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 $G_1 \approx G_2$.

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**

1

GROUPS

1.1 Some Sets of Numbers

The reader is familiar with the following sets of numbers :

1. $\mathbf{N} = \{1, 2, 3, \ldots\}$
   is the set of *natural numbers.*
2. $\mathbf{I}$ or $\mathbf{J}$ or $\mathbf{Z} = \{\ldots\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$
   is the set of *integers.*
   $\mathbf{Z}^+$ denotes the set of all non-negative integers.
3. $\mathbf{E} = \{\ldots\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\ldots\}$
   is the set of *even integers.*
4. $\mathbf{Q} = \left\{ \dfrac{m}{n} : m, n \in \mathbf{Z} \text{ and } n \neq 0 \right\}$
   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.**

17. **(Fundamental Theorem of Homomorphism)**
If f is a homomorphism of a group G onto a group G' with kernel K, then

$$\frac{G}{K} \approx G'.$$

18. A isomorphism of a group G onto G is called an **automorphism** of G. The set of all automorphisms of G is denoted by $Aut\ G$.
The set $I(G) = \{T_g : g \in G\}$, where $T_g : G \to G$ is defined as

$$T_g(x) = gxg^{-1}\ \forall\ x \in G,$$

is called the group of **inner automorphisms** of G.
We have

(i) $I(G) \triangleleft Aut\ G$. (ii) $\frac{G}{Z} \approx I(G)$, where

$Z = \{a \in G : ax = xa\ \forall\ x \in G\}$ and is called the **centre** of G.

19. The **class equation** of a finite group G is

$$o(G) = o(Z) + \sum_{a \notin Z} \frac{o(G)}{o(N(a))},$$

where $N(a) = \{x \in G : xa = ax\}$, and is called the **normalizer** of a in G.

20. If $o(G) = p^n$, where p is prime ; then $o(Z) > 1$.

21. A group of order p^2 is abelian, p being prime.

22. **(Cauchy's Theorem)**
If G is a finite group and p divides $o(G)$ (p a prime), then there exists some element $a \neq e \in G$ such that $a^p = e$.

23. If $o(G) = p^n$, p a prime, then every subgroup of G of order p^{n-1} is normal in G.

24. If G is a finite group, then a subgroup H of G such that $o(H) = p^m$ (p a prime), where $p^m \mid o(G)$, $p^{m+1} \nmid o(G)$; is called a **Sylow p-subgroup** of G.

25. **Sylow Theorems**

First Sylow Theorem. *If G is a finite group such that $p^n \mid o(G)$ and $p^{n+1} \nmid o(G)$ (p being prime), then G has a subgroup H of order p^n. H is called a Sylow p-subgroup of G.*

Second Sylow Theorem. *Any two Sylow p-subgroups of a finite group G are conjugate in G i.e., if P and Q are two Sylow p-subgroups of G then*

$$Q = xPx^{-1} \text{ for some } x \in G.$$

Third Sylow Theorem. *The number (n_p) of Sylow p-subgroups of a finite group G is given by*

$$n_p = 1 + kp\ (k = 0, 1, 2, \ldots), \text{ where } n_p \text{ divides } o(G).$$

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 $x_1, x_2 \in \mathbf{Z}^+$

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

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

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

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

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

1

GROUPS

1.1 Some Sets of Numbers

The reader is familiar with the following sets of numbers :

1. $\mathbf{N} = \{1, 2, 3, \ldots\}$
   is the set of *natural numbers*.
2. $\mathbf{I}$ or $\mathbf{J}$ or $\mathbf{Z} = \{\ldots\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$
   is the set of *integers*.
   $\mathbf{Z}^+$ denotes the set of all non-negative integers.
3. $\mathbf{E} = \{\ldots\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\ldots\}$
   is the set of *even integers*.
4. $\mathbf{Q} = \left\{ \dfrac{m}{n} : m, n \in \mathbf{Z} \text{ and } n \neq 0 \right\}$
   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*

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

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 $x_1, x_2 \in \mathbf{Z}^+$

$$x_1 \neq x_2 \quad \Rightarrow \quad x_1^2 \neq x_2^2 \quad \Rightarrow \quad f(x_1) \neq f(x_2).$$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Hence $\quad (hog) \circ f = h \circ (gof).$

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

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

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), $\quad g(f(a)) = c$

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

Hence gof is onto.

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

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

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

$\Rightarrow \quad a_1 = a_2,$ 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),

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

Now

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

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*
$$foi = iof = f, \quad \text{for each } f \in A(S).$$
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

$$(f \circ i)(x) = f(i(x)) = f(x),$$

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

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

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 $a \,.\, b \in \mathbf{N}$ 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 $a \sim b$ 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 $(b - c)$

$\Rightarrow \quad n$ 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* **Z** *as :*

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

is an equivalence relation on **Z**.

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

Example 1.4.5. *Show that the relation ~ defined on* **Z** *as :*

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

is an equivalence relation on **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* **Z** *defined by*

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

is an equivalence relation. Various equivalence classes in **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 **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 $a \sim b \Rightarrow x \sim b \Rightarrow x \in cl(b)$. ...(1)

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

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 $b \sim a \Rightarrow x \sim a \Rightarrow x \in cl(a)$ ...(2)

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

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 $a \sim a$, $a \in cl(a)$

$\Rightarrow$ $a \in \bigcup_{x \in A} cl(x)$. ...(3)

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

By definition, $cl(x) \subseteq A$ for each $x \in A$ ...(4)

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

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* $\sim$ *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 $\quad a^{-n} = (a^{-1})^n$.

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

Similarly, **(R, +)**, **(Q, +)** are groups.

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

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

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

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

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

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

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

(*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.**

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

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 α^r $(1 \le r \le n-1)$ is $\alpha^{n-r} \in G$, since $\alpha^r . \alpha^{n-r} = \alpha^n = 1$.

Example 1.7.11. *The set M_2 of all 2×2 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_α for each $A_\alpha \in G$, since

$$A_\alpha A_{-\alpha} = A_{\alpha+(-\alpha)} = A_0 = I_0, \text{ using (1).}$$

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 α^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 2×2 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_α for each $A_\alpha \in G$, since

$$A_\alpha A_{-\alpha} = A_{\alpha+(-\alpha)} = A_0 = I_0, \text{ using (1).}$$

Example 1.7.13. *Show that* $G = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \neq 0 \in \mathbb{R} \right\}$ *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

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

(*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

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

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 $\quad A^{-1} = A, B^{-1} = B, C^{-1} = C$ 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 2×2 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 $\quad A, B \in S$ 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 Moduto $n \equiv \mathbf{J_n}$ 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.

Example 1.7.21. *Give the examples of the following groups :*

(*i*) *An infinite group.* [**Ans.** (**I**, +), (**R***, .)]

(*ii*) *A finite group.* [**Ans.** $G = \{1, -1, i, -i\}$ under multiplication]

(*iii*) *An infinite abelian group.* [**Ans.** (**I**, +), (**R***, .)]

(*iv*) *An infinite non-abelian group.*

[**Ans.** The set S of all 2×2 non-singular matrices w.r.t. the multiplication of two matrices. See Example 1.7.15.]

(*v*) *A finite non-abelian group.*

[**Ans.** $G = \{\pm 1, \pm i, \pm j, \pm k\}$, $i^2 = j^2 = k^2 = -1$, and $ij = -ji = k, jk = -kj = i, ki = -ik = j$ is a non-abelian multiplicative group of order 8. This group is called **Quaternion Group.**]

Example 1.7.22. *Show that the set* $G = \{f_1, f_2, f_3, f_4\}$, *where*

$f_1(x) = x, f_2(x) = -x, f_3(x) = 1/x, f_4(x) = -1/x \ \forall \ x \in \mathbf{R} \sim \{0\}$

is a group w.r.t. the product of two mappings.

The *product or composite* of two mappings

$f : \mathbf{R} \to \mathbf{R}, g : \mathbf{R} \to \mathbf{R}$ is defined as

$fog : \mathbf{R} \to \mathbf{R}$, where $(fog)(x) = f(g(x)) \ \forall \ x \in \mathbf{R}$.

For example, $(f_1 \, o \, f_2)(x) = f_1(f_2(x)) = f_1(-x) = -x = f_2(x)$ and so $f_1 \, o \, f_2 = f_2$; $(f_3 \, o \, f_2)(x) = f_3(f_2(x)) = f_3(-x) = -1/x = f_4(x)$ and so $f_3 \, o \, f_2 = f_4$ etc.

The composition table of G is as follows :

o	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_1	f_4	f_3
f_3	f_3	f_4	f_1	f_2
f_4	f_4	f_3	f_2	f_1

Hence (G, o) is a group in which f_1 is the identity and

$$f_i^{-1} = f_i \quad \text{for} \quad i = 1, 2, 3, 4.$$

Example 1.7.23. *Show that the set* $G = \{f_1, f_2, f_3, f_4, f_5, f_6\}$, *where*

$$f_1(x) = x, f_2(x) = 1 - x, f_3(x) = 1/x,$$

$$f_4(x) = 1/(1-x), f_5(x) = (x-1)/x, f_6(x) = x/(x-1) \ \forall \ x \in \mathbf{R} \sim \{0, 1\}$$

is a group w.r.t. 'composite of functions'.

Solution. The composition table of G is as follows :

o	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_5	f_6	f_3	f_4
f_3	f_3	f_4	f_1	f_2	f_6	f_5
f_4	f_4	f_3	f_6	f_5	f_1	f_2
f_5	f_5	f_6	f_2	f_1	f_4	f_3
f_6	f_6	f_5	f_4	f_3	f_2	f_1

Hence (G, o) is a group in which f_1 is the identity element and the inverse elements of $f_1, f_2, f_3, f_4, f_5, f_6$ are $f_1, f_2, f_3, f_5, f_4, f_6$ respectively. Also G is not commutative, since $f_3 \, o \, f_5 \neq f_5 \, o \, f_3$.

Example 1.7.24. *Show that the set $G = \{x + y\sqrt{3} : x, y \in \mathbf{Q}\}$ is a group w.r.t. addition.*

Let $a = x_1 + y_1\sqrt{3}$, $b = x_2 + y_2\sqrt{3}$ and $c = x_3 + y_3\sqrt{3}$ be any three elements of G, where x_i and $y_i \in \mathbf{Q}$ for $i = 1, 2, 3$.

(*i*) **Closure law.** We have

$$a + b = (x_1 + x_2) + (y_1 + y_2)\sqrt{3} \in G,$$

since $x_1 + x_2 \in \mathbf{Q}$ and $y_1 + y_2 \in \mathbf{Q}$.

(*ii*) **Associative law.** We have

$$\begin{aligned}(a + b) + c &= \{(x_1 + x_2) + (y_1 + y_2)\sqrt{3}\} + (x_3 + y_3\sqrt{3}) \\ &= \{(x_1 + x_2) + x_3\} + \{(y_1 + y_2) + y_3\}\sqrt{3} \\ &= \{x_1 + (x_2 + x_3)\} + \{y_1 + (y_2 + y_3)\}\sqrt{3}, \\ &\qquad \text{by associative law in } \mathbf{Q} \\ &= (x_1 + y_1\sqrt{3}) + \{(x_2 + x_3) + (y_2 + y_3)\sqrt{3}\} \\ &= a + (b + c).\end{aligned}$$

(*iii*) **Identity element.** Clearly $0 = 0 + 0\sqrt{3} \in G$ is the additive identity in G.

(*iv*) **Inverse element.** Clearly, $-a = -x_1 - y_1\sqrt{3} \in G$ is the inverse of

$$a = x_1 + y_1\sqrt{3} \in G.$$

Hence $(G, +)$ is a group.

Example 1.7.25. *Show that the set I of all integers with binary operation, defined as $a \,.\, b = a + b + 1 \;\forall\; a, b \in I$ is an abelian group.*

It is given that $a \,.\, b = a + b + 1 \;\forall\; a, b \in I$. ...(1)

Let a, b, c be any three integers.

(*i*) **Closure law.** We have $a \,.\, b = a + b + 1 \in I$.

(*ii*) **Commutative law.** We have $a \cdot b = a + b + 1$

$\Rightarrow \quad a \cdot b = b + a + 1$, by commutative law in I.

$\Rightarrow \quad a \cdot b = b \cdot a$, by (1).

(*iii*) **Associative law.** We have

$$(a \cdot b) \cdot c = (a + b + 1) \cdot c, \text{ by (1)}$$
$$= (a + b + 1) + c + 1, \text{ by (1)}$$
$$= a + (b + c + 1) + 1,$$

by associative and commutative laws in I.

$$= a + x + 1, \text{ where } x = b + c + 1 = b \cdot c$$
$$= a \cdot x = a \cdot (b \cdot c).$$

(*iv*) **Identity element.** Clearly $e = -1 \in I$ is the identity, since

$$a \cdot e = a + e + 1 = a - 1 + 1 = a \quad \forall \quad a \in I.$$

(*v*) **Inverse element.**

Consider $a \cdot (-a - 2) = a + (-a - 2) + 1 = -1 = e$.

$\therefore \quad a^{-1} = -a - 2 \ \forall \ a \in I.$

Hence $(I, \cdot)$ is an abelian group.

Example 1.7.26. *Show that the set Q^+ of all positive rational numbers is an abelian group under the binary operation $*$ defined by $a * b = ab/3$, where ab is the ordinary multiplication of two positive rational numbers a and b.*

We have $\quad a * b = \dfrac{ab}{3}$ for all $a, b \in Q^+$ ...(1)

(*i*) **Closure law.** From (1), $a * b \in Q^+$ for all $a, b \in Q^+$.

(*ii*) **Commutative law.** Since $ab = ba \ \forall \ a, b \in Q^+$, so by (1)

$$a * b = b * a \quad \forall \quad a, b \in Q^+.$$

(*iii*) **Associative law.** From (1), $(a * b) * c = \dfrac{ab}{3} * c = \dfrac{abc}{9}$.

Similarly, $\quad a * (b * c) = \dfrac{abc}{9}$. Thus $(a * b) * c = a * (b * c)$.

(*iv*) **Identity.** Clearly $e = 3 \in Q^+$ is the identity, since by (1)

$$a * 3 = 3 * a = \frac{3a}{3} = a \quad \forall \quad a \in Q^+.$$

(*v*) **Inverse.** We have $a * \left(\dfrac{9}{a}\right) = \dfrac{9a}{3a} = 3$, by (1).

Thus $a^{-1} = 9/a$ for each $a \in Q^+$.

Hence $(Q^+, *)$ is an abelian group.

Example 1.7.27. *Show that the set* **Q** *of all rational numbers other than -1 is an abelian group w.r.t. the binary composition*

$$a * b = a + b + ab.$$

We have $a * b = a + b + ab \quad \forall \quad a, b \in \mathbf{Q}$. ...(1)

(*i*) **Closure law.** From (1), $a * b \in \mathbf{Q}$ for all $a, b \in \mathbf{Q}$.

(*ii*) **Associative law.** From (1), $(a * b) * c = (a + b + ab) * c$

$$= (a + b + ab) + c + (a + b + ab)\, c, \text{ by (1)}$$
$$= a + b + c + ab + ac + bc + abc.$$

Similarly, $a * (b * c) = a + b + c + ab + ac + bc + abc$.

Thus $\quad a * (b * c) = (a * b) * c$.

(*iii*) **Identity.** From (1), $a * 0 = a + 0 + a0 = a \ \forall \ a \in \mathbf{Q}$.

Thus 0 is the identity in $\mathbf{Q}$.

(*iv*) **Identity.** For $a \neq -1$, $a' = -a/(a+1) \in \mathbf{Q}$ and by (1)

$$a * a' = a - \frac{a}{a+1} - \frac{a^2}{a+1} = 0. \text{ Similarly, } a' * a = 0.$$

Thus a' is the inverse of a. Hence $(\mathbf{Q}, *)$ is an abelian group, since $a * b = a + b + ab = b + a + ba = b * a$.

Example 1.7.28. *Let $G = \{(a, b) : a \neq 0, b \in \mathbf{R}\}$ and $*$ be a binary composition defined by* ...(1)

$$(a, b) * (c, d) = (ac, bc + d).$$

Show that $(G, *)$ is a non-abelian group.

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

From (1), $(a, b) * (c, d) = (ac, bc + d) \in G$, since

$$a \neq 0 \quad \text{and} \quad c \neq 0 \quad \Rightarrow \quad ac \neq 0 \in \mathbf{R} \quad \text{and} \quad bc + d \in \mathbf{R}.$$

(*ii*) **Associative law.** Let $x = (a, b), y = (c, d), z = (e, f) \in G$.

Then $\quad (x * y) * z = (ab, bc + d) * (e, f)$, by (1)

$$= ((ac)\, e, (bc + d)\, e + f), \text{ by (1)}$$
$$= (a\,(ce), b\,(ce) + de + f)$$
$$= (a, b) * (ce, de + f), \text{ by (1)}$$
$$= (a, b) * \{(c, d) * (e, f)\}, \text{ by (1)}$$

$\therefore \quad (x * y) * z = x * (y * z) \ \forall \ x, y, z \in G$.

(*iii*) **Identity.** $(1, 0)$ is the identity in G, since

$$(a, b) * (1, 0) = (a1, b1 + 0) = (a, b), \text{ by (1)}$$

and $\quad (1, 0) * (a, b) = (1a, 0a + b) = (a, b)$, by (1).

(*iv*) **Inverse.** Let $x = (a, b) \in G$ so that $a \neq 0$, $b \in \mathbf{R}$. Then

$$x^{-1} = (a^{-1}, -ba^{-1}) \text{ is the inverse of } x, \text{ since}$$

$$x^{-1} * x = (a^{-1}, -ba^{-1}) * (a, b)$$
$$= (a^{-1}a, -ba^{-1}\, a + b) = (1, 0).$$

Similarly, $\quad x * x^{-1} = (1, 0)$.

Hence $(G, *)$ is a group, which is non-abelian, since

$$(1, 2) * (2, 3) = (1.2, 2.2 + 3) = (2, 7), \text{ by (1)}$$

and so

$$(2, 3) * (1, 2) = (2.1, 3.1 + 2) = (2, 5), \text{ by (1)}$$

$$(1, 2) * (2, 3) \neq (2, 3) * (1, 2).$$

Example 1.7.29. *Let $G = \{(a, b) : a, b \in \mathbf{R}$ and not both zero$\}$ and $*$ be a binary composition defined by* ...(1)

$$(a, b) * (c, d) = (ac - bd, ad + bc).$$

Show that $(G, *)$ is a commutative group.

(*i*) **Closure law**

From (1), $(a, b) * (c, d) \in G \quad \forall \ (a, b) \in G$ and $(c, d) \in G$,

since $ac - bd, ad + bc$ are not both zero.

(*ii*) **Associative law** can be verified as done in Example 1.7.28.

(*iii*) **Identity.** $(1, 0)$ is the identity element in G, since

$$(a, b) * (1, 0) = (a.1 - b.0, a.0 + b.1) = (a, b), \text{ by (1)}.$$

(*iv*) **Inverse.** Let $x = (a, b) \in G$ so that a and b are not both zero.

Then $$x^{-1} = \left(\frac{a}{a^2 + b^2}, -\frac{b}{a^2 + b^2}\right) \in G \text{ is the inverse of } x,$$

$$(a^2 + b^2 \neq 0)$$

since $$x * x^{-1} = \left(\frac{a^2 + b^2}{a^2 + b^2}, -\frac{ab + ba}{a^2 + b^2}\right) = (1, 0).$$

Similarly, $x^{-1} * x = (1, 0)$.

(*v*) **Commutative law.** From (1), we have

$$\begin{aligned}(a, b) * (c, d) &= (ac - bd, ad + bc)\\ &= (ca - db, cb + da), \text{ as } \mathbf{R} \text{ is commutative}\\ &= (c, d) * (a, b), \text{ by (1)}.\end{aligned}$$

Example 1.7.30. *Let $G = \{(a, b) : a, b \in \mathbf{R}\}$, and $*$ be a binary composition defined by* $(a, b) * (c, d) = (a + c, b + d) \quad \forall \ a, b, c, d \in \mathbf{R}$. ...(1)

Show that $(G, *)$ is a commutative group.

(*i*) **Closure law** is obviously true.

(*ii*) **Associative law.** We have

$$\begin{aligned}\{(a, b) * (c, d)\} * (e, f) &= (a + c, b + d) * (e, f)\\ &= ((a + c) + e, (b + d) + f), \text{ by (1)}\\ &= (a + (c + e), b + (d + f)),\\ &\qquad \text{by associative law in } \mathbf{R}\\ &= (a, b) * (c + e, d + f), \text{ by (1)}\\ &= (a, b) * \{(c, d) * (e, f)\}.\end{aligned}$$

(*iii*) **Identity.** $(0, 0)$ is the identity element in G, since

$$(a, b) + (0, 0) = (a + 0, b + 0) = (a, b) \ \forall \ a, b \in \mathbf{R}.$$

(*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 $a \,.\, e_1 = e_1 \,.\, a = a \;\; \forall \;\; a \in G,$ ...(1)

and $a \,.\, e_2 = e_2 \,.\, a = a \;\; \forall \;\; a \in G.$ ...(2)

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

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

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

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

$$a \,.\, c = c \,.\, a = e. \quad ...(4)$$

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

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

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

$= e \,.\, c$, 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*) $a \,.\, b = a \,.\, c \Rightarrow b = c.$ (*left cancellation law*)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$$\begin{aligned} c \,.\, d &= (a \,.\, b) \,.\, d = a \,.\, (b \,.\, d), \text{ by associative law} \\ &= a \,.\, [b \,.\, (b^{-1} \,.\, a^{-1})]. \\ &= a \,.\, [(b \,.\, b^{-1}) \,.\, a^{-1}], \text{ by associative law} \\ &= a \,.\, (e \,.\, a^{-1}), \qquad (\because b \,.\, b^{-1} = e) \\ &= a \,.\, a^{-1}, \text{ since } e \text{ is the identity} \end{aligned}$$

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

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

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

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

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

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

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

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

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

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

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

$$\begin{aligned} b \cdot e &= (y \cdot a) \cdot e, \text{ by (1)} \\ &= y \cdot (a \cdot e), \text{ since } G \text{ is a semi-group} \\ &= y \cdot a, \text{ by (2)} \\ &= b, \text{ by (1).} \end{aligned} \qquad \ldots(3)$$

$$\therefore \qquad b \cdot e = b \quad \forall \; b \in G.$$

Again

$$\begin{aligned} f \cdot b &= f \cdot (a \cdot x), \text{ by (1)} \\ &= (f \cdot a) \cdot x = a \cdot x = b, \text{ by (2) and (1).} \end{aligned} \qquad \ldots(4)$$

$$\therefore \qquad f \cdot b = b \quad \forall \; b \in G.$$

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

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

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

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

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

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

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

$$\therefore \qquad p = q.$$

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 $a \cdot x = b$ and $y \cdot a = b$ have solutions in G.*

Or

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

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

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

Proof. Condition is sufficient

Suppose G is a semi-group such that for any $a, b \in G$, the equations $a \cdot x = b$ and $y \cdot a = b$ 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 $a \cdot x = b$ and $y \cdot a = b$ 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 cancellation 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

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

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

$$a \cdot a_i = a \cdot a_j \quad \text{for some} \quad i \ne j,$$

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

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

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

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

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

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

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

$\Rightarrow \quad a_i = a_i \cdot a_k$, by right cancellation law ...(6)

Thus $\quad a_i = a_i \cdot a_k$ for all i, $1 \le i \le n$.

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

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

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

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

$\therefore \quad a_k = a_l$.

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

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

Hence a_k is the identity element in G.

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

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

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

Now $\quad a_p = e \cdot a_p$, 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

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

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

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.*,

$$\begin{aligned} a + b = a + c &\Rightarrow b = c \\ b + a = c + a &\Rightarrow b = c \end{aligned} \quad ; \quad a, b, c \in \mathbf{N}$$

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 :

$$a \cdot b = b \text{ for all } a, b \in G. \quad ...(1)$$

For any $a, b, c \in G$, we have

$a \cdot (b \cdot c) = a \cdot c = c$, by (1)

$(a \cdot b) \cdot c = b \cdot c = c$, by (1)

Thus G is a finite semi-group in which left cancellation law holds, since

$$a \cdot b = a \cdot c \Rightarrow b = c, \text{ using (1).}$$

Let a, b be any two distinct elements of G. Then

$$a \cdot b = b \text{ and } b \cdot b = b \text{ ; using (1).}$$

$\therefore$ $a \cdot b = b \cdot b$ but $a \neq b$.

Thus right cancellation law does not hold in G.

Hence G is **not** a group.

Theorem 1.8.8. *A finite semi-group G is a group if and only if G satisfies both the cancellation laws.*

Proof. Condition is necessary

Let a finite semi-group G be a group. Then by Theorem 1.8.2, both the cancellation laws hold in G.

Condition is sufficient

Suppose G is a finite semi-group which satisfies both the cancellation laws. Then by Theorem 1.8.7, G is a group.

Theorem 1.8.9. *A semi-group $(G, .)$ is a group iff the following conditions are satisfied.:*

(*i*) *There exists an element $e \in G$ such that $a \cdot e = a \ \forall \ a \in G$.*

(*ii*) *For each $a \in G$, there exists an element $a' \in G$ such that*

$$a \cdot a' = e.$$

Proof. Conditions are sufficient

Suppose a semi-group $(G, .)$ satisfies the given two conditions. Let $a \in G$ be arbitrary. Then, by (*ii*), there exists some $a' \in G$ such that

$$a \cdot a' = e. \quad \text{...(1)}$$

Since $a' \in G$, so by (*ii*) again, there exists some $a'' \in G$ such that

$$a' \cdot a'' = e. \quad \text{...(2)}$$

Since G is a semi-group, so $a, a' \in G \Rightarrow a' \cdot a \in G$.

By condition (*i*), we have

$$\begin{aligned} a' \cdot a &= (a' \cdot a) \cdot e \\ &= a' \cdot (a \cdot e), \text{ by associative law in } (G, .) \\ &= a' \cdot \{a \cdot (a' \cdot a'')\}, \text{ by (2)} \\ &= a' \cdot \{(a \cdot a') \cdot a''\}, \text{ by associative law in } (G, .) \\ &= a' \cdot (e \cdot a''), \text{ by (1)} \\ &= (a' \cdot e) \cdot a'', \text{ by associative law in } (G, .) \\ &= a' \cdot a'', \text{ by condition } (i) \\ &= e, \text{ by (2).} \end{aligned}$$

$\therefore$ $a' \cdot a = e.$ ...(3)

From (1) and (3), we have

$$a \cdot a' = a' \cdot a = e. \qquad \ldots(4)$$

Now $\quad e \cdot a = (a \cdot a') \cdot a$, by (1)

$= a \cdot (a' \cdot a)$, by associative law in $(G, .)$

$= a \cdot e$, by (3)

$= a$, by condition (i).

$\therefore \quad a \cdot e = e \cdot a = a \ \forall \ a \in G.$

Thus e is the identity in G and by (4), each $a \in G$ has its inverse $a' \in G$. Hence G is a group.

Conditions are necessary

Let G be a group. By the definition of a group, the conditions (i) and (ii) immediately follow.

Remark. The above theorem may be restated as :

A semi-group $(G, .)$ is a group iff

(i) *G has a right identity.*

(ii) *Each element in G has a right inverse in G.*

Theorem 1.8.10. *A semi-group $(G, .)$ is a group iff it satisfies the following conditions :*

(i) *There exists an element $e \in G$ such that $e \cdot a = a$ for all $a \in G$.*
(i.e., G has a left identity)

(ii) *For each $a \in G$, there exists $a' \in G$ such that $a' \cdot a = e$.*
(i.e., each element in G has a left inverse)

Proof. Conditions are sufficient

Suppose a semi-group $(G, .)$ satisfies the conditions (i) and (ii). Let $a \in G$ be arbitrary. Then by (ii), there exists some $a' \in G$ such that

$$a' \cdot a = e. \qquad \ldots(1)$$

Again by (ii), for $a' \in G$, there exists some $a'' \in G$ such that

$$a'' \cdot a' = e. \qquad \ldots(2)$$

Since $a \cdot a' \in G$, so by (i)

$a \cdot a' = e \cdot (a \cdot a')$

$= (e \cdot a) \cdot a'$, by associative law in G

$= [(a'' \cdot a') \cdot a] \cdot a'$, by (2)

$= [a'' \cdot (a' \cdot a)] \cdot a'$, by associative law in G

$= (a'' \cdot e) \cdot a'$, by (1)

$= a'' \cdot (e \cdot a')$, by associative law in G

$= a'' \cdot a'$, by condition (i)

$= e$, by (2)

$\therefore \quad a \cdot a' = a' \cdot a = e.$

Now $\quad a \cdot e = a \cdot (a' \cdot a)$, by (1) $\qquad \ldots(3)$

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

$= e \cdot a$, by (3)

$= a$, by condition (*i*).

$\therefore \quad a \,.\, e = e \,.\, a = a \quad \forall \quad a \in G.$

Thus e is the identity in G and by (3), each $a \in G$ has the inverse $a' \in G$. Hence G is a group.

Conditions are necessary

Let G be a group. By the definition of a group, the conditions (*i*) and (*ii*) immediately follow.

Theorem 1.8.11. *Prove, by an example, that the conclusion of Theorem 1.8.9 is false if*

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

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

(*i.e., G has a right identity*)

(*ii*) *For each $a \in G$, there exists $a' \in G$ such that $a' \,.\, a = e$.*

(*i.e., each element in G has a left inverse*)

Proof. Let G be any set having at least two elements. Define a composition in G as follows :

$$a \,.\, b = a \quad \forall \quad a, b \in G. \qquad \text{—(1)}$$

For any $a, b, c \in G$, we have

$$(a \,.\, b) \,.\, c = a \,.\, c = a, \text{ using (1)}$$

and $\quad a \,.\, (b \,.\, c) = a \,.\, b = a$, using (1).

Thus $(G, .)$ is a semi-group.

Let $e \in G$ be any fixed element. By (1), we have

$$a \,.\, e = a \quad \forall \quad a \in G.$$

Thus e is a right identity in G.

For $e \in G$ and $a \in G$, we have

$$e \,.\, a = e, \text{ by (1).}$$

Thus e is the left inverse for all $a \in G$.

Thus the semi-group $(G, .)$ satisfies the conditions (*i*) and (*ii*).

For any two distinct elements a, b in G, we have

$$a \,.\, b = a \quad \text{and} \quad a \,.\, a = a, \text{ by (1)}$$

$$\therefore \quad a \,.\, b = a \,.\, a, \text{ but } b \neq a.$$

Thus left cancellation law does not hold in G and so G is not a group.

Ex. *Give an example of a semi-group G which has a left identity and right inverse for each of its elements but it fails to be a group.*

Hint. Let G be any set having at least two elements, where $a \,.\, b = b \;\forall$ $a, b \in G$.

EXAMPLES

Example 1.8.1. *If an element a of a group G satisfies $a^2 = a$, then show that $a = e$.*

(*An element $a \in G$ satisfying $a^2 = a$ is called* **idempotent**)

$= a$, by condition (*i*).

$\therefore \quad a \cdot e = e \cdot a = a \quad \forall \quad a \in G.$

Thus e is the identity in G and by (3), each $a \in G$ has its inverse $a' \in G$. Hence G is a group.

Conditions are necessary

Let G be a group. By the definition of a group, the conditions (*i*) and (*ii*) immediately follow.

Theorem 1.8.11. *Prove, by an example, that the conclusion of Theorem 1.8.9 is false if*

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

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

(*i.e., G has a right identity*)

(*ii*) *For each* $a \in G$, *there exists* $a' \in G$ *such that* $a' \cdot a = e$.

(*i.e., each element in G has a left inverse*)

Proof. Let G be any set having at least two elements. Define a composition in G as follows :

$$a \cdot b = a \quad \forall \quad a, b \in G. \qquad \text{...(1)}$$

For any $a, b, c \in G$, we have

$$(a \cdot b) \cdot c = a \cdot c = a, \text{ using (1)}$$

and $\quad a \cdot (b \cdot c) = a \cdot b = a$, using (1).

Thus $(G, .)$ is a semi-group.

Let $e \in G$ be any fixed element. By (1), we have

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

Thus e is a right identity in G.

For $e \in G$ and $a \in G$, we have

$$e \cdot a = e, \text{ by (1).}$$

Thus e is the left inverse for all $a \in G$.

Thus the semi-group $(G, .)$ satisfies the conditions (*i*) and (*ii*).

For any two distinct elements a, b in G, we have

$$a \cdot b = a \quad \text{and} \quad a \cdot a = a, \text{ by (1)}$$

$\therefore \quad a \cdot b = a \cdot a$, but $b \neq a$.

Thus left cancellation law does not hold in G and so G is not a group.

Ex. *Give an example of a semi-group G which has a left identity and right inverse for each of its elements but it fails to be a group.*

Hint. Let G be any set having at least two elements, where $a \cdot b = b \ \forall$ $a, b \in G$.

EXAMPLES

Example 1.8.1. *If an element a of a group G satisfies* $a^2 = a$, *then show that* $a = e$.

(*An element* $a \in G$ *satisfying* $a^2 = a$ *is called* **idempotent**).

Solution. $a^2 = a \Rightarrow a \,.\, a = a \Rightarrow a \,.\, a = a \,.\, e, \Rightarrow a = e$, by left cancellation law in G. Hence $a = e$.

Example 1.8.2. *Prove that if G is an abelian group, then $(a \,.\, b)^n = a^n \,.\, b^n$ for all $a, b \in G$ and all positive integers n.*

Solution. Obviously the result is true for $n = 1$.

Let the result be true for $n = m$, so that ...(1)

$$(a \,.\, b)^m = a^m \,.\, b^m.$$

Then $(a \,.\, b)^{m+1} = (a \,.\, b)^m \,.\, (a \,.\, b)$

$= a^m \,.\, b^m \,.\, b \,.\, a$, by (1) and since G is abelian

$= a^m \,.\, b^{m+1} \,.\, a$

$= a^m \,.\, a \,.\, b^{m+1}$, since G is abelian

$= a^{m+1} \,.\, b^{m+1}$.

Thus the result is true for $n = m + 1$. By the principle of induction, we see that

$$(a \,.\, b)^n = a^n \,.\, b^n \text{ for all positive integers } n.$$

Example 1.8.3. *If G is a group and if $a, b \in G$, show that*

$$a \,.\, b = b \,.\, a \;\Rightarrow\; (a \,.\, b)^n = a^n \,.\, b^n,$$

n being any positive integer.

Solution. First we show that $a^n \,.\, b = b \,.\, a^n \;\; \forall \;\; n \in \mathbf{N}$. ...(1)

Since $a \,.\, b = b \,.\, a$, so (1) is true for $n = 1$.

Let (1) be true for $n = k$. Then $a^k \,.\, b = b \,.\, a^k$. ...(2)

Consider $a^{k+1} \,.\, b = a \,.\, a^k \,.\, b$

$= a \,.\, b \,.\, a^k$, by (2)

$= b \,.\, a \,.\, a^k$ $\quad (\because a \,.\, b = b \,.\, a)$

$= b \,.\, a^{k+1}$.

Thus (1) is true for $n = k + 1$ and so (1) is proved.

Now we show that $(a \,.\, b)^n = a^n \,.\, b^n$. .(3)

Obviously (3) is true for $n = 1$.

Let (3) be true for $n = k$. Then $(a \,.\, b)^k = a^k \,.\, b^k$. ...(4)

Consider $(a \,.\, b)^{k+1} = (a \,.\, b) \,.\, (a \,.\, b)^k$

$= (a \,.\, b) \,.\, (a^k \,.\, b^k)$, by (4)

$= a \,.\, (b \,.\, a^k) \,.\, b^k$, by associative law

$= a \,.\, (a^k \,.\, b) \,.\, b^k$, by (1)

$= a \,.\, a^k \,.\, b \,.\, b^k = a^{k+1} \,.\, b^{k+1}$.

Hence (3) is true for $n = k + 1$ and so

$$(a \,.\, b)^n = a^n \,.\, b^n \;\; \forall \;\; n \in \mathbf{N}.$$

Example 1.8.4. *Show that a group G satisfying $a^2 = e \ \forall \ a \in G$ must be abelian.*

Solution. Let $a, b \in G$ so that $a^2 = a \cdot a = e, b^2 = b \cdot b = e$. ...(1)

Since $a \cdot b \in G$, by the given property $(a \cdot b)^2 = e$.

$\Rightarrow \quad a \cdot b \cdot a \cdot b = e \cdot e$

$\Rightarrow \quad a \cdot b \cdot a \cdot b = a \cdot a \cdot b \cdot b$, using (1)

Applying the cancellation laws, we get

$$b \cdot a = a \cdot b \quad \forall \ a, b \in G.$$

Hence G is abelian.

Example 1.8.5. *Prove that a group G is abelian if and only if*

$$(a \cdot b)^2 = a^2 \cdot b^2 \quad \forall \quad a, b \in G.$$

Solution. Let G be abelian so that

$$a \cdot b = b \cdot a \quad \forall \quad a, b \in G. \qquad ...(1)$$

We shall show that $(a \cdot b)^2 = a^2 \cdot b^2$.

We have $(a \cdot b)^2 = a \cdot b \cdot a \cdot b = a \cdot a \cdot b \cdot b$, by (1)

Hence $(a \cdot b)^2 = a^2 \cdot b^2$.

Conversely, let $(a \cdot b)^2 = a^2 \cdot b^2 \ \forall \ a, b \in G$

$\Rightarrow \quad a \cdot b \cdot a \cdot b = a \cdot a \cdot b \cdot b$

$\Rightarrow \quad b \cdot a \cdot b = a \cdot b \cdot b$, by left cancellation law

$\Rightarrow \quad b \cdot a = a \cdot b$, by right cancellation law.

Hence G must be abelian.

Example 1.8.6. *Show that if every element of the group G is its own inverse, then G is abelian.*

Solution. We have $a = a^{-1} \ \forall \ a \in G$. ...(1)

Let $a, b \in G$ so that $a \cdot b \in G$. From (1), we have

$$a = a^{-1}, b = b^{-1} \text{ and } (a \cdot b)^{-1} = a \cdot b. \qquad ...(2)$$

Now $(a \cdot b)^{-1} = a \cdot b \Rightarrow b^{-1} \cdot a^{-1} = a \cdot b$ (Theorem 1.8.3).

$\Rightarrow \quad b \cdot a = a \cdot b$, using (2).

Hence G is abelian.

Example 1.8.7. *Prove that a group G is abelian if and only if*

$$(a \cdot b)^{-1} = a^{-1} \cdot b^{-1} \text{ for all } a, b \in G.$$

Solution. Let G be abelian. We know $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.

Hence $(a \cdot b)^{-1} = a^{-1} \cdot b^{-1}$, since G is abelian.

Conversely, let $(a \cdot b)^{-1} = a^{-1} \cdot b^{-1}$

$\Rightarrow \quad (a \cdot b)^{-1} = (b \cdot a)^{-1}$, by Theorem 1.8.3.

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

$\Rightarrow \quad a \cdot b = b \cdot a$. Hence G is abelian.

Example 1.8.8. *Show that the equation $x \cdot a \cdot x = b$ is solvable for x in a group G if and only if $a \cdot b$ is the square of some element in G.*

Solution. Suppose $x \cdot a \cdot x = b$ is solvable for $x \in G$. Then

$$a \cdot b = a \cdot x \cdot a \cdot x, \text{ pre-multiply by } a$$

Hence $\quad a \cdot b = (a \cdot x)^2, \quad$ where $\quad a \cdot x \in G$.

Conversely, let $a \cdot b = c^2$ for some $c \in G$. Then $a = c^2 \cdot b^{-1}$.

Taking $\quad x = b \cdot c^{-1}$ and $a = c^2 \cdot b^{-1}$, we see that

$$x \cdot a \cdot x = b \cdot c^{-1} \cdot c^2 \cdot b^{-1} \cdot b \cdot c^{-1}.$$
$$= b \cdot (c^{-1} \cdot c) \cdot c \cdot e \cdot c^{-1}$$
$$= b \cdot e \cdot e = b.$$

Hence $\quad x = b \cdot c^{-1} \in G$ is a solution of $x \cdot a \cdot x = b$.

Example 1.8.9. *Show that the equation $x^2 \cdot a \cdot x = a^{-1}$ is solvable for x in a group G if and only if a is the cube of some element in G.*

Solution. Suppose $x^2 \cdot a \cdot x = a^{-1}$ is solvable in G.

Then there exists some element $c \in G$ such that $c^2 \cdot a \cdot c = a^{-1}$

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

$\Rightarrow c \cdot a \cdot c \cdot a \cdot c \cdot a = e \cdot a = a \quad \Rightarrow a = (c \cdot a)^3$, where $c \cdot a \in G$.

Conversely, let $a = b^3$ for some $b \in G$.

We shall show that $x = b^{-2} \in G$ is a solution of $x^2 \cdot a \cdot x = a^{-1}$.

For $x = b^{-2}$, we have

$$x^2 \cdot a \cdot x = x \cdot x \cdot a \cdot x = b^{-2} \cdot b^{-2} \cdot a \cdot b^{-2}$$
$$= b^{-1} \cdot b^{-3} \cdot a \cdot b^{-2} = b^{-1} \cdot a^{-1} \cdot a \cdot b^{-2} \qquad (\because b^3 = a)$$
$$= b^{-1} \cdot e \cdot b^{-2} = b^{-3} = a^{-1}.$$

Hence $x = b^{-2}$ is a solution of $x^2 \cdot a \cdot x = a^{-1}$.

Example 1.8.10. *If G is a group such that $(a \cdot b)^n = a^n \cdot b^n$ for three consecutive integers n and for all $a, b \in G$, show that G is abelian.*

Solution. Let $\quad (a \cdot b)^n = a^n \cdot b^n, \qquad$ ...(1)

$$(a \cdot b)^{n+1} = a^{n+1} \cdot b^{n+1}, \qquad \text{...(2)}$$

and $\quad (a \cdot b)^{n+2} = a^{n+2} \cdot b^{n+2}. \qquad$ ...(3)

We have $\quad (a \cdot b)^{n+2} = (a \cdot b)^{n+1} \cdot (a \cdot b)$

$\Rightarrow \quad a^{n+2} \cdot b^{n+2} = a^{n+1} \cdot b^{n+1} \cdot a \cdot b$, by (2) and (3)

$\Rightarrow \quad a \cdot a^{n+1} \cdot b^{n+1} \cdot b = a \cdot a^n \cdot b^n \cdot b \cdot a \cdot b$

$\Rightarrow \quad a^{n+1} \cdot b^{n+1} = a^n \cdot b^n \cdot b \cdot a \quad$ (Cancellation laws in G)

$\Rightarrow \quad (a \cdot b)^{n+1} = a^n \cdot b^n \cdot b \cdot a$, by (2)

$\Rightarrow \quad (a \cdot b)^n \cdot (a \cdot b) = (a \cdot b)^n \cdot b \cdot a$, by (1)

$\Rightarrow \quad a \cdot b = b \cdot a$, by left cancellation law.

Hence G is abelian.

Example 1.8.11. *Show that the conclusion of Problem 1.8.10 does not follow if we assume the relation $(a \,.\, b)^i = a^i \,.\, b^i$ for just two consecutive integers.*

Solution. Consider the Quaternion group

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

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

Clearly G is non-abelian. It can be verified that for any $a, b \in G$;

$$(a \,.\, b)^i = a^i \,.\, b^i \text{ for } i = 4, 5$$

but the group G is not abelian. For example,

$$i^4 = (i^2)^2 = (-1)^2 = 1, j^4 = 1 \text{ and so } i^4 \,.\, j^4 = 1.$$

Now $(i \,.\, j)^4 = k^4 = (-1)^2 = 1$. Thus $(i \,.\, j)^4 = i^4 \,.\, j^4$.

Also $i^5 = i^4 \,.\, i = 1 \,.\, i = i$. Similarly, $j^5 = j$.

$\therefore$ $i^5 \,.\, j^5 = i \,.\, j = k$.

