PIE Tech

POLLACHI INSTITUTE OF ENGINEERING AND TECHNOLOGY

(Approved by AICTE and Affiliated to Anna University)

sky is the limit

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

&

DEPARTMENT OF ARTIFICIAL INTELLIGENCE AND DATA SCIENCE

REGULATION 2021

II YEAR /III SEM

MA3354 DISCRETE MATHEMATICS

MA3354 **DISCRETE MATHEMATICS** **L T P C**
3 1 0 4

OBJECTIVES:

- To extend student's logical and mathematical maturity and ability to deal with abstraction.
- To introduce most of the basic terminologies used in computer science courses and application of ideas to solve practical problems.
- To understand the basic concepts of combinatorics and graph theory.
- To familiarize the applications of algebraic structures.
- To understand the concepts and significance of lattices and boolean algebra which are widely used in computer science and engineering.

UNIT I LOGIC AND PROOFS **9+3**

Propositional logic – Propositional equivalences - Predicates and quantifiers – Nested quantifiers – Rules of inference - Introduction to proofs – Proof methods and strategy.

UNIT II COMBINATORICS **9+3**

Mathematical induction – Strong induction and well ordering – The basics of counting – The pigeonhole principle – Permutations and combinations – Recurrence relations – Solving linear recurrence relations – Generating functions – Inclusion and exclusion principle and its applications

UNIT III GRAPHS **9+3**

Graphs and graph models — Graph terminology and special types of graphs — Matrix representation of graphs and graph isomorphism – Connectivity – Euler and Hamilton paths.

UNIT IV ALGEBRAIC STRUCTURES **9+3**

Algebraic systems – Semi groups and monoids - Groups – Subgroups – Homomorphism's – Normal subgroup and cosets – Lagrange's theorem – Definitions and examples of Rings and Fields.

UNIT V LATTICES AND BOOLEAN ALGEBRA **9+3**

Partial ordering – Posets – Lattices as posets – Properties of lattices - Lattices as algebraic systems – Sub lattices – Direct product and homomorphism – Some special lattices – Boolean algebra-Sub Boolean Algebra – Boolean Homomorphism.

TOTAL: 60 PERIODS

UNIT - I

Logic and proofs

Proposition:

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

Examples:

1) Chennai is the capital of Tamilnadu (True)
2) $1+5=6$ (True)   3) $2+7=10$ (False)
4) Delhi is in America (False).

Some sentences that are not propositions are given in the following example. 1) What time is it ?
2) $x+1=2$.

The truth value of a proposition is true, denoted by T, if it is a true proposition and false, denoted by F, if it is a false proposition.

Negation of a proposition:

If p is a proposition, then its negation is denoted by $\neg p$ and is defined by the following truth table.

p	$\neg p$
T	F
F	T

Example: 1) p: Today is Monday
$\neg p$: Today is not Monday

2) $p: x<y$
$\neg p: x \nless y$ (or) $x \geq y$

Conjunction [$\wedge$] [AND]

If p and q are two propositions, then the conjunction of p and q is denoted by $p \wedge q$ (read as p and q) and is defined by the following truth table.

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

Example : 1) P : It is snowing
2) Q : I am cold
$P \wedge Q$: It is snowing and I am cold

2) P : $2 < 6$
Q : $2+6 = 9$
$P \wedge Q$: $2 < 6$ and $2+6=9$

Disjunction [$\vee$] [OR]

If P and Q are two propositions, then the disjunction of P and Q is denoted by $P \vee Q$ [Read as P or Q] and is defined by the following truth table.

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

Example : 1) P : 2 is a positive integer
2) Q : $\sqrt{2}$ is a rational number
$P \vee Q$: 2 is a positive integer or $\sqrt{2}$ is a rational number.

2) P : $2+3 = 5$
Q : $3 < 2$
$P \vee Q$: $2+3 = 5$ or $3 < 2$

Conditional statement : [If, ... then] [$\rightarrow$]

If P and Q are two propositions, then the statement $P \rightarrow Q$ (read as "If P then Q", is called a conditional statement and is defined by the following truth table

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

Example : 1) P : I am hungry

Q : I will eat

$P \to Q$: If I am hungry, then I will eat

Converse, Contrapositive & Inverse Statements :

If $P \to Q$ is a conditional statement, then

i) $Q \to P$ is called converse of $P \to Q$.

ii) $\neg Q \to \neg P$ is called contrapositive of $P \to Q$.

iii) $\neg P \to \neg Q$ is called Inverse of $P \to Q$.

Example : If it is raining, then the home team wins.

P : If it is raining, Q : The home team wins.

Converse : If the home team wins, then it is raining

Contrapositive : If the home team does not win, then it is not raining.

Inverse : If it is not raining then the home team does not win.

Biconditional statement [$\leftrightarrow$] [If and only if]

If P and Q are two propositions, then the statement $P \leftrightarrow Q$, read as "P if and only if Q" (or) "P iff Q", is called a biconditional statement and is defined by the following truth table

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

Example : P : You can take the flight

Q : You buy a ticket

$P \leftrightarrow Q$: You can take the flight if and only if you buy a ticket.

Exclusive OR [$P \oplus Q$]

If P and Q are two propositions, the exclusive OR of P and Q is denoted by $P \oplus Q$ is the proposition that is true, when exactly one of P and Q is true and is false otherwise.

P	Q	$P \oplus Q$
T	T	F
T	F	T
F	T	T
F	F	F

Symbolize the following statements:

1) If the moon is out and it is not snowing, then Ram goes out for walk. $P \to (\neg Q \to R)$

2) If the moon is out, then if it is not snowing, Ram goes out for a walk.

3) It is not the case that Ram goes out for a walk if and only if it is not snowing or the moon is out.

Soln: Let P: The moon is out

Q: It is snowing

R: Ram goes out for a walk.

1) $(P \wedge \neg Q) \to R$ 2) $P \to (\neg Q \to R)$

3) $\neg(R \leftrightarrow (\neg Q \vee P))$.

Construction of truth tables.

1) Construct the truth table for $\neg P \wedge Q$.

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

2) Construct the truth table for $P \wedge (P \vee Q)$

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

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

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

4) $(P \wedge Q) \vee (\neg P \wedge Q) \vee (P \wedge \neg Q) \vee (\neg P \wedge \neg Q)$

P	Q	$\neg P$	$\neg Q$	$P \wedge Q$	$\neg P \wedge Q$	$P \wedge \neg Q$	$\neg P \wedge \neg Q$	S
T	T	F	F	T	F	F	F	T
T	F	F	T	F	F	T	F	T
F	T	T	F	F	T	F	F	T
F	F	T	T	F	F	F	T	T

Propositional Equivalences:

Tautology:

A statement formula which is always true for all possible values of its propositional values is called a tautology.
(eg) $P \vee \neg P$ is always a tautology.

Contradiction:

A statement formula which is always false is called a contradiction. (eg) $P \wedge \neg P$ is always a contradiction.

Example:

1) Prove that $Q \vee (P \wedge \neg Q) \vee (\neg P \wedge \neg Q)$ is a tautology.

Soln: 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

Since all the truth values in the last column is true, the given formula is a tautology.

2) Prove that $(P \wedge Q) \wedge \neg (P \vee Q)$

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

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

Since all the truth values in the last column is false, the given formula is a contradiction.

Logical Equivalence:

The propositions P and Q are called logically equivalent if $P \leftrightarrow Q$ is a tautology (or) P and Q have the same set of truth values. We write it as $P \equiv Q$ (or) $P \Leftrightarrow Q$

Example: Show that $P \rightarrow Q$ and $\neg P \vee Q$ are logically equivalent

Soln:

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

Since the truth values of $P \rightarrow Q$ and $\neg P \vee Q$ are equal, $P \rightarrow Q$ and $\neg P \vee Q$ are logically equivalent.

2) Show that $P \Leftrightarrow q$ and $(P \rightarrow q) \wedge (q \rightarrow P)$ are logically equivalent.

II) i) $P \rightarrow Q \Leftrightarrow \neg P \vee Q$

ii) $P \leftrightarrow Q \Leftrightarrow (P \wedge Q) \vee (Q \wedge P)$

iii) $P \leftrightarrow Q \Leftrightarrow (P \rightarrow Q) \wedge (Q \rightarrow P)$

Laws of Logic:

1) $P \wedge T \Leftrightarrow P$
$P \vee F \Leftrightarrow P$
Identity laws

2) $P \vee T \Leftrightarrow T$
$P \wedge F \Leftrightarrow F$
Domination laws

3) $P \vee P \Leftrightarrow P$
$P \wedge P \Leftrightarrow P$
Idempotent laws.

4) $\neg(\neg P) \Leftrightarrow P$ Double Negation law

5) $P \vee Q \Leftrightarrow Q \vee P$
$P \wedge Q \Leftrightarrow Q \wedge P$
Commutative law

6) $(P \vee Q) \vee R \Leftrightarrow P \vee (Q \vee R)$
$(P \wedge Q) \wedge R \Leftrightarrow P \wedge (Q \wedge R)$
Associative Laws

7) $P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$
$P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$
$(P \vee Q) \wedge R \Leftrightarrow (P \wedge R) \vee (Q \wedge R)$
$(P \wedge Q) \vee R \Leftrightarrow (P \vee R) \wedge (Q \vee R)$
Distributive Laws.

8) $\neg(P \wedge Q) \Leftrightarrow \neg P \vee \neg Q$
$\neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q$
DeMorgan's Law

9) $P \vee (P \wedge Q) \Leftrightarrow P$
$P \wedge (P \vee Q) \Leftrightarrow P$
Absorption Laws

10) $P \vee \neg P \Leftrightarrow T$
$P \wedge \neg P \Leftrightarrow F$
Negation laws.

Tautological Implication:

A statement formula A logically implies another statement formula B if and only if $A \to B$ is a tautology.

Example: Prove that $(P \wedge Q) \Rightarrow (P \vee Q)$

To prove: $(P \wedge Q) \to (P \vee Q)$ is a tautology.

P	Q	$P \wedge Q$	$P \vee Q$	$(P \wedge Q) \to (P \vee Q)$
T	T	T	T	T
T	F	F	T	T
F	T	F	T	T
F	F	F	F	T

The last column shows that $(P \wedge Q) \to (P \vee Q)$ is a tautology

$\therefore (P \wedge Q) \Rightarrow (P \vee Q)$.

2) Prove that $(P \to Q) \wedge (Q \to R) \Rightarrow P \to R$.

Logical Equivalence without using truth table.

1) Show that $(\neg P \wedge (\neg Q \wedge R)) \vee (Q \wedge R) \vee (P \wedge R) \Leftrightarrow R$

Soln:

(i) $\neg P \wedge (\neg Q \wedge R)$

$\Leftrightarrow (\neg P \wedge \neg Q) \wedge R$ [Associative Law]

$\Leftrightarrow \neg (P \vee Q) \wedge R$ [DeMorgan's Law]

(ii) $(Q \wedge R) \vee (P \wedge R)$

$\Leftrightarrow (Q \vee P) \wedge R$ [Distributive Law]

$\Leftrightarrow (P \vee Q) \wedge R$ [Commutative Law]

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

$\Leftrightarrow [\neg (P \vee Q) \wedge R] \vee [(P \vee Q) \wedge R]$ (by (i) and (ii))

$\Leftrightarrow [\neg (P \vee Q) \vee (P \vee Q)] \wedge R$ [Distributive Law]

$\Leftrightarrow T \wedge R$ [Negation Law, $\neg P \vee P \Leftrightarrow T$]

$\Leftrightarrow R$ [Identity Law]

2) Show that $\neg(P \wedge Q) \rightarrow (\neg P \vee (\neg P \vee Q)) \Leftrightarrow (\neg P \vee Q)$

Soln:

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

$\Leftrightarrow (\neg P \vee \neg P) \vee Q$ (Associative Law)

$\Leftrightarrow \neg P \vee Q$ [Idempotent law $P \vee P \Leftrightarrow P$]

$\neg(P \wedge Q) \rightarrow (\neg P \vee (\neg P \vee Q))$

$\Leftrightarrow \neg(P \wedge Q) \rightarrow (\neg P \vee Q)$ (by (i))

$\Leftrightarrow \neg(\neg(P \wedge Q)) \vee (\neg P \vee Q)$ [$P \rightarrow Q \Rightarrow \neg P \vee Q$]

$\Leftrightarrow (P \wedge Q) \vee (\neg P \vee Q)$ [Double Negation Law]

$\Leftrightarrow P \vee (\neg P \vee Q) \wedge (Q \vee (\neg P \vee Q))$ [Distributive Law]

$\Leftrightarrow [(P \vee \neg P) \vee Q] \wedge [Q \vee (Q \vee \neg P)]$ [Associative law & Commutative Law]

$\Leftrightarrow (T \vee Q) \wedge ((Q \vee Q) \vee \neg P)$ [Negation & Associative Law]

$\Leftrightarrow T \wedge (Q \vee \neg P)$ [Domination Law & Idempotent Law]

$\Leftrightarrow Q \vee \neg P$ [Identity Law]

$\Leftrightarrow \neg P \vee Q$ [Commutative Law].

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

Soln: $(P \vee Q) \wedge \neg P$

$\Leftrightarrow \neg P \wedge (P \vee Q)$ [Commutative Law]

$\Leftrightarrow (\neg P \wedge P) \vee (\neg P \wedge Q)$ [Distributive Law]

$\Leftrightarrow F \vee (\neg P \wedge Q)$ [Negation Law]

$\Leftrightarrow \neg P \wedge Q$ [Identity Law].

4) Show that $P \rightarrow (Q \vee R) \Leftrightarrow (P \rightarrow Q) \vee (P \rightarrow R)$

Soln: i) $P \rightarrow (Q \vee R)$

$\Leftrightarrow \neg P \vee (Q \vee R)$ [$P \rightarrow Q \Leftrightarrow \neg P \vee Q$]

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

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

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

$\Leftrightarrow \neg P \vee \neg P \vee Q \vee R$

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

$\Leftrightarrow \neg P \vee (Q \vee R)$ Idempotent law

From (i) and (ii), we get $P \to (Q \vee R) \Leftrightarrow (P \to Q) \vee (P \to R)$

5) Show that $\neg (P \leftrightarrow Q) \Leftrightarrow (P \vee Q) \wedge \neg (P \wedge Q)$.

Soln: $\neg (P \Leftrightarrow Q)$

$\Leftrightarrow \neg [(P \to Q) \wedge (Q \to P)]$ $[\because P \Leftrightarrow Q \Leftrightarrow (P \to Q) \wedge (Q \to P)]$

$\Leftrightarrow \neg [(\neg P \vee Q) \wedge (\neg Q \vee P)]$. $[\because P \to Q \Leftrightarrow \neg P \vee Q]$

$\Leftrightarrow \neg \{[(\neg P \vee Q) \wedge \neg Q] \vee [(\neg P \vee Q) \wedge P]\}$

$\Leftrightarrow \neg [(\neg P \wedge \neg Q) \vee (Q \wedge \neg Q) \vee (\neg P \wedge P) \vee (Q \wedge P)]$

$\Leftrightarrow \neg [\neg (P \vee Q) \vee F \vee F \vee (Q \wedge P)]$

$\Leftrightarrow \neg [\neg (P \vee Q) \vee (Q \wedge P)]$. Domination law.

$\Leftrightarrow (P \vee Q) \wedge \neg (P \wedge Q)$ Demorgan's law

Tautological implications:

1) Show that $(P \wedge Q) \Rightarrow (P \to Q)$

To prove $(P \wedge Q) \to (P \to Q)$ is a tautology

$\Leftrightarrow (P \wedge Q) \to (\neg P \vee Q)$ $[\because P \to Q \Leftrightarrow \neg P \vee Q]$

$\Leftrightarrow \neg [P \wedge Q] \vee (\neg P \vee Q)$ Demorgan's law

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

$\Leftrightarrow \neg P \vee \neg Q \vee \neg P \vee Q$

$\Leftrightarrow \neg P \vee \neg P \vee \neg Q \vee Q$ Negation.

$\Leftrightarrow \neg P \vee T \Leftrightarrow T$

Some more Connectives :

Exclusive Disjunction :

If P and Q are any two formulas, then $P \overline{\vee} Q$ is called the exclusive disjunction of P and Q and is defined by the truth table

P	Q	$P \overline{\vee} Q$
T	T	F
T	F	T
F	T	T
F	F	F

NAND ($\uparrow$)

It is a combination of $\neg$ and $\wedge$ and is defined by

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

NOR ($\downarrow$)

It is a combination of $\neg$ and $\vee$ and is defined by

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

Properties of NAND and NOR :

1) $P \uparrow Q \Leftrightarrow Q \uparrow P$ and $P \downarrow Q \Leftrightarrow Q \downarrow P$.
2) $(P \uparrow Q) \uparrow R \neq P \uparrow (Q \uparrow R)$ and $(P \downarrow Q) \downarrow R \neq P \downarrow (Q \downarrow R)$.

Functionally complete set of connectives :

A set of connectives is said to be functionally complete if any formula can be written as an equivalent formula containing only these connectives.

Example :

1) Show that $\{\vee, \neg\}$ is functionally complete.

Soln:

To prove a statement formula containing any of the connectives can be replaced in terms of the connectives $\neg$ and $\vee$.

$$P \rightarrow Q \Leftrightarrow \neg P \vee Q$$

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

$$P \leftrightarrow Q \Leftrightarrow (P \rightarrow Q) \wedge (Q \rightarrow P)$$

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

$$\Leftrightarrow \neg[\neg(\neg P \vee Q) \vee \neg(\neg Q \vee P)]$$

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

$$\Leftrightarrow \neg P \vee \neg Q$$

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

Therefore $\{\neg, \vee\}$ is a functionally complete set of connectives

Note: In this way, we can prove $\{\neg, \wedge\}$ is functionaly complete

2) Show that $\{\vee, \wedge\}$ is not functionally complete.

Soln: Consider $\neg P$

$\neg P$ cannot be expressed using the connectives $\{\vee, \wedge\}$

$\therefore$ $\{\vee, \wedge\}$ is not functionally complete.

Normal Forms:

Elementary Product:

The product of variables and their negations is called the elementary product.

Example: $P \wedge Q$, $P \wedge Q \wedge \neg R$.

Elementary Sum:

The sum of variables and their negations is called elementary sum.

Example: $P \vee Q$, $P \vee \neg Q \vee R$.

Note: $\vee$ is called sum and $\wedge$ is called product.

Sum of products:

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

products of sums:

$$(P \vee Q) \wedge (P \vee \neg Q) \wedge (\neg P \vee \neg Q).$$

Minterms: (product consisting of all variables)

1) $P \wedge Q$, $P \wedge \neg Q$, $\neg P \wedge Q$, $\neg P \wedge \neg Q$ are minterms in two variables P and Q.

2) $P \wedge Q \wedge R$, $P \wedge \neg Q \wedge R$, $P \wedge Q \wedge \neg R$, $\neg P \wedge Q \wedge R$, $\neg P \wedge \neg Q \wedge R$, $\neg P \wedge Q \wedge \neg R$, $P \wedge \neg Q \wedge \neg R$, $\neg P \wedge \neg Q \wedge \neg R$ are minterms in the variables P, Q and R.

Maxterms (Sum consisting of all variables)

1) $P \vee Q$, $P \vee \neg Q$, $\neg P \vee Q$, $\neg P \vee \neg Q$ are maxterms of two variables P and Q.

2) $P \vee Q \vee R$, $\neg P \vee Q \vee R$, $P \vee \neg Q \vee R$, $P \vee Q \vee \neg R$, $P \vee \neg Q \vee \neg R$, $\neg P \vee \neg Q \vee R$, $\neg P \vee Q \vee \neg R$, $\neg P \vee \neg Q \vee \neg R$ are maxterms of the variables P, Q and R.

Disjunctive Normal form:

A formula which is equivalent to a given formula and which consists of sum of elementary products is called the Disjunctive Normal Form (DNF) of the given formula.

Conjunctive Normal form:

A formula which is equivalent to a given formula and which consists of product of elementary sums is called Conjunctive Normal Form (CNF) of the given formula.

Principle Disjunctive Normal Form (PDNF):

The PDNF of a given formula P is an equivalent given formula consisting of disjunction of minterms only.

Principle conjunctive Normal Form (PCNF):

The PCNF of a given formula P is equivalent formula consisting of conjunction of maxterms only.

Example:

1) Obtain the Disjunctive Normal form and Conjunctive Normal Form of the formula $\neg(P \vee Q) \leftrightarrow (P \wedge Q)$.

Soln: $\neg(P \vee Q) \leftrightarrow (P \wedge Q)$

$\Leftrightarrow [\neg(P \vee Q) \wedge (P \wedge Q)] \vee [(P \vee Q) \wedge \neg(P \wedge Q)]$

$[\because P \leftrightarrow Q = (P \wedge Q) \vee (\neg P \wedge \neg Q)]$

$\Leftrightarrow [(\neg P \wedge \neg Q) \wedge (P \wedge Q)] \vee [(P \vee Q) \wedge (\neg P \vee \neg Q)]$

$\Leftrightarrow (\neg P \wedge \neg Q \wedge P \wedge Q) \vee [(P \vee Q) \wedge \neg P] \vee [(P \vee Q) \wedge \neg Q]$

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

The RHS is a sum of the elementary products.

Hence R.H.S is the required DNF.

Consider

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

$\Leftrightarrow [\neg(P \vee Q) \rightarrow (P \wedge Q)] \wedge [(P \wedge Q) \rightarrow \neg(P \vee Q)]$

$\Leftrightarrow [(P \vee Q) \vee (P \wedge Q)] \wedge [\neg(P \wedge Q) \vee \neg(P \vee Q)]$

$\Leftrightarrow (P \vee Q \vee P) \wedge (P \vee Q \vee Q) \wedge [(\neg P \vee \neg Q) \vee (\neg P \wedge \neg Q)]$

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

The R.H.S is the product of the elementary sums.

Hence RHS is the required CNF.

1) Obtain the PCNF of the formula $(\neg P \to R) \wedge (Q \Leftrightarrow P)$ and hence obtain its PDNF.

Soln: $(\neg P \to R) \wedge (Q \Leftrightarrow P)$

$\Leftrightarrow (\neg P \to R) \wedge [(Q \to P) \wedge (P \to Q)]$

$\Leftrightarrow (P \vee R) \wedge [(\neg Q \vee P) \wedge (\neg P \vee Q)]$

$\Leftrightarrow (P \vee R \vee F) \wedge (\neg Q \vee P \vee F) \wedge (\neg P \vee Q \vee F)$

$\Leftrightarrow [P \vee R \vee (Q \wedge \neg Q)] \wedge [\neg Q \vee P \vee (R \wedge \neg R)] \wedge [\neg P \vee Q \vee (R \wedge \neg R)]$

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

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

The RHS is the product of sums form.

Hence RHS is the required PCNF of S.

PCNF of $\neg S \Leftrightarrow (P \vee Q \vee \neg R) \wedge (\neg P \vee \neg Q \vee R) \wedge (\neg P \vee \neg Q \vee \neg R)$

PDNF of $S \Leftrightarrow \neg[\text{PCNF of } \neg S]$

PDNF of $S \Leftrightarrow (\neg P \wedge \neg Q \wedge R) \vee (P \wedge Q \wedge \neg R) \vee (P \wedge Q \wedge R)$.

2) Find the PCNF and PDNF of $(P \wedge Q) \vee (\neg P \wedge R)$

Soln: $(P \wedge Q) \vee (\neg P \wedge R)$

$\Leftrightarrow (P \wedge Q \wedge T) \vee (\neg P \wedge R \wedge T)$

$\Leftrightarrow [P \wedge Q \wedge (R \vee \neg R)] \vee [\neg P \wedge R \wedge (Q \vee \neg Q)]$

$\Leftrightarrow (P \wedge Q \wedge R) \vee (P \wedge Q \wedge \neg R) \vee [\neg P \wedge R \wedge \neg Q] \vee [\neg P \wedge \neg Q \wedge R]$

The RHS is the sum of the products form.

Hence RHS is the required PDNF of S

PDNF of $\neg S \Leftrightarrow (P \wedge \neg Q \wedge R) \vee (P \wedge \neg Q \wedge \neg R) \vee (\neg P \wedge Q \wedge \neg R)$
$\vee (\neg P \wedge \neg Q \wedge \neg R)$

PCNF of $S \equiv \neg(\text{PDNF of } \neg S)$

$$\equiv (\neg P \vee Q \vee \neg R) \wedge (\neg P \vee Q \vee R) \wedge (P \vee \neg Q \vee R) \wedge (P \vee Q \vee R).$$

3) obtain PDNF and PCNF of $(\neg P \to R) \wedge (Q \Leftrightarrow P)$.

