Algebraic Systems
and
Number Theory

Algebraic Systems

Definition : A mapping $f: A \times A \rightarrow A$ is called a binary operation (A is any set)

A mapping $f: A^n \rightarrow A$ is called an n-ary operation

Definition : A system consisting a set and one or more n-ary operations defined on the set is called an algebraic system or algebra.

Examples : i) Semigroups, monoids and groups are algebraic systems with one binary operation

ii) Rings, integral domains and fields are algebraic systems with two binary operations.

Properties of Binary Operations

Closure property : A binary operation $*: A \times A \rightarrow A$ is said to be closed if $a, b \in A \Rightarrow a * b \in A; \forall a, b \in A$

Associative property : A binary operation $*$ on A is said to satisfy associative property if

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

Existence of Identity:

If there exists an element $e \in A$ such that $a * e = e * a = a$, $\forall a \in A$, then e is called the identity element.

Existence of Inverse

For each $a \in A$, if there exists $b \in A$ such that $a * b = b * a = e$, then b is called the inverse of a and is denoted by $b = a^{-1}$.

Commutative Property

If $a * b = b * a$ for all $a, b \in A$, then $*$ is said to be commutative on A.

Distributive Properties

For all $a, b, c \in A$, $a * (b \cdot c) = (a * b) \cdot (a * c)$

(Left distributive law)

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

(Right distributive law)

Cancellation Properties

For all $a, b, c \in A$, $a * b = a * c \Rightarrow b = c$

(Left cancellation law)

$b * a = c * a \Rightarrow b = c$

(Right cancellation law)

Semi Groups

Definition: A non empty set S together with a binary operation $*$ is said to be a semi group if it satisfies closure and associative properties

That is, $(S,*)$ is said to be a semigroup if

i) $a, b \in S \Rightarrow a*b \in S$, $\forall a,b \in S$

ii) $a*(b*c) = (a*b)*c$, $\forall a,b,c \in S$.

Examples:

1) The set of all natural numbers under addition and multiplication are semi groups

i.e $(N,+)$ and $(N,\times)$ are semigroups.

2) The set of all even integers under addition and multiplication are semi groups

i.e $(E,+)$ and $(E,\times)$ are semigroups where

$E = \{0, \pm 2, \pm 4, \pm 6, \ldots\}$

Sub Semi groups

Let A be a non-empty subset of a semigroup $(S,*)$. Then A is called a subsemigroup of S if A is itself a semigroup with respect to the same operation $*$ on S.

Examples: Let A and B denote the set of even and odd positive integers respectively. Then

i) $(A, \times)$ and $(B, \times)$ are subsemigroups of $(N, \times)$

ii) $(A, +)$ is a subsemigroup of $(N, +)$ but $(B, +)$ is not a subsemigroup of $(N, +)$, since addition of two odd positive integers is an even integer.

Commutative Semigroup: A semigroup $(S, *)$ is said to be commutative or abelian if $x * y = y * x$ for all $x, y \in S$.

ex) The set of integers is an abelian semigroup under the operations of addition and multiplication

Cyclic Semigroup: A semigroup $(S, *)$ is said to be cyclic if there exists an element $a \in S$ such that every element of S can be written as some power of a i.e a^n for some positive integer n.

In this case, we say that S is the cyclic semigroup generated by the element 'a' and 'a' is called the generator of the cyclic semigroup.

Semigroup Homomorphism

Let $(S, *)$ and $(T, \circ)$ be two Semigroups.

A mapping $f: S \to T$ is called a semigroup homomorphism if $f(a*b) = f(a) \circ f(b)$, for all $a, b \in S$.

- A one-to-one semigroup homomorphism is called a semigroup monomorphism.
- An onto semigroup homomorphism is called a semigroup epimorphism.
- A one-to-one and onto semigroup homomorphism is called a semigroup isomorphism.
- An isomorphism of a semigroup onto itself is called a semigroup automorphism.
- A homomorphism of a semigroup onto itself is called a semigroup endomorphism.

pb) Given an example of semigroup homomorphism

Sol. Let $(N, +)$ and $(Z_m, +_m)$ be any two semigroups. Define a map $g: N \to Z_m$ by $g(a) = [a]_m$, for all $a \in N$.

