Unit I

LOGIC AND PROOFS

1.1 INTRODUCTION

PROPOSITION (OR) STATEMENT:

Proposition is a declarative statement that is either true or false but not both. The truth value of proposition is true or false.

Truth table

It displays the relationship between the truth values of proposition.

Negation of a proposition

If P is a proposition, then its negation is denoted by ¬P or ~p and is defined by the following truth table.

P	¬P
T	F
F	T

EXAMPLE

P - Ram is intelligent

¬P -Ram is not intelligent

proposition is a declarative sentence which is either true or false but not both.

COMPOUND PROPOSITION

It is a proposition consisting of two or more simple proposition using logical operators.

1.2 LOGICAL CONNECTIVES

(1) DISJUNCTION (OR)

The disjunction of two proposition P and Q is the proposition P∨Q [read as P or Q] and is defined by the following truth table.

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

(1) CONJUNCTION (AND)

If P and Q are two propositions , then the conjunction of P and Q is denoted by P∧Q (read as P and Q) and is defined by following truth table.

P	Q	P∧Q
T	T	T
T	F	F
F	T	F
F	F	F

CONDITIONAL AND BI- CONDITIONAL PROPOSITION

(1) Conditional proposition

If p and q are propositions, then the implication "If p then q " denoted by p→q , called the conditional statement of p and q , is defined by following truth table.

p	q	p→q
T	T	T
T	F	F
F	T	T
F	F	T

NOTE

p→q is false when p is true and q is false. Otherwise it is true.

The different situations where the conditional statements applied are listed below.

(1) If p then q
(2) p only if q
(3) q whenever p
(4) q is necessary for p
(5) q follows from p
(6) q when p
(7) p is sufficient for q
(8) p implies q

Converse, contrapositive and Inverse statement

If p→q is a conditional statement, then

(1) q→p is called converse of p→q
(2) ¬q→¬p is called contrapositive of p→q
(3) ¬p→¬q is called inverse of p→q

EXAMPLE

q : Ram study DBMS

p→q: If Ram is a computer science student, then he will study DBMS.

(2) Bi-conditional proposition

If p and q are proposition, then the proposition p if and only if q, denoted by $p \leftrightarrow q$is called the bi-conditional statement and is defined by the following truth table.

p	q	
T	T	T
T	F	F
F	T	F
F	F	T

NOTE

$P \leftrightarrow Q$is true if both p and q have same truth values. Otherwise $P \leftrightarrow Q$ is false.

EXAMPLE

P: You can take the flight

q: You buy a ticket

p↔q: You can take the flight if and only if buy a ticket.

Symbolize the statements using Logical Connectives

Example: 1

The automated reply can be sent when the file system is full.

P: The automated reply can be sent

Q: The file system is full

Solution:

Symbolic form :q→¬ p

EXAMPLE: 2

Write the symbolized form of the statement. If either Ram takes C++ or Kumar takes pascal, then Latha will take Lotus.

R:Ram takes C++

K:Kumar takes Pascal

L:Latha takes Lotus

Symbolic form: $(R \vee K) \rightarrow L$

Example 3

Let p,q,r represent the following propositions,

P:It is raining

q: The sun is shining

r: There are clouds in the sky

Symbolize the following statements.

(1) If it is raining, then there are clouds in the sky
(2) If it is not raining, then the sun is not shining and there are clouds in the sky.
(3) The sun is shining if and only if it is not raining.

Solution:

Symbolic form:

(1) $p \rightarrow r$
(2) $\neg p \rightarrow (\neg q \wedge r)$
(3) $q \leftrightarrow \neg r$

Example: 4

Symbolize the following statements:

(1) If the moon is out and it is not snowing, then Ram goes out for a walk.
(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.

Solution:

Let the propositions be,

P: The moon is out

Q: It is snowing

R: Ram goes out for a walk.

Symbolic form:

(1) $(p \wedge \neg q) \rightarrow r$
(2) $p \rightarrow (\neg q \rightarrow r)$
(3) $\neg(r \leftrightarrow (\neg q \vee p))$

Example: 5

propositions.

P:I finish writing my computer program before lunch.

q: I shall play Tennis in afternoon.

r: The sun is shining

s: The boundary is low.

(1) If the sun is shining, I shall play tennis in the afternoon.
(2) Finishing the writing of my computer program before lunch is necessary for playing tennis in this afternoon.
(3) Low boundary and sunshine are sufficient to play Tennis in this afternoon.

Solution:

Symbolic form:

(1) $r \rightarrow q$
(2) $q \rightarrow p$
(3) $(s \wedge r) \rightarrow q$

Construction of Truth Tables

EXAMPLE: 1

Show that the truth values of the formula $P \wedge (P \rightarrow Q) \rightarrow Q$ are independent of their components.

Solution:

The truth table for the formula is,

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

The truth values of the given formula are all true for every possible truth values of P and Q. Therefore, the truth value of the given formula is independent of their components.

Example 1. Without constructing the truth table show that

$p \rightarrow (q \rightarrow p) \equiv \neg p(p \rightarrow q)$

Solution

$p \rightarrow (q \rightarrow p) \equiv p \rightarrow (\neg q \vee p)$

$\equiv \neg p \vee (\neg q \vee p)$

$\neg q)$

$\equiv (\neg p \vee p) \vee \neg q$

$\equiv T \vee \neg q$

$\equiv T.$

Example 2. Prove that $p \rightarrow q$ is logically prove that $(\neg p \vee q)$

Solution:

p	q	$p \rightarrow q$	$\neg p \vee \vee q$
T	T	T	T
T	F	F	F
F	T	T	T
F	F	T	T

EXAMPLE: 2

Write the symbolized form of the statement. If either Ram takes C++ or Kumar takes pascal, then Latha will take Lotus.

R:Ram takes C++

K:Kumar takes Pascal

L:Latha takes Lotus

Solution:

Symbolic form: $(R \vee K) \rightarrow L$

Tautology.

A statement that is true for all possible values of its propositional variables is called a tautology universely valid formula or a logical truth.

Example:1. Write the converse, inverse, contra positive of 'If you work hard then you will be rewarded'

Solution:

p: you will be work hard.

q: you will be rewarded.

$\neg p$: You will not be work hard.

$\neg q$: You will no tbe rewarded.

Converse: $q \rightarrow p$, If you will be rewarded then you will be work hard

Contrapositive: $\neg q \rightarrow p$,if You will not be rewarded then You will not be work hard.

Inverse: $\neg p \rightarrow \neg q$, if You will not be work hard then You will no tbe rewarded.

Example:2. Write the converse, inverse, contra positive of 'If you work hard then you will be rewarded'

Solution:

p: you will be work hard.
q: you will be rewarded.
¬p: You will not be work hard.
¬ q: You will no tbe rewarded.
Converse: q→ p, If you will be rewarded then you will be work hard
Contrapositive: ¬ q→ p,if You will not be rewarded then You will not be work hard.
Inverse: ¬ p→ ¬ q, if You will not be work hard then You will no tbe rewarded.

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

Proof:

Let S: $(P \rightarrow Q) \wedge (Q \rightarrow R) \rightarrow (P \rightarrow R)$

To prove: S is a tautology

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

The last column shows that S is a tautology

1.3 PROPOSITIONAL EQUIVALENCE:

Logical Equivalence:

Let p and q be two statements formulas, p is said to be logically equivalent to q if p & q have the same set of truth values or equivalently p & q are logically equivalent if $p \leftrightarrow q$ is tautology.

Hence, $p \Leftrightarrow q$ if and only if $p \leftrightarrow q$ is a tautology.

Logical Implication or Tautological Implication

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

$\therefore A \Rightarrow B$ [A logically iff $A \rightarrow B$ is tautology, implies B]

If $A \Rightarrow B$, then

B is called consequent.

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

∴ In order to show any of the given implications, it is sufficient to show that an assignment of the truth value T to the antecedent of the given conditional leads to the truth value T for the consequent.

1. Prove without using truth table $(P \rightarrow Q) \wedge \neg Q \Rightarrow \neg P$

Proof:

Antecedent: $(P \rightarrow Q) \wedge \neg Q$

Consequent: $\neg P$

Assume that, the antecedent has the truth value T.

∴ $\neg Q$ And $(P \rightarrow Q)$ both are true.

⇒ Truth value of Q is F and the truth value of P is also F.

∴ Consequent $\neg P$ is true.

∴ The truth of the antecedent implies the truth of the consequent.

$$\therefore (P \rightarrow Q) \wedge \neg Q \Rightarrow \neg P$$

Example:1Without constructing the truth table show that $p \rightarrow (q \rightarrow p) \equiv \neg p(p \rightarrow q)$

Solution

$p \rightarrow (q \rightarrow p) \equiv p \rightarrow (\neg q \vee p)$

$\equiv \neg p \vee (\neg q \vee p)$

$\equiv \neg p \vee (p \vee \neg q)$

$\equiv (\neg p \vee p) \vee \neg q$

$\equiv T \vee \neg q$

$\equiv T.$

Example 2:Show that $\neg (p \leftrightarrow q) \equiv (p \vee q) \wedge \neg (p \wedge q)$ without constructing the truth table

Solution :

$\neg (p \leftrightarrow q) \equiv (p \vee q) \wedge \neg (p \wedge q)$

$\neg (p \leftrightarrow q) \equiv \neg (p \rightarrow q) \wedge (q \rightarrow p)$

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

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

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

$\equiv \neg(\neg p \vee q) \vee F \vee F \vee (q \wedge p)$

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

$\equiv (p \vee q) \wedge (q \wedge p).$

Consider $(\neg P \wedge \neg Q) \vee (\neg P \wedge \neg R) \Rightarrow \neg(P \vee Q) \vee \neg(P \vee R) \Rightarrow \neg((P \vee Q) \wedge (P \vee R))$ (2)

Using (1) and (2)

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

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

Prove the following equivalences by proving the equivalences of the dual

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

Solution: It"s dual is

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

Consider,

$\neg((\neg P \vee Q) \wedge (\neg P \vee \neg Q)) \wedge (P \vee Q) \equiv P$	**Reasons**
$\Rightarrow ((P \wedge \neg Q) \vee (P \wedge Q)) \wedge (P \vee Q)$	(Demorgan"s law)
$\Rightarrow ((Q \wedge P) \vee (\neg Q \wedge P)) \wedge (P \vee Q)$	(Commutative law) (Distributive law)
$\Rightarrow ((Q \vee \neg Q) \wedge P) \wedge (P \vee Q)$	$(P \vee \neg P \Rightarrow T)$
$\Rightarrow (T \wedge P) \wedge (P \vee Q)$	$(P \wedge T = P)$ (Absorption law)

Obtain DNF of $Q \vee (P \wedge R) \wedge \neg((P \vee R) \wedge Q)$.
Solution:

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

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

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

(Extended distributed law)

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

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

Obtain Pcnf and Pdnf of the formula $(\neg P \vee \neg Q) \rightarrow (P \leftrightarrow \neg Q)$

Solution:

Let S = $(\neg P \vee \neg Q) \rightarrow (P \leftrightarrow \neg Q)$

P	Q	$\neg$ P	$\neg$ Q	$\neg P \vee \neg Q$	$P \leftrightarrow \neg Q$	S	Minterm	Maxterm
T	T	F	F	F	F	T	$P \wedge Q$	
T	F	F	T	T	T	T	$P \wedge \neg Q$	
F	T	T	F	T	T	T	$\neg P \wedge Q$	
F	F	T	T	T	F	F		$P \vee Q$

PCNF: $P \vee Q$ and PDNF: $(P \wedge Q) \vee (P \wedge \neg Q) \vee (\neg P \wedge Q)$

Obtain PDNF of $P \rightarrow (P \wedge (Q \rightarrow P))$.

Solution:

$P \rightarrow (P \wedge (Q \rightarrow P)) \Leftrightarrow \sim P \vee (P \wedge (\sim Q \vee P))$

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

$\Leftrightarrow (\sim P \wedge T) \vee (P \wedge \sim Q) \vee (P \wedge P)$

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

$\Leftrightarrow$ (

$\Leftrightarrow$ (~

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

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

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

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

1.4 PREDICATES & QUANTIFIERS:

Quantifiers.

Universal Quantifiers:

The universal Quantification of P(x) is the proposition."P(x) is true for all values of x in the universe of discourse".

The notation ¥x P(x) denotes the universal quantification of P(x).here ¥ is called the universal quantifier.

Existential Quantifier:

The existential Quantification of P(x) is the proposition." There exists an element x in the universe of discourse such that P(x) is true".

We use the notation ∃x P(x) for the existential quantification of p(x).here ∃ is called the existential quantifier.

Normal Forms:

DNF:

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

PDNF: a formula which is equivalent to a given formula which is consists of sum its minterms is called PDNF.

PCNF: a formula which is equivalent to a given formula which consists of product of maxterms is called PCNF.

Obtain PCNF of (¬ p→ r) ∧(q↔ p). and hence obtain its PDNF.

Solution:

PCNF:

$S \Leftrightarrow (\neg p \rightarrow r) \wedge (q \leftrightarrow p)$.

→ p).

$\wedge (p \rightarrow q)$

$\Leftrightarrow (p \vee r) \wedge ((\neg q \vee p). \wedge (\neg p \vee q)$

$\Leftrightarrow ((p \vee r) \vee F) \wedge ((\neg q \vee p). \vee F) \wedge ((\neg p \vee q) \vee F)$

$\Leftrightarrow ((p \vee r) \vee (q \wedge \neg q)) \wedge ((\neg q \vee p). \vee (r \wedge \neg r)) \wedge ((\neg p \vee q) \vee (p \wedge \neg p))$.

$\Leftrightarrow ((p \vee r \vee q) \wedge (p \vee r \vee \neg q)) \wedge ((\neg q \vee p \vee r) \wedge .(\neg q \vee p \vee \neg r) \wedge ((\neg p \vee q \vee r) \vee (\neg p \vee q \vee \neg r)$

$\Leftrightarrow ((p \vee r \vee q) \wedge ((\neg q \vee p \vee r) \wedge .(\neg q \vee p \vee \neg r) \wedge ((\neg p \vee q \vee r) \vee (\neg p \vee q \vee \neg r)$

PCNF of S: $((p \vee r \vee q) \wedge ((\neg q \vee p \vee r) \wedge .(\neg q \vee p \vee \neg r) \wedge ((\neg p \vee q \vee r) \vee (\neg p \vee q \vee \neg r)$

PCNF of $\neg$ S: $(p \vee q \vee r) \wedge (\neg p \vee \neg q \vee r|\ ) \wedge (\neg p \vee \neg q \vee \neg r)$

PDNF of S: $(p \wedge q \wedge r) \vee (\neg p \wedge \neg q \wedge r) \vee (\neg p \vee \wedge \neg q \wedge \neg r)$.

1.5 RULES OF INFERENCE:

EXAMPLE:1 Verify that validating of the following inference. If one person is more successful than another, then he has worked harder to deserve success. Ram has not worked harder than Siva. Therefore, Ram is not more successful than Siva.

Solution:

Let the universe consists of all persons.

Let S(x,y): x is more successful than y.

H(x,y): x has worked harder than y to deserve success.

a: Ram

b: Siva

Then, given set of premises are

1) (x) (y) [S(x,y) $\rightarrow$ H(x,y)]

2) ¬ H(a,b)

3) Conslution is ¬ S(a,b).

{1}	1) (x) (y) [S(x,y) → H(x,y)]	Rule P
{2}	2) (y) [S(a,y) → H(a,y)]	Rule US
{3}	3) [S(a,b) → H(a,b)]	Rule US
{4}	4) ¬ H(a,b)	Rule P
{5}	5) ¬ S(a,b)	Rule T (¬ P, P →Q ⇒ ¬ Q)

EXAMPLE: 2Show that (x) (H(x) →M(x)) ∧ H(s) ⇒ $M(s)$

Solution :

Steps	Premises	Rule	Reason
1	(x) (H(x) →M(x))	P	Given premise
2	H(s) →M(s)	US (1)	(Vx) p (x) ⇒ $p(y)$
3	H(s)	P	Given premise
4	M(s)	T	(2) (3) (p → q, p ⇒ q)

EXAMPLE: 3 Show that ¬ p(a,b) follows logically from (x) (y) (p(x,y) →w(x,y)) and $\neg w(a, b)$

Solution :

1.	(x) (y) (p(x,y) → w(x,y)	p
2.	(y), p(a,y) → w(a,y)	US, (1)
3.	P(a,b) → w(a,b)	US (2)
4.	$\neg w(a,b)$	p Given
5.	$\neg p(a,b)$	T (3),(4), (p→ Q) ∧ ¬ Q⇒ ¬p

EXAMPLE:4.

Symbolise: For every x, these exixts a y such that $x^2+y^2 \geq 100$

Solution :

$(\forall x)\ (\exists y\ )\ (x^2+y^2 \geq 100)$

Example:Let p, q, r be the following statements:

p: I will study discrete mathematics q: I will watch T.V.

r: I am in a good mood.

Write the following statements in terms of p, q, r and logical connectives. (1) If I do not study and I watch T.V., then I am in good mood.

(2) If I am in good mood, then I will study or I will watch T.V.

(3) If I am not in good mood, then I will not watch T.V. or I will study.

$(1)\ (\neg p \wedge q) \rightarrow r$

$(2)\ r \rightarrow (p \vee q)$

$(3)\ \neg r \rightarrow (\neg q \vee p)$

1.6 Introduction to proofs & statergy

Method of proofs :

Trival proof:

In an implication $p \rightarrow q$, if we can establish that q is true , then regardless of the truth value of p, the implication $p \rightarrow q$ So the construction of a trivial proof of $p \rightarrow q$ needs to show that the truth value of q is true.

Vacous proof:

If the hypothesis p of an implication $p \rightarrow q$ is false , then $p \rightarrow q$ is true for any proposition q.

Prove that $\sqrt{2}$ is irrational.

Solution :

Suppose $\sqrt{2}$ is irrational.

$\therefore \sqrt{2} = \frac{p}{q}$ for p,q $\in z, q \neq 0, p \& q$ have no common divisor.

$\therefore \frac{p^2}{q^2} = 2 \Rightarrow p^2 = 2q^2$.

Since p^2 is an even integer, p is an even integer.

$\therefore$ p= 2m for some integer m.

$\therefore (2m)^2 = 2q^2 \Rightarrow q^2 = 2m^2$

Since q^2 is an even integer, q is an even integer.

$\therefore$ q= 2k f or some integer k.

Thus p & q are even . Hence they have a common factor 2. Which is a contradiction to our assumption.

$\therefore \sqrt{2}$ is irrational.

UNIT II COMBINATORICS

Pigeon Hole Principle:

If (n=1) pigeon occupies ‘n’ holes then atleast one hole has more than 1 pigeon.
Proof:
Assume (n+1) pigeon occupies ‘n’ holes.
Claim: Atleast one hole has more than one pigeon.
Suppose not, ie. Atleast one hole has not more than one pigeon.
Therefore, each and every hole has exactly one pigeon.
Since, there are ‘n’ holes, which implies, we have totally ‘n’ pigeon.
Which is a $\Rightarrow \Leftarrow$ to our assumption that there are (n+1) pigeon.
Therefore, atleast one hole has more than 1 pigeon.

2.1 MATHEMATICAL INDUCTION

EXAMPLE 1:show that

SOLUTION: $\frac{1}{1.2} + \frac{1}{2.3} + \ldots\ldots + \frac{1}{n(n+1)} = \frac{n}{n+1}$

Let P(n) : $\frac{1}{1.2} + \frac{1}{2.3} + \ldots\ldots + \frac{1}{n(n+1)}$

1.P(1): $\frac{1}{1.2} = \frac{1}{1(1+1)}$ is true.

2.ASSUME

P(k): $\frac{1}{1.2} + \frac{1}{2.3} + \ldots\ldots + \frac{1}{k(k+1)}$

$= \frac{k}{k+1}$ is true. -> (1)

CLAIM : P(k+1) is true.

P(k+1) = $\frac{1}{1.2} + \frac{1}{2.3} + \ldots\ldots + \frac{1}{k(k+1)} + \frac{1}{(k+1)(k+2)}$

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

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

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

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

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

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

P(k+1) is true.

BY THE PRINCIPLE OF MATHEMATICAL INDUCTION

$\frac{1}{1.2} + \frac{1}{2.3} + \ldots\ldots + \frac{1}{n(n+1)} = \frac{n}{n+1}$ Is true for all n .

EXAMPLE 2 : Using mathematical induction prove that if

n>=1, then 1.1! + 2.2! +3.3! +……+n.n! = (n+1)! - 1

SOLUTION:

Let p(n) : 1.1! + 2.2! +3.3! +……+n.n! = (n+1)! - 1

1.P(1) : 1.1! = (1+1)! – 1 is true

2 . ASSUME p(k) : 1.1! + 2.2! +3.3! +……+k.k!

= (k+1)! – 1 is true

CLAIM : p(k+1) is true.

P(k+1) = 1.1! + 2.2! +3.3! +……+k.k! +(k+1)(k+1)!

= (k+1)!-1 +(k+1)(k+1)!

= (k+1)! [(1+k+1)] – 1

= (k+1)! (k+2) – 1

= (k+2) ! – 1

= [(k+1) + 1]! - 1

P(k+1)is true.

BY THE PRINCIPLE OF MATHEMATICAL INDUCTION,

P(n) : 1.1! + 2.2! +3.3! +……+n.n! = (n+1)! – 1 , n>=1

EXAMPLE 3 : Use mathematical induction , prove that $\sum^{n}_{m=0} 3^m = \frac{(3\wedge n+1)-1}{2}$

SOLUTION:

Let p(n): $3^0 + 3^1 + \ldots\ldots\ldots 3^n = \frac{(3\wedge n+1)-1}{2}$

1.p(0) : $3^0 = \frac{(3\wedge 0+1)-1}{2} = \frac{2}{2} = 1$ is true .

2.ASSUME

P(k):): $3^0 + 3^1 + \ldots\ldots\ldots 3^n = \frac{(3\wedge k+1)-1}{2}$ is true.

CLAIM : p(k+1)is true.

P (k+1) :): $3^0 + 3^1 + 3^2 + \ldots\ldots\ldots + 3^k + 3^{k+1}$

$= \frac{(3\wedge k+1)-1}{2} + 3^{k+1}$ using (1)

$= \frac{(3\wedge k+1)+2.(3\wedge k+1)-1}{2}$

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

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

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

P(k+1)is true.

By the principle of mathematical induction.

P(n): $\sum^{n}_{m=0} 3^{m} = \frac{(3\wedge n+1)-1}{2}$ is true for n>=0

EXAMPLE 4 :Use mathematical induction , prove that $\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \ldots + \frac{1}{\sqrt{n}} > \sqrt{n}$, n>=2

SOLUTION:

Let p(n): $\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \ldots + \frac{1}{\sqrt{n}} > \sqrt{n}$, n>=2

1.p(2): that $\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}}$ = (1.707) > $\sqrt{2}$ + (1.414) is true

2.ASSUME

P(k): that $\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \ldots + \frac{1}{\sqrt{k}} > \sqrt{k}$ is true -> (1)

CLAIM : p(k+1) is true.

P(k+1) : $\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \ldots + \frac{1}{\sqrt{k}} + \frac{1}{\sqrt{k+1}}$

$\sqrt{k} + \frac{1}{\sqrt{k+1}}$ using (1)

$\frac{\sqrt{k}\sqrt{k+1}+1}{\sqrt{k+1}}$

$\frac{\sqrt{k(k+1)}+1}{\sqrt{k+1}}$

$> \frac{\sqrt{k.k}+1}{\sqrt{k+1}}$

$> \frac{k+1}{\sqrt{k+1}}$

$> \sqrt{k+1}$

P(k+1) $> \sqrt{k+1}$

P(K+1) is true

BY THE PRINCIPLE OF MATHEMATICAL INDUCTION.

that $\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \ldots + \frac{1}{\sqrt{n}} > \sqrt{n+1}$

EXAMPLE 5: Using mathematical induction ,prove that $1^2 + 3^2 + 5^2 + \ldots\ldots (2n-1)^2 = \frac{n(2n-1)(2n+1)}{3}$

SOLUTION :

Let p(n): $1^2 + 3^2 + 5^2 + \ldots\ldots (2n-1)^2 = \frac{1}{3} n(2n-1)(2n+1)$

1.p(1): $1^2 = \frac{1}{3} 1(2-1)(2+1) = \frac{1}{3} . 3$

=1 is true.

2.ASSUME p(k)is true.

$1^2 + 3^2 + 5^2 + \ldots\ldots (2k-1)^2 = \frac{1}{3} n(2k-1)(2k+1)$ -> (1) Is true.

CLAIM : p(k+1) is true.

P (k+1) = $\frac{1}{3}$ k (2k-1) (2k+1) +$(2k+1)^2$ using (1)

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

= $\frac{1}{3}$ (2k+1) (2k2+5k+3)

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

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

P(k+1) is true .

BY THE PRINCIPLE OF MATHEMATICAL INDUCTION,

P(n) = $1^2 + 3^2 + 5^2 + \ldots\ldots (2n-1)^2 = \frac{n(2n-1)(2n+1)}{3}$

EXAMPLE 6:Use mathematical induction to show that $n^3 - n$ is divisible by 3. For n Ɛ Z^+

SOLUTION:

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

1. p(1): $1^3 - 1$ is divisible by 3,is true.
2. ASSUME p(k): $k^3 - k$ is divisible by 3. -> (1)

CLAIM : p(k+1) is true .

P (k+1): $(k+1)^3 - (k+1)$

= $k^3 +3k^2 + 3k+1 - k-1$

$= (k^3-k) + 3(k^2+k)$ ->(2)

(1) => $k^3 - k$ Is divisible by 3 and $3(k^2 + k)$ is divisible by 3 ,we have equation (2) is divisibleby 3

Therefore P(k+1) is true.

By the principle of mathematical induction , $n^3 - n$ is divisible by 3.

2.2 Strong Induction

There is another form of mathematics induction that is often useful in proofs.In this form we use the basis step as before, but we use a different inductive step. We assume that p(j)is true for j=1…,k and show that p(k+1)must also be true based on this assumption . This is called strong Induction (and sometimes also known as the second principles of mathematical induction).

We summarize the two steps used to show that p(n)is true for all positive integers n.

Basis Step : The proposition P(1) is shown to be true

Inductive Step: It is shown that

$[P(1) \wedge P(2) \wedge \ldots\ldots \wedge P(k)] \rightarrow P(k+1)$

NOTE:

The two forms of mathematical induction are equivalent that is, each can be shown to be valid proof technique by assuming the other

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

SOLUTION:

Let P(n) be the proportion 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

Inductive Step: Assume that P(j) is positive for all integer j with j<=k. To complete the Inductive Step, it must be shown that P(k+1) is trueunder the assumption.

There are two cases to consider namely

i) When (k+1) is prime
ii) When (k+1) is composite

Case 1 : If (k+1) is prime, we immediately see that P(k+1) is true.

Case 2: If (k+1) is composite

Then it can be written as the product of two positive integers a and b with 2<=a<b<=k+1. By the Innduction hypothesis, both a and b can be written as the product of primes, namely those primes in the factorization of a and those in the factorization of b .

The Well-Ordering Property:

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

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

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

Problem :

What is wrong with this “Proof” by strong induction ?

Theorem :

For every non negative integer n, 5n = 0

Proof:

Basis Step: 5 – 0 = 0

Inductive Step: Suppose that 5j = 0 for all non negative integers j with o<=j<=k. Write k+1 = i+j where I and j are natural numbers less than k+1. By the induction hypothesis

5(k+1) = 5(i+j) = 5i + 5j = 0+ 0 =0

Example 1:

Among any group of 367 people, there must be atleast 2 with same birthday, because there are only 366 possible birthdays.

Example 2:

In any group of 27 English words, there must be at least two, that begins with the same letter, since there are only 26 letters in English alphabet

Example 3:

Show that among 100 people , at least 9 of them were born in the same month

Solution :

Here, No of Pigeon = m = No of People = 100

No of Holes = n = No of Month = 12

Then by generalized pigeon hole principle

{[100-1]/12}+1 = 9, were born in the same month

Combinations:

Each of the difference groups of sections which can be made by taking some or all of a number of things at a time is called a combinations.

The number of combinations of 'n' things taken 'r' as a time means the number as groups of 'r' things which can be formed from the 'n' things.

It denoted by nCr.

The value of nCr :

Each combination consists /r/ difference things which can be arranged among themselves in r! Ways. Hence the number of arrangement for all the combination is nCr x r! . This is equal to the permulations of 'n' difference things taken 'r' as a time.

nCr x r! =n P r

nCr = n P r / r! ----------→(A)

= n (n-1) , (n-2).....(n-r+1) / 1,2,3,.....r

Cor 1 : nPr = n! / (n-r)! --------→(B)

Substituting (B) in (A) we get

nCr = n! / (n-r)!r!

Cor 2: To prove that nCr = nCn-r

Proof :

nCr = n! / r!(n-r)! ----------→(1)

nCn-r = n! / (n-r)! [n-(n-r)]!

= n! / (n-r) ! r! ----------→(2)

From 1 and 2 we get

nCr=nCn-r

Example :

$30C_{28} = 30\ C_{30-28}$

$=30\ C_2$

30 x 29 / 1x2

Example 2:

In how many can 5 persons be selected from amongs 10 persons ?

Sol :

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

=10x9x8x7x6 / 1x2x3x4x5

= 9 x 28 ways.

Example 5 :

How many ways are there to from a commitiee , if the consists of 3 educanalis and 4 socialist if there are 9 educanalists and 11 socialists.

Sol : The 3 educanalist can be choosen from a educanalist in 9C3 ways. The 4 socialist can be choosen from 11 socialist in 11C4 ways.

∴. By products rule , the number of ways to select the commitiee is

$=9C_3.11C_4$

= 9! / 3! 6! . 11! / 4! 7!

= 84 x 330

27720 ways.

Example 6 :

1. A team of 11 players is so be chosen from 15 members. In how ways can this be done if

i. One particular player is always included.

ii. Two such player have always to be included.

Sol : Let one player be fixed the remaining players are 14 . Out of these 14 players we have to select 10 players in $14C_{10}$ ways.

$14C_4$ ways. [.`. $nCr = nC_{n-r}$]

➔ 14x13x12x11 / 1x2x3x4

➔1001 ways.

2. Let 2 players be fixed. The remaining players are 13. Out of these players we have to select a players in $13C_9$ ways.

$13C_4$ ways [.`. $nC_r = nC_{n-r}$]

➔13x12x11x10 / 1x2x3x4 ways

➔715 ways.

Example 9 :

Find the value of 'r' if $20C_r = 20_{Cr-2}$

Sol : Given $20\ C_r = 20C_{20-(r-2)}$ ➔r=20-(r+2) ----------→(1)

(1)-----→ r=20 - r – 2

2r = 18

r = 9

Example 12 :

From a commitiee consisting of 6 men and 7 women in how many ways can be select a committee of

(1) 3men and 4 women.
(2) 4 members which has atleast one women.
(3) 4 persons of both sexes.
(4) 4 person in which Mr. And Mrs kannan is not included.

Sol :

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

.`. By product rule the committee of 3 men and 4 women can be selected in

$$6C_3 \times 7C_4 \text{ ways} = \frac{6x5x4x}{1x2x3} \times \frac{7x6x5x4}{1x2x3x4}$$

=700 ways.