Soln:

P	Q	R	$\neg P$	$\neg P \to R$	$Q \Leftrightarrow P$	$(\neg P \to R) \wedge (Q \Leftrightarrow P)$	Minterm	Maxterm
T	T	T	F	T	T	T	$P \wedge Q \wedge R$	
T	T	F	F	T	T	T	$P \wedge Q \wedge \neg R$	
T	F	T	F	T	F	F		$\neg P \vee Q \vee \neg R$
T	F	F	F	T	F	F		$\neg P \vee Q \vee R$
F	T	T	T	T	F	F		$P \vee \neg Q \vee \neg R$
F	T	F	T	F	F	F		$P \vee \neg Q \vee R$
F	F	T	T	T	T	T	$\neg P \wedge \neg Q \wedge R$	
F	F	F	T	F	T	F		$P \vee Q \vee R$

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

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

4) Find the PCNF and PDNF of $(P \wedge R) \vee (P \wedge \neg Q)$

Soln:

PDNF : $(P \wedge \neg Q \wedge \neg R) \vee (P \wedge \neg Q \wedge R) \vee (P \wedge Q \wedge R)$

PCNF : $(P \vee Q \vee R) \wedge (P \vee Q \vee \neg R) \wedge (P \vee \neg Q \vee R) \wedge (P \vee \neg Q \vee \neg R) \wedge (\neg P \vee \neg Q \vee R)$.

Rules Of Inference

Table of Logical Implications:

1) $(P \wedge Q) \Rightarrow P$; $(P \wedge Q) \Rightarrow Q$ (Simplification)
2) $P \Rightarrow (P \vee Q)$; $Q \Rightarrow (P \vee Q)$ (Addition)
3) $\neg P \Rightarrow P \rightarrow Q$ 4) $Q \Rightarrow P \rightarrow Q$ 5) $P, Q \Rightarrow P \wedge Q$
6) $\left.\begin{array}{l}\neg P,\ P \vee Q \Rightarrow Q \\ P \vee Q,\ \neg Q \Rightarrow P\end{array}\right\}$ (Disjunctive syllogism)
7) $P, P \rightarrow Q \Rightarrow Q$ [Modus ponens]
8) $P \rightarrow Q, \neg Q \Rightarrow \neg P$ [Modus Tollens]
9) $P \rightarrow Q, Q \rightarrow R \Rightarrow P \rightarrow R$ [Hypothetical syllogism].

Example: Direct proof:

1) Show that R is a valid inference from the premises $P \rightarrow Q$, $Q \rightarrow R$ and P.

Solution:

proof of Sequence

Steps	premises	Rule	Reason
(1)	$P \rightarrow Q$	P	Given premise
(2)	$Q \rightarrow R$	P	Given premise
(3)	$P \rightarrow R$	T Rule	(1), (2), $(P \rightarrow Q), (Q \rightarrow R) \Rightarrow P \rightarrow R$
(4)	P	P	Given premise
(5)	R	T	(3), (4). $P, P \rightarrow R \Rightarrow R$

Hence R is concluded from the given premises.

2) Show that $R \wedge (P \vee Q)$ is a valid conclusion from the premises $P \vee Q$, $Q \rightarrow R$, $P \rightarrow M$ and $\neg M$.

Soln: proof of sequence

Steps	premises	Rule	Reason
(1)	$P \rightarrow M$	P	Given premise
(2)	$\neg M$	P	Given premise
(3)	$\neg P$	T	(1), (2), $(P \rightarrow Q), \neg Q \Rightarrow \neg P$
(4)	$P \vee Q$	P	Given premise
(5)	Q	T	(3), (4) $(P \vee Q); \neg P \Rightarrow Q$
(6)	$Q \rightarrow R$	P	Given premise
(7)	R	T	(5), (6), $(P \rightarrow Q), P \Rightarrow Q$
(8)	$R \wedge (P \vee Q)$	T	(4), (7), $P, Q \Rightarrow P \wedge Q$

Hence we conclude $R \wedge (P \vee Q)$ from the given premises.

Indirect proof:

(3) Given an indirect proof of $(\neg P \wedge \neg Q) \Rightarrow \neg (P \wedge Q)$ (or)

Show that $\neg (P \wedge Q)$ follows from $\neg P \wedge \neg Q$.

Soln: The conclusion is $\neg (P \wedge Q)$. So we take $\neg(\neg (P \wedge Q))$ as a additional premise.

proof of sequence

steps	Premises.	Rule	Reason
(1)	$\neg(\neg(P \wedge Q))$	P	Negated Conclusion
(2)	$P \wedge Q$	T	(1), $\neg(\neg P) \Rightarrow P$
(3)	P	T	(2), $P \wedge Q \Rightarrow P$
(4)	$\neg P \wedge \neg Q$	P	Given premise
(5)	$\neg P$	T	(4), $P \wedge Q \Rightarrow P$

(6) $P \wedge \neg P \equiv F$ T   (3), (5). $P, Q \Rightarrow P \wedge Q$.

$\therefore \neg(P \wedge Q)$ follows from $\neg P \wedge \neg Q$.

Rule CP (or) Conditional proof:

1) Show that $R \to S$ can be derived from the premises $P \to (Q \to S)$, $\neg R \vee P$ and Q.

proof:

It is enough to prove $P \to (Q \to S)$, $\neg R \vee P$, Q, $R \Rightarrow S$.

proof of sequence:

Steps	premises	Rule	Reason
(1)	$\neg R \vee P$	P	Given premise
(2)	$R \to P$	T	(1), $P \to Q \Leftrightarrow \neg P \vee Q$.
(3)	R	P	Added premise
(4)	P	T	(2), (3), $P \to Q, P \Rightarrow Q$.
(5)	$P \to (Q \to S)$	P	Given premise
(6)	$Q \to S$	T	(5), (4), $P \to Q, P \Rightarrow Q$
(7)	Q	P	Given premise
(8)	S	T	(6), (7), $P \to Q, P \Rightarrow Q$
(9)	$R \to S$	CP	

Hence the proof.

2) Show that using C.P rule, $\neg P \vee Q$, $\neg Q \vee R$, $R \to S \Leftrightarrow P \to S$.

proof:

It is enough to prove $\neg P \vee Q$, $\neg Q \vee R$, $R \to S$, $P \Rightarrow S$.

proof of sequence

Steps	premises	Rule	Reason
(1)	$\neg P \vee Q$	P	Given premise
(2)	$P \to Q$	T	(1), $P \to Q \Leftrightarrow \neg P \vee Q$
(3)	P	P	Additional premise
(4)	Q	T	(2), (3), $P \to Q, P \Rightarrow Q$
(5)	$\neg Q \vee R$	P	Given premise
(6)	$Q \to R$	T	(5), $P \to Q \Leftrightarrow \neg P \vee Q$
(7)	R	T	(4), (6) $P \to Q, P \Rightarrow Q$
(8)	$R \to S$	P	Given premise
(9)	S	T	(7), (8), $P \to Q, P \Rightarrow Q$
(10)	$P \to S$	CP	

Inconsistency of premises:

A set of premises $H_1, H_2, \dots, H_n$ is said to be inconsistent if $H_1 \wedge H_2 \wedge \dots \wedge H_n \Rightarrow F$ where F stands for a contradiction.

Example:

Show that the following premises are inconsistent.

$P \to Q, \ P \to R, \ Q \to \neg R, \ P.$

Soln: To prove: $P \to Q, \ P \to R, \ Q \to \neg R, \ P \Rightarrow F$.

Steps	premises	Rule	Reason
1)	P	P	Given premise
(2)	$P \to Q$	P	Given premise
(3)	Q	T	(1), (2), $P \to Q, P \Rightarrow Q$
(4)	$Q \to \neg R$	P	Given premise
(5)	$\neg R$	T	(3), (4); $P \to Q, P \Rightarrow Q$

(6)	$P \rightarrow R$	P	Given premise
(7)	$\neg P$	T	(6), (5), $P \rightarrow Q, \neg Q \Rightarrow \neg P$
(8)	$P \wedge \neg P$	T	(1), (7), $P, Q \Rightarrow P \wedge Q$
(9)	F	T	

$\therefore$ The given premises are inconsistent.

1) Show that the following premises are inconsistent.

A diagnostic message is stored in a buffer or it is retransmitted. A diagonostic message is not stored in the buffer. If a diagnostic message is stored in a buffer then it is retransmitted. A diagnostic message is not retransmitted.

Soln: P: A diagnostic message is stored in buffer

Q: Message is retransmitted.

The given premises are $P \vee Q$, $\neg P$, $P \rightarrow Q$, $\neg Q$.

Steps	premises	Rule	Reason
(1)	$\neg P$	P	Given premise
(2)	$P \vee Q$	P	Given premise
(3)	Q	T	(1), (2), $P \vee Q; \neg P \Rightarrow Q$
(4)	$\neg Q$	P	Given premise
(5)	$Q \wedge \neg Q \Leftrightarrow F$	T	(3), (4), $P, Q \Rightarrow P \wedge Q$.

$\therefore$ The given premises are inconsistent.

2) Show that the premises are inconsistent.

$P \rightarrow Q, P \rightarrow R, Q \rightarrow \neg R, P$.

Predicates and Quantifiers.

Quantifiers:

1) Universal Quantification

(2) Existential Quantification

Universal Quantifier ($\forall$) replaces the phrase "for all".

Existential Quantifier ($\exists$) replaces the phrase "There exists".

"For all x, x is an integer" is written as $(\forall x) I(x)$ or $(x) I(x)$

"There exists an integer x which is prime" is written as $(\exists x) P(x)$

where $P(x)$: x is prime.

Example:

1) Write in symbolic form of "All lions are dangerous".

Soln: $P(x)$: x is a lion, $Q(x)$: x is dangerous.

Symbolic form: $(x)(P(x) \rightarrow Q(x))$

2) Write in symbolic form of "Some animals are dangerous".

Soln: $P(x)$: x is an animal, $Q(x)$: x is dangerous

Symbolic form: $(\exists x)(P(x) \wedge Q(x))$.

Negation of a Quantified statement:

1) $\neg((\forall x) P(x)) \Leftrightarrow (\exists x)(\neg P(x))$

2) $\neg[(\exists x) P(x)] \Leftrightarrow (\forall x)(\neg P(x))$

3) $\neg[(\forall x) \neg P(x)] \Leftrightarrow (\exists x)(P(x))$.

4) $\neg[(\exists x) \neg P(x)] \Leftrightarrow (\forall x)(P(x))$.

Example: Negate the statement "Every student in this class is intelligent"

Some student in this class is not intelligent.

Theory of Inference and valid arguments.

Universal specification: [US Rule]

$(\forall x)(p(x)) \Rightarrow p(y)$

Universal Generalization: [UG Rule]

$p(y) \Rightarrow (\forall x)\, p(x)$

Existential specification: [ES Rule]

$(\exists x)(p(x)) \Rightarrow p(y)$

Existential Generalization: [E.G Rule]

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

Examples:

1) Use predicate logic to prove $(\forall x)(p(x) \to Q(x)) \wedge (\forall x)\, p(x) \Rightarrow (\forall x)\, Q(x)$

Soln:

Steps	premises	Reason
(1)	$(\forall x)(p(x) \to Q(x))$	Rule P
(2)	$p(y) \to Q(y)$	Rule US, (1)
(3)	$(\forall x)\, p(x)$	Rule P
(4)	$p(y)$	Rule US, (3)
(5)	$Q(y)$	Rule T, (2), (4), $P \to Q, P \Rightarrow Q$
(6)	$(\forall x)\, Q(x)$	Rule UG, (5).

$\therefore$ The argument is valid.

2) Use predicate logic, prove the argument.

$(\forall x)(p(x) \wedge Q(x)) \Rightarrow (x)\, p(x) \wedge (x)\, Q(x)$.

Soln:

Steps	premises	Reason
(1)	$(\forall x)(p(x) \wedge Q(x))$	Rule P
(2)	$p(y) \wedge Q(y)$	Rule US, (1)

(3) $P(y)$ Rule T, (2), $P \wedge Q \Rightarrow P$

(4) $(x)\,P(x)$ Rule UG, (3)

(5) $Q(y)$ Rule T, (2), $P \wedge Q \rightarrow Q$.

(6) $(x)Q(x)$ Rule UG, (5)

(7) $(x)\,P(x) \wedge (x)\,Q(x)$ Rule T (4), (6), $P, Q \Rightarrow P \wedge Q$.

(3) Show that the premises, "A student in this class has not read the book and everyone in this class passed the first exam" imply the conclusion "Someone who passed the first exam has not read the book".

Soln: Let $P(x)$: x in this class

$Q(x)$: x has read the book

$R(x)$: x passed the first exam

Premises: $(\exists x)(P(x) \wedge \neg Q(x))$, $(x)(P(x) \rightarrow R(x))$

Conclusion: $(\exists x)(R(x) \wedge \neg Q(x))$.

proof of sequence

Steps	premises	Reason
(1)	$(\exists x)(P(x) \wedge \neg Q(x))$	Rule P.
(2)	$P(y) \wedge \neg Q(y)$.	Rule ES, (1)
(3)	$P(y)$	T, (2), $P \wedge Q \Rightarrow P$.
(4)	$(x)(P(x) \rightarrow R(x))$	Rule P
(5)	$P(y) \rightarrow R(y)$	Rule US, (4)
(6)	$R(y)$	T, (3), (5), $P \rightarrow Q$, $P \Rightarrow Q$
(7)	$\neg Q(y)$	T, (2), $P \wedge Q \Rightarrow Q$
(8)	$R(y) \wedge \neg Q(y)$	T (6), (7), $P, Q \Rightarrow P \wedge Q$
(9)	$(\exists x)(R(x) \wedge \neg Q(x))$	Rule EG, (8)

4) Use CP rule, prove $(\forall x)(P(x) \to Q(x)), (\forall x)(R(x) \to \neg Q(x)) \Rightarrow (\forall x)(R(x) \to \neg P(x))$.

Soln: proof of sequence

Steps	Premises	Reason
(1)	$(\forall x)(R(x) \to \neg Q(x))$	Rule P
(2)	$R(y) \to \neg Q(y)$	Rule US (1)
(3)	$Q(y) \to \neg R(y)$	Rule T, (2) $P \to Q \Leftrightarrow \neg Q \to \neg P$
(4)	$(\forall x)(P(x) \to Q(x))$	Rule P
(5)	$P(y) \to Q(y)$	Rule US (4)
(6)	$P(y) \to \neg R(y)$	Rule T, $P \to Q, Q \to R \Rightarrow P \to R$
(7)	$R(y) \to \neg P(y)$	Rule T, (6) $P \to Q \Leftrightarrow \neg Q \to \neg P$
(8)	$(\forall x)(R(x) \to \neg P(x))$	Rule UG, (7).

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

(6) Using CP rule, show that $(x)(P(x) \to Q(x)) \Rightarrow (x)P(x) \to (x)Q(x)$.

proof of sequence

Step's	Premises	Reason
(1)	$(x)(P(x) \to Q(x))$	Rule P
(2)	$P(y) \to Q(y)$	Rule US, (1)
(3)	$(x) \cdot P(x)$	Rule P
(4)	$P(y)$	Rule US (3)
(5)	$Q(y)$	Rule T, (2), (4) $P \to Q, P \Rightarrow Q$
(6)	$(x) Q(x)$	Rule UG, (5)
(7)	$(x) P(x) \to (x) Q(x)$	Rule CP, (3), (6).

(7) Prove that $(\exists x)(P(x) \wedge Q(x)) \Rightarrow (\exists x) P(x) \wedge (\exists x)(Q(x))$.

Negating nested Quantifiers:

1) Write the negation for each of the following.

1) $\forall x \exists y (x^2 < y)$

$\exists x \forall y (x^2 \geq y)$

2) $\exists y \forall x (x^2 < y)$

$\forall y \exists x (x^2 \geq y)$.

3) $\forall x \exists y (xy = 1)$

$\exists x \forall y (xy \neq 1)$..

Methods of proving theorem:

Direct proof:

It is a proof that the implication $p \to q$ is true that proceeds by showing that q must be true when p is true.

Example:

Give a direct proof of the theorem "If n is an odd integer then n^2 is an odd integer..

Soln: Suppose that n is odd. Then $n = 2K+1$

$n^2 = (2K+1)^2 = 4K^2+4K+1 = 2(2K^2+2K)+1 = 2m+1, m = 2K^2+2K$

$\therefore n^2$ is an odd integer.

Indirect proof:

The implication $p \to q$ can be proved by showing that its contrapositive $\neg q \to \neg p$ is true.

Example:

Give an indirect proof of the theorem "If $3n+2$ is odd then n is odd.

Soln: Assume n is even

Then $n = 2K$ for some integer K.

$3n+2 = 3(2K)+2 = 6K+2 = 2(3K+1) =$ even integer.

$\therefore$ If $3n+2$ is odd then n is odd.

proof by contradiction:

1) prove that $\sqrt{2}$ is irrational by giving a proof by contradiction

soln:

Suppose that $\sqrt{2}$ is rational

So $\sqrt{2} = a/b$ where a and b have no common factors.

$\sqrt{2} = a/b \Rightarrow 2 = a^2/b^2$. Hence $2b^2 = a^2$

This means that a^2 is even implies a is even. Hence $a = 2c$ for some integer c. $\therefore 2b^2 = 4c^2 \Rightarrow b^2 = 2c^2$

This means that b^2 is even and hence b is even.

Thus $\sqrt{2} = a/b$ where a and b have no common factors and 2 divides a and b. This is a contradiction.

Hence $\sqrt{2}$ is irrational.

proof by cases:

Show that the following statements are equivalent.

(i) n is an even integer (ii) $n-1$ is an odd integer (iii) n^2 is an even integer.

case (1): (i) $\Rightarrow$ (ii)

Assume n is even. $\therefore n = 2K$ for some integer K.

$\therefore n-1 = 2K-1 = 2K-2+1 = 2(K-1)+1 = 2m+1$ where m is an integer. This means that $n-1$ is odd.

case (2): (ii) $\Rightarrow$ (iii)

Suppose that $n-1$ is odd. Then $n-1 = 2K+1$ for some integer K.

Hence $n = 2K+2$, $n^2 = (2K+2)^2 = 4K^2+8K+4 = 2(2K^2+4K+2)$

This means that n^2 is even.

case (3) (iii) $\Rightarrow$ (i)

We prove this by giving an indirect proof.

Suppose that n is odd. Then $n = 2K+1$ where K is an integer.

$\therefore n^2 = (2K+1)^2 = 4K^2+4K+1 = 2(2K^2+2K)+1$

$\therefore n^2$ is an odd integer.

$\therefore$ If n^2 is an even integer then n is an even integer.

UNIT – II

2) Combinatorics

Principle of Mathematical Induction:

The statement $p(n)$ is true for all natural numbers if

1) $p(1)$ is true (Basis step)

2) For any integer K, $p(K)$ is true implies $p(K+1)$

ie) If $p(K)$ is true, then $p(K+1)$ is true (Induction step)

Example:

1) prove that $1+2+2^2+\cdots+2^n = 2^{n+1}-1$ for $n \geq 1$

Soln: $p(1) = 1+2 = 2^2-1$

$3 = 3$

$\therefore p(1)$ is true.

Assume $p(K)$ is true

ie) $1+2+2^2+\cdots+2^K = 2^{K+1}-1$

Consider $p(K+1)$

$1+2+2^2+\cdots+2^K+2^{K+1} = 2^{K+1}-1+2^{K+1}$

$= 2 \cdot 2^{K+1}-1$

$= 2^{K+2}-1 = 2^{(K+1)+1}-1$

$\therefore p(K+1)$ is true.

ie) $p(K) \Rightarrow p(K+1)$

$\therefore$ By mathematical induction, $1+2+2^2+\cdots+2^K = 2^{K+1}-1$.

2) prove by induction $1+2+3+\cdots+n = \frac{n(n+1)}{2}$

Soln: Let $p(n)$: $1+2+3+\cdots+n = \frac{n(n+1)}{2}$

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

$1 = 1$, which is true

$\therefore p(1)$ is true.

Assume $p(K)$ is true

ie) $1+2+3+\cdots+K = \frac{K(K+1)}{2}$

Consider $p(K+1)$

$$1+2+3+\cdots+k+(k+1) = 1+2+3+\cdots+k+(k+1)$$

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

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

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

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

$\therefore$ $p(k+1)$ is true.

$\therefore$ By induction, $1+2+\cdots+n = \frac{n(n+1)}{2}$.

3) prove by induction, $1^2+2^2+3^2+\cdots+n^2 = \frac{n(n+1)(2n+1)}{6}$.

Soln:

Let $p(n): 1^2+2^2+3^2+\cdots+n^2 = \frac{n(n+1)(2n+1)}{6}$

$p(1): 1 = \frac{1(1+1)(2+1)}{6} = \frac{(1)(2)(3)}{6} = 1$, which is true.

$\therefore$ $p(1)$ is true.

Assume $p(k)$ is true.

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

consider $p(k+1)$

$$1^2+2^2+3^2+\cdots+(k+1)^2 = 1^2+2^2+\cdots+k^2+(k+1)^2$$

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

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

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

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

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

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

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

$\therefore$ $P(k+1)$ is true.

ie) $p(K) \Rightarrow p(K+1)$

$\therefore$ By induction, $1^2+2^2+3^2+\dots+n^2 = \frac{n(n+1)(2n+1)}{6}$.

4) prove that n^3-n is divisible by 3 for $n \geq 1$.

Let $p(n)$ be n^3-n is divisible by 3

$p(1) = 1^3-1 = 1-1 = 0$, which is divisible by 3.

$\therefore$ $p(1)$ is true.

Assume $p(K)$ is true.

ie) K^3-K is divisible by 3.

$\therefore K^3-K = 3m$ for some integer m.

Consider $p(K+1)$

$$(K+1)^3-(K+1) = K^3+3K^2+3K+1-(K+1)$$
$$= K^3+3K^2+3K+1-K-1$$
$$= (K^3-K)+3(K^2+K),$$
$$= 3m+3(K^2+K), \text{ which is divisible by 3.}$$

$\therefore$ $p(K+1)$ is true.

$\therefore$ By induction, n^3-n is divisible by 3 for $n \geq 1$.

Strong induction and well ordering property:

Example:

Show that if n is an integer greater than 1, then n can be written as the product of primes.

Soln: Let $p(n)$ be the proposition that n can be written as the product of primes.

Basis Step:

$p(2)$ is true since 2 can be written as the product of one prime.

Induction step:

Assume that $p(j)$ ~~for~~ is true for all integers j with $j \leq K$.

Consider $p(K+1)$

The integer $K+1$ is prime or composite

If $K+1$ is prime, we immediately see that $p(K+1)$ is true.

If $K+1$ is composite then $K+1 = ab$ with $2 \le a \le b \le K$.

By induction hypothesis, both a and b can be written as the product of primes. Thus if $K+1$ is composite, it can be written as the product of primes namely, those primes in the factorization of a and those in the factorization of b.

Well ordering property:

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

Basics of Counting

The two basic counting principles are

(1) product Rule and (2) Sum rule.

Product Rule:

If there are n_1 ways to do the first task and n_2 ways to do the second task after the first task has been done, then there are $n_1 n_2$ ways to do both the tasks.

Example:

There are 32 microcomputers in a computer center. Each microcomputer has 24 ports. How many different ports to a microcomputer in the center are there?

Soln: The procedure of choosing a port consists of two tasks.

Task 1: picking a microcomputer

Task 2: picking a port on this microcomputer.

There are 32 ways to choose the microcomputer and

24 ways to choose the port

∴ By product rule there are $(32)(24) = 768$ ports.

2) How many different bit strings are there of length seven?

Soln:

Each of the seven bits can be chosen in two ways since each bit is either 0 or 1.

By product rule, there are $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^7 = 128$ different bit strings of length seven.

3) How many different 8 bit - strings are there that begin and end with 1?

Soln: 1 x x x x x x 1

Each bit marked x can be selected in 2 ways.

∴ The total number of 8-bit string that begin and end with 1 $= 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^6 = 64$.

4) How many three letter words can be constructed with English alphabet (i) When repetition of alphabets is allowed?
(ii) When repetition is not allowed?

Soln: I II III

i) The alphabet for I place can be selected in 26 ways.
The second place can be selected in 26 ways.
The third place can be selected in 26 ways.
There are $26 \times 26 \times 26 = 17576$ three letter words.

ii) The no of ways of choosing first letter = 26
The no of ways of choosing second letter = 25
The no of ways of choosing third letter = 24.
Hence there are $26 \times 25 \times 24 = 15600$ three letter words.

Sum Rule:

If a first task can be done in n_1 ways and a second task in n_2 ways and if these tasks cannot be done at the same time, there are $n_1 + n_2$ ways to do one of these tasks.

Example:

A student can choose the computer project from one of the three tasks. The three tasks contain 23, 15 and 19 possible projects respectively. How many projects possible are there to choose from?

Soln:

The student can choose a project from the first list in 23 ways, second list in 15 ways and from the third list in 19 ways. Hence there are $23+15+19 = 57$ projects to choose them.

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.

