Chapter 2

GROUPS

The concept of a binary operation on a nonempty set has already been explained in the previous classes. One may recall that a **binary operation** on a nonempty set A is just a function $* : A \times A \longrightarrow A$. So, for each (a, b) in $A \times A$, $*$ associates an element $*(a, b)$ of A. We shall denote $*(a, b)$ by $a * b$. If A is a nonempty set with a binary operation $*$, then A is said to be **closed** under $*$.

DEFINITIONS AND EXAMPLES

We define a group as follows:

(2.1) Definition. A pair $(G, *)$, where G is a nonempty set and $*$ is a binary operation on G, is called a **group** if the following conditions, called **axioms of a group**, are satisfied in G:

(i) The binary operation $*$ is **associative**. That is,

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

(ii) There is an element e in G such that

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

e is called **the identity** element of G.

(iii) For each $a \in G$, there is an $a' \in G$ such that

$$a * a' = a' * a = e.$$

a' is called **the inverse** of a.

Note: Use of word **the** before identity element and inverse of an element is to signify their uniqueness.

(2.2) Definition. A group $(G, *)$ is said to be **abelian**[1] or **commutative** if

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

If there is a pair of elements $a, b \in G$ such that $a * b \neq b * a$, then G is called a **non-abelian** group.

Usually the binary operation in a group is either denoted by ".", called **multiplication** or by +, called **addition.** The pair $(G, .)$ then denotes **group under multiplication** while $(G, +)$ denotes a **group under addition.** In $(G, .)$ the inverse of an element a is written a^{-1}, while in $(G, +)$ the inverse of a is written as $-a$.

In practice, the product $a \cdot b$ of two elements in a group G under multiplication is written simply as ab. Also, we shall denote a group $(G, .)$ by G only.

(2.3) Definition. An element x of a group G is said to be **idempotent** if

$$x^2 = x$$

(2.4) Theorem. The only idempotent element in a group G is the identity element.

Proof. Let $x \in G$ be an idempotent element. Then

$$x^2 = x$$

$$\Rightarrow \quad x^{-1} \cdot x^2 = x^{-1} \cdot x = e$$

$$\Rightarrow \quad x^{-1} \cdot x \cdot x = e$$

$$\Rightarrow \quad e \cdot x = e$$

Thus $\quad x = e.$

Example 1. Consider the set

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

and let the binary operation defined on G be the ordinary multiplication of real numbers. Then $(G, .)$ is a group.

Example 2. The pairs $(Z, +)$, $(Q, +)$, $(R, +)$ and $(C, +)$ where Z, Q, R and C are the sets of integers, rational numbers, real numbers and complex numbers respectively and + denotes ordinary addition in them, are all groups.

To verify that a finite set is a group it is some times convenient to list the products in the form of a table called **Cayley's group table**[2]. This is illustrated by the following examples:

Example 3. (Group Tables). Let $G = \{1, \omega, \omega^2\}$, where ω is a complex cube root of unity. We write the elements of G along a row and along a column as shown in the

1. Named for the Norwegian mathematician N.H. Abel (1802 – 1829).

2. ... for the British mathematician A. Cayley (1821 – 1895)

table below indicating the binary operation in the top left corner. The column headed by a_j in the upper row is called the jth column and the row with a_i in the left column is referred to as the ith row. The blanks are then filled in by writing in the ijth position the product of an element a_i in the ith row with the element a_j in the jth column.

Thus, for $G = \{ 1, \omega, \omega^2 \}$, we have the following table. Here the binary operation '.' is the multiplication of complex numbers.

$\cdot$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1

Here we have used the fact that $\omega^3 = 1$. It is now easy to verify the conditions for the group like closure law, associative law, etc., from this table.

A group is abelian if its table is symmetric about its main diagonal.

Example 4. The set $C_4 = \{ 1, -1, i, -i \}$ of all the fourth roots of unity is a group under the usual multiplication of complex numbers. Here

$$(i)^{-1} = -i \quad \text{and} \quad (-i)^{-1} = i.$$

In general, the set C_n of all the nth roots of unity, for a fixed natural number n, forms a group under multiplication. The elements of C_n are

$$e^{2k\pi i/n}, \qquad k = 0, 1, 2, \cdots, n-1.$$

Example 5. Let $Q \setminus \{ 0 \}$, $R \setminus \{ 0 \}$ and $C \setminus \{ 0 \}$ denote the sets of nonzero rational numbers, nonzero real numbers and nonzero complex numbers respectively. Then under the usual multiplication of real and complex numbers $(Q \setminus \{ 0 \}, .)$, $(R \setminus \{ 0 \}, .)$ and $(C \setminus \{ 0 \}, .)$ are all groups.

Query: Why 0 has been deleted from the respective sets?

Example 6. Let

$$G = \{ I, -I, i, -i, j, -j, k, -k \}$$

where the symbols satisfy the relations

$$ij = k, \quad jk = i, \quad ki = j$$

$$ji = -k, \quad kj = -i, \quad ik = -j$$

and

$$i^2 = j^2 = k^2 = -I.$$

Then, under the multiplication of the symbols defined defined above, G is group. Since in G

$$ij = k \neq -k = ji,$$

G is non-abelian. G is called the **group of quaternions.**

Example 7. Let G be the set of all 2×2 nonsingular real matrices. Then, under the usual multiplication of matrices, G is a group. Moreover, it is a non-abelian group. For example,

$$A = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$$

are in G and

$$AB = \begin{bmatrix} 1 & 2 \\ 2 & 5 \end{bmatrix}, \quad BA = \begin{bmatrix} 5 & 2 \\ 2 & 1 \end{bmatrix}$$

Thus $AB \neq BA$ and so G is not an abelian group.