Now $(i \,.\, j)^5 = k^5 = k^4 \,.\, k = 1 \,.\, k = k$. Thus $(i \,.\, j)^5 = i^5 \,.\, j^5$.

Example 1.8.12. (*a*) *Show that there are four elements in S_3 satisfying $x^2 = e$ and three elements satisfying $y^3 = e$.*

(*b*) *Give an example of two elements $x, y \in S_3$ such that $(x \,.\, y)^2 \neq x^2 \,.\, y^2$.*

Solution. We know $S_3 = \{i, \sigma_1, \sigma_2, \sigma_3, \tau_1, \tau_2\}$ [See Example 1.7.5]

(*a*) We have $\sigma_1^2 = \sigma_1 \, o \, \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = i.$

Similarly, $\sigma_2^2 = i$, $\sigma_3^2 = i$ and $i^2 = i$.

Now $\tau_1^2 = \tau_1 \, o \, \tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

$\therefore$ $\tau_1^3 = \tau_1^2 \, o \, \tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = i.$

Similarly, $\tau_2^3 = i$ and $i^3 = i$.

(*b*) Let $x = \sigma_1, y = \sigma_2$. Then $x^2 \,.\, y^2 = \sigma_1^2 \, o \, \sigma_2^2 = i \, o \, i = i$,

and $x \,.\, y = \sigma_1 \, o \, \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$,

$$(x \,.\, y)^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Hence $(x \,.\, y)^2 \neq x^2 \,.\, y^2$.

Example 1.8.13. *If G is a group of even order, prove it has an element $a \neq e$ satisfying $a^2 = e$.*

Solution. Let $o(G) = 2n, n \in \mathbf{N}$.

It may be noticed that

$$a^2 = e \Rightarrow a \,.\, a = e \Rightarrow a^{-1} = a.$$

Obviously, $\quad e^{-1} = e.$

If the conclusion of the given problem is not true, then there are $(2n-1)$ non-identity elements of G for which $a^{-1} \neq a$. (Notice that $e^{-1} = e$). Consequently, we should be able to divide the remaining $2n-1$ elements into pairs of elements of the form (a, b) ; where $a, b \in G$ and $a^{-1} = b \neq a$. But this arrangement is impossible, since $2n-1$ is odd. Hence there exists some element $a \neq e$ in G such that $a^{-1} = a$ *i.e.*, $a^2 = e$.

Example 1.8.14. *If G is a finite group, show that there exists a positive integer N such that*

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

Solution. Let $a \in G$ be arbitrary.

Since G is a group, by the closure property

$$a^2 = a \,.\, a \in G,\ a^3 = a^2 \,.\, a \in G \text{ and so on.}$$

Thus $a^2, a^3, a^4, \ldots$ are all elements of G. Since G is finite, there must be repetitions in the above collection of elements *i.e.*,

$$a^i = a^j \text{ for some integers } i \text{ and } j,\ i > j.$$

$$\Rightarrow \quad a^i \,.\, a^{-j} = a^j \,.\, a^{-j}$$

$$\Rightarrow \quad a^{i-j} = a^0 = e \quad \Rightarrow \quad a^N = e, \text{ where } N = i - j > 0.$$

Hence there exists a positive integer N such that

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

Example 1.8.15. *Show that if G is a finite semi-group with cross-cancellation laws i.e.,*

$$x \,.\, y = y \,.\, z \Rightarrow x = z, \qquad \ldots(1)$$

then G is an abelian group.

Solution. Let $x, y, z \in G$ be arbitrary.

By the associative law in G, we have

$$(x \,.\, y) \,.\, x = x \,.\, (y \,.\, x). \qquad \ldots(2)$$

Using (1) in (2), we obtain

$$x \,.\, y = y \,.\, x \ \forall\ x, y \in G. \qquad \ldots(3)$$

Using (3) in (1), we see that

Also $\quad x \,.\, y = z \,.\, y \Rightarrow x = z.$

$$y \,.\, x = y \,.\, z \Rightarrow x = z, \text{ using (3).}$$

Hence G is a finite semi-group in which both the cancellation laws hold and so G is a group. [Theorem 1.8.7]. In view of (3), G is an abelian group.

EXERCISES

1. Show that the set $G = \{a + b\sqrt{2} : a, b \in \mathbf{Q}\}$ is an abelian group w.r.t. usual addition.
2. Show that the set $G = \{1, -1\}$ is an abelian group under multiplication.
3. Show that the set of all positive rational numbers forms an abelian group under the composition $*$ defined by $a * b = ab/2$.

   [**Hint.** Identity element is 2 and $a^{-1} = 4/a$.]
4. Show that $G = \{a + ib : a, b \in \mathbf{Q}$ and $a^2 + b^2 \neq 0\}$ is an abelian group w.r.t. multiplication of complex numbers.
5. Show that the set $S = \{z \in \mathbf{C} : |z| = 1\}$ is a group w.r.t. multiplication of complex numbers.
6. Show that the set $\mathbf{Q}$ of all rational numbers other than 1 is an abelian group w.r.t. the binary composition

$$a * b = a + b - ab \quad \forall \quad a, b \in \mathbf{Q}.$$

   [**Hint.** 0 is the identity and $a^{-1} = a/(a-1)$.]
7. Show that the set $\mathbf{I}$ of all integers is an abelian group under the binary composition $a * b = a + b + 2$.

   [**Hint.** -2 is the identity and $a' = -a - 4$ is the inverse of a.]
8. If two elements a and b in a group commute, show that

   (*i*) a^{-1} and b^{-1} commute, (*ii*) a^{-1} and b commute,

   (*iii*) a and b^{-1} commute.

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

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

   $\Rightarrow b . a^{-1} = a^{-1} . b$.

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

   $\Rightarrow b^{-1} . a = a . b^{-1}$.]
9. Show that a group G is abelian if and only if $a . b . a^{-1} . b^{-1} = e$ for all $a, b \in G$.
10. Show that the set $S = \{1, 3, 7, 9\}$ is a commutative group under $\odot_{10}$, multiplication modulo 10.

    [**Hint.** 1 is the identity and the inverses of 1, 3, 7, 9 are 1, 7, 3, 9 respectively.]
11. Show that $\{S, \odot_{10}\}$ is a commutative group, $S = \{2, 4, 6, 8\}$

    [**Hint.** Identity element is 6 and inverses of 2, 4, 6, 8 are 8, 4, 6, 2 respectively.]
12. Show that $G = \left\{ \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} : a \in \mathbf{R} \right\}$ is a group under matrix multiplication.

    [**Hint.** $\mathbf{I}_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is the identity and $\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & -a \\ 0 & 1 \end{bmatrix}$.]

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. $\{\mathbf{E}, +\} < \{\mathbf{I}, +\}$, where $\mathbf{E}$ is the set of all even integers.
3. Let $H = \{3x : x \in \mathbf{I}\} = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$
   Then $\{H, +\} < \{\mathbf{I}, +\}$.

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

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

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

Note. We shall now onwards drop the composition . while writing $a \,.\, b$. Thus we shall write $a \,.\, b$ as ab, $a \,.\, b^{-1}$ as ab^{-1}, $a \,.\, (b \,.\, c)$ 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 $ab^{-1} \in H \ \forall \ a, b \in H$. ...(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), $a(b^{-1})^{-1} \in H \Rightarrow ab \in H$. $(\because (b^{-1})^{-1} = b)$

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*

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

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

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

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

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_λ is a subgroup of G, so

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

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

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

$$\Rightarrow \quad ak \in H \quad \text{or} \quad ak \in K.$$

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 $a^2 = aa \in H$, $a^3 = a^2 a \in H$, $a^4 = a^3 a \in H$ 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 $\quad x^{-1} = (1, -b) \in H$,

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

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

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 2×2 non-singular matrices over* $\mathbf{R}$.

Solution. Refer to Example 1.7.15. Let S be the multiplicative group of 2×2 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

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

Now $Y^{-1} = \begin{pmatrix} a_2^{-1} & -b_2/a_2 \\ 0 & 1 \end{pmatrix}$, since $YY^{-1} = Y^{-1}Y = I_2$

and $XY^{-1} = \begin{pmatrix} a_1a_2^{-1} & -(a_1b_2/a_2)+b_1 \\ 0 & 1 \end{pmatrix} \in H.$

Hence H is a subgroup of S.

Example 1.9.3. *If G is a group, then $N(a) = \{x \in G : xa = ax\}$ is a subgroup of G. ($N(a)$ is called the* **normalizer** *of a in G).*

Solution. Since $ea = ae$, so $e \in N(a)$ *i.e.*, $N(a) \neq \phi$.

Let $x, y \in N(a)$ so that $xa = ax$ and $ya = ay$.

Now $ya = ay \Rightarrow (ya)^{-1} = (ay)^{-1} \Rightarrow a^{-1}y^{-1} = y^{-1}a^{-1}$

$\Rightarrow a(a^{-1}y^{-1}) = a(y^{-1}a^{-1}) \quad \Rightarrow (aa^{-1})y^{-1} = (ay^{-1})a^{-1}$, by associative law

$\Rightarrow \quad ey^{-1} = (ay^{-1})a^{-1} \Rightarrow y^{-1} = (ay^{-1})a^{-1} \Rightarrow y^{-1}a = ay^{-1}$.

$\Rightarrow \quad x(y^{-1}a) = x(ay^{-1}) \Rightarrow (xy^{-1})a = (xa)y^{-1} = (ax)y^{-1} \quad (\because xa = ax)$

$\therefore \quad (xy^{-1})a = a(xy^{-1})$, by associative law

$\Rightarrow \quad xy^{-1} \in N(a)$ and so $N(a)$ is a subgroup of G.

Example 1.9.4. *If G is a group, then $Z = \{z \in G : xz = zx \ \forall \ x \in G\}$ is a subgroup of G. (Z is called the* **centre** *of G).*

Solution. Since $ex = xe \quad \forall \ x \in G$, so $e \in Z$ *i.e.*, $Z \neq \phi$.

Let $a, b \in Z$ so that $ax = xa$ and $bx = xb \ \forall \ x \in G$.

$bx = xb \Rightarrow b^{-1}(bx) = b^{-1}(xb) \Rightarrow x = (b^{-1}x)b \Rightarrow b^{-1}x = xb^{-1}$.

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

$\Rightarrow (ab^{-1})x = (xa)b^{-1}$, as $ax = xa \ \forall \ x \in G$

$\Rightarrow (ab^{-1})x = x(ab^{-1}) \quad \forall \quad x \in G$

$\Rightarrow ab^{-1} \in Z$.

Hence Z is a subgroup of G.

Example 1.9.5. *Show that $aHa^{-1} = \{aha^{-1} : h \in H\}$ is a subgroup of G, where H is a subgroup of G and $a \in G$.*

Solution. Let $x, y \in aHa^{-1}$ so that

$$x = ah_1a^{-1}, y = ah_2a^{-1} \quad \text{for some} \quad h_1, h_2 \in H.$$

We have $\quad y^{-1} = (ah_2a^{-1})^{-1} = (a^{-1})^{-1}(ah_2)^{-1} \quad [\because (xy)^{-1} = y^{-1}x^{-1}]$

or $\quad y^{-1} = ah_2^{-1}a^{-1}$ and so $xy^{-1} = (ah_1a^{-1})(ah_2^{-1}a^{-1})$

or $\quad xy^{-1} = ah_1h_2^{-1}a^{-1}$.

$[\because a^{-1}a = e]$

Since $H \leq G$, $h_1h_2^{-1} \in H$ and so $xy^{-1} = ah_1h_2^{-1}a^{-1} \in aHa^{-1}$.

Hence aHa^{-1} is a subgroup of G.

Example 1.9.6. *Show that $HH = H$, where H is a subgroup of G and*

$$HH = \{h_1h_2 : h_1, h_2 \in H\}$$

Solution. Let $h \in H$. Then $h = he \to h \in HH$ $\quad (\because e \in H)$

$\to \quad h \in HH \ \forall\ h \in H \quad \to H \subseteq HH$.

Conversely, let $x \in HH$ so that $x = h_1h_2$, where $h_1, h_2 \in H$.

Since H is a subgroup of G, $h_1h_2 \in H$ i.e., $x \in H$. So $HH \subseteq H$.

Hence $H \subseteq HH$ and $HH \subseteq H \to HH = H$.

Example 1.9.7. *Show that a non-empty subset H of a group G is a subgroup of G iff $HH^{-1} \subset H$.*

Solution. We have $\quad HH^{-1} = \{ab^{-1} : a, b \in H\}$.

We know $\quad H < G \leftrightarrow ab^{-1} \in H \ \forall\ a \in H,\ b \in H$. (Theorem 1.9.1)

Hence $\quad H < G \leftrightarrow HH^{-1} \subset H$.

Example 1.9.8. *Show that a non-empty finite subset H of a group G is a subgroup of G iff $HH = H$.*

Solution. *Condition is necessary*

Let $H < G$. By Example 1.9.6, $HH = H$.

Condition is sufficient

Let H be a finite subset of G such that $HH = H$.

Then $\quad ab \in H \quad \forall \quad a \in H, b \in H$.

By Theorem 1.9.6, it follows that H is a subgroup of G.

EXERCISES

1. Show that $H = \{nx : x \in \mathbf{I}\}$ is a subgroup of $\{\mathbf{I}, +\}$, $n \in I$.
2. If a be a fixed element of a group G and if

$$H = \{x \in G : xa^2 = a^2x\},\ K = \{x \in G : xa = ax\},$$

then show that $H < G$ and $K < H$. ...(1)

[**Hint.** Let $\quad x, y \in H$ so that $xa^2 = a^2x$ and $ya^2 = a^2y$.

Then $(xy)\,a^2 = x\,(ya^2) = x\,(a^2y) = (xa^2)\,y = (a^2x)\,y = a^2\,(xy)$, by (1)

$\Rightarrow \quad (xy)\,a^2 = a^2\,(xy) \Rightarrow xy \in H \quad \forall\ x, y \in H$.

Let $\quad x \in H \quad$ so that $\quad xa^2 = a^2x$. Then

$(xa^2)^{-1} = (a^2x)^{-1} \Rightarrow a^{-2}x^{-1} = x^{-1}a^{-2} \Rightarrow x^{-1}a^2 = a^2x^{-1}$

$\Rightarrow \quad x^{-1} \in H \quad \forall\ x \in H$.

Hence $H < G$. Verify that $K \subset H$ to show that $K < H$.]

Since $H < G$, $h_1h_2^{-1} \in H$ and so $xy^{-1} = ah_1h_2^{-1}a^{-1} \in aHa^{-1}$.

Hence aHa^{-1} is a subgroup of G.

Example 1.9.6. *Show that $HH = H$, where H is a subgroup of G and*

$$HH = \{h_1h_2 : h_1, h_2 \in H\}.$$

Solution. Let $h \in H$. Then $h = he \Rightarrow h \in HH$. $(\because e \in H)$

$\Rightarrow \quad h \in HH \ \forall \ h \in H \quad \Rightarrow H \subseteq HH.$

Conversely, let $x \in HH$ so that $x = h_1h_2$, where $h_1, h_2 \in H$.

Since H is a subgroup of G, $h_1h_2 \in H$ i.e., $x \in H$. So $HH \subseteq H$.

Hence $H \subseteq HH$ and $HH \subseteq H \Rightarrow HH = H$.

Example 1.9.7. *Show that a non-empty subset H of a group G is a subgroup of G iff $HH^{-1} \subset H$.*

Solution. We have $HH^{-1} = \{ab^{-1} ; a, b \in H\}$.

We know $H < G \Leftrightarrow ab^{-1} \in H \ \forall \ a \in H, b \in H$. (Theorem 1.9.1.)

Hence $\quad H < G \Leftrightarrow HH^{-1} \subset H$.

Example 1.9.8. *Show that a non-empty finite subset H of a group G is a subgroup of G iff $HH = H$.*

Solution. *Condition is necessary*

Let $H < G$. By Example 1.9.6, $HH = H$.

Condition is sufficient

Let H be a finite subset of G such that $HH = H$.

Then $ab \in H \quad \forall \quad a \in H, b \in H$.

By Theorem 1.9.6, it follows that H is a subgroup of G.

EXERCISES

1. Show that $H = \{nx : x \in \mathbf{I}\}$ is a subgroup of $\{\mathbf{I}, +\}$, $n \in I$.
2. If a be a fixed element of a group G and if

$$H = \{x \in G : xa^2 = a^2x\}, \ K = \{x \in G : xa = ax\},$$

then show that $H < G$ and $K < H$.

[**Hint.** Let $x, y \in H$ so that $xa^2 = a^2x$ and $ya^2 = a^2y$. ...(1)

Then $(xy)\, a^2 = x\,(ya^2) = x\,(a^2y) = (xa^2)\, y = (a^2x)\, y = a^2\,(xy)$, by (1)

$\Rightarrow \quad (xy)\, a^2 = a^2\,(xy) \Rightarrow xy \in H \quad \forall \ x, y \in H.$

Let $x \in H$ so that $xa^2 = a^2x$. Then

$(xa^2)^{-1} = (a^2x)^{-1} \Rightarrow a^{-2}x^{-1} = x^{-1}a^{-2} \Rightarrow x^{-1}a^2 = a^2x^{-1}$

$\Rightarrow \quad x^{-1} \in H \quad \forall \ x \in H.$

Hence $H < G$. Verify that $K \subset H$ to show that $K < H$.]

Since $H < G$, $h_1 h_2^{-1} \in H$ and so $xy^{-1} = ah_1 h_2^{-1} a^{-1} \in aHa^{-1}$.
Hence aHa^{-1} is a subgroup of G.

Example 1.9.6. *Show that $HH = H$, where H is a subgroup of G and $HH = \{h_1 h_2 : h_1, h_2 \in H\}$.*

Solution. Let $h \in H$. Then $h = he \Rightarrow h \in HH$.

$\Rightarrow \quad h \in HH \ \forall \ h \in H \quad \Rightarrow H \subseteq HH.$ $\quad (\because e \in H)$

Conversely, let $x \in HH$ so that $x = h_1 h_2$, where $h_1, h_2 \in H$.
Since H is a subgroup of G, $h_1 h_2 \in H$ *i.e.*, $x \in H$. So $HH \subseteq H$.
Hence $H \subseteq HH$ and $HH \subseteq H \Rightarrow HH = H$.

Example 1.9.7. *Show that a non-empty subset H of a group G is a subgroup of G iff $HH^{-1} \subset H$.*

Solution. We have $HH^{-1} = \{ab^{-1} ; a, b \in H\}$.
We know $H < G \Leftrightarrow ab^{-1} \in H \ \forall \ a \in H, b \in H$. (Theorem 1.9.1.)
Hence $\quad H < G \Leftrightarrow HH^{-1} \subset H$.

Example 1.9.8. *Show that a non-empty finite subset H of a group G is a subgroup of G iff $HH = H$.*

Solution. *Condition is necessary*
Let $H < G$. By Example 1.9.6, $HH = H$.
Condition is sufficient
Let H be a finite subset of G such that $HH = H$.
Then $ab \in H \quad \forall \quad a \in H, b \in H$.
By Theorem 1.9.6, it follows that H is a subgroup of G.

EXERCISES

1. Show that $H = \{nx : x \in \mathbf{I}\}$ is a subgroup of $\{\mathbf{I}, +\}$, $n \in \mathbf{I}$.
2. If a be a fixed element of a group G and if

$$H = \{x \in G : xa^2 = a^2 x\}, \ K = \{x \in G : xa = ax\},$$

then show that $H < G$ and $K < H$.

[**Hint.** Let $x, y \in H$ so that $xa^2 = a^2 x$ and $ya^2 = a^2 y$. ...(1)
Then $(xy)\, a^2 = x\,(ya^2) = x\,(a^2 y) = (xa^2)\, y = (a^2 x)\, y = a^2\,(xy)$, by (1)
$\Rightarrow \quad (xy)\, a^2 = a^2\,(xy) \Rightarrow xy \in H \quad \forall \ x, y \in H.$
Let $x \in H$ so that $xa^2 = a^2 x$. Then

$$(xa^2)^{-1} = (a^2 x)^{-1} \Rightarrow a^{-2} x^{-1} = x^{-1} a^{-2} \Rightarrow x^{-1} a^2 = a^2 x^{-1}$$

$\Rightarrow \quad x^{-1} \in H \quad \forall \ x \in H.$

Hence $H < G$. Verify that $K \subset H$ to show that $K < H$.]

3. Show that $a^{-1}Ha = \{a^{-1}ha : h \in H\}$ is a subgroup of G, where H is a subgroup of G and $a \in G$.
[**Hint.** Proceed like Example 1.9.5.]

4. Show that $H^{-1} = H$, where H is a subgroup of G.
[**Hint.** $x \in H^{-1} \Rightarrow x = h^{-1}$ for some $h \in H \Rightarrow x \in H$ $(\because H < G)$.
So $H^{-1} \subseteq H$. Conversely, $y \in H \Rightarrow y^{-1} \in H$ $(\because H < G)$.
Now $y = (y^{-1})^{-1}$ means $y \in H^{-1}$ and so $H \subseteq H^{-1}$. Thus $H = H^{-1}$.]

5. Prove that every subgroup of an abelian group is abelian.
[**Hint.** Let $H < G$, G being abelian. Then $a, b \in H \Rightarrow a, b \in G$ and so $ab = ba$.]

6. Give an example of a non-abelian group having an abelian subgroup.
[**Hint.** Refer to Example 1.9.1. G is a non-abelian group but H is an abelian subgroup of G.]

7. Prove that if K is a subgroup of H and if H is a subgroup of G, then K is a subgroup of G.
[**Hint.** Use Theorem 1.9.1.]

8. Show that $H = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} : a \in \mathbf{R} \right\}$ is a subgroup of the multiplicative group of 2×2 non-singular matrices over $\mathbf{R}$.
[**Hint.** $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a-b \\ 0 & 1 \end{pmatrix} \in H$.]

9. Show that a non-empty subset H of a group G is a subgroup of G iff $a^{-1}b \in H \ \forall\, a, b \in H$.
[**Hint.** Proceed like Theorem 1.9.1.]

10. Show that a non-empty subset H of a group G is a subgroup of G iff $H^{-1}H \subset H$, where $H^{-1}H = \{a^{-1}b : a, b \in H\}$.
[**Hint.** Use Ex. 9 above and proceed like Example 1.9.7.]

1.10 Order of an Element

Definition. *Let G be a group, and $a \in G$. If there exists a least positive integer n such that $a^n = e$, then n is called the* **order** *of a, written as $o(a) = n$. If no such positive integer exists, then a is said to be of* **infinite order**.

Illustrations.

1. In the group $G = \{1, w, w^2\}$, w being cube root of unity ;
$$o(w) = 3,\ o(w^2) = 3 \text{ and } o(1) = 1.$$

2. The order of any non-zero element in the group $(\mathbf{Z}, +)$ is infinite.

Theorem 1.10.1. *If a and b are two elements of a group G, then*

(*i*) $o(a) = o(xax^{-1}) = o(x^{-1}ax)\ \forall\ x \in G$.

(*ii*) $o(ab) = o(ba)$. [D.U., 1997]

(*iii*) $o(a) = o(a^{-1})$. [D.U., 1997]

(*iv*) *If* $a^m = e$, *then* $o(a)$ *divides* m.

Proof. (*i*) Let n be any positive integer. Then

$$a^n = e \Leftrightarrow x\,a^n\,x^{-1} = x\,e\,x^{-1} = e$$

$$\Leftrightarrow (x\,a\,x^{-1})^n = x\,a^n\,x^{-1} = e.$$

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

Again $a^n = e \Leftrightarrow (x^{-1}\,a\,x)^n = x^{-1}\,a^n\,x = x^{-1}\,e\,x = x^{-1}\,x = e$.

Hence $o(a) = o(x^{-1}\,a\,x)$, therefore

(*ii*) Since $ab = a\,(ba)\,a^{-1}$,

$$\therefore \quad o(ab) = o\{a\,(ba)\,a^{-1}\} = o(ba), \text{ using part } (i)$$

(*iii*) $a^n = e \Leftrightarrow a\,a \ldots a\ (n \text{ times}) = e \Leftrightarrow e = ea^{-1}\,a^{-1} \ldots a^{-1}\ (n \text{ times})$

$$\Leftrightarrow a^{-n} = e.$$

Hence $o(a) = o(a^{-1})$.

(*iv*) Let $o(a) = n$. By definition, n is the least positive integer satisfying

$$a^n = e. \qquad \ldots(1)$$

On dividing m by n, there exist two integers q and r such that

$$m = nq + r,\ 0 \le r < n.$$

Now $a^m = e \Rightarrow e = a^{nq+r} = a^{nq}\,a^r = (a^n)^q\,.\,a^r = e\,a^r$, by (1)

$\therefore \quad a^r = e.$

If $0 < r < n$, then $a^r = e$ contradicts (1).

Thus $r = 0$ and so $m = nq \Rightarrow n \mid m \Rightarrow o(a) \mid m$.

EXAMPLES

Example 1.10.1. *Find the order of each of the elements of the group*

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

Solution. We have

$$(1)^1 = 1 \Rightarrow o(1) = 1,$$

$$(-1)^2 = 1 \text{ and } (-1) \ne 1 \Rightarrow o(-1) = 2,$$

$$(i)^1 = i,\ i^2 = -1,\ i^3 = (-1)\,i = -i,\ i^4 = -i\,.\,i = 1 \Rightarrow o(i) = 4.$$

Similarly, $o(-i) = 4$.

Example 1.10.2. *If in a group G,* $a^5 = e$, $aba^{-1} = b^2$ *for* $a, b \in G$, *then show that* $o(b) = 31$.

Solution. $b^2 = aba^{-1} \Rightarrow b^4 = (aba^{-1})\,(aba^{-1}) = ab\,(a^{-1}a)\,ba^{-1}$

$$= ab^2\,a^{-1} = (aa\,ba^{-1})\,a^{-1} \quad (\because b^2 = ab\,a^{-1})$$

$$\therefore \quad b^4 = a^2\,b\,a^{-2}$$

$$\Rightarrow \quad b^8 = (a^2 b a^{-2})(a^2 b a^{-2}) = a^2 b (a^{-2} a^2) b a^{-2}$$

$$= a^2 b^2 a^{-2} = (a^2 a b a^{-1}) a^{-2} \qquad (\because b^2 = a b a^{-1})$$

$$\therefore \quad b^8 = a^3 b a^{-3}.$$

Similarly, $b^{16} = a^4 b a^{-4}$ and $b^{32} = a^5 b a^{-5}$.

$$\therefore \quad b^{32} = e b e^{-1} \ (\because a^5 = e) \Rightarrow b^{32} = b \Rightarrow b^{31} b = eb \Rightarrow b^{31} = e.$$

Since 31 is a prime number, so 31 is the least positive integer such that $b^{31} = e$. Hence $o(b) = 31$.

Example 1.10.3. *If a, b are two elements of a group G such that $ab = ba$ and $(o(a), o(b)) = 1$, then* [D.U., 1993]

$$o(ab) = o(a)\, o(b).$$

Solution. Let $o(a) = m$, $o(b) = n$. Then m and n are least positive integers such that ...(1)

$$a^m = e \text{ and } b^n = e.$$

We shall show that $o(ab) = mn$, if

$$ab = ba \text{ and } (m, n) = 1.$$

We know $\quad ab = ba \Rightarrow (ab)^{mn} = a^{mn}\, b^{mn}$ [See Example 1.8.3.]

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

$$= e^n . e^m = e, \text{ using (1)}$$

$$\therefore \quad (ab)^{mn} = e. \qquad ...(2)$$

Next we show that mn is the least positive integer satisfying (2). Suppose r is *any* positive integer such that

$$(ab)^r = e.$$

Then $\quad a^r b^r = e$, as $ab = ba$ [See Example 1.8.3.]

$$\Rightarrow \quad a^r = b^{-r} \Rightarrow (a^r)^n = (b^{-r})^n$$

$$\Rightarrow \quad a^{rn} = (b^n)^{-r} = e. \qquad (\because b^n = e)$$

Now $a^m = e \Rightarrow o(a)$ divides rn [Theorem 1.10.1 (*iv*)] $\Rightarrow m \mid rn$.

Since $(m, n) = 1$ *i.e.*, m and n are relative prime integers, so $m \mid rn \Rightarrow m \mid r$. Similarly, $n \mid r$.

Since $(m, n) = 1$, so $m \mid r$ and $n \mid r \Rightarrow mn \mid r$, where r is any positive integer such that $(ab)^r = e$.

Hence by (2), $o(ab) = mn = o(a)\, o(b)$.

Remark. *The conclusion of the above problem may not follow, if*

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

Consider the Quaternion group :

$$G = \{\pm 1, \pm i, \pm j, \pm k\}, i^2 = j^2 = k^2 = -1,$$

$$ij = -ji = k, jk = -kj = i, ki = -ik = j.$$

We have $\quad ij \neq ji$. Also $(i)^1 = i, i^2 = -1, i^3 = -i, i^4 = 1$.

$\therefore \quad o(i) = 4$. Similarly, $o(j) = 4$, $o(k) = 4$ and $o(ij) = o(k) = 4$.

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

Hence $\quad o(ij) \neq o(i)\, o(j)$, 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 $m \quad \Rightarrow \dfrac{n}{d}, \dfrac{m}{d}$ are relatively prime integers.

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

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

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

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

$\Rightarrow m$ divides nr

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

$(a^n)^r = e$

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

This shows that $\dfrac{m}{d}$ 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*

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

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

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

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

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

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

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

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

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

since $x \in H$ and $a^m \in H$.

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

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

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 $q = \dfrac{m}{n}$ (m and n are integers, $n \neq 0$).
   Then for each $x \in \mathbf{Q}$, $x = kq$ for some integer k.
   In particular, for $x = \dfrac{1}{3n} \in \mathbf{Q}$, 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

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

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

since $x \in H$ and $a^m \in H$.

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

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

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 $q = \dfrac{m}{n}$ (m and n are integers, $n \neq 0$).
   Then for each $x \in \mathbf{Q}$, $x = kq$ for some integer k.
   In particular, for $x = \dfrac{1}{3n} \in \mathbf{Q}$, 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

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

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

since $x \in H$ and $a^m \in H$.

As stated earlier,

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

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

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.

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

Since G is infinite, therefore

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

[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.

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

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

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

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

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

Definition (Euler ϕ-function)

If n is any positive integer, then **Euler ϕ-function**, *denoted by $\varphi(n)$, 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 ϕ-function.*

Or

If $G = \langle a \rangle$ be a finite cyclic group of order n, then a^m is a generator of G iff $0 < m < n$ and $(m, n) = 1$. [D.U., 1997]

Proof. Let $G = \langle a \rangle$ be a finite cyclic group of order n.

Then $G = \{a, a^2, ..., a^{n-1}, a^n = e\}$.

We show that a^m is a generator of G iff $0 < m < n$ and $(m, n) = 1$ *i.e.*, m and n are relatively prime. Suppose

$$G = \langle a^m \rangle, 0 < m < n.$$

Since $a \in G$, $a = (a^m)^i$ for some integer i

$\Rightarrow a = a^{mi} \Rightarrow a^{mi-1} = e \Rightarrow o(a) \mid (mi - 1)$

$\Rightarrow n \mid (mi - 1) \Rightarrow mi - 1 = nj$ for some integer j

$\Rightarrow mi + (-n) j = 1$

$\Rightarrow m$ and n are relatively prime.

Conversely, let m and n be relatively prime integers $(0 < m < n)$. Then there exist integers r and s such that $mr + ns = 1$.

$$\therefore \quad a = a^1 = a^{mr+ns} = a^{mr} . a^{ns} = (a^m)^r (a^n)^s = (a^m)^r. \qquad (\because a^n = e)$$

Hence $G = \langle a^m \rangle$, since for any $x \in G = \langle a \rangle$, we have

$$x = a^l \, (1 \le l \le n) \Rightarrow x = (a^m)^{rl}.$$

It follows that a^m is a generator of $G = \langle a \rangle$; $a^n = e$ iff $0 < m < n$ and $(m, n) = 1$. Consequently, a cyclic group of order n has $\phi(n)$ number of generators.

Theorem 1.11.4. *If G is a finite cyclic group and m a positive integer such that m divides o (G), then there exists a unique subgroup of G of order m.* [D.U., 1992]

Proof. Let $G = \langle a \rangle$ be a finite cyclic group of order n so that $a^n = e$. ...(1)

Since m divides $o(G) = n$, there exists a positive integer q such that

$$n = mq. \qquad ...(2)$$

Let $H = \{a^q, a^{2q}, a^{3q}, ..., a^{mq}\} = \langle a^q \rangle$, where

$$a^{mq} = a^n = e, \text{ by (1) and (2).}$$

Thus $H = \langle a^q \rangle$ is a subgroup of G of order m. Now we show that H is unique (as a subgroup of G of order m). Let K be any other subgroup of G such that $o(K) = m$. Since a subgroup of a cyclic group is cyclic, therefore K is cyclic. Let $K = \langle b \rangle$ for some $b \in K$, $b^m = e$. Since $b \in G = \langle a \rangle$, $b = a^k$ for some integer k. On dividing k by q, there exist integers t and r such that

$$k = qt + r, \; 0 \le r < q$$

$$\Rightarrow a^{mk} = a^{mqt+mr} = (a^{mq})^t . a^{mr} = (a^n)^t . a^{mr} = a^{mr}, \qquad \text{using (1) and (2)}$$

$$\therefore \; a^{mr} = a^{mk} = (a^k)^m = b^m = e, \quad \text{where} \quad 0 \le mr < mq = n.$$

In view of (1), we must have $mr = 0 \Rightarrow r = 0$, as $m \ne 0$.

Or

If $G = \langle a \rangle$ be a finite cyclic group of order n, then a^m is a generator of G iff $0 < m < n$ and $(m, n) = 1$. [D.U., 1997]

Proof. Let $G = \langle a \rangle$ be a finite cyclic group of order n.

Then $G = \{a, a^2, ..., a^{n-1}, a^n = e\}$.

We show that a^m is a generator of G iff $0 < m < n$ and $(m, n) = 1$ *i.e.*, m and n are relatively prime. Suppose

$$G = \langle a^m \rangle, 0 < m < n.$$

Since $a \in G$, $a = (a^m)^i$ for some integer i

$\Rightarrow a = a^{mi} \Rightarrow a^{mi-1} = e \Rightarrow o(a) \mid (mi - 1)$

$\Rightarrow n \mid (mi - 1) \Rightarrow mi - 1 = nj$ for some integer j

$\Rightarrow mi + (-n) j = 1$

$\Rightarrow m$ and n are relatively prime.

Conversely, let m and n be relatively prime integers $(0 < m < n)$. Then there exist integers r and s such that $mr + ns = 1$.

$$\therefore \quad a = a^1 = a^{mr+ns} = a^{mr} . a^{ns} = (a^m)^r (a^n)^s = (a^m)^r. \qquad (\because a^n = e)$$

Hence $G = \langle a^m \rangle$, since for any $x \in G = \langle a \rangle$, we have

$$x = a^l \, (1 \le l \le n) \Rightarrow x = (a^m)^{rl}.$$

It follows that a^m is a generator of $G = \langle a \rangle$; $a^n = e$ iff $0 < m < n$ and $(m, n) = 1$. Consequently, a cyclic group of order n has $\phi(n)$ number of generators.

Theorem 1.11.4. *If G is a finite cyclic group and m a positive integer such that m divides o (G), then there exists a unique subgroup of G of order m.* [D.U., 1992]

Proof. Let $G = \langle a \rangle$ be a finite cyclic group of order n so that $a^n = e$. ...(1)

Since m divides $o(G) = n$, there exists a positive integer q such that

$$n = mq. \qquad ...(2)$$

Let $H = \{a^q, a^{2q}, a^{3q}, ..., a^{mq}\} = \langle a^q \rangle$, where

$$a^{mq} = a^n = e, \text{ by (1) and (2).}$$

Thus $H = \langle a^q \rangle$ is a subgroup of G of order m. Now we show that H is unique (as a subgroup of G of order m). Let K be any other subgroup of G such that $o(K) = m$. Since a subgroup of a cyclic group is cyclic, therefore K is cyclic. Let $K = \langle b \rangle$ for some $b \in K$, $b^m = e$. Since $b \in G = \langle a \rangle$, $b = a^k$ for some integer k. On dividing k by q, there exist integers t and r such that

$$k = qt + r, \; 0 \le r < q$$

$$\Rightarrow a^{mk} = a^{mqt+mr} = (a^{mq})^t . a^{mr} = (a^n)^t . a^{mr} = a^{mr}, \qquad \text{using (1) and (2)}$$

$$\therefore \; a^{mr} = a^{mk} = (a^k)^m = b^m = e, \quad \text{where} \quad 0 \le mr < mq = n.$$

In view of (1), we must have $mr = 0 \Rightarrow r = 0$, as $m \ne 0$.

$\therefore \quad k = qt$ and so $b = a^k = a^{qt} = (a^q)^t$.

Now $\quad b = (a^q)^t \Rightarrow b \in H = \langle a^q \rangle \Rightarrow \langle b \rangle \subseteq H \Rightarrow K \subseteq H$.

Since $K \subseteq H$ and $o(H) = o(K)$, $K = H$.

Hence H is a unique subgroup of G of order m.

EXAMPLES

Example 1.11.1. *If a is a generator of a cyclic group G, then a^{-1} is also a generator of G.*

Solution. Let $G = \langle a \rangle$. Then each element $x \in G$ can be expressed as $x = a^n$, for some integer n. We have

$$x = a^n = (a^{-1})^m, \; m = -n \text{ is an integer.}$$

The above expression holds for each $x \in G$.

Hence $\quad G = \langle a^{-1} \rangle$.

Example 1.11.2. *Show that a cyclic group is necessarily abelian. Show by an example that the converse may not be true.*

Solution. Let $G = \langle a \rangle$ be a cyclic group.

Let x and y be any two elements of G. Then

$$x = a^m, \quad y = a^n \text{ for some integers } m \text{ and } n.$$

$$\therefore \quad xy = a^m a^n = a^{m+n} = a^{n+m} = a^n a^m = yx.$$

Hence G is abelian.

However, an abelian group may not be cyclic. For example : $(\mathbf{Q}, +)$ is abelian, but not cyclic. [See Illustration 5 of Sec. 1.11].

Remark. *Non-abelian groups cannot be cyclic.*

Example 1.11.3. *Give an example of a finite abelian group, which is not cyclic.*

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

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

It is easy to verify that G is an abelian group w.r.t. multiplication of matrices. Further

$$o(I) = 1, \; o(A) = o(B) = o(C) = 2.$$

Thus G is a finite abelian group of order 4 in which no element is of order 4. Hence G is not cyclic.

Example 1.11.4. *Show that the Klein's 4-group is not cyclic.*

Solution. The Klein's 4-group is defined as follows :

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

It is clear that G is abelian. Further

$$(ab)^2 = (ab)(ab) = a(ba)b = a(ab)b = a^2 b^2 = e.$$

Thus $o(a) = o(b) = o(ab) = 2$ and $o(e) = 1$.

Since no element of G is of order 4, G is not cyclic.

Example 1.11.5. *Find the generators of a cyclic group of order 8.*

Solution. We have $G = \langle a \rangle, a^8 = e$.

All the generators of G are a, a^3, a^5, a^7

i.e., $G = \langle a \rangle = \langle a^3 \rangle = \langle a^5 \rangle = \langle a^7 \rangle$. [Theorem 1.11.3]

Notice that 1, 3, 5, 7 are positive integers less than 8 and prime to 8.

Example 1.11.6. *Find the generators of* $G = \langle a \rangle, a^{12} = e$.

Hint. All the generators of G are a, a^5, a^7, a^{11}.

Notation. *Let U_n denote the group of integers relatively prime to n under multiplication mod n.*

Example 1.11.7. *Show that U_9 is a cyclic group. What are all its generators ?*

Solution. We have $U_9 = \{1, 2, 4, 5, 7, 8\}$.

It is easy to verify that $U_9 = \langle 2 \rangle$, since

$$2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 = 7, 2^5 = 5, 2^6 = 1.$$

Thus U_9 is a cyclic group. We have $o(U_9) = 6$.

The positive integers less than 6 and prime to 6 are 1, 5. Hence all the generators of U_9 are 2 and 5, since $2^1 = 2$ and $2^5 = 5$.

Example 1.11.8. *Show that U_{17} is a cyclic group. What are all its generators ?*

Solution. $U_{17} = \{1, 2, \ldots, 16\}$ and $o(U_{17}) = 16$.

All the positive integers less than 16 and prime to 16 are 1, 3, 5, 7, 9, 11, 13, 15. It can be verified that $U_{17} = \langle 3 \rangle$ *i.e.*, every element of U_{17} is a power of 3. All the generators of U_{17} are

$$3^1 = 3, 3^3 = 10, 3^5 = 5, 3^7 = 11, 3^9 = 14, 3^{11} = 7, 3^{13} = 12, 3^{15} = 6.$$

Hence all the generators of U_{17} are

$$3, 5, 6, 7, 10, 11, 12, 14.$$

Example 1.11.9. *Show that U_8 is not a cyclic group.*

Solution. We have $U_8 = \{1, 3, 5, 7\}$.

We notice that $3^2 = 1, 3^3 = 3, 3^4 = 1, 3^5 = 3$ etc.

Thus 3 cannot be a generator of U_8.

Now $5^2 = 1, 5^3 = 5, 5^4 = 1, 5^5 = 5$ etc.

Thus 5 cannot be a generator of U_8.

Again $7^2 = 1, 7^3 = 7, 7^4 = 1, 7^5 = 7$ etc.

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

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

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

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

1.12 Cosets and Lagrange's Theorem

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

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

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

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

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

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

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

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

Hence all the distinct right cosets of K in G are

$$K, Ka, Ka^2, Ka^3, Ka^4.$$

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,

$$H = \{I, (12)\} \text{ is a subgroup of the group}$$
$$S_3 = \{I, (12), (23), (13), (123), (132)\}.$$

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

$$H = \{\ldots, -15, -10, -5, 0, 5, 10, 15, \ldots\},$$
$$1 + H = \{\ldots, -14, -9, -4, 1, 6, 11, 16, \ldots\},$$
$$2 + H = \{\ldots, -13, -8, -3, 2, 7, 12, 17, \ldots\},$$
$$3 + H = \{\ldots, -12, -7, -2, 3, 8, 13, 18, \ldots\},$$
$$4 + H = \{\ldots, -11, -6, -1, 4, 9, 14, 19, \ldots\},$$

It is easy to verify that

$$5 + H = H,\ 6 + H = 1 + H,\ 7 + H = 2 + H \text{ etc.}$$
$$-1 + H = 4 + H,\ -2 + H = 3 + H \text{ etc.}$$

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 $Ha = H$.

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,

$$H = \{I, (12)\} \text{ is a subgroup of the group}$$
$$S_3 = \{I, (12), (23), (13), (123), (132)\}.$$

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

$$H = \{\ldots, -15, -10, -5, 0, 5, 10, 15, \ldots\},$$
$$1 + H = \{\ldots, -14, -9, -4, 1, 6, 11, 16, \ldots\},$$
$$2 + H = \{\ldots, -13, -8, -3, 2, 7, 12, 17, \ldots\},$$
$$3 + H = \{\ldots, -12, -7, -2, 3, 8, 13, 18, \ldots\},$$
$$4 + H = \{\ldots, -11, -6, -1, 4, 9, 14, 19, \ldots\},$$

It is easy to verify that

$$5 + H = H,\ 6 + H = 1 + H,\ 7 + H = 2 + H \text{ etc.}$$
$$-1 + H = 4 + H,\ -2 + H = 3 + H \text{ etc.}$$

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

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

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

$\therefore \quad H \subseteq Ha$.

Hence $\quad Ha = H$.

(*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) ...(2)

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

Now $x \in Hb \Rightarrow x = h_3 b = h_3 (h_1^{-1} a) = (h_3 h_1^{-1}) a$, by (1). ...(3)

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

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

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

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

$\Rightarrow \qquad x = a^{-1} h^{-1} \Rightarrow x \in a^{-1} H$, 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 $h_1 \in H$.

