Case I. Let $o(Z) = p^2$. Then

$$o(Z) = o(G), \text{ since } o(G) = p^2$$

$$\Rightarrow \quad Z = G, \text{ since } Z \text{ is a subgroup of } G$$

$\Rightarrow G$ is abelian, since for any

$$a \in G \Rightarrow a \in Z \Rightarrow ax = xa \ \forall \ x, a \in G.$$

Case II. Let $o(Z) = p$.

Since $o(G) = p^2 > p$, Z is a *proper* subgroup of G so that there exists some $a \in G$ such that $a \notin Z$.

We know that $N(a) = \{x \in G : xa = ax\}$ is a subgroup of G. Further $Z \subset_{\neq} N(a)$, since $a \in N(a)$ but $a \notin Z$. Consequently,

$$o[N(a)] > o(Z) = p.$$

By Lagrange's Theorem, $o[N(a)]$ divides $o(G) = p^2$ and $o[N(a)] > p$.

Consequently,

$$o[N(a)] = p^2 \Rightarrow o[N(a)] = o(G)$$

$$\Rightarrow \quad N(a) = G, \text{ since } N(a) < G$$

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

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

$$\Rightarrow \quad a \in Z, \text{ a contradiction.}$$

Hence the case $o(Z) = p$ is impossible.

We have only $o(Z) = p^2$ and in this case we have already shown that G is abelian.

Remark 1. The above theorem gives us interesting results such as : *Groups of orders 4, 9, 25, 49, 121, 169 etc. are all abelian, since these numbers are of the form p^2, $p = 2, 3, 5, 7, 11, 13$ etc.*

Remark 2. We know that every group of prime order is cyclic and so is abelian. *Hence every group of order p and p^2 (p a prime) is abelian. However, a group of order p^3 may not be abelian.* For example, the Quaternion group of order $8 = 2^3$ ($p = 2$) is non-abelian.

Theorem 3.4.3. (Cauchy's Theorem for finite abelian groups)

Let G be a finite abelian group such that p divides $o(G)$, p being a prime number. Then there exists an element $a \neq e \in G$ such that $a^p = e$.

[D.U., 1998, 93]

Proof. Let $o(G) = n$. We shall prove the theorem by induction on n. Obviously, the theorem is true for $n = 1$. Suppose the result is true for all abelian groups of orders less than n. It means :

If $p \mid o(T)$, where T is an abelian group such that $o(T) < n$; then there exists some $t \neq e \in T$ such that $t^p = e$. We call the above statement as *Induction Hypothesis*. We shall now prove the result for G, $o(G) = n$.

Case I. *Suppose G has no proper subgroups.*

Then G must be cyclic of prime order.

Since p is prime and p divides $o(G)$, so

$$o(G) = p \text{ and } G = \langle g \rangle, g \neq e \text{ and } g^p = e.$$

Thus the result is true in this case.

Case II. *Suppose G has a proper subgroup, say N i.e., $N < G$, $N \neq (e)$ and $N \neq G$.* Let $o(N) = m < n$.

If $p \mid o(N)$, where N is abelian and $o(N) < o(G)$; then by induction hypothesis, there exists an element $x \in N$ (and so $x \in G$), $x \neq e$ such that $x^p = e$. Thus the result is true.

Let $p \dagger o(N)$.

Since G is abelian and $N < G$, so $N \lhd G$. We have

$$o(G) = o\left(\frac{G}{N}\right) . o(N) \qquad \ldots(1)$$

Since $p \mid o(G)$ and $p \dagger (N)$, therefore by (1),

$$p \mid o\left(\frac{G}{N}\right), \quad \text{where} \quad o\left(\frac{G}{N}\right) = \frac{o(G)}{o(N)} < o(G) .$$

and further G/N is abelian (since G is abelian).

Hence by induction hypothesis (as applied to the group G/N), there exists an element $X \in G/N$, $X \neq \bar{e}$ $(= N)$ such that

$$X^p = \bar{e} \text{ or } X^p = N.$$

Now $X \in G/N \Rightarrow X = Ng$ for some $g \in G$.

$$\therefore \quad X^p = N \Rightarrow (Ng)^p = N \Rightarrow Ng^p = N \Rightarrow g^p \in N \qquad \ldots(2)$$

and $X \neq \bar{e} \Rightarrow Ng \neq N \Rightarrow g \notin N.$

Since $g^p \in N$ and $o(N) = m$, therefore

$$(g^p)^m = e \text{ (By Lagrange's Theorem)}$$

$$\Rightarrow \quad g^{pm} = e \Rightarrow (g^m)^p = e \Rightarrow a^p = e, \text{ where } a = g^m \in G.$$

Finally, we show that $a \neq e$.

Let, if possible, $a = e$. Then

$$g^m = e \Rightarrow Ng^m = Ne \Rightarrow (Ng)^m = N$$

$$\Rightarrow \quad o(Ng) \mid m \Rightarrow o(X) \mid o(N) \Rightarrow p \mid o(N).$$

This is contrary to the hypothesis that $p \dagger o(N)$. Hence $a \neq e \in G$ and $a^p = e$. This completes the induction and the theorem is proved.

Now we prove the above theorem for any finite group G.

Theorem 3.4.4. (Cauchy's Theorem)

If G is any finite group such that $p \mid o(G)$, where p is a prime number, then G has an element of order p. [D.U., 1998, 93]

Proof. We shall prove that theorem by induction on $o(G)$. Obviously, the theorem is true when $o(G) = 1$ *i.e.*, $G = (e)$. Suppose the result is true for all groups of orders $< o(G)$. *It means if T is any finite group such that $p \mid o(T)$ and $o(T) < o(G)$, then there exists some element $t \neq e \in T$ such that* (*Induction Hypothesis*)

$$t^p = e.$$

Let T be any subgroup of G such that $o(T) < o(G)$.

If $p \mid o(T)$, then by induction hypothesis T (and hence G) has an element of order p. Thus the result is true in this case.

Let $p \dagger o(T)$ for *all proper* subgroups T of G. ...(1)

In particular, $p \dagger o(N(a))$ for $a \notin Z$, since $a \notin Z \Rightarrow N(a) \neq G$.

The class equation of G is

$$o(G) = o(Z) + \sum_{a \notin Z} \frac{o(G)}{o(N(a))}. \qquad \ldots(2)$$

We have

$$o(G) = \frac{o(G)}{o(N(a))} \cdot o(N(a)). \qquad \ldots(3)$$

Since $p \mid o(G)$ and $p \dagger o(N(a))$, therefore, by (3),

$$p \mid \frac{o(G)}{o(N(a))} \text{ for each } a \notin Z$$

$$\Rightarrow \qquad p \mid \sum_{a \notin Z} \frac{o(G)}{o(N(a))}. \quad \text{Also } p \mid o(G).$$

Thus p divides $\left[o(G) - \sum_{a \notin Z} \frac{o(G)}{o(N(a))} \right] \Rightarrow p \mid o(Z)$, by (2).

By our assumption in (1), $o(Z) = o(G)$

$\Rightarrow$ $G = Z$, since $Z < G$

$\Rightarrow$ G is abelian and $p \mid o(G)$.

Hence, by Cauchy's Theorem for abelian groups, G has an element of order p.

Corollary. *If G is any finite group and $p \mid o(G)$, p being a prime number, then G has a subgroup of order p.*

Proof. By Cauchy's Theorem, there exists an element $a \neq e \in G$ such that $a^p = e$.

Let $H = \{a, a^2, \ldots, a^{p-1}, a^p = e\}$.

Then H is a subgroup of G of order p.

Remark. By virtue of the above corollary, we observe that a *weak converse* of Lagrange's theorem holds when p divides $o(G)$, p being a prime number.

As a consequence of this :

(*a*) *A group of order 12 must have subgroups of orders 2 and 3*, since 2 and 3 are prime numbers which divide $o(G) = 12$. However, we can not say whether such a group will have a subgroup of order 4 or 6.

(*b*) *A group of order 30 must have a subgroup of order 2, 3 and 5.* However, such a group may not have a subgroup of order 6, 10, 15.

Ex. *Tick the correct answer :*

Let $o(G) = 15$. *Then*

(*i*) *G may have a subgroup of order 5.*

(*ii*) *G may have a subgroup of order 3.*

(*iii*) *G must have subgroups of orders 3 and 5.*

(*iv*) *G has a subgroup of order 3 or 5.*

Theorem 3.4.5. *If G is a finite abelian group, m a positive integer such that m divides o (G), then show that G contains a subgroup of order m.* [D.U., 1997, 96]

Proof. Let $o(G) = n$. We shall prove the result by induction on n. Obviously, the result is true for $n = 1$ *i.e.*, $G = (e)$. Suppose the given result is true for all finite abelian groups of orders $< n$. *It means if T is any finite abelian group of order* $< n$, *and if k is a positive integer such that k divides* $o(T)$, *then T has a subgroup of order k.* (*Induction Hypothesis*).

We are given that $m \mid n$. Let p be a prime number such that $p \mid m$.

Then

$$m = pk \text{ for some positive integer } k.$$

Now $p \mid m$ and $m \mid n \Rightarrow p \mid n$ *i.e.*, $p \mid o(G)$.

By Cauchy's Theorem, there exists an element $a \neq e \in G$ such that

$$a^p = e.$$

Let $N\{a, a^2, ..., a^{p-1}, a^p = e\}$.

Then N is a normal subgroup of G of order p, since $N < G$ and G is abelian.

Now $$o\left(\frac{G}{N}\right) = \frac{o(G)}{o(N)} = \frac{n}{p} < n.$$

Also $$o(G) = o\left(\frac{G}{N}\right) o(N), \text{ where } o(N) = p. \qquad ...(1)$$

Since $m = pk$ divides $o(G)$, therefore, by (1)

k divides $o\left(\frac{G}{N}\right)$ and $o\left(\frac{G}{N}\right) < n$.

By induction hypothesis, G/N has a subgroup, say H/N of order k

i.e., $o\left(\frac{H}{N}\right) = k$, where $H < G, H \supseteq N$

$\Rightarrow \quad \frac{o(H)}{o(N)} = k \Rightarrow o(H) = pk \Rightarrow o(H) = m.$

Hence H is a subgroup of G of order m. This completes the induction and the result is proved.

Remark. The above result shows that :

The converse of Lagrange's Theorem is true for finite abelian groups.

Ex. *State the two situations under which the converse of Lagrange's theorem holds.*

[**Hint.** See the Remarks of Theorem 3.4.4 and 3.4.5]

EXAMPLES

Example 3.4.1. *If G is a non-abelian group of order p^3, where p is a prime number, show that $o[Z(G)] = p$.*

Solution. Since $o(G) = p^3$, $o[Z(G)] > 1$. ...(1)

By Lagrange's Theorem, $o[Z(G)]$ divides $o(G) = p^3$

$\Rightarrow \quad o[Z(G)] = 1$ or p or p^2.

Using (1), $o[Z(G)] = p$ or p^2.

Let, if possible, $o[Z(G)] = p^2$.

Then $o\left(\frac{G}{Z}\right) = \frac{o(G)}{o(Z)} = \frac{p^3}{p^2} = p$

$\Rightarrow G/Z$ is cyclic, since a group of prime order is cyclic

$\Rightarrow G$ is abelian, a contradiction.

[$\because$ if G/Z is cyclic, then G is abelian].

$\therefore \quad o[Z(G)] \neq p^2$. Hence $o[Z(G)] = p$.

Example 3.4.2. *Find the number of conjugate classes of a non-abelian group of order p^3, p being a prime number.*

Solution. By Example 3.4.1, $o(Z) = p$ ...(1)

Let m be the number of conjugate classes of G. Let $a \in G$ be arbitrary. We know

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

If $a \in Z$, then $o(G) = o(N(a))$ and so $o[C(a)] = 1$. ...(3)

If $a \notin Z$, then $Z \subset_{\neq} N(a)$

$\Rightarrow \quad o(N(a)) > o(Z) = p$, by (1)

$\Rightarrow \quad o(N(a)) = p^2$ or p^3, since $o(N(a)) \mid o(G) = p^3$.

If $o(N(a)) = p^3$, then $o(N(a)) = o(G) \Rightarrow G = N(a)$

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

$\Rightarrow \quad xa = ax \ \forall \ x \in G \ \Rightarrow a \in Z$, a contradiction.

$\therefore \quad o(N(a)) = p^2$.

From (2), $\quad o[C(a)] = \dfrac{p^3}{p^2} = p$ for $a \notin Z$. ...(4)

From (3) and (4), it follows that each conjugate class $C(a)$ of G is of order 1 or p according as $a \in Z$ or $a \notin Z$. The number of conjugate classes each of order 1 is $p\ (= o(Z))$.

Consequently, the remaining $m - p$ conjugate classes are each of order p.

$\therefore \qquad o(G) = p \cdot 1 + (m-p)\, p \Rightarrow p^3 = p + (m-p)\, p$

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

Hence a non-abelian group of order p^3 has $p^2 + p - 1$ number of conjugate classes.

Example 3.4.3. *If G is a non-abelian group such that $o(G) = p^3$, show that $o(Z) = p$ and G has $p^2 + p - 1$ conjugate classes.*

Hint. See Examples 3.4.1 and 3.4.2.

Example 3.4.4. *Find the number of conjugate classes of a non-abelian group of order 27.* **[Ans.** 11]

Hint. Here $p = 3$ and so $p^2 + p - 1 = 11$.

Example 3.4.5. *Find the number of conjugate classes of a non-abelian group of order 125. Also find $o(Z)$.* **[Ans.** 29 and 5]

Please try yourself

Example 3.4.6. *Show that if p is a prime number, then any group G of order $2p$ has a normal subgroup of order p.*

Solution. Since $p \mid o(G) = 2p$, by Cauchy's theorem, there exists an element $a \neq e \in G$ such that $a^p = e$.

Consequently, $H = \{a, a^2, \ldots, a^{p-1}, a^p = e\}$ is a subgroup of G of order p *i.e.*, $o(H) = p$. We have

$$i_G(H) = \frac{o(G)}{o(H)} = \frac{2p}{p} = 2.$$

Hence H is a normal subgroup of G, since any subgroup of G of index 2 is normal in G.

Example 3.4.7. *If $o(G) = p^n$, p a prime number, and if $N \neq (e)$ is a normal subgroup of G, prove that $N \cap Z \neq (e)$, where Z is the centre of G.*

Solution. $N \neq (e) \ \Rightarrow o(N) > 1$. By Lagrange's Theorem,

$$o(N) \mid o(G) = p^n \ \Rightarrow o(N) = p^k,\ 0 < k \leq n \ \Rightarrow p \mid o(N). \qquad ...(1)$$

Since $\quad N \triangleleft G, \ Z \triangleleft G; \quad N \cap Z \triangleleft N \quad$ and $\quad N \cap Z \triangleleft Z$.

The class equation of N is given by

$$o(N) = o(N \cap Z) + \sum_{N(a) \neq N} \frac{o(N)}{o(N(a))}. \qquad ...(2)$$

Now $N(a) \underset{\neq}{<} N \Rightarrow o(N(a)) = p^l$, where $0 < l < k$.

$$\therefore \quad \frac{o(N)}{o(N(a)} = \frac{p^k}{p^l} = p^{k-l},\ k - l > 0$$

$\Rightarrow p$ divides $\dfrac{o(N)}{o(N(a))}$, whenever $N(a) \neq N$

$$\Rightarrow p \text{ divides } \sum_{N(a) \neq N} \frac{o(N)}{o(N(a))}. \qquad \ldots(3)$$

From (1), (2) and (3) ; we obtain

$$p \text{ divides } \left[o(N) - \sum_{N(a) \neq N} \frac{o(N)}{o(N(a))} \right] = o(N \cup Z)$$

$\Rightarrow p$ divides $o(N \cap Z)$, where p is prime.

Since the lowest prime is $p = 2$, $o(N \cap Z) > 1$.

Hence $N \cap Z \neq (e)$.

Example 3.4.8. *If $o(G) = p^n$, p a prime number ; show that G has a subgroup of order p^α for all α satisfying $0 \leq \alpha \leq n$.*

Equivalently : If $o(G) = p^n$, p a prime number ; show that G has subgroups each of order $p, p^2, p^3, \ldots, p^n$.

Solution. We shall prove the problem by induction on n. If $n = 1$, then $o(G) = p$ and the only subgroups of G are (e) and G itself (since a group of prime order has no proper subgroup). Thus G has a subgroup of order p^α, $\alpha = 0$ and $\alpha = 1$ and so the result is true for $n = 1$. Suppose the result is true for all groups of orders p^m, $0 < m < n$.

Since $o(G) = p^n$, $o(Z) > 1$ [Theorem 3.4.1]

By Lagrange's Theorem, $o(Z) \mid o(G) = p^n$

$\Rightarrow \quad o(Z) = p^k$, where $0 < k \leq n$

$\Rightarrow p \mid o(Z)$. Hence by Cauchy's Theorem, Z has a subgroup, say W, of order p

$\Rightarrow \quad W < Z,\ o(Z) = p$

$$\Rightarrow \quad W \lhd G \text{ and } o\left(\frac{G}{W}\right) = \frac{o(G)}{o(W)} = \frac{p^n}{p} = p^{n-1},\ n - 1 < n.$$

By induction hypothesis, G/W has a subgroup, say H/W of order p^γ for all γ satisfying $0 \leq \gamma \leq n - 1$.

Here $H < G$, $H \supseteq W$ and

$$o(H) = o\left(\frac{H}{W}\right) o(W) = p^\gamma . p = p^{\gamma+1} = p^\alpha,\ \alpha = \gamma + 1.$$

Thus G has a subgroup of order p^α for all α satisfying

$$0+1 \le \alpha \le n-1+1 \quad i.e., \quad 1 \le \alpha \le n.$$

For $\alpha = 0$, (e) is trivially a subgroup of G of order p^α. Hence G has a subgroup of order p^α for all α satisfying $0 \le \alpha \le n$. This completes the induction and the result is proved.

Example 3.4.9. *If $o(G) = p^n$, p a prime number, prove that there exist subgroups N_i, $i = 0, 1, \ldots, r$ (for some r) such that*

$$G = N_0 \supset N_1 \supset N_2 \supset \ldots \supset N_r = (e),$$

where N_i is a normal subgroup of N_{i-1} and where N_{i-1}/N_i is abelian.

Solution. We shall prove the result by induction on n. If $n = 1$, then $o(G) = p$. The only subgroups of G are $N_0 = G$ and $N_1 = (e)$. Thus $G = N_0 \supset N_1$, where $N_1 \lhd N_0$ and $N_0/N_1 = G/(e) \approx G$, which is abelian (since a group of prime order is cyclic and hence abelian). It follows that the result is true for $n = 1$. Suppose the result is true for all groups of orders p^m, $0 < m < n$. We shall prove that result for G.

Since $o(G) = p^n$, $o(Z) > 1$. [Theorem 3.4.1]

By Lagrange's Theorem, $o(Z) \mid o(G) = p^n$

$\Rightarrow o(Z) = p^k$, where $0 < k \le n$

$\Rightarrow p \mid o(Z)$. By Cauchy's Theorem, Z has a subgroup, say N, of order p *i.e.*, $N < Z$, $o(Z) = p$

$$\Rightarrow N \lhd G \text{ and } o\left(\frac{G}{N}\right) = \frac{o(G)}{o(N)} = \frac{p^n}{p} = p^{n-1},\ n-1 < n.$$

By induction hypothesis, $\overline{G} = G/N$ has subgroups

$$\overline{N}_i = \frac{N_i}{N}\ (N_i < G) \quad \text{for} \quad i = 0, 1, 2, \ldots, r$$

such that
$$\overline{G} = \overline{N}_0 \supset \overline{N}_1 \supset \ldots \supset \overline{N}_r = (\bar{e}); \qquad \ldots(1)$$

where
$$\overline{N}_i \lhd \overline{N}_{i-1} \text{ and } \overline{N}_{i-1}/\overline{N}_i \text{ is abelian.} \qquad \ldots(2)$$

From (1),
$$G = N_0 \supset N_1 \supset N_2 \supset \ldots \supset N_r = (e). \qquad \ldots(3)$$

From (2), we see that

$$\frac{N_i}{N} \lhd \frac{N_{i-1}}{N} \text{ and } \frac{N_{i-1}/N}{N_i/N} \approx \frac{N_{i-1}}{N_i} \text{ is abelian.}$$

$\Rightarrow$
$$N_i \lhd N_{i-1} \text{ and } N_{i-1}/N_i \text{ is abelian ; } i = 1, 2, \ldots, r. \qquad \ldots(4)$$

From (3) and (4), we see that the result is true for G. This completes the induction and the result is proved.

Example 3.4.10. *Prove that every abelian group of order 6 is cyclic.* [D.U., 1998]

Solution. Let G be an abelian group of order 6. Since the prime numbers 2 and 3 are both divisors of $o(G) = 6$, therefore, by Cauchy's theorem for abelian groups, there exist two elements $a \neq e$, $b \neq e \in G$ such that $o(a) = 2$ and $o(b) = 3$ *i.e.*, $a^2 = e$, $b^3 = e$.

We now proceed to show that $o(ab) = 6$.

It is clear that $ab \neq e$, for $ab = e \Rightarrow a = b^{-1}$

$\Rightarrow$ $o(a) = o(b^{-1}) = o(b) = 3 \Rightarrow o(a) = 3$, a contradiction.

Now $(ab)^2 = a^2 b^2$, since G is abelian.

$= eb^2 = b^2 \neq e$, since $o(b) = 3$.

Again $(ab)^3 = a^3 b^3$, since G is abelian

$= a(a^2)\, e = ae = a \neq e$.

Thus $o(ab) > 3$. By Lagrange's theorem, $o(ab)$ divides $o(G) = 6$. Hence $o(ab) = 6$ and so $G = \langle ab \rangle$, $(ab)^6 = e$, is cyclic.

Example 3.4.11. *If an abelian group G has subgroups of orders m and n, respectively, then show that it has a subgroup whose order is the least common multiple of m and n.*

Solution. Let H and K be two subgroups of G such that $o(H) = m$ and $o(K) = n$. Let k be the l.c.m of m and n. Since G is abelian, HK is a subgroup of G. Clearly, $m \mid o(HK)$ and $n \mid o(HK)$. It follows that $k \mid o(HK)$.

Hence, by Theorem 3.4.5, HK (and hence G) has a subgroup of order k, where k is the l.c.m. of m and n.

EXERCISES

1. Let Z be the centre of a group G and $N(a)$, the normalizer of an element $a \in G$. Show that $a \in Z$ iff $N(a) = G$. Further show that if G is finite, $a \in Z$ iff $o[N(a)] = o(G)$. [D.U., 1996]
2. Determine the conjugate classes of S_3 and verify that the number of elements in each conjugate class is a divisor of the order of the group. [**Hint.** See Example 3.3.1.]
3. Let G be an abelian group and suppose that G has elements of orders m and n, respectively. Prove that G has an element whose order is the least common multiple of m and n.

   [**Hint.** Let $a^m = e$, $b^n = e$; $a, b \in G$. Then $H = \langle a \rangle$, $K = \langle b \rangle$ are subgroups of orders m and n, respectively. Now proceed like Example 3.4.11].
4. Show that two elements a, b of a group G are conjugate iff $a = xy$ and $b = yx$ for some $x, y \in G$.

[**Hint.** Let $a = xy$ and $b = yx$. Then $x = y^{-1} b$ and so $a = xy \Rightarrow a = y^{-1} b y \Rightarrow a \sim b$. Conversely, let $a \sim b$ so that $a = c^{-1} bc$ for some $c \in G$. Take $c^{-1} b = x$ and $c = y$. Then $a = xy$ and $b = cx = yx$.]

5. Let X be a conjugacy class of elements in G and let $\overline{X} = \{x^{-1} : x \in X\}$. Show that $\overline{X}$ is a conjugacy class of elements in G.

[**Hint.** $X = \{x : x = g^{-1} a g, g \in G\}$. For $x = g^{-1} a g$, we have $x^{-1} = (g^{-1} a g)^{-1} = g^{-1} a^{-1} g$.]

6. Show that if T is an automorphism of a group G, then $T[C(a)] = C(T(a))$, where $C(a)$ is the conjugate class of $a \neq e \in G$.

7. If N is a normal subgroup of G, then N is the union of some conjugate classes in G.

[**Hint.** See Example 3.3.3.]

8. Prove that in any group, the subset of all elements which have only a finite number of conjugates in G, is a characteristic subgroup.

3.5 Conjugate and Similar Permutations

Definition 1. *Two permutations $f, g \in S_n$ are called* **similar**, *if they have the same cycle decomposition.*

Illustrations.

1. $f = (12)\,(345)\,(6789) \in S_9$
   and $g = (89)\,(1345)\,(267) \in S_9$ are similar.
2. $f = (12)\,(349) \in S_9$, $g = (4567)\,(12389) \in S_9$ are not similar.

Definition 2. *Two permutations $f, g \in S_n$ are called* **conjugate**, *if there exists some permutation $\theta \in S_n$ such that $g = \theta f \theta^{-1}$.*

For example, (123) and (132) $\in S_3$ are conjugate,

since $(123) = (23)\,(132)\,(23)^{-1}$ [$= (23)\,(132)\,(23)$]

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

Definition 3. *The* **conjugate class** *of $f \in S_n$ is*

$$C(f) = \{\theta f \theta^{-1} : \theta \in S_n\}. \quad \text{[See Sec. 3.3]}$$

We have a simple method to find out $\theta f \theta^{-1}$ as described in the following :

Lemma 3.5.1. *If $f \in S_n$ be such that $f : i \to j$, then*

$$\theta f \theta^{-1} : \theta(i) \to \theta(j) \text{ for all } \theta \in S_n.$$

Proof. Let $\theta : i \to s$ and $j \to t$.

Then $\theta^{-1} : s \to i$ and $t \to j$.

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

where we have applied right to left rule.

Hence $\theta f \theta^{-1} : s \to t$ or $\theta f \theta^{-1} : \theta(i) \to \theta(j)$.

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

For example, $\theta(123)\theta^{-1} = (\theta(1)\,\theta(2)\,\theta(3))$.

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

$$\theta(123)\theta^{-1} = (541).$$

Theorem 3.5.2. *Two permutations in* S_n *are similar if and only if they are conjugate in* S_n. [D.U., 1997, 93]

Proof. Necessary condition

Let $f, g \in S_n$ be similar. Then they are expressible as

$$f = (a_1\, a_2 \ldots a_{n_1})\,(b_1\, b_2 \ldots b_{n_2}) \ldots (x_1\, x_2 \ldots x_{n_r})$$

and $\quad g = (A_1\, A_2 \ldots A_{n_1})\,(B_1\, B_2 \ldots B_{n_2}) \ldots (X_1\, X_2 \ldots X_{n_r})$.

Let $\quad \theta = \begin{pmatrix} a_1 \ldots a_{n_1} & b_1 \ldots b_{n_2} & \ldots\ldots & x_1 \ldots x_{n_r} \\ A_1 \ldots A_{n_1} & B_1 \ldots B_{n_2} & \ldots\ldots & X_1 \ldots X_{n_r} \end{pmatrix} \in S_n$.

By Lemma 3.5.1, $\theta f \theta^{-1}$ is given by replacing every symbol in f by its θ-image *i.e.*,

$$\theta f \theta^{-1} = (\theta(a_1) \ldots \theta(a_{n_1}))\,(\theta(b_1) \ldots \theta(b_{n_2})) \ldots (\theta(x_1) \ldots \theta(x_{n_r}))$$

$$= (A_1 \ldots A_{n_1})\,(B_1 \ldots B_{n_2}) \ldots (X_1 \ldots X_{n_r}) = g.$$

$\therefore \quad g = \theta f \theta^{-1} \Rightarrow f$ and g are conjugate in S_n.

Sufficient Condition

Let $f, g \in S_n$ be conjugate. Then there exists some $\theta \in S_n$ such that

$$g = \theta f \theta^{-1}.$$

Let $\quad f = (\alpha_1\, \alpha_2 \ldots \alpha_{m_1})\,(\beta_1\, \beta_2 \ldots \beta_{m_2}) \ldots (\gamma_1\, \gamma_2 \ldots \gamma_{m_k})$.

Then $\quad g = \theta f \theta^{-1}$

or $\quad g = (\theta(\alpha_1) \ldots \theta(\alpha_{m_1}))\,(\theta(\beta_1) \ldots \theta(\beta_{m_2})) \ldots (\theta(\gamma_1) \ldots \theta(\gamma_{m_k}))$.

Since f and g have the same cycle decomposition, f and g are similar permutations in S_n.

Ex. *Show that two cycles in S_n are conjugate iff they are of the same length.*

[**Hint.** Let $f = (a_1\ a_2 \dots a_k)$, $g = (b_1\ b_2 \dots b_k)$ be two cycles each of length k. [D.U., 1998]

Let $$\theta = \begin{pmatrix} a_1 & a_2 \dots a_k \\ b_1 & b_2 \dots b_k \end{pmatrix}.$$

Then $\theta f \theta^{-1} = (\theta(a_1), \dots, \theta(a_k)) = (b_1\ b_2 \dots b_k) = g$ and so f and g are conjugate.

Conversely, let f and g be conjugate, where $f = (a_1\ a_2 \dots a_k)$. Then there exists some $\theta \in S_n$ such that $g = \theta f \theta^{-1} = (\theta(a_1), \dots, \theta(a_k))$

$\Rightarrow f$ and g are cycles each of length k.

Definition 4. (Partition of a positive integer)

If n is any positive integer, then a sequence of positive integers $n_1, n_2, \dots, n_r$, $n_1 \le n_2 \le \dots \le n_r$ is said to be a **partition** *of n, if*

$$n = n_1 + n_2 + \dots + n_r .$$

The number of partitions of n is denoted by $p(n)$.

For example, $n = 1$ has just one partition *i.e.*, $1 = 1$.

$\therefore \quad p(1) = 1.$

$n = 2$ has two partitions *viz.* $2 = 1 + 1$ and $2 = 2$.

$\therefore \quad p(2) = 2.$

$n = 3$ has three partitions *viz.* $3 = 1 + 1 + 1$, $3 = 1 + 2$, $3 = 3$.

$\therefore \quad p(3) = 3$

$n = 4$ has five partitions *viz.*

$4 = 1 + 1 + 1 + 1$, $4 = 1 + 1 + 2$, $4 = 2 + 2$, $4 = 1 + 3$, $4 = 4$.

$\therefore \quad p(4) = 5.$

Similarly, we can verify that

$$p(5) = 7, \quad p(6) = 11 \quad \text{etc.}$$

Illustration. Consider a permutation $f \in S_9$ as follows :

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 1 & 6 & 5 & 9 & 7 & 3 & 4 & 8 \end{pmatrix}$$

or $$f = (12)\,(367)\,(4598).$$

Thus f is expressible as a product of disjoint cycles of lengths 2, 3, 4 and further $9 = 2 + 3 + 4$, which gives a partition of 9. We generalize this property in the following

Theorem 3.5.3. *Show that the number of conjugate classes in S_n is $p(n)$, the number of partitions of n.* [D.U., 1996]

Proof. Let $f \in S_n$ be arbitrary. The conjugate class of f is given by

$$C(f) = \{\theta f \theta^{-1} : \theta \in S_n\}.$$

We know that every permutation in S_n can be expressed as a product of disjoint cycles. Let

$$f = (a_1\ a_2 \ldots a_{n_1})\ (b_1\ b_2 \ldots b_{n_2}) \ldots (x_1\ x_2 \ldots x_{n_r})$$

be a product of disjoint cycles of lengths $n_1, n_2, \ldots, n_r$; where

$$n_1 \le n_2 \le \ldots \le n_r \quad \text{and} \quad n = n_1 + n_2 + \ldots + n_r.$$

Thus $f \in S_n$ determines a partition of n.

For any $\theta \in S_n$, we have

$$\theta f \theta^{-1} = (\theta(a_1) \ldots \theta(a_{n_1}))\ (\theta(b_1) \ldots \theta(b_{n_2})) \ldots (\theta(x_1) \ldots \theta(x_{n_r})),$$

[Lemma 3.5.1]

which determines the same partition of n as f. It follows that any conjugate class $C(f)$ in S_n determines exactly one partition of n, obtained when f is expressed as a product of disjoint cycles.

Conversely, let $\{m_1, m_2, \ldots, m_k\}$ be a partition of n so that

$$n = m_1 + m_2 + \ldots + m_k\ ,\ m_1 \le m_2 \le \ldots \le m_k.\ \text{Then}$$

$$g = (\alpha_1\ \alpha_2 \ldots \alpha_{m_1})\ (\beta_1\ \beta_2 \ldots \beta_{m_2}) \ldots (\gamma_1\ \gamma_2 \ldots \gamma_{m_k}) \in S_n\ .$$

It follows that the partition $\{m_1, m_2, \ldots, m_k\}$ of n determines the conjugate class $C(g)$ in S_n. Hence there exists a one-to-one correspondence between the conjugate classes in S_n and the partitions of n. Since the number of partitions of n is $p(n)$, the number of conjugate classes in S_n is $p(n)$.

Remark. As a consequence of the above theorem, S_3 has $p(3) = 3$ conjugate classes and S_4 has $p(4) = 5$ conjugate classes. These facts are confirmed by the following example.

EXAMPLES

Example 3.5.1. (*i*) *Find out all the conjugate classes of* S_3.

[D.U., 1996]

(*ii*) *Find out all the conjugate classes of* S_4.

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

Various conjugate classes in S_3 are

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

$$[(12)] = \{\theta (12) \theta^{-1} : \theta \in S_3\} = \{(\theta(1)\ \theta(2)) : \theta \in S_3\},\ \text{by Lemma 3.5.1.}$$

Thus $[(12)]$ consists of all 2-cycles of S_3 *i.e.*,

$$[(12)] = \{(12), (23), (13)\}.$$

Similarly, $[(23)] = [(13)] = \{(12), (23), (13)\}$.

Now $[(123)] = \{\theta (123) \theta^{-1} : \theta \in S_3\}$

$$= \{(\theta(1), \theta(2), \theta(3)) : \theta \in S_3\}\ ,\ \text{by Lemma 3.5.1.}$$

Thus $[(123)]$ consists of all 3-cycles of S_3 *i.e.*,

$$[(123)] = \{(123), (132)\}.$$

We know that every permutation in S_n can be expressed as a product of disjoint cycles. Let

$$f = (a_1\ a_2 \ldots a_{n_1})\ (b_1\ b_2 \ldots b_{n_2}) \ldots (x_1\ x_2 \ldots x_{n_r})$$

be a product of disjoint cycles of lengths $n_1, n_2, \ldots, n_r$; where

$$n_1 \le n_2 \le \ldots \le n_r \quad \text{and} \quad n = n_1 + n_2 + \ldots + n_r.$$

Thus $f \in S_n$ determines a partition of n.

