Sri SAI RAM ENGINEERING COLLEGE
INSTITUTE OF TECHNOLOGY
West Tambaram, Chennai - 44

Sairam INSTITUTIONS

SAIRAM DIGITAL RESOURCES

# UNIT IV
## ALGEBRAIC STRUCTURES

### 4.1 SEMIGROUPS AND MONOIDS

YEAR II | SEM III

MA8351

DISCRETE MATHEMATICS
( COMMON TO CSE & IT )

SCIENCE & HUMANITIES

## ALGEBRAIC STRUCTURE:

A non- empty set G together with one or more n-ary operations say " $*$ " (binary) is called an algebraic structure. We denote it by $[G,*]$.

**Note:** $+, -, \cdot, \times, *, \cup, \cap$, etc. are some of binary operations.

**Properties of Binary operations:**

1. Closure Property:
   $a * b \in G$, for all $a, b \in G$.

2. Commutativity:
   $a * b = b * a$, for all $a, b \in G$.

3. Associativity:
   $(a * b) * c = a * (b * c)$, for all $a, b, c \in G$.

4. Identity element:

   $a * e = e * a = a$, for all $a \in G$

   'e' is called the identity element.

5. Inverse element:

   If $a * b = b * a = e(identity)$, then 'b' is called the inverse of 'a' and it is denoted by $b = a^{-1}$.

6. Distributive Properties:

   $a * (b \cdot c) = (a * b).(a * c)$ [ Left distributive law]

   $(b \cdot c) * a = (b * a) \cdot (c * a)$ [ Right distributive law]

7. Cancellation Properties:

   $a * b = a * c \Longrightarrow b = c$ [left cancellation law]

   $b * a = c * a \Longrightarrow b = c$ [Right cancellation law]

**Examples:** $(Z, +), (Z, -), (Z, \times), (R, +)$ and $(R, \times)$ is an algebraic system.

## Semigroup:

If a non-empty set S together with the binary operation '*' satisfying the following two properties:

(i) Closure Property:

$a * b \in S$; for all $a, b \in S$

(i) Associative Property:

$(a * b) * c = a * (b * c)$ ; $a, b, c \in S$

Then $(S,*)$ is called a semigroup.

**Examples:** (i) Let $N = \{1,2,3, \dots \dots\}$ be the set of natural numbers, then $(N, +)$ and $(N,\times)$ are semigroups, since both $+$ and $\times$ satisfies closure and associative property.

(ii) $(Z, +)$ and $(Z,\times)$ is a semigroup since it satisfies both the properties of semigroup.

(ii) Let $E = \{2,4,6,8, \dots \dots\}$ be the set of all even numbers, then $(E, +)$ and $(E,\times)$ is a semigroup since it satisfies both the properties of semigroup.

## Monoid:

A semigroup $(S,*)$ with an identity element with respect to $' * '$ is called Monoid.

A non-empty set 'M' with respect to $*$ is said to be a monoid, if $*$ satisfies the following properties:

For $a, b, c \in M$

(i) Closure Property:

$$a * b \in S; \text{ for all } a, b \in S$$

(i) Associative Property:

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

(i) Identity Property:

$$\forall a \in M, \ \exists \quad e \in M \text{ such that } \quad a * e = e * a = a \ ;$$

**Examples:** (i) Let $N = \{1,2,3, \ldots\ldots\}$ , then $(N,\times)$ is a monoid since it satisfies closure, associative property and 1 is the identity element.

(ii) $(Z, +)$ and $(Z,\times)$ is a monoid since it satisfies both Closure and Associative property and '0' and '1' is the identity element under addition and multiplication.

**Note:** (i) $(N,+)$ is not a monoid since the identity element '0' does not belongs to N.

(ii) Let $E = \{2,4,6,8, \ldots\ldots\}$ be the set of all even numbers, then $(E,+)$ and $(E,\times)$ is not a monoid since the identity element '0' and '1' under addition and multiplication does not belongs to E.

**Problem 1:** Show that the set $N = [0,1,2, \ldots\ldots\}$ is a semigroup under the operations $x * y = \max\{x,y\}$. Is it monoid?

**Proof:** **(1) Closure Property:**

$$x * y = \max\{x,y\} = \begin{Bmatrix} x;\ if\ x > y \\ y; if\ x < y \end{Bmatrix}$$

$$\Longrightarrow \forall x, y \in N \Longrightarrow x * y \in N$$

Since $\max\{x,y\}$ is in N whenever $x, y \in N$

$\therefore$ $' * '$ is closed.

**(2) Associative Property:**

$$x * (y * z) = \max\{x, (y * z)\} = \max\{x, y, z\} \quad .....(A)$$

$$(x * y) * z = \max\{(x * y), z\} = \max\{x, y, z\} \quad ......(B)$$

From (A) and (B), we get

$$(x * y) * z = x * (y * z)$$

$\therefore$ $'*'$ satisfies Associative property.

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

**(3) Identity element:**

Since $0 \in N$, satisfies

$$x * 0 = \max\{x, 0\} = x = \max\{0, x\} = 0 * x$$

The identity element is ‘0’.

$\therefore$ $N$ is a monoid.

**Problem 2:** Let $X^X$ be the set of all functions $f: X \to X$. For $f, g, h \epsilon X^X$, define the composition of f and g by $(f \circ g)(x) = f(g(x))$. Show that $(X^X, \circ)$ is a semigroup. Is it a monoid?

