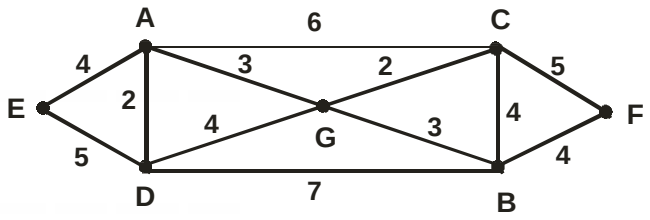
Logic & Discrete Mathematics

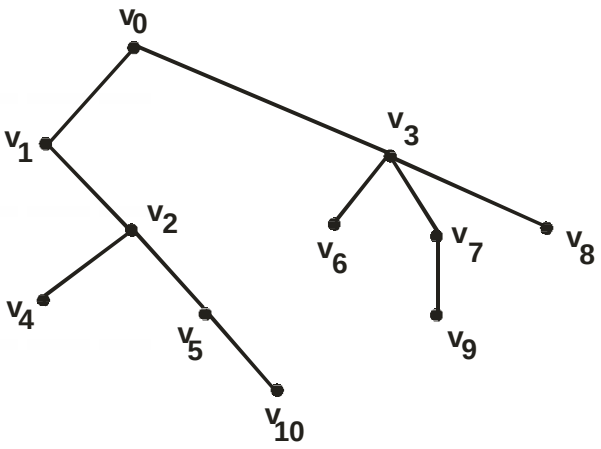
Part-5

c) 

, at vertex E.

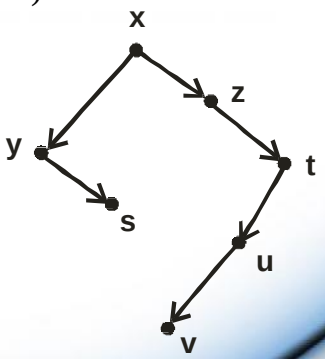
8) Use Krushkal's algorithm to find minimal spanning tree for the graphs given in Exercise 7.

9) Refer following tree and answer.

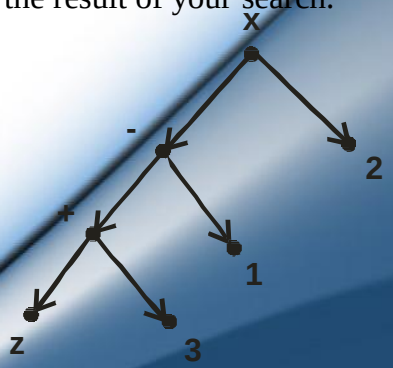


a) What is height of the tree?
b) List the leaves of T.
c) How many subtrees of T condition v_4 ?
d) List the siblings of v_7 .

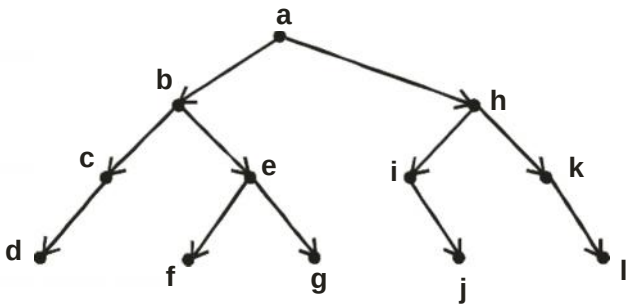
10) For the graphs given below perform
i) Preorder search
ii) Inorder search
iii) Post order search and write the result of your search.



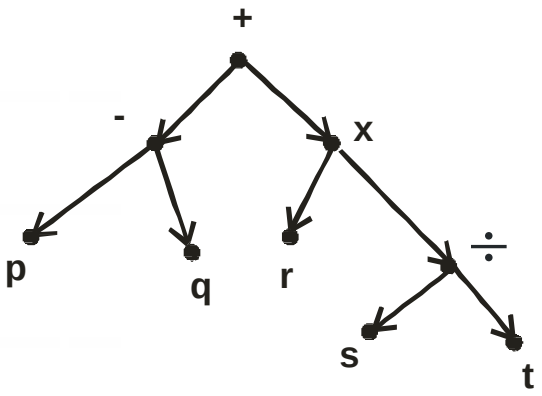
(a)



(b)



(c)



(d)

8. LET US SUM UP

In this chapter, we have learnt the structure of trees and its properties we have also seen different ways of searching trees in a graph. One can also find the spanning tree using the Prim's and Kruskal's algorithm. The trees are very useful models for different situations in computer science.

9. REFERENCES FOR FURTHER READING

1. Discrete Mathematical structures by Kolamn, Busby and Ross. Pearson education.
2. Introduction to graph theory by Douglas B. West.
3. Discrete Mathematics and its applications by Kenneth. H.Rosen. McGraw Hill edition.
4. Graph theory by Frank Harary. Narosa Publication.
5. Discrete Mathematics by Norman Priggs. Oxford.

11

SEMI-GROUPS AND GROUPS

Unit Structure :

11.0 OBJECTIVES

After going through this chapter students will be able to:

- about binary operations
- Algebraic structures like semi-groups and groups will be known
- Operations like product and quotient of these algebraic structure will be known

11.1 INTRODUCTION

Semi-groups and groups are mathematical structures. Semi-groups help in the study of finite state machines. While studying group structure we develop an understanding for coding theory. To study groups and semi-groups some knowledge of set theory and number system is required.

In this chapter we are going to discuss following topics.

- What are binary operations?
- The structure called semi-group, their products and quotients.
- The group structure and its product and quotient.

2. BINARY OPERATION

Binary operation is basic tool to study discrete mathematics. A collection of objects with operations defined on them and the properties associated with the operation together gives us a system which we call mathematical structure or system. An operation that combines two objects is a binary operation. Binary operation is a function with certain properties. A set with binary operation is a set in which an abstract product is defined such that the product of two elements of the set is again an element of the set.

1.Definition 1: A binary operation on set G is defined as a function $f : G \times G \to G$. If a and b $\in$ G then $f(a, b) \in G$.

Remark : A binary operation is a rule which assigns to each ordered pair of element of *G*, a unique element of *G*.

Notation : We use the symbol $a * b$ to denote f (a, b).

2. Examples of binary operation :

1. Let G = = The set of integers.
   Define $*$: G $\times$ G $\to$ G as $a * b = a + b$
   Since $a + b \in$ = G, $*$ is binary operation on .

2. Let G = = set of real numbers.
   Define $*$: $\times$ $\to$ as $a * b = a \div b$

   Then $*$ is not binary operation, since it is not defined for every pair of elements of . For example; $3 \in$ and $0 \in$ but $3 \div 0$ is not defined.

3. Let G = $^+$ = set of positive integers, where $*$ is defined as $a * b = a - b$.
   $*$ is not binary operation since it is not defined for every pair of elements of $^+$. For example; $2 \in$ $^+$, $3 \in$ $^+$ but $2 - 3 = -1 \notin$ $^+$.

4. Let G = , be set of integers
   Define $*$: G $\times$ G $\to$ G as $a * b = a + b - ab$
   Then $*$ is binary operation. Note that if G = $^+$ = set of positive integers then $*$ defined above will not be binary operation as $2 \in$ $^+$, $3 \in$ $^+$ but $2 * 3 = 2 + 3 - 2.3 = 2 + 3 - 6 = -1 \notin$ $^+$.

5. Let M be set of all $n \times n$ Boolean matrices.

A Boolean matrix is $n \times n$ matrix whose entries are zero or one. Let $A = [a_{ij}]$ and $B = [b_{ij}]$ be $n \times n$ Boolean matrices. Define $A \vee B$, the **join** of A and B, by $C = [c_{ij}]$ where

$$c_{ij} = \begin{cases} 1 & \text{if } a_{ij} = 1 \quad \text{or} \quad b_{ij} = 1 \\ 0 & \text{if } a_{ij} \text{ and } b_{ij} \text{ both are } 0 \end{cases}$$

Define $A \wedge B$, the **meet** of A and B by $D = [d_{ij}]$ where

$$d_{ij} = \begin{cases} 1 & \text{if } a_{ij} \text{ and } b_{ij} \text{ are both } 1 \\ 0 & \text{if } a_{ij} = 0 \quad \text{or} \quad b_{ij} = 0 \end{cases}$$

Let M be set of Boolean matrices. Let G = M. Define $*$ on M as follows : For A, B $\in$ M; $A * B = A \vee B$. The $*$ is a binary operation. If $*$ is defined as $A * B = A \wedge B$ then, again $*$ is binary operation.

11.2.3 Properties of binary operation :

1. **Definition 2:** A binary operation on a set G is said to be closed if $a * b \in G$ for all elements a and b in G. We say $*$ satisfies closure property.

Note : Whenever $*$ is binary operation, it always hold closure property and we say G is closed with respect to $*$.

2.Definition 3: A binary operation on set G is said to be commutative if $a * b = b * a$ for all a, b $\in$ G. We say $*$ satisfies commutative property.

3.Definition 4: A binary operation $*$ on a set G is said to be associative if $a * (b * c) = (a * b) * c$ for all a, b, c $\in$ G. We say $*$ satisfies associative property.

4.Definition 5: A binary operation $*$ on a set G is said to be idempotent if $a * a = a$ for all $a \in G$. We say $*$ satisfies idempotent property.

To summaries properties of binary operation we have following table where $*$ is binary operation on a set G and $*$ satisfies properties for a, b, c $\in$ G.

1. $a * b \in G$	Closure Property
2. $a * a = a$	Idempotent Property
3. $a * b = b * a$	Commutative Property
4. $a * (b * c) = (a * b) * c$	Associative Property

Table No. 11.1

Examples based on definition 2 to 5.

1. Let G = and a $*$ b = a + b, $\forall$ a, b $\in$, Then $*$ satisfies closure property as a $*$ b = a + b $\in$.
$*$ satisfies commutative property because a $*$ b = a + b while b $*$ a = b + a and a $*$ b = a + b = b + a = b $*$ a.

Also, $(a * b) * c = (a + b) * c$
$= (a + b) + c$
$= a + (b + c)$ [$+$ *is associative in*]
$= a + (b * c)$
$= a * (b * c)$

* holds associative property. Now, 2 * 2 = 2 + 2 = 4 2, hence * does not satisfy idempotent property.

2. Let L be a lattice. Define a $*$ b = a $\wedge$ b (greatest lower bound of a and b) Then $*$ satisfies all four properties.