Then $g(a+b) = [a+b]_m = [a]_m + [b]_m$

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

Therefor g is a semigroup homomorphism.

<u>Theorem</u>: The composition of semigroup homomorphism is also a semigroup homomorphism.

<u>proof</u>:- Let $(S,*)$, (T,o) and $(V,\oplus)$ be three semigroups and $g: S \to T$, $h: T \to V$ be semigroup homomorphism.

Since g is a homomorphism, $g(a*b) = g(a) o g(b)$ for all $a,b \in S$ and since h is a homomorphism $h(x o y) = h(x) \oplus h(y)$ for all $x,y \in T$

Now for all $a,b \in S$,

$$(hog)(a*b) = h[g(a*b)]$$

$$= h[g(a) o g(b)]$$

$$= h(g(a)) \oplus h(g(b))$$

$$= (hog)(a) \oplus (hog)(b)$$

Hence hog is a semigroup homomorphism.

i.e The composition of semigroup homomorphisms is also a semigroup homomorphism.

Theorem:- Semigroup homomorphism preserves the property of idempotency

proof:- Let $f : (S, *) \to (T, \circ)$ be a semigroup homomorphism.

Then $f(a * b) = f(a) \circ f(b)$, $\forall\, a, b \in S$

Let x be an idempotent element in S

Then $x * x = x$

$\Rightarrow f(x * x) = f(x)$

$\Rightarrow f(x) \circ f(x) = f(x)$

$\Rightarrow f(x)$ is an idempotent element.

Theorem: Let $(S, *)$ be a given semigroup. Then there exists a homomorphism $g : S \to S^S$ where $(S^S, \circ)$ is a semigroup of functions from S to S under the operation of composition.

proof:- Let $(S, *)$ be a given semigroup.

For any element $a \in S$, let $g(a) = f_a$ where $f_a \in S^S$, is defined as follows

$$f_a(b) = a * b \quad \text{for all } b \in S.$$

we now prove that g is a homomorphism.

Now $g(a*b) = f_{a*b}$ where

$$f_{a*b}(c) = (a*b)*c$$
$$= a*(b*c)$$
$$= f_a(b*c)$$
$$= f_b(f_b(c))$$
$$= f_a f_b(c)$$
$$= (f_a \circ f_b)(c)$$

$$\therefore f_{a*b} = f_a \circ f_b$$

Hence $g(a*b) = f_{a*b} = f_a \circ f_b = g(a) \circ g(b)$

Thus $g : S \to S^S$ is a homomorphism.

Monoid: A non empty set M together with a binary operation $*$ is said to be a monoid if $*$ satisfies the closure, associative and identity properties.

That is, $(M,*)$ is said to be monoid if

i) $a, b \in M \Rightarrow a*b \in M, \forall a, b \in M$

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

iii) There exists $e \in M$ such that

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

Note: A semigroup with identity element is a monoid.

ex: 1) $(N, \times)$ is a monoid with 1 as the identity element

2) Let W be the set of all nonnegative integers then $(W,+)$ and $(W,\times)$ are monoids with 0 and 1 as the identity elements.

Scanned with CamScanner

Submonoid : Let $(M, *)$ be a monoid and let A be a subset of M. Then A is said to be the submonoid of M if A is closed w.r.t the operation $*$ and the same identity element e.

Cyclic monoid : A monoid $(M, *, e)$ is said to be cyclic if every element $x \in M$ is of the form a^n for some $a \in M$, where n is any integer i.e $x = a^n$ for all $x \in M$. In this case M is a cyclic monoid generated by a and a is called the generator of the cyclic monoid.

ex : Let $N = \{0, 1, 2, 3, \ldots\}$ be the set of whole numbers. Then $(N, +)$ is an infinite cyclic monoid under the operation addition generated by 1.