Generalized pigeonhole principle:

If N objects are placed into K boxes, then there is atleast one box containing $\lceil N/K \rceil$ objects. $\lceil N/K \rceil$ is the smallest integer greater than or equal to $\frac{N}{K}$. ie) $\left\lceil \frac{38}{9} \right\rceil = 5$.

1) What is the minimum number of students required in a class to be sure that atleast six will receive the same grade, if there are five possible grades A, B, C, D and F?

Soln:

No of pigeonholes n = possible grades = 5, since atleast six students to receive the same grade $K+1 = 6 \Rightarrow K = 5$

Now $N = n.K+1 = 5.5+1 = 26$.

Thus 26 is the minimum number of students needed to ensure that atleast six students will receive the same grade.

2) How many cards must be selected from a standard deck of 52 cards guarantee that atleast three cards of the same suit are chosen?

Soln:

Suppose that there are four boxes.

Using the generalised pigeonhole principle, we see that if N cards are selected, there is atleast one box containing atleast $\lceil N/K \rceil$ cards.

$\therefore K+1 = 3 \Rightarrow K = 2$ N = no of suits.

The smallest N such that $\left\lceil \frac{N}{4} \right\rceil \geq 3$ is $N = nK+1 = 2 \cdot 4+1 = 9$.

Permutation and Combination:

Permutation:

A permutation is an arrangement of a number of objects in a definite order, taken some or all at a time.

For example, the permutation of the letters x, y, z taken two at a time are xy, yz, xz, zx, yx, zy.

The number of permutations of 'n' different things taken 'r' at a time is denoted by ^nP_r or $P(n, r)$.

Formula for $P(n,r)$: $P(n,r) = \frac{n!}{(n-r)!}$

Note: $P(n, n) = n!$

$P(n, 0) = 1$

Example:

1) How many different ways can the letters of the word HEXAGON be permuted?

Soln: The word HEXAGON has 7 different letters, which can be arranged among themselves in $P(7, 7) = 7! = 5040$ ways

2) How many different 5 letter words can be formed out of the letters of the word DELHI? How many of these will begin with D and with I?

Soln: The word DELHI has 5 different letters which can be arranged among themselves in $P(5,5) = 5! = 120$ ways.

For the words beginning with D and ending with I, (D x x x I), we have to arrange the remaining three letters E, L, H in the three places marked x. This can be done in $P(3, 3) = 3! = 6$ ways.

Permutation of like objects:

1) In how many different ways can the letters of the word "ALLAHABAD" be permuted?

Soln:

The word "ALLAHABAD" has 9 letters in all. The letter A appears 4 times, the letter L appears 2 times and the remaining three letters H, B, D appear once.

∴ The required number of permutations $= \dfrac{9!}{4!\,2!\,1!\,1!\,1!}$

$$= \frac{9 \times 8 \times 7 \times 6 \times 5 \times 4!}{4!\,2!} = 7560$$

2) How many bit string of length 7 can be formed?

Soln:

No of bit strings of length $7 = 2\times2\times2\times2\times2\times2\times2 = 2^7$

3) How many bit string of length 10 that begin and end with 1?

Soln:

The bits in the remaining 8 places can be filled in 2^8 ways after fixing 1 in the first and last places.

$\therefore$ No of bit strings of length 10, start and end with 1

$= 2^8 = 256.$

3) How many bit strings of length 10 contain (a) exactly four 1's (b) atmost four 1's (c) atleast four 1's (d) an equal number of 0's and 1's.

Soln:

(a) A bit string of length 10 can be considered to have 10 positions. These 10 positions should be filled with four 1's and six 0's.

No of required bit strings $= \frac{10!}{4!\,6!} = 210.$

(b) The 10 positions should be filled up with no 1 and ten 0's (or) one 1 and 9 0's (or) two 1's and eight 0's (or) three 1's and seven 0's (or) four 1's and six 0's.

Required no of bit strings

$= \frac{10!}{0!\,10!} + \frac{10!}{1!\,9!} + \frac{10!}{2!\,8!} + \frac{10!}{3!\,7!} + \frac{10!}{4!\,6!}$

$= 386$

(c) The ten positions are to be filled up with 4 1's and 6 0's (or) 5 1's and 5 0's etc ... or ten 1's and no 0's.

$= \frac{10!}{4!\,6!} + \frac{10!}{5!\,5!} + \frac{10!}{6!\,4!} + \frac{10!}{7!\,3!} + \frac{10!}{8!\,2!} + \frac{10!}{9!\,1!} + \frac{10!}{10!\,0!}$

$= 848.$

(d) The ten positions are to be filled up with five 1's and five 0's $= \frac{10!}{5!\,5!} = 252$.

Combination:

A combination is a selection of some or all of a number of different objects.

For example, the combination of three letters a, b, c taken three at a time is {a,b,c}

Formula for nC_r (or) $C(n,r) = \frac{n!}{(n-r)!\,r!}$

Example:

1) A committee of 5 is to be selected from 6 boys and 5 girls. Determine the number of ways of selecting the committee if it is to consist of atleast 1 boy and 1 girl.

Soln: The committee may consist of

(i) 1 boy, 4 girls

(ii) 2 boys, 3 girls

(iii) 3 boys, 2 girls

(iv) 4 boys, 1 girl.

The number of committees of type (i) $= 6C_1 \times 5C_4 = 6 \times 5 = 30$.

The number of committees of type (ii) $= 6C_2 \times 5C_3 = 15 \times 10 = 150$.

The number of committees of type (iii) $= 6C_3 \times 5C_2 = 20 \times 10 = 200$

The number of committees of type (iv) $= 6C_4 \times 5C_1 = 15 \times 5 = 75$

$\therefore$ The total number of ways of forming the committee $= 30 + 150 + 200 + 75 = 455$.

2) From a club consisting of 6 men and 7 women, in how many ways can we select a committee of (a) 3 men and 4 women? (b) 4 persons which has atleast one woman?

(c) 4 persons that has atmost one man? (d) 4 persons that has persons of both sexes (e) 4 persons so that two specific members are not included!

soln:

(a) 3 men can be selected from 6 men in $6C_3$ ways, 4 women can be selected from 7 women in $7C_4$ ways.

∴ The committee of 3 men and 4 women can be selected in $6C_3 \times 7C_4$ ways $= \frac{6!}{3!\,3!} \times \frac{7!}{4!\,3!} = 700$ ways.

(b) For the committee to have atleast one woman, we have to select 3 men and 1 woman or 2 men and 2 women or 1 man and 3 women or no man and 4 women. This selection can be done in $[6C_3 \times 7C_1] + [6C_2 \times 7C_2] + [6C_1 \times 7C_3] + [6C_0 \times 7C_4]$

$= (20 \times 7) + (15 \times 21) + (6 \times 35) + (1 \times 35) = 140 + 315 + 210 + 35$

$= 700$ ways.

(c) For the committee to have atmost one man, we have to select no man and 4 women (or) 1 man and 3 women. This selection can be done in $[6C_0 \times 7C_4] + [6C_1 \times 7C_3]$

$= [1 \times 35] + [6 \times 35] = 245$ ways.

(d) For the committee to have persons of both sexes. the selection must include 1 man and 3 women or 2 men and 2 women or 3 men and 1 women. This selection can be done in

$[6C_1 \times 7C_3] + [6C_2 \times 7C_2] + [6C_3 \times 7C_1] = (6 \times 35) + (15 \times 21) \times (20 \times 7)$

$= 210 + 315 + 140 = 665$ ways.

(e) After removing the two specific members, 2 members can be selected from the remaining in $11C_2$ ways. In each of these selection, if we include the removed two specific members, we get $11C_2$ selections containing the 2 specific members.

∴ The no of selections not including these 2 members

$= 13C_4 - 11C_2 = 715 - 55 = 660.$

3) There are 6 white marbles and 5 black marbles in a bag. Find the number of ways of drawing 4 marbles from the bag if (i) they can be of any colour (ii) 2 must be white and 2 must be black (iii) they must all be of the same colour.

Soln: Total no of marbles in the bag $= 6+5 = 11$.

(i) No of ways of drawing 4 marbles of any colour $= 11C_4$

$$= \frac{11 \times 10 \times 9 \times 8}{1 \times 2 \times 3 \times 4} = 330.$$

(ii) No of ways of drawing 2 white and 2 black marbles

$= 6C_2 \times 5C_2 = 15 \times 10 = 150.$

(iii) No of ways of drawing 4 black marbles $= 5C_4 = 5$

No of ways of drawing 4 white marbles $= 6C_4 = 15$

No of ways of drawing 4 marbles of the same colour

$= 5 + 15 = 20.$

$S(K+2) + S(K+1)\ S(K)$

$S(K) - S(K-1)\ S(K-2)$

Recurrence Relation.

Formation of Reccurence Relation

1) Form the reccurence relation from $S(K) = 5 \cdot 2^K, K > 0$.

$S(K-1) = 5 \cdot 2^{K-1}$

Soln:

$= 5 \cdot 2^K \cdot 2^{-1}$

If $K > 1$, $S(K) = 5 \cdot 2^K = 2 \cdot 5 \cdot 2^{K-1} = 2S(K-1)$

$= \frac{S(K)}{2}$

∴ The reccurence relation is $S(K) - 2S(K-1) = 0$ and the initial condition $S(0) = 5$.

$2S(K-1) = S(K)$

2) Find the reccurence relation for the Fibonacci sequence of numbers.

Soln: The sequence of numbers 0, 1, 1, 2, 3, 5, 8, 13, ... is the Fibonacci sequence of numbers.

If F_n is the n^{th} term, then $F_n = F_{n-1} + F_{n-2}, n \geq 2$.

∴ The reccurence relation is $F_n - F_{n-1} - F_{n-2} = 0, n \geq 2$ with initial conditions $F_0 = 0, F_1 = 1$.

3) Find the reccurence relation from $S(K) = 2K+9$.

Ans: The reccurence relation is $S(K) - S(K-1) = 2$.

4) Find the reccurence relation from $y_n = A \cdot 2^n + B \cdot 3^n$.

Soln: $y_n = A \cdot 2^n + B \cdot 3^n$

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

$y_{n+2} = 4 \cdot A \cdot 2^n + 9 \cdot B \cdot 3^n$

$y_{n+1} - 2y_n = B \cdot 3^n, \quad y_{n+2} - 2y_{n+1} = 3 \cdot B \cdot 3^n$

$y_{n+2} - 2y_{n+1} = 3(y_{n+1} - 2y_n)$

$\therefore y_{n+2} - 5y_{n+1} + 6y_n = 0$ is the required reccurence relation.

Reccurence Relation:

Solution of Reccurence Relation:

Consider the reccurence relation $C_0 y_{n+2} + C_1 y_{n+1} + C_2 y_n = f(n)$.
The solution of the above reccurence relation is $y_n = H.S + P.S$
where $H.S$ = Homogeneous solution, $P.S$ = particular Solution.

Rules to find H.S:

1) First write the characteristic equation $C_0 x^2 + C_1 x + C_2 = 0$.
2) Solve the ch equation and get the roots.
3) If α_1 and α_2 are the roots of the ch equation, then
   i) $H.S = A_1 \alpha_1^n + A_2 \alpha_2^n$ if α_1, α_2 are distinct
   2) $H.S = (A_1 + nA_2)\alpha^n$ if $\alpha_1 = \alpha_2 = \alpha$
   3) $H.S = A_1(\alpha_1 + i\beta)^n + A_2(\alpha - i\beta)^n$ if $\alpha_1 = \alpha + i\beta$, $\alpha_2 = \alpha - i\beta$.

Rules to find P.S

Form of $f(n)$	General form to be assumed
K, a constant	A
K^n, where K is a constant	$A \cdot K^n$
$f(n) = K^n$	AnK^n if K is a root of characteristic equation.

$f(n) = K^n$	An^2K^n if K is a double root of characteristic equation
$f(n)$, a polynomial in n of degree 'r'	$A_0n^r + A_1n^{r-1} + \dots + A_n$
$K^n f(n)$ where $f(n)$ is a polynomial of degree $= r$ in 'n'. and K is a constant	$[A_0n^r + A_1n^{r-1} + \dots + A_n]K^n$.

1) Solve the reccurence relation $y_n - 7y_{n-1} + 10y_{n-2} = 0$ satisfying the conditions $y_0 = 6$ and $y_1 = 6$.

Soln: The characteristic equation is $x^2 - 7x + 10 = 0$

$(x-5)(x-2) = 0$

$\Rightarrow x = 2, 5$.

$\therefore$ The Homogeneous solution H.S is given by

$H.S = A_1 2^n + A_2 5^n$

$y_n^{(H)} = A_1 2^n + A_2 5^n$.

Since the R.H.S is zero, the particular solution $y_n^{(P)} = 0$

$\therefore$ The solution is $y_n = A_1 2^n + A_2 5^n$

$y_0 \Rightarrow 6 \Rightarrow A_1 + A_2 = 6$

$y_1 = 6 \Rightarrow 2A_1 + 5A_2 = 6$

Solving $A_2 = -2$ and $A_1 = +8$

$\therefore y_n = (+8)2^n + (-2)(5^n)$.

2) Solve the reccurence relation $y_{n+2} - 5y_{n+1} + 6y_n = 5^n$ Subject to the conditions $y_0 = 0$ and $y_1 = 2$.

Soln: The characteristic equation is $x^2 - 5x + 6 = 0$

$(x-2)(x-3) = 0 \Rightarrow x = 2, 3$

$\therefore$ The H.S is $y_n^{(H)} = c_1 2^n + c_2 3^n$.

Assume the particular solution as $y_n^{(P)} = A \cdot 5^n$

Put $y_n = A \cdot 5^n$ in the given reccurence relation,

$$A \cdot 5^{n+2} - 5 \cdot A \cdot 5^{n+1} + 6 A 5^n = 5^n$$

$$6A5^n = 5^n \Rightarrow 6A = 1 \Rightarrow A = 1/6.$$

$\therefore$ The particular solution is $y_n^{(P)} = 1/6 \, (5^n)$.

$\therefore y_n = c_1 2^n + c_2 3^n + 5^n/6 \rightarrow (1)$

$y_0 = 0 \Rightarrow c_1 + c_2 = -1/6$

$y_1 = 2 \Rightarrow 2c_1 + 3c_2 = 7/6$

Solving $c_2 = 3/2$ and $c_1 = -5/3$

Hence $y_n = 3/2 (3^n) - 5/3 (2^n) + 5^n/6$ is the solution.

3) Find the reccurrence relation for the Fibonacci sequence of the numbers and obtain its solution.

Soln: The Fibonacci sequence of number is $\{0, 1, 1, 2, 3, \ldots\}$

The reccurrence relation is $F_n - F_{n-1} - F_{n-2} = 0$ satisfying the initial conditions $F_0 = 0$ and $F_1 = 1$.

The characteristic equation is $x^2 - x - 1 = 0$

Solving $x = \dfrac{1 \pm \sqrt{5}}{2}$

$\therefore$ The roots are $\dfrac{1+\sqrt{5}}{2}, \dfrac{1-\sqrt{5}}{2}$

Hence the solution is given by $F_n = c_1\left(\dfrac{1+\sqrt{5}}{2}\right)^n + c_2\left(\dfrac{1-\sqrt{5}}{2}\right)^n$

$F_0 = 1 \Rightarrow c_1 + c_2 = 0$ and

$F_1 = 1 \Rightarrow c_1\left(\dfrac{1+\sqrt{5}}{2}\right) + c_2\left(\dfrac{1-\sqrt{5}}{2}\right) = 1$

$c_1\left[\dfrac{1+\sqrt{5}}{2} - \dfrac{1-\sqrt{5}}{2}\right] = 1 \Rightarrow c_1\left[\dfrac{2\sqrt{5}}{2}\right] = 1$

$\Rightarrow c_1(\sqrt{5}) = 1 \Rightarrow c_1 = \dfrac{1}{\sqrt{5}}$

$c_2 = -c_1 \Rightarrow c_2 = \dfrac{-1}{\sqrt{5}}$

$\therefore$ The solution is given by $F_n = \dfrac{1}{\sqrt{5}}\left(\dfrac{1+\sqrt{5}}{2}\right)^n + \dfrac{-1}{\sqrt{5}}\left(\dfrac{1-\sqrt{5}}{2}\right)^n$

4) Solve the reccurrence relation $y_{n+2} - 6y_{n+1} + 8y_n = 3n+5$.

Solution :

The characteristic equation is $x^2 - 6x + 8 = 0$

$$(x-4)(x-2) = 0 \Rightarrow x = 2, 4.$$

H.S $y_n^{(H)} = c_1 2^n + c_2 4^n$

Assume the particular solution $y_n^{(P)} = A + Bn$

put $y_n = A + Bn$ in the given reccurrence relation

$$A + B(n+2) - 6A - 6B(n+1) + 8A + 8Bn = 3n+5$$

$$(3A - 4B) + 3Bn = 3n+5$$

Solving $A = 3$ and $B = 1$

$\therefore y_n^{(P)} = n+3$

The solution is given by $y_n = y_n^{(H)} + y_n^{(P)}$

$$y_n = c_1 \cdot 2^n + c_2 4^n + n + 3.$$

5) Solve the recurrence relation $y_K - y_{K-1} - 6y_{K-2} = -30$ given that $y_0 = 20$ and $y_1 = -5$.

Solution: The characteristic equation is $x^2 - x - 6 = 0$

$$\Rightarrow (x-3)(x+2) = 0 \Rightarrow x = 3, -2$$

The homogeneous solution is $y_K^{(H)} = c_1 3^K + c_2(-2)^K$

Assume the particular solution is $y_K^{P} = A$.

put $y_K = A$ in the given relation,

$$A - A - 6A = -30 \Rightarrow -6A = -30 \Rightarrow A = 5$$

$\therefore$ The solution is $y_K = c_1 3^K + c_2(-2)^K + 5$

$y_0 = 20 \Rightarrow c_1 + c_2 = 15$

$y_1 = -5 \Rightarrow 3c_1 - 2c_2 = -10$

Solving, $c_1 = 4$ and $c_2 = 11$

The solution is given by $y_K = c_1(3^K) + c_2(-2)^K + 5$

ie) $y_K = 4(3^K) + 11(-2)^K + 5.$

6) Solve the reccurrence relation $y_{n+1} - 5y_n = 5^n$ satisfying the initial condition $y_0 = 3$.

Solution:

The ch equation is $x - 5 = 0 \Rightarrow x = 5$

The homogeneous solution is $y_n^{(H)} = c_1 5^n$

Assume the particular solution $y_n^{(P)} = An5^n$

Put $y_n = An5^n$ in the given recurrence relation

$$A(n+1)5^{n+1} - 5An5^n = 5^n$$

$$5A5^n = 5^n$$

$\therefore 5A = 1 \Rightarrow A = 1/5$

$\therefore$ The particular solution is $y_n^{(P)} = \frac{n5^n}{5}$

$\therefore$ The solution is given by $y_n = c_1 5^n + n/5\, 5^n$

$$\therefore y_n = (c_1 + n/5)5^n$$

Using $y_0 = 3$, $c_1 = 3$

$\therefore y_n = (3 + n/5)5^n$ is the solution.

Solution of Recurrence Relation using Generating Function:

Generating function:

Let $a_0, a_1, a_2, \ldots$ be a sequence of real numbers. The function $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots = \sum_{n=0}^{\infty} a_n x^n$ is called the generating function for the given sequence.

Some useful expansions:

(1) $(1-x)^{-1} = \sum_{n=0}^{\infty} x^n$ (2) $\sum_{n=0}^{\infty} (-1)^n x^n = (1+x)^{-1}$

(3) $\sum_{n=0}^{\infty} a^n x^n = (1-ax)^{-1}$ (4) $\sum_{n=0}^{\infty} (-1)^n a^n x^n = (1+ax)^{-1}$

(5) $\sum_{n=0}^{\infty} (n+1)x^n = (1-x)^{-2}$ (6) $\sum_{n=0}^{\infty} \frac{(n+1)(n+1)}{2} x^n = (1-x)^{-3}$

Example 1:

1) Solve the recurrence relation $a_{n+2} - 3a_{n+1} + 2a_n = 0$ by the method of generating functions with the initial condition $a_0 = 2$ and $a_1 = 3$.

Solution:

Given the relation $a_{n+2} - 3a_{n+1} + 2a_n = 0 \rightarrow (1)$

Assume that $G(x) = \sum_{n=0}^{\infty} a_n x^n$.

Multiply the eqn (1) by x^n and summing from $n=0$ to $n=\infty$, we have

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

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

$$\frac{G(x) - a_0 - a_1 x}{x^2} - \frac{3[G(x) - a_0]}{x} + 2G(x) = 0$$

$$\frac{G(x) - 2 - 3x}{x^2} - \frac{3}{x}[G(x) - 2] + 2G(x) = 0$$

$$G(x) - 2 - 3x - 3x(G(x) - 2) + 2x^2 G(x) = 0$$

$$\therefore G(x)[1 - 3x + 2x^2] = 2 - 3x$$

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

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

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

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

Put $x = 1$, $2 - 3 = A(-1)$

$\Rightarrow A = 1$

Put $x = 1/2 = 2 - 3(1/2) = B(1 - 1/2)$

$\Rightarrow B = 1$

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

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

$$= \sum_{n=0}^{\infty} 1^n x^n + \sum_{n=0}^{\infty} 2^n x^n$$

$$= \sum_{n=0}^{\infty} (1^n + 2^n) x^n .$$

2) Solve the recurrence relation $a_n - 7a_{n-1} + 10a_{n-2} = 0$ by the method of generating functions with the initial conditions $a_0 = a_1 = 3$.

Solution:

Given: $a_n - 7a_{n-1} + 10a_{n-2} = 0$, $n \geq 2$ and $a_0 = a_1 = 3 \rightarrow ①$

Multiply ① by x^n and summing from $n=2$ to ∞, we have

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

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

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

$$G(x) - 3 - 3x - 7x[G(x) - 3] + 10x^2 G(x) = 0$$

$$G(x)[1 - 7x + 10x^2] = 3 + 3x - 21x$$

$$(1-2x)(1-5x)\,G(x) = 3 - 18x$$

$$G(x) = \frac{3-18x}{(1-2x)(1-5x)} \rightarrow ②$$

Let $\frac{3-18x}{(1-2x)(1-5x)} = \frac{A}{1-2x} + \frac{B}{1-5x}$

$$3 - 18x = A(1-5x) + B(1-2x)$$

put $x = 1/2$, $-3/2\, A = -6$

$\therefore A = 4$

put $x = 1/5$, $3/5\, B = -3/5 \Rightarrow B = -1$

$$\frac{3-18x}{(1-2x)(1-5x)} = \frac{4}{1-2x} - \frac{1}{1-5x}$$

From (2), $G(x) = 4(1-2x)^{-1} - (1-5x)^{-1}$

$$\sum_{n=0}^{\infty} a_n x^n = 4 \sum_{n=0}^{\infty} 2^n x^n - \sum_{n=0}^{\infty} 5^n x^n$$

$$= \sum_{n=0}^{\infty} \left[4(2)^n - 5^n\right] x^n .$$

Principle of Inclusion and Exclusion

1) If A and B are two sets, then the number of elements in their union set $(A \cup B)$ is given by

$$|A \cup B| = |A| + |B| - |A \cap B| \quad \text{(or)}$$

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

2) If A, B, C are any three sets then,

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |A \cap C| + |A \cap B \cap C| \quad \text{(or)}$$

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

$$n(\bar{A} \cap \bar{B} \cap \bar{C}) = N - n(A \cup B \cup C)$$

1) A total of 1232 students 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.

Soln:

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

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

Let c be the students who have taken a course in Hindi.

Then $|A| = 1232$, $|B| = 879$, $|c| = 114$

$|A \cap B| = 103$, $|A \cap c| = 23$, $|B \cap c| = 14$, $|A \cup B \cup c| = 2092$

By the principle of Inclusion - Exclusion, we have

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

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

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

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

2) 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.

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

$$|B| = \left[\frac{250}{2}\right] = 83$$

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

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

Now The number of integer between 1 - 250 that are divisible by 2 & 3 - $|A \cap B| = \left[\frac{250}{2 \times 3}\right] = 41$.

$|A \cap C| = \left[\frac{250}{2 \times 5}\right] = 25$

$|B \cap C| = \left[\frac{250}{3 \times 5}\right] = 16$

$|A \cap D| = \left[\frac{250}{2 \times 7}\right] = 17$

$|B \cap D| = \left[\frac{250}{3 \times 7}\right] = 11$

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

The number of integer divisible by 2, 3 and 5,

$|A \cap B \cap C| = \left[\frac{250}{2 \times 3 \times 5}\right] = 8$.

Similarly, $|A \cap B \cap D| = \left[\frac{250}{2 \times 3 \times 7}\right] = 5$.

$|A \cap C \cap D| = \left[\frac{250}{2 \times 5 \times 7}\right] = 3$

$|B \cap C \cap D| = \left[\frac{250}{3 \times 5 \times 7}\right] = 2$.