$a * b = a \wedge b \in L$, $\therefore$ $*$ holds closure property
$a * a = a \wedge a = a$, $\therefore$ $*$ holds idempotent property
$a * b = a \wedge b = b \wedge a = b * a$ $\therefore$ $*$ holds commutative property

$(a * b) * c = (a \wedge b) \wedge c$
$= a \wedge (b \wedge c)$
$= a * (b * c)$, $\therefore$ $*$ holds associative property

3. Let G and * be defined as, $a * b$ ab $2b$

Then a $*$ b $\in$, hence $*$ holds closure property.
$a * a = a.a + 2a = a\,(a + 2) \neq a$, hence $*$ does not hold idempotent property.

$a * b = ab + 2b$ and
$b * a = ba + 2a$
Since $a * b \neq b * a$, $*$ is not commutative on .

$(a * b) * c$
$= (ab + 2b) * c$
$= (ab + 2b) \,.\, c + 2c$
$= abc + 2bc + 2c$ and

a $*$ (b $*$ c)
= a $*$ (bc + 2c)
= a (bc + 2c) + 2 (bc + 2c)

= abc + 2ac + 2bc + 4c

Thus, $(a * b) * c \neq a * (b * c)$ and hence $*$ is not associative on .

4. Consider the set G = {a, b, c, d} with binary operation $*$ defined by following table.

*	a	b	c	d
a	a	c	b	d
b	d	a	b	c
c	c	d	a	a
d	d	b	a	c

i) $c * d = a$ and $d * c = a$

Thus, $c * d = d * c$

ii) $b * d = c$ and $d * b = b$

Thus, $b * d \neq d * b$

iii) $a * (b * c) = a * b$

$= c$

$(a * b) * c = c * c = a$

$\therefore a * (b * c) \neq (a * b) * c$

From (ii), $*$ is not commutative.

and from (iii), $*$ is not associative.

Check your progress

1. Determine whether $*$ is binary operation. If it is determine whether $*$ is closed, idempotent, commutative and associate on given set.
   a) On where $a * b = 2a + b$
   b) On $^{+}$ where $a * b = a / b$
   c) On where $a * b = a - b$
   d) On lattice L where $a * b = a \vee b$
   (least upper bound of a and b)
2. Consider binary operation $*$ defined on set G = {a, b, c} given by following table.

*	a	b	c
a	b	c	b
b	a	b	c
c	c	a	b

   a) Is $*$ commutative?
   b) Compute $a * (b * c)$ and $(a * b) * c$
   c) Is $*$ associative?

11.3 SEMI-GROUPS

Definition 6 : Algebraic Structure

A nonempty set G with one or more binary operations is called an algebraic structure.

If $*$ is binary operation on G then (G, $*$) is an algebraic structure.

Examples of algebraic structure

1. The set : set of natural numbers is algebraic structure with respect to binary operation +. Thus we denote (, +) is an algebraic structure.
2. (, +) : set of integers with binary operation + is an algebraic structure.
3. (, + ,) : set of real numbers with binary operations + and , is an algebraic structure.

Definition 7: Semi-group :

An algebraic structure (G, $*$) is called a semi-group if the binary operation $*$ is associative in G. Thus, if a, b, c $\in$ G, then (a $*$ b) $*$ c = a $*$ (b $*$ c).

Definition 8: Commutative Semi-group :

The semi-group (G, $*$) is said to be commutative if $*$ is commutative.

Examples of Semi-group :

1.(, +) : Set of natural numbers with respect to binary operation + is semi group as + satisfies associative property i.e. $\forall$ a, b, c $\in$, (a + b) + c = a + (b + c)

2.(, +) : set of integers with binary operation + is commutative semi-group because + is associative and commutative in .

Definition 9: Identity element:

An element e in a semi group (G, $*$) is called the identity element if e $*$ a = a $*$ e = a $\forall$ a $\in$ G. (read $\forall$ as 'for all')

Note that identity element is unique. Otherwise if it is not unique then there exist another identity element i such that i $*$ a = a $*$ i = a.

Thus if a = e then; i $*$ e = e $*$ i = e (1)
Also, if a = i then; e $*$ i = i $*$ e = i (2)

From (1) and (2) we get e = i. Thus, identity element if it exists is unique.

Definition 10: Monoid

A monoid is a semigroup $(G, *)$ that has an identity element.

Examples of Monoid

1.(, +) : Set of integers with binary operation + is monoid. Here; 0 is identity element as $0 + a = a + 0 = a \ \forall \ a \in$.

2.Let S be fixed non empty set and let S^S be set of all functions f : S $\rightarrow$ S. If f and g are elements of S^S, define f $*$ g = f g, the composite function. Then (S^S, $*$) is a semigroup which is not commutative and is a monoid since S^S has identity element 1_S, i.e.

$\forall \ f \in S^S; \ 1_S * f = f * 1_S = f$

Definition 11: Sub semi-group

Let $(G, *)$ be a semi-group. Let H be subset of G. If H is closed under binary operation $*$ then $(H, *)$ is called sub-semi-group of $(G, *)$

Definition 12: Sub monoid

Let $(G, *)$ be a monoid with identity element e. If H be nonempty subset of G. If H is closed under binary operation $*$ and e $\in$ H, then $(H, *)$ is called submonoid.

Note : 1) Subsemigroup of a semigroup is itself a semigroup.
2) Submonoid of a monoid is itself a monoid.

Examples of submonoid

1.If $(G, *)$ is a semigroup, then $(G, *)$ is subsemigroup of $(G, *)$. Similarly if $(G, *)$ is a monoid then $(G, *)$ is submonoid of $(G, *)$. If T = {e} then $(T, *)$ is also a submonoid of monoid $(G,*)$.

2. Let H be set of all even integers then (H, X) is a sub semigroup of (, X) where 'x' is binary operation multiplication. But (H, X) is not a submonoid of (, X) because 1 is identity element of which does not belong to H.

Group Theory

A group is formally defined as below. We denote the binary operation as **"0" or "*"** until or otherwise specified.

Definition: Let G be a non-empty set and 0 be a binary operation on G.We say that (G, 0) is a group if the following **four properties** are satisfied.

1. G. is **closed** with respect to '*' i.e .,for all a , b in G the element a * b is a uniquely defined element of G
2. G. is **associative** with respect to '*'
   i.e., for all a , b , c in G a * (b*c) = (a*b) *c
3. **Identity** element **exists** in G for '*'
   i.e., if there exists 'e' such that a * e = e * a = a a in G.
4. **Inverse exists** for **each element** in G with respect to '0'
   i.e., for each a in G there exists an element a^{-1} in G such that $a * a^{1}$ $a^{1} * a$ e (where e is identity element of G)

Example 1: Set of all non-zero rational numbers from a group under ordinary multiplication.

Solution: Let Q* is the set of all non-zero rational numbers.

Closure law: Let a , b ∈ Q*
a . b also belongs to Q* (Product of two rational numbers is a ational number)

Q* is closed with respect to multiplication.
Q* satisfies fist condition of a group

Associative law: Let $a,b,c \quad Q^*$ let $a \quad \frac{u}{x}, b \quad \frac{v}{y}$ and $c \quad \frac{w}{3}$

Consider $a\,b \quad \frac{u}{x}\,\frac{v}{y} \quad \frac{uv}{xy}; a.b.c \quad \frac{uv}{xy}\,\frac{w}{z} \quad \frac{uv\,w}{xy\,z} \quad \frac{u\,vw\,w}{x\,yz}$

(∴ (uv)w = u(vw) and (xy)z = x(yz) where u,v,w,x,y,z ∈ Z and satisfies associative law)

$$\frac{u}{x}\ \frac{v}{y}\ \frac{w}{z}$$

$$a\,b.c$$

From the above example it is clear that (a . b) . c = a .(b.c) and it si true a , b , c∈Q*

Q* is associative with respect to multiplication.

Existence of Identity: since 1 is a rationa1 number 1 ∈Q*
Let a ∈Q*
We have a.1 = a = 1.a
So 1 is the identity element of Q* which exists in Q*

Existence of Inverse: To prove existence of inverse, let $a \quad \frac{p}{q}$ be an element Q* There exists $\frac{q}{p} \quad Q^*$ such that $\frac{p}{q}\frac{q}{p} = 1$

That shows $\frac{q}{p}$ is the inverse of $\frac{p}{q}$ and it is true for all a ∈Q*

Hence inverse exists for such element of Q* and inverse of a denoted by 1/a or a^{-1}.

Q* satisfies all four properties of a group, Q* is a group under multiplication (Q*, .) is a group

Properties of a Group :

Abelian Group: In addition to the above mentioned four properties of a group if it also satisfies another property called commutative property , i.e.,a*b = b*a a , b ∈ G

The group is calles either **Abelian group or commutative group**. A group which is not abelian is calles as non-abelian group

Example 3: C = { a + ib / a,b ∈**R**} C is an abelian group with two addition.

Addition is defined on C as $(a_1 + i\, b_1) + (a_2 + i\, b_2) = (a_1 + a_2) + (b_1 + b_2)$

Commutative Property

Let x , y ∈*C* where $x = a_1 + i\, b_1$ and $y = a_2 + i\, b_2$, a_1 , a_2 , b_1 , $b_2 \in R$

$X + y = (a_1 + i\, b_1) + (a_2 + i\, b_2)$

$= (a_1 + a_2) + i(b_1 + b_2)$

Since addition two real number satisfies the commutative law.

$a_1 + a_2 = a_2 + a_1$ and $b_1 + b_2 = b_2 + b_1$

$= (a_2 + a_1) + i(b_2 + b_1)$

$= (a_2 + i\, b_2) + (a_1 + i\, b_1)$

$= y + z$

C satisfies the commutative law with respect to **addition.**

(*C* , +) is an abelian group or (*C* , +) is a **commutative group.**

Set of complex number also forms an **abelian group** with respect to **multiplication.**

(Leftas an exercise)

Commutative Law : $a,b \;\; Q \;\; a*b \;\; \frac{ab}{5} \;\; \frac{ba}{5} \;\; b*A \;\; ab \;\; ba$

Hance Q_+ is an abelian group with respect to *.

Example 4: G = {1, -1} is an abelian group under multiplication.

.	1	-1
1	1	-1
-1	-1	1

From the above table, it is clear that (G , .) satisfies both closure, associative property ,and abelian property with 1 being identity and -1 is its own inverse

Addition modulo "m"

We shall now define a new type of addition called "addition modulo "and is denoted by $a +_m b$ where a and b are integers and 'm' is a fixed positive integers.

By definition , $a +_m b = r \; 0 \le r < m$ where r is the least non-negative remainder when a + b is devided by m and we read itas a addition modulo m b.

Example 5: If a = 7; b = 8 then add 7 and 8 gives 15 divide by 2 the remainder is 1.

