2

Groups and Normal Subgroups

1. INTRODUCTION

This chapter begins with the assumption that the reader is well acquianted with the concepts of group, subgroup, Lagrange's theorem, cosets, normal subgroups etc. In this chapter, we shall be discussing conjugacy relation, normalizer, centre, class equation, in the context of a group.

2. NOTATION

Let G be a group with binary operation $*$. Let $x, y \in G$. For the sake of convenience, the element $x * y$ of G is written as xy. Under this notation, the axioms of a group G takes the following form :

(*i*) $x(yz) = (xy)z \ \forall \ x, y, z \in G$

(*ii*) There exists an element e in G such that $xe = x = ex$

(*iii*) For $x \in G$, there exists an element y in G such that $xy = e = yx$.

3. CONJUGACY RELATION

Let G be a group and $a, b \in G$. a is said to be a **conjugate** of b if there exists an element $x \in G$ such that $a = x^{-1} bx$.

If a is conjugate to b then we write $a \sim b$ and this relation '~' is called the **conjugacy relation** on G.

For example in the group S_3, the element (1 2 3) is conjugate of (1 3 2), because we have :

$$(1\ 2\ 3) = (2\ 3)^{-1}\ (1\ 3\ 2)\ (2\ 3).$$

Example 1. *Show that two elements of a group are conjugate if and only if they can be put in the form ab and ba respectively, where a and b are some suitable elements of G.*

Sol. Let x and y be conjugate elements of G.

$\therefore$ $x = z^{-1}yz$ for some $z \in G$

Let $a = z^{-1}y$ and $b = z$.

$\therefore$ $ab = (z^{-1}y)z = z^{-1}yz = x$ and $ba = z(z^{-1}y) = (zz^{-1})\, y = y$

$\therefore$ $x = ab$ and $y = ba$.

Conversely, let $x = ab$ and $y = ba$

Now $a^{-1}xa = a^{-1}(ab)a = (a^{-1}a)(ba) = ey = y$ *i.e.*, y is conjugate to x.

Also, $b^{-1}yb = b^{-1}(ba)b = (b^{-1}b)(ab) = ex = x$ *i.e.*, x is conjugate to y.

$\therefore$ x and y are conjugate. $\therefore$ The result holds.

Theorem 1. *The conjugacy relation on a group is an equivalence relation.*

Proof. Let G be a group and the conjugacy relation on G be denoted by ~. We shall show that ~ is an equivalence relation.

1. **Reflexivity.** Let $a \in G$.

We have $e^{-1}ae = eae = a$

$\therefore$ $a = e^{-1}ae$ *i.e.*, $a \sim a$

$\therefore$ $a \sim a \ \forall\ a \in G$. $\therefore$ $\sim$ is reflexive.

2. **Symmetry.** Let $a, b \in G$ and $a \sim b$.

$\therefore$ $\exists\ x \in G : a = x^{-1}bx$

$\Rightarrow$ $xax^{-1} = x(x^{-1}bx)\,x^{-1} = (xx^{-1})\,b(xx^{-1}) = ebe = b$

$\Rightarrow$ $b = xax^{-1}$ *i.e.*, $b = (x^{-1})^{-1}\,a(x^{-1})$

$\therefore$ $b \sim a$, because $x^{-1} \in G$

$\therefore$ $a \sim b \Rightarrow b \sim a$. $\therefore$ $\sim$ is symmetric.

3. **Transitivity.** Let $a, b, c \in G$ and $a \sim b$ and $b \sim c$.

$\therefore$ $\exists\ x, y \in G : a = x^{-1}bx$ and $b = y^{-1}cy$,

$\therefore$ $a = x^{-1}(y^{-1}cy)x = (x^{-1}y^{-1})\,c(yx) = (yx)^{-1}\,c(yx)$

$\therefore$ $a \sim c$, because $yx \in G$

$\therefore$ $a \sim b$ and $b \sim c \Rightarrow a \sim c$. $\therefore$ $\sim$ is transitive.

$\therefore$ The conjugacy relation on a group is an equivalence relation.

4. CONJUGATE CLASS

We know that an equivalence relation on a set partitions it into mutually disjoint equivalence classes.

Let $C(a)$ denote the equivalence class of an element a of G with respect to the conjugacy relation $\sim$ on the group G. The set $C(a)$ is called the **conjugate class** of a in G.

$\therefore$ $C(a) = \{b : b \in G \text{ and } b \sim a\}$

$= \{b : b \in G \text{ and } b = x^{-1}ax \text{ for some } x \in G\}$

$= \{x^{-1}ax : x \in G\}$

= set of all conjugates of a.

Since the relation '$\sim$' is reflexive, $a \in C(a) \ \forall\ a \in G$.

