NORMAL SUBGROUPS

Set - V

Defn: A subgroup H of a group G is said to be a normal subgroup of G if $\forall x \in G$ and $\forall h \in H$, $xhx^{-1} \in H$.

From the definition we conclude that

(i) H is a normal subgroup of G iff $xHx^{-1} \subseteq H$ $\forall x \in G$

where $xHx^{-1} = \{xhx^{-1} / h \in H, x \in G\} \subseteq H$.

(ii) H is a normal subgroup of G iff $x^{-1}Hx \subseteq H$ $\forall x \in G$

$(\because x \in G \Rightarrow x^{-1} \in G$

$\forall h \in H,\ x^{-1}h(x^{-1})^{-1} \in H$

$\Rightarrow x^{-1}hx \in H)$

(iii) the improper subgroup $H = \{e\}$ is a normal subgroup

$(\because e \in H \Rightarrow xex^{-1} \in H \ \forall x \in G)$

(iv) and the improper subgroup $H = G$ is a normal subgroup.

$(\because h \in G \Rightarrow xhx^{-1} \in G, \forall x \in G)$

$H = \{e\}$ and $H = G$ are called improper (or) trivial normal subgroups of a group G and all other normal subgroups of G, if exist, are called proper normal subgroups of G.

Note: Any non-abelian group whose every subgroup is normal is called a Hamilton group.

Simple group: A group having no proper normal subgroups is called a simple group

→ Every group of prime order is simple.

Theorem: A subgroup H of a group G is normal iff $xHx^{-1} = H$ $\forall x \in G$.

proof: (i) Let $xHx^{-1} = H$ $\forall x \in G$

we prove that H is normal.

Since $xHx^{-1} \in H$ $\forall x \in G$.

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

(ii) Let H be a normal subgroup of G.

we prove that $xHx^{-1} = H \ \forall x \in G$

Since H is normal subgroup of G

$\therefore xHx^{-1} \subseteq H \ \forall x \in G$ —— (1)

Also $x \in G \Rightarrow x^{-1} \in G$

$\therefore \forall x \in G, \ x^{-1}H(x^{-1})^{-1} \subseteq H$

$\Rightarrow x^{-1}Hx \subseteq H$

$\Rightarrow x(x^{-1}Hx)x^{-1} \subseteq xHx^{-1}$

$\Rightarrow H \subseteq xHx^{-1}$ —— (2)

from (1) & (2), we have

$xHx^{-1} = H \ \forall x \in G$

→ A subgroup H of a group G is a normal subgroup of G iff each left coset of H in G is a right coset of H in G.

proof: (i) Let H be a normal subgroup of G

Then $xHx^{-1} = H \ \forall x \in G$

$\Rightarrow (xHx^{-1})x = Hx \ \forall x \in G$

$\Rightarrow xH = Hx \ \forall x \in G$

$\Rightarrow$ every left coset of H in G is a right coset of H in G.

(ii) Let every left coset of H in G be a right coset if H in G.

Let $x \in G$ then $xH = Hy$ for some $y \in G$.

Since $e \in H$, $x = xe \in xH$

$\Rightarrow x \in xH$

Since $xH = Hy$

$\Rightarrow x \in Hy$

$\Rightarrow Hx = Hy$ $\quad$ ($\because a \in bH \Rightarrow aH = bH$ & $a \in Hb \Rightarrow Ha = Hb$)

$\therefore xH = Hx \quad \forall x \in G$

$\Rightarrow xHx^{-1} = Hxx^{-1} \quad \forall x \in G$

$\Rightarrow xHx^{-1} = H \quad \forall x \in G$

H is a normal subgroup of G.

$\therefore$ H is a normal subgroup of G $\Leftrightarrow$ Every left coset of H in G is a right coset of H in G.

→ A subgroup H of a group G is a normal subgroup of G iff the product of two right (left) cosets of H in G is again a right (left) coset of H in G.

Proof: (i) Let H be a normal subgroup of G.

$\forall a, b \in G \Rightarrow ab \in G$

$\therefore Ha, Hb, Hab$ are right cosets of H in G.

Then $Ha \cdot Hb = H(aH)b$.

$= H(Ha)b$ $\quad$ ($\because$ H is normal $\Rightarrow aH = Ha$)

$= HHab$

$= Hab$ $\quad$ ($\because HH = H$)

$\therefore$ The product of two right cosets of H in G is again a right coset of H in G.

(ii) For $a, b \in G$, $Ha \cdot Hb = Hab$.

for $h \in H$, $x \in G$

we have $xhx^{-1} = (ex)(hx^{-1}) \in (Hx)(Hx^{-1})$

$\Rightarrow xhx^{-1} \in Hxx^{-1}$ $\quad$ ($\because Ha\,Hb = Hab$)

$\Rightarrow xhx^{-1} \in H$

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

Similarly we can prove theorem for left cosets.

Note: [1]. Let H be a normal subgroup of $(G, \cdot)$

Let $a, b \in G$ then Ha, Hb are two right cosets of H in G. Then right cosets multiplication is defined as $Ha \cdot Hb = Hab$.

12. If H is a normal subgroup of a group $(G,\cdot)$ then the following statements are equivalent to one another.

(i) $x^{-1}hx \in H$ for $x \in G$ and $h \in H$

(ii) $xHx^{-1} = H$ for $x \in G$

(iii) $xH = Hx$ for $x \in G$

(iv) the set of right (left) cosets of H in G is closed w.r.t coset multiplication.

