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 $S_5 = \frac{1}{2}\frac{5!}{(5-2)!} = 10$.]

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 $a \in S$

10. If $f \in S_n$ is expressible as a product of disjoint cycles : $f = \sigma_1 \sigma_2 \ldots \sigma$
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 $Ker\,\psi = \{f \in S_n : \psi(f) = 1\}$.

Now $f \in Ker\,\psi \Leftrightarrow \psi(f) = 1$

$\Leftrightarrow f$ is an even permutation

$\Leftrightarrow f \in A_n$.

$\therefore \quad Ker\,\psi = A_n$. ...(4)

Since $Ker\,\psi$ is a normal subgroup of S_n, $A_n \triangleleft S_n$.

From (3) and (4), $\dfrac{S_n}{A_n} \approx W$

$$\Rightarrow \quad o(W) = o\left(\frac{S_n}{A_n}\right) \quad \text{or} \quad 2 = \frac{o(S_n)}{o(A_n)} = \frac{n!}{o(A_n)}$$

Hence $o(A_n) = \dfrac{n!}{2} = \dfrac{1}{2}\,o(S_n)$. ...(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, $A_n \triangleleft S_n$ 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 $A_3 \triangleleft S_3$ 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 $A_3 = \{I, (123), (132)\}$ and

$$i(A_3) = o\left(\frac{S_3}{A_3}\right) = \frac{o(S_3)}{o(A_3)} = \frac{6}{3} = 2.$$

Since $i(A_3) = 2$, $A_3 \triangleleft S_3$ and $o(A_3) = \frac{1}{2}\,o(S_3)$.

Further $$\frac{S_3}{A_3} = \{A_3, A_3(12)\},$$

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 $\frac{S_3}{A_3}$ 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 $\phi : S_3 \to \frac{S_3}{A_3}$ 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*

$$(123),\ (124),\ \ldots.\ (12n). \qquad \text{[D.U., 1993]}$$

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 $(1\ \alpha)\ (1\ \beta) = (1\ \alpha)\ (12)\ (2\ \beta)\ (12)$

$$= (12\ \alpha)\ (1\ \beta\ 2)$$

$$= (12\ \alpha)\ (12\ \beta)^{-1} \in K \text{ for each pair } (1\ \alpha),\ (1\ \beta) \in T.$$

$\therefore$ $(1\ \alpha)\ (1\ \beta) \in K$.

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), ..., (1*n*).

(*ii*) *Every permutation f in* S_n $(n > 1)$ *is expressible as a product of* (12), (23), (34), ..., $(n-1, n)$.

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 $(1x)$, $x \in \{2, 3, ..., n\}$.

(*ii*) Let H be the subgroup of S_n generated by the transpositions :

$$(12), (23), (34), \ldots, (n-1, n).$$

We have

$$\left.\begin{aligned} (12) &= (12) \in H, \\ (13) &= (12)\,(23)\,(12) \in H, \\ (14) &= (13)\,(34)\,(13) \in H, \\ &\cdots\cdots\cdots \\ (1n) &= (1, n-1)\,(n-1, n)\,(1, n-1) \in H. \end{aligned}\right\} \quad \ldots(1$$

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), ..., $(n-1, n)$.

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 ... *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 ... *n*) *is* S_n.

Solution. Let H be the subgroup of S_n generated by (12) and (123 ... 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

$$(12) = (12) \in H$$

$$(13) = (12)\ (23)\ (12) \in H$$

$$(14) = (13)\ (34)\ (13) \in H$$

$$\overline{\qquad\qquad}$$

$$(1n) \in H.$$

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 $Ker\,\psi = \{f \in H : \psi(f) = 1\}$.

$\therefore\ f \in Ker\,\psi \Leftrightarrow \psi(f) = 1 \Leftrightarrow f$ is an even permutation in H.

Thus $Ker\,\psi = A_H$ (the set of all even permutations in H).

Putting in (1), $$\frac{H}{A_H} \approx W. \qquad \ldots(2)$$

Since $Ker\,\psi \lhd H$, $A_H \lhd H$ 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,

$$\frac{H}{A_H} \simeq W, \qquad \ldots(1)$$

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 $\quad H \cap K = \{I\}$

Now $\qquad (\because \sigma \notin H$ and $\sigma^2 \notin H)$

$$o(HK) = \frac{o(H)\, o(K)}{o(H \cap K)} = \frac{6 \times 3}{1} = 18.$$

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 $\sigma^3 = I, \sigma^2 = \sigma^{-1} \notin H$

$(\because \sigma^{-1} \in H \Rightarrow \sigma \in H$, which is a contradiction)

Thus $H \cap K = \{I\}$ $(\because \sigma \notin H$ 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 $f : (Z, +) \to (Z, +)$ 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 $x \in Z$, $x = -(-x) \Rightarrow x = f(-x)$, $-x \in Z \Rightarrow f$ is onto.
   Thus f is an automorphism of Z.
3. The mapping $f : (R^+, .) \to (R^+, .)$ defined as $f(x) = x^2$ is an automorphism.
   Here $(R^+, .)$ 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
   $a \neq a^5$ but $f(a) = f(a^5) = a^3$.
   [Indeed $f(a^5) = a^{15} = a^{12} . a^3 = e . a^3 = a^3$]

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

$$T \in Aut\,(G) \Leftrightarrow T : G \to G \text{ is a homo. ; } 1-1 \text{ and onto.}$$

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 $G = (a)$, $a^{12} = e$. 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
   $a \neq a^5$ but $f(a) = f(a^5) = a^3$.
   [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

$$T \in Aut(G) \Leftrightarrow T: G \to G \text{ is a homo.; } 1-1 \text{ and onto.}$$

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 $f : (Z, +) \to (Z, +)$ 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 $x \in Z$, $x = -(-x) \Rightarrow x = f(-x)$, $-x \in Z \Rightarrow f$ is onto.
   Thus f is an automorphism of Z.
3. The mapping $f : (R^+, .) \to (R^+, .)$ defined as $f(x) = x^2$ is an automorphism.
   Here $(R^+, .)$ 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
   $a \neq a^5$ but $f(a) = f(a^5) = a^3$.
   [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

$$T \in Aut(G) \Leftrightarrow T : G \to G \text{ is a homo. ; } 1\text{-}1 \text{ and onto.}$$

3.3 Theorems on Automorphisms

Theorem 3.3.1. *If $f \in Aut\ (G)$, then*

(i) $f(e) = e$

(ii) $o(f(a)) = o(a)$, *where $a \in G$ is of finite order and* $o(a) \neq 0$

Proof. (i) By Theorem 3.2.1 (a finite f), if $f : G \to G'$ is a homomorphism, then

$$f(e) = e',$$

where $f : G \to G'$ is a homomorphism, so

$$f(e) = e, \qquad (\because e^2 = e \text{ in } G)$$

(ii) Let $o(a) = n$ so that n is the least positive integer such that

$$a^n = e.$$

Now
$$a^n = e \quad \Rightarrow \quad f(a^n) = f(e)$$

$$\Rightarrow \quad \underbrace{f(a) \cdot f(a) \cdots f(a)}_{n \text{ times}} = e, \quad \text{since } f \text{ is a homomorphism}$$

$$\Rightarrow \quad (f(a))^n = e.$$

We shall prove that n is the least positive integer satisfying (2), for if possible, $(f(a))^m = e$ for some positive integer m, $0 < m < n$. Then

$$f(a^m) = f(e), \text{ since } f \text{ is a homomorphism}$$

$$\Rightarrow \quad a^m = e, \ 0 < m < n; \text{ since } f \text{ is one-to-one.}$$

This contradicts (1).

Hence
$$o(f(a)) = n = o(a).$$

Theorem 3.2.2. *Show that $Aut\ (G)$ is a subgroup of $A\ (G)$.*

Proof. Let $T_1, T_2 \in Aut\ (G)$. Then each of T_1 and T_2 is a homomorphism, one-to-one mapping of G onto G. Consequently,

$$T_1 \circ T_2 : G \to G \text{ is one-to-one and onto.}$$

Now we show that $T_1 \circ T_2$ is a homomorphism.

Let $a, b \in G$. Then

$$\begin{aligned}(T_1 \circ T_2)(ab) &= T_1[T_2(ab)], \text{ by definition of } \circ \\ &= T_1[T_2(a)\, T_2(b)], \text{ since } T_2 \text{ is a homo.} \\ &= T_1(T_2(a))\, T_1(T_2(b)), \text{ since } T_1 \text{ is a homo.} \\ &\quad \text{and } T_2(a), T_2(b) \in G \\ &= (T_1 \circ T_2)(a)\,(T_1 \circ T_2)(b).\end{aligned}$$

Thus $T_1 \circ T_2$ is a homomorphism and so

$$T_1 \circ T_2 \in Aut\ (G) \text{ for all } T_1, T_2 \in Aut\ (G).$$

Finally, we show that

$$T \in Aut\ (G) \quad \Rightarrow T^{-1} Aut\ (G).$$

3.2 Theorems on Automorphisms

Theorem 3.2.1. *If $T \in Aut\,(G)$, then*

(i) $T(e) = e$.

(ii) $o(T(a)) = o(a)$, *where* $a \in G$ *is of order* $o(a) > 0$.

Proof. (i) By Theorem 2.2.1 (Chapter 2), if $f : G \to G'$ is a homomorphism, then

$$f(e) = e'.$$

Here $T : G \to G$ is a homomorphism, so

$$T(e) = e. \qquad (\because e' = e \text{ in } G)$$

(ii) Let $o(a) = n$ so that n is the least positive integer such that

$$a^n = e. \tag{1}$$

Now $$a^n = e \Rightarrow T(a^n) = T(e)$$

$$\Rightarrow \underbrace{T(a)\,.\,T(a)\,...\,T(a)}_{n \text{ times}} = e, \quad \text{since } T \text{ is a homomorphism}$$

$$\Rightarrow \{T(a)\}^n = e. \tag{2}$$

We shall prove that n is the least positive integer satisfying (2). If, if possible, $\{T(a)\}^m = e$ for some positive integer m, $0 < m < n$. Then

$$T(a^m) = T(e), \text{ since } T \text{ is a homomorphism}$$

$$\Rightarrow a^m = e, 0 < m < n \text{ ; since } T \text{ is one-to-one.}$$

This contradicts (1).

Hence $$o\{T(a)\} = n = o(a).$$

Theorem 3.2.2. *Show that $Aut\,(G)$ is a subgroup of $A\,(G)$.*

Proof. Let $T_1, T_2 \in Aut\,(G)$. Then each of T_1 and T_2 is a homomorphism, one-to-one mapping of G onto G. Consequently,

$$T_1 \circ T_2 : G \to G \text{ is one-to-one and onto.}$$

Now we show that $T_1 \circ T_2$ is a homomorphism.