Also, $C(a) \subseteq G \ \forall\ a \in G$

$\therefore$ $G = \bigcup_{a \in G} \{a\} \subseteq \bigcup_{a \in G} C(a) \subseteq G$

$\therefore$ $G = \bigcup_{a \in G} C(a)$.

In particular, let G be a finite group and $G = \bigcup_{i=1}^{t} C(a_i)$, where the equivalence classes $C(a_1), C(a_2), \ldots\ldots, C(a_t)$ are mutually disjoint.

$\therefore$ $o(G) = \sum_{i=1}^{t} o(C(a_i))$.

For example, $C(e) = \{x^{-1}ex : x \in G\} = \{x^{-1}x : x \in G\} = \{e\}$.

Example 2. *If G is an abelian group, then show that* $C(a) = \{a\} \ \forall\ a \in G$.

Sol. For $a \in G$,

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

$= \{x^{-1}(xa) : x \in G\}$

$$= \{(x^{-1}x)a : x \in G\} = \{ea : x \in G\} = \{a\}.$$

$\therefore$ $C(a) = \{a\}\ \forall\ a \in G.$

Example 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. If N is finite then show that $o(N) = \sum_{a \in N} o(C(a))$, where the sum runs over the elements a taken one from each conjugate class.*

Sol. Let $a \in N$ and $b(\in G)$ be a conjugate of a.

$\therefore$ $b = x^{-1}ax$ for some $x \in G$

$\therefore$ $b = x^{-1}a(x^{-1})^{-1}$, where $a \in N$ and $x^{-1} \in G$

$\therefore$ $b \in N$, because N is normal

$\therefore$ Every conjugate of a in G is also in N.

$\therefore$ $C(a) \subseteq N\ \forall\ a \in N$

Now $$N = \bigcup_{a \in N} \{a\} \subseteq \bigcup_{a \in N} C(a) \subseteq N$$

$\therefore$ $$N = \bigcup_{a \in N} C(a) \qquad \ldots(1)$$

Let N be finite.

$\therefore$ $$o(N) = o\left(\bigcup_{a \in N} C(a)\right)$$

$\Rightarrow$ $$o(N) = \sum_{a \in N} o(C(a)),$$

where the sum runs over elements a, taken one from each conjugate class.

Example 4. *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.*

Sol. Let $a\ (\neq e)$ be an element of group G of order n.

We know that $C(e) = \{e\}$ and $a \neq e$.

$\therefore$ $a \notin C(e)$.

Also $a \in C(a)$ $\therefore$ $C(e) \neq C(a)$

$\therefore$ $C(e)$ and $C(a)$ are disjoint conjugate classes.

Since G has exactly two conjugate classes, we have

$$G = C(e) \cup C(a)$$

$\Rightarrow$ $$G = \{e\} \cup C(a)$$

Let $b(\neq e)$ be any element of G.

$\therefore$ $b \in C(a)$

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

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

$\therefore$ $o(b) = n\ \ \forall\ b(\neq e) \in G$ $\qquad \ldots(1)$

We know show that n is prime.

Let $n = lm$, where l, m are positive integer $\leq n$.

$\therefore$ $a^n = e \Rightarrow a^{lm} = e \Rightarrow (a^l)^m = e$

$\therefore$ $o(e^l) = n$ $\qquad (\because\ a^l \neq e)$

$\Rightarrow$ $n \leq m$ $\therefore$ $m = n$ $\qquad (\because\ m \leq n)$

$\Rightarrow$ $m = lm \Rightarrow l = 1$ $\therefore$ n is prime.

Now we shall show that $a^2 = e$.

If possible, let $a^2 \neq e$.

$\therefore$ $a^2 \in C(a)$ $(\because\ C(e) = \{e\})$

$\Rightarrow$ $a^2 = y^{-1}ay$ for some $y \in G$

$\Rightarrow$ $(a^2)^2 = (y^{-1}ay)(y^{-1}ay) = y^{-1}a(yy^{-1})ay = y^{-1}aeay$

$= y^{-1}a^2y = y^{-1}(y^{-1}ay)y = y^{-2}ay^2$

$\therefore$ $a^{2(2)} = y^{-2}ay^2$

Proceeding in this manner, we have $a^{2n} = y^{-n}ay^n$.

$\Rightarrow$ $a^{2n} = (y^n)^{-1}ay^n = e^{-1}ae = a$

$\Rightarrow$ $a^{2n}a^{-1} = aa^{-1} \Rightarrow a^{2n-1} = e$

$\Rightarrow$ $n/2n - 1$ $(\because\ o(a) = n)$

Also $n/2n$. $\Rightarrow$ $n/(2n - (2n - 1))$ $\Rightarrow$ $n/1$

This is impossible, because $n > 1$.