(b) For the committee of atleast one women we have the following possibilities

1. 1 women and 3 men
2. 2 women and 2 men
3. 3 women and 1 men
4. 4 women and 0 men

There fore the selection can be done in

$= 7C_1 \times 6C_3 + 7C_2 \times 6C_2 + 7C_3 \times 6C_1 + 7C_4 \times 6C_6$ ways

$= 7x20+21x15+35x6+35x1$

$=140x315x210x35$

$=700$ ways.

(d) For the committee of bath sexes we have the following possibilities .

1. 1 men and 3 women
2. 2 men and 2 women
3. 3 men and 1 women

Which can be done in

$=6C_1x7C_3+6C_2x7C_2+6C_3x7C_1$

$=6x35+15x21+20x7$

$=210+315+140$

$=665$ ways.

Sol : (1) 4 balls of any colour can be chosen from 11 balls (6+5) in $11C_4$ ways.

$=330$ ways.

(2) The 2 white balls can be chosen in $6C_2$ ways. The 2 red balls can be chosen in $5C_2$ ways. Number of ways selecting 4 balls 2 must be red.

$=6C_2 + 5C_2$

$$= \frac{6x5}{1 \times 2} + \frac{5x4}{1 \times 2}$$

$$=15 + 10$$

$$=25 \text{ ways.}$$

Number of ways selecting 4 balls and all Of same colour is $= {}^6C_4 + {}^5C_4$

$$=15+5$$

$$=20\text{ways.}$$

Definition

.

A Linear homogeneous recurrence relation of degree K with constant coefficients is a recurrence relation of the form

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

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

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

The degree is k because an is exrressed in terms of the previous k terms of the sequence

Ex:4 The recurrence relation

$H_n = 2H_{n-1} + 1$

Is not homogenous

Ex: 5 The recurrence relation

$B_n = nB_{n-1}$

Does not have constant coefficient

Ex:6 The relation $T(k) = 2[T(k-1)]^2 KT(K-3)$

Is a third order recurrence relation &

T(0),T(1),T(2) are the initial conditions.

Ex:7 The recurrence relation for the function

f : N->Z defined by

f(x)=2x,∀ x € N is given by

f(n+1)=f(n)+2,n>=0 with f(0)=0

f(1)=f(0)+2=0+2=2

f(2)=f(1)+2=2+2=4 and so on.

It is a first order recurrence relation.

2.3 Recurrence relations.

Definition

An equation that expresses a_n, the general term of the sequence $\{a_n\}$ in terms of one or more of the previous terms of the sequence , namely $a_0, a_{1,\ldots\ldots,} a_{n-1}$,for all integers n with n>=0,where n_0 is a non –ve integer is called a recurrence relation for $\{a_n\}$ or a difference equation.

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

For example ,we consider the famous Fibonacci sequence

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

which can be represented by the recurrence relation.

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

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

It is a second order recurrence relation.

2.4 Solving Linear Homogenous Recurrence Relations with Constants Coefficients.

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

Step 2: By solving the characteristics equation first out the characteristics roots.

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

Case 1: Let the roots be real and distinct say $r_1,r_2,r_3.....,r_n$ then

$A_n= \alpha_1 r_1^n+ \alpha_2 r_2^n+ \alpha_3 r_3^n+.....+ \alpha_n r_n^n$,

Where $\alpha_1, \alpha_2, ...,\alpha_n$ are arbitrary constants.

Case 2: Let the roots be real and equal say $r_1=r_2=r_3=r_n$ then

$A_n= \alpha_1 r_1^n+ n\alpha_2 r_2^n+n^2 \alpha_3 r_3^n+.....+n^2 \alpha_n r_n^n$,

Where $\alpha_1, \alpha_2, ...,\alpha_n$ are arbitrary constants.

Case 3: When the roots are complex conjugate, then

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

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

Note:

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

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

Example 1: If sequence $a_n=3.2^n$,n>=1, then find the recurrence relation.

Solution:

For n>=1

$a_n=3.2^n$,

now, $a_{n-1}=3.2^{n-1,}$

‘

$=3.2^n / 2$

$a_{n-1}=a^n/2$

$a_n = 2(a_n-1)$

$a_n = 2a_n-1$, for $n \geq 1$ with $a_n=3$

Example 2 :

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

Sol :

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

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

$=6(-5)^n / -5$

$S(n-1) = S(n) / -5$

$S_n = -5.5 (n-1)$, $n \geq 0$ with s(0) =6

Example 5: Find the relation from $Y_k =A.2^k + B.3^k$

Sol :

Given $Y_k =A.2^k + B.3^k$ ----------→(1)

$Y_{k+1} = A.2^{k+1} + B.3^{k+1}$

$= A.2^k.2 + B3^k.3$

$Y_{k+1} = 2A.2^k + 3B.3^k$ ----------→(2)

$Y_{k+2} = 4A.2^k + 9B.3^k$ ----------→(3)

(3) – 5(2) + 6(1)

→$y_{k+2} - 5y_{k+1} + 6y_k = 4A.2^k + 9B.3^k - 10A.2^k - 15B.3^k + 6A.2^k + 6B.3^k$

$= 0$

∴ $Y_{k+1} - 5y_{k+1} + 6y_k = 0$ in the required recurrence relation.

Example 9 :

Solve the recurrence relation defind by $S_o = 100$ and S_k (1.08) S_{k-1} for $k \geq 1$

Sol ;

Given $S_0 = 100$

$S_k = (1.08)\ S_{k-1}$, $k \geq 1$

$S_1 = (1.08)\ S_0 = (1.08)100$

$S_2 = (1.08)\ S_1 = (1.08)(1.08)100$

$= (1.08)^2\ 100$

$S_3 = (1.08)\ S_2 = (1.08)(1.08)^2 100$

$= = (1.08)^3\ 100$

$S_k = (1.08) S_{k-1} = (1.08)^k 100$

Example 15 : Find an explicit formula for the Fibonacci sequence .

Sol ;

Fibonacci sequence 0,1,2,3,4..... satisify the recurrence relation

$$fn = f_{n-1} + f_{n-2}$$

$$fn - f_{n-1} - f_{n-2} = 0$$

& also satisfies the initial condition $f_0=0, f_1=1$

Now , the characteristic equation is

$$r_2 - r - 1 = 0$$

Solving we get $r = 1 \pm 1+4 / 2$

$$= 1 \pm 5 / 2$$

Sol :

$$fn = \alpha_1 (1+ 5 / 2)^n + \alpha_2 (1- 5 / 2)^n \text{ ----}\rightarrow (A)$$

given $f_0 = 0$ put n=0 in (A) we get

$$f0 = \alpha_1 (1+ 5 / 2)^0 + \alpha_2 (1- 5 / 2)^0$$

$$(A) \rightarrow \alpha 1 + \alpha 2 = 0 \text{ ----------}\rightarrow (1)$$

given $f_1 = 1$ put n=1 in (A) we get

$$f_1 = \alpha_1 (1+ 5 / 2)^1 + \alpha_2 (1- 5 / 2)^1$$

$$(A) \rightarrow (1+ 5 / 2)^n + \alpha_2 (1- 5 / 2)^n \alpha_2 = 1 \text{ -------}\rightarrow (2)$$

To solve(1) and (2)

(1) X(1+ 5 / 2) => (1+ 5 / 2) α_1 + (1+ 5 / 2) α_2 =0 -----→(3)

(1+ 5 / 2) α_1 + (1+ 5 / 2) α_2 = 1------→(2)

(-) (-) (-)

1/2 α_2 + 5/2 α_2 -1/2 α_2 + 5/2 α_2 = -1

2 5 d_2 = -1

α_2 = - 1/5

Put α_2 = -1/5 in eqn (1) we get α_1 1/5

Substituting these values in (A) we get

Solution fn=1/5 $(1+5/2)^n$ -1/5 $(1+5/2)^n$

Example 13 ;

Solve the recurrence equation

$a_n = 2a_{n-1} – 2a_{n-2}$, $n \geq 2$ & $a_0 = 1$ & $a_1 = 2$

Sol :

The recurrence relation can be written as

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

The characteristic equation is

r2 – 2r -2 =0

Roots are r= 2± 2i / 2

=1± i

LINEAR NON HOMOGENEOUS RECRRENCE RELATIONS WITH CONSTANT COEFFICIENTS

A recurrence relation of the form

$a_n = c_1\ a_{n-1} + c_2\ a_{n-2} + \ldots\ldots\ldots c_k\ a_{n-k} + F(n) \ldots\ldots\ldots\ldots\ldots$ (A)

Where $c_1, c_2, \ldots c_k$ are real numbers and F(n) is a function not identically zero depending only on n,is called a non-homogeneous recurrence relation with constant coefficient.

Here ,the recurrence relation

$a_n = c_1\ a_{n-1} + c_2\ a_{n-2} + \ldots\ldots\ldots c_k\ a_{n-k} + F(n) \ldots\ldots\ldots\ldots\ldots$ (B)

Is called Associated homogeneous recurrence relation.

NOTE:

(B) is obtained from (A) by omitting F(n) for example ,the recurrence relation

$a_n = 3\ a_{n-1} + 2_n$ is an example of non-homogeneous recurrence relation .Its associated

Homogeneous linear equation is

$a_n = 3\ a_{n-1}$ [By omitting F(n) = 2n]

PROCEDURE TO SOLVE NON-HOMOGENEOUS RECURRENCE RELATIONS:

The solution of non-homogeneous recurrence relations is the sum of two solutions.

1.solution of Associated homogeneous recurrence relation (By considering RHS=0).

2.Particular solution depending on the RHS of the given recurrence relation

STEP1:

a) if the RHS of the recurrence relation is

$a_0 + a_1$ n .... a_r n^r, then substitute

c_0 $+c_1\ n + c_2$ n^2+……..c_r $(n-1)^r$ in place of $a_n - 1$ ……..and so on ,in the LHS of the given recurrence relation

(b) if the RHS is a^n then we have

Case1:if the base a of the RHS is the characteristric root,then the solution is of the can^n .therefore substitute ca^n in place of a_n ,ca^{n-1} in place of $c(n-1)\ a_{n-1}$ etc..

Case2: if the base a of RHS is not a root , then solution is of the form ca^n therefore substitute ca^n in place of a_n , ca^{n-1} in place of a_{n-1} etc..

STEP2:

At the end of step-1, we get a polynomial in 'n' with coefficient c_0,c_1……on LHS

Now, equating the LHS and compare the coefficients find the constants c_0,c_1,….

Example 1:

Solve $a_n = 3\ a_{n-1}$ +2n with a_1 =3

Solution:

Give the non-homogeneous recurrence relation is

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

It's associated homogeneous equation is

$a_n - 3\ a_{n-1}$ =0 [omitting f(n) =2n]

It's characteristic equation is

r-3=0 => r=3

now, the solution of associated homogeneous equation is

$a_n\ (n) = \propto, 3^{\ n}$

To find particular solution

Since F(n) =2n is a polynomial of degree one,then the solution is of the from

$a_n = c_n$ +d (say) where c and d are constant

Now, the equation

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

c_n +d =3(c(n-1)+d)+2n

[replace a_n by c_n +d a_{n-1} by c(n-1)+d]

- ⇨ c_n +d =3cn-3c+3d+2n
- ⇨ 2cn+2n-3c+2d=0
- ⇨ (2+2c)n+(2d-3c)=0
- ⇨ 2+2c=0 and 2d-3c=0
- ⇨ Saving we get c=-1 and d=-3/2 therefore cn+d is a solution if c=-1 and d=-3/2

a_n (p)=-n-3/2

Is a particular solution.

General solution

a_n=a_n(n)+ a_n(p)

$a_n = \propto 3^{\ n}$ -n-3/2 ……..(A)

Given $a_1 = 3$ put n=1 in (A) we get

$a_1 = \propto\ 1(3)^{\ 1}$ -1-3/2

$3=3\propto_{\ 1}$-5/2

$3 \propto_1 = 11/2$

$\propto_1 = 11/6$

Substituting $\propto_1 = 11/6$ in (A) we get

General solution

$a_n = -n - 3/2 + (11/6)3^n$

Example:2

Solve s(k)-5s(k-1)+6s(k-2)=2

With s(0)=1 ,s(1)=-1

Solution:

Given non-homogeneous equation can be written as

$a_n = 5a_{n-1} + 6a_{n-2} - 2 = 0$

The characteristic equation is

$r^2 - 5r + 6 = 0$

roots are r=2,3

the general solution is

$3_n(n) = \propto_1 (2)^n + \propto_2 (3)^n$

To find particular solution

As RHS of the recurrence relation is constant ,the solution is of the form C , where C is a constant

Therefore the equation

$a_n - 5a_{n-1} - 6a_{n-2} - 2 = 2$

$c - 5c + 6c = 2$

2c=2

c=2

the particular solution is

$s_n(p)=1$

the general solution is

$s_n = s_n(n) + s_n(p)$

$s_n = \propto_1 (2)^n + \propto_2 (3)^n + 1$.....(A)

Given $s_0=1$ put n=0 in (A) we get

$s_0 = \propto_1 (2)^0 + \propto_2 (3)^0 + 1$

$s_0 = \propto_1 + \propto_2 + 1$

(A) => $s_0 = 1 = \propto_1 + \propto_2 + 1$

$\propto_1 + \propto_2 = 0$.....(1)

Given a_1=-1 put n=1 in(A)

⇨ $S_1 = \propto_1 (2)^1 + \propto_2 (3)^1 + 1$

⇨ (A) $-1 = \propto_1 (2) + \propto_2 (3) + 1$

⇨ $2 \propto_1 + 3 \propto_2 = -2$.....(1)

$\propto_1 + \propto_2 = 0$

$2 \propto_1 + 3 \propto_2 = -2$.....(2)

By solving (1) and (2)

$\propto_1 = 2, \propto_2 = -2$

Substituting $\propto_1 = 2, \propto_2 = -2$ in (A) we get

Solution is

⇨ $S_{(n)} = 2.(2)^n - 2.(3)^n + 1$

Example :3

Solve $a_n - 4\,a_{n-1} + 4\,a_{n-2} = 3n + 2^n$

$a_0 = a_1 = 1$

Solution:

The given recurrence relation is non-homogeneous

Now, its associated homogeneous equation is,

$a_n - 4\,a_{n-1} + 4\,a_{n-2} = 0$

Its characteristic equation is

$r^2 - 4r + 4 = 0$

r=2,2

solution , $a_n(n) = \propto_1 (2)^n + n \propto_2 (2)^n$

$a_n(n) = (\propto_1 + n \propto_2) 2^n$

To find particular solution

The first term in RHS of the given recurrence relation is 3n.therefore ,the solution is of the form $c_1 + c_2 n$

Replace a_n by $c_1 + c_2 n$, a_{n-1} by $c_1 + c_2(n-1)$

And a_{n-2} by $c_1 + c_2(n-2)$ we get

$(c_1 + c_2 n) - 4(c_1 + c_2(n-1)) + 4(c_1 + c_2(n-2)) = 3n$

⇨ $c_1 - 4c_1 + 4c_1 + c_2 n - 4c_2 n + 4c_2 n + 4c_2 - 8c_2 = 3n$

⇨ $c_1 + c_2 n - 4c_2 = 3n$

Equating the corresponding coefficient we have

c_1-4c_2=0 and c_2=3

c_1=12 and c_2=3

Given a_0=1 using in (2)

(2) => $\propto_1$+12=1

Given a_1=1 using in (2)

(2)=> ($\propto_1$+$\propto_2$)2+12+3+1/2 .2=1

=> (2 $\propto_1$+2 $\propto_2$)+16=1……..(14)

(3) $\propto_1$=-11

Using in (4) we have $\propto_2$=7/2

Solution a_n=(-11+7/2n)2^n+12+3n+1/2$n^2 2^n$

Example:

HOW MANY INTEGERS BETWEEN 1 to 100 that are

i) not divisible by 7,11,or 13

ii) divisible by 3 but not by 7

Solution:

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

now,

|A| =[100/7]=14

|B| =[100/11]=9

|C| =[100/13]=7

|A^B| =[100/7]=1

|A^C| =[100/7*13]=1

|B^C| =[100/11*13]=0

|A^B^C| =[100/7*11*13]=0

That are divisible by 7, 11 or 13 is |AvBvC|

By principle of inclusion and exclusion

|AvBvC| =|A|+|B|+|C|-|A^B|-|A^C|-|B^C|+|A^B^C|

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

=30-2=28

Now,

The number of integer not divisible by any of 7,11,and 13=total-|AvBvC|

=100-28=72

ii) let A and B denote the no. between 1 to 100 that are divisible by 3 and 7 respectively

|A| =[100/3]=33

|B|=[100/7]=14

| A^B |=[100/3*7]=14

The number of integer divisible by 3 but not by 7

=|A|-| A^B |

=33-4=29

Example:

There are 2500 student in a college of these 1700 have taken a course in C, 1000 have taken a course pascal and 550 have taken course in networking .further 750 have taken course in both C and pascal ,400 have taken courses in both C and Networking and 275 have taken courses in both pascal and networking. If 200 of these student have taken course in C pascal and Networking.

i)how many these 2500 students have taken a courses in any of these three courses C ,pascal and networking?

ii)How many of these 2500 students have not taken a courses in any of these three courses C,pascal and networking?

Solution:

Let A,B and C denotes student have taken a course in C,pascal and networking respectively

Given

|A|=1700

|B|=1000

|C|=550

| A^B | =750

| A^C|=40

| B^C =275

| A^B^C |=200

Number of student who have taken any one of these course=| A^B^C |

By principle of inclusion and exclusion

|AvBvC| =|A|+|B|+|C|-|A^B|-|A^C|-|B^C|+|A^B^C|

=(1700+1000+550)-(750+400+275)+200

=3450-1425=2025

The number between 1-100 that are divisible by 7 but not divisible by 2,3,5,7= =|D|- | A^B^C ^CD|

=142-4=138

Example:

A survey of 500 television watches produced the following information.285 watch hockey games.195 watch football games 115 watch basketball games .70 watch football and hockey games.50 watch hockey and

basketball games and 30 watch football and hockey games.how many people watch exactly one of the three games?

Solution:

H=> let television watches who watch hockey

F=> let television watches who watch football

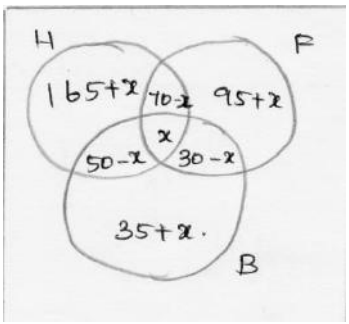
B=> let television watches who watch basketball

Given

n(H)=285,n(F)=195,n(B)=115,n(H^F)=70,n(H^B),n(F^B)=30

let x be the number television watches who watch all three games

now, we have



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

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

=445+x=500

X=55

Number of students who watches exactly one game is=165+x+95+x+35+x

=295+3*55

=460

2.5 .Generating function:

Of real numbers is the infinite sum.

$G(x)=G(s,x)= a_0+a_1x+,\ldots. a_nx^n+\ldots.= \sum_{n=0}^{\infty} a^n x^n$

For example,

i) the generating function for the sequence 'S' with the terms 1,1,1,1…..i.s given by,

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

ii)the generation function for the sequence 'S' with terms 1,2,3,4…..is given by

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

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

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

2.Solution of recurrence relation using generating function

Procedure:

Step1:rewrite the given recurrence relation as an equation with 0 as RHS

Step2:multiply the equation obtained in step(1) by x^n and summing if form 1 to ∞ (or 0 to ∞) or (2 to ∞).

Step3:put $G(x)= \sum_{n=0}^{\infty} a^n x^n$ and write G(x) as a function of x

Step 4:decompose G(x) into partial fraction

Step5:express G(x) as a sum of familiar series

Step6:Express a_n as the coefficient of x^n in G(x)

The following table represent some sequence and their generating functions

step1	**sequence**	**generating function**
1	1	1/1-z
2	$(-1)^n$	1/1+z
3	a^n	1/1-az
4	$(-a)^n$	1/1+az
5	n+1	$1/1-(z)^2$
6	n	$1/(1-z)^2$
7	n^2	$z(1+z)/(1-z)^3$
8	na^n	$az/(1-az)^2$

Eg:use method of generating function to solve the recurrence relation

$a_n=3a_{n-1}+1$; $n\geq1$ given that $a_0=1$

solution:

let the generating function of $\{a_n\}$ be

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

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

multiplying by x^n and summing from 1 to ∞,

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

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

$G(x)-a_0=3xG(x)+x/1-x$

$G(x)(1-3x)=a_0+x/1-x$

$=1+x/1-x$

$G(x)(1-3x)=1=x+x/1-x$

$G(x)=1/(1-x)(1-3x)$

By applying partial fraction

$G(x)=-1/2/1-x+3/2/1-3x$

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

$G(x)[1-x-x^2]=a_0-a_1x-a_0x$

$G(x)[1-x-x^2]= a_0-a_0x+a_1x$

$G(x)=1/1-x-x^2 \quad [a_0=1, a_1=1]$

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

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

Now,

$$1/1-x-x^2 =\frac{A}{(1-(\frac{1+\sqrt{5}}{2})x)}+\frac{B}{(1-(\frac{1-\sqrt{5}}{2})x)}\ldots\ldots\ldots\ldots(1)$$

$$1=A[1-(\frac{1+\sqrt{5}}{2})x)]+ B[1-(\frac{1-\sqrt{5}}{2})x)]\ldots\ldots(2)$$

Put x=0 in (2)

(2)=> A+B=1

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

$$(2)=> \quad 1=B[1-\frac{1+\sqrt{5}}{1-\sqrt{5}}]$$

$$1=B[\frac{1-\sqrt{5}-1-\sqrt{5}}{1-\sqrt{5}}\ ]$$

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

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

(3) => $A=\frac{1+\sqrt{5}}{2\sqrt{5}}$

Sub A and B in (1)

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

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

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

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

solving we get

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

2.6THE PRINCIPLE OF INCLUSION –EXCLUSION

Assume two tasksT
time(simultaneously) now to find the number of ways to do one of the two tasks $T_1$and T_2, if we add number ways to do each task then it leads to an over count. since the ways to do both tasks are counted twice. To correctly count the number of ways to do each of the two tasks and then number of ways to do both tasks

i.e $^(T_1vT_2)=^(T_1)+^(T_2)-^(T_1^T_2)$

this technique is called the principle of Inclusion –exclusion

FORMULA:$_4$

1) $| A_1vA_2vA_3|=|A_1|+|A_2|+|A_3|-|A_1^A_2|-|A_1^A_3|-|A_2^A_3|+|A_1^A_2^ A_3|$

2) $|A_1vA_2vA_3v A_4|=|A_1|+|A_2|+|A_3|+| A_4 |-|A_1^A_2|-|A_1^A_3|-|A_1^A_4|-|A_2^A_3|-|A_2^A_4|-|A_3^A_4|+|A_1^A_2^ A_3 |+|A_1^A_2^ A_4 |+|A_1^A_3^ A_4 |+|A_2^A_3^ A_4 |+|A_1^A_2^ A_3^A_4 |$

Example1:

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

Solution:

Let A denote the students who volleyball

Let B denote the students who play hockey

It is given that

n=500

|A|=200

|B|=120

|A^B|=60

Bt the principle of inclusion-exclusion, the number of students playing either volleyball or hockey

|AvB|=|A|+|B|-|A^B|

|AvB|=200+120-60=260

The number of students not playing either volleyball or hockey=500-260

=240

Example2:

In a survey of 100 students it was found that 30 studied mathematics,54 studied statistics,25 studied operation research,1 studied all the three subjects.20 studied mathematics and statistic,3 studied mathematics and operation research And 15 studied statistics and operation research

1.how many students studied none of these subjects?

2.how many students studied only mathematics?

Solution:

1) Let A denote the students who studied mathematics

Let B denote the students who studied statistics

Let C denote the student who studied operation research

Thus |A|=30 ,|B|=54 ,|C|=25 ,|A^B|=20 ,|A^C|=3 ,|B^C|=15 ,and |A^B^C|=1

By the principle of inclusion-exclusion students who studied any one of the subject is

|AvBvC|=|A|+|B|+|C|=|A^B|-|A^C|-|B^C|+|A^B^C|

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

=110-38=72

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

2) now ,

The number of students studied only mathematics and statistics=n(A^B)-n(A^B^C)

=20-1=19

The number of students studied only mathematics and operation research=n(A^C)-n(A^B^C)

=3-1=2

Then The number of students studied only mathematics =30-19-2=9

Example3:

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

Solution:

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

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

Then |A|=[1000/7]=[142.8]=142

|B|=[1000/11]=[90.9]=90

|A^B|=[1000/7*11]=[12.9]=12

The number of positive integers not exceeding 1000 that are divisible either 7 or 11 is |AvB|

By the principle of inclusion –exclusion

|AvB|=|A|+|B|-|A^B|

=142+90-12=220

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

Example:

A survey among 100 students shows that of the three ice cream flavours vanilla,chocolate,and strawberry ,50 students like vanilla,43 like chocalate ,28 like strawberry,13 like vanilla, and chocolate,11like chocalets and strawberry,12 like strawberry and vanilla and 5 like all of them.

Find the number of students surveyed who like each of the following flavours

1.chocalate but not strawberry

2.chocalate and strawberry ,but not vanilla

3.vanilla or chocolate, but not strawberry

Solution:

Let A denote the set of students who like vanilla

Let B denote the set of students who like chocalate

Let C denote the set of students who like strawberry

Since 5 students like all flavours

|A^B^C|=5

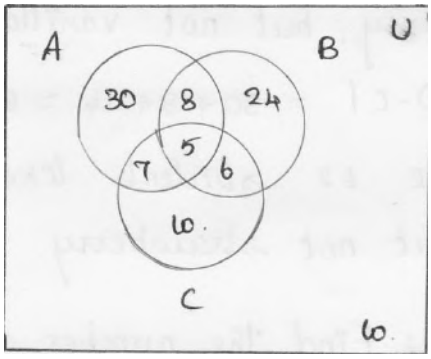
12 students like both strawberry and vanilla

|A^C|=12

But 5 of them like chocolate also, therefore

|A^C-B|=7

Similarly |B^C-A|=6



Of the 28 students who like strawberry we have already accounted for

7+5+6=18

So, the remaining 10 students belong to the set C-|AvB| similarly

|A-BvC|=30 and |B-AvC|=24

Thus for we have accounted for 90 of the 100 students the remaining 10 students like outside the region AvBvC

Now,

1.|B-C|=24+8=32

So 32 students like chocolate but not strawberry

2.|B^C-A|=6

Therefore 6 students like both chocolate and strawberry but not vanilla

3.|AvB-C|=30+8+24=62

Therefore 62 students like vanilla or chocolate but not strawberry

Example 5: 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|=[250/2]=125

|B|=[250/3]=83

|C|=[250/5]=50

|D|=[250/7]=35

Now, the number of integer between 1-250 that are divisible by 2 and 3=|A^B|=[250/2*3]=41

The number of integer divisible by 2 and 5=|A^C|=[250/2*5]=25

Similarly

|A^D|=[250/2*7]=17

|B^C|=[250/3*5]=16

|B^D|=[250/3*7]=11

|C^D| =[250/5*7]=7

The number of integer divisible by 2,3,5=|A^B^C|=[250/2*3*5]=8.

1. Solve the recurrence relation a_{n+2}- a_{n+1}-6 $a_{n=0}$ given a_0=2 and a_1=1 using generating functions

Solution:

Given recurrence relation is

a_{n+2}- a_{n+1}-6 $a_{n=0}$

⇨ $\sum_{n=0}^{\infty} a_n+2\, x^n - \sum_{n=0}^{\infty} a_n+1\, x^n - 6\sum_{n=0}^{\infty} a_n\, x^n = 0$

⇨ $1/x^2 \sum_{n=0}^{\infty} a_n+2\, x^{n+2}$-$1/x \sum_{n=0}^{\infty} a_n+1\, x^{n+1}$-$6\sum_{n=0}^{\infty} a_n\, x^n = 0$

⇨ $1/x^2[G(x)-a_0-a_1x]-1/x[G(x)-a_0]-6[G(x)] = 0$

⇨ $1/x^2[G(x)-2-x]-1/x[G(x)-2]-6G(x) = 0$

Multiply by x^2 we have

Generating functions

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

Now apply partial fraction

$$\frac{2-x}{1-x-6x^2} = \frac{A}{1-3x} + \frac{B}{1+2x}$$

2-x = A(1+2x) + B(1-3x)……(1)

Put x = -1/2 in (1) we get

5/2 = 5/2B => B = 1

Put x = 1/3 in (1) we get A = 1

a_n = co efficient of x^n in $[(1+3x+3x^2+\ldots.3x^n)+1-2x+2x^2\ldots\ldots+(-1)^n2x^n]$

$a_n = 3^n+(-1)^n2n$

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

Solution:

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

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

Now

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

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

Put $x=1/2, 5+1=2B \Rightarrow B=3$

$x=-1/2$, $5-1=2A \Rightarrow A=2$

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

$=2\ [1+2x]^{-1}+3[1-2x]^{-1}$

$=2\ [1-2x+2x^2-2x^3+\ldots.]+3[1+2x+2x^2+\ldots.]$

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

UNIT III GRAPHS

3.1GRAPHS & GRAPH MODELS

DEFINITION: Graph:

A *Graph G=(V,E,ϕ) consists of a non empty set v={v1,v2,…..} called the set of nodes (Points, Vertices) of the graph, E={e1,e2,…} is said to be the set of edges of the graph, and – is a mapping from the set of edges E to set off ordered or unordered pairs of elements of V.*

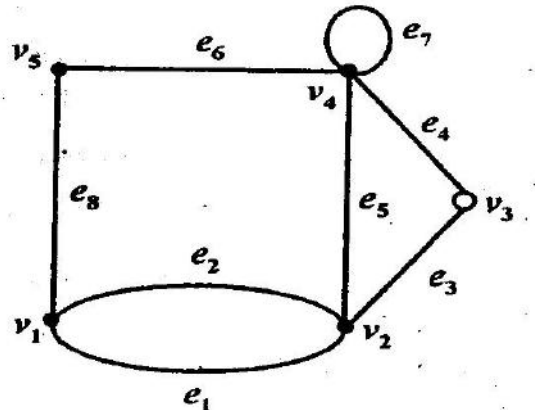
The vertices are represented by points and each edge is represented by a line diagrammatically.

DEFINITIONS:

From the figure we have the following definitions

V_1,v_2,v_3,v_4,v_5 are called vertices.

$e_1,e_2,e_3,e_4,e_5,e_6,e_7,e_8$ are called edges.



DEFINITION: Self Loop:

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

For example, the edge e7 is called a self loop. Since the edge e_7 has the same vertex (v_4) as both its terminal vertices.

DEFINITION: Parallel Edges:

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

For example, the edge e_1 and e_2 are called parallel edges since e_1 and e_2 have the same pair of vertices (v_1,v_2) as their terminal vertices.

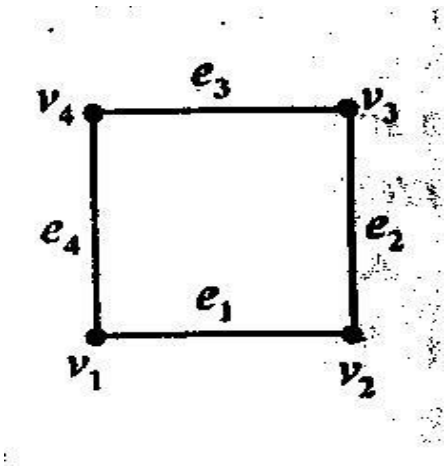
DEFINITION: Incident:

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

DEFINITION: Adjacent edges and vertices:

Two edges are said to be adjacent if they are incident on a common vertex. In fig (i) the edges e_6 and e_8 are adjacent.

