E-Content on "Groups" (Unit-I)

By

Dr. Ashok Kumar

Assistant Professor

Department of Mathematics

Govt. College for Women, Udhampur

Introduction

In this unit, we discuss the binary operations and their properties, semigroup, and groups with lot of illustrated examples. In the end we will discuss the permutation groups and some examples.

Definition 0.1 *Let G be a non-empty set. Then a function $f : G \times G \to G$ is called a binary operations on the set G. The set G is called underlying set. Generally binary operation is denoted by o or $*$ i.e aob or $a * b$ denotes $f(a, b)$.*

Example 0.2 *Let $G = \mathbb{N}$. Then the relation $o : G \times G \to G$ defined by $aob = a + b, \forall\, a, b \in G$ is a function and hence is a binary operation.*

Example 0.3 *Let $G = \mathbb{N}$. Then the relation $o : G \times G \to G$ defined by $aob = a - b, \forall\, a, b \in G$ is not a function. Then o is not a binary operation because if we take $a = 1$ and $b = 2$, then $a - b = 1 - 2 = -1 \notin G$.*

Example 0.4 *Let $G = \mathbb{N}$. Then the relation $o : G \times G \to G$ defined by $aob = ab, \forall\, a, b \in G$ is a function and hence is a binary operation.*

Example 0.5 *Let $G = \mathbb{Z}$. Then usual addition, subtraction and multiplication of integers are binary operations on G. Moreover, the usual addition, multiplication and subtraction are also binary operations on $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$.*

Example 0.6 *Let $G = M(\mathbb{R})$ be the set of matrices over the set of real numbers. Then the relation $o : G \times G \to G$ defined by $AoB = A + B, \forall\, A, B \in G$ is not a function. Then o is not a binary operation because if we take $A = \begin{bmatrix} 1 & 2 & 3 \\ 0 & -1 & 3 \\ -1 & 2 & 4 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 2 & 3 & -1 \\ 0 & -1 & 3 & -2 \\ -1 & 2 & 4 & -2 \end{bmatrix}$, then $A + B$ cannot be even defined.*

Example 0.7 *Let $G = F$ be the set of all real valued functions. Then operations addition, subtraction, multiplication and composition of functions defined*

$$\begin{aligned} (f+g)(x) &= f(x) + g(x), \forall\, x \in \mathbb{R} \\ (f-g)(x) &= f(x) - g(x), \forall\, x \in \mathbb{R} \\ (fg)(x) &= f(x).g(x), \forall\, x \in \mathbb{R} \\ (fog)(x) &= f(g(x)), \forall\, x \in \mathbb{R} \end{aligned}$$

respectively are binary operations on G.

Definition 0.8 *A binary operation o on a set G is said to be* **commutative** *if*

$$aob = boa, \forall\, a, b \in G.$$

Definition 0.9 *A binary operation o on a set G is said to be* **associative** *if*

$$(aob)oc = ao(boc), \forall\, a, b, c \in G.$$

Definition 0.10 *Let (G, o) be a set with binary operation o. Then the element $e \in G$ is said to be left identity if $eoa = a, \forall\, a \in G$ and the element $e' \in G$ is said to be right identity if $aoe = a, \forall\, a \in G$. The element $e \in G$ is said to be an* **identity** *if $aoe = a = eoa, \forall\, a \in G$.*

Definition 0.11 *Let (G, o) be a set with binary operation o and a be any element of G. Then the element $b \in G$ is said to be* **left inverse** *of a if $boa = e$ and the element $b' \in G$ is said to be* **right inverse** *of a if $aob' = e$. The element $b \in G$ is said to be an* **inverse** *of a if $aob = e = boa$.*

Example 0.12 *Let $G = \mathbb{Z}$ be the set of integers. Then the binary operations $+, .$ addition, multiplication respectively are commutative and associative. But the binary operation $-$ difference is neither commutative nor associative.*

Definition 0.13 *A non-empty set G with a binary operation o is said to be a* **semi-group** *if $ao(boc) = (aob)oc, \forall\, a, b, c \in G$. In otherwords, we say that (G, o) the set G with operation o is* **semi-group** *if G is closed under o and o is associative.*