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

Thus $\quad x \in (Ha)^{-1} \quad$ 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,

$$c = h_1 a \text{ and } c = h_2 b, \quad \text{for some } h_1, h_2 \in H.$$

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

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

Using (1), we have

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

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

Conversely, let y be any element of Hb so that $y = h'b$, for some $h' \in H$. Using (1), we have

$$y = h'(h_2^{-1} h_1 a) = (h' h_2^{-1} h_1) a \in Ha, h' h_2^{-1} h_1 \in H. \qquad (\because H < G)$$

$$\therefore \quad Hb \subseteq Ha \qquad ...(3)$$

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 ϕ is one-to-one.

Suppose $\phi(h_1 a) = \phi(h_2 a)$. Then $h_1 b = h_2 b$, by (1)

$\Rightarrow \; h_1 = h_2$, by right cancellation law

$\Rightarrow h_1 a = h_2 a$, by right cancellation law.

Thus ϕ is one-to-one. Now we show that ϕ 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 ϕ is onto. Hence ϕ 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 $b = c \pmod{H}$

$\Rightarrow \quad ab^{-1} \in H$ and $bc^{-1} \in H \Rightarrow (ab^{-1})(bc^{-1}) \in H \quad [\because H < G]$

$\Rightarrow \quad ac^{-1} \in H \Rightarrow a \equiv c \pmod{H}$.

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 $\quad x \in [a]$ so that $xa^{-1} \in H \Rightarrow x \in Ha$.

$\therefore \quad [a] \subseteq Ha$.

Conversely, let $y \in Ha$. Then $y = ha$ for some $h \in H$

$\Rightarrow \quad ya^{-1} = h \Rightarrow ya^{-1} \in H \Rightarrow y \in [a]$, by (3)

$\therefore \quad Ha \subseteq [a]$. 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].

Remark 2. *The converse of Lagrange's theorem holds in case of finite cyclic groups.* Refer to Theorem 1.11.4 which states : *If G is a finite cyclic group and if m is any positive integer such that m divides o (G), then G has a unique subgroup of order m.*

Definition. (Index of a Subgroup)

The **index** *of a subgroup H of a group G is defined as the number of distinct right (or left) cosets of H in G. It is denoted by* $i_G(H)$ *or* $[G : H]$.

Theorem 1.12.5. *The index of a subgroup H of a finite group G divides the order of the group and*

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

Proof. As shown in the proof of Lagrange's theorem,

$$G = Ha_1 \cup Ha_2 \cup \ldots \cup Ha_r \text{ and}$$

$$n = mr \quad i.e., o(G) = r\,o(H). \qquad \ldots(1)$$

It is clear that H has r distinct right cosets so that $i_G(H) = r$.

By (1), r divides $o(G)$ *i.e.*, $i_G(H) \mid o(G)$. Also $o(G) = i_G(H) \,.\, o(H)$.

Hence, $i_G(H) = \dfrac{o(G)}{o(H)}$.

Theorem 1.12.6. *If G is a finite group and* $a \in G$, *then order of a divides o (G).* [D.U., 1996]

Proof. Let $o(G) = n$ and $o(a) = m$.

Then m is the least positive integer such that $a^m = e$. ...(1)

Let $H = \{a, a^2, a^3, \ldots, a^m = e\}$. Then H is a subgroup of G, which has at most m elements. If $o(H) < m$, then we must have

$$a^i = a^j \text{ for some integers } 0 \le j < i < m$$

$$\Rightarrow \quad a^{i-j} = e, \text{ where } 0 < i - j < m.$$

This contradicts (1). Hence $o(H) = m$.

By Lagrange's theorem, $o(H)$ divides $o(G)$

$$\Rightarrow \quad m \mid o(G) \Rightarrow o(a) \mid o(G).$$

Corollary 1. *If G is a finite group and* $a \in G$, *then*

$$a^{o(G)} = e.$$

Proof. By Theorem 1.12.6, $o(a)$ divides $o(G)$. Let $o(a) = m$ so that

$$a^m = e.$$

Since $m \mid o(G)$, $o(G) = ml$ for some integer l.

Hence $\quad a^{o(G)} = a^{ml} = (a^m)^l = e^l = e.$

Corollary 2. *If n is a positive integer and a is relatively prime to n, then* $a^{\phi(n)} \equiv 1 \pmod{n}$, $\phi(n)$ *being the Euler* ϕ*-function.*

Proof. We know that the set U_n of integers less than n and relatively prime to n is a group under multiplication modulo n. Further $o(U_n) = \phi(n)$, where $\phi(n)$ is Euler ϕ-function. Since a is relatively prime to n, $a \in U_n$. By corollary 1, we have

$$a^{o(U_n)} = 1 \text{ in } U_n \quad \Rightarrow \quad a^{\phi(n)} = 1 \text{ in } U_n$$

Hence $a^{\phi(n)} \equiv 1 \pmod{n}$.

[For example, $2^6 = 1$ in U_9 means $2^6 \equiv 1 \pmod{9}$]

Corollary 3. [Fermat's Theorem]

If p is a prime number and a is any integer, then

$$a^p \equiv a \pmod{p}.$$

Proof. For any prime number p,

$$\phi(p) = p - 1.$$

Since a is relatively prime to p, by corollary 2, we have

$$a^{\phi(p)} \equiv 1 \pmod{p} \quad \Rightarrow a^{p-1} \equiv 1 \pmod{p}$$

$$\Rightarrow \quad a \cdot a^{p-1} \equiv a \cdot 1 \pmod{p} \Rightarrow \quad a^p \equiv a \pmod{p}.$$

Theorem 1.12.7. *Every group of prime order is cyclic.*

Proof. Let $o(G) = p$, p being a prime. Let H be any subgroup of G. By Lagrange's theorem, $o(H)$ divides $o(G) = p$. Consequently,

$$o(H) = 1 \quad \text{or} \quad o(H) = p$$

$$\Rightarrow \quad H = (e) \quad \text{or} \quad H = G. \qquad \ldots(1)$$

It follows that a group of prime order has no non-trivial (proper) subgroups. [$\{e\}$ and G are called **trivial** subgroups of G]

Let $H = \langle a \rangle$, where $a \neq e \in G$.

Then H is a subgroup of G and $H \neq (e)$, since $a \neq e \in H$. Hence by (1), $G = H = \langle a \rangle$, which proves that G is cyclic.

Remark 1. *Every group of prime order is abelian*, since it is cyclic.

As shown above :

Remark 2. *A group of prime order has no non-trivial subgroups.*

Theorem 1.12.8. *Show that a finite group G of composite order has a non-trivial subgroup.*

Proof. Let $o(G) = mn$, where $m > 1$ and $n > 1$. Since $mn > 1$, there exists some element $a \neq e \in G$. We have two cases :

Case I. Let $a^m = e$. Then $o(a) \leq m$.

Let $o(a) = k$, where $1 < k \leq m < o(G)$.

(Notice that $k \neq 1$, as $a \neq e$)

Then $H = \langle a \rangle = \{a, a^2, \ldots, a^k = e\}$ is a proper subgroup of G.

Case II. Let $a^m \neq e$. We have

$$(a^m)^n = a^{mn} = a^{o(G)} = e \qquad \text{[Cor. 1 of Theorem 1.12.6]}$$

Proof. We know that the set U_n of integers less than n and relatively prime to n is a group under multiplication modulo n. Further $o(U_n) = \phi(n)$, where $\phi(n)$ is Euler ϕ-function. Since a is relatively prime to n, $a \in U_n$. By corollary 1, we have

$$a^{o(U_n)} = 1 \text{ in } U_n \quad \Rightarrow \quad a^{\phi(n)} = 1 \text{ in } U_n.$$

Hence $a^{\phi(n)} \equiv 1 \pmod{n}$.

[For example, $2^6 = 1$ in U_9 means $2^6 \equiv 1 \pmod{9}$]

Corollary 3. [Fermat's Theorem]

If p is a prime number and a is any integer, then

$$a^p = a \pmod{p}.$$

Proof. For any prime number p,

$$\phi(p) = p - 1.$$

Since a is relatively prime to p, by corollary 2, we have

$$a^{\phi(p)} \equiv 1 \pmod{p} \quad \Rightarrow a^{p-1} \equiv 1 \pmod{p}$$

$$\Rightarrow \quad a \,.\, a^{p-1} \equiv a \,.\, 1 \pmod{p} \Rightarrow \quad a^p \equiv a \pmod{p}.$$

Theorem 1.12.7. *Every group of prime order is cyclic.*

Proof. Let $o(G) = p$, p being a prime. Let H be any subgroup of G. By Lagrange's theorem, $o(H)$ divides $o(G) = p$. Consequently,

$$o(H) = 1 \quad \text{or} \quad o(H) = p$$

$$H = (e) \text{ or } \quad H = G. \qquad \ldots(1)$$

It follows that a group of prime order has no non-trivial (proper) subgroups. [$\{e\}$ and G are called **trivial** subgroups of G]

Let $H = \langle a \rangle$, where $a \neq e \in G$.

Then H is a subgroup of G and $H \neq (e)$, since $a \neq e \in H$. Hence by (1), $G = H = \langle a \rangle$, which proves that G is cyclic.

Remark 1. *Every group of prime order is abelian,* since it is cyclic.

As shown above :

Remark 2. *A group of prime order has no non-trivial subgroups.*

Theorem 1.12.8. *Show that a finite group G of composite order has a non-trivial subgroup.*

Proof. Let $o(G) = mn$, where $m > 1$ and $n > 1$. Since $mn > 1$, there exists some element $a \neq e \in G$. We have two cases :

Case I. Let $a^m = e$. Then $o(a) \leq m$.

Let $o(a) = k$, where $1 < k \leq m < o(G)$.

(Notice that $k \neq 1$, as $a \neq e$)

Then $H = \langle a \rangle = \{a, a^2, \ldots, a^k = e\}$ is a proper subgroup of G.

Case II. Let $a^m \neq e$. We have

$$(a^m)^n = a^{mn} = a^{o(G)} = e \qquad \text{[Cor. 1 of Theorem 1.12.6]}$$

$\Rightarrow \quad o(a^m) \leq n$. Let $o(a^m) = l$, $1 < l \leq n < o(G)$.

Then $K = \langle a^m \rangle = \langle a^m, a^{2m}, \ldots, a^{lm} \rangle$ is a proper subgroup of G.

Theorem 1.12.9. *If a group G has no non-trivial subgroups, show that G must be finite of prime order.*

Proof. It is given that G has no proper subgroups. Let $a \in G$ be such that $a \neq e$. Then $H = \langle a \rangle$ is a subgroup of G, and $H \neq \{e\}$. Since G has no proper subgroups,

$$H = G \quad i.e., \quad G = \langle a \rangle.$$

If $o(a)$ is infinite, then

$$K = \langle a^2 \rangle = \{a^2, a^4, a^6, \ldots\}$$

is a proper subgroup of $G = \langle a \rangle$, which is contrary to the given hypothesis. Hence $o(a)$ must be finite and so $G = \langle a \rangle$ is a finite group. If $o(G)$ is composite, then G must have a non-trivial subgroup [Theorem 1.12.8], which is again contrary to the given hypothesis. Hence G is finite of prime order.

Remark. From Theorems 1.12.7 and 1.12.9, it follows that

A group $G \neq \{e\}$ has no proper subgroups iff G is a finite cyclic group of prime order.

EXAMPLES

Example 1.12.3. *Let H be a subgroup of G and $a, b \in G$. Show that*

$$Ha \neq Hb \Leftrightarrow a^{-1}H \neq b^{-1}H.$$

Solution. Suppose $Ha \neq Hb$.

Let, if possible, $a^{-1}H = b^{-1}H$. Then, by Theorem 1.12.1 (*iii*),

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

$\Rightarrow \quad ab^{-1} \in H \Rightarrow Ha = Hb$, which is a contradiction.

$\therefore \quad a^{-1}H \neq b^{-1}H$.

Conversely, let $a^{-1}H \neq b^{-1}H$.

Let, if possible, $Ha = Hb$. Then $ab^{-1} \in H$

$\Rightarrow (a^{-1})^{-1}(b^{-1}) \in H \Rightarrow a^{-1}H = b^{-1}H$, which is a contradiction.

$\therefore Ha = Hb$.

Example 1.12.4. *If $H \subseteq K$ be two subgroups of a finite group G, then show that*

$$[G : H] = [G : K]\,[K : H].$$

Solution. Since $H \subseteq K \subseteq G$ and H, K are subgroups of G, therefore H is a subgroup of K. By Lagrange's Theorem,

$$[G : H] = \frac{o(G)}{o(H)}.$$

Similarly, $[G : K] = \dfrac{o(G)}{o(K)}$, $[K : H] = \dfrac{o(K)}{o(H)}$.

Hence $[G : K]\,[K : H] = \dfrac{o(G)}{o(K)} \times \dfrac{o(K)}{o(H)} = \dfrac{o(G)}{o(H)} = [G : H]$.

Example 1.12.5. *Show that there exists a one-to-one correspondence between the right and left cosets of H in G, where H is any subgroup of a group G.*

Solution. Let S and T be the sets of right and left cosets of H in G, respectively. We have to show that there exists a one-to-one mapping of S onto T.

Define a mapping $\phi : S \to T$ as

$$\phi(Ha) = a^{-1}H \quad \forall\ a \in G. \qquad \text{...(1)}$$

(Note that Ha is a right coset and $a^{-1}H$ is a left coset).

First of all we show that ϕ is well defined *i.e.*, to show

$$Ha = Hb \Rightarrow a^{-1}H = b^{-1}H.$$

Now $\quad Ha = Hb \Rightarrow ab^{-1} \in H$

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

$\Rightarrow a^{-1}H = b^{-1}H.$ [Theorem 1.12.1 (*iii*)]

Thus ϕ is well-defined. Now we show that ϕ is one-to-one.

Let $\phi(Ha) = \phi(Hb)$; $a, b \in G$.

By (1), $a^{-1}H = b^{-1}H \Rightarrow (a^{-1})^{-1}b^{-1} \in H \Rightarrow ab^{-1} \in H \Rightarrow Ha = Hb$.

Thus ϕ is one-to-one. Now we show that ϕ is onto.

Let $Y \in T$ so that $Y = cH$ for some $c \in G$. Then

$$Y = (c^{-1})^{-1}H = d^{-1}H, \quad \text{where } d = c^{-1} \in G$$

$\Rightarrow Y = \phi(Hd)$, where $Hd \in S$, by (1)

$\Rightarrow \phi$ is onto. Hence the result.

Example 1.12.6. *If $H < G$, prove that*

(*i*) $Hh = H \Leftrightarrow h \in H$,

(*ii*) $b \in Ha \Leftrightarrow Ha = Hb$.

Solution. (*i*) $Hh = H \Leftrightarrow Hh = He \Leftrightarrow he^{-1} \in H$

$\Leftrightarrow he \in H \Leftrightarrow h \in H.$

(*ii*) $b \in Ha \Rightarrow b = ha$ for some $h \in H \Rightarrow Hb = Hha$

$\Rightarrow \quad Hb = Ha$, by part (*i*).

Conversely, $Ha = Hb \Rightarrow ab^{-1} \in H$

$\Rightarrow \quad ab^{-1} = h_1$ for some $h_1 \in H \Rightarrow h_1^{-1}a = b$.

$\Rightarrow \quad b \in Ha$, since $h_1^{-1} \in H$. $\quad (\because H < G)$.

Example 1.12.7. *Show that if H and K are subgroups of a group G and $a \in G$, then $Ha \cap Ka = (H \cap K)\,a$.*

Solution. Let $x \in Ha \cap Ka$. Then $x \in Ha$ and $x \in Ka$

$\Rightarrow \quad x = ha$ and $x = ka$ for some $h \in H$, $k \in K$

$\Rightarrow ha = ka \Rightarrow h = k$, by right cancellation law in G.

Thus $h \in H \cap K$ and $x = ha \Rightarrow x \in (H \cap K)\, a$

$$\therefore \quad Ha \cap Ka \subseteq (H \cap K)\, a. \qquad \ldots(1)$$

Conversely, let $x \in (H \cap K)\, a$. Then $x = pa$ for some $p \in H \cap K$

$\Rightarrow \quad x = pa$ for $p \in H$ and $x = pa$ for $p \in K$.

$\Rightarrow \quad x \in Ha$ and $x \in Ka \Rightarrow x \in Ha \cap Ka$.

$$\therefore \quad (H \cap K)\, a \subseteq Ha \cap Ka. \qquad \ldots(2)$$

From (1) and (2), $Ha \cap Ka = (H \cap K)\, a$.

Example 1.12.8. (Poincare's Theorem)

If G is a group and H, K are two subgroups of finite index in G, prove that $H \cap K$ is of finite index.

Solution. Since H and K are two subgroups of G, therefore $H \cap K$ is a subgroup of G. By Example 1.12.7,

$$(H \cap K)\, a = Ha \cap Ka \quad \forall \quad a \in G.$$

Thus any right coset of $H \cap K$ is the intersection of a right coset of H and a right coset of K. But the number of such intersections is finite, since $i_G(H)$ and $i_G(K)$ is each finite. Consequently, the number of right cosets of $H \cap K$ in G is finite.

Hence $H \cap K$ is of finite index.

Example 1.12.9. *Suppose that H is a subgroup of G such that whenever $Ha \neq Hb$, then $aH \neq bH$. Prove that $gHg^{-1} \subseteq H$ for all $g \in G$.*

Solution. The condition

$$Ha \neq Hb \Rightarrow aH \neq bH$$

is equivalent to the following condition

$$aH = bH \Rightarrow Ha = Hb.$$

By definition, $\quad gHg^{-1} = \{ghg^{-1} : h \in H\}$. $\quad \ldots(1)$

Let $g \in G$ and $h \in H$. We have

$$(g^{-1}h)\, H = g^{-1}(hH) = g^{-1}H. \text{ [See Example 1.12.6. (i)]}$$

Using (1), $\quad (g^{-1}h)\, H = g^{-1}H \Rightarrow H\,(g^{-1}h) = Hg^{-1}$

$\Rightarrow \quad (g^{-1}h)\,(g^{-1})^{-1} \in H \Rightarrow g^{-1}hg \in H \;\forall\; g \in G, \forall\; h \in H$

$\Rightarrow \quad g^{-1}Hg \subseteq H \quad \forall \quad g \in G.$

Hence $\quad gHg^{-1} = (g^{-1})^{-1}H\,(g^{-1}) \subseteq H$, using (2). $\quad \ldots(2)$

Example 1.12.10. *Prove that a finite group can never be expressed as the union of two of its proper subgroups.*

Solution. Let G be a finite group of order n. Let, if possible, $G = H \cup K$; where H and K are two proper subgroups of G. Obviously,

Solution. Let $x \in Ha \cap Ka$. Then $x \in Ha$ and $x \in Ka$

$\Rightarrow \quad x = ha$ and $x = ka$ for some $h \in H$, $k \in K$

$\Rightarrow ha = ka \Rightarrow h = k$, by right cancellation law in G.

Thus $h \in H \cap K$ and $x = ha \Rightarrow x \in (H \cap K)\, a$

$\therefore \qquad Ha \cap Ka \subseteq (H \cap K)\, a.$

Conversely, let $x \in (H \cap K)\, a$. Then $x = pa$ for some $p \in H \cap K$

$\Rightarrow \quad x = pa$ for $p \in H$ and $x = pa$ for $p \in K$.

$\Rightarrow \quad x \in Ha$ and $x \in Ka \Rightarrow x \in Ha \cap Ka.$

$\therefore \quad (H \cap K)\, a \subseteq Ha \cap Ka.$ ...(2)

From (1) and (2), $Ha \cap Ka = (H \cap K)\, a.$

Example 1.12.8. (Poincare's Theorem)

If G is a group and H, K are two subgroups of finite index in G, prove that $H \cap K$ is of finite index.

Solution. Since H and K are two subgroups of G, therefore $H \cap K$ is a subgroup of G. By Example 1.12.7,

$$(H \cap K)\, a = Ha \cap Ka \quad \forall \quad a \in G.$$

Thus any right coset of $H \cap K$ is the intersection of a right coset of H and a right coset of K. But the number of such intersections is finite, since $i_G(H)$ and $i_G(K)$ is each finite. Consequently, the number of right cosets of $H \cap K$ in G is finite.

Hence $H \cap K$ is of finite index.

Example 1.12.9. *Suppose that H is a subgroup of G such that whenever $Ha \neq Hb$, then $aH \neq bH$. Prove that $gHg^{-1} \subseteq H$ for all $g \in G$.*

Solution. The condition

$$Ha \neq Hb \Rightarrow aH \neq bH$$

is equivalent to the following condition

$$aH = bH \Rightarrow Ha = Hb.$$

By definition, $\quad gHg^{-1} = \{ghg^{-1} : h \in H\}.$ ...(1)

Let $g \in G$ and $h \in H$. We have

$$(g^{-1}h)\, H = g^{-1}(hH) = g^{-1}H. \text{ [See Example 1.12.6. (i)]}$$

Using (1), $\quad (g^{-1}h)\, H = g^{-1}H \Rightarrow H(g^{-1}h) = Hg^{-1}$

$\Rightarrow \quad (g^{-1}h)(g^{-1})^{-1} \in H \Rightarrow g^{-1}hg \in H \;\forall\; g \in G, \forall\; h \in H$

$\Rightarrow \quad g^{-1}Hg \subseteq H \quad \forall \quad g \in G.$

Hence $\quad gHg^{-1} = (g^{-1})^{-1}H(g^{-1}) \subseteq H$, using (2). ...(2)

Example 1.12.10. *Prove that a finite group can never be expressed as the union of two of its proper subgroups.*

Solution. Let G be a finite group of order n. Let, if possible, $G = H \cup K$; where H and K are two proper subgroups of G. Obviously,

Solution. Let $x \in Ha \cap Ka$. Then $x \in Ha$ and $x \in Ka$

$\Rightarrow \quad x = ha$ and $x = ka$ for some $h \in H$, $k \in K$

$\Rightarrow ha = ka \Rightarrow h = k$, by right cancellation law in G.

Thus $h \in H \cap K$ and $x = ha \Rightarrow x \in (H \cap K)\, a$

$\therefore \qquad Ha \cap Ka \subseteq (H \cap K)\, a.$

Conversely, let $x \in (H \cap K)\, a$. Then $x = pa$ for some $p \in H \cap K$

$\Rightarrow \quad x = pa$ for $p \in H$ and $x = pa$ for $p \in K$.

$\Rightarrow \quad x \in Ha$ and $x \in Ka \Rightarrow x \in Ha \cap Ka.$

$\therefore \quad (H \cap K)\, a \subseteq Ha \cap Ka.$ ...(2)

From (1) and (2), $Ha \cap Ka = (H \cap K)\, a.$

Example 1.12.8. (Poincare's Theorem)

If G is a group and H, K are two subgroups of finite index in G, prove that $H \cap K$ is of finite index.

Solution. Since H and K are two subgroups of G, therefore $H \cap K$ is a subgroup of G. By Example 1.12.7,

$$(H \cap K)\, a = Ha \cap Ka \quad \forall \quad a \in G.$$

Thus any right coset of $H \cap K$ is the intersection of a right coset of H and a right coset of K. But the number of such intersections is finite, since $i_G(H)$ and $i_G(K)$ is each finite. Consequently, the number of right cosets of $H \cap K$ in G is finite.

Hence $H \cap K$ is of finite index.

Example 1.12.9. *Suppose that H is a subgroup of G such that whenever $Ha \neq Hb$, then $aH \neq bH$. Prove that $gHg^{-1} \subseteq H$ for all $g \in G$.*

Solution. The condition

$$Ha \neq Hb \Rightarrow aH \neq bH$$

is equivalent to the following condition

$$aH = bH \Rightarrow Ha = Hb.$$

By definition, $\quad gHg^{-1} = \{ghg^{-1} : h \in H\}.$ ...(1)

Let $g \in G$ and $h \in H$. We have

$$(g^{-1}h)\, H = g^{-1}(hH) = g^{-1}H. \text{ [See Example 1.12.6. (i)]}$$

Using (1), $\quad (g^{-1}h)\, H = g^{-1}H \Rightarrow H(g^{-1}h) = Hg^{-1}$

$\Rightarrow \quad (g^{-1}h)(g^{-1})^{-1} \in H \Rightarrow g^{-1}hg \in H \;\forall\; g \in G, \forall\; h \in H$

$\Rightarrow \quad g^{-1}Hg \subseteq H \quad \forall \quad g \in G.$

Hence $\quad gHg^{-1} = (g^{-1})^{-1}H(g^{-1}) \subseteq H$, using (2). ...(2)

Example 1.12.10. *Prove that a finite group can never be expressed as the union of two of its proper subgroups.*

Solution. Let G be a finite group of order n. Let, if possible, $G = H \cup K$; where H and K are two proper subgroups of G. Obviously,

$e \in H$ and $e \in K$. Since $G = H \cup K$, it follows that both H and K cannot have less than $\frac{1}{2}n$ elements of G [Imagine a group of order of order 12]. Suppose H has more than half the elements of G. Let $o(H) = m$, where $\frac{1}{2}n < m < n$ ($m < n$, as H is a proper subgroup of G).

Since $\frac{1}{2}n < m < n$, m cannot divide n *i.e.*, $o(H)$ does not divide $o(G)$, which contradicts Lagrange's theorem. Hence a finite group cannot be 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 $x^{-1} \in HK$ $\quad (\because HK < G)$

$\Rightarrow \quad x^{-1} = hk$, for some $h \in H, k \in K$

$\Rightarrow \quad x = (x^{-1})^{-1} = (hk)^{-1} = k^{-1}h^{-1} \in KH,$

since $k^{-1} \in K$ and $h^{-1} \in H$ $\quad (\because K < G$ and $H < G)$.

Thus $\quad HK \subseteq KH.$ ...(1)

Suppose that $y \in KH$ is arbitrary. Then

$$y = k_1 h_1, \text{ for } k_1 \in K \text{ and } h_1 \in H$$
$$= (k_1^{-1})^{-1}(h_1^{-1})^{-1} = (h_1^{-1}k_1^{-1})^{-1} \quad ...(2)$$

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).

Thus $\qquad KH \subseteq HK. \qquad$ ...(3)

From (1) and (3), $HK = KH$.

Condition is sufficient

Suppose that $\quad HK = KH. \qquad$ ...(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 $\qquad xy = hkh' k'. \qquad$ ...(5)

Since $\qquad kh' \in KH = HK$, we can write

$\qquad kh' = h_2 k_2$ 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 $k_2 k' \in K \quad (\because H < G$ and $K < G)$

Thus $\qquad xy \in HK \quad \forall \quad x, y \in HK. \qquad$ ...(6)

Also $\qquad x^{-1} = (hk)^{-1} = k^{-1} h^{-1} \in KH = HK.$

$\therefore \qquad x^{-1} \in HK \quad \forall \quad x \in HK \qquad$ ...(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 is a subgroup of G.*

Proof. Since G is abelian, then $HK = KH$. Hence HK is a subgroup of G.

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 is a 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 $Tk_1, Tk_2 \ldots, Tk_m$; $k_1, k_2, \ldots, k_m \in K$. Furthermore,

$$K = Tk_1 \cup Tk_2 \cup \ldots \cup Tk_m$$

$$\Rightarrow \quad HK = H(Tk_1 \cup Tk_2 \cup \ldots \cup Tk_m)$$

$$= HTk_1 \cup HTk_2 \cup \ldots \cup HTk_m$$

$$= Hk_1 \cup Hk_2 \cup \ldots \cup Hk_m. \qquad [\because T \subseteq H \Rightarrow HT = H]$$

...(2)

Next we show that $Hk_1, Hk_2, ..., Hk_m$ are all distinct.

Let, if possible, $Hk_i = Hk_j$ for $1 \le i < j \le m$

$\Rightarrow \quad k_i k_j^{-1} \in H$. Also $k_i k_j^{-1} \in K \quad (\because K < G)$

$\Rightarrow \quad k_i k_j^{-1} \in H \cup K = T$

$\Rightarrow \quad T k_i = T k_j$, 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 $\quad o(HK) = \dfrac{o(H)\, o(K)}{o(H \cup K)}$.

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.,* $H \cap K \ne \{e\}$.

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 $\quad o(G) > \dfrac{o(G)}{o(H \cap K)} \Rightarrow o(H \cap K) > 1.$

Hence $\quad H \cap K \ne \{e\}$.

EXAMPLES

Example 1.13.1. *If G is a group of order 35, show that it cannot have two subgroups of order 7.*

Solution. Let, if possible, G have two subgroups H and K, where $o(H) = o(K) = 7$ and $H \ne K$.

Since $H \cup K$ is a subgroup of H, by Lagrange's theorem, $o(H \cap K)$ divides $o(H) = 7$. Thus

$$o(H \cap K) = 1.$$

[Notice that $o(H \cap K) = 7 \Rightarrow H \cap K = H \Rightarrow H = K$, a contradiction.]

Now $\quad o(HK) = \dfrac{o(H)\, o(K)}{o(H \cap K)} = \dfrac{7 \times 7}{1} = 49 > o(G) = 35.$

This is impossible. Hence the result.

Example 1.13.2. *If G is a group of order 91, show that it cannot have two subgroups of order 13.*

Hint. Similar to Example 1.13.1.

Example 1.13.3. *Suppose G is a finite group of order pq, where p and q are primes* $(p > q)$. *Show that G has at most one subgroup of order p.*

Solution. Suppose G has two subgroups H and K each of order p i.e., $o(H) = o(K) = p$.

Now $\quad p > q \Rightarrow p^2 > pq = o(G) \Rightarrow p > \sqrt{o(G)}$.

Thus $\quad o(H) > \sqrt{o(G)}$ and $o(K) > \sqrt{o(G)}$.

Since $HK \subseteq G$, $o(HK) \leq o(G)$ i.e.,

$$o(G) \geq o(HK) = \frac{o(H)\,o(K)}{o(H \cap K)} > \frac{\sqrt{o(G)}\,\sqrt{o(G)}}{o(H \cap K)} = \frac{o(G)}{o(H \cap K)}$$

$$\Rightarrow o(G) > \frac{o(G)}{o(H \cap K)} \Rightarrow o(H \cap K) > 1.$$

By Lagrange's Theorem, $o(H \cap K)$ divides $o(H) = p$

$\Rightarrow o(H \cap K) = p$, since $o(H \cap K) > 1$ and p is prime

$\Rightarrow o(H \cap K) = o(H) \Rightarrow H \cap K = H \qquad (\because H \cap K \subseteq H)$

$\Rightarrow \qquad H = K.$

Hence G has at most one subgroup of order p.

Example 1.13.4. *Show that a group of G of order 15 has at most one subgroup of order 5.*

Hint. $o(G) = 3 \times 5\ (5 > 3)$. The result follows by Example 1.13.3.

Example 1.13.5. *Show that a group G of order 2p, where p is prime and $p > 2$, has exactly one subgroup of order p.*

Solution. Suppose G has two distinct subgroups H and K, where $o(H) = o(K) = p$, $H \neq K$.

By Lagrange's Theorem, $o(H \cap K)$ divides $o(H) = p$

$\Rightarrow \quad o(H \cap K) = 1$ or p, since p is prime.

If $\quad o(H \cap K) = p$, then $o(H \cap K) = o(H)$ or $H \cap K = H$

$(\because H \cap K \subseteq H)$

$\Rightarrow \quad H = K$, which is a contradiction. Thus $o(H \cap K) = 1$.

We have

$$o(HK) = \frac{o(H)\,o(K)}{o(H \cap K)} = \frac{p \cdot p}{1} = p^2 > o(G) = 2p,$$

since $p > 2$ and p is prime.

But $o(HK) > o(G)$ is impossible. Hence the result.

Example 1.13.6. *Consider two subgroups $H = \{I, (12)\}$ and $K = \{I, (13)\}$ of S_3. Show that HK is not a subgroup of S_3.*

Solution. We have

$$HK = \{II = I, I(13) = (13), (12)I = (12), (12)(13)\}$$

or $\qquad HK = \{I, (13), (12), (132)\}$.

Also $\qquad KH = \{I, (12), (13), (13)(12)\} = \{I, (12), (13), (123)\}$.

Since $\qquad HK \neq KH$, HK is not a subgroup of G. [Theorem 1.13.1.]

Alternatively, $o(HK)$ does not divide $o(S_3) = 6$.

Hence by Lagrange's theorem, HK is not a subgroup of S_3.

Example 1.13.7. *Let G be a cyclic group of order 6 generated by a. Let $H = \langle a^2 \rangle$ and $K = \langle a^3 \rangle$. Show that $G = HK$.*

Solution. We have $G = \{a, a^2, a^3, a^4, a^5, a^6 = e\}$,

$$H = \{a^2, a^4, a^6 = e\},\ K = \{a^3, a^6 = e\}.$$

Then $\quad o(H) = 3,\ o(K) = 2,\ H \cap K = \{e\}.$

Since G is cyclic, G is abelian and so HK is a subgroup of G.

[Cor. of Theorem 1.13.1]

Now $\quad o(HK) = \dfrac{o(H)\,o(K)}{o(H \cap K)} = \dfrac{2 \times 3}{1} = 6 = o(G).$

Hence $\quad G = HK$, 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 $A = \langle a^2 \rangle, B = \langle a \rangle$.

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

$$H = \{a, a^2 = e\},\ K = \{b, b^2 = e\} \text{ and } a \neq b \quad (\because H \neq K)$$

$\Rightarrow \quad H \cap K = \{e\}.$

Now $\quad o(HK) = \dfrac{o(H)\,o(K)}{o(H \cap K)} = \dfrac{2 \times 2}{1} = 4.$

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 $N \lhd G$. 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,

$N \lhd G \Leftrightarrow gNg^{-1} = N \ \forall\ g \in G \Leftrightarrow (gNg^{-1})\, g = Ng \ \forall\ g \in G.$

Hence $N \lhd G \Leftrightarrow gN = Ng \ \forall\ g \in G.$ $[\because g^{-1}g = e$ 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 $N \lhd G$.

$= NN\,ab = N\,ab$, 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 $H \lhd G$ 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 $H \lhd G$

$= HH\,ab = H\,ab$, 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 $H \lhd G$.

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

$$x \in Hx,\ h \in H = He \text{ and } x^{-1} \in Hx^{-1} \Rightarrow xhx^{-1} \in HxHeHx^{-1}$$

$$\Rightarrow xhx^{-1} \in Hxe\,Hx^{-1} = HxHx^{-1} = Hxx^{-1} = He = H, \text{ using (1)}$$

$$\Rightarrow xhx^{-1} \in H \;\forall\, x \in G,\ h \in H. \text{ Hence } H \lhd G.$$

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 $N \lhd G$, $gag^{-1} \in N$.

Since $M \lhd G$, $gag^{-1} \in M$.

$\therefore \qquad gag^{-1} \in N \cap M \;\forall\, g \in G$ 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 $Z \lhd G$. Let $g \in G$ and $a \in Z$.

Since $a \in Z$, $ag = ga \;\forall\, g \in G$

$\Rightarrow \qquad gag^{-1} = a \in Z.$

$\therefore \qquad gag^{-1} \in Z \;\forall\, g \in G$ and $a \in Z$. Hence $Z \lhd G$.

Example 1.14.3. *Show that $H = \{(1, b) : b \in \mathbf{R}\}$ is a normal subgroup of $G = \{(a, b) : a \neq 0, b \in \mathbf{R}\}$ under the composition $*$ defined by*

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

Solution. By Example 1.7.28, we see that $\{H, *\}$ is a subgroup of $\{G, *\}$. Now we show that H is a normal subgroup of G.

Let $g = (a, b) \in G$ and $h = (1, c) \in H$.

We have to show that $g * h * g^{-1} \in H$. We have

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

Also $\qquad g^{-1} = (a^{-1}, -ba^{-1}).$

$$\therefore \quad g * h * g^{-1} = (a, b+c) * (a^{-1}, -ba^{-1})$$
$$= (aa^{-1}, (b+c)a^{-1} - ba^{-1}) = (1, ca^{-1}), \text{ by (1).}$$

$\therefore \quad g * h * g^{-1} \in H \; \forall \; g \in G$ and $h \in H$. Hence $H \lhd G$.

Example 1.14.4. *If H is a subgroup of G and N is a normal subgroup of G, then $H \cap N$ is a normal subgroup of H.*

Solution. Since $H < G$ and $N < G$, $H \cap N < G$.

Since $H \cap N \subset H$, $H \cap N$ is a subgroup of H.

Now we show $H \cap N \lhd H$.

Let $h \in H$ and $a \in H \cap N$ (*i.e.*, $a \in H$ and $a \in N$).

We shall show that $hah^{-1} \in H \cap N$.

Since $H < G$, $h^{-1} \in H$ and $a \in H \Rightarrow hah^{-1} \in H$.

Since $N \lhd G$, so $h \in H$ ($\Rightarrow h \in G$) and $a \in N$ implies $hah^{-1} \in N$.

Now $hah^{-1} \in H$ and $hah^{-1} \in N \Rightarrow hah^{-1} \in H \cap N$.

Hence $H \cap N$ is a normal subgroup of H.

Example 1.14.5. *If N and M are normal subgroups of a group G and if $N \cap M = (e)$, then $nm = mn$ for each $n \in N$ and $m \in M$.*

Solution. Consider $mnm^{-1}n^{-1} = (mnm^{-1})n^{-1}$,

where $\quad mnm^{-1} \in N \; (\because N \lhd G)$ and $n^{-1} \in N \quad (\because N < G))$.

$\therefore \; mnm^{-1}n^{-1} \in NN = N \quad (\because N < G)$.

Again $\quad mnm^{-1}n^{-1} = m(nm^{-1}n^{-1})$,

where $\quad nm^{-1}n^{-1} \in M \quad (\because M \lhd G)$.

$\therefore \quad mnm^{-1}n^{-1} \in MM = M \quad (\because M < G)$.

Now $mnm^{-1}n^{-1} \in M \cap N = (e)$ implies that

$$mnm^{-1}n^{-1} = e \Rightarrow mnm^{-1} = en = n.$$

Hence $\quad mn = nm \; \forall \; n \in N, m \in M$.

Example 1.14.6. *If G is a group and H is a subgroup of index 2 in G, prove that H is a normal subgroup of G.*

Solution. Let $g \in G$ be arbitrary.

If $g \in H$, then $gH = H = Hg$.

If $g \notin H$, then $gH \neq H$ and $Hg \neq H$

Consequently, $\quad H \cap gH = \phi \quad$ and $\quad H \cap Hg = \phi$.

Since the index of H in G is 2, it follows that ...(1)

$$G = H \cup gH \quad \text{and} \quad G = H \cap Hg.$$

Thus $\quad H \cup gH = H \cup Hg \; \forall \; g \in G$.

Using (1), $\quad gH = Hg \; \forall \; g \in G$.

Hence H is a normal subgroup of G.

Example 1.14.7. *If H is a subgroup of a group G such that $x^2 \in H$ for every $x \in G$, prove that H is a normal subgroup of G.*

Solution. Let $g \in G$, so that $g^{-1} \in G$. Then $(g^{-1})^2 \in H$, by the given hypothesis. Thus $g^{-2} \in H$ and so

$$h^{-1} g^{-2} \in H \ \forall\ h \in H. \qquad (\because H < G \text{ and } h^{-1} \in H)$$

Since $gh \in G$, therefore $(gh)^2 \in H$, by the given hypothesis.

Now $(gh)^2 \in H$ and $h^{-1} g^{-2} \in H \Rightarrow (gh)^2 h^{-1} g^{-2} \in H$, as $H < G$.

$\Rightarrow \quad ghghh^{-1} g^{-1} g^{-1} \in H \Rightarrow ghgeg^{-1} g^{-1} \in H$

$\Rightarrow \quad ghg^{-1} \in H \quad \forall\ g \in G, h \in H. \qquad (geg^{-1} = gg^{-1} = e).$

Hence H is a normal subgroup of G.

Example 1.14.8. *If H is the only subgroup of finite order m in the group G, then show that H is a normal subgroup of G.*

Solution. We have $H < G$ and $o(H) = m$.

Let $\quad H = \{h_1, h_2, \ldots, h_m\}$. For any $g \in G$, we have

$$gHg^{-1} = \{gh_1g^{-1}, gh_2g^{-1}, \ldots, gh_mg^{-1}\}.$$

Then gHg^{-1} is a subgroup of G, [by Example 1.9.5]

Further $o(gHg^{-1}) = m$, since by cancellation laws in G

$gh_ig^{-1} = gh_jg^{-1} \Rightarrow h_i = h_j$, which is a contradiction.

Thus for each $g \in G$, gHg^{-1} is also a subgroup of G of order m.

Since H is the only subgroup of order m in G, so we must have

$$gHg^{-1} = H \quad \forall\ g \in G.$$

Hence H is a normal subgroup of G [Theorem 1.14.1.]

Example 1.14.9. *Give an example of a non-abelian group each of whose subgroup is normal.*

Solution. Consider the Quaternion group of order 8 :

$$G = \{\pm 1, \pm i, \pm j, \pm k\}\ ;\ i^2 = j^2 = k^2 = -1,$$

and $\qquad ij = -ji = k, jk = -kj = i, ki = -ik = j.$

Clearly G is non-abelian. By Lagrange's Theorem, G can have proper subgroups of orders 4 and 2 only. If H is any subgroup of G of order 4, then $i_G(H) = o(G)/o(H) = 8/4 = 2$.

Now $\quad i_G(H) = 2 \Rightarrow H \lhd G.$ [Example 1.14.6]

Thus all subgroups of G of order 4 are normal. The only subgroup of G of order 2 is $\{1, -1\}$, which is obviously normal in G.

Hence G is a non-abelian group each of whose subgroup is normal.

Example 1.14.10. *Let $H < G$ and $N(H) = \{g \in G : gHg^{-1} = H\}$.*

Prove that

(*i*) *$N(H)$ is a subgroup of G.*

(*ii*) *H is normal in $N(H)$.*

(iii) *If H is a normal subgroup of the subgroup K of G, then $K \subset N(H)$.*

(iv) *H is normal in $G \Leftrightarrow N(H) = G$.*

Solution. (i) We show that $N(H)$ is a subgroup of G.

Let $g_1, g_2 \in N(H) \Rightarrow g_1 H g_1^{-1} = H$ and $g_2 H g_2^{-1} = H$.

Now $g_2 H g_2^{-1} = H \Rightarrow g_1 g_2 H g_2^{-1} g_1^{-1} = g_1 H g_1^{-1} = H$

$\Rightarrow \quad (g_1 g_2) H (g_1 g_2)^{-1} = H.$

$\therefore g_1 g_2 \in N(H)$. Again, $g_1 H g_1^{-1} = H \Rightarrow H = g_1^{-1} H g_1$.

$\Rightarrow H = g_1^{-1} H (g_1^{-1})^{-1} \Rightarrow g_1^{-1} \in N(H) \ \forall \ g_1 \in N(H)$.

Hence $N(H)$ is a subgroup of G.

(ii) Let $g \in N(H)$ and $h \in H$. Then $gHg^{-1} = H$ and so

$ghg^{-1} \in H \ \forall \ g \in N(H)$ and $h \in H$. Hence $H \lhd N(H)$.

(iii) Let $k \in K$. Then $kH = Hk \quad [\because H \lhd K]$.

$\Rightarrow kHk^{-1} = H \Rightarrow k \in N(H)$. Hence $K \subset N(H)$.

(iv) $H \lhd G \Leftrightarrow gHg^{-1} = H \ \forall \ g \in G \Leftrightarrow G = N(H)$.

Example 1.14.11. *If N is a normal subgroup of G and H is a subgroup of G, then show that HN is a subgroup of G.*

Solution. By definition, $HN = \{hn : h \in H, n \in N\}$.

Let $x, y \in HN$ so that $x = h_1 n_1, y = h_2 n_2$ for some $h_1, h_2 \in H$ and $n_1, n_2 \in N$.