For any $\theta \in S_n$, we have

$$\theta f \theta^{-1} = (\theta(a_1) \ldots \theta(a_{n_1}))\ (\theta(b_1) \ldots \theta(b_{n_2})) \ldots (\theta(x_1) \ldots \theta(x_{n_r})),$$

[Lemma 3.5.1]

which determines the same partition of n as f. It follows that any conjugate class $C(f)$ in S_n determines exactly one partition of n, obtained when f is expressed as a product of disjoint cycles.

Conversely, let $\{m_1, m_2, \ldots, m_k\}$ be a partition of n so that

$$n = m_1 + m_2 + \ldots + m_k\ ,\ m_1 \le m_2 \le \ldots \le m_k.$$ Then

$$g = (\alpha_1\ \alpha_2 \ldots \alpha_{m_1})\ (\beta_1\ \beta_2 \ldots \beta_{m_2}) \ldots (\gamma_1\ \gamma_2 \ldots \gamma_{m_k}) \in S_n\ .$$

It follows that the partition $\{m_1, m_2, \ldots, m_k\}$ of n determines the conjugate class $C(g)$ in S_n. Hence there exists a one-to-one correspondence between the conjugate classes in S_n and the partitions of n. Since the number of partitions of n is $p(n)$, the number of conjugate classes in S_n is $p(n)$.

Remark. As a consequence of the above theorem, S_3 has $p(3) = 3$ conjugate classes and S_4 has $p(4) = 5$ conjugate classes. These facts are confirmed by the following example.

EXAMPLES

Example 3.5.1. (*i*) *Find out all the conjugate classes of* S_3.

[D.U., 1996]

(*ii*) *Find out all the conjugate classes of* S_4.

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

Various conjugate classes in S_3 are

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

$[(12)] = \{\theta(12)\theta^{-1} : \theta \in S_3\} = \{(\theta(1)\ \theta(2)) : \theta \in S_3\}$, by Lemma 3.5.1.

Thus $[(12)]$ consists of all 2-cycles of S_3 *i.e.*,

$$[(12)] = \{(12), (23), (13)\}.$$

Similarly, $[(23)] = [(13)] = \{(12), (23), (13)\}$.

Now $[(123)] = \{\theta(123)\theta^{-1} : \theta \in S_3\}$

$= \{(\theta(1), \theta(2), \theta(3)) : \theta \in S_3\}$, by Lemma 3.5.1.

Thus $[(123)]$ consists of all 3-cycles of S_3 *i.e.*,

$$[(123)] = \{(123), (132)\}.$$

Similarly, $[(132)] = [(123)]$.

Hence all the distinct conjugate classes of S_3 are

$$\{I\},\ \{(12), (23), (31)\},\ \{(123), (132)\}$$

and their union is S_3. The number of conjugate classes of S_3 is $p(3) = 3$.

(*ii*) Arguing as above, all the distinct conjugate classes of S_4 are as given below :

$$[I] = \{I\} ;$$

$$[(12)] = \{(12), (13), (14), (23), (24), (34)\} ;$$

$$[(123)] = \{(123), (124), (132), (134), (142), (143), (234), (243)\} ;$$

$$[(1234)] = \{(1234), (1243), (1324), (1342), (1423), (1432)\} ;$$

$$[(12)(34)] = \{\theta (12)(34) \theta^{-1} : \theta \in S_4\}$$

$$= \{(\theta (12) \theta^{-1})(\theta (34) \theta^{-1}) : \theta \in S_4\} \qquad (\because\ \theta^{-1}\theta = I)$$

$$= \{(\theta (1), \theta (2))(\theta (3), \theta (4)) : \theta \in S_4\}\ ,\ \text{by Lemma 3.5.1}$$

$$= \{(12)(34), (13)(24), (14)(23)\}.$$

The number of conjugate classes of S_4 is $p(4) = 5$.

Example 3.5.2. *Verify the class equation for S_3 and S_4.*

Solution. By Theorem 3.3.2, we have

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

The class equation of $G = S_3$ is verified, if we prove that

$$o(S_3) = \Sigma\, o[C(a)],$$

where the summation runs over one element in each conjugate class.

By Example 3.5.1,

$$o[C(I)] = 1,\ o[C(12)] = 3,\ o[C(123)] = 2$$

Since $1 + 3 + 2 = o(S_3)$, the result follows.

(*ii*) In S_4, we have seen that

$$o[C(I)] = 1,\ o[C\{(12)\}] = 6,\ o[C\{(123)\}] = 8,$$

$$o[C\{(1234)\}] = 6,\ o[C\{(12)(34)\}] = 3.$$

Since $1 + 6 + 8 + 6 + 3 = 24 = o(S_4)$, class equation for S_4 is verified.

Theorem 3.5.4. *Prove the centre of the symmetric group S_n for $n \geq 3$ is trivial.*

Or

Prove that : $Z(S_n) = \{I\}$ *for* $n \geq 3$.

Proof. We know $S_1 = \{I\}$ and so $Z(S_1) = \{I\}$.

For $S_2 = \{I, (12)\}$, $Z(S_2) = \{I, (12)\} = S_2$

i.e., $o[Z(S_2)] > 1$.

Now we show that

$$o[Z(S_n)] = 1 \quad i.e., \quad Z(S_n) = \{I\} \quad \text{for} \quad n \geq 3.$$

Let $\sigma \neq I \in Z(S_n)$ be arbitrary.

We can express σ as a product of disjoint cycles, say $\sigma = \sigma_1 \sigma_2 \ldots \sigma_r$ where σ_i is a cycle of length n_i ; $n_1 \geq n_2 \geq \ldots \geq n_r$ and $n_i \geq 2$ for each i.

Case I. Let $\sigma_1 = (a_1\ a_2)$.

Since $n \geq 3$, we can choose $a_3 \neq a_1$, $a_3 \neq a_2$.

Now $\sigma \in Z(S_n) \Rightarrow \sigma\theta = \theta\sigma\ \forall\ \theta \in S_n$.

In particular, $\sigma(a_1\ a_2\ a_3) = (a_1\ a_2\ a_3)\sigma$

or $$\sigma_1 \sigma_2 \ldots \sigma_r (a_1\ a_2\ a_3) = (a_1\ a_2\ a_3)\sigma_1 \sigma_2 \ldots \sigma_r$$

or $$(a_1\ a_2)\sigma_2 \ldots \sigma_r (a_1\ a_2\ a_3) = (a_1\ a_2\ a_3)(a_1\ a_2)\sigma_2 \ldots \sigma_r \quad \ldots(1)$$

Applying 'right to left rule' on the L.H.S. of (1), we see that $a_1 \to a_2$ and a_2 does not belong to any of the cycles $\sigma_2, \ldots, \sigma_r$ (since $\sigma_1, \sigma_2, \ldots, \sigma_r$ are disjoint) and finally $a_2 \to a_1$, it follows that

$$a_1 \to a_1. \quad \ldots(2)$$

Applying the same rule on the R.H.S. of (1), a_1 does not belong to any of the cycles $\sigma_2, \ldots, \sigma_r$; $a_1 \to a_2$ and finally $a_2 \to a_3$, it follows that

$$a_1 \to a_3. \quad \ldots(3)$$

In view of (2) and (3), the relation (1) is impossible.

Hence $\sigma = I\ \forall\ \sigma \in Z(S_n)$ *i.e.*,

$$Z(S_n) = \{I\}.$$

Case II. Let $\sigma_1 = (a_1\ a_2 \ldots a_{n_1}), n_1 \geq 3$.

Now $\sigma \in Z(S_n) \Rightarrow \sigma\theta = \theta\sigma\ \forall\ \theta \in S_n$.

In particular, $\sigma(a_1\ a_2) = (a_1\ a_2)\sigma$

or $$\sigma_1 \sigma_2 \ldots \sigma_r (a_1\ a_2) = (a_1\ a_2)\sigma_1 \sigma_2 \ldots \sigma_r$$

or $$\sigma_1 (a_1\ a_2)\sigma_2 \ldots \sigma_r = (a_1\ a_2)\sigma_1 \sigma_2 \ldots \sigma_r,$$

since each of $\sigma_2, \ldots, \sigma_r$ is disjoint from σ_1 (which contains a_1 and a_2).

$\therefore$ $$\sigma_1 (a_1\ a_2) = (a_1\ a_2)\sigma_1$$

or $$(a_1\ a_2 \ldots a_{n_1})(a_1\ a_2) = (a_1\ a_2)(a_1\ a_2 \ldots a_{n_1}). \quad \ldots(4)$$

Applying 'right to left rule' on the L.H.S. of (4), we see that

$$a_{n_1} \to a_{n_1} \quad \text{and} \quad a_{n_1} \to a_1 \Rightarrow a_{n_1} \to a_1.$$

Similarly, in the R.H.S. of (4), we see that

$$a_{n_1} \to a_1 \quad \text{and} \quad a_1 \to a_2 \Rightarrow a_{n_1} \to a_2.$$

It follows that (4) is again impossible and so our assumption $\sigma \neq I \in Z(S_n)$ is wrong.

Hence $Z(S_n) = \{I\}$ for $n \geq 3$.

Ex. *Tick the false one :*

(*i*) $Z(S_1) = \{I\}$ (*ii*) $Z(S_2) = \{I\}$

(*iii*) $Z(S_3) = \{I\}$ (*iv*) $Z(S_4) = \{I\}$.

EXAMPLES

Example 3.5.3. *In S_n, prove that the number of distinct r-cycles is*

$$\frac{n!}{r(n-r)!}.$$

Solution. See Example 2.4.3 of Chapter 2.

For example : The number of distinct 3-cycles in S_5 is

$$\frac{5!}{3 \times (5-3)!} = \frac{120}{6} = 20.$$

Example 3.5.4. *Find the number of conjugates of a r-cycle*

$$\sigma = (123 \ldots r) \in S_n.$$

Solution. The conjugate class of σ is

$$C(\sigma) = \{\theta \sigma \theta^{-1} : \theta \in S_n\}$$

$$= \{\theta (123 \ldots r) \theta^{-1} : \theta \in S_n\}$$

$$= \{(\theta(1), \theta(2), \ldots, \theta(r)) : \theta \in S_n\}, \text{ by Lemma 3.5.1.}$$

Thus $C(\sigma)$ consists of all distinct r-cycles in S_n. Using the result of Example 3.5.3, we see that

$$o[C(\sigma)] = \frac{n!}{r(n-r)!}. \quad \ldots(1)$$

Note. The above expression gives us the formula for the number of conjugates of a r-cycle in S_n.

Example 3.5.5. *Show that the number of conjugate of the n-cycle $(1\,2\,3 \ldots n)$ in S_n is $(n-1)!$.*

Solution. Taking $r = n$ in (1), we see that

$$o[C(\sigma)] = \frac{n!}{n(n-n)!} = \frac{n.(n-1)!}{n} = (n-1)!,$$

where $\sigma = (1\,2\,3 \ldots n) \in S_n$.

Example 3.5.6. *Find two elements in A_5, the alternating group of degree 5, which are conjugate in S_5 but not in A_5.*

Solution. Let $f = (1\,2\,3\,4\,5)$, $g = (1\,2\,3\,5\,4)$.

Then $f, g \in A_5$, since $f = (15)(14)(13)(12)$ is even etc.

It can be verified that if $\theta = (45) \in S_5$, then

$f = \theta g \theta^{-1}$ and so f and g are conjugate in S_5.

Alternatively, f and g being similar are conjugate in S_5. [Theorem 3.5.2]

Now we show that f and g are not conjugate in A_5. Let, if possible, f and g be conjugate in A_5. Then there exists some $\theta \in A_5$ such that $f = \theta g \theta^{-1}$ *i.e.*,

$$(\theta(1), \theta(2), \theta(3), \theta(5), \theta(4)) = (1\ 2\ 3\ 4\ 5).$$

The above relation gives rise to the following cases :

Case I. $\theta(1) = 1, \theta(2) = 2, \theta(3) = 3, \theta(5) = 4, \theta(4) = 5$

$\Rightarrow$ $\theta = (54) \notin A_5$, a contradiction.

Case II. $\theta(1) = 2, \theta(2) = 3, \theta(3) = 4, \theta(5) = 5, \theta(4) = 1$

$\Rightarrow$ $\theta = (1\ 2\ 3\ 4) = (14)\ (13)\ (12) \notin A_5$, a contradiction.

Case III. $\theta(1) = 3, \theta(2) = 4, \theta(3) = 5, \theta(5) = 1, \theta(4) = 2$

$\Rightarrow$ $\theta = (135)\ (24) = (15)\ (13)\ (24) \notin A_5$, a contradiction.

Case IV. $\theta(1) = 4, \theta(2) = 5, \theta(3) = 1, \theta(5) = 2, \theta(4) = 3$

$\Rightarrow$ $\theta = (143)\ (25) = (13)\ (14)\ (15) \notin A_5$, a contradiction.

Case V. $\theta(1) = 5, \theta(2) = 1, \theta(3) = 2, \theta(5) = 3, \theta(4) = 4$

$\Rightarrow$ $\theta = (1532) = (12)\ (13)\ (15) \notin A_5$, a contradiction.

We obtain a contradiction in each of the five cases. Hence f and g are not conjugate in A_5.

Example 3.5.7. *Find two permutations in A_5 which are similar but not conjugate in A_5.*

Solution. $f = (12345) \in A_5$, $g = (12354) \in A_5$ are similar in A_5 (since each is a 5-cycle) but are not conjugate in A_5 (See Example 3.5.6).

Ex. *Show that the permutations (1 2 3 4 5) and (1 3 2 4 5) are conjugate in S_5 but not so in A_5.* [D.U., 1993]

[**Hint.** Proceed like Example 3.5.6.]

Example 3.5.8. *Show that permutations in S_n commuting with $\sigma = (1\ 2\ 3 \ldots n)$ are $\sigma, \sigma^2, \ldots, \sigma^{n-1}, \sigma^n = I$.*

Solution. It is clear that σ commutes with $\sigma, \sigma^2, \sigma^3, \ldots, \sigma^{n-1}, \sigma^n = I$, which are n in number *i.e.*,

$$\sigma \circ \sigma^i = \sigma^i \circ \sigma \quad \text{for} \quad i = 1, 2, \ldots, n.$$

The conjugate class of σ is given by

$$C(\sigma) = \{\theta\ (1\ 2\ 3 \ldots n)\ \theta^{-1} : \theta \in S_n\}$$

$$= \{(\theta(1), \theta(2), \ldots, \theta(n)) : \theta \in S_n\}.$$

Thus $C(\sigma)$ consists of all n-cycles, which are

$$\frac{n!}{n(n-n)!} = (n-1)!\ \text{in number.}$$

[See Example 3.5.5]

We know

$$o[C(\sigma)] = \frac{o(S_n)}{o[N(\sigma)]} \quad \text{or} \quad (n-1)! = \frac{n!}{o[N(\sigma)]}$$

Hence $o[N(\sigma)] = \dfrac{n!}{(n-1)!} = n,$

where $N(\sigma) = \{\theta \in S_n : \theta\sigma = \sigma\theta\}.$

This shows that there are exactly n elements in S_n which commute with σ and as shown above, these are precisely $\sigma, \sigma^2, \ldots, \sigma^n$. Hence σ commutes only with its powers *viz.* $\sigma, \sigma^2, \ldots, \sigma^n$.

Example 3.5.9. *Prove that any element f in S_n which commutes with (12) is of the form*

$$f = (12)^i g, \quad \text{where} \quad i = 0 \text{ or } 1$$

and g is a permutation leaving both 1 and 2 fixed.

Solution. Since any two disjoint cycles commute, therefore, any cycle not containing 1 and 2 (or any permutation leaving 1 and 2 fixed *i.e.*, $1 \to 1$ and $2 \to 2$) commutes with (12). There are $(n-2)!$ such permutations, where both 1 and 2 remain fixed. Obviously, (12) and $(12)^2 = I$ commute with (12). Thus there are $2(n-2)!$ permutations in S_n which commute with (12). ...(A)

Now we want to investigate whether there are other permutations in S_n (apart from those discussed above) which commute with (12). All permutation in S_n commuting with (12) constitute

$$N\{(12)\} = \{\theta \in S_n : \theta(12) = (12)\theta\}.$$

Let $o[N\{(12)\}] = r$. The conjugate class of (12) is

$$C[(12)] = \{\theta(12)\theta^{-1} : \theta \in S_n\}$$

$$= \{(\theta(1)\theta(2)) : \theta \in S_n\}.$$

Thus $C[(12)]$ consists of all 2-cycles in S_n and these are

$$\frac{n!}{2(n-2)!} = \frac{n(n-1)}{2} \text{ in number.}$$

We know

$$o\{C[(12)]\} = \frac{o(S_n)}{o[N\{(12)\}]}$$

or $$\frac{n(n-1)}{2} = \frac{n!}{r} \quad \text{or} \quad r = 2(n-2)!$$

$\therefore$ $$o[N\{(12)\}] = 2(n-2)!.$$

This shows that there are exactly $2(n-2)!$ permutations in S_n which commute with (12) and these are precisely those as described in (A). Hence any permutation f in S_n which commutes with (12) is of the form :

$$f = (12)^i g, \quad \text{where} \quad i = 0, 1$$

and g is a permutation leaving both 1 and 2 fixed.

[Note that $(12)^0 = I = (12)^2$]

Example 3.5.10. *Prove that any element f in S_n which commutes with (123) is of the form*

$$f = (123)^i g, \quad \text{where} \quad i = 0, 1, 2$$

and g is a permutation leaving each of 1, 2, 3 fixed.

Hint. Similar to Example 3.5.9.

Example 3.5.11. *Prove that any element f in S_n which commutes with $(1\ 2 \ldots r)$ is of the form*

$$f = (1\ 2 \ldots r)^i g, \; i = 0, 1, 2, \ldots, r ;$$

g is a permutation leaving all of 1, 2, ..., r fixed.

Solution. Refer to Example 3.5.9.

It is clear that any permutation $g \in S_n$ leaving each of the elements 1, 2, ..., r fixed (*i.e.*, $1 \to 1, 2 \to 2, \ldots, r \to r$) commutes with $(1\ 2 \ldots r)$, since the cycle decomposition of g will be disjoint from $(1\ 2 \ldots r)$. There are $(n-r)!$ permutations in S_n which leave each of the elements 1, 2, ..., r fixed. Apart from these permutations ; $\sigma, \sigma^2, \ldots \sigma^r = I$ also commute with $\sigma = (1\ 2 \ldots r)$. Thus there are $r(n-r)!$ permutations in S_n which commute with $\sigma = (1\ 2 \ldots r)$. ...(A)

Now we proceed to show that these are the *only* permutations in S_n which commute with σ. The conjugate class of σ is

$$C(\sigma) = \{\theta (1\ 2 \ldots r) \theta^{-1} : \theta \in S_n\}$$

$$= \{(\theta(1), \theta(2), \ldots, \theta(r)) : \theta \in S_n\}.$$

Thus $C(\sigma)$ consists of all r-cycles in S_n, which are

$$\frac{n!}{r(n-r)!} \quad \text{in number.}$$

We know

$$o[C(\sigma)] = \frac{o(S_n)}{o[N(\sigma)]} \quad \text{or} \quad \frac{n!}{r(n-r)!} = \frac{n!}{o[N(\sigma)]}$$

$$\therefore \quad o[N(\sigma)] = r(n-r)!,$$

where $$N(\sigma) = \{\theta \in S_n : \theta\sigma = \sigma\theta\}.$$

This shows that there are exactly $r(n-r)!$ permutations in S_n which commute with σ and these are precisely those as described in (A).

Hence any element $f \in S_n$ which commutes with $\sigma = (1\ 2\ \ldots\ r)$ is of the form :

$$f = (1\ 2\ \ldots\ r)^i\ g,\ i = 0, 1, 2, \ldots\ r$$

and g is a permutation leaving all of $1, 2, \ldots, r$ fixed.

[Notice that $\sigma^0 = \sigma^r = I$]

Example 3.5.12. *(a) Find the number of conjugates of (12) (34) in* S_n, $n \geq 4$.

(b) Find the form of all elements commuting with (12) (34) in S_n.

Solution. (*a*) Let $\sigma = (12)\ (34)$. The conjugate class of σ is

$$C(\sigma) = \{\theta\ (12)\ (34)\ \theta^{-1} : \theta \in S_n\}.$$

or
$$C(\sigma) = \{(\theta\ (1)\ \theta\ (2))\ (\theta\ (3)\ \theta\ (4)) : \theta \in S_n\}.$$

We observe that the first element in σ can be chosen in n ways, second element in $(n-1)$, third element in $(n-2)$ and the fourth element in $(n-3)$ ways. Thus σ can be chosen in $n\ (n-1)\ (n-2)\ (n-3)$ ways. But out of these, the following 8 forms of σ are same *viz.*

$$(12)\ (34),\quad (21)\ (34),\quad (12)\ (43),\quad (21)\ (43),$$
$$(34)\ (12),\quad (43)\ (12),\quad (34)\ (21),\quad (43)\ (21).$$

Hence the total number of distinct permutations in S_n $(n \geq 4)$ of the form $(\theta\ (1)\ \theta\ (2))\ (\theta\ (3)\ \theta\ (4))$ is equal to

$$\frac{n\ (n-1)\ (n-2)\ (n-3)}{8}$$

i.e.,
$$o\ [C(\sigma)] = \frac{n\ (n-1)\ (n-2)\ (n-3)}{8}.$$

(*b*) It is clear that any permutation $f \in S_n$ leaving each of the elements 1, 2, 3, 4 fixed (*i.e.*, $1 \to 1, 2 \to 2, 3 \to 3, 4 \to 4$) commutes with $\sigma = (12)\ (34)$ and such permutations are $(n-4)\ !$ in number. Apart from these permutations, the following 8 permutations :

I, (12), (34), $(12)\ (34)$, $(13)\ (24)$, $(14)\ (23)$, (1324), (1423)

commute with σ. Thus there are $8\ (n-4)\ !$ permutations in S_n which commute with σ. We know

$$o\ [C(\sigma)] = \frac{o\ (S_n)}{o\ [N(\sigma)]}$$

or
$$\frac{n\ (n-1)\ (n-2)\ (n-3)}{8} = \frac{n\ !}{o\ [N(\sigma)]}$$

$\therefore$
$$o\ [N(\sigma)] = 8\ (n-4)\ !,\ \text{where}$$
$$N(\sigma) = \{\theta \in S_n : \theta\ \sigma = \sigma\ \theta\}.$$

This shows that there are exactly $8\ (n-4)\ !$ permutations in S_n which commute with $\sigma = (12)\ (34)$ and these are precisely :

f, $(12)\ f$, $(34)\ f$, $(12)\ (34)\ f$, $(13)\ (24)\ f$, $(14)\ (23)\ f$, $(1324)\ f$, $(1423)\ f$;

where f is a permutation in S_n leaving each of 1, 2, 3, 4 fixed.

Example 3.5.13. *Find all the conjugate classes in A_5 and the number of elements in each conjugate class.*

Solution. We know that A_5 consists of all even permutations defined on the set $\{1, 2, 3, 4, 5\}$ and $o(A_5) = \frac{5!}{2} = 60$.

Various conjugate classes in A_5 are :

(*i*) $C(I) = \{\theta I \theta^{-1} : \theta \in A_5\} = \{I\}$.

(*ii*) $C[(123)] = \{\theta (123) \theta^{-1} : \theta \in A_5\}$
$= \{(\theta(1), \theta(2), \theta(3)) : \theta \in A_5\}$.

(*iii*) $C[(12)(34)] = \{\theta (12)(34) \theta^{-1} : \theta \in A_5\}$
$= \{(\theta (12) \theta^{-1})(\theta (34) \theta^{-1}) : \theta \in A_5\}$
$= \{(\theta(1)\theta(2))(\theta(3)\theta(4)) : \theta \in A_5\}$.

(*iv*) $C[(12345)] = \{\theta (12345) \theta^{-1} : \theta \in A_5\}$
$= \{(\theta(1), \theta(2), \theta(3), \theta(4), \theta(5)) : \theta \in A_5\}$.

However, this conjugate class does not consist of all 5-cycles in A_5, since by Example 3.5.6, (12345) and (12354) are not conjugate in A_5 *i.e.*, $(12354) \notin C[(12345)]$. Thus we have another conjugate class determined by (12354) *viz.*

(*v*) $C[(12354)] = \{(\theta(1), \theta(2), \theta(3), \theta(5), \theta(4)) : \theta \in A_5\}$.

Now we shall determine the order of each of the above conjugate classes.

(*i*) Obviously, $o\{C[I]\} = 1$.

(*ii*) By Example 3.5.10, any permutation f in S_5 which commutes with (123) is given by

$$f = (123)^i g, \; i = 0, 1, 2$$

and g is a permutation leaving each of 1, 2, 3 fixed *i.e.*, either $g = (45) \notin A_5$ or $g = I \in A_5$. Hence the only permutations in A_5 commuting with (123) are $(123)^0 = I$, $(123)^1 = (123)$ and $(123)^2 = (132)$.

$\therefore$ $o\{N[(123)]\} = 3$ in A_5.

In A_5, we have $o\{C[(123)]\} = \dfrac{o(A_5)}{o\{N[(123)]\}} = \dfrac{60}{3} = 20$.

(*iii*) As shown in Example 3.5.12, there are only 8 permutations in S_5 *viz.*

I, (12), (34), (12)(34), (13)(24), (14)(23), (1324), (1432)

which commute with (12)(34). Out of these, $(1324) \notin A_5$, $(1432) \notin A_5$ and

I, (12)(34), (13)(24), (14)(23) $\in A_5$

$\therefore$ $o\{N[(12)(34)]\} = 4$ in A_5.

In A_5, we have

$$o\{C[(12)(34)]\} = \frac{o(A_5)}{o\{N[(12)(34)]\}} = \frac{60}{4} = 15.$$

(*iv*) By Example 3.5.8, $\sigma = (12345) \in S_5$ commutes only with $\sigma, \sigma^2, \sigma^3, \sigma^4, \sigma^5 = I$. Since $\sigma, \sigma^2, \sigma^3, \sigma^4$ are all 5-cycles ; they all belong to A_5. Obviously $I \in A_5$

$\therefore$ $o[N(\sigma)] = 5$ in A_5.

In A_5, we have

$$o\{C[(12345)]\} = \frac{o(A_5)}{o\{N(\sigma)\}} = \frac{60}{5} = 12.$$

(*v*) Since $(12354) \notin C[(12345)]$, we have

$o\{C[(12354)]\} = 12$.

Example 3.5.14. *Verify the class equation for* A_5.

Solution. Refer to Example 3.5.13. We have

$$1 + 20 + 15 + 12 + 12 = 60$$

i.e., $o(A_5) = o\{C[I]\} + o\{C[(123)]\} + o\{C[(12)(34)]\} + o\{C[(12345)]\} + o\{C[(12354)]\}$

Hence the class equation is verified for A_5.

Example 3.5.15. *Find the order of the normalizer of each of the following elements in* A_5 :

(i) (123), (ii) (12) (34), (iii) (12345).

Or

Find all permutations in A_5 *which commute with each of the following* :

(i) (123), (ii) (12) (34), (iii) (12345).

Solution. Refer to Example 3.5.13. In A_5, we have shown that

$o\{N[(123)]\} = 3$, $o\{N[(12)(34)]\} = 4$,

$o\{N[(12345)]\} = 5$.

Example 3.5.16. *Find the order of the normalizer of each of the following elements in* S_5 :

(i) (123) (ii) (1234) (iii) (12) (34) (iv) (12345).

Solution. (*i*) $o\{C[(123)]\} = \dfrac{o(S_5)}{o\{N[(123)]\}}$

or $\dfrac{5!}{3(5-3)!} = \dfrac{5!}{o\{N[(123)]\}}$

Hence $o\{N[(123)]\} = 6$.

(*ii*) Similarly, $o\{N[(1234)]\} = 4$.

(*iii*) $o\{N[(12)(34)]\} = 8$ $(5-4)! = 8$. [Take $n = 5$ in Example 3.5.12]

(*iv*) $N(\sigma) = \{\sigma, \sigma^2, \sigma^3, \sigma^4, \sigma^5 = I\}$, where $\sigma = (12345)$.

$\therefore$ $o\{N[(12345)]\} = 5$.

Example 3.5.17. *Prove that in A_5 there is no normal subgroup N other than (I) and A_5.*

Or

Prove that A_5 is a simple group.

Solution. Let N be a normal subgroup of an arbitrary group G.

The conjugate class of any element $a \in N$ is

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

$[\because N \lhd G \Rightarrow x a x^{-1} \in N \; \forall \; x \in G, a \in N]$

...(1)

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

Suppose N is any normal subgroup of A_5, where $N \neq (I)$ and $N \neq A_5$. By (1), N is the union of *some* conjugate classes in A_5. The class equation of A_5 is

$$o(A_5) = \{C[I]\} + o\{C[(123)]\} + o\{C[(12)(34)]\} + o\{C[(12345)]\} + o\{C[(12354)]\}.$$

or $$o(A_5) = 1 + 20 + 15 + 12 + 12. \qquad ...(2)$$

[See Example 3.5.14]

Since $N \lhd A_5$, $I \in N$ and $o\{C(I)\} = 1$, therefore by (1),

$$o(N) = 1 + k, \quad \text{where}$$

$k = 20$ or 15 or 12 or $20 + 15$ or $20 + 12$ or $12 + 12$ or $15 + 12$ or $20 + 15 + 12$ or $20 + 12 + 12$ or $15 + 12 + 12$ but $o(N) \neq 1 + 20 + 15 + 12 + 12$, since $N \neq A_5$.

For the above values of k, we notice that $1 + k$ does not divide $o(A_5) = 60$ *i.e.*, $o(N)$ does not divide $o(A_5)$, which is impossible. Hence if N is any normal subgroup of A_5, then either $N = (I)$ or $N = A_5$ *i.e.*, A_5 has no proper normal subgroups. Consequently, A_5 is a simple group.

4

SYLOW THEOREMS & DIRECT PRODUCT OF GROUPS

We begin this chapter with a *p-group* and prove some of its properties. In section 4.2, we prove the celebrated *Three Sylow Theorems* and discuss their applications in finite groups. Section 4.3 is devoted to the study of *direct product of groups*. We conclude this chapter by giving a complete *survey of groups of order 6 and 8.*

The following results proved in Chapter 3 will be frequently used in this chapter :

1. *If* $o(G) = p^n$, *where p is prime ; then* $o(Z) > 1$. [Theorem 3.4.1.]
2. $a \in Z$ *iff* $N(a) = G$, *Z being the centre of G.*
3. $H < Z \Rightarrow H \lhd G$.
4. *If G is a finite group such that p divides* $o(G)$, *p a prime number, then there exists some* $a \neq e \in G$ *satisfying* $a^p = e$. **(Cauchy's Theorem)**

4.1 *p*-Group

Definition. *A group G is said to be a* **p-group** (*p a prime number*), *if the order of every element of G is some power of p.*

For example, the Quaternion group G of order 8 is a p-group, since by Lagrange's Theorem, $o(a)$ divides $o(G) = 8$ for each $a \neq e \in G$ and so $o(a) = 2$ or 2^2 or 2^3 ($p = 2$ is prime) for each $a \neq e \in G$. Also $o(e) = 1 = 2^0$.

Theorem 4.1.1. *Show that a finite group G is a p-group iff* $o(G) = p^n$, *p being a prime number.*

Proof. Condition is necessary

Suppose G is a p-group. We shall prove that $o(G) = p^n$ for some positive integer n. Let $q \neq p$ be a prime number such that q divides $o(G)$. Then by Cauchy's Theorem, there exists some element $a \in G$ of order q. But $o(a) = p^r$, since G is a p-group.

$\therefore \quad q = p^r \Rightarrow q = p$ (since p and q are both primes).

Thus p is the only prime such that p divides $o(G)$.

Hence $o(G) = p^n$ for some positive integer n.

Condition is sufficient

Let $o(G) = p^n$, where p is prime. By Lagrange's Theorem,

$o(a) \mid o(G) = p^n$, for each $a \in G$.

$\Rightarrow \quad o(a) = p^r \ (0 \le r \le n)$ for each $a \in G$

Hence, by definition, G is a p-group.

Ex. 1. *Which of the following is a p-group :*

(i) $o(G) = 36$, *(ii)* $o(G) = 128$, *(iii)* $o(G) = 21$, *(iv)* $o(G) = 98$. **[Ans. (ii)]**

Theorem 4.1.2. *If G is a p-group and* $o(G) = p^n$, *then G has subgroups each of order* $1, p, p^2, \ldots, p^{n-1}, p^n$.

Proof. See Example 3.4.8. (Chapter 3).

Ex. 2. *Find out the orders of all the subgroups of a group of order 128.*

[Hint. $o(G) = 128 = 2^7$ $(p = 2, \ n = 7)$. Thus G has subgroups each of order $1, 2, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7$ *i.e.*, 1, 2, 4, 8, 16, 32, 64, 128.]

Ex. 3. *Find out the orders of all the subgroups of a group of order 81.*

We recall that if H is a subgroup of a group G, then the *normalizer of* H is defined as

$$N(H) = \{x \in G : x^{-1} Hx = H\}.$$

We know $N(H) < G$ and $H \subseteq N(H)$.

Further, $H \lhd G \quad \Leftrightarrow \quad N(H) = G$.

Theorem 4.1.3. *Prove that every proper subgroup H of a finite p-group G is a proper subgroup of N (H).*

Or

If $o(G) = p^n$, *p a prime number, and* $H \neq G$ *is a subgroup of G, show that there exists an* $x \in G$, $x \notin H$ *such that* $x^{-1} Hx = H$.

Proof. We shall prove the result by induction on n. Let $n = 1$ so that $o(G) = p \Rightarrow G$ is cyclic $\Rightarrow G$ is abelian $\Rightarrow H \lhd G$ (since every subgroup of an abelian group of normal).

$\therefore \quad g^{-1} Hg = H \quad \forall \ g \in G.$

Since $H \underset{\neq}{<} G$, surely there exists an $x \in G$, $x \notin H$ such that

$$x^{-1} Hx = H.$$

Thus the result is true for $n = 1$.

Let the result be true for all groups of orders p^m, where $0 < m < n$. It means : *If T is any group such that*

$$o(T) = p^m, \ 0 < m < n \text{ and } K \neq T$$

is a subgroup of T, then there exists some $x \in T$, $x \notin K$ *such that*

$$x^{-1} Kx = K. \qquad \text{(Induction Hypothesis)}$$

We shall prove the result for G. Since $o(G) = p^n$, therefore

$$o(Z) > 1. \qquad \text{[Theorem 3.4.1 ; Chapter 3]}$$

Further $o(Z) \mid o(G)$, by Lagrange's Theorem. Consequently,

$$o(Z) = p^k, \qquad \text{where} \quad 0 < k \leq n.$$

Now $$o\left(\frac{G}{Z}\right) = \frac{o(G)}{o(Z)} = \frac{p^n}{p^k} = p^{n-k}, \qquad \text{where} \quad n-k < n$$

and $\frac{H}{Z} \neq \frac{G}{Z}$ is a subgroup of $\frac{G}{Z}$.