Example 0.14 *Let $G = \mathbb{N}$ be the set of natural numbers. Define an operation o by $aob = ab, \forall\, a, b \in \mathbb{N}$. Then (G, o) is a semigroup because the multiplication of natural numbers is associative and G is closed under multiplication of natural numbers.*

Example 0.15 *Let $G = \mathbb{Z}$, be the set of integers. Define an operation $*$ on G by $a * b = a + 3b, \forall\, a, b \in \mathbb{Z}$. Then clearly, $*$ is binary operation. Also, we see that $(2 * 3) * 4 = 11 * 4 = 23$ and $2 * (3 * 4) = 2 * (15) = 47$. This shows that $*$ is not associative binary operation. So, $(G, *)$ is not a semigroup.*

Definition 0.16 *A non-empty set G with a binary operation o is said to be monoid if o is associative and there exists an identity element $e \in G$ such that $aoe = eoa = a, \forall\, a \in G$.*

Example 0.17 *Let $G = \mathbb{N}$ be the set of natural numbers. Define an operation o by $aob = ab, \forall\, a, b \in \mathbb{N}$. Then (G, o) is a monoid because the multiplication of natural numbers is associative and G is closed under multiplication of natural numbers. Also $1 \in \mathbb{N}$ such that $ao1 = a = 1oa, \forall\, a \in \mathbb{N}$.*

Definition 0.18 *A non-empty set G with binary operation o is said to be a group if*
(i) o is associative. i.e,

$$(aob)oc = ao(boc), \forall\, a,\, b,\, c \in G$$

(ii) there exists an identity element in $e \in G$ such that

$$aoe = eoa = a, \forall\, a \in\ G.$$

(iii) for each element $a \in G$, there exists an element $b \in G$ such that

$$aob = boa = e.$$

Remark: If in a group $(G,\, o)$, the binary operation o is commutative, then (G, o) is called *abelian group.*

Theorem 0.19 *Let $(G,\, o)$ be a group. Then G has a unique identity and every element of G has a unique inverse.*

proof First, let's suppose that G has two identities e and e'. Then

$$eoe' = e'.....(1)$$

when e is an identity and

$$eoe' = e.....(2)$$

when e' is an identity.
From (1) and (2), we have

$$e = e'.$$

Thus an identity is unique in a group G. Similarly, let $a \in G$ be any element. Now, suppose there exist two inverses of a say a' and a''. Then

$$a' = a'oe = a'(aoa'') = (a'oa)oa'' = eoa'' = a''.$$

Hence the inverse of an element of a group is unique.

Theorem 0.20 *Let* (G, o) *be a group. Then*

$$(i)\ aob = aoc \Rightarrow b = c, \forall, a, b, c \in\ G \text{ (Left Cancellation Law)}$$

and

$$(ii)\ boa = coa \Rightarrow b = c, \forall\, a, b, c \in G \text{ (Right Cancellation Law).}$$

Proof (i) We have

$$\begin{aligned} aob &= aoc \\ \Rightarrow a^{-1}o(aob) &= a^{-1}o(aoc) \\ (a^{-1}oa)ob &= (a^{-1}oa)oc \text{ because of associativity} \\ eob &= eoc \\ b &= c \end{aligned}$$

(ii) We have

$$\begin{aligned} boa &= boa \\ \Rightarrow (boa)oa^{-1} &= (boa)oa^{-1} \\ bo(a^{-1}oa) &= bo(a^{-1}oa) \text{ because of associativity} \\ boe &= coe \\ b &= c \end{aligned}$$

Theorem 0.21 *Let* (G, o) *be a group. Then*

$$(i)\ (a^{-1})^{-1} = a, \forall\, a \in\ G \quad (ii)\ (aob)^{-1} = b^{-1}oa^{-1}, \forall\, a, b \in G.$$

Proof (i) We know that $aoa^{-1} = a^{-1}oa = e, \forall\, a \in\ G$
$\Rightarrow (a^{-1})^{-1} = a, \forall\, a \in G.$

(ii) We have

$$\begin{aligned}(aob)o(b^{-1}oa^{-1}) &= ao(bob^{-1})oa^{-1}\\ &= ao(e)oa^{-1}\\ &= aoa^{-1}\\ &= e\end{aligned}$$

Similarly,

$$\begin{aligned}(b^{-1}oa^{-1})o(aob) &= b^{-1}o(a^{-1}oa)ob\\ &= b^{-1}oeob\\ &= b^{-1}ob\\ &= e\end{aligned}$$

Thus,

$$(aob)^{-1} = b^{-1}oa^{-1},\ \forall\, a,\ b \in G.$$

Theorem 0.22 *The equations $aox = b$ and $yoa = b$ have unique solutions in a group (G, o), where $a, b \in G$, x and y are unknown.*

Proof We have $aox = b$.....(1) and $yoa = b$.....(2).