Example 8. Let $\bar{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ be the set of residue classes modulo 5. Define + in $\bar{Z}_5$ as the addition modulo 5. Thus, for $\bar{a}, \bar{b} \in \bar{Z}_5$, $\bar{a} + \bar{b} = \bar{r}$ where r is the remainder obtained after division of $a + b$ by 5. Then $(\bar{Z}_5, +)$ is a group.

Example 9. Let $S = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ be the set of nonzero residue classes modulo 5 and define multiplication in S as multiplication modulo 5. Thus if $\bar{a}, \bar{b} \in S$, then $\bar{a} . \bar{b} = \bar{r}$, where r is the remainder obtained after dividing the usual product ab of a and b by 5. Then $(S, .)$ is a group.

Example 10. Let

$$G = \{I, -I, X, -X, Y, -Y, Z, -Z\}$$

be the set of 2×2 matrices where

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, X = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, Y = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, Z = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$$

It is easy to check that

$$X^2 = Y^2 = Z^2 = -I \quad \text{and}$$

$$YZ = X, \ ZY = -X, \ ZX = Y, \ XZ = -Y, \ XY = Z, \ YX = -Z.$$

G is a group under the usual multiplication of matrices. It is the 'same' group as the group of Example 6.

The concept of 'sameness' among groups is related with that of **isomorphism** of groups.

PROPERTIES OF GROUPS

(2.5) Theorem. (The Cancellation Laws). For any three elements a, b, c in a group G,

(i) $ab = ac$ implies $b = c$ **(Left Cancellation Law)**

(ii) $ba = ca$ implies $b = c$ **(Right Cancellation Law)**

Proof. (i) For a, b, c in G,

$$\begin{aligned} ab = ac &\Rightarrow a^{-1}(ab) = a^{-1}(ac) \\ &\Rightarrow (a^{-1}a)b = (a^{-1}a)c, \quad \text{using the associative law} \\ &\Rightarrow eb = ec, \quad e \text{ is the identity of } G. \\ &\Rightarrow b = c \end{aligned}$$

Thus the left cancellation law holds.

(ii) The proof similar to (i) and is left as an exercise.

(2.6) Theorem. (Solutions of Linear Equations). For any two elements a, b in a group G, the equations

$ax = b$ and $xa = b$ have unique solutions.

Proof. For a, b in G,

$$\begin{aligned} ax = b &\Rightarrow a^{-1}(ax) = a^{-1}b \\ &\Rightarrow (a^{-1}a)x = a^{-1}b, \text{ by the associative law} \\ &\Rightarrow ex = a^{-1}b \\ &\Rightarrow x = a^{-1}b. \end{aligned}$$

So $x = a^{-1}b$ is a solution of $ax = b$.

To see that the solution is unique, suppose that, for x_1, x_2 in G,

$$ax_1 = b, \qquad ax_2 = b$$

Then $ax_1 = ax_2$

so that, by the cancellation law, $x_1 = x_2$. Hence the solution is unique.

The case for the solution of $xa = b$ is similar.

(2.7) Theorem. For a, b in a group G, $(ab)^{-1} = b^{-1}a^{-1}$.

Proof. This follows from the following simplifications of the product $(ab)(b^{-1}a^{-1})$.

$$\begin{aligned}(ab)(b^{-1}a^{-1}) &= a(bb^{-1})a^{-1} && \text{, (Associative Law)}\\ &= a\,e\,a^{-1} && \\ &= aa^{-1} && (e \text{ is the identity})\\ &= e\end{aligned}$$

$$\begin{aligned}\text{Similarly}\quad (b^{-1}a^{-1})(ab) &= b^{-1}(a^{-1}a)\,b && \\ &= b^{-1}e\,b && \text{(Associative Law)}\\ &= b^{-1}b && \text{, } e \text{ is the identity}\\ &= e\end{aligned}$$

Hence $\quad (ab)^{-1} = b^{-1}a^{-1}$.

Remark: In general, for $a_1, a_2, \cdots, a_k$ in G, we have

$$(a_1 a_2 \cdots a_k)^{-1} = a_k^{-1}\, a_{k-1}^{-1} \cdots a_2^{-1}\, a_1^{-1}.$$

(2.8) Theorem For any element a of a group G, the following exponentiation rules hold: $(m, n \in Z^+)$

(i) $a^m = a\,.\,a\,.\cdots a$ (m factors)

(ii) $(a^{-1})^m = a^{-m} = (a^m)^{-1}$

(iii) $a^m\,.\,a^n = a^{m+n}$

(iv) $(a^m)^n = a^{mn}$.

The proofs follow by induction on m and n and are left as an exercise.

(2.9) Definition (Order of a group). The number of elements in a group G is called the **order** of G and is denoted by $|G|$. A group G is said to be **finite** if G consists of only a finite number of elements. Otherwise G is said to be an **infinite** group.

The groups in Examples 1, 3, 4, 6, 8, 9 and 10 are finite groups.

The orders of these groups are 2, 3, 4, 8, 5, 4 and 8 respectively.

The groups in Examples 2, 5 and 7 are infinite groups.

(2.10) Definition (Order of an Element). Let a be an element of a group G. A positive integer n is said to be the **order** of a if $a^n = e$ and n is the least such positive integer. (e is the identity element of G)

For any element x of G we always take $x^0 = e$. If $n = 0$ is the only integer for which $a^n = e$ then a is said to be of **infinite order**.

The order of an element $a \in G$ is denoted by $|a|$.