Module : 3

Algebraic Structures

R. Udhayakumar

Introduction

n-ary operations on a set S.

(1) Uniary operations

Let S be any set. We say that $*$ is an uniary operation on S if $* : S \to S$.

Example :- $* : R^{+} \to R^{+}$ by $*(x) = x$

(2) Binary operations

If $* : S \times S \to S$, then $*$ is called as binary operation. Also we can say that $*$ satisfies the closure property.

Ex : $+ : R \times R \to R$ defined by $+(a,b) = a+b$

Algebraic systems

A system consisting of a set, and one or more n-ary operations on the set is called an algebraic system or simply algebra.

Notation : $\langle S, f_1, f_2, \dots f_n, \dots \rangle$, where S is a nonempty set and $f_1, f_2, \dots f_n \dots$ are operations on S.

Algebraic structures

Since the operations and relations on the set S define a structure on the elements of S, then an algebraic system is called an algebraic structure.

Example: 1 Let I be the set of Integers.

Consider the algebraic system $\langle I, +, \times \rangle$ where $+$ and $\times$ are the operations of addition and multiplication of I.

A list of important properties of $\langle I, +, \times \rangle$

(A1) Associativity

For any $a, b, c \in I$

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

(A2) Commutativity

For any $a, b \in I$, then $a+b = b+a$.

(A3) Identity element

$\exists$ a distinguished element $0 \in I$ s.t for any $a \in I$

$$a+0 = 0+a = a$$

Here $0 \in I$ is the identity element w.r.to addition.

(A4) Inverse element

For each $a \in I$, $\exists$ a element different from identity element in I denoted by '$-a$' and called the negative of a (or) additive inverse of a s.t $a+(-a) = 0$.

(M1) Associativity

For $a, b, c \in I$, $(a \times b) \times c = a \times (b \times c)$

(M2) Commutativity

For $a, b \in I$, $a \times b = b \times a$

(M3) Identity element

There exists a distinguished element $1 \in I$ s.t for any $a \in I$,

$$a \times 1 = 1 \times a = a$$

(D) Distributivity

For any $a, b, c \in I$,

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

The operation $\times$ distributes over $+$.

(c) Cancellation property

For any $a, b, c \in I$ and $a \neq 0$.

$$a \times b = a \times c \Rightarrow b = c.$$

Example 2.

Let $\mathbb{R}$ be the set of real numbers and $+$ and $\times$ be the operations of addition and multiplication on $\mathbb{R}$. The algebraic systems $\langle \mathbb{R}, +, \times \rangle$ satisfies all the properties given for the system $\langle I, +, \times \rangle$.

Semigroups and Monoids

Semigroup : Let S be a nonempty set and $\circ$ be a binary operation on S. The algebraic system $\langle S, \circ \rangle$ is called a semigroup if the operation $\circ$ is associative.

In other words, $\langle S, \circ \rangle$ is a semigroup if for any $x, y, z \in S$, $(x \circ y) \circ z = x \circ (y \circ z)$.

Monoid A Semigroup $\langle M, \circ \rangle$ with an identity element with respect to the operation $\circ$ is called a monoid. In other words, an algebraic system $\langle M, \circ \rangle$ is called a monoid if for any $x, y, z \in M$,

$$(x \circ y) \circ z = x \circ (y \circ z)$$

and $\exists$ an elt $e \in M$ s.t for any $x \in M$,

$$e \circ x = x \circ e = x.$$

Note: (1) An identity elt of any binary operation, if it exists, is unique.

(2) Sometimes represent a monoid as $\langle M, \circ, e \rangle$ to emphasize the fact that e is a distinguished elt of such a monoid.

Example: ①

Let X be a nonempty set and X^X be the set of all mappings from X to X.

Let $\circ$ denote the operation of composition of the mappings, ie, for $f, g \in X^X$, $f \circ g$ is given by

$$f \circ g(x) = f(g(x)) \quad \forall\, x \in X \text{ is in } X^X.$$

$$\text{ie, } f \circ g \in X^X$$

$\therefore$ the algebra $\langle X^X, \circ \rangle$ is a monoid, because the operation of composition is associative and the identity mapping $f(x) = x \;\forall\, x \in X$ is the identity of the operation.

② Let X be a nonempty set and $B(X)$ be the set of all relations from X to X.

Let '$\circ$' denote the composition operation of relations in $B(X)$ then $\langle B(X), \circ \rangle$ is a monoid in which the identity relation is the identity of the monoid.