Then $a^{-1}o(aox) = a^{-1}ob$

$\Rightarrow (a^{-1}oa)ox = a^{-1}ob$

$\Rightarrow eox = a^{-1}ob$

$\Rightarrow x = a^{-1}ob$ and $y = boa^{-1}$. To prove the uniqueness, suppose x_1 and x_2 be two solutions of (1). Then $aox_1 = b$ and $aox_2 = b \Rightarrow aox_1 = aox_2$

$\Rightarrow x_1 = x_2$ by left cancellation law.

Hence the equation (1) has unique solution.

Similarly, let y_1, y_2 be two solutions of equation (2).

Then $y_1oa = b$ and $y_2oa = b$

$\Rightarrow y_1oa = y_2oa$

$\Rightarrow y_1 = y_2$.

Theorem 0.23 *Every semi-group* (G, o) *in which* $aox = b$ *and* $yoa = b$ *have unique solutions in* G *for* $a, b \in G$ *is a group.*

Proof We have the equations $aox = b$ and $yoa = b$ have unique solutions in G for $a, b \in G$. Therefore, $aoe = a$ and $e'oa = a$. We claim that $e = e'$. For this, let $c \in G$ be any element such that $aox = c$ has unique solution say p, i.e $aop = c$ and let the equation $yoa = c$ has unique solution say q such that $qoa = c$. Now,

$$\begin{aligned} coe &= (qoa)oe \\ &= qo(aoe) \\ &= qoa \\ &= c.....(1) \end{aligned}$$

and

$$\begin{aligned} e'oc &= e'o(aop) \\ &= (e'oa)op \\ &= aop \\ &= c.....(2) \end{aligned}$$

Take $c = e'$ in (1) and $c = e$ in (2), we get $e'oe = e'$ and $e'oe = e$. It follows that $e = e'$. Similarly, for the uniqueness of inverse, we suppose that a' and a'' be the solutions of the equations $aox = e$ and $yoa = e$ respectively. So that $aoa' = e = a''oa$. Now,

$$a' = eoa' = (a''oa)oa' = a''o(aoa') = a''oe = a''.$$

Hence (G, o) is a group.

Definition 0.24 *A group (G, o) is said to be finite if the number of elements in G is finite. This number is called an order of G. A group G is called infinite group if it is not finite.*

Example 0.25 *Let $G = \{1, w, w^2\}$ be the set of cube roots of unity. Then $(G, .)$ is a group under usual multiplication.*

Solution G is clearly, closed under usual multiplication as $w^3 = 1$ and multiplication is associative. 1 is an identy element in G and inverse of 1 is 1, inverse of w is w^2. Hence G is a finite group.

Theorem 0.26 *Let (G, o) be a semi-group having both the cancellation properties is a group.*

Proof Let $G = \{a_1, a_2, \ldots, a_n\}$ be a semigroup. To show that G is a group, it is enough to show that the equations $a_i o x = a_j$ and $y o a_i = a_j$ for $i, j = 1, 2, \ldots, n$ have unique solutions. For this, let us take a particular equation $a_k o x = a_l$. We see that $a_k o a_1, a_k o a_2, \ldots, a_k o a_n$ are all distinct. For this, suppose that $a_k o a_i = a_k o a_j \Rightarrow a_i = a_j$ (by left cancellation), which is a contradiction. Then there exists $a_m \in G$ such that $a_k o a_m = a_l \Rightarrow a_k o x = a_l$ has solution. For the uniqueness of solution, let $a_k o a_m = a_l$ and $a_k o a_n = a_l \Rightarrow a_k o a_m = a_k o a_n \Rightarrow a_m = a_n$. This shows that the equation $a_k o x = a_l$ has unique solution. Similarly, the equation $y o a_i = a_j$ has unique solution. Thus, G is a group.