$|A \cap B \cap C \cap D| = \left[\frac{250}{2 \times 3 \times 5 \times 7}\right] = 1$

The number of integers between 1 - 250 that are divisible by 2, 3, 5 and 7 is $|A \cup B \cup C \cup D|$.

By the principle of Inclusion - 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 $= \text{Total} - |A \cup B \cup C \cup D|$

$= 250 - 193$

$= 57.$

UNIT - 3

Graphs

Definition:

A graph $G = (V(G), E(G))$ consists of V, a non empty set of vertices and E, a set of edges.

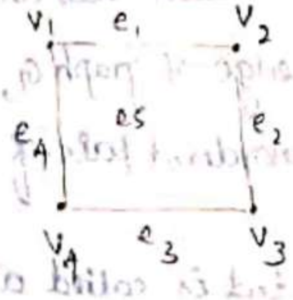
(ie) A graph G is an ordered triple $(V(G), E(G), \phi)$ consists of a non-empty set V called the set of vertices of the graph G, E is said to be the set of edges of the graph G, and ϕ is a mapping from the set of edges E to a set of order or unordered pairs of elements of V.

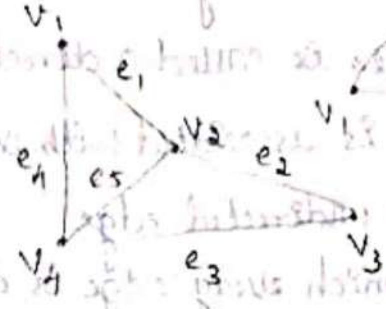
Example:

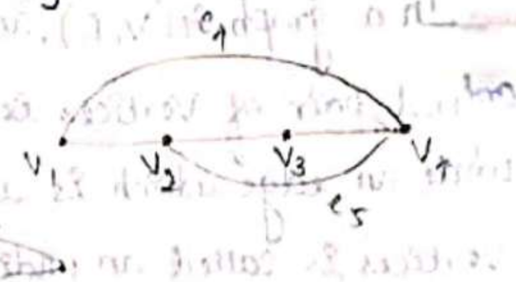
Let $G = (V(G), E(G), \phi)$ where $V(G) = \{v_1, v_2, v_3, v_4\}$ and $E(G) = \{e_1, e_2, e_3, e_4, e_5\}$ and ϕ is defined by

$\phi(e_1) = \{v_1, v_2\}$, $\phi(e_2) = \{v_2, v_3\}$, $\phi(e_3) = \{v_3, v_4\}$,

$\phi(e_4) = \{v_4, v_1\}$, $\phi(e_5) = \{v_1, v_3\}$

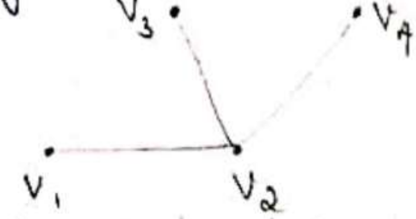






Adjacent Vertices:

Any pair of vertices which are connected by an edge in a graph is called adjacent vertices.



Here v_1, v_2 ; v_2, v_4 ; v_2, v_3 are adjacent, v_1, v_3, v_3, v_4, v_1, v_4 are not adjacent

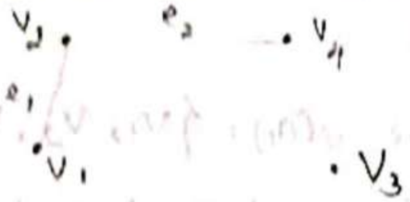
Adjacent edges:

If two distinct edges are incident with a common vertex then they are called adjacent edges.

Here e_1 and e_2 are incident with a common vertex v_2.

Isolated vertex:

In any graph, a vertex which is not adjacent to any other vertex is called an isolated vertex.

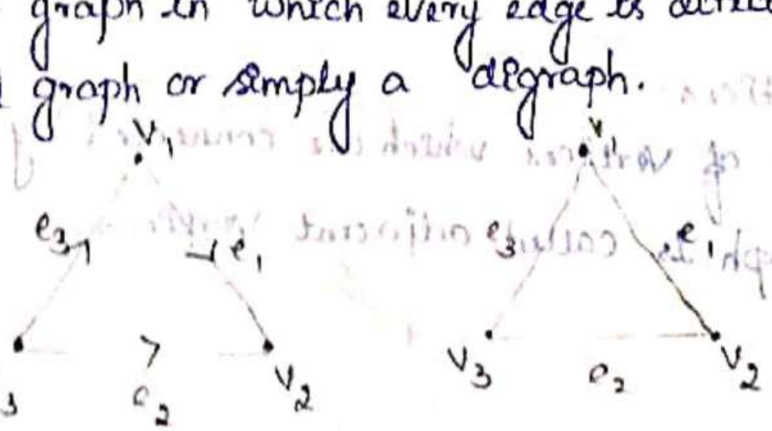


Here v_3 has no incident edge. Therefore v_3 is called isolated vertex.

Directed graph and undirected graph:

In a graph $G(V, E)$, an edge which is associated with an ordered pair of vertices is called a directed edge of graph G, while an edge which is associated with an unordered pair of vertices is called an undirected edge.

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

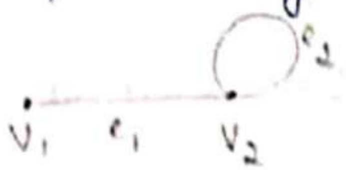


Mixed graph:

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

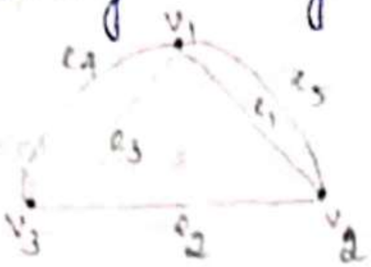
Loop:

A loop is an edge whose end vertices are equal.



parallel edges:

Multiple edges are edges having the same pair of vertices.

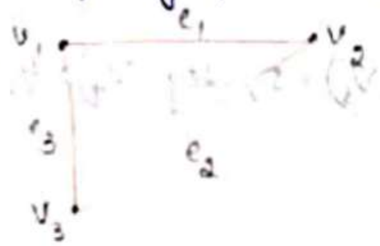


Multigraph:

Any graph which contains some parallel edges and loops is called as multigraph.

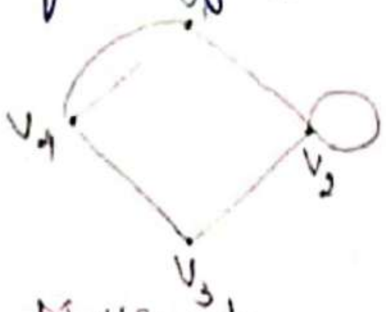
Simple graph:

A simple graph is a graph having no loops or multiple edges.

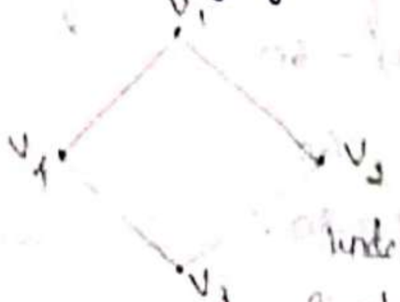


underlying simple graph:

A graph obtained by deleting all loops and parallel edges from a graph is called underlying simple graph.



Multigraph



underlying Simple graph of G.

Finite graph:

A graph G is finite if and only if both the vertex set $V(G)$ and the edge set $E(G)$ are finite, otherwise the graph is infinite.

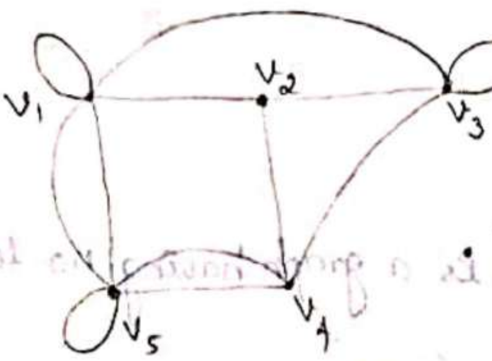
Graph terminology and special types of Graphs:

Two vertices u and v in an undirected graph G are called adjacent in G if u, v are endpoints of an edge of G.

The degree of a vertex:

The degree of a vertex in an undirected graph is the number of edges incident with it, except that a loop at a vertex contributes twice to the degree of that vertex.

Example:



$\deg(v_1) = 6$, $\deg(v_2) = 3$, $\deg(v_3) = 5$, $\deg(v_4) = 4$, $\deg(v_5) = 6$

$\deg(v_6) = 0$.

problems:

1) How many edges are there in a graph with 10 vertices each of degree six?

Soln: Sum of the degrees of the 10 vertices is

$(6)(10) = 60$

$2e = 60$

$e = 30$.

2) Show that the sum of the degree of all the vertices in a graph G, is even.

proof: Each edge contribute two degrees in a graph.

Also, each edge contributes one degree to each of the vertices on which it is incident.

Hence, if there are N edges in G, then

$$2N = d(v_1) + d(v_2) + \cdots + d(v_N)$$

Thus 2N is always even.

The Handshaking theorem:

The sum of degrees of the vertices in an un-directed graph G is twice the number of edges in G.

(or)

For any graph G with E edges and V vertices $v_1, v_2, \cdots, v_n$

$$\sum_{i=1}^{n} d(v_i) = 2|E|.$$

proof:

Let $G = G(V, E)$ be any graph, where $V = \{v_1, v_2, \cdots, v_n\}$ and $E = \{e_1, e_2, \cdots, e_n\}$ and $|E| = e$.

Since, each edge contributes twice as the degree, the sum of the degree of all vertices in G is twice as the number of edges in G.

ie) $\sum_{i=1}^{n} d(v_i) = 2|E| = 2e.$

Theorem:

The number of odd degree vertices is always 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 $G=(V,E)$.

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

By Handshaking theorem, we have

$$2e = \sum_{v_i \in V_1} \deg(v_i) + \sum_{v_j \in V_2} \deg(v_j) \rightarrow (1)$$

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

As the L.H.S of eqn (1) is even and the first expression on the R.H.S of (1) is even, we have the 2nd expression on the RHS must be even.

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

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

The number of vertices of odd degree is even.

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.

$\therefore$ The result is true for $n=1$.

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

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

The result is true for $n=2$.

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

(i) 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'.

$\therefore$ The total number of edges in G, are

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

$\therefore$ The result is true for $n = K+1$.

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

Incidence and Degree:

Indegree:

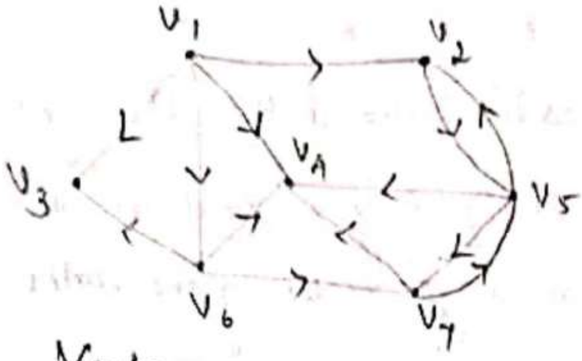
In a digraph G, the number of edges ending at vertex v of G is called the indegree of v. Indegree of v denoted by $d^{(-)}(v)$.

Outdegree:

Let G be a digraph and v be the vertex of G. The outdegree of v is the number of edges beginning at v and is denoted by $d^{+}(v)$.

Degree of a vertex:

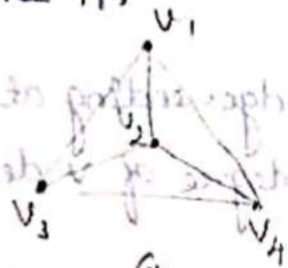
In case of a digraph G, $d(v) = d^{(-)}(v) + d^{+}(v)$.



Vertex	Indegree	Outdgree
v_1	0	4
v_2	2	1
v_3	2	0
v_4	4	0
v_5	2	3
v_6	1	3
v_7	2	2

K-Regular graph:

A graph G is said to be K-regular, if every vertex of G has degree K.

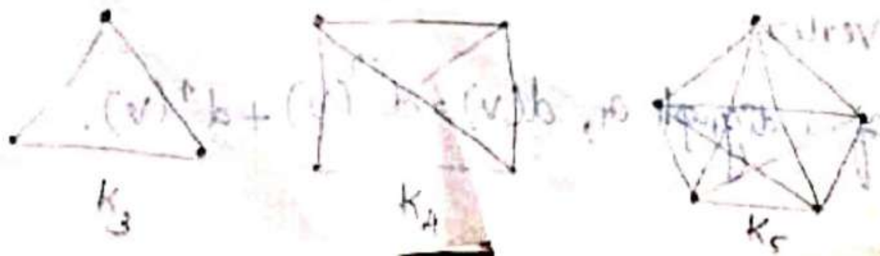


3-regular graph.

G

Complete graph:

A simple graph G in which every pair of distinct vertices are connected by an edge is called a complete graph. If G is a complete graph on n vertices then it is denoted by K_n.



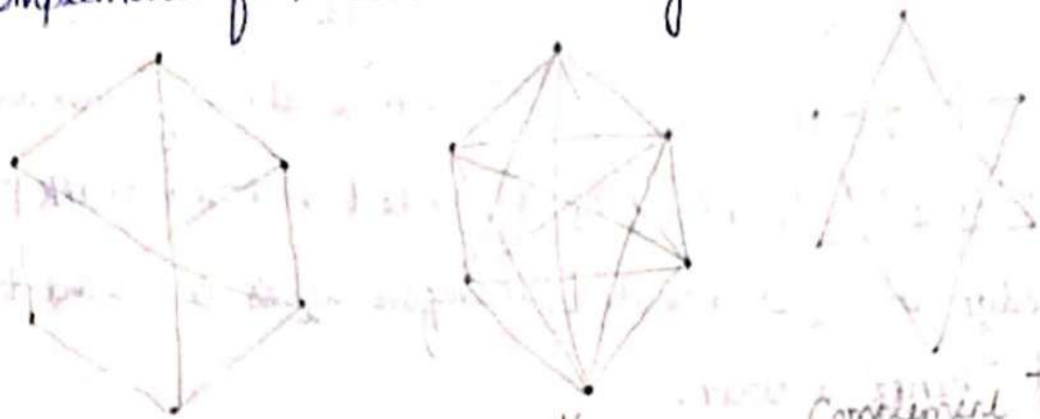
Note:

1) K_n is called $(n-1)$ regular graph.

2) Total number of edges in $K_n = \frac{n(n-1)}{2}$.

Complement of a graph:

Let G be a graph with n vertices, then $K_n - G$ is called the complement of G. It is denoted by $\overline{G}$.



G K_6 Complement $\overline{G}$

Walk, paths and circuits:

Walk:

A walk in a graph is an alternating sequence of vertices and edges $v_0 e_1 v_1 e_2 v_2 e_3 \ldots v_{n-1} e_n v_n$, beginning and ending with vertices in which each edge is incident with two vertices.

If $v_0 \neq v_n$ then the walk is an open walk and if $v_0 = v_n$, then the walk is called a closed walk.

A walk is also called a chain.

Length of a walk:

The number of edges in a walk is called the length of the walk.

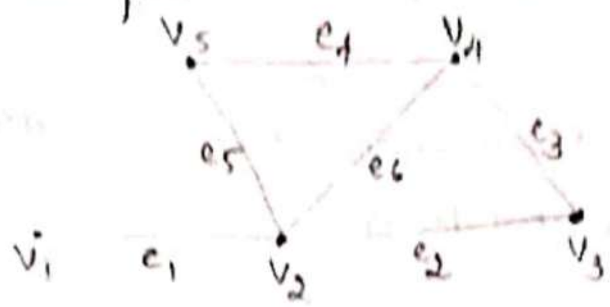
Trail:

A walk in a graph in which no edge is repeated is called a trail.

Tour:

A closed trail is called tour in a graph G.

Example:



In the graph G

$W_1 : v_1 e_1 v_2 e_2 v_3 e_3 v_4 e_4 v_5$ is called a walk and is of length 4. It is also a trail since the edges are not repeated.

$W_2 : v_2 e_2 v_3 e_3 v_4 e_4 v_5 e_5 v_2$ is called a closed walk and no edge in W_2 is repeated, therefore W_2 is a closed trail and hence a tour.

Path:

A path between vertices v_0 and v_n is given by $v_0 e_1 v_1 e_2 v_2 \cdots v_{n-1} e_n v_n$.

If $v_0 \neq v_n$, the path is called an open path and if $v_0 = v_n$, the path is called a closed path.

Path length:

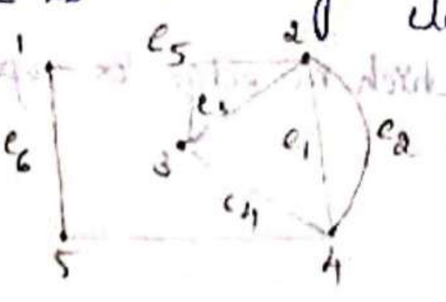
The number of edges in the path is called the path length.

Simple path:

If all the edges and vertices in a path are distinct except possibly the end points, then the path is called simple path.

Cycle:

A closed path in which all the vertices and edges are distinct is called a cycle.



closed path: $2 e_1 4 e_2 2$ is a closed pa

path: 1 - 2 - 3 - 2 - 1 - 5 is a path

1 - 2 - 3 - 4 - 5 is a simple path

2 - 4 - 3 - 2 is a cycle.

Bipartite graph:

A graph G is called a bipartite graph if its vertex set V can be divided into two disjoint subsets A and B such that every edge in G joins a vertex in A to a vertex in B.

Example:

Complete Bipartite graph:

A bipartite graph G in which every vertex of A is adjacent to every vertex in B is called a complete bipartite graph.

If $|A| = m$ and $|B| = n$, then the complete bipartite graph is denoted by $K_{m,n}$ and it has mn edges.

$K_{3,3}$

Matrix Representation of Graph:

Adjacency Matrix:

Let G be a graph with n vertices and no parallel edges. The adjacency matrix of G is an $n \times n$ symmetric matrix $A(G) = (a_{ij})_{n \times n}$, where $a_{ij} = \begin{cases} 1 & \text{if } v_i \text{ and } v_j \text{ are adjacent} \\ 0 & \text{if } v_i \text{ and } v_j \text{ are not adjacent} \end{cases}$

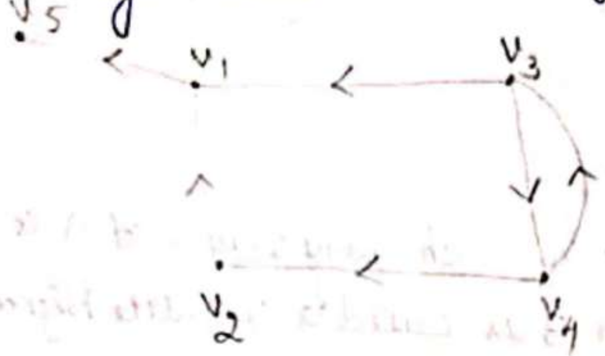
where v_i and v_j are vertices in G.

Example:

$$A(G) = \begin{array}{c} \\ a \\ b \\ c \\ d \\ e \end{array} \begin{array}{c} \begin{array}{ccccc} a & b & c & d & e \end{array} \\ \begin{bmatrix} 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 \end{bmatrix} \end{array}$$

Adjacency matrix of a directed graph:

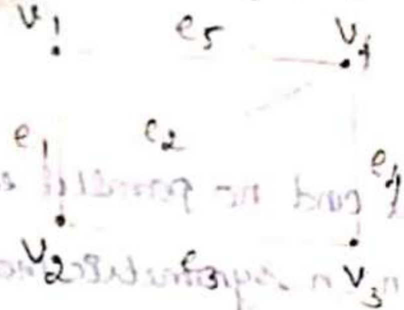
Let G be a digraph with n vertices containing no parallel edges. The adj matrix $A(G)$ of the graph G is an $n\times n$ matrix defined by $A(G) = [a_{ij}]_{n\times n}$ where $a_{ij}=1$ if there is an edge directed from v_i to v_j and $=0$ otherwise.



$$A(G) = \begin{array}{c|c} & \begin{array}{ccccc} v_1 & v_2 & v_3 & v_4 & v_5 \end{array} \\ \begin{array}{c} v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{array} & \begin{bmatrix} 0 & 0 & 1 & 0 & \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \end{array}$$

Incidence Matrix:

Let G be a graph with n vertices and m edges. The incidence matrix denoted by $B(G)$ is defined as $n\times m$ matrix $B=(b_{ij})$, where $b_{ij}=1$ if jth edge e_j is incident on ith vertex v_i and $=0$ otherwise.



$$B(G) = \begin{array}{c|c} & \begin{array}{ccccc} e_1 & e_2 & e_3 & e_4 & e_5 \end{array} \\ \begin{array}{c} v_1 \\ v_2 \\ v_3 \\ v_4 \end{array} & \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix} \end{array}$$

Incidence matrix of a Digraph:

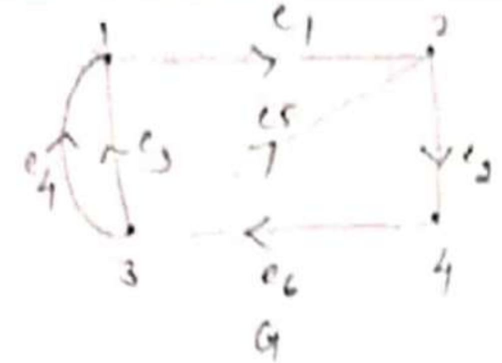
If e_k is an edge from v_i to v_j, all elements in column k are zero except $b_{ik}=+1$ and $b_{jk}=-1$.

ie) If edge e_j is directed from v_i

$b_{ij} = 1$

$= -1$ if edge e_j is directed to v_i

$= 0$ otherwise.

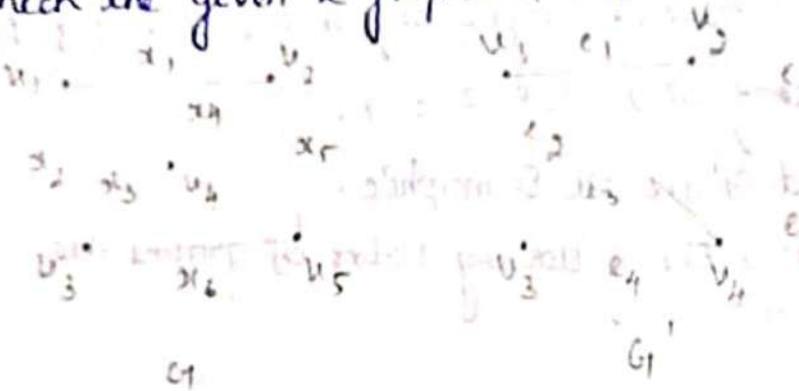


$$B = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \begin{array}{c} \begin{array}{cccccc} e_1 & e_2 & e_3 & e_4 & e_5 & e_6 \end{array} \\ \begin{bmatrix} 1 & 0 & -1 & -1 & 0 & 0 \\ -1 & 1 & 0 & 0 & -1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & -1 & 0 & 0 & 0 & 1 \end{bmatrix} \end{array}$$

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 the adjacency of the vertices.

1) Check the given 2 graphs G_1 and G_1' are isomorphic or not.



Soln:

The number of vertices (5) and the number of edges (6) are same. The degree sequence are same.

Since, in G_1 we have the vertices u_2 and u_3 of degree 2, they must be mapped to the vertices v_2 and v_4 in G_1'.

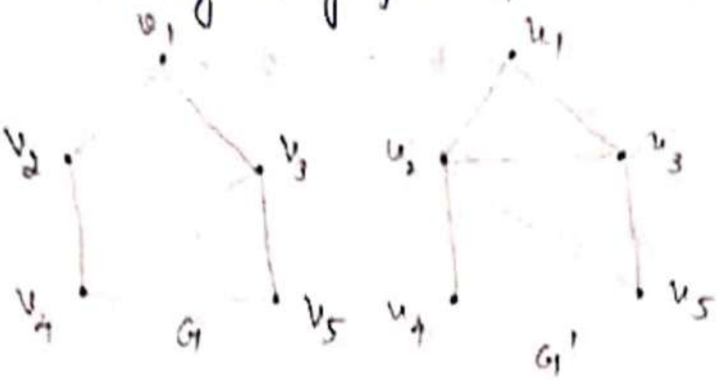
Define a mapping $u_1 \to v_1$, $u_3 \to v_2$, $u_5 \to v_3$, $u_2 \to v_4$ and $u_4 \to v_5$.

Then the edges x_2, x_1, x_6, x_5, x_3 and x_4 are mapped into e_1, e_2, e_3, e_4, e_5 and e_6.

Therefore, there is a 1-1 correspondence between the vertices and edges.

Therefore, the given 2 graphs G_1 and G_1' are isomorphic.

2) Check the 2 given graphs G_1 and G_2 are isomorphic or not.



