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 $a, b \in G$

Proof:

Assume that G is abelian.

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

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

$= a * [a * (b * b)]$ ∵ (∗ is Associative)

$= a * [(a * b) * b]$ ∵ (∗ is Associative)

$= a * [(b * a) * b]$ ∵ (By (1))

$= (a * b) * (a * b)$ ∵ (∗ 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.

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

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

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

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

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

∴ 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 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 defined 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:

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

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

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

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

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

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

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

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:

·	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}.