Example 0.27 *Let $G = \mathbb{Z}$ be the set of integers. Then $(G, +)$ is an abelian group.*

Solution (i) Since the addition of two integers is also an integer, i.e, $a+b \in G$, $forall\, a, b \in G$. So, G is closed under $+$.
(ii) $a + (b + c) = (a + b) + c$, $\forall\, a, b, c \in G$ i.e, $+$ is associative.

(iii) There exists $0 \in G$ such that $a + 0 = a = 0 + a$, $\forall\, a \in G$.

(iv) For each $a \in G$, there exist $-a \in G$ such that $-a + a = 0 = a + (-a)$.

(v) $a + b = b + a$, $\forall\, a, b \in G$. Hence, G is an abelian group under the usual addition.

Example 0.28 *Let $G = \mathbb{Q}$ be the set of rational numbers. Then $(G, +)$ is an abelian group.*

Solution (i) Let $a = \frac{p}{q}$ and $b = \frac{r}{s}$, where $q \neq 0$ and $s \neq 0$ be any two elements of G. Then $a + b = \frac{p}{q} + \frac{r}{s} = \frac{sp+qr}{rs} \in G$. Thus G is closed under $+$.

(ii) Let $a = \frac{p}{q}$, $b = \frac{r}{s}$ and $c = \frac{t}{u}$ be any elements of G. Then

$$\begin{aligned}
(a+b)+c &= \left(\frac{p}{q} + \frac{r}{s}\right) + \frac{t}{u} \\
&= \left(\frac{ps+rq}{qs}\right) + \frac{t}{u} \\
&= \frac{u(ps+rq)+t(qs)}{(qs)u} \\
&= \frac{u(ps)+u(rq)+t(qs)}{q(su)} \\
&= \frac{(ps)u+(ru)q+(ts)q}{q(su)} \\
&= \frac{p}{q} + \left(\frac{r}{s} + \frac{t}{u}\right) \\
&= a + (b + c)
\end{aligned}$$

(iii) There exists $0 \in G$ such that $a + 0 = a = 0 + a$, $\forall\, a \in G$.

(iv) For each $a \in G$, there exist $-a \in G$ such that $-a + a = 0 = a + (-a)$.

(v) $a + b = b + a$, $\forall\, a, b \in G$. Hence, G is an abelian group under the usual addition.

Example 0.29 *Let $G = \mathbb{R}$ be the set of real numbers. Then $(G, +)$ is an abelian group.*

Solution (i) Since the addition of two real numbers is also a real number, i.e, $a + b \in G$, $forall\, a, b \in G$. So, G is closed under $+$.

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

(iii) There exists $0 \in G$ such that $a + 0 = a = 0 + a$, $\forall\, a \in G$.

(iv) For each $a \in G$, there exist $-a \in G$ such that $-a + a = 0 = a + (-a)$.

(v) $a + b = b + a$, $\forall\, a,\, b \in G$. Hence, G is an abelian group under the usual addition.

Example 0.30 *Let $G = \mathbb{C}$ be the set of complex numbers. Then $(G, +)$ is an abelian group.*

Solution(i) Let $z_1 = a_1 + ib_1$ and $z_2 = a_2 + ib_2$ be two cvomplex numbers. Then $z_1 + z_2 = (a_1 + ib_1) + (a_2 + ib_2) = (a_1 + a_2) + i(b_1 + b_2)\ \in\ \mathbb{C}$. Thus G is closed under $+$.
(ii) Let $z_1,\, z_2,\, z_3$ be any elements of G. Then

$$\begin{aligned} z_1 + (z_2 + z_3) &= (a_1 + ib_1) + (a_2 + ib_2 + a_3 + ib_3) \\ &= (a_1 + ib_1) + \{(a_2 + a_3) + i(b_2 + b_3)\} \\ &= \{a_1 + (a_2 + a_3)\} + i\{b_1 + (b_2 + b_3)\} \\ &= \{(a_1 + a_2) + a_3\} + i\{(b_1 + b_2) + b_3\} \\ &= \{(a_1 + a_2) + i(b_1 + b_2)\} + (a_3 + ib_3) \\ &= (z_1 + z_2) + z_3 \end{aligned}$$

(iii) There exists $0 = 0 + i0$ in G such that $0 + z = z + 0 = z$, $\forall\, z \in G$.
(iv) For each $z = a + ib$ in G, there exist $-z = -a - ib$ in G such that $z + (-z) = (a - a) + i(b - b) = 0 + i0 = 0$. Similarly, $-z + z = 0$.
(v) $z_1 + z_2 = (a_1 + ib_1) + (a_2 + ib_2) = (a_1 + a_2) + i(b_1 + b_2)$
$= (a_2 + a_1) + i(b_2 + b_1) = z_2 + z_1$. Hence, G is an abelian group.

