Algebraic Systems

Need to study Algebraic systems:

- Algebraic Model : Real Worlds Situation, Mathematical model, connecting mathematical model with real world situation to get real world solution.

Algebraic Systems or Algebras

- **Structure / Definition:** An algebra is characterised by specifying 3 components
  - a **set** called **Carrier** of the Algebra
  - **Operations** defined on the carrier
  - **Distinguished** elements of the carrier, called **constants** of the algebra
- **Example:** let carrier be Set of integers Z and define operation + (addition) on Z
  - it means if a and b are integers, then you can perform a + b
  - this operation is from I^2 -> I, it's a binary operation

Contd…

- In general, let carrier be S
  - then an operation from S^m -> S
  - here m is called as **arity of the operation**
  - Example:
    - Binary operations:
      - Multiplication *
      - Subtraction -
    - Unary Operation
      - Negation –
      - absolute value or Mod

Contd…

- **Constants of algebra**: elements of the carrier having some special property
  - **Example**: (I, +, 0)
    - 0 is identity element for addition
  - **Example**: (R, *, 0, 1)
    - 1 is identity element for Multiplication
    - 0 is Zero element for multiplication

- **Fundamental Algebraic Structures**: groupoids, semi-groups, monoids, groups, lattices, rings and fields.

Algebras of same signature or from same species

- Algebras are said to have same signature if they have
    1. A Carrier
    2. Same number of operations with corresponding arity
    3. same number of constants
- **Example 1**:
    - <I, +, *, -, 1, 0>
    - <R, +, *, -, 1, 0>
    - <P(S), ∪, ∩, ′, S, Ø >
- The above algebras have same signatures, or they are from same species
- **Example 2:**
    - <I, -, 0> and <Q, +, 0>
  - Here the above algebras do have same signature, but they do not have same properties

Axioms

- **Axioms** are rules that algebras follow.
  - **Example**: Semi groups will follow a set of axioms, groups will follow a set of operations

Closure Property

- **Definition**: let $\circ$ and Δ be a binary and unary operation on a set T and let T' be a subset of T. T' is closed with respect to $\circ$ if a, b $\in$ T implies $a \circ b \in T'$. The subset T' is closed with respect to Δ if a $\in$ T implies $\Delta a \in T'$.
- **Example:** <I, +, 0>
    - Let S = (x | 0<= x<= 10)
    - here, 12 + 15 = 27 which does not belong to S

      so, S is not closed wrt +
    - Consider operation max(a, b)
        - here S is closed under max operation

Contd…

- **Example 2:** Let If A = {0, 1},
  - We have
    - $0 \times 0 = 0$,
    - $0 \times 1 = 0$,
    - $1 \times 0 = 0$, and
    - $1 \times 1 = 1$
  - so A is closed under multiplication.
  - But A is not closed under the binary operation addition. Since $1 + 1 = 2$ does not belong to A.

Groupoid

- **Definition:** A groupoid is an algebraic structure consisting of non-empty set A and a binary operation *, such that A is closed under *.

- **Example:** The set of real numbers is closed under addition, therefore (R, +) is a groupoid.
- **Example 2:** If E denotes the set of even numbers then E is closed under addition. and (E, +) is a groupoid.
- **Example 3:** Let Z^+ denotes the set of positive integers and * be a binary operation on Z^+ defined as

$$a * b = 3a + 4b \ \forall a, b \in Z^+$$

Clearly (Z^+, *) is a groupoid

Semi-Group

- **Definition:** Let S be a non-empty set and * be a binary operation on S. The algebra (S,*) is called a semi-group if the operation * is associative.
    - In other words, the groupoid is a semi-group

    if $(a * b) * c = a * (b * c)$ for all $a, b, c \in S$

- Thus, a semi-group requires the following:

    (i) A set S.

    (ii) A binary operation * defined on the elements of S.

    (iii) Closure, $a * b$ whenever $a, b \in S$

    (iv) Associativity $(a * b) * c = a * (b * c)$ for all $a, b, c \in S$

- **Example 1:** Let N be the set of natural numbers. Then (N, +) and (N, *) are semi-groups.

Contd…

- **Example 2**: X be a non-empty set and P (X) denote the power set of X. Then (P(x), $\cup$) and (P (x), $\cap$) are semi-groups.
- **Example 3**: Let Z be the set of integers and Z_m be the set equivalence classes generated by the equivalence relation "congruent modulo M" for any positive integers m. Then $+_m$ be defined integers of + on Z as follows:

  For any [i], [j] $\in Z_m$

  $[i] +_m [j] = [(i + j) \bmod m]$

  The algebraic system (Z_m, + m) is a semi-group

Homomorphism of Semi-Groups

- **Definition**: Let (S, *) and (T, o) be any two semi-groups. A mapping $f: S \rightarrow T$ such that for any two elements $a, b \in S$

  $$f(a * b) = f(a) \circ f(b)$$

is called a semi-group homomorphism.