Soln:

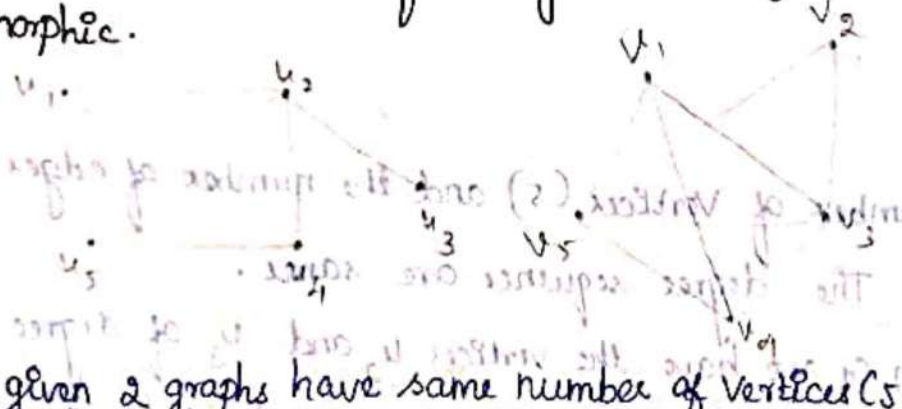
The two graphs G_1 and G_1' have same number of vertices (5) and the same number of edges (6).

But, there is no one-to-one correspondence between edges in G_1 and G_1'

For, the graph G_1 have the degree sequence 2, 2, 2, 3, 3. But the degree sequence of G_1' is 1, 2, 2, 3, 4.

Therefore, G_1 and G_1' are not isomorphic.

3) Determine whether the following pairs of graphs are isomorphic.



Soln:

The given 2 graphs have same number of vertices (5) and the same number of edges (8).

Moreover, in the given diagram u_1 and u_5 are of degree 3 each, u_2 and u_4 are of degree 4 each and u_3 is degree 2. Similarly v_1 and v_4 are of degree 3 each, v_3 and v_5 are of degree 4 each and v_2 is of degree 2.

Now if we assign, $u_1 \to v_1$, $u_2 \to v_5$, $u_3 \to v_2$, $u_4 \to v_3$, $u_5 \to v_4$ then the adjacency is preserved, which is given by their adjacency matrix:

$$
\begin{array}{c|ccccc|c|ccccc}
 & u_1 & u_2 & u_3 & u_4 & u_5 & & v_1 & v_5 & v_2 & v_3 & v_4 \\
u_1 & 0 & 1 & 0 & 1 & 1 & v_1 & 0 & 1 & 0 & 1 & 1 \\
u_2 & 1 & 0 & 1 & 1 & 1 & v_5 & 1 & 0 & 1 & 1 & 1 \\
u_3 & 0 & 1 & 0 & 1 & 0 & v_2 & 0 & 1 & 0 & 1 & 0 \\
u_4 & 1 & 1 & 1 & 0 & 1 & v_3 & 1 & 1 & 1 & 0 & 1 \\
u_5 & 1 & 1 & 0 & 1 & 0 & v_4 & 1 & 1 & 0 & 1 & 0
\end{array}
$$

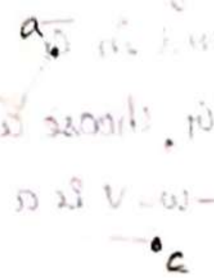
$\therefore$ The given 2 graphs are isomorphic.

problem:

Draw the graph of the given adjacency matrix.

$$
\begin{array}{c}
\\ a \\ b \\ c
\end{array}
\begin{array}{c}
\begin{array}{ccc} a & b & c \end{array} \\
\begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}
\end{array}
$$

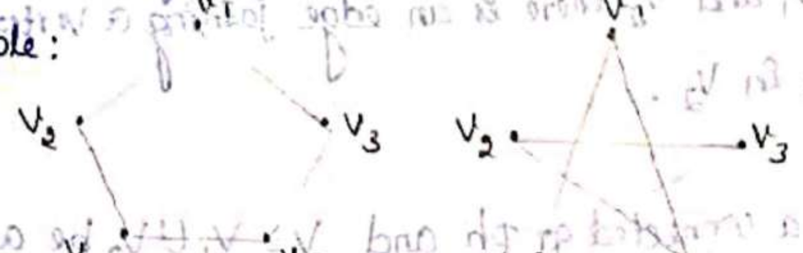
Soln:



Self - complementary graph:

A graph G is said to be Self - complementary if G is isomorphic to its complement $\overline{G}$.

Example:



G is isomorphic to $\overline{G}$ and hence G is self - complementary.

Connectivity (or) Connectedness in graphs

A graph G is said to be connected if every pair of vertices in G are joined by a path. If G is not connected then G is called a disconnected graph.

Theorem:

If G is disconnected then $\overline{G}$ is connected.

(or)

The complement of a disconnected graph is connected.

Proof:

Let G be a disconnected graph.

Then G has more than one component.

Let u, v be any two vertices of G.

The theorem is proved if we show that there is a $u-v$ path in $\overline{G}$.

If u and v are in different components of G, then u, v are not adjacent in G. Hence they are adjacent in $\overline{G}$.

If u and v are in same component of G, choose a vertex w in a different component of G. Then $u-w-v$ is a $u-v$ path in $\overline{G}$.

Hence $\overline{G}$ is connected.

Theorem:

A graph G is connected if and only if for any partition of V into subsets V_1 and V_2 there is an edge joining a vertex of V_1 to a vertex in V_2.

Proof:

Let G be a connected graph and $V = V_1 \cup V_2$ be a partition of V into subsets.

Let $u \in V_1$ and $v \in V_2$. Since the graph G is connected, a path in G say $u = v_0 v_1 v_2 \dots v_n = v$.

Let i be the least positive integer such that $v_i \in V_2$.

Then $v_{i-1} \in V_1$ and the vertices v_{i-1}, v_i are adjacent.

Thus there is an edge joining $v_{i-1} \in V_1$ and $v_i \in V_2$.

Conversely, Let G be a disconnected graph, then G contains atleast two components.

Let V_1 be the set of all vertices of one component and V_2 be the set of all remaining vertices of G.

clearly $V_1 \cup V_2 = V$ and $V_1 \cap V_2 = \phi$

The collection $\{V_1, V_2\}$ is a partition of V and there is no edge joining any vertex of V_1 to any vertex of V_2.

Hence the theorem.

Theorem:

A graph G is disconnected iff its vertex set V is partitioned into two non-empty disjoint subsets V_1 and V_2 such that there is no edge in G whose one end vertex is in subset V_1 and the other is in subset V_2.

proof:

Let us assume that such a partitioning exists.

Consider, two arbitrary vertices v_1 and v_2 of graph $G = G(V, E)$ such that $v_1 \in V_1$ and $v_2 \in V_2$.

As per our assumption, no path can exist between vertices v_1 and v_2, otherwise there would be atleast one edge whose one end vertex would be in V_1 and other in V_2. Hence, if a partition exists, the graph G is not connected.

Converse part:

The proof of the converse part is same as the proof of the converse part of the above theorem.

Theorem:

A simple graph with n vertices and K components can have almost $\frac{(n-K)(n-K+1)}{2}$ edges.

proof:

Let $n_1, n_2, \ldots, n_K$ be the number of vertices in each of the K components of the graph G.

Then $n_1 + n_2 + \cdots + n_K = n = |V(G)|$

$$\sum_{i=1}^{K} n_i = n \longrightarrow (1)$$

Now, $\sum_{i=1}^{K}(n_i - 1) = (n_1 - 1) + (n_2 - 1) + \cdots + (n_K - 1)$

$$= \sum_{i=1}^{K} n_i - K = n - K$$

$$\sum_{i=1}^{K}(n_i - 1) = n - K$$

Squaring on both sides

$$\left[\sum_{i=1}^{K}(n_i - 1)\right]^2 = (n-K)^2$$

$$(n_1 - 1)^2 + (n_2 - 1)^2 + \cdots + (n_K - 1)^2 \leq n^2 + K^2 - 2nK$$

$$n_1^2 + 1 - 2n_1 + n_2^2 + 1 - 2n_2 + \cdots + n_K^2 + 1 - 2n_K \leq n^2 + K^2 - 2nK$$

$$\sum_{i=1}^{K} n_i^2 + K - 2n \leq n^2 + K^2 - 2nK$$

$$\sum_{i=1}^{K} n_i^2 \leq n^2 + K^2 - 2nK + 2n - K$$

$$= n^2 + K^2 - K - 2nK + 2n$$

$$= n^2 + K(K-1) - 2n(K-1)$$

$$= n^2 + (K-1)(K-2n)$$

ie) $\sum_{i=1}^{K} n_i^2 \leq n^2 + (K-1)(K-2n) \longrightarrow (2)$

Since G is simple, the maximum number of edges in G in its components is $\frac{n_i(n_i - 1)}{2}$

$\therefore$ Maximum number of edges of G

$$= \sum_{i=1}^{K} \frac{n_i(n_i - 1)}{2}$$

$$= \sum_{i=1}^{K} \left[\frac{n_i^2 - n_i}{2}\right]$$

$$= \frac{1}{2}\left[n_i^2 - \frac{1}{2}\sum_{i=1}^{K} n_i\right.$$

$$\leq \frac{1}{2}\left[n^2 + (k-1)(k-2n)\right] - n/_2 \quad \left[\text{using (1) and (2)}\right]$$

$$= \frac{1}{2}\left[n^2 - 2nK + K^2 + 2n - K - n\right]$$

$$= \frac{1}{2}\left[n^2 - 2nK + K^2 + n - K\right]$$

$$= \frac{1}{2}\left[(n-K)^2 + (n-k)\right]$$

$$= \frac{1}{2}\left[(n-K)(n-K+1)\right]$$

$\therefore$ Maximum number of edges of $G \leq \frac{(n-K)(n-K+1)}{2}$.

problem:

1) prove that a simple graph with n vertices must be connected if it has more than $\frac{(n-1)(n-2)}{2}$ edges.

Soln:

Let G be a simple graph with n vertices and more than $\frac{(n-1)(n-2)}{2}$ edges.

Suppose that 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, $|E(G)| = |E(G_1)| + |E(G_2)|$

$$\leq \frac{m(m-1)}{2} + \frac{(n-m)(n-m-1)}{2}$$

$$\leq \frac{1}{2}\left[m^2 - m + n(n-m-1) - m(n-m-1)\right]$$

$$= \frac{1}{2}\left[m^2 - m + n(n-1) - nm - m(n-m-1)\right]$$

$$= \frac{1}{2}\left[n(n-1) + (2n-2) - (2n+2) - nm - m(n-m-1) + m^2 - m \right]$$

$$= \frac{1}{2}\left[n(n-1) - 2(n-1) + 2n - 2 - nm - mn + m^2 + \cancel{m} + m^2 - \cancel{m} \right]$$

$$= \frac{1}{2}\left[(n-2)(n-1) + 2n - 2 - 2mn + 2m^2 \right]$$

$$= \frac{1}{2}\left[(n-1)(n-2) + 2n(1-m) + 2(m^2-1) \right]$$

$$= \frac{1}{2}\left[(n-1)(n-2) - 2n(m-1) + 2(m-1)(m+1) \right]$$

$$= \frac{1}{2}\left[(n-1)(n-2) - 2(m-1)(n-m-1) \right]$$

$|E(G)| \leq \frac{(n-1)(n-2)}{2}$, 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.

Euler and Hamilton paths:

Euler path:

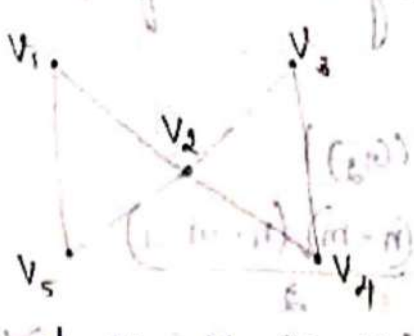
Let G be a graph. An Euler path is a path that contains every edge of G exactly once.

Eulerian circuit:

An Eulerian circuit in G is an Eulerian path whose end points are identical.

Eulerian graph:

A graph G is said to be Eulerian if it has an Eulerian circuit.



In the graph $v_1 - v_2 - v_3 - v_4 - v_2 - v_5 - v_1$ is closed and so it is an Eulerian circuit.

Theorem:

A connected graph is an Euler graph (or) Eulerian 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 (cycle) and let 'C' be an Eulerian circuit of G with origin and terminus vertex as u. Each time a vertex v 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 of 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

$\therefore$ G has all vertices of even degree.

Conversely, assume each of its vertices has even degree.

To prove: G has an Eulerian circuit.

Suppose not, ie) Assume G be a connected graph which is not having an Euler circuit, with all vertices of even degree and less number of edges.

Since each vertex of G has degree atleast two, therefore G contains closed path. Let C be a closed path.

If C itself has all the edges of G, then C 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 vertices of even degree, thus the connected graph G' also has all 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 for the choices of C.

$\therefore$ G has an Eulerian circuit and so G is a Euler graph.

Theorem:

If G is a connected graph and has exactly two vertices of odd degree, there is an Euler path in G.

(or)

If G is a connected graph and has not more than two vertices of odd degree, there is an Euler path in G.

Proof:

Let u and v be the two vertices of odd degree in G. By adding the edge $\{u, v\}$ to G, we can produce a connected graph say G_1, all of whose vertices are of even degree.

Since G_1 is a connected graph and every vertex of G_1 is of even degree, we can find an Euler circuit C in G_1. Deleting the edge $\{u, v\}$ from the circuit C, we get an Euler path that begins at u (or v) ends at v (or u).

Hamilton path:

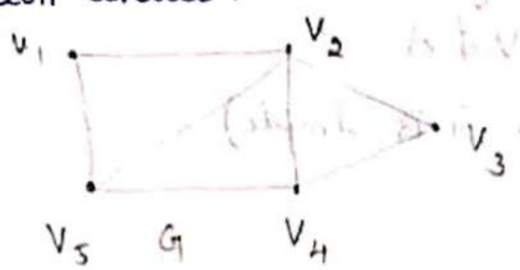
Let G be a graph. A Hamilton path is a path that passes through every vertex of G exactly once.

Hamilton circuit or Hamilton cycle:

A circuit of G is called a Hamilton circuit if it includes each vertex of G exactly once, except the starting and ending vertices.

Hamiltonian graph:

A graph G is said to be Hamiltonian if it has a Hamilton circuit.



In the graph $v_1 - v_2 - v_3 - v_4 - v_5$ is a Hamilton path

$v_4 - v_3 - v_2 - v_1 - v_5 - v_4$ is a Hamilton circuit, since it contains all the vertices, except the starting and ending vertex

Theorem:

If G is a connected simple graph with n vertices with $n \geq 3$ such that degree of every vertex in G is atleast $n/2$ then G has a Hamilton circuit or cycle.

Proof:

Assume that G is a simple graph with n vertices and the degree of every vertex is atleast $n/2$. i.e) $d(v) \geq n/2 \ \forall \ v \in V(G)$

To prove: G is Hamiltonian.

Suppose G is not Hamiltonian.

$\Rightarrow$ G is not complete.

$\Rightarrow$ There exist a pair of vertices (u, v) such that u and v are not adjacent.

Consider the graph $G' = G + \overline{uv}$ where $\overline{uv}$ is the edge joining u and v.

$\Rightarrow G'$ is complete.

$\Rightarrow G'$ becomes Hamiltonian.

$\Rightarrow$ The circuit must contain the newly introduced edge $\overline{uv}$ in G'.

$\Rightarrow$ The removal of newly added edge from the Hamiltonian circuit becomes as a Hamiltonian path in G.

Let us denote the Hamiltonian path as $p = v_1, v_2, \ldots v_n$ with $v_1 = u$ and $v_n = v$ as the terminal vertices of the path.

Define $A = \{ v_j \mid \text{there is an edge } uv_j \in E(G) \}$

$B = \{ v_j \mid \text{there is an edge } v_j v \in E(G) \}$

Since $uv \notin E(G)$, $u \notin B$ and $v \notin A$

Also $u \notin A$ and $v \notin B$ (Since, G is simple)

$\Rightarrow u, v \notin A$ and $u, v \notin B$

$\Rightarrow u, v \notin A \cup B$

$\Rightarrow |A \cup B| < n$, we claim that $A \cap B = \phi$

Suppose $A \cap B \neq \phi$

$\Rightarrow$ There exists a vertex $v_k \in A \cap B$

$\Rightarrow v_k \in A$ and $v_k \in B$

$\Rightarrow$ There is an edge uv_k in $E(G)$ and there is an edge vv_k in $E(G)$.

$\Rightarrow$ There exist a circuit covering all vertices passing through v_k in G

$\Rightarrow G$ is Hamiltonian, which is a contradiction to our assumption that G is not Hamiltonian.

$\therefore A \cap B = \phi \Rightarrow |A \cap B| = 0$

Also from the def of A and B, $|A| = d(u)$ and $|B| = d(v)$.

We know that $|A \cup B| + |A \cap B| = |A| + |B|$

$\Rightarrow |A| + |B| < n + 0 \Rightarrow d(u) + d(v) < n$

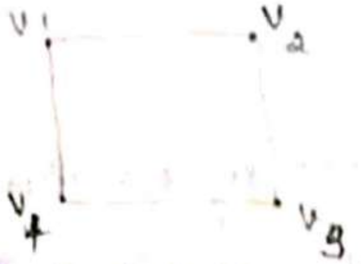
By our hypothesis, $d(u) \geq n/2$ and $d(v) \geq n/2$

$\Rightarrow d(u) + d(v) \geq n/2 + n/2 = n$, which is a contradiction.

Therefore, G must be Hamiltonian.

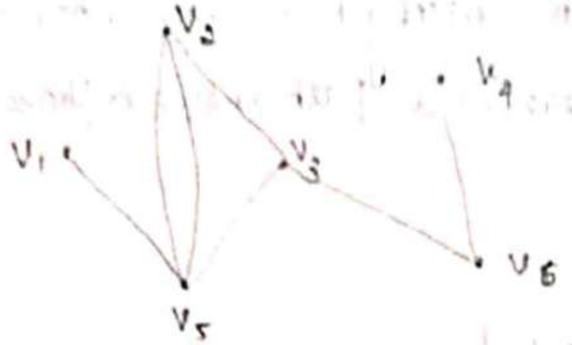
Given an example for a graph which is

i) both Eulerian and Hamiltonian.



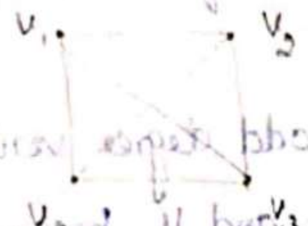
The circuit $v_1 v_2 v_3 v_4 v_1$ is both an Euler circuit and Hamilton circuit.

ii) Eulerian but not Hamiltonian.



Euler circuit : $v_1 v_5 v_2 v_5 v_3 v_6 v_4 v_3 v_2 v_1$

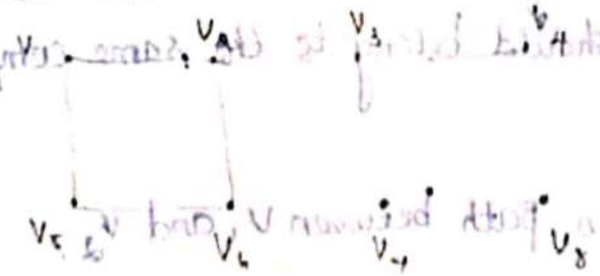
iii) Hamiltonian but not Eulerian



Hamilton circuit : $v_1 v_2 v_3 v_4 v_1$

There is no Euler circuit for this graph.

iv) Neither Eulerian nor Hamiltonian



The above graph has neither Euler circuit nor Hamilton circuit.

2-marks:

1) Can you draw a graph of 5 vertices with degree sequence 1, 2, 3, 4, 5?

Soln:

We know that the number of odd degree vertices is always even. But we have 3 odd degree vertices, so we cannot draw a graph of 5 vertices with degree sequence 1, 2, 3, 4 and 5

Theorem:

Let G be a graph with exactly two vertices has odd degree. Then prove that there is a path between those two vertices.

Proof:

Case (i) Let G be connected.

Let v_1 and v_2 be the only vertices of G with are of odd degree.

But we know that the number of odd degree vertices is even

Clearly there is a path between v_1 and v_2, because G is connected.

Case (ii): Let G be disconnected.

Then the components of G are connected.

Hence v_1 and v_2 should belong to the same component of G.

Hence there is a path between v_1 and v_2.

unit - 4.

Algebraic structures.

Definition:

Let A be any non-empty set. The binary operation $*$ is a function from $A \times A$ to A ie) a rule which assigns to every pair $(a,b) \in A \times A$, a unique element $a*b \in A$.

Notations:

$N = \{0, 1, 2, \ldots, \}$, the set of Natural Numbers

Z or $I = \{\ldots, -3, -2, -1, 0, 1, 2, 3,\}$ the set of Integers

$C = \{a+ib / a, b \in R\}$, the set of complex numbers

R - the set of real numbers

Q = the set of rational numbers = $\{a/b : a, b \in I\}$

Properties of Binary operation:

1) Associative

$*$ is associative if $a*(b*c) = (a*b)*c$ for all $a, b, c \in A$.

2) commutative

$a*b = b*a$ for all $a, b \in A$.

3) Existence of identity:

$*$ possesses the identity element $e \in A$ if $a*e = e*a = a \ \forall a \in A$.

4) The binary operation is called idempotent if it possesses idempotent element. An element $a \in A$ is called idempotent if $a*a = a$.

5) Existence of Inverse element.

The element b is called an inverse of the element a if $a*b = b*a = e$.

Algebraic system:

Definition:

A non-empty set together with one or more binary operations defined on A is called algebraic system.

If $*$ is a binary operation defined on a set A, then $(A, *)$ is called an algebraic system.

Semigroup:

Let S be a non-empty set with a binary operation $*$ on it. Then S is called a semigroup w.r.to $*$ if $*$ is associative.

ie) $a*(b*c) = (a*b)*c$ for all $a, b, c \in S$.

Example:

Show that the set of all Natural numbers N is a semigroup w.r.to operation $*$ defined by $a*b = \max\{a,b\}$

Solution:

N is closed for the operation $*$.

For $a, b, c \in N$

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

$\therefore a*(b*c) = (a*b)*c \ \forall a, b, c \in N$

$\therefore *$ is associative.

$(N, *)$ is a semigroup.

Commutative Semigroup:

The semigroup $(S, *)$ is called commutative semigroup if $a*b = b*a \ \forall a, b \in S$.

Example:

Let $(S, *)$ be a commutative semigroup. If $x*x = x$, $y*y = y$, prove that $(x*y)*(x*y) = x*y$.

Solution:

$$
\begin{aligned}
L.H.S &: (x*y)*(x*y) \\
&= x*(y*(x*y)) \\
&= x*((y*x)*y) \\
&= x*((x*y)*y) \\
&= x*(x*(y*y)) \\
&= x*(x*y) \\
&= (x*x)*y \\
&= x*y = R.H.S.
\end{aligned}
$$

Monoid:

Let M be a non-empty set with a binary operation * on it. Then M is called a monoid for the operation * if

(i) * is associative

ie) $(a*b)*c = a*(b*c) \ \forall a \in M$

ii) there exists an element $e \in M$ such that

$e*a = a*e = a \ \forall a \in M$ (e is called the identity of M w.r.to *).

∴ A semigroup with an identity element is Monoid.

Symbolically we represent a monoid by $(M, *, e)$ with e as identity element.

Example:

Show that the set of integers, I is a monoid for the operation * defined by $a*b = a+b-ab$, $a, b \in I$.

Solution:

I is closed for operation *

Further I is associative.

The element $0 \in I$ is the identity for * since

$x*0 = x+0-x*0 = x$ and $0*x = 0+x-0 \cdot x = x \ \forall x \in I$

∴ $(I, *)$ is a monoid, with identity $0 \in I$.

commutative monoid:

A monoid $(M, *, e)$ is said to be commutative if $a*b = b*a \ \forall a, b \in M$.

Example:

$(I, +)$, $(I, \times)$ are commutative monoids.

Group

Definition:

A non empty set G with a binary operation $*$ is called a group if the following axioms are satisfied.

1) G is closed with respect to $*$

2) $*$ is associative ie) $(a*b)*c = a*(b*c) \ \forall a, b \in G$.

3) There exists an element $e \in G$ such that $a*e = e*a = a, \forall a \in G$
(e is the identity element)

4) For every $a \in G$, there exists an element $a^{-1} \in G$ such that
$a*a^{-1} = a^{-1}*a = e$
(a^{-1} is called the inverse element of a).

Abelian group (or) commutative group:

A group $(G, *)$ is called abelian if $a*b = b*a \ \forall a, b \in G$

ie) $*$ is commutative in G.

Examples:

1. $(I, +)$ is a group called the additive group of integers.