Example 0.31 *Let $G = \{1,\, -1\}$ forms a group under multiplication.*

Solution This set G is closed under multiplication. There exists $1 \in G$ as an identity

element and inverse of 1 is 1 and inverse of -1 is -1. Also multiplication is associative in G. Thus, G is a group.

Example 0.32 *Prove that the set $G = \{1, -1, i, -i\}$, where $i^2 = -1$ is a group under usual multiplication.*

Solution G is clearly closed under multiplication as $1(-1) = -1$, $(-1)(-1) = 1$, $i(-1) = -i$, $(-i)^2 = -1$, $i(-i) = 1$. Also, multiplication of complex numbers is associative so the multiplication is associative in G. There exists $1 \in G$ such that $z(1) = 1(z) = z \,\forall\, z \in G$. Further, every element of G has inverse such as $1(1) = 1$, $(-1)(-1) = 1$, $(i)(-i) = 1$. Thus G is a group.

Example 0.33 *Show that the n-th root of unity forms a multiplicative group i.e $G = \{e^{\frac{i2k\pi}{n}}; k = 0, 1, 2, \ldots, n-1\}$ is a group under multiplication.*

Solution Let $\alpha = e^{\frac{i2k\pi}{n}}$. Then $G = \{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$. For closure property, we have $\alpha^r.\alpha^s = \alpha^{r+s}$. If $r + s < n$, then $\alpha^{r+s} \in G$, if $r + s = n$, then $\alpha^{p+q} = \alpha^n = 1$ and $\alpha^{r+s} \in G$ but if $r + s = n + p$ and $p \leq n - 1$ then $\alpha^{r+s} = \alpha^{n+p} = \alpha^p \in G$. Since the multiplication is associative in complex numbers so multiplication is associative in G. The element 1 is an identity element and inverse of α^r is $\alpha^{n-r} \in G$. Hence G is a group under multiplication.

Example 0.34 *Let $G = \mathbb{Z}_n = \{\bar{0}, \bar{1}, \ldots, \bar{n-1}\}$ be the set of residue classes modulo n. Then G forms a group under the operation $\oplus$ defined by $\bar{a} \oplus \bar{b} = \overline{a+b} = \bar{r}$, where r is the remainder upon dividing $a + b$ by n.*

Proof (i) Closure Property: Let $\bar{a}$, $\bar{b}$ be any elements of G.
Then $\bar{a} + \bar{b} = \overline{a+b} \in G$ (because $\overline{a+b}$ is the remainder upon dividing $a + b$ by n and G is the set of remainders of integers upon by n).

(ii) Let $\bar{a}$, $\bar{b}$, $\bar{c} \in G$. Then

$$\begin{aligned} \bar{a} \oplus (\bar{b} \oplus \bar{c}) &= \bar{a} \oplus \overline{b+c} \\ &= \overline{a+(b+c)} \\ &= \overline{(a+b)+c} \\ &= \overline{a+b} \oplus \bar{c} \\ &= (\bar{a} \oplus \bar{b}) \oplus \bar{c} \end{aligned}$$

Therefore, $\oplus$ is associative.

(iii) There exists $\bar{0} \in G$ such that $\bar{a} \oplus \bar{0} = \overline{a+0} = \bar{a}$ and $\bar{0} \oplus \bar{a} = \overline{0+a} = \bar{a}$ for all $\bar{a} \in G$.

(iv) For each $\bar{a} \in G$ there exists $\overline{n-a} \in G$ such that

$$\bar{a} \oplus \overline{n-a} = \overline{a+(n-a)} = \overline{n} = \bar{0}$$

and

$$\overline{n-a} \oplus \bar{a} = \overline{(n-a)+a} = \overline{n} = \bar{0}$$

(v) $\bar{a} \oplus \bar{b} = \overline{a+b} = \overline{b+a} = \bar{b} \oplus \bar{a}$. Hence G is an abelian group.

