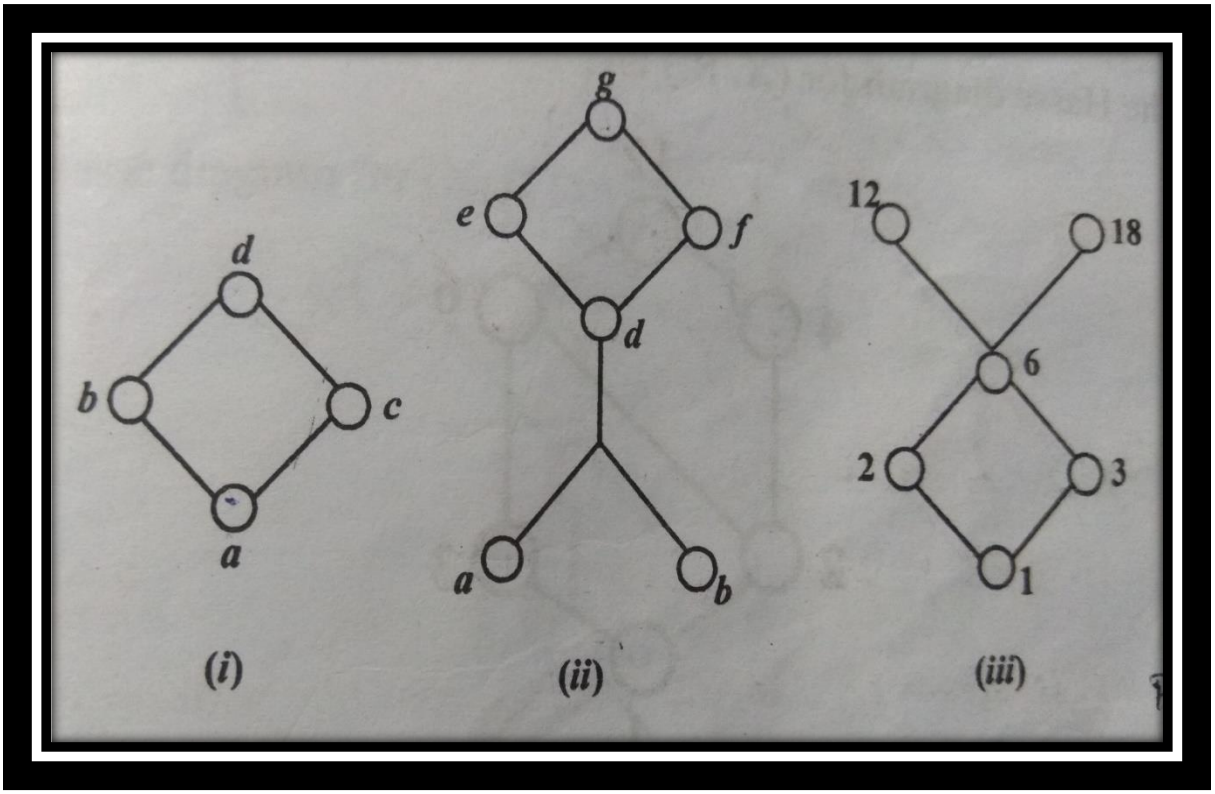
An element $b \in P$ is called greatest element in P, if $b \geq x$ for all $x \in P$

Note:

The least element is called "0" element and the greatest element is called "1" element.

Example:

Consider the following Hasse Diagram



In (i) “a” is the least element and “d” is the greatest element.

In (ii) “g” is the greatest element and there is no least element.

In (iii) “1” is the least element and there is no greatest element.

Definition:

Let $(P, \leq)$ be a Poset an A be any non - empty subset of P. An element $a \in P$ is an upper bound of A, if $a \geq x$ for all $x \in A$.

An element $b \in P$ is said to be lower bound in P, if $b \leq x$ for all $x \in A$.

Least Upper Bound: (LUB)

Let $(P, \leq)$be a Poset and $A \subseteq P$. An element $a \in P$ is said to be least upper bound (LUB) or supremum (sup) of A, if a is a upper bound of A.

$a \leq c$, where c is any other upper bound of A.

Greatest Lower Bound: (GLB)

Let $(P, \leq)$be a Poset and $A \subseteq P$. An element $b \in P$ is said to be least upper bound (GLB) or infimum (inf) of A, if b is a lower bound of A.

$b \geq d$, where d is any other lower bound of A.

Examples:

1. If $X = \{1, 2, 3, 4, 6, 12\}$ and the relation R defined on X by $R = \{\langle a, b\rangle / a / b\}$. Find LUB and GLB for the Poset (X, R).

Solution:

The relation

$$R = \{\langle 1,2\rangle\ \langle 1,3\rangle\ \langle 1,4\rangle\ \langle 1,6\rangle\ \langle 1,12\rangle\ \langle 2,4\rangle\ \langle 2,6\rangle\ \langle 2,12\rangle\ \langle 3,6\rangle\ \langle 3,12\rangle\ \langle 4,12\rangle\}$$

