## Glossary of Main Definitions and Theorems of Group Theory

**1.** **A group** is a non-empty set $G$ with a binary composition . such that

(*i*) $a \,.\, b \in G$ for all $a, b \in G$.

(*ii*) $(a \,.\, b) \,.\, c = a \,.\, (b \,.\, c)$ for all $a, b, c \in G$.

(*iii*) There exists an element $e \in G$ such that

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

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

(*iv*) For each $a \in G$, there exists some element $b \in G$ such that

$$a \,.\, b = b \,.\, a = e.$$

$b$ is called the *inverse* of $a$ and is written as $a^{-1}$.

Some well known groups are :

(*i*) **Symmetric Group of degree 3**

$$S_3 = \{ I, (12), (23), (13), (123), (132) \}$$

**$S_n$ is symmetric group of degree $n$.** $o(S_n) = n!$

(*ii*) **Klein's 4-group**

$G = \{e, a, b, ab\}$ ; $a^2 = b^2 = e$ and $ab = ba$.

(*iii*) **Quaterian Group**

$$G = \{\pm 1, \pm i, \pm j, \pm k\}, \text{ where}$$

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

(*iv*) **Dihedral Group**

$G = \{x^i y^j : i = 0, 1 ; j = 0, 1, ..., n-1 ; x^2 = e = y^n, xy = y^{-1}x\}$.

**2.** A group of $G$ is called **abelian** if $a \,.\, b = b \,.\, a$ for all $a, b \in G$.

**3.** A non-empty subset of a group $G$ is called a **subgroup** of $G$, written as $H < G$, if $H$ is also a group w.r.t. the binary composition of $G$.

**4.** $H < G \Leftrightarrow ab^{-1} \in H \; \forall \; a \in H, b \in H$.

**5.** If $H$ is a subgroup of a group $G$, then

$aH = \{ah : h \in H\}$ is called a **left coset** of $H$ in $G$ and $Ha = \{ha : h \in H\}$ is called a **right coset** of $H$ in $G$. The total number of distinct left or right cosets of $H$ in $G$ is called the **index** of $H$ in $G$. It is denoted by $i_G(H)$ or $[G : H]$. We have

(*i*) $HH = H$, where $HH = \{h_1 h_2 : h_1 \in H, h_2 \in H\}$.

(*ii*) $aH = H \Leftrightarrow a \in H$.

(*iii*) $Ha = Hb \Leftrightarrow ab^{-1} \in H$.

(*iv*) $aH = bH \Leftrightarrow a^{-1}b \in H$.

**6.** A subgroup $N$ of a group $G$ is called a **normal subgroup** of $G$, written as $N \lhd G$, if $gng^{-1} \in N \; \forall \; g \in G, \forall \; n \in N$.

**7.** $N \lhd G \Leftrightarrow aN = Na \; \forall \; a \in G$.

8. If $N \lhd G$, then $Na\,Nb = Nab$. ...(i)

Further $\frac{G}{N} = \{Na : a \in G\}$ is a group w.r.t. the composition (i). $\frac{G}{N}$ is called a **quotient group**.

9. If $H$ and $K$ are subgroups of a group $G$, then

$$HK = \{hk : h \in H, k \in K\}$$

is a subgroup of $G$ iff $HK = KH$.

Further $o(HK) = \frac{o(H)\, o(K)}{o(H \cap K)}$.

10. **(Lagrange's Theorem)**

If $H$ is any subgroup of a finite group $G$, then $o(H)$ divides $o(G)$. However, the converse need not be true.

Also $i_G(H) = \frac{o(G)}{o(H)}$.

11. If $G$ is a finite group, then $a^{o(G)} = e \ \forall\ a \in G$.
12. The **order** of an element $a \in G$ is defined as the least positive integer $n$ such that $a^n = e$. We write $o(a) = n$.
13. Let $a, b \in G$. Then
    (i) $o(ab) = o(ba)$.
    (ii) $o(a) = o(a^{-1})$.
    (iii) $o(a) = o(b^{-1} a b)$.
    (iv) If $ab = ba$ and $(o(a), o(b)) = 1$, then
    $$o(ab) = o(a)\, o(b).$$
    (v) If $a^m = e$, then $m$ divides $o(a)$.
14. If $G_1$ and $G_2$ are two groups, then a mapping $f : G_1 \to G_2$ is called a **homomorphism**, if

$$f(ab) = f(a) f(b) \ \forall\ a, b \in G_1.$$

The set $K = \{a \in G_1 : f(a) = e_2$, identity of $G_2\}$ is called the **kernel** of homomorphism $f : G_1 \to G_2$. We write $K = Ker\, f$.

15. A mapping $f : G_1 \to G_2$ is an **isomorphism**, if
    (i) $f$ is a homomorphism.
    (ii) $f$ is one-to-one *i.e.*, $f(a) = f(b) \Rightarrow a = b$ ; $a, b \in G_1$.

If in addition, $f$ is onto ; we say that the groups $G_1$ and $G_2$ are **isomorphic**, denoted as $G_1 \simeq G_2$.

16. If $f : G \to G'$ is a homomorphism, then
    (i) $f(e) = e'$.
    (ii) $f(x^{-1}) = \{f(x)\}^{-1}$; $x \in G$.
    (iii) $Ker\, f$ is a normal subgroup of $G$.
    (iv) $Ker\, f = \{0\}$ iff $f$ is one-to-one.

# 1

# GROUPS

## 1.1 Some Sets of Numbers

The reader is familiar with the following sets of numbers :

1. $\mathbf{N} = \{1, 2, 3, ...\}$
   is the set of *natural numbers*.
2. $\mathbf{I}$ or $\mathbf{J}$ or $\mathbf{Z} = \{....., -3, -2, -1, 0, 1, 2, 3, ....\}$
   is the set of *integers*.
   $\mathbf{Z}^+$ denotes the set of all non-negative integers.
3. $\mathbf{E} = \{....., -6, -4, -2, 0, 2, 4, 6, .....\}$
   is the set of *even integers*.
4. $\mathbf{Q} = \left\{ \frac{m}{n} : m, n \in \mathbf{Z} \text{ and } n \neq 0 \right\}$
   is the set of *rational numbers*.
5. $\mathbf{R}$ is the set of *real numbers*. $\mathbf{R}$ contains all rational and irrational numbers.
   $\mathbf{R}^+$ denotes the set of all non-negative real numbers.
6. $\mathbf{C} = \{x + iy : x, y \in \mathbf{R} \text{ and } i = \sqrt{-1}\}$
   is the set of all *complex numbers*.

## 1.2 Mappings

If $S$ and $T$ are two non-empty sets, then a *mapping* from $S$ to $T$ is a rule, written as $f : S \to T$, which associates to each element $x \in S$, a unique element $y \in T$. The element $y$ is called the *image* of $x$ under $f$ and is written as $y = f(x)$. The element $x$ is called a *pre-image* of $y$. The set $S$ is called the *domain* of $f$, and $T$ its *co-domain*.

*A mapping $f : S \to T$ is called* **one-to-one**, *if*

$$x \neq y \quad \Rightarrow \quad f(x) \neq f(y) \; ; \; x, y \in S.$$

*Or*

$$f(x) = f(y) \quad \Rightarrow \quad x = y \; ; \; x, y \in S.$$

*A mapping $f : S \to T$ is called* **onto**, *if for* **each** $t \in T$, *there exists* **some** $s \in S$ *such that* $f(s) = t$.

*Two mappings $f : S \to T$ and $g : S \to T$ are said to be* **equal**, *if*

$$f(x) = g(x) \quad \text{for each} \quad x \in S.$$

*The mapping $i : S \to S$ defined as $i(x) = x \; \forall \; x \in S$ is called the* **identity mapping**.

*The* **product** *or the* **composition** *of two mappings*

$$f: S \to T \quad \text{and} \quad g: T \to U$$

*is defined as the mapping* $gof: S \to U$, *where* $(gof)(x) = g(f(x))$ *for each* $x \in S$.

**Examples of Mappings**

**Example 1.2.1.** Let $f: \mathbf{Z} \to \mathbf{Z}$ be defined as

$$f(x) = x^2 \quad \forall \quad x \in \mathbf{Z}.$$

Then $f$ is **not** one-to-one, since, for example,

$$2 \neq -2 \quad \text{but} \quad f(2) = f(-2) = 4.$$

Also $f$ is **not** onto, since, for example, $-2 \in \mathbf{Z}$ but there does not exist any $x \in \mathbf{Z}$ such that $f(x) = x^2 = -2$.

**Example 1.2.2.** Let $f: \mathbf{Z}^+ \to \mathbf{Z}^+$ be defined as

$$f(x) = x^2, \quad \forall \quad x \in \mathbf{Z}^+.$$

(Here $\mathbf{Z}^+$ denotes the set of all non-negative integers).

Then $f$ is one-to-one, since for any $x_1, x_2 \in \mathbf{Z}^+$

$$x_1 \neq x_2 \implies x_1^2 \neq x_2^2 \implies f(x_1) \neq f(x_2).$$

However, $f$ is **not** onto, since, for example, $2 \in \mathbf{Z}^+$ but there does not exist any $x \in \mathbf{Z}^+$ such that $f(x) = x^2 = 2$.

**Example 1.2.3.** Let $f: \mathbf{R}^+ \to \mathbf{R}^+$ be defined as

$$f(x) = x^2 \quad \forall \quad x \in \mathbf{R}^+.$$

(Here $\mathbf{R}^+$ denotes the set of all non-negative real numbers).

Then $f$ is one-to-one, since

$$x_1 \neq x_2 \implies x_1^2 \neq x_2^2 \implies f(x_1) \neq f(x_2); \; x_1, x_2 \in \mathbf{R}^+.$$

Also $f$ is onto, since for any $x \in \mathbf{R}^+$, there exists $\sqrt{x} \in \mathbf{R}^+$ such that

$$f(\sqrt{x}) = x.$$

**Example 1.2.4.** Let $f: \mathbf{R} \to \mathbf{R}^+$ be defined as

$$f(x) = x^2 \quad \forall \quad x \in \mathbf{R}.$$

Then $f$ is **not** one-to-one, since

$$\tfrac{1}{2} \neq -\tfrac{1}{2} \quad \text{but} \quad f(\tfrac{1}{2}) = f(-\tfrac{1}{2}) = \tfrac{1}{4}.$$

It may be noted that $f$ is onto, since for any $x \in \mathbf{R}^+$, there exists $\sqrt{x} \in \mathbf{R}$ such that

$$f(\sqrt{x}) = x. \quad \text{Also } f(-\sqrt{x}) = x.$$

Thus each $x \neq 0 \in \mathbf{R}^+$ has two pre-images in $\mathbf{R}$.

**Example 1.2.5.** Let $S = \{1, 2, 3\}$. Consider two mapping $f: S \to S$ and $g: S \to S$ defined as

$$f: \begin{matrix} 1 \to 2 \\ 2 \to 3 \\ 3 \to 1 \end{matrix} \quad \text{and} \quad g: \begin{matrix} 1 \to 3 \\ 2 \to 2 \\ 3 \to 1. \end{matrix}$$

Then $(fog)(x) = f(g(x))$, $x \in S$. Consequently,

$(fog)(1) = f(g(1)) = f(3) = 1$,
$(fog)(2) = f(g(2)) = f(2) = 3$,
$(fog)(3) = f(g(3)) = f(1) = 2$.

$$\therefore \quad fog : \begin{matrix} 1 \to 1 \\ 2 \to 3 \\ 3 \to 2. \end{matrix}$$

Again, $(gof)(1) = g(f(1)) = g(2) = 2$,
$(gof)(2) = g(f(2)) = g(3) = 1$,
$(gof)(3) = g(f(3)) = g(1) = 3$.

$$\therefore \quad gof : \begin{matrix} 1 \to 2 \\ 2 \to 1 \\ 3 \to 3. \end{matrix}$$

It may be observed that $fog \neq gof$.

**Example 1.2.6.** If $S = \{1, 2, 3\}$, then all one-to-one mappings of $S$ onto $S$ are

$$i : \begin{matrix} 1 \to 1 \\ 2 \to 2 \\ 3 \to 3 \end{matrix}, \quad \sigma_1 : \begin{matrix} 1 \to 1 \\ 2 \to 3 \\ 3 \to 2 \end{matrix}, \quad \sigma_2 : \begin{matrix} 1 \to 3 \\ 2 \to 2 \\ 3 \to 1 \end{matrix}$$

$$\sigma_3 : \begin{matrix} 1 \to 2 \\ 2 \to 1 \\ 3 \to 3 \end{matrix}, \quad \tau_1 = \begin{matrix} 1 \to 2 \\ 2 \to 3 \\ 3 \to 1 \end{matrix}, \quad \tau_2 = \begin{matrix} 1 \to 3 \\ 2 \to 1 \\ 3 \to 2. \end{matrix}$$

It can be verified that

$$\tau_1 o \tau_2 = \tau_2 o \tau_1 = i \; ; \; \sigma_1 o \sigma_1 = \sigma_2 o \sigma_2 = \sigma_3 o \sigma_3 = i;$$

$$i o i = i, \; \sigma_1 o i = \sigma_1, \; \sigma_2 o i = \sigma_2, \; \sigma_3 o i = \sigma_3, \; \tau_1 o i = \tau_1, \; \tau_2 o i = \tau_2.$$

$i$ is called the *identity mapping* on $S$. The above six mappings are called the *permutations* of $S$ and the set of all permutations of $S = \{1, 2, 3\}$ is denoted by $S_3$, where

$$S_3 = \{i, \sigma_1, \sigma_2, \sigma_3, \tau_1, \tau_2\} \text{ and } o(S_3) = 6 = 3!.$$

**Remark.** *If $S$ is a non-empty set, then the set of all one-to-one mappings of $S$ onto itself is denoted by $A(S)$. If $S$ is a finite set having $n$ elements, then a one-to-one mapping of $S$ onto itself is called a* **permutation** *of $S$. The set of all permutations of $S$ is denoted* by $S_n$. *It can be proved that* $o(S_n) = n!$. [For more details, see Section 2.4 of Chapter 2.]

**Some Results on Mappings**

**Lemma 1.2.1.** *If $f : A \to B$, $g : B \to C$ and $h : C \to D$, then*

$$(hog) \, o \, f = h \, o \, (gof). \qquad \textbf{[Associative Law]}$$

**Proof.** We have $gof : A \to C$ and $hog : B \to D$.

Consequently, $h \, o \, (gof) : A \to D$ and $(hog) \, o \, f : A \to D$.

Let $x \in A$ be arbitrary. Then, by definition

$$[(hog)\ o\ f]\ (x) = (hog)\ (f(x))$$
$$= (hog)\ y, \text{ where } y = f(x) \in B$$
$$= h\ (g\ (y))$$
$$= h\ (z), \text{ where } z = g\ (y) \in C.$$

Again $$[h\ o\ (gof)]\ (x) = h\ [(gof)\ (x)]$$
$$= h\ [g\ (f(x))]$$
$$= h\ [g\ (y)]$$
$$= h\ (z).$$

$\therefore$ $$[(hog)\ o\ f]\ (x) = [h\ o\ (gof)]\ (x), \quad \forall \quad x \in A$$

Hence $$(hog)\ o\ f = h\ o\ (gof).$$

**Corollary.** *If $f$, $g$, $h$ are any three elements of $A(S)$, then*

$$(f\ o\ g)\ o\ h = f\ o\ (g\ o\ h).$$

**Lemma 1.2.2.** *Let $f : A \to B$ and $g : B \to C$. Then*

*(i) $gof$ is onto if $f$ and $g$ are both onto.*

*(ii) $gof$ is one-to-one if $f$ and $g$ are both one-to-one.*

**Proof.** We have $gof : A \to C$.

(i) Let $c$ be any arbitrary element of $C$.

Since $g : B \to C$ is onto, there exists some $b \in B$ such that

$$g\ (b) = c. \qquad \ldots(1)$$

Since $f : A \to B$ is onto, there exists some element $a \in A$ such that

$$f\ (a) = b. \qquad \ldots(2)$$

From (1) and (2), $$g\ (f\ (a)) = c$$

or $$(gof)\ (a) = c, \quad \text{where} \quad a \in A.$$

Hence $gof$ is onto.

(ii) Let $(gof)\ (a_1) = (gof)\ (a_2)\ ;\ a_1, a_2 \in A$

$\Rightarrow$ $g\ (f(a_1)) = g\ (f(a_2))$, where $f(a_1), f(a_2) \in B$

$\Rightarrow$ $f(a_1) = f(a_2)$, since $g$ is one-to one

$\Rightarrow$ $a_1 = a_2$, since $f$ is one-to-one.

Hence $gof$ is one-to-one.

**Lemma 1.2.3. (Inverse of a mapping)**

*Let $f : A \to B$ be one-to-one and onto. Then there exists a mapping $g : B \to A$, which is one-to-one and onto. Further $gof : A \to A$ and $fog : B \to B$ are identity mappings.*

**Proof.** Let $b$ be any arbitrary element of $B$. Since $f : A \to B$ is onto, there exists some $a \in A$ such that $f(a) = b$. We now show that $a$ is a unique element such that $f(a) = b$. Let, if possible, there exist two elements $a_1, a_2 \in A$ such that $f(a_1) = b$ and $f(a_2) = b$.

Then $f(a_1) = f(a_2) \Rightarrow a_1 = a_2$, since $f$ is one-to-one.

Hence we have shown that for *each* $b \in B$, there exists a unique element $a \in A$ such that $b = f(a)$. In this way a mapping from $B$ to $A$ is defined. Suppose we write this mapping as

$$g : B \to A, \text{ where}$$
$$g(b) = a \Leftrightarrow b = f(a). \qquad \ldots(1)$$

For any $a \in A$, we have

$$(gof)(a) = g(f(a)) = g(b) = a, \text{ using (1).}$$

Hence $gof$ is an identity mapping on $A$.

