Algebric Structures

Unit 2

Algebraic Structure

A non-empty set **G** equipped with one or more binary operations is said to be an **algebraic structure**. Suppose ***** is a binary operation on **G**. Then **(G, *)** is an **algebraic structure**. **(N,*), (1, +), (1, -)** are all the **algebraic structure**. Here, **(R, +, .)** is an **algebraic structure** equipped with two operations.

Binary operation on a set

- N = {1,2,3,4,.....∞ } = Set of all natural numbers.
- Z = { 0, ± 1, ± 2, ±3, ±4 , ... ±} = Set of all integers.
- Q = Set of all rational numbers.
- R = Set of all real numbers
- **Binary Operation:** Suppose **G** is a non-empty set. The **G X G = {(a,b) : a E G, b E G)}**. If **f : G X G → G** then **f** is called a binary operation on a set **G**. The image of the ordered pair **(a,b)** under the function **f** is denoted by **afb**.
- A binary operation on asset **G** is sometimes also said to be the binary composition in the set **G**. If ***** is a binary composition in **G** then, **a * b E G, a, b E G**. Therefore **g** is closed with respect to the composition denoted by *****.

Binary operation on a set

Example:

- An addition is a binary operation on the set **N** of natural number. The sum of two natural number is also a natural number. Therefore, **N** is a natural number with respect to addition i.e. **a+b**.
- Subtraction is not a binary operation on **N**. We have **4 – 7 = -3** not belong to **N** whereas **4 belongs to N**. thus, **N** is not closed with respect to subtraction, but subtraction is a binary operation on the set of an integer.

Properties of an algebraic structure

- **Commutative:** Let * be a binary operation on a set A.

  The operation * is said to be commutative in A if

  a * b= b * a for all a, b in A
- **Associativity:** Let * be a binary operation on a set A.

  The operation * is said to be associative in A if

  (a * b) * c = a *(b * c) for all a, b, c in A
- **Identity:** For an algebraic system (A, *), an element 'e' in A is said to be an identity element of A if

  a * e = e * a = a for all $a \in A$.
- **Note:** For an algebraic system (A, *), the identity element, if exists, is unique.
- **Inverse:** Let (A, *) be an algebraic system with identity 'e'. Let a be an element in A. An element b is said to be inverse of A if

  a * b = b * a = e

Cancellation laws

An operation ***** on a set **S** is a said to satisfy the left cancellation law if, **a * b = a * c implies b = c** and is said to satisfy the right cancellation law if, **b * a = c * a implies b = c**

Semi Group

- **Semi Group:** An algebraic system (A, *) is said to be a semi group if
  1. * is closed operation on A.
  2. * is an associative operation, for all a, b, c in A.
- Ex. (N, +) is a semi group.
- Ex. (N, .) is a semi group.
- Ex. (N, −) is not a semi group.

addition is an associative operation on **N**. similarly, the algebraic structure **(N, .)(I, +)** and **(R, +)** are also semigroup

Monoid

- A group which shows property of an identity element with respect to the operation ***** is called a monoid. In other words, we can say that an algebraic system **(M,*)** is called a monoid if **x, y, z E M**.
- **(x *y) * z = x * (y * z)**
- And there exists an elements **e E M** such that for any **x E M**
- **e * x = x * e = x** where **e** is called identity element.

i. **Closure property**

- The operation **+** is closed since the sum of two natural number is a natural number.

ii. **Associative property**

- The operation **+** is an associative property since we have **(a+b) + c = a + (b+c) a, b, c E I**.

iii. **Identity**

- There exist an identity element in a set **I** with respect to the operation **+**. The element 0 is an identity element with respect to the operation since the operation **+** is a closed, associative and there exists an identity. Since the operation **+** is a closed associative and there exists an identity. Hence the algebraic system **(I, +)** is a **monoid**.

Example

- Ex. Show that the set 'N' is a monoid with respect to multiplication.
- Solution: Here, $N = \{1,2,3,4,......\}$

1. Closure property : We know that product of two natural numbers is again a natural number.

i.e., $a.b = b.a$ for all $a,b \in N$

$\therefore$ Multiplication is a closed operation.

2. Associativity : Multiplication of natural numbers is associative.

i.e., $(a.b).c = a.(b.c)$ for all $a,b,c \in N$

3. Identity : We have, $1 \in N$ such that

$a.1 = 1.a = a$ for all $a \in N$.