Let $a, b \in G$. Then

$$(T_1 \circ T_2)(ab) = T_1[T_2(ab)], \text{ by definition of } \circ$$

$$= T_1[T_2(a)\,T_2(b)], \text{ since } T_2 \text{ is a homo.}$$

$$= T_1(T_2(a))\,T_1(T_2(b)), \text{ since } T_1 \text{ is a homo.}$$

and $T_2(a), T_2(b) \in G$

$$= (T_1 \circ T_2)(a)\,(T_1 \circ T_2)(b).$$

Thus $T_1 \circ T_2$ is a homomorphism and so

$$T_1 \circ T_2 \in Aut\,(G) \text{ for all } T_1, T_2 \in Aut\,(G).$$

Finally, we show that

$$T \in Aut\,(G) \Rightarrow T^{-1} Aut\,(G).$$

3.2 Theorems on Automorphisms

Theorem 3.2.1. *If $T \in Aut\,(G)$, then*

(i) $T(e) = e$.

(ii) $o(T(a)) = o(a)$, *where $a \in G$ is of order $o(a) > 0$.*

Proof. (*i*) By Theorem 2.2.1 (Chapter 2), if $f : G \to G'$ is a homomorphism, then

$$f(e) = e'.$$

Here $T : G \to G$ is a homomorphism, so

$$T(e) = e. \qquad (\because\ e' = e \text{ in } G)$$

(*ii*) Let $o(a) = n$ so that n is the least positive integer such that

$$a^n = e.$$

Now $a^n = e \Rightarrow T(a^n) = T(e)$

$$\Rightarrow \underbrace{T(a)\,.\,T(a)\,...\,T(a)}_{n \text{ times}} = e, \quad \text{since } T \text{ is a homomorphism}$$

$$\Rightarrow \{T(a)\}^n = e.$$

We shall prove that n is the least positive integer satisfying (2). If possible, $\{T(a)\}^m = e$ for some positive integer m, $0 < m < n$. Then

$$T(a^m) = T(e), \text{ since } T \text{ is a homomorphism}$$

$$\Rightarrow a^m = e,\ 0 < m < n\ ; \text{ since } T \text{ is one-to-one.}$$

This contradicts (1).

Hence $o\{T(a)\} = n = o(a)$.

Theorem 3.2.2. *Show that $Aut\,(G)$ is a subgroup of $A\,(G)$.*

Proof. Let $T_1, T_2 \in Aut\,(G)$. Then each of T_1 and T_2 is a homomorphism, one-to-one mapping of G onto G. Consequently,

$$T_1 \circ T_2 : G \to G \text{ is one-to-one and onto.}$$

Now we show that $T_1 \circ T_2$ is a homomorphism.

Let $a, b \in G$. Then

$$\begin{aligned}(T_1 \circ T_2)(ab) &= T_1[T_2(ab)], \text{ by definition of } \circ \\ &= T_1[T_2(a)\,T_2(b)], \text{ since } T_2 \text{ is a homo.} \\ &= T_1(T_2(a))\,T_1(T_2(b)), \text{ since } T_1 \text{ is a homo} \\ &\quad \text{and } T_2(a), T_2(b) \in G \\ &= (T_1 \circ T_2)(a)\,(T_1 \circ T_2)(b).\end{aligned}$$

Thus $T_1 \circ T_2$ is a homomorphism and so

$$T_1 \circ T_2 \in Aut\,(G) \text{ for all } T_1, T_2 \in Aut\,(G).$$

Finally, we show that

$$T \in Aut\,(G) \Rightarrow T^{-1}\ Aut\,(G).$$

Since $T : G \to G$ is one-to-one and onto, so $T^{-1} : G \to G$ is also one-to-one and onto. Now we show that T^{-1} is a homomorphism.

Let $a, b \in G$ be arbitrary. Since T is onto, there exist $a_1, b_1 \in G$ such that

$$T(a_1) = a \text{ and } T(b_1) = b$$

$$\Rightarrow \quad a_1 = T^{-1}(a) \text{ and } b_1 = T^{-1}(b).$$

Now $$ab = T(a_1)\, T(b_1)$$

$$\Rightarrow \quad ab = T(a_1 b_1), \text{ since } T \text{ is a homomorphism}$$

$$\Rightarrow \quad T^{-1}(ab) = a_1 b_1$$

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

$$\Rightarrow \quad T^{-1} \text{ is a homomorphism}$$

$$\Rightarrow \quad T^{-1} \in Aut(G) \text{ for all } T \in Aut(G). \qquad \ldots(2)$$

From (1) and (2), it follows that $Aut(G)$ is a subgroup of $A(G)$.

Remark. *$Aut(G)$ is referred to as the group of automorphisms of G.*

Theorem 3.2.3. *If a be any fixed element of a group G, then the mapping $T_a : G \to G$ defined by $T_a(x) = axa^{-1}$ for all $x \in G$ is an automorphism of G.*

Proof. Let x, y be any two arbitrary elements of G. Then

$$T_a(xy) = a(xy)\, a^{-1}$$

$$= (axa^{-1})\,(aya^{-1}) \qquad (\because\ a^{-1}a = e)$$

$$= T_a(x)\, T_a(y).$$

Thus T_a is a homomorphism.

Now $T_a(x) = T_a(y) \Rightarrow axa^{-1} = aya^{-1} \Rightarrow x = y$, by cancellation law in G.

Thus T_a is one-to-one.

Let $g \in G$ be arbitrary. Then

$$g = a(a^{-1} g\, a)\, a^{-1} \qquad (\because\ a\, a^{-1} = e)$$

$$g = a\, g_1\, a^{-1}, \text{ where } g_1 = a^{-1} g\, a \in G$$

$$\Rightarrow \quad g = T_a(g_1),\ g_1 \in G$$

$$\Rightarrow \quad T_a \text{ is onto.}$$

Hence T_a is an automorphism of G.

Ex. *Show that the mapping $T_a : G \to G$ defined by*

$$T_a(x) = a^{-1} x\, a \quad \forall \ x \in G \text{ is an automorphism of } G.$$

Definition. (Inner Automorphism)

Let a be any element of a group G. The automorphism $T_a : G \to G$ defined by

$$T_a(x) = a\,x\,a^{-1} \quad \forall\ x \in G$$

is called an **inner automorphism** *of G.*

The set of all inner automorphisms of G is denoted by I (G). Thus

$$I(G) = \{T_a : a \in G\}.$$

Theorem 3.2.4. *For any group G, show that I (G) is a normal subgroup of Aut (G).* [D.U., 1992, S]

Proof. Firstly, we show that $I(G)$ is a subgroup of $Aut(G)$.

Let $T_a, T_b \in I(G)$. We proceed to show that

$$T_a \circ T_b = T_{ab}.$$

For any $x \in G$, we have

$$\begin{aligned}(T_a \circ T_b)(x) &= T_a(T_b(x)) \\ &= T_a(b\,x\,b^{-1}) = a(b\,x\,b^{-1})\,a^{-1} \\ &= (ab)\,x\,(ab)^{-1}, \text{ since } (ab)^{-1} = b^{-1}a^{-1} \\ &= T_{ab}(x)\end{aligned}$$

$$\therefore \qquad T_a \circ T_b = T_{ab} \quad \forall\ a, b \in G. \qquad \ldots(1)$$

From (1), it follows that $T_a \circ T_b \in I(G)$.

Using (1), we see that

$$T_a \circ T_a^{-1} = T_{aa^{-1}} = T_e,$$

where $\qquad T_e(x) = e\,x\,e^{-1} = x = I(x),\ x \in G$

$\Rightarrow \qquad T_e = I$ and so $T_a \circ T_a^{-1} = I$ implies that

$$(T_a)^{-1} = T_a^{-1}\ \forall\ T_a \in I(G). \qquad \ldots(2)$$

From (2), it follows that $(T_a)^{-1} \in I(G)$ for each $T_a \in I(G)$. Hence $I(G)$ is a subgroup of $Aut(G)$. Now we prove that $I(G)$ is a normal subgroup of $Aut(G)$.

i.e., $\qquad T \circ T_a \circ T^{-1} \in I(G) \quad \forall\ T \in Aut(G)$ and $T_a \in I(G)$.

Let $x \in G$ be arbitrary. Then

$$\begin{aligned}(T \circ T_a \circ T^{-1})(x) &= (T \circ T_a)(T^{-1}(x)) \\ &= (T \circ T_a)(y), \text{ where } y = T^{-1}(x) \in G \\ &= T(T_a(y)) = T(a\,y\,a^{-1}) \\ &= T(a)\,T(y)\,T(a^{-1}), \text{ as } T \text{ is a homo.} \\ &= T(a)\,T(T^{-1}(x))\,\{T(a)\}^{-1}, \text{ as } T \text{ is a homo.} \\ &= b\,(T \circ T^{-1})(x)\,b^{-1}, \text{ where } b = T(a) \in G \\ &= b\,I(x)\,b^{-1}, \text{ as } T \circ T^{-1} = I \\ &= b\,x\,b^{-1} = T_b(x)\end{aligned}$$

$$\therefore \qquad T \circ T_a \circ T^{-1} = T_b \in I(G). \qquad (\because\ b \in G)$$

Hence $I(G)$ is a normal subgroup of $Aut(G)$.

$$T_a(x) = a\,x\,a^{-1} \quad \forall\ x \in G$$

is called an **inner automorphism** *of G.*

The set of all inner automorphisms of G is denoted by I (G). Thus

$$I(G) = \{T_a : a \in G\}.$$

Theorem 3.2.4. *For any group G, show that I (G) is a normal sub-group of Aut (G).* [D.U., 1998, 93]

Proof. Firstly, we show that $I(G)$ is a subgroup of $Aut(G)$.

Let $T_a, T_b \in I(G)$. We proceed to show that

$$T_a \circ T_b = T_{ab}.$$

For any $x \in G$, we have

$$\begin{aligned}(T_a \circ T_b)(x) &= T_a(T_b(x)) \\ &= T_a(b\,x\,b^{-1}) = a\,(b\,x\,b^{-1})\,a^{-1} \\ &= (ab)\,x\,(ab)^{-1}, \text{ since } (ab)^{-1} = b^{-1}\,a^{-1} \\ &= T_{ab}(x)\end{aligned}$$

$$\therefore \qquad T_a \circ T_b = T_{ab} \quad \forall\ a, b \in G. \qquad \ldots(1)$$

From (1), it follows that $T_a \circ T_b \in I(G)$.

Using (1), we see that

$$T_a \circ T_a^{-1} = T_{aa^{-1}} = T_e,$$

where

$$T_e(x) = e\,x\,e^{-1} = x = I(x),\ x \in G$$

$$\Rightarrow \qquad T_e = I \quad \text{and so} \quad T_a \circ T_a^{-1} = I \text{ implies that}$$

$$(T_a)^{-1} = T_a^{-1}\ \forall\ T_a \in I(G). \qquad \ldots(2)$$

From (2), it follows that $(T_a)^{-1} \in I(G)$ for each $T_a \in I(G)$. Hence $I(G)$ is a subgroup of $Aut(G)$. Now we prove that $I(G)$ is a normal subgroup of $Aut(G)$.

i.e., $\quad T \circ T_a \circ T^{-1} \in I(G) \quad \forall\ T \in Aut(G)$ and $T_a \in I(G)$.