$\therefore$ $a^2 = e$

$\therefore$ $o(a) = 2$ *i.e.*, $n = 2$

$\therefore$ (1) $\Rightarrow$ $o(b) = 2$ $\forall\ b(\neq e) \in G$

$\therefore$ G is abelian.*

$\therefore$ $C(a) = \{a\}$

$\therefore$ $G = \{e\} \cup \{a\}$

$\Rightarrow$ $o(G) = 1 + 1 = 2$.

Hence the result holds.

5. NORMALIZER OF AN ELEMENT

Let G be a group. For $a \in G$, the set $\{x \in G : ax = xa\}$ is called the **normalizer** of the element a in G and it is denoted by $N(a)$.

Thus, the normalizer of a contains all those elements of G which commute with a.

Remarks 1. We have $ex = xe$ $\forall\ x \in G$.

$\therefore$ $N(e) = G$

2. If G is an abelian group and $a \in G$, then $ax = xa$ $\forall\ x \in G$.

$\therefore$ $N(a) = G$ $\forall\ a \in G$.

Theorem 1. *Let G be a group. For any a in G, the normalizer N(a) of a in G is a subgroup of G.*

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

$e \in N(a)$, because $ae = ea$ $\therefore$ $N(a)$ is non-empty.

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

Now $a(xy) = (ax)y = (xa)y = x(ay) = x(ya) = (xy)a$

$\Rightarrow$ $a(xy) = (xy)a$ $\therefore$ $xy \in N(a)$

Let $x \in N(a)$ $\therefore$ $ax = xa$

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

---

* Let $a, b \in G$. $\therefore$ $(ab)^2 = e$ and $a^2b^2 = ee = e$.

$\Rightarrow$ $(ab)^2 = a^2b^2 \Rightarrow abab = aabb \Rightarrow ba = ab$.

$\Rightarrow \quad (x^{-1}a)e = e(ax^{-1}) \quad \Rightarrow \quad x^{-1}a = ax^{-1}$

$\Rightarrow \quad ax^{-1} = x^{-1}a \quad \therefore \quad x^{-1} \in N(a)$

$\therefore$ $N(a)$ is a subgroup of G.

Remark. The normalizer $N(a)$ may not be a normal subgroup of G.

Example 5. *Give an example to show that in a group G, the normalizer of an element is not necessarily a normal subgroup of G.*

Sol. Let $X = \{a, b, c\}$. Let S_3 be the set of all one-to-one mappings of X onto X.

$\therefore \quad S_3 = \{I, (ab), (bc), (ca), (abc), (acb)\}$.

Here the mapping (ab) stands for $a \to b, b \to a, c \to c$.

The set S_3 is a group with composition of mappings as the binary operation. We find the normalizer of the element (ab) of S_3.

We have $\quad I(ab) = (ab)I \quad \therefore \quad I \in N((ab))$

Also $\quad (ab) \in N((ab))$

We find $(ab)(bc)$.

Under $(ab)(bc)$: $a \to a \to b, b \to c \to c, c \to b \to a$

$\therefore \quad (ab)(bc) = (abc)$

Under $(bc)(ab)$: $a \to b \to c, b \to a \to a, c \to c \to b$

$\therefore \quad (bc)(ab) = (acb)$

$\therefore \quad (ab)(bc) \neq (bc)(ab)$

$\therefore \quad (bc) \notin N((ab))$

Similarly $(ca), (abc), (acb)$ are not in $N((ab))$.

$\therefore \quad N((ab)) = \{I, (ab)\}$

Since in general, a normalizer is a subgroup, $N((ab))$ is also a subgroup of S_3.

Now $\quad (bc) \in S_3$ and $(ab) \in N((ab))$

and $(bc)(ab)(bc)^{-1} = (bc)(ab)(bc) = (bc)(abc) = (ac) \notin N((ab))$.

$\therefore$ $N((ab))$ is not a normal subgroup of S_3.

Example 6. *Let a be any element of a group G. Show that the cyclic subgroup of G generated by a is a normal subgroup of the normalizer of a.*

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

Let $\quad a^n \in (a)$.

Now $\quad aa^n = a^{n+1} = a^n a \quad \therefore \quad a^n \in N(a)$

$\therefore \quad (a) \subseteq N(a)$ ...(1)

Since $N(a)$ is a subgroup of G, the subgroup generated by a *i.e.*, (a) is a subgroup of $N(a)$ (Using (1))

Let $a^n \in (a)$ and $x \in N(a)$.