Example 0.35 *Let* $M_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} | a, b, c, d \in \mathbb{R} \right\}$ *be a set of* 2×2 *matrices over the set of real numbers. Then* $M_2(\mathbb{R})$ *is an abelian group under the operation matrix addition defined as*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix}, \forall\, a, b, c, d, e, f, g, h \in \mathbb{R}.$$

Solution (i) **Closure Property**: Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $B = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$. Then $A + B = \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix}$ which is also 2×2 matrix on the real numbers, so $A + B \in M_2(\mathbb{R})$.

Hence $M_2(\mathbb{R})$ is closed under addition.

(ii) **Associative Property**: Let $A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}$, $B = \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix}$ and $C = \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix}$ be any elements. Then

$$\begin{aligned} A + (B + C) &= \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} + \left(\begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} + \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix} \right) \\ &= \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} + \begin{pmatrix} b_1 + c_1 & b_2 + c_2 \\ b_3 + c_3 & b_4 + c_4 \end{pmatrix} \\ &= \begin{pmatrix} a_1 + (b_1 + c_1) & a_2 + (b_2 + c_2) \\ a_3 + (b_3 + c_3) & a_4 + (b_4 + c_4) \end{pmatrix} \\ &= \begin{pmatrix} (a_1 + b_1) + c_1 & (a_2 + b_2) + c_2 \\ (a_3 + b_3) + c_3 & (a_4 + b_4) + c_4 \end{pmatrix} \\ &= \begin{pmatrix} a_1 + b_1 & a_2 + b_2 \\ a_3 + b_3 & a_4 + b_4 \end{pmatrix} + \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix} \\ &= (A + B) + C \end{aligned}$$

(iii) There exists $O = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ in $M_2(\mathbb{R})$ such that $A + O = O + A = A$, $\forall\, A \in M_2(\mathbb{R})$.

(iv) For each $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $M_2(\mathbb{R})$ there exists $-A = \begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$ such that $A + (-A) = \begin{pmatrix} a-a & b-b \\ c-c & d-d \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = -A + A$.

(v) $A + B = \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix} = \begin{pmatrix} e+a & f+b \\ g+c & h+d \end{pmatrix} = B + A$.

Hence $M_2(\mathbb{R})$ is an abelian group.

Example 0.36 *Let* $GL_2(\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} | ad - bc \neq 0 \text{ and } a, b, c, d \in \mathbb{R} \right\}$ *be a set of*

2×2 *matrices over the set of real numbers. Then* $GL_2(\mathbb{R})$ *is a non-abelian group under the operation matrix multiplication defined as*

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{bmatrix}, \forall\, a,\, b,\, c,\, d,\, e,\, f,\, g,\, h \in \mathbb{R}.$$

Solution (i) **Closure Property**: Let A, B be any elements of $GL_2(\mathbb{R})$. Then $|A| \neq 0$ and $|B| \neq 0 \Rightarrow |AB| = |A||B| \neq 0$. Thus $AB \in GL_2(\mathbb{R})$. Therefore, $GL_2(\mathbb{R})$ is closed under multiplication of matrices.

(ii) **Associative Property**: Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, $B = \begin{bmatrix} e & f \\ g & h \end{bmatrix}$ and $C = \begin{bmatrix} i & j \\ k & l \end{bmatrix}$. Then

$$(AB)C = \begin{bmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{bmatrix} \begin{bmatrix} i & j \\ k & l \end{bmatrix}$$

$$= \begin{bmatrix} (ae+bg)i+(af+bh)k & (ae+bg)j+(af+bh)l \\ (ce+dg)i+(cf+dh)k & (ce+dg)j+(cf+dh)l \end{bmatrix}$$

$$= \begin{bmatrix} a(ei+fk)+b(hk+gi) & a(ej+fl)+b(hl+gj) \\ (ei+fk)c+(gi+kh)d & c(ej+fl)+d(gj+hl) \end{bmatrix} = A(BC)$$

(iii) **Existence of identity element**: There exist $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ in $GL_2(\mathbb{R})$ such that $AI = IA = A$, $\forall\, A \in GL_2(\mathbb{R})$.