Let $x \in G$ be arbitrary. Then

$$\begin{aligned}(T \circ T_a \circ T^{-1})(x) &= (T \circ T_a)(T^{-1}(x)) \\ &= (T \circ T_a)(y), \text{ where } y = T^{-1}(x) \in G \\ &= T(T_a(y)) = T(a\,y\,a^{-1}) \\ &= T(a)\,T(y)\,T(a^{-1}), \text{ as } T \text{ is a homo.} \\ &= T(a)\,T(T^{-1}(x))\,\{T(a)\}^{-1}, \text{ as } T \text{ is a homo.} \\ &= b\,(T \circ T^{-1})(x)\,b^{-1}, \text{ where } b = T(a) \in G \\ &= b\,I(x)\,b^{-1}, \text{ as } T \circ T^{-1} = I \\ &= b\,x\,b^{-1} = T_b(x)\end{aligned}$$

$$\therefore \qquad T \circ T_a \circ T^{-1} = T_b \in I(G). \quad (\because\ b \in G)$$

Hence $I(G)$ is a normal subgroup of $Aut(G)$.

Theorem 3.2.5. *For any group G, prove that*

$$I(G) \simeq \frac{G}{Z},$$

where $I(G)$ is the group of inner automorphisms of G and Z is the centre of G. [D.U., 1998, 94]

Proof. We know that

$$Z = \{g \in G : gx = xg \ \forall\, x \in \ \}, \ Z \lhd G$$

and $I(G) = \{T_a : a \in G\}$, where

$$T_a(x) = a\,x\,a^{-1} \ \forall\, x \in G. \qquad ...(1)$$

We define a mapping

$$\psi : \psi : G \to I(G) \text{ as } \psi(a) = T_a \ \forall\, a \in G. \qquad ...(2)$$

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

$$\psi(ab) = T_{ab}. \qquad ...(3)$$

For any $x \in G$, we have

$$\begin{aligned} T_{ab} &= ab\,x\,(ab)^{-1}, \text{ by (1)} \\ &= ab\,x\,b^{-1}\,a^{-1} \\ &= a\,y\,a^{-1}, \text{ where } y = b\,x\,b^{-1} \in G \\ &= T_a(y), \text{ by (1)} \\ &= T_a(T_b(x)), \text{ since } y = b\,x\,b^{-1} = T_b(x) \\ &= (T_a \, o \, T_b)(x). \end{aligned}$$

Thus $T_a \, o \, T_b = T_{ab} \ \forall\ a, b \in G.$ ...(4)

From (3) and (4), we get

$$\psi(ab) = T_a \, o \, T_b$$

or $$\psi(ab) = \psi(a) \, o \, \psi(b), \text{ by (2)}.$$

Thus ψ is a homomorphism. Obviously, ψ is onto. Hence by Fundamental Theorem of Homomorphism,

$$\frac{G}{Ker\,\psi} \simeq I(G) \quad \text{or} \quad I(G) \simeq \frac{G}{Ker\,\psi}. \qquad ...(5)$$

$$\begin{aligned} \text{Now } g \in Ker\,\psi &\Leftrightarrow \psi(g) = I, \text{ identity of } I(G) \\ &\Leftrightarrow T_g = I, \text{ by (2)} \\ &\Leftrightarrow T_g(x) = x, \ \forall\, x \in G \\ &\Leftrightarrow g\,x\,g^{-1} = x, \ \forall\, x \in G \\ &\Leftrightarrow g\,x = xg, \ \forall\, x \in G \\ &\Leftrightarrow g \in Z. \end{aligned}$$

$$\therefore \quad Ker\,\psi = Z. \qquad ...(6)$$

From (5) and (6), we obtain

$$I(G) \simeq \frac{G}{Z}.$$

EXAMPLES

Example 3.2.1. *Show that $T : G \to G$ such that $T(x) = x^{-1}$ is an automorphism of G if and only if G is abelian.*

Solution. Let T be an automorphism of G. Let $g_1, g_2 \in G$ be arbitrary.

As given,

$$T(g_1 g_2) = (g_1 g_2)^{-1}$$

$$\Rightarrow \quad T(g_1)\, T(g_2) = g_2^{-1} g_1^{-1}, \text{ since } T \text{ is a homomorphism}$$

$$\Rightarrow \quad g_1^{-1} g_2^{-1} = g_2^{-1} g_1^{-1}, \text{ as given}$$

$$\Rightarrow \quad (g_1^{-1} g_2^{-1})^{-1} = (g_2^{-1} g_1^{-1})^{-1}$$

$$\Rightarrow \quad (g_2^{-1})^{-1} (g_1^{-1})^{-1} = (g_1^{-1})^{-1} (g_2^{-1})^{-1}$$

$$\Rightarrow \quad g_2 g_1 = g_1 g_2 \quad \forall \ g_1, g_2 \in G.$$

Hence G is abelian.

Conversely, let G be abelian. We shall prove

$$T : G \to G \text{ defined by } T(x) = x^{-1} \ \forall \ x \in G$$

is an automorphism. Let $x, y \in G$. We have

$$T(xy) = (xy)^{-1} = y^{-1} x^{-1}$$
$$= x^{-1} y^{-1}, \text{ since } G \text{ is abelian}$$
$$= T(x)\, T(y)$$

Thus T is a homomorphism.

Now $T(x) = T(y) \Rightarrow x^{-1} = y^{-1} \Rightarrow (x^{-1})^{-1} = (y^{-1})^{-1} \Rightarrow x = y$.

Thus T is one-to-one.

For any $x \in G$, $x = (x^{-1})^{-1} = g^{-1}$, where $g = x^{-1} \in G$.

Thus $x = g^{-1} \Rightarrow x = T(g) \Rightarrow T$ is onto. Hence T is an automorphism of G.

Example 3.2.2. *Let G be a finite abelian group of order n, and let m be a positive integer prime to n. Show that the mapping $\sigma : x \to x^m$ is an automorphism of G.*

Solution. We are given, $\sigma(x) = x^m \ \forall \ x \in G$.

Let $x, y \in G$. Then

$$\sigma(xy) = (xy)^m$$
$$= x^m y^m, \text{ since } G \text{ is abelian}$$
$$= \sigma(x)\, \sigma(y).$$

Thus σ is a homomorphism.

Since $(m, n) = 1$, there exist integers r and s such that $mr + ns = 1$.

Let $x \in G$. Then

$$x = x^{mr+ns} = x^{mr} x^{ns} = (x^r)^m (x^n)^s, \text{ where } x^n = e.$$

$\therefore$

$$x = x^{mr} \quad \forall \quad x \in G \qquad \ldots(1)$$

or $x = y^m$, where $y = x^r \in G$.

$\therefore$ $x = \sigma(y)$, $y \in G$. Thus σ is onto.

In order to show that σ is one-to-one, we prove that

$Ker(\sigma) = \{e\}$.

Let $g \in Ker(\sigma)$ be arbitrary. Then $\sigma(g) = e$

$\Rightarrow$ $g^m = e \Rightarrow g^{mr} = e \Rightarrow g = e$, by (1)

$\Rightarrow$ $Ker(\sigma) = \{e\} \Rightarrow \sigma$ is one-to-one.

Hence σ is an automorphism of G.

Example 3.2.3. *Let $G = \langle a \rangle$ be a finite cyclic group of order n. Show that the mapping $\sigma : a \to a^m$ is an automorphism if and only if m and n are relatively prime.*

Solution. Let $(m, n) = 1$. Then by Example 3.2.2, $\sigma : a \to a^m$ is an automorphism.

Conversely, let σ be an automorphism.

Then $o(a) = o\{\sigma(a)\} \Rightarrow o(a^m) = n.$ ...(1)

Let $(m, n) = d$ so that d divides m and $n \Rightarrow m/d$ and n/d are positive integers. We have

$$(a^m)^{n/d} = (a)^{mn/d} = (a^n)^{m/d} = (e)^{m/d} = e.$$

$\therefore$ $o(a^m)^{n/d} = e.$ ...(2)

From (1) and (2), it follows that n divides n/d and so $d = 1$.

Hence $(m, n) = 1$.

Example 3.2.4. *Show that $I(G) = \{I\}$ if and only if G is abelian.*

Solution. We know $I(g) = \{T_g ; g \in G\}$, where

$$T_g(x) = g x g^{-1} \quad \forall \quad x \in G.$$

Now $I(G) = \{I\}$ $\Leftrightarrow$ $T_g = I$ $\forall$ $g \in G$

$\Leftrightarrow$ $T_g(x) = I(x)$ $\forall$ $x \in G$ and $g \in G$

$\Leftrightarrow$ $g x g^{-1} = x$ $\forall$ $g, x \in G$

$\Leftrightarrow$ $gx = xg$ $\forall$ $g, x \in G$

$\Leftrightarrow$ G is abelian.

Example 3.2.5. *If G is a group such that $x^2 \neq e$ for some $x \in G$, then G has a non-trivial automorphism.*

Solution. The identity mapping $I : G \to G$ defined as $I(x) = x$ $\forall$ $x \in G$ is called a *trivial automorphism.*

If G is abelian, then $T : G \to G$ defined as $T : x \to x^{-1}$ is an automorphism. [See Example 3.2.1]

Further $T \neq I$, for $T = I \Rightarrow T(g) = I(g)$ $\forall$ $g \in G$

$\Rightarrow$ $g^{-1} = g$ $\forall$ $g \in G$ $\Rightarrow$ $g^2 = e$ $\forall$ $g \in G$,

where is contrary to the given hypotheses. Thus T is a non-trivial automorphism of G, if G is abelian.

If G is non-abelian, then there exists some inner automorphism $T_g \neq I$, for if $T_g = I \ \forall \ g \in G$, then

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

$$\Rightarrow \qquad gx = xg \quad \forall \ g, x \in G \ \Rightarrow \ G \text{ is abelian,}$$

which is a contradiction. In any case, G has a non-trivial automorphism.

Example 3.2.6. *Find Aut (G), if G is an infinite cyclic group.* [D.U., 199

Or

Show that if G is an infinite cyclic group, then Aut (G) is isomorphic to a cyclic group of order 2.

Solution. Let $G = \langle a \rangle = \{a^i : i = 0, \pm 1, \pm 2, \ldots\}$ be an infinite cyclic group. Since G is infinite, therefore

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

Let T be any automorphism of G. Since $T(a) \in G = \langle a \rangle$,

$$T(a) = a^m \qquad \ldots(2)$$

for some integer m. Since T is onto ; for $a \in G$, there exists some $x \in G$ such that $T(x) = a$. Now $x \in G = \langle a \rangle \Rightarrow x = a^n$ for some integer n.

Thus $a = T(x) = T(a^n) = T(a) \cdot T(a) \ldots T(a)$ (n times),

since T is a homomorphism

$$\therefore \quad a = \{T(a)\}^n = \{a^m\}^n = a^{mn}, \text{ using (2)}$$

$$\Rightarrow \qquad a^{mn-1} = e \ \Rightarrow \ mn - 1 = 0, \text{ using (1)}$$

$$\Rightarrow \qquad mn = 1 \ \Rightarrow \ m = \pm 1 \text{ (Also } n = \pm 1).$$

Using in (2), it follows that if T is any automorphism of G, then

$$T(a) = a \quad \text{or} \quad T(a) = a^{-1}.$$

Hence $Aut(G) = \{I, T\}$, where

$$I(x) = x \quad \forall \ x \in G \quad \text{and} \quad T(x) = x^{-1} \quad \forall \ x \in G.$$

Since $o\,[Aut(G)] = 2$; $Aut(G)$ is cyclic. Since any two cyclic groups of the same order are isomorphic,

$$Aut(G) \simeq C_2,$$

where C_2 is a cyclic group of order 2.