$\therefore$ Identity element exists, and 1 is the identity element.

Hence, N is a monoid with respect to multiplication.

Subsemigroup & submonoid

Subsemigroup : Let (S, *) be a semigroup and let T be a subset of S. If T is closed under operation * , then (T, *) is called a subsemigroup of (S, *).

Ex: (N, .) is semigroup and T is set of multiples of positive integer m then (T,.) is a sub semigroup.

Submonoid : Let (S, *) be a monoid with identity e, and let T be a non- empty subset of S. If T is closed under the operation * and $e \in T$, then (T, *) is called a submonoid of (S, *).

Group

- An algebraic system (G, *) is said to be a group if the following conditions are satisfied.

1. **Closure property:** * is a closed operation.

For all a, b ∈ G => a, b ∈ G

2. Associativity: * is an associative operation.

(a,b).c = a.(b.c) a, b, c ∈ G.

3. Existence of identity :

There exits an unique element in G. Such that e.a = a = a.e for every a ∈ G.

4. Existence of inverse: For each a ∈ G , there exists an element a^{-1} ∈ G such that a. a^{-1} = e = a^{-1}.a the element a^{-1} is called the inverse of a .

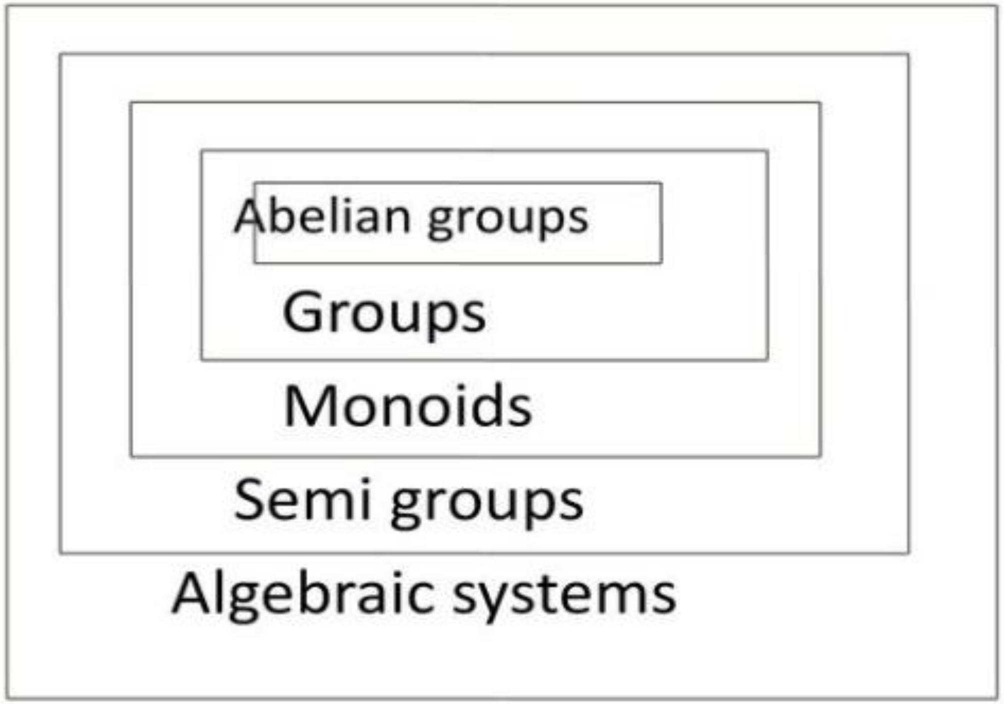
Abelian Group or Cummutative Group

A group **G** is said to be abelian or commutative if in addition to the above four postulates the following postulate is also satisfied.

5. Commutativity

$a.b = b.a$ for every $a, b \in G$.

Algebraic systems



Properties

- In a Group (G, *) the following properties hold good

1. Identity element is unique.
2. Inverse of an element is unique.
3. Cancellation laws hold good

$$a * b = a * c \Rightarrow b = c \quad \text{(left cancellation law)}$$

$$a * c = b * c \Rightarrow a = b \quad \text{(Right cancellation law)}$$

4. $(a * b)^{-1} = b^{-1} * a^{-1}$

- In a group, the identity element is its own inverse.

- ***Order of a group*** : The number of elements in a group is called order of the group.

- Finite group: If the order of a group G is finite, then G is called a finite group.

Example 1.

Ex. Show that, the set of all integers is a group with respect to addition.