By induction hypothesis, there exists some element $\bar{x}\,(= xZ) \in G/Z$ and $\bar{x} \notin H/Z$ such that

$$\bar{x}^{-1}\left(\frac{H}{Z}\right)\bar{x} = \frac{H}{Z}$$

or
$$(x^{-1}Z)\left(\frac{H}{Z}\right)(xZ) = \frac{H}{Z}\,; x \in G, x \notin H. \qquad \ldots(1)$$

For any $h \in H$, we have

$$(x^{-1}hx)Z = (x^{-1}Z)(hZ)(xZ). \qquad (\because Z \triangleleft G) \qquad \ldots(2)$$

From (1) and (2), we observe that

$$(x^{-1}hx)Z \in \frac{H}{Z} \qquad \left(\because hZ \in \frac{H}{Z}\right)$$

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

$$\Rightarrow \quad x^{-1}Hx \subseteq H\,; x \in G \text{ but } x \notin H. \qquad \ldots(3)$$

Since $H < G$, $x^{-1}Hx < G$ and $o(x^{-1}Hx) = o(H)$. $\ldots(4)$

From (3) and (4), we obtain

$$x^{-1}Hx = H\,; \; x \in G \text{ but } x \notin H.$$

This completes the induction and the result is proved.

Theorem 4.1.4. *Prove that any subgroup of order p^{n-1} in a group G of order p^n is normal in G, p being a prime number.* [D.U., 1996, 93]

Solution. We shall prove the result by induction on n. If $n = 1$, then $o(G) = p$ (p is prime) $\Rightarrow$ G is cyclic. The only subgroup (of G) of order $p^{n-1} = p^0 = 1$ is (e), which is obviously a normal subgroup of G. Thus the result is true for $n = 1$. Suppose the result is true for all groups of orders p^m, $0 < m < n$; *If T is any group such that $o(T) = p^m$, $0 < m < n$; then any subgroup K of T, $o(K) = p^{m-1}$, must be normal in T.* (Induction Hypothesis)

We now prove the result for G, $o(G) = p^n$. Let $H < G$, where $o(H) = p^{n-1}$. We shall show that H is normal in G.

The *normalizer* of H in G is defined as

$$N(H) = \{x \in G : xHx^{-1} = H\}.$$

Then $N(H) < G$ and $H \triangleleft N(H)$.

If $N(H) \neq H$, then $o(N(H)) > p^{n-1}$.

By Lagrange's Theorem, $o(N(H)) \mid o(G) = p^n$.

Further $o(Z) \mid o(G)$, by Lagrange's Theorem. Consequently,

$$o(Z) = p^k, \quad \text{where} \quad 0 < k \leq n.$$

Now $$o\left(\frac{G}{Z}\right) = \frac{o(G)}{o(Z)} = \frac{p^n}{p^k} = p^{n-k}, \quad \text{where} \quad n-k < n$$

and $\frac{H}{Z} \neq \frac{G}{Z}$ is a subgroup of $\frac{G}{Z}$.

By induction hypothesis, there exists some element $\bar{x}\,(= xZ) \in G/Z$ and $\bar{x} \notin H/Z$ such that

$$\bar{x}^{-1}\left(\frac{H}{Z}\right)\bar{x} = \frac{H}{Z}$$

or
$$(x^{-1}Z)\left(\frac{H}{Z}\right)(xZ) = \frac{H}{Z}\,;\, x \in G, x \notin H. \qquad ...(1)$$

For any $h \in H$, we have

$$(x^{-1}hx)Z = (x^{-1}Z)(hZ)(xZ). \qquad (\because Z \lhd G) \qquad ...(2)$$

From (1) and (2), we observe that

$$(x^{-1}hx)Z \in \frac{H}{Z} \qquad \left(\because hZ \in \frac{H}{Z}\right)$$

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

$$\Rightarrow \quad x^{-1}Hx \subseteq H\,;\, x \in G \text{ but } x \notin H. \qquad ...(3)$$

Since $H < G$, $x^{-1}Hx < G$ and $o(x^{-1}Hx) = o(H)$. ...(4)

From (3) and (4), we obtain

$$x^{-1}Hx = H\,;\; x \in G \text{ but } x \notin H.$$

This completes the induction and the result is proved.

Theorem 4.1.4. *Prove that any subgroup of order p^{n-1} in a group G of order p^n is normal in G, p being a prime number.* [D.U., 1996, 93]

Solution. We shall prove the result by induction on n. If $n = 1$, then $o(G) = p$ (p is prime) $\Rightarrow$ G is cyclic. The only subgroup (of G) of order $p^{n-1} = p^0 = 1$ is (e), which is obviously a normal subgroup of G. Thus the result is true for $n = 1$. Suppose the result is true for all groups of orders $p^m, 0 < m < n$. It means : *If T is any group such that $o(T) = p^m$, $0 < m < n$; then any subgroup K of T, $o(K) = p^{m-1}$, must be normal in T.*

(Induction Hypothesis)

We now prove the result for G, $o(G) = p^n$. Let $H < G$, where $o(H) = p^{n-1}$. We shall show that H is normal in G.

The *normalizer* of H in G is defined as

$$N(H) = \{x \in G : xHx^{-1} = H\}.$$

Then $N(H) < G$ and $H \lhd N(H)$.

If $N(H) \neq H$, then $o(N(H)) > p^{n-1}$.

By Lagrange's Theorem, $o(N(H)) \mid o(G) = p^n$.

Consequently, $o(N(H)) = p^n \Rightarrow o(N(H)) = o(G)$

$\Rightarrow$ $N(H) = G \Rightarrow H \lhd G.$

Thus the result is true in this case.

Now we consider the case : $N(H) = H.$

Since $Z \lhd G$, $aGa^{-1} = G \; \forall \; a \in Z.$

In particular, $aHa^{-1} = H \; \forall \; a \in Z.$ $(\because H < G)$

$\Rightarrow$ $a \in N(H) \quad \forall \quad a \in Z.$

$\Rightarrow$ $Z \subseteq N(H) \Rightarrow Z \subseteq H.$ $(\because N(H) = H)$

Since $o(G) = p^n$, $o(Z) > 1.$ [Theorem 3.4.1]

By Lagrange's Theorem $o(Z) \mid o(G) = p^n$

$\Rightarrow$ $o(Z) = p^k, \; 0 < k \leq n$

$\Rightarrow$ $p \mid o(Z).$

Hence by Cauchy's Theorem, Z has a subgroup, say W, of order p

$\Rightarrow$ $W < Z, \; o(W) = p$

$\Rightarrow$ $W \lhd G.$

Also $W \lhd H$, since $Z \subseteq H.$

$$\therefore \quad o\left(\frac{H}{W}\right) = \frac{o(H)}{o(W)} = \frac{p^{n-1}}{p} = p^{n-2},$$

and $$o\left(\frac{G}{W}\right) = \frac{o(G)}{o(W)} = \frac{p^n}{p} = p^{n-1}, \; n-1 < n.$$

By induction hypothesis, $\frac{H}{W}$ is normal in $\frac{G}{W}$.

Hence H is normal in G. This completes the induction and the result is proved.

Illustrations.

(i) In a group G of order 27, every subgroup of order 9 is normal.

Notice that $o(G) = 3^3$ $(p = 3)$. If $H < G$ such that $o(H) = 9 = 3^2$, then

$$H \lhd G.$$

(ii) In a group of order 16 $(= 2^4)$, *every subgroup of order* $2^3 = 8$ *is normal in G.*

4.2 Sylow Theorems

Sylow Theorems, contributed by the Norwegian mathematician Sylow, are of great significance in the theory of finite groups. the *First Sylow Theorem* provides a partial converse of Lagrange's Theorem. It states :

If p^m divides the order of a finite group G (p being a prime number), then G has a subgroup of order p^m.

We know that a group is *simple* if it has no proper normal subgroups. An important application of Sylow Theorems is to determine whether a given finite group is simple or not.

Theorem 4.2.1. (**First Sylow's Theorem**)
If p is a prime number and p^m divides $o(G)$, then G has a subgroup of order p^m.

Proof. Let $o(G) = n$. We shall prove the result by induction on n. If $n = 1$, then $G = (e)$ has a subgroup of order $p^0 = 1$ viz. (e) itself. Thus the result is true for $n = 1$. Suppose that the result holds for all groups of orders less than n. It means if T is any group of order $o(T) < n$ and if p^k divides $o(T)$, then T has a subgroup of order p^k. (Induction Hypothesis)

We shall prove the result for G.

We are given that $p^m \mid o(G)$.

Case I. *Let p^m divide the order of a proper subgroup H of G i.e., $p^m \mid o(H)$, where $H \leq G$.* By induction hypothesis, H (and hence G) has a subgroup of order p^m.

Case II. *Let $p^m \nmid o(H)$ for all proper subgroups H of G.*

The class equations of G is

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

By our assumption, $p^m \nmid o(N(a))$, whenever $N(a) \neq G$. We have

$$o(G) = \frac{o(G)}{o(N(a))} \cdot o(N(a)), \qquad \ldots(2)$$

Since $p^m \mid o(G)$ and $p^m \nmid o(N(a))$, therefore by (2),

$$p^m \text{ divides } \frac{o(G)}{o(N(a))}, \quad \text{whenever} \quad N(a) \neq G$$

$$\Rightarrow \quad p^m \text{ divides } \sum_{N(a) \neq G} \frac{o(G)}{o(N(a))}$$

$$\Rightarrow \quad \sum_{N(a) \neq G} \frac{o(G)}{o(N(a))} = p^l, \quad \text{where} \quad 0 < l \leq m$$

$$\Rightarrow \quad p \text{ divides } \sum_{N(a) \neq G} \frac{o(G)}{o(N(a))}.$$

Also $p \mid o(G)$. Consequently,

$$p \text{ divides } \left[o(G) - \sum_{N(a) \neq G} \frac{o(G)}{o(N(a))} \right] = o(Z), \text{ by (1).}$$

Since $p \mid o(Z)$, therefore, by Cauchy's theorem for abelian groups, there exists some $a \neq e \in Z$ such that $a^p = e$. Consequently,

$$K = (a) = \{a, a^2, \ldots a^p = e\}$$

is a subgroup of Z and $o(K) = p$.

Theorem 4.2.1. (First Sylow's Theorem)

If p is a prime number and p^m divides $o(G)$, then G has a subgroup of order p^m.

Proof. Let $o(G) = n$. We shall prove the result by induction on n. If $n = 1$, then $G = (e)$ has a subgroup of order $p^0 = 1$ *viz.* (e) itself. Thus the result is true for $n = 1$. Suppose that the result holds for all groups of orders less than n. *It means if T is any group of order $o(T) < n$ and if p^k divides $o(T)$, then T has a subgroup of order p^k.* *(Induction Hypothesis)*

We shall prove the result for G.

We are given that $p^m \mid o(G)$.

Case I. *Let p^m divide the order of a proper subgroup H of G i.e., $p^m \mid o(H)$,* where $H \underset{\neq}{<} G$. By induction hypothesis, H (and hence G) has a subgroup of order p^m.

Case II. *Let $p^m \nmid o(H)$ for all proper subgroups H of G.*

The class equations of G is

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

By our assumption, $p^m \nmid o(N(a))$, whenever $N(a) \neq G$. We have

$$o(G) = \frac{o(G)}{o(N(a))} \cdot o(N(a)). \quad \ldots(2)$$

Since $p^m \mid o(G)$ and $p^m \nmid o(N(a))$, therefore by (2),

$$p^m \text{ divides } \frac{o(G)}{o(N(a))}, \quad \text{whenever} \quad N(a) \neq G$$

$$\Rightarrow \quad p^m \text{ divides } \sum_{N(a) \neq G} \frac{o(G)}{o(N(a))}$$

$$\Rightarrow \quad \sum_{N(a) \neq G} \frac{o(G)}{o(N(a))} = p^l, \quad \text{where} \quad 0 < l \leq m$$

$$\Rightarrow \quad p \text{ divides } \sum_{N(a) \neq G} \frac{o(G)}{o(N(a))}.$$

Also $p \mid o(G)$. Consequently,

$$p \text{ divides } \left[o(G) - \sum_{N(a) \neq G} \frac{o(G)}{o(N(a))} \right] = o(Z), \text{ by (1).}$$

Since $p \mid o(Z)$, therefore, by Cauchy's theorem for abelian groups, there exists some $a \neq e \in Z$ such that $a^p = e$. Consequently,

$$K = \langle a \rangle = \{a, a^2, \ldots, a^p = e\}$$

is a subgroup of Z and $o(K) = p$.

Now $K < Z \Rightarrow K \triangleleft G$ and so

$$o\left(\frac{G}{K}\right) = \frac{o(G)}{o(K)} < o(G).$$

Further p^{m-1} divides $o\left(\frac{G}{K}\right)$, since $o(K) = p$ and $p^m \mid o(G)$.

By induction hypothesis, G/K has a subgroup, say H/K, of order p^{m-1}. [Here $H < G$ and $H \supseteq K$].

Hence H is the required subgroup of G, where

$$o(H) = o\left(\frac{H}{K}\right) o(K) = p^{m-1} \cdot p = p^m.$$

This completes the induction and the theorem is proved.

Corollary. A particular case of the above theorem is the following:

If p is a prime number such that $p^m \mid o(G)$ and $p^{m+1} \nmid o(G)$, then G has a subgroup of order p^m.

Definition. (Sylow *p*-subgroup)

If G is a finite group and p a prime number, then a subgroup of G of order p^m, where

$$p^m \mid o(G) \quad \text{but} \quad p^{m+1} \nmid o(G)$$

is called a **Sylow *p*-subgroup** *or* ***p*-Sylow subgroup** *of G or briefly* ***p*-SSG** *of G.*

Remark 1. The above definition implies that all Sylow p-subgroups of G are of the same order *viz.* p^m. Since any p-subgroup of G is of order a power of p, it follows that :

No p-subgroup of G can contain properly a Sylow p-subgroup of G.

Remark 2. By virtue of the above corollary, it follows that

A finite group G has a p-Sylow subgroup for each prime p which divides $o(G)$.

Remark 3. The conditions $p^m \mid o(G)$ and $p^{m+1} \nmid o(G)$ imply that m is the highest power of p such that $p^m \mid o(G)$. Equivalently, the above conditions enable us to write $o(G)$ as follows :

$$o(G) = p^m \cdot n, \text{ where } p \nmid n.$$

The First Sylow Theorem can be restated as :

If $o(G) = p^m.n$ (p is prime and $p \nmid n$), then G has a Sylow p-subgroup of order p^m.

This form is quite helpful in determining Sylow p-subgroups of a finite group.

Illustrations.

1. If $o(G) = 48 = 16 \times 3 = 2^4 \times 3$, where $2 \nmid 3$; then G has a 2-SSG of order $2^4 = 16$. Also G has a 3-SSG of order 3.

2. If $o(G) = 108 = 3^3 \times 2^2$, then G has a 3-SSG of order $3^3 = 27$ and a 2-SSG of order $2^2 = 4$.

3. If $o(G) = 56 = 2^3 \times 7$, then G has a 2-SSG of order $2^3 = 8$ and a 7-SSG of order 7.

Remark 4. From the above illustrations, we notice that

The First Sylow Theorem tells us as to which *type of p-Sylow subgroups a given finite group possesses.*

Ex. 1. *State First Sylow theorem and give its importance.*

Ex. 2. *What are Sylow subgroups ? State Sylow's First theorem. Find all Sylow subgroups of* S_3. [D.U., 1994]

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

and $o(S_3) = 6 = 2 \times 3$.

Hence by First Sylow Theorem S_3 has 2-SSGs and 3-SSG. Sylow 2-subgroups of S_3 are each of order 2 *viz.* $\{I, (12)\}$, $\{I, (23)\}$, $\{I, (13)\}$. Sylow 3-subgroup of S_3 of order 3 is $\{I, (123), (132)\}$.

Ex. 3. *What types of Sylow p-subgroups the groups of following orders have ?*

(*i*) $o(G) = 15$, (*ii*) $o(G) = 30$, (*iii*) $o(G) = 32$,

(*iv*) $o(G) = 72$, (*v*) $o(G) = 231$, (*vi*) $o(G) = 385$.

[**Hint.** (*iii*) $231 = 3.7.11$ and so G has 3-SSG, 7-SSG and 11-SSG.]

Ex. 4. *Show that no p-subgroup of G can contain properly a Sylow p-subgroup of G.*

[**Hint.** See Remark 1.]

Lemma 4.2.2. (Double Coset Decomposition)

If A and B are two subgroups of a group G, then

$$G = \bigcup_{x \in G} A x B.$$

Proof. For $x, y \in G$, we define a relation $\sim$ as follows :

$$x \sim y \text{ if } y = a x b \text{ for some } a \in A, b \in B. \qquad ...(1)$$

We now show that the relation $\sim$ is an equivalence relation.

Let $x, y, z \in G$.

(*i*) **Reflexive.** $x \sim x$, since $x = e x e$ $(e \in A, e \in B)$.

(*ii*) **Symmetric.** Let $x \sim y \Rightarrow y = a x b$ for $a \in A, b \in B$.

Since A and B are subgroups of G, therefore

$$a \in A \Rightarrow a^{-1} \in A \text{ and } b \in B \Rightarrow b^{-1} \in B.$$

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

(*iii*) **Transitive.** Let $x \sim y$ and $y \sim z$. Then

$$y = a x b \text{ and } z = a_1 y b_1 \text{ for } a, a_1 \in A \text{ and } b, b_1 \in B.$$

$$\therefore \quad z = a_1 (a x b) b_1 = (a_1 a) x (b b_1) \Rightarrow x \sim z,$$

since $a_1 a \in A$ and $b b_1 \in B$. $(\because A < G \text{ and } B < G)$

Hence $\sim$ is an equivalence relation on G. The equivalence class of $x \in G$ is

$$[x] = \{y \in G : x \sim y\}$$

or $$[x] = \{y \in G : y = a\,x\,b \text{ for } a \in A, b \in B\}.$$

$$\therefore \quad [x] = \{a\,x\,b : a \in A, b \in B\} = A\,x\,B.$$

The set $A\,x\,B$ is called a **double coset** *of A and B in G.*

Since G is expressible as the union of disjoint equivalence classes,

$$G = \bigcup_{x \in G} [x] = \bigcup_{x \in G} A\,x\,B.$$

This expression is called the **double coset decomposition** *of G given by A and B.*

Lemma 4.2.3. *If A and B are finite subgroups of a group G, then*

$$o(A\,x\,B) = \frac{o(A)\,o(B)}{o(A \cap x\,B\,x^{-1})},\ x \in G.$$

Proof. Notice that $B < G \Rightarrow x\,B\,x^{-1} < G,\ x \in G.$

Define a mapping $\phi : A\,x\,B \to A\,x\,B\,x^{-1}$ as

$$\phi(a\,x\,b) = ax\,bx^{-1} \quad \text{for} \quad a \in A \quad \text{and} \quad b \in B.$$

Then ϕ is one-to-one, since for $a_1, a_2 \in A$ and $b_1, b_2 \in B$

$$\phi(a_1\,x\,b_1) = \phi(a_2\,x\,b_2) \Rightarrow a_1\,x\,b_1\,x^{-1} = a_2\,x\,b_2\,x^{-1}$$

$$\Rightarrow \quad a_1\,x\,b_1 = a_2\,x\,b_2, \text{ by cancellation law in } G.$$

Also T is onto, since for any $t \in A\,x\,Bx^{-1}$,

$$t = a\,x\,bx^{-1} \quad \text{for some} \quad a \in A,\ b \in B$$

or $$t = \phi(a\,x\,b),\ a\,x\,b \in A\,x\,B.$$

Thus there exists a one-to-one correspondence between $A\,x\,B$ and $Ax\,Bx^{-1}$. Since A and B are finite, it follows that

$$o(A\,x\,B) = o(A\,x\,B\,x^{-1}) = o(A\,K),\ K = x\,B\,x^{-1} < G$$

$$= \frac{o(A)\,o(K)}{o(A \cap K)} = \frac{o(A)\,o(x\,B\,x^{-1})}{o(A \cap x\,B\,x^{-1})}$$

Hence $$o(A\,x\,B) = \frac{o(A)\,o(B)}{o(A \cap x\,B\,x^{-1})}, \text{ since } o(x\,B\,x^{-1}) = o(B).$$

Theorem 4.2.4. (Second Sylow Theorem)

Any two Sylow p-subgroups of a finite group G are conjugate in G.

Proof. Let A and B be two Sylow p-subgroups of a finite group G, where

$$o(A) = o(B) = p^n;\ p^n \mid o(G) \quad \text{and} \quad p^{n+1} \nmid o(G). \qquad \ldots(1)$$

We have to show that A and B are conjugate in G *i.e.*, to show

$$A = g\,B\,g^{-1} \text{ for some } g \in G. \qquad \ldots(2)$$

Let, if possible, (2) be false. Then

$$A \neq x\,B\,x^{-1} \text{ for all } x \in G$$

$\Rightarrow A \cap x B x^{-1}$ is a proper subgroup of A and so by Lagrange's Theorem,

$$o(A \cap x B x^{-1}) = p^m, \quad \text{where} \quad 0 < m < n. \qquad \ldots(3)$$

By double coset decomposition of G, we have

$$G = \bigcup_{x \in G} A x B.$$

Since G is finite, $o(G) = \sum_{x \in G} o(A x B)$. $\qquad \ldots(4)$

By Lemma 4.2.3., we have

$$o(A x B) = \frac{o(A)\, o(B)}{o(A \cap x B x^{-1})} = \frac{p^n \cdot p^n}{p^m}, \text{ by (1) and (3)}$$

or $\quad o(A x B) = p^{n+(n-m)}$, where $n > m \Rightarrow n - m > 0 \Rightarrow n - m \geq 1$.

From the above relation, it follows that

p^{n+1} divides $o(A x B)$ for each $x \in G$

$\Rightarrow$ p^{n+1} divides $\sum_{x \in G} o(A x B)$

$\Rightarrow$ p^{n+1} divides $o(G)$, by (4).

This is a contradiction. Hence $A = g B g^{-1}$ for some $g \in G$.

Theorem 4.2.5. *Show that a Sylow p-subgroup of a finite group G is unique if and only if it is normal.*

Proof. Condition is necessary

Let H be a unique Sylow p-subgroup of G.

Let $o(H) = p^m$, where $p^m \mid o(G), p^{m+1} \nmid o(G)$.

Let $g \in G$ by arbitrary. Then $g H g^{-1}$ is a subgroup of G, where

$$o(g H g^{-1}) = o(H) = p^m$$

$\Rightarrow$ $o(g H g^{-1}) = p^m \ \forall \ g \in G$; $p^m \mid o(G), p^{m+1} \nmid o(G)$

$\Rightarrow$ $g H g^{-1}$ is a Sylow p-subgroup of G for all $g \in G$.

Since H is the only Sylow p-subgroup of G, therefore

$$H = g H g^{-1} \quad \forall \quad g \in G.$$

Hence H is a normal subgroup of G.

Condition is sufficient

Let H be a normal subgroup of G, where H is a Sylow p-subgroup of G. Suppose K is any other Sylow p-subgroup of G. Then, by Second Sylow Theorem, H and K are conjugate in G *i.e.*, $K = g H g^{-1}$ for some $g \in G$

$\Rightarrow$ $K = H$, since $H \lhd G \Rightarrow g H g^{-1} = H$.

Hence H is a unique Sylow p-subgroup of G.

Remark. It will help to remember the following result :

If H is the only p-SSG of G, then H is normal in G.

Ex. 5. *State Second Sylow Theorem and verify it for* S_3.

Solution. $S_3 = \{I, (12), (23), (31), (123), (132)\}$.

We have earlier seen that two Sylow 2-subgroups of S_3 are

$$A = \{I, (12)\}, \quad B = \{I, (23)\}.$$

Let $g = (13) \in S_3$ so that $g^{-1} = (13)$. We have

$$g B g^{-1} = \{(13)\, I\, (13), (13)\, (23)\, (13)\} = \{I, (12)\} = A.$$

Hence $A = g B g^{-1}$ shows that A and B are conjugate in S_3. Further the unique 3-SSG : $H = \{I, (123), (132)\}$ is conjugate to itself *i.e.*, $H = I H I^{-1}$.

Lemma 4.2.6. *Let P be a Sylow p-subgroup of a finite group G. Then the number n_p of Sylow p-subgroups of G is given by*

$$n_p = \frac{o(G)}{o(N(P))} \quad \text{and} \quad n_p \text{ divides } o(G).$$

Proof. By Theorem 3.3.2 (Chapter 3),

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

or
$$o\{x a x^{-1} : x \in G\} = \frac{o(G)}{o(N(a)}.$$

We shall generalize this result as

$$o\{x P x^{-1} : x \in G\} = \frac{o(G)}{o(N(P))}, \qquad \ldots(A)$$

where $N(P) = \{x \in G : x P x^{-1} = P\}$.

Since $N(P)$ is a subgroup of G, G can be decomposed as the union of a finite number of mutually disjoint left cosets of $N(P)$ in G *i.e.*,

$$G = \bigcup_{i=1}^{n} x_i N(P), x_i \in G. \qquad \ldots(1)$$

Let $S = \{x_1 P x_1^{-1}, x_2 P x_2^{-1}, \ldots, x_n P x_n^{-1}\}$ ...(2)

and $T = \{x P x^{-1} : x \in G\}$.

Obviously $S \subseteq T$.

Conversely, let $x P x^{-1} \in T$ be arbitrary, where $x \in G$.

Since $x \in G$, therefore by (1)

$$x \in x_i N(P) \quad \text{for some } i,\ 1 \le i \le n$$

$$\Rightarrow \quad x = x_i y \quad \text{for some } y \in N(P).$$

$$\therefore \quad x P x^{-1} = (x_i y) P (x_i y)^{-1} = x_i (y P y^{-1}) x_i^{-1}$$

or
$$x P x^{-1} = x_i P x_i^{-1}, \text{ since } y \in N(P) \Rightarrow y P y^{-1} = P$$

$\Rightarrow x P x^{-1} \in S$ for all $x \in G \Rightarrow T \subseteq S$. Thus $S = T$.

Now $x_i P x_i^{-1} = x_j P x_j^{-1} \Rightarrow x_j^{-1} x_i P = P x_j^{-1} x_i$

Ex. 5. *State Second Sylow Theorem and verify it for* S_3.

Solution. $S_3 = \{I, (12), (23), (31), (123), (132)\}$.

We have earlier seen that two Sylow 2-subgroups of S_3 are

$$A = \{I, (12)\}, \quad B = \{I, (23)\}.$$

Let $g = (13) \in S_3$ so that $g^{-1} = (13)$. We have

$$g B g^{-1} = \{(13)\, I\, (13), (13)\,(23)\,(13)\} = \{I, (12)\} = A.$$

Hence $A = g B g^{-1}$ shows that A and B are conjugate in S_3. Further the unique 3-SSG : $H = \{I, (123), (132)\}$ is conjugate to itself *i.e.*, $H = I H I^{-1}$.

Lemma 4.2.6. *Let P be a Sylow p-subgroup of a finite group G. Then the number n_p of Sylow p-subgroups of G is given by*

$$n_p = \frac{o(G)}{o(N(P))} \quad \textit{and} \quad n_p \textit{ divides } o(G).$$

Proof. By Theorem 3.3.2 (Chapter 3),

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

or
$$o\{x a x^{-1} : x \in G\} = \frac{o(G)}{o(N(a))}.$$

We shall generalize this result as

$$o\{x P x^{-1} : x \in G\} = \frac{o(G)}{o(N(P))}, \qquad \ldots(A)$$

where $N(P) = \{x \in G : x P x^{-1} = P\}$.

Since $N(P)$ is a subgroup of G, G can be decomposed as the union of a finite number of mutually disjoint left cosets of $N(P)$ in G *i.e.*,

$$G = \bigcup_{i=1}^{n} x_i N(P), x_i \in G. \qquad \ldots(1)$$

Let $S = \{x_1 P x_1^{-1}, x_2 P x_2^{-1}, \ldots, x_n P x_n^{-1}\}$ ...(2)

and $T = \{x P x^{-1} : x \in G\}$.

Obviously $S \subseteq T$.

Conversely, let $x P x^{-1} \in T$ be arbitrary, where $x \in G$.

Since $x \in G$, therefore by (1)

$$x \in x_i N(P) \quad \text{for some } i,\ 1 \le i \le n$$

$$\Rightarrow \quad x = x_i y \quad \text{for some } y \in N(P).$$

$$\therefore \quad x P x^{-1} = (x_i y) P (x_i y)^{-1} = x_i (y P y^{-1}) x_i^{-1}$$

or
$$x P x^{-1} = x_i P x_i^{-1}, \quad \text{since } y \in N(P) \Rightarrow y P y^{-1} = P$$

$\Rightarrow x P x^{-1} \in S$ for all $x \in G \Rightarrow T \subseteq S$. Thus $S = T$.

Now $x_i P x_i^{-1} = x_j P x_j^{-1} \Rightarrow x_j^{-1} x_i P = P x_j^{-1} x_i$

$\Rightarrow \quad x_j^{-1} x_i \in N(P) \Rightarrow x_j N(P) = x_i N(P) \Rightarrow i = j.$

From (1) and (2), it follows that

$o(S) = n = i_G((N(P))$. Since $S = T$, therefore

$$\therefore \quad o(T) = o\{x P x^{-1} : x \in G\} = \frac{o(G)}{o(N(P))}. \qquad \ldots(3)$$

By Second Sylow Theorem, if P is a Sylow p-subgroup of G, then all Sylow p-subgroups of G are conjugate to P. In other words, the number n_p of all distinct Sylow p-subgroups of G is given by

$$n_p = o\{x P x^{-1} : x \in G\}. \qquad \ldots(4)$$

Hence $\quad n_p = \dfrac{o(G)}{o(N(P))}$, by (3) and (4).

Since $n_p = i_G(N(P))$ and $i_G(N(P))$ divides $o(G)$, n_p divides $o(G)$.

Remark 5. Whereas the First Sylow Theorem tells us as to *what types* of Sylow p-subgroups, a finite group G can have. The Third Sylow Theorem tells us as to *how many* Sylow p-subgroups, G can have. This answer is provided in the following

Theorem 4.2.7. (Third Sylow Theorem)

Show that the number n_p of Sylow p-subgroups of a finite group G is given by

$$n_p = 1 + kp, \quad \text{where} \quad k = 0, 1, 2, \ldots$$

and n_p divides $o(G)$.

Proof. Let P be a Sylow p-subgroup of G, $o(P) = p^n$. Then

$$p^n \mid o(G) \quad \text{and} \quad p^{n+1} \nmid o(G). \qquad \ldots(1)$$

Decomposing G into double cosets of $A = P$ and $B = P$, we obtain

$$G = \bigcup_{x \in G} P x P \quad \Rightarrow \quad o(G) = \sum_{x \in G} o(P x P)$$

or
$$o(G) = \sum_{x \in N(P)} o(P x P) + \sum_{x \in G - N(P)} o(P x P), \qquad \ldots(2)$$

where each sum runs over one element from each double coset.

Now $\quad x \in N(P) \Rightarrow x P x^{-1} = P \Rightarrow x P = P x \Rightarrow P x P = P P x$

$$\Rightarrow \quad P x P = P x. \quad (\because P < G \Rightarrow PP = P)$$

$$\therefore \quad \bigcup_{x \in N(P)} P x P = \bigcup_{x \in N(P)} P x = N(P), \text{ since } P < N(P) \qquad \ldots(3)$$

$$\Rightarrow \quad \sum_{x \in N(P)} o(P x P) = o(N(P)).$$

Let $\quad x \in G - N(P) \Rightarrow x \notin N(P) \Rightarrow x P x^{-1} \neq P$

$\Rightarrow \quad P \cap x P x^{-1} < P$ and so by Lagrange's Theorem,

$$o(P \cap x P x^{-1}) \mid o(P) = p^n$$

$\Rightarrow$ $o(P \cap x P x^{-1}) = p^m$, where $0 < m < n$.

By Lemma 4.2.3, we have

$$o(P x P) = \frac{o(P)\, o(P)}{o(P \cap x P x^{-1})} = \frac{p^n \cdot p^n}{p^m} = p^{n+(n-m)}.$$

Since $n - m > 0$, it follows that

p^{n+1} divides $o(P x P)$ $\forall$ $x \in G \sim N(P)$ *i.e.*, $x \notin N(P)$

$\Rightarrow$ p^{n+1} divides $\sum_{x \notin N(P)} o(P x P)$

$\Rightarrow$ $\sum_{x \notin N(P)} o(P x P) = p^{n+1} \cdot u$ for some integer u. ...(4)

Using (3) and (4) in (2), we get

$$o(G) = o(N(P)) + p^{n+1} \cdot u$$

or $$\frac{o(G)}{o(N(P))} = 1 + \frac{p^{n+1} \cdot u}{o(N(P))}.$$ ...(5)

By Lagrange's Theorem, $o(N(P)) \mid o(G)$ and so $\frac{o(G)}{o(N(P))}$ must be an integer. Consequently, by (5)

$\frac{p^{n+1} u}{o(N(P))}$ must be an integer.

By (1), $p^{n+1} \dagger o(G)$ and so $p^{n+1} \dagger o(N(P))$, as $N(P) < G$.

Now $p^{n+1} \dagger o(N(P))$ $\Rightarrow$ $\frac{p^{n+1} u}{o(N(P))}$ must be divisible by p.

$\therefore$ $\frac{p^{n+1} u}{o(N(P))}$ is of the form $\frac{p^{n+1} u}{o(N(P))} = kp$, ...(6)

where k is an integer. From (5) and (6), we obtain

$$\frac{o(G)}{o(N(P))} = 1 + kp,\ k = 0, 1, 2, \ldots$$

By Lemma 4.2.6, the number n_p of Sylow p-subgroups of G is

$$n_p = \frac{o(G)}{o(N(P))} \quad \text{and} \quad n_p \mid o(G).$$

Hence $n_p = 1 + kp,\ k = 0, 1, 2, \ldots$

and $n_p \mid o(G)$.

Rule. *The number (n_p) of p-SSGs of G is given by*

$$n_p = 1 + kp\ ;\ k = 0, 1, 2, \ldots \text{ and } n_p \mid o(G)$$

Remark 6. It must be borne in mind that in the above formula : $k = 0$ is always true, for then $n_p = 1$ and 1 divides $o(G)$. The problem becomes more interesting if we can find some positive integral value of k such that $n_p = 1 + kp$ and n_p divides $o(G)$.