Two vertices v_i and v_j are said to adjacent if v_i v_j is an edge of the graph. (or equivalently (v_i,v_j) is an end vertices of the edge e_k)



For example, in fig., v_1 and v_5 are adjacent vertices.

DEFINITION: Simple Graph:

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

NOTE: In this chapter, unless and otherwise stated we consider only simple undirected graphs.

DEFINITION: Isolated Vertex:

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

One can easily note that Isolated vertex is not adjacent to any vertex.

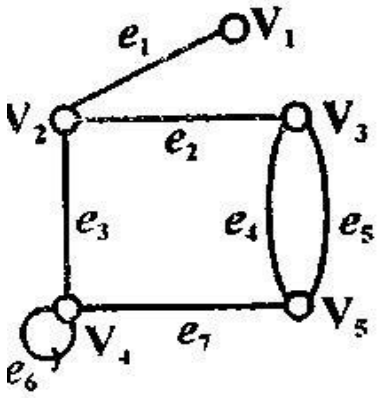
If fig (ii), v5 is isolated Vertex.

DEFINITION: Pendentant Vertex:

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

EXAMPLE:

Consider the graph



In the above undirected graph

Vertices V={V_1, V_2, V_3, V_4, V_5}

Edges E={ e_1,e_2,....}

And e_1= < V_1, V_2> or < V_2,V_1>

e_2= < V_2,V_3> or < V_3,V_2>

e_4= < V_4,V_2> or < V_4,V_2>

e_5= < V_4,V_4>

In the above graph vertices V_1 and V_2, V_2 and V_3, V_3 and V_4, V_3 and V_5 are adjacent. Whereas V_1 and V_3, V_3 and V_4 are not adjacent.

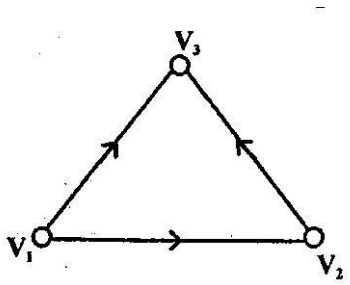
The edge e6 is called loop. The edges e_4 and e_5 are parallel edges.

Directed Edges:

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

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

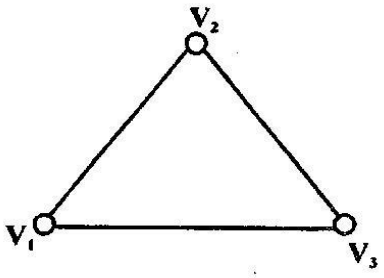
Digraph:



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

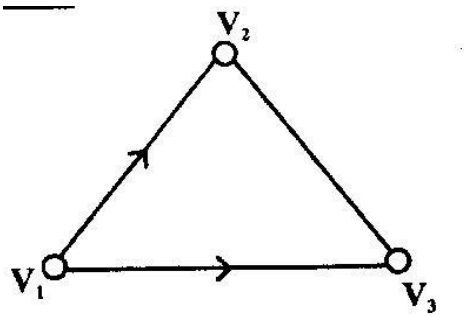
Undirected Graph:

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



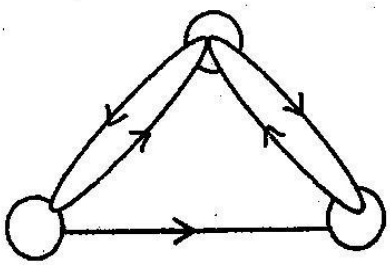
Mixed Graph:

If some edges are directed and some are undirected in a graph, the graph is called an ***mixedgraph.***



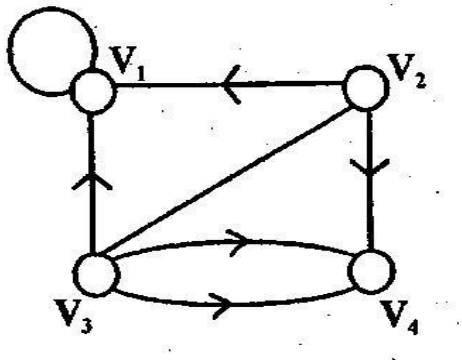
Multi Graph:

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



Pseudograph:

A graph in which loops and parallel edges are allowed is called a ***Pseudograph.***

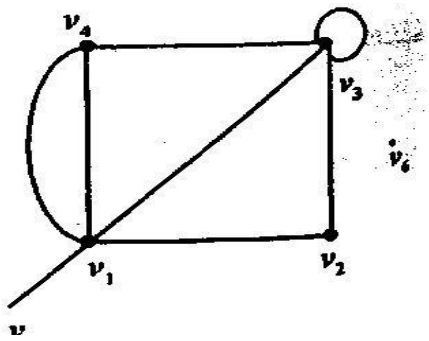


3.2 GRAPH TERMINOLOGY

DEF

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

Example 1:



d (v_1) = 5 d (v_4) = 3

d (v_2) = 2 d (v_5) = 1

d (v_3) = 5 d (v_6) = 0

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

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

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

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

Theorem 1: (The Handshaking Theorem)

Let G= (V, E) be an undirected graph with 'e' edges. Then

deg(v)= 2e

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

Proof:

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

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

Therefore, **deg(v)= 2e**

Theorem 2:

In an undirected graph, the numbers of odd degree vertices are even.

Proof:

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

Therefore,

$$\mathbf{d(v)= \ d(v_i)+ \ d(v_j)}$$

By handshaking theorem, we have

Since each deg (v_i) is even, is even.

As left hand side of equation (1) is even and the first expression on the RHS of (1) is even, we have the 2nd expression on the RHS must be even.

Since each deg (v_j) is odd, the number of terms contained in

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

Theorem 3:

The maximum number of edges in a simple graph with 'n' vertices is 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 at most one edge.

Therefore, 22-12=1

The result is true for n=2.

Assume that the result is true for n=k. i.e., a graph with k vertices has at most kk-12 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 ϵ V (G).

Since G’ has k vertices, then by the hypothesis G’ has at most kk-12 edges. Now add the vertex ‘v’ to G’. such that ‘v’ may be adjacent to all k vertices of G’.

Therefore, the total number of edges in G is,

Therefore, the result is true for n=k+1.

Hence the maximum number of edges in a simple graph with ‘n’ vertices is nn-12.

Theorem 4:

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

Proof:

Let 2n be the number of vertices of the given graph.

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

By Handshaking theorem, we have

Therefore, the number of edges of the given graph is amultiple of k.

3.3

Regular graph:

Definition: *Regular graph:*

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

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

DEFINITION : *Complete graph:*

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

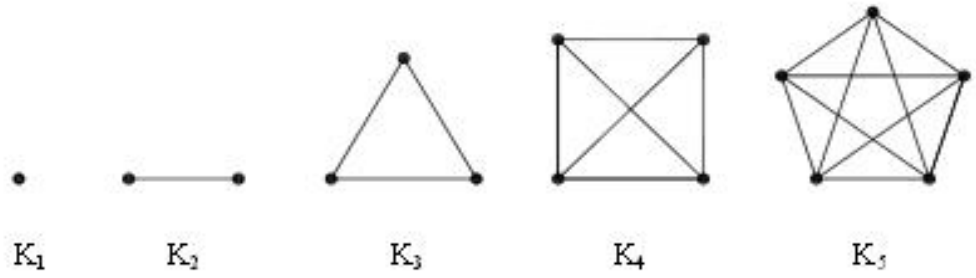


Fig. 1.10 Some complete graphs.

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

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

SUBGRAPH

A graph H =(V', E') is called a subgraph of G = (V, E), if V' **C V** and **E' C E.**

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

Hence, we have the following:

(i) **Each graph has its own subgraph.**

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

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

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

Note: Any sub graph of a graph G can be obtained by removing certain vertices and edges from G. It is to be noted that the removal of an edges does not go with the removal of its adjacent vertices, where as the removal of any edge incident on it.

Bipartite graph:

A graph G is said to be **bipartite** if its vertex set V (G) can be partitioned into two disjoint non empty sets V1 and V2, V1 U V2=V(G), such that every edge in E(G) has one end vertex in V1 and another end vertex in V2. (So that no edges in G, connects either two vertices in V1 or two vertices in V2.)

Examples of bipartite and complete bipartite graphs are shown in Figure 1.11.

(a) A bipartite graph. (b) A complete bipartite graph $K_{3,4}$.

Fig. 1.11 Two bipartite graphs.

Complete Bipartite Graph:

A bipartite graph G, with the bipartition V1 and V2, is called ***complete bipartite graph,*** if every vertex in V1 is adjacent to every vertex in V2.Clearly, every vertex in V2 is adjacent to every vertex in V1.

A complete bipartite graph with ‘m’ and ‘r’ vertices in the bipartition is denoted by km,n.

Incidence Matrix

Let G be a graph with n vertices, m edges and without self-loops. The incidence matrix A of G is an $n \times m$ matrix $A = [a_{ij}]$ whose n rows correspond to the n vertices and the m columns correspond to m edges such that

$$a_{ij} = \begin{cases} 1, & \text{if } j\text{th edge } m_j \text{ is incident on the } i\text{th vertex} \\ 0, & \text{otherwise.} \end{cases}$$

It is also called *vertex-edge incidence matrix* and is denoted by $A(G)$.

Example Consider the graphs given in Figure 10.1. The incidence matrix of G_1 is

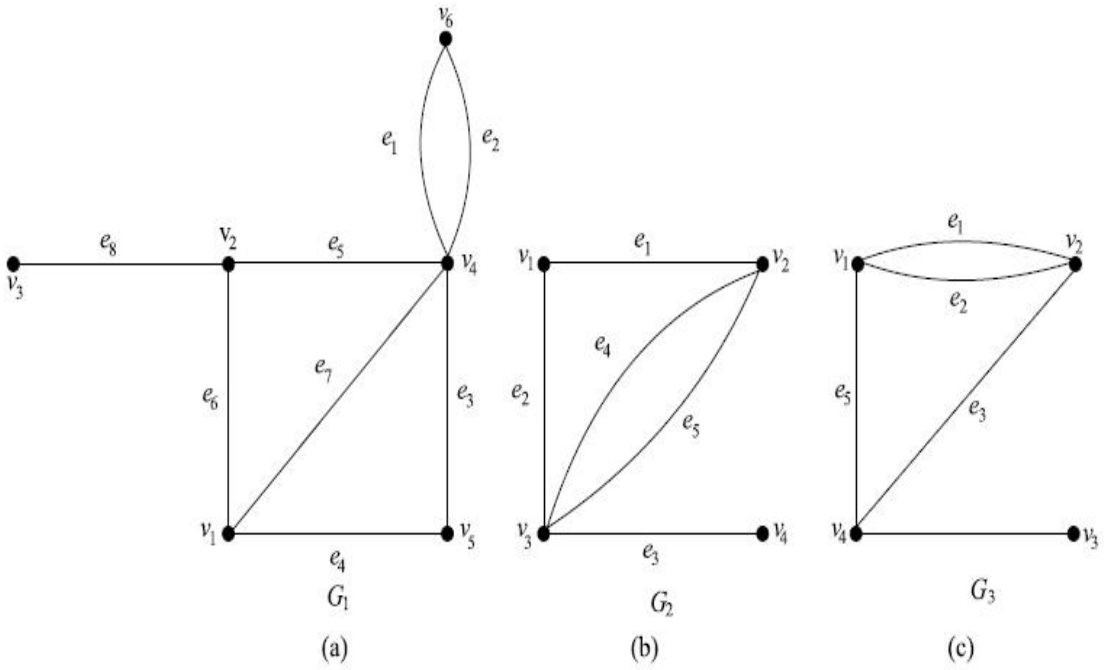
$$A(G_1) = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \\ v_6 \end{array} \begin{array}{c} \begin{array}{cccccccc} e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 & e_8 \end{array} \\ \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \end{array}.$$

The incidence matrix of G_2 is

$$A(G_2) = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \end{array} \begin{array}{c} \begin{array}{ccccc} e_1 & e_2 & e_3 & e_4 & e_5 \end{array} \\ \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix} \end{array}.$$

The incidence matrix of G_3 is

$$A(G_3) = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \end{array} \begin{array}{c} \begin{array}{ccccc} e_1 & e_2 & e_3 & e_4 & e_5 \end{array} \\ \begin{bmatrix} 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix} \end{array}.$$



The incidence matrix contains only two types of elements, 0 and 1. This clearly is a binary matrix or a (0, 1)-matrix.

We have the following observations about the incidence matrix A.

1. Since every edge is incident on exactly two vertices, each column of A has exactly two one's.

2. The number of one's in each row equals the degree of the corresponding vertex.

3. A row with all zeros represents an isolated vertex.

4. Parallel edges in a graph produce identical columns in its incidence matrix.

5. If a graph is disconnected and consists of two components G_1 and G_2, the incidence matrix $A(G)$ of graph G can be written in a block diagonal form as

$$A(G) = \begin{bmatrix} A(G_1) & 0 \\ 0 & A(G_2) \end{bmatrix},$$

where $A(G_1)$ and $A(G_2)$ are the incidence matrices of components G_1 and G_2. This observation results from the fact that no edge in G_1 is incident on vertices of G_2 and vice versa. Obviously, this is also true for a disconnected graph with any number of components.

6. Permutation of any two rows or columns in an incidence matrix simply corresponds to relabeling the vertices and edges of the same graph.

Path Matrix

Let G be a graph with m edges, and u and v be any two vertices in G. The path matrix for vertices u and v denoted by $P(u, v) = [p_{ij}]_{q \times m}$, where q is the number of different paths between u and v, is defined as

$$p_{ij} = \begin{cases} 1, & \textit{if jth edge lies in the ith path}, \\ 0, & \textit{otherwise}. \end{cases}$$

Clearly, a path matrix is defined for a particular pair of vertices, the rows in $P(u, v)$ correspond to different paths between u and v, and the columns correspond to different edges in G. For example, consider the graph in Figure 10.10.

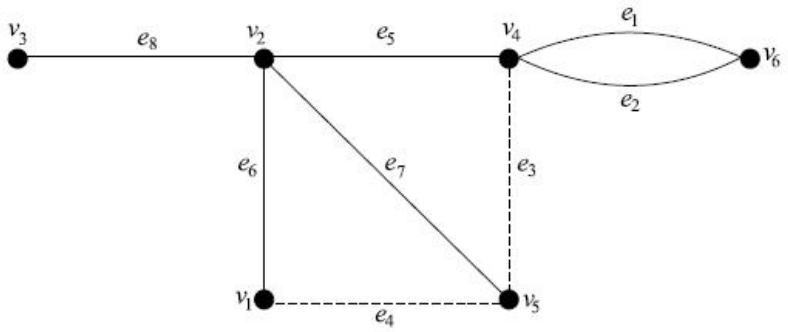


Fig. 10.10

The different paths between the vertices v_3 and v_4 are

$p_1 = \{e_8, e_5\}$, $p_2 = \{e_8, e_7, e_3\}$ and $p_3 = \{e_8, e_6, e_4, e_3\}$.

The path matrix for v_3, v_4 is given by

$$P(v_3, v_4) = \begin{array}{c} \begin{matrix} e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 & e_8 \end{matrix} \\ \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \end{array}.$$

We have the following observations about the path matrix.

1. A column of all zeros corresponds to an edge that does not lie in any path between u and v.
2. A column of all ones corresponds to an edge that lies in every path between u and v.
3. There is no row with all zeros.
4. The ring sum of any two rows in $P(u, v)$ corresponds to a cycle or an edge-disjoint union of cycles.

Adjacency Matrix

Let $V = (V, E)$ be a graph with $V = \{v_1, v_2, \ldots, v_n\}$, $E = \{e_1, e_2, \ldots, e_m\}$ and without parallel edges. The adjacency matrix of G is an $n \times n$ symmetric binary matrix $X = [x_{ij}]$ defined over the ring of integers such that

$$x_{ij} = \begin{cases} 1, & \text{if } v_i v_j \in E, \\ 0, & \text{otherwise}. \end{cases}$$

Example Consider the graph G given in Figure 10.12.

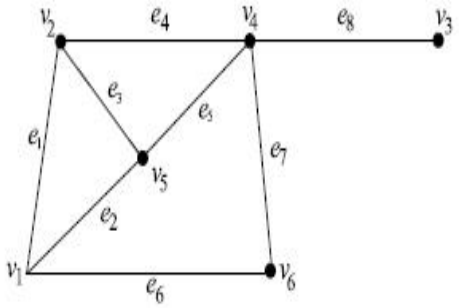


Fig. 10.12

The adjacency matrix of G is given by

$$X = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \\ v_6 \end{array} \begin{array}{c} \begin{array}{cccccc} v_1 & v_2 & v_3 & v_4 & v_5 & v_6 \end{array} \\ \begin{bmatrix} 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \end{bmatrix} \end{array}.$$

We have the following observations about the adjacency matrix X of a graph G.

1. The entries along the principal diagonal of X are all zeros if and only if the graph has no self-loops. However, a self-loop at the ith vertex corresponds to $x_{ii} = 1$.
2. If the graph has no self-loops, the degree of a vertex equals the number of ones in the corresponding row or column of X.
3. Permutation of rows and the corresponding columns imply reordering the vertices. We note that the rows and columns are arranged in the same order. Therefore, when two rows are interchanged in X, the corresponding columns are also interchanged. Thus two graphs G_1 and G_2 without parallel edges are isomorphic if and only if their adjacency matrices $X(G_1)$ and $X(G_2)$ are related by

$$X(G_2) = R^{-1}X(G_1)R,$$

where R is a permutation matrix.

4. A graph G is disconnected having components G_1 and G_2 if and only if the adjacency matrix $X(G)$ is partitioned as

4. A graph G is disconnected having components G_1 and G_2 if and only if the adjacency matrix $X(G)$ is partitioned as

$$X(G) = \begin{bmatrix} X(G_1) & : & O \\ \cdot\cdot & : & \cdot\cdot \\ O & : & X(G_2) \end{bmatrix},$$

where $X(G_1)$ and $X(G_2)$ are respectively the adjacency matrices of the components G_1 and G_2. Obviously, the above partitioning implies that there are no edges between vertices in G_1 and vertices in G_2.

5. If any square, symmetric and binary matrix Q of order n is given, then there exists a graph G with n vertices and without parallel edges whose adjacency matrix is Q.

GRAPH ISOMORPHISM

DEFINITION:

Two graphs G_1 and G_2 are said to be isomorphic to each other, if there exists a one-to-one correspondence between the vertex sets which preserves adjacency of the vertices.

Note: If G_1 and G_2 are isomorphic then G_1 and G_2 have,

(i) The same number of vertices.

(ii) The same number of edges

(iii) An equal number of vertices with a given degree.

Note: However, these conditions are not sufficient for graph isomorphism.

ISOMORPHISM AND ADJACENCY:

RESULT 1:

Two graphs are isomorphic if and only if their vertices can be labeled in such a way that the corresponding adjacency matrices are equal.

RESULT 2:

Two simple graphs G1 and G2 are isomorphic if and only if their adjacency matrices A1 and A2 are related $A1=P^{-1} A_2 P$ where P is a permutation matrix.

Note:

A matrix whose-rows are the rows of the unit matrix but not necessarily in their natural order is called permutation matrix.

Example:
Test the Isomorphism of the graphs by considering the adjacency matrices.

Let A1 and. A2 be the adjacency matrices of G1 and G2 respectively.

$$A_1 = \begin{array}{c} \\ u_1 \\ u_2 \\ u_3 \\ u_4 \end{array} \begin{array}{c} \begin{array}{cccc} u_1 & u_2 & u_3 & u_4 \end{array} \\ \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} \end{array}$$

$$A_2 = \begin{array}{c} \\ V_1 \\ V_2 \\ V_3 \\ V_4 \end{array} \begin{array}{c} \begin{array}{cccc} V_1 & V_2 & V_3 & V_4 \end{array} \\ \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix} \end{array}$$

Now $A_1 = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$

$\sim \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix}$ (Interchaning Column 3 and Column 4)

$\sim \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$ (Interchaning Row 3 and Row 4)

$\sim A_2$

Since A_1 and A_2 are similar, the corresponding graphs G_1 and G_2 are Isomorphic.

Paths,Reachability and Connectedness:

DEFINTTIONS:

Path:

A Path in a graphi s a sequence v1,v2,v3……vk of vertices each adjacent to the next.ln other words,starting with the vertex v1 one can travel along edges(v1,v2),(v2,v3)..and reach the vertex vk.

Length of the path:

The number of edges appearingi n the sequence of a path is called the length of Path.

Cycle or Circuit:

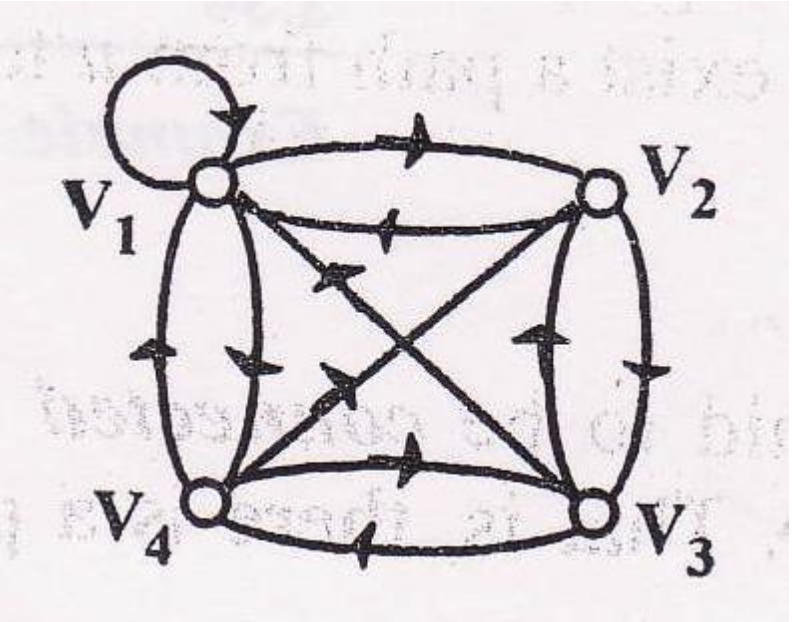
A path which originates and ends in the same node is called a cycle of circuit.

A path is said to be simple if all the edges in the path are distinct.

A path in which all the vertices are traversed only once is called an elmentary Path.

Example I :

Consider the graph:



Then some of the paths originating in node V1 and ending in node v1 are:

P1=(<V1 ,V2> ,<V2V3>)

P2=(<V1 ,V4> ,<V4 ,V3>)

P3 = (<V1 ,V2>,(V2, V4), <V4, V3>)

P4 = (<V1;V2>,<V2,V4>,<V4,V1>,<V1,V2>, <V2,V3>)

P5 = (<V1,V2>,<V2,V4>,<V4,V1 >,<V1,V4>,<V4,V3>)

P6= (<V1,Vl>, (V1,V1), (V1,V2), < V2, V3>)

Here,paths P1P2 and P3 are elementary path.

Path P5 is simple but not elementary.

DEFINITION:

REACHABLE:

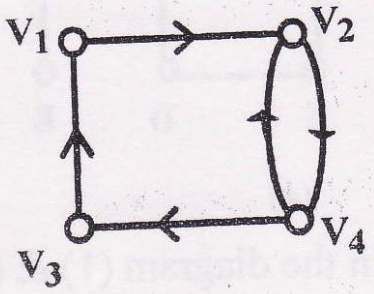
A node v of a simple digraph is-said to ber eachable from the node u of the same graph, if there exist a path from u to v.

Connected Graph :

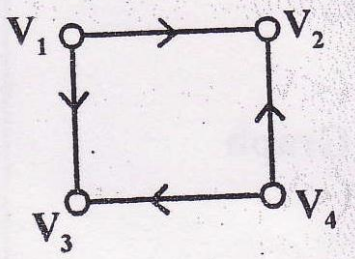
An directed graph is said to be connected if any pair of nodes are reachable from one another that is, there is a path between any pair of nodes.

A graph which is not connected is called disconnected graph.

Example 1 :



Connected Graph



Not Connected Graph

Components of a Graph :

The connected subgraphs of a graph G are called components of the.' graph G.

Theorem :

A simple graph with 'n' vertices and 'k' components can have atmost $\frac{(n-k)(n-k+1)}{2}$ ***edges***

Proof :

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

Then $n_1 + n_2 + \ldots\ldots + n_k = n = |\,V(G)\,|$

$$\sum_{i=1}^{k} n_i = n \qquad \ldots (1)$$

Now, $$\sum_{i=1}^{k} (n_i - 1) = (n_1 - 1) + (n_2 - 1) + \ldots\ldots + (n_k - 1)$$

$$= \sum_{i=1}^{k} n_i - k$$

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

Squaring on both sides

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

$$(n_1 - 1)^2 + (n_2 - 1)^2 + \ldots\ldots + (n_k - 1)^2 \leq n^2 + k^2 - 2nk$$

$$n_1^2 + 1 - 2n_1 + n_2^2 + 1 - 2n_2 + \ldots + n_k^2 + 1 - 2n_k \leq n^2 + k^2 - 2nk$$

DEFINITION:

Unilaterally Connected:

A simple digraph is said to be unilaterally connected if for any pair of nodes of the graph atleast one of the node of the pair is reachable from the node.

Strongly Connected:

A simple digraph is said to be strongly connected if for any pair of nodes of the graph both the nodes of the pair are reachable from the one another.

Weakly Connected:

We call a digraph is weakly.connected if it is connected.as an undirected graph in which the direction of the edges is neglected.

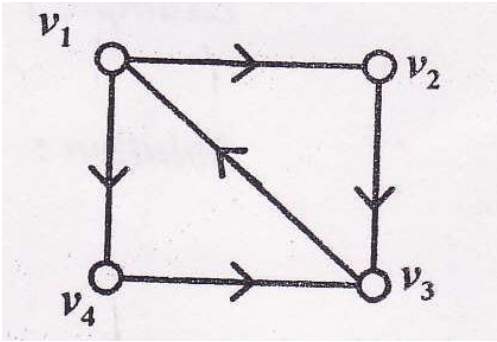
Note:

1.A unilateraaly connected digraph is weakly connectedbut a weakly connected digraph is not necessarily unilaterally connected.

2.A strongly connected digraph is both unilaterally and weakly connected.

EXAMPLE:

For example consider the graph:



It is strongly connected graph.

For,

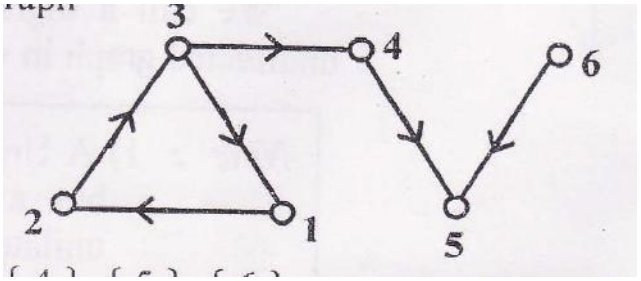
The possible pairs of vertices of the graph are (v1 v2), (v1 v3), (v1 V4), (V2 V3) and (v2 V4)

(1) Consider the pair (v1 v2)

Then there is a path from v1 to v2,via v1-> v2 and path from v2-> v1,via v2->v3->v1
(2) Consider the pair (v1 v3)
There is a path from v1 to v3, via v1 -> v2-> v3 and path from v3 to v1 via v3 -> v1.
similarly we can prove it for the remaining pair of vertices,each vertices is reachable from other.
Given graph is strongly connected

DEFINITION:

For a simple digraph maximal strongly connected subgraph is called strong component.
For the digraph:



{1,2,3},{4},{5},{6} are strong component.

The possible Hamilton cycles are
(l) A-B-C-D-A
(2) A-D-C-B-A
(3) B->C-D-A-B
(4) B-A-D-C-B
(s) C-D-A-B-C
(6) C-B-A-D-C
(7) D-A-B-C-D
(S) D-C-B-A-D
(Since all the vertices appeares exactly once),but not all the edges.
Since,G 1 contains Hamiltonian cycle,G 1- is a Hamiltonian graph.
(2) G2 contains Hamiltonian paths,namely
(1) A-> B-C-D
(2) A -> B-D-C
(3) D->C-B-A etc.

We cannot find Hamiltonian cycle in G2.
Therefore G2 is not a Hamiltonian graph

Properties :

(1) A Hamiltonianc irbuitc ontainsa Hamiltonian path but a graph , Containing a Hamiltonian path need not have a Hamiltonian cycle.
(2) By deleting any one edge from Hamiltonian cycle,we can get Hamiltonian path.
(3) A graph may contain more than one Hamiltonian cycle.
(4) A complete graph k_n, will always have a Hamiltonian cycle, when n>=3

Note :

We don't have simple necessary and sufficient criteria for the existence of Hamiltonian cycles. However, we have many theorems that give sufficient conditions for the existence of Hamiltonian cycles.
Also, certain properties can be used to show that a graph
Has no Hamiltonian cycle.F or example a, graph with a vertex of degree one cannot have a Hamiltonian cycle, since in a Hamiltonian cycle each vertex is incident with two edges in the cycle.

3.4 EULER GRAPH & HAMILTON GRAPH:

Example:Explain Konisberg bridge problem.Repersent the problem by mean of graph.Does the problem have a solution?

Solution: There are two islands A and B formed by a river.They are connected to each other and to the river banks C and D by means of 7-bridges

The problem is to start from any one of the 4 land areas.A,B,C,D, walk across each bridge exactly once and return to the starting point.(without swimmimg across the river)

This problem is the famous Konisberg bridge problem.

When the situation is represented by a graph,with vertices representating the land areas the edges representing the bridges,the graph will be shown as fig:

Theorem:

In a simple digraph,G=(V,E) every node of the digraph lies in exactly one strong component.

Proof:

Let v € V(G) and S be the set of all those vertices of G which are mutually reachable with v.

The problem is to find whether there is an Eulerian circuit or cycle(i.e.a circuit containing every edge exactly once) in a graph.

Here, we can not find a Eulerian circuit.Hence,Konisberg bridge problem has no solution .

EULER GRAPH:

Definition: Euler path:

A path of a graph G is called an Eulerian path,if it contains each edge of the graph exactly once.

Eulerian Circuit or Eulerian Cycle:

A circuit or cycle of a graph G is called an Eulerian circuit or cycle,if it includes each of G exactly once.

(Here starting and ending vertex are same).

An Eulerian circuit or cycle should satisfies the following conditions.

(1)Starting and ending points(vertices) or same.

(2)Cycle should contain all the edges of the graph but exactly once.

Eulerian Graph or Euler Graph:

Any graph containing an Eulerian circuit or cycle is called an Eulerian graph.

Theorem:

A connected graph is Euler graph(contains Eulerian circuit) if and only if each of its vertices is of even degree.

Proof:

Let G be any graph having Eulerian circuit(cycle) and let "C" be an Eulerian circuit of G with origin(and terminus) vertex as u.Each time a vertex as an internal of C,then two of the edges incident with v are accounted for degree.

We get,for internal vertex v € (G)

d(v)=2+2*{number of times u occur inside V

=even degree.

Conversely, assume each of its vertices has an even degree.