Similarly, $fog$ is an identity mapping on $B$.

Now we show that $g$ is one-to-one.

Let $b_1, b_2 \in B$. Then there exist unique $a_1, a_2 \in A$ such that

$$g(b_1) = a_1 \quad \text{and} \quad g(b_2) = a_2.$$

Using (1), $\quad b_1 = f(a_1)$ and $\quad b_2 = f(a_2)$.

Now $\quad g(b_1) = g(b_2) \Rightarrow a_1 = a_2 \Rightarrow f(a_1) = f(a_2) \Rightarrow b_1 = b_2$.

Thus $g$ is one-to-one.

Lastly, we show that $g$ is onto.

Let $a^* \in A$ be arbitrary. Then $f(a^*) \in B$.

Let $f(a^*) = b^* \in B$. By (1), $g(b^*) = a^*$; where $b^* \in B$.

Hence $g$ is onto.

**Remark.** *The mapping $g : B \to A$ is called the* **inverse** *of the mapping $f : A \to B$.* We write $g$ as $f^{-1}$. Hence we conclude that

*If $f : A \to B$ is one-to-one and onto, then $f$ has inverse mapping $f^{-1} : B \to A$ such that*

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

**Corollary.** *If $f \in A(S)$, then $f^{-1} \in A(S)$. Further*

$$fof^{-1} = f^{-1}of = i,$$

*$i$ being the identity mapping on $S$.*

**Proof.** $f \in A(S) \Rightarrow f : S \to S$ is one-to-one and onto.

By the above Lemma, $f^{-1} : S \to S$ exists, which is one-to-one and onto. Hence $f^{-1} \in A(S)$ and as shown above

$$fof^{-1} = f^{-1}of = i.$$

**Theorem 1.2.4.** *If $f$, $g$, $h$ are any three elements of $A(S)$, then*

1. $fog \in A(S)$.
2. $(fog)oh = fo(goh)$.
3. *There exists an element $i$ (the identity mapping) such that*
$$foi = iof = f, \quad \text{for each} \quad f \in A(S).$$
4. *For each $f \in A(S)$, there exists $f^{-1} \in A(S)$ such that*
$$fof^{-1} = f^{-1}of = i.$$

**Proof. 1.** Since $f, g \in A(S)$, therefore $f: S \to S$ and $g: S \to S$ are both one-to-one and onto.
By Lemma 1.2.2, $fog: S \to S$ is one-to-one and onto. Thus
$fog \in A(S)$.

**2.** It follows from the corollary of Lemma 1.2.1.

**3.** The identity mapping $i: S \to S$ defined by $i(x) = x$ for each $x \in S$ is obviously one-to-one and onto. Thus $i \in A(S)$.

For any $f \in A(S)$ and $x \in S$, we have

$$(f \circ i)(x) = f(i(x)) = f(x), \qquad (\because f(x) \in S)$$
$$(i \circ f)(x) = i(f(x)) = f(x).$$

Thus $foi = iof = f, \quad \forall \quad f \in A(S)$.

**4.** It follows from the corollary of Lemma 1.2.3.

## 1.3 Binary Composition

*The* **cartesian product** *of two sets S and T is defined as*

$$S \times T = \{(x, y) : x \in S, y \in T\}.$$

We say that $(x_1, y_1) = (x_2, y_2)$ if and only if $x_1 = x_2$ and $y_1 = y_2$.

**Definition.** *A mapping* $* : S \times S \to S$ *is called a* **binary composition** *on the set S, where* $S \times S = \{(a, b) : a, b \in S\}$.

The image of an element $(a, b) \in S \times S$ under $*$ is usually written as $a * b$.

**Note.** *If* $*$ *is a binary composition on a set S, then* $a * b \in S$ *for all* $a, b \in S$.

**Illustrations.**

1. Addition and multiplication are binary compositions in the set **N** of natural numbers, since $a + b \in \mathbf{N}$ and $a \cdot b \in \mathbf{N}$ for all $a, b \in \mathbf{N}$. However, subtraction is not a binary composition in **N**, since $2 \in \mathbf{N}$ and $3 \in \mathbf{N}$, but $2 - 3 = -1 \notin \mathbf{N}$.
2. Let $m * n = m + n + 1$, where $m, n \in \mathbf{Z}$.
   Then $*$ is a binary composition in the set of all odd integers, but $*$ is not a binary composition in the set of all even integers, since $2 * 4 = 2 + 4 + 1 = 7$, which is not an even integer.
3. Let $a * b = a + b - ab$ for all $a, b \in \mathbf{Z}$.
   Then $*$ is a binary composition in **Z**.
   Note that $3 * 4 = 3 + 4 - 12 = -5$,
   $-2 * 5 = -2 + 5 + 10 = 13$, $2 * 0 = 2 + 0 - 0 = 2$ etc.

## 1.4 Equivalence Relation

*If A is any non-empty set, then a subset R of* $A \times A$ *is defined as a* **relation** *on A.*

If $(a, b) \in R$, then we can express this fact as $aRb$ and speak it as : *a is R-related to b.*

**Definition.** *A subset $R$ of $A \times A$ is said to be an* **equivalence relation** *on $A$, if*

1. $(a, a) \in R$ *for all* $a \in A$. **(Reflexive Property)**
2. $(a, b) \in R$ *implies* $(b, a) \in R$. **(Symmetric Property)**
3. $(a, b) \in R$ *and* $(b, c) \in R$ *implies* $(a, c) \in R$. **(Transitive Property)**

*In other words, a relation $R$ on $A$ is said to be an* **equivalence relation** *on $A$, if for all $a, b, c \in A$ ;*

1. $aRa$. *(Reflexive Property)*
2. $aRb \Rightarrow bRa$. *(Symmetric Property)*
3. $aRb$ *and* $bRc \Rightarrow aRc$. *(Transitive Property)*

**Example 1.4.1.** *The relation $\sim$ on $\mathbf{Z}$ (set of all integers) defined by*

$$a \sim b \text{ iff } a\text{-}b \text{ is an even integer}$$

*is an equivalence relation.*

**1.** For all $a \in \mathbf{Z}$, $a - a = 0$ is even and so $a \sim a$.

**2.** For any $a, b \in \mathbf{Z}$ ; let $a \sim b \Rightarrow a - b$ is even

$\Rightarrow \quad b - a = -(a - b)$ is even $\Rightarrow \quad b \sim a$.

**3.** For any $a, b, c \in \mathbf{Z}$ ; let $a - b$ and $b \sim c$

$\Rightarrow a - b$ and $b - c$ are even $\Rightarrow (a - b) + (b - c)$ is even

$\Rightarrow a - c$ is even $\Rightarrow a \sim c$.

Hence the relation $\sim$ is an equivalence relation on $\mathbf{Z}$.

**Example 1.4.2.** *Let $n$ be a fixed positive integer and $a, b \in \mathbf{Z}$. Show that the relation $\equiv$ defined on $\mathbf{Z}$ as follows :*

$$a \equiv b \pmod{n} \text{ iff } n \text{ divides } a - b$$

*is an equivalence relation on $\mathbf{Z}$.*

*[The relation $a \equiv b \pmod{n}$ is read as* ***a is congruent to b modulo n.***]

**1.** Since $n$ divides $0 = a - a$, therefore

$$a \equiv a \pmod{n} \text{ for all } a \in \mathbf{Z}.$$

**2.** Let $a \equiv b \pmod{n}$. Then $n$ divides $(a - b)$ and so $n$ divides $-(a - b) = b - a$.

$\therefore \quad b \equiv a \pmod{n}$.

**3.** Let $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$. Then

$n$ divides $(a - b)$ and $n$ divides $(b - c)$

$\Rightarrow$ $n$ divides $[(a - b) + (b - c)] = a - c$

$\therefore \quad a \equiv c \pmod{n}$.

Hence the relation 'congruence modulo $n$' is an equivalence relation on $\mathbf{Z}$.

**Example 1.4.3.** *Show that the relation $\sim$ defined on $\mathbf{Z}$ as :*

$$a \sim b \text{ iff } a = b \ (a, b \in \mathbf{Z})$$

*is an equivalence relation on $\mathbf{Z}$.*

**Example. 1.4.4.** *Show that the relation ~ defined on* $\mathbf{Z}$ *as :*

$a \sim b$ *iff* $a - b$ *is a multiple of* $n$ ; $a, b \in \mathbf{Z}$ ($n > 1$ *is a fixed integer*)

*is an equivalence relation on* $\mathbf{Z}$.

**Hint.** $a \sim b$ iff $n$ divides $a - b$.

**Example 1.4.5.** *Show that the relation ~ defined on* $\mathbf{Z}$ *as :*

$a \sim b$ *iff* $a + b$ *is an even integer*

*is an equivalence relation on* $\mathbf{Z}$.

## 1.5 Equivalence Class

**Definition.** *If ~ is an equivalence relation on a non-empty set A, then the set*

$$\{x \in A : x \sim a\}$$

*is called the* **equivalence class** *of* $a \in A$.

We write it as $[a]$ or $cl\,(a)$. Thus

$$cl\,(a) = \{x \in A : x \sim a\}.$$

**Example 1.5.1.** *The relation* $\equiv$ *on* $\mathbf{Z}$ *defined by*

$a \equiv b \pmod 5$ *iff* 5 *divides* $a - b$ ; $a, b \in \mathbf{Z}$

*is an equivalence relation. Various equivalence classes in* $\mathbf{Z}$ *are :*

$$[0] = \{x \in \mathbf{Z} : x \sim 0\} = \{x \in \mathbf{Z} : x - 0 = x \text{ is divisible by } 5\}$$

or $$[0] = \{\ldots, -15, -10, -5, 0, 5, 10, 15, \ldots.\}.$$

$$[1] = \{x \in \mathbf{Z} : x \sim 1\} = \{x \in \mathbf{Z} : x - 1 \text{ is divisible by } 5\}$$

or $$[1] = \{\ldots, -14, -9, -4, 1, 6, 11, 16, \ldots.\}.$$

$$[2] = \{x \in \mathbf{Z} : x \sim 2\} = \{x \in \mathbf{Z} : x - 2 \text{ is divisible by } 5\}$$

or $$[2] = \{\ldots, -13, -8, -3, 2, 7, 12, 17, \ldots.\}.$$

$$[3] = \{\ldots, -12, -7, -2, 3, 8, 13, 18, \ldots.\}.$$

$$[4] = \{\ldots, -11, -6, -1, 4, 9, 14, 19, \ldots.\}.$$

It can be easily verified that

$$[5] = [0], [6] = [1], [7] = [2] \text{ etc.}$$

Also $[-1] = [4]$, $[-2] = [3]$ etc.

From the above discussion, we notice that the equivalence relation $a \equiv b \pmod 5$ on $\mathbf{Z}$ has 5 distinct equivalence classes :

$$[0], \quad [1], \quad [2], \quad [3], \quad [4].$$

These equivalence classes are mutually disjoint (*i.e.*, any pair has no common element) and further

$$\mathbf{Z} = [0] \cup [1] \cup [2] \cup [3] \cup [4].$$

These are the distinctive properties of all equivalence classes as shown in the following

**Theorem 1.5.1.** *If ~ be an equivalence relation on a non-empty set A, then A can be expressed as a union of mutually disjoint equivalence classes in A.*

**Proof.** Let $a, b \in A$. Since $a \sim a$, so $a \in cl\,(a)$. Thus $cl\,(a) \neq \phi$.

Now we show that either $cl\,(a) \cap cl\,(b) = \phi$ or $cl\,(a) = cl\,(b)$.

If $cl(a) \cap cl(b) = \phi$, there is nothing to prove.

Suppose $cl(a) \cap cl(b) \neq \phi$. We shall prove that $cl(a) = cl(b)$.

Let $t \in cl(a) \cap cl(b)$.

$\Rightarrow$ $t \in cl(a)$ and $t \in cl(b)$

$\Rightarrow$ $t \sim a$ and $t \sim b$

$\Rightarrow$ $a \sim t$ and $t \sim b$, by symmetry

$\Rightarrow$ $a \sim b$, by transitivity.

Let $x$ be any element of $cl(a)$ so that $x \sim a$.

Now $x \sim a$ and $a \sim b \Rightarrow x \sim b \Rightarrow x \in cl(b)$.

$\therefore$ $cl(a) \subseteq cl(b)$. ...(1)

Conversely, let $x$ be any element of $cl(b)$.

Then $x \sim b$. Since $a \sim b$, so $b \sim a$.

Now $x \sim b$ and $b \sim a \Rightarrow x \sim a \Rightarrow x \in cl(a)$

$\therefore$ $cl(b) \subseteq cl(a)$. ...(2)

From (1) and (2), $cl(2) = cl(b)$.

Thus any two equivalence classes are either equal or disjoint (*i.e.*, they have no element in common).

Lastly, we show that $A$ equals the union of all equivalence classes in $A$.

Let $a \in A$ be arbitrary. Since $a \sim a$, $a \in cl(a)$

$\Rightarrow$ $a \in \bigcup_{x \in A} cl(x)$.

Thus $A \subseteq \bigcup_{x \in A} cl(x)$. ...(3)

By definition, $cl(x) \subseteq A$ for each $x \in A$

$\Rightarrow$ $\bigcup_{x \in A} cl(x) \subseteq A$. ...(4)

From (3) and (4), $A = \bigcup_{x \in A} cl(x)$.

**Note.** *The above theorem is of great importance. It helps in proving many results of Abstract Algebra. The students are advised to remember the statement of the theorem.*

**Example. 1.5.2.** *Show that $a \equiv b \pmod 3$ is an equivalence relation on $\mathbf{Z}$ and that $\mathbf{Z} = [0] \cup [1] \cup [2]$.*

**Example. 1.5.3.** *Show that the relation congruence modulo $n$ has $n$ distinct equivalence classes $[0], [1], [2], \ldots, [n-1]$.*

*The set of these $n$ equivalence classes is denoted by $\mathbf{Z}_n$.* These equivalence classes are called the *residue classes of integers mod $n$.*

**Example 1.5.4.** *Show that the equivalence classes of $\mathbf{Z}$ for the equivalence relation $-$ of Example 1.4.5. are*

$$\{\ldots, -3, -1, 1, 3, \ldots\} \text{ and } \{\ldots, -4, -2, 0, 2, 4, \ldots\}.$$

## 1.6 Group

**Definition 1.** *A non-empty set $G$ with a binary composition $*$ is called a* **group**, *if the following conditions are satisfied :*

**G.1.** $a * b \in G$ *for all* $a, b \in G$. (Closure law).

**G.2.** $a * (b * c) = (a * b) * c$ *for all* $a, b, c \in G$. (Associative law).

**G.3.** *There exists an element* $e \in G$ *such that*
$a * e = e * a = a$ *for all* $a \in G$. (Existence of identity).
($e$ *is called* **identity** *in* $G$).

**G.4.** *For each* $a \in G$, *there exists an element* $a' \in G$ *such that*
$a * a' = a' * a = e$. (Existence of inverse)
($a'$ *is called* **inverse** *of* $a$ *and is written as* $a' = a^{-1}$)

We write a group $G$ w.r.t. binary composition $*$ as $(G, *)$.

**Remark.** From Theorem 1.2.4, it follows that

*The set $A(S)$ of all one-to-one mappings of a non-empty set $S$ onto itself is a group w.r.t. the product of mappings.*

**Definition 2.** *A group $G$ is called* **finite** *or* **infinite** *according as it contains a finite or infinite number of elements.*

*If a group $G$ contains $n$ elements, we say that the* **order** *of $G$ is $n$ and we write it as $o(G) = n$.*

**Definition 3.** *A group $(G, *)$ is called* **abelian** *or* **commutative**, *if*

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

**Definition 4.** *If $a$ be an element of a group $G$, then we define $a^0 = e$ and for any positive integer $n$, $a^n$ is defined as $a^n = a * a * a \ldots * a$ ($n$ times).*

*Also* $a^{-n} = (a^{-1})^n$.

It is easy to verify that $a^m * a^n = a^{m+n}$ and $(a^m)^n = a^{mn}$, where $m$ and $n$ are any two integers.

## 1.7 Examples of Groups

**Example 1.7.1.** $(\mathbf{I}, +)$ is a group, where 0 is the identity and the inverse of $a \in \mathbf{I}$ is $-a \in \mathbf{I}$.

Similarly, $(\mathbf{R}, +)$, $(\mathbf{Q}, +)$ are groups.

**Example 1.7.2.** $(\mathbf{N}, +)$ is not a group, as the axioms **G.3.** and **G.4.** are not satisfied in $\mathbf{N}$.

**Example 1.7.3.** The set $\mathbf{I}$ of integers is not a group under usual multiplication, since the axiom **G.4.** is not satisfied in $\mathbf{I}$.

**Example 1.7.4.** The set $\mathbf{R}^*$ of all non-zero real numbers is an abelian group under multiplication, where 1 is the identity and the inverse of $a \in \mathbf{R}^*$ is $1/a$.

**Example 1.7.5.** *The set $S_3 = \{i, \sigma_1, \sigma_2, \sigma_3, \tau_1, \tau_2\}$ is a non-abelian group of order 6 under the product of two mappings.*

Refer to Example 1.2.6. $S_3$ is the set of all one-to-one mappings of the set $\{1, 2, 3\}$ onto itself. The identity in $S_3$ is $i$. The inverse elements of $i, \sigma_1, \sigma_2, \sigma_3, \tau_1, \tau_2$ are $i, \sigma_1, \sigma_2, \sigma_3, \tau_2, \tau_1$ ; respectively.