- Solution: Let Z = set of all integers.

  Let a, b, c are any three elements of Z.

1. <u>Closure property</u> : We know that, Sum of two integers is again an integer.

   i.e., $a + b \in Z$ for all $a, b \in Z$

2. <u>Associativity</u>: We know that addition of integers is associative.

   i.e., $(a+b)+c = a+(b+c)$ for all $a,b,c \in Z$.

3. <u>Identity</u> : We have $0 \in Z$ and $a + 0 = a$ for all $a \in Z$.

   $\therefore$ Identity element exists, and '0' is the identity element.

4. <u>Inverse</u>: To each $a \in Z$, we have $-a \in Z$ such that

   $a + (-a) = 0$

   Each element in Z has an inverse.

- 5. Commutativity: We know that addition of integers is commutative.

  i.e., $a + b = b + a$ for all $a, b \in Z$.

  Hence, $(Z, +)$ is an abelian group.

Example 2

Ex. Show that set of all non zero real numbers is a group with respect to multiplication .

- Solution: Let R^* = set of all non zero real numbers.

  Let a, b, c are any three elements of R^* .

1. Closure property : We know that, product of two nonzero real numbers is again a nonzero real number .

   i.e., $a \cdot b \in R^*$ for all $a,b \in R^*$.

2. Associativity: We know that multiplication of real numbers is associative.

   i.e., $(a.b).c = a.(b.c)$ for all $a,b,c \in R^*$.

3. Identity : We have $1 \in R^*$ and $a .1 = a$ for all $a \in R^*$.

   $\therefore$ Identity element exists, and '1' is the identity element.

4. Inverse: To each $a \in R^*$, we have $1/a \in R^*$ such that

   $a .(1/a) = 1$ i.e., Each element in R^* has an inverse.

- 5.<u>Commutativity</u>: We know that multiplication of real numbers is commutative.

  i.e., $a . b = b . a$ for all $a,b \in R^*$.

  Hence, $(R^* , .)$ is an abelian group.

- <u>Ex:</u> Show that set of all real numbers 'R' is not a group with respect to multiplication.
- Solution: We have $0 \in R$.

  The multiplicative inverse of 0 does not exist.

  Hence. R is not a group.

Example 3

- Ex. Show that the set of all strings 'S' is a monoid under the operation 'concatenation of strings'.

  Is S a group w.r.t the above operation? Justify your answer.
- Solution: Let us denote the operation

  'concatenation of strings' by + .

Let s_1, s_2, s_3 are three arbitrary strings in S.

Closure property: Concatenation of two strings is again a string.

i.e., $s_1+s_2 \in S$

Associativity: Concatenation of strings is associative.

$$(s_1+s_2)+s_3 = s_1+(s_2+s_3)$$

- Identity: We have null string , $\lambda \in S$ such that $s_1 + \lambda = S$.
- $\therefore$ S is a monoid.
- Note: S is not a group, because the inverse of a non empty string does not exist under concatenation of strings.

Example 4

- Ex. Let (Z, *) be an algebraic structure, where Z is the set of integers and the operation * is defined by $n * m$ = maximum of (n, m).

  Show that (Z, *) is a semi group.

  Is (Z, *) a monoid ?. Justify your answer.
- Solution: Let a , b and c are any three integers.

<u>Closure property</u>: Now, $a * b$ = maximum of $(a, b) \in Z$ for all $a,b \in Z$

<u>Associativity</u> : $(a * b) * c$ = maximum of $\{a,b,c\} = a * (b * c)$

$\therefore$ (Z, *) is a semi group.

<u>Identity</u> : There is no integer x such that

$a * x$ = maximum of (a, x) = a for all $a \in Z$

$\therefore$ Identity element does not exist. Hence, (Z, *) is not a monoid.

Example 5

- Ex. Let S be a finite set, and let F(S) be the collection of all functions $f: S \rightarrow S$ under the operation of composition of functions, then show that F(S) is a monoid.

  Is S a group w.r.t the above operation? Justify your answer.

- Solution:

  Let f_1, f_2, f_3 are three arbitrary functions on S.

Closure property: Composition of two functions on S is again a function on S.

$$\text{i.e., } f_1 o\, f_2 \in F(S)$$

Associativity: Composition of functions is associative.

$$\text{i.e., } (f_1 o\, f_2) o\, f_3 = f_1 o\, (f_2 o\, f_3)$$

- Identity: We have identity function $I : S \to S$

  such that $f_1 \circ I = f_1$.