Claim: G has an Eulerian circuit.Support not, i.e.,Assume G be a connected graph which is not having an Euler circuit with all vertices of even degree and less number of edges.That is ,any degree having less number of edges than G,then it has an Eulerian circuit.Since each vertex of G has degree atleast two,therefore G contains closed path.Let C be a closed path of maximum possible length in G.If C itself has all the edges of G,then C itself an Euler circuit in G.

By assumption,C is not an Euler circuit of G and G-E© has some component G' with |E(G')|>0.C has less number of egdes than g, therefore C itself ia an Eulerian,and C has all the vertices of even degtee,thus the connected graph G' also has all the vertices of even degree.Since |E(G')|< |E(G)|,therefore G' has an Euler circuit C'.Bec ause G is connected,there is vertex v in both C and C'. Now join C and C' and transverse all the edges of C and C' with commen vertex v,we get CC' is a closed path in G and E (C C') > E (C), which is not possible for the chioices of C.

G has an Eulerian circuit.

G is Euler graph.

4.0 Introduction

In this unit we shall embark on the study of the algebraic object known as a group which serves as one of the fundamental building blocks for the subject today called abstract algebra.

4.1 ALGEBRAIC SYSTEMS - DEFINITIONS - EXAMPLES - PROPERTIES

Definition 1: Algebraic system or Algebra

A system consisting of a set and one or more n-ary operations on the set will be called an algebraic system or simply an algebra.

We shall denote an algebraic system by $(S, f_1, f_2, \ldots)$ where S is a nonempty set and $f_1, f_2, \ldots$ are operations on S.

Definition 2 : Algebraic structure

The operations and relations on the set S define a structure on the elements of S, an algebraic system is called an algebraic structure.

Example : Let I be the set of integers. Consider the algebraic system $(I, +, \times)$ where $+$ and $\times$ are the operations of addition and multiplication on I.

A list of important properties

(A-1) For any $a, b, c \in I$

$$(a + b) + c = a + (b + c) \qquad \text{(Associativity)}$$

(A-2) For any $a, b \in I$

$$a + b = b + a$$ (Commutativity)

(A-3) There exists a distinguished element $0 \in I$ such that for any $a \in I$

$$a + 0 = 0 + a = a$$ (Identity element)

Here $0 \in I$ is the identity element with respect to addition

(A-4) For each $a \in I$, there exists an element in I denoted by $-a$ and called the negative of a such that

$$a + (-a) = 0$$ (Inverse element)

(M-1) For any $a, b, c \in I$

$$(a \times b) \times c = a \times (b \times c)$$ (Associativity)

(M-2) For any $a, b \in I$

$$a \times b = b \times a$$ (Commutativity)

(M-3) There exists a distinguished element $1 \in I$ such that for any $a \in I$

$$a \times 1 = 1 \times a = a$$ (Identity element)

(D) For any $a, b, c \in I$

$$a \times (b + c) = (a \times b) + (a \times c)$$ (Distributivity)

The operation $\times$ distributes over $+$.

(C) For $a, b, c \in I$ and $a \neq 0$

$$a \times b = a \times c \Rightarrow b = c$$ (Cancellation property)

The algebraic system $(I, +, \times)$ should have been expressed as $(I, +, \times, 0, 1)$ in order to emphasize the fact that 0 and 1 are distinguished elements of I.

Definition 3 : Homomorphism

If $\{X, \circ\}$ and $\{Y, *\}$ are two algebraic systems, where $\circ$ and $*$ are binary (n-ary) operations, then a mapping $g : X \to Y$ satisfying

$g(x_1 \circ x_2) = g(x_1) * g(x_2)$ $\forall$ $x_1, x_2 \in X$ is called a homomorphism

$= [a_1 (E_1 \cap E_2) a_1'] \wedge [a_2 (E_1 \cap E_2) a_2']$

$= (a_1 E_1 a_1')$ and $(a_1 E_2 a_1') \wedge (a_2 E_1 a_2')$ and $(a_2 E_2 a_2')$

$= (a_1 E_1 a_1') \wedge (a_2 E_1 a_2')$ and $(a_1 E_2 a_1') \wedge (a_2 E_2 a_2')$

$= (a_1 * a_2) E_1 (a_1' * a_2')$ and $(a_1 * a_2) E_2 (a_1' * a_2')$

$= (a_1 * a_2) (E_1 \cap E_2) (a_1' * a_2')$

$= (a_1 * a_2) E (a_1' * a_2')$

Hence, E is a congruence relation on A.

Example 2. Let $f : S \to T$ be a homomorphism from (S, $*$) to (T, Δ) and $g : T \to P$ is also a homomorphism from (T, Δ) to (P, ∇), then g o f : S → P is a homomorphism from (S, $*$) to (P, ∇).

Solution : As $g \circ f\ (S_1 * S_2) = g\ (f\ (S_1 * S_2))$

$= g\ (f\ (S_1\ \Delta f\ (S_2))$ [Since f is [homomorphism]

$= g\ (f\ (S_1\ \nabla g\ (f\ (S_2)))$ [Since g is homomorphism]

$= g \circ f\ (S_1)\ \nabla\ g \circ f\ (S_2)$

$= g \circ f : S \to T$ is a homomorphism

Example 3. Let (A, $*$) and (B, Δ) be two algebra systems and g be homomorphism from A → B. Let (A_1, $*$) be subalgebra of (A, $*$). Then show that an the homomorphic image of (A_1, $*$) is a subalgebra of (B, Δ)

Solution : Let g be an homomorphism from A to B. Then for any two elements $a_1, a_2 \in A$.

$g\ (a_1 * a_2) = g\ (a_1)\ \Delta\ g\ (a_2)$. Let A_1 be a subset of A. As g is homomorphism from A to B, for any two elements, a_i, $a_j \in A_1 \subseteq A$.

$g\ (a_i * a_j) = g\ (a_i)\ \Delta\ g\ (a_j)$ and $g\ (A_1) \subseteq g\ (A) \subseteq B$. Therefore the image of A_1 and g forms an algebraic system with operation Δ, which becomes a subalgebra of B.

4. Given two algebraic system (W, +) and $(Z_4, +_4)$ where W is the set of all non-negative integers and + is the usual addition operation defined on W. Then show that there is a homomorphism from W to Z_4.

5. Let (W, +) be an algebraic system of non-negative integers, where + is the usual addition. Define an equivalence relation R on W such that $n_1 R n_2$ if and only if either $n_1 - n_2$ or $n_2 - n_1$ is divisible by 5. Show that R is an equivalence relation and that the homomorphism g defined from (W, +) to Z_5 by $g(i) = [i]$ is the natural homomorphism associated with R.

4.2 Semi groups and Monoids - Groups - Subgroups- Homomorphisms

Definition 1 : Semi-group : [A.U N/D 2014]

A non-empty set S, together with a binary operation $*$ is called a semi-group if $*$ satisfies the following conditions.

(i) Closure : $\forall\ a, b \in S \Rightarrow a * b \in S$

(ii) Associative : $\forall\ a, b, c \in S,\ a * (b * c) = (a * b) * c$

Example : $(Z, \cdot)$ is a semi-group.

i.e., set of integers under multiplication operation is a semi-group.

Definition 2 : Monoid : [A.U N/D 2014]

A non-empty set M, together with a binary operation $*$ is called a monoid if $*$ satisfies the following conditions

(i) Closure : $\forall\ a, b \in M \Rightarrow a * b \in M$

(ii) Associative : $\forall\ a, b, c \in M \Rightarrow a * (b * c) = (a * b) * c$

(iii) Identity : $\forall\ a \in G,\ \exists\ e \in G$

s.t. $a * e = e * a = a$

Example : $(Z, +)$ is a monoid.

Definition 3 : Group :

A non-empty set G, together with a binary operation $*$ is said to form a group, if it satisfies the following conditions.

(i) Closure : $\forall\ a, b \in G \Rightarrow a * b \in G$

(ii) Associative : $\forall\ a, b, c \in G \Rightarrow a * (b * c) = (a * b) * c$

(iii) Identity : $\forall\ a \in G, \exists\ e \in G$, s.t. $a * e = e * a = a$

(iv) Inverse : $\forall\ a \in G, \exists\ a^{-1} \in G$, s.t. $a * a^{-1} = a^{-1} * a = e$

Example : $(Z, +)$ is a group.

Definition 4 : Abelian group :

A group $(G, *)$ is said to be an abelian group or commutative group if $a * b = b * a,\ \forall\ a, b \in G$

Example : 1. $(Z, +)$ is an abelian group.

2. S_3 is a non-abelian group.

Definition 5 : Subgroup :

A non-empty subset H of a group G $(H \subseteq G)$ is a subgroup of G iff $a, b \in H \Rightarrow ab^{-1} \in H$

Example : $(Z, +)$ is a subgroup of group $(R, +)$

Definition 6 : Order of a group :

Let G be a group under the binary operation $*$. The number of elements in G is called the order of the group G and is denoted by $O(G)$

Note : If the $O(G)$ is finite, then G is called a finite group, otherwise it is called an infinite group.

Definition 7 : Semi-group homomorphism

Let (S, $*$) and (T, Δ) be any two semigroups. A mapping g : S→T such that for any two elements $a, b \in S$.

$$g(a * b) = g(a)\ \Delta\ g(b)$$

is called a semigroup homomorphism.

Illustraion :

1. $G = \{-1, 1\}$ is a cyclic group generated by -1, since $(-1)^1 = -1$ and $(-1)^2 = 1$. Thus $G = (-1)$
2. $G = \{-1, 1, i, -i\}$ is a cyclic group, where $G = <i>$. Notice that $i^1 = i$, $i^2 = -i$, $i^3 = -i$, $i^4 = 1$. Also $G = <i>$.

Definition 12 : Permutation :

Any one-to-one mapping of a set S onto S is called a permutation of S.

Definition 13 : Even and odd permutation

A permutation of a finite set is called **even** if it can be written as a product of an even number of transpositions, and it is called **odd** if it can be written as a product of an odd number of transpositions.

4.2(a) Semi-group and Monoids

Theorem 1 : The composition of semi-group homomorphism is also a semi-group homomorphism.

Proof :

Let $(S, *)$, (T, Δ) and $(V, \oplus)$ be semi-groups

Let $a, b \in S$

Define : $f : S \to T$ be semi-group homomorphism

$$\Rightarrow f(a * b) = f(a) \Delta f(b) \quad \ldots (1) \text{ where } f(a), f(b) \in T$$

Define : $g : T \to V$ be semi-group homomorphism

$$\Rightarrow g[f(a) \Delta f(b)] = g\left(f(a)\right) \oplus g\left(f(b)\right) \quad \ldots (2)$$
$$\text{where } g\left(f(a)\right), g\left(f(b)\right) \in V$$

To prove : $g \circ f : S \to V$ is a semi-group homomorphism

Proof : $g \circ f(a * b) = g[f(a * b)]$

$$= g[f(a) \Delta f(b)] \qquad \text{by (1)}$$

$$= g[f(a)] \oplus g[f(b)] \qquad \text{by (2)}$$

$$= (g \circ f)(a) \oplus (g \circ f)(b)$$

Hence, $g \circ f : S \to V$ is a semi-group homomorphism.

Note : $g \circ f(a) = g\left(f(a)\right)$

Definition : Semi-group endomorphism :

A homomorphism of a semi-group into itself is called a semi-group endomorphism.

Theorem 2. The set of all semi-group endomorphisms of a semi-group is a semi-group under the operation of left composition

Proof : Let F be the set of all semi-group homomorphism

$f : S \to S$ where $(S, *)$ is a semigroup.

To prove : $(F, \circ)$ is a semi-group with binary operation o, the left composition of mapping.

Proof :

(i) Closure : $\forall\ f, g \in F \quad \Rightarrow f \circ g \in F$

(ii) Associative : $\forall\ f, g, h \in F, \forall\ a \in S$

$$(f \circ g) \circ h\ (a) = f \circ g\left(h\ (a)\right)$$
$$= f\left(g\ (h\ (a))\right)$$
$$= f\left(g \circ h\ (a)\right)$$
$$= f \circ (g \circ h)\ (a)$$
$$\Rightarrow (f \circ g) \circ h = f \circ (g \circ h)$$

$\therefore$ $(F, \circ)$ is a semi-group.

Note : Infact (F, o) is a monoid, because the identity mapping I is the identity under o. Thus (F, o, I) is a monoid. Therefore the set of all semigroup homomorphisms of a semigroup is a monoid.

Theorem 3. Let $(S, *)$ be a given semi-group. There exists a homomorphism $g : S \to S^S$, where $(S^S, \circ)$ is a semi-group of functions from S to S under the operation of (left) composition.

[A.U N/D 2011]

Proof : For any $a \in S$

We define a function $f_a : S \to S$,

defined by $f_a(b) = a * b, \quad \forall\ b \in S$

$$\therefore f(a) \in S^S$$

Now, we define $g : S \to S^S$ by

$$g(a) = f_a, \quad \forall\ a \in S$$

Let $a, b \in S$, then $a * b \in S$

$$g(a * b) = f_{a*b}$$

$$f_{a*b}(c) = (a * b) * c, \ \forall\ c \in S$$

$$= f_a(b * c)$$

$$= f_a\left(f_b(c)\right)$$

$$= f_a \circ f_b(c)$$

$$\Rightarrow \quad f_{a*b} = f_a \circ f_b$$

$$\Rightarrow \quad g(a * b) = g(a) \circ g(b)$$

Hence, the proof.

Theorem 4. Let X be a set containing n elements, let X^* denote the free semigroup generated by X, and let (S, $\oplus$) be any other semigroup generated by any n generators ; then there exists a homomorphism $g : X^* \to S$.

Proof : Let Y be the set of n generators of S. Let $g : X \to Y$ be a one-to-one mapping given by $g(x_1) = y_i$ for $i = 1, 2, \ldots n$. Now for any string

$$\alpha = x_1, x_2, \ldots x_m$$

of X^*, we define

$$g(\alpha) = g(x_1) \oplus g(x_2) \oplus \ldots \oplus g(x_m)$$

From this definition it follows that for a string $\alpha\beta \in X^*$,

$$g(\alpha\beta) = g(\alpha) \oplus g(\beta)$$

so that g is the required homomorphism.

Theorem 5. Let (S, $*$) and (T, Δ) be two semigroups and g be a semigroup homomorphism from (S, $*$) to (T, Δ). Corresponding to the homomorphism g, there exists a congruence relation R on (S, $*$) defined by

$$x \; R \; y \qquad \text{iff } g(x) = g(y) \qquad \text{for } x, y \in S$$

Proof : It is easy to see that R is an equivalence relation on S. Let $x_1, x_2, x_1', x_2' \in S$ such that $x_1 \; R \; x_1'$ and $x_2 \; R \; x_2'$. From

$$g(x_1 * x_2) = g(x_1) \; \Delta \; g(x_2) = g(x_1') \; \Delta \; g(x_2') = g(x_1' * x_2')$$

it follows that R is a congruence relation on (S, $*$).

Theorem 6. Let (S, $*$) be a semigroup and R be a congruence relation on (S, $*$). The quotient set S/R is a semigroup (S/R, $\oplus$) where the operation $\oplus$ corersponds to the operation $*$ on S. Also, there exists a homorphism from (S, $*$) onto (S/R, $\oplus$) called the natural homomorphism.

Proof : For any $a \in S$, let $[a]$ denote the equivalence class corresponding to the congruence relation R. For $a, b \in S$ define an operation $\oplus$ on S/R given by

$$[a] \oplus [b] = [a * b]$$

The associativity of the operation $*$ guarantees the associativity of the operation $\oplus$ on S/R, so that (S/R, $\oplus$) is a semigroup. Next, define a mapping $g : S \to S/R$ given by

$$g(a) = [a] \text{ for any } a \in S$$

Property 1 : A semigroup homomosphism preserves the property of associativity.

Solution : Let $a, b, c \in S$

$$g[(a * b) * c] = g(a * b) \circ g(c)$$

$$= [(g(a) \circ g(b)) \circ g(c)] \qquad \ldots (1)$$

$$g[a * (b * c)] = g(a) \circ g(b * c)$$

$$= g(a) \circ [g(b) \circ g(c)] \quad \ldots (2)$$

But in S, $(a * b) * c = a * (b * c) \ \forall \ a, b, c \in S$

$\therefore \quad g[(a * b) * c] = g[a * (b * c)]$

$\therefore [g(a) \circ g(b)] \circ g(c) = g(a) \circ [g(b) \circ g(c)]$

The property of associativity is preserved.

Property 2 : A semigroup homomorphism preserves idempotency.

Solution : Let $a \in S$ be an idempotent element.

$\therefore \quad a * a = a$

$\therefore \quad g(a * a) = g(a)$

$g(a) \circ g(a) = g(a)$

This shows that $g(a)$ is an idempotent element in T.

$\therefore$ The property of idempotency is preserved under semigroup homomorphism.

Property 3 : A semigroup homomosphism preserves commutativity.

Solution : 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.

Property 4 : Show that every finite semigroup has an idempotent element.

Solution : Consider the subsemigroup S generated by s (i.e.,) $S = \{s, s^2, s^3, \ldots s^n\}$, where n is finite. S is a finite subset of a finite semigroup G. Therefore there exist r_1, r_2 such that $s^{r_1} = s^{r_2}$. Without loss of generality, we assume that $r_1 > r_2$.

$$g(\alpha\beta) = g(\alpha) \oplus g(\beta)$$

so that g is the required homomorphism.

Theorem 5. Let (S, $*$) and (T, Δ) be two semigroups and g be a semigroup homomorphism from (S, $*$) to (T, Δ). Corresponding to the homomorphism g, there exists a congruence relation R on (S, $*$) defined by

$$x \; R \; y \qquad \text{iff } g(x) = g(y) \qquad \text{for } x, y \in S$$

Proof : It is easy to see that R is an equivalence relation on S. Let $x_1, x_2, x_1', x_2' \in S$ such that $x_1 \; R \; x_1'$ and $x_2 \; R \; x_2'$. From

$$g(x_1 * x_2) = g(x_1) \; \Delta \; g(x_2) = g(x_1') \; \Delta \; g(x_2') = g(x_1' * x_2')$$

it follows that R is a congruence relation on (S, $*$).

Theorem 6. Let (S, $*$) be a semigroup and R be a congruence relation on (S, $*$). The quotient set S/R is a semigroup (S/R, $\oplus$) where the operation $\oplus$ corersponds to the operation $*$ on S. Also, there exists a homorphism from (S, $*$) onto (S/R, $\oplus$) called the natural homomorphism.

Proof : For any $a \in S$, let $[a]$ denote the equivalence class corresponding to the congruence relation R. For $a, b \in S$ define an operation $\oplus$ on S/R given by

$$[a] \oplus [b] = [a * b]$$

The associativity of the operation $*$ guarantees the associativity of the operation $\oplus$ on S/R, so that (S/R, $\oplus$) is a semigroup. Next, define a mapping $g : S \to S/R$ given by

$$g(a) = [a] \text{ for any } a \in S$$

Property 1 : A semigroup homomosphism preserves the property of associativity.

Solution : Let $a, b, c \in S$

$$g[(a * b) * c] = g(a * b) \circ g(c)$$

$$= [(g(a) \circ g(b)) \circ g(c)] \qquad \ldots (1)$$

$$g[a*(b*c)] = g(a) \circ g(b*c)$$

$$= g(a) \circ [g(b) \circ g(c)] \quad \ldots (2)$$

But in S, $(a*b)*c = a*(b*c) \ \forall \ a, b, c \in S$

$$\therefore \quad g[(a*b)*c] = g[a*(b*c)]$$

$$\Rightarrow [g(a) \circ g(b)] \circ g(c) = g(a) \circ [g(b) \circ g(c)]$$

$\therefore$ The property of associativity is preserved.

Property 2 : A semigroup homomorphism preserves idempotency.

Solution : Let $a \in S$ be an idempotent element.

$$\therefore \quad a*a = a$$

$$\therefore \quad g(a*a) = g(a)$$

$$g(a) \circ g(a) = g(a)$$

This shows that $g(a)$ is an idempotent element in T.

$\therefore$ The property of idempotency is preserved under semigroup homomorphism.

Property 3 : A semigroup homomosphism preserves commutativity.

Solution : 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.

Property 4 : Show that every finite semigroup has an idempotent element.

Solution : Consider the subsemigroup S generated by s (i.e.,) $S = \{s, s^2, s^3, \ldots s^n\}$, where n is finite. S is a finite subset of a finite semigroup G. Therefore there exist r_1, r_2 such that $s^{r_1} = s^{r_2}$. Without loss of generality, we assume that $r_1 > r_2$.

Now we have two cases.

Case 1 : Suppose $r_1 - 2r_2 \geq 0$

Put $r = r_1 - 2r_2$

Now

$$s^{r_1} s^r = s^{r_2} s^r = s^{r_1 - r_2}$$

$$(\because r_2 + r = r_2 + r_1 - 2r_2 = r_1 - r_2)$$

$$s^{r_1 + r} = s^{2(r_1 - r_2)}$$

This implies that S has an idempotent.

Case 2 : Suppose $r_1 - 2r_2 < 0$

Put $r_1 - r_2 = r$

$$s^{r_1} s^r = s^{r_2 + r} = s^{r_1} = s^{r_2}$$

$$s^{r_1} s^r s^r = s^{r_2 + r} = s^{r_1} = s^{r_2}$$

Proceeding in this way, we can find an integer $r_1' \geq 2r_2$ such that

$$s^{r_1'} = s^{r_2}$$

which leads to case 1.

Thus we have proved that S has an idempotent which inturn implies that the semigroup G has an idempotent.

Problems under semi-group and monoid

Example 1. Give an example of a semi-group which is not a monoid.

[A.U. M/J 2009]

Solution : Let $D = \{..., -4, -2, 0, 2, 4, ...\}$

$(D, \cdot)$ is a semi-group but not a monoid since multiplicative identity is 1, but $1 \notin D$

Example 2. Give an example of a monoid which is not a group.

Solution : $(Z^+, .)$ is a monoid which is not a group.

Since $\forall\ a \in G, \frac{1}{a} \notin G$

Example 3. What do you call a homomorphism of a semi-group into itself? **[A.U. A/M 2003]**

Solution : A homomorphism of a semi-group into itself is called a semi group endomorphism.

Example 4. If (Z, +) and (E, +) where Z is the set all integers and E is the set of all even integers, show that the two semi groups (Z, +) and (E, +) are isomorphic. **[A.U. N/D 2010]**

Solution :

Step 1 : We define the function

$G : Z \to E$ given by $g(a) = 2a$ where $a \in Z$

Step 2 : Suppose $g(a_1) = g(a_2)$ where $a_1, a_2 \in Z$

Then $2a_1 = 2a_2$ i.e., $a_1 = a_2$

Hence mapping by g is one-to-one.

Step 3 : Suppose b is an even integer

Let $a = b/2$. Then $a \in Z$ and

$g(a) = g(b/2) = 2 . b/2 = b$

i.e., every element b in E has a preimage in Z.

So mapping by g is onto.

Step 4 : Let a and $b \in Z$

$$g(a + b) = 2(a + b)$$
$$= 2a + 2b$$
$$= g(a) + g(b)$$

Hence, $(Z, +)$ and $(E, +)$ are isomorphic semigroups.

Example 5. If * is a binary operation on the set R of real numbers defined by a * b = a + b + 2ab,

(1) Find <R, *> is a semigroup.

(2) Find the identify element if it exists.

(3) Which elements has inverse and what are they?

Solution :

[A.U A/M 2011]

(1) $(a * b) * c = (a + b + 2ab) + c + 2(a + b + 2ab)c$

$= a + b + c + 2(ab + bc + ca) + 4abc$

$a * (b * c) = a + (b + c + 2bc) + 2a(b + c + 2bc)$

$= a + b + c + 2(ab + bc + ca) + 4abc$

Hence, $(a * b) * c = a * (b * c)$

i.e., $*$ is associative.

(2) If the identity element exists, let it be e.

Then for any $a \in R$.

$$a * e = a$$

i.e., $$a + e + 2ae = a$$

i.e., $$e(1 + 2a) = 0$$

$\therefore e = 0$, since $1 + 2a \neq 0$, for any $a \in R$

(3) Let a^{-1} be the inverse of an element $a \in R$. Then $a * a^{-1} = e$

i.e., $$a + a^{-1} + 2a \cdot a^{-1} = 0$$

i.e., $$a^{-1} \cdot (1 + 2a) = -a$$

$$\therefore a^{-1} = -\frac{a}{1 + 2a}$$

$\therefore$ If $a \neq \frac{1}{2}$, then $a^{-1} = \frac{-a}{1 + 2a}$

Example 6. Let $< M, *, e_M >$ be a monoid and $a \in M$. If a invertible, then show that its inverse is unique.

[A.U A/M 2011]

olution : Let b and c be elements of M
ch that $a * b = b * a = e$ and
$a * c = c * a = e$

since
$$\begin{aligned} b &= b * e \\ &= b * (a * c) \\ &= (b * a) * c \\ &= e * c \\ &= c \end{aligned}$$

Example 7. Show that a semi-group with more than one idempotents cannot be a group. Give an example of a semi-group which is not a group. **[A.U N/D 2014]**

Solution : Let $(S, *)$ be semi-group.

Let a, b are two idempotents

$\therefore\ a * a = a$ and $b * b = b$

Let us assume that $(S, *)$ is group then each element has the inverse.

$$(a * a) * a^{-1} = a * (a * a^{-1})$$

$$\text{L.H.S} = (a * a) * a^{-1} = a * a^{-1} \qquad [\because\ a * a = a]$$

$$= e$$

$$\therefore\quad (a * a) * a^{-1} = e \qquad \ldots (1)$$

$$\text{also R.H.S} = a * (a * a^{-1}) = a * e = a \qquad \ldots (2)$$

From (1) & (2), we get $a = e$

Similarly we can prove that $b = e$

In a group we can not have two identities and hence $(S, *)$ cannot ɔe group.

This contradiction is due to an assumption that $(S, *)$ has two idenpotents.

Example : Let $S = \{a, b, c\}$ under the operation $*$

Now for $x, y \in A^*$,

$$g(x) = g(y) \Leftrightarrow x \; R \; y$$

so that the congruence relation R is induced by the homomorphism g

Example 15. If $*$ is the operation defined on $S = Q \times Q$, the set of ordered pairs of rational numbers and given by $(a, b) * (x, y) = (ax, ay + b)$, show that $(S, *)$ is a semi group. Is it commutative? Also find the identity element of S. [A.U N/D 2012]

Solution : Given : $(a, b) * (x, y) = (ax, ay + b)$ ... (1)

To prove : $(S, *)$ is a semigroup.

i.e., To prove : $*$ operation is associative.

$$\{(a, b) * (x, y)\} * (c, d)$$

$$= (ax + ay + b) * (c, d) \quad \text{by (1)}$$

$$= (acx, adx + ay + b) \quad \text{... (2)}$$

$$(a, b) * \{(x, y) * (c, d)\} \quad \text{by (1)}$$

$$= (a, b) * \{cx, dx + y\}$$

$$= (acx, adx + ay + b) \quad \text{... (3)}$$

From (2) & (3), $*$ is associative on S.

To prove : $(S, *)$ is not commutative.

$$(x, y) * (a, b) = (ax, bx + y) \quad \text{... (4)}$$

$$(a, b) * (x, y) = (ax, ay + b) \quad \text{... (5)}$$

$(4) \neq (5)$ $\therefore \{S, *\}$ is not commutative.

To find the identity element of $(S, *)$

Let (e_1, e_2) be the identity element of $(S, *)$, $\forall \; (a, b) \in S$

i.e., $(a, b) * (e_1, e_2) = (a, b)$

$$(ae_1, ae_2 + b) = (a, b)$$

$$\Rightarrow \quad a e_1 = a, \; a e_2 + b = b$$

$\Rightarrow e_1 = 1, \qquad ae_2 = 0$

$e_2 = 0$

$\therefore$ (1, 0) is the identity element of $\{S, *\}$

MONOID :

Example 1 : Let X be any given set and P (X) is its power set. Then find the zeros of the semigroups (P (X), $\cap$) and (P (X), $\cup$). Are these monoids ? If so, what are the identities ?

Solution : Let X be any given set. Then its power set p (X) contains 2^X subsets of X.

If $Z \in p$ (X) is zero with respect to the operation $\cap$ for p (X), then $Z \cap X_1 = X_1 \cap Z = Z$ implies that $Z = \phi$, empty set.

The zero Z of (p (X), $\cup$) is such that $Z \cup X_1 = X_1 \cup Z = Z$ for all $X_1 \in p$ (X), implies that Z = the whole set X.

The identity of (p (X), $\cap$) is given by the set S_e, such that $S \cap S_e = S_e \cap S = S$ for all $S \in p$ (X).

Therefore S_e = X, the whole set.

The identity of (p (X), $\cup$) is S_e, which satisfies the property that $S = S_e \cup S = S \cup S_e$. Therefore S_e is the empty set ϕ.

With this it is clear that (p(X) $\cap$ X) and (p(X)$\cup \phi$) are monoids.

Example 2 : Let V = {a, b} and A be set of all sequences on V including $\wedge$ beginning with a. Show that (A, $\circ$ $\wedge$) is a monoid.

Solution : Let V = {a, b} and A be set of all sequence on V including $\wedge$ beginning with a. Then A = {$\wedge$, a, ab, aa, ab , aba, abb, ...}. Let $\circ$ be a concatenation operation on the sequences in A. Clearly for any two elements α, $b \in$ A.

$\alpha \circ \beta = \alpha\beta$ also belongs to A and hence (A, $\circ$) is closed. Also '$\circ$' is associative. Because

$$(\alpha \circ \beta) \circ \gamma = \alpha\beta\gamma = a \circ (\beta\gamma)$$
$$= (\alpha \circ \beta \circ \gamma)$$

$\wedge$ is identity as $\wedge \circ \alpha = \alpha \circ \wedge = \alpha$ for all $\alpha \in A$.

Therefore $(A, \circ, \wedge)$ is a monoid.

Example 3 : Show that the set N of natural numbers is a semigroup under the operation $x * y = \max \{x, y\}$. Is it a monoid ?

Solution : Let $N = \{0, 1, 2, ...\}$

Define the operation $x * y = \max \{x, y\}$ for $x, y \in N$.

Clearly $(N, *)$ is closed because $x * y = \max \{x, y\} \in N$ and $*$ is associative as

$$(x * y) * z = \max \{x * y, z\}$$
$$= \max \{\max \{x, y\}, z\}$$
$$= \max \{x, y, z\}$$
$$= \max \{x, \max \{y, z\}$$
$$= \max \{x, \max \{y * z\}$$
$$= x * (y * z)$$

Therefore, $(N, *)$ is semigroup.

The identity e of $(W, *)$ must satisfy the property that $x * e = e * x = e$. But as $x * e = e * x = \max \{x, e\}$, $e = x, \infty$ (the infinity). Therefore $(N, *, \infty)$ is monoid.

Example 4 : Every monoid (M, *, e) is isomorphic to $(M^M, \bullet, \Delta)$ where Δ is the identity mapping to M.

Solution : Define a mapping f from M to M^M by

$$f(a) = f_a \text{ where } f_a \in M^M$$

defined by $f_a(b) = a * b$ for any $b \in M$

Now

$$f(a * b) = f_{a*b}, \text{ where}$$

$$f_{a*b}(c) = (a * b) * c = a * (b * c)$$

$$= f_a(b * c) = f_a \cdot f_b(c)$$

Therefore, $f_{a*b} = f_a \circ f_b$, which implies that

$$f(a * b) = f_{a*b} = f_a \circ f_b = f(a) \circ f(b)$$

Therefore f is a homomorphism.