Example 3.2.7. *Find Aut (G), if G is a finite cyclic group of order n.*

Or

Show that $o\,[Aut(G)] = \phi(n)$, where G is a finite cyclic group of order n and $\phi(n)$ is Euler ϕ-function. [D.U., 1997]

Or

Show that if G is a finite cyclic group of order n, then $Aut(G) \simeq U_n$, where U_n is the group of integers less than n and relatively prime to n under multiplication modulo n. [D.U., 1996]

If G is non-abelian, then there exists some inner automor $T_g \neq I$, for if $T_g = I \; \forall \; g \in G$, then

$$T_g(x) = I(x) \quad \forall \quad x \in G \Rightarrow g x g^{-1} = x \quad \forall \quad g, x \in G$$

$$\Rightarrow \quad gx = xg \quad \forall \; g, x \in G \Rightarrow G \text{ is abelian,}$$

which is a contradiction. In any case, G has a non-trivial automorphism

Example 3.2.6. *Find Aut (G), if G is an infinite cyclic group.*

Or [D.U., 1

Show that if G is an infinite cyclic group, then Aut (G) is isomor to a cyclic group of order 2.

Solution. Let $G = \langle a \rangle = \{a^i : i = 0, \pm 1, \pm 2, \ldots\}$ be an infinite cy group. Since G is infinite, therefore

$$a^i = e \quad \Leftrightarrow \quad i = 0.$$

Let T be any automorphism of G. Since $T(a) \in G = \langle a \rangle$,

$$T(a) = a^m$$

for some integer m. Since T is onto ; for $a \in G$, there exists so $x \in G$ such that $T(x) = a$. Now $x \in G = \langle a \rangle \Rightarrow x = a^n$ for some integer

Thus $a = T(x) = T(a^n) = T(a) \cdot T(a) \ldots T(a)$ (n times),

since T is a homomorphis

$$\therefore \quad a = \{T(a)\}^n = \{a^m\}^n = a^{mn}, \text{ using (2)}$$

$$\Rightarrow \quad a^{mn-1} = e \Rightarrow mn - 1 = 0, \text{ using (1)}$$

$$\Rightarrow \quad mn = 1 \Rightarrow m = \pm 1 \text{ (Also } n = \pm 1).$$

Using in (2), it follows that if T is any automorphism of G, then

$$T(a) = a \quad \text{or} \quad T(a) = a^{-1}.$$

Hence $Aut(G) = \{I, T\}$, where

$$I(x) = x \quad \forall \; x \in G \quad \text{and} \quad T(x) = x^{-1} \quad \forall \; x \in G.$$

Since $o[Aut(G)] = 2$; $Aut(G)$ is cyclic. Since any two cyclic group of the same order are isomorphic,

$$Aut(G) \simeq C_2,$$

where C_2 is a cyclic group of order 2.

Example 3.2.7. *Find Aut (G), if G is a finite cyclic group of order*

Or

Show that $o[Aut(G)] = \phi(n)$, where G is a finite cyclic group of orde n and $\phi(n)$ is Euler ϕ-function. [D.U., 199

Or

Show that if G is a finite cyclic group of order n, then Aut (G) $\simeq U_n$ where U_n is the group of integers less than n and relatively prime to n under multiplication modulo n. [D.U., 199

Solution. Let $G = \langle a \rangle$, where $a^n = e$ $(a \neq e)$.

Let $T \in Aut\,(G)$ be arbitrary. Since $T(a) \in G$, therefore

$$T(a) = a^i, \text{ for some integer } i,\ 0 < i < n. \qquad ...(1)$$

[Note that $i = 0$ or $n \Rightarrow a^i = e \Rightarrow T(a) = e \Rightarrow T(a) = T(e) \Rightarrow a = e$, which is a contradiction]

Since T is an automorphism, therefore

$$o\,(T(a)) = o\,(a) = n. \qquad ...(2)$$

Now we show that $(i, n) = 1$. ...(3)

Let, if possible, $(i, n) = k$ (k being a positive integer).

Then k divides i and n and so i/k and n/k are positive integers.

We have

$$\{T(a)\}^{n/k} = \{a^i\}^{n/k} = a^{in/k} = (a^n)^{i/k} = e^{i/k} = e$$

$\Rightarrow$ $o\,\{T(a)\} = n$ divides n/k

$\Rightarrow$ $k = 1 \Rightarrow (i, n) = 1$.

From (1) and (3), it follows that

$$Aut\,(G) = \{T : T(x) = x^i,\ 0 < i < n \text{ and } (i, n) = 1\}. \qquad ...(4)$$

Hence $o\,[Aut\,(G)] = \phi(n)$, where $\phi(n)$ is Euler ϕ-function.

Finally, we show that $Aut\,(G) \approx U_n$.

For the sake of convenience, we write (4) as follows :

$$Aut\,(G) = \{T_i : T_i(x) = x^i \ \forall\ x \in G,\ 0 < i < n \text{ and } (i, n) = 1\}. \qquad ...(5)$$

Define a mapping $\phi : U_n \to Aut\,(G)$ as

$$\phi(i) = T_i \ \forall\ i \in U_n \qquad ...(6)$$

[Recall that $i \in U_n \Leftrightarrow 0 < i < n$ and $(i, n) = 1$.]

Clearly ϕ is onto and one-to-one.

Now we show that ϕ is a homomorphism.

Let $i, j \in U_n$. Then $\phi(ij) = T_{ij}$, by (6).

For any $x \in G$, $T_{ij}(x) = x^{ij}$, by (5)

$$= (x^j)^i = T_i(x^j) = T_i(T_j(x)), \text{ by (5)}$$

$$= T_i\, o\, T_j(x) \text{ and so } T_{ij} = T_i\, o\, T_j = \phi(i)\, o\, \phi(j).$$

$\therefore$ $\phi(ij) = \phi(i)\, o\, \phi(j) \Rightarrow \phi$ is a homomorphism, Hence

$U_n \approx A(G)$ or $A(G) \approx U_n$.

Example 3.2.8. *Find* $Aut\,(G)$, *if* $G = \langle a \rangle$, $a^{12} = e$.

Solution. The positive integers less than 12 and relatively prime to 12 are 1, 5, 7, 11. *i.e.*, $\phi(12) = 4$. We have

$$Aut\,(G) = \{I, T_1, T_2, T_3\};$$

where $I(x) = x \ \forall\ x \in G$,

$T_1(x) = x^5 \ \forall\ x \in G$,

$$T_2(x) = x^7 \quad \forall \ x \in G,$$

$$T_3(x) = x^{11} \quad \forall \ x \in G.$$

Hence $o[Aut(G)] = \phi(12)$.

Ex. 1. *Find Aut (G), where* $G = \langle a \rangle$, $a^{10} = e$.

Ex. 2. *Find Aut (G), where* $G = \langle a \rangle$, $a^{15} = e$.

Example 3.2.9. *Determine Aut (G), where G is Klein's 4-group.* [D.U., 1995, 94]

Or

Let G be a group of order 4, $G = \{e, a, b, ab\}$, $a^2 = b^2 = e$, $ab = ba$. *Determine Aut (G).*

Solution. We have $(ab)^2 = ab\,ab = aa\,bb$ $(\because ba = ab)$

$$= a^2 b^2 = e \,.\, e = e$$

Thus $x^2 = e \quad \forall \ x \in G.$

Let $T \in Aut(G)$ be arbitrary. Then $T(e) = e$.

We know $o(x) = o\{T(x)\} \ \forall \ x \in G.$

Since a, b, ab are all of order 2, therefore

$$T(a) = a \text{ or } b \text{ or } ab.$$

If $T(a)$ is fixed, $T(x)$ is known for each $x \in G$. Thus T is completely determined and further there cannot be more then six automorphisms of G *viz.*

$I : e \to e,\ a \to a,\ b \to b,\ ab \to ab$;

$T_1 : e \to e,\ a \to a,\ b \to ab,\ ab \to b$;

$T_2 : e \to e,\ a \to b,\ b \to a,\ ab \to ab$;

$T_3 : e \to e,\ a \to b,\ b \to ab,\ ab \to a$;

$T_4 : e \to e,\ a \to ab,\ b \to a,\ ab \to b$;

$T_5 : e \to e,\ a \to ab,\ b \to ab,\ ab \to a$.

Hence $Aut(G) = \{I, T_1, T_2, T_3, T_4, T_5\}$.

Example 3.2.10. *Show that* $Aut(G) \approx S_3$, *where G is Klein's 4-group.*

Solution. Refer to above example. We know

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

and $Aut(G) = \{I, T_1, T_2, T_3, T_4, T_5\}$.

Define a mapping $\phi : Aut(G) \to S_3$ as

$$\phi(I) = e,\ \phi(T_2) = (12),\ \phi(T_1) = (23)$$

$$\phi(T_5) = (13),\ \phi(T_3) = (123),\ \phi(T_4) = (132)$$

[Take $1 \leftrightarrow a$, $2 \leftrightarrow b$, $3 \leftrightarrow ab$]

It is easy to verify that ϕ is one-to-one, onto and homomorphism. Hence $Aut(G) \approx S_3$.

Example 3.2.11. *For $G = S_3$, prove that $G \approx I(G)$.*

Or

Show that : $I(S_3) \approx S_3$.

Solution. We know

$$G = S_3 \Rightarrow Z(G) = \{e\}.$$

By Theorem 3.2.5, we have

$$\frac{G}{Z(G)} \approx I(G)$$

For $G = S_3$, $\quad \frac{G}{\{e\}} \approx I(G).$ ...(1)

We know $\quad G \approx \frac{G}{\{e\}}.$ ...(2)

From (1) and (2),

$$G \approx I(G),\ G = S_3 \text{ or } I(S_3) \approx S_3.$$

Notice that $\quad I(S_3) = \{T_e, T_{(12)}, T_{(23)}, T_{(13)}, T_{(123)}, T_{(132)}\}.$

Example 3.2.12. *Determine Aut (S_3).*

Or

Show that : $Aut(S_3) \approx S_3$. [D.U., 1998, 97]

Solution. We know

$$S_3 = \{e, (12), (23), (31), (123), (132),\} \text{ where}$$

$$(12)^2 = (23)^2 = (31)^2 = e \text{ and } (123)^3 = (132)^3 = e.$$

Thus the elements (12), (23) and (13) are all of order 2 and (123), (132) are of order 3.

If T be any automorphism of G ; then

$$o(x) = o\{T(x)\} \quad \forall \quad x \in S_3.$$

Consequently, $T\{(123)\} = (123)$ or (132) ;

and $\quad T\{(12)\} = (12)$ or (23) or (13).

