SEMESTER III.
MODULE 4
CO-3
ALGEBRAIC STRUCTURE

MODULE 4 (CO-3)
UNIT :4.1
INTRODUCTION TO ALGEBRAIC STRUCTURE

INTRODUCTION:

In this chapter, we will study, binary operation as a function, and algebraic structures- monoid, semigroups, groups and rings, integral domains, field. They are called an algebraic structure because the operations on the set define a structure on the elements of that set

Definition: BINARY OPERATION

Let A be non empty set A.

a function $f : A \times A \rightarrow A$ is called a binary operation on a set A

generally the binary operation is denoted by * on A, then $a * b \in A \; \forall a, b \in A.$

Example :

Q. Is + binary operation on N, the set of natural numbers ?

Ans : yes

Q. Is + binary operation on Z, the set of integers ?

Ans : yes

Q. Is - binary operation on N, the set of natural numbers ?

Ans : No

Q. Is - binary operation on Z, the set of integers ?

Ans : yes

Definition: Associative property

Let A be non empty set A.

* is binary operation on A

$(a * b) * c = a *(b * c) \ \forall a, b, c \in A$

Example :

Q. Is + associative in Z, the set of integers ?

Ans : yes

Q. Is - associative in Z, the set of integers ?

Ans : No

Q. Is multiplcation associative in Z, the set of integers ?

Ans : yes

Definition: Identity Property

Let A be non empty set A.

* is binary operation on A

If $e \in A$ and a * e = a $\forall a, \in A$ then e is the identity element of A with respect to *

Example :

Q. What is the identity element of R with respect to addition ?

Ans : 0

Q. What is the identity element of R with respect to multiplication ?

Ans : 1

Definition : Inverse property

If for $a \in A$ there exist $b \in A$ such that a * b = e= $b*a$ then b is called inverse of a with respect to *

Example :

Q. What is the inverse of 3 in R with respect to addition ?

Ans : -3

Q. What is the inverse of 3 in R with respect to multiplication ?

Ans : 1/3

Definition: SEMIGROUP

A non-empty set S together with a binary operation * is called as a semigroup if –
binary operation * is associative we denote the semigroup by (S, *)

Definition: Commutative Semigroup

A semigroup (S, *) is said to be Commutative if * is commutative

Example :

(z, +) is a commutative semigroup

(z, .) is a commutative semigroup

Definition: Monoid

A non-empty set M together with a binary operation *defined on it, is called as a monoid if

i) binary operation * is associative

ii) M has an identity with respect to * .

Note: A semi group that has an identity is a monoid

Example :

(z, +) is a monoid

(z, .) is a monoid

Definition: Group

A non-empty set G together with a binary operation * defined on it is called a group if

(i) binary operation * is closed,

(ii) binary operation * is associative,

(iii) G has an identity with respect to *

(iv) Every element in G has inverse in G, with respect to *

We denote the group by (G,*)

Commutative (Abelian) Group : A group (G, *) is said to be commutative if * is commutative.

Example : Determine whether A= Z-{1}, the set of integers except 1 is a semigroup, a monoid with respect to * where $a * b = a + b - ab$

Closure Property : -

Let a , $b \in$ =A= Z-{1}, the set of integers except 1

$\therefore$ a , b are integers and $a \neq 1$, $b \neq 1$

$a * b = a + b - ab$ is integer

Assume $a * b = 1 \Rightarrow a+b-ab =1 a+(1-a)b=1$

$\Rightarrow 0=1-a -(1-a)b \Rightarrow 0=(1-a)(1-b)$

$\Rightarrow$ a=1 or b=1 but $a \neq 1$, $b \neq 1$

Assumption $a * b = 1$ is wrong $\Rightarrow$ $a*b \neq 1$

$a * b = a + b - ab$ is integer and $a*b \neq 1 \Rightarrow a * b \in$ =A= Z-{1},

$\therefore a * b \in A \ \forall a, b \in A.$

so * is closure.

Example : Determine whether A= Z-{1}, the set of integers except 1 is a semigroup, a monoid with respect to * where $a * b = a + b - ab$

Associative Property:

$$a * (b * c) = a * (b + c - bc) = a + (b + c - bc) - a(b + c + bc)$$
$$= a + b + c - bc - ab - ac - abc$$

And $$(a * b) * c = (a + b - ab) * c = (a + b - ab) + c - (a + b + ab)c$$
$$= a + b + c - ab - ac - bc - abc.$$

Hence, $a * (b * c) = (a * b) * c$. $\therefore$ $*$ is associative.

