Monoid

~~A ge~~ A semi-group $(M, *)$ with an identity element with respect to binary operation $*$ is called monoid. In other words, An algebraic structure $(M, *)$ is called a monoid if:

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

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

$$e*a = a*e = a \quad \forall a \in M.$$

eg:- Let N be set of Natural numbers $(N, \times)$ is a monoid. 1 is the identity element in N with respect to composition $\times$.

If M is 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 a cyclic monoid may have more than one generator.

eg:- If $M = \{-1, 1, -i, i\}$ where $i = \sqrt{-1}$, then $(M, *)$ is a cyclic monoid : The elements i and $-i$ are its generators.

Monoid Homomorphism

Let $(M, *)$ and $(T, \circ)$ be any two monoid e_m and e_t denote the identity elements of $(M, *)$ and $(T, \circ)$ respectively. A mapping

$$f : M \rightarrow T$$

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

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

$$\text{and } f(e_m) = e_t$$

is called monoid homomorphism.

Monoid homomorphism presents the associativity and identity. It also preserves commutative.

Groups

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

(i) $a * (b * c) = (a * b) * c$ for all $a, b, c \in G$ [Associativity]

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

(iii) $a * a^{-1} = a^{-1} * a = e$ (Inverse of a in G)

~~(i) Alg~~ (i) Abelian Group (or Commutative Group)

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

eg:- $(Z, +)$ is an abelian Group

(ii) Finite Group

A Group G is said to be finite Group if the set G is a finite set.

eg:- $G = \{-1, 1\}$ is a group w.r.t. operation multiplication. Where G is a finite set having 2 elements. Therefore G is a finite Group.

(iii) Infinite Group

A Group G, which is not finite is called an infinite Group.

(iv) Order of a group

The order of a group $(G, *)$ is the number of distinct element in G. The order of G is denoted by $O(G)$ or $|G|$

eg:- $G = \{-1, 1\}$

The set G is group w.r.t. binary operation multiplication and $O(G) = 2$.

eg:- 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.

Sol^n

$\times$	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	-1	+1
-i	-i	+i	1	-1

Composition table

Associativity : for any three element $a,b,c \in G \Rightarrow (a\times b)\times c = a\times(b\times c)$

Since $(1\times -1)\times i = -1\times i = -i$

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

Similarly with any other three elements of G the properties holds.

$\therefore$ Associative law holds in $(G,\times)$

Existence of identity: 1 is the identity element $(G,\cdot)$ such that $1\cdot a = a\cdot 1 = a \ \forall a \in G$.

Existence of inverse: $1.1 = 1 = 1.1 \Rightarrow 1$ is a inverse of 1

$-1.-1 = 1 = -1.-1 \Rightarrow -1$ is a inverse of -1

$i.-i = 1 = -i.i \Rightarrow -i$ is a inverse of $+i$

Hence inverse of every element exists.

Thus, all the properties of groups are satisfies.

Commutative: $a.b = b.a \ \forall a,b \in G$

$1.1 = 1 = 1.1$, $-1.1 = -1 = 1.-1$

$i.1 = i = 1.i$, $i.-i = 1 = -i.i$ and so on.

commutative law is satisfied.

Hence $(G, \times)$ is an abelian group.

Ex Prove that $G = \{1, \omega, \omega^2\}$ is a group w.r.t. multiplication where $1, \omega, \omega^2$ are cube roots of unity.

Sol

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

Composition table

The abelian group or system is $(G, \cdot)$, where $\omega^3 = 1$ and multiplication '$\cdot$' is the binary operation on G. From composition table; it is clear that $(G, \cdot)$ is closed w.r.t. operation multiplication and the operation '$\cdot$' is associative.

1 is the identity element in G such that

$$1 \cdot a = a = a \cdot 1 \quad \forall a \in G$$

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 is the inverse of ω^2 in G.

$\therefore (G, \cdot)$ is a group and $a \cdot b = b \cdot a \ \forall a, b \in G$ that is commutative law holds in G with respect to multiplication.

$\therefore (G, \cdot)$ is an abelian group.

Ex Prove that the set Z of integers with binary operation $*$ is defined by $a*b = a+b+1 \cdot \forall a,b \in G$ is an abelian group.

Sol^n Sum of two integers is again an integers, therefore,

$$a+b \in Z \quad \forall a,b \in Z$$

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

$\Rightarrow$ Z is called with respect to $*$

Associative Law for all $a,b,c \in G$ we have

$$(a*b)*c = (a+b+1)*c$$
$$= a+b+1+c+1$$
$$= a+b+c+2$$

~~(a*b)~~ $a*(b*c) = a*(b+c+1)$
$$= a+b+c+1+1$$
$$= a+b+c+2$$

Hence $\boxed{(a*b)*c = a*(b*c)}$

Existence of Identity

Let $a \in Z$. Let $e \in Z$ such that $e*a = a*e = a$

i.e. $a+e+1 = a$.

$\Rightarrow e = -1$

$\boxed{e=-1}$ is the identity element in Z.

Existence of Inverse

Let $a \in Z$. let $b \in Z$ such that $a*b = e$

$$\Rightarrow a+b+1 = -1$$
$$b = -2-a$$

$\therefore$ for every $a \in Z$, there exists $-2-a \in Z$ such that $a*(-2-a) = (-2-a)*a = -1$.

$\therefore$ $(Z,*)$ is an abelian Group.

Q Show that the set Q^+ for all positive rational numbers forms an abelian group under composition defined by $\circ$ ~~and~~ such that $a \circ b = ab/3$ for $a, b \in Q^+$

Sol Q^+ is the set of all positive real numbers, for all $a, b \in Q^+$, we have the operation $\circ$ such that

$a \circ b = ab/3$.

Associativity: $a, b, c \in Q^+ \Rightarrow (a \circ b) \circ c = a \circ (b \circ c)$

$$(a \circ b) \circ c = \frac{ab}{3} \circ c = \frac{abc}{3 \times 3} = \frac{abc}{9}$$

$$a \circ (b \circ c) = a \circ \frac{bc}{3} = \frac{abc}{3 \times 3} = \frac{abc}{9}$$

Existence of identity element

Let $a \in Q^+$ & $e \in Q^+$ such that $e \circ a = a$..

i.e. $\boxed{\frac{ea}{3} = a}$

$$\frac{ea}{3} = a \Rightarrow ea = 3a \Rightarrow ea - 3a = 0$$
$$\Rightarrow a(e-3) = 0$$
$$\Rightarrow e - 3 = 0$$
$$\Rightarrow \boxed{e = 3}$$

$\therefore$ $e = 3$ is the identity element in Q^+.

Existence of Inverse:

Let $a \in Q^+$ & let $b \in Q^+$ such that $a \circ b = e$

$$\Rightarrow \frac{ab}{3} = e \quad (\because e = 3)$$
$$b = 9/a \quad (\because a \neq 0)$$

$\therefore$ for every $a \in Q^+$, there exists $9/a \in Q^+$ such that

$$a \circ b = a \circ 9/a = 9/a \circ a = 3.$$

Commutativity

Let $a, b \in Q^+ \Rightarrow a \circ b = b \circ a$

Since $a \circ b = \frac{ab}{3} = \frac{ba}{3} = b \circ a$

$\therefore (Q^+, \circ)$ is an abelian Group