The Hasse Diagram for (X, R) is

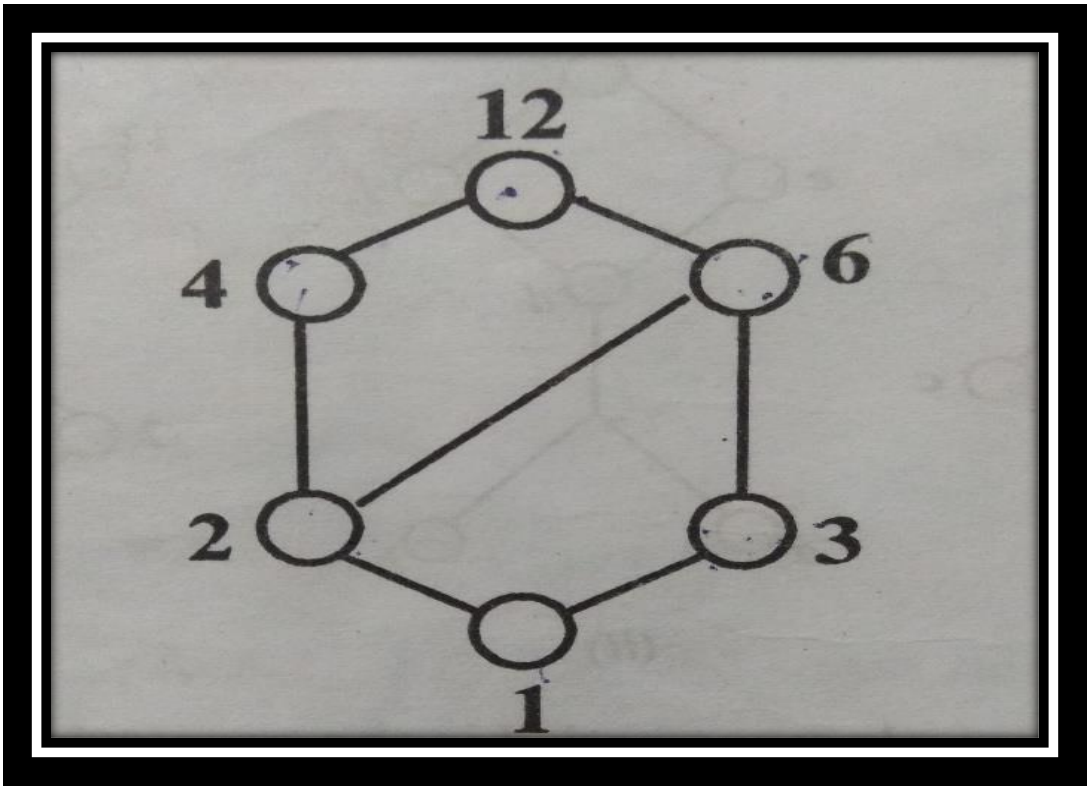


Table for LUB and GLB

1	$\text{UB}\{1,3\} = \{3,6,12\}$ $\text{LUB}\{1,3\} = 3$	**1**	$\text{LB}\{1,3\} = \{1\}$ $\text{GLB}\{1,3\} = 1$
2	$\text{UB}\{1,2,3\} = \{6,12\}$ $\text{LUB}\{1,2,\ 3\} = 6$	**2**	$\text{LB}\{1,2,3\} = \{1\}$ $\text{GLB}\{1,2,\ 3\} = 1$
3	$\text{UB}\{2,3\} = \{3,6,12\}$ $\text{LUB}\{2,3\} = 6$	**3**	$\text{LB}\{2,3\} = \{1\}$ $\text{GLB}\{2,3\} = 1$
4	$\text{UB}\{2,3,6\} = \{6,12\}$ $\text{LUB}\{2,3,6\} = 6$	**4**	$\text{LB}\{2,3,6\} = \{1\}$ $\text{GLB}\{2,3,6\} = 1$
5	$\text{UB}\{4,6\} = \{12\}$ $\text{LUB}\{4,6\} = 12$	**5**	$\text{LB}\{4,6\} = \{1,2\}$ $\text{GLB}\{4,6\} = 2$

2. If $X = \{2, 3, 6, 12, 24, 36\}$ and the relation R defined on X by $R = \{\langle a, b\rangle / a/\ b\}$. Draw the Hasse diagram for (X, R).

Solution:

The relation

$$R = \left\{ \begin{matrix} \langle 2,6\rangle\ \langle 2,12\ \rangle\ \langle 2,24\rangle\ \langle 2,36\rangle\ \langle 3,6\rangle\ \langle 3,12\rangle\ \langle 3,24\rangle\ \langle 3,36\rangle\ \langle 6,12\rangle \\ \langle 6,24\rangle\ \langle 6,36\rangle\ \langle 12,24\rangle\ \langle 2{,}36\rangle \end{matrix} \right\}$$

The Hasse Diagram for (X, R) is

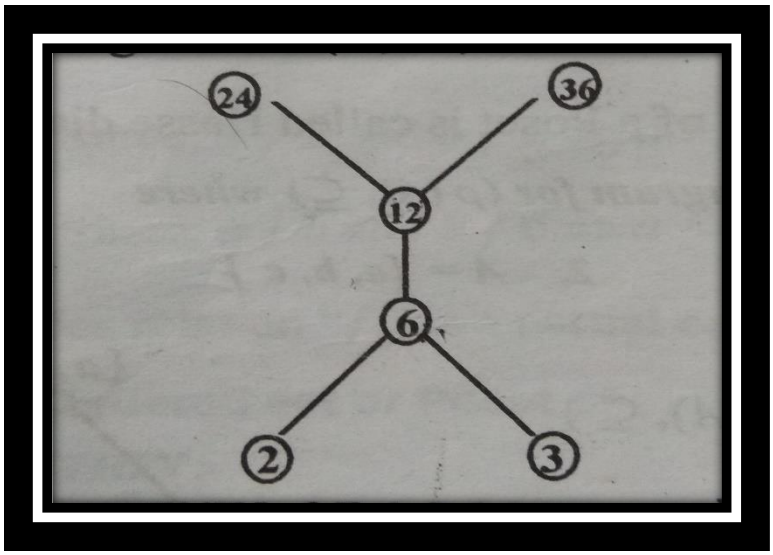


Table of LUB and GLB

1	$\text{UB}\{2,3\} = \{6,12,24,36\}$ $\text{LUB}\{2,3\} = 6$	**1**	$\text{LB}\{2,3\}$ =does not exists $\text{GLB}\{2,3\}$ =does not exists
2	$\text{UB}\{24,36\}$ = does not exists $\text{LUB}\{24,36\}$ = does not exists	**2**	$\text{LB}\{24,36\} = \{2,3,6,12\}$ $\text{GLB}\{24,36\} = 12$

Lattice:

A Lattice is a partially ordered set(Poset) $(L, \leq)$ in which for every pair of elements $a, b \in L$, both greatest lower bound (GLB) and least upper bound (LUB) exists.