Clearly f is one-one and onto and hence f is an isomorphism from M onto M^M.

Example 5 : Prove that monoid homorphism preserves invertibility and monoid epimorphism preserves zero element (if it exists).

[A.U. N/D 2003]

Sol. Let $(M, *, e_M)$ and (T, Δ, e_T) be any two monoids and let $g: M \to T$ be a monoid homomorphism. If $a \in M$ is invertible, let a^{-1} be the inverse of a in M. We will now show that $g(a^{-1})$ will be an inverse of $g(a)$ in T.

$$a * a^{-1} = a^{-1} * a = e_M \qquad \text{(By definition of inverse)}$$

So $$g(a * a^{-1}) = g(a^{-1} * a) = g(e_M)$$

Hence $$g(a) \Delta g(a^{-1}) = g(a^{-1}) \Delta g(a) = g(e_M)$$

(since g is a homomorphism)

But $$g(e_M) = e_T \qquad \text{(since } g \text{ is a monoid hmomorphism)}$$

$$\therefore g(a) \Delta g(a^{-1}) = g(a^{-1}) \Delta g(a) = e_T$$

This means $g(a^{-1})$ is an inverse of $g(a)$ i.e., $g(a)$ is invertible. Thus the property of invertibility is preserved under monoid homomorphism.

Assume g is monoid epimorphism

$$t \Delta g(z) = g(b) \Delta g(z) = g(b * z) = g(z)$$

and $$g(z) \Delta t = g(z) \Delta g(b) = g(z * b) = g(z)$$

$\therefore$ $g(z)$ is zero element of T.

Example 6 : On the set Q of all rational numbers, the operation * is defined by a * b = a + b − ab. Show that, under this operation, Q is a commutative monoid.

Solution : Since $a + b - ab$ is rational number for all rational numbers a, b the given operation $*$ is a binary operation on Q.

We note that, for all $a, b, c \in Q$.

$$\begin{aligned}(a * b) * c &= (a + b - ab) * c \\ &= (a + b - ab) + c - (a + b - ab)c \\ &= a + b - ab + c - ac - bc + abc \\ &= a + (b + c - bc) - a(b + c - bc) \\ &= a * (b + c - bc) \\ &= a * (b * c)\end{aligned}$$

Hence $*$ is associative.

We check that, for any $a \in Q$,

$$a * 0 = a + 0 - a.0 = a$$

and $$0 * a = 0 + a - 0.a = a$$

As such, 0 is the identity element in Q under the given $*$.

The definition of $*$ itself indicates that $*$ is commutative.

Thus, under the given $*$, Q is a commutative monoid with 0 as the identity.

Example 7: Let V = {a, b}. Show that $(V^*, \bullet, \wedge)$ is an infinite monoid.

Solution : While defining alphapet and set of strings V^*, we proved that $(V^*, \bullet, \wedge)$ is a monoid where $\wedge$ is a empty string. So, it is

enough to show that V^* is an infinite set. As a is an element of V, a, aa, aaa, $aaaa$, ... b, bb, bbb, $bbbb$, ... ab, abb, $abbb$, ... are the elements of V^* and hence V^* contains infinitely many strings including empty set.

Example 8. Let $(M, *)$ be a monoid. Prove that there exists a subset $T \subseteq M^M$ such that $(M, *)$ is isomorphic to the monoid (T, O) ; here M^M denotes the set of all mappings from M to M and "O" denotes the composition of mappings. **[A.U M/J 2014]**

Proof : $\forall a \in M$, let $g(a) = f_a$ where $f_a \in M^M$ is defined by $f_a(b) = a * b$ for any $b \in M$.

Clearly, g is a function from M to M^M.

Now, $g(a * b) = f_{a*b}$, where $f_{a*b}(c) = (a * b) * c$

$= a * (b * c)$ [$\because$ Associative law]

$= f_a(b * c)$

$= (f_a \circ f_b)(c)$

$\therefore \quad f_{a*b} = f_a \circ f_b$

Hence, $g(a * b) = f_{a*b}$

$= f_a \circ f_b$

$= g(a) \circ g(b)$

$\therefore \; g(a * b) = g(a) \circ g(b) \;\; \forall \; a, b \in M$

$\therefore \; g : M \to M^M$ is a homomorphism.

Corresponding to an element $a \in M$, the function f_a is completely determined from the entries in the row corresponding to the element a in the composition table of $(M, *)$.

Since, $f_a = g(a)$, every row of such a table determines the image of 'a' under the homomorphism g.

Let $g(M)$ be the image of M under the homomorphism g such that $g(M) \subseteq M^M$.

Let $a, b \in M$, then $g(a) = f_a$ and $g(b) = f_b$ are elements in $g(M)$.

Also, $f_a \circ f_b = f(a * b) \in g(M)$ since, $a * b \in M$.

$\therefore$ $g(M)$ is closed under the operation, composition of functions.

The mapping $g : M \to g(M)$ is onto size $(M, *)$ is a monoid. No two rows of the composition table can be identical.

$\Rightarrow$ Two functions defined by these rows will be identical.

$\therefore$ The mapping $g : M \to g(M)$ is one-to-one and onto.

$\therefore$ $g : M \to g(M)$ is an isomorphism. If e is the identity element of M then we define $f_c(a) = a \ \forall \ a \in M$.

Clearly, this function $f_e \in T = g(M)$

Now, $f_e = g(e)$

Also $f_a \circ f_e = g(a) \circ g(e)$

$= g(a * e) = g(a)$

$\therefore f_a \circ f_e = g(a) = f(a)$.

This shows that f_e is the identity element of $T = g(M)$, since $f_a, f_b \in T$, $f_a \circ f_b \in T$.

$\therefore$ T is closed under the operation composition of functions.

$\therefore$ $T = g(M)$ is a monoid.

Further, $g : M \to T$ is a isomorphism.

Hence, $(M, *)$ is isomorphic to the monoid (T, o).

4.2.(b) Groups

Theorem 1.

If a and b are any two elements of a group $(G, *)$, then show that G is an abelian group if and only if

$$(a * b)^2 = a^2 * b^2$$

[A.U A/M 2003, A/M 2011, N/D 2010, M/J 2013]

Proof : If part

Given : G is an abelian group

$\Rightarrow \forall\ a, b \in G$, then $a * b = b * a$ ... (1)

To prove : $(a * b)^2 = a^2 * b^2$

$$\begin{aligned}(a * b)^2 &= (a * b) * (a * b)\\ &= a * (b * a) * b\\ &= a * (a * b) * b \quad \text{by (1)}\\ &= (a * a) * (b * b)\\ &= a^2 * b^2\end{aligned}$$

Only if part

Given : $(a * b)^2 = a^2 * b^2$ ... (2)

To prove : $a * b = b * a$

$$\begin{aligned}(2) \Rightarrow \quad (a * b)^2 &= a^2 * b^2\\ \Rightarrow (a * b) * (a * b) &= (a * a) * (b * b)\\ \Rightarrow a * [b * (a * b)] &= a * [a * (b * b)]\\ \Rightarrow \quad b * (a * b) &= a * (b * b) \text{ [Left cancellation law]}\\ \Rightarrow \quad (b * a) * b &= (a * b) * b \text{ [Associative law]}\\ \Rightarrow \quad b * a &= a * b \text{ [Right cancellation law]}\end{aligned}$$

$\Rightarrow G$ is an abelian.

Theorem 2.

If every element in a group is its own inverse, then the group must be abelian.

(OR)

For any group $(G, *)$ if $a^2 = e$ with $a \neq e$ then G is an abelian.

Proof :

Given $a = a^{-1}$ for all $a \in G$.

Let $a, b \in G$. Then $a = a^{-1}$ and $b = b^{-1}$

Now $(a * b) = (a * b)^{-1}$

i.e., $a * b = b^{-1} * a^{-1}$

$= b * a$

$\Rightarrow G$ is abelian.

Theorem 3 :

The identity element of a group is unique. [A.U. M/J 2014]

Proof :

Let $(G, *)$ be a group.

Let e_1 and e_2 be two identity elements in G.

Then

$e_1 * e_2 = e_1$ [$\because e_2$ is the identity]

$e_1 * e_2 = e_2$ [$\because e_1$ is the identity]

Thus $e_1 = e_2$

Hence the identity is unique.

Theorem 4 :

For any element a in a group G, the inverse is unique.

Proof

Let 'a' be any element of a group G.

If possible let a' and a'' be two inverses of a.

Then

$$a * a' = a' * a = e \quad \text{... (i)}$$

$$a * a'' = a'' * a = e \quad \text{... (ii)}$$

Now $a' = a' * e = a' * (a * a'') = (a' * a) * a'' = e * a'' = a''$

Hence, the inverse is unique.

$$(a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1}$$

$$= a * e * a^{-1} = a * a^{-1} = e$$

and $$(b^{-1} * a^{-1}) * (a * b) = b^{-1} * a^{-1} * a * b$$

$$= b^{-1} * e * b$$

$$= b^{-1} * b = e$$

$$\therefore \quad (a * b)^{-1} = b^{-1} * a^{-1}$$

Theorem 5.

The identity element is the only idempotent element of a group.

Solution : Given $(G, *)$ is a group.

Since $e * e = e$, e is indempotent.

Let a be any idempotent element of G.

Then $a * a = a$.

$e * a = a$. [$\because$ e is the identity element]

It follows that $a * a = e * a$.

By right cancellation law, we have $a = e$ and so e is the only idempotent element.

Now let $q \in B_n$. Then $q_0 \circ q \in A_n$, and

$$f(q_0 \circ q) = q_0 \circ (q_0 \circ q) = (q_0 \circ q_0) = 1_A \circ q = q,$$

which means that f is an onto function. Since $f : A_n \to B_n$ is one to one and onto, we conclude that A_n and B_n have the same number of elements. Note that $A_n \cap B_n = \phi$ since no permutation can be both even and odd. Also, by Theorem $|A_n \cup B_n| = n!$.

$$n! = |A_n \cup B_n| = |A_n| + |B_n| - |A_n \cap B_n| = 2|A_n|.$$

We then have

$$|A_n| = |B_n| = \frac{n!}{2}$$

PROBLEMS BASED ON GROUP

Example 1. State any two properties of a group. **[A.U N/D 2010]**

Solution : (i) The identity element of a group is unique.

(ii) The inverse of each element is unique.

Example 2. In a group G prove that an element $a \in G$ such that $a^2 = e$, $a \neq e$ iff $a = a^{-1}$

Solution : Let us assume that $a = a^{-1}$

Then $a^2 = a * a = a * a^{-1} = e$

Conversely assume that $a^2 = e$ with $a \neq e$.

That is $a * a = e$

$$a^{-1} * a * a = a^{-1} * e$$

i.e., $e * a = a^{-1}$

i.e., $a = a^{-1}$

Example 3. Determine whether the set

*	−1	1
−1	1	−1
1	−1	1

With the binary operation form a group. **[A.U June 2011]**

Solution : Yes. '1' is the identity element.

Inverse of each element is the element itself.

Example 4. Define the homomorphism of two groups.

[A.U June 2011]

Solution : Let $(G, *)$ and (H, Δ) be any two groups.

A mapping $f : G \to H$ is said to be a homomorphism if

$$f(a * b) = f(a) \Delta f(b), \text{ for any } a, b \in G$$

Example 5. If any group (G, *) and $a \in G$, then $(a^{-1})^{-1} = a$

Solution : Given : a^{-1} is the inverse of a.

$$a * a^{-1} = a^{-1} * a = e$$

$\Rightarrow$ a is the inverse of a^{-1}

i.e., $(a^{-1})^{-1} = a$

Example 6. If any group (G, *), show that $(a * b)^{-1} = b^{-1} * a^{-1}$

Solution : Given : $(G, *)$ is a group.

$\forall\ a \in G \Rightarrow a^{-1} \in G$ also $a * a^{-1} = a^{-1} * a = e$

$\forall\ b \in G \Rightarrow b^{-1} \in G$ also $b * b^{-1} = b^{-1} * b = e$

To prove : $(a * b)^{-1} = b^{-1} * a^{-1}$

i.e., To prove : $(a * b) * (b^{-1} * a^{-1}) = (b^{-1} * a^{-1}) * (a * b) = e$

$$(a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1}$$

$$= a * e * a^{-1}$$

$$= a * a^{-1} \qquad [\because a * e = a]$$

$$= e \qquad \ldots (1)$$

$$(b^{-1} * a^{-1}) * (a * b) = b^{-1} * (a^{-1} * a) * b$$

$$= b^{-1} * e * b$$

$$= b^{-1} * b \qquad [\because e * b = b]$$

$$= e \qquad \ldots (2)$$

By (1) and (2), we get

$$(a * b) * (b^{-1} * a^{-1}) = (b^{-1} * a^{-1}) * (a * b) = e$$

$$\Rightarrow \quad (a * b)^{-1} = b^{-1} * a^{-1}$$

Example 7. Every group of order 4 is abelian.

Solution : Let $(G, *)$ be a group of order 4 where $G = \{e, a, b, c\}$. Since G is of even order, there exists at least one element (say) a such that $a^{-1} = a$.

Then two cases arise

(i) $b^{-1} = b$, $c^{-1} = c$, (ii) $b^{-1} = c$, $c^{-1} = b$.

Case (i) : $e^{-1} = e$, $a^{-1} = a$, $b^{-1} = b$, $c^{-1} = c$

Every element as its own inverse.

The $(G, *)$ is abelian.

Case (ii) : $a^{-1} = a$, $b^{-1} = c$, $c^{-1} = b$

$\therefore$ $a^2 = e$, $b * c = e$, $c * b = e$

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

Since $(G, *)$ is a group, its elements will appear in a row (column) only once.

Since, a, e appears in the second row and b appears in the third column, c will appear as (2, 3)th element.

$\therefore$ (2, 4)th element is b

(3, 3)th element is a

(3, 2)th element is c

(4, 2)th element is b

(4, 4)th element is a

Example 8. Show that G $= \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \neq 0 \in R \right\}$ is an abelian group under matrix multiplication.

Solution :

(i) **Closure law**

Let $A = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$, $B = \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} \in G$.

Then $AB = \begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix} \in G$.

(ii) **Commutative Law :** $AB = BA$ is true $\forall\ A, B \in G$, since

$AB = BA = \begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix}$ $\quad [\because ab = ba$ is true in $R]$

(iii) Matrix multiplication is associative.

(iv) **Identity :** $I = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in G$ is the identity in G, since

$$AI = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = A \ \forall\ A \in G.$$

(iv) **Inverse :** If

$A = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \in G$. Then $A^{-1} = \begin{pmatrix} 1/a & 0 \\ 0 & 0 \end{pmatrix} \in G$.

is the inverse of A, since

$$AA^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = 1 \qquad (\because a \neq 0 \in R \Rightarrow 1/a \neq 0 \in R)$$

Hence G is an abelian group under matrix multiplication.

Example 9. Show that the set S = {1, 5, 7, 11} is a group w.r.t multiplication modulo 12.

Solution : The composition tables of S w.r.t O_{12} of as follows :

O_{12}	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

Here $5\ O_{12}\ 7 = 35$, which on division by 12 gives the remainder 11, $11\ O_{12}\ 7 = 77$, which on division by 12 gives the remainder 5 etc.

Hence S is a group, in which 1 is the identity and each element of S is its own inverse.

Example 10. Show that the set of matrices

$$\mathbf{G = \left\{ \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}, a \in R \right\}}$$ **forms a group under matrix multiplication.**

Solution : (i) Closure law

Let $A_\alpha = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \in G$ and $A_\beta = \begin{pmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{pmatrix} \in G$.

Then $A_\alpha A_\beta = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \begin{pmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{pmatrix}$

$$A_\alpha A_\beta = \begin{bmatrix} \cos\alpha\cos\beta - \sin\alpha\sin\beta & -(\cos\alpha\sin\beta + \sin\alpha\cos\beta) \\ \sin\alpha\cos\beta + \cos\alpha\sin\beta & \cos\alpha\cos\beta - \sin\alpha\sin\beta \end{bmatrix}$$

$$= \begin{bmatrix} \cos(\alpha+\beta) & -\sin(\alpha+\beta) \\ \sin(\alpha+\beta) & \cos(\alpha+\beta) \end{bmatrix} = A_{\alpha+\beta} \in G.$$

Note that $A_\alpha A_\beta = A_{\alpha+\beta}$ ... (1)

(ii) We know that the matrix multiplication is associative.

(iii) **Identity :** $I_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the identity in G.

Since $A_\alpha I_0 = I_0 A_\alpha = A_\alpha$ for $A_\alpha \in G$.

(iv) **Inverse :** $A_{-\alpha}$ is the inverse of A_α for each $A_\alpha \in G$, since $A_\alpha A_{-\alpha} = A_{\alpha+(-\alpha)} = A_0 = I_0$, using (1)

Example 11. Find the left cosets of {[0], [3]} in the addition modular group $(Z_6, +_6)$. **[MCA, N/D. 2002] [A.U N/D 2010]**

Solution : Let $Z_6 = \{[0], [1], [2], [3], [4], [5], [6]\}$ be a group and $H = \{[0], [3]\}$ be a sub-group of Z_6 under $+_6$ (addition mod 6)

The left cosets of H are

$$[0] + H = \{[0], [3]\} = H$$

$$[1] + H = \{[1], [4]\}$$

$$[2] + H = \{[2], [5]\}$$

$$[3] + H = \{[3], [6]\} = \{[3], [0]\} = \{[0], [3]\} = H$$

$$[4] + H = \{[4], [7]\} = \{[4], [1]\} = [1] + H$$

$$[5] + H = \{[5], [8]\} = \{[5], [2]\} = [2] + H$$

$$\therefore \quad [0] + H = [3] + H = H$$

and $$[1] + H = [4] + H, \quad [2] + H = [5] + H$$

are the distinct left cosets of H in Z_6

Example 12. If $f: G \to G'$ is a group homomorphism from {G, *} to {G', Δ} then prove that for any $a \in G$, $f(a^{-1}) = [f(a)]^{-1}$

[A.U N/D 2012]

Solution : $\forall\ a \in G$ and $\forall\ a^{-1} \in G$

$$\therefore \quad f(a * a^{-1}) = f(a)\,\Delta f(a^{-1})$$

i.e., $$f(e) = f(a)\,\Delta f(a^{-1})$$

i.e., $e' = f(a)\,\Delta f(a^{-1})$ ... (1)

|||ly, $f(a^{-1} * a) = f(a^{-1})\,\Delta f(a)$

i.e., $f(e) = f(a^{-1})\,\Delta f(a)$

$e' = f(a^{-1})\,\Delta f(a)$ ... (2)

From (1) & (2), we get

$f(a)\,\Delta f(a^{-1}) = f(a^{-1})\,\Delta f(a)$

$\Rightarrow f(a^{-1})$ is the inverse of $f(a)$

i.e., $f(a^{-1}) = [f(a)]^{-1}$

Example 13. Let G be a group and a $\in$ G. Let f : G $\to$ G be given by f(x) = a x a^{-1} for all $x \in$ G. Prove that f is an isomorphism of G on to G. **[A.U. A/M. 2005, N/D 2010]**

Solution : The map f is a homomorphism if $x, y \in$ G, then

$f(x)\,f(y) = (axa^{-1})\,(aya^{-1})$

$= ax\,(a^{-1}a)\,ya^{-1}$

$= axya^{-1}$

$= a\,(xy)\,a^{-1} = f(xy).$

So f is a homomorphism.

f is one-to-one : If $f(x) = f(y)$, then $axa^{-1} = aya^{-1}$, so by left cancellation, we have $xa^{-1} = ya^{-1}$, again by right cancellation we get $x = y$.

f is onto : Let $y \in$ G, then $a^{-1}ya \in$ G and $f(a^{-1}ya)$

$= a\,(a^{-1}ya)\,a^{-1}$

$= (aa^{-1})\,y\,(aa^{-1})$

$= y.$ So $f(x) = y$ for some $x \in$ G.

Thus f is an isomorphism.

PERMUTATION FUNCTIONS

Definition :

A bijection from a set A to itself is called a **permutation** of A.

Example 14 : Let A=R and let $f : A \to A$ be defined by $f(a) = 2a + 1$. Since f is one to one and onto, it follows that f is a permutation of A.

Example 15 : Let $A = \{1, 2, 3\}$. Then all the permutations of A are

$$I_A = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad p_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

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

Using the permutations of compute

(a) p_4^{-1} ; (b) $p_3 \circ p_2$

Solution : (a) Viewing p_4 as a function, we have

$$p_4 = \{(1, 3), (2, 1), (3, 2)\}$$

Then $$p_4^{-1} = \{(3, 1), (1, 2), (2, 3)\}$$

or, when written in increasing order of the first component of each ordered pair, we have

$$p_4^{-1} = \{(1, 2), (2, 3), (3, 1)\}$$

Thus $$p_4^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = p_3$$

(b) The function p_2 takes 1 to 2 and p_3 takes 2 to 3, so $p_3 \circ p_2$ takes 1 to 3. Also, p_2 takes 2 to 1 and p_3 takes 1 to 2, so $p_3 \circ p_2$ takes 2 to 2. Finally, p_2 takes 3 to 3 and p_3 takes 3 to 1, so $p_3 \circ p_2$ takes 3 to 1. Thus

$$p_3 \circ p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

We may view the process of forming $p_3 \circ p_2$ as shown in fig. Observe that $p_3 \circ p_2 = p_5$.

$$p_3 \circ p_2 = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & & \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & & \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = p_5$$

Theorem : If $A = \{a_1, a_2, \ldots a_n\}$ is a set containing n elements, then there are

$n! = n \,.\, (n-1) \ldots 2.1$ permutations of A

Definition : Cyclic permutation

Let $b_1, b_2, \ldots b_r$ be r distinct elements of the set $A = \{a_1, a_2, \ldots a_n\}$. The permutation $p : A \to A$ defined by

$$p(b_1) = b_2$$

$$p(b_2) = b_3$$

$$\vdots$$

$$\vdots$$

$$p(b_{r-1}) = b_r$$

$$p(b_r) = b_1$$

$p(x) = x$, if $x \in A$, $x \notin \{b_1, b_2, \ldots b_r\}$ is called a **cyclic permutation** of length r, or simply a **cycle** of length r, and will be denoted by $(b_1, b_2, \ldots b_r)$.

Example 16: Let $A = \{1, 2, 3, 4, 5\}$. The cycle (1, 3, 5) denotes the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix}$$

Example 17: Let $A = \{1, 2, 3, 4, 5, 6\}$. Compute (4, 1, 3, 5) $\circ$ (5, 6, 3) and (5, 6, 3) $\circ$ (4, 1, 3, 5).

Solution : We have

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

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

Then $(4, 1, 3, 5) \circ (5, 6, 3)$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 5 & 1 & 4 & 6 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 5 & 4 & 6 & 3 \end{pmatrix}$$

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

and $(5, 6, 3) \circ (4, 1, 3, 5)$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 5 & 4 & 6 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 5 & 1 & 4 & 6 \end{pmatrix}$$

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

Observe that

$$(4, 1, 3, 5) \circ (5, 6, 3) \neq (5, 6, 3) \circ (4, 1, 3, 5)$$

and that neither product is a cycle.

Definition :

Two cycles of a set A are said to be **disjoint** if no element of A appears in both cycles.

Example 18 : Let $A = \{1, 2, 3, 4, 5, 6\}$. Then the cycles $(1, 2, 5)$ and $(3, 4, 6)$ are disjoint, whereas the cycles $(1, 2, 5)$ and $(2, 4, 6)$ are not.

Theorem : A permutation of a finite set that is not the identity or a cycle can be written as a product of disjoint cycles of length ≥ 2.

Example 19: Write the permutation $p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 6 & 5 & 2 & 1 & 8 & 7 \end{pmatrix}$ of the set $A = \{1, 2, 3, 4, 5, 6, 7, 8\}$ as a product of disjoint cycles.

Solution : We start with 1 and find that $p(1) = 3$, $p(3) = 6$, and $p(6) = 1$, so we have the cycle (1, 3, 6). Next we choose the first element of A that has not appeared in a previous cycle. We choose 2, and we have $p(2) = 4$, $p(4) = 5$ and $p(5) = 2$, so we obtain the cycle (2, 4, 5). We now choose 7, the first element of A that has not appeared in a previous cycle. Since $p(7) = 8$ and $p(8) = 7$, we obtain the cycle (7, 8). We can then write p as product of disjoint cycles as

$$p = (7, 8) \circ (2, 4, 5) \circ (1, 3, 6).$$

Definition : Even and Odd Permutations

A cycle of length 2 is called a **transposition**. That is, a transposition is a cycle $p = (a_i, a_j)$, where $p(a_i) = a_j$ and $p(a_j) = a_i$.

Observe that if $p = (a_i, a_j)$ is a transposition of A, then $p \circ p = I_A$, the identity permutation of A.

Every cycle can be written as a product of transpositions. In fact,

$$(b_1, b_2, \ldots b_r) = (b_1, b_r) \circ (b_1, b_{r-1}) \circ \ldots \circ (b_1, b_3) \circ (b_1, b_2)$$

This case can be verified by induction on r, as follows :

Basis Step

If $r = 2$, then the cycle is just (b_1, b_2), which already has the proper form.

Induction Step

We use P (k) to show P $(k + 1)$. Let $(b_1, b_2, \ldots b_k, b_{k+1})$ be a cycle of length $k + 1$. Then $(b_1, b_2, \ldots b_k, b_{k+1}) = (b_1, b_{k+1}) \circ (b_1, b_2, \ldots b_k)$ as may be verified by computing the composition. Using P(k), $(b_1, b_2, \ldots b_k) = (b_1, b_k) \circ (b_1, b_{k-1}) \circ \ldots \circ (b_1, b_2)$. Thus, by substitution,

$(b_1, b_2, \ldots b_{k+1}) = (b_1, b_{k+1}) \circ (b_1, b_k) \circ \ldots \circ (b_1, b_3)\ (b_1, b_2)$.

This completes the induction step. Thus, by the principle of mathematical induction, the result holds for every cycle. For example,

$(1, 2, 3, 4, 5) = (1, 5) \circ (1, 4) \circ (1, 3) \circ (1, 2)$

Corollary 1 : Every permutation of a finite set with atleast two elements can be written as a product of transpositions.

Theorem : If a permutation of a finite set can be written as a product of an even number of transpositions, then it can never be written as a product of an odd number of transpositions, and conversely.

A permutation of a finite set is called **even** if it can be written as a product of an even number of transpositions, and it is called **odd** if it can be written as a product of an odd number of transpositions.

Example 20 : Is the permutation

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 5 & 7 & 6 & 3 & 1 \end{pmatrix}$$

even or odd ?

Solution : We first write p as a product of disjoint cycles, obtaining

$$p = (3, 5, 6) \circ (1, 2, 4, 7).$$

Next we write each of the cycles as a product of transpositions :

$$(1, 2, 4, 7) = (1, 7) \circ (1, 4) \circ (1, 2)$$
$$(3, 5, 6) = (3, 6) \circ (3, 5)$$

Then $p = (3, 6) \circ (3, 5) \circ (1, 7) \circ (1, 4) \circ (1, 2)$. Since p is a product of an odd number of transpositions, it is an odd permutation.

Note : From the definition of even and odd permutations, it follows.

(a) The product of two even permutation is even.

(b) The product of two odd permutations is even.

(c) The product of an even and an odd permutation is odd.

Example 21 : Show that the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 2 & 4 & 1 & 3 \end{pmatrix}$ **is odd, while the permutation** $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 4 & 5 & 2 & 1 \end{pmatrix}$ **is even.**

Solution :

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

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

The given permutation can be expressed as the product of an odd number of transpositions and hence the permutation is odd. Again

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

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

Since it is a product of even number of transposition, the permutation is an even permutation.

Example 22 : Express the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 2 & 4 & 3 & 1 \end{pmatrix}$ **as a product of transposition.**

Solution :

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

Example 23 : Find the inverse of the permutation.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$$

Solution : Given $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$

Let the inverse of the permutation be $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ x & y & z & u & v \end{pmatrix}$

Then $\begin{pmatrix}1&2&3&4&5\\2&3&1&5&4\end{pmatrix}\begin{pmatrix}1&2&3&4&5\\x&y&z&u&v\end{pmatrix}=\begin{pmatrix}1&2&3&4&5\\1&2&3&4&5\end{pmatrix}$

$\Rightarrow \begin{pmatrix}1&2&3&4&5\\y&z&x&v&u\end{pmatrix}=\begin{pmatrix}1&2&3&4&5\\1&2&3&4&5\end{pmatrix}$

$\Rightarrow y = 1, z = 2, x = 3, v = 4, u = 5.$

Hence the inverse permutation is $\begin{pmatrix}1&2&3&4&5\\3&1&2&5&4\end{pmatrix}$.

Example 24 : If A = (1 2 3 4 5), B = (2 3) (4 5). Find AB.

Solution : Given A = (1 2 3 4 5), B = (2 3) (4 5)

$$AB = \begin{pmatrix}1&2&3&4&5\\2&3&4&5&1\end{pmatrix}\begin{pmatrix}1&2&3&4&5\\1&3&2&5&4\end{pmatrix}$$

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

$$= (1\ 3\ 5)$$

Example 25 : If A = {1, 2, 3, 4, 5, 6, 7, 8} then express the following permutations as a product of disjoint cycles.

(a) $\mathbf{p} = \begin{pmatrix}1&2&3&4&5&6&7&8\\6&5&7&8&4&3&2&1\end{pmatrix}$

(b) $\mathbf{p} = \begin{pmatrix}1&2&3&4&5&6&7&8\\2&3&1&4&6&7&8&5\end{pmatrix}$

Solution :

(a) $p(1)=6,\ p(6)=3,\ p(3)=7,\ p(7)=2,\ p(2)=5,\ p(5)=4,\ p(4)=8,$
$p(8)=1.$

$\therefore p = (1, 6, 3, 7, 2, 5, 4, 8\}$

(b) $p(1) = 2,\ p(2) = 3,\ p(3) = 1 \Rightarrow (1, 2, 3)$

$p(5) = 6,\ p(6) = 7,\ p(7) = 8,\ p(8) = 5 \Rightarrow (5, 6, 7, 8)$

$p = (5, 6, 7, 8) \circ (1, 2, 3)$

Example 26 : Let A = {1, 2, 3, 4, 5, 6} and

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 1 & 5 & 6 \end{pmatrix}$$ **be a permutation of A.**

(a) Write p as a product of disjoint cycles.

(b) Compute p^{-1}

(c) Compute p^2

(d) Find the period of p, that is, the smallest positive integer k such that $p^k = 1_A$.

Solution :

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

Since $p(1) = 2$, $p(2) = 4$ and $p(4) = 1$, we write $p = (1, 2, 4)$ as the other elements are fixed.

(b) $p^{-1} = \begin{pmatrix} 2 & 4 & 3 & 1 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 3 & 2 & 5 & 6 \end{pmatrix}$

(c) $p^2 = p \circ p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 3 & 2 & 5 & 6 \end{pmatrix}$

(d) $p^3 = p^2 \circ p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = 1_A$.

$p^4 = p$, $p^5 = p^2$ etc.