$\therefore \quad xa^nx^{-1} = x(aa \ldots\ldots a)x^{-1}$

$= xa(x^{-1}x)\,a(x^{-1}x) \ldots\ldots (x^{-1}x)\,ax^{-1}$

$= (xax^{-1})(xax^{-1}) \ldots\ldots (xax^{-1})$

$= (xax^{-1})^n = (axx^{-1})^n \qquad (\because \quad x \in N(a) \quad \Rightarrow \quad ax = xa)$

$= (ae)^n = a^n \in (a)$.

$\therefore$ (a) is a normal subgroup of $N(a)$.

Theorem 2. *If G is a finite group and $a \in G$, then $o(C(a)) = \dfrac{o(G)}{o(N(a))}$.*

Proof. We have $C(a) = \{x^{-1}ax : x \in G\}$.

Let A be the set of all right cosets of the subgroup $N(a)$ in G.

Define $\phi : A \to C(a)$ by $\phi(N(a)\,x) = x^{-1}ax \quad \forall\, x \in G$

ϕ is well defined. Let $x, y \in G$.

$$N(a)\,x = N(a)\,y \Rightarrow xy^{-1} \in N(a) \quad (\because\ Ha = Hb \Leftrightarrow ab^{-1} \in H)$$

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

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

$$\Rightarrow \phi(N(a)x) = \phi(N(a)y).$$

$\therefore$ ϕ is well defined.

ϕ in one-one. Let $x, y \in G$.

$$\phi(N(a)x) = \phi(N(a)y) \Rightarrow x^{-1}ax = y^{-1}ay \Rightarrow (x^{-1}ax)(y^{-1}y) = (x^{-1}x)(y^{-1}ay)$$

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

$$\Rightarrow (xx^{-1})(axy^{-1})(yy^{-1}) = (xx^{-1})(xy^{-1}a)(yy^{-1}) \Rightarrow a(xy^{-1}) = (xy^{-1})\,a$$

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

$\therefore$ ϕ is one-one.

ϕ is onto. Let $y \in C(a)$

$\therefore$ $\exists\, x \in G : y = x^{-1}ax$

Now $N(a)\,x \in A$ and $\phi(N(a)x) = x^{-1}ax = y$.

$\therefore$ ϕ is onto.

$\therefore$ There is one-to-one correspondence between the right cosets of $N(a)$ in G and the conjugates of a.

Since the group G is finite, we have

$$o(C(a)) = \text{number of elements of } C(a)$$
$$= \text{number of conjugates of } a$$
$$= \text{number of right cosets of } N(a) \text{ in } G \quad (\because\ \phi \text{ is } 1-1 \text{ and onto})$$
$$= \frac{o(G)}{o(N(a))}^{*}$$

$$\therefore \quad \mathbf{o(C(a)) = \frac{o(G)}{o(N(a))}}.$$

In other words, the number of conjugates of a in G is equal to the index of $N(a)$ in G *i.e.*, $o(C(a)) = [G : N(a)]$.

Theorem 3. *If G is a finite group, then* $o(G) = \sum_{a} \frac{o(G)}{o(N(a))}$, *where the sum runs over elements a, taken one from each conjugate class.*

Proof. The relation of conjugacy is an equivalence relation on G.

$\therefore$ This relation partitions G into mutually disjoint conjugate classes.

Since G is finite, the number of distinct conjugate classes will be finite, say k. Let $C(a)$ denote the conjugate class of a. Let the k distinct conjugate classes of G be $C(a_1)$, $C(a_2)$, ..., $C(a_k)$.

$$\therefore \quad G = C(a_1) \cup C(a_2) \cup \ldots\ldots \cup C(a_k)$$

---

* This is because the distinct right cosets of $N(a)$ in G forms a partition of G and the order of each right coset of $N(a)$ is same as the order of $N(a)$.

$\therefore \quad o(G) = o(C(a_1)) + o(C(a_2)) + \ldots\ldots + o(C(a_k))$

$$= \frac{o(G)}{o(N(a_1))} + \frac{o(G)}{o(N(a_2))} + \ldots\ldots + \frac{o(G)}{o(N(a_k))} = \sum_{i=1}^{k} \frac{o(G)}{o(N(a_i))}$$

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

where the sum runs over elements a, taken one from each conjugate class.

Example 7. *If in a finite group G an element 'a' has exactly two conjugates, show that G is not simple.*

Sol. We have $o(C(a)) = 2$.

Since G is finite, we have

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

$$\therefore \quad \frac{o(G)}{o(N(a))} = 2$$

$\therefore$ No. of right cosets of $N(a)$ in $G = 2$

$\therefore$ Index of $N(a)$ in $G = 2$

$\therefore$ $N(a)$ is a normal subgroup of G.

If possible, let $N(a) = \{e\}$.