$7 +_2 8 = 1$

If a = 5 and b = 6 add 5 and 6 gives 11 divide by 3 we get the remainder is 2.

$5 +_3 6 = 2$

Note: If a and b are two integers such that a-b divisible by fixed positive integer 'm' we write a = b (mod m) and we read it as "a is congruent to b modulo m"

Note: It can be easily seen that $a +_m b = b +_m c$ (take any example and try it in your own)

Example 6: prove that the set G = { 0, 1, 2, 3, 4, 5} is a finite abelian group of group of order '6' with respect to addition modulo '6'.

From the composition table as shown below

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

From the above table we see that all entries in the composite table are the element of G.

That shows G is closed under addition modulo 6.("+6".)
To prove G is associative, let a = 2 b = 4 c=1
Consider $2+_6 (4+_6 1) = 2+_6 5 = 1$
$(2+_6 4) +_6 1 = 0+_6 1 = 1$
$2+_6 (4+_6 1) = (2+_6 4) +_6 1$ and it is true a , b , c $\in$G
G is associative under addition modulo 6 ('$+_6$".)

Existence of identity : let a $\in$ G $a +_6 0 = 0+_6 a = a$ a $\in$G.
0 is the identity element in G.

Existence of inverse: from the above table,

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

Inverse of 0 is 0 , inverse of 1 is 5 , inverse of 2 is 4 , inverse of 3 is 3 , inverse of 4 is 2 , inverse of 5 is 1 $\Rightarrow$ inverse exists for each element of G and belongs to G

$\Rightarrow$ G is a group with respect to the binary operation $+_6$.
Commutative Law : $a +_6 b = b +_6 a$ $\forall$ a, b $\in$ G.
If a = 2 b = 4 $2+_6 4 = 0 = 4+_6 2$.
$(G, +_6)$ is an abelian group)

Note: The set of first m non-negative forms an abelian hroup with respect to addition modulo 'm'

Finite and identity Group: If the set G contains a finite number of element then the group then the group (G, *) is called a finite group. Otherwise the group (G, *) is called as *Infinite* group

Order of a group: Another natural characteristic of a group G is the number of element it contains. We call it as order of a group and is denoted by O(G).

Example 10: Let G = {1, -1} is a group
Then *O*(G) = 2**.**

If G is a group containing the set of all integers or set of all natural numbers, then ***O***(G) is infinite.

Order of an element of a group: If G is a group and a ∈ G. The order of a is the least positive integer m such that $a^m = e$.

So, to find the order of a group element compute a,a^2,a^3,.. until you reach the identity for the first time. See the following example.

In the group { 1 , -1 , I , -i} 1 is identity element i^1 =I , i^2 = -1 , i^3 = -I , i^4 = 1 , i^5 =I , i^6 = -1 , i^7 = -I , i^8 = 1. Identity appeared twice at i^4 and i^8 , but o (i) = 4 (it is the least)

If such integer does not exists we say that the order of a is infinity. We use the notation ***O*** (a) for the order of a.

Co-prime

Two number are said to be co prime if they do not have any common factory except '1'. If a are co primes then there exists two integers x , y such that xa + by = 1.

Example:-7.

On a group G, O (a) = 18, State that the orders of a^6, a^{15}, a^{-7}.

Solution:- $O\ a \quad n$

$$O\ a^k \quad \frac{n}{n,k}$$

1) O (a) = 18

$$O\ a^6 \quad \frac{18}{18,6} \quad \frac{18}{6}$$

2) O (a) = 18

$$Oa^{15} \quad \frac{18}{18,15} \quad \frac{18}{2}$$

3) O (a) = 18

$$Oa^{7} \quad \frac{18}{18,7}$$

Now Oa^{7}

Oa^{7} Oa^{7} O (a^{-7}) = O (a^{7}) (the order of element of group is same as its inverse)

$$O\ a^{7} \quad \frac{18}{18,7} \quad 18\,.$$

Example 11: Find the order of such element of the group G = {1, 2, 4, 7, 8, 11, 13, 14} the composition being multiplication modulo 15.

Solution: Identity element of G = 1:***O*** (1) =1

To Find the order of $2,2x_{15}2x_{15}2 = 4x_{15}2=8$

$2x_{15}2x_{15}2 = 4x_{15}2=8$

$2x_{15}2x_{15}2x_{15}2 = 8x_{15}2=$**1(identity)**

Hence ***O***(2) = 4

To Find the order of $4,4x_{15}4$ =1(identity)

Hence ***O***(4) = 2

To Find the order of $7,7x_{15}7 = 4$

$7x_{15}7x_{15}7 = 13$

$7x_{15}7x_{15}7x_{15}7 = 13x_{15}7 =$ **1(identity)**

Similarly, we can compute the order of 8,11,13,14.

Sub Group :

Sub Group: In general we are not interested in a subset of a group G. but certain subset of elements in a group is itself a group. This situation arises so often that we introduce a special name to describe it, called sub group. See the following definition for a subgroup.

Definition: A non-empty subset H of a group G is said to be a subgroup of G if H itself is a group, with respect to the same binary operation defined on G.

Every subgroup of G is a complex of G every complex is not always a subgroup.

Example 12: Q*under multiplication is a proper subgroup of R* under multiplication.

Example 13: Additive group of even integer is a subgroup of the additive group of all integers.

Two-Step Subgroup Test:

Theorem: A non-empty subset of H of a group G is a subgroup of G if and only if

i. a,b ∈H implies ab ∈H
ii. a ∈H implies that a^{-1} ∈ H

Theorem: A non-empty subset of H of a group G is a subgroup of G if and only if a , b ∈H => ab^{-1} ∈H.

One-Step Subgroup Test

Example 14 : See the example to under stand one-step subgroup Test.

G be the group of non-zero complex numbers under multiplication.

H = {a+ib/a^2+b^2 = 1,a∈R b∈R} is a sub group of G.

Let x , y ∈H where x = a + ib and y = c + id

Inverse of y $\frac{1}{C \quad id}$ $\frac{C \quad id}{C^2 \quad d^2}$

we have $xy^{-1} = (a + ib)\ \frac{C \quad id}{C^2 \quad d^2} = ac+bd +i(bc-ad)/c^2 + d^2$

real part of xy^{1} $\frac{ac \quad id}{C^2 \quad d^2}$

imaginary part of xy^{1} $\frac{bc \quad ad}{C^2 \quad d^2}$

consider $\frac{ac \quad bd}{C^2 \quad d^2}_2$ $\frac{bc \quad ad}{C^2 \quad d^2}_2$

$$\frac{a^2c^2 \quad b^2d^2 \quad 2abcd \quad b^2c^2 \quad a^2d^2 \quad 2abcd}{c^2 \quad d^2}$$

$$\frac{a^2 \quad b^2c^2 \quad d^2}{c^2 \quad d^2} \quad \frac{1.1}{1} \quad 1$$

Xy^{-1} ∈H , hence H is a subgroup of G.

Example 15: Let Z be the group of all integers

Let $H_1 = \{\ldots..-6,-4,-2, 0, 2, 4, 6\ldots\}$
$H_2 = \{\ldots..-12,-9,-6,-3, 0, 3, 6, 9, 12\ldots\}$ be two subgroups of Z.

$H_1 \cup H_2 = \{ -12, -9, -6, -4, -3, -2, 0, 2, 3, 4, 6, 9,\ldots\}$
Since $-2 \in H_1 \cup H_2$, $-3 \in H_1 \cup H_2$ but $-2 + -3 \notin H_1 \cup H_2$
$H_1 \cup H_2$, is not closed under '+'.
$\therefore$ $H_1 \cup H_2$, is not subgroup of (Z, +).

Example 16 : G = {1, -1} is a group
H = {-1} is a subset of G.
$H^{-1} = \{-1\}$
$H = H^{-1}$ but H is not a group since identity does not exists.
$\therefore$ H is not a subgroup of G.

Check your progress

1. Show that AB is a sub-group of G if and only if AB = BA.
2. When does the semi-group form a group?
3. Prove that the set {0, 1, 2, 3, 4, 5} is a finite abelian group of order 6 with respect to addition modulo 6.
4. Show that the set $G = \{a + b\sqrt{2} : a, b \in Q\}$ is a group with respect to addition.

7. LET US SUM UP

In this chapter we have learnt the details of algebraic structures semi-group and groups. The examples of semi-group and group are varying because of the properties related to the structure. The study of semi-groups and groups will make the study of finite state machines and coding theory simpler.

8. UNIT END EXERCISE

1. Show that the set of all positive rational numbers forms an abelian group under the composition defined by $a * b = \frac{ab}{2}$.
2. Show that set IN of all natural numbers is not a group with respect addition.
3. Find the order of the elements of the group $(z_4, + 4)$.
4. Find the order of the elements of the group ({1, w, w^2}, .). Where w isa cube root of 1.

5. Prove that the fourth roots of unity form an abelian group under multiplication.
6. Prove that the set {0, 1, 2, 3, 4} is a finite Abelian group of order 5 under addition modulo 5 as composition.
7. Check whether (Z, -) is semi-group or not. Where "-" denotes integer subtraction.
8. Check whether (Z, +) and (Z, .) are monoids or not.

Q.9 Show that the set of matrices $A = \begin{bmatrix} \cos & -\sin \\ \sin & \cos \end{bmatrix}$, where $\in IR$, forms a group under matrix multiplication.

Q.10 Show that the integer multiples of 5 form a sub-group of the additive group of integers.

11.9 REFERENCES FOR FURTHER READING

1. University Algebra by N.S. Gopalkrishnan.
2. Contemptary Algebra by Gallian.
3. Discrete mathematics by Kenneth and Rosen.
4. Discrete mathematical structures by Kolman, Busby and Ross.
5. Modern Algebra by Vasishtha.

12

NORMAL SUBGROUP

Unit Structure

1. OBJECTIVES :

After going through this chapter students will be able to know:

- Operations like product and quotient of these algebraic structures.
- Isomorphism, Homomorphism and Automorphism group.
- Generators of Cyclic group.
- Normal sub-group.
- Coding and Encoding of group.

2. INTRODUCTION :

After having all the basic property of group and sub-group, we now begin our journey with more detail about group study. In this we are going to discuss about product of group and quotients group, isomorphic group, homomorphic group, automorphic group. In group theory cyclic group are the simplest group also it is very interesting. In previous chapter we learn about sub-group, now here we discuss about cosets and normal sub-group.