$\therefore$ The period of $p = 3$.

$$(p_2 \circ p_1)^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 2 & 1 & 4 & 3 \end{pmatrix}$$

$\therefore$ $(p_2 \circ p_1)^{-1} = p_1^{-1} \circ p_2^{-1}$

Example 27 : If $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$ and

$g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ are permutations,

prove that $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Solution : $f^{-1} = \begin{pmatrix} 3 & 2 & 1 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$ and

$$g^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

$$f^{-1} \circ g^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

$$g \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

$$(g \circ f)^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

Hence $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Example 28 : Let $p_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 3 & 2 & 1 & 4 & 5 & 6 \end{pmatrix}$ and

$p_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 3 & 2 & 1 & 5 & 4 & 7 \end{pmatrix}$

(a) Compute $p_1 \circ p_2$

(b) Compute p_1^{-1}

(c) Is p_1 an even or odd permutation ? Explain.

Solution :

(a) $p_1 \circ p_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 3 & 2 & 1 & 4 & 5 & 6 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 3 & 2 & 1 & 5 & 4 & 7 \end{pmatrix}$

$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 2 & 3 & 7 & 4 & 1 & 6 \end{pmatrix}$

(b) $p_1^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 3 & 2 & 5 & 6 & 7 & 1 \end{pmatrix}$

(c) $p_1 = (1, 7, 6, 5, 4) \circ (2, 3)$

(i) **Closure :** Let $b \in H \Rightarrow b^{-1} \in H$

$\therefore$ For $a, b \in H \quad \Rightarrow a, b^{-1} \in H$

$\Rightarrow a * (b^{-1})^{-1} \in H$

$\Rightarrow a * b \in H$

$\therefore$ H is closed under the operation "$*$"

(ii) **Associative :** Since $H \subseteq G$, the elements of H are also the elements of G.

Since $*$ is associative in G, it must also be associative in H.

(iii) **Identity :** Let $a \in H, \quad \Rightarrow a * a^{-1} \in H$

$\Rightarrow e \in H$

$\therefore$ e is the identity element of H.

(iv) **Existence of inverse :** Let $e \in H$, $a \in H$

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

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

$\therefore$ Every element of H has an inverse in H.

$\therefore$ H itself is a group under the operation $*$ in G.

Theorem 2 :

Let $(G, *)$ be a finite group, and H is non-empty subset of G and H is closed under $*$. Then H is a subgroup of G.

Proof : $(G, *)$ is a finite group and H is a subset of G which is closed under $*$.

i.e., $a, b \in H \Rightarrow a * b \in H$.

Let $O(G) = n$

Now $a, a \in H$

Then $\quad a * a = a^2 \in H$

$a^2, a \in H$. Then $a^2 * a = a^3 \in H$ and so on.

Since G is finite there exists a 'm' with $1 \leq m \leq n$ such that

$$a^m = e \in H$$

That is $e \in H$

Hence identity exists.

Let $a \in H$, then $a^{m-1} \in H$.

$$\text{i.e., } a^{m-1} = a^m * a^{-1} \in H$$

$$\text{i.e., } e * a^{-1} \in H$$

$$\text{i.e., } a^{-1} \in H.$$

$\Rightarrow$ inverse exists.

Since every element of H is G, associative property is true in H.

Hence $(H, *)$ is a group and so H is a subgroup of G.

Theorem 3.

The kernal of a homomorphism g from a group $<G, *>$ to $<H, \Delta>$ is a subgroup of $<G, *>$.

Proof : Since $g(e_G) = e_H$, $e_G \in ker\,(g)$

Also , if $a, b \in ker\,(g)$,

$$\text{i.e., } g(a) = g(b) = e_H, \text{ then}$$

$$g(a * b) = g(a)\,\Delta\, g(b) = e_H \Delta e_H = e_H$$

so that $a * b \in ker\,(g)$.

Finally, if $a \in ker\,(g)$, then $g(a^{-1}) = [g(a)]^{-1} = e_H^{-1} = e_H$.

Hence $a^{-1} \in ker\,(g)$ and $ker\,(g)$ is a subgroup of $<G, *>$.

Theorem 4.

Every cyclic group is abelian. **[A.U. M/J 2013, N/D 2013]**

Solution: Let $(G, *)$ be a cyclic group generated by an element $a \in G$.

(i.e.,) $G = (a)$

Then for any two elements $x, y \in G$

We have $x = a^n$, $y = a^m$, where m, n are integer.

Therefore $x * y = a^n * a^m = a^{n+m}$

$= a^{m+n} = a^m * a^n$

$= y * x$

Thus, $(G, *)$ is abelian.

Problems based on sub group

Example 1. Is the union of two subgroups of a group, a subgroup of G? Justify your answer.

Solution : The union of two subgroups of a group need not be a subgroup of G.

Let the group $(Z, +)$

Let $H = 3Z = \{0, \pm 3, \pm 6, ...\}$

Let $K = 2Z = \{0, \pm 2, \pm 4, ...\}$

$\Rightarrow H$ and K are subgroups of $(Z, +)$.

$\Rightarrow \quad 3 \in 3Z \in 3Z \cup 2Z = H \cup K$

$\Rightarrow \quad 2 \in 2Z \in 2Z \cup 3Z = H \cup K$

But $3 + 2 = 5 \notin 2Z \cup 3Z$

$\therefore H \cup K$ is not a subgroup of $(Z, +)$

Example 2. The identity element of a subgroup is same as that of the group. **[A.U N/D 2012]**

Solution : Let H be the subgroup of the group G and e and e' be the identity elements of G and H respectively.

Now if $a \in H$, then $a \in G$ and $ae = a$, because e is the identity element of G.

Again $a \in H$, then $ae' = a$ since e' is the identity element of H.

Thus $ae = ae'$ which gives $e = e'$

Example 3. If H and K are subgroup of G, prove that H ∪ K is a subgroup of G if and only if either H ⊆ K or K ⊆ H.

[A.U N/D 2014]

Solution : Given H and K are two subgroups of G and $H \subseteq K$ or $K \subseteq H$.

If $H \subseteq K$ then $H \cup K = K$ which is a subgroup of G.

If $K \subseteq H$ then $H \cup K = H$ which is a subgroup of G.

Conversely suppose $K \not\subseteq H$ and $H \not\subseteq K$.

Then there exists $a \in H$ and $a \notin K$ and there exists a $b \in K$ and $b \notin H$.

Now $a, b \in H \cup K$. Because $H \cup K$ is a subgroup, it follows that $a * b \in H \cup K$. Hence $a * b \in H$ or $a * b \in K$.

Case (i) : If $a * b \in H$

Then $a^{-1} * (a * b) \in H$

That is $b \in H$ which is a contradiction.

Case (ii) : If $a * b \in K$

Then $a * b * b^{-1} \in K$

i.e., $a \in K$ which is a contradiction.

Thus either $H \subseteq K$ or $K \subseteq H$

Example 4. Prove that the intersection of two subgroups of a group is a subgroup of G. **[A.U M/J 2013, N/D 2013, N/D 2014]**

Solution : Given H and K are subgroups of G.

Let $a, b \in H \cap K \Rightarrow a, b \in H$ and $a, b \in K$

$\Rightarrow$ $a * b^{-1} \in H$ and $a * b^{-1} \in K$ (as H and K are subgroups)

$\Rightarrow$ $a * b^{-1} \in H \cap K$.

Thus $H \cap K$ is a subgroup of G.

Example 5. Show that the set of all elements a of a group (G, $*$) such that $a * x = x * a$ for every $x \in G$ is a subgroup of G.

[A.U N/D 2010]

Solution : Let $H = \{a \in G \mid ax = xa, \forall x \in G\}$

As $ey = ye = y$, $\forall y \in G$, $e \in G$, H is non empty.

Let x and z in H

Then $xy = yx$ and $zy = yz$ for all $y \in G$

$(xz)y = x(yz) \Rightarrow (yx)z = y(xz)$, $\forall y \in G$

$\therefore$ $xz \in H$, $\forall x, z \in H$

$x \in H \Leftrightarrow xy = yx$, $\forall y \in G$

$\Leftrightarrow x^{-1}(xy)x^{-1} = x^{-1}(yx)x^{-1}$, $\forall y \in G$

$\Leftrightarrow (x^{-1}x)(yx^{-1}) = (x^{-1}y)(xx^{-1})$

$\Leftrightarrow yx^{-1} = x^{-1}y$

$\Leftrightarrow x^{-1} \in H$

$\therefore$ H is a subgroup.

Example 6. If 'a' is a generator of a cyclic group G, then show that 'a^{-1}' is also a generator of G. **[A.U M/J 2012]**

Solution : Let $G = (a)$ be a cyclic generated by 'a'

If $x \in G$, then $x = a^n$ for some $n \in Z$

$\therefore$ $x = a^n = (a^{-1})^{-n}$, $(-n \in Z)$

$\therefore$ 'a^{-1}' is also a generator of G.

Example 7. Find all the subgroups of $(Z_9, +_9)$ **[A.U M/J 2014]**

Solution : $Z_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$

The operation is addition modulo 9.

Consider the subsets

$H_1 = \{0, 2, 4, 6, 8\}$

$H_2 = \{0, 3, 6\}$

$H_3 = \{0, 4, 8\}$

$H_4 = \{0, 5\}$

The improper subgroups of $(Z_9, +_9)$ are $[\{0\}, +_9]$ and $[Z_9, +_9]$

$+_9$	0	5
0	0	5
5	5	1

[H_4 is closed]

$+_9$	0	4	8
0	0	4	8
4	4	8	3
8	8	3	7

[H_3 is closed]

$+_9$	0	3	6
0	0	3	6
3	3	6	0
6	6	0	3

[H_2 is closed]

$+_9$	0	2	4	6	8
0	0	2	4	6	8
2	2	4	6	8	1
4	4	6	8	1	3
6	6	8	1	3	5
8	8	1	3	5	7

[H_1 is closed]

The operation tables shows that

H_1, H_2, H_3 and H_4 are closed for $+_9$

$\therefore$ The possible proper subgroups of $(Z_9, +_9)$ are $(H_1, +_9)$, $(H_2, +_9)$, $(H_3, +_9)$ and $(H_4, +_9)$

Example 8. Any cyclic group of order n is isomorphic to the additive group of residue classes of integers modulo n.

Proof :

Let $G = \{a, a^2, ..., a^n = e\}$ be a cyclic group of order n generated by a.

We know that $(Z_n, +_n)$ is the additive group of residue classes modulo n.

$\Rightarrow Z_n = \{[1], [2], ..., [n] = [0]\}$

Let $f: G \to Z_n$ defined by $f(a^r) = [r]$ for all $a^r \in G$.

For all $[r] \in Z_n$, there exists a $a^r \in G$ such that $f(a^r) = [r]$

$\Rightarrow f$ is onto.

For $r \neq s$, $[r] \neq [s]$ and hence $f(a^r) \neq f(a^s)$

$\Rightarrow f$ is one-to-one.

For all $a^r, a^s \in G$, $f(a^r . a^s) = f(a^{r+s}) = [r+s] = [r] + [s]$

$= f(a^r) +_n f(a^s)$

$\Rightarrow f$ is a homomorphism. Hence $(G, \cdot)$ is isomorphic to $(Z_n, +_n)$

Example 9. Prove that every finite group of order "n" is isomorphic to a permutation group of degree n. **[A.U M/J 2013]**

(OR)

State and prove Cayley's theorem on permutation groups.

[MCA, Nov, 93, May 95]

Proof : Let G be the given group and A (G) be the group of all permutations of the set G.

For any $a \in$ G, define a map f : G $\to$ G such that $f(x) = ax$.

f_a is well defined :

Let $x = y \Rightarrow ax = ay \Rightarrow f_a(x) = f_a(y)$. Thus f_a is well defined.

f_a is $1-1$:

Again $f_a(x) = f_a(y) \Rightarrow ax \Rightarrow x = y$. Thus f_a is $1-1$.

f_a is onto : For any $y \in$ G, $f_a(a^{-1}y) = a\,a^{-1}y$

$= y \in$ G

Thus we find a preimage $a^{-1}y$ for any "y" in G. Thus f_a is onto.

Hence f_a is permutation. (i.e.,) $f_a \in A(G)$.

Let K be the set of all such permutations. We can show that K is a subgroup of A (G). Since $e \in G$, $f_a \in K$. Thus K is non-empty.

Let $f_a, f_b \in K$.

Then $(f_a \circ f_a^{-1})(x) = f_a(a^{-1}x)$

$= aa^{-1}x$

$= ex$

$= f_e(x)$

Thus the inverse of f_a is f_a^{-1}

$(f_a \circ f_b)(x) = f_a(f_b(x))$

$= f_b(bx)$

$= abx$

$= f_{ab}(x)$

$\Rightarrow f_a \circ f_b = f_{ab} \in K.$

Thus K is a subgroup of A (G).

Next we will show that G is isomorphic to K.

Define a map : $\chi : G \to K$ such that $\chi(a) = f_a$.

χ is well defined :

For $a, b \in G$, $a = b \Leftrightarrow ax = bx$

$\Leftrightarrow f_a(x) = f_b(x)$

$\Leftrightarrow f_a = f_b$

$\Leftrightarrow \chi(a) = \chi(b)$

χ is one-one and onto.

χ is a homomorphism :

$$\chi(ab) = f_{ab} = f_a \circ f_b = \chi(a) \cdot \chi(b)$$

Thus χ is a homomorphism and hence an isomorphism which proves the theorem.

Example 10. Show that every cyclic group of order n is isomorphic to $(Z_n, +_n)$

Solution : Let (G, o) be a cyclic group of order n.

The element of G are $\{a, a^2, a^3, ..., a^n = e\}$.

The elements of Z_n are $\{[0], [1], [2], ..., [n-1]\}$.

Define

$f : D \to Z_n$ by

$f(e) = [0]$ and $f(a^i) = [i]$ for $i < n$ where f is one-one and onto.

Then $f(a^i a^j) = f(a^{i+j}) = [i + j]$

$= [i] +_n [j]$

$= f(a^i) +_n f(a^j)$

Hence f is an isomorphism.

Example 11. Define : Symmetric group, Dihedral group. Show that if (G, $*$) is a cyclic group, then every sub group of (G, $*$) must be cyclic.

(OR) **[MCA, May 93, M.U]**

Show that every subgroup of a cyclic group is cyclic.

Solution : Let (G, $*$) be a cyclic group generated by "a", and let H be a subgroup of G. If H contains the identity element alone, then trivially H is cyclic and H = (e). Suppose that H $\neq$ (e). Since H $\subseteq$ G, any element of H is of the form a^k for some integer K. Let

(ii) Group homomorphism preserves inverse

Since $a * a^{-1} = e_G = a^{-1} * a$ we have

$$g(a * a^{-1}) = g(e_G) = g(a^{-1} * a)$$

$$\Rightarrow g(a) \Delta g(a^{-1}) = e_H = g(a^{-1}) \Delta g(a)$$

$\Rightarrow g(a^{-1})$ is the inverse of $g(a)$

$$\therefore g(a^{-1}) = [g(a)]^{-1}$$

(iii) Group homomorphism

Let S be a subgroup of (G, *)

To show that $g(S) = \{x \in H / x = g(a)$ for some $a \in G\}$ is a subgroup of (H, Δ)

(i) As $e_G \in S$, $g(e_G) = e_H \in g(s)$

(ii) For each $x \in g(s)$, $\exists \quad a \in s$ such that $g(a) = x$

Since s is a sub group of G,

for each $a \in s$, $a^{-1} \in s$

$$g(a^{-1}) = [g(a)]^{-1} \in g(s)$$

$$\Rightarrow x^{-1} \in g(s)$$

(iii) For $x, y \in g(s)$, $\exists \quad a, b \in s$

Such that $g(a) = x$ and $g(b) = y$

As s is a subgroup, $a * b \in s$

$$\Rightarrow \quad g(a * b) = g(a) \Delta g(b)$$

$$= x \Delta y \in g(s)$$

$\therefore g(s)$ is a subgroup of H.

4.3 NORMAL SUB-GROUP AND COSETS - LAGRANGE'S THEOREM :

Definition 1 : Left coset of H in G.

Let (H, $*$) be a subgroup of (G, $*$). For any $a \in G$, the set a H defined by

a H = $\{a * h / h \in H\}$ is called the left coset of H in G determined by the element $a \in G$.

The element a is called the representative element of the left coset a H.

Note : The left coset of H in G determined by $a \in G$ is the same as the equivalence class $[a]$ determined by the relation left coset modulo H.

Definition 2 : Index of H in G $[i_G(H)]$

Let $(H, *)$ be a subgroup of $(G, *)$, then the number of different left (or right) cosets of H in G is called the index of H in G.

Definition 3. Normal sub-group

A subgroup (H, $*$) of (G, $*$) is called a normal sub-group if for any $a \in G$, a H = H a.

Definition 4. Quotient group (or) factor group :

Let N be a normal subgroup of a group (G, $*$).

The set of all right cosets of N in G be denoted by

$$G/N = \{Na \mid a \in G\}$$

Now, define $\otimes$ as binary operation on G/N as

$$N\ a \otimes N\ b = N\ (a * b)$$

Then (G/N $\otimes$} will form a group, called quotient group (or) factor group.

Definition 5. Direct product

Let (G, $*$) and (H, Δ) be two groups. The direct product of these two groups is the algebraic structure (G $\times$ H, $\circ$) in which the binary operation $\circ$ on G $\times$ H is given by

$$(g_1, h_1) \circ (g_2, h_2) = (g_1 * g_2, h_1 \circ \Delta h_2)$$

for any $(g_1, h_1), (g_2, h_2) \in G \times H$.

Definition 6. Group homomorphism :

Let $(G, *)$ and $(G', \cdot)$ be two groups. A mapping $f: G \to G'$ is called a group homomorphism if

$$\forall\ a, b \in G,\ f(a * b) = f(a) \cdot f(b)$$

Definition 7. Kernel of group homomorphism :

Let $(G, *)$ and $(G', \cdot)$ be two groups with e' as the identity element of G'

Let $f: G \to G'$ be a homomorphism.

$$\ker f = \{a \in G \mid f(a) = e'\}$$

Statement 1 : [Lagrange's theorem] **[A.U A/M 2004, 2005, N/D 2004]**

The order of a subgroup of a finite group divides the order of the group. (OR) If G is a finite group, then 0(H) | 0(G), for all sub-group H of G.

Statement 2 : Fundamental theorem on homomorphism of groups

If f is a homomorphism of G onto G' with kernal k, then $G/K \approx G'$.

Theorem 1 :

Let (H, $*$) be a subgroup of (G, $*$). The set of left cosets of H in G form a partition of G. Every element of G belongs to one and only one left coset of H in G.

Proof : (i) *To prove :* Every element of G belongs to one and only one left coset of H in G.

Let H be a subgroup of a group G. Let $a \in G$. Then $aH = H$ if and only if $a \in H$.

Proof : Let $a \in G$

$$aH = H = ae \in H = H \Rightarrow a \in H$$

Conversely assume that $a \in H$

Then $ah \in H$, for all $h \in H$.

So $aH \subseteq H$ ... (1)

Given any $y \in H$, $a^{-1}y \in H$ and $y = a(a^{-1}y) \in H$.

So $y \in aH$ for all $y \in H$.

(i.e.,) $H \subseteq aH$ ... (2)

From (1) and (2) $H = aH$

Hence every element of G belongs to one and only one left coset of H in G.

(ii) *To prove :* The set of left cosets of H in G form a partition of G.

Let $a, b \in G$ and H be a sub group of G.

If $aH \cap Ha \neq \phi$

Let $c \in aH \cap Ha$

As $c \in aH$ we have $cH = aH$

[$\because$ Let H be a subgroup of a group G. Let $a, b \in G$ if $b \in aH$, then $bH = aH$]

As $c \in bH$, we have $cH = bH$

So $aH = cH = bH$

Thus if $aH \cap bH \neq \phi$, then $aH = bH$.

Therefore any two distinct left cosets are disjoint. Hence the set of all (distinct) left cosets of H in G forms a partition of G.

Theorem 2 : [Lagrange's theorem]

[A.U A/M 2004, 2005, N/D 2004, 2010]
[A.U A/M 2011, June 2011, M/J 2012, M/J 2013, M/J 2014]

The order of a subgroup of a finite group divides the order of the group. (OR) If G is a finite group, then O(H) | O(G), for all sub-group H of G.

Solution : Statement : If G is a finite group and H is a subgroup of G, then order of H is a divisor of order of G.

Proof :

Let $O(G) = n$, (Here n is finite)

Let $G = \{a_1 = e, a_2, a_3, \ldots a_n\}$ and let H be a subgroup of G

Consider the left cosets as follows

$e * H = \{e * h \setminus \in H\}$

$a_2 * H = \{a_2 * H \setminus h \in H\}$

$a_n * H = \{a_n * h \setminus h \in H\}$

We know that any two left cosets are either identical or disjoint.

Also $O(e * H) = O(H)$

$\therefore$ $O(a_i * H) = O(H), \quad \forall\, a_i \in G.$

Otherwise if $a * h_i = a * h_j$ for $i \neq j$, by cancellation laws, we would have $h_i = h_j$, which is a contradiction.

Let there be k – disjoint cosets of H in K. Clearly their union equals G (i.e.,) $G = (a_1 * H) \cup (a_2 * H) \cup \ldots \cup (a_k * H)$

$$\therefore O(G) = O(a_1 * H) + O(a_2 * H) + \ldots + O(a_k * H)$$

$$= \underbrace{O(H) + O(H) + \ldots + O(H)}_{K \text{ - times}}$$

$$O(G) = K \cdot O(H)$$

This implies O(H) is a divisor of O(G).

Theorem 3 : Let (G, $*$) and (H, Δ) be groups and g : G → H be a homomorphism. Then the Kernel of g is a normal sub-group.

[A.U. N/D, 2004] [A.U A/M 2011, M/J 2012, M/J 2013]

Solution : Let K be the Kernel of the homomorphism g (i.e.,) $K = \{x \in G \backslash g(x) = e'$, where $e' \in H$ is the identity element of H$\}$

To prove that K is a subgroup :

Let $x, y \in K$, then $g(x) = e'$ and $g(y) = e'$.

Claim : $x * y^{-1} \in K$

By definition of homomorphism,

$$g(x * y^{-1}) = g(x) \Delta g(y^{-1}) = g(x) \Delta [g(y)]^{-1}$$

$$= e' \Delta (e')^{-1}$$

$$= e' \Delta e' = e'.$$

Hence $x * y^{-1} \in K$ and this proves K is a sub-group of G by a criterion for sub-groups.

To prove that K is normal : Let $x \in K$, $f \in G$, then $g(x) = e'$

Claim : $f * x * f^{-1} \in K$

$$g(f * x * f^{-1}) = g(f) * g(x) * g(f^{-1})$$

$$= g(f) \cdot e^{-1} [g(f)]^{-1}$$

$$= g(f) [g(f)]^{-1}$$

$$= e'$$

$\therefore f * x * f^{-1} \in K$.

Thus K is a normal subgroup of G.

Theorem 4 : (Fundamental Thereom on homomorphism of groups) If f is a homomorphism of G onto G′ with kernal K, then $G/K \cong G'$.

[A.U June 2011, N/D 2013]

Proof :

Let $f : G \to G'$ be a homomorphism from the group $(G, *)$ to the group (G', Δ).

Then $K = \text{Ker } (f) = \{x \in G \mid f(x) = e'\}$

is a normal sub-group of $(G, *)$

Also we know that the quotient set $(G/K, \otimes)$ is a group.

Define $\phi : G/K \to G'$ is mapping from the group $(G/K, \otimes)$ to the group (G', Δ), given by

$$\phi\ (K\ a) = f(a), \text{ for any } a \in G$$

Since, if $K\ a = K\ b$

$$\Rightarrow a * b^{-1} \in K$$

$$\Rightarrow f(a * b^{-1}) = e'$$

$$\therefore f(a)\ \Delta\ f(b^{-1}) = e'$$

$$f(a)\ \Delta\ [f(b)]^{-1} = e'$$

$$f(a)\ \Delta\ [f(b)]^{-1}\ \Delta\ [f(b)] = e'\ \Delta f(b)$$

$$\Rightarrow \quad f(a)\ \Delta\ e' = f(b)$$

$$\Rightarrow \quad f(a) = f(b)$$

$$\Rightarrow \quad \phi\ (Ka) = \phi\ (Kb)$$

ϕ is well defined.

Claim : ϕ is a homomorphism.

Let $Ka, K\ b \in G/K$

Now $\phi\ (K\ a \otimes K\ b) = \phi\ [K\ (a * b)\ ]$

$= f[\ (a * b)\ ]$

$= f(a)\ \Delta f(b)$

$= \phi\ (Ka)\ \Delta\ (K\ b)$

$\therefore\ \phi$ is a homomorphism.

Claim : ϕ is one-to-one.

If $\phi\ (Ka) = \phi\ (K\ b)$

then $f(a) = f(b)$

$f(a)\ \Delta f(b^{-1}) = f(b)\ \Delta f(b^{-1})$

$f(a * b^{-1}) = f(b * b^{-1}) = f(e) = e'$

$\therefore\ a * b^{-1} \in K \Rightarrow K\ a = K\ b$

$\therefore\ \phi$ is one-to-one.

Claim : ϕ is onto.

Let y be any element of G'.

Since $f : G \to G'$ is a homomorphism from G onto G', therefore there exists an element $a \in G$ such that $f(a) = y$.

$\therefore$ For every $a \in G$, $K\ a \in G/K$

We get $\phi\ (K\ a) = f(a)$, for all $f(a) = y \in G'$

$\therefore\ \phi$ is onto.

$\therefore\ \phi : G/K \to G'$ is an isomorphism

$$G/K \equiv G'.$$

Theorem 5 : Prove that the intersection of two normal subgroups is a normal subgroup. **[MCA May, 91, MU] [A.U M/J 2013]**

Solution : Let H and K be any two normal subgroups of a group G.

We have to prove that $H \cap K$ is normal in G.

Since H and K are subgroups of G, $e \in H$ and $e \in K$.

Hence $e \in H \cap K$. Thus $H \cap K$ is a non-empty set.

Let $a, b \in H \cap K$

Claim : $ab^{-1} \in H \cap K$

Since, $a, b \in H \cap K$, both a, b being to H and K.

Since H and K are subgroups of G, $ab^{-1} \in H$ and $ab^{-1} \in K$ so that $ab^{-1} \in H \cap K$.

Hence $H \cap K$ is a subgroup of G, by a criterion for subgroup.

To prove : $H \cap K$ is normal :

Let $x \in H \cap K$, and let $g \in H$

Since $x \in H \cap K$ and $x \in H$ and $x \in K$.

Since $x \in H$, $g \in G$, $\Rightarrow gxg^{-1} \in K$ (as H is normal)

Likewise $x \in K$, $g \in G \in gxg^{-1} \in K$ (as K is normal)

Hence $x \in H \cap K$ and $g \in G \Rightarrow gxg^{-1} \in H \cap K$.

This $H \cap K$ is a normal subgroup of G.

Theorem 6 : Every subgroup of an abelian group is a normal subgroup.

[A.U N/M 2013]

Proof : Let (G, $*$) be an abelian group and (N, $*$) be a subgroup of G.

Let g be any element in G and let $n \in N$.

Now, $g * n * g^{-1} = (n * g) * g^{-1}$ [$\because$ G is abelian]

$= n * (g * g^{-1})$

$= n * e$

$= n \in N$

$\therefore \forall A\ g \in G$ and $n \in N$, $g * n * g^{-1} \in N$

$\therefore$ (N, $*$) is a normal subgroup.

Theorem 7 : Let $< H, * >$ be a subgroup of $< G, * >$. Then show that $< H, * >$ is a normal subgroup iff $a * h * a^{-1} = H, \forall a \in G$.

[MCA, Nov., 93, May 92, MU]

Solution : Let H be normal in G.

Then by definition $a * H = H * a$, for all $a \in G$.

$$\text{Then } a * H * a^{-1} = a * (a^{-1} * H)$$

$$= (a * a^{-1}) * H$$

$$= e * H$$

$$= H$$

Conversely let $a^{-1} * H * a = H$, for all $a \in G$.

(i.e.,) $a * (a^{-1} * H * a) = a * H)$

(i.e.,) $(a * a^{-1}) * (H * a) = a * H$

(i.e.,) $e * (H * a) = a * H$

(i.e.,) $H * a = a * H$

Thus H is a normal subgroup.

Theorem 8 : Let $< A, * >$ be a group. Let $H = \{a/a \in G$ and $a * b = b * a\ \forall\ b \in G\}$. Show that H is a normal subgroup.

[MCA May, 1990, March, 96, MU]

Solution : $H = \{a \in G \mid a * b = b * a, \forall\ b \in G\}$.

Since $e * a = a * e = a, \forall\ a \in G$, we have $e \in H$.

$\therefore$ H is non-empty

Let $x, y \in H$. Then

$a * x = x * a, \forall\ x \in G$ and $a * y = y * a, \forall\ y \in G$.

4.4 DEFINITIONS AND EXAMPLES OF RINGS AND FIELDS :

Definition 1 : Ring **[A.U M/J 2014]**

An algebraic system (S, +, .) is called a ring if the binary operations + and . on S satisfy the following three properties :

1. (S, +) is an abelian group
2. (S, .) is a semigroup
3. The operation . is distributive over + ; that is, for any $a, b, c \in S$,

$a . (b + c) = a . b + a . c$ and $(b + c) . a = b . a + c . a$

Examples :

1. The set of all integers Z, the set of all rational numbers R^+, the set of all real numbers R are rings under the usual addition and usual multiplication.

2. The set of all $n \times n$ matrices M_n is a ring under the matrix addition and matrix multiplication.

3. If n is a positive integer, then $Z_n = \{\overline{0}, \overline{1}, \ldots \overline{n-1}\}$ is a ring under $+_n$, the addition modulo n and $\times_n$, the multiplication modulo n.

4. Let (R, +, .) be a ring and X be a non-empty set. Let A be the set of all functions from X to R. (i.e.,) $A = \{f \mid f : X \to R$ is a function$\}$ we define $\oplus$ and . on A as follows :

(i) if $f, g \in A$, then $f \oplus g : X \to R$ is given by $(f \oplus g)(x) = f(x) + g(x)$ for all $x \in X$.

(ii) if $f, g \in X$ then $f . g : X \to R$ is given by $(f . g)(x) = f(x) . g(x)$ for all $x \in X$.

Definition 2 : Integral domain.

A commutative ring $(S, +, \bullet)$ with identity and without divisors of zero is called can integral domain.

Definition 3 : Field

A commutative ring $(S, +, \bullet)$ which has more than one element such that every non-zero element of S has a multiplicative inverse in S is called a field.

Definition 4 : Sub ring.

A subset $R \subseteq S$ where $(S, +, \bullet)$ is a ring is called a subring if $(R, +, \bullet)$ is itself with the operations $+$ and $\bullet$ restricted to R.

Examples :

1. The ring of integers Z is a subring of the ring of all rational numbers Q.

2. In Z the ring of all integers the set of all even integers is a subring.

Definition 5 : Ring homomorphism

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

$$g(a + b) = g(a) \oplus g(b) \text{ and}$$

$$g(a \,.\, b) = g(a) \odot g(b)$$

Examples :

1. The ring M_n of all non-matrices is not commutative and has non-zero zero divisors. For example : Let $n = 2$, then if $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ then $AB = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ and $BA = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. So $AB \neq BA$ and A is non-zero zero divisor.