2. $G = \{1, -1, i, -i\}$. In G, the operation '$\cdot$' is defined by the following table. Then $(G, \cdot)$ is an abelian group

$\cdot$	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1

Here '$\cdot$' is the operation, multiplication of complex numbers.

Example of a monoid which is not a group:

$(I, \times)$ is a monoid but not a group where I is the set of integers and $\times$ is the operation usual multiplication of integers.

Examples:

Show that $[Z_5, +_5]$ is an abelian group.

Solution:

The operation table for addition modulo 5 is

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

$[a] +_5 [b]$ = remainder when is devided by $[5]$

From the operation table $[a], [b] \in Z_5$ implies $[a] +_5 [b] \in Z_5$

$$[a] +_5 ([b] +_5 [c]) = ([a] +_5 [b]) +_5 [c]$$

$[0] \in Z_5$ is the identity element

The inverse of $[1]$ is $[4]$

The inverse of $[2]$ is $[3]$

The inverse of $[3]$ is $[2]$

The inverse of $[4]$ is $[1]$

The element $[0] \in Z_5$ has self inverse.

Further $[a] +_5 [b] = [b] +_5 [a]$, $\forall [a], [b] \in Z_5$

$\therefore (Z_5, +_5)$ is an abelian group.

properties of Group:

property 1:

The identity element in a group is unique.

proof:

Let e_1 and e_2 be two identity elements in G.

$e_1 * e_2 = e_2$ (Taking e_1 as identity) and

$e_1 * e_2 = e_1$ (Taking e_2 as identity)

$\therefore e_1 = e_2$.

property 2:

The inverse of every element in a group is unique.

proof:

Let $(G, *)$ be a group, with identity element e. Let b and c be inverses of an element $a \in G$.

$$a * b = b * a = e$$

$$a * c = c * a = e$$

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

property 3:

If a is an element in a group $(G, *)$ then $(a^{-1})^{-1} = a$.

property 4:

If a and b are two elements in a group $(G, *)$, then $(a*b)^{-1} = b^{-1} * a^{-1}$.

[prove $(a*b) * (b^{-1} * a^{-1}) = e$ and $(b^{-1} * a^{-1}) * (a * b) = e$].

property 5:

Cancellation law:

In a group $(G, *)$, $a * c = b * c \Rightarrow a = b$ [$\because$ Right cancellation]

$a * b = a * c \Rightarrow b = c$ [$\because$ Left cancellation]

Property 6:

In a group $(G, *)$, the equation $x * a = b$ and $a * y = b$ have unique solutions.

Proof: Consider $x * a = b$

Post multiplying by a^{-1}, $(x * a) * a^{-1} = b * a^{-1}$

$$x * (a * a^{-1}) = b * a^{-1}$$
$$x * e = b * a^{-1}$$
$$x = b * a^{-1}$$

Proof of uniqueness

Let x_1 and x_2 be two solutions of $x * a = b$

Then $x_1 * a = b$ and $x_2 * a = b$

$\therefore x_1 * a = x_2 * a$

$\Rightarrow x_1 = x_2$ (by right cancellation law)

In a similar manner, the equation $a * y = b$ has a solution $y = a^{-1} * b$ and this solution is unique.

Definitions

Order of a group:

The number of elements in a group is denoted by the symbol $O(G)$ or $|G|$, called the order of the group G.

Order of an element:

Let G be a group and $a \in G$, If for some positive integer n, $a^n = e$, then n is called the order of the element a and is denoted by the symbol $O(a)$.

$\therefore O(a) = n$ if $a^n = e$.

Note: Order of a = order of a^{-1} (ie) $O(a) = O(a^{-1})$.

Powers of an element 'a'.

Let $a \in G$

We define $a^2 = a * a$, $a^3 = a * a * a = a^2 * a$, $\ldots$, $a^n = (a^{n-1}) * a$.

Let $G = \{1, -1\}$

Then $(G, \cdot)$ is a group with identity 1, where $\cdot$ is the usual multiplication. $(-1)^2 = 1$

$\therefore o(-1) = 2$

Let $G = \{1, -1, i, -i\}$

$(G, \cdot)$ is a group where '$\cdot$' is the usual multiplication of complex numbers.

$o(i) = 4$ because $i^4 = 1$

$o(-i) = 4$, $o(-1) = 2$.

Cyclic group:

Definition:

A group $(G, *)$ is called a cyclic group if for some element $a \in G$, every element $x \in G$ is expressed as $x = a^m$ or $x = ma$ where m is an integer. Here a is called the generator of the cyclic group G.

We say that G is a cyclic group generated by $a \in G$ and it can be written as $G = (a)$.

Example:

1) The additive group $(Z, +)$ is a cyclic group generated by 1 and -1 since every integer is either a multiple for 1 or -1.

2) $(G, \cdot)$ is a group where $G = \{1, -1, i, -i\}$. $1 = i^4$

This group G is cyclic with generators i and $-i$. $-1 = i^2$

$i = i^1$

$-i = -(i)$

Theorem:

Any cyclic group is abelian.

$-1 = -i^2 = (-i^2)$

proof: $-1 = i \cdot (-i)$

Let $(G, *)$ be a cyclic group generated by $a \in G$. $i = -i$

$i = -i$

Let $b, c \in G$. Then $b = a^m$ and $c = a^n$ for some integers m and n.

$$\therefore b * c = a^m * a^n$$
$$= a^{m+n} = a^{n+m}$$
$$= a^n * a^m = c * b$$

Sub-Structures

Subsemigroup:

Let $(S, *)$ be a semigroup and $T \subseteq S$. If the set T is closed for the operation $*$ then $(T, *)$ is called the subsemigroup of $(S, *)$.

Example:

$(E, +)$ is a subsemigroup of $(Z, +)$, where E = Set of even int

Submonoid:

Let $(M, *, e)$ be a monoid and $T \subseteq M$. If T is closed under the operation $*$ and $e \in T$, then $(T, *)$ is called a submonoid of $(M, *)$.

Example:

Let T = Set of odd integers, then $(T, *)$ is a submonoid of $(Z, *)$ where $*$ is the usual multiplication.

Theorem:

Prove that in any commutative monoid $(M, *, e)$, the set of all idempotent elements of M forms a sub-monoid of M.

Proof:

Let S be the set of all idempotent elements of the monoid M

$e * e = e$

$\therefore$ e is an idempotent element and so $e \in S$.

$\therefore$ S is non-empty.

Let $a, b \in S$

To prove: $a * b \in S$.

Consider $(a*b)*(a*b) = a*(b*(a*b))$

$= a*(b*a)*b$

$= a*(a*b)*b$ [$\because a, b \in M$ and $a*b = b*a$]

$= (a*a)*(b*b)$

$= a*b$

[$\because a*a = a$ and $b*b = b$ because a, b are idempotent]

$\therefore$ $a*b$ idempotent element and hence $a*b \in S$.

$\therefore$ S is closed for the operation $*$. This means that $(S, *)$ is a sub-monoid of $(M, *)$.

$\therefore$ The set of all idempotent elements of a commutative monoid M forms a sub-monoid.

Subgroup:

Let $(G, *)$ be a group and $H \subseteq G$. $(H *)$ is called a Subgroup of $(G, *)$ if H itself is a group w.r.to $*$.

Trivial subgroups:

For any group $(G, *)$, $\{\{e\}, *\}$ and $(G, *)$ are subgroups, called trivial subgroups. All other subgroups are called non-trivial subgroups.

Condition for a non-empty subset H to be a subgroup of G.

A non-empty set H is a subgroup of a group $(G, *)$ if

i) H is closed for the operation $*$.

ii) H contains the identity element $e \in G$.

iii) For every $a \in H$, $a^{-1} \in H$.

Necessary and sufficient conditions for a subgroup:

A non-empty subset H of a group $(G, *)$ is a subgroup of G if and only if $a * b^{-1} \in H$ for all $a, b \in H$.

proof:

Necessary part

First we assume that H is a subgroup of G.

Let $a, b \in H$

Since H is a subgroup, $b \in H \Rightarrow b^{-1} \in H$.

Further H is closed for $*$ then $a \in H, b^{-1} \in H$ implies $a * b^{-1} \in H$

$\therefore$ $a * b^{-1} \in H \ \forall a, b \in H$.

Sufficient part:

We suppose that H is a non-empty subset of G with the condition $a \in H, b \in H$ implies $a * b^{-1} \in H$.

We shall show that H is a subgroup of $(G, *)$.

For $a \in H, a^{-1} \in H$, we have

$a * a^{-1} = e \in H$ [taking $b = a$ in the condition]

∴ The identity element $e \in H$

For $a \in H$, $e \in H$, $e * a^{-1} = a^{-1} \in H$ [taking $a = e$ and $b = a$]

∴ For every $a \in H$, $a^{-1} \in H$ — Let $a, e \in H$

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

Consider $b \in H$ and $b^{-1} \in H$ — $\Rightarrow a^{-1} \in H$

Every element 'a' of H has its inverse a^{-1} is in H.

For $a \in H, b^{-1} \in H$, $a * (b^{-1})^{-1} = a * b \in H$

∴ H is closed for the operation $*$. Closure: Let $b \in H \Rightarrow b^{-1} \in H$

The elements of H are also the elements of G and $*$ is associative in G. For $a, b \in H \Rightarrow a * b^{-1} \in H$

$\Rightarrow a * (b^{-1})^{-1} \in H \Rightarrow a * b \in H$

We have $a * (b * c) = (a * b) * c \ \forall a, b, c \in H$ implies $*$ is associative in ~~G~~ H. H is closed

H is a subgroup of G

∴ H is a group for the operation $*$.

Hence $(H, *)$ is a subgroup of $(G, *)$.

Theorem:

Prove that the intersection of two subgroups of a group G is also a subgroup of G (or) Let G be a group and H and K are subgroups of G then $H \cap K$ is also a subgroup of G.

proof:

Let H and K be two subgroups of group $(G, *)$.

Clearly, $e \in H \cap K$ where e is the identity element of G.

So $H \cap K$ is non-empty.

Let $a, b \in H \cap K$.

To prove: $a * b^{-1} \in H \cap K$, $\forall a, b \in H \cap K$

$a, b \in H \cap K$ implies $a \in H, b \in H$ and $a \in K$ and $b \in K$.

Since H is a subgroup of G, $a \in H, b \in H$ implies $a * b^{-1} \in H$.

Also K is a subgroup of G, $a \in K, b \in H$ implies $a * b^{-1} \in K$

∴ $a * b^{-1} \in H \cap K \ \forall a, b \in H \cap K$.

∴ $H \cap K$ is a subgroup of G.

Hence the intersection of two subgroups of group G is also a subgroup.

Note:

The union of two subgroups need not be a subgroup.

Theorem:

If H and K are subgroups of a group $(G, *)$, then $H \cup K$ is a subgroup of G if and only if $H \subseteq K$ or $K \subseteq H$.

Note:

If $(G, *)$ is a finite group and $H \subseteq G$, then $(H, *)$ is a subgroup of G if H is closed for the operation $*$.

Example:

1) $(G, \cdot)$ is a group where $G = \{1, -1, i, -i\}$, $H = \{1, -1\}$

$(H, \cdot)$ is a subgroup of G since H is closed for operation '$\cdot$'.

The operation table is

$\cdot$	-1	1
-1	1	-1
1	-1	1

Examples:

1) prove that if $(G, *)$ is a cyclic group then every subgroup of G must be cyclic (or) prove that every subgroup of a cyclic group is cyclic.

Solution:

Let G be a cyclic group generated by an element $a \in G$.

ie) $G = \langle a \rangle$.

$\therefore$ Every element of G is 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.

$\therefore$ 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.

clearly, every element of H is of the form a^n for some Integer n.

Let m be the least positive Integer such that $a^m \in H$

We will prove that H is a cyclic group generated by a^m.

Let $b \in H$ then $b = a^n$ for some Integer n.

Let $n = mq + r$ where $0 \leq r < m$.

$$\therefore b = a^n = a^{mq+r}$$

$$= a^{mq} * a^r$$

$$= (a^m)^q * a^r$$

$$a^r = (a^m)^{-q} * b$$

Now $b \in H$, $(a^m)^{-q} \in H$ and H is closed for $*$, we have $(a^m)^{-q} * b \in H$.

ie) $a^r \in H$ where $0 \leq r < m$.

This shows that there exists an Integer r such that $0 \leq r < m$ with $a^r \in H$.

Since m is the least positive Integer for which $a^m \in H$, $a^r \in H$ with $0 \leq r < m$ is not possible.

$\therefore r = 0$, so $b = a^{mq}$

ie) $b = (a^m)^q$.

This implies that every element $b \in H$ is expressed as a power of a^m.

ie) 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.

2) Show that the set of all elements 'a' of a group $(G, *)$ such that $a * x = x * a \ \forall \ x \in G$ is a subgroup of G.

Solution:

Let $H = \{a \in G / a * x = x * a \ \forall x \in G\}$.

Homomorphism of Semigroups and monoids.

Semigroup homomorphism:

Let $(S, *)$ and $(T, \circ)$ be two semigroups. A mapping $g: S \to T$ is called a semigroup homomorphism if $g(a * b) = g(a) \circ g(b)$ $\forall$ $a, b \in S$.

Note:

1) If g is one-to-one, then $g: S \to T$ is called semigroup monomorphism.

2) If g is onto, $g: S \to T$ is called semigroup epimorphism.

3) If g is both 1-1 and onto then $g: S \to T$ is called semigroup isomorphism.

properties:

property 1:

A semigroup homomorphism preserves the property of associativity.

proof:

Let $a, b, c \in S$

$$g[(a*b)*c] = g(a*b) \circ g(c)$$
$$= [(g(a) \circ g(b)) \circ g(c)] \to (1)$$

$$g[a*(b*c)] = g(a) \circ g(b*c)$$
$$= g(a) \circ [g(b) \circ g(c)] \to (2)$$

But in S, $(a*b)*c = a*(b*c)$ $\forall$ $a, b, c \in S$

$$g[(a*b)*c] = g[a*(b*c)]$$
$$\Rightarrow [g(a) \circ g(b)] \circ g(c) = g(a) \circ [g(b) \circ g(c)]$$

$\therefore$ The property of associativity is preserved.

property 2:

A semigroup homomorphism preserves idempotency and commutativity.

Proof:

Let $a \in S$ be an idempotent element.

$\therefore a * a = a$.

$\therefore g(a * a) = g(a)$

$g(a) \circ g(a) = g(a)$

This shows that $g(a)$ is an idempotent element in T.

$\therefore$ The property of idempotency is preserved under semigroup homomorphism.

Let $a, b \in S$

Assume that $a * b = b * a$

$g(a * b) = g(b * a)$

$g(a) \circ g(b) = g(b) \circ g(a)$

This means that the operation $\circ$ is commutative in T.

$\therefore$ The semigroup homomorphism preserves commutativity.

Monoid homomorphism:

Let $(M, *, e)$ and $(T, \circ, e)$ be any two monoids.

A mapping $g: M \to T$ is called a monoid homomorphism if

i) $g(a * b) = g(a) \circ g(b)$, $a, b \in M$

ii) $g(e) = e_1$.

Note:

A monoid homomorphism preserves not only associativity and the identities but also commutativity.

Example 1:

Prove that a monoid homomorphism preserves the property of invertibility. (i.e.) it preserves inverse elements.

Solution:

To prove: If a^{-1} is the inverse of $a \in M$, then $g(a^{-1})$ is the inverse of $g(a)$.

Consider $g(a * a^{-1}) = g(e)$

$g(a) \circ g(a^{-1}) = e_1 \rightarrow (1)$

Also $g(a^{-1} * a) = g(e)$

$g(a^{-1}) \circ g(a) = e_1 \rightarrow (2)$

From (1) and (2), $g(a^{-1}) = [g(a)]^{-1}$

Thus the property of invertibility is preserved.

Example 2:

~~Eg~~ If $g: M \rightarrow T$ is a monoid homomorphism of $(M, *, e)$ onto $(T, \circ, e_1)$ then it preserves the zero elements.

Solution:

Let $z \in M$ be a zero element of M.

ie) $z * x = x * z = z \ \forall x \in M$

$\therefore z * x = z$

$g(z * x) = g(z)$

$g(z) \circ g(x) = g(z)$

Also $g(x * z) = g(z)$

$g(x) \circ g(z) = g(z)$

$\therefore$ For any $t \in T$, we can find $t \in M$ such that $t = g(b)$.

$\therefore g(z) \in T$ has a preimage $z \in M$, since z is a zero element of M, $g(z)$ is a zero element of T.

$\therefore$ A monoid epimorphism preserves the zero element, if it exists.

Theorem:

If $(S, *)$ and $(T, \circ)$ and $(V, \oplus)$ be semigroups and $g: S \rightarrow T$ and $h: T \rightarrow V$ are semigroup homomorphism then $h \circ g: S \rightarrow V$ is a semigroup homomorphism from $(S, *)$ to $(V, \oplus)$ and is defined by

$$(h \circ g)(a) = h[g(a)]$$

Proof:

Let $a, b \in S$

To prove : $(h \circ g)(a * b) = (h \circ g)(a) \oplus (h \circ g)(b)$

Consider $(h \circ g)(a * b) = h[g(a * b)]$

$= h[g(a) \circ g(b)]$

$= h[g(a)] \oplus h[g(b)]$

$= (h \circ g)(a) \oplus (h \circ g)(b) \; \forall a, b \in S$.

$\therefore h \circ g : S \to V$ is a semigroup homomorphism.

Theorem:

Let $(S, *)$ be a semigroup. Then there exists a homomorphism $g : S \to S^S$, where $(S^S, \circ)$ is a semigroup of functions from S to S under the operation of left composition.

proof: To prove: $g : S \to S^2$ is a homomorphism.

(i) $g(a * b) = g(a) \circ g(b)$ for all $a, b \in S$.

We define $g : S \to S^S$ by $g(a) = f_a$ for $a \in S$, where $f_a : S \to S$ such that $f_a(b) = a * b$ for $b \in S$.

Since $a * b \in S$, $g(a * b) = f_{a+b}$ for $a, b \in S$

We first prove that $f_{a*b} = f_a \circ f_b$

Consider $f_{a*b}(c) = (a * b) * c$

$= a * (b * c)$

$= a * f_b(c)$

$= f_a[f_b(c)]$

$= (f_a \circ f_b)(c)$

$\therefore f_{a*b} = f_a \circ f_b \; , \forall a, b \in S$

$f : G_1 \to G_1$ is a group homomorphism

$\therefore f(a * b) = f(a) \circ f(b) \; \forall a, b \in G_1$.

Consider $g(a * b) = f_{a*b}$

$= f_a \circ f_b$

$\therefore \; g(a * b) = g(a) \circ g(b)$ for all $a, b \in S$

Hence $g : S \to S^S$ is a homomorphism.

Group Homomorphism:

Let $(G, *)$ and $(G_1, \circ)$ be two groups. A mapping $g: G \to G_1$ is called a group homomorphism if $g(a * b) = g(a) \circ g(b) \ \forall a, b \in G$.

properties of group homomorphism:

A group homomorphism preserves identities, inverses and subgroups

Theorem:

If $f: G \to G_1$ is a group homomorphism then

i) $f(e) = e_1$ where e and e_1 are the identity elements of G and G_1 respectively.

ii) $f(a^{-1}) = [f(a)]^{-1}$.

iii) If H is a subgroup of G then $f(H)$ is a subgroup of G_1.

proof of (i):

Let $a \in G$, then $a * e = e * a = a$

$$a * e = a$$

$$\Rightarrow f(a * e) = f(a)$$

$$f(a) \circ f(e) = f(a) \circ e_1$$

$[\because e_1 \in G_1$ is the identity element and $f(a) \in G_1]$

By left cancellation law,

$$f(e) = e_1$$

Similarly, $f(e * a) = f(a)$

$$\Rightarrow f(e) \circ f(a) = e_1 \circ f(a)$$

By right cancellation law, $f(e) = e_1$

proof of (ii)

Let $a \in G$, then $a^{-1} \in G$ and $a * a^{-1} = a^{-1} * a = e$

$$a * a^{-1} = e$$

$$\Rightarrow f(a * a^{-1}) = f(e)$$

$$f(a) \circ f(a^{-1}) = e_1$$

$$f(a^{-1}) = [f(a)]^{-1}.$$

Similarly, $a^{-1} * a = e$

$\Rightarrow f(a^{-1} * a) = f(e)$

$f(a^{-1}) \circ f(a) = e_1$

This shows that $f(a^{-1}) = [f(a)]^{-1} \; \forall a \in G$.

Proof of (iii):

Let H be a subgroup of G.

$\therefore$ for $a, b \in H$, $a * b^{-1} \in H$

Let $f(a) \in f(H)$ and $f(b) \in f(H)$

To prove: $f(a) \circ [f(b)]^{-1} \in f(H)$

Consider $f(a) \circ [f(b)]^{-1}$

$= f(a) \circ \cancel{f(b)} f(b) = f(a) \circ f(b^{-1})$ (by property 2)

$= f(a * b^{-1})$

Since $a * b^{-1} \in H$ implies $f(a * b^{-1}) \in f(H)$.

$\therefore f(a) \circ [f(b)]^{-1} \in f(H) \; \forall f(a) \in f(H)$ and $f(b) \in f(H)$.

$\therefore f(H) \subseteq G_1$ is a subgroup of G_1.

Kernel of a homomorphism:

Let $f : G \rightarrow G_1$ be a group homomorphism. Then the set of all elements of G which are mapped into the identity element e_1 of G_1 is called the kernel of the homomorphism f and is denoted by the symbol 'Ker f'.

$\therefore$ Ker $f = \{x \in G \mid f(x) = e_1$ where $e_1 \in G_1$ is the identity element$\}$.

Theorem:

If $f : G \rightarrow G_1$ is a group homomorphism then Ker f is a subgroup of G.

proof: By definition Ker $f = \{x \in G \mid f(x) = e_1\}$

Clearly, Ker f is a subset of G.

By property of group homomorphism, we have $f(e) = e_1$, where e and e_1 are the identity elements of G and G_1, respectively.

So $e \in \ker f$ is non-empty.

Let $a, b \in \ker f$

To prove: $a * b^{-1} \in \ker f$

Since $a, b \in \ker f$, $f(a) = e_1$ and $f(b) = e_1$.

$$
\begin{aligned}
f(a * b^{-1}) &= f(a) \cdot f(b^{-1}) \\
&= f(a) \cdot [f(b)]^{-1} \\
&= e_1 \cdot e_1^{-1} \\
&= e_1 \cdot e_1 = e
\end{aligned}
$$

$\therefore a * b^{-1} \in \ker f$ for $a, b \in \ker f$

$\therefore \ker f$ is a subgroup of G.

Group Isomorphism:

Definition:

Let $f: G \to G_1$ be a group homomorphism. Then $f: G \to G_1$ is called a group isomorphism if

i) f is one-to-one and

ii) f is onto.

Equivalently a bijection $f: G \to G_1$ is called a group isomorphism if $f(a * b) = f(a) \cdot f(b)$ for all $a, b \in G$.

Two groups are said to be isomorphic if there exists an isomorphism between them.

$\therefore f: G \to G_1$ is a group isomorphism then we write $G \cong G_1$ (G is isomorphic to G_1).

Example:

1) Prove that any infinite cyclic group is isomorphic to the additive group of integers $(Z, +)$.

Solution:

Let G be an infinite cyclic group generated by the element $a \in G$.

Then $G = \{ \dots a^{-3}, a^{-2}, a^{-1}, a^0 = e, a^1, a^2, a^3, \dots \}$

The additive group of integers is $(\mathbb{Z}, +)$ where

$$\mathbb{Z} = \{ \dots -3, -2, -1, 0, 1, 2, 3, \dots \}$$

Define a function $f : \mathbb{Z} \to G$ by $f(n) = a^n \ \forall n \in \mathbb{Z}$.

Clearly, f is well defined and it is both one-to-one and onto.

$\therefore f$ is a bijection.

It remains to prove $f(a+b) = f(a) \cdot f(b)$

Consider $f(m+n) = a^{m+n}$

$$= a^m \cdot a^n$$

$\therefore f(m+n) = f(m) \cdot f(n) \ \forall m, n \in \mathbb{Z}$

$\therefore f$ is a homomorphism.

Further $f : \mathbb{Z} \to G$ is both one-to-one and onto.

$\therefore f : \mathbb{Z} \to G$ is an isomorphism.

$\therefore \mathbb{Z}$ is isomorphic to G.

Hence an infinite cyclic group is isomorphic to additive group of integers $(\mathbb{Z}, +)$.

* Cosets and Lagrange's theorem.

Cosets :

Let $(H, *)$ be a subgroup of a group $(G, *)$ and let $a \in G$.

we define $a * H = \{ a * h \mid h \in H \}$

$$H * a = \{ h * a \mid h \in H \}$$

$a * H$ is called the left coset of H.

$H * a$ is called the right coset of H in G.

The element $a \in G$ is called the representative element.