It may be noticed that for $\sigma_2, \sigma_3 \in S_3$ ; where

$$\sigma_2 : \begin{matrix} 1 \to 3 \\ 2 \to 2 \\ 3 \to 1 \end{matrix}, \quad \sigma_3 : \begin{matrix} 1 \to 2 \\ 2 \to 1 \\ 3 \to 3 \end{matrix} ; \text{ then}$$

$$\sigma_2 o \sigma_3 : \begin{matrix} 1 \to 2 \\ 2 \to 3 \\ 3 \to 1 \end{matrix} \qquad \text{(First consider } \sigma_3 \text{ and then } \sigma_2\text{)}$$

$$\sigma_3 o \sigma_2 : \begin{matrix} 1 \to 3 \\ 2 \to 1 \\ 3 \to 2. \end{matrix} \qquad \text{(First consider } \sigma_2 \text{ and then } \sigma_3\text{)}$$

Thus $\sigma_2 o \sigma_3 \neq \sigma_3 o \sigma_2$.

**Remark.** *The group $S_3$ is a rich source of providing counter-examples in Group Theory.*

**Example 1.7.6.** The set $G = \{1, -1\}$ is an abelian group of order 2 under the multiplication of real numbers.

**Example 1.7.7.** The set $G = \{1, -1, i, -i\}$ $(i = \sqrt{-1})$ is a finite abelian group under usual multiplication of complex numbers, 1 being the identity and the inverse elements of $1, -1, i, -i$ being $1, -1, -i, i$ respectively.

**Example 1.7.8. (Quaternion Group)**

*The set $G = \{\pm 1, \pm i, \pm j, \pm k\}$, where*

$$i^2 = j^2 = k^2 = -1 \quad \text{and} \quad ij = -ji = k, jk = -kj = i,$$
$$ki = -ik = j$$

*is a non-abelian multiplication group of order 8. This group is called* **Quaternion Group**. *Here 1 is the identity. The inverse elements of 1, i, j, k are $1, -i, -j, -k$, respectively. Notice that $ij \neq ji$ etc.*

**Example 1.7.9.** *Show that $S = \{3^n : n \in \mathbf{Z}\}$ is a commutative group w.r.t. multiplication.*

(*i*) **Closure law.** Let $3^n \in S$ and $3^m \in S$. Then

$$3^n . 3^m = 3^{n+m} \in S, \text{ since } n + m \text{ is an integer.}$$

(*ii*) **Associative law.**

Clearly, $(3^n . 3^m) . 3^p = 3^n . (3^m . 3^p)$ ; $n, m, p \in \mathbf{Z}$.

(*iii*) **Identity.** $1 = 3^0$ is the identity of $S$.

(*iv*) **Inverse.** The inverse of $3^n \in S$ is $3^{-n} \in S$, since

$$3^n . 3^{-n} = 3^{n+(-n)} = 3^0 = 1.$$

(*v*) **Commutative law.**

$$3^n . 3^m = 3^{n+m} = 3^{m+n} = 3^m . 3^n \text{ ; } n, m \in \mathbf{Z}.$$

Hence $S$ is a commutative group.

Refer to Example 1.2.6. $S_3$ is the set of all one-to-one mappings of the set $\{1, 2, 3\}$ onto itself. The identity in $S_3$ is $i$. The inverse elements of $i, \sigma_1, \sigma_2, \sigma_3, \tau_1, \tau_2$ are $i, \sigma_1, \sigma_2, \sigma_3, \tau_2, \tau_1$ ; respectively.

It may be noticed that for $\sigma_2, \sigma_3 \in S_3$ ; where

$$\sigma_2 : \begin{matrix} 1 \to 3 \\ 2 \to 2 \\ 3 \to 1 \end{matrix}, \quad \sigma_3 : \begin{matrix} 1 \to 2 \\ 2 \to 1 \\ 3 \to 3 \end{matrix} ; \text{ then}$$

$$\sigma_2 o \sigma_3 : \begin{matrix} 1 \to 2 \\ 2 \to 3 \\ 3 \to 1 \end{matrix} \qquad \text{(First consider } \sigma_3 \text{ and then } \sigma_2)$$

$$\sigma_3 o \sigma_2 : \begin{matrix} 1 \to 3 \\ 2 \to 1 \\ 3 \to 2. \end{matrix} \qquad \text{(First consider } \sigma_2 \text{ and then } \sigma_3)$$

Thus $\sigma_2 o \sigma_3 \neq \sigma_3 o \sigma_2$.

**Remark.** *The group $S_3$ is a rich source of providing counter-examples in Group Theory.*

**Example 1.7.6.** The set $G = \{1, -1\}$ is an abelian group of order 2 under the multiplication of real numbers.

**Example 1.7.7.** The set $G = \{1, -1, i, -i\}$ $(i = \sqrt{-1})$ is a finite abelian group under usual multiplication of complex numbers, 1 being the identity and the inverse elements of $1, -1, i, -i$ being $1, -1, -i, i$ respectively.

**Example 1.7.8. (Quaternion Group)**

*The set $G = \{\pm 1, \pm i, \pm j, \pm k\}$, where*

$$i^2 = j^2 = k^2 = -1 \text{ and } ij = -ji = k, jk = -kj = i,$$
$$ki = -ik = j$$

*is a non-abelian multiplication group of order 8. This group is called* **Quaternion Group**. *Here 1 is the identity. The inverse elements of 1, i, j, k are $1, -i, -j, -k$, respectively. Notice that $ij \neq ji$ etc.*

**Example 1.7.9.** *Show that $S = \{3^n : n \in \mathbf{Z}\}$ is a commutative group w.r.t. multiplication.*

(*i*) **Closure law.** Let $3^n \in S$ and $3^m \in S$. Then

$$3^n . 3^m = 3^{n+m} \in S, \text{ since } n + m \text{ is an integer.}$$

(*ii*) **Associative law.**

Clearly, $(3^n . 3^m) . 3^p = 3^n . (3^m . 3^p)$ ; $n, m, p \in \mathbf{Z}$.

(*iii*) **Identity.** $1 = 3^0$ is the identity of $S$.

(*iv*) **Inverse.** The inverse of $3^n \in S$ is $3^{-n} \in S$, since

$$3^n . 3^{-n} = 3^{n+(-n)} = 3^0 = 1.$$

(*v*) **Commutative law.**

$$3^n . 3^m = 3^{n+m} = 3^{m+n} = 3^m . 3^n \text{ ; } n, m \in \mathbf{Z}.$$

Hence $S$ is a commutative group.

**Example 1.7.10.** *Prove that the set of all n nth roots of unity forms an abelian group w.r.t. multiplication.*

We have $(1)^{1/n} = (1 + 0\,i)^{1/n} = (\cos 0 + i \sin 0)^{1/n}$

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

$$= e^{2k\pi i/n}, k = 0, 1, 2, \ldots, n-1. \qquad [\because e^{i\theta} = \cos\theta + i \sin\theta]$$

Thus the set of all $n$ nth roots of unity is

$$G = \{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}, \text{ where } \alpha = e^{2\pi i/n}.$$

It is clear that $G$ is an abelian group w.r.t. multiplication of complex numbers, where 1 is the identity and the inverse of any element $\alpha^r (1 \le r \le n-1)$ is $\alpha^{n-r} \in G$, since $\alpha^r \cdot \alpha^{n-r} = \alpha^n = 1$.

**Example 1.7.11.** *The set $M_2$ of all $2 \times 2$ matrices :*

$$M_2 = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbf{R} \right\}$$

*is an abelian group under the addition of two matrices.*

Note that the identity in $M_2$ is $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$,

and the inverse of $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is $\begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$.

**Example 1.7.12.** *Show that the set of matrices*

$$G = \left\{ \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}, \alpha \in \mathbf{R} \right\}$$

*forms a group under matrix multiplication.*

(*i*) **(Closure law).**

Let $A_\alpha = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$ and $A_\beta = \begin{pmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{pmatrix} \in G.$

Then

$$A_\alpha A_\beta = \begin{bmatrix} \cos\alpha\cos\beta - \sin\alpha\sin\beta & -(\cos\alpha\sin\beta + \sin\alpha\cos\beta) \\ \sin\alpha\cos\beta + \cos\alpha\sin\beta & \cos\alpha\cos\beta - \sin\alpha\sin\beta \end{bmatrix}$$

$$= \begin{bmatrix} \cos(\alpha+\beta) & -\sin(\alpha+\beta) \\ \sin(\alpha+\beta) & \cos(\alpha+\beta) \end{bmatrix} = A_{\alpha+\beta} \in G.$$

Note that $A_\alpha A_\beta = A_{\alpha+\beta}$. ...(1)

(*ii*) We know that the matrix multiplication is associative.

(*iii*) **(Identity)** $I_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the identity in $G$,

since $A_\alpha I_0 = I_0 A_\alpha = A_\alpha$ for all $A_\alpha \in G$.

(*iv*) **(Inverse).** $A_{-\alpha}$ is the inverse of $A_\alpha$ for each $A_\alpha \in G$, since

$$A_\alpha A_{-\alpha} = A_{\alpha+(-\alpha)} = A_0 = I_0$$

**Example 1.7.13.** *Show that* $G=\left\{\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \neq 0 \in \mathbf{R}\right\}$ *is an abelian group under matrix multiplication.*

(*i*) **(Closure law).**

Let $A=\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}, B=\begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} \in G$. Then $AB=\begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix} \in G$.

(*ii*) **(Commutative law).** $AB = BA$ is true $\forall\ A, B \in G$, since

$$AB = BA = \begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix}.$$ (Note $ab = ba$ is true in **R**).

(*iii*) Matrix multiplication is associative.

(*iv*) **(Identity)** $I=\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in G$ is the identity in $G$, since

$$AI=\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}=\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}=A \quad \forall\ A \in G.$$

(*v*) **(Inverse).** If

$$A=\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \in G \text{ , then } A^{-1}=\begin{pmatrix} 1/a & 0 \\ 0 & 0 \end{pmatrix} \in G$$

is the inverse of $A$, since

$$AA^{-1}=\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}=I.$$ (Note that $a \neq 0 \in \mathbf{R} \Rightarrow 1/a \neq 0 \in \mathbf{R}$)

Hence $G$ is an abelian group under matrix multiplication.

**Example 1.7.14.** *Prove that the following matrices :*

$$I=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, A=\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, B=\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \text{ and } C=\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

*form a group under the multiplication of two matrices.*

Let $G = \{I, A, B, C\}$.

**Closure law.** We have

$$AB=\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}=C,\ BC=\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}=A,$$

$$AC = B,\ AI = A,\ AA = I \quad \text{etc.}$$

Thus the product of any two matrices of $G$ is an element of $G$.

**Associative law.** We know that the matrix multiplication is associative.

**Identity.** Obviously $I=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the identity in $G$, since

$$AI = A,\ BI = B,\ CI = C,\ II = I.$$

**Inverse.** We can verify that $AA = BB = CC = I$.

Thus $A^{-1} = A, B^{-1} = B, C^{-1} = C$ and $I^{-1} = I$.

Hence $G$ is a group under the multiplication of two matrices.

It can be verified that $G$ is abelian too.

**Example 1.7.15.** *Show that the set $S$ of all $2 \times 2$ non-singular matrices over* **R** *is a group under matrix multiplication.*

A matrix $P$ of order $n \times n$ is called a **non-singular matrix** if its determinant $|P| \neq 0$.

It is a well known fact that the inverse $P^{-1}$ of a matrix $P$ exists if and only if $P$ is non-singular.

(*i*) **Closure law.**

Let $A, B \in S$ so that $|A| \neq 0$ and $|B| \neq 0$.

Now $|AB| = |A||B| \neq 0$ and so $AB \in S$.

(*ii*) **Associative law.** We know matrix multiplication is associative.

(*iii*) **Identity.** $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the identity element of $S$.

(*iv*) **Inverse.** Let $A \in S$ so that $A$ is non-singular. Then $A^{-1} \in S$ exists and

$$AA^{-1} = A^{-1}A = I_2.$$

Hence $S$ is a group, which is non-abelian, since

$$\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$$

and so $\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$.

It may be noted that if

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, ad - bc \neq 0, \text{ then } A^{-1} = \frac{1}{ad - bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

**Remark.** *The set of all $n \times n$ non-singular matrices over* **R** *is a group under matrix multiplication.*

**Example 1.7.16. (The Group of Integers Modulo $n \equiv \mathbf{J}_n$ or $\mathbf{Z}_n$).**

For any positive integer $n$, let us take

$$\mathbf{J}_n = \{0, 1, 2, \ldots, n-1\}.$$

We define two binary compositions $\oplus_n$ and $\odot_n$ in $\mathbf{J}_n$ as follows :

For any $a, b \in \mathbf{J}_n$ ;

$a \oplus_n b$ = *least non-negative remainder obtained when $a + b$ is divided by $n$*

$a \odot_n b$ = *least non-negative remainder obtained when $ab$ is divided by $n$*

The compositions $\oplus_n$ and $\odot_n$ are called **addition modulo $n$** and **multiplication modulo $n$**, respectively.

When $n = 5$, we have

$$J_5 = \{0, 1, 2, 3, 4\}.$$

It is easy to verify that

$3 \oplus_5 4 = 2$, *since the least non-negative remainder when* $3 + 4 = 7$ *is divided by* 5 *is* 2.

$4 \odot_5 2 = 3$, *since the least non-negative remainder when* $4.2 = 8$ *is divided by* 5 *is* 3.

Now we show that

$J_5 = \{0, 1, 2, 3, 4\}$ *is an abelian group w.r.t. addition modulo* 5.

We shall write all the elements of the form $a \oplus_5 b$ $(a, b \in J_5)$ in the form of a table known as **composition table.** The composition table of $J_5$ consists of 5 rows and 5 columns in which the entry at the intersection of a row headed by an element $a \in J_5$ and the column headed by an element $\in J_5$ is $a \oplus_5 b$.

The composition table of $J_5$ w.r.t. $\oplus_5$ is as follows :

| $\oplus_5$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 |
| 1 | 1 | 2 | 3 | 4 | 0 |
| 2 | 2 | 3 | 4 | 0 | 1 |
| 3 | 3 | 4 | 0 | 1 | 2 |
| 4 | 4 | 0 | 1 | 2 | 3 |

From the composition table, we notice that 0 is the identity element, since $a \oplus_5 0 = a \ \forall \ a \in J_5$.

The inverse elements of 0, 1, 2, 3, 4 are 0, 4, 3, 2, 1 respectively.

**Remark.** $\{J_n, \oplus_n\}$ is an abelian group called the **group of integers under addition modulo $n$.**

**Example 1.7.17.** *The set* $S = \{1, 2, 3, 4, 5\}$ *is* **not** *a group w.r.t. multiplication modulo* 6, *since* $2 \odot_6 3 = 0 \notin S$.

**Example 1.7.18.** *The set* $S = \{1, 2, 3, 4\}$ *is an abelian group under* $\odot_5$, *multiplication modulo* 5.

The composition table of $S$ w.r.t. $\odot_5$ is as follows :

| $\odot_5$ | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 |
| 2 | 2 | 4 | 1 | 3 |
| 3 | 3 | 1 | 4 | 2 |
| 4 | 4 | 3 | 2 | 1 |

From the composition table, we notice that 1 is the identity element of $S$ and the inverse elements of 1, 2, 3, 4 are 1, 3, 2, 4 respectively.

**Remark.** For any positive prime integer $p$, the set

$$S = \{1, 2, 3, \ldots, p-1\}$$

is an abelian group under $\odot_p$, multiplication modulo $p$.

**Example 1.7.19.** *Show that the set* $S = \{1, 5, 7, 11\}$ *is a group w.r.t. multiplication modulo 12.*

The composition table of $S$ w.r.t. $\odot_{12}$ is as follows :

| $\odot_{12}$ | 1 | 5 | 7 | 11 |
|---|---|---|---|---|
| 1 | 1 | 5 | 7 | 11 |
| 5 | 5 | 1 | 11 | 7 |
| 7 | 7 | 11 | 1 | 5 |
| 11 | 11 | 7 | 5 | 1 |

Notice that $5 \odot_{12} 7 = 35$, which on division by 12 gives the remainder 11, $11 \odot_{12} 7 = 77$, which on division by 12 gives the remainder 5 etc.

Hence $S$ is a group, in which 1 is the identity and each element of $S$ is its own inverse.

**Example 1.7.20.** *Prove that* $\{S, \odot_{14}\}$ *is a group,* $S = \{2, 4, 8\}$.

The composition table of $S$ w.r.t. $\odot_{14}$ is as follows :

| $\odot_{14}$ | 2 | 4 | 8 |
|---|---|---|---|
| 2 | 4 | 8 | 2 |
| 4 | 8 | 2 | 4 |
| 8 | 2 | 4 | 8 |

Hence $\{S, \odot_{14}\}$ is a group, in which 8 is the identity

$(2 \odot_{14} 8 = 2,\ 4 \odot_{14} 8 = 4,\ 8 \odot_{14} 8 = 8)$

and the inverse elements of 2, 4, 8 are 4, 2, 8 respectively.

(iv) **Inverse.** The inverse of $(a, b) \in G$ is $(-a, -b) \in G$.

(v) **Commutative law.** $(a, b) * (c, d) = (a + c, b + d)$
$= (c + a, d + b) = (c, d) * (a, b)$.

Hence $(G, *)$ is a commutative group.

## 1.8 Properties of Groups

For the sake of convenience, we shall now onwards write the binary composition $*$ as $.$ ($.$ is called the **product**). The statement that $G$ is a *group will henceforth mean that* $(G, .)$ *is a group.*

**Theorem 1.8.1.** *If $G$ is a group, then*

(i) *identity element of $G$ is unique,*

(ii) *inverse of every element of $G$ is unique.*

**Proof.** (i) Let $e_1$ and $e_2$ be two identity elements in $G$.

Then $a \cdot e_1 = e_1 \cdot a = a \quad \forall \quad a \in G,$ ...(1)

and $a \cdot e_2 = e_2 \cdot a = a \quad \forall \quad a \in G.$ ...(2)

Taking $a = e_2$ in (1), $e_1 \cdot e_2 = e_2$.