2. The ring Q of all rational numbers, and the ring R of real numbers are fields.

3. The ring $(Z_7, +_7, \times_7)$ is a field.

4. The ring $(Z_{10}, +_{10}, \times_{10})$ is not an integral domain. (as $5 \times_{10} 2 = 0$, yet $5 \neq 0$, $2 \neq 0$ in Z_{10}).

5. The ring Z of all integers is an integral domain but not a field.

Definition 6. Commutative Ring :

A ring $(R, +, codt)$ is said to be commutative if $a \,.\, b = b \,.\, a \;\forall\; a, b \in R$

Theorem 1 : Every finite integral domain is a field.

Proof : Let (R, +, •) be a finite integral domain.
To prove (R − {0}, •) is a group
i.e., to prove

(i) there exists an element $1 \in R$ such that $1 \,.\, a = a \,.\, 1 = a$, for all $a \in R$ ($1 \in R$ is an identity)

(ii) for every element of $0 \neq a \in R$, there exists an element $a^{-1} \in R$ such that

$$a \,.\, a^{-1} = a^{-1} \,.\, a = 1$$

Let $R - \{0\} = \{a_1, a_2, a_3, \ldots a_n\}$

Let $a \in R - \{0\}$, then the elements $aa_1, aa_2, \ldots aa_n$ are all in R - {0} and they are all distinct.

(i.e.,) If $a \,.\, a_i = a \,.\, a_j$, $i \neq j$

then $a \,.\, (a_i - a_j) = 0$

Since R is an integral domain and $a \neq 0$, we must have $a_i - a_j = 0$,

(i.e.,) $a_i = a_j$ which is a contradiction.

$\therefore$ R - {0} has exactly n elements, and R is a commutative ring with cancellation law

$\therefore$ we get $a = a \cdot a_{i_0}$, for some i_0 (since $a \in$ R - {0})

i.e., $a \cdot a_{i_0} = a_{i_0} \cdot a$ (Since R is commutative)

Thus, let $x = a \cdot a_i$ for same $a_i \in R - \{0\}$, and

$$y \cdot a_{i_0} = a \cdot a_{i_0} = (a_i \cdot a)\, a_{i_0} = a_i \cdot a = a \cdot a_j = y$$

$\therefore$ Hence a_{i_0} is an unity R - {0}. We write it as 1.

Since $1 \in$ R - {0}, therefore there exists an element $aa_k \in$ R-{0} such that

$$aa_k = 1$$

$\therefore$ $ba = ab = 1$ (let $a_k = b$)

$\therefore$ b is the inverse of a, and conversely.

Hence (R, +, $\cdot$) is a field.

Thereom 2 : Every field is an integral domain, but the converse need not be true.

Proof :

Let (F, +, $\cdot$) is a field.

(i.e.,) F is a commutative ring with unity.

To prove F is an integral domain it is enough to show that it has non zero divisor.

Let $a, b \in$ F, such that $a \cdot b = 0$

Let $a \neq 0$, then $a^{-1} \in$ F

$$\therefore a \cdot b = 0$$

$$\Rightarrow a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0$$

5.1 PARTIAL ORDERING-POSETS - LATTICES AS POSETS

Def. Partial order relation

A binary relation R in a set P is called a partial order relation or a partial ordering in P iff R is reflexive, antisymmetric, and transitive.

Def. Poset

A set P together with a partial ordering R is called a partially ordered set or a poset.

Note : It is conventional to denote a partial ordering by the symbol $\leq$. This symbol does not necessarily mean "lessthan or equal to" as is used for real numbers.

Def. Totally ordered set.

Let $(P, \leq)$ be a partially ordered set. If for every $x, y \in P$ we have either $x \leq y \vee y \leq x$, then $\leq$ is called **simple ordering** or **linear ordering** on P and $(P, \leq)$ is called a **totally ordered** or **simply ordered set** or a **Chain**

Example : The poset $(Z, \leq)$ is totally ordered, since $a \leq b$ or $b \leq a$ whenever a and b are integers.

Def. Let $(P, \leq)$ be a partially ordered set and let $A \subseteq P$. Any element $x \in P$ is an upper bound for A if for all $a \in A$, $a \leq x$.

Similarly, any element $x \in P$ is a lower bound for A if for all $a \in A$, $x \leq a$

Def. Let $(P, \leq)$ be a partially ordered set and let $A \subseteq P$. Any element $x \in P$ is a least upper bound or supremum, for A if x is an upper bound for A and $x \leq y$ where y is any upper bound for A. Similarly, then greatest lower bound, or infimum, for A is an element $x \in P$ such that x is a lower bound and $y \leq x$ for all lower bounds y.

Def. Well-ordered

A partially ordered set is called well-ordered if every nonempty subset of it has a least member.

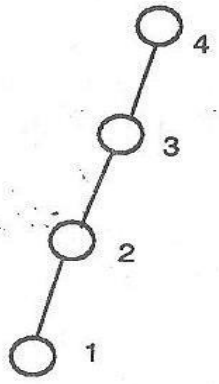
Def. Hasse diagram or partially ordered set diagram.

A partial ordering $\leq$ on a set P can be represented by means of a diagram known as a Hasse diagram or a partially ordered set diagram of $(P, \leq)$. In such a diagram, each element is represented by a small circle or a dot.

The circle for $x \in P$ is drawn below the circle for $y \in P$ if $x < y$, and a line is drawn between x and y if y covers x.

If $x < y$ but y does not cover x, then x and y are not connected directly by a single line. However, they are connected through one ore more elements of P. It is possible to obtain the set of ordered pairs in $\leq$ from such a diagram.

Example : Let $P = \{1, 2, 3, 4\}$ and $\leq$ be the relation "lessthan or equal to" then the Hasse diagram is



Note :

1. Hasse diagram, named after the twentieth - Century German mathematician Helmut Hasse.
2. In a digraph we apply the following rules then we get Hasse diagram.

(i) Each vertex of A must be related to itself. So the arrows from a vertex to itself are not necessary.

(ii) If a vertex b appears above vertex a and if vertex a is connected to vertex b by an edge, then aRb, so direction arrows are not necessary.

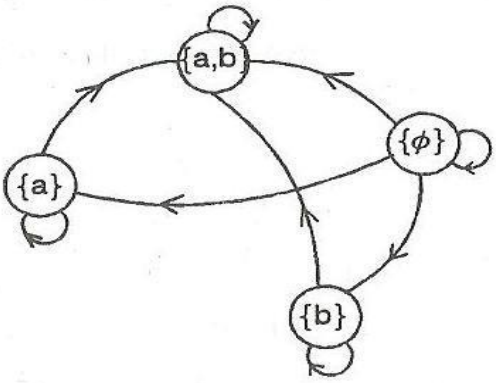
(iii) If vertex C is above a and if c is connected to a by a sequence of edges then arc.

(iv) The vertices are denoted by points rather than by circles.

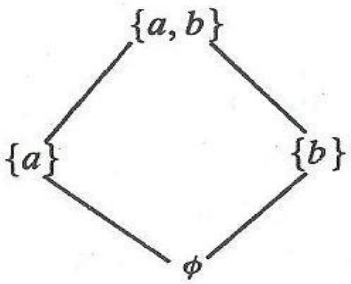
Example. Let $A = \{a, b\}$

$B = P(A) = \{\{\phi\},\{a\},\{b\},\{a,b\}\}$

Then $\subseteq$ is a relation an a whose diagraph is as follows



Hasse diagram



Example 1. Show that the "greater than or equal" relation ($\geq$) is a partial ordering on the set of integers.

Solution : Since $a \geq a$ for every integer a, $\geq$ is reflexive. If $a \geq b$ and $b \geq a$, then $a = b$. Hence, $\geq$ is antisymmetric. Finally, $\geq$ is transitive since $a \geq b$ and $b \geq c$ imply that $a \geq c$. It follows that $\geq$ is a partial ordering on the set of integers and $(Z, \geq)$ is a poset.

Example 2. Show that the inclusion relation $\subseteq$ is a partial ordering on the power set of a set S.

Solution : Since $A \subseteq A$ whenever A is a subset of S, $\subseteq$ is reflexive. It is antisymmetric since $A \subseteq B$ and $B \subseteq A$ imply that $A = B$. Finally $\subseteq$ is transitive, since $A \subseteq B$ and $B \subseteq C$ imply that $A \subseteq C$. Hence, $\subseteq$ is a partial ordering on P(S), and (P (S), $\subseteq$) is a poset.

Example 3. Let R be a binary relation on the set of all positive integers such that R = {(a, b)/a = b^2)}. Is R reflexive ? Symmetric ? Antisymmetric ? Transitive ? An equivalence relation ? A partial ordering relation ? **[MCA, MU, Nov. 1990, Dec. 1992]**

Solution : R = $\{(a, b)/a, b$ are positive integers and $a = b^2\}$. For R to be reflexive, we should have a R a for all positive integers a. But aRa holds only when $a = a^2$ by hypothesis. Now $a = a^2$ is not true for all positive integers. Infact only for the positive integer $a = 1$, we have a = a^2. Hence R is not reflexive.

For R to be symmetric, if aRb then we should have bRa. But aRb implies $a = b^2$. But $a = b^2$ does not imply $b = a^2$ always for positive integers. For instance $16 = 4^2$ but $4 \neq 16^2$. Hence aRb does not imply bRa. Hence R is not symmetric.

For R to be anti-symmetric, for positive integers a, b if a R, b and $b\,R\,a$ hold, then $a = b$. aRb implies $a = b^2$ and bRa implies $b = a^2$, So if $a = b^2$ and $b = a^2$, then $a = b^2 = (a^2)^2 = a^4$ i.e, $a^4 - a = 0$, i.e., $a\,(a^3 - 1) = 0$. Since a is not a positive integer, $a \neq 0$ so that $a^3 - 1 = 0$ i.e., $a^3 = 1$ i.e., $a = 1$. This means $b = a^2 = 1$. Thus aRb and bRa imply $a = b = 1$. Hence R is anti-symmetric.

For R to be transitive, if aRb holds and bRc holds, the aRc should hold.

i.e., aRb implies $a = b^2$ and bRc implies $b = c^2$.

So that $a = b^2 = c^4$. Hence aRc does not hold.

For example, $256 = 16^2$ and $16 = 4^2$ but $256 \neq 4^2$ (in fact $256 = 4^4$). Thus R is not transitive.

Also, R is not an equivalence relation as an equivalence relation is reflexive, symmetric and transitive. R is also not a partial ordering relation, as a partial ordering relation is reflexive, anti-symmetric and transitive.

Example 4. Let X = {2, 3, 6, 12, 24, 36} and the relation ≤ be such that x ≤ y if x divides y. Draw the Hasse diagram of (x, ≤)

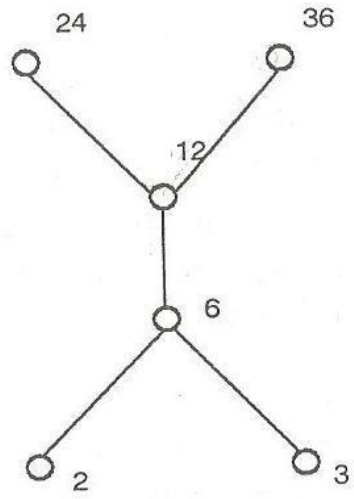
Solution :

The relation

$R = \{(x, y) / x \mid y\},\ x \leq y$

$= \{(2, 6), (2, 12), (2, 24), (2, 36),$
$(3, 6), (3, 12), (3, 24), (3, 36),$
$(6, 12), (6, 24), (6, 36)$
$(12, 24), (12, 36)\}$

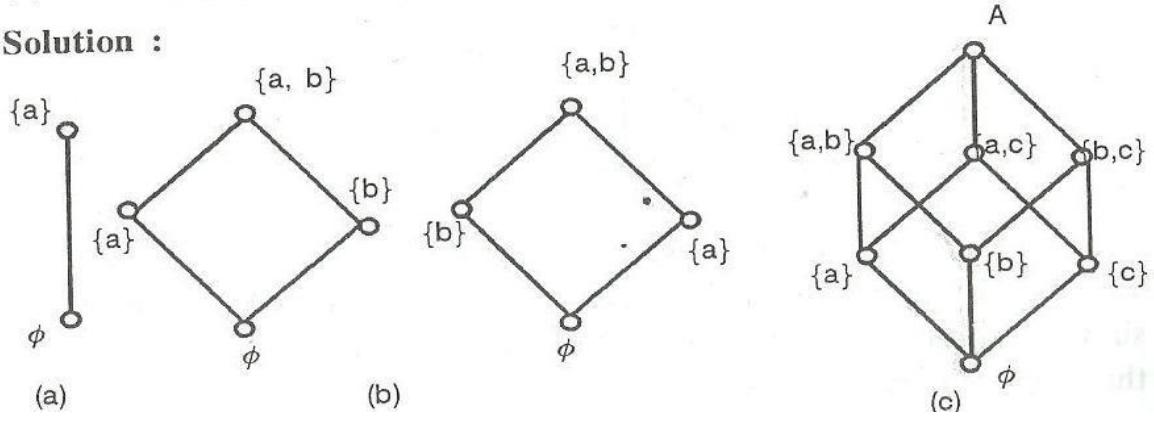
The Hasse diagram is

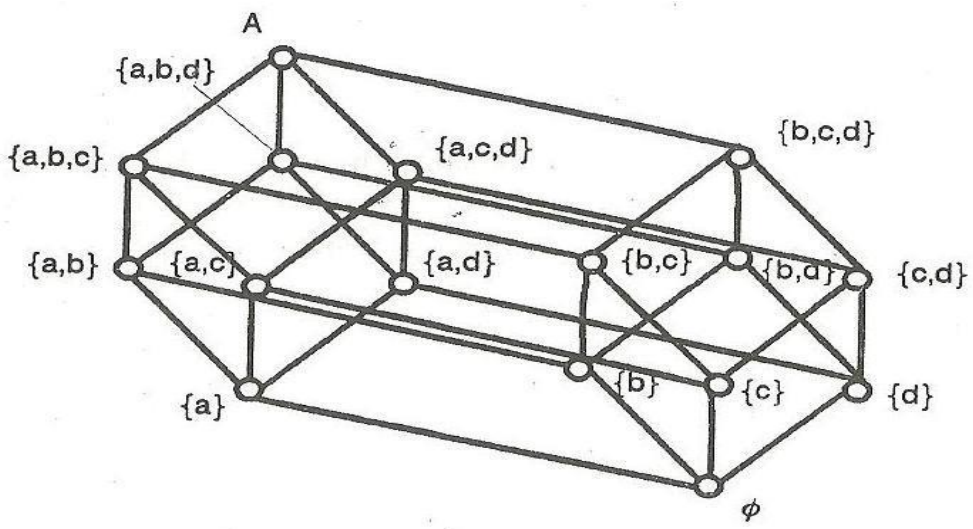


Example 5. Let A be a given finite set and P(A) its power set. Let ⊆ be the inclusion relation on the elements of ρ(A). Draw Hasse diagram of $P(A), \subseteq$) for (a) A = $\{a\}$ (b) A = $\{a, b\}$

(c) A = $\{a, b, c\}$ (d) A = $\{a, b, c, d\}$

Solution :



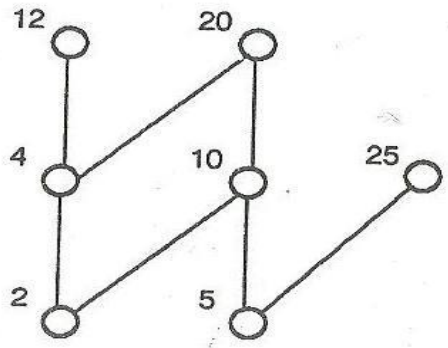


Example 6. Give a relation which is both a partially ordering relation and an equivalence relation on a set.

Solution : Equality, similarity of triangles are the examples of relation which are both a partial ordering relation and an equivalence relation.

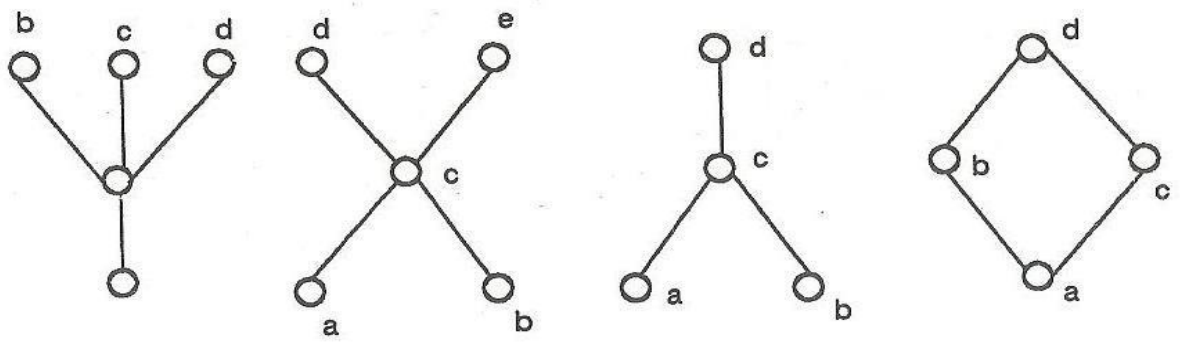
Example 7. Which elements of the poset {{2, 4, 5, 10, 12, 20, 25}, |} are maximal, and which are minimal?

Solution : Draw Hasse diagram



From the figure this poset shows that the maximal elements are 12, 20 and 25 and the minimal elements are 2 and 5. As this example shows, a poset can have more than one maximal element and more than one minimal element.

Example 8. Determine whether the posets represents by each of the Hasse diagrams in the following figure, have a greatest element and a least element.



(a) (b) (c) (d)

Solution : The least element of the poset with Hasse diagram (a) is a. This poset has no greatest element. The poset with Hasse diagram (b) has neither a least not a greatest element. The poset with Hasse diagram (c) has no least element. Its greatest element is *d*. The poset with Hasse diagram (d) has least element *a* and greatest element *d*.

Example 9. Let S be a set. Determine whether there is a greatest element and a least element in the poset (P(S), ⊆).

Solution : The least element is the empty set since $\phi \subseteq T$ for any subset T of S. The set S is the greatest element in this poset. Since $T \subseteq S$ whenever T is a subset of S.

Example 10. Is there a greatest element and a least element in the poset $(Z^+, 1)$?

Solution : The integer 1 is the least element since 1/n whenever *n* is a positive integer. Since then is no integer that is divisible by all positive integers, there is no greatest element.

5.2 Properties of Lattices - Lattices as Algebraic Systems - Sublattices - Direct Product and Homomorphism - Some Special Lattices

In order to emphasize the role of an ordering relation, a lattice is first introduced as a partially ordered set. Both lattices and Boolean algebra have important applications in the theory and design of computers. There are many other areas such as engineering and science to which Boolean algebra is applied.

Def. Lattice

A lattice in a partially ordered set $(L, \leq)$ in which every pair of elements $a, b \in L$ has a greatest lower bound and a least upper bound.

Def. Greatest Lower Bound (GLB) and Least Upper Bound (LUB)

The GLB of a subset $\{a, b\} \subseteq L$ will be denoted by $a * b$ and the least upper bound by $a \oplus b$

i.e., GLB $\{a, b\} = a * b$ (meet or product of a and b)

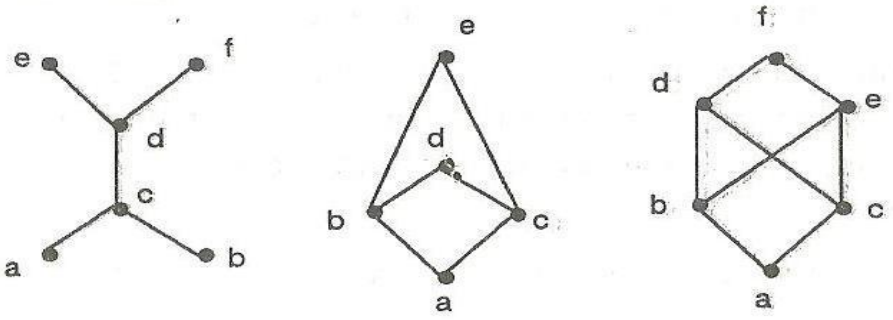
LUB $\{a, b\} = a \oplus b$ (join or sum of a and b)

Note : 1. From the definition of a lattice that both $*$ and $\oplus$ are binary operations on L because of the uniqueness of the LUB and GLB of any subset of a poset.

2. If is obvious that, a totally ordered set is trivially a lattice, but not all partially ordered sets are lattices, can be concluded from Hasse diagrams of posets.

Remark : GLB, LUB may or may-not exist for a subset.

Solution : Given :



(i) (ii) (iii)

(i) Doesnot represent a lattice, because $e \oplus f$ does not exists.

(ii) Does not represent a lattice, because $b \oplus c$ does not exits.

(iii) Does not represent a lattice, because neither $d \oplus c$ not $b * c$ exists.

Example 7.

Let the sets S_0, S_1, ..., S_7 be given by

$S_0 = \{a, b, c, d, e, f\}$, $S_1 = \{a, b, c, d, e\}$

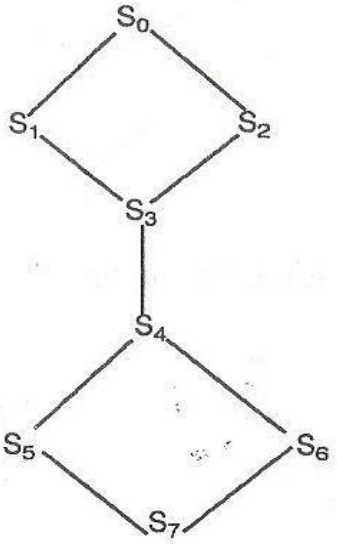
$S_2 = \{a, b, c, d, e, f\}$, $S_3 = \{a, b, c, e\}$

$S_4 = \{a, b, c\}$ $S_5 = \{a, b\}$, $S_6 = \{a, c\}$

$S_7 = \{a\}$

Draw the diagram of (L, $\subseteq$) where $L = \{S_0, S_1, S_2, \ldots, S_7\}$

Solution :



Some properties of Lattices

PROPERTY 1 : Let (L, ≤) be a lattice. For any $a, b, c \in L$ we have $a * a = a$ and $a \oplus a = a$

[Idempotent law]

Proof: Let $a, b, c \in L$, by the definition of GLB of a and b we have

$$a * b \leq a \qquad \ldots (i)$$

and if $a \leq a$ and $a \leq b$, then

$$a \leq a * b \qquad \ldots (ii)$$

As $a \leq a$ from (i) and (ii) we have

$a * a \leq a$ and $a \leq a * a$

By the antisymmetric property if follows that $a = a * a$

Similarly we can prove that $a \oplus a = a$

PROPERTY 2. Show that the operation of meet are join on a lattice are associative.

Solution : To prove : $(a * b) * c = a * (b * c)$

Let $a, b, c \in L$ by the definition we have

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

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

By the definition of GLB of a and b, we have $a * b \leq a$ and $a * b \leq b$, so by transitive property of $\leq$ we have

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

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

As $(a * b) * c \leq b$ and $(a * b) * c \leq c$

We see that $(a * b) * c$ is lower bound for b and c. From the definition of $b * c$ it follows that $(a * b) * c \leq b * c$

As $(a * b) * c \leq a$ and $(a * b) * c \leq b * c$

From the definition of $a * (b * c)$, we have

$$(a * b) * c \leq a * (b * c) \qquad \ldots (i)$$

Now $a * (b * c) \leq a$ and $a * (b * c) \leq b * c$

As $b * c \leq b$, by tansitivity $a * (b * c) \leq b$

since $a * (b * c) \leq a$, and $a * (b * c) \leq b$

We have $a * (b * c) \leq (a * b)$

As $a * (b * c) \leq b * c \leq c$

$$a * (b * c) \leq (a * b) * c \qquad \text{(ii)}$$

From (i) and (ii), by antisymmetric property, if follows that

$$a * (b * c) = (a * b) * c$$

Similarly, we can prove that $a \oplus (b \oplus c) = (a \oplus b) \oplus c$

PROPERTY 3. Show that the operation of meet and join on a lattice are commutative law. i.e., $a * b = b * a$ and $a \oplus b = b \oplus a$

Solution : Given $a, b \in L$ both $a * b$ and $b * a$ are GLB of a and b. By the uniqueness of GLB of a and b, we have $a * b = b * a$. Similarly $a \oplus b = b \oplus a$ holds good.

PROPERTY 4. Absorption law $a * (a \oplus b) = a$ and $a \oplus (a * b) = a$

Solution : Let $a, b \in L$. Then $a \leq a$ and $a \leq a \oplus b$. So $a \leq a * (a \oplus b)$. On the other hand $a * (a \oplus b) \leq a$. By annisymmetric property of $\leq$ we have $a = a * (a \oplus b)$

Similarly we have $a = a \oplus (a * b)$ $\forall$ $a, b \in L$

THEOREMS

Theorem 1.

Let (L, $\leq$) be a lattice in which $*$ and $\oplus$ denotes the operations of meet and join respectively. For any $a, b \in L$.

$$a \leq b \Leftrightarrow a * b = a \Leftrightarrow a \oplus b = b$$

Proof : First let us prove that $a \leq b \Leftrightarrow a * b = a$

Let us assume that $a \leq b$ and also we know that $a \leq a$.

$$\therefore a \leq a * b \qquad \ldots (1)$$

But, from definition of $a * b$, we have

$$a * b \leq a \qquad \ldots (2)$$

Hence $a \leq b \Rightarrow a * b = a$ [From (1) and (2)]

Next, assume that $a * b = a$, but it is only possible if $a \leq b$.

That is $a * b = a \Rightarrow a \leq b$

Combining these two results, we get

$$a \leq b \Leftrightarrow a * b = a$$

To show that $a \leq b \Leftrightarrow a \oplus b = b$ in a similar way.

From $a * b = a$, We have

$$b \oplus (a + b) = b \oplus a = a \oplus b$$

But $\quad b \oplus (a * b) = b$

Hence $\quad a \oplus b = b$ follows that $a * b = a$

Theorem 2.

Let (L, ≤) be a lattice. For any $a, b \in L$ the following are equivalent. (i) $a \leq b$, (ii) $a * b = a$, (iii) $a \oplus b = b$

Proof : At first, consider (i) ⇔ (ii)

We have $a \leq a$, assume $a \leq b$. Therefore $a \leq a * b$. By the definition of GLB, we have

$$a * b \leq a$$

Hence by antisymmetric property, $a * b = a$

Assume that $a * b = a$, but is only possible if

$$a \leq b \Rightarrow a * b = a \Rightarrow a \leq b.$$

Combining these two results, we have $a \leq b \Leftrightarrow a * b = a$

Similarly, $a \leq b \Leftrightarrow a \oplus b = b$

Alternatively, (ii) ⇔ (iii) as follows :

Assume $a * b = a$, we have $b \oplus (a * b) = b \oplus a = a \oplus b$, but by absorption $b \oplus (a * b) = b$. Hence $a \oplus b = b$.

But, from definition of $a * b$, we have

$$a * b \leq a \qquad \ldots (2)$$

Hence $a \leq b \Rightarrow a * b = a$ [From (1) and (2)]

Next, assume that $a * b = a$, but it is only possible if $a \leq b$.

That is $a * b = a \Rightarrow a \leq b$

Combining these two results, we get

$$a \leq b \Leftrightarrow a * b = a$$

To show that $a \leq b \Leftrightarrow a \oplus b = b$ in a similar way.

From $a * b = a$, We have

$$b \oplus (a + b) = b \oplus a = a \oplus b$$

But $\quad b \oplus (a * b) = b$

Hence $\quad a \oplus b = b$ follows that $a * b = a$

Theorem 2.

Let (L, ≤) be a lattice. For any $a, b \in L$ the following are equivalent. (i) $a \leq b$, (ii) $a * b = a$, (iii) $a \oplus b = b$

Proof : At first, consider (i) ⇔ (ii)

We have $a \leq a$, assume $a \leq b$. Therefore $a \leq a * b$. By the definition of GLB, we have

$$a * b \leq a$$

Hence by antisymmetric property, $a * b = a$

Assume that $a * b = a$, but is only possible if

$$a \leq b \Rightarrow a * b = a \Rightarrow a \leq b.$$

Combining these two results, we have $a \leq b \Leftrightarrow a * b = a$

Similarly, $a \leq b \Leftrightarrow a \oplus b = b$

Alternatively, (ii) ⇔ (iii) as follows :

Assume $a * b = a$, we have $b \oplus (a * b) = b \oplus a = a \oplus b$, but by absorption $b \oplus (a * b) = b$. Hence $a \oplus b = b$.

which is inequality (i) in 2.

Hence the theorem.

Theorem 4.

In a lattice (L, ≤), show that (i) $(a * b) \oplus (c * d) \leq (a \oplus c) * (b \oplus d)$ (ii) $(a * b) \oplus (b * c) \oplus (c * a) \leq (a \oplus b) * (b \oplus c) * (c \oplus a)$, $\forall a, b, c \in L$

Proof : Let $a, b, c \in L$

Then $a * b \leq a$ (or) $b \leq a\, a \oplus b$ ... (1)

$a * b \leq a \leq c \oplus a$ ... (2)

$a * b \leq b \leq b \oplus c$ ... (3)

Using (1), (2) and (3), we get

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

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

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

This proves (ii)

We have $a \leq a \oplus c$

$$b \leq b \oplus d$$

$$\therefore \quad (a * b) \leq (a \oplus c) * (b \oplus d)$$

We know that $c \leq a \oplus c$ ... (4)

$d \leq b \oplus d$ ... (5)

$$\therefore \quad c * d \leq (a \oplus c) * (b \oplus d)$$

By (4) and (5), $(a * b) \oplus (c * d) \leq (a \oplus c) * (b \oplus d)$. This proves (i)

Theorem 5.

In a lattice (L, ≤), prove that for $a, b, c \in L$

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

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

Proof : We know that $a * b \leq a, a * c \leq a$

$\therefore (a * b) \oplus (a * c) \leq a \oplus a = a$ ... (1)

Also $a * b \leq b$, $a * c \leq a * c$

$\Rightarrow (a * b) \oplus (a * c) \leq b \oplus (a * c)$ ... (2)

From (1) and (2), $(a * b) \oplus (a * c) \leq a * (b \oplus (a * c))$

This proves (i)

We know that $a \leq a \oplus b$; $a \leq a \oplus c$

$\Rightarrow a = a * a \leq (a \oplus b) * (a \oplus c)$

Further $b \leq a \oplus b$; $a \oplus c \leq a \oplus c$

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

By (3) & (4), $a \oplus (b * (a \oplus c)) \leq (a \oplus b) * (a \oplus c)$

This proves (ii)

Theorem 6.