Remark 7. We shall frequently use the following result proved in Theorem 4.2.5 :

If H is exactly one p-SSG of G, then H is a normal subgroup of G.

Ex. 6. *State Third Sylow Theorem and verify it for S_3.*

Solution. $S_3 = \{(I, (12), (23), (13), (123), (132)\}$, $o(S_3) = 6$.

The number (n_2) of Sylow 2-subgroups of S_3 is

$$n_2 = 1 + 2k \ (k = 0, 1, 2, \ldots), \text{ where } n_2 \mid o(S_3) = 6$$

$$\Rightarrow \quad k = 0 \text{ or } 1 \quad \Rightarrow \quad n_2 = 1 \text{ or } 3.$$

Hence $n_2 = 3$ *i.e.*, S_3 has 3 Sylow 2-subgroups of G *viz.*

$$P_1 = \{I, (12)\}, \ P_2 = \{I, (23)\} \quad \text{and} \quad P_3 = \{I, (13)\}.$$

The number (n_3) of Sylow 3-subgroups of S_3 is

$$n_3 = 1 + 3k \ (k = 0, 1, 2, \ldots), \quad \text{where } n_3 \mid o(S_3) = 6$$

$$\Rightarrow \quad k = 0 \text{ only} \quad \Rightarrow \quad n_3 = 1.$$

Hence there exists exactly one Sylow 3-subgroup of S_3 *viz.*

$P_4 = \{I, (123), (132)\}$. Notice that $P_4 \lhd S_3$.

Ex. 7. *State the three Sylow Theorems and verify them for S_3.* [D.U., 1993]

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

Second Sylow Theorem. *Any two Sylow p-subgroups of a finite group G are conjugate in G i.e., if P and Q are two Sylow p-subgroups of G, then $Q = x P x^{-1}$ for some $x \in G$.*

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

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

For the verification of these theorems for S_3, refer to Ex. 2, Ex. 5 and Ex. 6.

EXAMPLES

Example 4.2.1. *Verify the three Sylow Theorems for A_4.*

Solution. We know A_4 is the set of all even permutations defined on the set $\{1, 2, 3, 4\}$. Further,

$$A_4 \lhd S_4 \quad \text{and} \quad o(A_4) = \frac{o(S_4)}{2} = \frac{4!}{2} = 12$$

i.e., $\quad o(A_4) = 2^2 \times 3.$

Since A_4 has subgroups of order 3 and $2^2 = 4$ *i.e.*, A_4 has Sylow 3-subgroups of order 3 and Sylow 2-subgroups of order 4, First Sylow Theorem is verified for A_4.

The number (n_3) of Sylow 3-subgroups of A_4 is given by

$$n_3 = 1 + 3k \ (k = 0, 1, 2, \ldots), \text{ where } n_3 \mid o(A_4) = 12$$

$$\Rightarrow \quad k = 0 \text{ or } 1 \Rightarrow n_3 = 1 \text{ or } 4$$

Hence $n_3 = 4$, where 4 Sylow 3-subgroups of A_4 are

$$P_1 = \{I, (123), (132)\}, \quad P_2 = \{I, (124), (142)\},$$
$$P_3 = \{I, (134), (143)\}, \quad P_4 = \{I, (234), (243)\}.$$

The number (n_2) of Sylow 2-subgroups of A_4 is given by

$$n_2 = 1 + 2k \ (k = 0, 1, 2, \ldots), \quad \text{where} \quad n_2 \mid o(A_4) = 12$$

$\Rightarrow k = 0$ or $1 \Rightarrow n_2 = 1$ or 3. But $n_2 = 1$, since the only Sylow 2-subgroup of A_4 of order 4 is

$$H = \{I, (12)(34), (13)(24), (14)(23)\}.$$

Notice that H is normal in A_4. Hence Third Sylow Theorem is verified for A_4. Now we shall verify Second Sylow Theorem. We observe that P_1 and P_4 are conjugate in A_4 *i.e.*, $P_4 = x P_1 x^{-1}$, where $x = (124) \in A_4$.

Indeed $x P_1 x^{-1} = \{(124) I (142), (124)(123)(142), (124)(132)(142)\}$
$= \{I, (243), (234)\} = P_4$.

Similarly, $P_4 = y P_2 y^{-1}$, where $y = (123) \in A_4$ and so on.

Hence any pair of Sylow 3-subgroups of A_4 is conjugate in A_4.

Finally, H is conjugate to H, since $H = I H I^{-1}$.

Example 4.2.2. *Prove that a group of order 28 has a normal subgroup of order 7.*

Or

Prove that a group of order 28 is not simple.

Solution. We have $o(G) = 28 = 7 \times 2^2$.

By First Sylow Theorem, G has Sylow 7-subgroups (7-SSGs) and Sylow 2-subgroups (2-SSGs). The number (n_7) of 7-SSGs is given by

$$n_7 = 1 + 7k, \ k = 0, 1, 2, \ldots, \text{ and } n_7 \mid o(G) = 28.$$

Obviously, $k = 0 \Rightarrow n_7 = 1$ and n_7 divides $o(G) = 28$.

For $k = 1$, $n_7 = 8$ but 8 does not divide $o(G) = 28$.

For $k = 2$, $n_7 = 15$ but 15 does not divide $o(G) = 28$ and so on.

$\therefore n_7 = 1$ *i.e.*, there exists exactly one 7-SSG say H, where $o(H) = 7$.

Hence H is a normal subgroup of order 7.

[See Remark 7 of Theorem 4.2.7]

Recall that a group G is simple if it has no proper normal subgroup.

Since the group G of order 28 has a proper normal subgroup of order 7, G is **not** simple.

Example 4.2.3. *Prove that if a group G of order 28 has a normal subgroup of order 4, then G is abelian.*

Solution. By Example 4.2.2, G has a normal subgroup H, $o(H) = 7$. Also H is abelian, since a group of prime order is cyclic and so abelian.

As given, let K be a normal subgroup of G, where $o(K) = 4 = 2^2$.

Since a group of order p^2 (p prime) is abelian, K is abelian.

Now $H \lhd G$ and $K \lhd G \Rightarrow HK \lhd G$.

Further $$o(HK) = \frac{o(H)\, o(K)}{o(H \cap K)} = \frac{7 \times 4}{1} = 28 = o(G)$$

[Notice that $o(H \cap K)$ divides $o(H) = 7 \Rightarrow H \cap K = (e)$]

Now $o(G) = o(HK) \Rightarrow G = HK$, since $HK < G$.

Finally, we show that G is abelian.

Since $H \lhd G$, $K \lhd G$ and $H \cap K = (e)$, therefore

$$hk = kh \quad \forall \quad h \in H, k \in K. \qquad \ldots(1)$$

[See Example 1.14.5, chapter 1]

Let $g_1, g_2 \in G$ be arbitrary, where $G = HK$.

Then $g_1 = h_1 k_1$ and $g_2 = h_2 k_2$

where $h_1, h_2 \in H$ and $k_1, k_2 \in K$.

$$\begin{aligned}
\therefore \quad g_1 g_2 &= (h_1 k_1)(h_2 k_2) = h_1 (k_1 h_2) k_2 \\
&= h_1 (h_2 k_1) k_2, \text{ by (1)} \\
&= (h_1 h_2)(k_1 k_2) \\
&= (h_2 h_1)(k_2 k_1) \text{ since } H \text{ and } K \text{ are abelian} \\
&= h_2 (h_1 k_2) k_1 \\
&= h_2 (k_2 h_1) k_1, \text{ by (1)} \\
&= (h_2 k_2)(h_1 k_1) = g_2 g_1
\end{aligned}$$

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

Hence G is abelian.

Example 4.2.4. *Find the possible number of 11-Sylow subgroups, 7-Sylow subgroups, and 5-Sylow subgroups in a group of order $5^2.7.11$.*

Solution. The number (n_{11}) of 11-SSGs of G is

$n_{11} = 1 + 11k$ ($k = 0, 1, 2, \ldots$); where $n_{11} \mid o(G) = 5^2.7.11$.

$\Rightarrow k = 0$ only and so $n_{11} = 1$.

Hence there exists exactly one 11-SSG of G.

The number (n_7) of 7-SSGs of G is

$n_7 = 1 + 7k$ ($k = 0, 1, 2, \ldots$); where $n_7 \mid o(G) = 5^2.7.11$.

$\Rightarrow k = 0$ only and so $n_7 = 1$.

Hence there exists exactly one 7-SSG of G.

The number (n_5) of 5-SSGs of G is

$$n_5 = 1 + 5k, \quad \text{where} \quad n_5 \mid o(G) = 5^2.7.11.$$

Now $k = 0 \Rightarrow n_5 = 1$ and $n_5 \mid o(G)$

and $k = 2 \Rightarrow n_5 = 11$ and $n_5 \mid o(G)$.

Hence G has 1 or 11 Sylow 5-subgroups of G of order $5^2 = 25$.

Example 4.2.5. *Discuss the number and nature of the 3-Sylow subgroups and 5-Sylow subgroups of a group of order 225.*

Solution. $o(G) = 225 = 3^2 . 5^2$.

The number (n_5) of 5-SSGs of G is given by

$$n_5 = 1 + 5k \ (k = 0, 1, 2, \ldots), \quad \text{where} \quad n_5 \mid o(G) = 225$$

$\Rightarrow$ $k = 0$ only $\Rightarrow n_5 = 1$.

Hence there exists exactly one 5-SSG of G and so it must be normal in G.

The number (n_3) of 3-SSGs of G is given by

$$n_3 = 1 + 3k \ (k = 0, 1, 2, \ldots) \ ; \ \text{where} \quad n_3 \mid o(G) = 225$$

For $k = 0, \ n_3 = 1$ and $n_3 \mid o(G) = 225$.

For $k = 8, \ n_5 = 25$ and $n_3 \mid o(G) = 225$.

Hence G has 1 or 25 Sylow 3-subgroups each of order 3^2 and they are abelian, since any group of order p^2 (p prime) is abelian.

Example 4.2.6. *Prove that any group of order 15 is cyclic.*

Solution. Let $o(G) = 15 = 3 \times 5$.

By First Sylow Theorem, G has Sylow 3-subgroups and Sylow 5-subgroups. The number (n_3) of 3-SSGs is given by

$$n_3 = 1 + 3k \ (k = 0, 1, 2, \ldots), \quad \text{where} \quad n_3 \mid o(G) = 15$$

$\Rightarrow$ $k = 0$ only $\Rightarrow n_3 = 1$.

Thus there exists exactly one 3-SSG say A, $o(A) = 3$ and so $A \lhd G$. Furthermore, A is cyclic. Let

$$A = \langle a \rangle, a^3 = e.$$

The number (n_5) of 5-SSGs is given by

$$n_5 = 1 + 5k \ (k = 0, 1, 2, \ldots) \quad \text{and} \quad n_5 \mid o(G) = 15$$

$\Rightarrow$ $k = 0$ only $\Rightarrow n_5 = 1$.

Thus there exists exactly one 5-SSG say B, $o(B) = 5$ and so $B \lhd G$. Also B is cyclic. Let $B = \langle b \rangle, b^5 = e$.

We have $A \cap B = (e)$.

Since $A \lhd G$, $B \lhd G$ and $A \cap B = (e)$, therefore

$$xy = yx \ \forall \ x \in A, y \in B.$$

In particular, $ab = ba$. ...(1)

Further $(o(a), o(b)) = (3, 5) = 1$. ...(2)

By virtue of conditions (1) and (2), we have

$$o(ab) = o(a)\, o(b) = 3 \times 5 = 15.$$

[See Example 1.10.3. of Chapter 1]

Hence $G = \langle ab \rangle$, $(ab)^{15} = e$ *i.e.*, G is cyclic.

The generalized version of the above problem is given below.

Example 4.2.7. *If $o(G) = pq$, p and q are distinct primes and $p < q$, show that if p does not divide $(q-1)$, then G is cyclic.*

Solution. The number (n_p) of p-SSGs of G is given by

$$n_p = 1 + kp \quad \text{where} \quad n_p \mid o(G) \text{ i.e., } 1 + kp \mid pq.$$

We have the following cases :

1. $1 + kp = 1$; **2.** $1 + kp = p$; **3.** $1 + kp = q$; **4.** $1 + kp = pq$.

Since p is prime, $1 + kp$ is never a multiple of p for $k = 0, 1, 2, \ldots$.

It follows that

$$1 + kp \neq p \quad \text{and} \quad 1 + kp \neq pq.$$

If $1 + kp = q$, then $kp = q - 1 \Rightarrow p \mid (q-1)$, a contradiction.

Thus we have $1 + kp = 1$ *i.e.*, $n_p = 1$.

Consequently, G has exactly one p-SSG of G, say A or order p and so $A \triangleleft G$, $o(A) = p$. Since a group of prime order is cyclic, we may take

$$A = \langle a \rangle, \; a^p = e.$$

The number (n_q) of q-SSGs of G is given by

$$n_q = 1 + kq, \quad \text{where} \quad n_q \mid o(G) \text{ i.e., } 1 + kq \mid pq.$$

Again, we have the following cases :

1. $1 + kq = 1$, **2.** $1 + kq = p$, **3.** $1 + kq = q$, **4.** $1 + kq = pq$.

Since q is prime, $1 + kq$ is never a multiple of q and so

$$1 + kq \neq q, \; 1 + kq \neq pq.$$

Now $p = 1 + kq \Rightarrow p > q$ for $k \neq 0$, which is contrary to the given hypothesis.

$\therefore \quad n_q = 1 + kq = 1.$

Consequently, there exists exactly one q-SSG of G, say B of order q and so $B \triangleleft G$, $o(B) = q$. Clearly, B is cyclic.

Let $B = \langle b \rangle$, $b^q = e$.

Since $A \triangleleft G, B \triangleleft G$ and $A \cap B = (e)$, therefore

$$ab = ba. \qquad \ldots(1)$$

Also $(o(a), o(b)) = (p, q) = 1$ $\qquad \ldots(2)$

From (1) and (2), we have

$$o(ab) = o(a)\, o(b) = pq = o(G).$$ [See Example 1.10.3.]

Hence $G = \langle ab \rangle$, $(ab)^{pq} = e$ *i.e.*, G is cyclic.

Remark. *We shall use the result of the above example as a formula in many problems.*

Example 4.2.8. *Show that a group of order 33 is cyclic.*

[Hint. $o(G) = 3 \times 11$ where 3, 11 are distinct primes and 3 does not divide $(11 - 1) = 10$. Now use the result of Example 4.2.7.]

Example 4.2.9. *Prove that a group of order 56 is not simple.*

Solution. $o(G) = 56 = 7 \times 2^3$.

By First Sylow Theorem, G has 7-SSGs and 2-SSGs. The number (n_7) of 7-SSGs is given by

$$n_7 = 1 + 7k \ (k = 0, 1, 2, \ldots) \ ; \text{ where } n_7 \mid o(G) = 56.$$

$$\Rightarrow \qquad k = 0 \text{ or } 1 \ \Rightarrow \ n_7 = 1 \text{ or } 8.$$

The number (n_2) of 2-SSGs is given by

$$n_2 = 1 + 2k \ (k = 0, 1, 2, \ldots) \text{ and } n_2 \mid o(G) = 56.$$

$$\Rightarrow \qquad k = 0 \text{ or } 3 \ \Rightarrow \ n_2 = 1 \text{ or } 7.$$

Thus we have the following cases :

Case I. $n_7 = 1$ and $n_2 = 1$.

Case II. $n_7 = 1$ and $n_2 = 7$.

Case III. $n_7 = 8$ and $n_2 = 1$.

Case IV. $n_7 = 8$ and $n_2 = 7$.

In Case I, we must have normal subgroups of G each of order 7 and $2^3 = 8$. Hence G is not simple. In case II, we have a normal subgroup of order 7 and so G is not simple. In case III, we have a normal subgroup of order 8 and so G is not simple.

Now we discuss case IV.

$n_7 = 8$ implies that there are 8 distinct Sylow 7-subgroups each of order 7. Thus there are $8(7 - 1) = 48$ non-identity elements of order 7. But then the remaining eight elements must form a unique Sylow 2-subgroup of order 8 and so $n_2 \neq 7$. Thus case IV is impossible. In the other three cases, we have already shown that G is not simple.

Example 4.2.10. *Prove that a group of order 30 is not simple.* [D.U., 1996]

Solution. $o(G) = 30 = 2 \times 3 \times 5$.

By First Sylow Theorem, G has 2-SSGs, 3-SSGs and 5-SSGs.

The number (n_3) of 3-SSGs is given by

$$n_3 = 1 + 3k \ (k = 0, 1, 2, 3, \ldots) \text{ and } n_3 \mid o(G) = 30$$

$$\Rightarrow \qquad k = 0 \text{ or } 3 \ \Rightarrow \ n_3 = 1 \text{ or } 10.$$

The number (n_5) of 5-SSGs is given by

$$n_5 = 1 + 5k \ (k = 0, 1, \ldots) \quad \text{and} \quad n_5 \mid o(G) = 30$$

$$\Rightarrow \qquad k = 0 \text{ or } 1 \ \Rightarrow \ n_5 = 1 \text{ or } 6.$$

Thus we have the following cases :

Case I. $n_3 = 1$ and $n_5 = 1$.

Case II. $n_3 = 1$ and $n_5 = 6$.

Case III. $n_3 = 10$ and $n_5 = 1$.

Case IV. $n_3 = 10$ and $n_5 = 6$.

In the first three cases, either a 3-SSG or a 5-SSG must be normal in G. Hence G is not simple in the first three cases.

Consider case IV.

We have 10 distinct Sylow 3-subgroups each of order 3. It means there are $10(3-1) = 20$ non-identity elements of G each of order 3. Similarly, there are 6 distinct Sylow 5-subgroups each of order 5 and these subgroups have $6(5-1) = 24$ non-identity elements of G each of order 5. Hence in Case IV, G must have $20 + 24 = 44$ non-identity elements of G of order 3 or 5 ; which is clearly impossible, as $o(G) = 30$. So case IV is impossible. In the remaining three cases, we have already shown that G is not simple.

Example 4.2.11. *If $o(G) = 30$, show that a 3-Sylow subgroup or a 5-Sylow subgroup of G must be normal in G.*

[**Hint.** Same as Example 4.2.10.]

Example 4.2.12. *If $o(G) = 30$, then prove that every 3-Sylow subgroup and every 5-Sylow subgroup of G must be normal in G.*

Solution. As shown in Example 4.2.10, we have

Case I. $n_3 = 1$ and $n_5 = 1$.

Case II. $n_3 = 1$ and $n_5 = 6$.

Case III. $n_3 = 10$ and $n_5 = 1$.

In the first case, each 3-SSG and each 5-SSG of G must be normal in G.

In Case II, let $H \triangleleft G$, where $o(H) = 3$.

Let K be any 5-SSG (out of a total of six) of G, where $o(K) = 5$.

We shall prove that $K \triangleleft G$.

Since $H \triangleleft G$, $kH = Hk \; \forall \; k \in K \quad (\because K < G)$

$\Rightarrow \quad KH = HK \quad \Rightarrow HK < G$, where

$$o(HK) = \frac{o(H)\, o(K)}{o(H \cap K)} = \frac{3 \times 5}{1} = 15, \text{ as } H \cap K = (e).$$

We know that a group of order 15 is cyclic. Consequently, HK is a cyclic subgroup of G.

Now $\quad i_G(HK) = \dfrac{o(G)}{o(HK)} = \dfrac{30}{15} = 2$

$\Rightarrow \quad HK \triangleleft G$ and HK is a cyclic subgroup of G.

We know that if T is a cyclic subgroup of G and T is normal in G, then every subgroup of T is normal in G. [See Example 1.14.16., Chapter 1]

Hence every subgroup of HK is normal in G. Since $K < HK$, K must be normal in G. Hence every 3-SSG and every 5-SSG of G in Case II must be normal in G. Similarly, Case III can be disposed off.

Example 4.2.13. *If $o(G) = 30$, show that G has a normal subgroup of order 15.*

Solution. By Example 4.2.12, every 3-SSG (of order 3) and every 5-SSG (of order 5) of G must be normal in G. Let $o(A) = 3$, $A \lhd G$ and $o(B) = 5$, $B \lhd G$.

Now $A \lhd G, B \lhd G \Rightarrow AB \lhd G$ and

$$o(AB) = \frac{o(A)\, o(B)}{o(A \cap B} = \frac{3 \times 5}{1} = 15$$

Hence AB is a normal subgroup of G of order 15.

Example 4.2.14. *Discuss the number and nature of Sylow subgroups of a group of order 30.* [D.U., 1993]

Solution. We have $o(G) = 30 = 2 \times 3 \times 5$.

By First Sylow Theorem, G has 2-SSGs, 3-SSGs and 5-SSGs.

As shown in Example 4.2.10 ; we have the following cases :

(*a*) $n_3 = 1$ and $n_5 = 1$. (*b*) $n_3 = 1$ and $n_5 = 6$.

(*c*) $n_3 = 10$ and $n_5 = 1$.

As regards the nature of 3-SSGs and 5-SSGs ; each 3-SSGs of G and each 5-SSG of G is normal in G [See Example 4.2.12].

Now the number (n_2) of 2-SSGs of G is given by

$$n_2 = 1 + 2k \ (k = 0, 1, 2, \ldots) \text{ and } n_2 \mid o(G) = 30$$

$$\Rightarrow \quad k = 0 \text{ or } 1 \text{ or } 2 \text{ or } 7 \Rightarrow n_2 = 1 \text{ or } 3 \text{ or } 5 \text{ or } 15.$$

Hence G may have 1 or 3 or 5 or 15 number of 2-SSGs each of order 2 ; which must be cyclic.

Example 4.2.15. *Let G be a group of order 108. Show that there exists a normal subgroup of order 27 or 9.*

Or

If G is of order 108, show that G has a normal subgroup of order 3^k, where $k \geq 2$. [D.U., 1998, 97]

(In view of Lagrange's Theorem, $k = 2$ or 3 only).

Solution. We have $o(G) = 108 = 2^2 \cdot 3^3$.

The number (n_3) of 3-SSGs of G is given by

$$n_3 = 1 + 3k \ (k = 0, 1, 2, \ldots) \text{ and } n_3 \mid o(G) = 108$$

$$\Rightarrow \quad k = 0 \text{ or } 1 \Rightarrow n_3 = 1 \text{ or } 4.$$

If $n_3 = 1$, then there exists exactly one 3-SSG, say H of G, $o(H) = 3^3$. Hence H is a normal subgroup of G of order 27, which proves the first part. Consider the case when G has 4 Sylow 3-subgroups of G each of order 27. In this case we shall prove that G has a normal subgroup of order 9. Let H and K be any two distinct Sylow 3-subgroups of G each of order 27.

Since $H \cap K \underset{\neq}{<} H$, $o(H \cap K) \mid o(H) = 27$. Thus we have

$o(H \cap K) = 1$ or 3 or 9.

If $o(H \cap K) = 1$ or 3, then

$$o(HK) = \frac{o(H)\, o(K)}{o(H \cap K)} = \frac{27 \times 27}{1 \text{ or } 3} > 108 = o(G), \text{ a contradiction.}$$

$o(H \cap K) \neq 1$ and $o(H \cap K) \neq 3$.

Thus $o(H \cap K) = 9$. We now proceed to show that $H \cap K$ is a normal subgroup of G of order 9.

Since $o(H) = 3^3$ and $o(H \cap K) = 3^2$, it follows that $H \cap K \lhd H$. Similarly, $H \cap K \lhd K$.

[Recall that if $o(G) = p^n$ (p a prime), then every subgroup of G of order p^{n-1} is normal in G (Theorem 4.1.4).]

Since $H \cap K \lhd H$, $h(H \cap K)h^{-1} = H \cap K \; \forall \; h \in H$

$\Rightarrow$ $h \in N(H \cap K) \; \forall \; h \in H$

$\Rightarrow$ $H \subseteq N(H \cap K)$. Similarly, $K \subseteq N(H \cap K)$.

$\therefore$ $HK \subseteq N(H \cap K)$.

$$\Rightarrow o[N(H \cap K)] \geq o(HK) = \frac{o(H)\, o(K)}{o(H \cap K)} = \frac{27 \times 27}{9} = 81$$

$\Rightarrow$ $o[N(H \cap K)] \geq 81$ and $o[N(H \cap K)]$ divides $o(G) = 108$

$\Rightarrow$ $o[N(H \cap K)] = 108 = o(G)$

$\Rightarrow$ $G = N(H \cap K)$, since $N(H \cap K) < G$

$\Rightarrow$ $H \cap K \lhd G$, $o(H \cap K) = 9$.

[Recall that $N(H) = G \Leftrightarrow H \lhd G$.]

Hence G has a normal subgroup of order 27 or 9.

Example 4.2.16. *If $o(G) = 96$, show that G has a normal subgroup of order 32 or 16.*

Hint. Similar to Example 4.2.15.

Example 4.2.17. *If G is a group of order 231, prove that the 11-Sylow subgroup is in the centre of G.*

Solution. We have $o(G) = 231 = 3 \times 7 \times 11$.

The number (n_3) of 3-SSGs of G is given by

$n_3 = 1 + 3k$ ($k = 0, 1, 2, \ldots$), $n_3 \mid o(G) = 231$

$\Rightarrow$ $k = 0$ or 2 $\Rightarrow$ $n_3 = 1$ or 7.

Let H be any 3-SSG of G, $o(H) = 3$.

The number (n_7) of 7-SSGs of G is given by

$n_7 = 1 + 7k$ ($k = 0, 1, 2, \ldots$), $n_7 \mid o(G) = 231$

$\Rightarrow$ $k = 0 \Rightarrow n_7 = 1$

i.e., there exists exactly one 7-SSG, say K, of order 7.

$\therefore$ $K \triangleleft G$, $o(K) = 7$. Also K is cyclic, since a group of prime order is cyclic.

Similarly, we can show that there exists exactly one 11-SSG, say L of order 11.

i.e., $L \triangleleft G$, $o(L) = 11$ and L is cyclic.

Now $K \triangleleft G$ and $L \triangleleft G \Rightarrow KL \triangleleft G$ and

$$o(KL) = \frac{o(K)\, o(L)}{o(K \cap L)} = \frac{7 \times 11}{1} = 77.$$

Since $KL \triangleleft G$, $x(KL) = (KL)\, x \ \forall\ x \in G$.

In particular, $x(KL) = (KL)\, x \ \forall\ x \in H$ *i.e.*, $H(KL) = (KL)\, H$

$\Rightarrow H(KL)$ is a subgroup of G, where

$$o[H(KL)] = \frac{o(H)\, o(KL)}{o(H \cap KL)} = \frac{3 \times 77}{1} = 231 = o(G).$$

$\therefore$ $$G = H(KL) = HKL.$$

We have to show that $L \subset Z(G)$.

Since $L \triangleleft G$, $xL = Lx \quad \forall \quad x \in G$.

In particular, $xL = Lx \quad \forall \quad x \in H$ and so $HL = LH$.

Since $K \triangleleft G$, $L \triangleleft G$ and $K \cap L = (e)$, therefore

$$kl = lk \quad \forall \quad k \in K, l \in L. \qquad \ldots(1)$$

Since $LH = HL$, LH is a subgroup of G and

$$o(LH) = \frac{o(L)\, o(H)}{o(L \cap H)} = \frac{11 \times 3}{1} = 3 \times 11,$$

where 3 and 11 are distinct primes and $3 \dagger (11 - 1) = 10$. It follows that LH is cyclic (Example 4.2.7) and so LH is abelian. Let $a \in L$ be arbitrary. In order to show that $a \in Z(G)$, we shall prove that

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

Let $x \in G$ be arbitrary. Since $G = HKL$, we have

$x = hkl$ for some $h \in H$, $k \in K$, $l \in L$.

Consider $ax = a(hkl) = (ah)\, kl$; $a \in L$, $h \in H$

Now $a \in L$ and $h \in H \Rightarrow a, h \in LH \Rightarrow ah = ha$, since LH is abelian.

$\therefore$ $ax = (ha)\, kl = h(ak)\, l$; $a \in L, k \in K$

$= h(ka)\, l$, by (1)

$= hk(al)$; $a \in L, l \in L$

$= hk(la)$, as L being cyclic is abelian

$= (hkl)\, a = xa$.

Thus $ax = xa \ \forall\ x \in G \quad \Rightarrow \quad a \in Z(G) \quad \forall \quad a \in L$.

Hence $L \subseteq Z(G)$, L being the 11-SSG of G.

Example 4.2.18. *If G is a non-abelian group of order 231, show that $Z(G)$ is Sylow 11-subgroup of G.*

Solution. Refer to Example 4.2.17. The 11-SSG of G is L, where $o(L) = 11$ and $L \triangleleft G$. We have to show that $L = Z(G)$.
Let, if possible, $L \subset Z$. Then $o(L) < o(Z)$ *i.e.*, $o(Z) > o(L) = 11$.

By Lagrange's theorem,

$$o(Z) \mid o(G) = 231 \text{ and } o(Z) > 11$$

$$\Rightarrow \quad o(Z) = 231 = o(G) \Rightarrow Z = G$$

$\Rightarrow G$ is abelian, a contradiction.

Hence $L = Z(G)$.

Example 4.2.19. *If G is a group of order 385, show that its 11-Sylow subgroup is normal and its 7-Sylow subgroup is in the centre of G.*

Solution. $o(G) = 231 = 5 \times 7 \times 11$.

The number (n_5) of 5-SSGs of G is given by

$$n_5 = 1 + 5k \ (k = 0, 1, 2, \ldots) \quad \text{and} \quad n_5 \mid o(G) = 231$$

$$\Rightarrow \quad k = 0 \text{ or } 2 \quad \Rightarrow \quad n_5 = 1 \text{ or } 7.$$

Let H be any 5-SSGs of G, $o(H) = 5$.

The number (n_7) of 7-SSGs of G is given by

$$n_7 = 1 + 7k \quad \text{and} \quad n_7 \mid o(G) = 385$$

$$\Rightarrow \quad k = 0 \text{ only} \quad \Rightarrow \quad n_7 = 1.$$

Thus there exists exactly one 7-SSG, say K, of G.

$$\therefore \quad K \triangleleft G, \ o(K) = 7.$$

The number (n_{11}) of 11-SSGs of G is given by

$$n_{11} = 1 + 11k \quad \text{and} \quad n_{11} \mid o(G) = 385$$

$$\Rightarrow \quad k = 0 \text{ only} \quad \Rightarrow \quad n_{11} = 1.$$

Thus there exists exactly one 11-SSG, say L, of G.

$$\therefore \quad L \triangleleft G, \ o(L) = 11.$$

Now $K \triangleleft G$ and $L \triangleleft G \Rightarrow KL \triangleleft G$ and $K \cap L = (e)$.

$$\therefore \quad o(KL) = \frac{o(K)\, o(L)}{o(K \cap L)} = \frac{7 \times 11}{1} = 77.$$

Again, $KL \triangleleft G \Rightarrow x(KL) = (KL)x \ \forall \ x \in G$

In particular, $x(KL) = (KL)x \ \forall \ x \in H$, as $H < G$

$$\Rightarrow \quad H(KL) = (KL)H$$

$\Rightarrow H(KL)$ is a subgroup and

$$o[H(KL)] = \frac{o(H)\, o(KL)}{o(H \cap KL)} = \frac{5 \times 77}{1} = 385 = o(G).$$

It follows that $G = H(KL) = HKL$.

Since $K \triangleleft G$ and $L \triangleleft G$ and $K \cap L = (e)$, therefore

$$kl = lk \quad \forall \quad l \in L, k \in K. \qquad \ldots(1)$$

Now $K \triangleleft G \Rightarrow kg = gk \ \forall \ g \in G$. In particular,

$$kh = hk \ \forall\ h \in H \Rightarrow KH = HK \ \Rightarrow\ KH < G, \text{ where}$$

$$o(KH) = \frac{o(K)\, o(H)}{o(K \cap H)} = \frac{7 \times 5}{1} = 5 \times 7.$$

Here 5 and 7 are distinct primes and $5 \dagger (7 - 1) = 6$.

Consequently, KH is cyclic (Example 4.2.8) and so abelian. We have to prove that $K \subseteq Z(G)$, K being 7-SSG of G.

Let $a \in K$. Then $a \in Z(G)$, if $ax = xa\ \forall\ x \in G$.

Let $x \in G$ be arbitrary. Since $G = HKL$,

$$x = hkl \quad \text{for some} \quad h \in H, k \in K, l \in L.$$

We have $ax = a(hkl) = (ah)\, kl$,

where $a \in K$ and $h \in H \ \Rightarrow\ a \in KH$ and $h \in KH$

$\Rightarrow$ $ah = ha$, since KH is abelian.

$\therefore$ $ax = (ha)\, kl = h(ak)\, l$; $a \in K, k \in K$

$= h(ka)\, l$, since K being cyclic is abelian

$= hk(al)$; $a \in K$ and $l \in L$

$= hk(la)$, by (1)

$= (hkl)\, a = xa$.

Thus $ax = xa\ \forall\ x \in G \ \Rightarrow\ a \in Z(G)\ \forall\ a \in K$.

Hence $K \subseteq Z(G)$.

Example 4.2.20. *Prove that any group of order $2p$ must have a normal subgroup of order p, where p is prime.*

Solution. We have $o(G) = 2p$, p is prime.

The number n_p of p-SSGs of G is given by

$$n_p = 1 + kp, \quad \text{where} \quad 1 + kp \mid o(G) = 2p.$$

Thus we have the following cases :

1. $1 + kp = 1$, **2.** $1 + kp = 2$, **3.** $1 + kp = p$, **4.** $1 + kp = 2p$.

Since p is prime, $p \dagger (1 + kp)$ and so $1 + kp$ is never a multiple of p. Consequently,

$$1 + kp \neq p \quad \text{and} \quad 1 + kp \neq 2p.$$

Further, p is prime $\Rightarrow 1 + kp \neq 2$ for $k = 0, 1, 2, \ldots$

Thus $1 + kp = 1$ *i.e.*, $n_p = 1$ and so there exists exactly one p-SSG of G, say H, $o(H) = p$. Hence H is a normal subgroup of G of order p.

Example 4.2.21. *If $o(G) = p^2 q$ (p and q are primes), show that either a p-Sylow subgroup or a q-Sylow subgroup of G must be normal in G.*

Or

If $o(G) = p^2 q$ (p and q are primes), prove that G has a non-trivial normal subgroup.

Or

Show that a group of order $p^2 q$ (p and q are primes) is not simple.

Solution. Since p and q are primes, let us take $p < q$.