12.2 PRODUCT AND QUOTIENTS OF GROUPS :

12.6.1 Definition : If G_1 and G_2 are groups then the product of G_1 and G_2 denoted as $G_1 \times G_2$ is a group with binary operation defined by $(a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1 b_2)$

Examples 1: Let $G_1 = G_2 = {}_2 = \{\bar{0}, \bar{1}\}$, $\bar{0}$ is notation for [0] find $G_1 \times G_2$.

Solution: $G = G_1 \times G_2 = {}_2 \times {}_2$

$= \{(\bar{0}, \bar{0}), (\bar{0}, \bar{1}), (\bar{1}, \bar{0}), (\bar{1}, \bar{1})\}$

Composition table for ${}_2 \times {}_2$ is

x	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$
$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$
$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{1})$
$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$
$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{0})$

Note that in $({}_2, +)$, $\bar{1} + \bar{1} = \bar{2} = \bar{0}$. G is group of order four.

12.3 HOMOMORPHISM

Group of Homomorphism: Till now we have seen the notion of a group and various type of group. Now we see the relation between two groups by introducing "Homomorphism". A relation between groups G and G, is generally exhibited in terms of a structure relating map from G to G_1.

Let G and G_1, be two groups. We are interested in a map that relates the group structure of G to the group structure of G_1, and this map often gives us information about the structure of G_1 from known structural properties of G, or information about the structure of G from known structural properties of G_1

We known that the group structure is determined by its binary operation. We now define such a structure relating map for groups, and then point out how the binary operations of G and G_1 are related by such a map.

Definition: Let G and G_1 be groups. A map $f : G \rightarrow G_1$ is said to be Homomorphism

If $f(ab) = f(a)\, f(b)$ for all $a , b \in G$.

Note: If the operation in G is denoted by '*' and the operation in G_1 is . The above condition for Homomorphism means the following.

$f(aob) = f(a) . f(b)$.

1. Properties of Homomorphism

Let G and G_1 be two groups. e and e_1 be the identity element of G and G_1 respectively. If f is Homomorphism from G to G_1 then $f(e) = e_1$

Range of Homomorphism: G and G_1 are two groups and f is homomorphism from G to G_1. The set of all f images of G in G_1 is called range of homomorphism.

It can be written as $f(G) = \{ f(a) / a \in G\}$

2. Types of Homomorphism

Onto Homomorphism: Let G and G_1 be two groups and f is a mapping from G onto G_1.

If $f(ab) = f(a)\, f(b)$ a, b ∈ G then f is said to be a **Homomorphism from G onto G_1.**

In some books it is referred as **epimorphism**.

Endomorphism: A homomorphism of a group into itself is called an endomorphism.

Monomorphism: If the homomorphism is one-one it is called monomorphism.

Example 2: Let G be the additive of integers and G_1 be the multiplicative group. Show that $f : G \rightarrow G_1$ a function defined as $f(m) = e^m$ is a homomorphism

Solution: Let $m , n \in G$; $f(m) = e^m \in G_1$ and $f(n) = e^n \in G_1$

$m+n \in G$ (G is additive group)

$f(m+n) = e^{m+n} = e^m e^n = f(m) f(n)$

f is homomorphism from G to G_1.

12.4 ISOMORPHISM

Isomorphism: A function f from G to G_1 Is said to be isomorphism, if

1. $f : G \rightarrow G_1$ is one-one
2. $f : G \rightarrow G_1$ is onto

3. $f: G \to G_1$ is homomorphism.
Says distinct element in G have distinct f - images in G_1
Says $X \quad G_1 \quad a \quad G$ such that $f\ a \quad x$.
Says image of the product is same as product of images.

Note: in the above definition, we have denoted the operation as multiplication. We can use different symbols to denote the compositions.

Note: There may exists more than one isomorphism from G onto G_1.

Example 3: Let G be the multiplication group of all positive real numbers, and G_1 be the additive group of all real numbers. The mapping defined by $f : G \to G_1$ such that $f(x) = \log x$ .is isomorphism from G to G_1

Solution: : $G \to G_1 = \log x$

To prove f is one – one

Let $x_1, x_2 \in$ and $f(x_1) = f(x_2)$

* $\log x_1 = \log x_2$

* $e^{\log x_1} = e^{\log x_2}$

$\Rightarrow \quad x_1 = x_2$

* f is one – one from G to G_1

To prove f is on-to

For any real number $y \in G_1$ e^y is a positive real number such that $e^y \in G$

$f(e^y) = \log e^y = y \in G_1$

$\therefore$ Each element of G_1 is the f - image of some element in G.

i.e. f is on-to.

To prove f as homomorphism.

Consider $x,y \in G$ where $f(x) = \log x$: $f(y) = \log y$

Then $f(xy) = \log(xy)$

$= \log(x) + \log(y)$

$= f(x) + f(y)$

f is homomorphism from G to G_1

$\therefore$ f is isomomorphism from G to G_1

Example 4: There exists isomomorphism from an additive group of integers.
G = {….,-3, -2, -1, 0, 1, 2, 3…} to another additive group
G_1 = {….,-3m, -2m, -m, m, 1m, 2m, 3m…} where m is any fixed integers not equal to zero.
Solution: Define mapping $f : G \rightarrow G_1$ such that $f(x) = mx$
To prove f is one- one : let $x_1, x_2 \in G$ and $f(x_1) = f(x_2)$
$mx_1 = mx_2$ (from the definition of f)
$x_1 = x_2$
f is one – one from G to G_1
To prove f is onto: for any element $y \in G_1$ $\exists$ $y/m \in G$ such that $f(y/m) = m(y/m) = y \in G_1$

* each element of G_1 is the f - image of some element in G.

i.e., f os on-to.
To prove f as n=homomorphism.
Consider x,y $\in$ G where $f(x) = mx$: $f(y) = my$

$f(x + y) = m(x+y)$
$= mx + my$
$= f(x) + f(y)$

f is homomorphism
$\therefore$ f Is isomorphism from G to G_1

12.5 AUTOMORPHISM OF A GROUP

Definition: If $f : G \rightarrow G$ is an isomorphism from a group G to itself, then f is called an automorphism of G.

Example 5: If G is an additive group of complex number, show that $f : G \rightarrow G$ such that f(Z) = pZ where p is a non-zero complex number, an automorphism of G.

Solution: G is an automorphism if $f : G \rightarrow G$ is an isomorphism.
To prove f is one-one.
Let $Z_1, Z_2 \in G$ and $f(Z_1) = f(Z_2)$

$PZ_1 = pZ_2$
$Z_1 = Z_2$

f is one-one.
To prove f is onto.
For any element $Z \in G$ there exists $Z/p \in G$ such that $f(Z/p) = p.(Z/p) = Z$.
Each element of G is the f- image of some element in G.
There fore f is onto.
To prove f is homomorphism.

Consider $f(Z_1 + Z_2) = p(Z_1 + Z_2) = pZ_1 + pZ_2 = f(Z_1) + f(Z_2)$
f is an homomorphism.
There fore f is isomorphism from G to G.
Hence $f : G \to G$ is an automorphism.

12.6 CYCLIC GROUP

Cyclic group: In the group theory, cyclic group are the simplest are the simplest among all group all groups. Because of this cyclic groups possess interesting properties. With the help of cyclic group we can find answer for some of the difficult questions in group theory. Now let us see what do we mean by a cyclic group?
The formal definition of a cyclic group is given below.

Definition: A group G is called *cyclic if for some* a ∈ G, every element x ∈ G is of the from such that a^n
Where n is some integer. The element 'a' is called a generator of G.
A cyclic group G generated by a can be represented as G = <a>
If G is a group with respect to the binary operation addition, cyclic group is defined as G = { na / n ∈ Z}

Example 6: G = {1, -1} is a cyclic group generated by -1 ($\because$ 1 = $(-1)^{2,}$ -1 = $(-1)^1$)

12.6.1 Cyclic Subgroup: *A subgroup H of a group G is called a* ***cyclic subgroup*** *if H is a cyclic group.*

Note: If a is a generator of a cyclic group G then a^{-1} is also a generator

Let G be a cyclic group generated by a.

Then for every x ∈G there exists an integer, such that $x = a^m$

$= (a^{-1})^{-m}$

$\therefore$ Every x can be expressed as integral power of a^{-1}

i.e.,a^{-1} is also a generator of G.

12.7 COSETS

Definition: If G is a Group and H is a subgroup of G. let a ∈ G Then

Ha = {ha : h∈H} is called right coset of H in G generated by a.

And the set aH = {ah: h ∈ H} is called left coset of H in G generated of a.

Example 7: Let G = { a, b, c, d, e, f} is a group. And H = { b, c, e} be the subgroup of G.

Solution: a ∈ G : Ha = { ba, ca , ea}

d ∈ G : Hd = { bd, cd , ed} are some right coset of H in G.

c ∈ G : Hc = { bc, cc , ec}

The set aH = { ah : h ∈ H} is called left coset of H in G generated by a.

a ∈ G : aH = { ab, ac , ae}

d ∈ G : Hd = { db, dc , de} are some right coset of H in G.

c ∈ G : Hc = { cb, cc , ce}

Note: If G is an abelian group then **aH = Ha**

Example 8: Let G be the additive group of integers, and H is a subset of group of G where element of H are obtained by multiplying each element of G by 2.

Solution:

Clearly (H, +) is a subgroup of (G, +).

Now G = {…..-3,-2,-1, 0, 1, 2, 3…}

H = {…..-6,-4,-2, 0, 2, 4, 6…}

1 ∈ G and 1 + H = {…..-5,-3,-1, 1, 3, 5, 7…}

Example 9: Let G= <a> a cyclic group of order 15. List all the cosets of $<a^5>$ in G.

Solution: Let G = <a> a cyclic group of order 15.

i.e. G = {e, a, a_1, a_2, ……., a_{14}}

H is a subgroup of G.

H = {e, a^5, a^{10}}

The left cosets of $<a^5>$ are

aH = {a, a^6 , a^{11}}, a^2H = {a^2, a^7, a^{12}}, a^3 H = {a^3, a^8,a^{13}},

a^4 H = {a^4,a^9,a^{14}} .

Remark: A coset may not essentially a subgroup

Remark: If e is the identity in G, it is also identity in H. Then eH = {eh/h ∈ H} = H

12.7.1 Normal Subgroup

If G is a group and H is a subgroup of G, it is not always true that aH = Ha for all a in G. If it happens i.e.,if Ha = aH a in G we call H as normal subgroup. And it is denoted by H ◁ G.

Definition: If G is a group and H is a subgroup of G.If Hx = xH ∀ x∈G then H is called a normal subgroup.

Note: Every normal subgroup but every subgroup need not be a normal subgroup.