If $T\{(12)\}$ and $T\{(123)\}$ are fixed, $T(x)$ is known for each $x \in S_3$.

Hence T is completely determined. Further there cannot be more than six automorphisms of S_3. Hence

$$Aut(S_3) = I(S_3) \approx S_3. \qquad \text{(See Example 3.2.11)}$$

Example 3.2.13. *Let G be a group, H a subgroup of G, T an automorphism of G. Prove that*

$$T(H) = \{T(h) : h \in H\}$$

is a subgroup of G.

Further show that if H is a normal subgroup of G, then T(H) is also a normal subgroup of G.

Solution. It is clear that $T(H)$ is non-empty, since $e \in H \Rightarrow T(e) \in H$.

Let $a, b \in T(H)$ be arbitrary. Then

$$a = T(h_1),\ b = T(h_2) \quad \text{for some} \quad h_1, h_2 \in H.$$

We have $ab^{-1} = T(h_1)\,[T(h_2)]^{-1}$

$= T(h_1)\,T(h_2^{-1})$, since T is a homomorphism

$= T(h_1 h_2^{-1})$, since T is a homomorphism

Now $H < G \Rightarrow h_1 h_2^{-1} \in H \Rightarrow T(h_1 h_2^{-1}) \in T(H)$.

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

Hence $T(H)$ is a subgroup of G.

Now we show that $H \lhd G \Rightarrow T(H) \lhd G$.

Let $g \in G$ and $n \in T(H)$ be arbitrary. Then

$$n = T(h) \quad \text{for some} \quad h \in H.$$

Since $T : G \to G$ is onto ; for $g \in G$, there exists some $g_1 \in G$ such that $T(g_1) = g$.

We have

$$g n g^{-1} = T(g_1)\,T(h)\,T(g_1)^{-1}$$

$= T(g_1 h)\,T(g_1^{-1})$, since T is a homomorphism

$= T(g_1 h g_1^{-1})$, since T is a homomorphism

Since $H \lhd G$, therefore $g_1 h g_1^{-1} \in H$ and so

$$T(g_1 h g_1^{-1}) \in T(H)$$

$$\Rightarrow \quad g n g^{-1} \in T(H)\ \forall\ g \in G \quad \text{and} \quad n \in T(H).$$

Hence $T(H)$ is a normal subgroup of G.

Remark. Sometimes we write $T(x)$ as xT. Accordingly $T(H)$ is denoted as $(H)T$, where

$$(H)T = \{hT : h \in H\}.$$

Example 3.2.14. *Let G be a group and Z the centre of G. If T is an automorphism of G, prove that $T(Z) \subset Z$.*

Solution. We know $\quad Z = \{a \in G : ag = ga\ \forall\ g \in G\}$

and $\quad T(Z) = \{T(a) : a \in Z\}$.

Let $y \in T(Z)$ be arbitrary. Then

$$y = T(a) \text{ for some } a \in Z. \qquad \ldots(1)$$

Now $\quad a \in Z \Rightarrow ag = ga\ \forall\ g \in G. \qquad \ldots(2)$

Since $T : G \to G$ is onto ; for any $g \in G$, there exists some $g_1 \in G$ such that

$$T(g_1) = g. \qquad \ldots(3)$$

We have $yg = T(a)\,T(g_1)$, by (1) and (3)

Solution. It is clear that $T(H)$ is non-empty,

since $e \in H \Rightarrow T(e) \in H$.

Let $a, b \in T(H)$ be arbitrary. Then

$$a = T(h_1),\ b = T(h_2) \quad \text{for some } h_1, h_2 \in H.$$

We have $ab^{-1} = T(h_1)\,[T(h_2)]^{-1}$

$= T(h_1)\,T(h_2^{-1})$, since T is a homomorphism

$= T(h_1 h_2^{-1})$, since T is a homomorphism

Now $H < G \Rightarrow h_1 h_2^{-1} \in H \Rightarrow T(h_1 h_2^{-1}) \in T(H)$.

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

Hence $T(H)$ is a subgroup of G.

Now we show that $H < G \Rightarrow T(H) < G$.

Let $g \in G$ and $n \in T(H)$ be arbitrary. Then

$$n = T(h) \quad \text{for some } h \in H.$$

Since $T : G \to G$ is onto ; for $g \in G$, there exists some $g_1 \in G$ such that

$$T(g_1) = g.$$

We have

$$g n g^{-1} = T(g_1)\,T(h)\,T(g_1)^{-1}$$

$= T(g_1 h)\,T(g_1^{-1})$, since T is a homomorphism

$= T(g_1 h g_1^{-1})$, since T is a homomorphism

Since $H < G$, therefore $g_1 h g_1^{-1} \in H$ and so

$$T(g_1 h g_1^{-1}) \in T(H)$$

$$\Rightarrow \quad g n g^{-1} \in T(H)\ \forall\ g \in G \quad \text{and} \quad n \in T(H).$$

Hence $T(H)$ is a normal subgroup of G.

Remark. Sometimes we write $T(x)$ as xT. Accordingly $T(H)$ is denoted as $(H)\,T$, where

$$(H)\,T = \{h\,T : h \in H\}.$$

Example 3.2.14. *Let G be a group and Z the centre of G. If T is an automorphism of G, prove that $T(Z) \subset Z$.*

Solution. We know $\quad Z = \{a \in G : ag = ga\ \forall\ g \in G\}$

and $\quad T(Z) = \{T(a) : a \in Z\}$.

Let $y \in T(Z)$ be arbitrary. Then

$$y = T(a) \text{ for some } a \in Z.$$

Now $\quad a \in Z \Rightarrow ag = ga\ \forall\ g \in G.$

Since $T : G \to G$ is onto ; for any $g \in G$, there exists some $g_1 \in G$ such that

$$T(g_1) = g.$$

We have $yg = T(a)\,T(g_1)$, by (1) and (3)

Solution. It is clear that $f(H)$ is non-empty.

since $e \in H \Rightarrow f(e) \in H$.

Let $a, b \in f(H)$ be arbitrary. Then

$$a = f(h_1),\ b = f(h_2) \quad \text{for some} \quad h_1, h_2 \in H.$$

We have $ab^{-1} = f(h_1)[f(h_2)]^{-1}$

$= f(h_1) f(h_2^{-1})$, since f is a homomorphism

$= f(h_1 h_2^{-1})$, since f is a homomorphism

Now $H < G \Rightarrow h_1 h_2^{-1} \in H \Rightarrow f(h_1 h_2^{-1}) \in f(H)$.

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

Hence $f(H)$ is a subgroup of G.

Now we show that $H < G \Rightarrow f(H) < G$.

Let $g \in G$ and $x \in f(H)$ be arbitrary. Then

$$x = f(h) \quad \text{for some} \quad h \in H.$$

Since $f : G \to G$ is onto ; for $g \in G$, there exists some $g_1 \in G$ such that

$$f(g_1) = g.$$

We have

$$gxg^{-1} = f(g_1) f(h) f(g_1)^{-1}$$

$= f(g_1 h) f(g_1^{-1})$, since f is a homomorphism

$= f(g_1 h g_1^{-1})$, since f is a homomorphism

Since $H \lhd G$, therefore $g_1 h g_1^{-1} \in H$ and so

$$f(g_1 h g_1^{-1}) \in f(H)$$

$\Rightarrow \quad gxg^{-1} \in f(H) \ \forall\ g \in G$ and $x \in f(H)$.

Hence $f(H)$ is a normal subgroup of G.

Remark. Sometimes we write $f(x)$ as xf. Accordingly $f(H)$ is denoted as $(H)f$, where

$$(H)f = \{hf : h \in H\}.$$

Example 3.2.14. Let G be a group and f the inner automorphism of G, given that $f(Z) \subset Z$.

Solution. We know $\quad Z = \{a \in G : ag = ga \ \forall\ g \in G\}$

and $\quad f(Z) = \{f(a) : a \in Z\}$.

Let $y \in f(Z)$ be arbitrary. Then

$$y = f(a) \quad \text{for some} \quad a \in Z.$$

Now $\quad a \in Z \Rightarrow ag = ga \ \forall\ g \in G$.

Since $f : G \to G$ is onto ; for any $g \in G$, there exists some $g_1 \in G$ such that

$$f(g_1) = g.$$

We have $yg = f(a) f(g_1)$, by (1) and (2)

Solution. It is clear that $T(H)$ is non-empty, since $e \in H \Rightarrow T(e) \in H$.

Let $a, b \in T(H)$ be arbitrary. Then

$$a = T(h_1),\ b = T(h_2) \quad \text{for some} \quad h_1, h_2 \in H.$$

We have $ab^{-1} = T(h_1)\,[T(h_2)]^{-1}$

$= T(h_1)\,T(h_2^{-1})$, since T is a homomorphism

$= T(h_1\,h_2^{-1})$, since T is a homomorphism

Now $H < G \Rightarrow h_1\,h_2^{-1} \in H \Rightarrow T(h_1\,h_2^{-1}) \in T(H)$.

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

Hence $T(H)$ is a subgroup of G.

Now we show that $H \lhd G \Rightarrow T(H) \lhd G$.

Let $g \in G$ and $n \in T(H)$ be arbitrary. Then

$$n = T(h) \quad \text{for some} \quad h \in H.$$

Since $T : G \to G$ is onto ; for $g \in G$, there exists some $g_1 \in G$ such that

$$T(g_1) = g.$$

We have

$$g\,n\,g^{-1} = T(g_1)\,T(h)\,T(g_1)^{-1}$$

$= T(g_1\,h)\,T(g_1^{-1})$, since T is a homomorphism

$= T(g_1\,h\,g_1^{-1})$, since T is a homomorphism

Since $H \lhd G$, therefore $g_1\,h\,g_1^{-1} \in H$ and so

$$T(g_1\,h\,g_1^{-1}) \in T(H)$$

$$\Rightarrow \qquad g\,n\,g^{-1} \in T(H)\ \forall\ g \in G \quad \text{and} \quad n \in T(H).$$

Hence $T(H)$ is a normal subgroup of G.

Remark. Sometimes we write $T(x)$ as xT. Accordingly $T(H)$ is denoted as $(H)\,T$, where

$$(H)\,T = \{h\,T : h \in H\}.$$

Example 3.2.14. *Let G be a group and Z the centre of G. If T is an automorphism of G, prove that $T(Z) \subset Z$.*

Solution. We know $\quad Z = \{a \in G : ag = ga\ \forall\ g \in G\}$

and $\quad T(Z) = \{T(a) : a \in Z\}$.

Let $y \in T(Z)$ be arbitrary. Then

$$y = T(a) \text{ for some } a \in Z. \qquad \ldots(1)$$

Now $\quad a \in Z \Rightarrow ag = ga\ \forall\ g \in G.$ $\qquad \ldots(2)$

Since $T : G \to G$ is onto ; for any $g \in G$, there exists some $g_1 \in G$ such that

$$T(g_1) = g. \qquad \ldots(3)$$

We have $yg = T(a)\,T(g_1)$, by (1) and (3)

$= T(a\, g_1)$, since T is a homomorphism

$= T(g_1\, a)$, by (2)

$= T(g_1)\, T(a)$, since T is a homomorphism

$= gy$, by (1) and (3).