$\therefore \quad a \in N(a) \Rightarrow a = e \Rightarrow C(a) = C(e) = \{e\} \Rightarrow o(C(a)) = 1$, which is impossible.

$\therefore \quad N(a) \neq \{e\}$

If possible, let $N(a) = G$.

$$\Rightarrow \quad \frac{o(G)}{o(N(a))} = \frac{o(G)}{o(G)} = 1 \Rightarrow o(C(a)) = 1, \text{ which is impossible.}$$

$\therefore \quad N(a) \neq G$

$\therefore$ Neither $N(a) = \{e\}$ nor $N(a) = G$.

$\therefore$ The group G is not simple.

Example 8. *Find the number of conjugate classes of a non-abelian group of order p^3, p being a prime number.*

Sol. Let G be a non-abelian group of order p^3.

$\therefore \quad o(Z) = p$ *(a standard result)*

Let $C(a_1), C(a_2), \ldots\ldots, C(a_m)$ be the m distinct conjugate classes of the group G.

$$\therefore \quad G = \bigcup_{i=1}^{m} C(a_i)$$

$$\therefore \quad o(G) = \sum_{i=1}^{m} o[C(a_i)]$$

The elements $a_1, a_2, \ldots\ldots a_m$ may or may not be in Z.

$$\therefore \quad o(G) = \sum_{a \in Z} o(C(a)) + \sum_{a \notin Z} o(C(a)) \qquad \ldots(1)$$

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

$$\Rightarrow \frac{o(G)}{o(N(a))} = 1 \Rightarrow o(C(a)) = 1$$

Since $o(Z) = p$, p conjugate classes are of order 1 each.

The remaining $m - p$ conjugate classes correspond to elements which are not in Z.

$$a \notin Z \Rightarrow Z \subset N(a) \Rightarrow o(Z) < o(N(a)) \qquad (\because\ a \in N(a))$$
$$\Rightarrow o(N(a)) > p$$

$\Rightarrow$ $o(N(a)) = p^2$ or p^3, because $o(N(a)) / p^3$

$o(N(a)) = p^3 \Rightarrow N(a) = G \Rightarrow x \in N(a) \quad \forall x \in G$

$\Rightarrow$ $ax = xa \quad \forall x \in G \Rightarrow a \in Z_1$, which is not true.

$\therefore$ $o(N(a)) \neq p^3 \quad \therefore \quad o(N(a)) = p^2 \quad \forall a \notin Z$

$$\therefore \quad \frac{o(G)}{o(N(a))} = \frac{p^3}{p^2} = p \quad \forall a \notin Z$$

$\Rightarrow$ $o(C(a)) = p \quad \forall p \notin Z$

$\therefore$ $m - p$ conjugate classes are of order p each.

(1) $\Rightarrow$ $p^3 = p(1) + (m - p)\,p$

$\Rightarrow$ $p^2 = 1 + m - p \Rightarrow m = p^2 + p - 1$

$\therefore$ Number of conjugate classes is $\mathbf{p^2 + p - 1}$.

6. SELF CONJUGATE ELEMENT

Let G be a group. An element a of G is said to be **self conjugate** if no element of G, other than a, is conjugate to a.

$\therefore$ $x^{-1}ax = a \quad \forall x \in G$

Equivalently $ax = xa, \forall x \in G$.

Thus, a self conjugate element of a group commutes with each element of the group.

A self conjugate element is also known as an **invariant** element.

Remark. If a is a self conjugate element of a group G, then $N(a) = G$.

7. CENTRE OF A GROUP *(K.U. 2005)*

Let G be a group. The set $\{z \in G : zx = xz\ \forall x \in G\}$ is called the **centre** of the group G and it is denoted by Z.

$$z \in Z \Rightarrow zx = xz \quad \forall x \in G$$

$\Rightarrow$ $x^{-1}(zx) = x^{-1}(xz) \Rightarrow x^{-1}zx = z \quad \forall x \in G.$

$\therefore$ z is a self conjugate element of G.

$\therefore$ The centre of a group consists of all its self conjugate elements.

Remark : $Z \subseteq N(a)\ \forall a \in G$ because $x \in Z$

$\Rightarrow$ $xy = yx\ \forall y \in G \Rightarrow xa = ax \Rightarrow x \in N(a)$.

Example 9. *Show that the centre of the group S_3 contains only one element.*

Sol. Let $X = \{a, b, c\}$. Let S_3 be the set of all one-to-one mappings of X onto X.

$\therefore$ $S_3 = \{I, (ab), (bc), (abc), (acb)\}$.

Here the mapping (ab) stands for $a \to b, b \to a, c \to c$.