Def :- A monoid $(M, *, e)$ is said to be abelian or commutative if $a * b = b * a$, $\forall a, b \in M$.

ex : The set of real numbers under addition and multiplication are abelian monoids.

Theorem Every cyclic monoid is commutative.

proof:- Let $(M,*,e)$ be a cyclic monoid generated by an element $a \in M$.

Let $x, y \in M$. Then $x = a^m$, $y = a^n$ for some integers m, n.

Now $x * y = a^m * a^n$

$= a^{m+n}$

$= a^{n+m}$ ($\because (\mathbb{Z},+)$ is commutative)

$= a^n * a^m$

$= y * x$

$\therefore x * y = y * x, \ \forall x, y \in M$.

Hence $(M,*,e)$ is abelian.

Thus every cyclic monoid is abelian

Monoid homomorphism

Let $(M,*,e)$ and (T,Δ,e') be two monoids

A mapping $f: M \to T$ is called a monoid homomorphism if $f(a*b) = f(a)\Delta f(b)$ and $f(e) = e'$, $\forall a, b \in M$.

Groups

A non empty set G together with a binary operation $*$ defined on G is called group if $*$ satisfies the following axioms

i) $*$ is closed in G i.e $a*b \in G$, $\forall a,b \in G$

ii) $*$ is associative in G i.e $a*(b*c) = (a*b)*c$ $\forall a,b,c \in G$.

iii) Existence of identity : if there exists an element $e \in G$ such that $e*a = a*e = a$, $\forall a \in G$

iv) Existence of inverse : For each $a \in G$ there exists $a^{-1} \in G$ such that $a*a^{-1} = a^{-1}*a = e$

In this we say that $(G,*)$ is a group.

Abelian group: A Group $(G,*)$ is called an abelian (commutative) group if $a*b = b*a$, $\forall a,b \in G$.

Order of a group : The number of elements in a group G is called the order of the group and is denoted by $O(G)$ or $|G|$

Ex 1) The set of all integers Z is not a group under multiplication i.e $(Z, \cdot)$ is not a group because there is multiplicative inverse in G. But $(Z, \cdot)$ is a monoid and hence a semigroup.

2) The set of all rational numbers under the operation of multiplication is not a group but it is a group under addition, i.e $(Q, +)$ is a group.

3) $(\mathbb{R}, +)$ is an abelian group under addition, where $\mathbb{R}$ is set of all real numbers.

pb) Show that the set of all cube roots of unity forms an abelian group with respect to the binary operation of multiplication.

Sol. Let G be the set of all cube roots of unity

i.e $G = \{1, \omega, \omega^2\}$

Construct the multiplication table

$\cdot$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

i) Since all the elements in the table are the elements of G, G is closed under multiplication.

ii) Since the product of complex numbers satisfies associative property, then $\cdot$ is associative in G.

iii) there exists identity element $1 \in G$.

iv) The inverse of 1 is 1 and the inverse of ω is ω^2 and the inverse of ω^2 is ω. i.e every element in G has inverse.

v) clearly commutative holds in G.

Hence $(G, \cdot)$ is abelian group

6b) Let $M_2(R)$ be the set of all matrices of the form $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ where a, b, c, d are real numbers. Show that $(M_2(R), +)$ is a group, where $+$ denotes the matrix addition.

Sol. Let $M_2(R) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{R} \right\}$

Clearly $M_2(R)$ is non-empty, since $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in M_2(R)$

i) Closure property:

Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, $B = \begin{bmatrix} e & f \\ g & h \end{bmatrix}$ be any two elements of $M_2(R)$.