Importer and proper normal subgroups: G is a group then G , {e} are subgroup of G and they are also normal subgroups of G. These two subgroups are called trivial or importer subgroups of "G"

The normal subgroup of G other than these two subgroups are called proper normal subgroups of G.

For example H = {1,-1} is a normal subgroup of multiplicative group of none zero real numbers.

Example :- Show that every subgroup of an Abelian group is normal.

Solution :- Let G be an abelian and H a subgroup of G. Let x be any element of G and H any element of H.

So, $xhx^{-1} = xx^{-1}$

$=h$ […G is Abelian ⇒ $x^{-1}h = hx^{-1}$]

$=eh$

*h ∈ H. Hence

x ∈ G,

* h ∈ H

* xhx^{-1} ∈ H

So H is normal in G.

Example :- Given that H = { I, (12)(13) (34)} is a subgroup of A_4. Show that (243)H = (142)H and (132)H = (234)H but (234)(132)H ≠ (142)(234)H. Is H a normal subgroup of Ah? Justify your answer.

Solution :- H = { I, (12)(34)} is a subgroup of Ah.

A_4 = { I, (12)(34)(13)(24)(23)(14)(123)(132)(142)(124)}

To show that (243)H = (142)H

(243)(12)(34) = (142)

(243)H = {(243)(142)}

(142)H = i.e. (142)I and (142)(12)(34)

(142)H = {(142)(243)}
….. (243)H = (142)H
To show that (132)H = (234)H
(132)H = (132)I
(132)(12)(34) = {(132), (234)}
(234I = (234)
(234)(12)(34) = (132)
(234)H = {(234)(132)}
…. (132)H = (234)H
To show that (234)(134)H ≠ (142)(234)H
(234)(132)H = (234)(132)
(234)(132)(12)(34) = I
(142)(243)(12)(34) = (124)
Thus (243)(132)H ≠ (142)(243)H
…GH = HG
… H is normal subgroup A_4.

12.8 CODE AND GROUP CODE

Word : A sequence of 0's and 1's is called a word.
e.g. 1101, 101, 00100 are words.

Code : A collection of words used to represent different messages is called code.

Codeword : A word in a code is called codeword.

Block of code : A code consisting of words having same length is called block of code.

Let B = {0, 1} then $B \times B = \{00, 01, 10, 11\} = B^2$ i.e. B^2 contains words of length 2, and it contains 4 elements or codes. Number of elements in the set is called cardinality of the set and it is denoted by two vertical bar.

$\therefore$ Number of elements in set $B^2 = |B^2| = 4$. Also |B| = 2.

$\therefore |B^2| = |B \times B| = |B| \times |B| = 2 \times 2 = 2^2$

$\therefore |B^2| = 2^2 = 4$

Similarly

$B^3 = B \times B \times B$ = {000, 001, 010, 011, 100, 101, 110, 111},

$|B^3| = |B \times B \times B| = |B| \times |B| \times |B| = 2 \times 2 \times 2 = 2^3 = 8$

$\therefore$ The set B^m is collection of codes of length m and it contains 2^m codes.

$\therefore$ $|B^m| = 2^m$

Weight : Let $x \in B^n$ then weight of x is number of 1's in x and it is denoted by w(x).

e.g. i) $x = 1101 \in B^4 \therefore w(x) = 3$

ii) $x = 110010 \in B^6 \therefore w(x) = 3$

iii) $x = 11 \in B^2 \therefore w(x) = 2$

iv) $x = 0000 \in B^4 \therefore w(x) = 0$

$x \oplus y$: (Read as x ring sum y). Let $x, y \in B^n$, then $x \oplus y$ is a sequence of length n that has 1's in those position x and y differ and 0's in those positions x and y are the same.

i.e. The operation + is defined as

$0 + 0 = 0$ $\quad$ $0 + 1 = 1$

$1 + 1 = 0$ $\quad$ $1 + 0 = 1$

e.g.

i) $x, y \in B^3$, x = 101, y = 110

x =	1	0	1
y =	1	1	0
$x \oplus y$ =	0	1	1

$\therefore$ $x \oplus y = 011$ and $w(x \oplus y) = 2$

ii) $x, y \in B^6$, x = 110100, y = 111111

x =	1	1	0	1	0	0
y =	1	1	1	1	1	1
$x \oplus y$ =	0	0	1	0	1	1

$\therefore$ $x \oplus y = 001011$ and $w(x \oplus y) = 3$

iii) $x, y \in B^7$, x = 1010001, y = 0001010

$\therefore$ $x \oplus y = 1011011$ and $w(x \oplus y) = 5$

Distance : The distance between x and y is the weight of $x \oplus y$. i.e. $w(x \oplus y)$, it is denoted by d(x, y). The distance between two words is exactly the number of positions at which they differ.

$\therefore$ $d(x, y) = w(x \oplus y)$.

It is also called Hamming distance. **Minimum distance**: Let $x, y \in B^n$ then minimum distance = min. $\{d(x, y) : x, y \in B^n\}$.

Let $x_1, x_2, ..., x_n$ are the code words, let any x_i, i = 1, 2, … n is a transmitted word and y be the corresponding received word. Then $y = x_k$ if $d(x_k, y)$ is the minimum distance for k = 1, 2, …n. This criteria is known as the minimum – distance criterion.

Encoding function : Let m < n (m, n∈N, N is set of natural numbers) then an one to one function $e : B^m \to B^n$ is called an (m, n) encoding function. i.e. for $x \in B^m$ we have $y \in B^n$ such that e(x) = y.

Detection of errors : Let $e : B^m \to B^n$ (m < n) is an encoding function then if minimum distance of e is (k + 1) then it can detect k or less than k errors.

Correction of errors : Let $e : B^m \to B^n$ (m < n) is an encoding function then if minimum distance of e is (2k + 1) then it can correct k or less than k errors.

Example 1 : Let e is (2, 4) encoding function defined as

e(00) = 0000 e(01) = 1011

e(11) = 1100 e(10) = 0110

i) Find minimum distance,

ii) How many errors can e detect,

iii) How many errors can e correct.

Solution :

Let $x_0 = 0000$, $x_1 = 1011$, $x_2 = 0110$, $x_3 = 1100$

i) $w(x_0 \oplus x_1) = w(x_1) = 3$ w

$(x_0 \oplus x_2) = w(x_2) = 2$ w

$(x_0 \oplus x_3) = w(x_3) = 2$ w

$(x_1 \oplus x_2) = w(1101) = 3$ w

$(x_1 \oplus x_3) = w(0111) = 3$ w

$(x_2 \oplus x_3) = w(1010) = 2$

∴ Minimum distance of e = 2.

Note that minimum distance is not unique. There are three pairs having distance 2.

ii) $\therefore$ k + 1 = 2 $\therefore$ k = 1,

$\therefore$ e can detect 1 or less than 1 i.e. 0 errors.

iii) $\therefore$ 2k + 1 = 2 $\therefore$ $k = \frac{1}{2}$

$\therefore$ e can correct $\frac{1}{2}$ or less than $\frac{1}{2}$ errors, i.e. e can correct 0 errors.

Example 2 : Let e is (3, 8) encoding function defined as

e(000) = 00000000 e(011) = 01110001

e(010) = 10011100 e(110) = 11110000

e(001) = 01110010 e(101) = 10110000

e(100) = 01100101 e(111) = 00001111

i) Find minimum distance.

ii) How many errors can e detect?

iii) How many errors can e correct?

Solution :

Let x_0 = 00000000, x_1 = 10011100, x_2 = 01110010, x_3 = 01100101, x_4 = 01110001, x_5 = 11110000, x_6 = 10110000, x_7 = 00001111.

i) $w(x_0 \oplus x_1) = w(x_1) = 4$, $w(x_0 \oplus x_2) = w(x_2) = 4$,

$w(x_0 \oplus x_3) = w(x_3) = 4$, $w(x_0 \oplus x_4) = w(x_4) = 4$,

$w(x_0 \oplus x_5) = w(x_5) = 4$, $w(x_0 \oplus x_6) = w(x_6) = 3$,

$w(x_0 \oplus x_7) = w(x_7) = 4$

Similarly, $w(x_1 \oplus x_2) = w(11101110) = 6$,

$w(x_1 \oplus x_3) = 6$, $w(x_1 \oplus x_4) = 6$, $w(x_1 \oplus x_5) = 4$, $w(x_1 \oplus x_6) = 3$,

$w(x_1 \oplus x_7) = 4$, $w(x_2 \oplus x_3) = 4$, $w(x_2 \oplus x_4) = 2$, $w(x_2 \oplus x_5) = 2$,

$w(x_2 \oplus x_6) = 3$, $w(x_2 \oplus x_7) = 6$, $w(x_3 \oplus x_4) = 2$, $w(x_3 \oplus x_5) = 4$,

$w(x_3 \oplus x_6) = 5$, $w(x_3 \oplus x_7) = 4$, $w(x_4 \oplus x_5) = 2$, $w(x_4 \oplus x_6) = 3$,

$w(x_4 \oplus x_7) = 6$, $w(x_5 \oplus x_6) = 1$, $w(x_5 \oplus x_7) = 8$, $w(x_6 \oplus x_7) = 7$

$\therefore$ The minimum distance of e = 1.

ii) $\therefore$ k + 1 = 1 $\therefore$ k = 0

$\therefore$ e can detect 0 or less than 0 errors i.e. 0 errors.

iii) $\therefore$ 2k + 1 = 1 $\therefore$ k = 0

$\therefore$ e can correct 0 or less than 0 errors. i.e. 0 errors.

Example 3 : Compute

$$\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \oplus \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

Solution :

$$\begin{bmatrix} 1+1 & 1+0 & 0+0 \\ 0+1 & 1+0 & 1+1 \\ 1+0 & 0+0 & 0+1 \\ 0+1 & 0+1 & 0+0 \end{bmatrix} \oplus \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

Same digit sum = 0, opposite digit sum = 1

Example 4 : Let B = {0, 1} and + is defined on B as follows.

+	0	1
0	0	1
1	1	0

Then show that (B, +) is a group.

Solution :

Addition is associative. Here B is set of bits and the operation of on B is +. $\therefore$ B with operation + is associative.

Also 0 + 1 = 1 and 0 + 0 = 0

$\therefore$ $0 \in B$ is an identity element. Here inverse of each element is itself. Since 0 + 0 = 0. $\therefore$ $0^{-1} = 0$

and 1 + 1 = 0 $\therefore$ $1^{-1} = 1$

$\therefore$ Inverse of each element exists.

$\therefore$ (B, +) is a group.