The set S_3 is a group with composition of mappings as the binary operation.

We have $fI = If \quad \forall f \in S_3$

$\therefore$ $I \in Z$

We find $(ab)(bc)$:

Under $(ab)(bc)$: $a \to a \to b,\ b \to c \to c,\ c \to b \to a$

$\therefore$ $(ab)(bc) = (abc)$

Under $(bc)(ab) : a \to b \to c,\ b \to a \to a,\ c \to c \to b$

$\therefore \quad (bc)(ab) = (acb)$

$\therefore \quad (ab)(bc) \neq (bc)(ab)$

$\therefore \quad (ab), (bc) = \notin Z$

Similarly $\quad (ab)(ca) \neq (ca)(ab)$

$\therefore \quad (ca) \notin Z$

Under $(abc)(ca) : a \to c \to a,\ b \to b \to c,\ c \to a \to b$

$\therefore \quad (abc)(ca) = (bc)$

Under $(ca)(abc) : a \to b \to b,\ b \to c \to a,\ c \to a \to c$

$\therefore \quad (ca)(abc) = (ab)$

$\therefore \quad (abc)(ca) \neq (ca)(abc)$

$\therefore \quad (abc) \notin Z$

Similarly $\quad (acb) \notin Z$

$\therefore \quad Z = \{I\}.$

Theorem 1. *Let G be a group. The centre Z of G is a normal subgroup of G.*

Proof. We have $\quad Z = \{z \in G : zx = xz \ \forall\ x \in G\}$

$e \in Z$ because $\quad ex = xe \quad \forall\ x \in G \quad \therefore$ Z is non-empty.

Let $\ z_1, z_2 \in Z \quad \therefore \quad z_1x = xz_1, z_2x = xz_2 \quad \forall\ x \in G$

Now $(z_1z_2)\,x = z_1(z_2x) = z_1(xz_2) = (z_1x)z_2 = (xz_1)\,z_2 = x(z_1z_2), \quad \forall\ x \in G.$

$\therefore \quad z_1z_2 \in Z$

Let $\quad z \in Z \quad \therefore \quad zx = xz \quad \forall\ x \in G$

$\Rightarrow \quad z^{-1}(zx)\,z^{-1} = z^{-1}(xz)\,z^{-1} \quad \Rightarrow \quad (z^{-1}z)(xz^{-1}) = (z^{-1}x)(zz^{-1})$

$\Rightarrow \quad xz^{-1} = z^{-1}x \quad \Rightarrow \quad z^{-1}x = xz^{-1} \quad \forall\ x \in G$

$\therefore \quad z^{-1} \in Z$

$\therefore$ **Z is a subgroup of G.**

Let $\quad z \in Z, x \in G.$

$xzx^{-1} = (xz)x^{-1} = (zx)x^{-1} = z(xx^{-1}) = ze = z \in Z$

$\therefore \quad xzx^{-1} \in Z \quad \forall\ z \in Z \quad$ and $\quad x \in G.$

$\therefore$ Z is a normal subgroup of G.

Example 10. *Let Z be the centre of a group G. If G/Z is cyclic, show that G is abelian.*

Sol. Let Zg be a generator of the cyclic ground G/Z, for some $g \in G$.

Let $\quad a, b \in G \quad \therefore \quad Za, Zb \in G/Z$

$\Rightarrow \quad Za = (Zg)^m \quad$ for some $m \in Z$

$\therefore \quad Za = (Zg)(Zg) \ldots\ldots m$ times

$= Zgg \ldots\ldots m$ times $= Zg^m \qquad (\because$ Z is a normal subgroup of G)

$\Rightarrow \quad a \in Zg^m \quad \Rightarrow \quad a = z_1g^m \quad$ for some $z_1 \in Z$

Similarly, let $\quad b = z_2g^n$ for some $z_2 \in Z$ and $n \in Z.$

Now $\quad ab = (z_1g^m)(z_2g^n) = z_1(g^mz_2)\,g^n = z_1(z_2g^m)\,g^n = z_1z_2\,g^{m+n}$

Also $\quad ba = (z_2g^n)(z_1g^m) = z_2(g^nz_1)\,g^m = z_2(z_1g^n)\,g^m = z_2z_1\,g^{n+m} = z_1z_2g^{m+n}$

$(\because \quad z_1 \in Z \quad \Rightarrow \quad z_2z_1 = z_1z_2)$

$\therefore$ $ab = ba$. $\therefore$ G is abelian.

Theorem 2. *Let G be a group. $a \in Z$ if and only if $N(a) = G$.*

Proof. Let $a \in Z$. $\therefore$ $ax = xa \quad \forall x \in G$

$\Rightarrow$ $x \in N(a) \quad \forall x \in G$

$\Rightarrow$ $N(a) = G$

Conversely, let $N(a) = G$

$\therefore$ $ax = xa \quad \forall x \in G \quad \therefore \quad x \in Z \quad \therefore$ The result follows.