The number (n_q) of q-SSGs of G is given by

$$n_q = 1 + kq, \quad \text{where} \quad n_q \mid o(G) \text{ i.e., } 1 + kq \mid p^2 q.$$

We have the following cases :

1. $1 + kq = 1$, 2. $1 + kq = q$, 3. $1 + kq = p$,
4. $1 + kq = p^2$, 5. $1 + kq = pq$, 6. $1 + kq = p^2 q$.

Since q is prime, $q \nmid (1 + kq)$ and so $1 + kq$ is never a multiple of q.

It follows that

$$1 + kq \neq q,\ 1 + kq \neq pq \quad \text{and} \quad 1 + kq \neq p^2 q.$$

Since $p < q$ and $1 + kq > q$ for $k \neq 0$, $1 + kq \neq p$.

Thus we have $n_q = 1$ or p^2. ..(1)

The number (n_p) of p-SSGs of G is given by

$$n_p = 1 + kp, \quad \text{where} \quad 1 + kp \mid p^2 q.$$

We have the following cases :

1. $1 + kp = 1$, 2. $1 + kp = q$, 3. $1 + kp = p$,
4. $1 + kp = p^2$, 5. $1 + kp = pq$, 6. $1 + kp = p^2 q$.

Since p is prime, $1 + kp$ is never a multiple of p and so

$$1 + kp \neq p,\ 1 + kp \neq p^2,\ 1 + kp \neq pq,\ 1 + kp \neq p^2 q.$$

Thus we have $n_p = 1$ or q. ...(2)

From (1) and (2), the following possibilities arise :

Case I. $n_p = 1$ and $n_q = 1$.

Case II. $n_p = 1$ and $n_q = p^2$.

Case III. $n_p = q$ and $n_q = 1$.

Case IV. $n_p = q$ and $n_q = p^2$.

In the first three cases, we observe that either a p-SSG or a q-SSG must be normal in G. We now discuss case IV.

$n_q = p^2$ implies that there are p^2 number of q-SSGs, each of order q and so we have $p^2 (q - 1) = p^2 q - p^2$ non-identity elements of G, each of order q. Including identity of G, the total number of q-SSGs of G need $p^2 q - p^2 + 1$ elements of G.

Again $n_p = q$ implies that there are q number (least value of q being 2) of p-SSGs each of order p^2. Thus these p-SSGs of G must have at least p^2 elements of G each of order p or p^2.

Consequently, the two types of Sylow subgroups must have at least

$$p^2 q - p^2 + 1 + p^2 = p^2 q + 1 > p^2 q$$

elements of G. This is clearly impossible.

Hence case IV is impossible and in the remaining three cases, we have shown that either a p-SSG or a q-SSG of G must be normal in G.

Example 4.2.22. *If $o(G) = pqr$, $p < q < r$ being primes, then show that some Sylow subgroup of G is normal.*

Or

If $o(G) = pqr$, $p < q < r$ being primes, then show that G is not simple.

Solution. By First Sylow Theorem, G has p-SSGs, q-SSGs and r-SSGs.

Suppose that G has no Sylow subgroup which is normal in G.

$\therefore$ $n_p \neq 1$, $n_q \neq 1$ and $n_r \neq 1$; since for example,

$n_p = 1 \Rightarrow$ there exists exactly one p-SSG of G and so it must be normal in G, a contradiction. We have

$n_p = 1 + kp$, where $(1 + kp) \mid o(G) = pqr$.

We have the following cases :

1. $1 + kp = 1$, **2.** $1 + kp = p$, **3.** $1 + kp = q$, **4.** $1 + kp = r$,

5. $1 + kp = pq$, **6.** $1 + kp = pr$, **7.** $1 + kp = qr$, **8.** $1 + kp = pqr$.

Since p is prime, $p \nmid (1 + kp)$ and so $1 + kp$ is never a multiple of p. Consequently,

$$1 + kp \neq p,\ 1 + kp \neq pq,\ 1 + kp \neq pr,\ 1 + kp \neq pqr.$$

By our assumption, $1 + kp \neq 1$.

Hence $n_p = q$ or r or qr, where $q < r < qr$. ...(1)

Similarly, $n_q = r$ or p (?) or pr.

But $n_q \neq p$, since $n_q = p \Rightarrow 1 + kq = p \Rightarrow p > q$, a contradiction.

$\therefore$ $n_q = r$ or pr, where $r < pr$. ...(2)

Arguing as above, $n_r = p$ (?) or q (?) or pq.

But $n_r \neq p$, since $n_r = p \Rightarrow 1 + kr = p \Rightarrow p > r$, a contradiction

and $n_r \neq q$, since $n_r = q \Rightarrow 1 + kr = q \Rightarrow q > r$, a contradiction

$\therefore$ $n_r = pq$. ...(3)

From (1), we observe that there are at least q number of p-SSGs each of order p (given by $n_p = q$). Consequently, p-SSGs of G require at least $q(p - 1)$ elements of order p.

From (2), q-SSGs of G require at least $r(q - 1)$ elements of order q (given by $n_q = r$).

From (3), r-SSGs of G require $pq(r - 1)$ elements of order r. Now

$$o(G) = pqr \geq q(p - 1) + r(q - 1) + pq(r - 1) + 1. \quad ...(4)$$

[1 on the R.H.S. of (4) is for the identity element of G].

From (4), we have

$$pqr \geq pq - q + rq - r + pqr - pq + 1$$

$$\Rightarrow \quad 0 \geq rq - q - r + 1 = (q - 1)(r - 1)$$

$\Rightarrow$ $(q - 1)(r - 1) \leq 0$, a contradiction ; since the least value of q, r is 2.

Example 4.2.22. *If $o(G) = pqr$, $p < q < r$ being primes, then show that some Sylow subgroup of G is normal.*

Or

If $o(G) = pqr$, $p < q < r$ being primes, then show that G is not simple.

Solution. By First Sylow Theorem, G has p-SSGs, q-SSGs and r-SSGs.

Suppose that G has no Sylow subgroup which is normal in G.

$\therefore$ $n_p \neq 1$, $n_q \neq 1$ and $n_r \neq 1$; since for example,

$n_p = 1 \Rightarrow$ there exists exactly one p-SSG of G and so it must be normal in G, a contradiction. We have

$n_p = 1 + kp$, where $(1 + kp) \mid o(G) = pqr$.

We have the following cases :

1. $1 + kp = 1$, **2.** $1 + kp = p$, **3.** $1 + kp = q$, **4.** $1 + kp = r$,
5. $1 + kp = pq$, **6.** $1 + kp = pr$, **7.** $1 + kp = qr$, **8.** $1 + kp = pqr$.

Since p is prime, $p \nmid (1 + kp)$ and so $1 + kp$ is never a multiple of p. Consequently,

$$1 + kp \neq p,\ 1 + kp \neq pq,\ 1 + kp \neq pr,\ 1 + kp \neq pqr.$$

By our assumption, $1 + kp \neq 1$.

Hence $n_p = q$ or r or qr, where $q < r < qr$. ...(1)

Similarly, $n_q = r$ or p (?) or pr.

But $n_q \neq p$, since $n_q = p \Rightarrow 1 + kq = p \Rightarrow p > q$, a contradiction.

$\therefore$ $n_q = r$ or pr, where $r < pr$. ...(2)

Arguing as above, $n_r = p$ (?) or q (?) or pq.

But $n_r \neq p$, since $n_r = p \Rightarrow 1 + kr = p \Rightarrow p > r$, a contradiction

and $n_r \neq q$, since $n_r = q \Rightarrow 1 + kr = q \Rightarrow q > r$, a contradiction

$\therefore$ $n_r = pq$. ...(3)

From (1), we observe that there are at least q number of p-SSGs each of order p (given by $n_p = q$). Consequently, p-SSGs of G require at least $q(p - 1)$ elements of order p.

From (2), q-SSGs of G require at least $r(q - 1)$ elements of order q (given by $n_q = r$).

From (3), r-SSGs of G require $pq(r - 1)$ elements of order r. Now

$$o(G) = pqr \geq q(p - 1) + r(q - 1) + pq(r - 1) + 1. \quad ...(4)$$

[1 on the R.H.S. of (4) is for the identity element of G].

From (4), we have

$$pqr \geq pq - q + rq - r + pqr - pq + 1$$

$$\Rightarrow \quad 0 \geq rq - q - r + 1 = (q - 1)(r - 1)$$

$\Rightarrow$ $(q - 1)(r - 1) \leq 0$, a contradiction ; since the least value of q, r is 2.

Hence our supposition is wrong and so some Sylow subgroup of G must be normal in G. In other words, G is not simple.

Example 4.2.23. *If P is a Sylow p-subgroup of a finite group G, show that P is a normal subgroup of $N(P)$ and P is the only Sylow p-subgroup of $N(P)$.* [D.U., 1995]

Solution. By definition, $N(P) = \{x \in G : xPx^{-1} = P\}$.

Then $P \subseteq N(P)$ and $N(P)$ is a subgroup of G. Also $P \lhd N(P)$. Obviously, P is a Sylow p-subgroup of $N(P)$. Let Q be any other Sylow p-subgroup of $N(P)$. By Second Sylow Theorem, Q and P must be conjugate in $N(P)$ *i.e.*,

$$Q = xPx^{-1} \quad \text{for some} \quad x \in N(P).$$

Now $x \in N(P) \Rightarrow xPx^{-1} = P \Rightarrow Q = P$.

Hence P is the only Sylow p-subgroup of $N(P)$.

Example 4.2.24. *Let P be a Sylow p-subgroup of a finite group G and H, any subgroup of G containing $N(P)$. Show that $N(H) = H$.*

Solution. We are given that $N(P) \subseteq H$. We know $P \subseteq N(P)$.

$\therefore \quad P \subseteq N(P) \subseteq H$.

Since $H \subseteq N(H)$, it suffices to show that $N(H) \subseteq H$.

Let $x \in N(H)$ be arbitrary. Then $xHx^{-1} = H$.

Now $P \subseteq H \Rightarrow xPx^{-1} \subseteq xHx^{-1} = H \Rightarrow xPx^{-1} \subseteq H$.

Thus P and xPx^{-1} are Sylow p-subgroups in H. By Second Sylow Theorem, we have

$$P = y(xPx^{-1})y^{-1} \quad \text{for some } y \in H$$

$$\Rightarrow \quad P = (yx)P(yx)^{-1}$$

$$\Rightarrow \quad yx \in N(P)$$

$$\Rightarrow \quad yx \in H, \text{ since } N(P) \subseteq H.$$

Now $y \in H$ and $yx \in H \Rightarrow x \in H$, for all $x \in N(H)$

$\Rightarrow \quad N(H) \subseteq H$. Hence $N(H) = H$.

Example 4.2.25. *If P is a p-Sylow subgroup of G, prove that $N(N(P)) = N(P)$.*

Solution. Let $H = N(P) = \{x \in G : xPx^{-1} = P\}$.

Then H is a subgroup G containing $N(P)$.

By Example 4.2.24, $N(H) = H$.

Hence $N(N(P)) = N(P)$.

Example 4.2.26. *If H is a normal subgroup of a finite group G and P is a Sylow p-subgroup of H, show that*

$$G = N_G(P)\,H, \quad \text{where} \quad N_G(P) = \{x \in G : xPx^{-1} = P\}.$$

Solution. We have

$$P < H \Rightarrow x^{-1}Px < x^{-1}Hx \;\forall\, x \in G$$

$$\Rightarrow \quad x^{-1}Px < H \quad \forall \quad x \in G \quad [\because H \lhd G \Rightarrow x^{-1}Hx = H \;\forall\, x \in G]$$

Since $o(x^{-1} P x) = o(P)$, $x^{-1} P x$ is a Sylow p-subgroup of H, for each $x \in G$. Since P and $x^{-1} P x$ are Sylow p-subgroups in H, by Second Sylow Theorem, we have

$$x^{-1} P x = h^{-1} P h \quad \text{for some } h \in H$$

$$\Rightarrow \quad P = x h^{-1} P h x^{-1} = (x h^{-1}) P (x h^{-1})^{-1},\ x h^{-1} \in G$$

$$\Rightarrow \quad x h^{-1} \in N_G(P)\ \forall\ x \in G$$

$$\Rightarrow \quad x \in N_G(P) H\ \forall\ x \in G$$

Hence $G = N_G(P) H$.

Example 4.2.27. *Let H be a subgroup of a finite group G. Let A be a Sylow p-subgroup of H contained in some Sylow p-subgroup B of G. Show that*

$$A = B \cap H.$$

Solution. Let $o(B) = p^n$, where $p^n \mid o(G)$ and $p^{n+1} \nmid o(G)$.

We have $A \subseteq B$ and $A \subseteq H$. Therefore,

$$A \subseteq B \cap H \subseteq H, \text{ where}$$

$$o(B \cap H) \mid o(B) = p^n \quad \Rightarrow \quad o(B \cap H) = p^k, \text{ where } 0 < k \leq n.$$

Thus $B \cap H$ is a p-subgroup of H containing a Sylow p-subgroup A of H. Since no p-subgroup of a group can contain properly a Sylow p-subgroup of the group, we have

$$A = B \cap H.$$

Example 4.2.28. *Show that if H is a normal subgroup of a finite group G and p, a prime dividing $o(G)$ such that $[G : H]$ is co-prime to p, then H contains all Sylow p-subgroups of G.*

Solution. Let P be any Sylow p-subgroup of G, where

$$o(P) = p^n;\ p^n \mid o(G) \quad \text{and} \quad p^{n+1} \nmid o(G).$$

Let $[G : H] = i_G(H) = m$. Since $(m, p) = 1$, $p \nmid m$.

Now $p \nmid m \Rightarrow p^n \nmid m$.

We have $o(G) = o\left(\frac{G}{H}\right) o(H) = i_G(H) \,.\, o(H) = m \,.\, o(H)$

Since $p^n \mid o(G)$ and $p^n \nmid m, p^n \mid o(H)$.

Also $p^{n+1} \nmid o(G) \Rightarrow p^{n+1} \nmid o(H)$.

Hence, by First Sylow Theorem, H (and hence G) has a Sylow p-subgroup, say K, $o(K) = p^n$.

By Second Sylow Theorem,

$$P = x K x^{-1} \quad \text{for some } x \in G.$$

Since $K \subseteq H, x K x^{-1} \subseteq x H x^{-1} = H.$ $(\because H \lhd G)$

Hence $P = x K x^{-1} \subseteq H$ *i.e.*, $P \subseteq H$.

Example 4.2.29. *Show that* $Aut\ S_4 = S_4$.

Solution. We know that

$$Z(S_n) = \{e\} \quad \text{for} \quad n \geq 3.$$

Here e denotes the identity mapping of S_n.

$\therefore \quad Z(S_4) = \{e\}$ or $Z(G) = \{e\}$, where $G = S_4$.

We also know that

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

where $I(G)$ denotes the group of inner automorphism of G and further $I(G)$ is a subgroup of $Aut\ G$. Thus we have

$$\frac{G}{\{e\}} = I(G) \Rightarrow G = I(G), \text{ since } G = \frac{G}{\{e\}}.$$

$$\therefore \quad G = I(G) \Rightarrow o\{I(G)\} = o(G) = o(S_4) = 4! = 24. \quad \ldots(1)$$

We have $o(G) = 2^3 \times 3$.

The number (n_3) of 3-SSGs of G is $n_3 = 1 + 3k$, where $n_3 \mid o(G) = 24$

$\Rightarrow \quad k = 0$ or $1 \Rightarrow n_3 = 1$ or 4.

Hence $n_3 = 4$ *i.e.*, G has 4 Sylow 3-subgroups viz.

$P_1 = \{I, (123), (132)\}$, $P_2 = \{I, (124), (142)\}$,

$P_3 = \{I, (134), (143)\}$, $P_4 = \{I, (234), (243)\}$.

Let $S = \{P_1, P_2, P_3, P_4\}$, so that $o\{A(S)\} = 4! = 24$. $\ldots(2)$

Let $T \in Aut\ G$ be arbitrary *i.e.*, $T : G \to G$ is onto, one-to-one and homomorphism. Then

$T_S(P_i) = \{T(x) : x \in P_i\}$ is a subgroup of G for each i.

T_S is called the *restriction mapping* of T to S.

Further $o\{T_S(P_i)\} = o(P_i) = 3$. Consequently, $T_S(P_i)$ is a 3-SSG of G for each $i \Rightarrow T_S(P_i) \in S$ for each i

$\Rightarrow \quad T_S : S \to S$ is one-to-one and onto, since T is one-to-one and onto

$\Rightarrow \quad T_S \in A(S)$ for all $T \in Aut\ G$.

We define a mapping $f : Aut\ G \to A(S)$ as

$$f(T) = T_S.$$

We show that f is one-to-one. Let $T_1, T_2 \in Aut\ G$. Then

$$f(T_1) = f(T_2) \Rightarrow (T_1)_S = (T_2)_S \Rightarrow T_1(P_i) = T_2(P_i) \ \forall\ i$$

$\Rightarrow \quad T_2^{-1} T_1(P_i) = P_i$ for each i

$\Rightarrow \quad T_2^{-1} T_1 = I \Rightarrow T_1 = T_2 \Rightarrow f$ is one-to-one

$\Rightarrow \quad o\{Aut\ G\} \leq o\{A(S)\} = 24 = o\{I(G)\}$, by (1) and (2)

$\Rightarrow \quad o\{Aut\ G\} \leq o\{I(G)\} \Rightarrow Aut\ G = I(G)$, since $I(G) \leq Aut\ G$

By (1), $I(G) = G$. Hence $Aut\ G = G$, $G = S_4$.

Remark. We have shown in Chapter 3 that $Aut\ S_3 = S_3$.

Example 4.2.29. *Show that* $Aut\ S_4 \approx S_4$.

Solution. We know that

$$Z(S_n) = \{e\} \quad \text{for} \quad n \geq 3.$$

Here e denotes the identity mapping of S_n.

$\therefore \quad Z(S_4) = \{e\}$ or $Z(G) \approx \{e\}$, where $G = S_4$.

We also know that

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

where $I(G)$ denotes the group of inner automorphism of G and further $I(G)$ is a subgroup of $Aut\ G$. Thus we have

$$\frac{G}{\{e\}} \approx I(G) \Rightarrow G \approx I(G), \text{ since } G \approx \frac{G}{\{e\}}.$$

$$\therefore \quad G \approx I(G) \Rightarrow o[I(G)] = o(G) = o(S_4) = 4! = 24. \quad ...(1)$$

We have $o(G) = 2^3 \times 3$.

The number (n_3) of 3-SSGs of G is $n_3 = 1 + 3k$, where $n_3 \mid o(G) = 24$

$\Rightarrow \quad k = 0$ or $1 \Rightarrow n_3 = 1$ or 4.

Hence $n_3 = 4$ *i.e.*, G has 4 Sylow 3-subgroups *viz.*

$$P_1 = \{I, (123), (132)\}, \quad P_2 = \{I, (124), (142)\},$$

$$P_3 = \{I, (134), (143)\}, \quad P_4 = \{I, (234), (243)\}.$$

Let $S = \{P_1, P_2, P_3, P_4\}$, so that $o[A(S)] = 4! = 24$. ...(2)

Let $T \in Aut\ G$ be arbitrary *i.e.*, $T : G \to G$ is onto, one-to-one and homomorphism. Then

$T_S(P_i) = \{T(x) : x \in P_i\}$ is a subgroup of G for each i.

T_S is called the *restriction mapping* of T to S.

Further $o[T_S(P_i)] = o(P_i) = 3$. Consequently, $T_S(P_i)$ is a 3-SSG of G for each $i \Rightarrow T_S(P_i) \in S$ for each i

$\Rightarrow \quad T_S : S \to S$ is one-to-one and onto, since T is one-to-one and onto

$\Rightarrow \quad T_S \in A(S)$ for all $T \in Aut\ G$.

We define a mapping $f : Aut\ G \to A(S)$ as

$$f(T) = T_S.$$

We show that f is one-to-one. Let $T_1, T_2 \in Aut\ G$. Then

$$f(T_1) = f(T_2) \Rightarrow (T_1)_S = (T_2)_S \Rightarrow T_1(P_i) = T_2(P_i) \ \forall\ i$$

$\Rightarrow \quad T_2^{-1} T_1(P_i) = P_i$ for each i

$\Rightarrow \quad T_2^{-1} T_1 = I \quad \Rightarrow \quad T_1 = T_2 \quad \Rightarrow f$ is one-to-one

$\Rightarrow \quad o[Aut\ G] \leq o[A(S)] = 24 = o[I(G)]$, by (1) and (2)

$\Rightarrow \quad o[Aut\ G] \leq o[I(G)] \Rightarrow Aut\ G = I(G)$, since $I(G) < Aut\ G$

By (1), $I(G) \approx G$. Hence $Aut\ G \approx G$, $G = S_4$.

Remark. We have shown in Chapter 3 that $Aut\ S_3 \approx S_3$.

Example 4.2.30. *Prove that every p-subgroup of a finite group G is contained in some Sylow p-subgroup of G.*

In order to prove this result, we first prove the following :

Lemma. *Let P be Sylow p-subgroup of a finite group G. If $x \in N(P)$ is such that $o(x) = p^i$ for some integer $i \geq 0$, then $x \in P$.*

Proof. We have $x^{p^i} = e$. Let $o(P) = p^n$, where

$$p^n \mid o(G) \text{ and } p^{n+1} \nmid o(G).$$

Since P is normal in $N(P)$, $N(P)/P$ is defined. Further $xP \in N(P)/P$, since $x \in N(P)$. We have

$$(xP)^{p^i} = x^{p^i} P = P \qquad (\because x^{p^i} = e)$$

$$\Rightarrow \quad o(xP) \mid p^i \Rightarrow o(xP) = p^k \text{ for some } k \geq 0.$$

Let $\overline{K} = \langle \overline{x} \rangle$ where $\overline{x} = xP$.

Then $\overline{K}$ is a subgroup of $N(P)/P$, where

$$o(\overline{K}) = o(\overline{x}) = p^k$$

and $\overline{K}$ is of the form given by

$$\overline{K} = K/P \text{ where } K < N(P) \text{ and } K \supseteq P$$

$$\Rightarrow \quad o(\overline{K}) = \frac{o(K)}{o(P)} \text{ or } o(K) = o(\overline{K})\, o(P) = p^k \cdot p^n$$

$$\Rightarrow \quad o(K) = p^{k+n} \Rightarrow K \text{ is a } p\text{-subgroup of } G \text{ containing } P.$$

Since no p-subgroup of G can contain a Sylow p-subgroup of G properly, $K = P$.

Now $K = P \Rightarrow \overline{K} = K/P = \{P\} \Rightarrow \overline{x} = P \Rightarrow xP = P \Rightarrow x \in P$.

Proof of the main result

Let H be any p-subgroup of G, where $o(H) = p^m$ (p is prime). Let $\mathfrak{I}$ be the set of all Sylow p-subgroups of G. By Third Sylow Theorem,

$$o(\mathfrak{I}) = n_p = 1 + kp \ (k = 0, 1, 2, \ldots). \qquad \ldots(1)$$

Let $P_1, P_2 \in \mathfrak{I}$ be arbitrary. We define a relation $\sim$ on $\mathfrak{I}$ as follows :

$$P_1 \sim P_2 \text{ iff } P_1 = x P_2 x^{-1} \text{ for some } x \in H.$$

It is easy to verify that $\sim$ is an equivalence relation on $\mathfrak{I}$. The equivalence class of $P \in \mathfrak{I}$ is given by

$$[P] = \{x P x^{-1} : x \in H\}.$$

We have $\mathfrak{I} = \cup [P]$ and so $o(\mathfrak{I}) = \Sigma\, o([P])$. $\ldots(2)$

By definition, $N_H(P) = \{x \in H : x P x^{-1} = P\}$.

Then $N_H(P)$ is a subgroup of H. Consequently,

$$o([P]) = \frac{o(H)}{o(N_H(P))}, \qquad \ldots(3)$$

[See (A) of Lemma 4.2.6]

By Lagrange's theorem, $o(N_H(P))$ divides $o(H) = p^m$.

Example 4.2.10. *Prove that every p-subgroup of a finite group G is contained in some Sylow p-subgroup of G.*

In order to prove this result, we first prove the following

Lemma. *Let P be Sylow p-subgroup of a finite group G. If $x \in N(P)$ is such that $o(x) = p^t$ for some integer $t \geq 0$, then $x \in P$.*

Proof. We have $x^{p^t} = e$. Let $o(P) = p^n$, where

$$p^n \mid o(G) \text{ and } p^{n+1} \nmid o(G)$$

Since P is normal in $N(P)$, $N(P)/P$ is defined. Further $xP \in N(P)/P$, since $x \in N(P)$. We have

$$(xP)^{p^t} = x^{p^t} P = P \qquad (\because x^{p^t} = e)$$

$$\rightarrow \quad o(xP) \mid p^t \rightarrow o(xP) = p^k \text{ for some } k \geq 0$$

Let $\bar{K} = \langle xP \rangle$ where $\bar{K} = xP$.

Then $\bar{K}$ is a subgroup of $N(P)/P$, where

$$o(\bar{K}) = o(xP) = p^k$$

and $\bar{K}$ is of the form given by

$$\bar{K} = K/P \text{ where } K \leq N(P) \text{ and } K \supseteq P$$

$$\rightarrow \quad o(\bar{K}) = \frac{o(K)}{o(P)} \text{ or } o(K) = o(\bar{K})\, o(P) = p^k \cdot p^n$$

$$\rightarrow \quad o(K) = p^{k+n} \rightarrow K \text{ is a } p\text{-subgroup of } G \text{ containing } P.$$

Since no p-subgroup of G can contain a Sylow p-subgroup of G properly, $K = P$.

Now $K = P \rightarrow \bar{K} = K/P = \{P\} \rightarrow xP = P \rightarrow x \in P$.

Proof of the main result

Let H be any p-subgroup of G, where $o(H) = p^m$ (p is prime). Let $\mathfrak{I}$ be the set of all Sylow p-subgroups of G. By Third Sylow Theorem,

$$o(\mathfrak{I}) = n_p = 1 + kp \ (k = 0, 1, 2, \ldots). \qquad \ldots(1)$$

Let $P_1, P_2 \in \mathfrak{I}$ be arbitrary. We define a relation $\sim$ on $\mathfrak{I}$ as follows :

$$P_1 \sim P_2 \text{ iff } P_1 = x P_2 x^{-1} \text{ for some } x \in H.$$

It is easy to verify that $\sim$ is an equivalence relation on $\mathfrak{I}$. The equivalence class of $P \in \mathfrak{I}$ is given by

$$[P] = \{x P x^{-1} : x \in H\}.$$

We have $\mathfrak{I} = \cup [P]$ and so $o(\mathfrak{I}) = \Sigma\, o([P])$. $\qquad \ldots(2)$

By definition, $N_H(P) = \{x \in H : x P x^{-1} = P\}$.

Then $N_H(P)$ is a subgroup of H. Consequently,

$$o([P]) = \frac{o(H)}{o\{N_H(P)\}}, \qquad \ldots(3)$$

[See (A) of Lemma 4.2.6.]

By Lagrange's theorem, $o\{N_H(P)\}$ divides $o(H) = p^m$.

Example 4.2.30. *Prove that every p-subgroup of a finite group G is contained in some Sylow p-subgroup of G.*

In order to prove this result, we first prove the following :

Lemma. *Let P be Sylow p-subgroup of a finite group G. If* $x \in N(P)$ *is such that* $o(x) = p^i$ *for some integer* $i \geq 0$, *then* $x \in P$.

Proof. We have $x^{p^i} = e$. Let $o(P) = p^n$, where

$$p^n \mid o(G) \text{ and } p^{n+1} \nmid o(G).$$

Since P is normal in $N(P)$, $N(P)/P$ is defined. Further $xP \in N(P)/P$, since $x \in N(P)$. We have

$$(xP)^{p^i} = x^{p^i} P = P \qquad (\because x^{p^i} = e)$$

$$\Rightarrow \quad o(xP) \mid p^i \Rightarrow o(xP) = p^k \text{ for some } k \geq 0.$$

Let $\overline{K} = \langle \overline{x} \rangle$, where $\overline{x} = xP$.

Then $\overline{K}$ is a subgroup of $N(P)/P$, where

$$o(\overline{K}) = o(\overline{x}) = p^k$$

and $\overline{K}$ is of the form given by

$$\overline{K} = K/P \quad \text{where} \quad K < N(P) \quad \text{and} \quad K \supseteq P$$

$$\Rightarrow \quad o(\overline{K}) = \frac{o(K)}{o(P)} \text{ or } o(K) = o(\overline{K})\, o(P) = p^k \cdot p^n$$

$$\Rightarrow \quad o(K) = p^{k+n} \Rightarrow K \text{ is a } p\text{-subgroup of } G \text{ containing } P.$$

Since no p-subgroup of G can contain a Sylow p-subgroup of G properly, $K = P$.

Now $K = P \Rightarrow \overline{K} = K/P = \{P\} \Rightarrow \overline{x} = P \Rightarrow xP = P \Rightarrow x \in P$.

Proof of the main result

Let H be any p-subgroup of G, where $o(H) = p^m$ (p is prime). Let $\mathfrak{I}$ be the set of all Sylow p-subgroups of G. By Third Sylow Theorem,

$$o(\mathfrak{I}) = n_p = 1 + kp \ (k = 0, 1, 2, \ldots). \qquad \ldots(1)$$

Let $P_1, P_2 \in \mathfrak{I}$ be arbitrary. We define a relation $\sim$ on $\mathfrak{I}$ as follows :

$$P_1 \sim P_2 \text{ iff } P_1 = x P_2 x^{-1} \text{ for some } x \in H.$$

It is easy to verify that $\sim$ is an equivalence relation on $\mathfrak{I}$. The equivalence class of $P \in \mathfrak{I}$ is given by

$$[P] = \{x P x^{-1} : x \in H\}.$$

We have $\mathfrak{I} = \cup [P]$ and so $o(\mathfrak{I}) = \Sigma\, o([P])$. $\qquad \ldots(2)$

By definition, $N_H(P) = \{x \in H : x P x^{-1} = P\}$.

Then $N_H(P)$ is a subgroup of H. Consequently,

$$o([P]) = \frac{o(H)}{o(N_H(P))}, \qquad \ldots(3)$$

[See (A) of Lemma 4.2.6.]

By Lagrange's theorem, $o(N_H(P))$ divides $o(H) = p^m$.

Example 4.2.30. *Prove that every p-subgroup of a finite group G is contained in some Sylow p-subgroup of G.*

In order to prove this result, we first prove the following :

Lemma. *Let P be Sylow p-subgroup of a finite group G. If* $x \in N(P)$ *is such that* $o(x) = p^i$ *for some integer* $i \geq 0$, *then* $x \in P$.

Proof. We have $x^{p^i} = e$. Let $o(P) = p^n$, where

$$p^n \mid o(G) \text{ and } p^{n+1} \nmid o(G).$$

Since P is normal in $N(P)$, $N(P)/P$ is defined. Further $xP \in N(P)/P$, since $x \in N(P)$. We have ,

$$(xP)^{p^i} = x^{p^i} P = P \qquad (\because x^{p^i} = e)$$

$$\Rightarrow \qquad o(xP) \mid p^i \Rightarrow o(xP) = p^k \text{ for some } k \geq 0.$$

Let $\overline{K} = \langle \overline{x} \rangle$, where $\overline{x} = xP$.

Then $\overline{K}$ is a subgroup of $N(P)/P$, where

$$o(\overline{K}) = o(\overline{x}) = p^k$$

and $\overline{K}$ is of the form given by

$$\overline{K} = K/P \quad \text{where} \quad K < N(P) \quad \text{and} \quad K \supseteq P$$

$$\Rightarrow \quad o(\overline{K}) = \frac{o(K)}{o(P)} \text{ or } o(K) = o(\overline{K})\, o(P) = p^k . p^n$$

$$\Rightarrow \quad o(K) = p^{k+n} \Rightarrow K \text{ is a } p\text{-subgroup of } G \text{ containing } P.$$

Since no p-subgroup of G can contain a Sylow p-subgroup of G properly, $K = P$.

Now $K = P \Rightarrow \overline{K} = K/P = \{P\} \Rightarrow \overline{x} = P \Rightarrow xP = P \Rightarrow x \in P$.

Proof of the main result

Let H be any p-subgroup of G, where $o(H) = p^m$ (p is prime). Let $\mathfrak{I}$ be the set of all Sylow p-subgroups of G. By Third Sylow Theorem,

$$o(\mathfrak{I}) = n_p = 1 + kp \ (k = 0, 1, 2, \ldots). \qquad \ldots(1)$$

Let $P_1, P_2 \in \mathfrak{I}$ be arbitrary. We define a relation $\sim$ on $\mathfrak{I}$ as follows :

$$P_1 \sim P_2 \text{ iff } P_1 = x P_2 x^{-1} \text{ for some } x \in H.$$

It is easy to verify that $\sim$ is an equivalence relation on $\mathfrak{I}$. The equivalence class of $P \in \mathfrak{I}$ is given by

$$[P] = \{x P x^{-1} : x \in H\}.$$

We have $\mathfrak{I} = \cup [P]$ and so $o\{\mathfrak{I}\} = \Sigma\, o\{[P]\}$. $\qquad \ldots(2)$

By definition, $N_H(P) = \{x \in H : x P x^{-1} = P\}$.

Then $N_H(P)$ is a subgroup of H. Consequently,

$$o\{[P]\} = \frac{o(H)}{o\{N_H(P)\}}. \qquad \ldots(3)$$

[See (A) of Lemma 4.2.6.]

By Lagrange's theorem, $o\{N_H(P)\}$ divides $o(H) = p^m$.

$\therefore$ $o\{N_H(P)\} = p^k$, where $0 < k \leq m$.

Using in (3), we have

$$o\{[P]\} = \frac{p^m}{p^k} = p^l,\ l = m - k \geq 0. \qquad \ldots(4)$$

Suppose, on the contrary, H is not contained in any Sylow p-subgroup of G. Then $H \not\subset P$ and so there exists some $x \in H$ such that $x \notin P$. If

$$x P x^{-1} = P, \quad \text{then} \quad x \in N(P).$$

Since H is a p-subgroup and $x \in H$, $o(x) = p^i$ for some $i > 0$. Thus we see that P is a Sylow p-subgroup of G and $x \in N(P)$ satisfies $o(x) = p^i$. By the above Lemma ; $x \in P$. This is a contradiction.

Thus

$$x P x^{-1} \neq P, \quad \text{where } x \in H.$$

It follows that P and $x P x^{-1}$ $(x \in H)$ belong to $[P]$. Therefore,

$$o\{[P]\} > 1.$$

Using this fact in (4), we see that

$$o\{[P]\} = p^l, \quad \text{where} \quad l > 0$$

$\Rightarrow o\{[P]\}$ is a multiple of p for each $P \in \mathfrak{S}$.