Taking $a = e_1$ in (2), $e_1 \cdot e_2 = e_1$. Hence $e_1 = e_2$.

(ii) Suppose $a \in G$ has two inverse elements $b$ and $c$ in $G$. Then

$a \cdot b = b \cdot a = e,$ ...(3)

$a \cdot c = c \cdot a = e.$ ...(4)

Consider $b = b \cdot e$, since $e$ is the identity in $G$

$= b \cdot (a \cdot c)$, using (4)

$= (b \cdot a) \cdot c$, by associative law in $G$

$= e \cdot c$, using (3)

$\therefore \quad b = c$, since $e$ is the identity in $G$.

Hence inverse of $a \in G$ is unique.

**Theorem 1.8.2. (Cancellation laws)**

*If $G$ is a group and $a, b, c \in G$, then*

(i) $a \cdot b = a \cdot c \Rightarrow b = c$. *(left cancellation law)*

(ii) $b \cdot a = c \cdot a \Rightarrow b = c$. *(right cancellation law)*

**Proof.** (i) Consider $a \cdot b = a \cdot c$. ...(1)

Since $a \in G, a^{-1} \in G$ and so by (1),

$a^{-1} \cdot (a \cdot b) = a^{-1} \cdot (a \cdot c)$

or $(a^{-1} \cdot a) \cdot b = (a^{-1} \cdot a) \cdot c$, (associative law)

or $e \cdot b = e \cdot c, \quad (\because a^{-1} \cdot a = e)$

or $b = c$, since $e$ is the identity in $G$.

Similarly, $b \cdot a = c \cdot a \Rightarrow (b \cdot a) \cdot a^{-1} = (c \cdot a) \cdot a^{-1}$

$\Rightarrow \quad b \cdot (a \cdot a^{-1}) = c \cdot (a \cdot a^{-1}) \Rightarrow b \cdot e = c \cdot e \Rightarrow b = c.$

**Theorem 1.8.3.** *If $G$ is a group and $a, b \in G$, then*

(*i*) $(a^{-1})^{-1} = a$.

(*ii*) $(a \,.\, b)^{-1} = b^{-1} \,.\, a^{-1}$.

**Proof.** (*i*) By definition, we have

$a^{-1} \,.\, a = e$ and $a^{-1} \,.\, (a^{-1})^{-1} = e$.

$\therefore \quad a^{-1} \,.\, a = a^{-1} \,.\, (a^{-1})^{-1}$.

Hence, by left cancellation law, $(a^{-1})^{-1} = a$.

(*ii*) Let $c = a \,.\, b$ and $d = b^{-1} \,.\, a^{-1}$. Then

$c \,.\, d = (a \,.\, b) \,.\, d = a \,.\, (b \,.\, d)$, by associative law

$= a \,.\, [b \,.\, (b^{-1} \,.\, a^{-1})]$.

$= a \,.\, [(b \,.\, b^{-1}) \,.\, a^{-1}]$, by associative law

$= a \,.\, (e \,.\, a^{-1}), \quad (\because\ b \,.\, b^{-1} = e)$

$= a \,.\, a^{-1}$, since $e$ is the identity

$\therefore \quad c \,.\, d = e$.

Similarly, $d \,.\, c = e$. $\therefore \quad c^{-1} = d$.

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

**Theorem 1.8.4.** *Show that in a group $G$, the equations $a \,.\, x = b$ and $y \,.\, a = b$ have unique solutions for all $a, b$ in $G$.*

**Proof.** Since $G$ is a group, so $a^{-1} \in G$ exists uniquely for each $a \in G$.

Consider the equation $a \,.\, x = b$. Then

$a^{-1} \,.\, (a \,.\, x) = a^{-1} \,.\, b \Rightarrow (a^{-1} \,.\, a) \,.\, x = a^{-1} \,.\, b$, by associative law

$\Rightarrow \quad e \,.\, x = a^{-1} \,.\, b$, since $a \,.\, a^{-1} = a^{-1} \,.\, a = e$

$\Rightarrow \quad x = a^{-1} \,.\, b$, since $x \,.\, e = e \,.\, x = x \ \forall\ x \in G$.

Hence $x = a^{-1} \,.\, b \in G$ is the unique solution of $a \,.\, x = b$.

Similarly, $y \,.\, a = b \quad \Rightarrow (y \,.\, a) \,.\, a^{-1} = b \,.\, a^{-1}$

$\Rightarrow \quad y \,.\, (a \,.\, a^{-1}) = b \,.\, a^{-1} \Rightarrow \quad y \,.\, e = b \,.\, a^{-1} \Rightarrow y = b \,.\, a^{-1} \in G$.

Hence $y = b \,.\, a^{-1}$ is the unique solution of $y \,.\, a = b$.

**Definition. (Semi-group)** *A non-empty set $G$ with a binary composition . is called a* **semi-group**, *if*

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

It is clear that *every group is a semi-group, but the converse need not be true.*

For example, the set **N** of natural numbers is a semi-group under multiplication, but **N** is not a group under multiplication.

**Ex.** *Define a semi-group and group. Give an example of a finite semi-group which is not a group.* [D.U., 1997]

**Hint.** $S = \{0, 1, -1\}$ is a finite semi-group under multiplication but $S$ is not a group under multiplication, since $0 \in S$ has no multiplicative inverse.

**Theorem 1.8.5.** *Show that a semi-group $G$ in which the equations $a \cdot x = b$ and $y \cdot a = b$ are solvable for every pair of elements $a, b$ is a group.* [D.U., 1997]

**Proof.** It is given that for **each** pair $a, b \in G$; there exist some elements $x, y \in G$ such that

$$a \cdot x = b \quad \text{and} \quad y \cdot a = b. \qquad \ldots(1)$$

In particular, for $a, a \in G$, there exist some elements $e, f \in G$ such that

$$a \cdot e = a \quad \text{and} \quad f \cdot a = a. \qquad \ldots(2)$$

For **any** $b \in G$, we have

$$b \cdot e = (y \cdot a) \cdot e, \text{ by (1)}$$
$$= y \cdot (a \cdot e), \text{ since } G \text{ is a semi-group}$$
$$= y \cdot a, \text{ by (2)}$$
$$= b, \text{ by (1)}.$$

$\therefore \quad b \cdot e = b \quad \forall \quad b \in G. \qquad \ldots(3)$

Again $f \cdot b = f \cdot (a \cdot x)$, by (1)

$$= (f \cdot a) \cdot x = a \cdot x = b, \text{ by (2) and (1)}.$$

$\therefore \quad f \cdot b = b \quad \forall \quad b \in G. \qquad \ldots(4)$

Taking $b = f$ in (3), $f \cdot e = f$.

Taking $b = e$ in (4), $f \cdot e = e$.

$\therefore \quad e = f. \qquad \ldots(5)$

Using (5) in (3) and (4), we see that

$$b \cdot e = e \cdot b = b \quad \forall \quad b \in G.$$

Thus $e \in G$ is the identity of $G$.

Again for the pair $a, e \in G$, there exist some elements $p, q \in G$ such that

$$a \cdot p = e \quad \text{and} \quad q \cdot a = e, \qquad \ldots(6)$$

Now $p = e \cdot p$, since $e$ is the identity of $G$

$$= (q \cdot a) \cdot p, \text{ by (6)}$$
$$= q \cdot (a \cdot p), \text{ since } G \text{ is a semi-group}$$
$$= q \cdot e, \text{ by (6)}$$
$$= q, \text{ since } e \text{ is the identity of } G$$

$\therefore \quad p = q.$

Using in (6), we have

$$a \cdot p = p \cdot a = e \quad \Rightarrow \quad a^{-1} = p \in G.$$

Thus each element $a \in G$ has its inverse in $G$. Hence $G$ is a group.

**Theorem 1.8.6.** *Show that a semi-group $G$ is a group if and only if for any $a, b \in G$, the equations $a \,.\, x = b$ and $y \,.\, a = b$ have solutions in $G$.*

*Or*

*A non-empty set $G$ with a binary composition . is a group if and only if*

(*i*) $a \,.\, (b \,.\, c) = (a \,.\, b) \,.\, c$ *for all* $a, b, c \in G$.

(*ii*) *For any* $a, b \in G$, *the equations* $a \,.\, x = b$ *and* $y \,.\, a = b$ *have solutions in* $G$.

**Proof. Condition is sufficient**

Suppose $G$ is a semi-group such that for any $a, b \in G$, the equations $a \,.\, x = b$ and $y \,.\, a = b$ have solutions in $G$. Then by Theorem 1.8.5, $G$ is a group.

**Condition is necessary**

Suppose $G$ is a group. By Theorem 1.8.4, the equations $a \,.\, x = b$ and $y \,.\, a = b$ have solutions in $G$ for all $a, b \in G$.

**Theorem 1.8.7.** *Suppose a finite set $G$ is closed under an associative product and that both concellation laws hold in $G$. Prove that $G$ must be a group.*

*Or*

*Show that a finite semi-group $G$ in which cancellation laws hold is a group.*

**Proof.** Suppose $G = \{a_1, a_2, \ldots, a_n\}$ ...(1)

is a finite semi-group in which both the cancellation laws hold. In order to prove that $G$ is a group, we shall show $G$ has the identity and further each element in $G$ possesses inverse in $G$. Let $a$ be *any* element of $G$. Here $a$ is one of $a_i$'s for $1 \le i \le n$. Since $G$ satisfies closure law, therefore

$$a \,.\, a_1, a \,.\, a_2, \ldots, a \,.\, a_n \qquad \ldots(2)$$

are elements of $G$ and further they are all distinct, for if

$$a \,.\, a_i = a \,.\, a_j \quad \text{for some} \quad i \neq j,$$

then by left cancellation law, $a_i = a_j$, which is a contradiction. Thus the list of elements in (2) is a mere rearrangement of (1). Similarly, by using right cancellation law, it follows that

$$a_1 \,.\, a,\ a_2 \,.\, a, \ldots, a_n \,.\, a \qquad \ldots(3)$$

are all distinct elements of $G$.

Let $a_i$ be **any** element of $G$ $(1 \le i \le n)$. Then $a_i$ must be one of the elements listed in (3).

Let $a_i = a_j \,.\, a$, for some $j$ satisfying $1 \le j \le n$. ...(4)

Since $a \in G$, then as argued above

$$a = a_k \,.\, a; \text{ for some } k \text{ satisfying } 1 \le k \le n. \qquad \ldots(5)$$

Consider $a_i \,.\, a = a_i \,.\, (a_k \,.\, a)$, by (5)

$a_i \cdot a = (a_i \cdot a_k) \cdot a$, since $G$ is a semi-group

$\Rightarrow$ $a_i \cdot a = a_i \cdot a_k$, by right cancellation law

$\Rightarrow$ $a_i = a_i \cdot a_k$ for all $i$, $1 \le i \le n$. ...(6)

Thus

Similarly, by taking $a_i$ to be one of the elements listed in (2), we have

$a_i = a_l \cdot a_i$ for all $i$ and for some $l$, $1 \le l \le n$. ...(7)

In particular, $a_k = a_l \cdot a_k$ [Take $i = k$ in (7)]

$= a_l$ [Take $i = l$ in (6)] ...(8)

$\therefore$ $a_k = a_l$.

Using (8) in (6) and (7), we get

$a_i \cdot a_k = a_k \cdot a_i = a_i$ for all $i = 1, 2, \ldots, n$.

Hence $a_k$ is the identity element in $G$.

We write $e$ for $a_k$. Since $e \in G$, so by (2) and (3),

$e = a \cdot a_p$ for some $p$, $1 \le p \le n$, ...(9)

and $e = a_q \cdot a$ for some $q$, $1 \le q \le n$. ...(10)

Now $a_p = e \cdot a_p$, since $e$ is the identity in $G$

$= (a_q \cdot a) \cdot a_p$, by (10)

$= a_q \cdot (a \cdot a_p)$

$= a_q \cdot e$, by (9)

$= a_q$, since $e$ is the identity in $G$.

Using $a_p = a_q$ in (9) and (10), we get

$a \cdot a_p = a_p \cdot a = e$

$\Rightarrow$ $a^{-1} = a_p \in G$.

Thus each $a \in G$ has its inverse in $G$. Hence $G$ is a group.

**Remark 1.** *The above theorem may not hold in an infinite semi-group.*

For example, the set N of natural numbers is an infinite semi-group under addition in which both the cancellation laws hold *i.e.*,

$a + b = a + c \Rightarrow b = c$

$b + a = c + a \Rightarrow b = c$ ; $a, b, c \in \mathbf{N}$

but (N, +) is not a group.

**Remark 2.** *The conclusion of the above theorem may not follow, if only one of the cancellation laws holds in a finite semi-group G.*

Let $G$ be a finite set having at least two elements. Define a composition on $G$ as follows :

$a \cdot b = b$ for all $a, b \in G$.

For any $a, b, c \in G$, we have ...(1)

13. Show that the set $Q_4$ consisting of the following matrices :

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ -1 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix},$$
$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}$$

is a non-abelian group under matrix multiplication.

14. Show that

$$G = \left\{ \begin{pmatrix} x & y \\ x & y \end{pmatrix} : x, y \in \mathbf{R}, x + y \neq 0 \right\}$$

is a semi-group under matrix multiplication and has a left identity and a right inverse for each element. Hence $G$ is not a group.

[**Hint.** $\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$ is the left identity of $G$ and

$$\begin{pmatrix} x & y \\ x & y \end{pmatrix}^{-1} = \begin{pmatrix} (x+y)^{-1} & 0 \\ (x+y)^{-1} & 0 \end{pmatrix}. \ ]$$

15. Show that the set $G = \{e, a, b, ab\}$, where

$$a^2 = b^2 = e, \quad ab = ba$$

is an abelian group. *This group is known as* **Klein's 4-group.**

[**Hint.** $(ab)^2 = abab = aabb = a^2b^2 = ee = e$.]

16. For any two real numbers $a, b \in \mathbf{R}$, define a mapping

$$f_{ab} : \mathbf{R} \to \mathbf{R} \quad \text{as} \quad f_{ab}(x) = ax + b \quad \forall \quad x \in \mathbf{R}.$$

Let $G = \{f_{ab} : a \neq 0\}$. Prove that $G$ is a group under the composition of mappings..

[For the solution, see Example 1.14.20.]

17. If $n$ is a positive integer, show that the set $U_n$ of integers less than $n$ and relatively prime to $n$ is a group under multiplication mod $n$.

## 1.9 Subgroup

**Definition.** *Let $\{G, .\}$ be a group. A non-empty subset $H$ of $G$ is called a* **subgroup** *of $G$, if $\{H, .\}$ is a group.*

A subgroup $H$ of $G$ is conveniently written as $H < G$.

**Illustrations.**

1. $H = \{1, -1\}$ is a subgroup of $G = \{1, -1, i, -i\}$.
2. $\{E, +\} < \{I, +\}$, where E is the set of all even integers.
3. Let $H = \{3x : x \in I\} = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$

   Then $\{H, +\} < \{I, +\}$.

**Note.** We shall now onwards drop the composition . while writing $a \cdot b$. Thus we shall write $a \cdot b$ as $ab$, $a \cdot b^{-1}$ as $ab^{-1}$, $a \cdot (b \cdot c)$ as $a(bc)$ etc.

**Theorem 1.9.1.** *A non-empty subset $H$ of a group $G$ is a subgroup of $G$ if and only if $ab^{-1} \in H$ for all $a, b \in H$.* [D.U., 1995, 94]

*Or*

$H < G \Leftrightarrow ab^{-1} \in H \; \forall \; a \in H, b \in H.$

**Proof. The condition is necessary**

Let $H$ be a subgroup of $G$ and $a, b \in H$.

Since $H$ is itself a group, $b^{-1} \in H$.

Hence $a \in H$ and $b^{-1} \in H \Rightarrow ab^{-1} \in H$.

**Condition is sufficient**

Let $ab^{-1} \in H \quad \forall \quad a, b \in H.$ ...(1)

Taking $b = a$ in (1), $e = aa^{-1} \in H$. Thus $e \in H$.

Taking $a = e$ in (1), $eb^{-1} \in H \Rightarrow b^{-1} \in H \; \forall \; b \in H$.

Let $a \in H$ and $b \in H$ so that $a \in H$ and $b^{-1} \in H$.

By (1), $\quad a(b^{-1})^{-1} \in H \;\Rightarrow\; ab \in H. \qquad (\because (b^{-1})^{-1} = b)$

Obviously, associative law holds in $H \subseteq G$.

Thus $\{H, .\}$ is a group, which proves that $H$ is a subgroup of $G$.

**Remark.** *If the composition in $G$ is denoted by $+$, then*

$$H < G \Leftrightarrow a - b \in H \quad \forall \quad a, b \in H.$$

**Theorem 1.9.2.** *A non-empty subset $H$ of a group $G$ is a subgroup of $G$ if and only if the following conditions hold :*

(*i*) $a \in H$ and $b \in H \Rightarrow ab \in H$.

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

**Proof.** Let $H$ be a subgroup of $G$. Since $\{H, .\}$ is a group, the conditions (*i*) and (*ii*) are obviously satisfied.

To prove the converse part, let $H \subseteq G$ satisfy (1) and (2). It is obvious that the associative law holds in $H$, since $H \subseteq G$.

Let $\quad a \in H$ so that by (2), $a^{-1} \in H$.

Now $a \in H$ and $a^{-1} \in H \;\Rightarrow e = aa^{-1} \in H$, by (1).

Hence $H$ is a subgroup of $G$.

**Theorem 1.9.3.** *The intersection of two subgroups of a group $G$ is a subgroup of $G$.*

**Proof.** Let $H$ and $K$ be any two subgroups of $G$. We have to show that $H \cap K$ is a subgroup of $G$. Obviously, $H \cap K$ is non-empty, since $e \in H \cap K$. Let $a, b \in H \cap K$ so that $a, b \in H$ and $a, b \in K$.