Then $A + B = \begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} e & f \\ g & h \end{bmatrix}$

$= \begin{bmatrix} a+e & b+f \\ c+g & d+h \end{bmatrix} \in M_2(R)$

$\therefore$ $+$ is binary operation on $M_2(R)$.

ii) Associative property

Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, $B = \begin{bmatrix} e & f \\ g & h \end{bmatrix}$ $C = \begin{bmatrix} i & j \\ k & l \end{bmatrix}$.

be any three elements of $M_2(R)$

Then $A+(B+C) = \begin{bmatrix} a & b \\ c & d \end{bmatrix} + \left[\begin{bmatrix} e & f \\ g & h \end{bmatrix} + \begin{bmatrix} i & j \\ k & l \end{bmatrix}\right]$

$$= \begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} e+i & f+j \\ g+k & h+l \end{bmatrix}$$

$$= \begin{bmatrix} a+(e+i) & b+(f+j) \\ c+(g+k) & d+(h+l) \end{bmatrix}$$

$$= \begin{bmatrix} (a+e)+i & (b+f)+j \\ (c+g)+k & (d+h)+l \end{bmatrix}$$

$$= \begin{bmatrix} a+e & b+f \\ c+g & d+h \end{bmatrix} + \begin{bmatrix} i & j \\ k & l \end{bmatrix}$$

$$= \left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} e & f \\ g & h \end{bmatrix}\right) + \begin{bmatrix} i & j \\ k & l \end{bmatrix}$$

$$= (A+B)+C$$

$\therefore$ $+$ is associative in $M_2(R)$.

iii) <u>Existence of identity</u>

we have $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in M_2(R)$

and $\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$

$\therefore$ $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ is the identity element in $M_2(R)$.

iv) Existence of inverse

Let $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(R)$, then $\begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix} \in M_2(R)$

and $\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

$\therefore$ The inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}$

Hence every element in $M_2(R)$ has an additive inverse.

Thus $(M_2(R), +)$ is a group.

pb) Show that $(\mathbb{Z}, *)$ is a group where $*$ is defined by $a * b = a + b + 1$

Sol. i) closure property

Let $a, b \in \mathbb{Z}$. Then $a + b + 1 \in \mathbb{Z}$

$\therefore a * b \in \mathbb{Z}$ for all $a, b \in \mathbb{Z}$

Hence $*$ is a binary operation on $\mathbb{Z}$.

ii) Associative property

Let $a, b, c \in \mathbb{Z}$

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

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

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

$\therefore a*(b*c) = (a*b)*c, \ \forall a,b,c \in \mathbb{Z}.$

Hence $*$ is associative in $\mathbb{Z}$.

iii) <u>Existence of identity</u>

Let e the identity element in $\mathbb{Z}$

Then $a*e = a$ for any $a \in \mathbb{Z}$

$\Rightarrow a+e+1 = a$

$\Rightarrow e+1 = 0$

$\Rightarrow e = -1 \in \mathbb{Z}$

and $a*e = a*(-1) = a+(-1)+1 = a$

$e*a = (-1)*a = (-1)+a+1 = a$

$\therefore a*e = e*a = a, \ \forall a \in \mathbb{Z}$

Hence $e=-1$ is the identity element in $\mathbb{Z}$

iv) <u>Existence of inverse</u>

Let b the inverse of a in $\mathbb{Z}$

$\therefore a*b = b*a = e = -1$

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

$\Rightarrow b = -2-a$

Also $a * b = a*(-2-a) = a+(-2-a)+1 = -1 = e$

$b*a = (-2-a)*a = (-2-a)+a+1 = -1 = e$

$\therefore$ $-2-a$ is the inverse of a in $\mathbb{Z}$.

Hence every element in $\mathbb{Z}$ has inverse.

Thus $(\mathbb{Z}, *)$ is a group.

Pb) Show that the set G of all nth roots of unity forms an abelian group under usual multiplication of complex numbers.