Now $\quad xy^{-1} = (h_1 n_1)(h_2 n_2)^{-1} = h_1 n_1 n_2^{-1} h_2^{-1} = h_1 n_3 h_2^{-1}, \qquad ...(1)$

where $\quad n_3 = n_1 n_2^{-1} \in N \quad (\because N < G)$.

Now $\quad n_3 h_2^{-1} \in N h_2^{-1} = h_2^{-1} N \quad (\because N \lhd G)$ and so

$n_3 h_2^{-1} = h_2^{-1} n_4$ for some $n_4 \in N$. Putting in (1), we obtain

$xy^{-1} = h_1 h_2^{-1} n_4 = (h_1 h_2^{-1}) n_4 \in HN,$

since $\quad h_1 h_2^{-1} \in H \quad (\because H < G)$ and $n_4 \in N$.

Hence $\quad xy^{-1} \in HN \Rightarrow HN$ is a subgroup of G.

Example 1.14.12. *If H and K are normal subgroups of G, then $HK = \{hk : h \in H, k \in K\}$ is a normal subgroup of G.*

Solution. $H \lhd G \Rightarrow gH = Hg \ \forall \ g \in G$. In particular,

$$kH = Hk \ \forall \ k \in K \quad (\because K \subseteq G)$$

$$\Rightarrow KH = HK \Rightarrow HK < G. \qquad \text{[Theorem 1.13.1]}$$

Now we show $HK \lhd G$. Let $g \in G$ and $a \in HK$.

Then $\quad a = hk$ for some $h \in H, k \in K$.

$\therefore gag^{-1} = ghkg^{-1} = (ghg^{-1})(gkg^{-1}). \qquad ...(1)$

Now $H \lhd G \Rightarrow ghg^{-1} \in H$ and $K \lhd G \Rightarrow gkg^{-1} \in K$. ...(2)

From (1) and (2), $gag^{-1} \in HK \ \forall\ g \in G$ and $a \in HK$.

Hence HK is a normal subgroup of G.

Example 1.14.13. *Show that a subgroup H of a group G is normal iff $Ha \neq Hb \Rightarrow aH \neq bH$.* [D.U., 1997]

Solution. Let H be a normal subgroup of G and $Ha \neq Hb$.

Let, if possible, $aH = bH$. Then

$$Ha = Hb. \qquad [\because H \lhd G]$$

This is a contradiction and so $aH \neq bH$

Conversely, let $Ha \neq Hb \Rightarrow aH \neq bH$.

Equivalently, $aH = bH \Rightarrow Ha = Hb$

or $$a^{-1}b \in H \Rightarrow ab^{-1} \in H. \qquad ...(1)$$

Let $g \in G$ and $h \in H$. We have

$$h \in H \Rightarrow h^{-1} \in H \Rightarrow g^{-1}(gh^{-1}) \in H \qquad (\because g^{-1}g = e)$$
$$\Rightarrow g(gh^{-1})^{-1} \in H, \text{ using (1)}$$
$$\Rightarrow g(h^{-1})^{-1} g^{-1} \in H$$
$$\Rightarrow g\,hg^{-1} \in H \ \forall\ g \in G, h \in H.$$

Hence H is a normal subgroup of G.

Example 1.14.14. *Let H be a non-empty subset of a group G. Show that H is a normal subgroup of G iff $(gx)(gy)^{-1} \in H \ \forall\ g \in G$ and $x, y \in H$.*

Solution. Let H be a normal subgroup of G. Let $g \in G$ and $x, y \in H$. Then

$$(gx)(gy)^{-1} = (gx)(y^{-1}g^{-1}) = g(xy^{-1})g^{-1} \qquad ...(1)$$

Since $H < G$, $xy^{-1} \in H \qquad (\because x, y \in H)$

Since $H \lhd G$, $g(xy^{-1})g^{-1} \in H$.

Using (1), $(gx)(gy)^{-1} \in H \ \forall\ g \in G$ and $x, y \in H$.

Conversely, let $(gx)(gy)^{-1} \in H \ \forall\ g \in G$ and $x, y \in H$. ...(2)

We shall prove that H is a normal subgroup of G.

Let $x, y \in H$. Taking $g = e$ in (2), we see that

$$(ex)(ey)^{-1} \in H \Rightarrow xy^{-1} \in H \Rightarrow H < G.$$

Let $g \in G$ and $h \in H$ be arbitrary. By (2), we have

$$(gh)(ge)^{-1} \in H \Rightarrow ghe^{-1}g^{-1} \in H \Rightarrow ghg^{-1} \in H \Rightarrow H \lhd G.$$

Example 1.14.15. *Show that a subgroup N of a group G is normal if and only if $xy \in N \Rightarrow yx \in N$.*

Solution. Let $N \lhd G$ and $xy \in N$ $(x, y \in G)$. By definition,

$$y(xy)y^{-1} \in N \quad \text{for } y \in G$$
$$\Rightarrow yxe \in N \Rightarrow yx \in N, \qquad ...(1)$$

Conversely, let $xy \in N \Rightarrow yx \in N$.

We have to show that $N \lhd G$. Let $g \in G$, $n \in N$.

Now $n \in N \Rightarrow g^{-1}(gn) \in N \quad (\because g^{-1}g = e)$

$\Rightarrow (gn)g^{-1} \in N$, using (1)

$\Rightarrow N \lhd G$.

Example 1.14.16. *If a cyclic subgroup T of G is normal in G, then show that every subgroup of T is normal in G.*

Solution. Let $T = \langle a \rangle$, $a \in G$ and $T \lhd G$.

Let H be any subgroup of T. We shall prove that $H \lhd G$.

Since every subgroup of a cyclic group is cyclic, H is cyclic.

Let $H = \langle a^m \rangle$. Since $H < T$ and $T < G$, $H < G$. Let $g \in G$ and $h \in H = \langle a^m \rangle$. Then

$$h = (a^m)^n = a^{mn} \text{ for some integer } n.$$

We have $ghg^{-1} = g\,a^{mn}\,g^{-1} = g\,(a^n)^m\,g^{-1} = ga_1^m\,g^{-1}$, where $a_1 = a^n \in T$

$= g\,(a_1 \cdot a_1 \ldots a_1)\,g^{-1} = (ga_1\,g^{-1})\,(ga_1g^{-1}) \ldots (ga_1g^{-1})$ (m times)

$\therefore \quad ghg^{-1} = (ga_1g^{-1})^m$, where $ga_1g^{-1} \in T. (\because T \lhd G, a_1 \in T)$

Since $ga_1g^{-1} \in T = \langle a \rangle$, $ga_1g^{-1} = a^l$ for some integer l

$\therefore \quad ghg^{-1} = (a^l)^m = a^{lm} = (a^m)^l \in H$. Hence $H \lhd G$.

Example 1.14.17. *If H is a subgroup of G and $N = \bigcap_{x \in G} x\,Hx^{-1}$, then prove that N is a normal subgroup of G.*

Solution. By Example 1.9.5,

$$xHx^{-1} = \{xhx^{-1} : h \in H\} \text{ is a subgroups of } G.$$

Since intersection of an arbitrary number of subgroups of G is a subgroup of G, N is a subgroup of G. Let $g \in G$ be arbitrary. By Example 1.12.7, if $H < G$ and $K < G$, then

$$(H \cap K)\,a = Ha \cap Ka, \text{ for } a \in G.$$

The above result can be extended to any number of subgroups of G. Consequently,

$$gNg^{-1} = g\,(\cap x\,Hx^{-1})\,g^{-1} = \cap\,(gx\,H\,x^{-1}g^{-1}) = \cap\,(gx)\,H\,(gx)^{-1}$$

or $\quad gNg^{-1} = \bigcap_{g_1 \in G} g_1\,Hg_1^{-1} = N$, $g_1 = gx \in G$.

Hence N is a normal subgroup of G.

Example 1.14.18. *Let G be a group in which, for some integer $n > 1$, $(ab)^n = a^n b^n$ for all $a, b \in G$*

Show that ...(1)

(*a*) $G^{(n)} = \{x^n : x \in G\}$ *is a normal subgroup of* G

(*b*) $G^{(n-1)} = \{x^{n-1} : x \in G\}$ *is a normal subgroup of* G

Solution. (*a*) First of all we show that $G^{(n)} < G$.

Let $\alpha, \beta \in G^{(n)}$. Then $\alpha = x^n$, $\beta = y^n$ for some $x, y \in G$.

We have to show that $N \lhd G$. Let $g \in G$, $n \in N$.

Now $n \in N \Rightarrow g^{-1}(gn) \in N \quad (\because g^{-1}g = e)$

$\Rightarrow (gn)\, g^{-1} \in N$, using (1)

$\Rightarrow N \lhd G$.

Example 1.14.16. *If a cyclic subgroup T of G is normal in G, then show that every subgroup of T is normal in G.*

Solution. Let $T = \langle a \rangle$, $a \in G$ and $T \lhd G$.

Let H be any subgroup of T. We shall prove that $H \lhd G$.

Since every subgroup of a cyclic group is cyclic, H is cyclic.

Let $H = \langle a^m \rangle$. Since $H < T$ and $T < G$, $H < G$. Let $g \in G$ and $h \in H = \langle a^m \rangle$. Then

$$h = (a^m)^n = a^{mn} \text{ for some integer } n.$$

We have $ghg^{-1} = g\, a^{mn}\, g^{-1} = g\,(a^n)^m\, g^{-1} = g a_1^m\, g^{-1}$, where $a_1 = a^n \in T$

$= g\,(a_1 \,.\, a_1 \ldots a_1)\, g^{-1} = (ga_1\, g^{-1})\,(ga_1 g^{-1}) \ldots (ga_1 g^{-1})$ (m times)

$\therefore \quad ghg^{-1} = (ga_1 g^{-1})^m$, where $ga_1 g^{-1} \in T. (\because T \lhd G, a_1 \in T)$

Since $ga_1 g^{-1} \in T = \langle a \rangle$, $ga_1 g^{-1} = a^l$ for some integer l.

$\therefore \quad ghg^{-1} = (a^l)^m = a^{lm} = (a^m)^l \in H$. Hence $H \lhd G$.

Example 1.14.17. *If H is a subgroup of G and $N = \bigcap_{x \in G} x H x^{-1}$, then prove that N is a normal subgroup of G.*

Solution. By Example 1.9.5,

$$xHx^{-1} = \{xhx^{-1} : h \in H\} \text{ is a subgroups of } G.$$

Since intersection of an arbitrary number of subgroups of G is a subgroup of G, N is a subgroup of G. Let $g \in G$ be arbitrary. By Example 1.12.7, if $H < G$ and $K < G$, then

$$(H \cap K)\, a = Ha \cap Ka, \text{ for } a \in G.$$

The above result can be extended to any number of subgroups of G. Consequently,

$$gNg^{-1} = g\,(\cap x H x^{-1})\, g^{-1} = \cap\,(gx\, H\, x^{-1} g^{-1}) = \cap\,(gx)\, H\, (gx)^{-1}$$

or $\quad gNg^{-1} = \bigcap_{g_1 \in G} g_1 H g_1^{-1} = N,\ g_1 = gx \in G.$

Hence N is a normal subgroup of G.

Example 1.14.18. *Let G be a group in which, for some integer $n > 1$, $(ab)^n = a^n b^n$ for all $a, b \in G$.* ...(1)

Show that

(*a*) $G^{(n)} = \{x^n : x \in G\}$ *is a normal subgroup of* G.

(*b*) $G^{(n-1)} = \{x^{n-1} : x \in G\}$ *is a normal subgroup of* G.

Solution. (*a*) First of all we show that $G^{(n)} < G$.

Let $\alpha, \beta \in G^{(n)}$. Then $\alpha = x^n$, $\beta = y^n$ for some $x, y \in G$.

We have to show that $N \lhd G$. Let $g \in G$, $n \in N$.

Now $n \in N \Rightarrow g^{-1}(gn) \in N \quad (\because g^{-1}g = e)$

$\Rightarrow (gn)\, g^{-1} \in N$, using (1)

$\Rightarrow N \lhd G$.

Example 1.14.16. *If a cyclic subgroup T of G is normal in G, then show that every subgroup of T is normal in G.*

Solution. Let $T = \langle a \rangle$, $a \in G$ and $T \lhd G$.

Let H be any subgroup of T. We shall prove that $H \lhd G$.

Since every subgroup of a cyclic group is cyclic, H is cyclic.

Let $H = \langle a^m \rangle$. Since $H < T$ and $T < G$, $H < G$. Let $g \in G$ and $h \in H = \langle a^m \rangle$. Then

$$h = (a^m)^n = a^{mn} \text{ for some integer } n.$$

We have $ghg^{-1} = g\, a^{mn}\, g^{-1} = g\,(a^n)^m\, g^{-1} = g a_1^m\, g^{-1}$, where $a_1 = a^n \in T$

$= g\,(a_1 \,.\, a_1 \ldots a_1)\, g^{-1} = (ga_1\, g^{-1})\,(ga_1 g^{-1}) \ldots (ga_1 g^{-1})$ (m times)

$\therefore \quad ghg^{-1} = (ga_1 g^{-1})^m$, where $ga_1 g^{-1} \in T. (\because T \lhd G, a_1 \in T)$

Since $ga_1 g^{-1} \in T = \langle a \rangle$, $ga_1 g^{-1} = a^l$ for some integer l.

$\therefore \quad ghg^{-1} = (a^l)^m = a^{lm} = (a^m)^l \in H$. Hence $H \lhd G$.

Example 1.14.17. *If H is a subgroup of G and $N = \bigcap_{x \in G} x H x^{-1}$, then prove that N is a normal subgroup of G.*

Solution. By Example 1.9.5,

$$xHx^{-1} = \{xhx^{-1} : h \in H\} \text{ is a subgroups of } G.$$

Since intersection of an arbitrary number of subgroups of G is a subgroup of G, N is a subgroup of G. Let $g \in G$ be arbitrary. By Example 1.12.7, if $H < G$ and $K < G$, then

$$(H \cap K)\, a = Ha \cap Ka, \text{ for } a \in G.$$

The above result can be extended to any number of subgroups of G. Consequently,

$$gNg^{-1} = g\,(\cap x H x^{-1})\, g^{-1} = \cap\,(gx\, H\, x^{-1} g^{-1}) = \cap\,(gx)\, H\, (gx)^{-1}$$

or $\quad gNg^{-1} = \bigcap_{g_1 \in G} g_1 H g_1^{-1} = N,\ g_1 = gx \in G.$

Hence N is a normal subgroup of G.

Example 1.14.18. *Let G be a group in which, for some integer $n > 1$, $(ab)^n = a^n b^n$ for all $a, b \in G$.* ...(1)

Show that

(*a*) $G^{(n)} = \{x^n : x \in G\}$ *is a normal subgroup of* G.

(*b*) $G^{(n-1)} = \{x^{n-1} : x \in G\}$ *is a normal subgroup of* G.

Solution. (*a*) First of all we show that $G^{(n)} < G$.

Let $\alpha, \beta \in G^{(n)}$. Then $\alpha = x^n$, $\beta = y^n$ for some $x, y \in G$.

$\Rightarrow \alpha\beta = x^n y^n = (xy)^n$, using (1).

$\Rightarrow \alpha\beta \in G^{(n)}$.

Now $\alpha^{-1} = (x^n)^{-1} = (x^{-1})^n$, where $x \in G \Rightarrow x^{-1} \in G$.

$\therefore \quad \alpha^{-1} \in G^{(n)}$. Thus $G^{(n)} < G$.

Now we show that $G^{(n)} \lhd G$.

Let $g \in G$ and $\alpha \in G^{(n)}$ so that $\alpha = x^n$, for some $x \in G$.

We have $g\,\alpha\,g^{-1} = g\,x^n\,g^{-1} = (g\,x\,g^{-1})^n$,

where $\quad g \in G$ and $x \in G \quad \Rightarrow \quad g\,x\,g^{-1} \in G$.

$\therefore \quad g\,\alpha\,g^{-1} = g_1^n$, where $g_1 = g\,x\,g^{-1} \in G$

$\Rightarrow \quad g\,\alpha\,g^{-1} \in G^{(n)}\ \forall\ g \in G, \alpha \in G^{(n)}$.

Hence $G^{(n)}$ is a normal subgroup of G.

(*b*) We first show that $(ab)^{n-1} = b^{n-1}\,a^{n-1}\ \forall\ a, b \in G$. ...(2)

From the relation $(ab)^n = a^n b^n \quad \forall\ a, b \in G$, we have

$$(ab)\,(ab)^{n-1} = a\,a^{n-1}\,b^{n-1}\,b \Rightarrow \underbrace{b\,(ab)\,(ab)\ldots(ab)}_{(n-1)\text{ times}} = a^{n-1}\,b^{n-1}\,b$$

$$\Rightarrow \underbrace{ba\,.\,ba\ldots ba}_{(n-1)\text{ times}} = a^{n-1}\,b^{n-1}$$

$\Rightarrow \quad (ba)^{n-1} = a^{n-1}\,b^{n-1} \quad \forall\ a, b \in G$.

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

Using (2) and proceeding like part (*a*), it can be shown that

$G^{(n-1)} = \{x^{n-1} : x \in G\}$ is a normal subgroup of G.

Example 1.14.19. *Let G be as in Example 1.14.18. Show that*

(*i*) $a^{n-1}\,b^n = b^n\,a^{n-1}$ *for all* $a, b \in G$.

(*ii*) $(aba^{-1}\,b^{-1})^{n(n-1)} = e$ *for all* $a, b \in G$.

Solution. (*i*) Let $M = G^{(n-1)}, N = G^{(n)}$.

Then $\quad M \lhd G$ and $N \lhd G$ and $M \cap N = (e)$.

Hence $mn = nm\ \forall\ m \in M$ and $n \in N$. ...(3) [See Example 1.14.5.]

Let $a, b \in G$ be arbitrary. Then

$a^{n-1} \in M$ and $b^n \in N$ and so by (3),

$$a^{n-1}\,b^n = b^n\,a^{n-1}\ \forall\ a, b \in G. \qquad ...(4)$$

(*ii*) For $x, y \in G$, we have

$$(xy)^{n(n-1)} = \{(xy)^n\}^{n-1} = (x^n\,y^n)^{n-1}, \text{ by (1).}$$

Using (2), we obtain

$$(xy)^{n(n-1)} = y^{n(n-1)}\,x^{n(n-1)}\ \forall\ x, y \in G. \qquad ...(5)$$

Now $(ab\,a^{-1}\,b^{-1})^{n(n-1)} = (a^{-1}\,b^{-1})^{n(n-1)}\,(ab)^{n(n-1)}$, by (5)

$$= b^{-n(n-1)} a^{-n(n-1)} b^{n(n-1)} a^{n(n-1)}, \text{ by (5)}$$
$$= b^{-n(n-1)} a^{-n(n-1)} b_1^{n-1} a_1^n ; b_1 = b^n, a_1 = a^{n-1}$$
$$= b^{-n(n-1)} a^{-n(n-1)} a_1^n b_1^{n-1}, \text{ using (4)}$$
$$= b^{-n(n-1)} a^{-n(n-1)} a^{n(n-1)} b^{n(n-1)}$$
$$= b^{-n(n-1)} . e . b^{n(n-1)} = e.$$

Hence $(ab\,a^{-1}\,b^{-1})^{n(n-1)} = e \;\; \forall\, a, b \in G.$

Example 1.14.20. *For any two real number $a, b \in \mathbf{R}$; define a mapping $f_{ab} : \mathbf{R} \to \mathbf{R}$ as*

$$f_{ab}(x) = ax + b \;\forall\, x \in \mathbf{R}. \qquad ...(1)$$

Let $G = \{f_{ab} : a \neq 0\}$. Prove that G is a group under the composition of mappings. Further show that $N = \{f_{1b} \in G\}$ is a normal subgroup of G.

Solution. Let $f_{ab}, f_{cd} \in G$; $a \neq 0, c \neq 0$. For any $x \in \mathbf{R}$, we have

$$(f_{ab} \circ f_{cd})(x) = f_{ab}(f_{cd})(x) = f_{ab}(cx + d), \text{ by (1)}$$
$$= a(cx + d) + b, \text{ by (1)}$$
$$= acx + (ad + b) = f_{ac,\, ad+b}(x), \text{ by (1).}$$

$\therefore$
$$f_{ab} \circ f_{cd} = f_{ac,\, ad+b}. \qquad ...(2)$$

This is the formula for the composition of two mappings in G.

(*i*) In view of (2), $f_{ab} \circ f_{cd} \in G$; since $ac \neq 0$.

(*ii*) Since associative law holds for all mappings, it holds in G too.

(*iii*) $f_{1,0}$ acts as the identity of G, since by (2),

$$f_{ab} \circ f_{1,0} = f_{a.1,\, a.0+b} = f_{ab} \;\; \forall\, f_{ab} \in G.$$

(*iv*) $(f_{ab})^{-1} = f_{a^{-1},\, -ba^{-1}}$,

since $f_{ab} \circ f_{a^{-1},\, -ba^{-1}} = f_{aa^{-1},\, -aba^{-1}+b} = f_{1,0}.$ ...(3)

Hence G is a group under the composition of mappings given by (2).

Now we proceed to show that $N \lhd G$.

Let $f_{1b} \in N, f_{1c} \in N$. Then

$$f_{1b} \circ f_{1c}^{-1} = f_{1b} \circ f_{1,-c}, \text{ by (3)}$$
$$= f_{1.1,\, 1.-c+b} = f_{1,\, b-c} \in N, \text{ using (2).}$$

Thus N is a subgroup of G.

Let $g = f_{ab} \in G$ and $n = f_{1c} \in N$ be arbitrary.

Then $gng^{-1} = f_{ab} \circ f_{1c} \circ f_{ab}^{-1}$
$$= (f_{a,\, ac+b}) \circ f_{a^{-1},\, -ba^{-1}}, \text{ by (2) and (3)}$$
$$= f_{aa^{-1},\, -aba^{-1}+ac+b}, \text{ by (2)}$$
$$= f_{1,\, ac} \in N.$$

Hence N is a normal subgroup of G.

Example 1.14.21. *Find a normal subgroup of S_3 and S_4.*

Solution. Refer to Section 2.4 of Chapter 2.

[Also see Examples 2.4.4 and 2.4.5]

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

Then $A_3 = \{I, (123), (132)\}$ is the normal subgroup of S_3, since

$$i(A_3) = \frac{o(S_3)}{o(A_3)} = \frac{6}{3} = 2.$$

We have $o(S_4) = 4! = 24$. Let A_4 denote the set of all even permutations of S_4 *i.e.*,

$$A_4 = \left\{ \begin{array}{l} I, (123), (124), (132), (134), (142), (143), (234), \\ \quad (243), (12)(34), (13)(24), (14)(23) \end{array} \right\}$$

Now $i(A_4) = \dfrac{o(S_4)}{o(A_4)} = \dfrac{24}{12} = 2.$

Hence A_4 is a normal subgroup of S_4.

Example 1.14.22. *Give an example of three groups $E \subset F \subset G$, where E is normal in F, F is normal in G, but E is not normal in G.*

[D.U., 1995]

Solution. We consider three subgroups of S_4 as follow :

$$E = \{I, (12)(34)\}, F = \{I, (12)(34), (13)(24), (14)(23)\},$$

$$G = \{I, (13), (24), (12)(34), (13)(24), (14)(23), (1234), (1432)\}$$

Clearly, $E \subset F \subset G$.

$$i_G(F) = \frac{o(G)}{o(F)} = \frac{8}{4} = 2 \Rightarrow F \lhd G,$$

$$i_F(E) = \frac{o(F)}{o(E)} = \frac{4}{2} = 2 \Rightarrow E \lhd F.$$

However, E is not normal in G as shown below :

Let $g = (1234) \in G$ and $n = (12)(34) \in E$. Then

$$gng^{-1} = (1234)(12)(34)(4321) = (14)(23) \notin E.$$

Example 1.14.23. *Show that the cyclic subgroup of S_3 generated by (12) is not normal in S_3.*

Solution. Let $H = \langle (12) \rangle = \{(12), (12)^2 = I\}$

For $(123) \in S_3$ and $(12) \in H$, we observe that

$$(123)(12)(123)^{-1} = (13)(123)^{-1} = (13)(321) = (23) \notin H.$$

Hence H is not a normal subgroup of S_3.

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 $\frac{G}{N}$ denote the set of all right cosets of N in G i.e., $\frac{G}{N} = \{Na : a \in G\}$.*

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. $N \lhd G \iff Na = aN \ \forall \ a \in G$. 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

$$X = Na,\ Y = Nb \text{ for some } a, b \in G. \text{ We have}$$
$$XY = NaNb = Nab = Nba, \text{ since } G \text{ is abelian}$$
$$= NbNa = YX.$$

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 $\quad G = S_3 = \{I, (12), (23), (31), (123), (132)\}$

and $\quad N = \{I, (123), (132)\}$.

Then G is a non-abelian group and N is a normal subgroup of G.

We have $\quad o\left(\frac{G}{N}\right) = \frac{o(G)}{o(N)} = \frac{6}{3} = 2.$

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 $\quad \frac{S_3}{N} = \{N, N(23)\}$, 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

$\Rightarrow \quad X = Ng = Na^m = N\,a\,.\,a \ldots a$ (m times)

$\Rightarrow \quad X = Na\,Na \ldots Na$ (m times)

$\therefore \quad X = (Na)^m, \forall\, X \in G/N.$

Hence $\dfrac{G}{N} = \langle Na \rangle$ and so $\dfrac{G}{N}$ 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 $\dfrac{G}{H}$ 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

$$a^n = e. \qquad \ldots(1)$$

Consider $(Na)^n = Na\,.\,Na \ldots Na$ (n times)

$= Na\,.\,a \ldots a$ (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 subgroup of G. Show that G/N is abelian iff $xyx^{-1}y^{-1} \in N$ for all $x, y \in G$.*

Solution. Let $X, Y \in G/N$ be arbitrary. Then

$X = Nx,\ Y = Ny$; for some $x, y \in G$.

G/N is abelian $\Leftrightarrow XY = YX$ for all $X, Y \in G/N$

$\Leftrightarrow Nx\,Ny = Ny\,Nx$ for all $x, y \in G$

$\Leftrightarrow Nxy = Nyx$ for all $x, y \in G$

$\Leftrightarrow (xy)\,(yx)^{-1} \in N$ for all $x, y \in G$.

$\Leftrightarrow xy\,x^{-1}y^{-1} \in N$ for all $x, y \in G$.

Example 1.15.2. *If H is a subgroup of a group G such that $x^2 \in H$ for all $x \in G$. Prove that G/H is abelian.*

Solution. We are given that

$$x^2 \in H \text{ for all } x \in G. \qquad \ldots(1)$$

By Example 1.14.7, H is a normal subgroup of G. Thus G/H is defined. By virtue of Example 1.15.1, G/H is abelian $\Leftrightarrow x\,y\,x^{-1}\,y^{-1} \in H$ for all $x, y \in G$.

Let $x, y \in G$ be arbitrary. Using (1), we have

$x^{-1}y \in G \Rightarrow (x^{-1}\,y)^2 \in H$. Also $x^2 \in H$ and $y^{-2} \in H$.

$\therefore\ x^2\,(x^{-1}\,y)^2\,y^{-2} \in H$, since $H < G$

or $\quad x\,x\,x^{-1}\,y\,x^{-1}\,y\,y^{-1}\,y^{-1} \in H$

or $\quad x\,y\,x^{-1}\,y^{-1} \in H\ \forall\, x, y \in G.$

Hence G/H is abelian.

Example 1.15.3. *Let G be the set of all real 2×2 matrices $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ where $ad \neq 0$, under matrix multiplication.*

Let $N = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \right\}$. Prove that

(*a*) *N is a normal subgroup of G.*

(*b*) *G/N is abelian.*

Solution. Firstly, we show that N is a subgroup of G.

Let $\quad n = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in N$ and $m = \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \in N$. Then

$$nm^{-1} = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & -c \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b-c \\ 0 & 1 \end{pmatrix} \in N.$$

Thus N is a subgroup of G.

Let $\quad g = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in G$ and $m = \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \in N$. Then

$$gmg^{-1} = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a^{-1} & -b/ad \\ 0 & d^{-1} \end{pmatrix}$$

$$= \begin{pmatrix} a & ac+b \\ 0 & d \end{pmatrix}\begin{pmatrix} a^{-1} & -b/ad \\ 0 & d^{-1} \end{pmatrix}$$

$$= \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \in N, \text{ where } \alpha = -\frac{ab}{ad} + \frac{ac+b}{d} \in \mathbf{R}.$$

Hence N is a normal subgroup of G. Now we show that G/N is abelian. Clearly

$$\frac{G}{N} \text{ is abelian } \Leftrightarrow Nx\,Ny = Ny\,Nx \;\forall\, x, y \in G$$

$$\Leftrightarrow Nxy = Nyx \;\forall\, x, y \in G$$

$$\Leftrightarrow (xy)\,(yx)^{-1} \in N \;\forall\, x, y \in G$$

$$\Leftrightarrow xyx^{-1}y^{-1} \in N \;\forall\, x, y \in G.$$

Any two elements of G are of the form

$$x = \begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix}, y = \begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix}; a_1d_1 \neq 0, a_2d_2 \neq 0.$$

Then $$x^{-1} = \begin{pmatrix} a_1^{-1} & -b_1/a_1d_1 \\ 0 & d_1^{-1} \end{pmatrix}, y^{-1} = \begin{pmatrix} a_2^{-1} & -b_2/a_2d_2 \\ 0 & d_2^{-1} \end{pmatrix}.$$

$$xy = \begin{pmatrix} a_1a_2 & a_1b_2 + b_1d_2 \\ 0 & d_1d_2 \end{pmatrix},$$

$$x^{-1}y^{-1} = \begin{pmatrix} a_1^{-1}a_2^{-1} & \dfrac{-b_2}{a_1a_2d_2} - \dfrac{b_1}{a_1d_1d_2} \\ 0 & d_1^{-1}d_2^{-1} \end{pmatrix}$$

Hence $xyx^{-1}y^{-1} = \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix} \in N,$

where $$\beta = a_1a_2\left(\frac{-b_2}{a_1a_2d_2} - \frac{b_1}{a_1d_1d_2}\right) + \frac{a_1b_2 + b_1d_2}{d_1d_2} \in \mathbf{R}.$$

It follows that G/N is abelian but G is not abelian.

Example 1.15.4. *If H is a normal subgroup of G and G is finite, then G/H is finite. Show by means of an example that the converse need not be true.*

Solution. Since G is finite, therefore G has only a finite number of distinct right cosets of H in G *i.e.*, $i_G(H)$ is finite. Hence

$$o\left(\frac{G}{H}\right) = i_G(H), \text{ which is finite.}$$

However, the converse need not be true *i.e.*, if G/H is finite, then G may be infinite.

For example, $H = \{3x : x \in \mathbf{Z}\}$ is a normal subgroup of $(\mathbf{Z}, +)$, where $\mathbf{Z}$ is infinite. However,

$$\frac{\mathbf{Z}}{H} = \{H, H+1, H+2\} \text{ is finite.}$$

Notice that

$$H = \{..., -9, -6, -3, 0, 3, 6, 9 ...\}$$
$$H + 1 = \{..., -8, -5, -2, 1, 4, 7, 10, ...\}$$
$$H + 2 = \{..., -7, -4, -1, 2, 5, 8, 11, ...\}$$
$$H + 3 = H, H + 4 = H + 1 \text{ etc.}$$

Example 1.15.5. *Let H and K be normal subgroups of a group G such that $H \subset K$, show that K/H is a normal subgroup of G/H.*

Solution. First we show that $H \lhd K$.

Since $H < G$ and $K < G$ and $H \subset K$, so $H < K$.

Let $h \in H$ and $k \in K$ $(\Rightarrow k \in G)$.

Now $H \lhd G \Rightarrow khk^{-1} \in H \quad \forall \; h \in H, k \in K \Rightarrow H \lhd K$.

Thus K/H is meaningful.

Let $X, Y \in K/H$. Then $X = Hk_1$, $Y = Hk_2$ for $k_1, k_2 \in K$. We have

$$XY^{-1} = (Hk_1)(Hk_2)^{-1} = Hk_1 Hk_2^{-1} = Hk_1k_2^{-1} \in K/H,$$
$$\text{since } K < G \Rightarrow k_1k_2^{-1} \in K.$$

Thus K/H is a subgroup of G/H.

Let $T \in G/H$ and $X \in K/H$ so that

$T = Hg$ for some $g \in G$ and $X = Hk$ for some $k \in K$.

$$\therefore \quad TXT^{-1} = Hg\,Hk\,(Hg)^{-1} = Hgk\,Hg^{-1} \qquad (\because H \lhd G)$$

or $$TXT^{-1} = Hgkg^{-1}. \qquad ...(1)$$

Since $K \lhd G$, $gkg^{-1} \in K$. Let $gkg^{-1} = k^* \in K$.

From (1), $TXT^{-1} = Hk^* \in K/H \; \forall \; T \in G/H, X \in K/H$.

Hence K/H is a normal subgroup of G/H.

Example 1.15.6. *If Z is the centre of a group G such that $\frac{G}{Z}$ is cyclic, then show that G is abelian.*

Solution. The *centre* Z of a group G is defined as

$$Z = \{z \in G : zx = xz \; \forall \; x \in G\}.$$

We know that Z is a normal subgroup of G. Since G/Z is cyclic, we may suppose that

$$\boxed{\frac{G}{Z} = \langle Za \rangle \text{ for some } a \in G.}$$

We have to show that G is abelian.

Let x, y be any two arbitrary elements of G.

Then $Zx, Zy \in G/Z = \langle Za \rangle$. It follows that

$$Zx = (Za)^m \text{ for some integer } m$$
$$= Za \,.\, Za \,...\, Za \; (m \text{ times})$$
$$= Za \,.\, a \,...\, a \; (m \text{ times}) \qquad [\because Z \lhd G]$$
$$\therefore \quad Zx = Za^m.$$

Since $\quad x = ex\ (e \in Z), x \in Zx = Za^m$.

$\therefore \quad x = z_1\, a^m$ for some $z_1 \in Z$

Similarly, $y = z_2\, a^n$ for some $z_2 \in Z$ and some integer n.

Now $xy = (z_1\, a^m)\,(z_2\, a^n) = z_1\,(a^m\, z_2)\, a^n$

$= z_1\,(z_2\, a^m)\, a^n$, as $z_2 \in Z$ and $a^m \in G$

$= (z_1\, z_2)\,(a^m\, a^n) = (z_2\, z_1)\,(a^{m+n})$

$(\because\ z_1 \in Z$ and $z_2 \in G \Rightarrow z_1 z_2 = z_2 z_1)$

$= (z_2\, z_1)\,(a^{n+m}) = (z_2\, z_1)\,(a^n\, a^m)$

$= z_2\,(z_1\, a^n)\, a^m = z_2\,(a^n\, z_1)\, a^m \qquad [\because\ z_1 \in Z$ and $a^n \in G]$

$= (z_2\, a^n)\,(z_1\, a^m) = yx.$

$\therefore \quad xy = yx\ \forall\ x, y \in G$. Hence G is abelian.

Example 1.15.7. *Show that there does not exist any non-abelian group G such that $o\,(G/Z) = 37$, where Z is the centre of G.*

Solution. Suppose there exists a non-abelian group G such that $o\,(G/Z) = 37$. Since a group of prime order is cyclic, therefore G/Z is cyclic. By Example 1.15.6, G must be abelian. This is contrary to the given hypothesis. Hence the result.

Example 1.15.8. *Let N be a normal subgroup of a finite group G such that $o\,(N)$ and $o\,(G/N)$ are co-prime. Show that N is the unique subgroup of G of order $o\,(N)$.*

Solution. Let K be any other subgroup of G such that $o\,(K) = o\,(N)$.

Since $K < G$ and $N \lhd G$, therefore $KN < G$ and $K \cap N \lhd K$.

[See Examples 1.14.4, 1.14.11]

Since $N \subset KN$ and $N \lhd G$, therefore $N \lhd KN$.

It follows that $\dfrac{KN}{N} < \dfrac{G}{N}$. [See Example 1.15.5] ...(1)

Now $\quad o\left(\dfrac{KN}{N}\right) = \dfrac{o\,(KN)}{o\,(N)} = \dfrac{o\,(K)\,o\,(N)}{o\,(K \cap N)\,o\,(N)} = \dfrac{o\,(K)}{o\,(K \cap N)}$.

$\therefore \quad o\left(\dfrac{KN}{N}\right) = \dfrac{o\,(N)}{o\,(K \cap N)}$. ...(2)

By Lagrange's Theorem,

$$o\left(\frac{KN}{N}\right) \text{ divides } o\left(\frac{G}{N}\right)$$

$$\Rightarrow \quad \frac{o\,(N)}{o\,(K \cap N)} \text{ divides } o\left(\frac{G}{N}\right), \text{ by (2)}$$

$$\Rightarrow \quad \frac{o\,(N)}{o\,(K \cap N)} = 1, \text{ since } o\,(N) \text{ and } o\left(\frac{G}{N}\right) \text{ are co-prime.}$$

$\Rightarrow \quad o(K) = o(K \cap N) \quad [\because o(N) = o(K)]$

$\Rightarrow \quad K = K \cap N \quad [\because K \cap N < K]$

$\Rightarrow \quad K = N.$

Hence N is the unique subgroup of G of order $o(N)$.

Example 1.5.9. *Let N be a normal subgroup of G of finite index and H a subgroup of G of finite order such that $[G : N]$ is relatively prime to $o(H)$. Show that $H \subseteq N$.*

Solution. Since $H < G$ and $N \lhd G$, $HN < G$ and $H \cap N \lhd H$.

Since $N \subset HN$ and $N \lhd G$, $N \lhd HN$.

It follows that $\dfrac{HN}{N} < \dfrac{G}{N}$. [See Example 1.15.5]

Now $$o\left(\frac{HN}{N}\right) = \frac{o(HN)}{o(N)} = \frac{o(H)\,o(N)}{o(H \cap N)\,o(N)} = \frac{o(H)}{o(H \cap N)}. \quad ...(1)$$

By Lagrange's Theorem,

$$o\left(\frac{HN}{N}\right) \text{ divides } o\left(\frac{G}{N}\right)$$

$$\Rightarrow \quad \frac{o(H)}{o(H \cap N)} \text{ divides } o\left(\frac{G}{N}\right), \text{ using (1)}$$

$$\Rightarrow \quad \frac{o(H)}{o(H \cap N)} = 1, \text{ since } o(H) \text{ and } o\left(\frac{G}{N}\right) = [G : N] \text{ are relatively prime}$$

$\Rightarrow \quad o(H) = o(H \cap N)$

$\Rightarrow \quad H = H \cap N \quad (\because H \cap N < H)$

Hence $\quad H \subseteq N.$

1.16 Commutator Subgroup

Definition 1. (Subgroup Generated by a Set)

Let S be a non-empty subset of a group G. The smallest subgroup of G containing S is called the **subgroup generated by S.** *It is denoted by $\langle S \rangle$ or $\hat{S}$. In other words, a subgroup H of G is said to be* **generated** *by a non-empty subset S of G, if*

(*i*) $S \subseteq H$

(*ii*) *If K is any subgroup of G such that $S \subseteq K$,* then $H \subseteq K$.

We write $\quad H = \langle S \rangle$ or $H = \hat{S}$.

Remark. *$\hat{S}$ always exists in a group G.*

Indeed $$\hat{S} = \bigcap_{\lambda \in \Delta} \{H_\lambda : H_\lambda < G \text{ and } S \subseteq H_\lambda\}$$

is the smallest subgroup of G containing S.

Theorem 1.16.1. *If S is any non-empty subset of a group G and if $H = \{\alpha \in G : \alpha = s_1 s_2 \dots s_n ; s_i \in S$ or $s_i^{-1} \in S$ for each $i\}$, n being a positive integer, then $H = \langle S \rangle$.*

Proof. Since S is non-empty, so H is non-empty. Also $S \subseteq H$.

Let $\alpha, \beta \in H$. Then

$$\alpha = s_1 s_2 \dots s_n ; s_i \text{ or } s_i^{-1} \in S \text{ for each } i$$

$$\beta = t_1 t_2 \dots t_m ; t_j \text{ or } t_j^{-1} \in S \text{ for each } j.$$

$$\therefore \quad \alpha \beta^{-1} = s_1 s_2 \dots s_n t_m^{-1} \dots t_2^{-1} t_1^{-1} \in H.$$

Thus H is a subgroup of G containing S. Let K be any subgroup of G such that $S \subseteq K$. Then for each $s \in S$, $s \in K$ and so $s^{-1} \in K$. $(\because K < G)$ ...(1)

Now we show that $H \subseteq K$.

Let $\alpha \in H$ so that $\alpha = s_1 s_2 \dots s_n$, where s_i or $s_i^{-1} \in S$ for each i. ...(2)

From (1) and (2), $\alpha \in K$. $(\because K < G)$. $\therefore$ $H \subseteq K$.

Hence H is the subgroup of G generated by S *i.e.*, $H = \langle S \rangle$.

Definition 2. (Commutator)

If x and y are any two elements of a group G, then $xyx^{-1}y^{-1}$ is called the **commutator** *of x and y.*

Remark 1. *It may be observed that inverse of a commutator is a commutator,* since

$$\alpha = xy x^{-1} y^{-1} \Rightarrow \alpha^{-1} = (xy x^{-1} y^{-1})^{-1} = (y^{-1})^{-1} (x^{-1})^{-1} y^{-1} x^{-1}.$$

$\therefore \alpha^{-1} = yxy^{-1} x^{-1}$, which is a commutator.

Definition 3. (Commutator Subgroup)

Let $S = \{xy x^{-1} y^{-1} : x, y \in G\}$ be the set of all commutators of a group G. Then the subgroup of G generated by S is called the **commutator subgroup** *of G. It is denoted by G'.* Thus $G' = \langle S \rangle$.

Remark 2. By virtue of Theorem 1.16.1, we see that

$$\alpha \in G' \Leftrightarrow \alpha = c_1 c_2 \dots c_n,$$

where c_i or $c_i^{-1} \in S$ for each i.

Since $c_i \in S$ is a commutator, therefore c_i^{-1} is also a commutator for each i [See Remark 1]. Hence

$\alpha \in G' \Leftrightarrow \alpha$ *is expressible as a product of finite number of commutators.*

Theorem 1.16.2. *Let G' be the commutator subgroup of a group G. Show that*

(*i*) *G' is a normal subgroup of G.*

(*ii*) *G/G' is abelian.*

(*iii*) *G' is the smallest subgroup of G such that G/G' is abelian.*

Or

If G/N is abelian, then $N \supset G'$.

(*iv*) *If H is a subgroup of G and $H \supset G'$, then H is normal in G.*

Proof. By definition, G' is the subgroup of G generated by the set S of all commutators of G *i.e.*, $G' = \langle S \rangle$, where $S = \{xyx^{-1}y^{-1} : x, y \in G\}$.

Let $g \in G$ and $\alpha \in G'$ be arbitrary. Then

$\alpha = c_1 c_2 \dots c_n$, where each c_i is a commutator in G. (See Remark 2)

Let $\quad c_i = x_i y_i x_i^{-1} y_i^{-1}, i = 1, 2, \dots, n \ (x_i, y_i \in G)$.

Now $\quad g \alpha g^{-1} = g (c_1 c_2 \dots c_n) g^{-1}$

or $\quad g \alpha g^{-1} = (g c_1 g^{-1})(g c_2 g^{-1}) \dots (g c_n g^{-1})$, $\quad$ ...(1)

where $\quad g c_i g^{-1} = g (x_i y_i x_i^{-1} y_i^{-1}) g^{-1}$

$$= (g x_i g^{-1})(g y_i g^{-1})(g x_i^{-1} g^{-1})(g y_i^{-1} g^{-1})$$

$$= s_i t_i s_i^{-1} t_i^{-1}, s_i = g x_i g^{-1} \in G, t_i = g y_i g^{-1} \in G.$$

Thus $g c_i g^{-1}$ is a commutator for each i.