Note: If G is an abelian group then $a * H$ and $H * a$ are both identical, and in this case we have the only coset $a * H$.

Example:

Find all the left cosets of the subgroup $H = \{[0][2]\}$ in the group $(Z_4, +_4)$.

Solution:

$Z_4 = \{[0][1][2][3]\}$

$[0] +_4 H = \{[0], [2]\}$

$[1] +_4 H = \{[1], [3]\}$

$[2] +_4 H = \{[2], [0]\} = [0] +_4 H$

$[3] +_4 H = \{[3], [1]\} = [1] +_4 H$

$\therefore$ The two different cosets are $[0] +_4 H$, $[1] +_4 H$

Similarly, the right cosets are $H +_4 [0]$, $H +_4 [1]$.

Theorem:

Let $(H, *)$ be a subgroup of $(G, *)$. Then any two left cosets (right cosets) of H of a group $(G, *)$ are neither 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 $a * H = b * H$ or $a * H \cap b * H = \phi$.

Suppose that $a * H$ and $b * H$ are not disjoint then $(a * H) \cap (b * H) \neq \phi$

$\therefore$ There exists an element $c \in (a * H) \cap (b * H)$.

This implies $c \in (a * H)$ and $c \in (b * H)$.

Let $c = a * h_1$ and $c = b * h_2$ for $h_1, h_2 \in H$.

Therefore $a * h_1 = b * h_2$

$(a * h_1) * h_1^{-1} = (b * h_2) * h_1^{-1}$

$a * (h_1 * h_1^{-1}) = b * (h_2 * h_1^{-1})$

$\therefore a*e = b*h_3$ where $h_3 = h_2 * h_1^{-1} \in H$

$\therefore a = b*h_3$

$a \in b*H$

$\Rightarrow a*H \subseteq b*H \rightarrow (1)$

Similarly $b*H \subseteq a*H \rightarrow (2)$

$\therefore$ From (1) and (2), $a*H = b*H$.

$\therefore$ Any two left cosets are either identical or disjoint.

Each element of the left coset $a*H$ is also an element of G.

$\therefore$ Every left coset $a*H$ is a subset of G.

Hence $\bigcup_{a \in G} a*H \subseteq G \rightarrow (3)$

If $a \in G$, then $a \in a*H$

Also $a \in a*H \Rightarrow a \in \bigcup_{a \in G} (a*H)$

$a \in \bigcup_{a \in G} a*H \Rightarrow G \subseteq \bigcup_{a \in G} (a*H) \rightarrow (4)$

From (3) and (4), $G = \bigcup_{a \in G} (a*H)$

$\therefore$ The group G is the union of distinct left cosets of H.

If G is a finite group then G has a finite number of distinct left cosets of H such that $G = \bigcup_{a \in G} a*H$.

ie) $G = a_1 * H \cup a_2 * H \cup \cdots \cup a_k * H$

where $a_1 * H, a_2 * H, \ldots, a_k * H$ are the distinct left cosets of H.

$\therefore$ The set of all distinct left cosets of H is a partition π of the group G.

Note:

The number of elements in any left coset of a subgroup H is the same as the number of elements of H.

Lagrange's theorem:

The order of a subgroup of a finite group is a divisor of the order of the group. (or)

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, a subgroup of G with order, $O(H) = m$.

We have to show that m divides n.

Since H contains m distinct elements, every left coset of H contains exactly m elements. We know that any two left cosets of H are either identical or disjoint and the collection of distinct left cosets of H is the group G.

Since G is a finite group, G has a finite number of distinct left cosets of H.

Let $a_1*H, a_2*H, \ldots, a_k*H$ be the distinct left cosets of H.

Then $G = a_1*H \cup a_2*H \cup \ldots \cup a_k*H$

$\Rightarrow O(G) = O(a_1*H) + O(a_2*H) + \ldots + O(a_k*H)$

$= O(H) + O(H) + \ldots + O(H)$ (k elements)

$= m + m + \ldots + m$ (k times)

$n = mk$

$\Rightarrow \frac{n}{m} = k$

$\therefore$ m divides n.

This means that $O(H)$ divides $O(G)$.

Hence the proof.

Note: The converse of the above theorem is not true.

Example:

Consider the symmetric group $(S_4, \circ)$ of degree 4.

Order of $S_4 = 4! = 24$

A_4 is the alternative group of even permutations whose order is given by $O(A_4) = \frac{4!}{2} = 12$

But there is no subgroup of A_4 with order 6 eventhough 6 divides 12.

Normal subgroup

Definition:

A subgroup $(H, *)$ of a group $(G, *)$ is called a normal subgroup of G iff $a * H = H * a \ \forall a \in G$ (ie) Every left coset of H is identical with the right coset of H.

Theorem:

A subgroup $(H, *)$ of a group $(G, *)$ is a normal subgroup iff $g * H * g^{-1} \subseteq H$ for $g \in G$.

Proof:

Let $g * H * g^{-1} \subseteq H$

This means that for any $g \in G$

$g * h * g^{-1} = h_1$ for $h, h_1 \in H$

$\Rightarrow g * h = h_1 * g$

$\therefore g * h \in H * g$

$\therefore g * H \subseteq H * g \rightarrow (1)$

Again $g * H * g^{-1} \subseteq H$ gives

$g * h * g^{-1} = h_1$ for some $h, h_1 \in H$

$\Rightarrow g * h = h_1 * g$

ie) $h_1 * g = g * h$

$\therefore h_1 * g \in g * H$

$\Rightarrow H * g \subseteq g * H \rightarrow (2)$

From (1) and (2), $g * H = H * g$

$\therefore$ H is a normal subgroup.

Conversely, assume that H is a normal subgroup of G.

Then $g * H = H * g$ for $g \in G$

$\Rightarrow g * h = h_1 * g$ for some $h, h_1 \in H$

$\Rightarrow g * h * g^{-1} = h_1$.

$\therefore g * h * g^{-1} \in H$

This shows that $g * H * g^{-1} \subseteq H$.

Examples:

1) Prove that the intersection of two normal subgroups is also a normal subgroup.

Solution:

Let H and K be two normal subgroup of the group $(G, *)$

To prove: $H \cap K$ is a normal subgroup.

Let $x \in H \cap K$

$\Rightarrow x \in H$ and $x \in K$

Since H is normal, $g*x*g^{-1} \in H$ for some $g \in G$.

Also since K is normal, $g*x*g^{-1} \in K$ for $g \in G$.

$\therefore g*x*g^{-1} \in H \cap K$

For $x \in H \cap K$, $g \in G$, we have $g*x*g^{-1} \in H \cap K$.

$\therefore H \cap K$ is a normal subgroup.

Hence the intersection of two normal subgroups is also a normal subgroup.

2) show that every subgroup of a cyclic group of normal.

proof:

Let $G = \langle a \rangle$, be a cyclic group generated by the element $a \in G$.

Let H be a proper subgroup of G. Therefore the elements of H are integral powers of the element a.

If $a^{s} \in H$, then $a^{-s} \in H$.

$\therefore$ H contains both positive and negative powers of the element a.

Let m be the least positive integer such that $a^m \in H$.

Then H is a cyclic group generated by the element a^m.

$\therefore$ Every element $a^t \in H$ is expressed in the form $(a^m)^q$.

To show that H is normal subgroup, let $g \in G$ and $h \in G$.

Then $h = (a^m)^K$ for some integer K.

Consider $g*h*g^{-1}$

$$= g*(a^m)^K*g^{-1}$$

$$= g*(a^K)^m*g^{-1}$$

$$= (g*a^K*g^{-1})*(g*a^K*g^{-1})* \cdots (g*a^K*g^{-1}) \text{ (m times)}$$

$\therefore g*h*g^{-1} = (g*a^K*g^{-1})^m$

Since a is a generator of G, $g*a^K*g^{-1} = a^s$ [g is expressed as power of a]

$$\therefore g*a^K*g^{-1} = (a^s)^m$$

$$= (a^m)^s$$

$\therefore g*h*g^{-1} \in H$ for some $g \in G$ and $h \in G$.

This implies that H is a normal subgroup of G.

Every subgroup of a cyclic group is normal.

Ring:

A non-empty set R with two binary operations '+' and '.' (addition and multiplication) is called a ring if the following conditions are satisfied.

(1) $(R, +)$ is an abelian group

(2) $(R, \cdot)$ is a semigroup

(3) The operation multiplication is distributive over addition.

i.e) $\forall a, b, c \in R$ $a\cdot(b+c) = (a\cdot b) + (a\cdot c)$ and

$$(a+b)\cdot c = (a\cdot c) + (b\cdot c)$$

Note:

The identity element w.r.to + is $0 \in R$.

The inverse of $a \in R$ w.r.to + is $-a \in R$

The multiplicative identity in a ring is denoted by the symbol $I \in R$.

Types of Rings

Ring with unity

If in a ring R, $\exists$ an element denoted by 1 such that. $1\cdot a = a\cdot 1 = a$ $\forall a \in R$, then R is called a ring with unit element.

The element $1 \in R$ is called the unit element of the ring.

Clearly $1 \in R$ is the multiplicative identity.

$\therefore$ A ring possesses multiplicative identity is a ring with unity.

commutative ring:

If in a ring R, the multiplication operation is also commutative

i.e) $a \cdot b = b \cdot a \; \forall a, b \in R$.

then R is called a commutative ring.

properties of a ring:

If R is a ring $\forall a, b, c \in R$, we have

i) $a \cdot 0 = 0 \cdot a = 0$

ii) $a(-b) = (-a)b = -ab$

iii) $(-a)(-b) = ab$

iv) $a(b-c) = ab - ac$

v) $(b-c)a = ba - ca$.

Example:

Show that the set of all even integers is a commutative ring under usual addition and multiplication is defined by $a * b = \frac{ab}{2}, \forall a, b \in R$.

Solution:

R, the set of even integers is closed for the usual addition

The operation addition is clearly associative in R.

i.e) $(a+b)+c = a+(b+c) \; \forall a, b, c \in R$.

$0 \in R$ is the identity element.

For every $a \in R$, the inverse element $-a \in R$ such that

$a + (-a) = 0 = (-a) + a, \; \forall a \in R$.

Further, $a+b = b+a, \; \forall a, b \in R$

$\therefore (R, +)$ is an abelian group.

Multiplication operation defined by $a * b = \frac{ab}{2}, \forall a, b \in R$

Then $(a*b)*c = \left(\frac{ab}{2}\right) * c = \frac{abc}{4}$

$a*(b*c) = a*\left(\frac{bc}{2}\right) = \frac{abc}{4}$

$\therefore a*(b*c) = (a*b)*c, \; \forall a, b, c \in R$

$\therefore (R, *)$ is a semigroup.

Further $a*b = \frac{ab}{2} = \frac{ba}{2} = b*a$

$\therefore$ $*$ is commutative in R.

Consider $a*(b+c) = \frac{a(b+c)}{2} = \frac{ab}{2} + \frac{ac}{2} = \cancel{a*b+a*c}$

$= a*b + a*c$

Also $(a+b)*c = \frac{(a+b)c}{2} = \frac{ac}{2} + \frac{bc}{2} = a*c + b*c$

$\therefore$ The operation $*$ is distributive over $+$.

For $a \in R$, we have $a*2 = \frac{a}{2} \times 2 = a$

$2*a = 2 \times \frac{a}{2} = a$

$a*2 = 2*a = a, \forall a \in R$

$\therefore$ $2 \in R$ is the multiplicative identity w.r.to $*$.

$\therefore$ $(R, +, *)$ is a commutative ring with unity.

Boolean Ring

Definition:

An element a of a ring R is said to be idempotent if $a^2 = a$.

A ring R is called a Boolean ring if $a^2 = a \; \forall \; a \in R$.

$\therefore$ A Boolean ring consists of elements all are idempotent.

Examples of rings:

Rings of Integers

Consider the set of integers. Then I is a commutative ring with unit element for the binary operations '+' and '·' where + is the usual addition and '·' is the usual multiplication.

Example for a non-commutative ring:

$M_2(R)$ - set of all 2×2 real matrices

$(M_2(R), +, \circ)$ is a non-commutative ring with unity, where unit element is the identity matrix.

Zero divisors:

Let R be a ring. A non-zero element, $a \in R$ is called a zero divisor if $\exists$ an element $b \neq 0 \in R$ such that $a \cdot b = 0$ or $b \cdot a = 0$.

ie) For $a \neq 0$, $b \neq 0$, $ab = 0$ or $ba = 0$ then b is called a zero divisor of a.

Ring without zero divisors:

A ring R is a without zero divisor if the product of no two nonzero-elements of R is 0 (ie) if $ab = 0 \Rightarrow a = 0, b = 0$.

Example:

In the ring $(Z_6, +_6, \times_6)$ the elements 2 and 3 are zero divisors since $2 \times_6 3 = 0$ and $3 \times_6 2 = 0$.

Ring with zero divisors:

If in a ring R, there exists non-zero elements a and b such that $ab = 0$ then R is said to be a ring with zero divisors.

Theorem:

A ring R is without zero divisors iff the cancellation laws hold in R.

Proof:

Suppose if R has no zero divisors, Let a, b, c be any three elements of a ring R such that $a \neq 0$, $ab = ac$.

We have $ab = ac$,

$\Rightarrow ab - ac = 0$

$\therefore a(b-c) = 0$

$\therefore$ R has no zero divisors, $a(b-c) = 0$ and $a \neq 0$

$\Rightarrow b - c = 0$

$b = c$

Hence, $ab = ac \Rightarrow b = c$.

$\therefore$ Left cancellation law holds in R.

Similarly, we show that the right cancellation law holds in R.

Conversely, suppose that the cancellation law hold in R.

If possible, let $ab = 0, a \neq 0, b \neq 0$

Then we have $ab = 0 \Rightarrow ab = a \cdot 0$

Since $a \neq 0$ by cancellation law $b = 0$.

$\therefore ab = 0 \Rightarrow a \neq 0$ but $b = 0$

This is a contradiction.

Hence R is without zero divisors.

Integral Domain

Definition:

A commutative ring $(R, +, \cdot)$ with identity having no zero divisor is called an integral domain.

ie) A ring $(R, +, \cdot)$ is said to be an integral domain if

(i) R is commutative ie) $ab = ba$.

(ii) R has multiplicative identity

(iii) For $a \neq 0, b \neq 0, a \cdot b \neq 0$.

Field:

Definition:

A ring R with atleast two elements is called a field if

(i) R is commutative

(ii) R has the multiplicative identity

(iii) Every non-zero element of R has multiplicative inverse in R.

Equivalent definition:

A non-empty set F with atleast two elements is called a field with two binary operations '+' and '·' defined on it if

(i) $(F, +)$ is an abelian group

ii) $(F - \{0\})$ is an abelian group

iii) Multiplication '·' is distributive over addition '+'.

ii) $a \cdot (b+c) = (a \cdot b) + (a \cdot c)$
$(a+b) \cdot c = (a \cdot c) + (b \cdot c)$ $\Big\}$ $\forall\, a, b, c \in F$.

Example:

The ring of integers $(\mathbb{Z}, +, \cdot)$ is an integral domain but not a field.

Important facts:

1) Every field is an integral domain.

2) Every finite integral domain is a field.

3) A finite commutative ring without zero divisors is a field.

Normal Subgroup:

If $f:(G,*) \to (G_1,\circ)$ is a group homomorphism then Kernel of f is a normal subgroup of G.

proof:

We know that Kernel of $f = \{x \in G \mid f(x) = e_1$, where e_1 is the Identity element of $G_1\}$

clearly $e \in \ker f$, so $\ker f$ is non empty.

Let $a, b \in \ker f$, $f(a) = e_1$ and $f(b) = e_1$

Consider $f(a*b^{-1}) = f(a) \circ f(b^{-1}) = f(a) \circ (f(b))^{-1}$
$= e_1 * e_1^{-1} = e_1$

$\therefore a*b^{-1} \in \ker f$.

For $a, b \in \ker f$, $a*b^{-1} \in \ker f$

$\therefore \ker f$ is a subgroup of G.

To prove: $\ker f$ is a normal subgroup of G.

Let $g \in G$ and $x \in \ker f$.

To prove: $g*x*g^{-1} \in \ker f$

consider
$$\begin{aligned} f(g*x*g^{-1}) &= f(g) \circ f(x*g^{-1}) \\ &= f(g) \circ f(x) \circ f(g^{-1}) \\ &= f(g) \circ e_1 \circ (f(g))^{-1} \\ &= f(g) \circ (f(g))^{-1} = e_1 \end{aligned}$$

$\therefore g*x*g^{-1} \in \ker f$ for $g \in G$ and $x \in \ker f$

$\therefore \ker f$ is a normal subgroup of G.

Semigroup:

Example:

1) Show that the set of rational numbers Q is a semigroup for the operation $*$ defined by $a*b = a+b-ab$.

Soln:

Q is closed for $*$

$a*(b*c) = a*(b+c-bc) = a+b+c-bc-a(b+c-bc)$
$= a+b+c-ab-bc-ac+abc. \rightarrow (1)$

$(a*b)*c = (a+b-ab)*c = a+b-ab+c-(a+b-ab)c$
$= a+b+c-ab-bc-ac+abc \rightarrow (2)$

From (1) and (2), $a*(b*c) = (a*b)*c, \forall a,b,c \in Q$

$\therefore$ $*$ is associative.

$\therefore$ $(Q,*)$ is a semigroup.

(2) Show that the set of rational numbers Q is a semigroup for the operation $*$ defined by $a*b = \frac{ab}{2} \forall a,b \in Q$.

Soln:

Q is closed for $*$

$a*(b*c) = a*\left(\frac{bc}{2}\right) = \frac{abc}{4}$

$(a*b)*c = \left(\frac{ab}{2}\right)*c = \frac{abc}{4}$

$(a*b)*c = a*(b*c) \forall a,b,c \in Q$

$\therefore$ $*$ is associative

$\therefore$ $(Q,*)$ is a semigroup.

Abelian group:

Show that $[\{1,2,3,4\}, X_5]$ is an abelian group.

Soln: $Z_5^* = \{1,2,3,4\}$

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

$a \times_5 b$ = remainder when ab is divisible by 5.

$1 \in Z_5^*$ is the identity element

The inverse of 1 is 1, The inverse of 2 is 3, The inverse of 3 is 2, the inverse of 4 is 4

Further $a \times_5 b = b \times_5 a$, $\forall a, b \in Z_5^*$

$\therefore [\{1, 2, 3, 4\}, \times_5]$ is an abelian group.

Abelian group:

1) Show that $(Q^+, *)$ is an abelian group where $*$ is defined by $a*b = \frac{ab}{2}$, $\forall a, b \in Q^+$.

Soln:

1) Closure property: Clearly $a*b = \frac{ab}{2} \in Q^+$

2) Associative property:

$(a*b)*c = \frac{ab}{2} * c = \frac{abc}{4} \rightarrow (1)$

$a*(b*c) = a * \frac{bc}{2} = \frac{abc}{4} \rightarrow (2)$

From (1) & (2), $(a*b)*c = a*(b*c)$ $\forall a, b \in Q^+$

(3) Identity: Let e be the identity element

Then $a*e = a$

$\Rightarrow \frac{ae}{2} = a$

$\Rightarrow e = 2$

$\therefore$ Identity element is $e = 2 \in Q^+$

(4) Inverse: Let a^{-1} be the inverse of a

Then $a * a^{-1} = 2$

$\Rightarrow \frac{aa^{-1}}{2} = 2 \Rightarrow a^{-1} = 4/a \in Q^+$

$\therefore$ Inverse of a is $a^{-1} = 4/a \in Q^+$.

(5) Commutative: Now $a * b = ab/2$

$b * a = ba/2 = \frac{ab}{2}$

$\therefore a * b = b * a \ \forall a, b \in Q^+$

$\therefore (Q^+, *)$ is an abelian group.

Properties of Group:

Let G be a group. If $a, b \in G$, then $(a*b)^{-1} = b^{-1} * a^{-1}$.

proof:

Let $a, b \in G$ and a^{-1}, b^{-1} be their inverses respectively.

$a * a^{-1} = e$ and $a^{-1} * a = e$

$b * b^{-1} = e$ and $b^{-1} * b = e$.

$(a*b) * (b^{-1} * a^{-1}) = a * (b * (b^{-1} * a^{-1}))$

$= a * [(b * b^{-1}) * a^{-1}]$

$= a * [e * a^{-1}] = a * a^{-1} = e$

$(a*b) * (b^{-1} * a^{-1}) = e \rightarrow (1)$

Similarly we can prove that $(b^{-1} * a^{-1}) * (a * b) = e \rightarrow (2)$

From (1) and (2), $(a*b)^{-1} = b^{-1} * a^{-1}$.

Fundamental theorem on Group homomorphism:

Let $f: G \rightarrow G'$ be an onto homomorphism of groups with kernel K

Then $\frac{G}{K} \simeq G'$.

Proof:

Let f be a homomorphism $f: G \rightarrow G'$

Let G' be the homomorphic image of the group G.

Let K be the kernel of this homomorphism

clearly K is a normal subgroup of G.

Define $\phi : G/K \to G'$ by $\phi(K*a) = f(a),\ \forall a \in G$.

ϕ is well defined:

We have $K*a = K*b$

$\Rightarrow a*b^{-1} \in K$

$\Rightarrow f(a*b^{-1}) = e'$ (e' is the identity in G').

$\Rightarrow f(a)*f(b^{-1}) = e'$

$\Rightarrow f(a)*(f(b))^{-1} = e'$

$\Rightarrow f(a)*(f(b))^{-1}*f(b) = e'*f(b)$

$\Rightarrow f(a) = f(b)$

$\Rightarrow \phi(K*a) = \phi(K*b)$

$\therefore$ ϕ is well defined.

ϕ is one-one

To prove: $\phi(K*a) = \phi(K*b) \Rightarrow K*a = K*b$

$\phi(K*a) = \phi(K*b)$

$\rightarrow f(a) = f(b)$

$\Rightarrow f(a)*f(b^{-1}) = f(b)*f(b^{-1})$

$= f(b*b^{-1})$

$= f(e)$

$\Rightarrow f(a)*f(b^{-1}) = e'$

$\Rightarrow f(a*b^{-1}) = e'$

$\Rightarrow a*b^{-1} \in K$

$\Rightarrow K*a = K*b$.

$\therefore$ ϕ is one-one.

ϕ is onto:

Let $y \in G'$

Since f is onto, there exists $a \in G$ such that $f(a) = y$

Hence $\phi(K*a) = f(a) = y$

$\therefore$ ϕ is onto.

ϕ is a homomorphism:

~~Since ϕ is 1-1, θ~~

Now
$$\phi(K * a * K * b) = \phi(K * a * b)$$
$$= f(a * b)$$
$$= f(a) * f(b)$$
$$= \phi(K * a) * \phi(K * b).$$

$\therefore$ ϕ is a homomorphism

Since ϕ is 1-1, onto and homomorphism, ϕ is an isomorphism between G/K and G'.

$\therefore$ $G/K \approx G'$.

Lattices and Boolean Algebra

Partial order relation:

A relation R on a set A is said to be a partial order relation if R is reflexive, antisymmetric and transitive.

Example:

Let N be the set of all natural numbers. prove that the relation R in N defined by $aRb \Rightarrow a$ divides b is a partial order relation.

Soln:

i) Reflexive:

$aRa,\ \forall a \in N$ since every natural number divides itself.

ii) Anti-Symmetric:

Let aRb and bRa

a divides b and b divides a. This is possible only when $a=b$.

iii) Transitive:

Let aRb and bRc ie) a divides b and b divides c.

$\therefore$ There exists natural numbers m and n such that

$b=ma$ and $c=nb$.

$\therefore c=nb \Rightarrow c=n(ma) = (nm)a$

$\therefore$ a divides c and so aRc.

$\Rightarrow R$ is transitive.

Hence R is a partial order relation.

poset (partially ordered set):

A set P together with a partial order relation $\leq$ on it is called a partially ordered set or poset and it is denoted by $(P, \leq)$.

(eg) Let R be the set of real numbers. The relation "less than or equal to" or "$\leq$" is a partial order relation on R. Therefore $(R, \leq)$ is a poset.

Comparability:

The elements a and b in a poset $(P, \leq)$ are called comparable if either $a \leq b$ or $b \leq a$.

If a and b are the elements of P, such that neither $a \leq b$ nor $b \leq a$, then a and b are called incomparable.

Example:

In the poset $(Z^+, /)$ the integers 3 and 6 are comparable while 3 and 5 are incomparable.

Totally ordered set (or) Linearly ordered set:

If every two elements of a poset $(P, \leq)$ are comparable, then P is called a totally ordered set or linearly ordered set and the relation $\leq$ is called a total order or linear order.

Example:

The poset $(Z, \leq)$ is a totally ordered set whereas the poset $(Z^+, /)$ is not totally ordered.

Note:

The totally ordered set is also called a chain.

Well ordered set:

A poset $(P, \leq)$ is called a well ordered set if it is a totally ordered set and every non-empty subset of P has a least element.