→ Every subgroup of an abelian group is normal.

Proof: Let H be a subgroup of an abelian group G. Let $h \in H$, $x \in G$ and e be the identity element in G.

$$
\begin{aligned}
h &= eh \\
&= (xx^{-1})h \\
&= x(x^{-1}h) \\
&= x(hx^{-1}) \quad (\because G \text{ is an abelian} \Rightarrow x^{-1}h = hx^{-1}) \\
&= xhx^{-1}
\end{aligned}
$$

i.e, $h \in H \Rightarrow xhx^{-1} \in H \ \forall x \in G$

$\therefore$ H is normal subgroup of G.

$\xrightarrow{\text{Imp}}$ If G is a group and H is a subgroup of index 2 in G, then H is a normal subgroup of G.

Proof: Since the index of the subgroup H in G is 2, the number of distinct right cosets of H in G = the number of distinct left cosets of H in G = 2.

Let $x \in G$

$\therefore$ The right cosets are H, Hx and two left cosets are H, xH.

Now $x \in H$ or $x \notin H$

— If $x \in H$ then $Hx = H = xH$ $\quad (\because a \in H \Rightarrow Ha = H$ or $aH = H)$

$\Rightarrow Hx = xH$

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

- If $x \notin H$ then $Hx \neq H$ and $xH \neq H$

Since the index of H in G is 2

$\therefore G = H \cup Hx = H \cup xH$

Since there is no element common to H, Hx.

$\therefore$ we must have $Hx = xH$.

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

$\longrightarrow$ The intersection of any two normal subgroups of a group is a normal subgroup.

Proof: Let H & K be normal subgroups of a group $(G, \cdot)$

Since H & K are subgroups of G.

$\therefore H \cap K$ is also a subgroup of G.

Let $n \in H \cap K$ and $x \in G$

$\therefore n \in H$ and $n \in K$;

$\therefore xnx^{-1} \in H$ and $xnx^{-1} \in K$ ($\because H$ & K are normal subgroups of G.

$\Rightarrow xnx^{-1} \in H \cap K$ for $x \in G$

$\therefore H \cap K$ is a normal subgroup of G.

Note: The arbitrary intersection of any number of normal subgroups of a group G is also normal subgroup of G.

$\longrightarrow$ Theorem:

A normal subgroup of a group G is commutative with every complex of G.

proof: Let N be a normal subgroup and H be a complex of G.

To prove that $NH = HN$

Let $nh \in NH$ where $n \in N$ & $h \in H$

we can write

$nh = e(nh)$ $\quad (\because e \in G)$

$nh = hh^{-1}(nh)$

$= h(h^{-1}nh)$

But N is a normal subgroup of G.

$\therefore h^{-1}nh \in N$.

$\therefore nh \in HN$.

$\therefore NH \subseteq HN$ — ①

Similarly $hn \in HN$.

$\Rightarrow hn \in NH \quad (\because hn = (hn)h^{-1}h = (hnh^{-1})h \in NH)$

$\therefore HN \subseteq NH$ — ②

$\therefore$ from ① & ② we have $NH = HN$

→ If N is a normal subgroup of G and H is any subgroup of G, then HN is a subgroup of G.

proof: Let N be a normal subgroup of G and H be a subgroup of G

Since a normal subgroup of G is commutative with every complex of G.

we have $NH = HN$.

$\therefore HN$ is a subgroup of G. $\left(\because H \,\&\, K \text{ are subgroups of } G \Rightarrow HK = KH \Leftrightarrow HK < G\right)$.

If H is a subgroup of G and N is a normal subgroup of G then (i) $H \cap N$ is a normal subgroup of H.

(ii) N is a normal subgroup of HN.

proof: (i) H, N are subgroups of $G \Rightarrow H \cap N$ is a subgroup of G.

$\Rightarrow H \cap N$ is a subgroup of H $(\because H \cap N \subseteq H)$

Let $x \in H$.

$\therefore x \in G$.

Let $y \in H \cap N$.

$\therefore y \in H$ and $y \in N$.

Now $y \in N \Rightarrow xyx^{-1} \in N$ ($\because N$ is normal in G)

and $y \in H, x \in H \Rightarrow x^{-1} \in H, y \in H$

$\Rightarrow xyx^{-1} \in H$

$\therefore xyx^{-1} \in H \cap N$.

$\therefore H \cap N$ is a normal subgroup of H.

(ii) $e \in H$ and $e \in N$

Since $H \neq \phi$, $N \neq \phi$.

$\therefore HN \neq \phi$.

Let $n \in N$ then $n = en$

$\therefore en \in HN \; \forall n \in N$

$\Rightarrow N \subset HN$.

Since HN is a subgroup of G,

N is a subgroup of G and $N \subseteq HN$

$\therefore N$ is also subgroup of HN.

Let $n \in N$ and $h_1 n_1 \in HN$.

where $h_1 \in H$, $n_1 \in N$.

Now $(h_1 n_1) n (h_1 n_1)^{-1} = h_1 n_1 n n_1^{-1} h_1^{-1}$

$= h_1 (n_1 n n_1^{-1}) h_1^{-1} \in N$

($\because h_1 \in H \Rightarrow h_1 \in G$ and N is a normal subgroup of G)

$\therefore N$ is a normal subgroup of HN.

→ If N, M are normal subgroups of G, then NM is also a normal subgroup of G.

proof: Since $N \neq \phi$, $M \neq \phi$

$\Rightarrow NM \neq \phi$ and $MN \neq \phi$.