Let $g c_i g^{-1} = d_i$ for each i, $1 \le i \le n$ and $d_i \in S$.

Substituting in (1), we get

$g \alpha g^{-1} = d_1 d_2 \dots d_n$, where each d_i is a commutator.

$\Rightarrow \quad g \alpha g^{-1} \in G'$. Hence G' is normal in G.

(*ii*) To show that G/G' is abelian.

Let $X, Y \in G/G'$. Then $X = G'x$, $Y = G'y$ for some $x, y \in G$.

Now $\quad XY = YX \Leftrightarrow G'x\, G'y = G'y\, G'x$

$$\Leftrightarrow G'xy = G'yx \qquad (\because G' \lhd G)$$

$$\Leftrightarrow (xy)(yx)^{-1} \in G'$$

$$\Leftrightarrow xyx^{-1}y^{-1} \in G', \text{ which is always true.}$$

Hence G/G' is abelian.

(*iii*) Suppose G/N is abelian. We shall prove that $G' \subset N$.

Since G/N is abelian, therefore

$$Nx\, Ny = Ny\, Nx \ \forall \ x, y \in G$$

$$\Rightarrow \quad Nxy = Nyx \quad \forall \ x, y \in G$$

$$\Rightarrow \quad (xy)(yx)^{-1} \in N \quad \forall \ x, y \in G$$

$$\Rightarrow \quad xyx^{-1}y^{-1} \in N \quad \forall \ x, y \in G. \qquad \text{...(2)}$$

Thus each commutator in G belongs to N.

Let $\alpha \in G'$ be arbitrary. Then

$$\alpha = c_1 c_2 \dots c_n \text{ where each } c_i \text{ is a commutator.} \qquad \text{...(3)}$$

From (2) and (3), $\alpha \in N$. $\quad (\because$ each $c_i \in N$ and $N < G)$

Hence $G' \subset N$.

(*iv*) We have $G' \subset H$ and $H < G$. We have to prove that H is normal in G. Let $g \in G$ and $h \in H$ be arbitrary. Then

$$ghg^{-1} = (ghg^{-1})(h^{-1}h) = (ghg^{-1}h^{-1})h. \quad \ldots(4)$$

Since $ghg^{-1}h^{-1} \in G' \subset H$, so $(ghg^{-1}h^{-1})h \in H$. By (4), we have

$$ghg^{-1} \in H \; \forall \; g \in G, h \in H.$$

Hence H is a normal subgroup of G.

Corollary. *A group G is abelian iff $G' = \{e\}$.*

Proof. G is abelian $\Leftrightarrow xy = yx \; \forall \; x, y \in G$

$\Leftrightarrow xyx^{-1}y^{-1} = e \; \forall \; x, y \in G$

$\Leftrightarrow S = \{xyx^{-1}y^{-1} : x, y \in G\} = \{e\}$

$\Leftrightarrow \langle S \rangle = \{e\}$, since the smallest subgroup of G containing $\{e\}$ is $\{e\}$.

$\Leftrightarrow G' = \{e\}$.

EXAMPLES

Example 1.16.1. *If H is a normal subgroup of G, then prove that G/H is abelian iff H contains G'.*

Solution. Let G/H be abelian. Then by Theorem 1.16.2 (*iii*),

$$H \supset G'.$$

Conversely, let $H \supset G'$ *i.e.*, $G' \subset H$. Then for all $x, y \in G$;

$$xyx^{-1}y^{-1} \in G' \Rightarrow xyx^{-1}y^{-1} \in H$$

$\Rightarrow \quad (xy)(yx)^{-1} \in H \Rightarrow Hxy = Hyx$

$\Rightarrow \quad HxHy = HyHx \; \forall \; x, y \in G$

$\Rightarrow G/H$ is abelian.

Example 1.16.2. *If H and K are subgroups of a group G, then show that*

$$H \subseteq K \Rightarrow H' \subseteq K'.$$

Solution. Let $\alpha \in H'$. Then $\alpha = c_1 c_2 \ldots c_n$, where each c_i is a commutator of the form

$$c_i = a_i b_i a_i^{-1} b_i^{-1} \; ; a_i, b_i \in H.$$

Since H is a subgroup of G, $c_i \in H$ and so $c_i \in K$ ($\because H \subseteq K$). Thus each c_i is a commutator in K and so $\alpha = c_1 c_2 \ldots c_n \in K'$.

Hence $H' \subseteq K'$.

Example 1.16.3. *If N is a normal subgroup of a group G and $N \cap G' = \{e\}$. Show that*

$$N \subseteq Z(G), \textit{ the centre of } G.$$

Solution. Let $n \in N$ and $x \in G$ be arbitrary.

Then $xnx^{-1}n^{-1} \in G'$.

Now $N \lhd G \Rightarrow x n x^{-1} \in G \Rightarrow xnx^{-1} n^{-1} \in N$

$\therefore \quad xnx^{-1} n^{-1} \in N \cap G' = \{e\}$

$\Rightarrow \quad xnx^{-1} n^{-1} = e \; \forall \; x \in G$

$\Rightarrow \quad xn = nx \; \forall \; x \in G$

$\Rightarrow \quad n \in Z(G)$, by definition of centre of G.

Hence $N \subseteq Z(G)$.

Example 1.16.4. *If G be a simple non-abelian group, then show that*

$$G = G'.$$

Solution. *A group G is called* **simple** *if its only normal subgroups are $\{e\}$ and G itself.*

Since G is non-abelian, $G' \neq \{e\}$. [See corollary of Theorem 1.16.2]

Further G' is a normal subgroup of G.

Since G is simple, where $G' \lhd G$ and $G' \neq \{e\}$, therefore

$$G' = G.$$

EXERCISES

1. Show that $H = \{1, -1\}$ is a normal subgroup of the group $G = \{1, -1, i, -i\}$. Find all the elements of G/H.
   [**Hint.** $G/H = \{H, Hi\}$.]
2. Show that $H = \{I, (123), (132)\}$ is a normal subgroup of S_3 and $K = \{I, (12)\}$ is not normal in S_3.
3. Show that the intersection of an arbitrary number of normal subgroups of a group G is a normal subgroup of G.
4. H and K are subgroups of a group G such that $H \subset K \subset G$. Prove that
   $$H \lhd G \Rightarrow H \lhd K.$$
5. Show that if H and N are subgroups of a group G and N is normal in G, then $H \cap N$ is normal in H. Show by an example that $H \cap N$ need not be normal in G.
   [**Hint.** (*i*) See Example 1.14.4 (*ii*) Consider the group G of Example 1.14.22, where
   $$N = F = \{I, (12)(34), (13)(24), (14)(23)\} \lhd G$$
   $$H = E = \{I, (12)(34)\} < G,$$
   but $\quad H \cap N = \{I, (12)(34)\}$ is not normal in G.]
6. Define a simple group and give an example of it. Is S_3 simple ?
   [**Hint.** A group G is called *simple* if its only normal subgroups are $\{e\}$ and G itself *i.e.*, a *simple* group has no proper normal subgroups. A group G of prime order is simple, since G has no proper subgroups. S_3 is not simple, since $H = \{I, (123), (132)\}$ is a proper normal subgroup of G.]

7. Show that the only abelian simple groups are groups of prime order.

Solution. Let $o(G) = p$ (p prime). Then G is cyclic and hence abelian. Further G has no proper subgroups and hence no proper normal subgroups. Consequently, G is simple. Conversely, let G be simple and abelian. Since G abelian, each subgroup of G is normal. But G being simple implies that it has no proper normal subgroups. Hence the only subgroups of G are $\{e\}$ and G and so G is finite of prime order.

8. Let $H < G$, $C(H) = \{x \in G : xh = hx \text{ for all } h \in H\}$ and

$$N(H) = \{x \in G : xHx^{-1} = H\}.$$

Show that $C(H)$ is a normal subgroup of $N(H)$.

[$C(H)$ is called the *centralizer* of H in G and $N(H)$ is called the *normalizer* of H in G]

9. Let H be a subgroup of a group G such that $x^2 \in H$ for every $x \in G$. Prove that H is normal in G and G/H is abelian.

[**Hint.** See Examples 1.14.7 and 1.15.2.]

10. Let H_1 and H_2 be two normal subgroups of a group G. Prove that

$$G/H_1 = G/H_2 \Leftrightarrow H_1 = H_2.$$

11. If the quotient group K/H is a normal subgroup of the quotient group G/H, then show that K is a normal subgroup of G such that $H \subset K$.

12. If H and K are two normal subgroups of a group G such that $o(H)$ and $o(K)$ are relatively prime, then prove that $hk = kh$ for all $h \in H$, $k \in K$.

[**Hint.** $(o(H), o(K)) = 1 \Rightarrow H \cap K = \{e\}$. Now see Example 1.14.5.]

13. If H is a normal subgroup of G such that $i_G(H) = m$, then show that $x^m \in H$ for all $x \in G$.

14. Show that a subgroup H of a group G is normal in G iff the set G/H of all its right cosets is closed under multiplication.

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 $n_1, n_2 \in \mathbf{Z}$;

$$f(n_1 + n_2) = 2^{n_1 + n_2} = 2^{n_1} . 2^{n_2} = f(n_1) . f(n_2).$$

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

$$f(x)\, e' = f(x) f(e) \quad \Rightarrow \quad e' = f(e).$$

(*ii*) We have $xx^{-1} = e = x^{-1}x$ for $x \in G$

$\Rightarrow \quad f(xx^{-1}) = f(e) = f(x^{-1}x)$.

Since f is a homomorphism, we obtain

$$f(x)f(x^{-1}) = e' = f(x^{-1})f(x) \quad [\because f(e) = e']$$

$\Rightarrow \quad [f(x)]^{-1} = f(x^{-1})$.

(*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

$\Rightarrow \quad f(x^n) = f(e)$

$\Rightarrow \quad x^n = e$, 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 ϕ 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 $Ker\,f = \{x \in G : f(x) = N, \text{ identity of } G/N\}$

$\therefore \quad x \in Ker\,f \Leftrightarrow f(x) = N \Leftrightarrow Nx = N \Leftrightarrow x \in N.$

Hence $\quad Ker\,f = N.$

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 $f(y) = e'$. ...(1)

$\therefore \quad f(xy) = f(x) f(y) = e' . e' = e' \Rightarrow xy \in K_f$.

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

$f(x k x^{-1}) = f(x) f(k) f(x^{-1})$, since f is a homomorphism

$= f(x) . e' . [f(x)]^{-1}$, since f is a homomorphism

$= f(x) [f(x)]^{-1}$, since $f(x)\, e' = f(x)$

$= e'$.

$\therefore \quad f(x k x^{-1}) = e' \Rightarrow x k x^{-1} \in K_f \quad \forall \; x \in G, k \in K_f$.

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 $\quad Ker f = \{e\}$. ...(1)

We shall prove that f is one-to-one.

Let $\quad f(x) = f(y)\ ;\ x, y \in G$

$\Rightarrow \quad f(x) [f(y)]^{-1} = f(y) [f(y)]^{-1} = e'$

$\Rightarrow \quad f(x) f(y^{-1}) = e'$, 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)

$\Rightarrow \quad x = y$.

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

$$\alpha = f(x) \text{ and } \beta = f(y), \text{ for some } x, y \in G$$

$$\Rightarrow \quad \alpha\beta^{-1} = f(x)\,[f(y)]^{-1}$$

$$= f(x)\,f(y^{-1}), \text{ since } f \text{ is a homomorphism}$$

$$= f(xy^{-1}), \text{ since } f \text{ is a homomorphism}$$

$$\in Im\, f, \text{ since } xy^{-1} \in G.$$

$$\therefore \quad \alpha\beta^{-1} \in Im\, f \text{ for all } \alpha, \beta \in Im\, f$$

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

$$\frac{G}{Ker\, f} \approx G' \quad or \quad \frac{G}{K} \approx G'. \qquad \text{[D.U., 1998, 94, 91]}$$

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

$$f: G \to G' \text{ is homomorphism and onto.}$$

$$\Rightarrow \quad f(g) \in G' \text{ for all } g \in G.$$

We define a mapping

$$\phi : \frac{G}{K} \to G' \text{ as}$$

$$\phi(Kg) = f(g)\ \forall\, g \in G. \qquad ...(2)$$

Firstly, we show that ϕ 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 ϕ is well-defined.

Next we show that ϕ is a homomorphism.

Let $X, Y \in G/K$. Then $X = Kx$, $Y = Ky$ for some $x, y \in G$. We have

$$XY = Kx\,Ky = Kxy, \text{ as } K \lhd G.$$

$$\begin{aligned} \therefore \quad \phi(XY) &= \phi(Kxy) \\ &= f(xy), \text{ by (2)} \\ &= f(x) f(y), \text{ since } f \text{ is a homomorphism} \\ &= \phi(Kx)\,\phi(Ky), \text{ by (2)} \\ &= \phi(X)\,\phi(Y). \end{aligned}$$

Thus ϕ is a homomorphism.

Now we show that ϕ 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 ϕ is one-to-one.

Lastly, we show that ϕ 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 ϕ 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

$$\frac{HK}{H} \text{ and } \frac{K}{H \cap K} \text{ are defined.}$$

We define a mapping

$$\phi : K \to \frac{HK}{H} \text{ as}$$

$$\phi(k) = Hk \quad \text{for all} \quad k \in K. \qquad ...(1)$$

It is easy to see that ϕ 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 ϕ is a homomorphism.

Let $k_1, k_2 \in K$. By (1), we have

$$\begin{aligned} \phi(k_1k_2) &= Hk_1k_2 \\ &= Hk_1\, Hk_2, \text{ as } H \lhd G \\ &= \phi(k_1)\,\phi(k_2), \text{ by (1).} \end{aligned}$$

Thus ϕ is a homomorphism.

Next we show that ϕ 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 ϕ is onto.

Since $\phi : K \to \frac{HK}{H}$ is homomorphism and onto, by Fundamental theorem of homomorphism, we have

$$\frac{K}{Ker\,\phi} \approx \frac{HK}{H}. \qquad ...(2)$$

Now $Ker\,\phi = \{x \in K : \phi(x) = H, \text{ identity of } HK/H\}$.

It follows that

$$\begin{aligned} x \in Ker\,\phi &\Leftrightarrow \phi(x) = H \text{ and } x \in K \\ &\Leftrightarrow Hx = H \text{ and } x \in K, \text{ by (1)} \\ &\Leftrightarrow x \in H \text{ and } x \in K \\ &\Leftrightarrow x \in H \cap K. \end{aligned}$$

$\therefore \quad Ker\,\phi = H \cap K.$

From (2) and (3), $\quad \frac{K}{H \cap K} \approx \frac{HK}{H}. \qquad ...(3)$

Hence $\quad \frac{HK}{H} \approx \frac{K}{H \cap K}.$

Ex. *If H and K are subgroups of a group G and K is normal in G, then*

$$\frac{HK}{K} \approx \frac{H}{H \cap K}.$$

[D.U., 1996]

Hint. Define $\phi : H \to \dfrac{HK}{K}$ as

$$\phi(h) = hK \quad \forall\ h \in H.$$

Verify that ϕ is well-defined and homomorphism. In order to show that ϕ is onto, let $X \in HK/K$. Then

$$X = gK \text{ for some } g \in HK \quad i.e.,\ g = h'k'\ (h' \in H, k' \in K).$$

$$\therefore \quad X = h'k'K = h'K \quad (\because k' \in K) \Rightarrow X = \phi(h') \Rightarrow \phi \text{ is onto.}$$

Verify that $Ker\,\phi = H \cap K$ and apply Fundamental theorem of homomorphism.

Theorem 2.2.8. *If H and K are two normal subgroups of a group G such that $H \subseteq K$, then show that*

$$\frac{G}{K} \cong \frac{G/H}{K/H}.$$ [D.U., 1990]

Proof. By the given hypotheses, the quotient groups G/H, G/K and K/H are meaningful. By virtue of Example 1.15.5 of Sec. 1.15 (Chapter 1), K/H is a normal subgroup of G/H. Thus $\dfrac{G/H}{K/H}$ is also meaningful.

We define a mapping

$$f : G/H \to G/K \quad \text{as} \quad f(Hg) = Kg,\ \forall\ g \in G. \qquad \ldots(1)$$

Then f is well-defined, since

$$Hg_1 = Hg_2 \Rightarrow g_1 g_2^{-1} \in H \Rightarrow g_1 g_2^{-1} \in K \qquad (\because H \subseteq K)$$

$$\Rightarrow \quad Kg_1 = Kg_2 \Rightarrow f(Hg_1) = f(Hg_2), \text{ by (1).}$$

Now we show that f is a homomorphism. Let $X, Y \in G/H$ so that $X = Hg_1$, $Y = Hg_2$ for some $g_1, g_2 \in G$.

Then $\quad XY = Hg_1\, Hg_2 = Hg_1 g_2 \qquad (\because H \lhd G)$

Using (1), $\quad f(XY) = Kg_1 g_2$

$$= Kg_1\, Kg_2, \text{ since } K \lhd G$$

$$= f(Hg_1) f(Hg_2), \text{ by (1)}$$

$$= f(X) f(Y).$$

Thus f is a homomorphism. Next we show that f is onto.

Let $T \in G/K$ be arbitrary so that $T = Ka$ for some $a \in G$.

Let $S = Ha$ so that $S \in G/H$. Using (1), we have

$f(S) = T$ and so f is onto. Also f is a homomorphism.

By Fundamental theorem of homomorphism, we have

$$\frac{G/H}{Ker f} \cong \frac{G}{K},$$

where $\quad Ker f = \{Hg \in G/H : f(Hg) = K, \text{ identity of } G/K\}. \qquad \ldots(2)$

Now $\quad Hg \in Ker f \Leftrightarrow f(Hg) = K$

$$\Leftrightarrow Kg = K, \text{ by (1)}$$

$$\Leftrightarrow g \in K$$

$\therefore$ $Ker f = K/H$. Putting in (2), we get

$$\frac{G/H}{K/H} \approx \frac{G}{K} \quad \text{or} \quad \frac{G}{K} \approx \frac{G/H}{K/H}.$$

EXAMPLES

Example 2.2.1. *Let $\overline{G}$ be the group of non-zero real numbers under multiplication and*

$$G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbf{R} \text{ and } ad - bc \neq 0 \right\}$$

be a group under matrix multiplication. Exhibit a homomorphism of G onto G.

Solution. Define $\phi : G \to \overline{G}$ by

$$\phi\left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right] = ad - bc. \qquad ...(1)$$

Then ϕ is well-defined, since

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G \Rightarrow ad - bc \neq 0 \Rightarrow ad - bc \in \overline{G}.$$

Let $X = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}$, $Y = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} \in G$. Using (1), we get

$$\phi(X) = a_1 d_1 - b_1 c_1, \ \phi(Y) = a_2 d_2 - b_2 c_2. \qquad ...(2)$$

Now $XY = \begin{pmatrix} a_1 a_2 + b_1 c_2 & a_1 b_2 + b_1 d_2 \\ c_1 a_2 + d_1 c_2 & c_1 b_2 + d_1 d_2 \end{pmatrix}$.

Using (1), we see that

$$\begin{aligned} \phi(XY) &= (a_1 a_2 + b_1 c_2)(c_1 b_2 + d_1 d_2) - (a_1 b_2 + b_1 d_2)(c_1 a_2 + d_1 c_2) \\ &= a_1 a_2 d_1 d_2 + b_1 c_2 c_1 b_2 - a_1 b_2 d_1 c_2 - b_1 d_2 c_1 a_2 \\ &= (a_1 d_1 - b_1 c_1)(a_2 d_2 - b_2 c_2) \\ &= \phi(X)\,\phi(Y), \text{ by (2).} \end{aligned}$$

Thus ϕ is a homomorphism.

Let $x \in \overline{G}$ be arbitrary. Since x is a non-zero real number, we can always find real numbers p, q, r, s such that

$$x = ps - qr$$

or

$$x = \phi\left[\begin{pmatrix} p & q \\ r & s \end{pmatrix}\right], \text{ where } \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in G.$$

Hence ϕ is a homomorphism of G onto $\overline{G}$.

Example 2.2.2. *Let G be any group, g a fixed element in G. Define*

$$\phi : G \to G \text{ by } \phi(x) = gxg^{-1}. \qquad ...(1)$$

Prove that ϕ is an isomorphism of G onto G. [D.U., 1990]

Solution. Let $x, y \in G$. Using (1), we have

$$\phi(xy) = gxyg^{-1} = gxeyg^{-1}$$
$$= gx(g^{-1}g)yg^{-1} = (gxg^{-1})(gyg^{-1}) = \phi(x)\phi(y)$$

$\therefore \quad \phi(xy) = \phi(x)\phi(y)$ for all $x, y \in G$.

Thus ϕ is a homomorphism.

Now $\quad \phi(x) = \phi(y) \Rightarrow gxg^{-1} = gyg^{-1} \Rightarrow x = y,$

by cancellation laws in G.

It follows that ϕ is one-to-one. Lastly, we show that ϕ is onto.

Let $y \in G$ be arbitrary. We can write

$$y = g(g^{-1}yg)g^{-1} = gy_1g^{-1}, \quad \text{where} \quad y_1 = g^{-1}yg \in G$$

or $\quad y = \phi(y_1), y_1 \in G. \quad$ [Using (1)]

This shows that ϕ is onto.

Hence ϕ is an isomorphism of G onto G.

Ex. *Prove that $\phi : G \to G$ defined by $\phi(x) = g^{-1}xg \ \forall x \in G$ ($g \in G$ is fixed) is an isomorphism of G onto G.*

Example 2.2.3. *Prove that a group G is abelian if and only if the mapping $f : G \to G$, given by $f(x) = x^2$, is a homomorphism.*

Solution. Suppose G is abelian. Then $(xy)^2 = x^2y^2 \ \forall x, y \in G$. ...(1)

We shall prove that

$$f : G \to G \text{ defined as } f(x) = x^2 \qquad ...(2)$$

is a homomorphism. Let x, y be any two elements of G. Using (2), we have

$$f(xy) = (xy)^2$$
$$= x^2y^2, \text{ using (1)}$$
$$= f(x)f(y), \text{ using (2).}$$

Thus f is a homomorphism.

Conversely, let f, given by (2), be a homomorphism.

Then $f(xy) = f(x)f(y) \ \forall x, y \in G$

$\Rightarrow \quad (xy)^2 = x^2y^2$, using (2)

$\Rightarrow \quad xyxy = xxyy \Rightarrow yx = xy \ \forall x, y \in G$, by cancellation laws in G.

Hence G is abelian.

Example 2.2.4. *Prove that a group G is abelian if and only if the mapping $f : G \to G$, given by $f(x) = x^{-1}$, is a homomorphism.*

Solution. Let $f : G \to G$, given by $f(x) = x^{-1}$, be a homomorphism. ...(1)

We shall prove that G is abelian. Let $x, y \in G$ be arbitrary. We have

$$f(xy) = f(x)f(y) \quad \text{or} \quad (xy)^{-1} = x^{-1}y^{-1}, \text{ using (1).}$$

Pre-multiplying by xy on both sides, we get

$$e = (xy)x^{-1}y^{-1} \Rightarrow ey = (xy)x^{-1} \Rightarrow yx = xy, \ \forall x, y \in G.$$

Hence G is abelian.

Conversely, let G be abelian. We shall show that

$$f : x \to x^{-1} \text{ is a homomorphism.}$$

Let $x, y \in G$ be arbitrary. Then

$$\begin{aligned} f(xy) &= (xy)^{-1} \\ &= y^{-1} x^{-1} \\ &= x^{-1} y^{-1}, \text{ since } G \text{ is abelian} \\ &= f(x) f(y) \end{aligned}$$

Hence f is a homomorphism.

Example 2.2.5. *Let G be a finite abelian group and n a positive integer relatively prime to $o(G)$. Prove that every $g \in G$ can be written as $g = x^n$ for some $x \in G$.* [D.U., 1997]

Solution. Define a mapping $\phi : G \to G$ as

$$\phi(y) = y^n \quad \text{for all} \quad y \in G. \qquad ...(1)$$

Let $x, y \in G$. By (1), we have

$$\begin{aligned} \phi(xy) &= (xy)^n \\ &= x^n y^n, \text{ since } G \text{ is abelian} \\ &= \phi(x)\, \phi(y), \text{ by (1).} \end{aligned}$$

Thus ϕ is a homomorphism.

Now we show that ϕ is one-to-one.

Let $\quad \phi(x) = \phi(y), \quad$ where $\quad x, y \in G$

$\Rightarrow \qquad x^n = y^n$, using (1)

$\Rightarrow \qquad x^n y^{-n} = e \Rightarrow (xy^{-1})^n = e$, since G is abelian.

It follows that $o(xy^{-1})$ divides n. ...(2)

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

$$o(xy^{-1}) \text{ divides } o(G). \quad \text{[Lagrange's Theorem]} \qquad ...(3)$$

From (2) and (3), $o(xy^{-1})$ divides $(n, o(G))$, where $(n, o(G))$ denotes the g.c.d. of n and $o(G)$.

Since n is relatively prime to $o(G)$,

$$(n, o(G)) = 1.$$

Thus $o(xy^{-1})$ divides 1 implies $o(xy^{-1}) = 1 \Rightarrow xy^{-1} = e \Rightarrow x = y$.

Hence $\phi(x) = \phi(y) \Rightarrow x = y$ and so ϕ is one-to-one.

Since $\phi : G \to G$ is one-to-one and G is **finite**, ϕ must be onto.

Hence ϕ is an isomorphism of G onto G.

Since $\phi : G \to G$ is onto, for each $g \in G$ there exists some $x \in G$ such that $\phi(x) = g$. Using (1), $\quad g = x^n$ for some $x \in G$.

Example 2.2.6. *Let G be a finite abelian group of order n and m a positive integer such that $(m, n) = 1$. Show that the mapping*

$$\phi : G \to G \text{ defined by } \phi(g) = g^m \ \forall\, g \in G \qquad ...(1)$$

is an isomorphism. [D.U., 1998]

Solution. Refer to Example 2.2.5. Using (1), we get

$$\phi(xy) = (xy)^m = x^m y^m = \phi(x)\,\phi(y),\ \forall\, x, y \in G.$$

[Note that G is abelian implies $(xy)^m = x^m y^m$.]

Thus ϕ is a homomorphism. Now we show that ϕ is one-to-one.

Let $\phi(x) = \phi(y)$. Then, by (1),

$$x^m = y^m \Rightarrow x^m y^{-m} = e \Rightarrow (xy^{-1})^m = e, \text{ since } G \text{ is abelian} \quad ...(1)$$

$$\Rightarrow \quad o(xy^{-1}) \mid m. \quad ...(2)$$

By Lagrange's theorem, $o(xy^{-1}) \mid o(G) = n.$ ...(3)

From (2) and (3), $o(xy^{-1}) \mid (m, n) = 1$

$\Rightarrow o(xy^{-1}) = 1 \Rightarrow xy^{-1} = e \Rightarrow x = y \Rightarrow \phi$ is one-to-one.

Hence ϕ is an isomorphism.

Ex. *Let G be a finite abelian group. Suppose $o(G)$ and n are co-prime. Show that $\phi : G \to G$ defined by $\phi(x) = x^n$ is an isomorphism.*

Hint. See Example 2.2.6.

Example 2.2.7. *Show that :*

(*i*) *Every homomorphic image of an abelian group is abelian.*

(*ii*) *Every homomorphic image of a cyclic group is cyclic.*

(*iii*) *Show, by means of an example, that the converse of each of the above results is not true.*

Solution. (*i*) Let $f : G \to G'$ be an onto homomorphism, where G is abelian. We shall prove that G' is abelian. Let $\alpha, \beta \in G'$ be arbitrary. Since f is onto, there exist $x, y \in G$ such that

$$\alpha = f(x),\ \beta = f(y)$$

$\Rightarrow \quad \alpha\beta = f(x)f(y) = f(xy)$, as f is a homomorphism

or $\quad \alpha\beta = f(yx)$, since G is abelian

$= f(y)f(x)$, since f is a homomorphism

$\therefore \quad \alpha\beta = \beta\alpha\ \forall\ \alpha, \beta \in G'$. Hence G' is abelian.

(*ii*) Let $f : G \to G'$ be an onto homomorphism, where $G = \langle a \rangle$ is cyclic. We shall show that

$$G' = \langle f(a) \rangle.$$

Let $g' \in G'$ be arbitrary. Since f is onto, there exists some $g \in G$ such that

$$f(g) = g'.$$

Now $\quad g \in G = \langle a \rangle \Rightarrow g = a^m$ for some integer m.

$\therefore \quad g' = f(g) = f(a^m) = f(a \,.\, a \ldots a)$

or $\quad g' = f(a) \,.\, f(a) \ldots f(a)$ (m times), as f is a homomorphism.

$\therefore \quad g' = [f(a)]^m$, where $g' \in G'$ is arbitrary.

Hence $\quad G' = \langle f(a) \rangle$ and so G' is cyclic.

(*iii*) Let $G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbf{R} \text{ and } ad - bc \neq 0 \right\}$.

Then G is a non-abelian group under matrix multiplication.

For example : $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$.

Let G' be the group of non-zero real numbers under multiplication. Obviously, G' is abelian.

The mapping $f : G \to G'$ defined by

$$f\left[\begin{pmatrix} a & b \\ b & d \end{pmatrix}\right] = ad - bc \text{ is an onto homomorphism.}$$

[See Example 2.2.1]

Hence G' is a homomorphic image of G, where G' is abelian but G is non-abelian.

Now we show that the converse of part (*ii*) may not be true.

The group $(\mathbf{Z}, +)$ is cyclic, since $\mathbf{Z} = \langle 1 \rangle$.

Let $G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \text{ are integers} \right\}$.

Then G is a group under matrix addition.

The mapping $f : G \to \mathbf{Z}$ defined by

$$f\left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right] = a$$

is a homomorphism, since

$$f\left[\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} + \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}\right] = f\left[\begin{pmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{pmatrix}\right] = a_1 + a_2$$

$$= f\left[\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}\right] + f\left[\begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}\right].$$

Also f is onto, since for any $x \in \mathbf{Z}$,

$$f\left[\begin{pmatrix} x & y \\ z & t \end{pmatrix}\right] = x \,;\ \begin{pmatrix} x & y \\ z & t \end{pmatrix} \in G.$$

[Here y, z, t are any integers]

Hence $\mathbf{Z}$ is a homomorphic image of G, where $\mathbf{Z}$ is cyclic but G is not cyclic.

Note. For another counterexample, see Example 2.5.8 of Sec. 2.5.

Example 2.2.8. *Let $f : G \to G'$ be a homomorphism and H a subgroup G. Show that $f(H)$ is a subgroup of G'.*

Solution. We have $f(H) = \{f(h) : h \in H\}$.

Since $e \in H, f(e) \in f(H)$ and so $f(H)$ is not-empty.

Let $x, y \in f(H)$ be arbitrary.

Then $x = f(h_1)$ and $y = f(h_2)$ for some $h_1, h_2 \in H$.

$\therefore \quad xy^{-1} = f(h_1)\{f(h_2)\}^{-1} = f(h_1)f(h_2^{-1})$, as f is a homomorphism

$= f(h_1 h_2^{-1})$, as f is a homomorphism

$\in f(H)$, since $H \leq G \Rightarrow h_1 h_2^{-1} \in H$.

Hence $f(H)$ is a subgroup of G'.

Example 2.2.9. *If N and M are normal subgroups of G, prove that*

$$\frac{NM}{M} \cong \frac{N}{N \cap M}.$$

Solution. Since N and M are normal subgroups of G, $N \cap M$ is a normal subgroup of N. Further M is a normal subgroup of NM. Thus the quotient groups NM/M and $N/N \cap M$ are defined.

We define a mapping

$$f : N \to \frac{NM}{M} \text{ as}$$

$$f(n) = nM \quad \forall \; n \in N.$$

Clearly, f is well-defined, since

$$n_1 = n_2 \Rightarrow n_1 M = n_2 M \Rightarrow f(n_1) = f(n_2).$$

Also f is a homomorphism, since for $n_1, n_2 \in N$,

$$f(n_1 n_2) = n_1 n_2 M = n_1 M \cdot n_2 M$$

$$= f(n_1) f(n_2). \qquad (\because M \trianglelefteq G)$$

Now we show that f is onto. Let $X \in NM/M$ be arbitrary. Then $X = xM$ for some $x \in NM$. Now $x \in NM \Rightarrow x = nm$ for some $n \in N$, $m \in M$.

$\therefore$

$$X = nmM = nM \qquad (\because m \in M)$$

or

$$X = f(n), \; n \in N.$$

Thus f is an onto homomorphism. By Fundamental theorem of homomorphism, we obtain

$$\frac{N}{Ker f} \cong \frac{NM}{M}.$$

where $Ker f = \{x \in N : f(x) = M, \text{ identity of } NM/M\}$ ...(1)

Now $\quad x \in Ker f \Leftrightarrow f(x) = M$ and $x \in N$

$\Leftrightarrow xM = M$ and $x \in N$

$\Leftrightarrow x \in M$ and $x \in N$

$\Leftrightarrow x \in N \cap M$.

$\therefore \quad Ker f = N \cap M$. Putting in (1), we get

$$\frac{N}{N \cap M} \cong \frac{NM}{M}.$$

Hence $\quad \dfrac{NM}{M} \cong \dfrac{N}{N \cap M}.$

Then $x = f(h_1)$ and $y = f(h_2)$ for some $h_1, h_2 \in H$.

$\therefore \quad xy^{-1} = f(h_1)\,[f(h_2)]^{-1} = f(h_1)\,f(h_2^{-1})$, as f is a homomorphism

$= f(h_1 h_2^{-1})$, as f is a homomorphism

$\in f(H)$, since $H \leq G \Rightarrow h_1 h_2^{-1} \in H$.

Hence $f(H)$ is a subgroup of G'.

Example 2.2.9. *If N and M are normal subgroups of G, prove that*

$$\frac{NM}{M} \simeq \frac{N}{N \cap M}.$$

Solution. Since N and M are normal subgroups of G, $N \cap M$ is a normal subgroup of N. Further M is a normal subgroup of NM. Thus the quotient groups NM/M and $N/N \cap M$ are defined.

We define a mapping

$$f : N \to \frac{NM}{M} \text{ as}$$

$$f(n) = nM \quad \forall \; n \in N.$$

Clearly, f is well defined, since

$$n_1 = n_2 \;\Rightarrow\; n_1 M = n_2 M \;\Rightarrow\; f(n_1) = f(n_2).$$

Also f is a homomorphism, since for $n_1, n_2 \in N$,

$$f(n_1 n_2) = n_1 n_2 M = n_1 M \cdot n_2 M \qquad (\because M \lhd G)$$

$$= f(n_1)\,f(n_2).$$

Now we show that f is onto. Let $X \in NM/M$ be arbitrary. Then $X = xM$ for some $x \in NM$. Now $x \in NM \Rightarrow x = nm$ for some $n \in N$, $m \in M$.

$$\therefore \quad X = nmM = nM \qquad (\because m \in M)$$

or $\quad X = f(n), n \in N.$

Thus f is an onto homomorphism. By Fundamental theorem of homomorphism, we obtain

$$\frac{N}{Ker f} \simeq \frac{NM}{M}, \qquad \ldots(1)$$

where $Ker f = \{x \in N : f(x) = M$, identity of $NM/M\}$

Now $\quad x \in Ker f \Leftrightarrow f(x) = M$ and $x \in N$

$\Leftrightarrow xM = M$ and $x \in N$

$\Leftrightarrow x \in M$ and $x \in N$

$\Leftrightarrow x \in N \cap M.$

$\therefore \quad Ker f = N \cap M$. Putting in (1), we get

$$\frac{N}{N \cap M} \simeq \frac{NM}{M}.$$

Hence $\quad \dfrac{NM}{M} \simeq \dfrac{N}{N \cap M}.$

Then $x = f(h_1)$ and $y = f(h_2)$ for some $h_1, h_2 \in H$.

$\therefore \quad xy^{-1} = f(h_1)\,[f(h_2)]^{-1} = f(h_1)\,f(h_2^{-1})$, as f is a homomorphism

$= f(h_1 h_2^{-1})$, as f is a homomorphism

$\in f(H)$, since $H < G \Rightarrow h_1 h_2^{-1} \in H$.

Hence $f(H)$ is a subgroup of G'.

Example 2.2.9. *If N and M are normal subgroups of G, prove that*

$$\frac{NM}{M} \approx \frac{N}{N \cap M}.$$

Solution. Since N and M are normal subgroups of G, $N \cap M$ is a normal subgroup of N. Further M is a normal subgroup of NM. Thus the quotient groups NM/M and $N/N \cap M$ are defined.

We define a mapping

$$f : N \to \frac{NM}{M} \text{ as}$$

$$f(n) = nM \quad \forall \; n \in N.$$

Clearly, f is well-defined, since

$$n_1 = n_2 \;\Rightarrow\; n_1 M = n_2 M \;\Rightarrow\; f(n_1) = f(n_2).$$

Also f is a homomorphism, since for $n_1, n_2 \in N$,

$$f(n_1 n_2) = n_1 n_2 M = n_1 M \,.\, n_2 M \qquad (\because M \lhd G)$$

$$= f(n_1)\,f(n_2).$$

Now we show that f is onto. Let $X \in NM/M$ be arbitrary. Then $X = xM$ for some $x \in NM$. Now $x \in NM \Rightarrow x = nm$ for some $n \in N$, $m \in M$.

$\therefore \quad X = nmM = nM \qquad (\because m \in M)$

or $\quad X = f(n), n \in N.$

Thus f is an onto homomorphism. By Fundamental theorem of homomorphism, we obtain

$$\frac{N}{Ker f} \approx \frac{NM}{M}, \qquad \text{...(1)}$$

where $Ker f = \{x \in N : f(x) = M, \text{ identity of } NM/M\}$

Now $\quad x \in Ker f \Leftrightarrow f(x) = M$ and $x \in N$

$\Leftrightarrow xM = M$ and $x \in N$

$\Leftrightarrow x \in M$ and $x \in N$

$\Leftrightarrow x \in N \cap M.$

$\therefore \quad Ker f = N \cap M$. Putting in (1), we get

$$\frac{N}{N \cap M} \approx \frac{NM}{M}.$$

Hence $\quad \dfrac{NM}{M} \approx \dfrac{N}{N \cap M}.$

Example 2.2.10. *For any group G, show that* $\frac{G}{(e)} \approx G$ *and* $\frac{G}{G} \approx (e)$.

Solution. (*i*) Define a mapping $I : G \to G$ as $I(x) = x$, for each $x \in G$. Then I is an onto homomorphism. By Fundamental theorem of homomorphism, we have

$$\frac{G}{Ker\, I} \approx G, \qquad ...(1)$$

where $\quad Ker\, I = \{x \in G : I(x) = e\} = \{x \in G : x = e\}$.

$\therefore \quad Ker\, I = (e)$. Putting in (1), we get

$$\frac{G}{(e)} \approx G.$$

(*ii*) Define a mapping $\quad f : G \to (e)$ as $f(x) = e \ \forall\ x \in G$.

Then f is an onto homomorphism, where

$$Ker\, f = \{x \in G : f(x) = e\} = \{x \in G : e = e\} = G.$$

Hence by Fundamental theorem of homomorphism,

$$\frac{G}{Ker\, f} \approx (e) \quad \text{or} \quad \frac{G}{G} \approx (e).$$

Example 2.2.11. *Let* **R** *be the set of real numbers. For* $a, b \in \mathbf{R}$ $(a \neq 0)$; *let* $f_{ab} : \mathbf{R} \to \mathbf{R}$ *be defined as*

$$f_{ab}(x) = ax + b. \qquad ...(1)$$

Let $G = \{f_{ab} : a, b \in \mathbf{R}$ *and* $a \neq 0\}$ *and* $N = \{f_{1b} \in G\}$. *Prove that N is a normal subgroup of G and that G/N is isomorphic to the group of non-zero real numbers under multiplication.*

Solution. Refer to Example 1.14.20 of Chapter 1. We have shown that N is a normal subgroup of G. Let $\mathbf{R}^*$ denote the group of non-zero real numbers under multiplication.

Define a mapping $\quad \phi : G \to \mathbf{R}^*$ as

$$\phi(f_{ab}) = a, \text{ for all } f_{ab} \in G. \qquad ...(1)$$

(Notice that $a \neq 0 \Rightarrow a \in \mathbf{R}^*$)

Clearly, ϕ is onto, since for any $\alpha \in \mathbf{R}^*$, $f_{\alpha\beta} \in G$ and $\phi(f_{\alpha\beta}) = \alpha$.

(Here β is any real number).

Now we show that ϕ is a homomorphism.

Let f_{ab}, f_{cd} be any two elements of G. Then

$$f_{ab} \circ f_{cd} = f_{ac,\, ad+b}. \quad \text{[See Example 1.4.20]}$$

Using (1), $\quad \phi[f_{ab} \circ f_{cd}] = ac = \phi(f_{ab})\, \phi(f_{cd})$.

Hence ϕ is an onto homomorphism. By Fundamental theorem of homomorphism,

$$\frac{G}{Ker\, \phi} \approx \mathbf{R}^*, \qquad ...(2)$$

where $\quad Ker\, \phi = \{f_{ab} \in G : \phi(f_{ab}) = 1, \text{ identity of } \mathbf{R}^*\}. \qquad ...(3)$

Let $f_{ab} \in Ker\,\phi$ be arbitrary. Then

$$\phi(f_{ab}) = 1 \Rightarrow a = 1, \text{ by (1)}$$

$$\therefore \qquad f_{ab} = f_{1b} \in N \quad \Rightarrow Ker\,\phi \subseteq N.$$

Conversely, let $f_{1c} \in N$ be arbitrary.

Using (1), $\qquad \phi(f_{1c}) = 1 \Rightarrow f_{1c} \in Ker\,\phi.$

$\therefore \quad N \subseteq Ker f$ and so $Ker\,\phi = N$. Putting in (2), we get

$$\frac{G}{N} \approx \mathbf{R}^*.$$

Example 2.2.12. *Let G be the group of non-zero complex numbers under multiplication and N the set of complex numbers of absolute value 1. Show that G/N is isomorphic to the group of all positive real numbers under multiplication.*

Solution. We have $\quad G = \{z : z \in \mathbf{C} \text{ and } z \neq 0\}$,

and $\qquad N = \{z \in \mathbf{C} : |z| = 1\}$.

Let $\mathbf{R}^+$ denote the group of all positive real numbers under multiplication.

Define a mapping $\phi : G \to \mathbf{R}^+$ as

$$\phi(a + bi) = a^2 + b^2 \text{ for all } z = a + bi \neq 0 \in G. \qquad \text{...(1)}$$

Since a and b both cannot be zero, $a^2 + b^2 > 0$.

We show that ϕ is a homomorphism. Let $z_1 = a_1 + b_1 i$, $z_2 = a_2 + b_2 i$ be any two elements of G. Then

$$z_1 z_2 = (a_1 a_2 - b_1 b_2) + (a_1 b_2 + a_2 b_1)\, i.$$

Using (1), we have

$$\phi(z_1 z_2) = (a_1 a_2 - b_1 b_2)^2 + (a_1 b_2 + a_2 b_1)^2$$

$$= a_1^2 a_2^2 + b_1^2 b_2^2 + a_1^2 b_2^2 + a_2^2 b_1^2 = (a_1^2 + b_1^2)(a_2^2 + b_2^2)$$

$$= \phi(z_1)\,\phi(z_2), \text{ by (1)}.$$

Thus ϕ is a homomorphism.

For any $\alpha \in \mathbf{R}^+$; $\alpha = \{\sqrt{\alpha}\}^2 + 0 = \phi(\sqrt{\alpha} + 0i)$, where $\sqrt{\alpha} + 0i \in G$. Thus ϕ is onto.

By Fundamental theorem of homomorphism, we have

$$\frac{G}{Ker\,\phi} \approx \mathbf{R}^+, \qquad \text{...(2)}$$

where $\qquad Ker\,\phi = \{z \in G : \phi(z) = 1, \text{ identity of } \mathbf{R}^+\}$.