Using in (2), it follows that

$$o\{\mathfrak{S}\} = \Sigma\ o\{[P]\} \text{ is a multiple of } p.$$

This contradicts (1). Hence H is contained in some Sylow p-subgroup of G.

Example 4.2.31. *Show that a normal p-subgroup K of a finite group G is contained in every Sylow p-subgroup of G.*

Solution. By Example 4.2.30, K is contained in some Sylow p-subgroup, say Q, of G

i.e., $\quad K \subseteq Q \Rightarrow x K x^{-1} \subseteq x Q x^{-1} \ \forall\ x \in G$

$\therefore$ $\quad K \subseteq x Q x^{-1} \ \forall\ x \in G$, since $K \lhd G$. $\qquad \ldots(1)$

Let P be any Sylow p-subgroup of G. We shall prove that $K \subseteq P$.

Since P and Q are two Sylow p-subgroups of G, by Second Sylow Theorem, we have

$$P = y Q y^{-1} \quad \text{for some} \quad y \in G. \qquad \ldots(2)$$

From (1) and (2), we have

$K \subseteq y Q y^{-1} = P$. Hence $K \subseteq P$.

Example 4.2.32. *Let G be a finite group such that p divides $o(G)$, p being prime. If A is a normal subgroup of G and H is a Sylow p-subgroup of G, then prove that*

(i) $A \cap H$ is a Sylow p-subgroup of A.

(ii) $\frac{HA}{A}$ is a Sylow p-subgroup of $\frac{G}{A}$.

Solution. Let $o(H) = p^n$, where $p^n \mid o(G), p^{n+1} \nmid o(G)$.

Let, if possible, $A \cap H$ be **not** a Sylow p-subgroup of A. We have

$$o(A \cap H) \mid o(H) = p^n \Rightarrow o(A \cap H) = p^r, 0 \le r \le n.$$

By Example 4.2.30, there exists a Sylow p-subgroup P of A and a Sylow p-subgroup Q of G such that

$$A \cap H \subseteq P \subseteq Q \quad \ldots(1)$$

Since H and Q are two Sylow p-subgroups of G, they are conjugate in G (Second Sylow Theorem). Thus there exists some $x \in G$ such that

$$H = x Q x^{-1}. \quad \ldots(2)$$

Now $P \subseteq A$ and $P \subseteq Q \Rightarrow P \subseteq A \cap Q$

$\Rightarrow x P x^{-1} \subseteq x(A \cap Q) x^{-1}$

$\Rightarrow x P x^{-1} \subseteq (x A x^{-1}) \cap (x Q x^{-1})$

$\Rightarrow x P x^{-1} \subseteq (x A x^{-1}) \cap H$, by (2)

$\Rightarrow x P x^{-1} \subseteq A \cap H$, since $A \lhd G \Rightarrow x A x^{-1} = A$

$\Rightarrow x P x^{-1} \subseteq P$, using (1).

But $o(x P x^{-1}) = o(P) \Rightarrow x P x^{-1} = P$.

Since $x P x^{-1}$ is a Sylow p-subgroup of G, so P is a Sylow p-subgroup of G, which is a contradiction.

Hence $A \cap H$ is a Sylow p-subgroup of A.

(*ii*) By part (*i*), $A \cap H$ is a Sylow p-subgroup of A. Let $o(A \cap H) = p^m$ where $p^m \mid o(A)$ and $p^{m+1} \nmid o(A)$. We have

$$o\left(\frac{HA}{A}\right) = \frac{o(HA)}{o(A)} = \frac{o(H)\, o(A)}{o(H \cap A) \cdot o(A)} = \frac{o(H)}{o(H \cap A)} = \frac{p^n}{p^m} = p^{n-m}.$$

Since $p^n \mid o(G)$ and $p^m \mid o(A)$, $p^{n-m} \mid o(G/A)$

Also $p^{n-m+1} \nmid o(G/A)$

Hence HA/A is a Sylow p-subgroup of G/A.

EXERCISES

1. Show that a group of order 63 is not simple.
   [**Hint.** $n_7 = 1$.]
2. If the order of a group is 42, prove that its Sylow 7-subgroup is normal.
3. If $o(G) = 36$, prove that G has 1 or 4 Sylow 3-subgroups.
4. Prove that a group of order 99 is not simple.
   [**Hint.** $n_{11} = 1$.] [D.U., 1997]

5. Prove that a group of order 77 is cyclic.
[**Hint.** $o(G) = 7 \times 11$, where $7 \nmid (11 - 1) = 10$. Use Example 4.2.7.]
6. Prove that a group of order 35 is cyclic.
7. Let G be a group. Prove $o(G/Z) \neq 77$.
[**Hint.** If $G/Z = 77$, then G/Z is cyclic $\Rightarrow G$ is abelian, a contradiction.]
8. Prove that a group of order 48 must have a normal subgroup of 8 or 16.
[**Hint.** Similar to Example 4.2.15.]
9. Show that a group G is a p-group if and only if there exists a normal subgroup N of G such that N and G/N both are p-groups.
[**Hint.** If $o(N) = p^i$ and $o(G/N) = p^j$, then $o(G) = o(G/N)\, o(N)$
$\Rightarrow \quad o(G) = p^{i+j} \Rightarrow G$ is a p-group.
Conversely, $o(G) = p^r \Rightarrow p \mid o(G) \Rightarrow o(Z) > 1$, where $Z \triangleleft G$.
Since $o(Z) \mid o(G)$ and $o(Z) > 1$, $o(Z) = p^s$, $0 < s \leq r \Rightarrow Z$ is a p-group and
$$o\left(\frac{G}{Z}\right) = \frac{o(G)}{o(Z)} = p^{r-s} \Rightarrow \frac{G}{Z} \text{ is also a } p\text{-group.}]$$
10. If H is a normal subgroup of order p^k of a finite group G, show that H is contained in every Sylow p-subgroup of G.
[**Hint.** Same as Example 4.2.31.]

4.3 Direct Products

External Direct Product

Let $G_1, G_2, \ldots, G_n$ be any n groups, whose cartesian product is
$$G_1 \times G_2 \times \ldots \times G_n = \{(g_1, g_2, \ldots, g_n) : g_i \in G_i,\ 1 \leq i \leq n\}.$$
It is easy to verify that
$$G = G_1 \times G_2 \times \ldots \times G_n \text{ is a group}$$
w.r.t. the composition defined as follows :
$$(g_1, g_2, \ldots, g_n)(g_1', g_2', \ldots, g_n') = (g_1 g_1', g_2 g_2', \ldots, g_n g_n') \quad \ldots(1)$$
for all $(g_1, g_2, \ldots, g_n), (g_1', g_2', \ldots, g_n') \in G$.

The composition defined in (1) is called *componentwise multiplication.* It may be observed that the identity in G is $(e_1, e_2, \ldots, e_n)$, where each e_i is the identity of G_i, and
$$(g_1, g_2, \ldots, g_n)^{-1} = (g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1}) \in G.$$
Indeed, $(g_1, g_2, \ldots, g_n)(e_1, e_2, \ldots, e_n) = (g_1 e_1, g_2 e_2, \ldots, g_n e_n)$
$$= (g_1, g_2, \ldots, g_n)$$
and $(g_1, g_2, \ldots, g_n)(g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1}) = (g_1 g_1^{-1}, g_2 g_2^{-1}, \ldots, g_n g_n^{-1})$
$$= (e_1, e_2, \ldots, e_n).$$

The group $G = G_1 \times G_2 \times \ldots \times G_n$ *is called the* **external direct product** **(E.D.P.)** *of* $G_1, G_2, \ldots, G_n$.

Internal Direct Product

Definition. *A group G is said to be an* **internal direct product (I.D.P.)** *of its subgroups $H_1, H_2, ..., H_n$, if the following conditions are satisfied :*

(i) $h_i h_j = h_j h_i$ *for each* $h_i \in H_i$, $h_j \in H_j$ *and* $i \neq j$.

(ii) Each $x \in G$ *is uniquely expressible as*

$$x = x_1 x_2 \dots x_n,\ x_i \in H_i \text{ for } 1 \leq i \leq n.$$

Equivalently, if we have

$$x = x_1 x_2 \dots x_n \quad \text{and} \quad x = y_1 y_2 \dots y_n,$$

where $x_i, y_i \in H_i$ for $1 \leq i \leq n$; then

$$x_i = y_i \quad \text{for each } i,\ 1 \leq i \leq n.$$

Remark. If the group is additive, the internal direct product of subgroups $H_1, H_2, \dots, H_n$ of G is written as $H_1 \oplus H_2 \oplus \dots \oplus H_n$ and is called the **direct sum** of $H_1, H_2, ..., H_n$.

Theorem 4.3.1. *Show that the internal direct product of subgroups $H_1, H_2, ..., H_n$ of a group G is isomorphic to the external direct product of $H_1, H_2, ..., H_n$.* [D.U., 1993]

Or

If G is the internal direct product of its subgroups $H_1, H_2, ..., H_n$, then $G \approx H_1 \times H_2 \times \dots \times H_n$. [D.U., 1997]

Proof. Let $T = H_1 \times H_2 \times \dots \times H_n$.

Define a mapping $\phi : T \to G$ as

$$\phi(x) = x_1 x_2 \dots x_n,\ \forall\ x = (x_1, x_2, ..., x_n) \in T. \qquad ...(1)$$

First of all we show that ϕ is one-to-one.

Let $x = (x_1, x_2, ..., x_n) \in T,\ y = (y_1, y_2, ..., y_n) \in T.$

Then $\phi(x) = \phi(y) \Rightarrow x_1 x_2 \dots x_n = y_1 y_2 \dots y_n$, by (1)

$\Rightarrow$ $x_i = y_i$ for $i = 1, 2, ..., n,$

by the uniqueness in the definition of I.D.P.

$\Rightarrow$ $(x_1, x_2, ..., x_n) = (y_1, y_2, \dots, y_n) \Rightarrow x = y.$

Thus ϕ is one-to-one.

Next we show that ϕ is onto.

Let $g \in G$ be arbitrary. Since G is the internal direct product (I.D.P.) of $H_1, H_2, \dots, H_n$, we can uniquely express $g \in G$ as

$$g = h_1 h_2 \dots h_n\ ;\ h_i \in H_i \quad \text{for} \quad 1 \leq i \leq n.$$

Then $h = (h_1, h_2, ..., h_n) \in T = H_1 \times H_2 \times \dots \times H_n$

and $\phi(h) = g$. This shows that ϕ is onto.

Lastly, we show that ϕ is a homomorphism.

Let $x = (x_1, x_2, \dots, x_n) \in T,\ y = (y_1, y_2, \dots, y_n) \in T.$

Then $xy = (x_1 y_1, x_2 y_2, ..., x_n y_n)$. Using (1), we have

$$\phi(xy) = x_1 y_1 x_2 y_2 \dots x_n y_n. \qquad ...(2)$$

By definition of I.D.P., we have

$$x_i y_j = y_j x_i \text{ for } i \neq j. \qquad ...(3)$$

From (2) and (3),

$$\phi(xy) = x_1 x_2 \ldots x_n y_1 y_2 \ldots y_n = \phi(x)\,\phi(y)$$

$\Rightarrow \phi$ is a homomorphism. Hence $T \approx G$ or $G \approx T$.

Remark. In the light of the above theorem, we call G as the *direct product* of its subgroups $H_1, H_2, \ldots, H_n$ and write its as

$$G = H_1 \times H_2 \times \ldots \times H_n.$$

Theorem 4.3.2. *A group G is an internal direct product of its subgroups $H_1, H_2, \ldots, H_n$ if and only if the following conditions are satisfied :*

(a) Each H_i is a normal subgroup of G, $1 \leq i \leq n$.

(b) $H_i \cap H_1 H_2 \ldots H_{i-1} H_{i+1} \ldots H_n = (e)$ for each i.

(c) $G = H_1 H_2 \ldots H_n$.

Proof. Conditions are necessary

Let G be an internal direct product of $H_1, H_2, \ldots, H_n$. Then each $g \in G$ is uniquely expressible as $g = h_1 h_2 \ldots, h_n$; $h_i \in H_i$ for $1 \leq i \leq n$.

$\Rightarrow$ $G = H_1 H_2 \ldots H_n$, which proves (*c*).

Now we prove (*a*). Let $a_k \in H_k$ and $x \in G$.

Then $x = x_1 x_2 \ldots x_n$, $x_i \in H_i$ for $1 \leq i \leq n$.

By definition of I.D.P., we have

$$x_i a_k = a_k x_i \quad \text{for} \quad i \neq k$$

$$\Rightarrow \qquad x_i a_k x_i^{-1} = a_k \quad \text{for} \quad i \neq k. \qquad ...(1)$$

Now $$x a_k x^{-1} = (x_1 \ldots x_k \ldots x_n)\, a_k\, (x_n^{-1} \ldots x_k^{-1} \ldots x_1^{-1})$$

$$= x_k a_k x_k^{-1} \in H_k, \text{ using (1).}$$

Hence H_k is a normal subgroup of G for each k, $1 \leq k \leq n$.

To prove (*b*), let $y \in H_i \cap H_1 H_2 \ldots H_{i-1} H_{i+1} \ldots H_n$

$\Rightarrow$ $y \in H_i$ and $y \in H_1 H_2 \ldots H_{i-1} H_{i+1} \ldots H_n$

$\Rightarrow$ $y = y_i$ for some $y_i \in H_i$ and $y = y_1 \ldots y_{i-1} y_{i+1} \ldots y_n$,

where $y_j \in H_j$ for $j \neq i$.

$\therefore$ $$y_i = y_1 \ldots y_{i-1} y_{i+1} \ldots y_n$$

or $$e \ldots e \,.\, y_i \,.\, e \ldots e = y_1 \ldots y_{i-1}\, e\, y_{i+1} \ldots y_n$$

By the uniqueness in the definition of I.D.P.,

$$y_i = e \text{ for each } i,\ 1 \leq i \leq n$$

$\therefore$ $$y = y_i \Rightarrow y = e \quad \forall\ y \in H_i \cap H_1 \ldots H_{i-1} H_{i+1} \ldots H_n.$$

Hence $H_i \cap H_1 H_2 \ldots H_{i-1} H_{i+1} \ldots H_n = (e)$, which proves (*b*).

Conditions are sufficient

Let $H_1, H_2, ..., H_n$ be subgroup of G satisfying the three given conditions (a), (b) and (c). We shall prove that G is the internal direct product of $H_1, H_2, ..., H_n$.

Let $j \neq i$. Then $H_j \subseteq H_1 H_2 ... H_{i-1} H_{i+1} ... H_n$

$\Rightarrow$ $H_i \cap H_j \subseteq H_i \cap H_1 H_2 ... H_{i-1} H_{i+1} ... H_n = (e)$, by (b)

$\therefore$ $H_i \cap H_j = (e)$ for $i \neq j$.

Since $H_i \triangleleft G$, $H_j \triangleleft G$ and $H_i \cap H_j = (e)$ for $i \neq j$, it follows that

$h_i h_j = h_j h_i$ for all $h_i \in H_i$, $h_j \in H_j$ and $i \neq j$. ...(2)

Let $x \in G$ be arbitrary. Then by condition (c),

$x = x_1 x_2 ... x_n$, where $x_i \in H_i$ for $1 \leq i \leq n$.

We shall show that this is a unique representation.

Let $x = y_1 y_2 ... y_n$, where $y_i \in H_i$ for $1 \leq i \leq n$. Thus we have

$x_1 x_2 ... x_i ... x_n = y_1 y_2 ... y_i ... y_n$

$\Rightarrow$ $x_1 x_2 ... x_i ... x_{n-1} = y_1 y_2 ... y_i ... y_n x_n^{-1}$

$\Rightarrow$ $x_1 x_2 ... x_i ... x_{n-2} = y_1 y_2 ... y_i ... y_{n-1} (y_n x_n^{-1}) x_{n-1}^{-1}$

$\Rightarrow$ $x_1 x_2 ... x_i ... x_{n-2} = y_1 y_2 ... y_i ... (y_{n-1} x_{n-1}^{-1}) (y_n x_n^{-1})$, by (2)

Proceeding in the similar manner and using (2), we obtain

$x_i y_i^{-1} = (y_1 x_1^{-1}) (y_2 x_2^{-1}) ... (y_{i-1} x_{i-1}^{-1}) (y_{i+1} x_{i+1}^{-1}) ... (y_n x_n^{-1})$.

From the above relation, we observe that $x_i y_i^{-1} \in H_i$ and the element on the R.H.S. belongs to $H_1 H_2 ... H_{i-1} H_{i+1} ... H_n$. Consequently,

$x_i y_i^{-1} \in H_i \cap H_1 H_2 ... H_{i-1} H_{i+1} ... H_n = (e)$, by (b)

$\Rightarrow$ $x_i y_i^{-1} = e$ for each i, $1 \leq i \leq n$

$\Rightarrow$ $x_i = y_i$ for each i, $1 \leq i \leq n$.

Hence each $x \in G$ is uniquely expressible as

$x = x_1 x_2 ... x_n$; $x_i \in H_i$ for $1 \leq i \leq n$. ...(3)

By the conditions (2) and (3), it follows that G is the internal direct product of $H_1, H_2, ..., H_n$.

Corollary 1. *Let $H_1, H_2, ..., H_n$ be normal subgroups of a group G. Show that G is an internal direct product of $H_1, H_2, ..., H_n$ if and only if the following conditions are satisfied :*

(i) $G = H_1 H_2 ... H_n$

(ii) $H_i \cap (H_1 H_2 ... H_{i-1} H_{i+1} ... H_n = (e)$ *for each* i. [D.U., 1995, 94]

Note. The proof of this corollary is essentially the same as that of the above theorem. However in the necessary conditions, one need not prove the condition (a).

Now we give an independent proof of the following :

Corollary 2. *A group G is an internal direct product of its subgroups A and B if and only if the following conditions are satisfied :*

(a) A and B are normal subgroups of G, (b) $A \cap B = (e)$, (c) $G = AB$.

Proof. Conditions are necessary

Let G be an internal direct product of A and B. Then each $g \in G$ is uniquely expressible as

$$g = ab, \qquad \ldots(1)$$

where $a \in A$ and $b \in B$. Hence $G = AB$, which proves (c).

Let $g \in G$ and $\alpha \in A$ be arbitrary. Then

$$g \alpha g^{-1} = (ab)\, \alpha\, (ab)^{-1}, \text{ by (1)}$$

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

since $\alpha \in A$ and $b \in B \Rightarrow \alpha b = b \alpha$, by definition of I.D.P.

$$\therefore \quad g \alpha g^{-1} = a \alpha (bb^{-1}) a^{-1} = a \alpha e a^{-1} = a \alpha a^{-1} \in A, \text{ as } a, \alpha \in A.$$

Thus $g \alpha g^{-1} \in A \ \forall\ g \in G$ and $\alpha \in A \Rightarrow A \lhd G$. Similarly, $B \lhd G$.

Lastly, we show $A \cap B = (e)$.

Let $x \in A \cap B \Rightarrow x \in A$ and $x \in B$. We have

$$x = xe \ (x \in A \text{ and } e \in B)$$

and

$$x = ex \ (e \in A \text{ and } x \in B).$$

By the uniqueness in the definition of I.D.P.,

$$x = e \ \forall\ x \in A \cap B. \text{ Hence } A \cap B = (e).$$

Conditions are sufficient

Let A, B be subgroups of G satisfying conditions (a), (b), (c). Conditions (a) and (b) imply

$$ab = ba \quad \forall \quad a \in A \quad \text{and} \quad b \in B.$$

By condition (c), each $g \in G$ is expressible as

$$g = ab \text{ for some } a \in A,\ b \in B.$$

The above expression is unique, for if $g = a_1 b_1$ ($a_1 \in A$ and $b_1 \in B$), then

$$ab = a_1 b_1 \Rightarrow a_1^{-1} a = b_1 b^{-1}$$

$$\Rightarrow \quad a_1^{-1} a \text{ and } b_1 b^{-1} \in A \cap B = (e)$$

$$\Rightarrow \quad a_1^{-1} a = e \text{ and } b_1 b^{-1} = e \Rightarrow a = a_1,\ b = b_1.$$

Hence G is the internal direct product of A and B.

Theorem 4.3.3. *Prove that a finite abelian group G is direct product of its Sylow's subgroups.*

Proof. If $o(G) = n$, then n is expressible as

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r},$$

where $p_1, p_2, \ldots, p_r$ are distinct primes and $\alpha_i > 0$ for each i.

Since $p_i^{\alpha_i} \mid o(G)$ and $p_i^{\alpha_i + 1} \nmid o(G)$, therefore G has a Sylow p_i-subgroup (say P_i) of order $p_i^{\alpha_i}$ *i.e.*, $o(P_i) = p_i^{\alpha_i}$; $i = 1, 2, \ldots, r$.

We shall prove that G is the (internal) direct product of its Sylow's subgroups $P_1, P_2, ..., P_r$. As G is abelian, P_i is normal in G for each i. ...(1)

Next we show that

$$P_i \cap P_1 P_2 \dots P_{i-1} P_{i+1} \dots P_r = (e) \text{ for each } i. \quad \dots(2)$$

Let $x \in P_i \cap P_1 P_2 \dots P_{i-1} P_{i+1} \dots P_r$. Then

$x \in P_i$ and $x \in P_1 P_2 \dots P_{i-1} P_{i+1} \dots P_r$ so that

$$x = x_1 x_2 \dots x_{i-1} x_{i+1} \dots x_r, \; x_j \in P_j \text{ and } j \neq i$$

Since $x_j \in P_j$ and $o(P_j) = p_j^{\alpha_j}$, $(x_j)^{p_j^{\alpha_j}} = e$. ...(3)

Let $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_{i-1}^{\alpha_{i-1}} p_{i+1}^{\alpha_{i+1}} \dots p_r^{\alpha_r}$.

$\therefore$ $x^m = x_1^m x_2^m \dots x_{i-1}^m x_{i+1}^m \dots x_r^m$, since G is abelian.

For each $j \neq i$, we observe that

$$x_j^m = [(x_j)^{p_j^{\alpha_j}}]^{p_1^{\alpha_1} \dots p_{j-1}^{\alpha_{j-1}} p_{j+1}^{\alpha_{j+1}} \dots p_r^{\alpha_r}} = e, \text{ using (3).}$$

Consequently, $x^m = e$ and so $o(x)$ divides m.

Since $x \in P_i$, $o(x) \mid o(P_i) = p_i^{\alpha_i}$

$\Rightarrow$ $o(x) = p_i^{\beta_i}$, where $0 \leq \beta_i \leq \alpha_i$

$\Rightarrow$ $p_i^{\beta_i} \mid m$, since $o(x)$ divides m

$\Rightarrow$ $p_i^{\beta_i} \mid p_1^{\alpha_1} \dots p_{i-1}^{\alpha_{i-1}} p_{i+1}^{\alpha_{i+1}} \dots p_r^{\alpha_r}$

$\Rightarrow$ $\beta_i = 0 \Rightarrow o(x) = p_i^{\beta_i} = 1 \Rightarrow x = e$. This proves (2).

Now $$o(P_1 P_2 \dots P_r) = \frac{o(P_1)\, o(P_2 P_3 \dots P_r)}{o(P_1 \cap P_2 P_3 \dots P_r)}$$

$$= o(P_1)\, o(P_2 P_3 \dots P_r), \text{ using (2)}$$

$$= \frac{o(P_1)\, o(P_2)\, o(P_3 P_4 \dots P_r)}{o(P_2 \cap P_3 P_4 \dots P_r)},$$

where $P_2 \cap P_3 P_4 \dots P_r \subset P_2 \cap P_1 P_3 P_4 \dots P_r = (e)$, by (2)

and so $o(P_2 \cap P_3 P_4 \dots P_r) = 1$. Consequently,

$$o(P_1 P_2 \dots P_r) = o(P_1)\, o(P_2)\, o(P_3 P_4 \dots P_r).$$

Proceeding in the similar manner, we get

$$o(P_1 P_2 \dots P_r) = o(P_1)\, o(P_2) \dots o(P_r)$$

$$= p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} = o(G)$$

$\therefore$ $$G = P_1 P_2 \dots P_r. \quad \dots(4)$$

From (1), (2) and (4), it follows that G is (internal) direct product of its Sylow's subgroups $P_1, P_2, \dots, P_r$.

Remark. *Since internal direct product of $P_1, P_2, ..., P_r$ is isomorphic to their external direct product, therefore*

$$G \approx P_1 \times P_2 \times \dots \times P_r.$$

EXAMPLES

Example 4.3.1. *Find the external direct product of two cyclic groups :*

$$G_1 = \{a, a^2 = e_1\},\ G_2 = \{b, b^2, b^3 = e_2\}.$$

Solution. We have

$$G_1 \times G_2 = \{(e_1, e_2), (e_1, b), (e_1, b^2), (a, e_2), (a, b), (a, b^2)\}.$$

We now prove that $G_1 \times G_2 = \langle (a, b) \rangle$, $(a, b)^6 = (e_1, e_2)$.

We have

$$(a, b)^2 = (a, b)\,(a, b) = (aa, bb) = (a^2, b^2) = (e_1, b^2),$$

$$(a, b)^3 = (a, b)^2\,(a, b) = (e_1, b^2), (a, b) = (e_1 a, b^3) = (a, e_2),$$

$$(a, b)^4 = (a, b)^3\,(a, b) = (a, e_2)\,(a, b) = (a^2, e_2 b) = (e_1, b),$$

$$(a, b)^5 = (a, b)^4\,(a, b) = (e_1, b)\,(a, b) = (e_1 a, b^2) = (a, b^2),$$

$$(a, b)^6 = (a, b)^5\,(a, b) = (a, b^2)\,(a, b) = (a^2, b^3) = (e_1, e_2).$$

Hence $G = G_1 \times G_2$ is a cyclic group : $G = \langle (a, b) \rangle$ or order 6.

Example 4.3.2. *Let $G = \langle e \rangle$ be a cyclic group of order 6. Show that G is an internal direct product of its subgroups*

$$A = \{e, a^2, a^4\},\ B = \{e, a^3\}.$$

Solution. Since a cyclic group is necessarily abelian and a subgroup of an abelian group is normal, therefore

$$A \triangleleft G \quad \text{and} \quad B \triangleleft G. \qquad \ldots(1)$$

Clearly, $A \cap B = (e).$ ...(2)

Lastly,

$$AB = \{ee, ea^3, a^2e, a^2a^3, a^4e, a^4a^3\}$$

$$= \{e, a^3, a^2, a^5, a^4, a^7 = a^6a = ea = a\}$$

$$G = AB. \qquad \ldots(3)$$

∴ From (1), (2) and (3), it follows that G is the internal direct product of A and B [See Corollary 2].

Example 4.3.3. *Show that the Klein's 4-group*

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

is the internal direct product of its subgroups

$$A = \{e, a\} \quad \text{and} \quad B = \{e, b\}$$

Solution. Since G is abelian, $A \triangleleft G$ and $B \triangleleft G$. Further

$$AB = \{e, a, b, ab\} = G \text{ and } A \cap B = (e).$$

Hence G is the internal direct product of A and B.

Example 4.3.4. *Show that the quaternion group cannot be expressed as the internal direct product of its proper subgroups.* [D.U., 1995]

Solution. The quaternion group is

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

G has the following proper normal subgroups :

$$N_1 = \{1, -1\}, \quad N_2 = \{1, -1, i, -i\},$$
$$N_3 = \{1, -1, j, -j\}, \quad N_4 = \{1, -1, k, -k\}.$$

We see that $N_i \cap N_j = \{1, -1\}$ for $i \neq j$.

Indeed, $N_i \cap \prod_{j \neq i} N_j = \{1, -1\} \neq \{1\}$, for each i.

Hence G is not the internal direct product of its normal subgroups.

Example 4.3.5. *Show that S_3 cannot be written as the internal direct product of its two non-trivial subgroups.*

Solution. The only non-trivial normal subgroup of S_3 is

$$A = \{I, (123), (132)\}.$$

Since A is a subgroup of S_3, $AA = A \neq S_3$.

Hence S_3 cannot be the internal direct product of its two non-trivial subgroups.

Example 4.3.6. *Give an example of a group G and normal subgroups $N_1, N_2, \ldots, N_n$ such that*

$$G = N_1 N_2 \ldots N_n \quad \text{and} \quad N_i \cap N_j = (e) \text{ for } i \neq j$$

and yet G is not the internal direct product of $N_1, N_2, \ldots, N_n$.

Solution. Consider the Klein's 4-group :

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

Notice that $(ab)^2 = abab = aabb = a^2b^2 = e$.

Let $N_1 = \{e, a\}, N_2 = \{e, b\}, N_3 = \{e, ab\}$.

Since N_1, N_2, N_3 are subgroups of the abelian groups G, they are normal in G.

Further $N_i \cap N_j = (e)$ for $i \neq j$.

Consider the following expressions :

$$a = a \,.\, e \,.\, e \; ; \; a \in N_1, e_2 \in N_2, e \in N_3$$

and $\quad a = e \,.\, b \,.\, ab \; ; \; e \in N_1, b \in N_2, ab \in N_3.$

Since the above expressions of a are not unique, G is not the internal direct product of N_1, N_2, N_3.

Remark. It may, however, be observed that

$$G = N_1 N_2 N_3$$

but $N_3 \cap N_1 N_2 = \{e, ab\}$,

which violates the condition (b) of Theorem 4.3.2.

Example 4.3.7. *If G is a finite group and $N_1, N_2, \ldots, N_n$ are normal subgroups of G such that*

$$G = N_1 N_2 \ldots N_n \quad \text{and} \quad o(G) = o(N_1)\, o(N_2) \ldots o(N_n),$$

prove that G is the direct product of $N_1, N_2, \ldots, N_n$.

Solution. We are given that

(*i*) $N_i \triangleleft G$ for $i = 1, 2, \ldots, n$

(*ii*) $G = N_1 N_2 \ldots N_n$.

If we now show that $N_i \cap \prod_{j \neq i} N_j = (e)$ for each i, then by Theorem 4.3.2, G is the (internal) direct product of $N_1, N_2, \ldots, N_n$. We have

$N_i N_j \triangleleft G$ and so $N_i N_j = N_j N_i$ for $i \neq j$.

Using the above property in $G = N_1 N_2 \ldots N_i \ldots N_n$, we have

$$G = N_i N_1 N_2 \ldots N_{i-1} N_{i+1} \ldots N_n \quad \text{for each } i$$

$$\Rightarrow \quad G = N_i \left(\prod_{j \neq i} N_j \right)$$

$$\Rightarrow \quad o(G) = \frac{o(N_i)\, o\left(\prod_{j \neq i} N_j \right)}{o\left(N_i \cap \prod_{j \neq i} N_j \right)}. \qquad \ldots(1)$$

By the repeated application of the following result

$o(HK) = \dfrac{o(H)\, o(K)}{o(H \cap K)}$ on the R.H.S. of (1), we get

$$o(G) = \frac{o(N_i)\, o(N_1)\, o(N_2) \ldots o(N_{i-1})\, o(N_{i+1}) \ldots o(N_n)}{o\left(N_i \cap \prod_{j \neq i} N_j \right) \times o(N_1 \cap N_2 \ldots N_{i-1} N_{i+1} \ldots N_n)}$$

$$\times o(N_2 \cap N_3 \ldots N_{i-1} N_{i+1} \ldots N_n) \times \ldots \times o(N_{n-1} \cap N_n)$$

Using $o(G) = o(N_1)\, o(N_2) \ldots o(N_n)$ in the above expression, we get

$$o\left(N_i \cap \prod_{j \neq i} N_j \right) = 1 \quad \text{for each } i.$$

$$\therefore \quad N_i \cap \prod_{j \neq i} N_j = (e) \text{ for each } i. \qquad \ldots(iii)$$

From the conditions (*i*), (*ii*), (*iii*) ; we see that

G is the (internal) direct product of $N_1, N_2, \ldots, N_n$.

Example 4.3.8. *Let A and B be cyclic groups of orders m and n, respectively. Prove that $A \times B$ is cyclic if and only if m and n are relatively prime.* [D.U., 1998]

Solution. Let $A = \langle a \rangle$, $a^m = e_1$ and $B = \langle b \rangle$, $b^n = e_2$.

Let m and n be relatively prime integers.

We have $A \times B = \{(x, y) : x \in A \text{ and } y \in B\}$.

Consider $(a, b)^{mn} = (a^{mn}, b^{mn}) = ((a^m)^n, (b^n)^m)$

$$= (e_1^n, e_2^m) = (e_1, e_2),$$

$$\therefore \quad (a, b)^{mn} = (e_1, e_2), \text{ identity of } A \times B. \qquad \ldots(1)$$

We claim that mn is the smallest positive integer satisfying (1).

Let k be *any* positive integer such that

$$(a, b)^k = (e_1, e_2) \Rightarrow (a^k, b^k) = (e_1, e_2)$$

$\Rightarrow$ $a^k = e_1$ and $b^k = e_2$, where $o(a) = m$, $o(b) = n$

$\Rightarrow m \mid k$ and $n \mid k$,

$\Rightarrow mn \mid k$, since $(m, n) = 1$

$\Rightarrow mn \leq k$, which proves our assertion.

Hence $A \times B = \langle (a, b) \rangle$, $(a, b)^{mn} = (e_1, e_2)$ and so $A \times B$ is cyclic of order mn.

Conversely, let $A \times B$ be a cyclic group of order mn ; where

$$A = \langle a \rangle, a^m = e_1 \quad \text{and} \quad B = \langle b \rangle, b^n = e_2.$$

Let $A \times B = \langle (x, y) \rangle$, $x \in A$, $y \in B$ and $(x, y)^{mn} = (e_1, e_2)$.

We have to show that $(m, n) = 1$.

Let $(m, n) = d \Rightarrow d \mid m$ and $d \mid n$.

$\therefore$ $\frac{m}{d}$ and $\frac{n}{d}$ are positive integers. We have

$$(x, y)^{\frac{mn}{d}} = \left((x^m)^{\frac{n}{d}}, (y^n)^{\frac{m}{d}} \right) = \left((e_1)^{\frac{n}{d}}, (e_2)^{\frac{m}{d}} \right) = (e_1, e_2)$$

Since $o\{(x, y)\} = mn$, it follows that

mn divides $\frac{mn}{d} \Rightarrow d = 1 \Rightarrow (m, n) = 1$.

Hence m and n are relatively prime.

Example 4.3.9. *Show that a group of order 4 is either cyclic or is an internal direct product of two cyclic subgroups each of order 2.*

[D.U., 1997]

Solution. Let $o(G) = 4 = p^2$ ($p = 2$ is prime) so that G is abelian. If G is cyclic, there is nothing to prove. Suppose G is not cyclic. Since $p = 2$ divides $o(G) = 4$, by Cauchy's Theorem, there exists an element $a \neq e$ such that $a^2 = e$.