Example : Determine whether A= Z-{1}, the set of integers except 1 is a semigroup, a monoid with respect to * where $a * b = a + b - ab$

Existence of identity :

Let e be the identity element

a * e = a

a + e - ae = a

e (1-a) = 0

e = 0 or a = 1

But a≠1

e = 0 is the identity element

Example :Determine whether S = {1, 2, 3, 6, 12} is a monoid ,a semigroup, with respect to * where $a * b = G.C.D.(a, b)$

*	1	2	3	6	12
1	1	1	1	1	1
2	1	2	1	2	2
3	1	1	3	3	3
6	1	2	3	6	6
12	1	2	3	6	12

Closure Property : Since all the elements of the table $\in$ S, closure property is satisfied.

Associative Property : Since

$$a * (b * c) = a * (b * c) = a * GCD\{b, c\} = GCD\ \{a, b, c\}$$

And $(a * b) * c = GCD\{a, b\} * c = GCD\{a, b, c\}$

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

$\therefore$ $*$ is associative.

$\therefore$ (S, $*$) is a semigroup.

Existence of identity: From the table we observe that 12 $\in$ S is the identity

$\therefore$ (S, $*$) is a monoid.

Example : Prove that A is a group with respect to *

Where A= R-{1}, the set of real numbers except 1

And $a * b = a + b - ab$

Closure Property : -

Let a , b ∈ =A= R-{1}, the set of real numbers except 1

∴ a , b are real numbers and a≠1 , b≠1

$a * b = a + b - ab$ is real numbers

Assume $a * b = 1$ ⇒ a+b-ab =1a+(1-a)b=1

⇒0=1-a -(1-a)b ⇒ 0=(1-a) (1-b)

⇒ a=1 or b=1 but a≠1 , b≠1

Assumption $a * b = 1$ is wrong ⇒ a*b≠1

$a * b = a + b - ab$ is real and a*b≠1 ⇒$a * b$ ∈ =A= R-{1},

∴ $a * b \in A \ \forall a, b \in A.$

so * is closure.

Example : Prove that A is a group with respect to *
Where A= R-{1}, the set of real numbers except 1
And $a * b = a + b - ab$

Associative Property:

$$a * (b * c) = a * (b + c - bc) = a + (b + c - bc) - a\,(b + c + bc)$$

$$= a + b + c - bc - ab - ac - abc$$

And $$(a * b) * c = (a + b - ab) * c = (a + b - ab) + c - (a + b + ab)\,c$$

$$= a + b + c - ab - ac - bc - abc.$$

Hence, $a * (b * c) = (a * b) * c$. $\therefore$ $*$ is associative.

Example : Prove that A is a group with respect to *
Where A= R-{1}, the set of real numbers except 1
And $a * b = a + b - ab$

Existence of identity :

Let e be the identity element

$a * e = a$

$a + e - ae = a$

$e(1-a) = 0$

$e = 0$ or $a = 1$

But $a \neq 1$

e = 0 is the identity element

Example : Prove that A is a group with respect to *
Where A= R-{1}, the set of real numbers except 1
And $a * b = a + b - ab$

Existence of Inverse :

Let b be the inverse of a

$a * b = e = b*a$

$a + b - ab = 0$

$a+b(1-a)=0$

$b=a/(1-a)$ and $a/(1-a)$ is real number as $a \neq 1$

Inverse of a with respect to * is $a/(1-a)$ in A .

A is a group with respect to *

Example :Determine whether S = {1, 2, 3, 6, 9,18} is a semigroup, a monoid , commutative monoid with respect to * where $a * b = L.C.M.(a, b)$

*	1	2	3	6	9	18
1	1	2	3	6	9	18
2	2	2	6	6	18	18
3	3	6	3	6	9	18
6	6	6	6	6	18	18
9	9	18	9	18	9	18
18	18	18	18	18	18	18

Closure Property : Since all the elements of the table $\in$ S, closure property is satisfied.