Three Cartesian product of groups is again a group.

$\therefore$ $B^n = B \times B \times B \ldots n \text{ times} \ldots \times B$ with + operation defined as $(x_1, x_2, ..., x_n) \oplus (y_1, y_2, ..., y_n) = (x_1 + y_1, x_2 + y_2, ..., x_n + y_n)$ is also a group. Here identity element is $(0, 0, \ldots 0) \in B^n$ and every element is its own inverse.

$\therefore$ $(B^n, \oplus)$ is a group. Let $A \subseteq B^n$ such that $(A, \oplus)$ is a group then A is subgroup of B^n. Now we will see the encoding which uses this property of B^n.

Check Your Progress :

1. Let $e : B^2 \to B^6$ is an (2.6) encoding function defined as
   e(00) = 000000 e(01) = 011101
   e(11) = 111111 e(10) = 001110
   i) Find minimum distance.
   ii) How many errors can e detect?
   iii) How many errors can e correct?

2. Let e is (2, 5) encoding function defined as
   e(00) = 00000 e(01) = 11011
   e(11) = 11100 e(10) = 00101
   i) Find minimum distance.
   ii) How many errors can e detect?
   iii) How many errors can e correct?

Answers :

1. i) Minimum distance of e = 2.
   ii) Function can detect 1 or 0 errors.
   iii) Function can correct 0 errors.
2. i) Minimum distance of e = 2.
   ii) Function can detect 1 or 0 errors.
   iii) Function can correct 0 errors.

GROUP CODES:

An (m, n) encoding function $e : B^m \to B^n (m < n)$ is called a group code if range of e is subgroup of B^n. i.e. (Ran.(e), $\oplus$) is a group. Since Ran.(e) $\subseteq B^n$ and if (Ran.(e), $\oplus$) is a group then Ran.(e) is a subgroup of B^n.

If an encoding function $e : B^m \to B^n (m < n)$ is a group code, then the minimum distance of e is the minimum weight of a non zero codeword.

Example 5 : Show that an (3, 7) encoding function $e : B^3 \to B^7$ defined by

e(000) = 0000000 e(011) = 0111110
e(001) = 0010110 e(101) = 1010011
e(010) = 0101000 e(110) = 1101101
e(100) = 1000101 e(111) = 1111011

is a group code. Hence find minimum distance.

Solution : Let

$x_0 = 0000000$ $x_4 = 1000101$

$x_1 = 0010110$ $x_5 = 1010011$

$x_2 = 0101000$ $x_6 = 1101101$

$x_3 = 0111110$ $x_7 = 1111011$

$\therefore$ Ran.(e) = $\{x_0, x_1, ..., x_7\}$

$x_0 \oplus x_0 = x_0$, $x_0 \oplus x_1 = x_1$, $x_2 \oplus x_7 = 1010011 = x_5$ like this we can compute and this we will present in table.

The composition Table is,

$\oplus$	x_0	x_1	x_2	x_3	x_4	x_5	x_6	x_7
x_0	x_0	x_1	x_2	x_3	x_4	x_5	x_6	x_7
x_1	x_1	x_0	x_3	x_2	x_5	x_4	x_7	x_6
x_2	x_2	x_3	x_0	x_1	x_6	x_7	x_4	x_5
x_3	x_3	x_2	x_1	x_0	x_7	x_6	x_5	x_4
x_4	x_4	x_5	x_6	x_7	x_0	x_1	x_2	x_3
x_5	x_5	x_4	x_7	x_6	x_1	x_0	x_3	x_2
x_6	x_6	x_7	x_4	x_5	x_2	x_3	x_0	x_1
x_7	x_7	x_6	x_5	x_4	x_3	x_2	x_1	x_0

Like in Example 4 we can verity that (Ran.(e), $\oplus$) is group and Ran.(e) $\subset B^7$.

$\therefore$ Ran.(e) is subgroup of B^7.

$\therefore$ $e : B^3 \to B^7$ is a group code.

The minimum distance of a group code is the minimum weight of non zero code word.

Consider $w(x_0) = 0$, $w(x_1) = w(x_4) = 3$, $w(x_2) = 2$, $w(x_5) = 4$, $w(x_3) = w(x_6) = 5$, $w(x_7) = 6$.

$\therefore$ Minimum distance = 2.

Example 6 : Show that an (2, 5) encoding function $e : B^2 \to B^5$ defined as

e(00) = 00000 e(10) = 10101

e(01) = 01110 e(11) = 11011

is a group code. Hence find minimum distance and also find how many errors can e detect?

Solution :

$x_0 = 00000,\ x_1 = 01110,\ x_2 = 10101,\ x_3 = 11011$

$\therefore$ Ran.(e) = $\{x_0, x_1, x_2, x_3\}$

$\therefore$ The composition Table

$\oplus$	x_0	x_1	x_2	x_3
x_0	x_0	x_1	x_2	x_3
x_1	x_1	x_0	x_3	x_2
x_2	x_2	x_3	x_0	x_1
x_3	x_3	x_2	x_1	x_0

Addition is associative

$\therefore$ (Ran.(e),$\oplus$) is associative. We can see that the first row is same as heading row.

$\therefore$ x_0 is identity element. Also $x_0 \oplus x_0 = x_0$, $\therefore$ $x_0^{-1} = x_0$.

$x_2 \oplus x_2 = x_0$. $\therefore$ $x_2^{-1} = x_2$ so on. i.e. inverse of each element exists which is itself.

$\therefore$ $(\text{Ran.(e)}, \oplus)$ is a group and since $\text{Ran.(e)} \subset B^5$.

$\therefore$ Ran.(e) is subgroup of B^5.

$\therefore$ $e : B^2 \to B^5$ is a group code.

Consider,

$w(x_0) = 0,\ w(x_1) = w(x_2) = 3,\ w(x_3) = 4$.

The minimum distance of a group code is the minimum weight of nonzero code word.

$\therefore$ Minimum distance = 3.

Here k + 1 = 3, k = 2.

$\therefore$ e can detect 2 or less than 2 errors. i.e. e can detect 0, 1 or 2 errors.

Check your progress :

1. Show that an (2, 4) encoding function $e : B^2 \to B^4$ defined by

   e(00) = 0000 e(01) = 0011

   e(11) = 1110 e(10) = 1101

   is a group code.

12.9 LET US SUM UP

In this chapter we have learned that

- The product of G_1 and G_2 denoted as $G_1 \times G_2$.
- Homomorphism of a group, its property and types of homomorphism.
- Isomorphism of a group.
- Automorphism of a group.
- Cyclic group and its generators.
- Cosets and normal sub-group and Quotient group.

12.10 UNIT END EXERCISE

1. Define normal subgroup and give one example.
2. If (C, +) be a group, f:C $\rightarrow$ C define by f(Z) = $\bar{Z}$ for every Z $\in$ C, $\bar{Z}$ being conjugate of Z, then show that f is Automorphism.

Q.3 Show that A = ({0, 1, 2, 3, 4, 5}, $+_6$) is cyclic.

4. Show that multiplicative group G = {1, -1, i, -i } is cyclic.
5. Let (Z, +) be the group of integers and N = {3n / n $\in$ Z} then N is a normal subgroup of Z.

Q.6 If G = {1, -1, i, -i } is a group and G'= ({0, 1, 2. 3}, $+_4$) is another group then show that gG is isomorphism to G'.

7. If $f : R^+ \rightarrow R$ defined by f(x) = log(x) for every x $\in$ R^+ then show that f is isomorphism. Where R^+ and R are multiplicative group.
8. Prove that all finite group of order 2 are isomorphism.
9. Mapping $f : G \rightarrow G$ defined by f(x) = x^{-1}, for all x $\in$ G on a group (G, *) is an automorphism if and only if (G, *) is abelian.
10. Show that the group ({0, 1, 2, 3,……n-1}, t_n) is a cyclic group.

Q.11Show that (U_n, .) is a cyclic group of n^{th} roots of unity under multiplication.

Q.12 If H is subgroup of G and if x $\in$ G implies that x^2 $\in$ H, then prove that H is a normal subgroup of G.

Q.13 Compute $\begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix} \oplus \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$.

14. Find weights of the given words a) 001110, b) 0000, c) 111, d) 100100110.

15. Find the distance between x and y i)

x = 00111101, y = 00110010

ii) x = 1010001100, y = 0000111100

Answers :

13 $\begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$

14 a) 3 b) 0 c) 3 d) 4

15. i) 4 ii) 4

12.11 REFERENCES FOR FURTHER READING

1. University Algebra by N.S. Gopalkrishnan.

2. Contemptary Algebra by Gallian.

3. Discrete mathematics by Kenneth and Rosen.

4. Discrete mathematical structures by Kolman, Busby and Ross.

5. Modern Algebra by Vasishtha.

13

RINGS

Unit Structure

1. OBJECTIVES :

After going through this chapter students will be able to:

- Algebraic structures with two binary operations.
- Definition of ring and its property.
- Zero divisor and integral domain.
- Fields.
- Ring of homomorphism.
- Ring of isomorphism.

13.1 INTRODUCTION :

Groups were studied in the previous chapters, and the definition of group involves a single binary operation with respect to addition or multiplication. The distributive laws interlink the two operators addition and multiplication. This leads us to the study of one such algebraic system equipped with two binary operations called as rings.

Ring is the second algebraic system. The abstract concept of Rings has its origin from the set of integers. The algebra of rings follows the pattern already laid out for group. Only difference is algebraic structures with two binary operations.

13.2 ALGEBRAIC STRUCTURES WITH TWO BINARY OPERATIONS.

An algebraic structure is a nonempty set together with one or more binary operation on that set.

Addition and multiplication are both binary operations on the set R of real numbers is called algebraic structure with two binary operations. It is denoted by (R,+, .).

13.2.1 Rings

Definition: A ring R is a non-empty set with two binary operations denoted by '+' and $\cdot$ with respect to the following conditions.

- R is an abelian group with respect to +,i.e.,
  - I. $a + (b + c) = (a + b) + c \quad a,b,c \in R$
  - II. there exists $0 \in R$ such that $a + 0 = a = 0 + a \quad a \in R$
  - III. For each $a \in R$, there exists $-a \in R$ such that $a + (-a) = 0 = (-a) + a$
  - IV. $a + b = b + a \quad a, b \in R$
- R is a semi group for i.e., $a.(b.c) = (a.b).c \quad a, b, c \in R$
- Multiplication distributes over assition, i.e.,
  - I. $a.(b + c) = a.b + a.c \quad a,b,c \in R$
  - II. $(b + c).a = b.a + c.a \quad a,b,c \in R$

Note: we write a.b as ab.