Since $H < G, ab^{-1} \in H$. Similarly, $ab^{-1} \in K$.

Thus $ab^{-1} \in H \cap K \quad \forall \quad a, b \in H \cap K$

Hence by Theorem 1.9.1, $H \cap K$ is a subgroup of $G$.

**Remark.** *The union of two subgroups of a group $G$ need not be a subgroup of $G$.*

Let $G = (\mathbf{I}, +)$. Then

$H = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$, and $K = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$

are subgroups of $G$, but

$H \cup K = \{\ldots, -6, -4, -3, -2, 0, 2, 3, 4, 6, \ldots\}$

is **not** a subgroup of $G$, since $2, 3 \in H \cup K$ but $2 + 3 = 5 \notin H \cup K$.

**Theorem 1.9.4.** *The intersection of an arbitrary number of subgroups of a group $G$ is a subgroup of $G$.* [D.U., 1993]

**Proof.** Let $\{H_\lambda : \lambda \in \Delta\}$ be an arbitrary family of subgroups of a group $G$. We shall show that $\bigcap_{\lambda \in \Delta} H_\lambda$ is a subgroup of $G$. Obviously, $\bigcap_{\lambda \in \Delta} H_\lambda$ is non-empty, since $e \in H_\lambda$, for each $\lambda \in \Delta$.

Let $a, b$ be any two elements of $\bigcap_{\lambda \in \Delta} H_\lambda$. Then $a, b \in H_\lambda$, for each $\lambda \in \Delta$. Since $H_\lambda$ is a subgroup of $G$, so

$$ab^{-1} \in H_\lambda \text{ for each } \lambda \in \Delta$$

$$\Rightarrow \quad ab^{-1} \in \bigcap_{\lambda \in \Delta} H_\lambda. \quad \text{Hence } \bigcap_{\lambda \in \Delta} H_\lambda \text{ is a subgroup of } G.$$

**Theorem 1.9.5.** *If $H$ and $K$ are two subgroups of a group $G$, then $H \cup K$ is a subgroup of $G$ if and only if either $H \subset K$ or $K \subset H$.* [D.U., 1995, 94]

**Proof. Condition is necessary**

Suppose $H \cup K$ is a subgroup of $G$. We have to show that either $H \subset K$ or $K \subset H$. Suppose $H \not\subset K$. Then there eixsts some element $a \in H$ such that $a \notin K$. We shall prove that $K \subset H$. Let $k \in K$ be arbitrary. Since $a \in H$ and $k \in K$ ; $a, k \in H \cup K \Rightarrow ak \in H \cup K$, as $H \cup K$ is a subgroup of $G$

$\Rightarrow \quad ak \in H$ or $ak \in K$.

If $ak \in K$, then $a \in K$ (as $k \in K$ and $K < G$).

This is contrary to the assumption that $a \notin K$.

Thus $ak \in H$ and so $k \in H$, since $a \in H$ and $H < G$.

Hence $K \subset H$.

Similarly, we can show that if $K \not\subset H$, then $H \subset K$.

**Condition is sufficient**

Suppose $H \subset K$ or $K \subset H$.

Then $H \cup K = K$ or $H \cup K = H$.

In any case, $H \cup K$ is a subgroup of $G$ (since $H$ and $K$ are both subgroups of $G$).

**Theorem 1.9.6.** *If $H$ is a non-empty finite subset of a group $G$ such that $ab \in H$ for all $a, b \in H$, then $H$ is a subgroup of $G$.*

*Or*

*If $H$ is a non-empty finite subset of a group $G$ and $H$ is closed under the binary composition of $G$, then show that $H$ is a subgroup of $G$.*

**Proof.** By virtue of Theorem 1.9.2, it is sufficient to show that $a \in H$ implies that $a^{-1} \in H$.

Let $a \in H$. Then $a^2 = aa \in H$, $a^3 = a^2a \in H$, $a^4 = a^3a \in H$ and so on, since $H$ is closed under multiplication. Thus the infinite collection of elements $a, a^2, a^3, a^4, \ldots$ must all belong to $H$.

Since $H$ is a finite subset of $G$, we must have

$$a^m = a^n, \text{ for some integers } m \text{ and } n \text{ satisfying } m > n > 0$$

$$\Rightarrow \quad a^{m-n} = e. \qquad \ldots(1)$$

Now $m > n > 0 \Rightarrow m - n \geq 1 \Rightarrow m - n - 1 \geq 0$ and so $a^{m-n-1} \in H$.

Consider $aa^{m-n-1} = a^{m-n} = e$, by (1). Similarly, $a^{m-n-1}a = e$.

Thus $a^{-1} = a^{m-n-1} \in H$ and so $H$ is a subgroup of $G$.

## EXAMPLES

**Example 1.9.1.** *Show that $H = \{(1, b) : b \in \mathbf{R}\}$ is a subgroup of the group $G = \{(a, b) : a \neq 0, b \in \mathbf{R}\}$ under the composition $*$ given by*

$$(a, b) * (c, d) = (ac, bc + d). \qquad \ldots(1)$$

**Solution.** Refer to Example 1.7.28.

Obviously, $H$ is non-empty, since $(1, 0) \in H$.

Let $x = (1, b) \in H$ and $y = (1, c) \in H$.

Then $x * y = (1, b) * (1, c) = (1 \,.\, 1 \,,\, b \,.\, 1 + c) = (1, b + c) \in H$.

$\therefore \quad x * y \in H \quad \forall \; x, y \in H$.

Now $\qquad x^{-1} = (1, -b) \in H$,

since $\qquad x * x^{-1} = (1, b) * (1, -b) = (1.1, b.1 - b) = (1, 0)$, by (1),

Hence $\qquad \{H, *\} < \{G, *\}$.

Notice that $H$ is an abelian subgroup of $G$, since

$$(1, b) * (1, c) = (1, b + c) = (1, c + b) = (1, c) * (1, b), \text{ by (1)}.$$

**Example 1.9.2.** *Show that* $H = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a \neq 0 \,;\, a, b \in \mathbf{R} \right\}$ *is a subgroup of the multiplicative group of $2 \times 2$ non-singular matrices over $\mathbf{R}$.*

**Solution.** Refer to Example 1.7.15. Let $S$ be the multiplicative group of $2 \times 2$ non-singular matrices over $\mathbf{R}$. We have to show that $H$ is a subgroup of $S$.

Let $\quad X = \begin{pmatrix} a_1 & b_1 \\ 0 & 1 \end{pmatrix} \in H, Y = \begin{pmatrix} a_2 & b_2 \\ 0 & 1 \end{pmatrix} \in H$ ; where

$$a_1 \neq 0, a_2 \neq 0 \in \mathbf{R} \,;\, b_1, b_2 \in \mathbf{R}.$$

We see that $o(i)\, o(j) = 4 \times 4 = 16$ and $o(ij) = 4$.

Hence $o(ij) \neq o(i)\, o(j)$, where $ij \neq ji$.

*Similarly, the conclusion of the problem may not follow, if*

$$ab = ba \quad but \quad (o(a), o(b)) \neq 1.$$

Refer to the group $G = \{1, -1, i, -i\}$ of Example 1.10.1.

We have $o(i) = 4$, $o(-1) = 2$, $o(-1 \,.\, i) = o(-i) = 4$ and $-1 \,.\, i = i \,.\, -1$.

Thus $o(-1 \,.\, i) \neq o(-1)\, o(i)$, where

$$(o(-1), o(i)) = (2, 4) \neq 1 \text{ and } -1 \,.\, i = i \,.\, -1.$$

**Example 1.10.4.** *If $a$ is any element of a group $G$, show that*

$$o(a^n) = \frac{o(a)}{(n, o(a))},$$

*where $n$ is a positive integer and $(n, o(a))$ means the g.c.d. of $n$ and $o(a)$.*

**Solution.** Let $o(a) = m$. Then $m$ is the least positive integer such that

$$a^m = e. \qquad ...(1)$$

Let $d$ be g.c.d of $n$ and $m$ *i.e.*, $d = (n, m) = (n, o(a))$

$\Rightarrow d$ divides $n$ and $m \Rightarrow \frac{n}{d}, \frac{m}{d}$ are relatively prime integers.

We have $(a^n)^{\frac{m}{d}} = (a^m)^{\frac{n}{d}} = e$, using (1). ...(2)

We now show $\frac{m}{d}$ is the least positive integer satisfying (2).

Let $r$ be *any* positive integer such that $(a^n)^r = e$.

Then $a^{nr} = e \Rightarrow o(a)$ divides $nr$ [Theorem 1.10.1 (*iv*)]

$\Rightarrow m$ divides $nr$

$\Rightarrow \frac{m}{d}$ divides $\frac{n}{d} r$.

$\Rightarrow \frac{m}{d}$ divides $r$, since $\left(\frac{m}{d}, \frac{n}{d}\right) = 1$.

This shows that $\frac{m}{d}$ is the least positive integer satisfying (2). Hence

$$o(a^n) = \frac{m}{d} = \frac{o(a)}{(n, o(a))}.$$

## 1.11 Cyclic Group

**Definition.** *A group $G$ is called a* **cyclic group,** *if there exists an element $a \in G$ such that each element of $G$ is expressible as*

$$x = a^n = aa \ldots a \ (n \text{ times}),$$

*where $n$ is some integer.*

*The element $a \in G$ is called a* **generator** *of $G$ and $G$ is written as*

$$G = \langle a \rangle \quad or \quad G = (a).$$

*We also say that $G$ is generated by $a$.*

It may be observed that a group $\{G, +\}$ is **cyclic**, if there exists some element $a$ of $G$ such that each element $x$ of $G$ is expressible as

$$x = na = a + a + \ldots\ldots + a \ (n \text{ times}),$$

for some integer $n$.

**Illustrations.**

1. $G = \{-1, 1\}$ is a cyclic group generated by $-1$, since $(-1)^1 = -1$ and $(-1)^2 = 1$. Thus $G = \langle -1 \rangle$.
2. $G = \{-1, 1, i, -i\}$ is a cyclic group, where $G = \langle i \rangle$. Notice that $i^1 = i, i^2 = -1, i^3 = -i, i^4 = 1$.
   Also $G = \langle -i \rangle$.
3. $(\mathbf{Z}, +)$ is a cyclic group, where $\mathbf{Z} = \langle 1 \rangle$.
   Notice that for every integer $n$, $n = 1 + 1 + \ldots + 1$ ($n$ times).
4. *The group $G$ of $n$ nth roots of unity is a cyclic group.*
   We have $G = \{e^{2\pi i/n}, e^{4\pi i/n}, \ldots, e^{2(n-1)\pi/n}, 1\}$
   Let $\rho = e^{2\pi i/n}$. Then $G = \{\rho, \rho^2, \rho^3, \ldots, \rho^{n-1}, \rho^n = 1\} = \langle \rho \rangle$.
5. *The group $(\mathbf{Q}, +)$ is not cyclic.*
   Let, if possible, $\mathbf{Q} = \langle q \rangle$ for some $q = \frac{m}{n}$ ($m$ and $n$ are integers, $n \neq 0$).
   Then for each $x \in \mathbf{Q}$, $x = kq$ for some integer $k$.
   In particular, for $x = \frac{1}{3n} \in \mathbf{Q}$, we have

$$\frac{1}{3n} = lq \text{ for some integer } l$$

$$\Rightarrow \quad \frac{1}{3n} = \frac{lm}{n} \Rightarrow \frac{1}{3} = lm \ ; \ lm \in \mathbf{Z} \quad \Rightarrow \frac{1}{3} \text{ is an integer.}$$

This is impossible. Hence $(\mathbf{Q}, +)$ is not cyclic.

**Theorem 1.11.1.** *Show that a subgroup of a cyclic group is cyclic.*

**Proof.** Let $G = \langle a \rangle$ be a cyclic group. Let $H$ be any subgroup of $G$. We shall prove that $H$ is cyclic. Let $x \in H$ be arbitrary. Since $H < G$, $x \in G = \langle a \rangle$ and so $x = a^n$ for some integer $n$. Let $m$ be the smallest positive integer such that $a^m \in H$. It means that if $a^k \in H$ for $0 \leq k < m$, then $k$ must be zero. (Notice that $a^0 = e \in H$). On dividing $n$ by $m$, there two integers $q$ and $r$ such that

$$n = mq + r, \quad \text{where} \quad 0 \leq r < m.$$

$$\therefore \quad a^r = a^{n-mq} = a^n \cdot a^{-mq} = x \cdot (a^m)^{-q} \in H,$$

As stated earlier,

$$a^r \in H \quad \text{where} \quad 0 \le r < m \quad \Rightarrow r = 0 \quad \Rightarrow n = mq.$$

$$\therefore \qquad x = a^n = a^{mq} = (a^m)^q \quad \forall \quad x \in H.$$

Hence $H = \langle a^m \rangle$ and so $H$ is cyclic.

**Theorem 1.11.2.** *Show that the number of generators of an infinite cyclic group is two.*

**Proof.** Let $G = \langle a \rangle$ be any infinite cyclic group.

$$\therefore \qquad G = \{a^i : i = 0, \pm 1, \pm 2, \ldots\}.$$

Since $G$ is infinite, therefore

$$a^i = e \Leftrightarrow i = 0. \qquad \ldots(1)$$

[Notice that $a^m = e$ for $m \neq 0 \in \mathbf{Z}$ implies that

$G = \{a, a^2, \ldots a^{m-1}, a^m = e\}$, which is finite.]

Suppose $b \in G$ be any other generator of $G$ so that $G = \langle b \rangle$.

Since $b \in G = \langle a \rangle$, $b = a^n$ for some integer $n$.

Since $a \in G = \langle b \rangle$, $a = b^m$ for some integer $m$.

$$\therefore \qquad a = (a^n)^m = a^{nm}.$$

Now $\quad a = a^{nm} \quad \Rightarrow \quad a^{nm-1} = e \quad \Rightarrow \quad nm - 1 = 0$, using (1).

$$\Rightarrow \qquad nm = 1 \qquad \Rightarrow (n = 1, m = 1) \text{ or } (n = -1, m = -1)$$

$$\therefore \qquad b = a \quad \text{or} \quad a^{-1}.$$

Hence $G$ has exactly two generators $a$ and $a^{-1}$.

**Definition (Euler $\phi$-function)**

*If $n$ is any positive integer, then* **Euler $\phi$-function**, *denoted by $\phi(n)$, is defined as*

$$\phi(1) = 1,$$

$\phi(n)$ = *number of positive integers less than $n$ and relatively prime to $n$, if $n > 1$.*

**Illustrations.**

1. $\phi(4) = 2$, since 1, 3 are the positive integers less than 4 and relatively prime to 4.
2. $\phi(5) = 4$, since 1, 2, 3, 4 are the positive integers less than 5 and relatively prime to 5.
3. $\phi(6) = 2$, since 1, 5 are the positive integers less than 6 and relatively prime to 6.
4. $\phi(8) = 4$, since 1, 3, 5, 7 are the positive integers less than 8 and relatively prime to 8.
5. $\phi(p) = p - 1$, if $p$ is prime.

**Theorem 1.11.3.** *Show that the number of generators of a finite cyclic group of order $n$ is $\phi(n)$, where $\phi(n)$ is the Euler $\phi$-function.*

Thus 7 cannot be a generator of $U_8$.

Clearly, 1 is also not a generator of $U_8$.

Hence $U_8$ is not a cyclic group.

**Example 1.11.10.** *Show that a finite group of order n containing an element of order n must be cyclic.*

**Solution.** Let $G$ be a finite group such that $o(G) = n$. Let $a \in G$ be such that $o(a) = n$. Then $n$ is the least positive integer such that $a^n = e$.

Let $H = \langle a \rangle = \{a, a^2, a^3, \ldots, a^n = e\}$

Then $H$ is a subgroup of $G$ and $o(H) = n$.

Since $H \subseteq G$ and $o(H) = o(G)$, therefore

$G = H = \langle a \rangle$. Hence $G$ is cyclic.

## 1.12 Cosets and Lagrange's Theorem

Let $H$ be a subgroup of a group $G$ and $a \in G$. The set

$aH = \{ah : h \in H\}$ *is called a* **left coset** *of H in G*

*and* $Ha = \{ha : h \in H\}$ *is called a* **right coset** *of H in G.*

If the composition in G is denoted additively and if $(H, +) < (G, +)$, then

$a + H = \{a + h : h \in H\}$ and $H + a = \{h + a : h \in H\}$

are *left* and *right cosets* of $H$ in $G$, respectively.

**Example 1.12.1.** *Find out all the right cosets of H and K in G, where* $G = \langle a \rangle$ *is a cyclic group of order 10 and*

$$H = \langle a^2 \rangle, K = \langle a^5 \rangle.$$

**Solution.** We have

$$G = \{a, a^2, a^3, a^4, a^5, a^6, a^7, a^8, a^9, a^{10} = e\},$$

$$H = \{a^2, a^4, a^6, a^8, a^{10} = e\}, K = \{a^5, a^{10} = e\}.$$

It is easy to verify that $H < G$ and $K < G$. Now

$$Ha = \{a^3, a^5, a^7, a^9, a\}, Ha^2 = \{a^4, a^6, a^8, e, a^2\} = H,$$

$$Ha^3 = \{a^5, a^7, a^9, a, a^3\} = Ha.$$

Similarly, $Ha^4 = Ha^6 = Ha^8 = Ha^{10} = H$;

$$Ha^5 = Ha^7 = Ha^9 = Ha.$$

Hence there are only two distinct right cosets of $H$ in $G$ viz. $H$ and $Ha$. It may be noticed that

$$H \cap Ha = \phi \quad \text{and} \quad G = H \cup Ha.$$

Now $Ka = \{a^6, a\}, Ka^2 = \{a^7, a^2\}, Ka^3 = \{a^8, a^3\}, Ka^4 = \{a^9, a^4\},$

$$Ka^5 = \{e, a^5\} = K, Ka^6 = \{a, a^6\} = Ka, Ka^7 = \{a^2, a^7\} = Ka^2.$$

Similarly, $Ka^8 = Ka^3$, $Ka^9 = Ka^4$, $Ke = K$.