③ Let S be a nonempty set and $P(S)$ be its power set. The algebras $\langle P(S), \cup \rangle$ & $\langle P(S), \cap \rangle$ are monoids with the identities ϕ & S respectively.

④ * Let N be the set of all natural no's and '0'.
Then $\langle N, + \rangle$ and $\langle N, \times \rangle$ are monoids with the identities 0 and 1 respectively.

* Let E denotes the set of all positive even numbers. Then $\langle E, + \rangle$ & $\langle E, \times \rangle$ are semigroups but not monoids.

Homomorphisms of Semigroups and Monoids

Semigroup Homomorphism

Let $\langle S, * \rangle$ and $\langle T, \Delta \rangle$ be any two semigroups.
A mapping $g : S \to T$ is called semigroup homo., if for any $a, b \in S$,

$$g(a * b) = g(a) \,\Delta\, g(b).$$

Note:- A semigroup homo., is called a

(i) Semigroup monomorphism, if the mapping is 'one to one',

(ii) Semigroup epimorphism, if the mapping is 'onto'

and (iii) Semigroup isomorphism, if the mapping is 1-1 & onto.

Isomorphic

Two semigroups $\langle S, * \rangle$ and $\langle T, \Delta \rangle$ are said to be isomorphic, if there exists a semigroup isomorphism b/w S and T.

Note: (1) Homomorphism preserves the semigroup character because it preserves associativity

(2) Semigroup preserves the property of idempotency & commutativity.

Definition Monoid Homomorphism

Let $\langle M, *, e_M \rangle$ and $\langle T, \Delta, e_T \rangle$ be any two monoids. A mapping $g : M \to T$ s.t for any two elts $a, b \in M$ s.t

$$g(a * b) = g(a) \Delta g(b) \quad \text{and}$$

$$g(e_M) = e_T \quad \text{is called a monoid homo.,}$$

Note: The monoid homomorphism preserves

(1) associativity

(2) Commutativity

(3) identity

(4) Invertibility.

Example: 1

Let $\langle N, + \rangle$ be the semigroup of natural numbers with '0', and $\langle S, * \rangle$ be the semigroup on $S = \{e, 0, 1\}$ with the operation $*$ given by following table

$g(a+b) = g(a) * g(b)$

$*$	e	0	1
e	e	0	1
0	0	0	0
1	1	0	1

$g(0+1) = g(0) * g(1)$
$1 * 0 = 0 \in S$

A mapping $g : N \to S$ given by $g(0) = 1$ & $g(j) = 0$ for $j \neq 0$

is a Semigp homomorphism.

Both $\langle N, + \rangle$ and $\langle S, * \rangle$ are monoids with identities 0 and e respectively, but g is not a monoid homo., because $g(0) \neq e$.

Theorem : 1 Let $\langle S, * \rangle$, $\langle T, \Delta \rangle$ and $\langle V, \oplus \rangle$ be semigroups and $g: S \to T$, $h: T \to V$ be semigroup homomorphisms. Then $(h \circ g): S \to V$ is a semi gp homo., from $\langle S, * \rangle$ to $\langle V, \oplus \rangle$.

(or) composition of two homo is also a homo.

Soln:- Let $a, b \in S$. Then

$$(h \circ g)(a * b) = h\, g(a * b)$$
$$= h(g(a) \,\Delta\, g(b))$$
$$= h\, g(a) \oplus h\, g(b)$$
$$= (h \circ g)(a) \oplus (h \circ g)(b). \quad //$$

Definition:- A homomorphism of a semigroup into itself is called a semi gp endomorphism, while a isomorphism onto itself is called a semigroup automorphism.

Theorem : 2 Let $\langle S, * \rangle$ be a given semigroup. There exists a homomorphism $g: S \to S^S$ where $\langle S^S, \circ \rangle$ is a semi gp of functions from S to S under the operation of (left) composition.

Proof:- Let $a \in S$ be a fixed elt.

Let $g(a) = f_a$ where $f_a \in S^S$ & f_a is defined by $f_a(b) = a * b$ for any $b \in S$.

Also $g(a * b) = f_{a*b}$

Now
$$f_{a*b}(c) = (a * b) * c$$
$$= a * (b * c)$$
$$= a * f_b(c)$$
$$= f_a(f_b(c))$$
$$= (f_a \circ f_b)(c) \ \forall\ c \in S.$$

Therefore $g(a*b) = f_{a*b}$

$= f_a \circ f_b$

$= g(a) \circ g(b)$

$\therefore g: S \to S^S$ is a homomorphism of $(S, *)$ into $\langle S^S, \circ\rangle$.