Associative Property : Since $a * (b * c) = a * LCM\{b, c\} = LCM\{a, b, c\}$

And $(a * b) * c = LCM\{a, b\} * c = LCM\{a, b, c\}$

$\therefore \quad a * (b * c) = (a * b) * c$

$\therefore \quad *$ is associative.

$\therefore$ (S, *) is a semigroup.

Example :Determine whether S = {1, 2, 3, 6, 9,18} is a semigroup, a monoid , commutative monoid with respect to * where *a* * *b* =*L.C.M.*(*a*, *b*)

Existence of identity : From the table we observe that $1 \in S$ is the identity.

$\therefore$ $(S, *)$ is a monoid.

Commutative property : Since LCM{a, b} = LCM{b, a} we have $a * b = b * a$. Hence $*$ is commutative.

Therefore A is commutative monoid.

Result

If G is a group.

(i) The identity element is unique.

(ii) Each a in G has unique inverse

Example : Prepare table for multiplication in G= Z_7 -{0}
And find inverse of 2,3,6

*	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

From the table we observe that $1 \in G$ is identity.

From the table we get $2^{-1} = 4$, $3^{-1} = 5$, $6^{-1} = 6$

Definition: Ring

$(R, \oplus, \otimes)$ is said to be ring if

(i) $(R, \oplus)$ is a commutative group

(ii) $(R, \otimes)$ is a semigroup

(iii) $a \otimes (b \oplus c) = a \otimes b \oplus a \otimes c$

Definition: Field

$(R, \oplus, \otimes)$ is said to be field if

(i) $(R, \oplus)$ is a commutative group

(ii) $(R-\{0\}, \otimes)$ is a commutative group

(iii) $a \otimes (b \oplus c) = a \otimes b \oplus a \otimes c$

Example : Prove that $(Z_5\ +,.)$ is field

$(Z_5\ +)$ & $(Z_5\ \ -\{0\})$ are commutative groups

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

x	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Definition: Commutative Ring

(R, $\oplus$, $\otimes$) is said to be commutative ring if

(i) (R, $\oplus$, $\otimes$) is a ring

(ii) $\otimes$ is commutative

Definition: Ring with unity

(R, $\oplus$, $\otimes$) is said to be ring with unity if

(i) (R, $\oplus$, $\otimes$) is a ring

(ii) Identity w.r.t. $\otimes$ exits in R

Definition: Integral Domain

(R, $\oplus$, $\otimes$) is said to be Integral Domain if

(i) (R, $\oplus$, $\otimes$) is commutative ring with unity

(ii) R has no zero divisors

Example : Prove that set $\{\bar{2}, \bar{4}, \bar{6}, \bar{8}\}$ is a commutative ring modulo 10.

+	0	2	4	6	8
0	0	2	4	6	8
2	2	4	6	8	0
4	4	6	8	0	2
6	6	8	0	2	4
8	8	0	2	4	6

×	0	2	4	6	8
0	0	0	0	0	0
2	0	4	8	2	6
4	0	8	6	4	8
6	0	2	4	6	8
8	0	6	2	8	4

Definition : Zero divisors

(R, $\oplus$, $\otimes$) is ring

if $a \otimes b = 0$ (0- identity w.r.t. $\oplus$) but $a \neq 0$ &$b \neq 0$ then a & b are said to be zero divisors

Example :

In ring (Z_6 +,.)

$2.3=0$ but $2 \neq 0$,$3 \neq 0$

$4.3=0$ but $4 \neq 0$,$3 \neq 0$

2,4& 3 are zero divisors of Z_6

Definition : Units

(R, ⊕, ⊗) is ring and 1 is identity w.r.t. ⊗

if b is inverse of a w.r.t. ⊗ then a & b are called units

Example :

In ring (Z_9 +,.)

2.5=1

2& 5 are units of Z_9

Definition: Integral Domain

(R, ⊕, ⊗) is said to be Integral Domain if

(i) (R, ⊕, ⊗) is commutative ring with unity

(ii) R has no zero divisors

Example :ring (Z_5 +,.) is Integral Domain

Note :

Ring (Z_p +,.) is Integral Domain and field if p is prime

In Z_n , a is unit if G.C.D (a,n)=1

In Z_n , a is zero divisor if G.C.D (a,n) $\neq$ 1