4.1 Semigroups and Monoids

Define Algebraic System:

- A non – empty set G together with one or more n – ary operations say $*$ (binary) is called an Algebraic System or Algebraic Structure or Algebra.
- We denoted it by $[G, *]$.
- Note: $+, -, \cdot, \times, *, \cup, \cap$ etc are some of binary operations.

Properties of Binary Operations

Let the binary operation be $* : G \times G \rightarrow G$.

Then we have the following properties:

Closure Property:

a $*$ b = $x \in$ G, for all $a, b \in G$.

Commutativity Property:

$$a * b = b * a, \text{ for all } a, b \in G.$$

Associativity:

$$(a * b) * c = a * (b * c), \text{ for all } a, b, c \in G.$$

Identity Element:

$$a * e = e * a = a, \text{ for all } a \in G.$$

'e' is called the identity element.

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}.

Left Cancellation law:

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

Right Cancellation law:

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

If the binary operation defined on G is + and X, then we have the following table.

For all a, b, c ε G	**(G, +)**	**(G,×)**
Commutativity	a + b = b + a	a× b = b × a
Associativity	(a + b) + c = a + (b + c)	(a× b)× c =a × (b × c)
Identity element	a + 0 = 0 + a = a (0 → identity)	a× 1 = 1 × a = a (1 →identity)
Inverse element	a + (-a) = 0 (-a→ additive inverse)	a$\times \frac{1}{a} = \frac{1}{a} \times$ a = 1 ($\frac{1}{a}$ → multiplicative inverse)

NOTATIONS:

- Z - the set of all integers.
- Q - the set of all rational numbers.
- R - the set of all real numbers.
- C - the set of all complex numbers.
- R^+ - the set of all positive real numbers.
- Q^+ - the set of all positive rational numbers.

Semigroups and Monoids:

Define semigroup

If a non – empty set S together with the binary operation $*$ satisfying the following properties

Closure Property:

$a * b = b * a$, for all $a, b \, \varepsilon \, S$.

Associativity:

$$(a * b) * c = a * (b * c), \text{ for all } a, b, c \, \varepsilon \, S.$$

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

Monoid:

A semigroup $(S,*)$ with an identity element with respect to $*$ is called Monoid. It is denoted by $(M,*)$.

In other words, a non – empty set 'M' with respect to $*$ is said to be a monoid, if $*$ satisfies the following properties

For $a, b \in M$

Closure Property:

$a * b = b * a$, for all a, b ε M.

Associativity:

$(a * b) * c = a * (b * c)$, for all a, b, c ε M.

Identity Element:

$a * e = e * a = a$, for all a ε M.

'e' is called the identity element.

4.2 Groups

Define Group

A non-empty set G together with the binary operation $*$,i.e., $(G,*)$ is called a group if $*$ satisfies the following conditions.

(i) Closure Property: $a * b = x \epsilon G$, for all $a, b \varepsilon G$.

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

(iii) Identity: There exists an element $e \varepsilon G$ called the identity element such that $a * e = e * a = a$, for all a ε G.

(iv) Inverse: There exists an element $a^{-1} \varepsilon$ G called the inverse of 'a' such that

$a * a^{-1} = a^{-1} * a = a$, for all a ε G.

Define Abelian Group

In a group (G, $*$), if a $*$ b = b $*$a, for all a, b ε G, then the group (G, $*$) is called an Abelian group.

Example:$(Z, +)$ is an Abelian group.

Define an 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).

It is denoted by O(G) or $|G|$.

Define Finite and Infinite Group

(i) If O(G) is finite, then G is said to be a finite group.

(ii) If O(G) is infinite, then G is said to be a infinite group.

Theorems on Abelian Groups

Theorem: 1

If every element of a group G has its own inverse, then G is abelian.

(OR)

For any group G, if $a^2 = e$ with $a \neq e$, then G is abelian.

Proof:

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

For a, b ε G, we have a $*$ b ϵ G

Given $a = a^{-1}$ and $b = b^{-1}$

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

$= b^{-1} * a^{-1} = b * a (\because a = a^{-1} \& b = b^{-1})$

$\Longrightarrow a * b = b * a$

$\therefore G$ is abelian.