~~Theorem~~ Sub Semigroups and Sub monoids

Sub semigroups Let $\langle S, *\rangle$ be a Semigroup. and $T \subseteq S$. If the set T is closed under the operation, $*$, then $\langle T, *\rangle$ is said to be Sub Semigroup of $\langle S, *\rangle$.

i.e, If $T \subseteq S$ then $\forall\, a, b \in T \Rightarrow a * b \in T$.

Submonoid Let $\langle M, *, e\rangle$ be a monoid and $T \subseteq M$. If T is closed under the operations $*$ and $e \in T$, then $\langle T, *, e\rangle$ is said to be submonoid of $\langle M, *, e\rangle$.

i.e, If $T \subseteq M$ then $\forall\, a, b \in T \Rightarrow a * b \in T$ & $e \in T$.

Example : 1 For the semigroup $\langle N, \times\rangle$, let T be the set of multiples of the integer m.

Then clearly $T \subseteq N$, Also $\langle T, \times\rangle$ is a subsemigp of $\langle N, \times\rangle$.

For, $a, b \in T \Rightarrow a = k_a m$, $b = k_b \cdot m$ where $k_a, k_b \in N$

Then $a \times b = k_a m \times k_b \cdot m$

$= (k_a k_b m) m \in T$

$\therefore \langle T, \times\rangle$ is a subsemigroup of $\langle N, \times\rangle$.

(2) For the semigroup $\langle N, + \rangle$, the set E of all the even non-negative integers is a subsemigroup $\langle E, + \rangle$ of $\langle N, + \rangle$.

Proof:- Let $a, b \in T \Rightarrow a = 2m$ & $b = 2n$ where $m, n \geq 0$ & $m, n \in \mathbb{Z}$

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

Hence $\langle E, + \rangle$ is a sub semigp of $\langle N, + \rangle$.

(3) Let $\langle S, * \rangle$ be a semigp and monoid on $S = \{e, 0, 1\}$ with the identity 'e', defined by

*	e	0	1
e	e	0	1
0	0	0	0
1	1	0	1

Take $S' = \{0, 1\} \subseteq S = \{e, 0, 1\}$

Then $\langle S', * \rangle$ is a subsemi gp of $\langle S, * \rangle$ but not a submonoid of $\langle S, * \rangle$.

Proof:- Here $0 * 1 = 0 \in S' \Rightarrow \langle S', * \rangle$ is a subsemigp of $\langle S, * \rangle$

But $e \notin S' \Rightarrow \langle S', * \rangle$ is not a submonoid of $\langle S, * \rangle$.

<u>Commutative semigroup</u>: A semigp $\langle S, * \rangle$ is said to be commutative semigp if for any $a, b \in S$ s.t $a * b = b * a$.

Eg: $\langle N, + \rangle$

<u>Commutative Monoid</u>: A monoid $\langle M, *, e \rangle$ is said to be commutative monoid if for any $a, b \in M$ s.t

$a * b = b * a$ Eg: $\langle N, + \rangle$

Idempotent elt

Suppose $\langle S, * \rangle$ is a algebraic system and $a \in S$.

If $a * a = a$ then $a \in S$ is said to be idempotent elt.

Eg: Identity elt.

Theorem For any commutative monoid $\langle M, * \rangle$, the set of idempotent elements of M forms a submonoid.

Proof:- Let S be the set of idempotent elts of M.

To prove $\langle S, * \rangle$ is a submonoid of $\langle M, * \rangle$

Since, the identity elt 'e' of M is idempotent

then $e \in S$. $\because (e * e = e)$

It is enough to prove 'S' is closed under $*$.

Let $a, b \in S \Rightarrow a * a = a$ & $b * b = b$.

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

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

$$= a * b * a$$

$$= a * a * b$$

$$= a * b$$

$\therefore a * b \in S$.

Hence $\langle S, * \rangle$ is a submonoid of $\langle M, *, e \rangle$.

Direct product of Algebraic systems

Let $\langle S, * \rangle$ and $\langle T, \Delta \rangle$ be two algebraic systems. The direct product of $\langle S, * \rangle$ & $\langle T, \Delta \rangle$ is the algebraic system $\langle S \times T, \circ \rangle$ in which the operation '$\circ$' on $S \times T$ is defined by

$$\langle s_1, t_1 \rangle \circ \langle s_2, t_2 \rangle = \langle s_1 * s_2, t_1 \Delta t_2 \rangle$$

for any $\langle s_1, t_1 \rangle$ & $\langle s_2, t_2 \rangle \in S \times T$.