Note:

(i) GLB $\{a, b\} = a * b\ (or)\ a \wedge b\ (or)\ a \cdot b$

(ii) LUB $\{a, b\} = a \oplus b\ (or) a \vee b\ (or) a + b$

Properties of lattice:

Some important laws and its proof:

(i) Idempotent law:

$a \vee a = a, a \wedge a = a$

(ii) Commutative law:

$a \vee b = b \vee a \ \ and \ \ a \wedge b = b \wedge a$

(iii) Associative law:

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

(iv) Absorption law:

$a \vee (a \wedge b) = a \ and \ a \wedge (a \vee b) = a$

(v) Distributive law:

$a \wedge (b \vee c) \geq (a \wedge b) \vee (a \wedge c)$

$a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$

Note:

i) $a \leq a \vee b \; and \; b \leq a \vee b$

$a \vee b$ is the upper bound of a and b.

If $a \leq c \; and \; b \leq c$ then $a \vee b \leq c$

Hence $a \vee b$ is the lub of a and b.

(ii) $a \wedge b \leq a \; and \; a \wedge b \leq b$

$a \wedge b$ is the lower bound of a and b.

If $c \leq a \; and \; c \leq b$ then $c \leq a \wedge b$

Hence $a \wedge b$ is the glb of a and b.

Note:

If $a \leq b \; and \; a \leq c$ then $a \leq b \vee c$

If $a \leq b \; and \; a \leq c$ then $a \leq b \wedge c$

Problems:

1. State and prove Idempotent law:

Let $(L, \wedge, \vee)$ be given lattice. Then, for any $a, b, c \in L$,

$$a \vee a = a, a \wedge a = a.$$

Proof:

Given $a \vee a = \text{LUB}(a, a) = \text{LUB}(a) = a$

Hence $a \vee a = a$

Now, $a \wedge a = \text{GLB}(a, a) = \text{GLB}(a) = a$

Hence $a \wedge a = a$

Hence the proof.

2. State and prove Commutative law:

Let $(L, \wedge, \vee)$ be given lattice. Then, for any $a, b, c \in L$,

$$a \vee b = b \vee a \text{ and } a \wedge b = b \wedge a$$

Proof:

Given $a \vee b = \text{LUB}(a, b) = \text{LUB}(b, a) = b \vee a$

Hence $a \vee b = b \vee a$

Now, $a \wedge b = \text{GLB}(a, b) = \text{GLB}(b, a) = b \wedge a$

Hence $a \wedge b = b \wedge a$

Hence the proof.

3. State and prove Absorption law.

(or)

Prove that $\boldsymbol{a \vee (a \wedge b) = a}$ *and* $\boldsymbol{a \wedge (a \vee b) = a}$

Proof:

We have $a \wedge b \leq a$ *and* $a \leq a$

$\Rightarrow$ a is the upper bound of $a \wedge b$ and a.

$\Rightarrow a \vee (a \wedge b) \leq a$ . . . (1)

From the definition of lub we have

$\Rightarrow a \leq a \vee (a \wedge b)$ . . . (2)

From (1) and (2) we have $a \vee (a \wedge b) = a$

Similarly we can prove that $a \wedge (a \vee b) = a$

Hence the proof.

4. Every finite Lattice is bounded.

Proof:

Let $(L, \wedge, \vee)$ be a given lattice.

Since L is a Lattice both GLB and LUB exist.

Let "a" be GLB of L and "b" be LUB of L.

Then for any $x \in L$, we have $a \leq x \leq b$ . . . (1)

From (1)

GLB $\{a, x\} = a \wedge x = a$

LUB $\{a, x\} = a \vee x = x$

And

GLB $\{x, b\} = x \wedge b = x$

LUB $\{x, b\} = x \vee b = b$

Therefore any finite lattice is bounded.

Hence the proof.

5. State and prove Isotonicity property.

Let $(L, \leq)$ be a lattice. For any $a, b, c \in L$ then $b \leq c = \begin{cases} a \wedge b \leq a \wedge c \\ a \vee b \leq a \vee c \end{cases}$

Proof:

By consistency law we have, $a \leq b \Leftrightarrow a \wedge b = a \; and \; a \vee b = a$

Let $b \leq c \Rightarrow b \wedge c = b$ and $b \vee c = c$

Consider $(a \wedge b) \wedge (a \wedge c) = a \wedge [(b \wedge a) \wedge c]$ by Associative law

$= a \wedge [(a \wedge b) \wedge c]$ by Commutative law

$= (a \wedge a) \wedge (b \wedge c)$ by Associative law

$= a \wedge (b \wedge c)$ by Idempotent law

$= a \wedge b$ by $[b \wedge c = b]$

Hence $(a \wedge b) \wedge (a \wedge c) = a \wedge b$

$\Rightarrow a \wedge b \leq a \wedge c$ . . . (1)

Consider $(a \vee b) \wedge (a \vee c) = a \vee [(b \vee a) \vee c]$ by Associative law

$= a \vee [(a \vee b) \vee c]$ by Commutative law

$= (a \vee a) \vee (b \vee c)$ by Associative law

$= a \vee (b \vee c)$ by Idempotent law

$= a \vee b$ by $[b \vee c = b]$

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

$\Rightarrow a \vee b \leq a \vee c$ . . . (2)

Hence the proof.