Since a normal subgroup of G is commutative with every complex of G, $NM = MN$.

Since N, M are subgroups of G.

NM is also a subgroup of G

Let $x \in G$ and $nm \in NM$.

$\therefore x(nm)x^{-1} = x(n x^{-1} x) m x^{-1}$

$= (xnx^{-1})(xmx^{-1}) \in NM$

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

Theorem → 2005 If M, N are two normal subgroups of G such that $M \cap N = \{e\}$. Then every element of M commutes with every element of N.

proof: Let $m \in M$ and $n \in N$.

To prove that $nm = mn$.

Since $n \in N$, $n^{-1} \in N$. ($\because N$ is normal subgroup of G)

and $m \in G$

we have $m(n^{-1})m^{-1} \in N$.

Also by closure in N

$nmn^{-1}m^{-1} \in N$ —— (1)

Since M is normal

$nmn^{-1} \in M$ $(\because n \in G)$

By closure in M,

$nmn^{-1}m^{-1} \in M$ —— (2)

From (1) & (2) we have

$nmn^{-1}m^{-1} \in M \cap N$

But $M \cap N = \{e\}$

$\therefore nmn^{-1}m^{-1} = e$

$\Rightarrow nmn^{-1} = m$

$\Rightarrow nm = mn$

$\therefore$ Every element of M commutes with every element of N.

Quotient group:

Theorem → H is a normal subgroup of G The set $\frac{G}{H}$ of all cosets of H in G w.r.t coset multiplication is a group.

proof: Given that H is a normal subgroup of $(G, \cdot)$

for $a \in G$, $aH = Ha$.

$\therefore \frac{G}{H}$ is the set of all cosets of H in G.

Let $\frac{G}{H} = \{Ha / a \in G\}$.

for $a, b \in G$,

we have $Ha, Hb \in \frac{G}{H}$.

we define coset multiplication on $\frac{G}{H}$ as

$(Ha) \cdot (Hb) = Hab$

we prove that the operation is well defined

Let $Ha = Ha_1$ and $Hb = Hb_1$. in $\frac{G}{H}$

$\therefore ea = a = h_1 a_1$ and $eb = b = h_2 b_1$
for some $h_1 \in H$ for some $h_2 \in H$.

Now $Hab = H(h_1 a_1)(h_2 b_1)$

$= Hh_1 (a_1 h_2) b_1$

$= Hh_1 (h_3 a_1) b_1$ ($\because$ H is normal in G
$a_1 H = Ha_1$
so that $a_1 h_2 = h_3 a_1$
for some $h_3 \in H$)

$= H(h_1 h_3) a_1 b_1$

$= Ha_1 b_1$ ($\because h_1 h_3 \in H \Rightarrow H(h_1 h_3) = H$.)

i.e., $Ha \, Hb = Ha_1 \cdot Hb_1$.

$\therefore$ coset multiplication is well defined

(i) Closure prop: $Ha, Hb \in \frac{G}{H}$

$\Rightarrow Ha \cdot Hb \in \frac{G}{H}$.

Since $a, b \in G \Rightarrow ab \in G$ and

$Ha \, Hb = Hab \in \frac{G}{H}$.

(ii) Associative prop: $Ha, Hb, Hc \in \frac{G}{H}$

$\Rightarrow (Ha \, Hb) Hc = Ha(Hb \, Hc)$

Since $(Ha \, Hb) Hc = (Hab) Hc$

$= H(ab)c$

$= Ha(bc)$ ($\because G$ is a group)

$= Ha \cdot Hbc$

$= Ha \cdot (Hb \, Hc)$

Existence of right identity:

Let $Ha \in \frac{G}{H}$ $\exists He (= H) \in \frac{G}{H}$ such that

$Ha \cdot He = Hae$

$= Ha$ $(\because ae = a \ \forall a \in G)$

$\therefore$ identity exists in $\frac{G}{H}$ and it is $He (= H)$

Existence of right inverse:

Let $Ha \in \frac{G}{H}$ $\exists Ha^{-1} \in \frac{G}{H}$; $a \in G \Rightarrow a^{-1} \in G$

such that $Ha \cdot Ha^{-1} = H(a\,a^{-1})$

$= He$ $(\because aa^{-1} = e)$
$(= H)$

$\therefore$ Every element of $\frac{G}{H}$ is invertible.

and $(Ha)^{-1} = Ha^{-1}$.

$\therefore$ $\frac{G}{H}$ is a group w.r.t coset multiplication.

Defn: If G is a group and H is a normal subgroup of G, then the set $\frac{G}{H}$ of all cosets of H in G is a group w.r.t multiplication of cosets. It is called the quotient group or factor group of G by H.

— The identity element of the quotient group $\frac{G}{H}$ is H.

Theorem: If H is a normal subgroup of a finite group G then $O\left(\frac{G}{H}\right) = \frac{O(G)}{O(H)}$

proof: $O\left(\frac{G}{H}\right)$ = number of distinct cosets of H in G.

= the index of H in G

$= [G : H]$

$= \frac{\text{number of elements in } G}{\text{number of elements in } H}$

$= \frac{O(G)}{O(H)}$.

Theorem: Every quotient group of an abelian group is abelian. (8)

proof: Let H be a subgroup of an abelian group G

But every subgroup of an abelian group is normal.

So H is a normal subgroup of G.

Let $\frac{G}{H}$ be the quotient group of G by H.