- **Definition**: A homomorphism of a semi-group into itself is called a semi-group **endomorphism**.

Isomorphism of Semi-Group

- **Definition:** Let (S, *) and (T, 0) be any two semi-groups. A homomorphism f: S $\rightarrow$ T is called a semi-group isomorphism if f is one-to-one and onto.
- If f: S $\rightarrow$ T is an isomorphism then (S, *) and (T, 0) are said to be isomorphic.

- **Definition**: An isomorphism of a semi-group onto itself is called a semi-group automorphism.

Monoid

- **Definition**: A semi-group (M, *) with an identity element with respect to the binary operation * is called a monoid.
- In other words, an algebraic system (M, *) is called a monoid if:

  (i) $(a * b) * c = a * (b * c) \quad \forall\ a, b, c \in M$

  (ii) There exists an element $e \in M$ such that

  $e * a = a * e = a\ \forall\ a \in M$. (i.e. Identity Element)

- **Example 1**: Let Z be the set of integers (Z, +) is a monoid 0 is the identity element in Z with respect to +.

Contd…

- **Commutative Monoid**: Let (M, *) be a monoid. If the operation * is commutative then (M, *) is said to be commutative monoid.
- If $a^i \, a^j \in M$ we have $a^{i+j} = a^i * a^j = a^j * a^i$ for all i, j $\in$ M.

- **Cyclic Monoid:** A monoid (M, *) is said to be cyclic if there exists an element a $\in$ M. Such that every element of M can be expressed as some power of a.
    - If M is a cyclic monoid such that every element is some power of a $\in$ M, then a is called the generator of M.
    - A cyclic monoid is commutative and may have more than one generator.

Monoid Homomorphism

- **Definition**: Let (M, *) and (T, 0) be any two monoids e_m and e_t denote the identity elements of (M, *) and (T, 0) respectively. A mapping

  $$f: M \to T$$

  such that for any two elements a , b $\in$ M

  $$f\,(a * b) = f\,(a) \circ f\,(b)$$

  and $\quad f\,(e_m) = e_t$

  is called a monoid homomorphism.

- Monoid homomorphism presents the associativity and identity.
- It also preserves commutative.
- If a $\in$ M is invertible and $a^{-1} \in M$ is the inverse of a in M, then f (a^{-1}) is the inverse of f (a), i.e., f $(a^{-1}) = [f\,(a)]^{-1}$.

Groups

- **Definition:** A group is an algebraic structure (G, *) in which the binary operation * on G satisfies the following conditions:

  G – 1 for all a, b, c, $\in$ G

  a * (b * c) = (a * b) * c (**associativity**)

  G – 2 there exists an elements e G $\in$ such that for any a G $\in$

  a * e= e * a = a (existence of **identity**)

  G –3 for every a $\in$ G, there exists an element denoted by a^{-1} in G such that

  $a * a^{-1} = a^{-1} * a = e$

  a^{-1} is called the **inverse** of a in G

Contd…

- **Example 1:** (Z, +) is a group
  - where Z denote the set of integers.

- **Example 2:** (R, +) is a group
  - where R denote the set of real numbers.

Abelian Group

- **Definition**: Let (G, *) be a group. If * is commutative that is

  $$a * b = b * a \text{ for all } a, b \in G$$

  then (G, *) is called an Abelian group.

- **Example**: (Z, +) is an Abelian group

Finite and Infinite Group

- **Finite Group**
  - **Definition**: A group G is said to be a finite group if the set G is a finite set.
  - **Example**: G = {–1, 1} is a group with respect to the operation multiplication. Where G is a finite set having 2 elements. Therefore, G is a finite group.

- **Infinite Group**
  - A group G, which is not finite is called an infinite group.

Order of a Finite Group

- **Definition:** The order of a finite group (G, *) is the number of distinct elements in G.
- The order of G is denoted by O(G) or by |G|.

- **Example**: Let G = {–1, 1}

The set G is a group with respect to the binary operation multiplication and O(G) = 2.

Example 1

- Show that the set G = {1, –1, i, –i} where i = $\sqrt{-1}$ is an abelian group with respect to multiplication as a binary operation.
- **Solution**: Let us construct the composition table

$\bullet$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
$-i$	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

- From the table we can say (G, ·) is closed under the · operation

Contd…

- We have to check whether the above algebraic structure (G, $\cdot$) satisfies the following axioms
- Associativity

$$1 \cdot (-1 \cdot i) = 1 \cdot -i = -i$$

$$(1 \cdot -1) \cdot i = -1 \cdot i = -i$$

$$\Rightarrow 1 \cdot (-1 \cdot i) = (1 \cdot -1)\, i$$

- Existence of Identity
  - 1 is identity element of (G, $\cdot$) such that $1 \cdot a = a = a \cdot 1 \ \forall\ a \in G$

Contd…

- Existence of inverse

$$1 \cdot 1 = 1 = 1 \cdot 1 \;\Rightarrow\; 1 \text{ is inverse of } 1$$

$$(-1) \cdot (-1) = 1 = (-1) \cdot (-1) \;\Rightarrow\; -1 \text{ is the inverse of } (-1)$$

$$i \cdot (-i) = 1 = -i \cdot i \;\Rightarrow\; -i \text{ is the inverse of } i \text{ in } G.$$

$$-i \cdot i = 1 = i \cdot (-i) \;\Rightarrow\; i \text{ is the inverse of } -i \text{ in } G.$$

- Thus all the axioms of a group are satisfied.