Sol. Let z be an nth root of unity

Then $z^n = 1 = \cos 2k\pi + i\sin 2k\pi$

where k is an integer.

$$\therefore z = (\cos 2k\pi + i\sin 2k\pi)^{\frac{1}{n}}$$

$$= \cos \frac{2k\pi}{n} + i\sin \frac{2k\pi}{n}$$

$\therefore$ There are n distinct nth roots of unity, $\cos \frac{2k\pi}{n} + i\sin \frac{2k\pi}{n}$, for $k = 0, 1, 2 \ldots (n-1)$.

Let $G = \left\{ \cos \frac{2k\pi}{n} + i\sin \frac{2k\pi}{n},\ k = 0, 1, 2 \ldots n-1 \right\}$

i) Closure property : Let $a, b \in G$

$\Rightarrow a, b$ are nth roots of unity

$\Rightarrow a^n = 1,\ b^n = 1$

$\Rightarrow a^n b^n = 1 \Rightarrow (ab)^n = 1$

$\Rightarrow ab$ is also an nth root of unity

$\Rightarrow ab \in G$.

ii) Associative and commutative properties are true. Since multiplication of complex numbers is associative and commutative.

iii) Also $1 \in G$ and $a \cdot 1 = 1 \cdot a = a \ \forall a \in G$.

$\therefore 1$ is the identity element in G

iv) Let $a \in G$, then $\left(\frac{1}{a}\right)^n = \frac{1}{a^n} = \frac{1}{1} = 1$

$\Rightarrow \left(\frac{1}{a}\right)^n \in G$.

Also $a \cdot \frac{1}{a} = \frac{1}{a} \cdot a = 1$

i.e $\frac{1}{a}$ is the inverse of a

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

Properties of groups

1. The identity element of a group is unique
2. Every element in a group G has unique inverse in G.
3. If G is a group then $(a^{-1})^{-1} = a, \forall a \in G$.
4. The identity element has its own inverse i.e $e^{-1} = e$
5. If G is a group then $(a*b)^{-1} = b^{-1}*a^{-1}$, forall $a, b \in G$.
6. cancellation laws hold in any group.
7. A group cannot have any idempotent element except the identity element (i.e $e^2 = e$)
8. If every element of a group G has its own iverse then G is abelian.

proof:- Let $(G,*)$ be a group

Suppose $x^{-1} = x \;\forall x \in G$.

Let $a, b \in G$

Then $a*b \in G$ (by closure property)

Since every element in G has its own inverse, we have $a^{-1} = a$, $b^{-1} = b$ and $(ab)^{-1} = ab$

Now $a*b = (a*b)^{-1}$

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

$= b * a$

Hence G is abelian group.

Subgroup :

A nonempty subset H of a group G is said to be a subgroup of G if H is itself a group under the same operation defined on G with the same identity element.

In other words, a non-empty subset H of a group $(G,*)$ is said to be a subgroup of G if the following conditions are satisfied.

i) For $a, b \in H$, $a*b \in H$

ii) $e \in H$, where e is the identity in G

iii) For any $a \in H$, $a^{-1} \in H$.

Definition :- Any group $(G,*)$ and $(\{e\},*)$ are called improper (trivial) subgroups of G and all the other subgroups of G are called proper (nontrivial) subgroups of G.

Theorem:- The necessary and sufficient condition for a nonempty subset H of a group G to be a subgroup of G is

$a \in H, b \in H \Rightarrow a * b^{-1} \in H$

proof:- The condition is necessary :

Suppose H is a nonempty subset of group G.

Let H be a subgroup of G.

we have to prove that $a, b \in H \Rightarrow a * b^{-1} \in H$.

Since H is a group, we have $b^{-1} \in H$

Now $a \in H, b^{-1} \in H \Rightarrow a * b^{-1} \in H$ (by closure property in H)

$\therefore a, b \in H \Rightarrow a * b^{-1} \in H$

The condition is sufficient

Suppose $a, b \in H \Rightarrow a * b^{-1} \in H$

we need to prove that H is a subgroup of G

i) Let $a \in H$.

Now $a \in H, a \in H \Rightarrow a * a^{-1} \in H$

$\Rightarrow e \in H$

$\therefore$ e is the identity element in G.

ii) Let $a \in H$.