Hence the proof.

Theorem: 2

Prove that a group (G, $*$) is abelian iff $(a * b)^2 = a^2 * b^2$ for all $a, b \epsilon G$

Proof:

Assume that G is abelian.

$a * b = b * a$, a , b ϵ G $\rightarrow (1)$

Let $a^2 * b^2 = (a * a) * (b * b)$

$= a * [a * (b * b)] \because (*$ is Associative)

$= a * [(a * b) * b] \because (*$ is Associative)

$= a * [(b * a) * b] \because (By\ (1))$

$= (a * b) * (a * b) \because (*$ is Associative)

$= (a * b)^2$

$\therefore (a * b)^2 = a^2 * b^2$

Conversely assume that $(a * b)^2 = a^2 * b^2$

To prove G is abelian.

$\Longrightarrow (a * b) * (a * b) = (a * a) * (b * b)$

$\Longrightarrow a * [b * (a * b)] = a * [a * (b * b)]$ $\because (*$ is Associative)

$\Longrightarrow b * (a * b) = a * (b * b)$ (Left Cancellation law)

$\Longrightarrow (b * a) * b = (a * b) * b$ (Right Cancellation law)

$\Longrightarrow (b * a) = (a * b)$

$\therefore$ G is abelian.

Hence the proof.

Theorem: 3

If (G, ∗) is an abelian group, then for all a, b ε G then $(a * b)^n = a^n * b^n$

Proof:

Let (G, ∗) be an abelian group and a, b εG. Then for all n ε Z,

$$(a * b)^n = a^n * b^n$$

Case (i) Let $n = 0$

Then $a^0 = e,\ b^0 = e,\ (a * b)^0 = e$

$$\therefore (a * b)^0 = a^0 * b^0$$

Hence the result is true when n = 0

Case (ii) let $n = 1$

Let n be a positive integer

$$(a * b)^1 = a^1 * b^1$$

The result is true for $n = 1$

Assume that it is true for $n = k$, so that

$$(a * b)^k = a^k * b^k \rightarrow (1)$$

To prove it is true for $n = k + 1$

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

$$= a^k * b^k * a * b$$

$$= a^k * (b^k * a) * b$$

$$= a^k * (a * b^k) * b$$

$$= (a^k * a) * (b * b^k)$$

$$= a^{k+1} * b^{k+1}$$

Hence the result is true for $n = k + 1$.

Hence by induction, the result is true for positive integer values of n.

Hence the proof.

Problems on Groups:

1. Show that set $\mathbb{R}$ with the usual addition as a binary operation is an abelian group.

Solution: Let $a, b, c \in \mathbb{R}$

(i) Closure property: Clearly $a + b \in \mathbb{R}$

(ii) Associative property: $a + (b + c) = (a + b) + c$

(iii) Identity element: Since $0 \in \mathbb{R}$, we have

$\Rightarrow a + 0 = 0 + a = a$

(iv) Additive Inverse: For $a \in \mathbb{R}$, we have $-a \in \mathbb{R}$, such that

$$a + (-a) = 0 = (-a) + a$$

∴ The inverse of a is –a .

(v) Commutative property: $a + b = b + a \; for \; all \; a, b \in \mathbb{R}$

∴ $(\mathbb{R}, +)$ is an abelian group.

Since $\mathbb{R}$ contains infinite number of elements, $(\mathbb{R}, +)$ is an infinite abelian group

2. Show that $(\mathbb{R} - \{1\}, *)$ is an abelian group, where $*$ is defned by

$a * b = a + b + ab$, for all $a, b \in \mathbb{R}$.

Solution:

Here $\mathbb{R} - \{1\}$ means the set or real numbers except 1.

(i) Closure property:

Clearly $a * b = a + b + ab \in (\mathbb{R} - \{1\})$ $\quad [a \neq -1, b \neq -1]$

(ii) Associative property:

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

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

$$= a + b + ab + c + ac + bc + abc \qquad \text{....(A)}$$

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

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

$= a + b + c + bc + ab + ac + abc$ ….. (B)

From (A) and (B), we get

$(a * b) * c = a * (b * c),$ for all $a, b \in (\mathbb{R} - \{1\})$

(iii) Identity element:

Let 'e' be the identity element.

