Module 5 (Algebraic Structures)

Algebraic System

* Binary operation

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

A binary operation is denoted by $*, +, -, ;, \Delta, \square, \cup, \cap, \vee, \wedge, \ldots$

Thus $*$ is a binary operation on a set A if, for $a, b \in A$

$a * b \in A$

Example ① Let addition $+$ on $\mathbb{N}$, set of natural numbers

* For any two natural numbers a, b

Clearly $a+b$ also a natural number

$\therefore$ $+$ on $\mathbb{N}$ is a binary operation

(2) Now, consider the operation '−' subtraction on $\mathbb{N}$

It is not a binary operation, since $1, 2 \in \mathbb{N}$ but $1-2 \notin \mathbb{N}$

(3) Subtraction on $\mathbb{Z}$, set of all integers is a binary operation

Since for every $a, b \in \mathbb{Z}$

$a-b \in \mathbb{Z}$

---

* Operation which is defined from $A \times A \to A$ is called binary operation

* Operation from $A \times A \times A \to A$ is defined as 3-ary operation

* Similarly an n-ary operation is a function $f: \underbrace{A \times A \times \ldots \times A}_{n \text{ times}} \to A$.

Algebraic System

An algebraic system or simply an algebra is a system consisting of a non empty set A and one or more n-ary operations on the set A. It is denoted as $\langle A, f_1, f_2, \ldots \rangle$ where $f_1, f_2, f_3, \ldots$ are operations on A.

Example: $\langle N, + \rangle$, $\langle Z, + \rangle$, $\langle R, + \rangle$, $\langle Z, - \rangle$ are all algebraic system.

Properties of Algebraic Systems

* Let A be a non empty set then it can satisfies the following X properties. [where + and · are binary operations]

1. Associativity property for +

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

where $a, b, c \in A$

2. Commutative property for +

$a+b = b+a$, where $a, b \in A$

3 Identity element 0 for +

There exists an identity element $0 \in A$ such that for any $a \in A$

$a+0 = 0+a = a$

4 Inverse element under +

For each $a \in A$, there exist an element $b \in A$ such that

$a+b = b+a = 0$

5. Associative property for ·

for $a, b, c \in A$

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

6. Commutative property for ·

for $a, b \in A$

$a\cdot b = b\cdot a$

7 Identity element 1 for ·

for each $a \in A$

$$a \cdot 1 = 1 \cdot a = a$$

8 Distributive law of · over +

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

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

9 Cancellation property

for any $a, b, c \in A$

$a \cdot b = a \cdot c \Rightarrow b = c$ provided $a \neq 0$

10 Idempotent property

for every $a \in A$

$$a + a = a$$

$$a \cdot a = a$$

Define with example?

Semi-Group

The algebraic system $\langle S, * \rangle$ is known as a semigroup where S is a non empty set and $*$ is a binary operation such that $*$ is associative then $\langle S, * \rangle$ is called a semigroup.

* If (1) $*$ is associative and
(2) $*$ is commutative then
$\langle S, * \rangle$ is called commutative (abelian) semigroup

Monoid

A monoid $\langle M, * \rangle$ is a Semigroup with an identity element 'e'. Thus a monoid can also be represented as $\langle M, *, e \rangle$

Monoid $\langle M, *, e \rangle$

1. $*$ is associative $[(a*b)*c = a*(b*c)]$
2. an element 'e' exist such that
$$\forall a \in M \quad a*e = e*a = a$$

* If
1. $*$ is associative
2. $*$ is commutative and
3. there exist an element 'e' in M such that $a*e = e*a = a, \forall a \in M$

then $\langle M, *, e \rangle$ is called abelian monoid

Examples

1. Let us consider $\langle Z^+, + \rangle$

clearly $\forall a, b, c \in Z^+$
$$a+(b+c) = (a+b)+c$$
$\therefore$ + is associative

+ is a binary operation

also here

(since $\forall a, b \in Z^+$, $a+b \in Z^+$)

Thus $\langle Z^+, + \rangle$ is a semigroup.