For $a, b \in G$, $ab = ba$
($\because G$ is abelian)

$\therefore Ha, Hb \in \frac{G}{H}$

Now $(Ha)(Hb) = H(ab)$
$= H(ba)$
$= Hb\,Ha$.

$\therefore \frac{G}{H}$ is abelian

→ Let P_n be the symmetric group on 'n' symbols. prove that A_n is a normal subgroup of P_n.

proof: Let $\alpha \in P_n$ and $\beta \in A_n$

then β is an even permutation. and

α may be odd or even.

Now we have to prove that $\alpha\beta\alpha^{-1}$ is an even permutation.

— If α is even then α^{-1} is also even.

Now $\alpha\beta$ is even and $\alpha\beta\alpha^{-1}$ is even.

— If α is odd, then α^{-1} is also odd.

Now $\alpha\beta$ is odd and $\alpha\beta\alpha^{-1}$ is even.

$\therefore \alpha \in P_n, \beta \in A_n \Rightarrow \alpha\beta\alpha^{-1} \in A_n$

$\therefore A_n$ is a normal subgroup of P_n.

→ Show that $H = \{1, -1\}$ is a normal subgroup of the group of non-zero real numbers under $\times^n$.

Sol^n: Let $G = \mathbb{R} - \{0\}$ be a group w.r.t $\times^n$.

Clearly $H \subset G$ and H is a subgroup of G.

for $x \in G$, $x \cdot 1 \cdot x^{-1} = x \cdot \frac{1}{x} = 1$

and $x(-1)x^{-1} = -x \cdot \frac{1}{x} = -1$

$\therefore$ for $h \in H$ and $x \in G$

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

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

Note: Suppose H is the only subgroup of finite order 'm' in the group G. Then H is a normal subgroup of G.

→ Show that $H = \{1, -1\}$ is a normal subgroup of a group $G = \{1, -1, i, -i\}$ under $\times^n$. Also write the composition table for the quotient group $\frac{G}{H}$

Sol^n: Clearly $H \subset G$ and H is a subgroup of G

Since 1 is the identity element in H.

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

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

$iH = \{i, -i\}$, $-iH = \{-i, i\}$

$xH = Hx \ \forall x \in G$
$\Rightarrow H$ is normal

Also $1 \cdot H = H \cdot 1$

$(-1)H = H(-1)$.

$i \cdot H = H \cdot i$

$(-i)H = H(-i)$

$xH = Hx \ \forall x \in G$

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

$\therefore \frac{G}{H}$ is the quotient group of G by H.

Let $\frac{G}{H} = \{H, iH\}$.

composition table is:

	H	iH
H	H	iH
iH	iH	H

$(iH)(iH) = i^2 H$
$= -1H$
$= H$.

→ Show that $H = \{1, -1, i, -i\}$ is a normal subgroup of the group of non-zero complex numbers under $\times^n$. (86)

Sol^n: Let $G = C - \{0\}$ be the given group w.r.t $\times^n$.

Clearly $H \subset G$ and H is a subgroup of G.

for $z \in G$, $z \cdot 1 \cdot z^{-1} = z \cdot \frac{1}{z} = 1$,

$z(-1)z^{-1} = -z \cdot \frac{1}{z} = -1$

$z(i)z^{-1} = i$

$z(-i)z^{-1} = -i$.

$\therefore$ for $h \in H$ and $z \in G$, $zhz^{-1} \in H$.

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

→ Every subgroup of a cyclic group is a normal subgroup.

proof: Every cyclic group is abelian group.

→ The quotient group of a cyclic group is cyclic.

proof: Let $G = \langle a \rangle$ be a cyclic group with generator 'a'

Let N be a subgroup of G.

Since G is abelian

we take that N is normal in G.

W.K.T $\frac{G}{N} = \{Nx / x \in G\}$

Now $a \in G \Rightarrow Na \in \frac{G}{N}$

$\Rightarrow \langle Na \rangle \subseteq \frac{G}{N}$ —— ①

Also $Nx \in \frac{G}{N} \Rightarrow x \in G = \langle a \rangle$.

$\therefore x = a^n$ for some $n \in Z$.

$Nx = Na^n$

$= N(a \cdot a \cdots\cdots n \text{ times})$

when 'n' is +ve integer.

$= Na \cdot Na \cdots\cdots Na \,(n \text{ times})$

$= (Na)^n$

$\therefore$ we can prove that $Nx = (Na)^n$ when $n = 0$ or n is −ve integer.

$\therefore Nx \in \frac{G}{N} \Rightarrow N(x) \in \langle Na \rangle$

$\therefore \frac{G}{N} \subseteq \langle Na \rangle$ ——— (2)

from (1) & (2) we have $\frac{G}{N} = \langle Na \rangle$

$\therefore \frac{G}{N}$ is a cyclic group

→ P_3 be the symmetric group on three symbols a, b, c and A_3 be the alternating group on three symbols a, b, c. form the composition table for the quotient group $\frac{P_3}{A_3}$

Sol^n: Let $P = \{a, b, c\}$

Let $P_3 = \{f_1, f_2, f_3, f_4, f_5, f_6\}$.

where $f_1 = I$, $f_2 = (a\,b)$, $f_3 = (b\,c)$, $f_4 = (c\,a)$

$f_5 = (a\,b\,c)$ and $f_6 = (a\,c\,b)$.

Let A_3 = set of even permutations belonging to P_3.

i.e., $A_3 = \{f_1, f_5, f_6\}$

clearly A_3 is a normal subgroup of P_3.