6. State and prove Distributive law.

$\boldsymbol{a \wedge (b \vee c) \geq (a \wedge b) \vee (a \wedge c)}$

$\boldsymbol{a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c)}$

Proof:

We know that $a \wedge b \leq a$ and $a \wedge b \leq b$

Also $b \leq b \vee c$

Hence $a \wedge b \leq a$ and $a \wedge b \leq b \leq b \vee c$

Hence $a \wedge b$ is the lower bound of a and $b \vee c$.

$\Rightarrow a \wedge b \leq a \wedge (b \vee c)$ . . . (1)

Again $a \wedge c \leq a$ and $a \wedge c \leq c$

Also $c \leq b \vee c$

Hence $a \wedge c \leq a$ and $a \wedge c \leq c \leq b \vee c$

Hence $a \wedge c$ is the lower bound of a and $b \vee c$.

$\Rightarrow a \wedge c \leq a \wedge (b \vee c)$ . . . (2)

From (1) and (2) we have

$a \wedge (b \vee c)$ is the upper bound of $a \wedge b$ and $a \wedge c$

Hence $(a \wedge b) \vee (a \wedge c) \leq a \wedge (b \vee c)$

$\Rightarrow a \wedge (b \vee c) \geq (a \wedge b) \vee (a \wedge c)$ . . . (I)

We know that $a \leq a \vee b$ and $a \leq a \vee b$

Also $b \wedge c \leq b$

Hence $a \leq a \vee b$ and $b \wedge c \leq b \leq a \vee b$

Hence $a \vee b$ is the lower bound of a and $b \wedge c$.

$\Rightarrow a \vee (b \wedge c) \leq a \vee b$ . . . (3)

Again $a \leq a \vee a$ and $c \leq a \vee c$

Also $b \wedge c \leq c$

Hence $a \leq a \vee c$ and $b \wedge c \leq c \leq a \vee c$

Hence $a \vee c$ is the upper bound of a and $b \wedge c$.

$\Rightarrow a \vee (b \wedge c) \leq a \vee c$ . . . (4)

From (3) and (4) we have

$a \vee (b \wedge c)$ is the lower bound of $a \vee b$ and $a \vee c$

$\Rightarrow a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$ . . . (II)

Hence the proof.

7. State and prove Cancellation law.

Let $(L, \leq)$ be a distributive lattice. Then $a \vee b = a \vee c$ and $a \wedge b = a \wedge c \Rightarrow b = c \; \forall \; a, b, c \in L$

Proof:

By absorption law, we have $a \vee (a \wedge b) = a$

Consider $b = b \vee (a \wedge b)$

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

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

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

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

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

$= c$

Hence the proof.

8. State and prove Consistency Law.

Let $(L, \leq)$ be a lattice. Then $a \leq b \Leftrightarrow a \wedge b = a \Leftrightarrow a \vee b \; \forall \; a, b, c \in L$

Proof:

First we prove that $a \leq b \Leftrightarrow a \wedge b = a$

We assume that $a \leq b$

To prove $a \wedge b = a$

We have $a \leq b$ and $a \leq a$

$\Rightarrow$ a is the lower bound of a and b.

$\Rightarrow a \leq a \wedge b$ . . . (1)

By the definition of greatest lower bound

$\Rightarrow a \wedge b \leq a$ . . . (2)

From (1) and (2) we have, $a = a \wedge b$

Conversely assume that $a = a \wedge b$

To prove $a \leq b$

This is possible only when $a \leq b$

Hence $a \leq b \Leftrightarrow a \wedge b = a$

Next we prove that $a \wedge b = a \Leftrightarrow a \vee b = b$

Assume that $a \wedge b = a$

To prove $a \vee b = b$

By absorption law $a \vee (a \wedge b) = a \; and \; a \wedge (a \vee b) = a$

Consider $b = b \vee (a \wedge b)$

$= b \vee a$

Hence $a \vee b = b$

Conversely assume that $a \vee b = b$

To prove $a \wedge b = a$

By absorption law $a \wedge (a \vee b) = a$

Consider $a = a \wedge (a \vee b)$

$= a \wedge b$

Hence $a \wedge b = a \Leftrightarrow a \vee b = b$

9. Show that a chain is a lattice.

Proof:

Let $(L, \leq)$ be a lattice.

If $a, b \in L$ then $a \leq b$ or $b \leq a$

If $a \leq b$ then $a \wedge b = a$ and $a \vee b = b$

Therefore GLB and LUB of a and b exists.

If $b \leq a$ then $b \wedge a = b$ and $b \vee a = a$

Therefore GLB and LUB of a and b exists.

Hence every pair of elements has a GLB and LUB.

Hence chain is lattice.

Duality in Lattice:

When " $\leq$ " is a partial order relation on a set S, then its converse " $\geq$ " is also a partial order relation on S.

Distributive lattice:

A lattice $(L, \wedge, \vee)$ is said to be distributive lattice if $\wedge$ and $\vee$ satisfies the following conditions $\forall a, b, c \in L$

$D_1: a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$

$D_2: a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$

Modular Inequality:

If $(L, \wedge, \vee)$ is a Lattice, then for any $a, b, c \in L$, $a \leq c \Leftrightarrow a \vee (b \wedge c) \leq (a \vee b) \wedge c$.