Hence all the distinct right cosets of $K$ in $G$ are

These right cosets of $K$ are disjoint *i.e.*, have no element in common and further $G = K \cup Ka \cup Ka^2 \cup Ka^3 \cup Ka^4$.

*The above expression is called a* **right coset decomposition** *of* $G$.

**Remark.** It may be noticed that $Ha = aH$, $Ka = aK$, $Ka^2 = a^2K$ etc. Thus every left coset of $H$ (and $K$) in $G$ is a right coset of $H$ (and $K$) in $G$. *However, in general, a left coset of* $H$ *in* $G$ *may not be equal to a right coset of* $H$ *in* $G$. For example,

$H = \{I, (12)\}$ is a subgroup of the group

$S_3 = \{I, (12), (23), (13), (123), (132)\}$.

We notice that

$(23)\,H = \{(23), (23)\,(12)\} = \{(23), (132)\}$,

$H\,(23) = \{(23), (12)\,(23)\} = \{(23), (123)\}$.

Thus $(23)\,H \neq H\,(23)$, $(23) \in S_3$.

**Example 1.12.2.** *Find all the left cosets of* $(H, +)$ *in* $(G, +)$, *where* $G = \mathbf{Z}$ *and* $H = \{5x : x \in \mathbf{Z}\}$.

**Solution.** We have

$H = \{..., -15, -10, -5, 0, 5, 10, 15, ....\}$,

$1 + H = \{..., -14, -9, -4, 1, 6, 11, 16, ...\}$,

$2 + H = \{..., -13, -8, -3, 2, 7, 12, 17, ...\}$,

$3 + H = \{..., -12, -7, -2, 3, 8, 13, 18, ...\}$,

$4 + H = \{..., -11, -6, -1, 4, 9, 14, 19, ...\}$,

It is easy to verify that

$5 + H = H$, $6 + H = 1 + H$, $7 + H = 2 + H$ etc.

$-1 + H = 4 + H$, $-2 + H = 3 + H$ etc.

Hence there are 5 distinct left cosets of $H$ in $G$ *viz.*

$$H, 1 + H, 2 + H, 3 + H, 4 + H$$

and $$\mathbf{Z} = H \cup (1 + H) \cup (2 + H) \cup (3 + H) \cup (4 + H)$$

is the left coset decomposition of $(\mathbf{Z}, +)$.

**Ex. 1.** *Show that* $\mathbf{Z} = H \cup (1 + H) \cup (2 + H)$, $H = \{3x : x \in \mathbf{Z}\}$.

**Ex. 2.** *Find all the right cosets of* $H$ *in* $G$ *where*

$$G = \langle a \rangle, a^{12} = e \quad \text{and} \quad H = \langle a^3 \rangle.$$

**Theorem 1.12.1.** *Let* $H < G$ *and* $a, b \in G$. *Prove that*

(*i*) $Ha = H$ *iff* $a \in H$.

(*ii*) $Ha = Hb$ *iff* $ab^{-1} \in H$.

(*iii*) $aH = bH$ *iff* $a^{-1}b \in H$.

(*iv*) $(Ha)^{-1} = a^{-1}H$.

**Proof.** (*i*) Let $Ha = H$. Then $e \in H \Rightarrow ea \in Ha \Rightarrow ea \in H \Rightarrow a \in H$. Conversely, let $a \in H$. We shall prove that $Ha = H$.

Let $x \in Ha$ be arbitrary. Then $x = ha$ for some $h \in H$.

Now $h \in H$ and $a \in H \Rightarrow ha \in H \quad (\because H < G) \Rightarrow x \in H$.

$\therefore \quad Ha \subseteq H$.

For any $h \in H, ha^{-1} \in H \quad (\because a \in H \Rightarrow a^{-1} \in H$ as $H < G)$

Let $ha^{-1} = h_1$, where $h_1 \in H$

$\Rightarrow \quad h = h_1 a \in Ha \Rightarrow h \in Ha \; \forall \; h \in H$.

$\therefore \quad H \subseteq Ha$.

Hence $Ha = H$.

*(ii)* Let $Ha = Hb$. We have $a = ea \in Ha \quad (\because e \in H)$ and so

$a \in Hb \Rightarrow a = hb$ for some $h \in H \Rightarrow ab^{-1} = h \in H$.

Thus $ab^{-1} \in H$.

Conversely, let $ab^{-1} \in H$. Then $ab^{-1} = h_1$ for some $h_1 \in H \Rightarrow a = h_1 b$ ...(1)

Let $x \in Ha \Rightarrow x = h_2 a$ for some $h_2 \in H$

$\Rightarrow x = h_2 (h_1 b) = (h_2 h_1) b$, by (1)

Thus $x \in Hb$, since $h_1 h_1 \in H$. So $Ha \subseteq Hb$. ...(2)

Now $x \in Hb \Rightarrow x = h_3 b = h_3 (h_1^{-1} a) = (h_3 h_1^{-1}) a$, by (1).

Thus $x \in Ha$, since $h_3 h_1^{-1} \in H$. So $Hb \subseteq Ha$. ...(3)

From (2) and (3), $Ha = Hb$.

Similarly, we can prove part *(iii)*.

*(iv)* Let $x \in (Ha)^{-1} \Rightarrow x = (ha)^{-1}$ for some $h \in H$.

$\Rightarrow \quad x = a^{-1} h^{-1} \Rightarrow x \in a^{-1} H$, since $h^{-1} \in H$. Thus

$(Ha)^{-1} \subseteq a^{-1} H$. ...(4)

Conversely, let $x \in a^{-1} H \Rightarrow x = a^{-1} h_1$, for some $h_1 \in H$.

$\Rightarrow \quad x = (h_1^{-1} a)^{-1}$, where $h_1^{-1} a \in Ha \quad (\because h_1^{-1} \in H)$

Thus $x \in (Ha)^{-1}$ and so $a^{-1} H \subseteq (Ha)^{-1}$. ...(5)

From (4) and (5), $(Ha)^{-1} = a^{-1} H$.

**Theorem 1.12.2.** *Let $H$ be a subgroup of a group $G$ and $a, b \in G$. Show that either $Ha \cap Hb = \phi$ or $Ha = Hb$.*

*Or*

*Prove that any two right cosets of $H$ in $G$ are either identical or disjoint, $H$ being a subgroup of $G$.* [D.U., 1995, 94]

**Proof.** If $Ha \cap Hb = \phi$, the two right cosets $Ha$, $Hb$ have no element in common *i.e.*, they are disjoint.

Let $Ha \cap Hb \neq \phi$. In this case, we shall show that $Ha = Hb$.

Suppose that $c \in Ha \cap Hb$. Then $c \in Ha$ and $c \in Hb$. Consequently,

$c = h_1 a$ and $c = h_2 b$, for some $h_1, h_2 \in H$.

$\therefore \quad h_1 a = h_2 b \Rightarrow a = h_1^{-1} h_2 b$ and $b = h_2^{-1} h_1 a$. ...(1)

Let $x$ be any element of $Ha$ so that $x = ha$, for some $h \in H$.

Using (1), we have

$x = h(h_1^{-1} h_2 b) = (hh_1^{-1} h_2)\, b \in Hb$, $hh_1^{-1} h_2 \in H$ $(\because H < G)$

$\Rightarrow \quad x \in Hb \quad \forall \; x \in Ha \Rightarrow Ha \subseteq Hb.$ ...(2)

Conversely, let $y$ be any element of $Hb$ so that $y = h'b$, for some $h' \in H$. Using (1), we have

$y = h'(h_2^{-1} h_1 a) = (h' h_2^{-1} h_1)\, a \in Ha$, $h' h_2^{-1} h_1 \in H$. $(\because H < G)$

$\therefore \quad Hb \subseteq Ha$ ...(3)

From (2) and (3), $Ha = Hb$. Hence the theorem.

**Note.** Similarly we can prove that

*Any two left cosets of $H$ in $G$ are either identical or disjoint, where $H$ is a subgroup of $G$.*

**Theorem 1.12.3.** *Prove that there is a one-to-one correspondence between any two right cosets of $H$ in $G$.*

**Proof.** Let $Ha$ and $Hb$ be any two right cosets of $H$ in $G$, where $a, b \in G$. We are required to prove that there exists a one-to-one mapping of $Ha$ onto $Hb$.

Define a mapping $\phi : Ha \to Hb$ as

$\phi(ha) = hb \; \forall \; h \in H.$

Firstly, we show that $\phi$ is one-to-one.

Suppose $\phi(h_1 a) = \phi(h_2 a)$. Then $h_1 b = h_2 b$, by (1)

$\Rightarrow \quad h_1 = h_2$, by right cancellation law

$\Rightarrow h_1 a = h_2 a$, by right cancellation law.

Thus $\phi$ is one-to-one. Now we show that $\phi$ is onto.

Let $y \in Hb$ so that $y = hb$ for some $h \in H$.

Thus $y = \phi(ha)$, by (1)

$\Rightarrow \quad y = \phi(x), x = ha \in Ha.$

This shows that $\phi$ is onto. Hence $\phi$ is a one-to-one correspondence between $Ha$ and $Hb$.

**Remark.** *Similarly, we can show that there is a one-to-one correspondence between any two left cosets $aH$ and $bH$ of $H$ in $G$.*

**Hint.** Define $\phi : aH \to bH$ as $\phi(ah) = bh \; \forall \; h \in H$.

**Theorem 1.12.4. (Lagrange's Theorem)**

*The order of a subgroup of a finite group divides the order of the group.*

*Or*

*If $G$ is a finite group and $H$ is a subgroup of $G$, then $o(H)$ is a divisor of $o(G)$.*

**Proof.** Let $o(G) = n$ and $o(H) = m$.

For $a, b \in G$ ; we define a relation $\equiv$ as follows :

$$a \equiv b \pmod{H} \Leftrightarrow ab^{-1} \in H. \qquad ...(1)$$

Then $\equiv$ is an equivalence relation on $G$, since

(*i*) $a \equiv a \pmod{H}$ $\quad [\because aa^{-1} = e \in H]$.

(*ii*) $a \equiv b \pmod{H} \Rightarrow ab^{-1} \in H \Rightarrow (ab^{-1})^{-1} \in H \quad (\because H < G)$

$\Rightarrow (b^{-1})^{-1} a^{-1} \in H \Rightarrow ba^{-1} H \Rightarrow b \equiv a \pmod{H}$.

(*iii*) $a \equiv b \pmod{H}$ and $b = c \pmod{H}$

$\Rightarrow$ $ab^{-1} \in H$ and $bc^{-1} \in H \Rightarrow (ab^{-1})(bc^{-1}) \in H \quad [\because H < G]$

$\Rightarrow$ $ac^{-1} \in H \Rightarrow a \equiv c \pmod{H}$.

Consequently, $G$ is expressible as the union of mutually disjoint equivalence classes *i.e.*,

$$G = \bigcup_{a \in G} [a]. \qquad ...(2)$$

We now show that $[a] = Ha$, where

$$[a] = \{x \in G : x \equiv a \pmod{H}\} = \{x \in G : xa^{-1} \in H\}. \qquad ...(3)$$

Let $x \in [a]$ so that $xa^{-1} \in H \Rightarrow x \in Ha$.

$\therefore$ $[a] \subseteq Ha$.

Conversely, let $y \in Ha$. Then $y = ha$ for some $h \in H$

$\Rightarrow$ $ya^{-1} = h \Rightarrow ya^{-1} \in H \Rightarrow y \in [a]$, by (3)

$\therefore$ $Ha \subseteq [a]$. Thus $[a] = Ha$. $\qquad ...(4)$

From (2) and (4), we obtain

$$G = Ha_1 \cup Ha_2 \cup ... \cup Ha_r ;$$

where $a_i \in G\ (1 \le i \le r \le n)$ and $Ha_i \cap Ha_j = \phi$ ; for $i \ne j$.

Since $G$ is finite, therefore

$$o(G) = o(Ha_1) + o(Ha_2) + ... + o(Ha_r). \qquad ...(5)$$

Clearly $H = He$ is a right coset of $H$ in $G$.

Since there exists a one-to-one correspondence between any two right cosets of $H$ in $G$, therefore

$$o(Ha_i) = o(He) = o(H) = m,\ 1 \le i \le r. \qquad ...(6)$$

From (5) and (6), $n = m + m + ... + m$ ($r$ times) $= mr \Rightarrow$ $m$ divides $n$.

Hence $o(H)$ divides $o(G)$.

**Remark 1.** *The converse of Lagrange's theorem is not true.*

If $m$ divides $o(G)$, then $G$ need not have a subgroup of order $m$.

Let $S_4$ be the group of all permutations defined on the set $\{1, 2, 3, 4\}$ and $A_4$ be the set of all even permutations in $S_4$. Then $A_4$ is a subgroup of $S_4$, where $o(A_4) = \frac{1}{2} o(S_4) = \frac{4!}{2} = 12$. [See Theorem 2.4.3 ; chapter 2]

Obviously, 6 divides $o(A_4)$ but $A_4$ has no subgroup of order 6.

[See Example 2.4.17 ; Chapter 2].

expressed as the union of two of its proper subgroups.

**Example 1.12.11.** *Give an example of a group $G$ having a subgroup $H$ and two elements $a, b \in G$ such that $Ha = Hb$ but $aH \neq bH$.*

**Solution.** Let $G = S_3$ and $H = \{I, (23)\}$.

Let $a = (12)$ and $b = (132) \in S_3$. Then

$Ha = \{(12), (23)(12)\} = \{(12), (132)\}$,

$Hb = \{(132), (23)(132)\} = \{(132), (12)\}$,

$aH = \{(12), (12)(23)\} = \{(12), (123)\}$,

$bH = \{(132), (132)(23)\} = \{(132), (13)\}$.

Thus $Ha = Hb$ but $aH \neq bH$.

**Example 1.12.12.** *Give an example of a group $G$ having a subgroup $H$ and two elements $a, b \in G$ such that $aH = bH$ but $Ha \neq Hb$.*

**Please try yourself.**

## 1.13 Product of Two Subgroups

**Definition.** *Let $H$ and $K$ be two subgroups of a group $G$. Then their* **product,** *denoted by $HK$, is defined as*

$$HK = \{hk : h \in H, k \in K\}.$$

**Theorem 1.13.1.** *If $H$ and $K$ be two subgroups of a group $G$, then $HK$ is a subgroup of $G$ if and only if $HK = KH$.*

**Proof. Condition is necessary**

Let $HK$ be a subgroup of $G$. We shall prove that $HK = KH$.

Let $x \in HK$ be arbitrary. Then $x^{-1} \in HK$ $(\because HK < G)$

$\Rightarrow$ $x^{-1} = hk$, for some $h \in H, k \in K$

$\Rightarrow$ $x = (x^{-1})^{-1} = (hk)^{-1} = k^{-1} h^{-1} \in KH$,

since $k^{-1} \in K$ and $h^{-1} \in H$ $(\because K < G$ and $H < G)$.

Thus $HK \subseteq KH$. ...(1)

Suppose that $y \in KH$ is arbitrary. Then

$y = k_1 h_1$, for $k_1 \in K$ and $h_1 \in H$

$= (k_1^{-1})^{-1} (h_1^{-1})^{-1} = (h_1^{-1} k_1^{-1})^{-1}$ ...(2)

Since $H < G$ and $K < G$, therefore, $h_1^{-1} \in H$ and $k_1^{-1} \in K$

$\Rightarrow \quad h_1^{-1} k_1^{-1} \in HK \Rightarrow (h_1^{-1} k_1^{-1})^{-1} \in HK \qquad (\because HK < G)$

$\Rightarrow \quad y \in HK$, using (2). ...(3)

Thus $KH \subseteq HK$.

From (1) and (3), $HK = KH$.

**Condition is sufficient**

Suppose that $HK = KH$. ...(4)

We shall prove that $HK$ is a subgroup of $G$.

Let $x, y \in HK$. Then $x = hk$, $y = h'k'$ ; where $h, h' \in H$ and $k, k' \in K$.

We have $xy = hkh'k'$. ...(5)

Since $kh' \in KH = HK$, we can write

$kh' = h_2 k_2$ for $h_2 \in H$ and $k_2 \in K$.

Putting in (5), $xy = h(h_2 k_2)k' = (hh_2)(k_2 k') \in HK$,

since $hh_2 \in H$ and $k_2 k' \in K$ $(\because H < G$ and $K < G)$

Thus $xy \in HK \quad \forall \quad x, y \in HK$. ...(6)

Also $x^{-1} = (hk)^{-1} = k^{-1}h^{-1} \in KH = HK$.

$\therefore \quad x^{-1} \in HK \quad \forall \quad x \in HK$ ...(7)

From (6) and (7), it follows that $HK$ is a subgroup of $G$.

**Corollary.** *If $H$ and $K$ are subgroups of an abelian group $G$, then $HK$ subgroup of $G$.*

**Proof.** Since $G$ is abelian, then $HK = KH$. Hence $HK$ is a subgroup of

**Theorem 1.13.2.** *If $H$ and $K$ are finite subgroups of a group $G$, then*

$$o(HK) = \frac{o(H)\, o(K)}{o(H \cap K)}. \qquad \text{[D.U., 1997]}$$

**Proof.** Let $T = H \cap K$. Then $T$ is a subgroup of $K$ $(\because T \subseteq K)$. Since $K$ finite group,

$$i_K(T) = \frac{o(K)}{o(T)} = m, \text{ say.} \qquad ...(1)$$

Thus there exist $m$ distinct right cosets of $T$ in $K$, say $Tk_2, ..., Tk_m$ ; $k_1, k_2, ..., k_m \in K$. Furthermore,

$$K = Tk_1 \cup Tk_2 \cup ... \cup Tk_m$$

$$\Rightarrow \quad HK = H(Tk_1 \cup Tk_2 \cup ... \cup Tk_m)$$

$$= HTk_1 \cup HTk_2 \cup ... \cup HTk_m$$

$$= Hk_1 \cup Hk_2 \cup ... \cup Hk_m. \qquad [\because T \subseteq H \Rightarrow HT = H]$$

Next we show that $Hk_1, Hk_2, ..., Hk_m$ are all distinct.