The elements of $\frac{P_3}{A_3}$ are the cosets of A_3 in P_3

By Lagrange's theorem,

A_3 will have only two distinct cosets in P_3

One is A_3 itself and other is $A_3 f_2$

$$\left(\because A_3f_5 = A_3 f_6 = A_3 = A_3 f_1 \right.$$
$$\left. A_3f_2 = A_3f_3 = A_3 f_4 \right)$$

The composition table for $\frac{P_3}{A_3}$ is

	A_3	A_3f_2
A_3	A_3	A_3f_2
A_3f_2	A_3f_2	A_3

$$\left(\because (A_3f_2)(A_3f_2) = A_3 f_2f_2 = A_3f_1 = A_3 \right)$$

2003 $\rightarrow$ If H is a subgroup of a group G such that $x^2 \in H$ for every $x \in G$, prove that H is a normal subgroup of G.

Sol^n: Let $g \in G$, so that $g^{-1} \in G$.

then $(g^{-1})^2 \in H$ (by hyp).

$\Rightarrow g^{-2} \in H$

and $h^{-1}g^{-2} \in H \;\; \forall h \in H$. ($\because$ H is subgroup & $h^{-1} \in H$)

Since $gh \in G \Rightarrow (gh)^2 \in H$. (by hypothesis)

Now $(gh)^2 \in H$ and $h^{-1}g^{-2} \in H$

$\Rightarrow (gh)^2 h^{-1}g^{-2} \in H$ ($\because H < G$)

$\Rightarrow ghgh h^{-1}g^{-1}g^{-1} \in H$

$\Rightarrow ghge g^{-1}g^{-1} \in H$

$\Rightarrow ghgg^{-1}g^{-1} \in H$

$\Rightarrow ghg^{-1} \in H \;\; \forall g \in G, h \in H$

($\because geg^{-1} = gg^{-1} = e$)

Hence H is normal subgroup of G

2001 → Let N be a normal subgroup of G. Show that $\frac{G}{N}$ is abelian iff $xyx^{-1}y^{-1} \in N$ for all $x, y \in G$.

Soln: Let $X, Y \in \frac{G}{N}$ then $X = Nx$, $Y = Ny$; for some $x, y \in G$.

$\frac{G}{N}$ is abelian $\Leftrightarrow XY = YX \quad \forall X, Y \in \frac{G}{N}$.

$\Leftrightarrow NxNy = NyNx \quad \forall x, y \in G$.

$\Leftrightarrow Nxy = Nyx \quad \forall x, y \in G$.

$\Leftrightarrow (xy)(yx)^{-1} \in N \quad \forall x, y \in G$

$\Leftrightarrow (xy)(x^{-1}y^{-1}) \in N \quad \forall x, y \in G$.

$\Leftrightarrow xyx^{-1}y^{-1} \in N \quad \forall x, y \in G$.

→ If H is a subgroup of a group G such that $x^2 \in H$ for all $x \in G$. Prove that $\frac{G}{H}$ is abelian.

Soln: Given that H is a subgroup of G such that

$x^2 \in H \quad \forall x \in G$. — (1)

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

Now we have to prove that $\frac{G}{H}$ is abelian

W.K.T $\frac{G}{H}$ abelian $\Leftrightarrow xyx^{-1}y^{-1} \in H \quad \forall x, y \in G$.

Let $x, y \in G$,

$x^{-1}y \in G \Rightarrow (x^{-1}y)^2 \in H$ (by (1))

Also $x^2 \in H$ & $y^{-2} \in H$.

$\therefore x^2 (x^{-1}y)^2 y^{-2} \in H \quad (\because H < G)$

$\Rightarrow xx(x^{-1}y)(x^{-1}y)y^{-1}y^{-1} \in H$

$\Rightarrow x(xx^{-1})yx^{-1}(yy^{-1})y^{-1} \in H$

$\Rightarrow xeyx^{-1}ey^{-1} \in H$

$\Rightarrow xyx^{-1}y^{-1} \in H \quad \forall x, y \in G$.

$\therefore \frac{G}{H}$ is abelian

Conjugate Elements:

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

— If $a = x^{-1}bx$, then 'a' is called the transform of b by 'x'.

— If 'a' is conjugate to 'b' i.e, $a \sim b$ then this relation in G is called the relation of conjugacy

Note: we also define conjugate elements as follows:

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

Ex: $(\underset{a}{1\,2\,3}) \sim (\underset{b}{1\,3\,2})$ in S_3

Take $\theta = (2\,3) \in S_3$

Then $\theta(1\,3\,2)\theta^{-1} = (2\,3)(1\,3\,2)(2\,3)$
$= (2\,3)(1\,3)$
$= (1\,2\,3)$

→ 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 $a = eae$
$= e^{-1}ae$, $e \in G$

Symmetric:

Let $a \sim b$ then $a = x^{-1}bx$, $x \in G$

$\Rightarrow xax^{-1} = x(x^{-1}bx)x^{-1}$

$\Rightarrow xax^{-1} = (xx^{-1})b(xx^{-1})$
$= e.b.e$
$= b$

$\therefore xax^{-1} = b$

$\Rightarrow b = (x^{-1})^{-1}ax^{-1}$; $x^{-1} \in G$

$\Rightarrow b \sim a$

Transitive: Let $a \sim b$ and $b \sim c$ then $a = x^{-1}bx$ and $b = y^{-1}cy$ for some $x, y \in G$.

$\Rightarrow a = x^{-1}(y^{-1}cy)x$

$= (yx)^{-1}c(yx)$; $yx \in G$

$\Rightarrow a \sim c$.