Then, $a * e = a$

$\Rightarrow a + e + ae = a$

$\Rightarrow e(1 + a) = 0$

$\Rightarrow e = 0$

Here '0' is the identity element and $0 \in (\mathbb{R} - \{1\})$

(iv) Inverse:

Let the inverse of a be a^{-1}

Then, $a * a^{-1} = 0$ (identity)

$\Rightarrow a + a^{-1} + aa^{-1} = 0$

$\Rightarrow a^{-1}(1 + a) = -a$

$\Rightarrow a^{-1} = -\frac{a}{1+a} \in (\mathbb{R} - \{1\})$

$\therefore$ Inverse element is $-\frac{a}{1+a}$

(v) Commutative:

$\Rightarrow a * b = a + b + ab$

$= b + a + ba$

$= bb * a$

$\therefore a * b = b * a,$ for all $a, b \in (\mathbb{R} - \{1\})$

$\therefore (\mathbb{R} - \{1\})$ is an abelian group.

3. Show that $(\mathbb{Q}^{+}, *)$ is an abelian group where $*$ is defined by

$$a * b = \frac{ab}{2}, for\ all\ a, b \in \mathbb{Q}^{+}$$

Solution:

Let $\mathbb{Q}^{+}$ be the set of all positive rational numbers.

(i) Closure property:

Clearly $a * b = \frac{ab}{2} \in \mathbb{Q}^+$

(ii) Associative property:

$$(a * b) * c = \frac{ab}{2} * c = \frac{\frac{abc}{2}}{2} = \frac{abc}{4} \quad ...(1)$$

$$a * (b * c) = a * \frac{bc}{2} = \frac{\frac{abc}{2}}{2} = \frac{abc}{4} \quad ...(2)$$

From (1) and (2) we get,

$$(a * b) * c = a * (b * c), for\ all\ a, b \in \mathbb{Q}^+$$

(iii) Identity element:

Let 'e' be the identity element.

Then, $a * e = a$

$\Rightarrow \frac{ae}{2} = a \quad \Rightarrow e = 2$

Here '2' is the identity element and $2 \in \mathbb{Q}^+$

iv) Inverse:

Let the inverse of a be a^{-1}

Then, $a * a^{-1} = 2$ (identity)

$$\Rightarrow \frac{aa^{-1}}{2} = 2$$

$$\Rightarrow a^{-1} = \frac{4}{a}$$

$\therefore$ Inverse element is $\frac{4}{a} \in \mathbb{Q}^+$

v) Commutative:

Now $a * b = \frac{ab}{2}$

$\therefore b * a = \frac{ba}{2} = \frac{ab}{2}$

$\therefore a * b = b * a,$ for all $a, b \in \mathbb{Q}^+$

Hence $(\mathbb{Q}^+, *)$ is an abelian group.

4. Let $G = \left\{\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}\right\}$ Show that G is a group under the operation of matrix multiplication.

Solution:

Let I = $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, A = $\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$, B = $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, C = $\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$

$\therefore G = \{I, A, B, C\}$. Since it is finite set we shall form Cayley table and verify the axioms of a Group.

I is the identity element.

$$A \cdot I = I \cdot A = A, B \cdot I = I \cdot B = B,\ C \cdot I = I \cdot C = C$$

$$A^2 = A \cdot A = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

$$AB = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = C$$

$$AC = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = B$$

$$B^2 = B \cdot B = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

$$C^2 = C \cdot C = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

$$BC = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} = A$$

$$CA = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = B$$

Similarly BA = C, CB = A

Cayley table:

$\cdot$	I	A	B	C
I	I	A	B	C

A	A	I	C	B
B	B	C	I	A
C	C	B	A	I

(i) Closure property:

The first line of the table contains only all the elements of G. So G is closed under matrix multiplication.