**Proof: (1) Associative property:**

Let $f, g, h \epsilon X^X$. Then we have

$$((f \circ g) \circ h)(x) = (f \circ g)\big(h(x)\big) = f(g\big(h(x)\big) = f\big((g \circ h)x\big) = (f \circ (g \circ h)(x)$$

$$\therefore \ (f \circ g) \circ h = f \circ (g \circ h)$$

$\therefore \ (X^X, 0)$ is a semigroup.

**(2) Identity element:**

The identity map $i \in X^X$ defined by $i(x) = x$ for all $x \in X$ satisfies

$$(f \circ i)(x) = f\big(i(x)\big) = f(x) = i\big(f(x)\big) = (i \circ f)(x)$$

$$\therefore \ f \circ i = i \circ f$$

$\therefore$ " $i$ " is the identity element. Hence, $(X^X, \circ)$ is a monoid.

## Homomorphism of semigroups:

Let $(S,*)$ and $(T, \cdot)$ be two semi groups. A mapping $f: S \to T$ is called homomorphism if

$$f(a * b) = f(a) \cdot f(b); \ \forall \ a, b \in S$$

Example: Consider the semigroups $(N, +)$ and $(Z_m, +_m)$. Define $f: N \to Z_m$ by $f(a) = [a]$ then, $f(a+b) = [a+b] = [a] +_m [b] = f(a) +_m f(b)$

$\therefore$ $f$ is a semigroup homomorphism.

## Monoid homomorphism:

Let $(M,*)$ be a monoid with identity $e$ and $(T, \cdot)$ be a monoid with identity $e'$. A mapping $f: M \to T$ is called a homomorphism of monoids if $f(a * b) = f(a) \cdot f(b)$; $\forall \ a, b \in M$ and $f(e) = e'$.

**Problem 1:** Let $(S,*)$ be a semigroup and $S^S$ be the set of all functions from S to S. Then $(S^S, \cdot)$ is a semigroup under composition of functions. Prove that there is a homomorphism $g: S \to S^S$.

**Proof:** For each $a \in S$, we shall define a function,

$$f_a: S \to S \text{ by } f_a(x) = a * x \; ; \; \forall\, x \in S$$

$$\therefore \quad f_a \in S^S$$

Define $g: S \to S^S$ by $g(a) = f_a$ ; $\forall\, a \in S$

Let $a, b \in S$ be any two elements, then $a * b \in S$

$$\therefore \quad g(a * b) = f_{a*b}$$

But for any $x \in S$, $f_{a*b}(x) = (a * b) * x = a * (b * x) = f_a(b * x) = f_a\big(f_b(x)\big) = (f_a \cdot f_b)(x)$

$$\therefore \quad f_{a*b} = f_a \cdot f_b = g(a) \cdot g(b)$$

$\therefore$ $g$ is a homomorphism of $(S,*)$ into $(S^S, \cdot)$

**Problem 2:** Let $S = N \times N$, the set of ordered pairs of positive integers with the operation $*$ defined by $(a, b) * (c, d) = (ad + bc, bd)$ and if $f: (S, \ *) \to (Q, +)$ is defined by $f(a, b) = \frac{a}{b}$, then show that 'f ' is a semi-group homomorphism.

**Proof:** We have the semigroups $(S, \ *)$ and $(Q, +)$

Given $f: (S, \ *) \to (Q, +)$ is defined by $f(a, b) = \frac{a}{b}$

Let $x, y \in S$ be any two elements, then $x = (a, b), \ y = (c, d)$ for integers a, b, c, d.

Now $x * y = (a, b) * (c, d) = (ad + bc, bd)$

$\therefore \quad f(x * y) = f(ad + bc, bd) = \frac{ad+bc}{bd} = \frac{a}{b} + \frac{c}{d} = f(a, b) + f(c, d)$

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

$\therefore \quad f$ is semigroup homomorphism.

**Problem 3:** Let $S = Z^+ \times Z^+, Z^+$ being set of positive integer and $*$ be an operation on S given by $(a, b) * (c, d) = (a + c, b + d)$ , $\forall \ a, b, c, d \in Z^+$. Show that S is semigroup. Also show that f is a homomorphism, if $f: (S,*) \to (Z, +)$ defined by $f(a, b) = a - b$.

**Proof:** Let $x, y, z$ be the ordered pairs $(a, b), (c, d)$ and $(e, f)$ respectively in $Z^+ \times Z^+$.

Then $(xy)z = (x * y) * z = [(a, b) * (c, d)] * (e, f) = [(a + c, b + d) * (e, f)$

$$= [(a + c) + e, (b + d) + f]$$

$$(xy)z = [a + c + e, b + d + f] \quad \ldots\ldots\ldots\ldots \text{(A)}$$

$x(yz) = x * (y * z) = (a, b) * [(c, d) * (e, f)] = (a, b) * [c + e, d + f] = [a + (c + e), b + (d + f)]$

$$(xy)z = [a + c + e, b + d + f] \quad \ldots\ldots\ldots\ldots \text{(B)}$$

From (A) and (B), we get,

$$(xy)z = x(yz)$$

$\therefore \ '*'$ is Associative.

Obviously $*$ satisfies closure property.

$\therefore$ $S$ is a semigroup.

Claim: $f:(S,*) \to (Z,+)$ by $f(a,b) = a - b$ is a homomorphism. $\forall\ x,y \in X$

$$f(x * y) = f[(a,b) * (c,d)] = f[a + c, b + d] = (a + c) - (b + d)$$

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

$$= f(a,b) + f(c,d) = f(x) + f(y)$$

$\therefore$ $f(x * y) = f(x) + f(y)$

$\therefore$ $f$ is a homomorphism