Corollary. If G is a finite group and $a \in Z$, then $o(N(a)) = o(G)$.

Proof. $a \in Z \Rightarrow N(a) = G$.

$\therefore$ $o(N(a)) = o(G)$. ($\because$ G is finite)

Theorem 3. *If G be a finite group, then* $o(G) = o(Z) + \sum_{a \in Z} \frac{o(G)}{o(N(a))}$, *where the sum runs over elements a, taken one from each conjugate class which contain more than one element.*

Proof. We know that

$$o(G) = \sum_{a} \frac{o(G)}{o(N(a))}, \qquad \ldots(1)$$

where the sum runs over elements a, taken one from each conjugate class.

Let $a \in G \quad \therefore \quad a$ may or may not be in Z. Let $a \in Z$.

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

$\Rightarrow$ $x^{-1} ax = a \quad \forall x \in G$

$\Rightarrow$ $C(a) = \{a\}$

$\therefore$ The conjugate class of a contains exactly one element.

Also $ax = xa \ \forall x \in G$ implies $N(a) = G$.

$\therefore$ $\frac{o(G)}{o(N(a))} = \frac{o(G)}{o(G)} = 1$.

$\therefore$ For each $a \in Z$, we have $\frac{o(G)}{o(N(a))} = 1$

$\therefore$ $\sum_{a \in Z} \frac{o(G)}{o(N(a))} = 1 + 1 + \ldots\ldots o(Z)$ times $= o(Z)$

Also, when $a \notin Z$, the conjugate class of a will have more than one element.

$\therefore$ (1) $\Rightarrow$ $o(G) = \sum_{a \in Z} \frac{o(G)}{o(N(a))} + \sum_{a \notin Z} \frac{o(G)}{o(N(a))} = o(Z) + \sum_{a \notin Z} \frac{o(G)}{o(N(a))}$

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

where the sum runs over elements a taken one from each conjugate class which contain more than one element.

8. CLASS EQUATION OF A FINITE GROUP

Let G be a finite group. For $a \in G$, let $N(a)$ denote the normalizer of a.

We have the equation :

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

where the sum runs over elements a, taken one from each conjugate class which contain more than one element.

This equation is called the **class equation** of the finite group G.

Theorem 1. *If $o(G) = p^n$, where p is a prime number and n is a natural number, then centre $Z \neq \{e\}$.*

Proof. If $n = 1$, then $o(G) = p$, a prime number.

$\therefore$ G is a cyclic group and hence abelian.

$\therefore$ Centre Z of G = G

$\therefore$ $o(Z) > 1 \quad \therefore \quad Z \neq \{e\}$.

Now, let us suppose that $n > 1$. Since G is a finite group, its class equation is

$$o(G) = o(Z) + \sum_{a \notin Z} \frac{o(G)}{o(N(a))} \qquad \ldots(1)$$

$a \notin Z \Rightarrow N(a) \neq G \Rightarrow N(a) \subset G$

By *Lagrange's theorem*, let

$$o(N(a)) = p^{n_a} \text{ for some } o < n_a < n.$$

The number n_a cannot be 0, because N(a) contains at least e and a.

$$\therefore \quad \frac{o(G)}{o(N(a))} = \frac{p^n}{p^{n_a}} = p^{n-n_a} = p.\, p^{n-n_a-1}$$

$$(n_a < n \Rightarrow n - n_a > 0 \Rightarrow n - n_a - 1 \geq 0)$$

$$\therefore \quad p \Big/ \frac{o(G)}{o(N(a))} \quad \forall\, a \notin Z$$

$$\Rightarrow \quad p \Big/ \sum_{a \notin Z} \frac{o(G)}{o(N(a))}$$

Aslo $o(G) = p^n$ implies $p/o(G)$.

$$\therefore \quad p \Big/ \left(o(G) - \sum_{a \notin Z} \frac{o(G)}{o(N(a))} \right)$$

$\therefore$ (1) $\Rightarrow$ $p/o(Z)$.

$\Rightarrow$ $o(Z) > 1$ $\qquad (\because \quad e \in Z \Rightarrow o(Z) \neq 0)$

$\therefore$ **Z must contain at least one element.**

Example 11. *If G is a non-abelian group of order 343, show that $o(Z) = 7$.*

Sol. We have $o(G) = 343 = (7)^3$ and 7 is a prime number.

$\therefore$ $o(G) = (7)^n$, where $n = 3$

$\therefore$ $Z \neq \{e\}$.