Now $a \in H, e \in H \Rightarrow e * a^{-1} \in H$

$\Rightarrow a^{-1} \in H$

$\therefore$ every element in H has inverse in H.

iii) Let $a, b \in H$

Then $b^{-1} \in H$

Now $a, b^{-1} \in H \Rightarrow a * (b^{-1})^{-1} \in H$

$\Rightarrow a * b \in H$

$\therefore$ closure property is satisfied in H.

iv) Since all the elements of H are the elements of G, associative property holds in H.

Hence H is a group

Thus H is a subgroup of G.

ex:- i) $(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{R}, +)$

ii) The set of all even integers is a subgroup of $(\mathbb{Z}, +)$

iii) The set of all nonnegative integers is not a subgroup of $(\mathbb{Z}, +)$, since except 0, no other element has additive inverse.

Homomorphism of groups

Let $(G, *)$ and (H, Δ) be any two groups.
A mapping $f: G \rightarrow H$ is said to be a homomorphism if $f(a * b) = f(a) \Delta f(b)$, for all $a, b \in G$.

Theorem:- If f is a homomorphism of a group G into a group G' then

i) group homomorphism preserves identities i.e $f(e) = e'$, where e is the identity element in G and e' is the identity element in G'.

ii) $f(a) = [f(a)]^{-1}$ for all $a \in G$

iii) if H is a subgroup of G then $f(H) = \{f(h) / h \in H\}$ is a subgroup of G'.

proof:- Let $f: (G, *) \rightarrow (G', \Delta)$ be a group homomorphism. i.e $f(a * b) = f(a) \Delta f(b), \forall a, b \in G$.

i) Let e and e' be the identity elements in G and G' respectively.

Now, let $a \in G$

Then $f(a) \in G'$

Now $f(a) \Delta e' = f(a) = f(a * e) = f(a) \Delta f(e)$

$\Rightarrow f(a) \Delta e' = f(a) \Delta f(e)$

$\Rightarrow f(e) = e'$ (by left cancellation law)

ii) Let $a \in G$.

Then $a^{-1} \in G$ and $a * a^{-1} = a^{-1} * a = e$

Now $f(a * a^{-1}) = f(e)$

$\Rightarrow f(a) * f(a^{-1}) = e'$

$\Rightarrow [f(a)]^{-1} = f(a^{-1})$

iii) Let $f(G) = \{ f(x) / x \in G \}$

clearly $f(G)$ is nonempty subset of G'

Let $a', b' \in f(G)$

Then $a' = f(a)$ and $b'^{-1} = f(b)$ forme $a, b \in G$.

Now $a' \Delta (b')^{-1} = f(a) \Delta [f(b)]^{-1}$

$= f(a) \Delta f(b^{-1})$

$= f(a * b^{-1}) \in f(G)$

$(\because a * b^{-1} \in G.$

$\therefore a', b' \in \in f(G) \Rightarrow a' \Delta (b')^{-1} \in f(G)$

Hence $f(G)$ is a subgroup of G'.

Theorem : Let $f : G \to G'$ be a group homomorphism and K be a subgroup of G'. Then $f^{-1}(K)$ is a subgroup of G.

proof :- Let $f : G \to G'$ be a group homomorphism. and let K be a subgroup of G'.

$$f^{-1}(K) = \{ x = f^{-1}(y) \in G \,/\, f(x) = y \in K \}$$

clearly $f^{-1}(K)$ is nonempty subset of G.

$(\because f(e) = e' \in K$

$\Rightarrow e \in f^{-1}(K))$

Let $x_1, x_2 \in f^{-1}(K)$

Then $f(x_1), f(x_2) \in K$

$\Rightarrow f(x_1) * [f(x_2)]^{-1} \in K$ (since K is a subgroup)

$\Rightarrow f(x_1) * f(x_2^{-1}) \in K$

$\Rightarrow f(x_1 * x_2^{-1}) \in K$ $(\because f$ is a homomorphism

$\Rightarrow x_1 * x_2^{-1} \in f^{-1}(K)$

$\therefore x_1, x_2 \in f^{-1}(K) \Rightarrow x_1 * x_2^{-1} \in f^{-1}(K)$

Hence $f^{-1}(K)$ is a subgroup of G.