$\therefore \quad yg = gy \quad \forall \quad g \in G$

$\Rightarrow \quad y \in Z$ for each $y \in T(Z)$.

Hence $T(Z) \subset Z$.

Example 3.2.15. *Let G be a group and T an automorphism of G. Prove that for $a \in G$,*

$$N(aT) = (N(a))\, T,$$

where $N(a)$ is the normalizer of a in G.

Solution. By definition, $N(a) = \{x \in G : xa = ax\}$

and $(N(a))\, T = \{xT : x \in N(a)\}$.

(Here $T(x)$ is denoted as xT)

Let $y \in (N(a))\, T$ be arbitrary. Then

$y = xT$ for some $x \in N(a)$. ...(1)

Since $x \in N(a)$, $xa = ax$. ...(2)

Consider $y(aT) = (xT)(aT)$, by (1)

$= (xa)\, T$, since T is a homomorphism

$= (ax)\, T$, by (2)

$= (aT)(xT)$, since T is a homomorphism

$= (aT)\, y$, by (1)

$\therefore \quad y(aT) = (aT)\, y \quad \Rightarrow \quad y \in N(aT)$.

Consequently, $(N(a))\, T \subseteq N(aT)$. ...(3)

Conversely, let $g \in N(aT)$ be arbitrary. Then

$g(aT) = (aT)\, g$. ...(4)

Since $T : G \to G$ is onto ; for $g \in G$, there exists some $g_1 \in G$ such that $g_1 T = g$. Using in (4), we get

$(g_1 T)(aT) = (aT)(g_1 T)$

$\Rightarrow \quad (g_1 a)\, T = (a\, g_1)\, T$, since T is a homomorphism

$\Rightarrow \quad g_1 a = a\, g_1$, since T is one-to-one

$\Rightarrow \quad g_1 \in N(a)$

$\Rightarrow \quad g_1 T \in (N(a))\, T$

$\Rightarrow \quad g \in (N(a))\, T \quad \forall \quad g \in N(aT)$.

$\therefore \quad N(aT) \subseteq (N(a))\, T$. ...(5)

From (3) and (5), $N(aT) = (N(a))\, T$.

Example 3.2.16. *Let $f : G \to G$ defined as $f(a) = a^n$* ...(1)

be an automorphism, show that $a^{n-1} \in Z(G)$ for all $a \in G$.

Solution. Let $a, x \in G$ be arbitrary. By (1), we have

$$f(a^{-n} x a^n) = (a^{-n} x a^n)^n$$
$$= (a^{-n} x a^n)(a^{-n} x a^n) \ldots (a^{-n} x a^n) \quad (n \text{ times})$$
$$= a^{-n} (x x \ldots x) a^n \qquad [\because a^n a^{-n} = a^0 = e]$$
$$= a^{-n} x^n a^n$$
$$= f(a^{-1}) f(x) f(a), \text{ by (1).}$$

$\therefore$ $f(a^{-n} x a^n) = f(a^{-1} x a)$, since f is a homomorphism

$a^{-n} x a^n = a^{-1} x a$, since f is one-to-one.

On pre-multiplying by a^n and post-multiplying by a^{-1}, we get

$$x a^{n-1} = a^{n-1} x \quad \text{for all} \quad a, x \in G$$

Hence $a^{n-1} \in Z(G)$ for all $a \in G$.

Example 3.2.17. *Let G be a finite group, T an automorphism of G with the property :*

$$xT = x \text{ for } x \in G \text{ if and only if } x = e. \qquad \ldots(1)$$

Prove that every $g \in G$ can be represented as

$$g = x^{-1} (xT) \text{ for some } x \in G.$$

Solution. Define a mapping $\phi : G \to G$ as

$$\phi(x) = x^{-1} (xT) \; \forall \; x \in G. \qquad \ldots(2)$$

[Notice that $xT \in G$ for each $x \in G$ and so $x^{-1} (xT) \in G$ for each $x \in G$.]

We proceed to show that ϕ is one-to-one.

Let $x, y \in G$ by arbitrary. Then

$\phi(x) = \phi(y) \Rightarrow x^{-1} (xT) = y^{-1} (yT)$, by (2)

$\Rightarrow (xT)(yT)^{-1} = xy^{-1}$

$\Rightarrow (xT)(y^{-1}T) = x y^{-1}$, since T is a homomorphism

$\Rightarrow (xy^{-1}) T = xy^{-1}$, since T is a homomorphism

$\Rightarrow xy^{-1} = e$, using (1)

$\Rightarrow x = y \Rightarrow \phi$ is one-to-one.

Since G is a finite group and $\phi : G \to G$ is one-to-one, ϕ must be an onto mapping. Hence for any $g \in G$, there exists some $x \in G$ such that

$$g = \phi(x) \quad \text{or} \quad g = x^{-1} (xT), \text{ by (2).}$$

Example 3.2.18. *Let G be a finite group, T an automorphism of G with the property :*

$$xT = x \quad \text{if and only if} \quad x = e.$$

Suppose further that $T^2 = I$. Prove that G must be abelian.

Solution. By Example 3.2.17, each $g \in G$ can be represented as

$$g = x^{-1}(xT) \text{ for some } x \in G$$

$\Rightarrow$ $g^{-1} = (xT)^{-1}(x^{-1})^{-1} = (x^{-1}T)x$, since T is a homomorphism

$\Rightarrow$ $g^{-1}T = [(x^{-1}T)x]T$

$= (yx)T$, where $y = x^{-1}T \in G$

$= (yT)(xT)$, since T is a homomorphism

$= ((x^{-1}T)T)(xT)$

$= (x^{-1}T^2)(xT)$

$= (x^{-1}I)(xT)$, since $T^2 = I$

$= x^{-1}(xT) = g.$ ...(1)

Thus $g^{-1}T = g \ \forall \ g \in G.$

Let $g_1, g_2 \in G$ be arbitrary. By (1), we have

$$g_1^{-1}T = g_1 \text{ and } g_2^{-1}T = g_2.$$

Now $g_1 g_2 = (g_1^{-1}T)(g_2^{-1}T)$

$= (g_1^{-1}g_2^{-1})T$, since T is a homomorphism

$= (g_2 g_1)^{-1}T$

$= g_3^{-1}T$, where $g_3 = g_2 g_1 \in G$

$= g_3$, using (1)

$= g_2 g_1$

$\therefore$ $g_1 g_2 = g_2 g_1 \ \forall \ g_1, g_2 \in G.$

Hence G is abelian.

Example 3.2.19. *Let G be a group and T an automorphism of G. If N is a normal subgroup of G such that $T(N) \subset N$, show how you could use T to define an automorphism of G/N.*

Solution. The mapping $T: G \to G$ is an automorphism.

Define a mapping $\phi : \frac{G}{N} \to \frac{G}{N}$ as

$$\phi(Ng) = NT(g) \ \forall \ g \in G. \quad ...(1)$$

Notice that $T(g) \in G \ \forall \ g \in G$ and so $NT(g) \in G/N$.

We verify that ϕ is well-defined.

Let $Ng_1 = Ng_2 \Rightarrow g_1 g_2^{-1} \in N \Rightarrow T(g_1 g_2^{-1}) \in T(N)$

$\Rightarrow$ $T(g_1 g_2^{-1}) \in N$ $(\because T(N) \subset N)$

$\Rightarrow$ $T(g_1)T(g_2^{-1}) \in N$, since T is a homomorphism

$\Rightarrow$ $T(g_1)T(g_2)^{-1} \in N$, since T is a homomorphism

$\Rightarrow$ $NT(g_1) = NT(g_2)$.

Thus ϕ is well-defined.

Now we show ϕ is one-to-one.

Let $\phi(Ng_1) = \phi(Ng_2)$; $g_1, g_2 \in G$

$\Rightarrow$ $NT(g_1) = NT(g_2)$, by (1)

$\Rightarrow$ $T(g_1)\,T(g_2)^{-1} \in N$

$\Rightarrow$ $T(g_1)\,T(g_2^{-1}) \in N \quad \Rightarrow T(g_1 g_2^{-1}) \in N$,

since T is a homomorphism.

$\Rightarrow$ $g_1 g_2^{-1} \in N \qquad [\because T(N) \subset N]$

$\Rightarrow$ $Ng_1 = Ng_2 \Rightarrow \phi$ is one-to-one.

Next we show that ϕ is onto.

Let $X \in G/N$ be arbitrary so that $X = Ng$ for some $g \in G$. Since T is onto, there exists some $g' \in G$ such that $T(g') = g$.

$\therefore$ $X = Ng = NT(g') = \phi(Ng')$, by (1).

Thus ϕ is onto, as $Ng' \in G/N$.

Finally, we show that ϕ is a homomorphism.

Let $A = Ng_1, B = Ng_2 \in G/N$. Then

$AB = Ng_1\,Ng_2 = Ng_1g_2$. Using (1), we have

$$\begin{aligned}\phi(AB) &= \phi(Ng_1g_2) = NT(g_1g_2)\\ &= N[T(g_1)\,T(g_2)], \text{ as } T \text{ is a homomorphism}\\ &= NT(g_1)\,NT(g_2), \text{ as } T(g_1), T(g_2) \in G \text{ and } N \lhd G\\ &= \phi(Ng_1)\,\phi(Ng_2), \text{ by (1)}\\ &= \phi(A)\,\phi(B).\end{aligned}$$

Thus ϕ is a homomorphism.

Hence we have used T, as given in (1), to define an automorphism ϕ of G/N

Example 3.2.20. *Define a characteristic subgroup of a group G. Prove that a characteristic subgroup of G must be a normal subgroup of G. Show by an example that the converse need not be true.* [D.U., 1995]

Solution. *A subgroup H of a group G is called a* **characteristic subgroup** *of G, if*

$$T(H) \subset H \quad \forall\ T \in Aut(G)$$

or

$$T(h) \in H \quad \forall\ h \in H \text{ and } \forall\ T \in Aut(G). \qquad \ldots(1)$$

Let H be a characteristic subgroup of G, so that (1) is true. We shall prove that H is a normal subgroup of G. Let $h \in H$ and $g \in G$.

Since the mapping $T_g : G \to G$ defined as

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

is an automorphism of G, therefore by (1),

$$T_g(h) \in H \quad \forall\ h \in H$$

$$g\,h\,g^{-1} \in H \quad \forall\ h \in H \text{ and } g \in G.$$

Hence H is a normal subgroup of G.

However, the converse need not be true *i.e.*, a normal subgroup of G may not be a characteristic subgroup of G. Consider the Klein's 4-group

$$G = \{e, a, b, ab\}, \quad \text{where} \quad a^2 = b^2 = e,\ ab = ba.$$

Let $H = \{a, a^2 = e\}$. Then $H < G$ and

$$i_G(H) = \frac{o(G)}{o(H)} = \frac{4}{2} = 2 \Rightarrow H \lhd G.$$

The mapping $T : G \to G$ defined as

$$T : e \to e,\ a \to b,\ b \to a,\ ab \to ab$$

is an automorphism of G such that $a \in H$ but $T(a) = b \notin H$. Hence H is not a characteristic subgroup of G.