$\therefore$ The relation $(\sim)$ of conjugacy is an equivalence relation on G.

Note: [1]. for $a \in G$, the equivalence class of 'a', denoted by $C(a)$ (or) $[a]$, is given by

$C(a) = \{x \in G / x \sim a\}$

$= \{x \in G / x = y^{-1}ay, y \in G\}$

$\therefore C(a) = \{y^{-1}ay / y \in G\}$.

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

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

$\therefore$ It will partition G into disjoint equivalence classes, called classes of conjugate elements.

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

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

Lemma:
If $f \in S_n$ be such that $f : i \rightarrow j$ then $\theta f \theta^{-1} : \theta(i) \rightarrow \theta(j)$ for all $\theta \in S_n$.

proof: Let $\theta : i \rightarrow s$ and $j \rightarrow t$

then $\theta^{-1} : s \rightarrow i$ and $t \rightarrow j$

$\therefore \theta f \theta^{-1} : s \xrightarrow{\theta^{-1}} i \xrightarrow{f} j \xrightarrow{\theta} t$.

Here we have applied right to left.

Hence $\theta f \theta^{-1} : s \to t$

(or)

$$\boxed{\theta f \theta^{-1} : \theta(i) \to \theta(j)}$$

Rule: In order to compute $\theta f \theta^{-1}$: replace every symbol in f by its θ-image.

Ex: $\theta(1\ 2\ 3)\theta^{-1} = (\theta(1)\ \theta(2)\ \theta(3))$

if $\theta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix} \in S_5$

then $\theta(1 2 3)\theta^{-1} = (5\ 4\ 1)$

→ Find out all the conjugate classes of S_3

Sol^n: $S_3 = \{I, (1\ 2), (2\ 3), (1\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$

Now we write various conjugate classes in S_3 are:

$[I] = \{\theta I \theta^{-1} / \theta \in S_3\}$
$= \{I\}$

$[(1\ 2)] = \{\theta(1\ 2)\theta^{-1} / \theta \in S_3\}$
$= \{(\theta(1)\ \theta(2)) / \theta \in S_3\}$ (by Lemma)

Here $[(1\ 2)]$ consists of all 2-cycles of S_3

i.e, $[(1\ 2)] = \{(1\ 2), (1\ 3), (2\ 3)\}$

Similarly $[(2\ 3)] = \{(1\ 2), (2\ 3), (1\ 3)\} = [(1\ 3)]$

Now $[(1\ 2\ 3)] = \{\theta(1\ 2\ 3)\theta^{-1} / \theta \in S_3\}$
$= \{(\theta(1)\ \theta(2)\ \theta(3)) / \theta \in S_3\}$

Here $[(1\ 2\ 3)]$ consists of all 3-cycles of S_3

i.e, $[(1\ 2\ 3)] = \{(1\ 2\ 3), (1\ 3\ 2)\}$

Similarly $[(1\ 3\ 2)] = \{(1\ 2\ 3), (1\ 3\ 2)\}$

Hence all the distinct conjugate classes of S_3 are

$\{I\}$, $\{(1\,2), (2\,3), (3\,1)\}$, $\{(1\,2\,3), (1\,3\,2)\}$

and their union is S_3.

The number of conjugate classes of S_3 is 3.

H.W → Find out all the conjugate classes of S_4.

Note: [1] $C(e) = \{e\}$
where e is the identity element of the group G.

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

[2]. If G is finite group then the number of distinct elements in $C(a)$ is denoted by C_a (or) $O(C(a))$.

[3]. In an abelian group G.
$C(a) = \{a\}$ $\forall a \in G$
$(\because C(a) = \{x^{-1}ax \mid x \in G\}$
$= \{x^{-1}xa \mid x \in G\}$
$= \{a\}$ $\forall a \in G$.

$\therefore O(C(a)) = 1$

Normalizer of an element of a group:

If a is an element of a group G, then the normalizer of 'a' in G is the set of all those elements of G which commute with 'a'.

The normalizer of 'a' in G is denoted by $N(a)$.

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

— The normalizer of 'a' i.e, $N(a)$ is a subgroup of G.

Note: [1] If $e \in G$, $ex = xe = x$ $\forall x \in G$
$\Rightarrow N(e) = G$.

[2] If G is abelian group and $a \in G$
then $xa = ax$ $\forall x \in G$
$\therefore N(a) = G$

→ If G is a finite group then C_a (or) $o[C(a)] = \frac{o(G)}{o(N(a))}$

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

(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:

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

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

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

which is the conjugate class of 'a'.

further more $G = \bigcup_{a \in G} C(a)$ ——— ①

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

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

where $N(a) = \{x \in G \mid xa = ax\}$

Define a function $f: C(a) \to \Sigma$

as $f(x^{-1}ax) = N(a) \cdot x$, $x \in G$ ——— ②

TO prove f is well defined:

$x^{-1}ax = y^{-1}ay$

$\Rightarrow ax = xy^{-1}ay$

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

$\Rightarrow xy^{-1} \in N(a)$.

$\Rightarrow N(a)x = N(a)y$ ($\because N$ is subgroup)

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

$\therefore f$ is well defined.

To prove f is 1-1:

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

$\Rightarrow N(a)\cdot x = N(a)\cdot y$ (by ②)

$\Rightarrow xy^{-1} \in N(a)$

$\Rightarrow xy^{-1}a = axy^{-1}$ (by defn of $N(a)$)

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

$\therefore f$ is 1-1.