Scanned with CamScanner

Kernal of a homomorphism

Let $f : G \to G'$ be a group homomorphism. The set of all elements of G that are mapped into e', the identity of G', is called the kernal of f and is denoted by Ker(f)

i.e $\ker(f) = \{ x \in G \,/\, f(x) = e',\ e' \text{ is the identity element in } G' \}$

Theorem The Kernal of a homomorphism from a group $(G, *)$ to the group (G', Δ) is a subgroup of $(G, *)$

Sol. Let $f : G \to G'$ be a homomorphism.

$\text{Ker}(f) = \{ x \in G \,/\, f(x) = e', \text{ the identity of } G \}$

Since $f(e) = e'$, we have $e \in \text{Ker}(f)$

$\therefore$ Ker(f) is a nonempty subset of G.

Let $a, b \in \text{Ker}(f)$. Then $f(a) = e'$, $f(b) = e'$

Now $f(a * b^{-1}) = f(a) \,\Delta\, f(b^{-1})$

$= f(a) \,\Delta\, [f(b)]^{-1}$ ($\because f$ is a homomorphism)

$= e' \,\Delta\, e' = e'$

$\Rightarrow a * b^{-1} \in \text{Ker}(f)$

Hence Ker(f) is a subgroup of G.

Isomorphism

A mapping f from a group $(G, *)$ to a group (G', Δ) is said to be an isomorphism if

i) f is a homomorphism ii) f is one-one

iii) f is onto

i.e A bijective homorphism is called an isomorphism.

Cyclic group

A group $(G, *)$ is said to be a cyclic if there exists $a \in G$ such that every element $x \in G$ can be written as $x = a^n$ for some integer n. The element a is called the generator of the cyclic group G.

The cyclic group generated by a is denoted by $G = \langle a \rangle$ or $G = (a)$

ex:-
- $(\mathbb{Z}, +)$ is a cyclic group with 1 as a generator
- $(\mathbb{Z}_n, +_n)$ is a cyclic group with 1 as a generator.

Theorem Every cyclic group is abelian.

Sol. Let $(G, *)$ be a cyclic group.

Then $G = \langle a \rangle$ for some $a \in G$.

Let $x, y \in G$

Then $x = a^m$, $y = a^n$ for some integers m, n

Now $x * y = a^m * a^n = a^{m+n} = a^{n+m} = a^n * a^m$
$= y * x$

$\therefore$ $x * y = y * x$, $\forall x, y \in G$.

Hence $(G, *)$ is abelian.

Theorem If a is generator of a cyclic group G then a^{-1} is also a generator of G.

proof:- Let G be a cyclic group generated by a. Then $G = \langle a \rangle$

Let $x \in G$. Then $x = a^r$ for some integer r

Now $x = a^r = (a^{-1})^{-r}$, $-r$ is also an integer.

$\therefore$ each element of G is generated by a^{-1}.

Hence a^{-1} is also a generator of G.

Note:- Every subgroup of cyclic group is cyclic.

Pb) Show that the group $G = \{1, -1, i, -i\}$ is cyclic and find its generators:

Sol. we have $G = \{1, -1, i, -i\}$ is a group under the operation of multiplication.

Now $1 = (i)^4$, $-1 = i^2$

$i = (i)^1$, $-i = (i)^3$

That is, every element G can be expressed as i^n for some integer n.

Hence G is a cyclic group generated by i.

Since i is generator of G, $(i)^{-1}$ is also a generator of G.

we have $(i)^{-1} = \frac{1}{i} = -i$

Hence G is cyclic group and its generators are $i, -i$.