Now, here in Z^+ there does not exist element e of the form

$$a * e = e * a = a$$

ie, $a + e = e + a = a$

0 is the only such element but $0 \notin Z^+$

Thus $\langle Z^+, + \rangle$ is not a monoid

also $\langle Z^+, + \rangle$ is abelian semigroup (since + is commutable also)

2. Consider $\langle N, + \rangle$ where

$N = \{0, 1, 2, \ldots\}$

Clearly + is a binary operation

(since $\forall a, b \in N$, $a+b \in N$)

Now $\forall a, b, c \in N$

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

$\therefore$ + is associative

also $\forall\ a,b \in N$ $\quad a+b = b+a$

ie; + is commutative

Thus $\langle N, + \rangle$ is an abelian Semigroup

Here $N = \{0, 1, 2, \ldots\}$

there exist $e = 0$ such that

$$a+0 = 0+a = a \quad \forall a \in N$$

Thus $\langle N, + \rangle$ is a monoid

also here $a+b = b+a$ $\forall\ a,b \in N$

$\therefore \langle N, + \rangle$ is an abelian monoid.

NOTE

* Algebraic structures like $\langle N, + \rangle$ $\langle Z, + \rangle$, $\langle R, + \rangle$, $\langle N, \times \rangle$, $\langle Q, \times \rangle$, $\langle Q, + \rangle$ are all

Semigroups. [since in all these cases corresponding binary operation is associative]

Q (3) * Show that $M_n(Z) = \{A / A$ is an $n \times n$ matrix with entries from $Z\}$ is a commutative monoid under usual matrix addition?

Here we have $M_n(Z)$

Soln Let A, B, C be 3 elements in $M_n(Z)$

$$(A+B)+C = A+(B+C)$$ (since matrix addition is associative)

(1) Matrix addition is associative

Now there exist an element

$$e = \begin{bmatrix} 0 & 0 & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & \cdots & 0 \end{bmatrix}_{n \times n}$$

Thus for any $A \in M_n(Z)$

$A + e = e + A = A$

ie; 2 identity element exist in $M_n(Z)$

also for any two elements

3 $A, B \in M_n(Z)$

$A + B = B + A$

ie; Commutative

Thus $\langle M_n(Z), + \rangle$ is a Commutative monoid

NOTE

$\langle M_n(Q), + \rangle$, $\langle M_n(R), + \rangle$, $\langle M_n(C), + \rangle$

* are all commutative monoid

* Set of natural number $\langle IN, + \rangle$ is not a monoid since $IN = \{1, 2, 3, \dots\}$

Q: Show that the set of all permutations
(4) of the set $A = \{1, 2\}$ under the binary operation * as composition operator is a monoid?

* The set of all permutations of n symbols $\{1, 2, \ldots, n\}$ is denoted as S_n

Here we need to prove $\langle S_2, \circ \rangle$ is a monoid.

Here the possible permutations are

$f_1 = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$

$f_2 = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}$

$f_3 = \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix}$

$f_4 = \begin{pmatrix} 1 & 3 \\ 2 & 1 \end{pmatrix}$

Now, $f_2 \circ f_3 = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix} = f_3$

$f_4 \cdot f_4 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = f_1$

And so on, Thus we can obtain a table as follows

$\circ$	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_2	f_3	f_3
f_3	f_3	f_2	f_3	f_2
f_4	f_4	f_2	f_3	f_1

Clearly $\circ$ is a binary operation and is ① associative

$f_2 \circ f_3 = f_3$. Thus $*$ is not

$f_3 \circ f_2 = f_2$ Commutative.

Here ② $e = f_1$ since $\forall$ elements in S_2

$f_i \circ f_1 = f_1 \circ f_i = f_i \quad \forall i = 1, 2, 3, 4$

Q: (4) Show that the set of all permutations of the set $A = \{1, 2\}$ under the binary operation * as composition operator is a monoid?

* The set of all permutations of n symbols $\{1, 2, \ldots, n\}$ is denoted as S_n

Here we need to prove $\langle S_2, \circ \rangle$ is a monoid.

Here the possible permutations are

$$f_1 = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$$

$$f_2 = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}$$

$$f_3 = \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix}$$

$$f_4 = \begin{pmatrix} 1 & 3 \\ 2 & 1 \end{pmatrix}$$

Now, $f_2 \circ f_3 = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix} = f_3$

$f_4 \cdot f_4 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = f_1$

And so on, Thus we can obtain a table as follows

$\circ$	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_2	f_3	f_3
f_3	f_3	f_2	f_3	f_2
f_4	f_4	f_2	f_3	f_1

Clearly $\circ$ is a binary operation and is 1 associative

$f_2 \circ f_3 = f_3$. Thus $*$ is not

$f_3 \circ f_2 = f_2$ Commutative.