(iv) **Existence of inverse**: For each $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ there exist $A^{-1} = \frac{1}{ad-bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$ in $GL_2(\mathbb{R})$ such that $AA^{-1} = A^{-1}A = I$. Hence G is a group.

Example 0.37 *Let* $G = \{e,\, a,\, b,\, c\}$. *Then* G *is an abelian group under the operation defined as* $a^2 = b^2 = c^2 = e$, $ab = c = ba$, $bc = cb = a$, $ac = ca = b$. *This group is called Kelin* $4-$ *group.*

Solution We shall understand its properties from the below mentioned table:

o	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

(i) Since no element in the table is out of G, so G is closed under this operation.

(ii) Here we see that $a(bc) = aa = a^2 = e$ and $(ab)c = cc = c^2 = e$. Hence $a(bc) = (ab)c$.

(iii) $e \in G$ is an identity element.

(iv) In each row of the table, there is an identity element, so it follows that each element of G has inverse in G.

(v) From the definition, it follows that $ab = ba$, $\forall\, a,\, b \in G$. Hence G is an abelian group.

Example 0.38 *Let* $G = \{f_0,\, f_1,\, f_2,\, f_3,\, f_4,\, f_5\}$ *be the set of all symmetries of an equilateral triangle whose vertices are* 1, 2, 3 *where* $f_0(1) = 1$, $f_0(2) = 2$, $f_0(3) = 3$, $f_1(1) = 2$, $f_1(2) = 3$, $f_1(3) = 1$, $f_2(1) = 3$, $f_2(2) = 1$, $f_2(3) = 2$, $f_3(1) = 1$, $f_3(2) = 3$, $f_3(3) = 2$, $f_4(1) = 3$, $f_4(2) = 2$, $f_4(3) = 1$, $f_5(1) = 2$, $f_5(2) = 1$, $f_5(3) = 3$. *Then* G *forms a group under the composition of maps.*

Solution (i) **Closure Property**: The elements of G can be determined as follows:

$f_1 o f_1(1) = f_1(f_1(1)) = f_1(2) = 3$, $f_1 o f_1(2) = f_1(f_1(2)) = f_1(3) = 1$, $f_1 o f_1(3) = f_1(f_1(3)) = f_1(1) = 2 \Rightarrow f_1 o f_1 = f_2$. Similarly, $f_2 o f_2(1) = f_2(f_2(1)) = f_2(3) = 2$, $f_2 o f_2(2) = f_2(f_2(2)) = f_2(1) = 3$, $f_2 o f_2(3) = f_2(f_2(3)) = f_2(2) = 1 \Rightarrow f_2 o f_2 = f_1$

$f_3 o f_3(1) = f_3(f_3(1)) = f_3(1) = 1$, $f_3 o f_3(2) = f_3(f_3(2)) = f_3(3) = 2$, $f_3 o f_3(3) = f_3(f_3(3)) = f_3(2) = 3 \Rightarrow f_3 o f_3 = f_0$

$f_4 o f_4(1) = f_4(f_4(1)) = f_4(3) = 1$, $f_4 o f_4(2) = f_4(f_4(2)) = f_4(2) = 2$, $f_4 o f_4(3) = f_4(f_4(3)) = f_4(1) = 3 \Rightarrow f_4 o f_4 = f_0$

$f_5 o f_5 = f_0$. Similarly, the composition with other symmetries can be checked and we see that the composition of these maps is binary operation on G which is very clear from

the table given below.

o	f_0	f_1	f_2	f_3	f_4	f_5
f_0	f_0	f_1	f_2	f_3	f_4	f_5
f_1	f_1	f_2	f_0	f_5	f_3	f_4
f_2	f_2	f_0	f_1	f_4	f_5	f_3
f_3	f_3	f_1	f_2	f_0	f_4	f_5
f_4	f_4	f_1	f_2	f_3	f_0	f_5
f_5	f_5	f_3	f_4	f_1	f_2	f_0

(ii) **Associative law**: Since the symmetries are one-one onto maps on the set $\{1, 2, 3\}$ and composition of maps is associative. So the composition of symmetries is also associative.