(ii) Associative property:

Since matrix multiplication is associative it is true for G also. So Associative is satisfied.

(iii) Identity element:

I is the identity element.

(iv) Inverse:

Inverse of A is A, B is B and C is C.

So $(G, \cdot)$ is a group under matrix multiplication.

5. Check whether $H_1 = \{0, 5, 10\}$ and $H_2 = \{0, 4, 8, 12\}$ are subgroups of Z_{15} with respect to $+_{15}$.

Solution:

The addition tables (mod 15) for the sets H_1 and H_2 is given below:

For H_1

$+_{15}$	0	5	10
0	0	5	10
5	5	10	0
10	10	0	5

For H_2

$+_{15}$	0	4	8	12
0	0	4	8	12
4	4	8	12	1
8	8	12	1	5
12	12	1	5	9

Here all the entries in the addition table for H_1 are the elements of H_1.

$\therefore H_1$ is a subgroup of Z_{15}.

Also all the entries in the addition table for H_2 are not the elements of H_2.

$\therefore H_2$ is not closed under addition.

$\therefore H_2$ is not a subgroup of Z_{15}.

4.3 Subgroups

Define Subgroups

Let (G, $*$) be a group. Then (H, $*$) is said to be subgroup of (G, $*$) if $H \subseteq G$ and (H, $*$) itself is a group under the operation $*$

i.e., (H, $*$) is said to be a subgroup of (G, $*$) if

- $e \varepsilon H$, where e is the identity in G.
- For any $a \varepsilon H$, $a^{-1} \varepsilon H$
- For $a, b \varepsilon H$, $a * b \varepsilon H$

Define Trivial and Proper Subgroups

- $(\{e\}, *)$ and $(G, *)$ are trivial subgroups of $(G, *)$.
- All other subgroups of $(\boldsymbol{G}, *)$ are called proper subgroups.

Examples of Subgroups:

- (Z, +) is a Subgroup of (Q, +)
- (Q, +) is a Subgroup of (R, +)
- (R, +) is a Subgroup of(C,+)

Example of Subgroups

Find all the subgroups $(z_{12}, +_{12})$

Solution:

$z_{12} = \{0, 1, 2, 3, 4, 5, 6, 7,8,9, 10, 11\}$

- Let $S_1 = \{0, 6\}$
- $S_2 = \{0, 4,8\}$
- $S_3 = \{0, 3, 6, 9\}$
- $S_4 = \{0, 2, 4, 6, 8\}$
- S_1, S_2, S_3, S_4 are proper subgroups of $(z_{12}, +_{12})$
- $(\{0\}, +_{12})$ and $(z_{12}, +_{12})$ are its trivial subgroup

Theorems on Subgroups:

Theorem: 1

State and prove the necessary and sufficient condition for a subset of a group to be subgroup.

Statement:

Let (G, $*$) be a group. H is a nonempty subset of G, then H is a subgroup of G

if and only if whenever $\boldsymbol{a}, \boldsymbol{b} \in \boldsymbol{H} \Rightarrow \boldsymbol{a} * \boldsymbol{b}^{-1} \in \boldsymbol{H}$ for all

$\boldsymbol{a}, \boldsymbol{b} \in \boldsymbol{H}$

(**Definition:** (G, $*$) be a group, H nonempty subset of G. H is a subgroup of G if H itself is a group under the same binary operation $*$)

Proof:

Necessary Part

Let (G, $*$) be a group. H is a nonempty subset of G.

Assume that H is a subgroup of G.

By definition, (H, $*$) is a group.

So $a, b \in H \Rightarrow b^{-1} \in H$ by inverse property

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

Sufficient Part

Let (G, $*$) be a group. H is a nonempty subset of G.

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

Claim: H is a subgroup of

G i.e., (H, $*$) is a group.

H is nonempty so let $a \in H$

(iii) Identity

Now $a, a \in H$ by (1)

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

i.e., $e \in H$

Identity exists

(iv)Inverse

Let a $\in H$. Now by previous step $e \in H$

Now $e, a \in H$ by (1)

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

$\Rightarrow e \in H$

Hence Inverse exists.