Proof:

Assume $a \leq c$

$\Rightarrow a \vee c = c \qquad \ldots (1)$

By, distributive inequality, we have

$a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$

$\Rightarrow a \vee (b \wedge c) \leq (a \vee b) \wedge c$ (Using (1))

Therefore, $a \leq c \Leftrightarrow a \vee (b \wedge c) \leq (a \vee b) \wedge c$. . . . (2)

Conversely, assume $a \vee (b \wedge c) \leq (a \vee b) \wedge c$

Now, by the definition of LUB and GLB, we have

$a \leq a \vee (b \wedge c) \leq (a \vee b) \wedge c \leq c$

$\Rightarrow a \leq c$

Hence $a \vee (b \wedge c) \leq (a \vee b) \wedge c \Rightarrow a \leq c$ . . . (3)

From (2) and (3), we have $a \leq c \Leftrightarrow a \vee (b \wedge c) \leq (a \vee b) \wedge c$.

Hence the proof.

Modular Lattice:

A Lattice $(L, \wedge, \vee)$ is said to be Modular lattice if it satisfies the following condition.

M_1: if $a \leq c$ then $a \vee (b \wedge c) = (a \vee b) \wedge c$

Theorem: 1

Every distributive Lattice is Modular, but not conversely.

Proof:

Let $(L, \wedge, \vee)$ be the given distributive lattice

$D_1: a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$ . . . (1)

Now, if $a \leq c$ then $a \vee c = c$ . . . (2)

(1)(1) $\Rightarrow a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$

$= (a \vee b) \wedge c$ (using (2))

If $a \leq c$ then $a \vee (b \wedge c) = (a \vee b) \wedge c$

Therefore every distributive lattice is Modular.

But, converse is not true.

i.e., Every Modular Lattice need not be distributive.

For example, M_5 Lattice is Modular but it is not distributive.

Hence the proof.

Theorem: 2

In any distributive lattice $(L, \wedge, \vee)$ $\forall a, b, c \in L$. Prove that

$$a \vee b = a \vee c, a \wedge b = a \wedge c \Rightarrow b = c$$

Proof:

Consider $b = b \vee (b \wedge a)$ (Absorption law)

$= b \vee (a \wedge b)$ (Commutative law)

$= b \vee (a \wedge c)$ (Given condition)

$= (b \vee a) \wedge (b \vee c)$ (D1 – Condition)

$= (a \vee b) \wedge (b \vee c)$ (Commutative law)

$= (a \vee c) \wedge (b \vee c)$ (Using given condition)

$= (c \vee a) \wedge (c \vee b)$ (Commutative law)

$= c \vee (a \wedge b)$ (By D1- condition)

$= c \vee (a \wedge c)$ (Given Condition)

$= c \vee (c \wedge a)$ (Commutative law)

$= c$ (Absorption law)

Lattice as a Algebraic system

A Lattice is an algebraic system $(L, \wedge, \vee)$ with two binary operation $\wedge$ and $\vee$ on L which are both commutative, associative and satisfies absorption laws.

SubLattice:

Let $(L, \wedge, \vee)$ be a lattice and let $S \subseteq L$ be a subset of L. Then $(S, \wedge, \vee)$ is a sublattice of $(L, \wedge, \vee)$ iff S is closed under both operation $\wedge$ and $\vee$.

$\forall a, b \in S \Rightarrow a \wedge b \in S$ and $a \vee b \in S$

Lattice Homomorphism:

Let $(L_1, \wedge, \vee)$ and $(L_2, *, \oplus)$ be two given lattices.

A mapping $f: L_1 \to L_2$ is called Lattice homomorphism if $\forall a, b \in L_1$

$f(a \wedge b) = f(a) * f(b)$

$f(a \vee b) = f(a) \oplus f(b)$

A homomorphism which is also 1 – 1 is called an isomorphism.

Bounded lattice:

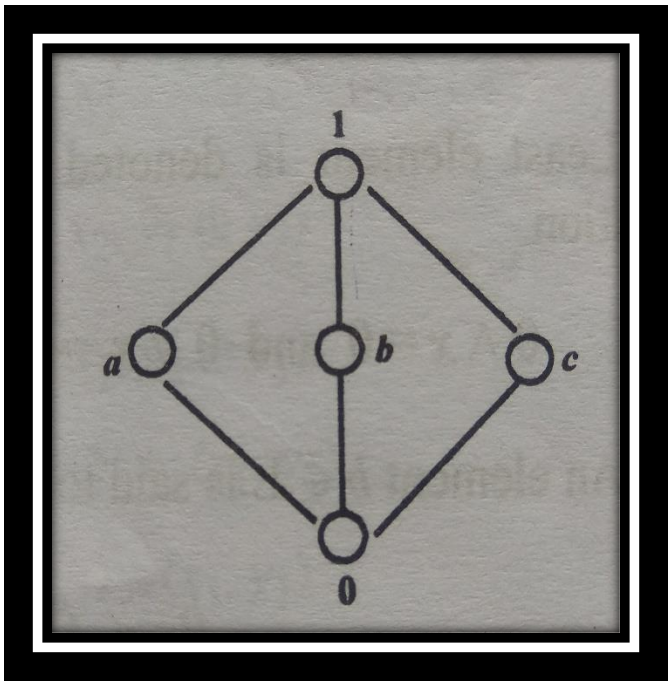
Let $(L, \wedge, \vee)$ be a given Lattice. If it has both "0" element and "1" element then it is said to be bounded Lattice. It is denoted by $(L, \wedge, \vee, 0, 1)$

Complement:

Let $(L, \wedge, \vee, 0, 1)$ be given bounded lattices. Let "a" be any element of L. We say that "b" is complement of a, if $a \wedge b = 0$ and $a \vee b = 1$ and "b" is denoted by the symbol a'. i.e., $(b = a')$. Therefore $a \wedge a' = 0$ and $a \vee a' = 1$.

Note: An element may have no complement or may have more than 1 complement.

Example for a complement.