To prove f is onto:

for any $X \in \Sigma$

$\Rightarrow X = N(a)\cdot g;\ g \in G$

$\Rightarrow X = f(g^{-1}ag)$ (by ②)

and $g^{-1}ag \in C(a)$.

$\therefore f$ is onto.

$\therefore$ there exists a one-to-one correspondence between $C(a)$ and Σ.

Since G is finite.

$\therefore$ Number of distinct elements in $C(a)$ = Number of distinct right cosets of $N(a)$ in G.

i.e., $o(C(a)) = o(\Sigma)$

= the number of distinct right cosets of $N(a)$ in G.

= the index of $N(a)$ in G.

$= \dfrac{o(G)}{o(N(a))}$

$= i_G N(a)$.

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

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: Define a relation on G as follows:

$a \sim b \Leftrightarrow a = x^{-1}bx$ for some $x \in G$.

Then $\sim$ is an equivalence relation on G and the equivalence class of 'a' in G is $C(a) = \{x^{-1}ax / x \in G\}$ which is the conjugate class of 'a' in G

Further more $G = \bigcup_{a\in G} C(a)$ —— ①

i.e, G = the union of mutually disjoint conjugate classes.

Since G is finite group.

$\therefore$ the number of distinct conjugate classes of G. will be finite say k.

i.e, If $C(a_1), C(a_2), \ldots\ldots C(a_k)$ are the 'k' distinct conjugate classes of G

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

i.e, the number of elements in G = the number of elements in $C(a_1)$ + the number of elements in $C(a_2) + \cdots$ + number of elements in $C(a_k)$.

($\because$ two distinct conjugate classes have no common element.

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

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

W.K.T $o(C(a)) = \dfrac{o(G)}{o(N(a))}$

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

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

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

→ verify the class equation for S_3.

Sol^n: $S_3 = \{I, (1\,2), (2\,3), (1\,3), (1\,2\,3), (1\,3\,2)\}$

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

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

Now $N(I) = S_3$.

$N(1\,2) = \{I, (1\,2)\}$

since $I \in S_3$, $I(1\,2) = (1\,2)I$

$(1\,2) \in S_3$

$(1\,2)(1\,2) = (1\,2)(1\,2)$

$(2\,3) \in S_3$, $(2\,3)(1\,2) = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$

$= (1\,3\,2)$

and $(1\,2)(2\,3) = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = (1\,2\,3)$

$\therefore (2\,3)(1\,2) \neq (1\,2)(2\,3)$

Similarly $(1\,3)(1\,2) \neq (1\,2)(1\,3)$

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

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

$N[(1\,2\,3)] = \{I, (1\,2\,3), (1\,3\,2)\}$

$$\therefore \sum_{a\in G} \frac{o(G)}{o(N(a))} = \frac{o(G)}{o(N(I))} + \frac{o(G)}{o[N(1\,2)]} + \frac{o(G)}{o\{N[(1\,2\,3)]\}} = \frac{6}{6} + \frac{6}{2} + \frac{6}{3} = 1+3+2 = 6 = o(G)$$

Self-conjugate element of a group:

Defn: $(G, \cdot)$ is a group and $a \in G$ such that $a = x^{-1}ax \;\forall x \in G$.

Then 'a' is called self conjugate element of G.

A self-conjugate element is some times called an invariant element.

Here $a = x^{-1}ax$.

The centre of a group:

The set Z of all self conjugate elements of a group G is called the centre of the group.

i.e. $Z = \{z \in G / zx = xz \;\forall x \in G\}$.

→ The centre Z of a group G is subgroup of G.

→ The centre Z of a group G is normal subgroup of G.

proof: Given that Z is the centre of a group G.

i.e. $Z = \{z \in G / zx = xz \;\forall x \in G\}$.

Clearly it is a subgroup of G.

Let $x \in G$ and $z \in Z$ then
$$\begin{aligned} xzx^{-1} &= (xz)x^{-1} \\ &= (zx)x^{-1} \text{ (by defn of Z)} \\ &= zxx^{-1} \\ &= ze \\ &= z \in Z \end{aligned}$$

$\therefore xzx^{-1} \in Z \;\forall x \in G$

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

→ $a \in Z$ iff $N(a) = G$

If G is finite, $a \in Z$ iff $O(N(a)) = O(G)$.

Proof: Let $a \in Z$ then by defn of Z we have $ax = xa \;\forall x \in G$.

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

now $a \in Z \Leftrightarrow ax = xa \ \forall x \in G$ (by defn of Z)

$\Leftrightarrow x \in N(a) \ \forall x \in G$ (by defn of $N(a)$)

$\Leftrightarrow N(a) = G$. ($\because N(a) \subseteq G$ and each element of G is in $N(a)$)

If the group G is finite,

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

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

$\therefore$ If the group G is finite then $a \in Z$

$\Leftrightarrow o(G) = o(N(a))$.

Theorem Second form of Class equation:

If G is a finite group then

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

where Z being the centre of the group G.

and the summation runs over one element 'a' in each conjugate class containing more than one element.