(i) Closure

Let $a, b \in H$ by previous step $b^{-1} \in H$

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

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

$\Rightarrow a * b \in H$

Closure is verified.

(ii) Associative

$a, b, c \in H$, $\boldsymbol{H} \subseteq \boldsymbol{G}$, $a, b, c \in G$

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

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

Associative is verified.

(H, $*$) be a group.

Hence H is a subgroup of G.

Hence the proof.

Theorem: 2

Prove that intersection of two subgroups of a group (G, $*$) is a subgroup of (G, $*$). Also, prove that union of subgroups need not be a group.

Proof:

Let (G, $*$) be a group. H and K are non – empty subgroups of (G, $*$). Both H and K satisfying the following necessary conditions

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

Let $a, b \in K \Rightarrow a * b^{-1} \in K \qquad ...(1)$

Consider the subset $H \cap K$ of G

(i) Since H is a subgroup of G, $e \in H$

Since K is a subgroup of G, $e \in K$

$\therefore e \in H \cap K$

so, $H \cap K$ is a non – empty subset of G.

(ii) Let a, b $\in H \cap K$

By Sufficient condition for aSubgroup

We need to prove $a * b^{-1} \in H \cap K$

$a, b \in H$ and $a, b \in K$

By (1) $a * b^{-1} \in H \cap K$

$\therefore H \cap K$ is a subgroup of (G, $*$)

Hence the proof.

Now we are going to Prove that Union of two Subgroups of a group need not be a Subgroup.

Let us prove the above fact by giving counter examples

Consider G = set of integers under addition $(Z, +)$

$= \{. . . , -3, -2, -1, 0, 1, 2, 3, . . . \}$

- H = 2Z = {. . . , − 6, − 4, − 2, 0, 2, 4, 6, . . . }
- K = 3Z = {. . . , − 9, − 6, − 3, 0, 3, 6, 9, . . . }

H and K are subgroups of $(Z, +)$

$H \cup K$ ={. . . , − 9, − 6, − 4, − 3, − 2, 0 , 2, 3 , 4, 6, 9, . . . }

$H \cup K$ is not closed under addition.

As $2,3 \in H \cup K$ but $2 + 3 = 5 \notin H \cup K$

So $H \cup K$ is not a subgroup of $(Z, +)$.

Hence the proof.

Cyclic Group:

Define Cyclic Groups

A group (G, ∗) is said to be cyclic if there exists an element $a \in G$ such that every element of G can be written as some power of "a".

i.e., a^n *for some integer n*.

G is said to be generated by "a" (or) "a" is a generator ofG.

We write $G = \prec a \succ$

Examples:

The set of complex numbers $\{1, -1, i, -i\}$ under multiplication operation is a cyclic group.

There are two generators – i and i as $i^1 = 1$, $i^2 = -1$, $i^3 = -i$, $i^4 = 1$ and also

$(-i)^1 = -i$, $(-i)^2 = -1$, $(-i)^3 = i$, $(-i)^4 = 1$ which covers all the elements of the group.

Hence it is a Cyclic Group.

However -1 is not a generator.

Theorem: 1

Every Subgroup of a Cyclic group is Cyclic.

Proof:

Let H be a cyclic group generated by an element $a \in G$.

∴ Every element in G can be expressed as a power of the element "a".

Let H be a subgroup of G.

If $H = \{e\}$, then H is a subgroup of G and it is cyclic.

∴ The result is trivial.

Suppose $H \neq \{e\}$ then there exists an element $x \in H$ with $x \neq e$.

$\therefore x = a^k$ for some integer k.

Let m be the least positive integer such that $a^m \epsilon H$.

Let $b \epsilon H$ then $b = a^n$ for some integer n.

Let $n = mq + r$ where $0 \leq r < m$

$\Rightarrow b = a^n$

$\Rightarrow b = a^{mq+r}$

$\Rightarrow b = a^{mq} * a^r$

$\Rightarrow b = (a^m)^q * a^r$

$\Rightarrow a^r = b/(a^m)^q$

$\Rightarrow a^r = b * (a^m)^{-q}$

Now $b \epsilon H$, $(a^m)^q \epsilon H$ and H is closed in $*$.