Here 2 $e = f_1$ since $\forall$ elements in S_2

$f_i \circ f_1 = f_1 \circ f_i = f_i \quad \forall i = 1, 2, 3, 4$

$\therefore$ existence of identity element

$\therefore \langle S_2, \circ \rangle$ is a monoid

Q: show that an algebraic structure $\langle Z_6, +_6 \rangle$
(5) is a monoid where $+_6$ is addition modulo 6 and $Z_6 = \{0, 1, 2, 3, 4, 5\}$.

$Z_n = \{0, 1, 2, 3, \ldots, (n-1)\}$

$+_n \Rightarrow a +_n b$ is the remainder when $(a+b)$ divided by n

Thus here $Z_6 = \{0, 1, 2, 3, 4, 5\}$

$2 +_6 4 = \text{remainder}\left((2+4)/6\right)$

$= 0$

$$6 \overline{\big)\, 6}\ 1 \quad \frac{6}{0}$$

$3 +_6 5 = \text{remainder of } \frac{3+5}{6}$

$= 2$

$$6 \overline{\big)\, 8}\ 1 \quad \frac{6}{2}$$

Thus we can form the corresponding table as follows

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Now, clearly $(a +_6 b) +_6 c = a +_6 (b +_6 c)$

for every $a, b, c \in \{0, 1, 2, 3, 4, 5\}$

① associative ✓

Now, here $e = 0$

since $a +_6 0 = 0 +_6 a = a$

$\forall a \in Z_6$

∴ Identity element exist

Thus $< Z_6, +_6 >$ is a monoid

Q: Is $\langle N, * \rangle$ a commutative monoid
(6) where $x * y = \max\{x, y\}$?

Clearly for a, b, c in N

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

$= \max\{a, b, c\}$

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

$= \max\{a, b, c\}$

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

$\therefore *$ is associative

Now $0 \in N$ such that for any $a \in N$

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

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

$\therefore$ Identity element exist

$\therefore \langle N, * \rangle$ is a monoid.

Also $a * b = \max\{a, b\}$

$$= \max\{b, a\}$$

$$= b * a$$

$\therefore *$ is Commutative

$\langle N, * \rangle$ is a Commutative monoid

Sub semi group and sub monoid

Let $\langle S, * \rangle$ be a semigroup. and let $T \subseteq S$ be a subset, such that $\langle T, * \rangle$ is a semigroup then we can say that $\langle T, * \rangle$ is a sub semigroup of $\langle S, * \rangle$

Let $\langle M, *, e_m \rangle$ be a monoid and $T \subseteq M$ be a subset of M such that $\langle T, *, e_m \rangle$ is a monoid then we can say $\langle T, *, e_m \rangle$ is a sub monoid of $\langle M, *, e_m \rangle$

Examples :>

(1) Let $N = \{0, 1, 2, 3, \ldots\}$

$Z^+ = \{1, 2, 3, \ldots\}$

Clearly $\langle N, + \rangle$ is a semigroup

Since $a, b, c \in N$

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

associativity holds

also $\langle Z^+, + \rangle$ is a semigroup

where $Z^+ \subseteq N$ $\therefore \langle Z^+, + \rangle$ is a sub semi group of $\langle N, + \rangle$

Whereas let $T = \{1, 3, 5, \cdots\}$.

$\langle T, + \rangle$ is not a semigroup

since addition is not a binary

operation in T

since $1 + 5 = 6 \notin T$

$\therefore \langle T, + \rangle$ is not a subsemigroup of $\langle N, + \rangle$

2. Let $\langle R, \cdot, 1 \rangle$ is a monoid

(since $\cdot$ is associative and ①

$1 \in R$ such that ②

$1 \cdot a = a \cdot 1 = a \quad \forall a \in R$)

Now $\langle N, \cdot, 1 \rangle$ where

$N = \{0, 1, 2, 3, \cdots\}$

$\langle N, \cdot, 1 \rangle$ is a monoid

also $N \subseteq R$

$\Longrightarrow$ $\langle N, \cdot, 1 \rangle$ is a sub monoid of $\langle R, \cdot, 1 \rangle$

Let $\langle E, \cdot \rangle$ is not a monoid where $E = \{0, 2, 4, \ldots\}$ since there does not exist an element 'e' such that $a \cdot e = e \cdot a = a$

(since $1 \notin E$)

$\therefore$ $\langle E, \cdot \rangle$ is not a sub monoid of $\langle R, \cdot, 1 \rangle$

Homomorphism & Isomorphism.