Since Z is a subgroup of G, we have $o(Z)/(7)^3$

$\therefore$ $o(Z) = 1$ or 7 or $(7)^2$ or $(7)^3$

$o(Z) = 1 \Rightarrow Z = \{e\}$, which is impossible.

$o(Z) = (7)^3 \Rightarrow Z = G \Rightarrow$ G is abelian, which is impossible.

$o(Z) = (7)^2 \Rightarrow o(G/Z) = \dfrac{o(G)}{o(Z)} = \dfrac{(7)^3}{(7)^2} = 7$, which is a prime number

$\therefore$ G/Z is cyclic.

$\Rightarrow$ G is abelian, which is impossible.

$\therefore$ $o(Z) = 7$.

Example 12. *If $o(G) = p^2$, where p is a prime number, then G is abelian.* (K.U. 2005)

Sol. Let Z be the centre of the group G.

$\therefore$ Z is a subgroup of G.

By *Lagrange's theorem*, $o(Z) | o(G)$ *i.e.*, $o(Z) | p^2$

$\therefore$ $o(Z) = 1$ or p or p^2

Since $o(G) = p^n$, where $n = 2$, we have $Z \neq \{e\}$.

$\therefore$ $o(Z) \neq 1$.

If possible, let $o(Z) = p$.

$\therefore$ $G - Z \neq \phi$. Let $a \in G - Z$

$\therefore$ $a \in G$ and $a \notin Z$.

For $b \in Z$, we have $ba = ab$. $\therefore$ $b \in N(a)$. Thus $Z \subseteq N(a)$

Also $a \in N(a)$ and $a \notin Z$ $\therefore$ $Z \neq N(a)$

$\therefore$ $o(N(a)) > o(Z)$ *i.e.*, $o(N(a)) > p$

By *Lagrange's theorem*, $o(N(a)) | p^2$.

$\therefore$ We have $o(N(a)) = p^2$ $\therefore$ $N(a) = G$.

$\Rightarrow$ $a \in Z$. This is against the choice of a.

$\therefore$ Our supposition is wrong.

$\therefore$ $o(Z) \neq p$. $\therefore$ The only choice is $o(Z) = p^2$.

$\therefore$ $Z = G$. Thus, $ab = ba \ \forall \ a, b \in G$.

$\therefore$ G is abelian.

Remark : The above example gives an interesting results as :

'Groups of orders 4, 9, 25, 49, 121, ... are all abelian.

IMPORTANT RESULTS

1. *The conjugacy relation on a group is an equivalence relation on the group G and the corresponding equivalence classes partitions the group G into mutually disjoint equivalence classes, called conjugate classes.*
2. *The normalizer N(a) of a in G is a subgroup of G.*
3. *If G is a finite group, then* $o(G) = \sum_a \frac{o(G)}{o(N(a))}$, *where the sum runs over elements a, taken one from each conjugate class.*
4. *The centre of a group G is a normal subgroup of G.*
5. *The number of conjugate classes of a non-abelian group of order p^3, where p is prime, is $p^2 + p - 1$.*
6. *If G is a finite group, then* $o(G) = o(Z) + \sum_{a \notin Z} \frac{o(G)}{(N(a))}$, *where the sum runs over elements a, taken one from each conjugate class which contain more than one element. This equation is called the class equation of the finite group G.*

EXERCISE 1

1. Show that in a group G the cyclic subgroup generated by an element a of G is contained in the normalizer of a.
2. Let a be any element of a group G. If $x, y \in G$ give rise to the same conjugate of a then they belong to the same right coset of $N(a)$ in G.
3. Let a be any element of a group G. If $x, y \in G$ belong to the same right coset of $N(a)$ in G, then they give rise to the same conjugate of a.
4. Show that the normalizer of a self conjugate element is the whole group.
5. Let Z be the centre of a group G. If $a \in Z$ then show that the cyclic subgroup of G which is generated by a is a normal subgroup of G.
6. If G is a non-abelian group and $o(G) = p^3$, where p is prime then show that the centre of G has exactly p elements.
7. Show that a group of order 9 is abelian.
8. Show that the centre of a non-abelian group of order 125 always have 5 elements in its centre.
9. Let H be a subgroup of the centre Z of a group G. If G/H is cyclic, show that G is abelian.
10. If $o(G) = p^n$, where p is a prime number and n is a natural number, then prove that $N \cap Z \neq \{e\}$, where $N (\neq \{e\})$ is any normal subgroup of G.
11. Find the number of conjugate classes of a non-abelian group G if :
    (*i*) $o(G) = 27$ (*ii*) $o(G) = 125$.

Answers

11. (*i*) 11 (*ii*) 29.