Now $\qquad z = a + bi \in Ker\,\phi \Leftrightarrow a^2 + b^2 = 1 \Leftrightarrow \sqrt{a^2 + b^2} = 1.$

$\therefore \qquad z \in Ker\,\phi \Leftrightarrow |z| = 1 \Leftrightarrow z \in N.$

Thus $Ker\,\phi = N$. Putting in (2), we have

$$\frac{G}{N} \approx \mathbf{R}^+.$$

Example 2.2.13. *Let G be the group of all non-zero complex numbers under multiplication and let $\overline{G}$ be the group of all real 2×2 matrices of the form $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, where a and b are not both zero, under matrix multiplication. Show that G and $\overline{G}$ are isomorphic by exhibiting an isomorphism of G onto $\overline{G}$.* [D.U., 1993]

Solution. Define $\phi : G \to \overline{G}$ as

$$\phi(a+bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}. \qquad \ldots(1)$$

Then ϕ is well defined, since

$$a + bi = c + di \Rightarrow a = c, b = d \text{ and so}$$

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \Rightarrow \phi(a+bi) = \phi(c+di).$$

Now we show that ϕ is a homomorphism.

Let $z_1 = a + bi, z_2 = c + di \in G$. Then

$$\phi(z_1 z_2) = \phi[(ac - bd) + (ad + bc)i]$$

$$= \begin{pmatrix} ac - bd & ad + bc \\ -(ad+bc) & ac - bd \end{pmatrix}, \text{ by (1)}$$

$$= \begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \phi(z_1)\phi(z_2).$$

Thus ϕ is a homomorphism.

Now we show that ϕ is one-to-one.

Let $\phi(z_1) = \phi(z_2)$; $z_1 = a + bi, z_2 = c + di \in G$.

Using (1), $\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \Rightarrow a = c, b = d$

$\Rightarrow$ $a + bi = c + di \Rightarrow z_1 = z_2$

Thus ϕ is one-to-one.

Clearly, ϕ is onto, since for any

$$X = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in \overline{G}, \text{ we have}$$

$$\phi(z) = X, \text{ where } z = a + bi \in G.$$

Hence $G \approx \overline{G}$.

Example 2.2.14. *Let G be the group of real numbers under addition and let N be the subgroup of G consisting of all the integers. Prove that G/N is isomorphic to the group of all complex numbers of absolute value 1 under multiplication.*

Solution. Let $G^* = \{z \in \mathbf{C} : |z| = 1\}$.

Define a mapping $\phi : G \to G'$ as

$$\phi(x) = e^{2\pi i x} \ \forall\ x \in G$$

where $|e^{2\pi i x}| = |\cos 2\pi x + i \sin 2\pi x| = \sqrt{\cos^2(2\pi x) + \sin^2(2\pi x)} = 1$

Firstly, we show that ϕ is a homomorphism. Let $\alpha, \beta \in G$ be arbitrary. Using (1), we have

$$\phi(\alpha + \beta) = e^{2\pi i(\alpha+\beta)} = e^{2\pi i\alpha} \cdot e^{2\pi i\beta} = \phi(\alpha)\,\phi(\beta)$$

Thus ϕ is a homomorphism.

Now we show that ϕ is onto.

Let $z = a + ib \in G'$ be arbitrary so that $|z| = \sqrt{a^2 + b^2} = 1$.

Let $a = r\cos\theta$ and $b = r\sin\theta$ so that

$$r^2 = a^2 + b^2 = 1 \Rightarrow r = 1$$

We have $z = r(\cos\theta + i\sin\theta) = \cos\theta + i\sin\theta = e^{i\theta}$ ...(2)

Let $\beta = \dfrac{\theta}{2\pi} \in G$. Using (1), we see that

$$\phi(\beta) = e^{2\pi i\beta} = e^{i\theta} = z \text{ by (2) and } z \in G'$$

This shows that ϕ is onto.

By Fundamental theorem of homomorphism, we have

$$\frac{G}{\operatorname{Ker}\phi} \cong G', \qquad \text{...(3)}$$

where

$$\operatorname{Ker}\phi = \{x \in G : \phi(x) = 1\}.$$

We have

$$\begin{aligned} x \in \operatorname{Ker}\phi &\Leftrightarrow \phi(x) = 1 \Leftrightarrow e^{2\pi i x} = 1 \\ &\Leftrightarrow \cos 2\pi x + i\sin 2\pi x = 1 + 0i \\ &\Leftrightarrow \cos 2\pi x = 1,\ \sin 2\pi x = 0 \\ &\Leftrightarrow 2\pi x = 2\pi n + 0,\ n \text{ is an integer} \\ &\Leftrightarrow x = n,\ n \in N. \end{aligned}$$

$\therefore$ $\operatorname{Ker}\phi = N$. Putting in (3), we have

$$\frac{G}{N} \cong G'.$$

Example 2.2.15. Show that any infinite cyclic group is isomorphic to $(Z, +)$.

Solution. Let $G = \langle a \rangle$ be any infinite cyclic group. Then

$$G = \{a^n : n \in Z\}.$$

Define a mapping $f : Z \to G$ as

$$f(n) = a^n \ \forall\ n \in Z. \qquad \text{...(1)}$$

Then f is a homomorphism, since for $m, n \in Z$,

$$f(m + n) = a^{m+n} = a^m a^n = f(m)\,f(n), \text{ using (1)}.$$

Now we show that f is onto. Let $g \in G$ be arbitrary. Then

$g = a^i$ for some $i \in Z$. Using (1), we have

$f(i) = g$. Thus f is onto.

Define a mapping $\phi : G \to U^2$ as

$$\phi(\alpha) = e^{2\pi i \alpha} \ \forall \ \alpha \in G$$

where $|e^{2\pi i \alpha}| = |\cos 2\pi\alpha + i \sin 2\pi\alpha| = \sqrt{\cos^2(2\pi\alpha) + \sin^2(2\pi\alpha)} = 1$

Firstly, we show that ϕ is a homomorphism. Let $\alpha, \beta \in G$ be arbitrary. Using (1), we have

$$\phi(\alpha + \beta) = e^{2\pi i(\alpha+\beta)} = e^{2\pi i\alpha} \cdot e^{2\pi i\beta} = \phi(\alpha)\,\phi(\beta)$$

Thus ϕ is a homomorphism.

Now we show that ϕ is onto.

Let $z = a + bi \in U^2$ be arbitrary so that $|z| = \sqrt{a^2 + b^2} = 1$

Let $a = r\cos\theta$ and $b = r\sin\theta$ so that

$$r^2 = a^2 + b^2 = 1 \Rightarrow r = 1$$

We have $z = r(\cos\theta + i\sin\theta) = \cos\theta + i\sin\theta = e^{i\theta}$ ... (1)

Let $\beta = \dfrac{\theta}{2\pi} \in G$. Using (1), we see that

$$\phi(\beta) = e^{2\pi i\beta} = e^{i\theta} = z \text{ by (1) and } z \in U^2.$$

This shows that ϕ is onto.

By Fundamental theorem of homomorphism, we have

$$\frac{G}{\operatorname{Ker}\phi} \cong U^2, \qquad \text{... (3)}$$

where $\operatorname{Ker}\phi = \{\alpha \in G : \phi(\alpha) = 1\}$.

We have $\alpha \in \operatorname{Ker}\phi \Leftrightarrow \phi(\alpha) = 1 \Leftrightarrow (e^{2\pi i\alpha} = 1)$

$\Leftrightarrow \cos 2\pi\alpha + i\sin 2\pi\alpha = 1 + 0i$

$\Leftrightarrow \cos 2\pi\alpha = 1, \sin 2\pi\alpha = 0$

$\Leftrightarrow 2\pi\alpha = 2n\pi \pm 0$, n is an integer

$\Leftrightarrow \alpha = n, n \in N$

$\therefore \operatorname{Ker}\phi = N$. Putting in (3), we have

$$\frac{G}{N} \cong U^2$$

Example 2.2.15. *Show that any infinite cyclic group is isomorphic to $(Z, +)$.*

Solution. Let $G = (a)$ be any infinite cyclic group. Then

$$G = \{a^n : n \in Z\}.$$

Define a mapping $f : Z \to G$ as

$$f(n) = a^n \quad \forall \ n \in Z. \qquad \text{... (1)}$$

Then f is a homomorphism, since for $m, n \in Z$,

$$f(m + n) = a^{m+n} = a^m a^n = f(m) f(n), \text{ using (1).}$$

Now we show that f is onto. Let $g \in G$ be arbitrary. Then

$g = a^t$ for some $t \in Z$. Using (1), we have

$f(t) = g$. Thus f is onto.

Define a mapping $\phi : G \to G^*$ as

$$\phi(\alpha) = e^{2\pi i \alpha} \ \forall \ \alpha \in G, \qquad \ldots(1)$$

where $|e^{2\pi i \alpha}| = |\cos 2\pi\alpha + i \sin 2\pi\alpha| = \sqrt{\cos^2(2\pi\alpha) + \sin^2(2\pi\alpha)} = 1$

Firstly, we show that ϕ is a homomorphism. Let $\alpha, \beta \in G$ be arbitrary. Using (1), we have

$$\phi(\alpha + \beta) = e^{2\pi i(\alpha+\beta)} = e^{2\pi i \alpha} \cdot e^{2\pi i \beta} = \phi(\alpha)\,\phi(\beta).$$

Thus ϕ is a homomorphism.

Now we show that ϕ is onto.

Let $z = a + bi \in G^*$ be arbitrary so that $|z| = \sqrt{a^2 + b^2} = 1$.

Let $a = r\cos\theta$ and $b = r\sin\theta$ so that

$$r^2 = a^2 + b^2 = \Rightarrow r = 1.$$

We have $z = r(\cos\theta + i\sin\theta) = \cos\theta + i\sin\theta = e^{i\theta}$. ...(2)

Let $\beta = \dfrac{\theta}{2\pi} \in G$. Using (1), we see that

$$\phi(\beta) = e^{2\pi i \beta} = e^{i\theta} = z \text{ by (2) and } z \in G^*.$$

This shows that ϕ is onto.

By Fundamental theorem of homomorphism, we have

$$\frac{G}{Ker\,\phi} \approx G^*, \qquad \ldots(3)$$

where $Ker\,\phi = \{\alpha \in G : \phi(\alpha) = 1\}$.

We have
$$\begin{aligned}
\alpha \in Ker\,\phi &\Leftrightarrow \phi(\alpha) = 1 \Leftrightarrow e^{2\pi i \alpha} = 1 \\
&\Leftrightarrow \cos 2\pi\alpha + i \sin 2\pi\alpha = 1 + 0i \\
&\Leftrightarrow \cos 2\pi\alpha = 1, \sin 2\pi\alpha = 0 \\
&\Leftrightarrow 2\pi\alpha = 2\pi n \pm 0, \ n \text{ is an integer} \\
&\Leftrightarrow \alpha = n, \ n \in N.
\end{aligned}$$

$\therefore$ $Ker\,\phi = N$. Putting in (3), we have

$$\frac{G}{N} \approx G^*.$$

Example 2.2.15. *Show that any infinite cyclic group is isomorphic to* $(\mathbf{Z}, +)$.

Solution. Let $G = \langle a \rangle$ be any infinite cyclic group. Then

$$G = \{a^n : n \in \mathbf{Z}\}.$$

Define a mapping $f : \mathbf{Z} \to G$ as

$$f(n) = a^n \quad \forall \ n \in \mathbf{Z}. \qquad \ldots(1)$$

Then f is a homomorphism, since for $m, n \in \mathbf{Z}$,

$$f(m+n) = a^{m+n} = a^m a^n = f(m) f(n), \text{ using (1).}$$

Now we show that f is onto. Let $g \in G$ be arbitrary. Then

$g = a^i$ for some $i \in \mathbf{Z}$. Using (1), we have

$f(i) = g$. Thus f is onto.

Lastly we show that f is one-to-one. Let $m, n \in \mathbf{Z}$. Then

$$f(m) = f(n) \Rightarrow a^m = a^n \Rightarrow a^{m-n} = e \Rightarrow m - n = 0, \text{ since } G \text{ is infinite.}$$

Thus $m = n$ and so f is one-to-one.

(Notice that $m - n \neq 0$ implies that G is a finite cyclic group, which is contrary to the given hypothesis).

Hence $\qquad \mathbf{Z} \approx G \quad \text{or} \quad G \approx \mathbf{Z}.$

Example 2.2.16. *Show that a finite cyclic group of order n is isomorphic to* $\mathbf{Z}_n$, *the group of integers modulo n.*

Solution. Let $G = \langle a \rangle = \{a, a^2, \ldots a^{n-1}, a^n = e\}$ be a cyclic group of order n. We know

$$\mathbf{Z}_n = \{\, \bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1} \,\}.$$

The mapping $f: \mathbf{Z}_n \to G$ defined by

$$f(\bar{i}) = a^i \quad \text{for } i = 0, 1, 2, \ldots, n-1$$

is obviously one-to-one and onto.

Also f is a homomorphism, since

$$f(\bar{i} + \bar{j}) = f(\overline{i+j}) = a^{i+j} = a^i a^j = f(\bar{i}) f(\bar{j}).$$

Hence $\qquad \mathbf{Z}_n \approx G \quad \text{or} \quad G \approx \mathbf{Z}_n.$

Example 2.2.17. *Show that a finite cyclic group of order n is isomorphic to the multiplicative group of n nth roots of unity.*

Solution. Let $G = \langle a \rangle = \{a, a^2, \ldots, a^{n-1}, a^n = e\}$ be a cyclic group of order n. The group of n nth roots of unity is

$$\overline{G} = \{\rho, \rho^2, \ldots, \rho^{n-1}, \rho^n = 1\}, \; \rho = e^{2\pi i/n}.$$

The mapping $f: G \to \overline{G}$ defined by

$$f(a^i) = \rho^i \quad \text{for } i = 1, 2, \ldots, n$$

is clearly one-to-one, onto and homomorphism. Hence $G \approx \overline{G}$.

Example 2.2.18. *Show that any two cyclic groups of the same order are isomorphic.*

Solution. Let G_1 and G_2 be two cyclic groups of the same order. If G_1 and G_2 are both infinite, then

$$G_1 \approx (\mathbf{Z}, +) \text{ and } G_2 \approx (\mathbf{Z}, +) \qquad \text{[Example 2.2.15]}$$

or

$$G_1 \approx (\mathbf{Z}, +) \text{ and } (\mathbf{Z}, +) \approx G_2.$$

Hence $\qquad G_1 \approx G_2.$

Suppose $\qquad o(G_1) = o(G_2) = n$. Then

$$G_1 \approx (\mathbf{Z}_n, +) \text{ and } G_2 \approx (\mathbf{Z}_n, +) \qquad \text{[Example 2.2.16]}$$

or

$$G_1 \approx (\mathbf{Z}_n, +) \text{ and } (\mathbf{Z}_n, +) \approx G_2.$$

Hence $\qquad G_1 \approx G_2.$

Example 3.3.19. *Show that a finite cyclic group of order n is homomorphic to the quotient group $\mathbb{Z}/N$, where $N = \{nx : x \in \mathbb{Z}\} = (n)$.*

Solution. Let $G = \{a, a^2, \ldots, a^{n-1}, a^n = e\}$ be a cyclic group of order n.

Define a mapping $f : \mathbb{Z} \to G$ as

$$f(i) = a^i, \; i = 1, 2, \ldots, n$$

Then f is a homomorphism, since for $i \geq 1$, $j \geq 1$,

$$f(i+j) = a^{i+j} = a^i a^j = f(i) f(j)$$

Clearly, f is onto. By Fundamental theorem of homomorphism,

$$\frac{\mathbb{Z}}{\ker f} \cong G \qquad (1)$$

where $\ker f = \{x \in \mathbb{Z} : f(x) = e\}$

Now
$$\begin{aligned} x \in \ker f &\Leftrightarrow f(x) = e \\ &\Leftrightarrow a^x = e \\ &\Leftrightarrow n \mid (x - 1) \\ &\Leftrightarrow n \mid x \\ &\Leftrightarrow x = nx, \text{ for } x \in \mathbb{Z} \\ &\Leftrightarrow x \in N. \end{aligned}$$

$\ker f = N$. Putting in (1), we get

$$\frac{\mathbb{Z}}{N} \cong G \quad \text{or} \quad G \cong \frac{\mathbb{Z}}{N}.$$

Example 3.3.20. *Show that the relation $\cong$ of isomorphism in groups is an equivalence relation.*

Solution. **Reflexive.** Let G be any group. Then $G \cong G$, since the identity mapping $I : G \to G$ defined as $I(x) = x$ for all $x \in G$ is one to one, onto and homomorphism.

Symmetric. Let G_1 and G_2 be two groups such that $G_1 \cong G_2$, then there exists a mapping $f : G_1 \to G_2$ such that f is one to one, onto and homomorphism. Since f is one to one and onto, the inverse mapping $f^{-1} : G_2 \to G_1$ exists and is one to one and onto. Now we show that f^{-1} is a homomorphism. Let $a', b' \in G_2$ be arbitrary. Then there exist unique elements $a, b \in G_1$ such that

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

and
$$f^{-1}(b') = b \Rightarrow f(b) = b'.$$

Now
$$\begin{aligned} f^{-1}(a'b') &= f^{-1}[f(a) f(b)] \\ &= f^{-1}[f(ab)], \text{ since } f \text{ is a homomorphism} \\ &= (f^{-1} \circ f)(ab) = I(ab) = ab \\ &= f^{-1}(a') f^{-1}(b'). \end{aligned}$$

Thus f^{-1} is a homomorphism and so $G_2 \cong G_1$.

Example 4.4.10 *Show that a finite group G is the group of order N if and only if there is the natural group H of order N such that $G \cong H$.*

Solution Let $H = \{1, a, a^2, \ldots, a^{N-1}\}$ be the group of order N.

Define a mapping $f : G \to H$ as

$$f(1) = a^0, \quad f(a) = a^1, \quad f(a^2) = a^2, \ldots, f(a^{N-1}) = a^{N-1}$$

Then f is a homomorphism since $f(1) = a^0 = 1$ and

$$f(1 \cdot a) = a^{1+1} = a^1 a^1 = f(1) f(a)$$

Clearly f is onto. By Fundamental theorem of homomorphism,

$$G/\ker f \cong H$$

where

$$\ker f = \{x \in G : f(x) = e\}$$

Thus

$$\begin{aligned} x \in \ker f &\Leftrightarrow f(x) = e \\ &\Leftrightarrow a^x = e \\ &\Leftrightarrow a(a(a(\ldots)) \\ &\Leftrightarrow a(1) \\ &\Leftrightarrow x = a(1) \text{ for } x \in G \\ &\Leftrightarrow x \in H \end{aligned}$$

$\ker f = H$. Putting in (1), we get

$$\frac{G}{H} \cong G \quad \text{or} \quad G \cong \frac{G}{H}.$$

Example 4.4.11 *Show that the relation $\cong$ of isomorphism in groups is an equivalence relation.*

Solution. Reflexive. Let G be any group. Then $G \cong G$, since the identity mapping $I : G \to G$ defined as $I(x) = x$ for all $x \in G$ is one to one, onto and homomorphism.

Symmetric. Let G_1 and G_2 be two groups such that $G_1 \cong G_2$, then there exists a mapping $f : G_1 \to G_2$ such that f is one to one, onto and homomorphism. Since f is one to one and onto, the inverse mapping $f^{-1} : G_2 \to G_1$ exists and is one to one and onto. Now we show that f^{-1} is a homomorphism. Let $a', b' \in G_2$ be arbitrary. Then there exist unique elements $a, b \in G_1$ such that

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

and

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

Now

$$\begin{aligned} f^{-1}(a'b') &= f^{-1}[f(a) f(b)] \\ &= f^{-1}[f(ab)], \text{ since } f \text{ is a homomorphism} \\ &= (f^{-1} \circ f)(ab) = I(ab) = ab \\ &= f^{-1}(a') f^{-1}(b') \end{aligned}$$

Thus f^{-1} is a homomorphism and so $G_2 \cong G_1$.

Example 2.2.19. *Show that a finite cyclic group of order n is isomorphic to the quotient group $\mathbb{Z}/N$ where $N = \{nx : x \in \mathbb{Z}\} = \langle n \rangle$*

Solution. Let $G = \langle a \rangle = \{a, a^2, \ldots, a^{n-1}, a^n = e\}$ be a cyclic group order n.

Define a mapping $f : \mathbb{Z} \to G$ as

$$f(i) = a^i, \; i = 1, 2, \ldots, n.$$

Then f is a homomorphism, since for $1 \le i, j \le n$,

$$f(i+j) = a^{i+j} = a^i a^j = f(i) f(j).$$

Clearly, f is onto. By Fundamental theorem of homomorphism,

$$\frac{\mathbb{Z}}{\mathrm{Ker}\, f} \approx G,$$

where $\mathrm{Ker}\, f = \{i \in \mathbb{Z} : f(i) = e\}$.

Now $i \in \mathrm{Ker}\, f \Leftrightarrow f(i) = e$

$\Leftrightarrow a^i = e$

$\Leftrightarrow o(a) \mid i$

$\Leftrightarrow n \mid i$

$\Leftrightarrow i = nx$, for $x \in \mathbb{Z}$

$\Leftrightarrow i \in N$.

$\therefore$ $\mathrm{Ker}\, f = N$. Putting in (1), we get

$$\frac{\mathbb{Z}}{N} \approx G \quad \text{or} \quad G \approx \frac{\mathbb{Z}}{N}.$$

Example 2.2.20. *Show that the relation $\approx$ of isomorphism in groups is an equivalence relation.*

Solution. **Reflexive.** Let G be any group. Then $G \approx G$, since the identity mapping $I : G \to G$ defined as $I(x) = x$ for all $x \in G$ is one-to-one, onto and homomorphism.

Symmetric. Let G_1 and G_2 be two groups such that $G_1 \approx G_2$, then there exists a mapping $f : G_1 \to G_2$ such that f is one-to-one, onto and homomorphism. Since f is one-to-one and onto, the inverse mapping $f^{-1} : G_2 \to G_1$ exists and is one-to-one and onto. Now we show that f^{-1} is a homomorphism. Let $a', b' \in G_2$ be arbitrary. Then there exist unique elements $a, b \in G_1$ such that

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

and

$$f^{-1}(b') = b \Rightarrow f(b) = b'.$$

Now

$$\begin{aligned} f^{-1}(a'b') &= f^{-1}[f(a) f(b)] \\ &= f^{-1}[f(ab)], \text{ since } f \text{ is a homomorphism} \\ &= (f^{-1} \circ f)(ab) = I(ab) = ab \\ &= f^{-1}(a') f^{-1}(b'). \end{aligned}$$

Thus f^{-1} is a homomorphism and so $G_2 \approx G_1$.

Example 2.2.19. *Show that a finite cyclic group of order n is isomorphic to the quotient group Z/N, where $N = \{nx : x \in Z\} = (n)$.*

Solution. Let $G = (a) = \{a, a^2, \ldots, a^{n-1}, a^n = e\}$ be a cyclic group of order n.

Define a mapping $\quad f : Z \to G$ as

$$f(i) = a^i, \; i = 1, 2, \ldots, n.$$

Then f is a homomorphism, since for $1 \le i, j \le n$,

$$f(i + j) = a^{i+j} = a^i a^j = f(i) f(j).$$

Clearly, f is onto. By Fundamental theorem of homomorphism,

$$\frac{Z}{Ker\, f} \approx G \quad (1)$$

where $\quad Ker\, f = \{i \in Z : f(i) = e\}$.

Now
$$\begin{aligned} i \in Ker\, f &\leftrightarrow f(i) = e \\ &\leftrightarrow a^i = e \\ &\leftrightarrow o(a) \mid i \\ &\leftrightarrow n \mid i \\ &\leftrightarrow i = nx, \text{ for } x \in Z \\ &\leftrightarrow i \in N. \end{aligned}$$

$\therefore \quad Ker\, f = N$. Putting in (1), we get

$$\frac{Z}{N} \approx G \quad \text{or} \quad G \approx \frac{Z}{N}.$$

Example 2.2.20. *Show that the relation $\approx$ of isomorphism in groups is an equivalence relation.*

Solution. Reflexive. Let G be any group. Then $G \approx G$, since the identity mapping $I : G \to G$ defined as $I(x) = x$ for all $x \in G$ is one-to-one, onto and homomorphism.

Symmetric. Let G_1 and G_2 be two groups such that $G_1 \approx G_2$, then there exists a mapping $f : G_1 \to G_2$ such that f is one-to-one, onto and homomorphism. Since f is one-to-one and onto, the inverse mapping $f^{-1} : G_2 \to G_1$ exists and is one-to-one and onto. Now we show that f^{-1} is a homomorphism. Let $a', b' \in G_2$ be arbitrary. Then there exist unique elements $a, b \in G_1$ such that

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

and
$$f^{-1}(b') = b \Rightarrow f(b) = b'.$$

Now
$$\begin{aligned} f^{-1}(a'b') &= f^{-1}[f(a) f(b)] \\ &= f^{-1}[f(ab)], \text{ since } f \text{ is a homomorphism} \\ &= (f^{-1} o f)(ab) = I(ab) = ab \\ &= f^{-1}(a') f^{-1}(b'). \end{aligned}$$

Thus f^{-1} is a homomorphism and so $G_2 \approx G_1$.

$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}$

Example 2.2.19. *Show that a finite cyclic group of order n is isomo*
phic to the quotient group $\mathbf{Z}/N$, *where* $N = \{nx : x \in \mathbf{Z}\} = \langle n \rangle$.

Solution. Let $G = \langle a \rangle = \{a, a^2, \ldots, a^{n-1}, a^n = e\}$ be a cyclic group o
order n.

Define a mapping $f : \mathbf{Z} \to G$ as

$$f(i) = a^i, i = 1, 2, \ldots, n.$$

Then f is a homomorphism, since for $1 \le i, j \le n$,

$$f(i+j) = a^{i+j} = a^i a^j = f(i) f(j).$$

Clearly, f is onto. By Fundamental theorem of homomorphism,

$$\frac{\mathbf{Z}}{Kerf} \approx G; \quad \ldots(1)$$

where $Kerf = \{i \in \mathbf{Z} : f(i) = e\}$.

Now
$$\begin{aligned} i \in Kerf &\Leftrightarrow f(i) = e \\ &\Leftrightarrow a^i = e \\ &\Leftrightarrow o(a) \mid i \\ &\Leftrightarrow n \mid i \\ &\Leftrightarrow i = nx, \text{ for } x \in \mathbf{Z} \\ &\Leftrightarrow i \in N. \end{aligned}$$

$i = e$

$o(a) \mid i$

$n \mid i$

$i = nx$

$\therefore$ $Kerf = N$. Putting in (1), we get

$$\frac{\mathbf{Z}}{N} \approx G \quad \text{or} \quad G \approx \frac{\mathbf{Z}}{N}.$$

Example 2.2.20. *Show that the relation* $\approx$ *of isomorphism in groups is an equivalence relation.*

Solution. Reflexive. Let G be any group. Then $G \approx G$, since the identity mapping $I : G \to G$ defined as $I(x) = x$ for all $x \in G$ is one-to-one, onto and homomorphism.

Symmetric. Let G_1 and G_2 be two groups such that $G_1 \approx G_2$. then there exists a mapping $f : G_1 \to G_2$ such that f is one-to-one, onto and homomorphism. Since f is one-to-one and onto, the inverse mapping $f^{-1} : G_2 \to G_1$ exists and is one-to-one and onto. Now we show that f^{-1} is a homomorphism. Let $a', b' \in G_2$ be arbitrary. Then there exist unique elements $a, b \in G_1$ such that

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

and
$$f^{-1}(b') = b \Rightarrow f(b) = b'.$$

Now
$$\begin{aligned} f^{-1}(a'b') &= f^{-1}[f(a) f(b)] \\ &= f^{-1}[f(ab)], \text{ since } f \text{ is a homomorphism} \\ &= (f^{-1} o f)(ab) = I(ab) = ab \\ &= f^{-1}(a') f^{-1}(b'). \end{aligned}$$

Thus f^{-1} is a homomorphism and so $G_2 \approx G_1$.

Transitive. Let G_1, G_2, G_3 be three groups such that $G_1 \approx G_2$ and $G_2 \approx G_3$. Then there exist two mappings $f : G_1 \to G_2$ and $g : G_2 \to G_3$ such that each is one-to-one, onto and homomorphism. Clearly, the mapping $g \circ f : G_1 \to G_3$ is one-to-one and onto. Now we show that $g \circ f$ is a homomorphism. Let $a, b \in G_1$ be arbitrary. Then

$$(g \circ f)(ab) = g[f(ab)], \text{ by definition of product}$$
$$= g[f(a) f(b)], \text{ since } f \text{ is a homomorphism}$$
$$= g(f(a)\, g(f(b))), \text{ since } g \text{ is a homomorphism}$$
$$(\text{Here } f(a), f(b) \in G_2)$$
$$= (g \circ f)(a)\,(g \circ f)(b), \text{ by definition of product}$$

Thus $g \circ f$ is a homomorphism and so $G_1 \approx G_3$. Hence the relation $\approx$ of isomorphism in groups is an equivalence relation.

Example 2.2.21. (Dihedral Group) Important

Let G be the dihedral group defined as

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

Prove

(*a*) *The subgroup $N = \{e, y, y^2, \ldots, y^{n-1}\}$ is normal in G.*

(*b*) *$G/N \approx W$, where $W = \{1, -1\}$ is the group under the multiplication of the real numbers.* [D.U., 1995]

Solution. The group G can be written as

$$G = \{x, y^2, \ldots, y^{n-1}, y^n = e, x, xy, xy^2, \ldots, xy^n\},$$

where $x^2 = e, y^n = e, xy = y^{-1}x.$

Then $o(G) = 2n.$

We write $G = D_{2n}.$

It may be observed that

$$xy = y^{-1}x \Rightarrow xyx^{-1} = y^{-1} \Rightarrow (xyx^{-1})^i = y^{-i}$$

$$\Rightarrow \quad xy^i x^{-1} = y^{-i} \Rightarrow y^i x y^i = x \ (i \in \mathbf{N}). \qquad \ldots(1)$$

(*a*) We proceed to show that N is normal in G.

Since $N = \langle y \rangle, y^n = e$; N is a subgroup of G.

Let $g \in G$ and $y^i \in N, i = 1, 2, \ldots, n.$

Now $g \in G \Rightarrow g = y^j$ or $xy^j, j = 1, 2, \ldots, n.$

If $g = y^j$, then $g y^i g^{-1} = y^j y^i y^{-j} = y^i \in N.$

If $g = xy^j$, then $g y^i g^{-1} = xy^j y^i y^{-j} x^{-1} = xy^i x^{-1} = y^{-i}$, by (1)

$\therefore \quad g y^i g^{-1} = y^{-i} \in N$, since $N < G$.

Hence N is a normal subgroup of G.

Transitive. Let G_1, G_2, G_3 be three groups such that $G_1 \approx G_2$ and $G_2 \approx G_3$. Then there exist two mappings $f : G_1 \to G_2$ and $g : G_2 \to G_3$ such that each is one-to-one, onto and homomorphism. Clearly, the mapping $g \circ f : G_1 \to G_3$ is one-to-one and onto. Now we show that $g \circ f$ is a homomorphism. Let $a, b \in G_1$ be arbitrary. Then

$$(g \circ f)(ab) = g[f(ab)], \text{ by definition of product}$$
$$= g[f(a) f(b)], \text{ since } f \text{ is a homomorphism}$$
$$= g(f(a)\, g(f(b))), \text{ since } g \text{ is a homomorphism}$$
$$(\text{Here } f(a), f(b) \in G_2)$$
$$= (g \circ f)(a)\,(g \circ f)(b), \text{ by definition of product}$$

Thus $g \circ f$ is a homomorphism and so $G_1 \approx G_3$. Hence the relation $\approx$ of isomorphism in groups is an equivalence relation.

Example 2.2.21. (Dihedral Group) Important

Let G be the dihedral group defined as

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

Prove

(*a*) *The subgroup $N = \{e, y, y^2, \ldots, y^{n-1}\}$ is normal in G.*

(*b*) *$G/N \approx W$, where $W = \{1, -1\}$ is the group under the multiplication of the real numbers.* [D.U., 1995]

Solution. The group G can be written as

$$G = \{x, y^2, \ldots, y^{n-1}, y^n = e, x, xy, xy^2, \ldots, xy^n\},$$

where $x^2 = e, y^n = e, xy = y^{-1}x.$

Then $o(G) = 2n.$

We write $G = D_{2n}.$

It may be observed that

$$xy = y^{-1}x \Rightarrow xyx^{-1} = y^{-1} \Rightarrow (xyx^{-1})^i = y^{-i}$$

$$\Rightarrow \quad xy^i x^{-1} = y^{-i} \Rightarrow y^i x y^i = x \ (i \in \mathbf{N}). \qquad \ldots(1)$$

(*a*) We proceed to show that N is normal in G.

Since $N = \langle y \rangle, y^n = e$; N is a subgroup of G.

Let $g \in G$ and $y^i \in N, i = 1, 2, \ldots, n.$

Now $g \in G \Rightarrow g = y^j$ or $xy^j, j = 1, 2, \ldots, n.$

If $g = y^j$, then $g y^i g^{-1} = y^j y^i y^{-j} = y^i \in N.$

If $g = xy^j$, then $g y^i g^{-1} = xy^j y^i y^{-j} x^{-1} = xy^i x^{-1} = y^{-i}$, by (1)

$\therefore \quad g y^i g^{-1} = y^{-i} \in N$, since $N < G$.

Hence N is a normal subgroup of G.

Transitive. Let G_1, G_2, G_3 be three groups such that $G_1 \cong G_2$ and $G_2 \cong G_3$. Then there exist two mappings $f : G_1 \to G_2$ and $g : G_2 \to G_3$ such that each is one-to-one, onto and homomorphism. Clearly, the mapping $g \circ f : G_1 \to G_3$ is one-to-one and onto. Now we show that $g \circ f$ is a homomorphism. Let $a, b \in G_1$ be arbitrary. Then

$$\begin{aligned}(g \circ f)(ab) &= g[f(ab)], \text{ by definition of product}\\ &= g[f(a) f(b)], \text{ since } f \text{ is a homomorphism}\\ &= g(f(a)) g(f(b)), \text{ since } g \text{ is a homomorphism}\\ &\qquad\qquad (\text{Here } f(a), f(b) \in G_2)\\ &= (g \circ f)(a)(g \circ f)(b), \text{ by definition of product.}\end{aligned}$$

Thus $g \circ f$ is a homomorphism and so $G_1 \cong G_3$. Hence the relation $\cong$ of isomorphism in groups is an equivalence relation.

Example 2.2.21. (Dihedral Group)

Let G be the dihedral group defined as

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

Prove

(a) *The subgroup $N = \{e, y, y^2, \ldots, y^{n-1}\}$ is normal in G.*

(b) *$G/N \cong W$, where $W = \{1, -1\}$ is the group under the multiplication of the real numbers.* [D.U., 1995]

Solution. The group G can be written as

$$G = \{y, y^2, \ldots, y^{n-1}, y^n = e, x, xy, xy^2, \ldots, xy^n\},$$

where $\quad x^2 = e, y^n = e, xy = y^{-1}x.$

Then $\quad o(G) = 2n.$

We write $\quad G = D_{2n}.$

It may be observed that

$$xy = y^{-1}x \Rightarrow xyx^{-1} = y^{-1} \Rightarrow (xyx^{-1})^i = y^{-i}$$

$$\Rightarrow \quad xy^i x^{-1} = y^{-i} \Rightarrow y^i x y^i = x \ (i \in \mathbf{N}). \qquad \ldots(1)$$

(a) We proceed to show that N is normal in G.

Since $\quad N = \langle y \rangle, y^n = e$; N is a subgroup of G.

Let $g \in G$ and $y^i \in N, i = 1, 2, \ldots, n$.

Now $g \in G \Rightarrow g = y^j$ or $xy^j, j = 1, 2, \ldots, n$.

If $\quad g = y^j$, then $g y^i g^{-1} = y^j y^i y^{-j} = y^i \in N$.

If $\quad g = xy^j$, then $g y^i g^{-1} = xy^j y^i y^{-j} x^{-1} = xy^i x^{-1} = y^{-i}$, by (1)

$\therefore \quad g y^i g^{-1} = y^{-i} \in N$, since $N < G$.

Hence N is a normal subgroup of G.

Transitive. Let G_1, G_2, G_3 be three groups such that $G_1 \approx G_2$ and $G_2 \approx G_3$. Then there exist two mappings $f: G_1 \to G_2$ and $g: G_2 \to G_3$ such that each is one-to-one, onto and homomorphism. Clearly, the mapping $g \circ f: G_1 \to G_3$ is one-to-one and onto. Now we show that $g \circ f$ is a homomorphism. Let $a, b \in G_1$ be arbitrary. Then

$$\begin{aligned}(g \circ f)(ab) &= g[f(ab)], \text{ by definition of product}\\ &= g[f(a) f(b)], \text{ since } f \text{ is a homomorphism}\\ &= g(f(a)\, g(f(b)), \text{ since } g \text{ is a homomorphism}\\ &\qquad\qquad (\text{Here } f(a), f(b) \in G_2)\\ &= (g \circ f)(a)\,(g \circ f)(b), \text{ by definition of product}\end{aligned}$$

Thus $g \circ f$ is a homomorphism and so $G_1 \approx G_3$. Hence the relation $\approx$ of isomorphism in groups is an equivalence relation.

Example 2.2.21. (Dihedral Group) Important

Let G be the dihedral group defined as

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

Prove

(*a*) *The subgroup $N = \{e, y, y^2, \ldots, y^{n-1}\}$ is normal in G.*

(*b*) *$G/N \approx W$, where $W = \{1, -1\}$ is the group under the multiplication of the real numbers.* [D.U., 1995]

Solution. The group G can be written as

$$G = \{y, y^2, \ldots, y^{n-1}, y^n = e, x, xy, xy^2, \ldots, xy^n\},$$

where $$x^2 = e, y^n = e, xy = y^{-1}x.$$

Then $o(G) = 2n$.

We write $G = D_{2n}$.

It may be observed that

$$xy = y^{-1}x \Rightarrow xyx^{-1} = y^{-1} \Rightarrow (xyx^{-1})^i = y^{-i}$$

$$\Rightarrow \quad xy^i x^{-1} = y^{-i} \Rightarrow y^i x y^i = x \; (i \in \mathbf{N}). \qquad \ldots(1)$$

(*a*) We proceed to show that N is normal in G.

Since $N = \langle y \rangle, y^n = e$; N is a subgroup of G.

Let $g \in G$ and $y^i \in N, i = 1, 2, \ldots, n$.

Now $g \in G \Rightarrow g = y^j$ or $xy^j, j = 1, 2, \ldots, n$.

If $g = y^j$, then $g y^i g^{-1} = y^j y^i y^{-j} = y^i \in N$.

If $g = xy^j$, then $g y^i g^{-1} = xy^j y^i y^{-j} x^{-1} = xy^i x^{-1} = y^{-i}$, by (1)

$\therefore \quad g y^i g^{-1} = y^{-i} \in N$, since $N < G$.

Hence N is a normal subgroup of G.

(*b*) Define a mapping $f : G \to W = \{1, -1\}$ as

$$f(y^j) = 1 \text{ and } f(xy^j) = -1 \; ; \qquad \text{for } j = 1, 2, \ldots, n. \qquad \ldots(2)$$

Obviously, f is onto. Now we show that f is a homomorphism.

Let $xy^k, y^j \in G \; ; 1 \le k, j \le n$. Then

$$f(xy^k y^j) = f(xy^{k+j}) = -1, \text{ by (2).}$$

Also $f(xy^k) f(y^j) = (-1)(1) = -1$, by (2).

$\therefore$ $f(xy^k y^j) = f(xy^k) f(y^j)$.

Again $f(y^j x y^k) = f(y^j x y^j y^{k-j}) = f(xy^{k-j})$, by (1)

$= -1$, by (2)

and $f(y^j) f(xy^k) = (1)(-1) = -1$, by (2).

$\therefore$ $f(y^j xy^k) = f(y^j) f(xy^k)$.

Thus f is a homomorphism. By Fundamental theorem of homomorphism,

$$\frac{G}{Ker f} \approx W, \qquad \ldots(3)$$

where $Ker f = \{g \in G : f(g) = 1\}$

Now $g \in Ker f \Leftrightarrow f(g) = 1 \Leftrightarrow g = y^j \; ; j = 1, 2, \ldots, n \Leftrightarrow g \in N$.

$\therefore$ $Ker f = N$. Putting in (3), we get

$$\frac{G}{N} \approx W.$$

2.3 Correspondence Theorems

Theorem 2.3.1. *Let ϕ be a homomorphism of G onto $\overline{G}$ with kernel K. Let $H = \{x \in G : \phi(x) \in \overline{H}\}$, where $\overline{H}$ is a subgroup of $\overline{G}$.*

Prove the following :

(*i*) *H is a subgroup of G and $H \supseteq K$.*

(*ii*) *If $\overline{H}$ is normal in $\overline{G}$, then H is normal in G.*

(*iii*) *There exists a one-to-one correspondence between the set of all subgroups of $\overline{G}$ and the set of all subgroups of G which contain K.*

Proof. We have $H = \{x \in G : \phi(x) \in \overline{H}\}, \overline{H} < \overline{G}$. $\qquad \ldots(1)$

(*i*) Since ϕ is a homomorphism, $\phi(e) = \overline{e} \Rightarrow \phi(e) \in \overline{H} \Rightarrow e \in H$

Thus H is non-empty.

Let $x, y \in H \Rightarrow \phi(x) \in \overline{H}$ and $\phi(y) \in \overline{H}$

$\Rightarrow \phi(x) \in \overline{H}$ and $[\phi(y)]^{-1} \in \overline{H}$, as $\overline{H} < \overline{G}$

$\Rightarrow \phi(x)[\phi(y)]^{-1} \in \overline{H}$, as $\overline{H} < \overline{G}$

$\Rightarrow \phi(x)\phi(y^{-1}) \in \overline{H}$, as ϕ is a homomorphism

$\Rightarrow \phi(xy^{-1}) \in \overline{H}$, as ϕ is a homomorphism

$\Rightarrow xy^{-1} \in H$, by (1).

Thus H is a subgroup of G.

Let $k \in K = Ker\,\phi$ so that $\phi(k) = \bar{e} \Rightarrow \phi(k) \in \bar{H} \Rightarrow k \in H$, by (1).
Thus $K \subseteq H$.

(*ii*) Let $\bar{H} \lhd \bar{G}$. We shall show that $H \lhd G$.
Let $g \in G$ and $h \in H$ be arbitrary. Then

$$\phi(g) \in \bar{G} \text{ and } \phi(h) \in \bar{H}, \text{ by (1).}$$

Since $\bar{H} \lhd \bar{G}$, $\phi(g)\,\phi(h)\,\phi(g)^{-1} \in \bar{H}$

$\Rightarrow \phi(gh)\,\phi(g^{-1}) \in \bar{H}$, as ϕ is a homomorphism

$\Rightarrow \phi(ghg^{-1}) \in \bar{H}$, as ϕ is a homomorphism

$\Rightarrow ghg^{-1} \in H$, by (1). Thus $H \lhd G$.

(*iii*) We have proved the following result in part (*i*) :

If $\bar{H}$ is any subgroup of $\bar{G}$, then there exists a subgroup H of G which contains K, where

$$H = \{x \in G : \phi(x) \in \bar{H}\}.$$

Now we have its converse part.
Let L be any subgroup of G such that $K \subseteq L$.