$\therefore$ we have $b * (a^m)^{-q} \epsilon H$

This shows that there exists an integer "r" such that $o \leq r < m$ with $a^r \epsilon H$.

Since m is the least positive integer for which $a^m \epsilon H$, $a^r \epsilon H$ with $o \leq r < m$ is not possible.

$\therefore r = 0$ so $b = a^{mq}$

$\Rightarrow b = (a^m)^q$

Every element $b \in H$ is expressed as a power of a^m.

i.e., H is generated by the element $a^m \in H$

H is a cyclic group generated by a^m.

Hence, every subgroup of a cyclic group is

cyclic.

Hence the proof.

4.4 Cosets

Define Left Coset and Right Coset of H in G.

Let $(H, *)$ be a subgroup of $(G, *)$.

For any $a \epsilon G$, the left coset of H, denoted by $a * H$, is the set

$a * H = \{a * h: h \epsilon H\}$ for all $a \epsilon G$

For any $a \epsilon G$, the right coset of H, denoted by $H * a$, is the set

$H * a = \{h * a: h \epsilon H\}$ for all $a \epsilon G$

Theorem: 1

Let $(H, *)$ be a subgroup of $(G, *)$. Then any two left Cosets (right Cosets) of H of a group $(G, *)$ are either identical or disjoint and the union of distinct left Cosets of H is G (or) The set of all distinct left Cosets of the subgroup H of the group $(G, *)$ forms a partition of G.

Proof:

Let $a, b \epsilon G$

Consider the Cosets $a * H$ and $b * H$

We shall prove that $a * H = b * H$ (or) $a * H \cap b * H = \emptyset$

Suppose $a * H \cap b * H \neq \emptyset$

Let c $\epsilon\ a * H \cap b * H = \emptyset$

$\Rightarrow c\ \epsilon\ a * H$ and $c\ \epsilon\ b * H$

Let $c = a * h_1$ and $c = b * h_2$ for all $h_1, h_2\ \epsilon\ H$

$\therefore a * h_1 = b * h_2$

Take h_1^{-1} on both sides

$\Rightarrow (a * h_1) * h_1^{-1} = (b * h_2) * h_1^{-1}$

$\Rightarrow a * (h_1 * h_1^{-1}) = b * (h_2 * h_1^{-1})$

$\Rightarrow a * e = b * h_3$ where $h_3 = h_2 * h_1^{-1}$

$\Rightarrow a = b * h_3$

$\Rightarrow a \in b * h_3$

$\Rightarrow a * H \subseteq b * H$ . . . (1)

IIIrly $b * H \subseteq a * H$ . . .(2)

From (1) and (2) we have $a * H = b * H$

$\therefore$ Any two left cosets are either identical or distinct.

Each element of the left Coset $a * H$ is also an element of G.

∴ Every left coset of $a * H$ is a subset of G.

Hence $\bigcup_{a \,\epsilon\, G} a * H \subseteq G$ . . . (3)

If $a \,\epsilon\, G$, $a \,\epsilon a * H$ then $a \,\epsilon \bigcup_{a \,\epsilon\, G} a * H$

$G \subseteq \bigcup_{a \,\epsilon\, G} a * H$ . . . (4)

∴The set of all distinct left cosets of H is a partition "n' of the group G.

Hence the proof.

LAGRANGE'S THEOREM:

The order of a subgroup of a finite group is a divisor of the order of the group.

i.e., if H is a subgroup of a finite group $(G, *)$ then O(H) divides O(G).

Proof:

Let $(G, *)$ be a finite group of order n and H be a subgroup of G with order m.

$\Rightarrow O(H) = m$ & $O(G) = n$

We will prove that ${O(H)}/{O(G)}$

Since H contains m distinct elements, every left cost of H contains exactly m elements.