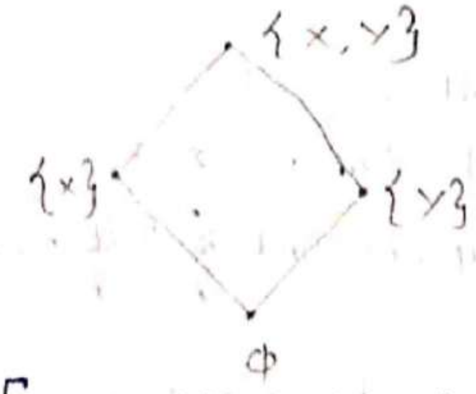
Hasse diagram:

Example 1:

1) Draw the Hasse diagram for the following:

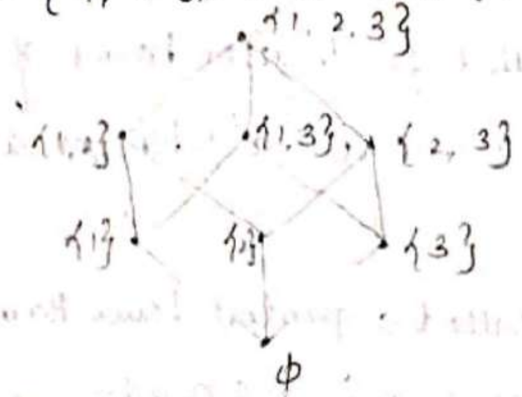
i) $[P(A), \subseteq]$ where $A = \{x, y\}$

$P(A) = \{\phi, \{x\}, \{y\}, A\}$.



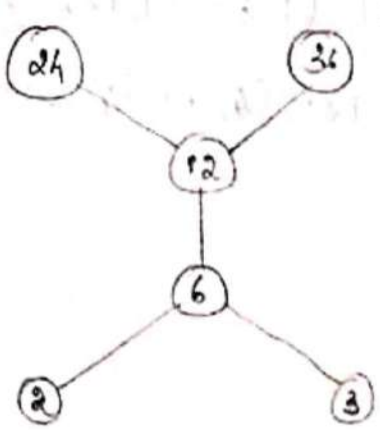
ii) $[P(A), \subseteq]$, where $A = \{1, 2, 3\}$

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



iii) If $X = \{2, 3, 6, 12, 24, 36\}$ and the relation R defined on X by $R = \{\langle a, b\rangle \mid a \mid b\}$. Draw the Hasse diagram for $\langle X, R\rangle$

The relation $R = \{\langle 2,6\rangle, \langle 2,12\rangle, \langle 2,24\rangle, \langle 2,36\rangle, \langle 3,6\rangle,$
$\langle 3,12\rangle, \langle 3,24\rangle, \langle 3,36\rangle, \langle 6,12\rangle, \langle 6,24\rangle,$
$\langle 6,36\rangle, \langle 12,24\rangle, \langle 12,36\rangle\}$



Greatest element and Least element:

An element $a \in A$ is called the greatest element of A if $x \leq a \ \forall x \in A$.

An element $a \in A$ is called a least element of A if $a \leq x \ \forall x \in A$.

Upper Bound and Lower Bound of a set:

Consider a poset $(A, \leq)$ and a subset B of A.

The element $a \in A$ is called a upper Bound of B if $b \leq a$ for every $b \in B$.

The element $a \in A$ is called a lower bound of B if $a \leq b \ \forall b \in B$.

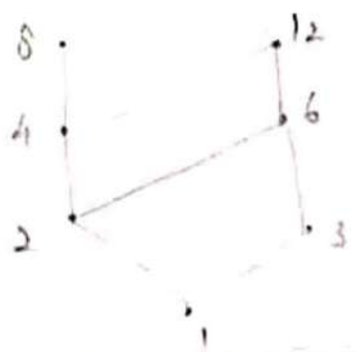
Least upper Bound (LUB) & Greatest Lower Bound (GLB).

An element $a \in A$ is called Least upper Bound of B if 'a' is an upper Bound of B and $a \leq a'$ whenever a' is an upper Bound of B.

An element $a \in A$ is called a greatest Lower Bound of B if a is a lower bound of B and $a' \leq a$ whenever a' is a lower bound of B.

Draw Hasse diagram for $\{(a, b) / a \text{ divides } b\}$ on
(1) $\{1, 2, 3, 4, 6, 8, 12\}$ (2) $\{1, 2, 3, 4, 6, 12\}$.

(1) The relation R is
$R = \{(1, 2), (1, 3), (1, 4), (1, 6), (1, 8), (1, 12), (2, 4), (2, 6), (2, 8), (2, 12), (3, 6), (3, 12), (4, 8), (4, 12), (6, 12)\}$



(2) The relation R is

$R = \{(1,2), (1,3), (1,4), (1,6), (1,12), (2,4), (2,6), (2,12), (3,6), (3,12), (4,12), (6,12)\}$

Lattice:

A lattice is a poset $(L, \leq)$ in which every pair of elements a and $b \in L$ has a LUB and GLB in L.

Note:

$A = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

1) GLB$\{a, b\}$ is denoted by $a * b$, which is pronounced as "a meet b" or "a product b".

$B = \{4, 5, 6\}$

$UB(B) = \{6, 7, 8, 9, 10\}$

$LUB(B) = 6$

$$GLB\{a, b\} = a * b \text{ or } a \wedge b \text{ or } a \cdot b$$

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

2) LUB$\{a, b\}$ is denoted by $a \oplus b$, which is pronounced as "a join b" or "a sum b".

$GLB(B) = \{4\}$

$$LUB\{a, b\} = a \oplus b \text{ or } a \vee b \text{ or } a + b.$$

Properties of Lattice:

Let $(L, \wedge, \vee)$ be a given lattice. Then $\wedge$ and $\vee$ satisfies the following conditions, $\forall a, b, c \in L$,

1) Idempotent Law:

Let $(L, \wedge, \vee)$ be a given lattice. Then $a \vee a = a$ and $a \wedge a = a$

Proof: $a \vee a = LUB(a, a) = a$

$\therefore a \vee a = a$

Now, $a \wedge a = GLB(a, a) = a$

$\therefore a \wedge a = a$.

2) Commutative law:

Let $(L, \wedge, \vee)$ be a given lattice. Then for any $a, b \in L$,

$a \vee b = b \vee a$ and $a \wedge b = b \wedge a$.

Proof: $a \vee b = LUB(a, b) = LUB(b, a) = b \vee a$

$\therefore a \vee b = b \vee a$

$a \wedge b = GLB(a, b) = GLB(b, a) = b \wedge a$

$\therefore a \wedge b = b \wedge a$

3) Associative law:

Let $(L, \wedge, \vee)$ be a given Lattice. Then for any $a, b, c \in L$

$a \vee (b \vee c) = (a \vee b) \vee c$ and $a \wedge (b \wedge c) = (a \wedge b) \wedge c$.

proof:

Let $a \vee (b \vee c) = d \rightarrow (1)$ and $(a \vee b) \vee c = e \rightarrow (2)$

$(1) \Rightarrow d$ is LUB of $(a, b \vee c)$

$\Rightarrow d \geq a$ and $d \geq b \vee c \rightarrow (3)$

$B = \{4, 5, 6\}$

$5 \vee 6 = 6$

We know that $b \vee c$ is the LUB of (b, c)

$4 \vee 6 = 6 \rightarrow d$

$\Rightarrow b \vee c \geq b$ and $b \vee c \geq c \rightarrow (4)$

$6 \geq 4, \; 6 \geq 6$

$6 \geq 5, \; 6 \geq 6$

From (3) and (4), we have $d \geq a$, $d \geq b$ and $d \geq c \rightarrow (5)$

From (5), d is an UB of (a, b) and $d \geq c$

$\Rightarrow d \geq a \vee b$ and $d \geq c$

$\Rightarrow d$ is an UB of $(a \vee b, c) \rightarrow (6)$

From (2) e is the LUB of $(a \vee b, c) \rightarrow (7)$

From (6) and (7) $d \geq e$

Similarly we can easily prove that $e \geq d$

$\therefore d = e$

$\therefore a \vee (b \vee c) = (a \vee b) \vee c$

proceeding similarly, we can easily prove $a \wedge (b \wedge c) = (a \wedge b) \wedge c$

4) Absorption Law:

Let $(L, \wedge, \vee)$ be a given Lattice. Then for any $a, b, c \in L$,

$a \vee (a \wedge b) = a$ and $a \wedge (a \vee b) = a$.

Proof:

GLB

Since $a \wedge b$ is the LUB of $\{a, b\}$, we have

$$a \wedge b \leq a \rightarrow (1)$$

Obviously $a \leq a \rightarrow (2)$

From (1) and (2), $a \vee (a \wedge b) \leq a \rightarrow (3)$

By the definition of LUB, we have

$$a \leq a \vee (a \wedge b) \rightarrow (4)$$

From (3) and (4), $a \vee (a \wedge b) = a$.

Similarly, we can prove $a \wedge (a \vee b) = a$.

Theorem 1:

Let $(L, \wedge, \vee)$ be a lattice in which $\wedge$ and $\vee$ denote the operation of meet and join respectively.

For any $a, b \in L$, $a \leq b \Leftrightarrow a \vee b = b \Leftrightarrow a \wedge b = a$

Proof:

(i) $\Rightarrow$ (ii)

Let $a \leq b$

Also $b \leq b$, by the definition of $a \vee b$, we have

$$a \vee b \leq b \rightarrow (1)$$

Since $a \vee b$ is the LUB of $\{a, b\}$, we have

$$b \leq a \vee b \rightarrow (2)$$

From (1) and (2), we have $a \vee b = b$.

(ii) $\Rightarrow$ (iii)

Let $a \vee b = b$

Now $a \wedge b = a \wedge (a \vee b) = a$ (by absorption Law)

$\Rightarrow a \wedge b = a$.

(iii) $\Rightarrow$ (i)

Let $a \wedge b = a$

Then Lower bound of $\{a, b\} = a$, which implies $a \leq b$.

Distributive Lattice:

A lattice L is called distributive lattice if for $a, b, c \in L$,

$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$; $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ (or)

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

Prove that every chain is a distributive lattice:

proof:

Let $(L, \leq)$ be a chain (every pair of elements are comparable).

Let $a, b, c \in L$

Case (i) Suppose that $a \leq b$ or $a \leq c$ then $a \leq b \vee c$

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

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

$\therefore$ $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$.

The distributive law holds.

Case (ii) Suppose that $a \geq b$ or $a \geq c$ so that $b \vee c \leq a$

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

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

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

Using principle of duality in both cases, the other form of distributive law $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$ also holds good.

$\therefore$ Every chain is a distributive lattice.

Theorem:

Let $(L, \leq)$ be a distributive lattice. Then $a \vee b = a \vee c$ and $a \wedge b = a \wedge c \Rightarrow b = c$.

proof:

Now $= b \vee (b \wedge a)$ (Absorption Law)

$= b \vee (a \wedge b)$ (Commutative Law)

$= b \vee (a \wedge c)$ (By Given condition)

$= (b \vee a) \wedge (b \vee c)$ (Distributive Law)

$= (a \vee b) \wedge (b \vee c)$ (Commutative Law)

$= (a \vee c) \wedge (b \vee c)$ (By Given condition)

$= (c \vee a) \wedge (c \vee b)$ (Commutative Law)

$= c \vee (a \wedge b)$ (Distributive Law)

$= c \vee (a \wedge c)$ (By Given condition)

$= c \vee (c \wedge a)$ (Commutative Law)

$= c$ (Absorption Law).

Modular Lattice:

A lattice $(L, \wedge, \vee)$ is said to be modular if it satisfies the condition if $a \leq c$ then $a \vee (b \wedge c) = (a \vee b) \wedge c$ $\forall a, b, c \in L$.

Theorem:

Every distributive lattice is modular.

proof:

Let $(L, \leq)$ be a distributive Lattice.

$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$ and $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$.

Also Let $a \leq c$.

To prove: $a \vee (b \wedge c) = (a \vee b) \wedge c$, $\forall a, b, c \in L$.

Since $a \le c$, we have $a \vee c = c$.

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

$\therefore$ Every distributive lattice is modular.

Theorem:

Every chain is modular.

proof:

The proof of this theorem is proof of

i) Every chain is a distributive lattice.

ii) Every distributive lattice is modular.

Complete lattice:

A lattice L is called complete lattice if each of its non-empty subset has GLB & LUB. Every finite lattice must be a complete lattice.

Bounded lattice:

A lattice L is called bounded if it has both LB & UB.

If L is a bounded lattice then $\forall a \in L$, $0 \le a \le 1$, $a \vee 0 = a$, $a \wedge 0 = 0$, $a \vee 1 = 1$, $a \wedge 1 = a$.

Complement of an element:

Let L be a bounded lattice with LB = 0 and UB = 1. Let $a \in L$. The element $x \in L$ is called the complement of $a \in L$ if $a \wedge x = 0$ and $a \vee x = 1$.

Complemented lattice:

A lattice L is said to be complemented if it is bounded and every element in it has atleast one complement.

Theorem:

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

$a \wedge b = 0, a \vee b = 1, a \wedge c = 0, a \vee c = 1$

$$
\begin{aligned}
b &= b \wedge 1 \\
&= b \wedge (a \vee c) \\
&= (b \wedge a) \vee (b \wedge c) \quad [\text{Distributive Law}] \\
&= (a \wedge b) \vee (b \wedge c) \quad [\text{commutative Law}] \\
&= 0 \vee (b \wedge c) \\
&= (a \wedge c) \vee (b \wedge c) \\
&= (a \vee b) \wedge c \\
&= 1 \wedge c \\
&= c \wedge 1 \\
&= c.
\end{aligned}
$$

Theorem:

State and prove Demorgan's Laws of Lattice

Proof: Let L be a bounded Lattice. The Demorgan's Laws are given by $(a \wedge b)' = a' \vee b'$ and $(a \vee b)' = a' \wedge b'$.

Let $a, b \in L$ and a' and b' be the complements of a and b respectively. Then $a \wedge a' = 0$, $a \vee a' = 1$

$b \wedge b' = 0$, $b \vee b' = 1$

To prove : i) $(a \wedge b)' = a' \vee b'$

For this we have to prove that (i) $(a \wedge b) \wedge (a' \vee b') = 0$

(ii) $(a \wedge b) \vee (a' \vee b') = 1$

Consider $(a \wedge b) \wedge (a' \vee b')$

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

$= (0 \wedge b) \vee (a \wedge 0)$

$= 0 \vee 0$

$= 0$

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

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

$= (1 \vee b') \wedge (1 \vee a')$

$= 1 \wedge 1$

$= 1$

To prove: $(a \vee b)' = a' \wedge b'$.

For this we have to prove that i) $(a \vee b) \wedge (a' \wedge b') = 0$

ii) $(a \vee b) \vee (a' \wedge b') = 1$.

Consider $(a \vee b) \wedge (a' \wedge b')$

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

$= (0 \wedge b') \vee (0 \wedge a')$

$= 0 \vee 0 = 0$.

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

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

$= (1 \vee b) \wedge (a \vee 1)$

$= 1 \wedge 1$

$= 1$

Hence the proof.

Theorem:

Show that in a complemented distributive lattice,

$a \leq b \Leftrightarrow a * b' = 0 \Leftrightarrow a' \oplus b = 1 \Leftrightarrow b' \leq a'$.

proof:

Let $(L, *, \oplus)$ be a complemented distributive lattice.

Let $a, b \in L$ and a' and b' be the complements of a and b respectively. Then $a \wedge a' = 0$, $a \vee a' = 1$, $b \wedge b' = 0$, $b \vee b' = 1$.

(i) $\Rightarrow$ (ii)

Let $a \leq b$

$\therefore a \wedge b = a$, $a \vee b = b$.

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

$\therefore\ a \oplus b = b$

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

$\Rightarrow (a * b') \oplus (b * b') = 0$

$\Rightarrow (a * b') \oplus 0 = 0$

$\Rightarrow a * b' = 0$.

(ii) $\Rightarrow$ (iii)

Let $a * b' = 0$

Taking complement on both sides

$(a * b')' = 0'$

$\Rightarrow a' \oplus (b')' = 1$

$\Rightarrow a' \oplus b = 1$

(iii) $\Rightarrow$ (iv)

Let $a' \oplus b = 1$

$(a' \oplus b) * b' = 1 * b'$

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

$\Rightarrow (a' * b') \oplus 0 = b'$

$\Rightarrow a' * b' = b'$

$\Rightarrow b' \leq a'$

(iv) $\Rightarrow$ (i)

Let $b' \leq a'$

$\therefore\ b' * a' = b',\ b' \oplus a' = a'$

$\Rightarrow (b' * a')' = (b')'$

$\Rightarrow (b')' \oplus (a')' = b$

$\Rightarrow b \oplus a = b$

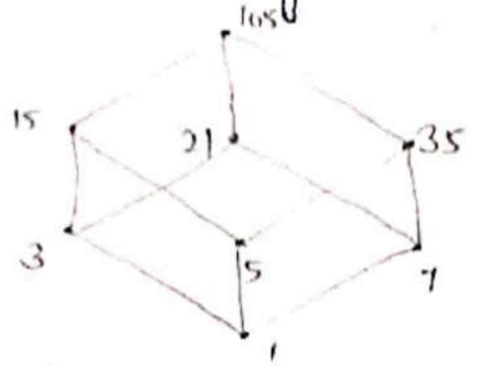
$\Rightarrow a \oplus b = b$

$\Rightarrow a \leq b$.

Hence the proof.

1) Consider the lattice D_{105} with the partial ordered relation divides, then

1) Draw the Hasse diagram of D_{105}



2) Find the complement of each element of D_{105}

1 - 105, 3 - 35, 5 - 21, 7 - 15 and the reverse order complements.

3) Find the set of atoms of D_{105}

Set of atoms of $D_{105} = \{3, 5, 7\}$

4) Find the number of subalgebras of D_{105}

Sub algebra with 2 elements = $\{1, 105\}$

Sub algebra with 4 elements = $\{1, 3, 35, 105\}$, $\{1, 5, 21, 105\}$, $\{1, 7, 15, 105\}$

Sub algebra with 8 elements = $\{1, 3, 5, 7, 15, 21, 35, 105\}$

No of subalgebras = 5.

2) Let $D_{30} = \{1, 2, 3, 5, 6, 10, 15, 30\}$ and R be the relation "divides" on D_{30}. Find

(1) All the lower bounds of 10 and 15

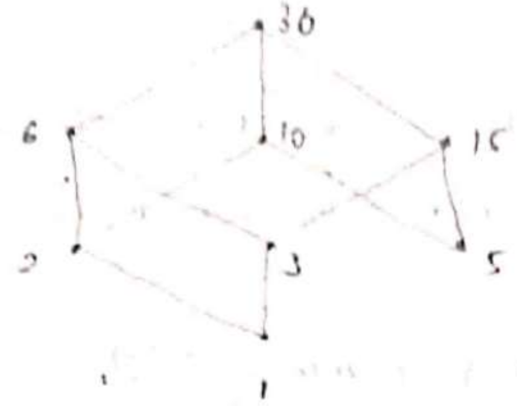
1, 5.

(2) The GLB of 10 and 15 : 5

(3) All the upper bounds of 10 and 15 : 30

(4) The LUB of 10 and 15 : 30.

(5) Draw the Hasse diagram:



Boolean Algebra:

A Boolean algebra is a complemented distributive lattice.

A Boolean algebra $(B, *, \oplus, 0, 1)$ satisfies the following properties $\forall\, a, b, c \in B$..

1) $a \oplus a = a, \quad a * a = a$.

2) $a \oplus b = b \oplus a, \; a * b = b * a$ Commutative Law

3) $\left.\begin{array}{l}(a \oplus b) \oplus c = a \oplus (b \oplus c) \\ (a * b) * c = a * (b * c)\end{array}\right\}$ Associative Law

(4) $a * (a \oplus b) = a, \; a \oplus (a * b) = a$

$(B, *, \oplus)$ is a distributive lattice and so satisfies

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

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

3) $a * b = a * c, \; a \oplus b = a \oplus c \Rightarrow b = c$.

$(B, *, \oplus, 0, 1)$ is a bounded lattice in which for any $a \in B$, we have $0 \le a \le 1$, $a * 0 = 0$, $a * 1 = a$, $a \oplus 0 = a$, $a \oplus 1 = 1$

$(B, *, \oplus, 0, 1)$ is a complemented lattice, $\forall\, a \in B$, there exists $a' \in B$ such that $a * a' = 0$, $a \oplus a' = 1$,

$0' = 1, \quad 1' = 0$.

Problem:

If $P(S)$ is the power set of a non-empty set S, prove that $(P(S), \cup, \cap, \phi, S)$ is a Boolean Algebra.

Soln:

Let X, Y, Z be any 3 elements of $P(S)$.

Clearly $X \cup \phi = X$, $X \cap S = X$, $X \cap \phi = \phi$, $X \cup S = S$.

ϕ and S are the identities (0 and 1) and the identity laws are satisfied.

$X \cup Y = Y \cup X$ and $X \cap Y = Y \cap X$, $\forall X, Y \in P(S)$.

$\therefore$ Commutative laws are satisfied.

$X \cup (Y \cup Z) = (X \cup Y) \cup Z$ and

$X \cap (Y \cap Z) = (X \cap Y) \cap Z$, $\forall X, Y, Z \in P(S)$

$\therefore$ Associative Law is also satisfied.

Also $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$

$X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$

$\therefore$ The distributive Law also holds.

The complement of the set X is $X' = S - X$

Further $X \cup X' = S$ and $X \cap X' = \phi$. The complement Law also hold.

Hence $\{P(S), \cup, \cap, \phi, S\}$ is a Boolean Algebra.

Theorem:

In a Boolean Algebra, prove the Demorgan's Law.

Proof:

Let $(B, \oplus, *)$ be a Boolean Algebra. The Demorgan's Laws are $(a \oplus b)' = a' * b'$

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

Lattice Homomorphism:

Let $(L_1, \wedge, \vee)$ and $(L_2, \otimes, \oplus)$ be two given lattices.

A mapping $f: L_1 \to L_2$ is called homomorphism if $\forall\, a, b \in L$

i) $f(a \wedge b) = f(a) \ast f(b)$

ii) $f(a \vee b) = f(a) \oplus f(b)$.

A Homomorphism which is also 1 to 1 is called an isomorphism.

A mapping $f: L_1 \to L_2$ is said to be order preserving from $(L_1, \leq)$ to $(L_2, \leq)$ if $a \leq b \Rightarrow f(a) \leq f(b)$, $\forall\, a, b \in L$.

Theorem:

Prove that any lattice Homomorphism is order preserving

proof:

Let $f: L_1 \to L_2$ be a homomorphism.

Let $a, b \in L$ and also let $a \leq b$.

$\therefore$ GLB$\{a, b\} = a$, LUB$\{a, b\} = b$. ie) $a \wedge b = a$, $a \vee b = a$

Now $f(a \wedge b) = f(a)$

$f(a) \wedge f(b) = f(a)$

$\therefore$ GLB$\{f(a), f(b)\} = f(a)$

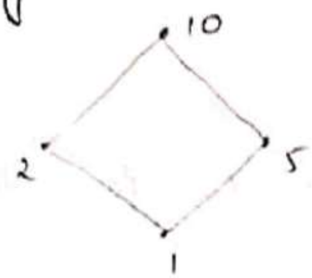
$\therefore f(a) \leq f(b)$

$\therefore a \leq b \Rightarrow f(a) \leq f(b)$

$\therefore f$ is order preserving.

Part - A.

1) Let $A = \{1, 2, 5, 10\}$ with the relation divides. Draw the Hasse diagram.



2) prove that a lattice with five elements is not a Boolean Algebra.

Soln:

A Boolean algebra must contain 2^n elements.

Since $5 \neq 2^n$ for any n, a lattice with 5 elements is not a Boolean algebra.

3) State modular inequality of lattices.

Let $(L, \wedge, \vee)$ be a lattice. Then $\forall\ a, b, c \in L$

modular inequality states that $a \leq b \Rightarrow a \vee (b \wedge c) = (a \vee b) \wedge c$

4) Let $X = \{1, 2, 3, 4, 5, 6\}$ and R be the relation defined as $\langle x, y \rangle \in R$ if and only if $x-y$ is divisible by 3. Find the elements of the relation R.

$R = \{\langle 1, 4\rangle, \langle 1, 1\rangle, \langle 2, 5\rangle, \langle 2, 2\rangle, \langle 3, 3\rangle, \langle 3, 6\rangle,$
$\langle 4, 4\rangle, \langle 4, 1\rangle, \langle 5, 5\rangle, \langle 5, 2\rangle, \langle 6, 3\rangle, \langle 6, 6\rangle\}.$

5) Show that the absorption laws are valid in Boolean algebra.

Soln: $a \oplus a = a, \quad a * a = a.$