Let $\langle X, \cdot \rangle$ and $\langle Y, * \rangle$ be two algebraic structures where $\cdot$ & $*$ are both n-ary operations. A function $f : X \rightarrow Y$ is known as a homomorphism from $(X, \cdot)$ to $\langle Y, * \rangle$ if for any $x_1, x_2 \in X$

we have

$$f(x_1 \cdot x_2) = f(x_1) * f(x_2)$$

[Since $x_1, x_2 \in X \rightarrow$ operation is $\cdot$
and $f(x_1), f(x_2) \in Y \rightarrow$ operation is $*$.]

* If the homomorphism f is one-to-one & onto then f is called an isomorphism or epimorphism or monomorphism.

* If $f : S \rightarrow T$ and $g : T \rightarrow P$ be two hommomorphism where $(S, *)$, $\langle P, \nabla)$ $\langle T, \Delta \rangle$ are any algebraic structures then $g \circ f : S \rightarrow P$ is again a homomorphism.

Homomorphism & Isomorphism of Semigroup

Let $\langle X, \circ \rangle$ and $\langle Y, * \rangle$ be two semigroup and f be a function $f : X \to Y$ is called a semigroup homomorphism If for any two elements $x_1, x_2 \in X$

we have

$$f(x_1 \circ x_2) = f(x_1) * f(x_2)$$

* If f is one-one and onto then such a semigroup homomorphism is called semigroup Isomorphism.

Homomorphism & Isomorphism of Monoid

Let $\langle M_1, \circ, e_{m_1} \rangle$ and $\langle M_2, *, e_{m_2} \rangle$ be two monoids. A function $f : M_1 \to M_2$ is a monoid homomorphism If for any $a, b \in M_1$, we have

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

(2) $f(e_{m_1}) = e_{m_2}$

ie image of the identity element in M_1 is the identity element in M_2.

Q. 1 Let $< Z^+, + >$ and $< Z^+, \cdot >$ be two semi groups define $f: Z^+ \longrightarrow Z^+$ as

$$f(m) = 2^m \text{ for any } m \in Z^+$$

Show that f is a semigroup homomorphism from $< Z^+, + >$ to $< Z^+, \cdot >$?

$\rightarrow$ $f: Z^+ \longrightarrow Z^+$ defined by

$$f(m) = 2^m \text{ for any } m \in Z^+$$

We need to prove f is a homomorphism

binary operation in $< Z^+, + >$

ie, $f(a+b) = f(a) \cdot f(b)$

binary operation in $< Z^+, \cdot >$

for any $a, b \in Z^+$

Let $a, b \in Z^+$

$$f(a+b) = 2^{a+b}$$

$$= 2^a \cdot 2^b$$

$$= f(a) \cdot f(b)$$

$\therefore$ f is a semigroup homomorphism.

Q 2. Let $< N, +, 0 >$ and $< N, \cdot, 1 >$ be two monoids define $f: N \rightarrow N$ as $f(m) = 3^m$ for any $m \in N$ (monoid homomorphism)

$\longrightarrow$ Let $a, b \in N$

We need to prove

① $f(a+b) = f(a) \cdot f(b)$ &

② $f(0) = 1$

for,

consider $f(a+b) = 3^{a+b}$

$= 3^a \cdot 3^b$

$= f(a) \cdot f(b)$

Now f (identity element in domain monoid)

= Identity element in codomain monoid

Identity element in $\langle N, +, 0 \rangle$

$\Longrightarrow f(0) = 3^0$

$= 1$

= Identity element in the monoid $\langle N, \cdot, 1 \rangle$

Thus $f: N \rightarrow N$ defined by

$f(m) = 3^m$ for any $m \in N$

is a monoid homomorphism

Q3. Let $E = \{2, 4, 6, 8, \ldots\}$ define $f: Z^+ \longrightarrow E$ by $f(n) = 2n$. Show that f is not a semigroup homomorphism from

from $\langle Z^+, \cdot \rangle$ to the semigroup $\langle E, \cdot \rangle$?