Let $\bar{L} = \phi(L) = \{\phi(l) : l \in L\}$. ...(2)

It is easy to verify that $\bar{L}$ is a subgroup of $\bar{G}$. Now we proceed to show that

$$L = T, \text{ where } T = \{g \in G : \phi(g) \in \bar{L}\}. \quad ...(3)$$

Let $l \in L$ be arbitrary. Then $\phi(l) \in \bar{L}$, by (2).
Using (3), $l \in T$ and so $L \subseteq T$.
Conversely, let $t \in T \Rightarrow \phi(t) \in \bar{L}$, by (3)
$\Rightarrow \phi(t) = \phi(a)$ for some $a \in L$, by (2)
$\Rightarrow \phi(t)\,\phi(a)^{-1} = \bar{e}$
$\Rightarrow \phi(t\,a^{-1}) = \bar{e}$, since ϕ is a homomorphism
$\Rightarrow t\,a^{-1} \in K \subseteq L \Rightarrow t\,a^{-1} \in L \Rightarrow t \in La$
$\Rightarrow t \in L \quad (\because a \in L \Rightarrow La = L)$
$\Rightarrow T \subseteq L$. Thus $L = T$.

From the above discussion, it follows that there exists a one-to-one correspondence between the set of all subgroups of $\bar{G}$ and the set of all subgroups of G which contain K. Hence the theorem.

In the above correspondence normal subgroups correspond with normal subgroups as shown below :

Theorem 2.3.2. *Let ϕ be a homomorphism of G onto $\bar{G}$ with kernel K. Show that there exists a one-to-one correspondence between the set of all normal subgroups of $\bar{G}$ and the set of all normal subgroups of G which contain K.*

Proof. In view of the above theorem, it suffices to show that

$$H \lhd G \Leftrightarrow \overline{H} \lhd \overline{G}, \text{ where } H \supseteq K.$$

Let H be normal in G. We shall prove that $\overline{H} = \phi(H) \lhd \overline{G}$. Let $\overline{g} \in \overline{G}$ and $\overline{h} \in \overline{H}$ be arbitrary. Since $\phi : G \to \overline{G}$ is onto, there exists some $g \in G$ such that $\phi(g) = \overline{g}$. Also $\phi(h) = \overline{h}$ for some $h \in H$.

Since $H \lhd G$, $g h g^{-1} \in H$

$\Rightarrow \quad \phi(g h g^{-1}) \in \overline{H} \Rightarrow \phi(g)\phi(h)\phi(g^{-1}) \in \overline{H}$, as ϕ is a homo.

$\Rightarrow \quad \phi(g)\phi(h)\phi(g)^{-1} \in \overline{H}$, as ϕ is a homomorphism

$\Rightarrow \quad \overline{g}\,\overline{h}\,\overline{g}^{-1} \in \overline{H} \Rightarrow \overline{H} \lhd \overline{G}$.

Conversely, let $\overline{H} \lhd \overline{G}$. We shall prove that

$$H = \{x \in G : \phi(x) \in \overline{H}\} \text{ is normal in } G.$$

Let $g \in G$ and $h \in H$ be arbitrary. Then

$$\phi(g) \in \overline{G} \text{ and } \phi(h) \in \overline{H}.$$

Since $\overline{H} \lhd \overline{G}$, $\phi(g)\phi(h)\phi(g)^{-1} \in \overline{H}$

$\Rightarrow \quad \phi(ghg^{-1}) \in \overline{H}$, since ϕ is a homomorphism

$\Rightarrow \quad ghg^{-1} \in H \Rightarrow H \lhd G$.

Corollary 1. *Let H be a normal subgroup of a group G. Show that there exists a one-to-one correspondence between the set of all subgroups of G/H and the set all subgroups of G that contain H.*

Proof. The mapping $\phi : G \to G/H$ defined by $\phi(g) = Hg$ for all $g \in G$ is an onto homomorphism with kernel $K = H$. [See Theorem 2.2.2.]

Since ϕ is a homomorphism of G onto G/H with kernel H, by Theorem 2.3.1.(*iii*), there exists a one-to-one corresponence between the set of all subgroups of G/H and the set of all subgroups of G that contain H.

Corollary 2. *Let H be a normal subgroup of a group G. Show that there exists a one-to-one correspondence between the set of all normal subgroups of G/H and the set of all normal subgroups of G that contain H.*

[D.U., 1998]

Proof. The mapping $\phi : G \to G/H$ defined by

$$\phi(g) = Hg \text{ for all } g \in G$$

is an onto homomorphism with kernel H.

The result follows by Theorem 2.3.2. [Take $\overline{G} = G/H$]

Theorem 2.3.3. ~~*Let*~~ *ϕ be a homomorphism of G onto $\overline{G}$ with kernel K. Let $\overline{N}$ be a normal subgroup of $\overline{G}$. Then there exists a subgroup N of G containing K such that*

$$\frac{G}{N} \cong \frac{\overline{G}}{\overline{N}}.$$

[D.U., 1997]

Proof. In view of the above theorem, it suffices to show that

$$H \lhd G \Leftrightarrow \overline{H} \lhd \overline{G}, \text{ where } H \supseteq K.$$

Let H be normal in G. We shall prove that $\overline{H} = \phi(H) \lhd \overline{G}$. Let $\bar{g} \in$ and $\bar{h} \in \overline{H}$ be arbitrary. Since $\phi : G \to \overline{G}$ is onto, there exists some $g \in$ such that $\phi(g) = \bar{g}$. Also $\phi(h) = \bar{h}$ for some $h \in H$.

Since $H \lhd G$, $g h g^{-1} \in H$

$\Rightarrow \quad \phi(g h g^{-1}) \in \overline{H} \Rightarrow \phi(g)\phi(h)\phi(g^{-1}) \in \overline{H}$, as ϕ is a homo.

$\Rightarrow \quad \phi(g)\phi(h)\phi(g)^{-1} \in \overline{H}$, as ϕ is a homomorphism

$\Rightarrow \quad \bar{g}\,\bar{h}\,\bar{g}^{-1} \in \overline{H} \Rightarrow \overline{H} \lhd \overline{G}$.

Conversely, let $\overline{H} \lhd \overline{G}$. We shall prove that

$$H = \{x \in G : \phi(x) \in \overline{H}\} \text{ is normal in } G.$$

Let $g \in G$ and $h \in H$ be arbitrary. Then

$$\phi(g) \in \overline{G} \text{ and } \phi(h) \in \overline{H}.$$

Since $\overline{H} \lhd \overline{G}$, $\phi(g)\phi(h)\phi(g)^{-1} \in \overline{H}$

$\Rightarrow \quad \phi(ghg^{-1}) \in \overline{H}$, since ϕ is a homomorphism

$\Rightarrow \quad ghg^{-1} \in H \Rightarrow H \lhd G$.

Corollary 1. *Let H be a normal subgroup of a group G. Show that there exists a one-to-one correspondence between the set of all subgroups of G/H and the set all subgroups of G that contain H.*

Proof. The mapping $\phi : G \to G/H$ defined by $\phi(g) = Hg$ for all $g \in G$ is an onto homomorphism with kernel $K = H$. [See Theorem 2.2.2.]

Since ϕ is a homomorphism of G onto G/H with kernel H, by Theorem 2.3.1.(*iii*), there exists a one-to-one corresponence between the set of all subgroups of G/H and the set of all subgroups of G that contain H.

Corollary 2. *Let H be a normal subgroup of a group G. Show that there exists a one-to-one correspondence between the set of all normal subgroups of G/H and the set of all normal subgroups of G that contain H.*

[D.U., 1998]

Proof. The mapping $\phi : G \to G/H$ defined by

$$\phi(g) = Hg \text{ for all } g \in G$$

is an onto homomorphism with kernel H.

The result follows by Theorem 2.3.2. [Take $\overline{G} = G/H$]

Theorem 2.3.3. ~~*Let*~~ *ϕ be a homomorphism of G onto $\overline{G}$ with kernel K. Let $\overline{N}$ be a normal subgroup of $\overline{G}$. Then there exists a subgroup N of G containing K such that*

$$\frac{G}{N} \approx \frac{\overline{G}}{\overline{N}}.$$

[D.U., 1997]

Proof. In view of the above theorem, it suffices to show that

$$H \lhd G \Leftrightarrow \overline{H} \lhd \overline{G}, \text{ where } H \supseteq K.$$

Let H be normal in G. We shall prove that $\overline{H} = \phi(H) \lhd \overline{G}$. Let $\overline{g} \in$ and $\overline{h} \in \overline{H}$ be arbitrary. Since $\phi : G \to \overline{G}$ is onto, there exists some $g \in$ such that $\phi(g) = \overline{g}$. Also $\phi(h) = \overline{h}$ for some $h \in H$.

Since $H \lhd G, g\,h\,g^{-1} \in H$

$\Rightarrow \quad \phi(g\,h\,g^{-1}) \in \overline{H} \Rightarrow \phi(g)\,\phi(h)\,\phi(g^{-1}) \in \overline{H}$, as ϕ is a homo.

$\Rightarrow \quad \phi(g)\,\phi(h)\,\phi(g)^{-1} \in \overline{H}$, as ϕ is a homomorphism

$\Rightarrow \quad \overline{g}\,\overline{h}\,\overline{g}^{-1} \in \overline{H} \Rightarrow \overline{H} \lhd \overline{G}.$

Conversely, let $\overline{H} \lhd \overline{G}$. We shall prove that

$$H = \{x \in G : \phi(x) \in \overline{H}\} \text{ is normal in } G.$$

Let $g \in G$ and $h \in H$ be arbitrary. Then

$$\phi(g) \in \overline{G} \text{ and } \phi(h) \in \overline{H}.$$

Since $\overline{H} \lhd \overline{G}, \phi(g)\,\phi(h)\,\phi(g)^{-1} \in \overline{H}$

$\Rightarrow \quad \phi(ghg^{-1}) \in \overline{H}$, since ϕ is a homomorphism

$\Rightarrow \quad ghg^{-1} \in H \Rightarrow H \lhd G.$

Corollary 1. *Let H be a normal subgroup of a group G. Show that there exists a one-to-one correspondence between the set of all subgroups of G/H and the set all subgroups of G that contain H.*

Proof. The mapping $\phi : G \to G/H$ defined by $\phi(g) = Hg$ for all $g \in G$ is an onto homomorphism with kernel $K = H$. [See Theorem 2.2.2.]

Since ϕ is a homomorphism of G onto G/H with kernel H, by Theorem 2.3.1.(*iii*), there exists a one-to-one corresponence between the set of all subgroups of G/H and the set of all subgroups of G that contain H.

Corollary 2. *Let H be a normal subgroup of a group G. Show that there exists a one-to-one correspondence between the set of all normal subgroups of G/H and the set of all normal subgroups of G that contain H.*

[D.U., 1998]

Proof. The mapping $\phi : G \to G/H$ defined by

$$\phi(g) = Hg \text{ for all } g \in G$$

is an onto homomorphism with kernel H.

The result follows by Theorem 2.3.2. [Take $\overline{G} = G/H$]

Theorem 2.3.3. ~~*Let*~~ *ϕ be a homomorphism of G onto $\overline{G}$ with kernel K. Let $\overline{N}$ be a normal subgroup of $\overline{G}$. Then there exists a subgroup N of G containing K such that*

$$\frac{G}{N} \approx \frac{\overline{G}}{\overline{N}}.$$

[D.U., 1997]

Proof. Let $N = \{x \in G : \phi(x) \in \overline{N}\}$. ...(1)

Then N is a subgroup of G containing K.

[See part (*i*) of Theorem 2.3.1]

Since $\overline{N} \lhd \overline{G}$, $\overline{G}/\overline{N}$ is defined. It is given that

$$\phi : G \to \overline{G} \text{ is an onto homomorphism.}$$

Define a mapping $\psi : G \to \overline{G}/\overline{N}$ as

$$\psi(g) = \overline{N}\,\phi(g) \quad \forall \quad g \in G. \qquad ...(2)$$

Notice that $\phi(g) \in \overline{G}$ for each $g \in G$ and so $\overline{N}\,\phi(g) \in \overline{G}/\overline{N}$.

We see that ψ is well-defined, since

$$g_1 = g_2 \Rightarrow \phi(g_1) = \phi(g_2) \Rightarrow \overline{N}\,\phi(g_1) = \overline{N}\,\phi(g_2) \Rightarrow \psi(g_1) = \psi(g_2).$$

Now we show that ψ is a homomorphism.

Let $g_1, g_2 \in G$. Using (2), we have

$$\begin{aligned}\psi(g_1 g_2) &= \overline{N}\,\phi(g_1\, g_2)\\ &= \overline{N}\,\phi(g_1)\,\phi(g_2), \text{ since } \phi \text{ is a homomorphism}\\ &= \overline{N}\,\phi(g_1)\,\overline{N}\,\phi(g_2), \text{ since } \overline{N} \lhd \overline{G}\\ &= \psi(g_1)\,\psi(g_2), \text{ by (2).}\end{aligned}$$

Thus ψ is a homomorphism. Now we show that ψ is onto.

Let $X \in \overline{G}/\overline{N}$ be arbitrary. Then $X = \overline{N}\,\overline{g}$ for some $\overline{g} \in \overline{G}$.

Since $\phi : G \to \overline{G}$ is onto, there exists some $g \in G$ such that $\phi(g) = \overline{g}$

$\Rightarrow \quad X = \overline{N}\,\phi(g)$

$\Rightarrow \quad X = \psi(g),\ g \in G.$ [Using (2)]

Thus ψ is onto. By Fundamental theorem of homomorphism, we have

$$\frac{G}{Ker\,\psi} \approx \frac{\overline{G}}{\overline{N}}, \qquad ...(3)$$

where $\quad Ker\,\psi = \{g \in G : \psi(g) = \overline{N}, \text{ identity of } \overline{G}/\overline{N}\}$

$$\begin{aligned}\therefore \quad g \in Ker\,\psi &\Leftrightarrow \psi(g) = \overline{N}\\ &\Leftrightarrow \overline{N}\,\phi(g) = \overline{N}, \text{ by (2)}\\ &\Leftrightarrow \phi(g) \in \overline{N}\\ &\Leftrightarrow g \in N, \text{ by (1)}\end{aligned}$$

$\therefore \quad Ker\,\psi = N$. Putting in (3), we get

$$\frac{G}{N} \approx \frac{\overline{G}}{\overline{N}}.$$

Corollary. *Under the hypotheses of Theorem 2.3.3, show that*

$$\frac{G}{N} \approx \frac{G/K}{N/K}.$$

Proof. Since $\phi : G \to \overline{G}$ is an onto homomorphism with kernel K,

$$\frac{G}{K} \approx \overline{G} \quad \text{or} \quad \overline{G} \approx \frac{G}{K}.$$

Let $$N = \{x \in G : \phi(x) \in \overline{N}\}.$$

Then N is a subgroup of G containing K. Clearly $\phi : N \to \overline{N}$ is an onto homomorphism with kernel K. Consequently,

$$\frac{N}{K} \approx \overline{N} \quad \text{or} \quad \overline{N} \approx \frac{N}{K}.$$

Hence $$\frac{G}{N} \approx \frac{\overline{G}}{\overline{N}} \approx \frac{G/K}{N/K}.$$

EXAMPLES

Example 2.3.1. *Let $f : G \to G'$ be an onto homomorphism of groups G and G' and $K = Kernel\, f$. Let H be a normal subgroup of G and H' any subgroup of G'. Prove that $f(H)$ is a normal subgroup of G' and $f^{-1}(H')$ is a subgroup of G such that $K \subseteq f^{-1}(H')$.*

Hence find all subgroup of $\mathbf{Z}/(12)$, where $\mathbf{Z}$ is the group of integers under addition and (12), the subgroup $12\,\mathbf{Z}$. [D.U., 1992]

Solution. (*i*) We have $H \lhd G, H' < G'$ and $K = Ker f$. We know $f(H) = \{f(h) : h \in H\}$. To show $f(H) \lhd G'$. Obviously, $f(H)$ is non-empty, since $f(e) \in f(H)$. Now we show that $f(H)$ is a subgroup of G'. Let $x, y \in f(H)$. Then $x = f(h_1), y = f(h_2)$; for some $h_1, h_2 \in H$. We have

$$x y^{-1} = f(h_1) f(h_2)^{-1} = f(h_1) f(h_2^{-1}) = f(h_1 h_2^{-1}),$$

since f is a homomorphism.

Now $\quad H < G \Rightarrow h_1 h_2^{-1} \in H$ and so

$$xy^{-1} = f(h_1 h_2^{-1}) \in f(H). \text{ Thus } f(H) < G'.$$

Now we proceed to show that $f(H) \lhd G'$.

Let $\quad y \in G'$ and $a \in f(H)$ be arbitrary. Then

$y = f(x)$ for some $x \in G$ (since $f : G \to G'$ is onto)

and $\quad a = f(h)$ for some $h \in H$.

Since $\quad H \lhd G, x h x^{-1} \in H$

$\Rightarrow \quad f(x h x^{-1}) \in f(H)$

$\Rightarrow \quad f(x) f(h) f(x^{-1}) \in f(H)$, since f is a homomorphism

$\Rightarrow \quad f(x) f(h) f(x)^{-1} \in f(H)$, since f is a homomorphism

$\Rightarrow \quad y a y^{-1} \in f(H) \Rightarrow f(H) \lhd G'$.

(*ii*) By definition, $f^{-1}(H') = \{x \in G : f(x) \in H'\}$. ...(1)

We proceed to show that $f^{-1}(H')$ is a subgroup of G.

Since $H' < G', f(e) = e' \in H'$, since f is a homomorphism.

Using (1), $e \in f^{-1}(H')$ and so $f^{-1}(H') \neq \phi$.

Let $x, y \in f^{-1}(H')$. Then $f(x), f(y) \in H'$, by (1)

$\Rightarrow f(x)f(y)^{-1} \in H'$, as $H' < G'$

$\Rightarrow f(xy^{-1}) \in H'$, since f is a homomorphism

$\Rightarrow xy^{-1} \in f^{-1}(H')$, by (1).

Thus $f^{-1}(H')$ is a subgroup of G.

Finally, we show that $K \subseteq f^{-1}(H')$.

Let $x \in K$ be arbitrary, $K = Ker f$.

$\therefore \quad f(x) = e' \Rightarrow f(x) \in H' \Rightarrow x \in f^{-1}(H')$, by (1).

Hence $\quad K \subseteq f^{-1}(H')$.

(*iii*) We know that the mapping $f: G \to \dfrac{G}{H}$ defined by

$$f(g) = Hg \quad \text{for all} \quad g \in G$$

is an onto homomorphism with kernel H. Further any subgroup of G/H is of the form L/H, where $L < G$ and $L \supseteq H$ [See example 2.3.2 below].

Let $H = (12) = \{\ldots, -24, -12, 0, 12, 24, \ldots\}$. Then $H \lhd \mathbf{Z}$.

All subgroups of $\mathbf{Z}$ containing H are

$$(2) = \{\ldots, -4, -2, 0, 2, 4, \ldots\},$$
$$(3) = \{\ldots, -6, -3, 0, 3, 6, \ldots\},$$
$$(4) = \{\ldots, -8, -4, 0, 4, 8, \ldots\},$$
$$(6) = \{\ldots, -12, -6, 0, 6, 12, \ldots\},$$
$$(12) = \{\ldots, -12, 0, 12, \ldots\}.$$

Hence all subgroups of $\mathbf{Z}/(12)$ are

$$\frac{(2)}{(12)}, \frac{(3)}{(12)}, \frac{(4)}{(12)}, \frac{(6)}{(12)} \text{ and } \frac{(12)}{(12)}; \text{ where}$$

$$\frac{(2)}{(12)} = \{(12), 2 + (12), 4 + (12), 6 + (12), 8 + (12), 10 + (12)\},$$

$$\frac{(3)}{(12)} = \{(12), 3 + (12), 6 + (12), 9 + (12)\},$$

$$\frac{(4)}{(12)} = \{(12), 4 + (12), 8 + (12)\},$$

$$\frac{(6)}{(12)} = \{(12), 6 + (12)\} \text{ and } \frac{(12)}{(12)} = \{(12)\}.$$

Example 2.3.2. *If H is a normal subgroup of a group G, then establish that any subgroup of G/H is of the form K/H, where K is a subgroup of G containing H and further K/H is normal in G/H iff K is normal in G. Hence find all the subgroups of $\mathbf{Z}/10\,\mathbf{Z}$, $\mathbf{Z}$ being the group of integers.*

[D.U., 1996].

Solution. Let T be any subgroup of G/H. Then T contains H (the identity of G/H) and the elements of T are right cosets of H of the form :

$$T = \{Hk : k \in K\}, \quad \text{where} \quad K \subseteq G \quad \text{and} \quad K \supseteq H.$$

We now show that K is a subgroup of G. Let $k_1, k_2 \in K$ be arbitrary. Then $X = Hk_1$ and $Y = Hk_2 \in T$.

Now $T < G/H \Rightarrow XY^{-1} \in T \Rightarrow Hk_1\, Hk_2^{-1} \in T \Rightarrow Hk_1k_2^{-1} \in T (\because H \lhd G)$

$\Rightarrow \quad k_1\, k_2^{-1} \in K \Rightarrow K < G.$

Hence $\quad T = \{Hk : k \in K\} = K/H$, where $K < G$ and $K \supseteq H$.

(*ii*) We prove that $K \lhd G \Leftrightarrow K/H \lhd G/H$.

Let $K \lhd G$. Let $Hg \in G/H$ and $Hk \in K/H$ be arbitrary, where $g \in G$ and $k \in K$.

Now $\quad K \lhd G \Rightarrow gkg^{-1} \in K \Rightarrow H(gkg^{-1}) \in K/H$

$\Rightarrow (Hgk)\, Hg^{-1} \in K/H \Rightarrow (Hg)\,(Hk)\,(Hg)^{-1} \in K/H \Rightarrow K/H \lhd G/H.$

Conversely, let $K/H \lhd G/H$. To show that $K \lhd G$.

Let $x \in G$ and $a \in K$ be arbitrary. Then $Hx \in G/H$ and $Ha \in K/H$

$\Rightarrow \quad Hx\, Ha\, (Hx)^{-1} \in K/H$, since $K/H \lhd G/H$

$\Rightarrow \quad Hxa\, Hx^{-1} \in K/H \Rightarrow H(xax^{-1}) \in K/H \Rightarrow xax^{-1} \in K$

$\Rightarrow \quad K \lhd G.$

(*iii*) All subgroups of $\dfrac{\mathbf{Z}}{10\mathbf{Z}} = \dfrac{\mathbf{Z}}{(10)}$ are

$$\frac{(2)}{(10)}, \frac{(5)}{(10)} \text{ and } \frac{(10)}{(10)} \text{ ; where}$$

$$\frac{(2)}{(10)} = \{(10), 2+(10), 4+(10), 6+(10), 8+(10)\},$$

$$\frac{(5)}{(10)} = \{(10), 5+(10)\} \text{ and } \frac{(10)}{(10)} = \{(10)\}.$$

EXERCISES

1. Show that $f : (\mathbf{R}, +) \to (\mathbf{R}, +)$ defined by $f(x) = 5x$ is a homomorphism.
2. Show that $f : (\mathbf{R}, +) \to (\mathbf{R}, +)$ defined by $f(x) = x + 1$ is not a homomorphism for all $x, y \in \mathbf{R}$.
   [**Hint.** $f(x+y) = x + y + 1 \neq f(x) + f(y)$.]
3. If G is any abelian group and $G' = G$, prove that $f : G \to G'$ defined by $f(x) = x^n$ for all $x \in G$ and n a positive integer, is a homomorphism.
   [**Hint.** $f(xy) = (xy)^n = x^n y^n \quad (\because G \text{ is abelian}) = f(x) f(y)$.]
4. Show that the mapping $f : (\mathbf{C}, +) \to (\mathbf{R}, +)$ defined by
   $$f(x + iy) = x$$
   is a homomorphism. Find the kernel of f.

[**Hint.** $Ker f = \{x + iy : f(x + iy) = 0, \text{ identity of } (\mathbf{R}, +)\}$

$= \{x + iy : x = 0\} = \{iy : y \in \mathbf{R}\}$.]

5. Let $\mathbf{C}^*$ denote the multiplicative group of non-zero complex numbers. Show that the mapping $f : \mathbf{C}^* \to \mathbf{C}^*$ defined by $f(z) = z^n \ \forall \ z \in \mathbf{C}$ is a homomorphism. Also, prove that the kernel of f is the set of n nth roots of unity.

[**Hint.** $Ker f = \{z \in \mathbf{C} : f(z) = 1\} = \{z \in \mathbf{C} : z^n = 1\}$.]

6. Let H be a normal subgroup of a group G. Define a mapping $f : G \to G/H$ by $f(x) = Hx \ \forall \ x \in G$. Show that f is a homomorphism and $Ker f = H$.

[**Hint.** See Theorem 2.2.2.]

7. Show that a subgroup N of G is normal in G if and only if there exists a group H and a homomorphism $\theta : G \to H$ such that $Ker\ \theta = N$.

[**Hint.** Let $N \lhd G$. Choose $H = G/N$. Then $\theta : G \to H = G/N$ defined by $\theta(x) = Nx \ \forall \ x \in G$ is a homomorphism with $Ker\ \theta = N$. Conversely, let $\theta : G \to H$ be a homomorphism with $Ker\ \theta = N$. Since $Ker\ \theta \lhd G$, $N \lhd G$.]

8. Show that the order of every homomorphic image of a finite order group is a divisor of the order of the group.

[**Hint.** Let $f : G \to G'$ be an onto homomorphism, where $o(G)$ is finite. Then

$$\frac{G}{Ker f} \approx G' \Rightarrow o(G') = \frac{o(G)}{o(Ker f)}.]$$

9. If f is a homomorphism of a group G into a group G', prove that

$$G/Ker f \approx f(G).$$

[**Hint.** The mapping $f : G \to f(G)$ is an onto homomorphism, $f(G) < G'$.]

10. Prove that if for a group $G, f : G \to G$ given by $f(x) = x^3$, is an isomorphism, then G is abelian.

11. Let $G = (\mathbf{R}, +)$ and $G' = \{z \in \mathbf{C} : |z| = 1\}$ be a multiplicative group. Prove that the mapping $x \to e^{ix}$ is a homomorphism. Find the kernel.

[**Hint.** Kernel $= \{x : e^{ix} = 1\} = \{2n\pi : n \in \mathbf{Z}\}$.]

12. Show that a homomorphism from a simple group is either trivial or one-to-one.

[**Hint.** Let $f : G \to G'$ be a homomorphism. Then $Ker f \lhd G$. Since G is simple, $Ker f = (e)$ or $Ker f = G$. Now $Ker f = (e)$ implies f is one-to-one. $Ker f = G \Rightarrow x \in Ker f \ \forall \ x \in G \Rightarrow f(x) = e \ \forall \ x \in G \Rightarrow f$ is a trivial homomorphism.]

13. Let $f : G \to G'$ be an onto homomorphism. Prove that if N is a normal subgroup of G, then $f(N)$ is a normal subgroup of G'.

[**Hint.** By Example 2.2.8, $f(N) < G'$. Let $g \in G'$ and $a \in f(N)$. Then $a = f(n)$ for $n \in N$ and $g = f(x)$ for some $x \in G$ (since f is onto). Now $N \lhd G \Rightarrow xnx^{-1} \in N \Rightarrow f(xnx^{-1}) \in f(N) \Rightarrow f(x)f(n)f(x^{-1}) \in f(N)$ $\Rightarrow gag^{-1} \in f(N) \Rightarrow f(N) \lhd G'$.]

14. If f is a homomorphism of G_1 onto G_2 and g a homomorphism of G_2 onto G_3, show that $g \circ f$ is a homomorphism of G_1 onto G_3. Also show that the kernel of f is a subgroup of that of $g \circ f$.

[**Hint.** See Example 2.2.20 (Transitive law). We have

$$f : G_1 \to G_2 \quad \text{and} \quad g \circ f : G_1 \to G_3.$$

Let $K = Ker f$ and $K' = Ker(g \circ f)$. Since K, K' are normal subgroups of G_1, it suffices to show that $K \subseteq K'$. Let $k \in K \Rightarrow f(k) = e_2$.

Now $(g \circ f)(k) = g(f(k)) = g(e_2) = e_3$

$\Rightarrow \quad k \in K'$. Hence $K \subseteq K'$.]

15. Let $f : G \to G'$ be a homomorphism of a group G into a group G'. Prove that $f(G)$ is a subgroup of G' and $f^{-1}(e')$ is a normal subgroup of G, where e' is the identity of G'.

[**Hint.** $f^{-1}(e') = \{x \in G : f(x) = e'\} = Ker f \lhd G$.]

2.4 Cayley's Theorem

Theorem 2.4.1. *Every group G is isomorphic to a permutation group.*

[D.U., 1995, 94]

Proof. Let G be a group and $A(G)$ the group of all permutations of G *i.e.*, $A(G)$ is the set of all one-to-one mappings of G onto G. For each $a \in G$, we define a mapping

$$f_a : G \to G \quad \text{as } f_a(x) = ax \ \forall \ x \in G. \qquad \text{...(1)}$$

Then f_a is a one-to-one, since

$$f_a(x) = f_a(y) \Rightarrow ax = ay \Rightarrow x = y, \forall x, y \in G.$$

(Using cancellation law in G)

Now we show that f_a is onto. For *any* $g \in G$, we have

$$g = e \,.\, g = a(a^{-1}g) = ag_1, \quad \text{where } g_1 = a^{-1}g \in G.$$

Using (1), $g = f_a(g_1) \Rightarrow f_a$ is onto.

Since f_a is one-to-one and onto, f_a is a permutation of G. Thus

$$f_a \in A(G) \ \forall \ a \in G.$$

Let $$\overline{G} = \{f_a : a \in G\}. \qquad \text{...(2)}$$

Now we proceed to show that $\overline{G}$ is a subgroup of $A(G)$.

Let $f_a, f_b \in \overline{G}$. For any $x \in G$, we have

$$\begin{aligned}(f_a f_b)(x) &= f_a[f_b(x)] = f_a(bx), \text{ by (1)}\\ &= a(bx), \text{ by (1)}\\ &= (ab)x, \text{ by associative law in } G\\ &= f_{ab}(x).\end{aligned}$$

$\therefore \quad f_a f_b = f_{ab}$ for each $a, b \in G$. ...(3)

From (3), it follows that

$$f_a \in \overline{G} \text{ and } f_b \in \overline{G} \Rightarrow f_a f_b \in \overline{G}. \quad ...(4)$$

Now we show that $(f_a)^{-1} = f_{a^{-1}}$ for all $f_a \in \overline{G}$. ...(5)

Using (3), we have

$$f_a f_{a^{-1}} = f_{aa^{-1}} = f_e, \quad \text{where}$$

$$f_e(x) = ex = x \ \forall \ x \in G \Rightarrow f_e = I \text{ is the identity.}$$

Similarly, $f_{a^{-1}} f_a = I$. This proves (5) and so $(f_a)^{-1} \in \overline{G} \ \forall \ f_a \in \overline{G}$.

From (4) and (5), $\overline{G} < A(G)$ and so $\overline{G}$ *is a permutation group.*

Finally, we prove that $G \approx \overline{G}$.

Define a mapping $\psi : G \to \overline{G}$ as

$$\psi(a) = f_a \ \forall \ a \in G. \quad ...(6)$$

Clearly, ψ is onto. Now we show that ψ is a homomorphism.

Let $a, b \in G$ be arbitrary. From (6) and (3), we have

$$\psi(ab) = f_{ab} = f_a f_b = \psi(a)\,\psi(b).$$

Thus ψ is a homomorphism. Also ψ is one-to-one, since

$$\psi(a) = \psi(b) \Rightarrow f_a = f_b \Rightarrow f_a(x) = f_b(x) \ \forall \ x \in G$$

$\Rightarrow$ $ax = bx$, using (1)

$\Rightarrow$ $a = b$, by cancellation law in G.

Since $\psi : G \to \overline{G}$ is homomorphism, one-to-one and onto, $G \approx \overline{G}$.

EXAMPLES

Example 2.4.1. *Verify Cayley's theorem for the cyclic group G of order 3. What is the corresponding permutation group isomorphic to G?* [D.U., 1995, 94]

Solution. We have $G = \{a, a^2, a^3 = e\}$. Its permutation group is

$$\overline{G} = \{f_e, f_a, f_{a^2}\}, \text{ where}$$

$$f_e(a) = ae = a, f_e(a^2) = a^2 e = a^2, f_e(e) = ee = e.$$

Thus $f_e = I$ is the identity mapping of G. Now

$$f_a(a) = aa = a^2, f_a(a^2) = aa^2 = e, f_a(e) = ae = a$$

and $$f_{a^2}(a) = a^2 a = e, f_{a^2}(a^2) = a^2 a^2 = ae = a, f_{a^2}(e) = a^2 e = a^2.$$

It may be observed that

$$\overline{G} = \langle f_a \rangle, \text{ since } f_{a^2} = f_{aa} = f_a f_a = (f_a)^2, f_e = f_{a^3} = (f_a)^3.$$

Since any two cyclic groups of the same order are isomorphic,

$$G \approx \overline{G}.$$

Example 2.4.2. *Find the permutation group isomorphic to the multiplicative group $G = \{1, w, w^2\}$ of cube roots of unity.*

Hint. Similar to Example 2.4.1.

Ans. $\overline{G} = \{f_1, f_w, f_{w^2}\}$, where $f_1 = I$;

$$f_w(1) = w, f_w(w) = w^2, f_w(w^2) = 1;$$

$$f_{w^2}(1) = w^2, f_{w^2}(w) = 1, f_{w^2}(w^2) = w.$$

Example 2.4.3. *Find the permutation group isomorphic to the group* $G = \{1, -1, i, -i\}$, $i^2 = 1$.

Solution. The permutation group isomorphic to G is

$$\overline{G} = \{f_1, f_{-1}, f_i, f_{-i}\}, \text{ where}$$

$$f_1(1) = 1.1 = 1, f_1(-1) = -1, f_1(i) = i, f_1(-i) = -i;$$

$$f_{-1}(1) = -1.1 = -1, f_{-1}(1) = 1, f_{-1}(i) = -i, f_{-1}(-i) = i;$$

$$f_i(1) = i.1 = i, f_i(-1) = -i, f_i(i) = i^2 = -1, f_i(-i) = -i^2 = 1;$$

$$f_{-i}(1) = -i, f_{-i}(-1) = i, f_{-i}(i) = -i^2 = 1, f_{-i}(-i) = i^2 = -1.$$

Example 2.4.4. *Find the permutation group isomorphic to the group G of four transformations f_1, f_2, f_3 and f_4 defined by*

$$f_1(z) = z, f_2(z) = -z, f_3(z) = 1/z, f_4(z) = -1/z$$

of the infinite complex plane onto itself.

Please try yourself.

Ans. $\overline{G} = \{T_{f_1}, T_{f_2}, T_{f_3}, T_{f_4}\}$,

$$T_{f_1} = \begin{pmatrix} f_1 & f_2 & f_3 & f_4 \\ f_1 & f_2 & f_3 & f_4 \end{pmatrix}, T_{f_2} = \begin{pmatrix} f_1 & f_2 & f_3 & f_4 \\ f_2 & f_1 & f_4 & f_3 \end{pmatrix},$$

$$T_{f_3} = \begin{pmatrix} f_1 & f_2 & f_3 & f_4 \\ f_3 & f_4 & f_1 & f_2 \end{pmatrix}, T_{f_4} = \begin{pmatrix} f_1 & f_2 & f_3 & f_4 \\ f_4 & f_3 & f_2 & f_1 \end{pmatrix}.$$

Theorem 2.4.2. *Let H be a subgroup of a group G and S the set of all left cosets of H in G. Show that there is a homomorphism*

$$\theta : G \to A(S)$$

and the kernel of θ is the largest normal subgroup of G which is contained in H.

Proof. We have $S = \{xH : x \in G\}$.

For each $g \in G$, we define a mapping $T_g : S \to S$ as

$$T_g(xH) = gxH, \text{ for each } xH \in S. \qquad ...(1)$$

Then T_g is well-defined and one-to-one, since

$$xH = yH \Leftrightarrow gxH = gyH \Leftrightarrow T_g(xH) = T_g(yH).$$

Now we show that T_g is onto. Let $xH \in S$ be arbitrary. We have

$$xH = exH = g(g^{-1}xH) = gx_1H, \quad \text{where} \quad x_1 = g^{-1}x \in G.$$

Using (1), $\quad xH = T_g(x_1H)$, where $x_1H \in S$.

This shows that T_g is onto. Also T_g is one-to-one. Consequently,

$$T_g \in A(S) \ \forall \ g \in G.$$

Next we show that

$$T_g T_h = T_{gh} \ \forall \ g, h \in G. \qquad ...(2)$$

For any $xH \in S$, we have

$$(T_g T_h)(xH) = T_g[T_h(xH)] = T_g[hxH], \text{ by (1)}$$
$$= g(hxH), \text{ by (1)}$$
$$= (gh)xH$$
$$= T_{gh}(xH), \text{ by (1). This proves (2).}$$

Define a mapping $\theta : G \to A(S)$

$$\theta(g) = T_g \ \forall \ g \in G. \qquad ...(3)$$

This θ is a homomorphism, since by (3) and (2),

$$\theta(gh) = T_{gh} = T_g T_h = \theta(g)\theta(h), \ \forall \ g, h \in G.$$

If $K = Ker\,\theta$, then

$$K = \{g \in G : \theta(G) = I, \text{ identity of } A(S)\},$$

or $$K = \{g \in G : T_g = I\}.$$

Now $$g \in K \Leftrightarrow T_g = I \Leftrightarrow T_g(xH) = I(xH), \ \forall \ xH \in S$$
$$\Leftrightarrow gxH = xH, \ \forall \ x \in G.$$

Hence $$K = \{g \in G : gxH = xH \ \forall \ x \in G\}. \qquad ...(4)$$

Since $Ker\,\theta$ is a normal subgroup of G, $K \lhd G$. Now we show that $K \subseteq H$. Let $k \in K$ be arbitrary. By (4), $kxH = xH \ \forall \ x \in G$.

In particular, $keH = eH \Rightarrow kH = H \Rightarrow k \in H \Rightarrow K \subseteq H$.

Lastly, we show that K is the *largest* normal subgroup of G which is contained in H. In other words, we have to show that if N is *any* normal subgroup of G such that $N \subseteq H$, then we must have $N \subseteq K$. Let $n \in N$ be arbitrary. Then

$$x^{-1}nx \in N \text{ for all } x \in G \quad (\because N \lhd G)$$
$$\Rightarrow \quad x^{-1}nx \in H \quad (\because N \subseteq H)$$
$$\Rightarrow \quad x^{-1}nxH = H$$
$$\Rightarrow \quad nxH = xH \ \forall \ x \in G$$
$$\Rightarrow \quad n \in K, \text{ by (4).}$$

Hence $N \subseteq K$ and the theorem is proved.

Theorem 2.4.3. *Let H be a subgroup of a group G, $S = \{Hx : x \in G\}$. Then prove that there is a homomorphism of G onto $A(S)$ such that $Ker\,\theta$ is the largest normal subgroup of G contained in H.* [D.U., 1996]

Proof. Define $T_g : S \to S$ as $(Hx)T_g = Hxg \ \forall \ x \in G$.

Then T_g is well defined and one-to-one, since

$$Hx = Hy \Leftrightarrow Hxg = Hyg \Leftrightarrow (Hx)T_g = (Hy)T_g.$$

Also T_g is onto, since for any $Hx \in S$,

$$Hx = H(xg^{-1})g = Hyg, \text{ where } y = xg^{-1} \in G$$
$$\Rightarrow \quad Hx = (Hy)T_g, \ Hy \in S.$$

Since T_g is one-to-one and onto, $T_g \in A(S) \ \forall \ g \in G$.

For any $Hx \in S$ and $g, h \in G$, we have

$$(Hx)(T_g T_h) = [(Hx) T_g] T_h = [Hxg] T_h = Hxgh = (Hx) T_{gh}.$$

$$\therefore \qquad T_g T_h = T_{gh} \ \forall \ g, h \in G.$$

The mapping $\theta : G \to A(S)$ defined as $\theta(g) = T_g$ is a homomorph since for $g, h \in G$,

$$\theta(gh) = T_{gh} = T_g T_h = \theta(g)\,\theta(h).$$

If $\qquad K = Ker\,\theta$, then $K = \{g \in G : \theta(g) = I\}$

or $\qquad K = \{g \in G : T_g = I\} = \{g \in G : (Hx) T_g = (Hx) I \ \forall \ x \in G$

$\therefore \qquad K = \{g \in G : Hxg = Hx \ \forall \ x \in G\}.$

Clearly, $K \subset H$; since for any $k \in K$, we have

$$Hxk = Hx \ \forall \ x \in K.$$

In particular, $Hek = He \Rightarrow Hk = H \Rightarrow k \in H.$

Hence $K = Ker\,\theta$ is a normal subgroup of G contained in H. Let N any normal subgroup of G such that $N \subset H$. We shall prove that $N \subset K$.

Let $n \in N$ be arbitrary. Then $xnx^{-1} \in N \ \forall \ x \in G \quad (\because N \lhd G)$

$\Rightarrow \quad xnx^{-1} \in H \quad (\because N \subset H)$

$\Rightarrow \quad Hxnx^{-1} = H \Rightarrow Hxn = Hx \ \forall \ x \in G \Rightarrow n \in K \Rightarrow N \subset K.$

Hence $Ker\,\theta$ is the largest normal subgroup of G contained in H.

Theorem 2.4.4. *If G is a finite group, and $H \neq G$ is a subgroup of such that $o(G)$ does not divide $i(H)$!, where $i(H)$ denotes the index of in G, then show that H contains a non-trivial normal subgroup of G.*

[D.U., 1998, 9

Proof. Let S be the set of all left cosets of H in G. The $o(S) = i(H)$ and so $o[A(S)] = i(H)$!, where $A(S)$ is te set of all permutations of S. ...(1)

By Theorem 2.4.2, there exists a homomorphism $\theta : G \to A(S)$ such that $Ker\,\theta$ is the largest normal subgroup of G such that $Ker\,\theta \subseteq H$.

Since $\quad H \neq G$ and $Ker\,\theta \subseteq H$, therefore $Ker\,\theta \neq G$. ...(2)

We shall prove that $Ker\,\theta \neq (e)$.

Let, if possible, $\quad Ker\,\theta = (e)$. ...(3)

Clearly, $\theta : G \to \theta(G)\ [< A(S)]$ is an onto homomorphsim, therefore by Fundamental theorem of homomorphism,

$$\frac{G}{Ker\,\theta} \approx \theta(G), \text{ where } \theta(G) < A(S)$$

or

$$\frac{G}{(e)} \approx \theta(G), \text{ using (3).}$$

We know $\quad G \approx G/(e)$. Consequently,

$$o(G) = o\left[\frac{G}{(e)}\right] = o[\theta(G)]. \qquad ...(4)$$

By Lagrange's theorem, $o[\theta(G)]$ divides $o[A(S)]$. ...(5)

Using (4) and (1) in (5), $o(G)$ divides $i(H)$!

This is contrary to the given hypothesis. It follows that $Ker\,\theta \neq (e)$. Also $Ker\,\theta \neq G$. Hence $Ker\,\theta$ is a non-trivial normal subgroup of G, which is contained in H.

Corollary. *If G is a finite group, and $H \neq G$ is a subgroup of G such that $o(G)$ does not divide $i(H)!$, then G is not a simple group.*

Recall that a group G is *simple* if it has no non-trivial normal subgroup.

EXAMPLES

Example 2.4.5. *Prove that a group of order 36 is not simple.*

Solution. Let $o(G) = 36 = 2^2 \times 3^2$.

By First Sylow's Theorem [See Chapter 4], G has a subgroup of order $3^2 = 9$. Let $o(H) = 9$, where $H < G$. We have

$$i(H) = \frac{o(G)}{o(H)} = \frac{36}{9} = 4.$$

$$\therefore \qquad i(H)! = 4! = 24.$$

Since $o(G) = 36$ does not divide $i(H)! = 24$, by Theorem 2.4.4, H contains a non-trivial normal subgroup N of G, $N \neq (e)$ *i.e.*, $o(N) > 1$.

By Lagrange's Theorem, $o(N)$ divides $o(H) = 9$.

Hence $N \lhd G$, where $o(N) = 3$ or 9.