Let $A = \{a, a^2 = e\} = \langle a \rangle$. Since $A \neq G$, there exists some element $b \in G$ such that $b \notin A$.

Since $o(b)$ divides $o(G) = 4$, $o(b) = 1$ or 2 or 4.

Now $o(b) = 1 \Rightarrow b = e \in A$, a contradiction.

$o(b) = 4 \Rightarrow G = \langle b \rangle \Rightarrow G$ is cyclic, a contradiction.

$\therefore$ $o(b) = 2$. Let $B = \{b, b^2 = e\} = \langle b \rangle$.

Since G is abelian, $A \lhd G$ and $B \lhd G$. Also $A \cap B = (e)$.

$\therefore$ $AB \lhd G$ and $o(AB) = \frac{o(A)\, o(B)}{o(A \cap B)} = \frac{2 \times 2}{1} = 4 = o(G)$

$\Rightarrow G = AB$, where $A \cap B = (e)$ and $A \lhd G$, $B \lhd G$.

Hence G is the internal direct product of A and B, where A and B are two cyclic subgroups of G each of order 2.

Example 4.3.10. *Show that every group of order p^2, p a prime, is either cyclic or is isomorphic to the direct product of two cyclic groups each of order p.*

Solution. Let $o(G) = p^2$. Since p is prime, G is abelian. If G is cyclic, there is nothing to prove. Suppose G is not cyclic. Since $p \mid o(G)$, by Cauchy's Theorem, there exists an element $a \neq e \in G$ such that $a^p = e$.

$\therefore$ $A = \langle a \rangle$, $a^p = e$ is a cyclic subgroup of order p.

Since $o(A) < o(G)$, $A \neq G$ and so there exists some element $b \in G$ such that $b \notin A$.

By Lagrange's Theorem, $o(b)$ divides $o(G) = p^2$

$\Rightarrow$ $o(b) = 1$ or p or p^2.

Now $o(b) = 1 \Rightarrow b = e \in A$, a contradiction.

$o(b) = p^2 \Rightarrow G = \langle b \rangle$ is cyclic, a contradiction.

$\therefore$ $o(b) = p$. Let $B = \langle b \rangle$, $b^p = e$.

Then B is a cyclic subgroup of order p. Since G is abelian,

$$A \lhd G \quad \text{and} \quad B \lhd G.$$

Also $A \cap B = (e)$, for otherwise $o(A \cap B) = p = o(A)$

$\Rightarrow$ $A \cap B = A \Rightarrow A = B \Rightarrow b \in A$, a contradiction.

Further $$o(AB) = \frac{o(A)\, o(B)}{o(A \cap B)} = \frac{p \times p}{1} = p^2 = o(G)$$

$\Rightarrow$ $G = AB$ $(\because AB < G)$, where

$A \cap B = (e)$ and $A \lhd G$, $B \lhd G$.

Hence G is the internal direct product of A and B and since I.D.P. of A and B is isomorphic to the E.D.P. of A and B, it follows that

$G \approx A \times B$, where A and B are two cyclic groups each of order p.

Example 4.3.11. *Let G be a group, $K_1, K_2, \ldots, K_n$ normal subgroups of G. Suppose that $K_1 \cap K_2 \cap \ldots \cap K_n = (e)$. Let $V_i = G/K_i$. Prove that there is an isomorphism of G into $V_1 \times V_2 \times \ldots \times V_n$.*

Solution. Define a mapping

$$\phi : G \to V_1 \times V_2 \times \ldots \times V_n = \frac{G}{K_1} \times \frac{G}{K_2} \times \ldots \times \frac{G}{K_n} \text{ as}$$

$$\phi(g) = (K_1 g, K_2 g, \ldots, K_n g) \ \forall\ g \in G. \qquad \ldots(1)$$

Then ϕ is one-to-one, since for $x, y \in G$

$\phi(x) = \phi(y) \Rightarrow (K_1 x, K_2 x, \ldots, K_n x) = (K_1 y, K_2 y, \ldots, K_n y)$

$\Rightarrow$ $K_i x = K_i y$ for each i, $1 \leq i \leq n$

$\Rightarrow$ $x y^{-1} \in K_i$ for each i, $1 \leq i \leq n$

$\Rightarrow$ $x y^{-1} \in K_1 \cap K_2 \cap \ldots \cap K_n = (e)$

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

Now we show that ϕ is a homomorphism. For $x, y \in G$, we have

$$\begin{aligned}\phi(xy) &= (K_1 xy, K_2 xy, \ldots, K_n xy)\\ &= (K_1 x K_1 y, K_2 x K_2 y, \ldots, K_n x K_n y), \text{ as } K_i \lhd G\\ &= (K_1 x, K_2 x, \ldots, K_n x)(K_1 y, K_2 y, \ldots, K_n y)\\ &= \phi(x)\,\phi(y).\end{aligned}$$

Hence ϕ is a homomorphism and so ϕ is an isomorphism of G into $V_1 \times V_2 \times \ldots \times V_n$.

Example 4.3.12. *If M and N are normal subgroups of a group G, then show that $G/M \cap N$ is isomorphic to a subgroup of the (external) direct product of $G/M \times G/N$.*

Solution. Define a mapping $\phi : G \to \dfrac{G}{M} \times \dfrac{G}{N}$ as

$$\phi(g) = (Mg, Ng) \;\forall\; g \in G. \qquad \ldots(1)$$

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

$$\begin{aligned}\phi(xy) &= (Mxy, Nxy)\\ &= (Mx\,My, Nx\,Ny), \text{ since } M \lhd G, N \lhd G\\ &= (Mx, Nx)(My, Ny) = \phi(x)\,\phi(y).\end{aligned}$$

Thus ϕ is a homomorphism. The kernel of ϕ is

$$Ker\,\phi = \left\{ x \in G : \phi(x) = (M, N), \text{ identity of } \frac{G}{M} \times \frac{G}{N} \right\}.$$

Then $x \in Ker\,\phi \Leftrightarrow \phi(x) = (M, N)$

$\Leftrightarrow (Mx, Nx) = (M, N)$

$\Leftrightarrow Mx = M$ and $Nx = N$

$\Leftrightarrow x \in M$ and $x \in N$

$\Leftrightarrow x \in M \cap N$

$\therefore \quad Ker\,\phi = M \cap N.$

Since ϕ is a homomorphism of G into $G/M \times G/N$, $\phi(G)$ is a subgroup of $G/M \times G/N$. Thus ϕ is a homomorphism of G onto $\phi(G)$ with kernel $M \cap N$.

By Fundamental Theorem of Homomorphism,

$$\frac{G}{M \cap N} \approx \phi(G),$$

where $\phi(G)$ is a subgroup of $\dfrac{G}{M} \times \dfrac{G}{N}$.

Example 4.3.13. *If $G_1, G_2, \ldots, G_n$ are n groups, show that*

$$Z(G_1 \times G_2 \times \ldots \times G_n) = Z(G_1) \times Z(G_2) \times \ldots \times Z(G_n).$$

[$Z(G)$ denotes the centre of G]

Solution. Let $G = G_1 \times G_2 \times \ldots \times G_n$.

Any $g \in G$ is of the form $g = (g_1, g_2, \ldots, g_n)$, $g_i \in G_i$ for $1 \le i \le n$.

Let $a = (a_1, a_2, \ldots, a_n) \in Z(G)$ be arbitrary.

Then $ag = ga \ \forall\ g \in G$

$\Rightarrow (a_1, a_2, \ldots, a_n)(g_1, g_2, \ldots, g_n) = (g_1, g_2, \ldots, g_n)(a_1, a_2, \ldots, a_n)$

$\Rightarrow (a_1 g_1, a_2 g_2, \ldots, a_n g_n) = (g_1 a_1, g_2 a_2, \ldots, g_n a_n)$

$\Rightarrow a_i g_i = g_i a_i$ for each i, $1 \le i \le n$

$\Rightarrow a_i \in Z(G_i)$ for each i, $1 \le i \le n$

$\Rightarrow a = (a_1, a_2, \ldots, a_n) \in Z(G_1) \times Z(G_2) \times \ldots \times Z(G_n)$.

$\therefore Z(G_1 \times G_2 \times \ldots \times G_n) \subseteq Z(G_1) \times Z(G_2) \times \ldots \times Z(G_n)$. ...(1)

Conversely, let $z = (z_1, z_2, \ldots, z_n) \in Z(G_1) \times Z(G_2) \times \ldots \times Z(G_n)$

$\Rightarrow z_i \in Z(G_i)$ for each i, $1 \le i \le n$

$\Rightarrow z_i x_i = x_i z_i \quad \forall\ x_i \in G_i$, $1 \le i \le n$

$\Rightarrow (z_1, z_2, \ldots, z_n)(x_1, x_2, \ldots, x_n) = (x_1, x_2, \ldots, x_n)(z_1, z_2, \ldots, z_n)$

$\Rightarrow zx = xz \ \forall\ x = (x_1, x_2, \ldots, x_n) \in G$

$\Rightarrow z \in Z(G)$.

$\Rightarrow Z(G_1) \times Z(G_2) \times \ldots \times Z(G_n) \subseteq Z(G_1 \times G_2 \times \ldots \times G_n)$.

From (1) and (2), we have

$$Z(G_1 \times G_2 \times \ldots \times G_n) = Z(G_1) \times Z(G_2) \times \ldots \times Z(G_n).$$

Example 4.3.14. *If* $G = G_1 \times G_2 \times \ldots \times G_n$ *and if* $a = (a_1, a_2, \ldots a_n) \in G$, *show that*

$$N(a) = N(a_1) \times N(a_2) \times \ldots \times N(a_n),$$

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

[**Hint.** Similar to Example 4.3.13.]

Example 4.3.15. *If* $T = G_1 \times G_2 \times \ldots \times G_n$, *prove that for each* $i = 1, 2, \ldots, n$; *there is a homomorphism* ϕ_i *of* T *onto* G_i. *Find the kernel of* ϕ_i.

Solution. Define $\phi_i : T \to G_i$ as

$$\phi_i(x_1, \ldots, x_i, \ldots, x_n) = x_i, \text{ for all } (x_1, \ldots, x_n) \in G. \quad \ldots(1)$$

Let $x = (x_1, \ldots, x_i, \ldots, x_n), y = (y_1, \ldots, y_i, \ldots, y_n) \in T$.

Then $xy = (x_1 y_1, \ldots, x_i y_i, \ldots, x_n y_n)$. Using (1), we get

$$\phi_i(xy) = x_i y_i = \phi_i(x)\, \phi_i(y), \text{ by (1)}.$$

Thus ϕ_i is a homomorphism for each $i = 1, 2, \ldots, n$. Now we show that ϕ_i is onto. Let $g_i \in G_i$ be arbitrary. Then $g = (g_1, g_2, \ldots, g_i, \ldots, g_n) \in T$ and by (1),

$$\phi_i(g) = g_i.$$

Hence ϕ_i is a homomorphism of T onto G_i for each $i = 1, 2, \ldots, n$.

Kernel $\phi_i = \{x = (x_1, x_2, \ldots, x_i, \ldots, x_n) \in T : \phi_i(x) = e_i$, identity of $G_i\}$

$= \{(x_1, \ldots x_{i-1}, x_i, x_{i+1}, \ldots x_n) \in T : x_i = e_i\}$

$= \{(x_1, \ldots, x_{i-1}, e_i, x_{i+1}, \ldots, x_n) \in T\}$.

Then $ag = ga \ \forall \ g \in G$

$\Rightarrow (a_1, a_2, \ldots, a_n)(g_1, g_2, \ldots, g_n) = (g_1, g_2, \ldots, g_n)(a_2, a_2, \ldots, a_n)$

$\Rightarrow (a_1 g_1, a_2 g_2, \ldots, a_n g_n) = (g_1 a_1, g_2 a_2, \ldots, g_n a_n)$

$\Rightarrow a_i g_i = g_i a_i$ for each i, $1 \le i \le n$

$\Rightarrow a_i \in Z(G_i)$ for each i, $1 \le i \le n$

$\Rightarrow a = (a_1, a_2, \ldots, a_n) \in Z(G_1) \times Z(G_2) \times \ldots \times Z(G_n)$.

$\therefore Z(G_1 \times G_2 \times \ldots \times G_n) \subseteq Z(G_1) \times Z(G_2) \times \ldots \times Z(G_n)$. ...(1)

Conversely, let $z = (z_1, z_2, \ldots, z_n) \in Z(G_1) \times Z(G_2) \times \ldots \times Z(G_n)$

$\Rightarrow z_i \in Z(G_i)$ for each i, $1 \le i \le n$

$\Rightarrow z_i x_i = x_i z_i \quad \forall \ x_i \in G_i$, $1 \le i \le n$

$\Rightarrow (z_1, z_2, \ldots, z_n)(x_1, x_2, \ldots, x_n) = (x_1, x_2, \ldots, x_n)(z_1, z_2, \ldots, z_n)$

$\Rightarrow zx = xz \ \forall \ x = (x_1, x_2, \ldots, x_n) \in G$

$\Rightarrow z \in Z(G)$.

$\Rightarrow Z(G_1) \times Z(G_2) \times \ldots \times Z(G_n) \subseteq Z(G_1 \times G_2 \times \ldots \times G_n)$.

From (1) and (2), we have

$$Z(G_1 \times G_2 \times \ldots \times G_n) = Z(G_1) \times Z(G_2) \times \ldots \times Z(G_n).$$

Example 4.3.14. *If* $G = G_1 \times G_2 \times \ldots \times G_n$ *and if* $a = (a_1, a_2, \ldots a_n) \in G$, *show that*

$$N(a) = N(a_1) \times N(a_2) \times \ldots \times N(a_n),$$

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

[Hint. Similar to Example 4.3.13.]

Example 4.3.15. *If* $T = G_1 \times G_2 \times \ldots \times G_n$, *prove that for each* $i = 1, 2, \ldots, n$; *there is a homomorphism* ϕ_i *of* T *onto* G_i. *Find the kernel of* ϕ_i.

Solution. Define $\phi_i : T \to G_i$ as

$$\phi_i(x_1, \ldots, x_i, \ldots, x_n) = x_i, \text{ for all } (x_1, \ldots, x_n) \in G. \quad \ldots(1)$$

Let $x = (x_1, \ldots, x_i, \ldots, x_n)$, $y = (y_1, \ldots, y_i, \ldots, y_n) \in T$.

Then $xy = (x_1 y_1, \ldots, x_i y_i, \ldots, x_n y_n)$. Using (1), we get

$$\phi_i(xy) = x_i y_i = \phi_i(x)\, \phi_i(y), \text{ by (1).}$$

Thus ϕ_i is a homomorphism for each $i = 1, 2, \ldots, n$. Now we show that ϕ_i is onto. Let $g_i \in G_i$ be arbitrary. Then $g = (g_1, g_2, \ldots, g_i, \ldots, g_n) \in T$ and by (1),

$$\phi_i(g) = g_i.$$

Hence ϕ_i is a homomorphism of T onto G_i for each $i = 1, 2, \ldots, n$.

Kernel $\phi_i = \{x = (x_1, x_2, \ldots, x_i, \ldots, x_n) \in T : \phi_i(x) = e_i$, identity of $G_i\}$

$= \{(x_1, \ldots x_{i-1}, x_i, x_{i+1}, \ldots x_n) \in T : x_i = e_i\}$

$= \{(x_1, \ldots, x_{i-1}, e_i, x_{i+1}, \ldots, x_n) \in T\}$.

Example 4.3.16. *If G is a group and H, K are subgroups of G such that $G = H \times K$, prove that*

$$H \approx \frac{G}{K} \text{ and } K \approx \frac{G}{H}.$$

Solution. Since $G = H \times K$, each $x \in G$ can be uniquely expressed as $x = hk$ for some $h \in H$ and $k \in K$. Define $f : G \to H$ as

$$f(x) = h \quad \forall \quad x \in G. \qquad ...(1)$$

We show that f is a homomorphism.

Let $x, y \in G = H \times K$. Then

$x = hk, y = h_1k_1$; $h, h_1 \in H$ and $k, k_1 \in K$

$\Rightarrow$ $xy = (hk)(h_1k_1) = h(k\,h_1)\,k_1 = h(h_1k)\,k_1$,

since $G = H \times K \Rightarrow hk = kh \quad \forall\ h \in H$ and $k \in K$.

$\therefore$ $xy = (h\,h_1)(k\,k_1)$. By (1), we have

$f(xy) = h\,h_1 = f(x)\,f(y) \Rightarrow f$ is a homomorphism.

Clearly f is onto, since for any $a \in H$,

$f(g) = a$, where $g = ab\ (b \in K) \in G = H \times K$.

By Fundamental Theorem of Homomorphism,

$$\frac{G}{Ker f} \approx H \text{ or } H \approx \frac{G}{Ker f}, \text{ where}$$

$x \in Ker f \Leftrightarrow f(x) = e\ (x = hk\ ;\ h \in H, k \in K)$

$\Leftrightarrow h = e$

$\Leftrightarrow x = ek = k$

$\Leftrightarrow x \in K$.

$\therefore$ $Ker f = K$.

Hence $$H \approx \frac{G}{K}.$$

Similarly, if we define $f : G \to K$ as

$$f(x) = k \quad \forall \quad x = hk \in G = H \times K,$$

we can easily prove that

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

Example 4.3.17. *Let N be a normal subgroup of a group G. If $G = H \times K$, where H and K are subgroups of G, then prove that either N is abelian or N intersects H or K non-trivially.*

Solution. If $N \cap H \neq \{e\}$ or $N \cap K \neq \{e\}$, we are done.

Let $N \cap H = \{e\}$ and $N \cap K = \{e\}$.

In the above case, we shall prove that N is abelian.

Since $G = H \times K$, therefore $H \lhd G$ and $K \lhd G$ and $G = HK$. [Use the concept of I.D.P.]

Now $H \lhd G, N \lhd G$ and $H \cap N = \{e\}$ implies that

$hn = nh\ \forall\ h \in H$ and $n \in N$. ...(1)

Similarly, $kn = nk \quad \forall \quad k \in K$ and $n \in N$. ...(2)

Let $n_1, n_2 \in N$. Then $n_2 \in N \Rightarrow n_2 \in G = HK$.

$\therefore \quad n_2 = h_2 k_2$ for some $h_2 \in H, k_2 \in K$.

We have $n_1 n_2 = n_1 (h_2 k_2) = (n_1 h_2) k_2$

$= (h_2 n_1) k_2$, by (1)

$= h_2 (n_1 k_2)$

$= h_2 (k_2 n_1)$, by (2)

$= (h_2 k_2) n_1 = n_2 n_1$

$\therefore \quad n_1 n_2 = n_2 n \; \forall \; n_1, n_2 \in N$.

Hence N is abelian.

Example 4.3.18. *Let G be a group and let $T = G \times G$.*

(a) Show that $D = \{(g, g) \in G \times G \mid g \in G\}$ is a group isomorphic to G.

(b) Prove that D is normal in T if and only if G is abelian.

Solution. (a) Let $\alpha, \beta \in D$ be arbitrary. Then

$\alpha = (x, x), \beta = (y, y)$ for some $x, y \in G$

$\Rightarrow \quad \alpha \beta^{-1} = (x, x)(y^{-1}, y^{-1}) = (xy^{-1}, xy^{-1}) \in D$, since $x y^{-1} \in G$.

Thus D is a subgroup of T. The mapping

$f : G \to D$ defined as

$f(g) = (g, g)$ for each $g \in G$

is clearly one-to-one, onto. Further f is a homomorphism, since

$f(g_1 g_2) = (g_1 g_2, g_1 g_2)$ for $g_1, g_2 \in G$

$= (g_1, g_1)(g_2, g_2) = f(g_1) f(g_2)$.

Hence $G \approx D$ or $D \approx G$.

(b) Now we show that

$D \lhd T \Leftrightarrow G$ is abelian.

Let $D \lhd T \Rightarrow tD = Dt \; \forall \; t \in T = G \times G$.

Let $x, y \in G$ be arbitrary. Then $(x, y) \in T$ and so

$(x, y)(y, y) \in (x, y) D = D (x, y)$

$\Rightarrow \quad (x, y)(y, y) = (z, z)(x, y)$ for some $(z, z) \in D$

$\Rightarrow \quad (xy, yy) = (zx, zy) \Rightarrow xy = zx$ and $yy = zy$

$\Rightarrow \quad xy = zx$ and $y = z$, by cancellation law in G

$\Rightarrow \quad xy = yx \; \forall \; x, y \in G$. Hence G is abelian.

Conversely, let G be abelian. Let $t \in T$ and $d \in D$ be arbitrary so that

$t = (g_1, g_2)$ and $d = (g, g)$ for $g, g_1, g_2 \in G$.

$\therefore \quad t d t^{-1} = (g_1, g_2)(g, g)(g_1^{-1}, g_2^{-1}) = (g_1 g g_1^{-1}, g_2 g g_2^{-1})$

$= (g_1 g_1^{-1} g, g_2 g_2^{-1} g)$, since G is abelian

$= (g, g) = d \in D$.

Thus $t d t^{-1} \in D \; \forall \; t \in T$ and $d \in D$ and so D is normal in T.

Example 4.3.19. *If N_1 is normal in G_1 and N_2 is normal in G_2, then show that*

(*i*) *$N_1 \times N_2$ is normal in $G_1 \times G_2$.*

(*ii*) $\dfrac{G_1 \times G_2}{N_1 \times N_2}$ *is isomorphic to* $\dfrac{G_1}{N_1} \times \dfrac{G_2}{N_2}$.

Solution. (*i*) If is easy to verify that $N_1 \times N_2$ is a subgroup of $G_1 \times G_2$. Let $G = G_1 \times G_2$, $N = N_1 \times N_2$.

Let $g \in G$ and $n \in N$ be arbitrary. Then

$g = (g_1, g_2)$ for some $g_1 \in G_1$ and $g_2 \in G_2$;

and $n = (n_1, n_2)$ for some $n_1 \in N_1$ and $n_2 \in N_2$.

Since $N_1 \lhd G_1$, $g_1 n_1 g_1^{-1} \in N_1$. Similarly, $g_2 n_2 g_2^{-1} \in N_2$.

We have $g\, n\, g^{-1} = (g_1, g_2)\,(n_1, n_2)\,(g_1^{-1}, g_2^{-1})$

$= (g_1 n_1 g_1^{-1},\ g_2 n_2 g_2^{-1}) \in N.$

Hence N is normal in G.

(*ii*) Define a mapping

$$\phi : G \to \frac{G_1}{N_1} \times \frac{G_2}{N_2} \text{ as}$$

$$\phi(g) = (N_1 g_1,\ N_2 g_2)\ \forall\ g = (g_1, g_2) \in G. \qquad \ldots(1)$$

Let $x, y \in G = G_1 \times G_2$ be arbitrary so that

$x = (x_1, x_2), y = (y_1, y_2)$; $x_1, y_1 \in G_1$ and $x_2, y_2 \in G_2$.

$\therefore$ $xy = (x_1 y_1, x_2 y_2)$ and so by (1), we have

$\phi(xy) = (N_1 x_1 y_1, N_2 x_2 y_2)$

$= (N_1 x_1\, N_1 y_1, N_2 x_2\, N_2 y_2)$, as $N_1 \lhd G_1$ and $N_2 \lhd G_2$

$= (N_1 x_1, N_2 x_2)\,(N_1 y_1, N_2 y_2)$

$= \phi(x)\,\phi(y)$, by (1).

Thus ϕ is a homomorphism. Also ϕ is onto, since for any

$(N_1 a_1, N_2 a_2) \in \dfrac{G_1}{N_1} \times \dfrac{G_2}{N_2}$; (1) yields

$\phi(a) = (N_1 a_1, N_2 a_2)$, where $a = (a_1, a_2) \in G$.

By Fundamental Theorem of Homomorphism, we have

$$\frac{G}{Ker\,\phi} \approx \frac{G_1}{N_1} \times \frac{G_2}{N_2}, \qquad \ldots(2)$$

where $Ker\,\phi = \{g \in G : \phi(g) = (N_1, N_2)\}$.

Notice that (N_1, N_2) is the identity of $\dfrac{G_1}{N_1} \times \dfrac{G_2}{N_2}$.

Now $g = (g_1, g_2) \in Ker\,\phi \Leftrightarrow (N_1 g_1, N_2 g_2) = (N_1, N_2)$, by (1)

$\Leftrightarrow N_1 g_1 = N_1$ and $N_2 g_2 = N_2$

$\Leftrightarrow g_1 \in N_1$ and $g_2 \in N_2$

$\Leftrightarrow g = (g_1, g_2) \in N_1 \times N_2 = N.$

$\therefore$ $Ker\ \phi = N$. Using in (2), we get

$\frac{G}{N} \approx \frac{G_1}{N_1} \times \frac{G_2}{N_2}$. Hence $\frac{G_1 \times G_2}{N_1 \times N_2} \approx \frac{G_1}{N_1} \times \frac{G_2}{N_2}$.

Example 4.3.20. (Chinese Remainder Theorem)

If m and n are relatively prime integers, and if a and b are any integers, show that there exists an integer x such that

$$x \equiv a \ (mod\ m) \text{ and } x \equiv b \ (mod\ n).$$

Solution. It is clear that

$$\mathbf{Z}_m = \{0, 1, 2, \ldots, m-1\} = \langle 1 \rangle$$

is a cyclic group w.r.t. addition modulo m.

Similarly, $\mathbf{Z}_n = \{0, 1, 2, \ldots, n-1\} = \langle 1 \rangle$

is also a cyclic group w.r.t. addition modulo n.

Since m and n are relatively prime integers,

$\mathbf{Z}_m \times \mathbf{Z}_n$ is a cyclic group. [See Example 4.3.8]

Indeed, $\mathbf{Z}_m \times \mathbf{Z}_n = \langle (1, 1) \rangle$.

By division algorithm, we have

$$a = m q_1 + r,\ 0 \le r < m \qquad \ldots(1)$$

and $$b = n q_2 + s,\ 0 \le s < n.$$

Clearly, $r \in \mathbf{Z}_m$ and $s \in \mathbf{Z}_n$

$\Rightarrow (r, s) \in \mathbf{Z}_m \times \mathbf{Z}_n = \langle (1, 1) \rangle$

$\Rightarrow$ $(r, s) = x\,(1, 1)$ for some integer x

$$= (1 \oplus_m \underset{x \text{ times}}{1 \oplus_m \ldots\ldots \oplus_m 1},\ 1 \oplus_n \underset{x \text{ times}}{1 \oplus_n \ldots\ldots \oplus_n 1})$$

$$= (x - mq_3, x - nq_4) \qquad \ldots(2)$$

$\therefore$ $r = x - mq_3$ and $s = x - nq_4$.

From (1) and (2), we have

$a = x + m\,(q_1 - q_3)$ and $b = x + n\,(q_2 - q_4)$

$\Rightarrow m \mid (a - x)$ and $n \mid (b - x)$ $\Rightarrow m \mid (x - a)$ and $n \mid (x - b)$.

Hence $x \equiv a \pmod m$ and $x \equiv b \pmod n$.

EXERCISES

1. If A and B are groups, prove that $A \times B$ isomorphic to $B \times A$.
   [Hint. Define $\phi : A \times B \to B \times A$ as
   $\phi(x) = (b, a)$, for all $x = (a, b) \in A \times B$.
   Show that ϕ is one-to-one, onto and homomorphism.]
2. Show that a cyclic group of order 6 is an internal direct product of two non-trivial subgroups.
   [Hint. See Example 4.3.2.]

3. Show that the group $Z/(10)$ is a direct sum of $H = \{0, 5\}$ and $K = \{0, 2, 4, 6, 8\}$.

[**Hint.** $Z/(10) = H \oplus K$, $H \cap K = \{0\}$ and H and K are normal in $Z/(10)$ ($\because$ $Z/(10)$ is abelian).]

4. If M and N are normal subgroups of a group G and if $M \cap N = (e)$, show that there is an isomorphism of G into $G/M \times G/N$.

[**Hint.** Similar to Example 4.3.12.]

5. Let G be a group and let $H = \{(g, g) : g \in G\}$. Show that H is a subgroup of $G \times G$ and H is normal in $G \times G$ if and only if G is abelian.

[**Hint.** See Example 4.3.18.]

6. Let G be a finite abelian group and let $H_1, H_2, \ldots, H_n$ be a finite number of subgroups of G such that $G = H_1 H_2 \ldots H_n$ and

$$o(G) = o(H_1)\, o(H_2) \ldots o(H_n),$$ prove that

$$G = H_1 \times H_2 \times \ldots \times H_n.$$

[**Hint.** See Example 4.3.7.]

7. If G is the internal direct product of its normal subgroups $N_1, N_2, \ldots, N_n$, show that

(*i*) $N_i \cap N_j = (e)$ for $i \neq j$

(*ii*) $ab = ba \; \forall \; a \in N_i$ and $b \in N_j$, $i \neq j$.

[**Hint.** By Theorem 4.3.2, $N_i \cap \left(\prod_{j \neq i} N_j \right) = (e)$.

For $j \neq i$, $N_i \cap N_j \subset N_i \cap \left(\prod_{j \neq i} N_j \right) = (e) \Rightarrow N_i \cap N_j = (e)$.

Since $N_i \lhd G$, $N_j \lhd G$ and $N_i \cap N_j = (e)$, therefore

$ab = ba \; \forall \; a \in N_i$ and $b \in N_j$ and $i \neq j$.]

8. Show that the multiplicative group $\mathbf{R}^*$ of non-zero real numbers is an internal direct product of two non-trivial subgroups.

[**Hint.** $\mathbf{R}^* = \mathbf{R}^+ \times \{1, -1\}$.]

9. Show that the group $(Z/(4), +)$ cannot be written as the direct sum of two subgroups of order 2.

[**Hint.** $G = Z/(4) = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ has only one subgroup of order 2 *viz.* $A = \{\bar{0}, \bar{2}\}$ and G is not the direct sum of A and A.]

10. Prove that the group $\mathbf{Q}$ of all rational numbers under addition cannot be written as a direct sum of two non-trivial subgroups.

11. If G is a finite group in which $x^2 = e$ for each $x \neq e$ in G, show that G is internal direct product of a finite number of subgroups each of order 2 and $o(G) = 2^n$.

[**Hint.** By the given hypothesis, G is abelian. Let $a_1 \neq e \in G$. If $G = \langle a_1 \rangle$, we are done. If $G \neq \langle a_1 \rangle$, then there exists $a_2 \in G$ such that $a_2 \notin \langle a_1 \rangle$. Then $\langle a_1 \rangle \times \langle a_2 \rangle$ is a direct product. If $G = \langle a_1 \rangle \times \langle a_2 \rangle$, we are done and $o(G) = 2^2$. Since G is finite, we have

$$G = \langle a_1 \rangle \times \langle a_2 \rangle \times \ldots \times \langle a_n \rangle,$$

where each $\langle a_i \rangle$ is a cyclic group of order 2 and $o(G) = 2^n$.

4.4 Finite Abelian Groups

In this section we shall discuss some important properties of finite abelian groups (without proofs). We have already proved one such property in Theorem 4.3.3. *viz.*,

A finite abelian group is a direct product of its Sylow subgroups.

The other properties are stated below :

Theorem 4.4.1. (Fundamental Theorem of Finite Abelian Groups) *Every finite abelian group G is the direct product of cyclic groups i.e.,*

$$G = A_1 \times A_2 \times \ldots \times A_n,$$

where each A_i is a cyclic group.

Theorem 4.4.2. *Let G be finite abelian group of order p^n, p being a prime. Let $G = A_1 \times A_2 \times \ldots \times A_k$, where each A_i is a cyclic group of order p^{n_i} and $n_1 \geq n_2 \geq \ldots \geq n_k > 0$.*

Then the integers $n_1, n_2, \ldots, n_k$ are uniquely determined, called the **invariants** *of G.*

Remark 1. *The decomposition of an abelian group G of order p^n (p a prime) into a direct product of cyclic groups is* **not** *unique. However, their orders are unique.*

For example, consider the Klein 4-group *viz.*

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

Then G is abelian and $G = A \times B$, where $A = \{a, a^2 = e\}$, $B = \{b, b^2 = e\}$ are cyclic groups each of order 2.

Also $G = C \times B$, whose $C = \{ab, (ab)^2 = e\}$, $B = \langle b \rangle$

Notice that $(ab)^2 = abab = aabb = a^2 b^2 = e$.

Thus we see that the cyclic groups in the two distinct decompositions of G (as direct products of cyclic groups) *are* **not** *unique, but their orders are unique*, as

$$o(A) = o(B) = o(C) = 2.$$

Remark 2. *The invariants of a finite abelian group of order p^n determine a partition of n as shown below :*

If $G = A_1 \times A_2 \times \ldots \times A_k$, where each A_i is a cyclic group of order p^{n_i}, $n_1 \geq n_2 \geq \ldots \geq n_k > 0$, then $o(G) = o(A_1)\, o(A_2) \ldots o(A_k)$

or $$p^n = p^{n_1}\, p^{n_2} \ldots p^{n_k} = p^{n_1 + n_2 + \ldots + n_k}.$$

Hence $n = n_1 + n_2 + \ldots + n_k$ determines a partition of n.

Theorem 4.4.3. *Two abelian groups of order p^n are isomorphic if and only if they have the same invariants.*

Theorem 4.4.4. (*a*) *The number of non-isomorphic abelian groups of order p^n (p being prime) is $p(n)$, where $p(n)$ denotes the number of partitions of n.*

(*b*) *The number of non-isomorphic abelian groups of order $n = p_1^{\alpha_1}\, p_2^{\alpha_2} \ldots p_r^{p_r}$ is $p(\alpha_1)\, p(\alpha_2) \ldots p(\alpha_r)$.*

The proofs of these theorems are omitted.

Remark. *The result of Theorem 4.4.4 (a) does* **not** *depend on the prime p ; it only depends on the exponent n.* Consequently, the number of non-isomorphic abelian groups of order 2^4 or 3^4 or p^4 (for any prime p) is $p(4)$.

Various partitions of 4 are

$$4 = 4, \quad 4 = 3 + 1, \quad 4 = 2 + 2, \quad 4 = 2 + 1 + 1, \quad 4 = 1 + 1 + 1 + 1$$

$\therefore \quad p(4) = 5.$

Hence there are five non-isomorphic abelian groups of order p^4 for any prime p.

Ex. 1. *State a few important properties of an abelian group of order p^n, p a prime. Find out the number of non-isomorphic abelian groups of orders p^3, p^4 and p^5.* **[Ans.** 3, 5, 7]

Ex. 2. *Define the invariants of an abelian group of order p^n, p a prime. Find the invariants of abelian groups of orders (i) 144, (ii) 360, (iii) 720.*

[Hint. (*iii*) $720 = 2^4 \times 3^2 \times 5^1$.]

[Ans. (*i*) 4, 2 ; (*ii*) 3, 2, 1 ; (*iii*) 4, 2, 1.]