Now let us see one example that satisfies the above-described axioms.

Example 1: Set of even integers is a ring with respect to usual addition and multiplications of integers.

Solution: Let E be the set of even integers i.e.,

$$E = \{2x : x \in Z\}$$

Let $a, b \in E$ where $a = 2m$ and $b = 2n$

$a+b = 2m + 2n = 2(m+n) \in E$ ($\because$ $m+n \in Z$)

$\therefore$ E is closed with respect to addition.

Let a, b, c ∈ E where a = 2m, b = 2n, c = 2p

a+(b+c)=2m+(2n+2p)=2m+2(n+p)=2[(m+n)+p]

=(2m+2n)+2p=(a+b)+c

∴ *E is associative with respect to addition.*

Since 0 ∈ Z, O = 2.0 ∈ E

Consider a + O = 2m+2.0 = 2(m+0) = 2m = a

∴ O is the identity element in E.

For m ∈ Z there exists –m ∈ Z and 2.(-m) ∈ E.

Let –a =2.(-m)

Consider a + (-a) = 2m +2.(-m)

= 2(m+(-m))

= 2.0

= O =(-a) +a

∈ (-a) is the inverse of a.

∴ *Inverse exists for each element in E.*

For a, b, ∈ E then a + b = 2m + 2n = 2(n+m) (sum of integers is commutative) = 2n + 2m

= b + a

E is commutative with respect to addition.

(E, +) is *an abelian group*.

Consider a, b, c ∈ Z where a = 2m,b = 2n, c = 2p

a(bc)= 2m(2n.2p) =2m,(4np) = 8 mnp

(ab)c = (2m.2n.)2p =(4mn)2p = 8 mnp

a(bc) = (ab).c a,b,c ∈ E

E is associative with respect to multiplication.

Consider a.(b+c) = 2m.(2n 2p)

= 2m. 2n + 2m.2p

= a.b + a.c

Similarly, (b + c).a = b.a + c.a

∴ Distributive laws hold in E.

∴ Hence (E, +, .) is a ring.

Example 2: Show that the set of all rational numbers is a ring with respect to ordinary addition and multiplication.

Solution: Let Q be the set of all rational numbers.

1) (Q, +) is abelian.

Closure: Let a, b ∈ Q then a + b ∈ Q
because sum of two rational numbers is a rational number.
Associative: Let a, b, c ∈ Q then (a + b) + c = a + (b + c)
because associative law for addition holds.
Existence of Identity: 0 ∈ Q and 0 + a = a + 0 = a for every a ∈ Q
i.e. 0 is additive identity in Q.
Existence of inverse: for every a ∈ Q, -a ∈ Q and a + (-a) = 0
Hence, additive inverse in Q exists for each element in Q.
Commutative: Let a, b ∈ Q then a + b = b + a
because addition is commutative for rational.

2) (Q, .) is a semi group.
Closure : Since the product of two rational numbers is a rational number.
a, b ∈ Q then a .b ∈ Q
Associativity: Multiplication in Q is associative.

3) Multiplication is left as well as right distributive over addition in the set of rational numbers. i.e.
a.(b + c) = a.b + a.c
(b + c).a = b.a + c.a for every a, b,c ∈ Q .
Hence, (Q, +, .) is a ring.

13.3.1 Ring with unity

A ring need not have an identity under multiplication, when a ring other than {0} has an identity under multiplication; we say that the *Ring is with unity.*

Definition: R is called a ring with unity element if there exists 1 ∈ R such that a1 = a = 1a for all a 0 ∈ R.

Note: A Ring with unity contains at least elements 0 and 1.

Commutative Ring

In a ring, multiplication need not be commutative, when it sis, we say that the ring is *commutative.*

Definition: A Ring R is said to be commutative if ab = ba a, b ∈R.

Example 3: Let the addition and multiplication in Q $\sqrt{2}$ be defined as x = a + b $\sqrt{2}$ and y = c + d $\sqrt{2}$

$\in Q(\sqrt{2})$ x + y $(a + c) + (b + d)\sqrt{2}$

xy = (ac + 2bd) + (ad + bc) $\sqrt{2}$ is a commutative ring with unity.

Solution: $Q(\sqrt{2}) = \{a + b\sqrt{2} / a, b \in Q\}$

$X = a + b\sqrt{2}$ and $y = c + d\sqrt{2} \in Q(\sqrt{2})$

$x + y = (a + c) + (b + d)\sqrt{2}$ since a + c and b + d belong to Q

$x + y \in Q\sqrt{2}$.

∴ $\mathbf{Q}\sqrt{2}$ is closed with respect to addition.

For $x = a + b\sqrt{2}$, $y = c + d\sqrt{2}$ $z = e + f\sqrt{2}$ where a, b, c, d, e, f $\in Q\sqrt{2}$

We have, $x + (y+z) = a + b\sqrt{2} + ((c + d\sqrt{2}) + (e + f\sqrt{2}))$

$= a + b\sqrt{2} + (c + e + (d + f)\sqrt{2})$

$= (a + c + e) + (b + d + f)\sqrt{2}$

$= ((a + c) + e) + ((b + d) + f)\sqrt{2}$

$= ((a + c) + (b + d)\sqrt{2}) + (e + f\sqrt{2})$

$= (x + y) +$

∴ $Q\sqrt{2}$ is *Associative with respect to* ***Addition.***

Since 0 is a rational number $0 + 0\sqrt{2} \in Q\sqrt{2}$

Consider $(a + b\sqrt{2}) + (0 + 0\sqrt{2}) = (a + 0) + (b + 0)\sqrt{2}$

$= a + b\sqrt{2}$

Similarly $(0 + 0\sqrt{2}) + (a + b\sqrt{2}) = a + b\sqrt{2}$.

Hence $0 + 0\sqrt{2}$ is the identity existing in $Q\sqrt{2}$

For a, b ∈ Q, -a, -b ∈ Q hence $(-a) + (-b)\sqrt{2}) \in Q\sqrt{2}$

Consider $a + b\sqrt{2} + ((-a) + (-b)\sqrt{2}) = (a + (-a) + b + (-b)\sqrt{2}) = 0 + 0\sqrt{2}$

Similarly $(-a) + (-b)\sqrt{2} + (a + b\sqrt{2}) = 0 + 0\sqrt{2}$.

Hence $(-a) + (-b)\sqrt{2}$ is the inverse of $a + b\sqrt{2}$

Inverse exists for each element in $Q\sqrt{2}$.

$X = a + b\sqrt{2}$ and $y = c + d\sqrt{2} \in Q(\sqrt{2})$ where a, b, c, d ∈ Q

Consider $x + y = (a + c) + (b + d)\sqrt{2}$

Since addition of rational numbers is commutative.

a + c = c + a and b + d = d + b

$$x + y = (c + a) + (d + b)\sqrt{2}$$
$$= (c + d\sqrt{2}) + (a + b\sqrt{2})$$
$$= y + x$$

$\therefore$ $Q\sqrt{2}$ is **commutative** with respect to **Addition.**

$(Q\sqrt{2}, +)$ is an **Abelian group.**

Example 4 : Let (G, *) be an arbitrary commutative group and Hom G be the set of all homomorphisms from (G, *) onto itself. Then show that (Hom G, +, .) is a ring with unity, where the operation + defined by

(f + g)(a) = f(a)*g(a), a ∈ G, for every f, g ∈ Hom G, and ∈ denotes the functional composition.

Solution:

Closure : For every f, g ∈ Hom G, and a, b ∈ G,

(f, g)(a * b) = f(a * b) * g(a * b)

= (f(a) * f(b)) *(g(a) * g(b))

=(f(a) * g(a) * f(b) * g(b))

= (f + g)(a) * (f + g)(b),

So that the sum f + g ∈ Hom G.

Associative : For every f, g, h ∈ Hom G, and a ∈ G,

We have ((f + g) + h) (a) = (f + g)(a) * h(a)

= ((f(a) * g(a)) * h(a)

= f(a) * ((g(a) * h(a))

= f(a) * (g + h)(a)

= (f + (g+h))(a).

Thus (f + g) + h = f + (g + h).

Existence of identity : For every f ∈ Hom G, there exists constant mapping Z which map all elements of G on e, the identity of (G, *) such that

(f +Z)(a) = f(a) * Z(a) = f(a) * e = f(a).

Thus f +Z = f ∈ Z is an identity in Hom G, that is, the mapping Z in Hom G is the Zero element.

Existence of inverse: For every f ∈ Hom G, ∈ -f ∈ Hom G defined by $(-f)(a) = f(a)^{-1}$, such that , For every a ∈ G,

$(f +(-f))(a) = f(a) * f(a)^{-1} = e = Z(a)$.

Which implies that f +(-f) = Z, therefore inverse also exists.

Commutative property: For every f, g ∈ Hom G, a ∈ G, we have

(f + g)(a) = f(a) * g(a) = g(a) * f(a) = (g +f)(a).

Thus (f +g) = f + g,

Hence (Hom G, +) is commutative group.

Similarly we prove that (Hom G, ∈) is a semi-group with identity.

Now to prove that (Hom G, +, ∈) is a ring with unity there remains to show that ∈ is distributive over +.

f∈ (g + h)(a) = f(g + h) a) = f(g(a) * h(a)) = f(g(a)) * f(h(a)) = (f∈g)(a) * (f∈h)(a).

Therefore f∈ (g + h) = (f∈g) + (f∈h), similarly, we can prove right distributive law.

Thus (Hom G, +, .) is a ring with unity.

13.4 ZERO DIVISORS

There are some properties, which are not true in a general ring. We know that product of two integers is zero, if one among them is zero, but this may no longer be true in any ring R of 2 x 2 matrices we have $\begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix}\begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix}$; even through $\begin{matrix} 0 & 0 \\ 0 & 1 \end{matrix}\begin{matrix} 1 & 0 \\ 0 & 0 \end{matrix}$ are non-zero and their product is zero in R.

Definition: Let R be a ring and a ∈ R, b ∈ R both are non-zero but their product

ab = 0 . Then we say that **a, b are zero divisors.**

13.4.1 Integral Domain

Definition: A commutative Ring, with unity is an integral domain if it has no zero divisors and it is donated by the symbol.

For example: The Ring of integrals, rational Numbers, and real numbers and complex numbers is all integral domain.

5. FIELD

Definition: A commutative Ring R with unit element i ≠ 0 in which every non-zero element has an inverse with respect to multiplication am called a **field.**

Example 5: Set of Gaussian integers is an integer's domain but not a field.