Pr: The class equation of finite group G is

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

(or)

$$o(G) = \sum_{a \in Z} \frac{o(G)}{o(N(a))} + \sum_{a \notin Z} \frac{o(G)}{o(N(a))} \quad \text{—— (1)}$$

($\because G = Z \cup G \setminus Z$)

W.K.T If G is finite, $a \in Z \Leftrightarrow o(N(a)) = o(G)$

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

$\Leftrightarrow$ the conjugate class of 'a' in G contains only one element.

i.e, the number of conjugate classes each having only one element is equal to $O(Z)$.

$$\therefore O(Z) = \sum_{a \in Z} \frac{O(G)}{O(N(a))}.$$

$$\therefore ① \equiv \quad O(G) = O(Z) + \sum_{a \notin Z} \frac{O(G)}{O(N(a))}$$

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

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

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

$$O(G) = O(Z) + \sum_{a \notin Z} i_G(N(a)),$$

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

→ If $O(G) = p^n$ where p is a prime number, then the centre $Z \neq \{e\}$ i.e, $O(Z) > 1$.

Proof. The class equation of a finite group G is

$$O(G) = O(Z) + \sum_{a \notin Z} \frac{O(G)}{O(N(a))} \quad \text{———} \quad ①$$

where the summation runs over one element 'a' in each conjugate class containing more than one element.

Now $\forall a \in G$, $N(a)$ is a subgroup of G

$\therefore$ By Lagrange's theorem

$O(N(a))$ divides $O(G)$ i.e, $\dfrac{O(G)}{O(N(a))}$

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

$\Rightarrow O(N(a)) < O(G) = p^n$

$\therefore$ If $a \notin Z$ then $O(N(a))$ must be of the form

p^k where $1 \le k \le n$

$\therefore \dfrac{O(G)}{O(N(a))} = \dfrac{p^n}{p^k} = p^{n-k}$

$\Rightarrow$ p divides $\dfrac{O(G)}{O(N(a))}$

$\Rightarrow$ p divides $\sum_{a \notin Z} \dfrac{O(G)}{O(N(a))}$ —— (2)

Also p divides $O(G) = p^n$ —— (3)

from (2) & (3),

p divides $\left[O(G) - \sum_{a \notin Z} \dfrac{O(G)}{O(N(a))}\right]$

$= O(Z)$ (by (1))

$\therefore$ p divides $O(Z)$

i.e, $\dfrac{O(Z)}{p}$

Since p is prime.

$O(Z)$ is atleast 2

$\therefore O(Z) > 1$

i.e, $Z \ne \{e\}$

2002 If $O(G) = p^2$, where p is prime number then G is abelian.

proof Since $O(G) = p^2$, p is prime

$\therefore Z \ne \{e\}$ i.e, $O(Z) > 1$

By Lagrange's theorem

$O(Z)$ divides $O(G) = p^2$

i.e, $\dfrac{O(G)}{O(Z)}$ i.e, $\dfrac{p^2}{O(Z)}$

$\therefore O(Z) = p^2$ or p.

case(i) Let $O(Z) = p^2$

then $O(Z) = O(G) \Rightarrow Z = G$ ($\because Z < G$)

Since $\forall a \in G \Rightarrow a \in Z \Rightarrow ax = xa \quad \forall x \in G$

$\therefore G$ is abelian.

Case(ii): Let $O(Z) = p$

since $O(G) = p^2 > p$

i.e, $p < p^2$

i.e, $O(Z) < O(G)$

$\therefore Z$ is proper subgroup of G.

So that there exists some $a \in G$ such that $a \notin Z$

W.K.T $N(a) = \{x \in G / xa = ax\}$ is a subgroup of G and $a \in N(a)$.

Also $x \in Z \Rightarrow x \in N(a)$

$\therefore Z \subseteq N(a)$

$a \notin Z \Rightarrow O(Z) < O(N(a))$

$\Rightarrow p < O(N(a))$

By Lagrange's theorem

$O(N(a))$ divides $O(G) = p^2$ i.e, $\frac{O(G)}{O(N(a))}$

and $O(N(a)) > p$

$\therefore O(N(a)) = p^2 \Rightarrow O(N(a)) = O(G)$

$\Rightarrow N(a) = G \quad (\because N(a) \subseteq G)$

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

$\Rightarrow a \in Z.$

which is a contradiction.

$\therefore O(Z) = p$ is impossible.

$\therefore O(Z) = p^2.$

In this case we have already proved that G is abelian.

$\longrightarrow$ If G is a non-abelian group of order p^3, where p is prime number, Show that $O(Z) = p$.

Solⁿ: Since $O(G)=p^3$, p is prime.

$\therefore Z \neq \{e\}$ i.e, $O(Z)>1$ —— (1)

By Lagrange's theorem

$O(Z)$ divides $O(G)=p^3$

i.e, $\frac{O(G)}{O(Z)} = \frac{p^3}{O(Z)}$

$O(Z)=1$ or p or p^2 or p^3.

By (1),

$O(Z)=p$ or p^2 or p^3

Let, if possible $O(Z)=p^2$

then $O\left(\frac{G}{Z}\right) = \frac{O(G)}{O(Z)} = \frac{p^3}{p^2} = p$.

$\therefore \frac{G}{Z}$ is cyclic

($\because$ a group of prime order is cyclic)

$\therefore G$ is abelian

($\because$ If $\frac{G}{Z}$ is cyclic then G is abelian)

which is contradiction to hyp.

$\therefore O(Z) \neq p^2$

Let ~~if~~ possible. $O(Z)=p^3$

$O(Z)=O(G)$

$\Rightarrow Z=G$ $(\because Z<G)$

$\forall a \in G \Rightarrow a \in Z$.

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

$\Rightarrow G$ is abelian

which is contradiction to hyp.

$\therefore O(Z) \neq p^3$

$\therefore O(Z)=p$