(Write the theorem: 1)

Let $a_1 * H, a_2 * H, \ldots, a_k * H$ be the distinct left cosets of H. Let $G = a_1 * H \cup a_2 * H \cup \ldots \cup a_k * H$

$O(G) = O(a_1 * H) + O(a_2 * H) + \ldots + O(a_k * H)$

$= O(H) + O(H) + \ldots + O(H)$

$= m + m + \ldots + m$ (n times)

$\Rightarrow n = mk$

$\Longrightarrow n/m = k$

$\Longrightarrow$ m divides n.

This means that $O(H) / O(G)$.

Hence the proof.

Normal Subgroup

A subgroup $(H,*)$ of $(G,*)$ is said to be normal subgroup of G, for $x \in G$ and for $h \in H$, if $x * h = h * x$ (or) for all $x \in G, xH = Hx$

Note:

Consider H as a subgroup of G, then the subgroup H is said to be normal, for all $x \in G, x * h * x^{-1} = H$(or) for all $x \in G, x * h * x^{-1} \in H$

Theorem: 1

Every subgroup of an abelian group is normal.

Proof:

Let $(G,*)$ be an abelian group and $(H,*)$ be a subgroup of G.

Let $x \in G$ be any element.

Then $xH = \{x * h \,/ h \in H\}$

$= \{h * x \,/ h \in H\}$ (G is abelian)

$= Hx$

Since "x" is arbitrary, $xH = Hx \;\forall\; x \in G$

Hence H is a normal subgroup of G.

Hence the proof.

Theorem: 2

Prove that intersection of two normal subgroup of $(G,*)$ is a normal subgroup of $(G,*)$.

Proof:

Let $(H,*)$ and $(K,*)$are two normal subgroup.

$\Rightarrow$ H and K are subgroups of G.

$\Rightarrow H \cap K$ is a subgroup of G. (Already proved)

To prove $(H \cap K, *)$ is a normal subgroup of $(G,*)$.

Let $h \in H \cap K$ be any element and $x \in G$ be any element.

Then $x \in G$ and$h \in H$ and $h \in K$

Since H and K are normal, $x * h * x^{-1} \in H$ . . . (1)

and $x * h * x^{-1} \in K$ . . . (2)

From (1) and (2) we get,

$$x * h * x^{-1} \in H \cap K$$

Hence $H \cap K$ is a normal subgroup of G.

Hence the proof.

4.5 Homomorphism

Let $(G, \cdot)$ and $(G',*)$ be any two groups.

A mapping $f: G \rightarrow G'$ is said to be a homomorphism, if $f(a \cdot b) = f(a) * f(b)$ for any $a, b \in G$ is called a group homomorphism.

Example: (i)

Let $f: (Z, +) \rightarrow (Z, +)$ given by $f(x) = 2x \; \forall \; x \in Z$ is a homomorphism.

For, $x, y \in Z$, $f(x + y) = 2(x + y) = 2x + 2y = f(x) + f(y)$

Example: (ii)

Let $f: (R, +) \rightarrow (R^{+}, \cdot)$ given by $f(x) = e^{x} \; \forall \; x \in R$ is a homomorphism.

For, $x \in R$, $f(x + y) = e^{x+y} = e^{x} \cdot e^{y} = f(x) \cdot f(y)$

Isomorphism:

Let $(G, \cdot)$ and $(G', *)$ be any two groups. A mapping $f: G \rightarrow G'$ is said to be isomorphism if

(i) f is one – one

(ii) f is onto

(iii) f is homomorphism

Types of Homomorphism

(i) If f is one – to – one then f is monomorphism.

(ii) (ii) If f is onto then f is epimorphism.

Theorem: 1

Homomorphism preserves identities.

Proof:

Let $a \in G$

Let f be a homomorphism from $(G, *)$ and $(G', *)$

Clearly $f(a) \in G'$

$\Rightarrow f(a) * e' = f(a)$ $(e' - identity\ in\ G')$

$= f(a * e)$ (e – identity in G)

$= f(a) * f(e)$ (f – homomorphism)

$\Rightarrow e' = f(e)$ (Left cancellation law)

Hence f preserves identities.

Hence the proof.

Theorem: 2

Homomorphism preserves inverse.