Solution: Set of Gaussian integers Z(i) = {a + ib/a, b∈Z)}

Let x , y ∈ Z(i)

Where x = a + ib and y = c + id where a, b, c, d ∈Z

x + y = (a + c) + (b + d) I = $a_i + ib_1 = a + c$ and $b_1 = b + d \in Z$.

x . y = (ac – bd) + (ad + bc) I

$= a_2 + ib_2$ where $a_2 = ac – bd$, $b_2 = ad + bc \in Z$.

∴ +, . are binary operation in Z(i).

Since the element of Z(i) are integers,

We have that

1. Addition and multiplication are commutative in Z(i)
2. Addition and Multiplication are associative in Z(i)
3. Multiplication is distributive over addition in Z(i)

Clearly, zero element $0 = 0 + 0_i \in Z$ and unit element $1 = 1 + 0_i \in Z$

Further, for every x = a + b ∈Z(i), x, y = 0 ∈ x = 0 since x , y are integers.

Z(i) is without zero divisors.

Hence Z(i) is an integral domain

Let $m \quad 3 \quad 4i \quad Z\,i$ and $n \quad \frac{3}{25} \quad \frac{i\,4}{25}$

So that $m.n \quad 9/25 \quad 16/25 \quad i \quad 12/25 \quad 12/25 \quad i$

But n ∈ Z(i), because 3/25 and 4/25 ∈ Z.

So every non-zero element of Z(i) is not invertible

Hence Z(i) is not a field.

6. RING HOMOMORPHISM

In groups, one way to discover information about a group is to examine its interaction with other groups by way of homomorphism. Now we show that just as a group homomorphism preserves the group operation, a ring homomorphism preserves the ring operations.

Definition: A ring homomorphism f from a ring R to another ring R_1 is a mapping from R to R_1 that preserves the two ring operations; that is, for all a, b in R

$$f(a + b) = f(a) + f(b)$$
$$f(ab) = f(a)\, f(b).$$

Example: Let $R = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} / a,b,c \in Z \right\}$. Prove or disprove that the map $: IR \to Z$ defined by $\left(\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \right) = a$ is a ring homomorphism.

Solution: $: IR \to Z$ defined by $\left(\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \right) = a$.

Let $A = \begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix}$ and $B = \begin{bmatrix} a_2 & b_2 \\ 0 & c_2 \end{bmatrix}$

$$(A+B) = \left(\begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ 0 & c_2 \end{bmatrix} \right)$$

$$= \left(\begin{bmatrix} a_1 + a_2 & b_1 + b_2 \\ 0 & c_1 + c_2 \end{bmatrix} \right)$$

$$= a_1 + a_2$$
$$= (A) + (B)$$

$$(AB) = \left(\begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix} \begin{bmatrix} a_2 & b_2 \\ 0 & c_2 \end{bmatrix} \right)$$

$$= \left(\begin{bmatrix} a_1 a_2 & a_1 b_1 + b_1 c_2 \\ 0 & c_1 c_2 \end{bmatrix} \right)$$

$$= a_1\, a_2$$
$$= (A)\ (B)$$

$\left(\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \right) = a$ is a ring homomorphism.

13.7 ISOMORPHISM

Definition: A homomorphism f:R $\to$ R_1 is called an isomorphism if, f is both one-one and onto mapping.

Propertied of homomorphism: Let f : R $\rightarrow$ R_1 be a homomorphism of a ring R into the ring R_1 and 0 $\in$ R, 0_1 $\in$ R_1 be the zero element of R and R_1 then

$f(0) = 0_1$

$f(-a) = -f(a)$ a $\in$ R

$f(a-b) = f(a) - f(b)$ a , b $\in$ R

Example :- Consider the sings . $S = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} / a,b \in IR \right\}$ and show that the map $(a+bi) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ is a ring isomorphism.

Solution :- $: C \rightarrow M_2[IR]$

$$(a+bi) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}.$$

To show that is homomorphism

A = a+bi B = c+di

(A+B) = [a+c+bi+di]

$$= \begin{bmatrix} a+c & b+d \\ -(b+d) & (a+c) \end{bmatrix}$$

$$= (a+b)+d(c+di)$$

$$(A \cdot B) = \begin{bmatrix} ac-bd & ad+bc \\ -(ad+bc) & (ac+bd) \end{bmatrix}$$

$$= \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \begin{bmatrix} c & d \\ -d & c \end{bmatrix}$$

== $(A).(B)$

To show that is 1-1

$(A) = (B)$

$(a+bi) = (c+di)$

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix} = \begin{bmatrix} c & d \\ -d & c \end{bmatrix}$$

a = c, b = d $\in$ a+bi = c+di

To show that is onto

For any $\begin{bmatrix} a & b \\ -b & a \end{bmatrix} (-M_2(IR)$

There exists at b, c $\in$ C such that

$$(a+bi) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

Hence, the map $(a+bi) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ is a ring isomorphism.

8. LET US SUM UP

In this chapter we have learned

- Algebraic structures with two binary operation.
- Definition of ring.
- Commutative ring and ring with zero divisor.
- Integral domains and fields.
- Ring homomorphism and isomorphism.

9. UNIT END EXERCISE

1.Prove that the set I of all integers with ordinary addition and multiplication as the compositions forms a ring.

2.Show that the set of number given by x +y $5\sqrt{}$where x and y are integers is a ring with ordinary addition and multiplication as the two compositions.

3. If E denotes the set of all even integers, then prove that {E, +, .} is a commutative ring, where a.b = $\frac{ab}{2}$ and + is the usual addition.

4.Show that the set of number of the form x +y $\sqrt{2}$, x and y are rational numbers is a field.

5.Show that Z[$\sqrt{5}$], the set of complex numbers x +y $\sqrt{5}$ where x, y are integers, ia an integral domain.

6. Let 'R' is ring with unity 'e'. $f : Z \to R$ is a mapping defined by $f(x) = xe \quad \forall x \in Z$. Prove that f is ring of homomorphism.

7.Let f be the function from the integer Z onto the even integers given by f(x) = 2x for all

x ∈ Z. Prove that f is not a homomorphism.

13.10 REFERENCES FOR FURTHER READING

1. University Algebra by N.S. Gopalkrishnan.
2. Contemptary Algebra by Gallian.
3. Discrete mathematics by Kenneth and Rosen.
4. Discrete mathematical structures by Kolman, Busby and Ross.
5. Modern Algebra by Vasishtha.

14

RECURRENCE RELATION

Unit Structure

14.0 OBJECTIVES

After going through this chapter you will be able to:

- Series and sequences.
- Generating function.
- Recurrence relation.
- The first order linear homogeneous recurrence relations.
- The second order homogeneous linear recurrence relations.
- The non-homogeneous relations.
- The method of generating functions.
- Applications.

14.1 INTRODUCTION:

We all know that the mathematical induction is a proof technique that verifies a formula or assertion by inductively checking its validity for increasing values of n. In a similar way, a recurrence relation is a counting technique that solves an

enumeration problem by recursively computing the answer for successively larger values of n.

The concept of a generating function is one of the most useful and basic concepts in the theory of combinatorial. The power of the generating function rests upon its ability nor only to solve the kinds of problems have we considered so far but also to aid us in new situations where additional restrictions may be involved.

14.2 SEQUENCES:

A sequence is an ordered list of objects. A sequence is denoted by $\{a_n\}$, where a_n represents n^{th} term of the sequence $(n \in \quad)$. If the list terminates after some steps then we say sequence is finite otherwise it is called as an infinite sequence.

Example:

(1) 3, 4, 5, 6, 7, 8, 9 is a finite sequence, in this $a_1 = 3$, $a_2 = 4$ and so on.

(2) 1, 4, 9, 16, 25,… is an infinite sequence, in this $a_1 = 1$, $a_2 = 4$, $a_3 = 9, ...$

(3) -1, 1, -1, 1,… is also an infinite sequence $a_1 = -1$, $a_2 = 1$, $a_3 = -1$

(4) 1, 3, 7,… is an infinite sequence.

In example (1) we can see that $a_2 = a_1 + 1$, $a_3 = a_2 + 1$ and so on i.e. $a_{n+1} = a_n + 1$, where $a_1 = 3$ and $n \leq 7$. Similarly in (4) we have, $a_{n+1} = 2a_n + 1$, where $a_1 = 1$.

A formula, like above is called as recursive formula, where next term depends on previous term. A recursive formula must have a starting value (i.e. a_1).

But in example (2), we have $a_1 = (1)^2$, $a_2 = (2)^2$, $a_1 = (3)^2$ and so on i.e. $a_n = (n)^2$ means value of $'a'_{n+1}$ does not depend on $'a'_n$ such a formula is called as Explicit formula. Similarly in (3), $a_n = (-1)^n$ value of a_n it is position number.

The set corresponding to a given sequence is the set of all distinct elements of a given sequence.

It can be finite or infinite.

For e.g. (1) for $a_n = (-1)^n$, corresponding set = {-1, 1}.

(2) for $a_n = n + 1$, corresponding set = {2, 3, 4,……}

The difference between set and sequence is, in a set order of the elements is not important but in a sequence order of the elements is important.

A set is called countable if it is elements can be arranged in order first, second, third etc. i.e. it is the set corresponding to some sequence for example, set of Natural numbers, set of rational etc.

A set which is not countable is called as an uncountable set. For example, set of Real Numbers.

Check your progress :

1. Write a formula for n^{th} term and identify it is recursive or explicit.

(a) $1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots$

(b) $1, 0, 1, 0, 1, 0, \ldots$

(c) 3, 6, 9,…

(d) 2, 5, 10, 17, 26

(e) 5, 25, 125,…

14.3 SERIES

An expression of the form $a_1 + a_2 + a_3 + \ldots\ldots + a_n + \ldots\ldots\ldots$ which is the sum of the elements of the sequence $\{a_n\}$ is called a series. If the series contains a finite number of elements, it is called finite series, otherwise called an infinite series.

If $S_n = a_1 + a_2 + a_3 + \ldots\ldots + a_n$, then S_n is called the sum of n terms of the series and is denoted by the Greek letter sigma $\sum$.

Thus $S_n = \sum_{i=1}^{n} a_n$.

Example 1: Find the sum of first 20 natural numbers.

Solution: To find sum of first 20natural numbers.

i.e $S_n = 1 + 2 + 3 + 4 + \ldots..+20$.

Here first term = a = 1 and the common difference = d =1

Bye arithmetic progression,

$S_n = \frac{n}{2}[2a + (n-1)d]$

$= \frac{20}{2}[2(1) + (20-1)1]$

$= 10[2 + 19] = 210.$

Thank You