Let, if possible, $Hk_i = Hk_j$ for $1 \le i < j \le m$

$\Rightarrow$ $k_i k_j^{-1} \in H$. Also $k_i k_j^{-1} \in K$ $(\because K < G)$

$\Rightarrow$ $k_i k_j^{-1} \in H \cup K = T$

$\Rightarrow$ $Tk_i = Tk_j$, which is a contradiction.

From (2), we obtain

$$o(HK) = o(Hk_1) + o(Hk_2) + ... + o(Hk_m)$$
$$= o(H) + o(H) + ... + o(H) \ (m \text{ times})$$
$$= m\, o(H) = \frac{o(K)}{o(T)}\, o(H), \text{ by (1).}$$

Hence $$o(HK) = \frac{o(H)\, o(K)}{o(H \cup K)}.$$

**Corollary.** *If H and K are subgroups of G and*

$$o(H) > \sqrt{o(G)},\ o(K) > \sqrt{o(G)};$$

*then* $o(H \cap K) > 1$ *i.e.,* $H \cap K \neq \{e\}$.

**Proof.** Since $HK \subseteq G$, $o(HK) \le o(G)$

$$\Rightarrow \quad o(G) \ge o(HK) = \frac{o(H)\, o(K)}{o(H \cap K)} > \frac{\sqrt{o(G)}\ \sqrt{o(G)}}{o(H \cap K)} = \frac{o(G)}{o(H \cap K)}$$

Thus $$o(G) > \frac{o(G)}{o(H \cap K)} \Rightarrow o(H \cap K) > 1.$$

Hence $H \cap K \neq \{e\}$.

## EXAMPLES

**Example 1.13.1.** *If G is a group of order 35, show that it cannot h two subgroups of order 7.*

**Solution.** Let, if possible, $G$ have two subgroups $H$ and $K$, wh

Now $o(HK) = \dfrac{o(H)\,o(K)}{o(H \cap K)} = \dfrac{2 \times 2}{1} = 4$.

Hence $G = HK$, as $HK < G$.

**Example 1.13.8.** *Let* $G = \langle a \rangle, a^{12} = e$. *Let* $H = \langle a^3 \rangle$ *and* $K = \langle a^4 \rangle$. *Show that* $G = HK$.

*Also show that* $G = AB$, *where* $A = \langle a^2 \rangle, B = \langle a^3 \rangle$.

**Please try yourself.**

**Example 1.13.9.** *If* $o(G) = 6$ *and* $H \neq K$ *are subgroups of* $G$ *each of order 2, then* $HK$ *cannot be a subgroup of* $G$. [D.U., 1996]

**Solution.** Since a group of prime order is cyclic, so we may take

$$H = \{a, a^2 = e\}, K = \{b, b^2 = e\} \text{ and } a \neq b \qquad (\because H \neq K)$$

$$\Rightarrow \quad H \cap K = \{e\}.$$

Now $o(HK) = \dfrac{o(H)\,o(K)}{o(H \cap K)} = \dfrac{2 \times 2}{1} = 4.$

Since 4 does not divide $o(G) = 6$, so by Lagrange's theorem, $HK$ cannot be a subgroup of $G$.

## 1.14 Normal Subgroup

**Definition.** *A subgroup* $N$ *of a group* $G$ *is said to be a* **normal subgroup** *of* $G$, *if*

$$gng^{-1} \in N \text{ for each } g \in G \text{ and } n \in N.$$

We denote it as $N \lhd G$.

It may be observed that

*Every subgroup* $N$ *of an abelian group* $G$ *is a normal subgroup of* $G$.

for $g \in G$ and $n \in N \Rightarrow gn = ng \Rightarrow gng^{-1} = n \in N$.

From the above observation, it follows that

*Every subgroup of a cyclic group is normal*, since a cyclic group is abelian.

**Illustrations.**

1. Let $G = \langle a \rangle, a^{12} = e$. Then

$$H_1 = \langle a^2 \rangle = \{a^2, a^4, a^6, a^8, a^{10}, a^{12} = e\},$$

$$H_2 = \langle a^3 \rangle = \{a^3, a^6, a^9, a^{12} = e\},$$

$H_3 = \langle a^4 \rangle = \{a^4, a^8, a^{12} = e\}$,

$H_4 = \langle a^6 \rangle = \{a^6, a^{12} = e\}$

are normal subgroups of $G$.

2. $N = \{1, -1\}$ is a normal subgroup of the multiplicative group $G = \{1, -1, i, -i\}$.

**Theorem 1.14.1.** *A subgroup $N$ of a group $G$ is a normal subgroup of $G$ if and only if $gNg^{-1} = N$ for each $g \in G$.*

**Proof.** *The condition is necessary.*

Let $N \triangleleft G$. Then $gng^{-1} \in N \ \forall \ g \in G$ and $n \in N$.

Thus $gNg^{-1} \subseteq N \ \forall \ g \in G$, ...(1)

where $gNg^{-1} = \{gng^{-1} : n \in N\}$.

We have $g^{-1}Ng = g^{-1}N(g^{-1})^{-1} \subseteq N$, using (1).

Now $N = g(g^{-1}Ng)g^{-1} \subseteq gNg^{-1}$ *i.e.*, $N \subseteq Ng^{-1}$. ...(2)

From (1) and (2), $gNg^{-1} = N$, for each $g \in G$.

*The condition is sufficient*

Let $gNg^{-1} = N$, for each $g \in G$.

For $g \in G$ and $n \in N$, we see that $gng^{-1} \in gNg^{-1} = N$

$\Rightarrow gng^{-1} \in N \ \forall \ g \in G, n \in N$.

Hence $N$ is normal subgroup of $G$.

**Theorem 1.14.2.** *A subgroup $N$ of a group $G$ is a normal subgroup of $G$ if and only if every left coset of $N$ in $G$ is a right coset of $N$ in $G$.*

**Proof.** By Theorem 1.14.1,

$N \triangleleft G \Leftrightarrow gNg^{-1} = N \ \forall \ g \in G \Leftrightarrow (gNg^{-1})g = Ng \ \forall \ g \in G$.

Hence $N \triangleleft G \Leftrightarrow gN = Ng \ \forall \ g \in G$. $[\because g^{-1}g = e$ and $Ne = N]$

**Corollary.** *If $N$ is a normal subgroup of a group $G$, then*

*(i)* $NaNb = Nab$.

*(ii)* $aNbN = abN$ ; $a, b \in G$.

**Proof.** *(i)* $NaNb = N(aN)b = N(Na)b$, as $N \triangleleft G$.

$= NN\,ab = N\,ab$, as $NN = N$. $[\because N < G]$

Hence $Na\,Nb = Nab$. The proof of *(ii)* is similar.

**Theorem 1.14.3.** *Prove that $H$ is a normal subgroup of a group $G$ iff the product of any two right cosets of $H$ in $G$ is a right coset of $H$ in $G$.*

**Proof.** *The condition is necessary*

Let $H \triangleleft G$ and $Ha$, $Hb$ be any two right cosets of $H$ in $G$ $(a, b \in G)$. We shall prove that $HaHb$ is a right coset.

We have $Ha\,Hb = H(aH)b = H(Ha)$, as $H \triangleleft G$

$= HH\,ab = H\,ab$, as $HH = H$ $(\because H < G)$

Thus $HaHb = Hab$, $(ab \in G)$ shows that the product of two right cosets $Ha$ and $Hb$ is the right coset $Hab$.

*The condition is sufficient*

Suppose the product of two right cosets of $H$ in $G$ is a right coset of $H$ in $G$. Let $Ha\,Hb = Hc$ ; $a, b, c \in G$.

We shall prove that $H \triangleleft G$.

Since $a = ea \in Ha$ and $b = eb \in Hb$, so $ab \in Ha\,Hb = Hc$.

Now $ab \in Hc \Rightarrow Hab = Hc$. [See Example 1.12.6 (*ii*)]

Thus $Ha\,Hb = Hab \;\; \forall\; a, b \in G$. ...(1)

Let $x \in G$ and $h \in H$. Then

$x \in Hx, h \in H = He$ and $x^{-1} \in Hx^{-1} \Rightarrow xhx^{-1} \in HxHeHx^{-1}$

$\Rightarrow xhx^{-1} \in Hxe\,Hx^{-1} = HxHx^{-1} = Hxx^{-1} = He = H$, using (1)

$\Rightarrow xhx^{-1} \in H \;\forall\; x \in G, h \in H$. Hence $H \triangleleft G$.

## EXAMPLES

**Example 1.14.1.** *If $N$ and $M$ are normal subgroups of a group $G$, then $N \cap M$ is a normal subgroup of $G$.*

**Solution.** Since $N$ and $M$ are subgroups of $G$, so $N \cap M$ is a subgroup of $G$. Let $g \in G$ and $a \in N \cap M$ so that $a \in N$ and $a \in M$.

Since $N \triangleleft G$, $gag^{-1} \in N$.

Since $M \triangleleft G$, $gag^{-1} \in M$.

$\therefore \qquad gag^{-1} \in N \cap M \;\forall\; g \in G$ and $a \in N \cap M$.

Hence $N \cap M$ is a normal subgroup of $G$.

**Example 1.14.2.** *Show that $Z = \{a \in G : ax = xa \;\forall\; x \in G\}$ is a normal subgroup of $G$.*

**Solution.** By Example 1.9.4, Z is a subgroup of $G$.

Now we show that $Z \triangleleft G$. Let $g \in G$ and $a \in Z$.

## 1.15 Quotient Groups

We have earlier seen that if $N$ is a normal subgroup of $G$, then

$$NaNb = Nab \ \forall \ a, b \in G.$$

This relation leads us to obtain a very important group known as *quotient group* as shown below :

**Theorem 1.15.1.** *Suppose $N$ is a normal subgroup of a group $G$. Let $\frac{G}{N} = \{Na : a \in G\}$. $\frac{G}{N}$ denote the set of all right cosets of $N$ in $G$ i.e.,*

*Show that $\frac{G}{N}$ is a group under the composition :*

$$NaNb = Nab \text{ for all } a, b \in G. \qquad ...(1)$$

*The group $\frac{G}{N}$ is called the* **quotient group** *or* **factor group** *of $G$ by $N$.*

**Proof.** Let $X, Y, Z \in \frac{G}{N}$. Then

$$X = Na,\ Y = Nb,\ Z = Nc \text{ for } a, b, c \in G.$$

We observe that

1. $XY = NaNb = Nab \in \frac{G}{N}$, as $ab \in G$.
2. $(XY)\,Z = (NaNb)\,Nc = (Nab)\,Nc$, by (1)
   $= N(ab)\,c$, by (1)
   $= Na(bc)$, by associative law in $G$
   $= Na(Nbc)$, by (1)
   $= Na(NbNc)$, by (1)
   $= X(YZ)$.
3. $Ne = N$ is the identity in $\frac{G}{N}$, since $XN = NaNe = Nae = Na = X$ for all $X \in G/N$. Similarly, $NX = X$ for all $X \in G/N$.
4. The inverse of any element $X = Na \in G/N$ is $X' = Na^{-1} \in G/N$, since

$$XX' = NaNa^{-1} = Naa^{-1} = Ne = N,$$

and $$X'X = Na^{-1}Na = Na^{-1}a = Ne = N.$$

Hence $G/N$ is a group.

**Remark.** $N \lhd G \Leftrightarrow Na = aN \ \forall \ a \in G$. Hence

$$\frac{G}{N} = \{Na : a \in G\} = \{aN : a \in G\}.$$

**Theorem 1.15.2.** *If $G$ is a finite group and $N$ is a normal subgroup of $G$, then*

$$o\left(\frac{G}{N}\right) = \frac{o(G)}{o(N)}.$$

**Proof.** Since $G$ is a finite group, therefore

$$o\left(\frac{G}{N}\right) = \text{Total number of distinct right cosets of } N \text{ in } G$$
$$= i_G(N)$$
$$= \frac{o(G)}{o(N)}, \text{ by Lagrange's Theorem.}$$

**Theorem 1.15.3.** *If $G$ is an abelian group and $N$ is a normal subgroup of $G$, then $G/N$ is abelian. Show by an example that the converse need not be true.*

**Proof.** Let $X, Y \in G/N$ be arbitrary. Then

$X = Na$, $Y = Nb$ for some $a, b \in G$. We have

$XY = NaNb = Nab = Nba$, since $G$ is abelian

$= NbNa = YX$.

Hence $G/N$ is abelian.

However, the converse need not be true *i.e.*, if $G/N$ is abelian, then $G$ may not be abelian as shown below :

Let $G = S_3 = \{I, (12), (23), (31), (123), (132)\}$

and $N = \{I, (123), (132)\}$.

Then $G$ is a non-abelian group and $N$ is a normal subgroup of $G$.

We have $o\left(\frac{G}{N}\right) = \frac{o(G)}{o(N)} = \frac{6}{3} = 2$.

Since every group of prime order is cyclic and so abelian, therefore $G/N$ is abelian but $G$ is not abelian.

**Ex.** *Find the elements of $S_3/N$, where $N = \{I, (123), (132)\}$.*

**Solution.** $i_{S_3}(N) = \frac{o(S_3)}{o(N)} = \frac{6}{3} = 2$.

Hence $\frac{S_3}{N} = \{N, N(23)\}$, where $N(23) = \{(23), (12), (13)\}$.

**Theorem 1.15.4.** *If $G$ is a cyclic group and $N$ a subgroup of $G$, then $G/N$ is cyclic. However, the converse need not be true.*

*Or*

*Show that every quotient group of a cyclic group is cyclic. However, the converse need not be true.*

**Proof.** Let $G = \langle a \rangle$ be a cyclic group. Let $N$ be any subgroup of $G$. Then $N$ is a normal subgroup of $G$, since a cyclic group is necessarily abelian. Since $N \lhd G$, so $G/N$ is defined. Now we show that

$$\frac{G}{N} = \langle Na \rangle.$$

Let $X$ be any element of $\frac{G}{N}$ so that $X = Ng$, for some $g \in G$.

Now $g \in G = \langle a \rangle \Rightarrow g = a^m$, for some integer $m$

$\Rightarrow \quad X = Ng = Na^m = N\,a\,.\,a\,...\,a$ ($m$ times)

$\Rightarrow \quad X = Na\,Na\,...\,Na$ ($m$ times)

$\therefore \quad X = (Na)^m, \forall\, X \in G/N.$

Hence $\frac{G}{N} = \langle Na \rangle$ and so $\frac{G}{N}$ is cyclic.

However, the converse need not be true *i.e.*, if $G/N$ is cyclic, then $G$ may not be cyclic. For example,

$$G = S_3 = \{I, (12), (23), (31), (123), (132)\}$$

is not cyclic. Let $H = \{I, (123), (132)\}$. Then $H$ is a normal subgroup of $G$ and

$$o\left(\frac{G}{H}\right) = \frac{o(G)}{o(H)} = \frac{6}{3} = 2.$$

Hence $\frac{G}{H}$ is cyclic (since any group of prime order is cyclic) but $G$ is not cyclic.

**Theorem 1.15.5.** *If $N$ is a normal subgroup of a group $G$ and $a \in G$ is of order $o(a)$, prove that $o(Na)$ divides $o(a)$. Also show that $a^m \in N$ if and only if $o(Na)$ divides $m$.*

**Proof.** Let $o(a) = n$ so that $n$ is the least positive integer such that

$$a^n = e. \qquad ...(1)$$

Consider $(Na)^n = Na\,.\,Na\,...\,Na$ ($n$ times)

$= Na\,.\,a\,....\,a$ ($n$ times)

$= Na^n = Ne = N$, by (1).

$\therefore \quad (Na)^n = N$, identity of $G/N$.

Hence $o(Na)$ divides $n$, where $n = o(G)$.

(*ii*) $a^m \in N \Leftrightarrow Na^m = N \Leftrightarrow (Na)^m = N \qquad (\because\ N \lhd G)$

$\Leftrightarrow$ $o(Na)$ divides $m$.

## EXAMPLES

**Example 1.15.1.** *Let $N$ be a normal [illegible] $G/N$ is abelian iff $xyx^{-1}y^{-1}$ [illegible]*

# 2

# HOMOMORPHISMS AND PERMUTATIONS

In this chapter, we shall discuss *Homomorphism of groups, Kernel of a homomorphism, Fundamental Theorem of Homomorphism* and its various applications, *Cayley's Theorem* and *Permutation groups* $S_n$ *and* $A_n$.

## 2.1 Homomorphism

**Definition 1.** *Let* $(G_1, \cdot)$ *and* $(G_2, *)$ *be two groups.*

*A mapping* $f: G_1 \to G_2$ *is called a* **homomorphism**, *if*

$$f(a \cdot b) = f(a) * f(b) \quad \text{for all} \quad a, b \in G_1.$$

In other words, a **homomorphism preserves the compositions** in the groups $G_1$ and $G_2$.

However, if we are not specific about the compositions of the groups $G_1$ and $G_2$, *we say that a mapping*

$$f: G_1 \to G_2 \text{ is a homomorphism, if}$$

$$f(ab) = f(a) f(b) \quad \text{for all} \quad a, b \in G.$$

It may be observed that in the above expression, $ab$ is in accordance with the composition of $G_1$ and $f(a) f(b)$ is in accordance with the composition of $G_2$.

**Definition 2.** *A group* $G_2$ *is said to be a* **homomorphic image** *of a group* $G_1$, *if there exists a homomorphism of* $G_1$ *onto* $G_2$.