Proof:

Let $a \in G$

Since G is a group, $a^{-1} \in G$

Since G is a group $a * a^{-1} = a^{-1} * a = e$

Consider $a * a^{-1} = e$

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

$$\Rightarrow f(\,a) * f(a^{-1}) = e' \because e' = f(e), f \text{ is homomorphism}$$

$\Rightarrow f(a^{-1})$ is the inverse of $f(a) \in G'$

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

Hence f preserves inverse.

Hence the proof.

Kernal of Homomorphism

Let $f: G \rightarrow G'$ be a group homomorphism. The set of elements of G which are mapped into e' (identity in G') is called the kernel of f and it is denoted by ker(f)

$$\ker(f) = \{x \in G \,/ f(x) = e'\}$$

Theorem: 1

Kernel of a homomorphism of a group into another group is a normalsubgroup.

Proof:

Let $(G,*)$ and $(G', \oplus)$ be two groups.

$f: (G,*) \rightarrow (G', \oplus)$ is a homomorphism.

Define $\ker(f) = \{x \in G \,/ f(x) = e'\}$

Claim: Ker f is a normal subgroup of G

We know that homomorphism preserves identity.

$i.e., f(e) = e'$, so $e \in kerf$

⇒Ker f is non empty.

(ii) $a, b \in \ker f \Rightarrow a * b^{-1} \in kerf$ then ker f is a subgroup.

$a \in kerf \;\; \Rightarrow f(a) = e'$ by definition of ker f

$b \in kerf \;\; \Rightarrow f(b) = e'$ by definition of ker f

Since homomorphism preserves inverse $\Rightarrow [f(a)]^{-1} = f(a^{-1})$

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

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

$= e' \oplus e'$

$= e'$

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

Hence kerf is a subgroup of G.

(iii) Let $a \in kerf \Rightarrow f(a) = e'$ by definition of kerf

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

So $f(g^{-1} * a * g) = f(g^{-1}) \oplus f(a) \oplus f(g)$

$= [f(g)]^{-1} \oplus e' \oplus f(g)$

$= [f(g)]^{-1} \oplus f(g)$

$= e'$

Hence by definition, $g^{-1} * a * g \in kerf$

Hence kerf is a normal subgroup.

Hence the proof.

Theorem:2

Fundamental theorem of group homomorphism

Every homomorphic image of a group G is isomorphic to some quotient group of G.

(OR)

Let $f: G \rightarrow G'$ be a onto homomorphism of groups with kernel K, then $\frac{G}{K} \cong G'$

Proof:

Let f be the homomorphism $f: G \rightarrow G'$

Let G' be the homomorphic image of a group G.

Let K be the kernel of this homomorphism.

Clearly K is a normal subgroup of G.

Claim: $\frac{G}{K} \cong G'$

Define φ: $\frac{G}{K} \rightarrow G'$ by $\varphi(K * a) = f(a)$ for all $a \in G$

(i) φ is well defined.

We have $K * a = K * b$

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

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

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

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

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

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

$\Rightarrow \varphi(K * a) = \varphi(K * b)$

Hence φ is well defined.

(ii) To prove φ is one – one.

To prove $\varphi(K * a) = \varphi(K * b) \Rightarrow K * a = K * b$

We know that $\varphi(K * a) = \varphi(K * b)$

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

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

$= f(b * b^{-1})$

$= f(e)$

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

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

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

$\Rightarrow K * a * b^{-1} = K$

$\Rightarrow K * a = K * b$

Hence φ is one – one.

(iii) φ is onto.

Let $y \in G'$

Since f is onto, there exists $a \in G$ such that $f(a) = y$

Hence $\varphi(K * a) = f(a) = y$

Hence φ is onto.

(iv) φ is a homomorphism.

Now $\varphi(K * a * K * b) = \varphi(K * a * b)$

$= f(a * b)$

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

$= \varphi(K * a) * (K * b)$

Hence φ is a homomorphism.

Since φ is one – one, onto, homomorphism φ is an isomorphism between $\frac{G}{K}$ and G'.

Hence $\frac{G}{K} \cong G'$

Hence the proof.