Hence G is not simple.

Example 2.4.6. *Prove that a group of order 99 is not simple.* [D.U., 1997]

Solution. Let $o(G) = 99 = 3^2 \times 11$.

By First Sylow's Theorem [See Chapter 4], G has a subgroup of order 11. Let $o(H) = 11$, where $H < G$. We have

$$i(H) = \frac{o(G)}{o(H)} = \frac{99}{11} = 9.$$

$$\therefore \qquad i(H)! = 9!$$

Since $o(G) = 99$ does not divide $i(H)! = 9!$, by Theorem 2.4.4, H contains a non-trivial normal subgroup N of G, $N \neq (e)$ *i.e.*, $o(N) > 1$.

By Lagrange's theorem, $o(N)$ divides $o(H) = 11$. Consequently, $o(N) = (H)$ and so $N = H$. Hence H is a normal subgroup of order G of order 11 and so G is not simple.

Example 2.4.7. *Show that a group G of order 56 is not simple.*

Hint. G has a normal subgroup of order 7.

Example 2.4.8. *Show that a group G of order 30 is not simple.*

Hint. G has a normal subgroup of order 5.

Example 2.4.9. *Prove that a group of order p^2, where p is a prime number, must have a normal subgroup of order p.*

Solution. Let $o(G) = p^2$. By First Sylow's Theorem, G has a subgroup (say H) of order p. Now

$$i(H) = \frac{o(G)}{o(H)} = \frac{p^2}{p} = p.$$

Since p^2 does not divide $p!$ for any prime p, $o(G)$ does not divide $i(H)$!. Hence H has a non-trivial normal subgroup (say N) of G, $N \neq (e)$.

By Lagrange's Theorem, $o(N)$ divides $o(H) = p$.

Since p is prime and $o(N) > 1$, $o(N) = o(H)$ and so $N = H$. Hence H is a normal subgroup of G of order p.

Example 2.4.10. *If p is a prime number, prove that any group G of order 2p must have a subgroup of order p, and that this subgroup is normal in G.*

Solution. $o(G) = 2p$. By First Sylow's Theorem, G has a subgroup (say H) of order p. Now

$$i_G(H) = \frac{o(G)}{o(H)} = \frac{2p}{2} = 2.$$

Since $i_G(H) = 2$, $H \lhd G$ and $o(H) = p$.

2.5 Permutation Groups

We have seen in Chapter 1 that for any set S, $A(S)$ is a group where $A(S)$ consists of all one-to-one mappings of S onto itself. If S is a finite set having n elements, then we write $A(S) = S_n$. S_n is called the *symmetric group of degree n* and the elements of S_n are called *permutations*. It can be proved that $o(S_n) = n!$. A permutation $f \in S_n$ is usually denoted as

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ f(1) & f(2) & f(3) & \dots & f(n) \end{pmatrix}.$$

Definition. (Cycle and Transposition).

A **cycle** *of length r (or* **r-cycle***) is defined as a permutation $f \in S_n$ satisfying*

$$f(a_1) = a_2,\ f(a_2) = a_3, \dots, f(a_{r-1}) = a_r, f(a_r) = a_1$$

and $\quad f(a) = a$ *if* $a \notin \{a_1, a_2, \dots, a_r\}$.

The above r-cycle is written as $(a_1 a_2 \dots a_r)$.

A cycle of length 2 is called a **transposition.**

Illustrations.

1. (132) is a 3-cycle, where

$$(132) = \begin{pmatrix} 1 & 3 & 2 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

2. (23) is a transposition, $(23) = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$.

3. $(1254) \in S_6$ is a 4-cycle, where

$$(1254) = \begin{pmatrix} 1 & 2 & 5 & 4 & 3 & 6 \\ 2 & 5 & 4 & 1 & 3 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 3 & 1 & 4 & 6 \end{pmatrix}.$$

4. The six elements of S_3 *viz.*

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$
$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

can be conveniently written as

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

Notice that $o(S_3) = 3! = 6$.

5. **(Product of two permutations)**

Let $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$, $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} \in S_4$.

Then
$$(fog)(1) = f(g(1)) = f(3) = 1,$$
$$(fog)(2) = f(g(2)) = f(2) = 4,$$
$$(fog)(3) = f(g(3)) = f(4) = 3,$$
$$(fog)(4) = f(g(4)) = f(1) = 2.$$

$$\therefore \quad fog = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = (24).$$

It may be noticed that while computing the product of two permutations, we apply *right to left* rule :

$$1 \xrightarrow{g} 3 \xrightarrow{f} 1, \quad 2 \xrightarrow{g} 2 \xrightarrow{f} 4, \quad 3 \xrightarrow{g} 4 \xrightarrow{f} 3, \quad 4 \xrightarrow{g} 1 \xrightarrow{f} 2.$$

We have

$$fog = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \text{ and } gof = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} = (12).$$

Thus $fog \neq gof$. In general, $fog \neq gof$ in S_n.

6. $(134)(24) = (1342)$,

$$\because (134)(24) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}.$$

7. The *inverse* of $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$ is

$$f^{-1} = \begin{pmatrix} 2 & 4 & 1 & 3 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}.$$

It can be verified that $fof^{-1} = f^{-1}of = I$. (Identity permutation)

8. The permutation

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 7 & 4 & 1 & 9 & 8 & 5 & 6 & 2 \end{pmatrix} \in S_9$$

can be expressed as

$$f = (134)(2759)(68)$$

i.e., f has been expressed as a product of disjoint cycles. Furthermore, can be expressed as a product of transpositions :

$$f = (14)\,(13)\,(29)\,(25)\,(27)\,(68).$$

The above result is always true.

Theorem 2.5.1. *Every permutation in S_n is uniquely expressible as product of disjoint cycles.*

For the proof, see Algebra by R. Kumar (Brilliant Series)

Corollary. *Every permutation in S_n is expressible as a product transpositions.*

Proof. The corollary follows by the above theorem and the observation

$$(1\ 2\ 3 \ldots m) = (1m)\,(1m-1) \ldots (13)\,(12).$$

Remark. *The decomposition into transpositions is not unique.*

For example, $(1243) = (13)\,(14)\,(12)$,

$(1243) = (13)\,(24)\,(14)$.

Theorem 2.5.2. *If a permutation σ in S_n has r and s number of transpositions in two decompositions of σ as a product of transpositions then r and s are either both even or both odd.*

For the proof, see Algebra by R. Kumar (Brilliant Series)

Definition. (Even and Odd Permutations)

A permutation is called an **even (odd)** *permutation if it can be expressed as a product of an even (odd) number of transpositions.*

Remark 1. From Theorem 2.5.2., it follows that :

Any permutation can either be an even permutation or an odd permutation but not both.

Remark 2. It is easy to verify that :

(*i*) *The product of two even permutations is an even permutation*, since the sum of two even integers is even.

(*ii*) *The product of two odd permutations is an even permutation*, since the sum of two odd integers is even.

(*iii*) *The product of an even (odd) permutation and an odd (even) permutation is an odd permutation*, since the sum of an even (odd) integer and an odd (even) integer is odd.

(*iv*) *The inverse of an even (odd) permutation is an even (odd) permutation*, for if $f = (a_1\, b_1)\,(a_2\, b_2) \ldots (a_m\, b_m)$, then

$$f^{-1} = (a_m\, b_m) \ldots (a_2\, b_2)\,(a_1\, b_1).$$

(*v*) *Identity permutation is an even permutation*, since for any $\sigma \in S_n$, $\sigma \circ \sigma^{-1} = I$ and by the above parts, I is even whether σ is an even (or odd) permutation.

Illustrations.

1. The identity permutation is an even permutation.
2. $(132) = (12)\,(13)$ is an even permutation.

i.e., f has been expressed as a product of disjoint cycles. Furthermore, can be expressed as a product of transpositions :

$$f = (14)\ (13)\ (29)\ (25)\ (27)\ (68).$$

The above result is always true.

Theorem 2.5.1. *Every permutation in S_n is uniquely expressible as a product of disjoint cycles.*

For the proof, see Algebra by R. Kumar (Brilliant Series)

Corollary. *Every permutation in S_n is expressible as a product of transpositions.*

Proof. The corollary follows by the above theorem and the observation :

$$(1\ 2\ 3\ \ldots\ m) = (1m)\ (1m-1)\ \ldots\ (13)\ (12).$$

Remark. *The decomposition into transpositions is not unique.*

For example, $(1243) = (13)\ (14)\ (12)$,

$(1243) = (13)\ (24)\ (14)$.

Theorem 2.5.2. *If a permutation σ in S_n has r and s number of transpositions in two decompositions of σ as a product of transpositions, then r and s are either both even or both odd.*

For the proof, see Algebra by R. Kumar (Brilliant Series)

Definition. (Even and Odd Permutations)

A permutation is called an **even (odd)** *permutation if it can be expressed as a product of an even (odd) number of transpositions.*

Remark 1. From Theorem 2.5.2., it follows that :

Any permutation can either be an even permutation or an odd permutation but not both.

Remark 2. It is easy to verify that :

(*i*) *The product of two even permutations is an even permutation,* since the sum of two even integers is even.

(*ii*) *The product of two odd permutations is an even permutation,* since the sum of two odd integers is even.

(*iii*) *The product of an even (odd) permutation and an odd (even) permutation is an odd permutation,* since the sum of an even (odd) integer and an odd (even) integer is odd.

(*iv*) *The inverse of an even (odd) permutation is an even (odd) permutation,* for if $f = (a_1\ b_1)\ (a_2\ b_2)\ \ldots\ (a_m\ b_m)$, then

$$f^{-1} = (a_m\ b_m)\ \ldots\ (a_2\ b_2)\ (a_1\ b_1).$$

(*v*) *Identity permutation is an even permutation,* since for any $\sigma \in S_n$, $\sigma \circ \sigma^{-1} = I$ and by the above parts, I is even whether σ is an even (or odd) permutation.

Illustrations.

1. The identity permutation is an even permutation.
2. $(132) = (12)\ (13)$ is an even permutation.

3. $(1234) = (14)(13)(12)$ is an odd permutation.
4. A k-cycle $(12 \ldots\ldots k)$ is an even or odd permutation according as k is an odd or even integer.
5. $A_3 = \{I, (123), (132)\}$ is the set of even permutations in S_3.

EXAMPLES

Example 2.5.1. *Determine which of the following permutations are even and odd :*

(*i*) $f = (1\,2\,3\,4\,5)(1\,2\,3)(4\,5)$,

(*ii*) $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 5 & 4 & 3 & 6 & 1 & 9 & 7 & 8 \end{pmatrix}$,

(*iii*) $h = (123)(235)$.

Solution. (*i*) We have

$$f = (15)(14)(13)(12)(13)(12)(45),$$

which being a product of 7 transpositions implies that f is an odd permutation.

(*ii*) $$g = (1256)(34)(798)$$
$$= (16)(15)(12)(34)(78)(79),$$

which being a product of 6 transpositions implies that g is an even permutation.

(*iii*) $$h = (123)(235) = (13)(12)(25)(23).$$

Hence h is an even permutation.

Example 2.5.2. *Prove that there is no permutation a such that*

$$a^{-1}(12)\,a = (34)(15). \qquad \ldots(1)$$

Solution. It is clear that R.H.S. of (1) is an even permutation.

Let $a \in S_n$ be an even permutation

$\Rightarrow a^{-1}$ is an even permutation, and (12) is an odd permutation

$\Rightarrow a^{-1}(12)$ is an odd permutation [Remark 2 (*iii*) of Theorem 2.5.2]

$\Rightarrow a^{-1}(12)\,a$ is an odd permutation. [Remark 2 (*iii*) of Theorem 2.5.2]

Let $a \in S_n$ be an odd permutation

$\Rightarrow a^{-1}$ is an odd permutation and (12) is odd

$\Rightarrow a^{-1}(12)$ is even and a is odd

$\Rightarrow a^{-1}(12)\,a$ is an odd permutation.

Thus L.H.S. of (1) is always an odd permutation for each $a \in S_n$ and R.H.S. of (1) is an even permutation. This is impossible and so the result follows.

Example 2.5.3. *In S_n, prove that there are $\frac{1}{r} \cdot \frac{n!}{(n-r)!}$ distinct cycles of length r $(r \le n)$.*

Solution. The number of distinct arrangements of r numbers out of n numbers $= {}_nP_r = \dfrac{n!}{(n-r)!}$.

Since the cycles

$$(123 \ldots r), (23 \ldots r\,1), \ldots, (r12 \ldots r-1)$$

are all same and these are r in number, it follows that the number of distinct r-cycles in S_n is equal to

$$\frac{1}{r} \cdot \frac{n!}{(n-r)!}.$$

In S_3 :

$$\text{Number of 2-cycles} = \frac{1}{2} \cdot \frac{3!}{(3-2)!} = 3.$$

$$\text{Number of 3-cycles} = \frac{1}{3} \cdot \frac{3!}{(3-3)!} = 2.$$

In S_4 :

$$\text{Number of 2-cycles} = \frac{1}{2} \cdot \frac{4!}{(4-2)!} = 6.$$

$$\text{Number of 3-cycles} = \frac{1}{3} \cdot \frac{4!}{(4-3)!} = 8.$$

$$\text{Number of 4-cycles} = \frac{1}{4} \cdot \frac{4!}{(4-4)!} = 6.$$

Example 2.5.4. *List all the elements of S_4.*

Solution. S_4 consists of all permutations of the set $S = \{1, 2, 3, 4\}$.

All the elements of S_4 are :

I ; (12), (13), (14), (23), (24), (34) ;
(123), (124), (132), (134), (142), (143), (234), (243) ;
(1234), (1243), (1324), (1342), (1423), (1432) ;
(12) (34), (13) (24), (14) (23).

We have $o(S_4) = 24 = 4!$.

Example 2.5.5. *List all the elements of A_4, where A_4 denotes the set of all even permutations in S_4.*

Solution. All the elements of A_4 are

I ; (123), (124), (132), (134), (142), (143), (234), (243) ;
(12) (34), (13) (24), (14) (23).

We have $o(A_4) = 12$.

Remark. By virtue of Theorem 2.5.3, we have

$$A_3 \lhd S_3 \text{ and } o(A_3) = \frac{1}{2}\, o(S_3) = 3,$$

$$A_4 \lhd S_4 \text{ and } o(A_4) = \frac{1}{2}\, o(S_4) = 12.$$

Example 2.5.6. *Find the cycle structure of all the powers of* $\sigma = (12345)$.

Since the cycles

$$(123 \ldots r), (23 \ldots r1), \ldots, (r12 \ldots r-1)$$

are all same and there are r in number, it follows that the number of distinct r-cycles in S_n is equal to

$$\frac{1}{r} \cdot \frac{n!}{(n-r)!}$$

In S_3 :

$$\text{Number of 2-cycles} = \frac{1}{2} \cdot \frac{3!}{(3-2)!} = 3.$$

$$\text{Number of 3-cycles} = \frac{1}{3} \cdot \frac{3!}{(3-3)!} = 2.$$

In S_4 :

$$\text{Number of 2-cycles} = \frac{1}{2} \cdot \frac{4!}{(4-2)!} = 6.$$

$$\text{Number of 3-cycles} = \frac{1}{3} \cdot \frac{4!}{(4-3)!} = 8.$$

$$\text{Number of 4-cycles} = \frac{1}{4} \cdot \frac{4!}{(4-4)!} = 6.$$

Example 2.5.4. *List all the elements of S_4.*

Solution. S_4 consists of all permutations of the set $S = \{1, 2, 3, 4\}$.

All the elements of S_4 are :

I : (12) (13) (14) (23) (24) (34) ;
(123) (124) (132) (134) (142) (143) (234) (243) ;
(1234) (1243) (1324) (1342) (1423) (1432) ;
(12) (34) (13) (24) (14) (23).

We have $o(S_4) = 24 = 4!$.

Example 2.5.5. *List all the elements of A_4, where A_4 denotes the set of all even permutations in S_4.*

Solution. All the elements of A_4 are

I : (123) (124) (132) (134) (142) (143) (234) (243) ;
(12) (34) (13) (24) (14) (23).

We have $o(A_4) = 12$.

Remark. By virtue of Theorem 2.5.3, we have

$$A_3 < S_3 \text{ and } o(A_3) = \frac{1}{2} o(S_3) = 3.$$

$$A_4 < S_4 \text{ and } o(A_4) = \frac{1}{2} o(S_4) = 12.$$

Example 2.5.6. *Find the cycle structure of all the powers of $\sigma = (12345)$.*

Since the cycles

$$(123 \ldots r), (23 \ldots r\,1), \ldots, (r12 \ldots r-1)$$

are all same and these are r in number, it follows that the number of dis r-cycles in S_n is equal to

$$\frac{1}{r} \cdot \frac{n!}{(n-r)!}.$$

In S_3 :

$$\text{Number of 2-cycles} = \frac{1}{2} \cdot \frac{3!}{(3-2)!} = 3.$$

$$\text{Number of 3-cycles} = \frac{1}{3} \cdot \frac{3!}{(3-3)!} = 2.$$

In S_4 :

$$\text{Number of 2-cycles} = \frac{1}{2} \cdot \frac{4!}{(4-2)!} = 6.$$

$$\text{Number of 3-cycles} = \frac{1}{3} \cdot \frac{4!}{(4-3)!} = 8.$$

$$\text{Number of 4-cycles} = \frac{1}{4} \cdot \frac{4!}{(4-4)!} = 6.$$

Example 2.5.4. *List all the elements of S_4.*

Solution. S_4 consists of all permutations of the set $S = \{1, 2, 3, 4\}$.

All the elements of S_4 are :

I ; (12), (13), (14), (23), (24), (34) ;
(123), (124), (132), (134), (142), (143), (234), (243) ;
(1234), (1243), (1324), (1342), (1423), (1432) ;
(12) (34), (13) (24), (14) (23).

We have $o(S_4) = 24 = 4!$.

Example 2.5.5. *List all the elements of A_4, where A_4 denotes the se of all even permutations in S_4.*

Solution. All the elements of A_4 are

I ; (123), (124), (132), (134), (142), (143), (234), (243) ;
(12) (34), (13) (24), (14) (23).

We have $o(A_4) = 12$.

Remark. By virtue of Theorem 2.5.3, we have

$$A_3 \lhd S_3 \text{ and } o(A_3) = \frac{1}{2}\, o(S_3) = 3,$$

$$A_4 \lhd S_4 \text{ and } o(A_4) = \frac{1}{2}\, o(S_4) = 12.$$

Example 2.5.6. *Find the cycle structure of all the powers of* $\sigma = (12345)$.

Solution. We have

$$\sigma^2 = (12345)\,(12345) = (13524),$$
$$\sigma^3 = \sigma^2 \,.\, \sigma = (13524)\,(12345) = (14253),$$
$$\sigma^4 = \sigma^3 \,.\, \sigma = (14253)\,(12345) = (15432),$$
$$\sigma^5 = \sigma^4 \,.\, \sigma = (15432)\,(12345) = I.$$

EXERCISES

1. Express the following as a product of disjoint cycles :

   (*i*) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 5 & 7 & 1 & 6 & 4 \end{pmatrix}$

   (*ii*) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 3 & 9 & 5 & 4 & 7 & 8 & 1 & 6 & 11 & 2 & 10 \end{pmatrix}$

   (*iii*) (1325) (143) (251), (*iv*) (1432) (241) (135).

2. Compute $a^{-1}ba$, where

   (*i*) $a = (134)$, $b = (2354)$.

   (*ii*) $a = (135)\,(12)$, $b = (1579)$.

3. Determine which of the following are even or odd permutations :

   (*i*) (123) (12) (*ii*) (123) (1456)

   (*iii*) (123) (45) (16789) (15) (*iv*) (123) (2345) (23).

4. Given that $f = (1325)\,(143)\,(251)$, express f as a product of disjoint cycles. Also, find the inverse of f and write it as a product of disjoint cycles.

5. Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 1 & 2 & - & - & 7 & 8 & 9 & 6 \end{pmatrix}$ be an even permutation. Find $\sigma(4)$ and $\sigma(5)$.

   [**Hint.** $\sigma = (132)\,(4\,x)\,(5\,y)\,(6789)$

   $= (12)\,(13)\,(4\,x)\,(5\,y)\,(69)\,(68)\,(67)$.

   If $x = 4, y = 5$; then $\sigma = (12)\,(13)\,(69)\,(68)\,(67)$ is an odd permutation, which is contrary to the given hypothesis.

   If $x = 5,\ y = 4$; then

   $\sigma = (12)\,(13)\,(45)\,(69)\,(68)\,(67)$, which is even.

   Hence $\sigma(4) = 5$ and $\sigma(5) = 4$.]

6. If $f = (12)$, $g = (123)$, $h = (1234)$; show that

   $$f^2 = g^3 = h^4 = I \text{ (identity permutation).}$$

7. Find the cycle structure of all the powers of (1 2 3 ... 8).

   [**Hint.** Similar to Example 2.5.6.]

8. Find all the transpositions in S_5. How many they are ?

   [**Hint.** Number of 2-cycles in $S_5 = \dfrac{1}{2}\,\dfrac{5\,!}{(5-2)\,!} = 10$.]

9. Prove that there is no permutation a such that

$$a^{-1}(123)\,a = (13)(578).$$

[Hint. R.H.S. $= (13)(58)(57)$ is an odd permutation.
L.H.S. $= a^{-1}(13)(12)\,a$ is always an even permutation for all $a \in$

10. If $f \in S_n$ is expressible as a product of disjoint cycles : $f = \sigma_1 \sigma_2 \ldots$
where $o(\sigma_i) = m_i$ for $i = 1, 2, \ldots, k$; show that

$$o(f) = \text{l.c.m. of } m_1, m_2, \ldots, m_k.$$

Theorem 2.5.3. *Show that the set A_n of all even permutation of S_n a normal subgroup of S_n and $o(A_n) = \frac{1}{2} n\,!$.* [D.U., 199

Proof. We know $o(S_n) = n\,!$ and A_n is the subset of S_n consisting all even permutations. First of all we show that A_n is a subgroup of S Clearly, A_n is non-empty, since the identity permutation I is an even pe mutation *i.e.*, $I \in A_n$. Let $f, g \in A_n$ so that f and g are even permutation Since the product of two even permutations is even, $fog \in A_n$. Consequentl A_n is a subgroup of S_n (since S_n is finite). Let $W = \{1, -1\}$ be the grou under multiplication. Define

$$\psi : S_n \to W \text{ as follows :}$$

$$\psi(f) = 1, \text{ if } f \text{ is an even permutation} \quad \ldots(1$$

$$= -1, \text{ if } f \text{ is an odd permutation.} \quad \ldots(2$$

We shall prove that ψ is a homomorphism. Let $f, g \in S_n$ be arbitrary

Case I. *Let f, g be both even permutations.*

Then $\psi(f) = \psi(g) = 1$, by (1).

Since fog is even, so by (1)

$$\psi(fog) = 1$$

$$= 1.1 = \psi(f)\,\psi(g).$$

Case II. *Let f, g be both odd permutations.*

Then $\psi(f) = \psi(g) = -1$, by (2).

Since the product of two odd permutations is even, so by (1)

$$\psi(fog) = 1$$

$$= (-1)(-1) = \psi(f)\,\psi(g).$$

Case III. *Let f be even and g be odd.*

Then $\psi(f) = 1$ and $\psi(g) = -1$.

Since fog is odd, $\psi(fog) = -1$, by (2)

$$= 1 \times -1 = \psi(f)\,\psi(g).$$

Similarly, $\psi(fog) = \psi(f)\,\psi(g)$,
where f is odd and g is even.

In any case, ψ is a homomorphism.

Obviously, ψ is onto, since S_n must contain both even and odd permutations ($n \geq 2$). By Fundamental theorem of homomorphism,

$$\frac{S_n}{Ker\,\psi} \approx W; \qquad ...(3)$$

where $\quad Ker\,\psi = \{f \in S_n : \psi(f) = 1\}$.

Now $\quad f \in Ker\,\psi \quad \Leftrightarrow \psi(f) = 1$

$\Leftrightarrow f$ is an even permutation

$\Leftrightarrow f \in A_n$.

$$\therefore \qquad Ker\,\psi = A_n. \qquad ...(4)$$

Since $Ker\,\psi$ is a normal subgroup of S_n, $A_n \lhd S_n$.

From (3) and (4), $\quad \dfrac{S_n}{A_n} \approx W$

$$\Rightarrow \qquad o(W) = o\left(\frac{S_n}{A_n}\right) \quad \text{or} \quad 2 = \frac{o(S_n)}{o(A_n)} = \frac{n!}{o(A_n)}$$

Hence $\quad o(A_n) = \dfrac{n!}{2} = \dfrac{1}{2}\,o(S_n). \qquad ...(5)$

Ex. 1. *Show that the multiplicative group $W = \{1, -1\}$ is a homomorphic image of S_n. Hence show that the set A_n of all even permutations of S_n is a normal subgroup of S_n.* [D.U., 1997]

Ex. 2. *Define an even permutation on a finite set. Show that there are exactly half even permutations on a finite set S which forms a normal subgroup of the group of permutations on S.* [D.U., 1998]

[**Hint.** Let $o(S) = n$ so that $o(S_n) = n!$. Let A_n be the set of all even permutations on S. As shown above, $A_n \lhd S_n$ and $o(A_n) = \frac{1}{2}\,o(S_n)$

i.e., A_n contains exactly half even permutations of S_n.]

EXAMPLES

Example 2.5.7. *If A_3 be the subgroup of S_3 consisting of all even permutations, show that $A_3 \lhd S_3$ and $o(A_3) = \frac{1}{2}\,o(S_3)$. Further show that S_3/A_3 is cyclic.*

Solution. We have

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

Then $\quad A_3 = \{I, (123), (132)\}$ and

$$i(A_3) = o\left(\frac{S_3}{A_3}\right) = \frac{o(S_3)}{o(A_3)} = \frac{6}{3} = 2.$$

Since $\quad i(A_3) = 2$, $A_3 \lhd S_3$ and $o(A_3) = \frac{1}{2}\,o(S_3)$.

Further $\dfrac{S_3}{A_3} = \{A_3, A_3(12)\}$,

where
$$[A_3(12)]^2 = A_3(12)\,A_3(12)$$
$$= A_3(12)(12), \text{ as } A_3 \lhd S_3$$
$$= A_3 I \quad [\because (12)(12) = I]$$
$$= A_3.$$

Hence $\dfrac{S_3}{A_3}$ is a cyclic group generated by $A_3(12)$.

Example 2.5.8. *Show that :*

(*i*) *Every homomorphic image of an abelian group is abelian.*

(*ii*) *Every homomorphic image of a cyclic group is cyclic.*

Show by means of an example that the converse of each of the above results is not true.

Solution. See Example 2.2.7 for parts (*i*) and (*ii*).

(*iii*) The mapping $\phi : S_3 \to \dfrac{S_3}{A_3}$ defined by

$$\phi(f) = A_3 f \;\; \forall \; f \in S_3$$

is an onto homomorphism (Recall $\phi : G \to G/N$ defined by $\phi(g) = Ng$ is an onto homomorphism).

Hence S_3/A_3 is a homomorphic image of S_3, but S_3 is not cyclic (not abelian) where S_3/A_3 is cyclic (abelian). [Example 2.5.7]

Note. From Section 1.16 of Chapter 1, we recall that

If S is a non-empty subset of a group G, then the smallest subgroup of G containing S is called the **subgroup generated** *by S. It is denoted by $\langle S \rangle$.* Further

$$\alpha \in \langle S \rangle \Leftrightarrow \alpha = s_1 s_2 \ldots s_n \; ; \; s_i \in S \text{ and } n \text{ is a positive integer.}$$

This definition will be used in the following problems.

Example 2.5.9. *Show that for $n \geq 3$, the subgroup generated by 3-cycles is A_n.*

Solution. We know A_n is the subgroup of S_n consisting of all even permutations defined on the set $S = \{1, 2, \ldots, n\}$. Let H be a subgroup (of S_n) generated by 3-cycles. We shall show that

$$H = A_n.$$

Let $f \in H$ be arbitrary. Then

$f = \theta_1 \theta_2 \ldots \theta_l$, where each θ_i is a 3-cycle. [See the above **Note**]

Since any 3-cycle $(a_1\, a_2\, a_3)$ is an even permutation and since the product of two even permutations is even, it follows that f is an even permutation *i.e.* $f \in A_n$ for each $f \in H$.

$\therefore \quad H \subseteq A_n.$

Conversely, let $f \in A_n$ be arbitrary. By definition, f is expressible as a product of even number of transpositions and each transposition $(\alpha\ \beta)$ where $\alpha \neq 1$, $\beta \neq 1$ can be expressed as $(1\ \alpha)\ (1\ \beta)\ (1\ \alpha)$. Thus $f \in A_n$ is of the form :

$f = (1\ \alpha_1)\ (1\ \alpha_2) \ldots (1\ \alpha_{k-1})\ (1\ \alpha_k)$; where k is even and $\alpha_i \in \{2, 3, \ldots n\}$

or $f = (1\ \alpha_2\ \alpha_1) \ldots (1\ \alpha_k\ \alpha_{k-1})$.

It follows that f is a product of finite number of 3-cycles. Thus $f \in H$ and so $A_n \subseteq H$.

Hence $A_n = H$.

Example 2.5.10. *Show that every element of A_n is a product of 3-cycles.*

Hint. See the converse part of Example 2.5.9.

Example 2.5.11. *Prove that the alternating group A_n $(n \geq 3)$ may be generated by $(n-2)$, 3-cycles of the form*

$$(123),\ (124),\ \ldots.\ (12n).$$ [D.U., 1993]

Solution. Let K be a subgroup (of S_n) generated by 3-cycles of the form :

$$(123),\ (124),\ \ldots\ (12n). \qquad \ldots(1)$$

We have to show that $K = A_n$.

Let $f \in K$ be arbitrary. Then

$f = \theta_1\ \theta_2 \ldots \theta_l$ where each θ_i is a 3-cycle of the form given in (1).

Since each 3-cycle is an even permutation, so each θ_i is an even permutation. Thus f is an even permutation (since the product of two even permutations is even). It follows that

$$f \in A_n \text{ for each } f \in K \quad i.e., \quad K \subseteq A_n.$$

Conversely, let $f \in A_n$ be arbitrary. Then f is expressible as a product of even number of transpositions and each transposition $(\alpha\ \beta)$ where $\alpha \neq 1$, $\beta \neq 1$ can be expressed as $(1\ \alpha)\ (1\ \beta)\ (1\ \alpha)$. *Hence each $f \in A_n$ is expressible as the product of even number of transpositions* from the set

$$T = \{(12), (13), \ldots, (1n)\}.$$

Let $(1\ \alpha), (1\ \beta) \in T$ be arbitrary.

If $\beta = 2$, then $(1\ \alpha)\ (1\ \beta) = (1\ \beta\ \alpha) = (12\ \alpha) \in K$.

If $\beta \neq 2$, then $(1\ \alpha)\ (1\ \beta) = (1\ \alpha)\ (12)\ (2\ \beta)\ (12)$

$$= (12\ \alpha)\ (1\ \beta\ 2)$$

$$= (12\ \alpha)\ (12\ \beta)^{-1} \in K \text{ for each pair } (1\ \alpha), (1\ \beta) \in T.$$

$\therefore \qquad (1\ \alpha)\ (1\ \beta) \in K.$

It follows that $f \in K\ \forall f \in A_n$. *i.e.,* $A_n \subseteq K$.

Hence $K = A_n$.

Example 2.5.12. *Prove the following :*

(*i*) *Every permutation f in S_n $(n > 1)$ is expressible as a product of transpositions $(12), (13), \ldots, (1n)$.*

(*ii*) *Every permutation f in S_n $(n > 1)$ is expressible as a product of $(12), (23), (34), \ldots, (n-1, n)$.*

Solution. (*i*) Let $f \in S_n$ be arbitrary. Then f is expressible as a product of transpositions. Further any transposition (ab) can be expressed as

$$(ab) = (1a)\,(1b)\,(1a).$$

It follows that $f \in S_n$ is expressible as a product of transpositions of the form $(1x)$, $x \in \{2, 3, \ldots, n\}$.

(*ii*) Let H be the subgroup of S_n generated by the transpositions :

$$(12), (23), (34), \ldots, (n-1, n).$$

We have

$$\left.\begin{aligned} (12) &= (12) \in H, \\ (13) &= (12)\,(23)\,(12) \in H, \\ (14) &= (13)\,(34)\,(13) \in H, \\ \hline (1n) &= (1, n-1)\,(n-1, n)\,(1, n-1) \in H. \end{aligned}\right\} \quad \ldots(1)$$

Let $f \in S_n$ be arbitrary. Then f is expressible as a product of transpositions. Consider any transposition (ab). If a or b is 1, then $(1\,b)$ or $(a\,1) = (1\,a) \in H$ [Using (1)]. If $a \neq 1$ and $b \neq 1$, then

$$(ab) = (1a)\,(1b)\,(1a) \in H, \text{ using (1).}$$

It follows that $f \in H\ \forall f \in S_n$ and so $S_n \subseteq H$.

Hence $f \in S_n \Rightarrow f \in H \Rightarrow f$ is expressible as a product of $(12), (23), (34), \ldots, (n-1, n)$.

It may, however, be noted that

$$S_n = H, \text{ since } H < S_n.$$

Example 2.5.13. *Prove that the permutation group S_n $(n \geq 2)$ is generated by $n-1$ transpositions*

$$(12), (23), (34), \ldots, (n-1, n).$$ [D.U., 1996]

Solution. See part (*ii*) of Example 2.5.12.

Example 2.5.14. *Show that the permutations (12) and $(1\,2\,3 \ldots n)$ generate the permutation group S_n.* [D.U., 1995, 94]

Or

Show that the smallest subgroup of S_n containing (12) and $(1\,2\,3 \ldots n)$ is S_n.

Solution. Let H be the subgroup of S_n generated by (12) and $(123 \ldots n)$. Let $f \in S_n$ be arbitrary. Then f can be expressed as the product of transpositions. Further any transposition (ab) is expressible as

$$(ab) = (1a)\,(1b)\,(1a).$$

Thus each $f \in S_n$ is expressible as a product of transpositions of the form $(1n)$. ...(1)

Clearly,

$$(1n) = (n, n-1, \ldots 3\ 2\ 1)\ (12)\ (1\ 2\ 3 \ldots n) \in H.$$

It follows that

$$(n, n-1) = (n, n-1, \ldots 3\ 2\ 1)\ (1n)\ (1\ 2\ 3 \ldots n) \in H\ ;$$

$$(n-1, n-2) = (n, n-1, \ldots 3\ 2\ 1)\ (n, n-1)\ (123 \ldots n) \in H\ ;$$

and so on. Proceeding likewise, we obtain

$(n-2, n-3), \ldots, (43), (32) \in H$. Consequently

$$(12) = (12) \in H$$

$$(13) = (12)\ (23)\ (12) \in H$$

$$(14) = (13)\ (34)\ (13) \in H$$

$$(1n) \in H.$$

Using these results in (1), it follows that $f \in H\ \forall f \in S_n$. So $S_n \subseteq H$. Obviously, $H \subseteq S_n$. Hence $S_n = H$.

Example 2.5.15. *Let H be a subgroup of S_n $(n \geq 2)$. If H contains an odd permutation, show that the set of all even permutations in H forms a normal subgroup of H of index 2.*

Solution. Consider the multiplicative group $W = \{1, -1\}$. Define a mapping $\psi : H \to W$ as

$$\psi(f) = 1, \text{ if } f \text{ is an even permutation in } H$$
$$= -1, \text{ if } f \text{ is an odd permutation in } H.$$

As shown in Theorem 2.5.3, ψ is a homomorphism. Since H contains an odd permutation and, of course, even permutations ; ψ is onto. By Fundamental theorem of homomorphism,

$$\frac{H}{Ker\,\psi} \approx W, \qquad \ldots(1)$$

where $\quad Ker\,\psi = \{f \in H : \psi(f) = 1\}$.

$\therefore \quad f \in Ker\,\psi \Leftrightarrow \psi(f) = 1 \Leftrightarrow f$ is an even permutation in H.

Thus $\quad Ker\,\psi = A_H$ (the set of all even permutations in H).

Putting in (1), $\quad \dfrac{H}{A_H} \approx W. \qquad \ldots(2)$

Since $\quad Ker\,\psi \lhd H,\ A_H \lhd H$ and further by (2),

$$i(A_H) = o\left(\frac{H}{A_H}\right) = o(W) = 2.$$

Example 2.5.16. *Let H be a subgroup of S_n $(n \geq 2)$. Show that either all permutations in H are even or exactly half are even.*

Solution. Refer to Example 2.5.15. It is clear that H cannot contain only odd permutations, since identity permutation in H is even. If H contains all even permutations, the first part of the problem is proved. Suppose now H contains an odd permutation, then by Example 2.5.15,

$$\frac{H}{A_H} \approx W, \qquad \ldots(1)$$

where A_H is the normal subgroup of even permutations of H.

From (1), we have

$$o\left(\frac{H}{A_H}\right) = \frac{o(H)}{o(A_H)} = o(W) = 2$$

$$\Rightarrow \qquad o(A_H) = \frac{1}{2}\, o(H).$$

Hence, in H, exactly half permutations are even.

Example 2.5.17. *Show that A_4 has no subgroup of order 6.*

Solution. By definition, A_4 is the set of all even permutations defined on the set $S = \{1, 2, 3, 4\}$. By Theorem 2.5.3,

$$A_4 < S_4 \text{ and } o(A_4) = \frac{1}{2}\, o(S_4) = \frac{4!}{2} = 12.$$

We know that any 3-cycle is even. $[\because (abc) = (bc)(ca)]$

Consequently, all 3-cycles of S_4 belong to A_4. We know that the number of distinct r-cycles $(r \le n)$ in $S_n = \dfrac{1}{r}\dfrac{n!}{(n-r)!}$ [See Example 2.5.3]

Thus the number of distinct 3-cycles in S_4 (and hence in A_4) is

$$= \frac{1}{3}\frac{4!}{(4-3)!} = 8.$$

Suppose, on the contrary, A_4 has a subgroup (say H) of order 6 *i.e.*, $H < A_4$ and $o(H) = 6$. Since there are 8 distinct 3-cycles in A_4 and $o(H) = 6$, all 3-cycles of A_4 cannot belong to H. Let σ be a 3-cycle of A_4 such that $\sigma \notin H$. As $o(\sigma) = 3$, $K = \{\sigma, \sigma^2, \sigma^3 = I\}$ is a subgroup of A_4 and $o(K) = 3$.

Since $\quad \sigma^3 = I, \sigma^2 = \sigma^{-1} \notin H$

$(\because \sigma^{-1} \in H \Rightarrow \sigma \in H$, which is a contradiction)

Thus $\quad H \cap K = \{I\} \qquad (\because \sigma \notin H$ and $\sigma^2 \notin H)$

Now

$$o(HK) = \frac{o(H)\, o(K)}{o(H \cap K)} = \frac{6 \times 3}{1} = 18.$$

This is impossible, since $HK \subseteq A_4$ and $o(A_4) = 12$. Hence A_4 has no subgroup of order 6.

Solution. Refer to Example 2.5.15. It is clear that H cannot contain only odd permutations, since identity permutation in H is even. If H contains *all* even permutations, the first part of the problem is proved. Suppose now H contains an odd permutation, then by Example 2.5.15,

$$\frac{H}{A_H} \approx W, \qquad \ldots(1)$$

where A_H is the normal subgroup of even permutations of H.

From (1), we have

$$o\left(\frac{H}{A_H}\right) = \frac{o(H)}{o(A_H)} = o(W) = 2$$

$$\Rightarrow \qquad o(A_H) = \frac{1}{2}\, o(H).$$

Hence, in H, exactly half permutations are even.

Example 2.5.17. *Show that A_4 has no subgroup of order 6.*

Solution. By definition, A_4 is the set of all even permutations defined on the set $S = \{1, 2, 3, 4\}$. By Theorem 2.5.3,

$$A_4 \lhd S_4 \text{ and } o(A_4) = \frac{1}{2}\, o(S_4) = \frac{4\,!}{2} = 12.$$

We know that any 3-cycle is even. $[\because (abc) = (bc)(ca)]$

Consequently, all 3-cycles of S_4 belong to A_4. We know that the number of distinct r-cycles $(r \le n)$ in $S_n = \dfrac{1}{r}\dfrac{n\,!}{(n-r)\,!}$ [See Example 2.5.3]

Thus the number of distinct 3-cycles in S_4 (and hence in A_4) is

$$= \frac{1}{3}\frac{4\,!}{(4-3)\,!} = 8.$$

Suppose, on the contrary, A_4 has a subgroup (say H) of order 6 *i.e.*, $H < A_4$ and $o(H) = 6$. Since there are 8 distinct 3-cycles in A_4 and $o(H) = 6$, all 3-cycles of A_4 cannot belong to H. Let σ be a 3-cycle of A_4 such that $\sigma \notin H$. As $o(\sigma) = 3$, $K = \{\sigma, \sigma^2, \sigma^3 = I\}$ is a subgroup of A_4 and $o(K) = 3$.

Since $\quad \sigma^3 = I, \sigma^2 = \sigma^{-1} \notin H$

$(\because \sigma^{-1} \in H \Rightarrow \sigma \in H$, which is a contradiction)

Thus $\quad H \cap K = \{I\} \qquad (\because \sigma \notin H$ and $\sigma^2 \notin H)$

Now

$$o(HK) = \frac{o(H)\, o(K)}{o(H \cap K)} = \frac{6 \times 3}{1} = 18.$$

This is impossible, since $HK \subseteq A_4$ and $o(A_4) = 12$. Hence A_4 has no subgroup of order 6.

3

AUTOMORPHISMS AND CONJUGATE ELEMENTS

In this chapter we discuss *Automorphisms of a group, Conjugate elements, Conjugate classes, Class equation of a finite group and its applications, Cauchy's Theorem, Similar and Conjugate permutations in S_n.*

3.1 Automorphism

Definition. *An isomorphism of a group G onto itself is called an* **automorphism** *of G.*

In other words, a mapping $f : G \to G$ is an **automorphism,** *if f is a homomorphism, one-to-one and onto.*

Illustrations.

1. The identity mapping $I : G \to G$ defined as $I(x) = x$ for all $x \in G$ is an automorphism. I is called a *trivial automorphism*.
2. The mapping $f : (\mathbf{Z}, +) \to (\mathbf{Z}, +)$ defined as $f(x) = -x$ is an automorphism. Notice that

   $f(x + y) = -(x + y) = (-x) + (-y) = f(x) + f(y) \Rightarrow f$ is a homomorphism ;

   $f(x) = f(y) \Rightarrow -x = -y \Rightarrow x = y \Rightarrow f$ is one-to-one.

   For any $x \in \mathbf{Z}$, $x = -(-x) \Rightarrow x = f(-x)$, $-x \in \mathbf{Z} \Rightarrow f$ is onto.

   Thus f is an automorphism of $\mathbf{Z}$.
3. The mapping $f : (\mathbf{R}^+, .) \to (\mathbf{R}^+, .)$ defined as $f(x) = x^2$ is an automorphism.

   Here $(\mathbf{R}^+, .)$ denotes the group of positive real numbers under multiplication.
4. Let $G = \langle a \rangle$, $a^{12} = e$. The mapping $f : G \to G$ defined as $f(x) = x^3$ for all $x \in G$ is **not** an automorphism, since f is not one-to-one. Notice that

   $$a \neq a^5 \quad \text{but} \quad f(a) = f(a^5) = a^3.$$

   [Indeed $f(a^5) = a^{15} = a^{12} \cdot a^3 = e \cdot a^3 = a^3$]

Notation. *The set of all automorphisms of a group G is denoted by $Aut\,(G)$.*

Recall that $A(G)$ is the group of all one-to-one mappings of G onto itself. Thus

$$Aut\,(G) \subseteq A(G).$$

It will help to remember that

$$T \in Aut\,(G) \Leftrightarrow T : G \to G \text{ is a homo. ; } 1-1 \text{ and onto.}$$