In a lattice if $a \leq b \leq c$, show that

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

Proof : Let $a \leq b \leq c$

$a \leq b \Rightarrow a \oplus b = b$, $a * b = a$

$b \leq c \Rightarrow b \oplus d = c$, $b * c = b$

$a \leq c \Rightarrow a \oplus c = c$, $a * c = a$

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

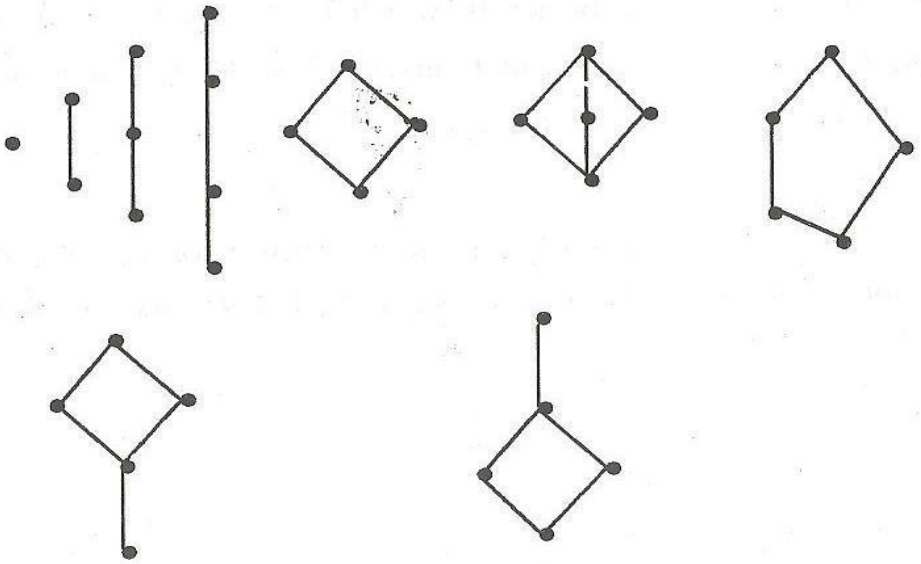
Now $(a * b) \oplus (b * c) = a \oplus b = b$

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

Theorem 7.

Draw Hasse diagram of all lattices with upto five elements.

Solution : The following Hasse diagrams are the lattice with 1, 2, 3, 4 and 5 elements.



Note :

Terminology

In logic notation	In set theory notation	Computer Designer's notation	Read as
$\vee$	$\cup$	$\oplus$	joint 'or' sum
$\wedge$	$\cap$	$*$	'Meet' and product
$\neg$	$\subset$	$-$, $'$	Complement
$\leq$	$\subseteq$	$\leq$	partially ordered set.

Def. A lattice is an algebraic system $(L, *, \oplus)$ with two binary operations $*$ and $\oplus$ on L which are both (1) commutative and (2) associative and (3) satisfy the absorption laws.

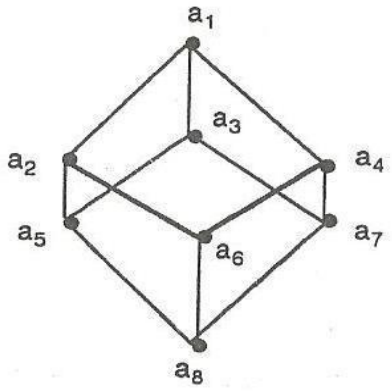
Def. Sublattice

Let $(L, *, \oplus)$ be a lattice and let $S \leq L$ be a subset of L. The algebra $(S, *, \oplus)$ is a sublattice of $(L, *, \oplus)$ iff S is closed under both operations $*$ and $\oplus$

Example 1. Let (L, ≤) be a lattice in which L = $\{a_1, a_2, \ldots a_8\}$ and S_1, S_2 and S_3 be the sublattices of L given by $S_1 = \{a_1, a_2, a_4, a_6\}$, $S_2 = \{a_3, a_5, a_7, a_8\}$ and $S_3 = \{a_1, a_2, a_4, a_8\}$

The diagram of (L, ≤) is

Observe that $(S_1, \leq)$ and $(S_2 \leq)$ are sublattices of (L, ≤), but $(S_3, \leq)$ is not a sublattices because $a_2, a_4 \in S_3$ but $a_2 * a_4 = a_6 \notin S_3$.



Note that $(S_3, \leq)$ is a lattice.

Def.: Let (L, *, ⊕) and (S, ∧, ∨) be two lattices. The algebraic system (L × S, ·, +) in which the binary operations + and ● on L × S are such that for any (a_1, b_1) and (a_2, b_2) in L × S

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 * a_2, b_1 \wedge b_2)$$

$$(a_1, b_1) + (a_2, b_2) = (a_1 \oplus a_2, b_1 \vee b_2)$$

is called the direct product of the lattices (L, *, ⊕) and (S, ∧, ∨)

Def. Lattice homomorphism

Let (L, *, ⊕) and (S, ∧, ∨) be two lattices. A mapping $g : L \to S$ is called a lattice homomorphism from the lattice (L, *, ⊕) to (S, ∧, ∨) if for any $a, b \in L$

$$g(a * b) = g(a) \wedge g(b) \text{ and } g(a \oplus b) = g(a) \vee g(b).$$

Note : Observe that both the operations of meet and join are preserved. These may be mappings which preserve only one of the two operations. Such mappings are not lattice homomorphisms.

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

Def. In a bounded lattice $(L, *, \oplus, 0, 1)$ an element $b \in L$ is called a complement of an element $a \in L$ if

$$a * b = 0 \text{ and } a \oplus b = 1$$

Def. A lattice $(L, *, \oplus, 0, 1)$ is said to be a complemented lattice if every element of L has atleast one complement.

Def. A lattice $(L, *, \oplus)$ is called a distributive lattice if for any $a, b, c \in L$

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

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

In other words, in a distributive lattice the operations $*$ and $\oplus$ distribute over each other.

Def. Modular

A lattice $(L, \wedge, \vee)$ is called modular if for all $x, y, z \in L$, $x \leq z \Rightarrow x \vee (y \wedge z) = (x \vee y) \wedge z$ (modular equations).

Note : We have (by modular inequality) if $x \leq z \Rightarrow x \vee (y \wedge z) \leq (x \vee y) \wedge z$ holds in any lattice. Therefore to show that a lattice L is modular it is enough to show if,

$x \leq z \Rightarrow x \vee (y \wedge z) \geq (x \vee y) \wedge z$ holds in L.

THEOREMS

Theorem 1.

Every chain is a distributive lattice. **[A.U M/J 2013]**

Proof : Let $(L, \leq)$ be a chain

Let $a, b, c \in L$

Consider the following possible cases

(i) $a \leq b$ or $a \leq c$ and

(ii) $a \geq b$ and $a \geq c$

2. If a homomorphism $g : L \to S$ of two lattices $(L, *, \oplus)$ and $(S, \wedge, \vee)$ is bijective i.e., one-to-one onto, then g is called an isomorphism. If there exists an isomorphism between two lattices then the lattices are called isomorphic.

3. A homomorphism $g : L \to L$ where $(L, *, \oplus)$ is a lattice is called an endomorphism.

If $g : L \to L$ is an isomorphism, then g is called an automorphism.

4. If $g : L \to L$ is an endomorphism, then the image set of g is a sublattice of L.

Def. Let $(P, \leq)$ and $(Q, \leq')$ be two partially ordered sets. A mapping $f : P \to Q$ is said to be order-preserving relative to the ordering $\leq$ in P and $\leq'$ in Q iff for any $a, b \in P$ such that $a \leq b$, $f(a) \leq' f(b)$ in Q.

Note : If $(P, \leq)$ and $(Q, \leq')$ are lattices and $g : P \to Q$ is a lattice homomorphism, then g is order-preserving.

Def. Two partially ordered sets $(P, \leq)$ and $(Q, \leq')$ are called order-isomorphic if there exists a mapping $f : P \to Q$ which is bijective and if both f and f^{-1} are order-preserving.

Def. Let $(L, *, \oplus)$ be a lattice and $S \subseteq L$ be a finite subset of L where $S = \{a_1, a_2, \ldots a_n\}$. The greatest lower bound and the least upper bound of S can be expressed as

$$\text{GLB } S = \overset{n}{\underset{i=1}{*}} a_i \quad \text{and} \quad \text{LUB } S = \overset{n}{\underset{i=1}{\oplus}} a_i \qquad \ldots (1)$$

where $\overset{2}{\underset{i=1}{*}} a_i = a_1 * a_2$ and $\overset{k}{\underset{i=1}{*}} a_i = \overset{k-1}{\underset{i=1}{*}} a_i * a_k, \quad k = 3,4,\ldots$

A similar representation can be given for $\overset{n}{\underset{i=1}{\oplus}} a_i$. Because of the associativity of the operations $*$ and $\oplus$, we can write

$$\overset{n}{\underset{i=1}{*}} a_i = a_1 * a_2 * \ldots * a_n \quad \text{and}$$

$$\overset{n}{\underset{i=1}{\oplus}} a_i = a_1 \oplus a_2 \oplus \ldots \oplus a_n$$

We shall now show that the distributive law

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

In case (i) $a \leq b$ or $a \leq c$ then we have $a * b = a$

$a \oplus a = a$, $a * c = a$ and

$\Rightarrow a \leq b \oplus c$

So $a * (b \oplus c) = a$ ... (1)

and $(a * b) \oplus (a * c) = a \oplus a = a$ ... (2)

(1) + (2) we get

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

In case (ii)

If $a \geq b$ and $a \geq c$ then we have $a * b = b$, $a * c = c$ and $b \oplus c \leq a$

So that $a * (b \oplus c) = b \oplus c$ ... (3) and

$(a * b) \oplus (a * c) = b \oplus c$ ... (4)

From (3) and (4) we get

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

Theorem 2.

Let (L, *, $\oplus$) be a distributive lattice. **[A.U. N/D 2004]**

For any a, b, c $\in$ L

$$(a * b = a * c) \wedge (a \oplus b = a \oplus c) \Rightarrow b = c$$

Proof : $(a * b) \oplus c = (a * c) \oplus c = c$ ... (1)

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

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

$= b \oplus (a * c)$

$= b \oplus (a * b)$

$= b$ ... (2)

From (1) and (2) $b = c$

Theorem 3.

Every distributive lattice is modular. **[A.U. N/D 2004]**

Proof : Let (L, $\leq$) be a distributive lattice

For all $a, b, c \in L$, we have

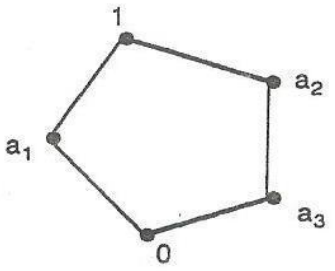
$$a \oplus (b * c) = (a \oplus b) * (a \oplus c)$$

Thus if $a \leq c$, then $a \oplus c = c$ and

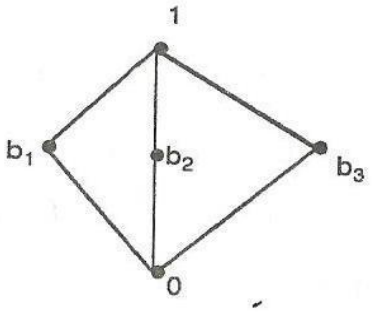
$$a \oplus (b * c) = (a \oplus b) * c$$

So if $a \leq c$, the modular equation is satisfied and L is modular.

Example 1. Show that the Lattices given by the diagrams are not distributive.



(A)



(B)

Solution : In lattice (A),

$$a_3 * (a_1 \oplus a_2) = a_3 * 1 = a_3 = (a_3 * a_1) \oplus (a_3 * a_2)$$

$$a_1 * (a_2 \oplus a_3) = 0 = (a_1 * a_2) \oplus (a_1 * a_3)$$

but $$a_2 * (a_1 \oplus a_3) = a_2 * 1 = a_2$$

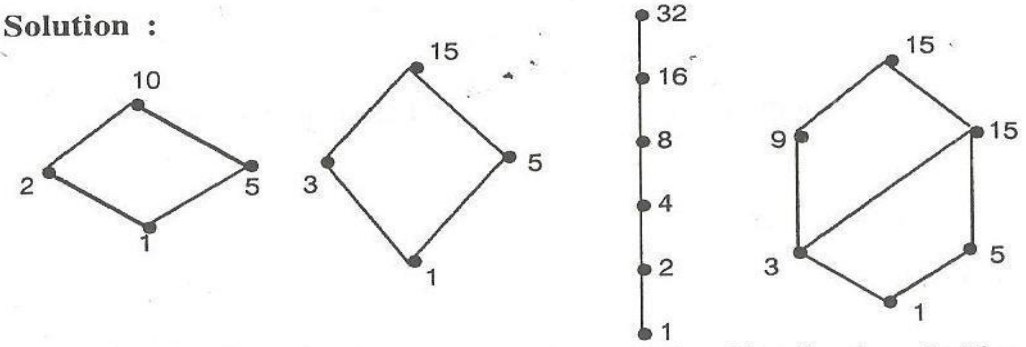
$$(a_2 * a_1) \oplus (a_2 * a_3) = 0 \oplus a_3 = a_3$$

Hence the Lattice (A) is not distributive.

In (B), $b_1 * (b_2 \oplus b_3) = b_1$ while $(b_1 * b_2) \oplus (b_1 * b_3) = 0$ which shows that the Lattice is not distributive.

Example 2. If D(n) denotes the lattice of all the divisors of the integer n draw the Hasse diagrams of D(10), D(15), D(32) and D(45)

Solution :



Example 3. Let L be a complemented, distributive lattice. For a, b $\in$ L the following are equivalent.

(i) a $\leq$ b (ii) a * b′ = 0 (iii) a′ $\oplus$ b = 1

(iv) b′ $\leq$ a′ where '1' denotes corresponding complement.

(OR)

Show that in a distributive and complemented lattice.

$a \leq b \Leftrightarrow a * b' = 0 \Leftrightarrow a' \oplus b = 1 \Leftrightarrow b' \leq a'$

Solution : $a \leq b \Rightarrow a \oplus b = b$ **[A.U. N/D 2004] [A.U M/J 2013]**

$\Rightarrow (a \oplus b) * b' = 0$ as $b * b' = 0$

$\Rightarrow (a * b') \vee (b * b') = 0$

$\Rightarrow a * b' = 0$ as $b * b' = 0$

Hence (i) $\Rightarrow$ (ii)

$a * b' = 0$

$\Rightarrow (a * b') = 1$

$\Rightarrow a' \oplus (b') = 1$

$\Rightarrow a' \oplus b = 1$

Hence (ii) $\Rightarrow$ (iii)

$a' \oplus b = 1 \Rightarrow (a' \oplus b) * b' = b'$

$\Rightarrow (a' * b') \oplus (b * b') = b'$ (distributive law)

$\Rightarrow a' * b' = b'$ as $b * b' = 0$

$\Rightarrow b' \leq a'$

Hence (iii) $\Rightarrow$ (iv)

$$b' \leq a' \Rightarrow a' * b' = b'$$

$$\Rightarrow a \oplus b = b^{\bullet\bullet}$$

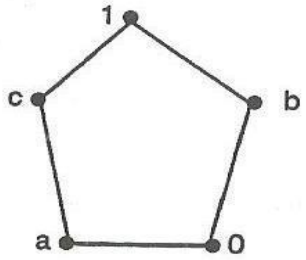
(taking complement on both sides by Demorgan's law)

$$\Rightarrow a \leq b$$

Hence (iv) $\Rightarrow$ (i)

Thus (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) $\Rightarrow$ (iv) $\Rightarrow$ (i)

Example 4. Prove that the following lattice is not modular.



Solution : For this lattice when $a \leq c$

$$a \oplus (b * c) \neq (a \oplus b) * c$$

Since $a \oplus (b * c) = a \oplus 0 = a$

but $(a \oplus b) * c = 1 * c = c$

$\therefore$ it is not a modular lattice.

Def. Enumeration : A one-to-one correspondence with the elements of a set is called an enumeration.

Example 5. Theorem : State and prove Isotonicity property in a lattice.

Proof : Let (L, $\leq$) be a lattice. For $a, b, c \in$ L, the following properties called isotonicity laws.

$$b \leq c \Rightarrow a * b \leq a * c \; ; \; a \oplus b \leq a \oplus c$$

(i.e.,) $b \leq c \Rightarrow a \wedge b \leq a \wedge c \; ; \; a \vee b \leq a \vee c$

Let us assume that $b \leq c$

(i) **Claim :** $a \vee b \leq a \vee c$

Let $x = a \vee c$. Then x is lub of a & c

$\Rightarrow x$ is an upper bound of a & c.

$\therefore a \leq x,\ c \leq x$

But $b \leq c,\ c \leq x \Rightarrow b \leq x$

Also $a \leq x$

$\therefore x$ is upper bound of a & b

But $a \vee b$ is lub of a & b

$\therefore a \vee b \leq x = a \vee c$

(ii) **Claim :** $a \wedge b \leq a \wedge c$

Let $y = a \wedge b \Rightarrow y$ is glb of a & b

$\therefore y$ is a lower bound of a & b

$y \leq a,\ y \leq b$

Using $b \leq c,\ y \leq a,\ y \leq c$

$\therefore y$ is a lower bound of a & c

But $a \wedge c$ is glb of a and c

$\therefore y \leq a \wedge c \Rightarrow a \wedge b \leq a \wedge c$

Example 6. If (L, $\wedge$, $\vee$) is a complemented distributive lattice, then the De Morgan's laws are valid. **[A.U M/J 2013]**

i.e., $\overline{a \vee b} = \bar{a} \wedge \bar{b}$ and $\overline{a \wedge b} = \bar{a} \vee \bar{b}$, $\forall\ a, b \in L$

Proof : If (L, $\wedge$, $\vee$) is a complemented distributive lattice. We have the complement of any element is unique in the distributive lattice.

Let $a, b \in L$

Let $\bar{a}$ and $\bar{b}$ are complements of a and b respectively.

$\therefore$ We have $a \wedge \bar{a} = 0,\ a \vee \bar{a} = 1,\ b \wedge \bar{b} = 0,\ b \vee \bar{b} = 1$

Now, $(a \vee b) \vee (\bar{a} \wedge \bar{b}) = ((a \vee b) \vee \bar{a}) \wedge ((a \vee b) \vee \bar{b})$

$= (a \vee (b \vee \bar{a})) \wedge (a \vee (b \vee \bar{b}))$

$$= (a \vee (\bar{a} \vee b)) \wedge (a \vee 1)$$

$$= ((a \vee \bar{a}) \vee b) \wedge (a \vee 1)$$

$$= 1 \wedge 1 = 1$$

and $$(a \vee b) \wedge (\bar{a} \wedge \bar{b}) = (a \wedge (\bar{a} \wedge \bar{b})) \vee (b \wedge (\bar{a} \wedge \bar{b}))$$

$$= ((a \wedge \bar{a}) \wedge \bar{b}) \vee (b \wedge (\bar{b} \wedge \bar{a}))$$

$$= (0 \wedge \bar{b}) \vee ((b \wedge \bar{b}) \wedge \bar{a})$$

$$= (0 \wedge \bar{b}) \vee (0 \wedge \bar{a})$$

$$= 0 \vee 0 = 0$$

$\therefore \bar{a} \wedge \bar{b}$ is the complement of $a \vee b$ and its unique.

Example 7. Let (L, $\wedge$, $\vee$) be a distributive lattice and a, b, c $\in$ L If $a \wedge b = a \wedge c$ and $a \vee b = a \vee c$, then b = c
[Cancellation laws are valid in a Distributive lattice]

Proof : Let (L, $\wedge$, $\vee$) be any distributive lattice and $a, b, c \in L$, such that

$$a \wedge b = a \wedge c$$

and $$a \vee b = a \vee c$$

Now, $$(a \wedge b) \vee c = (a \vee c) \wedge (b \vee c) \qquad (\because \text{L is distributive})$$

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

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

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

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

$$= b$$

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

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

So that, $a \wedge b = a \wedge c$

and $a \vee b = a \vee c$

$\Rightarrow b = c$

That is, the cancellation law is valid in a distributive lattice.

Example 8. Theorem : A modular lattice is distributive if and only if none of its sublattice is isomorphic to the diamond lattice M_5.

Proof : We have, the diamond lattice M_5 is not distributive lattice, therefore any lattice having sublattice isomorphic to M_5 cannot be distributive.

Conversely, let (L, $\leq$) be any modular lattice but not distributive lattice. We show that L has a sublattice isomorphic to M_5. Since (L, $\leq$) is not distributive lattice, then we an find $x, y, z \in$ L such that

$$(x \wedge y) \vee (y \wedge z) \vee (z \wedge x) < (x \vee y) \wedge (y \vee z) \wedge (z \vee x)$$

Now let, $u = (x \wedge y) \vee (y \wedge z) \vee (z \wedge x)$

$v = (x \vee y) \wedge (y \vee z) \wedge (z \vee x)$

$a = u \vee (x \wedge v)$

$b = u \vee (y \wedge v)$ and

$c = u \vee (z \wedge v)$

Then the elements u, v, a, b, c are distinct and form a sublattice to L, and S = $\{u, a, b, c, v\}$ is isomorphic to the diamond lattice M_5.

5.3 BOOLEAN ALGEBRA

Def. Boolean Algebra

A Boolean algebra is a complemented, distributive lattice.

Note : 1. George boole in 1854 had given a set of basic rules for logic in his book "The laws of thought". Boolean algebra provides the operations and rules working with the binary set {0, 1}

2. Electronic circuites and switching matchings are working with the rules of Boolean algebra.

Properties

A Boolean algebra will generally be denoted by $(B, *, \oplus, ', 0, 1)$ in which $(B, *, \oplus)$ is a lattice with two binary operations $*$ and $\oplus$ called the meet and join respectively. The corresponding partially ordered set will be denoted by $(B, \leq)$. The bounds of the lattice are denoted by 0 and 1, where 0 is the least element and 1 the greatest element of $(B, \leq)$. Since $(B, *, \oplus)$ is complemented and because of the fact that it is a distributive lattice, each element of B has a unique complement. We shall denote the unary operation of complementation by $'$, so that for any $a \in B$, the complement of a is denoted by $a' \in B$.

Most of the properties of a Boolean algebra have been derived in the previous section. We shall list some of the important properties

here. It may be mentioned that the properties listed here are not independent of each other.

A Boolean algebra (B, $*$, $\oplus$, $'$, 0, 1) satisfies the following properties in which a, b and c denote any elements of the set B.

1. (B, $*$, $\oplus$) is a lattice in which the operations $*$ and $\oplus$ satisfy the following identities :

(L-1)	$a * a = a$	**(L-1)'**	$a \oplus a = a$
(L-2)	$a * b = b * a$	**(L-2)'**	$a \oplus b = b \oplus a$ [Commutative law]
(L-3)	$(a * b) * c = a * (b * c)$	**(L-3)'**	$(a \oplus b) \oplus c = a \oplus (b \oplus c)$ [Associative law]
(L-4)	$a * (a \oplus b) = a$	**(L-4)'**	$a \oplus (a * b) = a$

2. (B, $*$, $\oplus$) is a distributive lattice and satisfies these identities :

(D-1) $a * (b \oplus c) = (a * b) \oplus (a * c)$
(D-2) $a \oplus (b * c) = (a \oplus b) * (a \oplus c)$ } [Distributive laws]

(D-3) $(a * b) \oplus (b * c) \oplus (c * a) = (a \oplus b) * (b \oplus c) * (c \oplus a)$

(D-4) $a * b = a * c$, and $a \oplus b = a \oplus c \Rightarrow b = c$

3. (B, $*$, $\oplus$, 0, 1) is a bounded lattice in which for any $a \in$ B, the following hold :

(B-1) $0 \leq a \leq 1$

(B-2)	$a * 0 = 0$	**(B-2)'**	$a \oplus 1 = 1$	[Dominance laws]
(B-3)	$a * 1 = a$	**(B-3)'**	$a \oplus 0 = a$	[Identity laws]

4. (B, $*$, $\oplus$, $'$, 0, 1) is a uniquely complemented lattice in which the complement of any element $a \in$ B is denoted by $a' \in$ B and satisfies the following identities :

(C-1)	$a * a' = 0$	**(C-1)'**	$a \oplus a' = 1$	[Complement laws]
(C-2)	$0' = 1$	**(C-2)**	$1' = 0$	[Zero and one law]
(C-3)	$(a * b)' = a' \oplus b'$	**(C-3)'**	$(a \oplus b)' = a' * b'$	[De-Morgan's laws]

5. There exists a partial ordering relation $\leq$ on B such that

(P-1) $a * b = \text{GLB}\ \{a, b\}$ **(P-1)'** $a \oplus b = \text{LUB}\ \{a, b\}$

(P-2) $a \leq b \Leftrightarrow a * b = a \Leftrightarrow a \oplus b = b$

(P-3) $a \leq b \Leftrightarrow a * b' = 0 \Leftrightarrow b' \leq a' \Leftrightarrow a' \oplus b = 1$

Example :

Let $B = \{0, 1\}$ be a set. The operations $*, \oplus, '$ on B are defined by

$*$	0	1
0	0	0
1	0	1

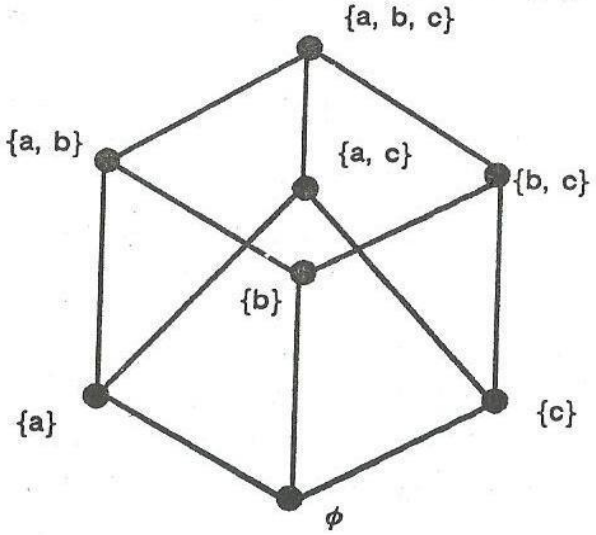
$\oplus$	0	1
0	0	1
1	1	1

x	x'
0	1
1	0

Clearly $< B, *, \oplus, ', 0, 1 >$ is a Boolean algebra.

Example :

Let $A = \{a, b, c\}$ and consider the lattice $P(A)$.



Clearly $< P(A), \cap, \cup >$ is a Boolean Algebra.

Def. Sub-Boolean algebra

Let (B, $*$, $\oplus$, $'$, 0, 1) be a Boolean algebra and S $\subseteq$ B. If S contains the elements 0 and 1 and is closed under the operations $*$, $\oplus$ and $'$, then (S, $*$, $\oplus$, $'$, 0, 1) is called a sub-boolean algebra.

Def. Join-irreducible.

Let $(L, *, \oplus)$ be a lattice. An element $a \in L$ is called join-irreducible if it cannot be expressed as the join of two distinct elements of L. In otherwords $a \in L$ is join-irreducible

If for any $a_1, a_2 \in L$

$$a = a_1 \oplus a_2 \Rightarrow (a = a_1) \vee (a = a_2)$$

Def. (Direct product)

Let $(L, \oplus, *)$ and $(S, \vee, \wedge)$ be two lattices. Then the direct product of L, and S is defined by $(L \times S, +, *)$ where $+$ and $*$ are defined by the following manners.

$$(a_1, b_1) + (a_2, b_2) = (a_1 \oplus a_2, b_1 \vee b_2)$$

$$(a_1, b_1) . (a_2, b_2) = (a_1 * a_2, b_1 \wedge b_2), \forall a_1, a_2 \in L, \forall b_1, b_2 \in$$

Def. Lattice homomorphism

Let $(L, \oplus, *)$ and $(S, \vee, \wedge)$ be two lattices. A map $f : L \to S$ is called a homomorphism if

$$g(a \oplus b) = g(a) \vee g(b)$$

$$g(a * b) = g(a) \wedge g(b) \; ; \forall a, b \in L$$

Note: 1. The binary operation $\oplus$ and $*$ are preserved under Lattice Homomorphism.

2. $g : (L, \oplus, *, \leq) \to (S, \vee, \wedge, \leq')$ is called an order homomorphism, then $a \leq b \Rightarrow g(a) \leq' g(b)$, for all $a, b \in L$

Example 1. Theorem : In a Boolean lattice, prove that the De-Morgan's laws. **[A.U. M/J 2006]**

Proof : Let $(L, \oplus, *)$ be Boolean lattice.

(i.e.,) L is a complemented and distributive lattice.

The De-Morgan's laws are

(i) $\overline{a \oplus b} = \bar{a} * \bar{b}$; (ii) $\overline{a * b} = \bar{a} \oplus \bar{b}$, $\forall \bar{a}, a, b \in L$

Assume that $a, b \in L$. There exists elts

$\bar{a}, \bar{b} \in L$ such that $a \oplus \bar{a} = 1$; $a * \bar{a} = 0$; $b \oplus \bar{b} = 1$; $b * \bar{b} = 0$

(i) Claim : $\overline{a \oplus b} = \bar{a} * \bar{b}$

$$\text{Now } (a \oplus b) \oplus (\bar{a} * \bar{b}) = [(a \oplus b) \oplus \bar{a}] * [(a \oplus b) \oplus \bar{b}]$$

$$= [a \oplus \bar{a} \oplus b] * [a \oplus b \oplus \bar{b}]$$

$$= [1 \oplus b] * [a \oplus 1]$$

$$= 1 * 1 = 1$$

$$(a \oplus b) * (\bar{a} * \bar{b}) = [(a \oplus b) * \bar{a}] * [(a \oplus b) * \bar{b})$$

$$= [(a * \bar{a}) \oplus (b * \bar{a})] * [(a * \bar{b}) \oplus (b * \bar{b})]$$

$$= [0 \oplus (b * \bar{a})] * [(a * \bar{b}) \oplus 0]$$

$$= (b * \bar{a} * (a * \bar{b})$$

$$= b * (\bar{a} * a) * b = \bar{b} * 0 * \bar{b} = 0$$

Hence claim (i) is proved.

(ii) Claim : $\overline{a * b} = \bar{a} \oplus \bar{b}$

$$\text{Now } (a * b) \oplus (\bar{a} \oplus \bar{b}) = [(a * b) \oplus \bar{a}] \oplus [(a * b) \oplus \bar{b}]$$

$$= [(a \oplus \bar{a}) * (b \oplus \bar{a})] \oplus [(a \oplus \bar{b}) * (b \oplus \bar{b})]$$

$$= [1 * (b \oplus \bar{a})] \oplus [(a \oplus \bar{b}) * 1]$$

$$= (b \oplus \bar{a}) \oplus (a \oplus \bar{b})$$

$$= b \oplus (\bar{a} \oplus a) \oplus \bar{b}$$

$$= b \oplus 1 \oplus \bar{b} = b \oplus \bar{b} = 1$$

$$(a * b) * (\bar{a} \oplus \bar{b}) = [(a * b) * \bar{a}] \oplus [(a * b) * \bar{b}]$$

$$= (a * \bar{a} * b) \oplus [a * b * \bar{b}]$$

$$= (0 * b) \oplus [a * 0]$$

$$= 0 * 0 = 0$$

Therefore claim (ii) is proved

Hence the De-Morgan's laws are proved.

Example 2. Show that (P(A), $\cup$, $\cap$, $\subseteq$) is a Boolean algebra.

Proof : We know that (P(A)), $\subseteq$) is a lattice.

For any X, Y, Z $\in$ P(A), $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$

$$X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$$

Also $\forall$ X $\in$ P(A), there exists a subset $\overline{X}$ of A such that

$$X \cup \overline{X} = A, \quad X \cap \overline{X} = \{\ \} = \phi$$

Zero elt of P(A) is { } = least elt.

The greatest elt of P(A) is A.

$\therefore$ (P(A), $\cup$, $\cap$, $\subseteq$) is a Boolean algebra.

Example 3. Consider the D_{30} = {1, 2, 3, 5, 6, 10, 15, 30} is a lattice (infact Boolean algebra) with relation "divides".

Solution : Now

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

$\therefore$ 2, 3, 5 are atoms in D_{30}.