Contd…

- Commutativity

$$a \cdot b = b \cdot a \;\; \forall \;\; a, b \in G \text{ hold in } G$$

$$1 \cdot 1 = 1 = 1 \cdot 1, -1 \cdot 1 = -1 = 1 \cdot -1$$

$$i \cdot 1 = i = 1 \cdot i; i \cdot -i = -i \cdot i = 1 \;= 1 \text{ etc.}$$

commutative law is satisfied

- Hence (G, ·) is an abelian group

Example 2

- Prove that $G = \{1, \omega, \omega^2\}$ is a group with respect to multiplication where $1, \omega, \omega^2$ are cube roots of unity.
- **Solution**: We construct the composition table as follows:

$\cdot$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	$\omega^3 = 1$
ω^2	ω^2	$\omega^3 = 1$	$\omega^4 = \omega$

- The algebraic system is $(G, \cdot)$ where $\omega^3 = 1$ and multiplication $\cdot$ is the binary operation on G.
- The algebraic system $(G, \cdot)$ is closed under multiplication "$\cdot$".

Contd…

- Let us check axioms of groups
  - Associativity
    - from the table we can say $\cdot$ is associative
  - Existence of Identity
    - 1 is identity element of (G, $\cdot$) such that

      $1 \cdot a = a = a \cdot 1 \;\forall\; a \in G$
  - Existence of inverse
    - Each element of G is invertible
    - $1 \cdot 1 = 1 \Rightarrow 1$ is its own inverse.
    - $\omega \cdot \omega^2 = \omega^3 = 1 \Rightarrow \omega^2$ is the inverse of ω and ω is the inverse of ω^2 in G
- Thus all the axioms of a group are satisfied.
- Commutativity
  - commutative law hold wrt multiplication
- Hence (G, $\cdot$) is an abelian group

Example 3

- **Example 3**: Prove that the set Z of all integers with binary operation * defined by a * b = a + b + 1 ∀ ∈ a b G , is an abelian group.
- ***Solution:*** Sum of two integers is again an integer; therefore $a+b \in Z \ \forall \ a, b \in Z$

$$\Rightarrow \ a+b+1 \cdot \in Z \ \forall \ a, b \in Z$$

$\Rightarrow$ Z is called with respect to *

Associative law for all $a, b, \ a, b \in G$ we have $(a * b) * c = a * (b * c)$ as

$$\begin{aligned}(a * b) * c &= (a + b + 1) * c \\ &= a + b + 1 + c + 1 \\ &= a + b + c + 2\end{aligned}$$

also

$$\begin{aligned}a * (b * c) &= a * (b + c + 1) \\ &= a + b + c + 1 + 1 \\ &= a + b + c + 2\end{aligned}$$

Hence $(a * b) * c = a * (b * c) \in a, b \in Z$.

Sub-Group

- **Definition:** Let (G, *) be a group and H, be a non-empty subset of G. If (H, *) is itself is a group, then (H, *) is called sub-group of (G, *).

- **Example 1:** Let a = {1, –1, i, –i} and H = {1, –1} G and H are groups with respect to the binary operation, multiplication.
    - H is a subset of G, therefore (H, X) is a sub-group (G, X).

- **Example 2:** Consider (Z_6, $+_6$), the group of integers modulo 6.

  H = {0, 2, 4} is a subset of Z_6 and

  {H, $+_6$} is a group.

  ∴ {H, $+_6$} is a sub-group.

Ring

- **Definition:** An algebraic system $(R, +, \cdot)$ is called a ring if the binary operations '+' and '$\cdot$' R satisfy the following properties:

  1. $(R, +)$ is an abelian group.
  2. $(R, \cdot)$ is a semi-group.
  3. The operation '$\cdot$' is distributive over +,

     that is for any $a, b, c \in R$,

     $a \cdot (b + c) = a \cdot b + a \cdot c$ and

     $(b + c) \cdot a = b \cdot a + c \cdot a$

Example

- **Example 1**: The set of integers Z, with respect to the operations + and × is a ring.

- **Example 2**: The set of all matrices of the form

$$\begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix}$$

where, a and b being real numbers,

with matrix addition and matrix multiplication is a ring.

Resource

- Discrete mathematics structures – G. Shanakr Rao - 2 Ed