(iii) There exists an identity element $f_0 \in G$ such that $f_i o f_0 = f_0 o f_i = f_i, \forall\, i = 1, 2, 3, 4, 5$ clearly follows from the table.

(iv) In each row of the table there exists identity element f_0 implies that the element on the top of column containing identity element possess the inverse as the first element of that very row. Hence, it follows that every element in G has inverse in G. This group in non-abelian because $f_3 o f_2 \neq f_2 o f_3$.

Example 0.39 *Let $G = \{1, -1, i, -i, j, -j, k, -k\}$ be a set with the elements satisfying the conditions*

$$i^2 = j^2 = k^2 = -1,\ ij = k,\ jk = i,\ ki = j,\ ji = -ij,\ kj = -jk,\ ki = -ik.$$

Then G is a non-abelian group under multiplication. This group is also called as group of Quartenions.

Solution To verify that G is a group under multiplication, we just observe the properties from the following table:

.	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	$-i$	i	1	-1

(i) The above table contains all the elements of G, so G is closed under multiplication.

(ii) The multiplication is associative, i.e, $(ab)c = a(bc)$, $\forall\, a,\, b,\, c \in G$.

(iii) There exists $1 \in G$ such that $a.1 = 1.a = a$, $\forall\, a \in G$.

(iv) From the table it follows that, each row ontains an identity element, the element on the top of this column is the inverse of first element of that row.

(v) Here, we see that $ij = k = -kj$.

Hence, G is a non-abelian group.

Definition 0.40 *Let $S = \{1, 2, 3, \ldots, n\}$. Then a one-one mapping $\sigma : S \to S$ is called a permutation on n symbols $\{1, 2, \ldots, n\}$. It is denoted by*

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}.$$

For instance, let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ denotes the permutation on 4-symbols $\{1, 2, 3, 4\}$ which maps 1 to 2, 2 to 1, 3 to 4 and 4 to 3. Since the composition of one-one and onto maps is also one-one and onto. Therefore, the composition of two permutations is also permutation. Now consider two permutations $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ and $\tau =$

$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$. *Then we see that*

$$\begin{aligned} \sigma o\tau &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \end{aligned}$$

and

$$\begin{aligned} \tau o\sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \end{aligned}$$

It follows that the composition of permutations is not commutative.

Example 0.41 *Let S_n denotes the set of all permutations on n-symbols. Then S_n is a group.*

Solution (i) **Closure property**: Let σ and τ be any elements of S_n. Then $\sigma o\tau$ being the composition of one-one maps on finite set $\{1, 2, \ldots, n\}$ is also one-one map. Thus G is closed under the composition of maps.

(ii) **Associative law**: Since the composition of maps is associative, so

$$(\sigma o\tau)o\gamma = \sigma o(\tau o\gamma), \forall\, \sigma, \tau, \gamma \in S_n.$$

(iii) **Existence of identity element**: There exist $I = \begin{pmatrix} 1 & 2 & \ldots & n \\ 1 & 2 & \ldots & n \end{pmatrix}$ in S_n such that

$$\sigma oI = \sigma = Io\sigma, \forall\, \sigma \in S_n.$$

(iv) **Existence of inverse**: Since each element σ of S_n is one-one and onto map on the set $\{1, 2, \ldots, n\}$ and then σ^{-1} is also one-one and onto map on the set $\{1, 2, \ldots, n\}$, so σ^{-1} is also a permutation on n-symbols such that

$$\sigma o \sigma^{-1} = \sigma^{-1} o \sigma = I.$$

Hence S_n is a group.

Definition 0.42 *Let $\sigma \in S_n$ be any element. Then the signature of σ is defined as the product*

$$\prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j}.$$

It is denoted by $\epsilon\sigma$. Notice that the value of $\epsilon\sigma$ is either 1 or -1. For instance, if $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$, then

$$\epsilon\sigma = \frac{(2-3)(2-1)(2-4)(3-1)(3-4)(1-4)}{(1-2)(1-3)(1-4)(2-3)(2-4)(3-4)} = 1$$

Definition 0.43 *A permutation σ is said to be an even permutation if $\epsilon\sigma = +1$ and it is said to be odd permutation if its signature $\epsilon\sigma = -1$. For instance $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$ is even permutation and the permutation $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ is odd permutation as $\epsilon\tau = -1$.*