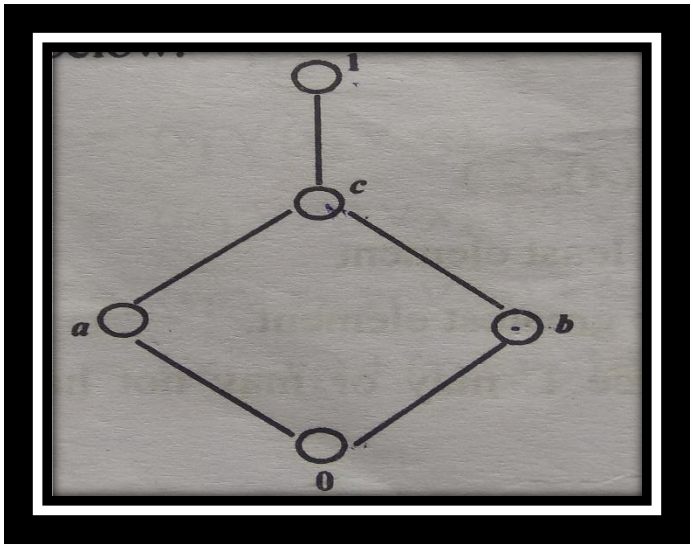


Complement of $a = a'$ is b and c.

Complement of $b = b'$ is a and c.

Complement of $c = c'$ is a and b.

In the example given below:



Complement of does not exist.

Complement of b does not exist.

Complement of c does not exist.

Complemented Lattice:

A bounded lattice $(L, \wedge, \vee, 0, 1)$ is said to be a complemented lattice if every element of L has atleast one complement.

Complete Lattice:

A lattice $(L, \wedge, \vee)$ is said to be complete lattice if every non empty subsets of L has both glb &lub.

1. Prove that in a bounded distributive lattice, the complement of any element is unique.

Proof:

Let L be a bounded distributive lattice.

Let b and c be complements of an element $a \in L$.

To prove $b = c$

Since b and c are complements of a we have

$a \wedge b = 0, a \vee b = 1, a \wedge c = 0, a \vee c = 1$

Now $b = b \wedge 1$

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

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

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

$= 0 \vee (b \wedge c)$

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

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

$= 1 \wedge c$

$= c$

Hence the proof.

2. Prove that every distributive lattice is modular.

Proof:

Let $(L, \leq)$ be a distributive lattice.

Let $a, b, c \in L$ such that $a \leq c$

To prove that $a \leq c \Rightarrow a \vee (b \wedge c) = (a \vee b) \wedge c$

Assume that $a \leq c$

To prove that $a \vee (b \wedge c) = (a \vee b) \wedge c$

When $a \leq c \Rightarrow a \vee c = c$

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

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

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

Hence the proof.

3. Show that in a complemented distributive lattice, $a \leq b \Leftrightarrow a * b' = 0 \Leftrightarrow a' \oplus b = 1 \Leftrightarrow b' \leq a'$ (or) , $a \leq b \Leftrightarrow a \wedge b' = 0 \Leftrightarrow a' \vee b = 1 \Leftrightarrow b' \leq a'$

Proof:

To prove $(i) \Rightarrow (ii)$

We assume that $a \leq b$

To prove that $a \wedge b' = 0$

We know that $a \leq b \Rightarrow a \wedge b = a$ and $a \vee b = b$

We take $a \vee b = b$

$\Rightarrow (a \vee b) \wedge b' = b \wedge b' = 0$

$\Rightarrow (a \wedge b') \vee (b \wedge b') = 0$

$\Rightarrow (a \wedge b') \vee 0 = 0$

$\Rightarrow (a \wedge b') = 0$

Hence $(i) \Rightarrow (ii)$

To prove $(\boldsymbol{ii}) \Rightarrow (\boldsymbol{iii})$

We assume that $a \wedge b' = 0$

To prove that $a' \vee b = 1$

Taking complement on both sides

$\Rightarrow (a \wedge b')' = 0'$

$\Rightarrow a' \vee b = 1$

Therefore $a \wedge b' = 0 \Rightarrow a' \vee b = 1$

Hence $(ii) \Rightarrow (iii)$

To prove $(\boldsymbol{iii}) \Rightarrow (\boldsymbol{iv})$

Assume that $a' \vee b = 1$

To prove that $b' \leq a'$

Now $a' \vee b = 1$

$\Rightarrow (a' \vee b) \wedge b' = 1 \cdot b'$

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

$\Rightarrow (a' \wedge b') \wedge (b \wedge b') = b'$

$\Rightarrow (a' \wedge b') \vee 0 = b'$

$\Rightarrow (a' \wedge b') = b'$

$\Rightarrow (b' \wedge a') = b'$ by Commutative law

Therefore $a' \vee b = 1 \Rightarrow b' \leq a'$

Hence $(iii) \Rightarrow (iv)$

To prove $(iv) \Rightarrow (i)$

Assume that $b' \leq a'$

To prove that $a \leq b$

We have $(b' \wedge a') = b'$

Taking complement on both sides

$\Rightarrow (b' \wedge a')' = (b')'$

$\Rightarrow b \vee a = b$

Therefore $a \vee b = b \Rightarrow a \leq b$

Hence $(iv) \Rightarrow (i)$

Hence $a \leq b \Leftrightarrow a \wedge b' = 0 \Leftrightarrow a' \vee b = 1 \Leftrightarrow b' \leq a'$

Hence the proof.