  $\therefore$ F(S) is a monoid.

- Note: F(S) is not a group, because the inverse of a non bijective function on S does not exist.

Example 6

- Ex. In a group (G, *) , Prove that
  $(a * b)^{-1} = b^{-1} * a^{-1}$ for all $a,b \in G$.
- <u>Proof :</u>
- Consider,
- $(a * b) * (b^{-1} * a^{-1})$
- $= (a * (b * b^{-1}) * a^{-1})$ (By associative property).
- $= (a * e * a^{-1})$ (By inverse property)
- $= (a * a^{-1})$ (Since, e is identity)
- $= e$ (By inverse property)
- Similarly, we can show that
- $(b^{-1} * a^{-1}) * (a * b) = e$
- Hence, $(a * b)^{-1} = b^{-1} * a^{-1}$.

Ex. If $(G, *)$ is a group and $a \in G$ such that $a * a = a$, then show that $a = e$, where e is identity element in G.

- <u>Proof</u>: Given that, $a * a = a$
- $\Rightarrow a * a = a * e$ (Since, e is identity in G)
- $\Rightarrow a = e$ (By left cancellation law)
- Hence, the result follows.

Cyclic Group

- Cyclic Group is a group which can be generated by one of its elements. That is, for some a in G,

G={a^n | n is an element of Z} Or, in addition notation,

G={na |n is an element of Z}

The single element a is called a generator of **G** and as the cyclic group is generated by a single element, so the cyclic group is also called **monogenic**.

1. The set of integers Z under ordinary addition is cyclic. Both 1 and −1 are generators.

(Recall that, when the operation is addition, 1n is interpreted as

$$\underbrace{1 + 1 + \cdots + 1}_{n \text{ terms when } n \text{ is positive}}$$

and as

$$\underbrace{(-1) + (-1) + \cdots + (-1)}_{|n| \text{ terms when } n \text{ is negative.)}}$$

The set $Z_n = \{0, 1, \ldots, n-1\}$ for $n \geq 1$ is a cyclic group under addition modulo n. Again, 1 and $-1 = n-1$ are generators.

Unlike Z, which has only two generators, Z_n may have many generators (depending on which n we are given).

Subgroup

Definition : A non empty sub set H of a group (G, *) is a sub group of G, if (H, *) is a group.

Note: For any group {G, *}, {e, * } and (G, *) are **trivial sub groups:** Group which contains a single element.

Example. G = {1, -1, i, -i } is a group w.r.t multiplication.

H1 = { 1, -1 } is a subgroup of G .

H2 = { 1 } is a trivial subgroup of G.

Ex. (Z , +) and (Q , +) are sub groups of the group (R +).

- Theorem: A non empty sub set H of a group (G, *) is a sub group of G iff

i) a * b $\in$ H $\forall$ a, b $\in$ H

ii) a^{-1} $\in$ H $\forall$ a $\in$ H

Theorem-Subgroup

- Theorem: A necessary and sufficient condition for a non empty subset H of a group (G, *) to be a sub group is that

  $a \in H,\ b \in H \Rightarrow a * b^{-1} \in H.$
- Proof: Case1: Let (G, *) be a group and H is a subgroup of G

  Let $a,b \in H \Rightarrow b^{-1} \in H$ (since H is is a group)

  $\Rightarrow a * b^{-1} \in H.$ (By closure property in H)
- Case2: Let H be a non empty set of a group (G, *).

  Let $a * b^{-1} \in H \quad \forall a, b \in H$
- Now, $a * a^{-1} \in H$ (Taking $b = a$)

  $\Rightarrow e \in H$ i.e., identity exists in H.
- Now, $e \in H,\ a \in H \Rightarrow e * a^{-1} \in H$

  $\Rightarrow a^{-1} \in H$

- $\therefore$ Each element of H has inverse in H.

  Further, $a \in H,\ b \in H \Rightarrow a \in H,\ b^{-1} \in H$

  $\Rightarrow a * (b^{-1})^{-1} \in H.$

  $\Rightarrow a * b \in H.$

  $\therefore$ H is closed w.r.t $*$.
- Finally, Let $a,b,c \in H$

  $\Rightarrow a,b,c \in G$ (since $H \subseteq G$)

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

  $\therefore$ $*$ is associative in H
- Hence, H is a subgroup of G.