**Definition 3.** *A mapping* $f: G_1 \to G_2$ *is called an* **isomorphism**, *if*

(*i*) *f is a homomorphism and*

(*ii*) *f is one-to-one i.e.,* $f(x) = f(y) \Rightarrow x = y \; ; \; x, y \in G$.

**Definition 4.** *Two groups* $G_1$ *and* $G_2$ *are called* **isomorphic**, *written as* $G_1 \approx G_2$, *if there is an isomorphism of* $G_1$ *onto* $G_2$. *Equivalently, two groups* $G_1$ *and* $G_2$ *are isomorphic, if there exists a mapping* $f: G_1 \to G_2$ *such that* (*i*) *f is a homomorphism,* (*ii*) *f is one-to-one and* (*iii*) *f is onto.*

**Remark.** *It can be verified that the relation* $\approx$ *is an equivalence relation i.e.,*

1. $G \approx G$.
2. $G_1 \approx G_2 \Rightarrow G_2 \approx G_1$.
3. $G_1 \approx G_2$ and $G_2 \approx G_3 \Rightarrow G_1 \approx G_3$. [See Example 2.2.20.]

(Here $G, G_1, G_2, G_3$ denote groups)

### Examples of Homomorphisms

**Example 2.1.1.** Let $G_1 = (\mathbf{Z}, +)$ and $G_2 = \{2^n : n \in \mathbf{Z}\}$, where $G_2$ is a group w.r.t. usual multiplication.

The mapping : $f: G_1 \to G_2$ defined as $f(n) = 2^n$ for all $n \in \mathbf{Z}$ is a homomorphism, since for $n_1, n_2 \in \mathbf{Z}$ ;

$$f(n_1 + n_2) = 2^{n_1 + n_2} = 2^{n_1} \cdot 2^{n_2} = f(n_1) \cdot f(n_2).$$

**Example 2.1.2.** Let $G_1 = (\mathbf{Z}, +)$, $G_2 = G_1$.

The mapping $f: G_1 \to G_2$ defined as $f(x) = 2x$ for all $x \in \mathbf{Z}$ is a homomorphism, since for any $x, y \in \mathbf{Z}$ ;

$$f(x + y) = 2(x + y) = 2x + 2y = f(x) + f(y).$$

**Example 2.1.3.** *The identity mapping on a group $G$ is a homomorphism.*

The identity mapping $I$ on a group $G$ is defined as $I(x) = x$ for all $x \in G$. For any $x, y \in G$ ; $xy \in G$ and

$$I(xy) = xy = I(x)\, I(y).$$

Hence $I$ is a homomorphism.

**Example 2.1.4.** *If $G$ is a group, then the mapping $f: G \to G$ defined as $f(x) = e$ for each $x \in G$ is a homomorphism.*

Let $x, y \in G$ so that $xy \in G$. We have

$$f(xy) = e = ee = f(x) f(y).$$

Hence $f$ is a homomorphism.

**Example 2.1.5.** *If $G$ is an abelian group, then the mapping $f: G \to G$ defined as $f(x) = x^5$ for all $x \in G$ is a homomorphism.*

Let $x, y \in G$. Then $f(xy) = (xy)^5$ ·

or

$$f(xy) = x^5 y^5 = f(x) f(y).$$

(Notice that $G$ is an abelian group iff $(xy)^n = x^n y^n$ for any $n \in \mathbf{N}$).

Hence $f$ is a homomorphism.

## 2.2 Theorems on Homomorphisms

In the following theorems ; $G$ and $G'$ denote two groups.

**Theorem 2.2.1.** *If $f: G \to G'$ is a homomorphism, then*

(*i*) $f(e) = e'$.

(*ii*) $f(x^{-1}) = [f(x)]^{-1}$, $x \in G$. [D.U., 1993]

(*iii*) *Further if $f$ is one-to-one, then $o[f(x)]$ divides $o(x)$, $x \in G$.* [D.U., 1993]

**Proof.** (*i*) Let $x \in G$ so that $f(x) \in G'$. Thus

$$f(x)\, e' = f(x), \text{ since } e' \text{ is the identity of } G'$$
$$= f(xe), \text{ since } e \text{ is the identity of } G$$
$$= f(x) f(e), \text{ since } f \text{ is a homomorphism.}$$

Hence by cancellation law in $G'$, we see that

$$f(x)\, e' = f(x) f(e) \Rightarrow e' = f(e)$$

(ii) We have $x x^{-1} = e = x^{-1} x$ for $x \in G$

$\Rightarrow$ $f(xx^{-1}) = f(e) = f(x^{-1} x)$.

Since $f$ is a homomorphism, we obtain

$f(x) f(x^{-1}) = e' = f(x^{-1}) f(x)$ $[\because f(e) = e']$

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

(iii) Let $o[f(x)] = n$. Then $n$ is the least positive integer such that

$$[f(x)]^n = e'$$

$\Rightarrow f(x) f(x) \ldots f(x)$ ($n$ times) $= e'$.

$\Rightarrow f(x . x \ldots x) = f(e)$, since $f$ is a homomorphism

$\Rightarrow$ $f(x^n) = f(e)$

$\Rightarrow$ $x^n = e$, since $f$ is one-to-one

$\Rightarrow n$ divides $o(x)$.

Hence $o[f(x)]$ divides $o(x)$.

**Definition (Kernel of a Homomorphism)**

*If $f: G \to G'$ be a homomorphism, then the* **kernel** *of $f$, denoted as $Ker\, f$ or $K_f$, is defined as*

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

**Remark.** Since $f$ is a homomorphism, $f(e) = e'$ and so $e \in Ker\, f$.

Hence kernel of a homomorphism is always non-empty.

**Theorem 2.2.2.** *Show that every quotient group of a group is a homomorphic image of the group.*

*Or*

*If $N$ is a normal subgroup of a group $G$, show that there is a homomorphism $f$ of $G$ onto $G/N$ with $Ker\, f = N$.* [D.U., 1996]

**Proof.** Define a mapping $f: G \to G/N$ as

$$f(x) = Nx \quad \text{for all} \quad x \in G. \qquad \ldots(1)$$

Clearly $\phi$ is well-defined, since for $x, y \in G$;

$$x = y \Rightarrow Nx = Ny \Rightarrow f(x) = f(y).$$

From (1), $f(xy) = Nxy$

$= Nx\, Ny$, as $N \lhd G$

$= f(x) f(y)$, by (1).

Thus $f$ is a homomorphism. Now we show that $f$ is onto.

Let $X \in G/N$. Then $X = Ng$ for some $g \in G$ or $X = f(g)$, $g \in G$.

Hence $f$ is a homomorphism of $G$ onto $G/N$.

*The mapping $f$ defined by (1) is called the* **natural homomorphism.**

We have $Ker\, f = \{x \in G : f(x) = N, \text{ identity of } G/N\}$

$\therefore$ $x \in Ker\, f \Leftrightarrow f(x) = N \Leftrightarrow Nx = N \Leftrightarrow x \in N$.

Hence $Ker\, f = N$.

**Theorem 2.2.3.** *If $f: G \to G'$ is a homomorphism, then kernel of $f$ is a normal subgroup of $G$.*

**Proof.** By definition, $K_f = \{x \in G : f(x) = e'\}$ is the kernel of $f$.

Since $f$ is a homomorphism, $f(e) = e'$. [Theorem 2.2.1]

Thus $e \in K_f$ and so $K_f$ is non-empty.

Let $x, y \in K_f$. Then $f(x) = e'$ and $f(y) = e'$.

$\therefore \quad f(xy) = f(x) f(y) = e' \cdot e' = e' \Rightarrow xy \in K_f$. ...(1)

Further $f(x^{-1}) = [f(x)]^{-1}$, since $f$ is a homomorphism

$= (e')^{-1} = e'$.

$\therefore \quad f(x^{-1}) = e' \Rightarrow x^{-1} \in K_f$.

It follows that $K_f$ is a subgroup of $G$. Finally, we show that $K_f$ is a normal subgroup of $G$. Let $x \in G$ and $k \in K_f$. Then $f(k) = e'$.

We have

$$\begin{aligned} f(xkx^{-1}) &= f(x) f(k) f(x^{-1}), \text{ since } f \text{ is a homomorphism} \\ &= f(x) \cdot e' \cdot [f(x)]^{-1}, \text{ since } f \text{ is a homomorphism} \\ &= f(x) [f(x)]^{-1}, \text{ since } f(x)\, e' = f(x) \\ &= e'. \end{aligned}$$

$\therefore \quad f(xkx^{-1}) = e' \Rightarrow xkx^{-1} \in K_f \quad \forall \ x \in G, k \in K_f$.

Hence $K_f$ is a normal subgroup of $G$.

**Theorem 2.2.4.** *If $f: G \to G'$ is a homomorphism, then*

$$Ker f = \{e\} \Leftrightarrow f \text{ is one-to-one.}$$ [D.U., 1995, 94]

**Proof.** By definition, $Ker f = \{x \in G : f(x) = e'\}$.

Let $Ker f = \{e\}$. ...(1)

We shall prove that $f$ is one-to-one.

Let $f(x) = f(y)\ ; x, y \in G$

$\Rightarrow \quad f(x) [f(y)]^{-1} = f(y) [f(y)]^{-1} = e'$

$\Rightarrow \quad f(x) f(y^{-1}) = e'$, since $f$ is a homomorphism

$\Rightarrow \quad f(xy^{-1}) = e'$, since $f$ is a homomorphism

$\Rightarrow \quad xy^{-1} \in Ker f$

$\Rightarrow \quad xy^{-1} = e$, by (1)

$x = y$.

Hence $f$ is one-to-one.

Conversely, let $f: G \to G'$ be one-to-one.

We shall show that $Ker f = \{e\}$.

Let $x \in Ker f$ be arbitrary. Then $f(x) = e'$

$\Rightarrow \quad f(x) = f(e)$, since $f$ is a homomorphism

$\Rightarrow \quad x = e$, since $f$ is one-to-one.

Hence $Ker f = \{e\}$.

**Theorem 2.2.5.** *If $f: G \to G'$ is a homomorphism, then $Im\ f$ is a subgroup of $G'$.*

*Or*

*Show that a homomorphic image of a group is a group.*

**Proof.** By definition, $Im\ f = \{f(x) : x \in G\}$.

Since $e \in G$, $f(e) \in Im\ f$ and so $Im\ f$ is non-empty. Let $\alpha, \beta \in Im\ f$.

Then $\alpha = f(x)$ and $\beta = f(y)$, for some $x, y \in G$

$$\Rightarrow \quad \alpha\beta^{-1} = f(x)\,[f(y)]^{-1}$$
$$= f(x) f(y^{-1}), \text{ since } f \text{ is a homomorphism}$$
$$= f(xy^{-1}), \text{ since } f \text{ is a homomorphism}$$
$$\in Im\ f, \text{ since } xy^{-1} \in G.$$

$\therefore \quad \alpha\beta^{-1} \in Im\ f$ for all $\alpha, \beta \in Im\ f$

Hence $Im\ f$ is a subgroup of $G'$.

**Ex.** *If $f: G \to G'$ is a homomorphism, then show that*

$$f(G) = \{f(a) : a \in G\}$$

*is a subgroup of $G'$.*

**Theorem 2.2.6. (Fundamental Theorem of Homomorphism)**

*If $f$ is a homomorphism of $G$ onto $G'$ with kernel $K$, then*

$$\frac{G}{Ker\ f} \simeq G' \quad or \quad \frac{G}{K} \simeq G'. \qquad \text{[D.U., 1998, 94, 91]}$$

*Or*

*Show that every homomorphic image of a group $G$ is isomorphic to a quotient group.* [D.U., 1995]

**Proof.** By definition, $K = \{x \in G : f(x) = e'\}$. ...(1)

We know that $K$ is a normal subgroup of $G$ and so the quotient group $G/K$ is defined, where

$$\frac{G}{K} = \{Kg : g \in G\}.$$

It is given that the mapping

$f: G \to G'$ is homomorphism and onto.

$\Rightarrow \quad f(g) \in G'$ for all $g \in G$.

We define a mapping

$$\phi : \frac{G}{K} \to G' \text{ as}$$

$$\phi(Kg) = f(g)\ \forall\ g \in G. \qquad \text{...(2)}$$

Firstly, we show that $\phi$ is well-defined *i.e.*, we have to show that

$$Kg_1 = Kg_2 \Rightarrow \phi(Kg_1) = \phi(Kg_2)\ ;\ g_1, g_2 \in G.$$

Now $\quad Kg_1 = Kg_2 \Rightarrow g_1 g_2^{-1} \in K$

$\Rightarrow \quad f(g_1 g_2^{-1}) = e'$, by (1)

$\Rightarrow \quad f(g_1) f(g_2^{-1}) = e'$, since $f$ is a homomorphism

$\Rightarrow f(g_1) [f(g_2)]^{-1} = e'$, since $f$ is a homomorphism

$\Rightarrow \quad f(g_1) = f(g_2)$

$\Rightarrow \quad \phi(Kg_1) = \phi(Kg_2)$, by (2).

Thus $\phi$ is well-defined.

Next we show that $\phi$ is a homomorphism.

Let $X, Y \in G/K$. Then $X = Kx$, $Y = Ky$ for some $x, y \in G$. We have

$$XY = Kx\,Ky = Kxy, \quad \text{as} \quad K \lhd G.$$

$$\therefore \quad \phi(XY) = \phi(Kxy)$$

$$= f(xy), \text{ by (2)}$$

$$= f(x) f(y), \text{ since } f \text{ is a homomorphism}$$

$$= \phi(Kx)\, \phi(Ky), \text{ by (2)}$$

$$= \phi(X)\, \phi(Y).$$

Thus $\phi$ is a homomorphism.

Now we show that $\phi$ is one-to-one.

Let $\quad \phi(X) = \phi(Y)$ ; $X = Kx$, $Y = Ky \in G/K$

$\Rightarrow \quad \phi(Kx) = \phi(Ky)$

$\Rightarrow \quad f(x) = f(y)$, by (2)

$\Rightarrow \quad f(x) [f(y)]^{-1} = e'$

$\Rightarrow \quad f(x) f(y^{-1}) = e'$, since $f$ is a homomorphism

$\Rightarrow \quad f(xy^{-1}) = e'$, since $f$ is a homomorphism

$\Rightarrow \quad xy^{-1} \in K$, by (1)

$\Rightarrow \quad Kx = Ky \quad \Rightarrow X = Y.$

Thus $\phi$ is one-to-one.

Lastly, we show that $\phi$ is onto.

Let $g' \in G'$ be arbitrary. Since $f: G \to G'$ is onto, there exists some $g \in G$ such that $f(g) = g'$

$\Rightarrow \quad \phi(Kg) = g'$, by (2). Here $Kg \in G/K$.

Thus $\phi$ is onto. We have now shown that $\phi: G/K \to G'$ is a homomorphism, onto and one-to-one. Hence

$$\frac{G}{K} \approx G' \quad \text{or} \quad G' \approx \frac{G}{K}.$$

**Theorem 2.2.7.** *If $H$ and $K$ are subgroups of a group $G$ and $H$ is normal in $G$, then*

$$\frac{HK}{H} \approx \frac{K}{H \cap K}.$$ [D.U., 1993]

**Proof.** Since $H \lhd G$ ; $H \cap K \lhd K$ and $H \lhd HK$. Consequently, the quotient groups

$\frac{HK}{H}$ and $\frac{K}{H \cap K}$ are defined.

We define a mapping

$$\phi : K \to \frac{HK}{H} \text{ as} \qquad \ldots(1)$$

$$\phi(k) = Hk \quad \text{for all} \quad k \in K.$$

It is easy to see that $\phi$ is well defined, since

$$k_1 = k_2 \Rightarrow Hk_1 = Hk_2 \Rightarrow \phi(k_1) = \phi(k_2), \text{ by (1).}$$

Now we show that $\phi$ is a homomorphism.

Let $k_1, k_2 \in K$. By (1), we have

$$\begin{aligned} \phi(k_1 k_2) &= Hk_1k_2 \\ &= Hk_1\, Hk_2, \text{ as } H \lhd G \\ &= \phi(k_1)\,\phi(k_2), \text{ by (1).} \end{aligned}$$

Thus $\phi$ is a homomorphism.

Next we show that $\phi$ is onto.

Let $X \in \frac{HK}{H}$. Then $X = Hg$ for some $g \in HK$.

Now $g \in HK \Rightarrow g = hk$ for some $h \in H, k \in K$.

$\therefore \quad X = Hhk = Hk$, since $h \in H \Rightarrow Hh = H$.

Using (1), $X = \phi(k)$ ; $k \in K$. Thus $\phi$ is onto.

Since $\phi : K \to \frac{HK}{H}$ is homomorphism and onto, by Fundamental theorem of homomorphism, we have

$$\frac{K}{Ker\,\phi} \approx \frac{HK}{H} \qquad \ldots(2)$$

Now $Ker\,\phi = \{x \in K : \phi(x) = H$, identity of $HK/H\}$.

It follows that

$$\begin{aligned} x \in Ker\,\phi &\Leftrightarrow \phi(x) = H \text{ and } x \in K \\ &\Leftrightarrow Hx = H \text{ and } x \in K, \text{ by (1)} \\ &\Leftrightarrow x \in H \text{ and } x \in K \\ &\Leftrightarrow x \in H \cap K. \end{aligned}$$

$\therefore \quad Ker\,\phi = H \cap K.$ ...(3)

From (2) and (3), $\frac{K}{H \cap K} \approx \frac{HK}{H}$.

Hence $\frac{HK}{H} \approx \frac{K}{H \cap K}$.

**Ex.** *If $H$ and $K$ are subgroups of a group $G$ and $K$ is normal in $G$, then*

$$\frac{HK}{K} \approx \frac{H}{H \cap K}. \qquad \text{[D.U., 1996]}$$