4. State and prove DeMorgan's law of lattice.

(OR)

Let $(L, \wedge, \vee, 0, 1)$ is a complemented lattice, then prove that

1. $(a \wedge b)' = a' \vee b'$

2. $(a \vee b)' = a' \wedge b'$

Proof:

1. Claim: $(a \wedge b)' = a' \vee b'$

To prove the above, it is enough to prove that

(i) $(a \wedge b) \wedge (a' \vee b') = 0$

(ii) $(a \wedge b) \vee (a' \vee b') = 1$

(i) Let $(a \wedge b) \wedge (a' \vee b')$

$\Rightarrow \big((a \wedge b) \wedge a'\big) \vee \big((a \wedge b) \wedge b'\big)$ (Distributive law)

$\Rightarrow (a \wedge b \wedge a') \vee (a \wedge b \wedge b')$ (Associative law)

$\Rightarrow (0 \wedge b) \vee (a \wedge 0)$ $(b \wedge b' = 0)$

$\Rightarrow 0 \vee 0$ $(a \wedge 0 = 0)$

Hence $(a \wedge b) \wedge (a' \vee b') = 0$ . . . (1)

(ii) Let $(a \wedge b) \wedge (a' \vee b')$

$\Rightarrow \big(a \vee (a' \vee b')\big) \wedge \big(b \vee (a' \vee b')\big)$ (Distributive law)

$\Rightarrow (a \vee b \vee a') \wedge (a \vee b \vee b')$ (Associative law)

$\Rightarrow (1 \vee b) \wedge (a \vee 1)$ $(b \vee b' = 1)$

$\Rightarrow 1 \wedge 1 = 1$ $(a \wedge 0 = 0)$

Hence $(a \wedge b) \wedge (a' \vee b') = 1$ . . . (2)

From (1) and (2) we have, $(a \wedge b)' = a' \vee b'$

2. Claim: $(\boldsymbol{a} \vee \boldsymbol{b})' = \boldsymbol{a}' \wedge \boldsymbol{b}'$

To prove the above, it is enough to prove that

(i) $(a \vee b) \wedge (a' \wedge b') = 0$

(ii) $(a \vee b) \vee (a' \wedge b') = 1$

(i) Let $(a \vee b) \wedge (a' \wedge b')$

$\Rightarrow \big(a \wedge (a' \wedge b')\big) \vee \big(b \wedge (a' \wedge b')\big)$ (Distributive law)

$\Rightarrow (a \wedge a' \wedge b') \vee (b \wedge b' \wedge a')$ (Associative law)

$\Rightarrow (0 \wedge b') \vee (0 \wedge a')$ $(b \wedge b' = 0)$

$\Rightarrow 0 \vee 0$ $(a \wedge 0 = 0)$

Hence $(a \vee b) \wedge (a' \wedge b') = 0$ . . . (3)

(ii) Let $(a \vee b) \vee (a' \wedge b')$

$\Rightarrow \big((a \vee b) \vee a'\big) \wedge \big((a \vee b) \vee b'\big)$ (Distributive law)

$\Rightarrow (a \vee b \vee a') \wedge (a \vee b \vee b')$ (Associative law)

$\Rightarrow (1 \vee b) \wedge (a \vee 1)$ $(b \vee b' = 0)$

$\Rightarrow 1 \wedge 1 = 1$ (Idempotent law)

Hence $(a \vee b) \vee (a' \wedge b') = 1$ . . . (4)

From (3) and (4) we have, $(a \vee b)' = a' \wedge b'$

Boolean Algebra:

A complemented distributive lattice is called Boolean Algebra.

A Boolean algebra is distributive lattice with "0" element and "1" element in which every element has a complement.

A Boolean algebra is a non empty set with 2 binary operations $\wedge$ and $\vee$ and is satisfied by the following conditions. $\forall a, b, c \in L$

1. $L_1: a \wedge a = a$ and $a \vee a = a$

2. $L_2: a \wedge b = b \wedge a$ and $a \vee b = b \vee a$

3. $L_3: a \wedge (b \wedge c) = (a \wedge b) \wedge c$ and $a \vee (b \vee c) = (a \vee b) \vee c$

4. $L_4: a \wedge (a \vee b) = a$ and $a \vee (a \wedge b) = a$

5. $D_1: a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$

6. $D_2: a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$

7. There exist between "0" and "1" such that $a \wedge 0 = 0, a \vee 0 = a, a \wedge 1 = a$ and

$a \vee 1 = 1 \forall a$

8. $\forall a \in L$, there exist corresponding element a' in L such that $a \wedge a' = 0$ and

$a \vee a' = 1$

Note:

Boolean Sum is defined as $1 + 1 = 1,\ 1 + 0 = 1,\ 0 + 1 = 1,\ 0 + 0 = 0$

Boolean Product is defined as $1 \cdot 1 = 1,\ 1 \cdot 0 = 0,\ 0 \cdot 1 = 0,\ 0 \cdot 0 = 0$

Absorption law in Boolean Algebra

1. Prove that $\boldsymbol{a + ab = a}$

Solution:

LHS $= a + ab$

$= a(1 + b)$ (Distributive law)

$= a(1)$ $(1 + a) = 1$

$a + ab = a$ $(a \cdot 1 = a)$

2. Prove that $\boldsymbol{a + \bar{a}b = a + b}$

Solution:

LHS $= a + \bar{a}b$

$= a + ab + \bar{a}b$ $(a = a + ab)$

$= a + b(a + \bar{a})$ (Distributive law)

$= a + b(1)$ $(a + \bar{a}) = 1$ $(a \cdot 1 = a)$

= RHS

3. Prove that $(a + b)(a + c) = a + bc$

Solution:

LHS = $(a + b)(a + c)$

$= aa + ac + ab + bc$ (Distributive law)

$= a + ac + ab + bc$ $(a \cdot a = a)$

$= a(1 + c) + ab + bc$ (Distributive law)

$= a + ab + bc$ $(1 + a = 1)$

$= a + bc$ $(a + ab = a)$

= RHS

4. In any Boolean Algebra, show that $a = b \Leftrightarrow a\bar{b} + \bar{a}b = 0$

Proof:

Let $(B, \cdot, +, 0, 1)$ be any Boolean Algebra.