Example 3.2.21. *If G is a group, N a normal subgroup of G, M a characteristic subgroup of N, prove that M is a normal subgroup of G.* [D.U., 1996]

Solution. We have $N \lhd G$ and $T(M) \subset M$ for all $T \in Aut(N)$.

We shall prove that $M \lhd G$. It is clear that M is a subgroup of G.

Now $N \lhd G \Rightarrow g n g^{-1} \in N \ \forall\ g \in G$ and $n \in N$. ...(1)

Using(1), it is easy to verify that the mapping

$$T_g : N \to N \text{ defined as } T_g(n) = g n g^{-1} \ \forall\ n \in N$$

is an automorphism of N *i.e.*, $T_g \in Aut(N)$.

Consequently, $T_g(M) \subset M \quad \forall \quad g \in G$

$\Rightarrow$ $T_g(m) \in M \quad \forall \quad m \in M$ and $g \in G$

$\Rightarrow$ $g m g^{-1} \in M \quad \forall \quad m \in M$ and $g \in G$.

Hence M is a normal subgroup of G.

Example 3.2.22. *Prove that the commutator subgroup of a group G is a characteristic subgroup of G.*

Solution. The commutator subgroup of a group G is denoted as G', where $\alpha \in G' \Rightarrow \alpha = c_1 c_2 \ldots c_n$, where each c_i is a commutator of G *i.e.*, $c_i = a_i b_i a_i^{-1} b_i^{-1}$ $(a_i, b_i \in G)$ and n is some positive integer. Let T be any automorphism of G. Then

$$\begin{aligned} T(c_i) &= T(a_i b_i a_i^{-1} b_i^{-1}) \\ &= T(a_i)\, T(b_i)\, T(a_i^{-1})\, T(b_i^{-1}), \text{ since } T \text{ is a homo.} \\ &= T(a_i)\, T(b_i)\, T(a_i)^{-1}\, T(b_i)^{-1}, \text{ since } T \text{ is a homo.} \\ &= \alpha_i \beta_i \alpha_i^{-1} \beta_i^{-1},\ \alpha_i = T(a_i),\ \beta_i = T(b_i) \in G. \end{aligned}$$

$\therefore$ $T(c_i) = d_i$,

where $d_i = \alpha_i \beta_i \alpha_i^{-1} \beta_i^{-1}$ is a commutator of G.

Now $T(\alpha) = T(c_1 c_2 \ldots c_n)$

$= T(c_1)\, T(c_2) \ldots T(c_n)$, since T is a homomorphism

$= d_1\, d_2 \ldots d_n$, where each d_i is a commutator of G.

Hence $T(\alpha) \in G' \ \forall\ \alpha \in G'$ and $T \in Aut\,(G)$ and so G' is a characteristic subgroup of G.

Example 3.2.23. *Let G be an abelian group. Show that*

$$H = \{x \in G \mid x^n = e,\ n \text{ being a fixed integer}\}$$

is a characteristic subgroup of G.

Solution. Let $x, y \in H$. Then $x^n = y^n = e$. We have [D.U., 19

$$(xy)^n = x^n y^n, \text{ since } G \text{ is abelian}$$

$$= e \,.\, e = e.$$

Thus $xy \in H$.

Again $x \in H \Rightarrow x^n = e \Rightarrow x^{-n} = e^{-1} \Rightarrow (x^{-1})^n = e$

$\Rightarrow$ $x^{-1} \in H \Rightarrow H < G$.

Let T be any automorphism of G and $x \in H$ so that $x^n = e$

$\Rightarrow$ $T(x^n) = T(e)$

$\Rightarrow$ $\{T(x)\}^n = T(e)$, since T is a homomorphism

$\Rightarrow$ $\{T(x)\}^n = e$, since T is a homomorphism

$\Rightarrow$ $T(x) \in H \quad \forall\ T \in Aut\,(G)$ and $x \in H$.

Hence H is a characteristic subgroup of G.

Example 3.2.24. *Define characteristic subgroup of a group. Give an example of a characteristic subgroup.*

Hint. Refer to Example 3.3.23. [D.U., 199

Example 3.2.25. *Show that every subgroup of a finite cyclic group is a characteristic subgroup.*

Solution. Let $G = \langle a \rangle$, $a^n = e$ be a finite cyclic group and H be any subgroup of G. Then $H = \langle a^m \rangle$ for some integer $0 \le m \le n$. Let T be any automorphism of G. Since [D.U., 199

$$T(a) \in G = \langle a \rangle,\ T(a) = a^l,\ 0 \le l \le n.$$

We shall prove that $T(H) \subset H$.

Let $x \in H$ be arbitrary. Then $x = (a^m)^k$ for some integer k, $0 \le k \le m$.

We have

$$T(x) = T(a^{mk}) = \{T(a)\}^{mk}, \text{ as } T \text{ is homomorphism}$$

or $T(x) = (a^l)^{mk} = (a^m)^{lk} \in H = \langle a^m \rangle$.

$\therefore$ $T(x) \in H \quad \forall\ x \in H$.

Hence H is a characteristic subgroup of G.

3.3 Conjugate Elements

Definition. *If a and b are two elements of a group G, we say that a is conjugate to b, denoted as $a \sim b$, if there exists some element $x \in G$ such that*

$$a = x^{-1} b x.$$

Remark. We may also define *conjugate elements* as follows :

$$a \sim b \text{ iff } a = x\, b\, x^{-1} \quad \text{for some} \quad x \in G.$$

For example, $(123) \sim (132)$ in S_3.

Take $\theta = (23) \in S_3$. Then $\theta\,(132)\,\theta^{-1} = (23)\,(132)\,(23) = (123)$.

Theorem 3.3.1. *Show that the relation $(\sim)$ of conjugacy is an equivalence relation on a group G.*

Proof. Let $a, b, c \in G$.

Reflexive. $a \sim a$, since $a = e\, a\, e = e^{-1} a\, e$, $e \in G$.

Symmetric. Let $a \sim b$ so that $a = x^{-1} b x$, $x \in G$

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

Thus $\quad a \sim b \Rightarrow b \sim a$.

Transitive. Let $a \sim b$ and $b \sim c$. Then

$$a = x^{-1} b\, x \text{ and } b = y^{-1} c\, y \text{ for some } x, y \in G$$

$\Rightarrow \quad a = x^{-1} (y^{-1} c\, y)\, x = (yx)^{-1} c\, (yx)$, $yx \in G$

$\Rightarrow \quad a \sim c$.

Hence the relation $(\sim)$ of conjugacy is an equivalence relation on G.

Remark 1. For $a \in G$, the equivalence class of a, denoted by $C(a)$ or $[a]$, is given by

$$C(a) = \{x \in G : x \sim a\} = \{x \in G : x = y^{-1} a\, y : y \in G\}$$

$$\therefore \quad C(a) = \{y^{-1} a\, y : y \in G\}.$$

This equivalence class of a is also called the *conjugate class* of a.

Since the conjugacy relation $\sim$ is an equivalence relation on G, so

$$G = \bigcup_{a \in G} [a]$$

i.e., G is expressible as the union of mutually disjoint conjugate classes.

Clearly, $\quad [a] = [b] \Leftrightarrow a \sim b$.

Remark 2. $C(e) = \{e\}$; *where e is the identity of the group G.*

$$C(e) = \{y^{-1} e\, y : y \in G\} = \{e\}.$$

Remark 3. *In an abelian group G,*

$$C(a) = \{a\} \quad \forall \quad a \in G \quad \textit{i.e.,} \quad o\,[C(a)] = 1.$$

Ex. *Define conjugate elements and conjugate classes of a group G..*

[D.U., 1995]

Theorem 3.3.2. *If G is a finite group, then*

$$o[C(a)] = \frac{o(G)}{o(N(a))} = i_G(N(a)),$$

where $N(a)$ is the normalizer of $a \in G$. [D.U., 1995, 94

Or

If G is a finite group, then the number of elements conjugate to a in G is the index of the normalizer of a in G.

Proof. Define a relation $\sim$ on G as follows :

$$a \sim b \text{ iff } a = x^{-1} b x \text{ for some } x \in G$$

Then $\sim$ is an equivalence relation on G and the equivalence class of a is

$$C(a) = \{x^{-1} a x : x \in G\},$$

which is the conjugate class of a in G. Furthermore,

$$G = \bigcup_{a \in G} C(a). \quad \ldots(1)$$

Let Σ denote the set of all distinct right cosets of $N(a)$ in G, where

$$N(a) = \{x \in G : xa = ax\}.$$

Define a mapping $f : C(a) \to \Sigma$ as

$$f(x^{-1} a x) = N(a)\, x,\ x \in G. \quad \ldots(2)$$

Then f is a well-defined mapping, since

$$x^{-1} a x = y^{-1} a y \Rightarrow ax = x y^{-1} ay$$

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

$$\Rightarrow \quad xy^{-1} \in N(a) \Rightarrow N(a)\, x = N(a)\, y.$$

Clearly f is onto, since for any $X \in \Sigma \Rightarrow X = N(a)\, g$ for some $g \in G$ $\Rightarrow X = f(g^{-1} a g)$, by (2) and $g^{-1} a g \in C(a)$.

Finally, f is one-to-one, since

$$f(x^{-1} a x) = f(y^{-1} a y) \Rightarrow N(a)\, x = N(a)\, y, \text{ by (2)}$$

$$\Rightarrow \quad x y^{-1} \in N(a) \Rightarrow xy^{-1} a = a\, xy^{-1}$$

$$\Rightarrow \quad x^{-1} a x = y^{-1} a y.$$

Hence there exists a one-to-one correspondence between $C(a)$ and Σ. Since G is finite, it follows that

$$o[C(a)] = o[\Sigma]$$

or $o[C(a)] = i_G(N(a))$. Using Lagrange's Theorem, we have

$$o[C(a)] = i_G(N(a)) = \frac{o(G)}{o(N(a))}.$$

Corollary 1. (Class Equation of a Group)
If G is a finite group, then

$$o(G) = \sum_{a \in G} i_G(N(a)) = \sum_{a \in G} \frac{o(G)}{o(N(a))},$$

where the sum runs over one element a in each conjugate class.

Proof. Since G is a finite group and since the R.H.S. of (1) is the disjoint union of conjugate classes, therefore

$$o(G) = \sum_{a \in G} o[C(a)],$$

where the sum runs over one element a in each conjugate class.

By Theorem 3.3.2,

$$o[C(a)] = \frac{o(G)}{o(N(a))} = i(N(a)).$$

Hence $$o(G) = \sum_{a \in G} \frac{o(G)}{o(N(a))} = \sum_{a \in G} i_G(N(a)).$$

This equation is known as *class equation* of the finite group G.

Corollary 2. (Second Form of Class Equation)

If G is a finite group, then

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

Z being the centre of G.