Let $m, n \in Z^+$

$f(m.n) = 2(mn)$

$\neq (2m)(2n) = f(m) \cdot f(n)$

$\therefore$ f is not a semigroup homomorphism.

Q4. Let R^+ be the set of all positive real numbers. Consider the two semigroup (monoids) $\langle R^+, \cdot, 1 \rangle$ and $\langle R, +, 0 \rangle$. Define $f : R^+ \to R$ by $f(x) = \ln x$? Show that f is an isomorphism from R^+ to R?

homomorphism. One one & onto

[since $\langle R^+, \cdot, 1 \rangle$ and $\langle R, +, 0 \rangle$ are both semigroup as well as monoid, the homomorphism is is semigroup monoid homomorphism.

$\rightarrow$ Let $x, y \in R^+$

$f(x.y) = \ln(x \cdot y)$

$= \ln x + \ln y$

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

$\Rightarrow$ f is a homomorphism.

Now Let $a_1, a_2 \in R^+$ and let $f(a_1) = f(a_2)$

$$\implies \ln(a_1) = \ln a_2$$

Taking exponential on both sides

$$\implies e^{\ln a_1} = e^{\ln a_2}$$

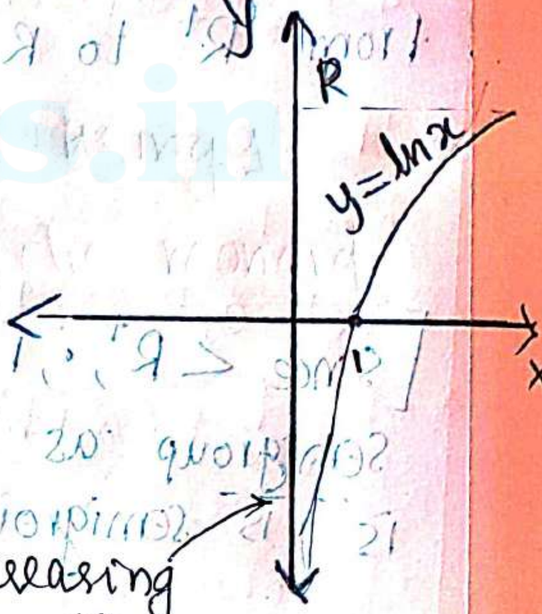
$$\boxed{e^{\ln x} = x}$$

$$\implies a_1 = a_2$$

$\implies$ f is <u>one-one</u> function

Now for any element in the codomain $\langle R, +, 0 \rangle$

<u>Range</u> $f = \{y \mid y = \ln x\}$ $= R$



ln x is an increasing function.

$$= \{\ln x : x \in R^+\}$$

$$= R$$

∴ f is onto function.

∴ f is an isomorphism from $\langle R^+, \cdot, 1 \rangle$ to $\langle R, +, 0 \rangle$

Cyclic Monoid

A cyclic monoid is a monoid $<M, *, e>$ in which every element of M can be expressed as some powers of a particular element $a \in M$. Then the element 'a' is called the generator of $<M, *, e>$

ie, any element x in a cyclic monoid can be expressed as $x = a^m$ for some $m \in N$

NOTE:

A cyclic monoid is an abelian monoid

Since, Let M be a cyclic monoid.

ie, $\exists$ $a \in M$ such that for every $x, y \in M$

$x = a^{m_1}$ and $y = a^{m_2}$

(Since a is the generator of M)

$$
\begin{aligned}
\text{Now} \quad x * y &= a^{m_1} * a^{m_2} \\
&= a^{m_1 + m_2} \\
&= a^{m_2 + m_1} \\
&= a^{m_2} * a^{m_1} \\
&= y * x
\end{aligned}
$$

ie $<M, *, e>$ is abelian

* Let $\langle N, +, 0 \rangle$ is an infinite cyclic monoid generated by $1 \in N$

Here $N = \{0, 1, 2, 3, \ldots\}$

Clearly, for any $a, b, c \in N$

$$a+(b+c) = (a+b)+c \text{ , associativity}$$

Since $0 \in N$ s. $a+0 = 0+a = a$ $\forall a \in N$.

also for any element $a \in N$

$a = \underbrace{1+1+\cdots+1}_{a \text{ times}}$ thus any element is N can be generated using 1

$\therefore \langle N, +, 0 \rangle$ is a cyclic monoid