Let $a, b \in B \; and \; a = b$ . . . (1)

Claim: $a\bar{b} + \bar{a}b = 0$

Now $a\bar{b} + \bar{a}b = a \cdot \bar{b} + \bar{a}.b$

$= a \cdot \bar{a} + \bar{a}.a$ using (1)

$= 0 + 0$ (since $a \cdot \bar{a} = 0$)

$= 0$

Conversely, assume $a\bar{b} + \bar{a}b = 0$

$\Rightarrow a + a\bar{b} + \bar{a}b = a$ (Left Cancellation law)

$\Rightarrow a + a\bar{b} = a$ (Absorption law)

$\Rightarrow (a + \bar{a}) \cdot (a + b) = a$ (Distributive law)

$\Rightarrow 1 \cdot (a + b) = a$ $(a + \bar{a} = 1)$

$\Rightarrow (a + b) = a$ $(a \cdot 1 = a)$ . . . (a)

Consider $a\bar{b} + \bar{a}b = 0$

$\Rightarrow a\bar{b} + \bar{a}b + b = b$ (Right Cancellation law)

$\Rightarrow a\bar{b} + b = b$ (Absorption law)

$\Rightarrow (a + b) \cdot \left(b + \bar{b}\right) = b$ (Distributive law)

$\Rightarrow (a + b) \cdot 1 = a$ $(b + \bar{b} = 1)$

$\Rightarrow (a + b) = b$ $(b \cdot 1 = b)$ . . . (b)

From (a) and (b) we get $a = a + b = b$

Hence $a = b$

5. If a and b are two elements of a Boolean algebra, then prove that

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

Proof:

Consider $a + (a \cdot b) = a = a \cdot 1 + (a \cdot b)$

$$= a \cdot (1 + b)$$

$$= a \cdot 1 \qquad [a + 1 = 1, 1 + a = 1]$$

$$= a$$

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

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

$$= a \cdot 1 + a \cdot b$$

$$= a \cdot (1 + b)$$

$$= a \cdot 1 \qquad [a \cdot a = a, a \cdot 0 = 0]$$

$$= a$$

Hence the proof.

6. Prove that in a Boolean algebra, the complement of any element is unique.

Proof:

Let b and c be the complements of the element a.

Then $b + a = 1,\ b \cdot a = 0$

$a + c = 1,\ a \cdot c = 0$

Consider $b = 1 \cdot b$

$= (a + c) \cdot b$

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

$= 0 + c \cdot b$

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

$= c \cdot (a + b)$

$= 1 \cdot c$

$= c$

Hence the complement is unique.

7. In a Boolean algebra show that the following statements are equivalent. For any a and b (i) $a + b = b$ (ii) $a \cdot b = a$ (iii) $a' + b = 1$ (iv) $a \cdot b' = 0$ (v) $a \leq b$

Proof:

To prove $(i) \Rightarrow (ii)$

Assume that $a + b = b$

To prove that $a \cdot b = a$

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

$= a \cdot b$

Hence $(i) \Rightarrow (ii)$

To prove $(ii) \Rightarrow (iii)$

Assume that $a \cdot b = a$

To prove that $a' + b = 1$

Now $a' + b = (a \cdot b') + b$

$= a' + b' + b$

$= a' + 1$

$= 1$

Hence $(ii) \Rightarrow (iii)$

To prove $(iii) \Rightarrow (iv)$

Assume that $a' + b = 1$

To prove that $a \cdot b' = 0$

Taking complement on both sides

$\Rightarrow (a' + b)' = 1'$

$\Rightarrow a \cdot b' = 0$

Hence $(iii) \Rightarrow (iv)$

To prove $(\boldsymbol{iv}) \Rightarrow (\boldsymbol{v})$

Assume that $a \cdot b' = 0$

To prove that $a \leq b$

Then $a \cdot b = a \cdot b + 0$

$= a \cdot b + a \cdot b'$

$= a(b + b')$

$= a \cdot 1$

$= a$

Hence $(iv) \Rightarrow (v)$

To prove $(\boldsymbol{v}) \Rightarrow (\boldsymbol{i})$

Assume that $a \leq b$

To prove that $a + b = b$

We have $a \cdot b = b$

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

$= a \cdot b + 1 \cdot b$

$= (a + 1) \cdot b$

$= 1 \cdot b$

$= b$

Hence the proof.

8. Prove that in a Boolean algebra

$$(\boldsymbol{a + b}) \cdot (\boldsymbol{a' + c}) = \boldsymbol{ac + a'b = ac + a'b + bc}$$

Proof:

Now, $(a + b) \cdot (a' + c) = (a + b) \cdot a' + (a + b) \cdot c$

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

$= aa' + a'b + ac + bc$

$= 0 + a'b + ac + bc$

$= a'b + ac + bc$

$= ac(b + b') + a'b(c + c') + bc(a + a')$

$= abc + ab'c + a'bc + a'bc' + abc + a'bc$

$= abc + ab'c + a'bc + a'bc'$

$= abc + ab'c + a'b(c + c')$

$= ac(b + b') + a'b(c + c')$

$= ac(1) + a'b(1)$

$= ac + a'b$

= RHS

9. Show that in a Boolean algebra the law of the double complement holds.

(or) Prove the involution law $(a')' = a$

Solution:

It is enough to prove that $a' + a = 1$ and $a \cdot a' = 0$

By domination laws of Boolean algebra, we get

$a' + a = 1$ and $a \cdot a' = 0$

By commutative law, we get $a' + a = 1$ and $a \cdot a' = 0$

Therefore complement of a' is a

$\Rightarrow (a')' = a$

$\Rightarrow a'' = a$

Hence the proof.