Proof. By corollary 1, the class equation of G is

$$o(G) = \sum_{a \in G} \frac{o(G)}{o(N(a))}$$

or
$$o(G) = \sum_{a \in Z} \frac{o(G)}{o(N(a))} + \sum_{a \notin Z} \frac{o(G)}{o(N(a))}. \quad \ldots(3)$$

$[\because G = Z \cup (G \sim Z)]$

We now show that
$$a \in Z \Leftrightarrow N(a) = G. \quad \ldots(4)$$

Let $a \in Z \Rightarrow xa = ax$ for all $x \in G$

$\Rightarrow x \in N(a)$ for all $x \in G$

$\Rightarrow N(a) = G.$

Conversely, $N(a) = G \Rightarrow x \in N(a)\ \forall\ x \in G$

$\Rightarrow xa = ax\ \forall\ x \in G$

$\Rightarrow a \in Z$

This proves (4). Since G is finite, it follows that

$$a \in Z \Leftrightarrow o(G) = o(N(a))$$

or
$$a \in Z \Leftrightarrow \frac{o(G)}{o(N(a))} = 1.$$

or
$$o(Z) = \sum \frac{o(G)}{o(N(a))}, \quad \ldots(5)$$

From (3) and (5), we obtain

$$o(G) = o(Z) + \sum_{a \in Z} \frac{o(G)}{o(N(a))}.$$

This is the second form of class equation of a finite group G.

This equation is of great importance in proving many interesting results of finite groups.

The equivalent forms of class equation of a finite group G are :

$$o(G) = \sum_{a \in G} \frac{o(G)}{o(N(a)},$$

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

$$o(G) = o(Z) + \sum_{a \in Z} i_G(N(a)),$$

$$o(G) = o(Z) + \sum_{N(a) \neq G} \frac{o(G)}{o(N(a))}.$$

EXAMPLES

Example 3.3.1. *Verify the class equation for S_3.*

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

If $G = S_3$, $o(G) = 6$.

By definition, $N(a) = \{x \in G : xa = ax\}$.

It is easy to verify that

$$N(I) = S_3,$$
$$N[(12)] = \{I, (12)\},$$
$$N[(123)] = \{I, (123), (132)\}.$$

$$\therefore \sum_{a \in G} \frac{o(G)}{o(N(a))} = \frac{o(G)}{o\{N(I)\}} + \frac{o(G)}{o\{N[(12)]\}} + \frac{o(G)}{o\{N[(123)]\}}$$

$$= \frac{6}{6} + \frac{6}{2} + \frac{6}{3}$$

$$= 1 + 3 + 2 = 6 = o(G).$$

Hence $o(G) = \sum_{a \in G} \frac{o(G)}{o(N(a))}$.

Example 3.3.2. *Verify the class equation for the group*

$$G = \{e, \theta, a, b, c, \theta a, \theta b, \theta c\},$$

where $a^2 = b^2 = c^2 = \theta$, $\theta^2 = e$, $ab = \theta ba = c$, $bc = \theta cb = a$, $ca = \theta ac = b$.

This group is known as the **group of quaternion units.**

Solution. It may be observed that e is the identity of G and the inverse elements of a, b, c are $\theta a, \theta b, \theta c$; respectively. It is interesting to verify that

$$Z(G) = \{e, \theta\}.$$

Also $N(e) = G, N(\theta) = G, N(a) = \{e, a, \theta, \theta a\} = N(\theta a)$,
$N(b) = \{e, b, \theta, \theta b\} = N(\theta b), N(c) = \{e, c, \theta, \theta c\} = N(\theta c)$.

$$\therefore \quad o[C(e)] = \frac{o(G)}{o[N(e)]} = \frac{8}{8} = 1, \; o[C(\theta)] = \frac{8}{8} = 1,$$

$$o[C(a)] = \frac{o(G)}{o[N(a)]} = \frac{8}{4} = 2 = o[C(\theta a)].$$

Similarly, $o[C(b)] = 2 = o[C(c)]$.

Hence $o[C(e)] + o[C(\theta)] + o[C(a)] + o[C(b)] + o[C(c)]$
$= 1 + 1 + 2 + 2 + 2 = 8 = o(G)$.

Hence the class equation is verified for G.

Example 3.3.3. *If N is a normal subgroup of G and $a \in N$, show that every conjugate of a in G is also in N. Hence show that*

$$o(N) = \sum_{a \in N} o[C(a)].$$

Solution. By definition, any conjugate of a in G is of the form

$$x^{-1} a x, \; x \in G.$$

Since N is a normal subgroup of G and $a \in N$, therefore

$$x^{-1} a x \in N \quad \forall \; x \in G. \qquad (\because \; a \in N)$$

Hence every conjugate of $a \in N$ is in N.

The conjugate class of $a \in N$ is

$$C(a) = \{x^{-1} a x : x \in G\} \subseteq N. \qquad (\because \; N \triangleleft G)$$

Hence $$N = \bigcup_{a \in N} C(a).$$

If N is finite, then

$$o(N) = \sum_{a \in N} o[C(a)].$$

Example 3.3.4. *If in a finite group G an element a has exactly two conjugates, prove that G has a normal subgroup $N \neq (e), N \neq G$.*

Solution. $C(a)$ denotes the conjugate class of $a \in G$. Since a has exactly two conjugates, $o[C(a)] = 2$.

We know $o[C(a)] = i_G(N(a))$. [Theorem 3.3.2]

$\therefore \quad i_G(N(a)) = 2$ and so $N(a) \triangleleft G$.

[$\because$ a subgroup of G of index 2 must be a normal subgroup of G]

Now we show that $N(a) \neq (e), N(a) \neq G$.

Let, if possible, $N(a) = G$. Then $o(G) = o(N(a))$

$$\Rightarrow \quad \frac{o(G)}{o(N(a))} = 1 \Rightarrow o[C(a)] = \frac{o(G)}{o(N(a))} = 1,$$

which is contrary to the given hypothesis.

Thus $N(a) \neq G$.

Let, if possible, $N(a) = (e)$. Then $a \in N(a) \Rightarrow a = e$

$\Rightarrow$ $C(a) = \{y^{-1} a y : y \in G\} = \{y^{-1} e y : y \in G\} = \{e\}$

$\Rightarrow$ $o[C(a)] = 1$,

which is again contrary to the given hypothesis.

Thus $N(a) \neq (e)$.

Ex. *Suppose $a \in G$ has only two conjugates in G, then show that $N(a)$ is a normal subgroup of G.*

Example 3.3.5. *Let G be a group containing an element of finite order $n > 1$ and exactly two conjugate classes. Show that G is a finite group of order 2.*

Solution. Let $a \neq e \in G$, where $o(a) = n$ *i.e.*, $a^n = e$.

Since G has only two conjugate classes, these must be (e) and $C(a)$. Further

$$G = (e) \cup C(a). \qquad \ldots(1)$$

It follows that if $b \neq e \in G$ is arbitrary, then $b \in C(a)$

$\Rightarrow$ $b = x^{-1} a x$ for some $x \in G$

$\Rightarrow$ $o(b) = o(x^{-1} a x) = o(a)$

$\therefore$ $o(b) = o(a) = n$ for all $b \neq e \in G$. $\ldots(2)$

We now show that n is prime. Let $n = lm$, where l and m are positive integers $< n$. Then

$$a^n = e \Rightarrow a^{lm} = e \Rightarrow (a^m)^l = e, \text{ where } a^m \neq e \in G.$$

By (2), $o(a^m) = n \Rightarrow \quad l = n \Rightarrow l = lm \Rightarrow m = 1$.

Thus n is a prime number. Next we prove that

$$n = 2 \quad i.e., \quad a^2 = e.$$

Let, if possible, $a^2 \neq e$. By (1), $a^2 \in C(a)$

$\Rightarrow$ $a^2 = g^{-1} a g$ for some $g \in G$

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

$\therefore$ $a^{2^2} = g^{-2} a g^2$.

Proceeding in the same manner, we get

$$a^{2^n} = g^{-n} a g^n \Rightarrow a^{2^n} = a, \text{ by (2)}$$

$\Rightarrow$ $a^{2^n - 1} = e \Rightarrow o(a) = n \mid 2^n - 1$.

This is impossible, since n is prime.

$\therefore$ $a^2 = e$ *i.e.*, $o(a) = 2$. Hence, by (2), $o(g) = 2 \; \forall \; g \neq e \in G$.

It follows that G is abelian and so $o[C(a)] = 1$.

[See Remark 3 of Theorem 3.3.1]

Hence, by (1),

$$o(G) = 1 + 1 = 2.$$

3.4 Applications of Class Equation of a Group

Theorem 3.4.1. *If $o(G) = p^n$, where p is a prime number ; then $Z(G) \neq (e)$ or $o[Z(G)] > 1$.* [D.U., 1998, 95, 94]

Equivalently, a group of prime power order must have a non-trivial centre.

Proof. The class equation of G is

$$o(G) = o(Z) + \sum_{a \notin Z} \frac{o(G)}{o(N(a))} \quad \ldots(1)$$

By Lagrange's Theorem, $o(N(a))$ divides $o(G) = p^n$ for each $a \notin Z$. Consequently,

$$o(N(a)) = p^k, \text{ where } 0 < k < n$$

$$\therefore \quad \frac{o(G)}{o(N(a))} = \frac{p^n}{p^k} = p^{n-k}$$

$$\Rightarrow \quad p \text{ divides } \frac{o(G)}{o(N(a))}, \text{ whenever } a \notin Z$$

$$\Rightarrow \quad p \text{ divides } \sum_{a \notin Z} \frac{o(G)}{o(N(a))}. \quad \ldots(2)$$

Also p divides $o(G) = p^n$. $\ldots(3)$

From (2) and (3), it follows that

$$p \text{ divides } \left[o(G) - \sum_{a \notin Z} \frac{o(G)}{o(N(a))} \right] = o(Z), \text{ using (1).}$$

Now $p \mid o(Z) \Rightarrow o(Z)$ is at least two (since the least value of p is 2).

Hence $o(Z) > 1$ *i.e.*, Z is non-trivial.

[Notice that $Z = \{e\}$ is a trivial centre and in this case $o(Z) = 1$]

Corollary. *If $o(G) = p^n$, p a prime number, then G has a normal subgroup of order p.*

Proof. As shown above, $p \mid o(Z)$ and so by Cauchy's Theorem, Z has a subgroup say N of order p *i.e.*, $N < Z$, $o(N) = p$

$\Rightarrow n \in Z \quad \forall\, n \in N$

$\Rightarrow gn = ng \;\forall\, g \in G, n \in N$

$\Rightarrow gng^{-1} = n \in N \;\forall\, g \in G, n \in N$

$\Rightarrow N \lhd G, o(N) = p.$

Note. $N < Z \quad \Rightarrow \quad N \lhd G.$

Theorem 3.4.2. *If $o(G) = p^2$, where p is a prime number ; then G is abelian.*

Proof. Since $o(G) = p^2$, by Theorem 3.4.1, G has a non-trivial centre *i.e.*, $o(Z) > 1$. By Lagrange's Theorem,

$o(Z)$ divides $o(G) = p^2$.

$\therefore \quad o(Z) = p \quad \text{or} \quad p^2.$

[Notice that $o(Z) \neq 1$, as $o(Z) > 1$.]