Note. *In the following Examples, $\mathbf{Z}_n$ denotes the group of integers under multiplication modulo n.*

EXAMPLES

Example 4.4.1. *Find all the non-isomorphic abelian groups of order 8.*

Solution. We have $8 = 2^3$ ($p = 2, n = 3$). By Theorem 4.4.4 (*a*), the number of non-isomorphic abelian groups of order 2^3 is $p(3)$. Various partitions of 3 are

$$3 = 1 + 1 + 1, \quad 3 = 1 + 2, \quad 3 = 3.$$

$\therefore \quad p(3) = 3.$

Hence there are 3 non-isomorphic abelian groups of order 8 *viz.*

$$\mathbf{Z}_8,\ \mathbf{Z}_2 \times \mathbf{Z}_4 \text{ and } \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2.$$

Example 4.4.2. *Find all the non-isomorphic abelian groups of order 9.*

Solution. Since $9 = 3^2$ ($p = 3, n = 2$), the number of non-isomorphic abelian groups of order 3^2 is $p(2) = 2$ ($\because 2 = 1 + 1, \ 2 = 2$). Hence there are two non-isomorphic abelian groups of order 9 *viz.* Z_9 and $Z_3 \times Z_3$.

Example 4.4.3. *Find all the non-isomorphic abelian groups of order 15.*

Solution. We have $15 = 3^1 \times 5^1$ ($p_1 = 3, \ p_2 = 5, \alpha_1 = 1, \ \alpha_2 = 1$).

Hence the number of non-isomorphic abelian groups of order 15 is

$$p(\alpha_1)\, p(\alpha_2) = p(1) \times p(1) = 1 \times 1 = 1.$$

Hence there is only one non-isomorphic abelian group of order 15 *viz.* Z_{15}.

Example 4.4.4. *Find all the non-isomorphic abelian groups of order 6.*

[**Hint.** Similar to Example 4.4.3.] **[Ans.** Z_6**]**

Example 4.4.5. *Describe all non-isomorphic abelian groups of order 16.*

Solution. Since $16 = 2^4$, there are $p(4) = 5$ non-isomorphic abelian groups of order 16. These are

$$Z_{16}, \ Z_8 \times Z_2, \ Z_4 \times Z_4, \ Z_4 \times Z_2 \times Z_2, \ Z_2 \times Z_2 \times Z_2 \times Z_2.$$

Example 4.4.6. *Describe all non-isomorphic abelian groups of order 2^6.*

[**Hint.** Similar to Example 4.4.5. Also $p(6) = 11$.]

Example 4.4.7. *Find all non-isomorphic abelian groups of order 20.*

Solution. Since $20 = 2^2 \times 5^1$, the number of non-isomorphic abelian groups of order 20 is

$$p(2) \times p(1) = 2 \times 1 = 2.$$

These are $Z_4 \times Z_5$ and $Z_2 \times Z_2 \times Z_5$.

Example 4.4.8. *Find all non-isomorphic abelian groups of order 12.*

[Ans. $Z_4 \times Z_3, \ Z_2 \times Z_2 \times Z_3$**]**

Example 4.4.9. *Find all non-isomorphic abelian groups of order 24.*

[Ans. $Z_8 \times Z_3, \ Z_2 \times Z_4 \times Z_3, \ Z_2 \times Z_2 \times Z_2 \times Z_3$**]**

Example 4.4.10. *Find all the non-isomorphic abelian groups of order 360.*

Solution. We have $360 = 2^3 \cdot 3^2 \cdot 5^1$.

Hence the number of non-isomorphic abelian groups of order 360 is

$$p(3)\, p(2)\, p(1) = 3 \times 2 \times 1 = 6.$$

Hence there are six non-isomorphic abelian groups of order 360 *viz.*

$$Z_8 \times Z_9 \times Z_5,$$
$$Z_8 \times Z_3 \times Z_3 \times Z_5,$$
$$Z_2 \times Z_4 \times Z_9 \times Z_5,$$
$$Z_2 \times Z_4 \times Z_3 \times Z_3 \times Z_5,$$
$$Z_2 \times Z_2 \times Z_2 \times Z_9 \times Z_5,$$
$$Z_2 \times Z_2 \times Z_2 \times Z_3 \times Z_3 \times Z_5.$$

4.5 Survey of Groups of Orders 6 and 8

Example 4.5.1. *Prove that an abelian groups G of order 6 is cyclic.* [D.U., 1998, 94]

Solution. $o(G) = 6 = 2^1 \times 3^1$.

The number of non-isomorphic abelian groups of order 6 is

$$p(1) \times p(1) = 1 \times 1 = 1.$$

It follows that there is exactly one non-isomorphic abelian group of order 6 *viz.* $\mathbf{Z}_6$, which is cyclic.

Hence $G = \mathbf{Z}_6$ is cyclic.

Note. For an independent proof, see Example 3.4.10 of Chapter 3.

Example 4.5.2. *Find all non-abelian groups of order 6.*

Solution. Let G be a non-abelian group of order 6. By Lagrange's theorem,

$$o(a) \mid o(G) = 6 \ \forall\ a \in G.$$

$$\therefore \quad o(a) = 2, 3 \text{ or } 6 \ \forall\ a \neq e \in G.$$

If $o(a) = 6$ for some $a \neq e \in G$, then $G = \langle a \rangle$, $a^6 = e$ is cyclic and so abelian, a contradiction. Thus G contains no element of order 6.

In each element of G is order 2, then G is abelian, which is again a contradiction. Hence we can find two elements a, b in G such that $o(a) = 3$ and $o(b) = 2$.

Let $H = \{a, a^2, a^3 = e\}$ so that $o(H) = 3$.

$$\Rightarrow \quad i_G(H) = \frac{o(G)}{o(H)} = \frac{6}{3} = 2$$

$\Rightarrow$ H is normal in G.

If $b \in H$, then $o(b) \mid o(H)$ *i.e.*, $2 \mid 3$, a contradiction.

$\therefore$ $b \notin H$

Since $i_G(H) = 2$ and $b \notin H$, we have

$$G = H \cup Hb = \{e, a, a^2, b, ab, a^2b\}.$$

Since $H \lhd G, b^{-1}ab \in H$ ($\because$ $a \in H$ and $b \in G$)

$\Rightarrow$ $b^{-1}ab = e$ or a or a^2.

Now $b^{-1}ab = e \Rightarrow ab = b \Rightarrow a = e$, a contradiction.

$b^{-1}ab = a \Rightarrow ab = ba \Rightarrow G$ is abelian, a contradiction.

$\therefore$ $b^{-1}ab = a^2 = a^{-1}$.

Hence there is only one non-abelian group G of order 6 *viz.*

$G = \{e, a, a^2, b, ab, a^2b\}$, where

$a^3 = e = b^2, b^{-1}ab = a^{-1}$.

Example 4.5.3. *Show that a non-abelian group of order 6 is isomorphic to S_3.* [D.U., 1995]

Solution. Refer to Example 4.5.2.

There is only one non-abelian group G of order 6 *viz.*

$$G = \{e, a, a^2, b, ab, a^2b\}, \text{ where}$$
$$a^3 = e = b^2, b^{-1} a b = a^{-1}.$$

We know

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

Define a mapping $\phi : G \to S_3$ as

$$\phi(e) = I, \phi(a) = (123), \phi(a^2) = (132),$$
$$\phi(b) = (12), \phi(ab) = (13), \phi(a^2b) = (23).$$

Clearly, ϕ is one-to-one and onto.

It can be verified that ϕ is a homomorphism.

[For example, $\phi(a^2 . a^2 b) = \phi(ab) = (13), \quad (\because a^3 = e)$

$\phi(a^2)\,\phi(a^2b) = (132)(23) = (13)$ and so

$\phi(a^2 . a^2b) = \phi(a^2)\,\phi(a^2b)$ etc. etc.]

Hence $G \approx S_3$.

Example 4.5.4. *Verify that a group G of order 6 is either cyclic or isomorphic to S_3.*

Solution. Refer to Examples 4.5.1 and 4.5.3. We have

$$G = \mathbf{Z}_6 \text{ (cyclic)} \quad \text{or} \quad G \approx S_3$$

according as G is abelian or non-abelian.

Example 4.5.5. *Find all abelian groups of order 8.*

Solution. Refer to Example 4.4.1.

All non-isomorphic abelian groups of order 8 are

$$\mathbf{Z}_8, \mathbf{Z}_2 \times \mathbf{Z}_4 \quad \text{and} \quad \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2.$$

Example 4.5.6. *Find all non-abelian groups of order 8.* [D.U., 1996]

Solution. Let G be a non-abelian group of order 8. By Lagrange's Theorem,

$$o(a) \mid o(G) = 8 \;\forall\; a \in G.$$

$\therefore$ $\quad o(a) = 2, 4 \text{ or } 8 \;\forall\; a \neq e \in G.$

If $o(a) = 8$, then $G = \langle a \rangle$, $a^8 = e$, is cyclic and so abelian, a contradiction.

Thus G has no element of order 8.

If each element of G is of order 2, then G is abelian, again a contradiction.

Thus G contains an element a of order 4.

Let $\quad H = \{a, a^2, a^3, a^4 = e\}, o(H) = 4$

$$\Rightarrow \quad i_G(H) = \frac{o(G)}{o(H)} = \frac{8}{4} = 2$$

$\Rightarrow H$ is normal in G.

Let $b \in G$ such that $b \notin H$. Then

$$G = H \cup Hb = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}.$$

It follows that $b^2 \in H$, for if $b^2 \notin H$; then H, Hb, Hb^2 are distinct right cosets of H in G, a contradiction.

Now $b^2 \in H \Rightarrow b^2 = e, a, a^2$ or a^3.

If $b^2 = a$, then $b^4 = a^2$, $b^6 = a^3$, $b^8 = e$

$b^5 = a^2b \neq e$, $b^7 = a^3b \neq e$.

Thus $o(b) = 8$, a contradiction.

Similarly, $b^2 = a^3 \Rightarrow b^2 = a^{-1} \Rightarrow o(b^2) = o(a^{-1}) = o(a) = 4$

$\Rightarrow o(b) = 8$, a contradiction.

$\therefore$ $\boldsymbol{b^2 = e}$ **or** $\boldsymbol{a^2}$. ...(1)

Since H is normal in G, $b^{-1}ab \in H$ $(\because a \in H, b \in G)$

and $o(b^{-1}ab) = o(a) = 4$.

$\therefore$ $b^{-1}ab = a$ or a^2 or a^3.

Let $b^{-1}ab = a^2 \Rightarrow o(b^{-1}ab) = 2$, a contradiction.

Let $b^{-1}ab = a \Rightarrow ab = ba \Rightarrow G$ is abelian, a contradiction.

$\therefore$ $\boldsymbol{b^{-1}ab = a^3}$. ...(2)

In view of the relations (1) and (2), *there exist only two non-abelian groups of order 8 viz.*

(*i*) $G = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, where

$a^4 = e$, $b^2 = e$, $b^{-1}ab = a^3$.

(*ii*) $G = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, where

$a^4 = e$, $b^2 = a^2$, $b^{-1}ab = a^3$.

The first group is the *Dihedral group* of order 8, and the second is the *Quaternion group* of order 8.

Ex. 1. *Write a short note on groups of order 6.*

Ex. 2. *Write a short note on groups of order 8.*

Ex. 3. *Give a survey of groups upto order 8.*

Hint. Group of order 1 is (e). Groups of order 2, 3, 5 and 7 are cyclic and any two cyclic groups of the same order are isomorphic. Hence (upto isomorphism) there exists exactly one cyclic group each of order 2, 3, 5 and 7 *viz.* C_2, C_3, C_5 and C_7. Groups of order 4 $(p^2, p = 2)$ are necessarily abelian *e.g.*, Klein 4-group. Groups of orders 6 and 8 have been discussed above.

Appendix

Additional Problems on Different Topics of Groups

1 Groups of Symmetries :

Let us consider all possible movements of the square with vertices A,B,C,D. The final position of the square can be obtained from the original position by the rotation of the square about the axis through the centre, perpendicular to the plane, through an angle of 90° anticlockwise. Let the plane of the square be horizontal (fig 1.1).

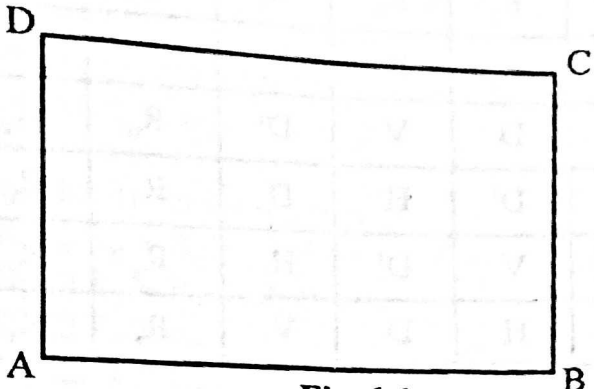

Fig. 1.1

The possible motions can be explained as following :

(i) R_0 = Rotation of 0° about Vertical axis in the plane of the square.

(ii) R_1 = Rotation of one right angle anticlockwise about the vertical axis perpendicular to the plane.

(iii) R_2 = Rotation of two right angles anticlockwise, about the vertical axis perpendicular to the plane of the square.

(iv) R_3 = Rotation of three right angles anticlockwise, about the vertical axis perpendicular to the plane of the square.

(v) H = Rotation of 180° anticlockwise about horizontal axis in the plane of the square.

(vi) V = Rotation of 180° anticlockwise about vertical axis in the plane of the square.

(vii) D = Rotation of 180° anticlockwise about the main diagonal

(viii) D' = Rotation of 180° anticlockwise about the other diagonal.

Two motions are equivalent if their net effect is same.

It can be shown that all above eight motions of a square form a group of symmetries and denoted by D_8. The set of motions of a square hence is given by–

$$D_8 = \{R_0, R_1, R_2, R_3, H, V, D, D'\}.$$

D_8 is called the dihedral group of order 8.

Example 1.1 *Let* $D_8 = \{R_0, R_1, R_2, R_3, H, V, D, D'\}$ *with a binary composition as for all* $x, y \in D_8$. $(xy)\,\square = x\,(y\,\square)$.

Where x □ stands for the effect of 'x' on the square ABCD. Prove that D_8 is a group. Is D_8 abelian?

Sol. The composition table of D_8 is as follow :

□	R_0	R_1	R_2	R_3	H	V	D	D^1
R_0	R_0	R_1	R_2	R_3	H	V	D	D^1
R_1	R_1	R_2	R_3	R_0	D^1	D	H	V
R_2	R_2	R_3	R_0	R_1	V	H	D^1	D
R_3	R_3	R_0	R_1	R_2	D	D^1	V	H
H	H	D	V	D^1	R_0	R_2	R_1	R_3
V	V	D^1	H	D	R_2	R_0	R_3	R_1
D	D	V	D^1	H	R_3	R_1	R_0	R_2
D^1	D^1	H	D	V	R_1	R_3	R_2	R_0

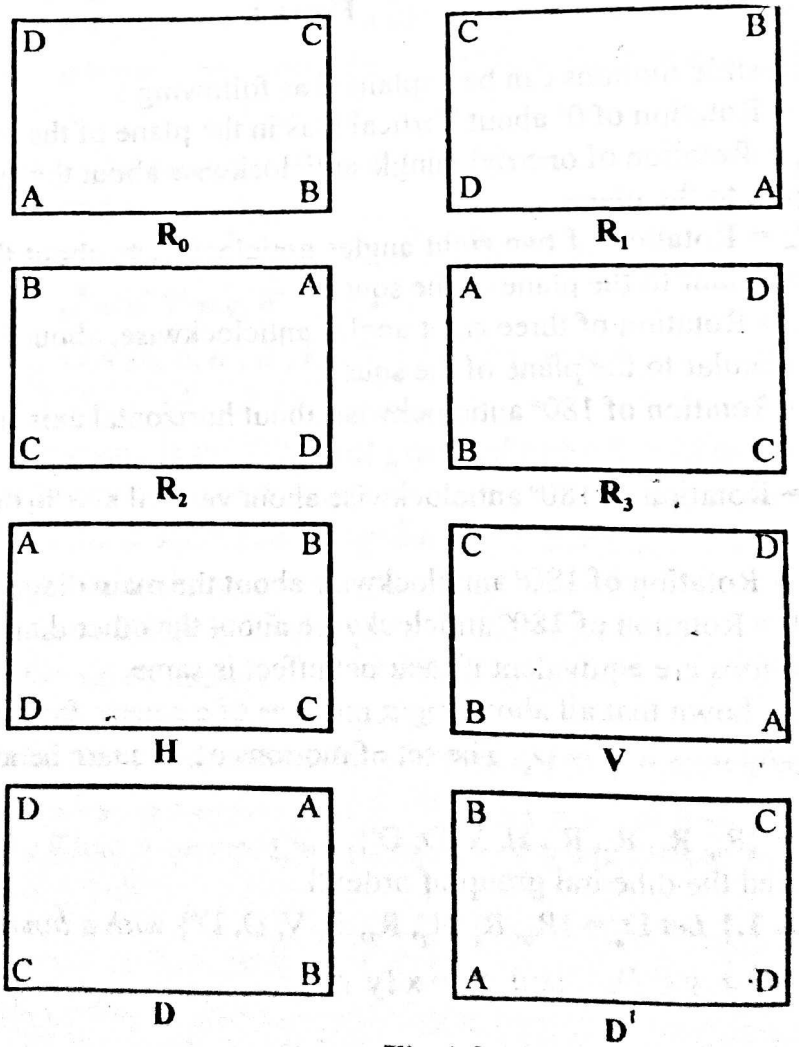

Fig 1.2

From the composition table we observe the following properties–

(i) **Closure properly :** All the entries in the composition table are elements of set D_8, therefore closure properly is verified.

(ii) **Associative property :** Eight motions describe in fig. 1.2 are mappings of {A, B, C, D} onto itself, and the operation is the compositions of mappings. Since the composition of mapping is associative, therefore

$$x \square (y \square z) = (x \square y) \square z \text{ for all } x, y, z \in D_8.$$

(iii) **Existence of identity :**

Since for all $x \in D_8$, $x \square R_0 = R_0 \square x = x$

Therefore R_0 is identity of D_8.

(iv) **Existence of inverse :**

From the composition table we see that

$$R_0 \square R_0 = R_0$$
$$R_1 \square R_3 = R_3 \square R_1 = R_0$$
$$R_2 \square R_2 = R_0$$
$$H \square H = R_0$$
$$V \square V = R_0$$
$$D \square D = R_0$$
$$D^1 \square D^1 = R_0$$

i.e. R_0, R_2, H, V, D and D^1 are their own inverses, while R_1 and R_3 are inverses of each other.

Since under the given binary composition the given set D_8 satisfies all the four required properties to be a group. Therefore D_8 is a group.

Now,

(v) **Commutative property :**

Since, we observe that

$$R_1 \square V = D$$

&

$$V \square R_1 = D^1,$$

so that $R_1 \square V \neq V \square R_1$.

Thus the binary composition is not commutative on D_8.

Hence the set D_8 under given composition is not an abelian group.

2. Symmetries of Non-square Rectangle :

Let we consider a rectangle ABCD with a centre 0.

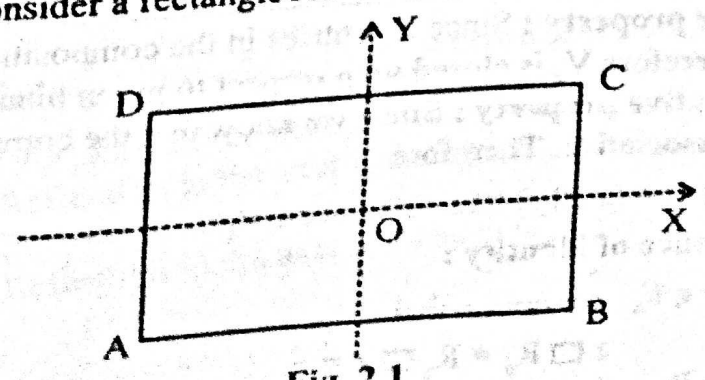

Fig. 2.1

R_0 = Rotation through 0°.

R_1 = rotation through 180° anticlockwise about the line through O perpendicular to the plane of rectangle.

H = Reflection in OX, or a rotation through 180° about OX in space.

V = Reflection in OY, or a rotation through 180° about OY in space.

Example 2.1 *Let $V_4 = \{R_0, R_1, H, V\}$ with binary composition of motions of non-square rectangle. Prove that V_4 is a group. Is V_4 an abelian group?*

Sol.

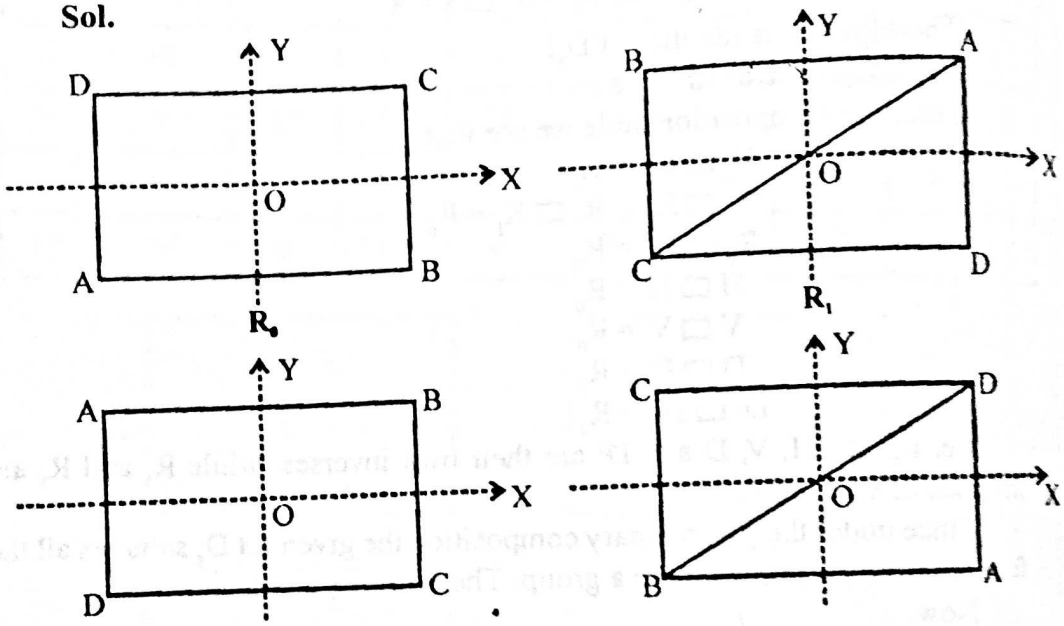

Fig. 2.2

Composition Table :

□	R_0	R_1	H	V
R_0	R_0	R_1	H	V
R_1	R_1	R_0	V	H
H	H	V	R_0	R_1
V	V	H	R_1	R_0

(i) Closure property : Since all entries in the composition table are elements of V_4, therefore V_4 is closed with respect to given binary composition.

(ii) Associative property : Since we know that the composition of mappings always associative. Therefore

$$x \square (y \square z) = (x \square y) \square z, \ \forall\, x, y, z \in V_4$$

(iii) Existence of identity :

Since $\forall\, x \in V_4$, we notice that

$$x \square R_0 = R_0 \square x = x.$$

Therefore R_0 is the identity element of V_4.

(iv) **Existence of inverse :**

From the composition table, we see that

$$R_1 \square R_1 = R_1$$
$$R_2 \square R_2 = R_2$$
$$H \square H = R_3$$
$$V \square V = R_4$$

Therefore all the elements of V_4 are self inverse.

(v) **Commutative property :**

From the composition table we see that

First row = first column

Second = Second column

third row = third column

fourth row = fourth column

therefore V_4 is commutative.

3. **: Symmetries of equilateral triagle :**

Let ABC be an equilateral triangle with centre O.

consider the following motions :

R_1 = Rotation about the (axis x–1) centre through O.

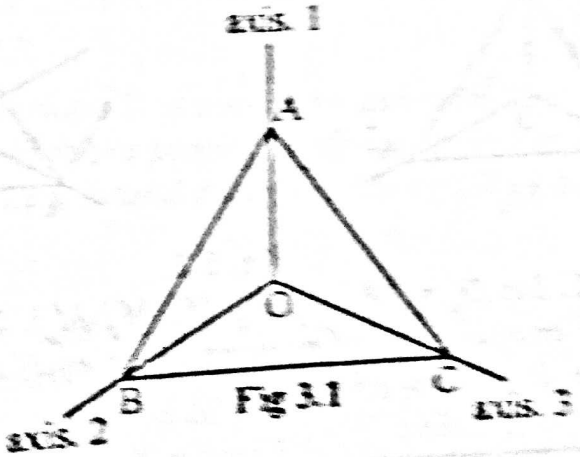

Fig 3.1

R_1 : Rotation through $\frac{2\pi}{3}$ anticlockwise about the line through O perpendicular to the plane of the triangle.

R_2 : Rotation through $\frac{4\pi}{3}$ anticlockwise about the line through O perpendicular to the plane of the triangle.

M_1 : Reflection in the axis 1, through A.

M_2 : Reflection in the axis 2, through B.

M_3 : Reflection in the axis 3, through C.

(iv) **Existence of inverse :**

From the composition table, we see that

$$R_0 \square R_0 = R_0$$
$$R_1 \square R_1 = R_0$$
$$H \square H = R_0$$
$$V \square V = R_0$$

Therefore all the elements of V_4 are self inverse.

(v) **Commutative property :**

From the composition table we see that

First row = first column

Second = Second column

third row = third column

fourth row = fourth column

therefore V_4 is commutative.

3. **: Symmetries of equilateral triagle :**

Let ABC be an equilateral triangle with centre O.

consider the following motions :

R_0 = Rotation about the (axis x–1) centre through O.

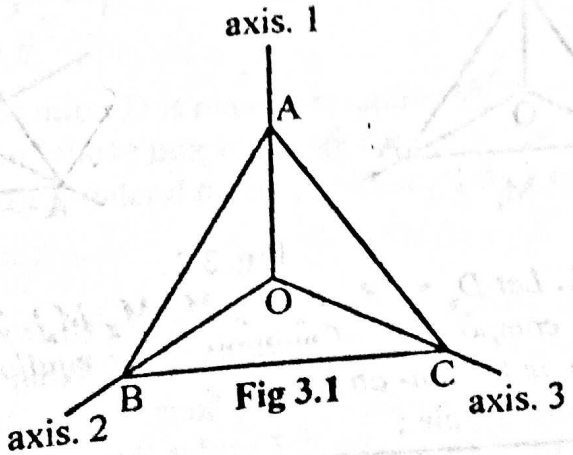

Fig 3.1

R_1 : Rotation through $\frac{2\pi}{3}$ anticlockwise about the line through O perpendicular to the plane of the triangle.

R_2 : Rotation through $\frac{4\pi}{3}$ anticlockwise about the line through O perpendicular to the plane of the triangle.

M_1 : Reflection in the axis 1, through A.

M_2 : Reflection in the axis 2, through B.

M_3 : Reflection in the axis 3, through C.

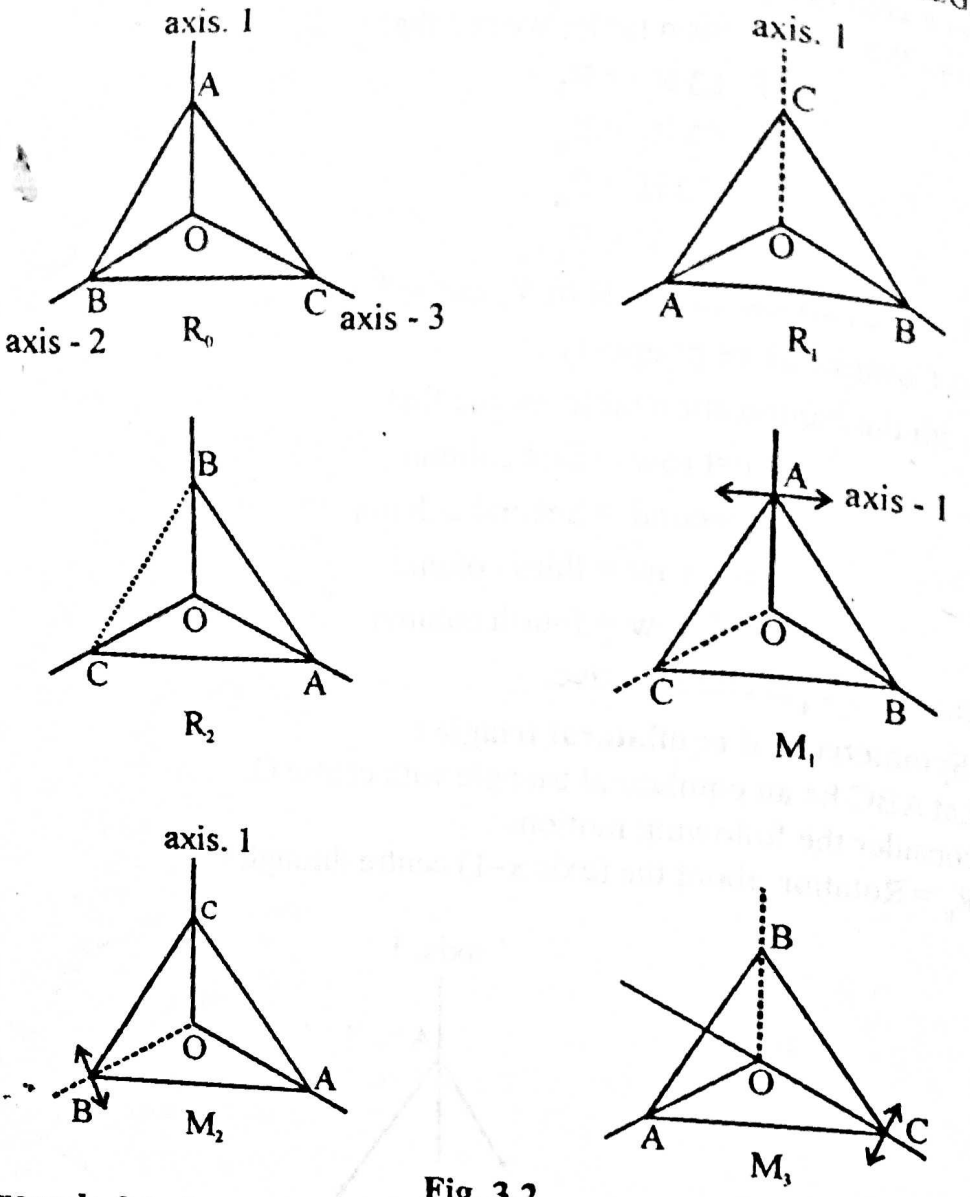

Fig. 3.2.

Example 3.1. *Let* $D_6 = \{R_0, R_1, R_2, M_1, M_2, M_3\}$. *The binary operation considered is the composition of motions of an equilateral triangle. Prove that* D_6 *is a group. Is* D_6 *non- abelion?*

Sol. Composition table :

Δ	R_0	R_1	R_2	M_1	M_2	M_3
R_0	R_0	R_1	R_2	M_1	M_2	M_3
R_1	R_1	R_2	R_0	M_3	M_1	M_2
R_2	R_2	R_0	R_1	R_2	M_3	M_1
M_2	M_2	M_3	M_1	R_2	R_0	R_1
M_3	M_3	M_1	M_2	R_1	R_2	R_0

From the composition table we can verify–

(i) Closure property : Since all entries in the composition table are elements of the set D_6, therefore closure property is verified.

i.e. $x \Delta y \in D_6 \ \forall \ x, y \in D_6$

(ii) **Associative property :** Since we observe that the six motions described above are mapping of {A, B, C} onto itself and the operation is composition of mappings. Therefore D_6 is associative.

(iii) **Existence of identity :** from the composition table we observe that

$$\forall\, x \in D_6,\ x \Delta R_0 = R_0 \Delta x = x.$$

Therefore R_0 is identity.

(iv) Existence of inverse :

From the composition table we observe that

$$R_0 \Delta R_0 = R_0$$
$$R_1 \Delta R_2 = R_2 \Delta R_1 = R_1$$
$$M_1 \Delta M_1 = R_0$$
$$M_2 \Delta M_2 = R_0$$
$$M_3 \Delta M_3 = R_0$$

i.e. R_0, M_1, M_2, M_3 are self inverses while R_1 and R_2 are inverses to each other.

(v) **Commutative property :**

From the table it is clear that

$$R_2 \Delta M_1 = M_3$$

& $$M_1 \Delta R_2 = M_2$$

so that $R_2 \Delta M \neq M_1 \Delta R_2$

Thus, the binary composition D is not commutative on D_6.

Therefore on the basis of above properties we conclude that D_6 is a group with respect to motion of an equilateral triangle. Although D_6 is not an abelian group.

4. Simple Linear Groups : The set of all 2X2 matrices with determinant 1 entries from Q (rationals), R (reals), C (complex numbers), or Zp (p a prime) is called a special linear group of 2 X 2 matrices over Q, R, C or Zp respectively. If the entries are from F, where F is any of the aobve, we denote this group by SL(2, F).

e.g. (i) $SL(2, Q) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : ad - bc = 1,\ \forall\, a,b,c,d \in Q \right\}$

(ii) $SL(2, R) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : ad - bc = 1,\ \forall\, a,b,c,d \in R \right\}$

(iii) $SL(2, C) = \left\{ \begin{bmatrix} a+ib & c+id \\ e+if & g+ih \end{bmatrix} : (a+ib)(g+ih) - (c+if)(c+id) = 1,\ \forall a,b,c,d \in R \right\}.$

(iv) $SL(2, Zp) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : ad - bc = 1, \forall a,b,c,d \in Z_p \right\}$

Example 4.1. *Prove that* $SL(2, Q) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : ad - bc = 1, \forall a,b,c,d \in Q \right\}$. *Now to discuss that SL(2, Q) is a group we need the following properties-*

(i) **Closure property :**

Let $$A = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} : a_1 d_1 - b_1 c_1 = 1$$

and $$B = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} : a_2 d_2 - b_2 c_2 = 1$$

are any two arbitrary elements of SL(2, Q).

Then $$AB = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$$

$$= \begin{bmatrix} a_1 a_2 + b_1 c_2 & a_1 b_2 + b_1 d_2 \\ c_1 a_2 + d_1 c_2 & c_1 b_2 + d_1 d_2 \end{bmatrix} \in SL(2,Q)$$

Notice that

$$|AB| = |A| \, . \, |B| = 1.1 = 1$$

Therefore $AB \in SL(2, Q)$

(ii) **Associative property :** Since multiplication of matrices is associative, therefore associative property is verified.

i.e. $A(BC) = (AB)\, C \;\forall\; A, B, C \in SL(2,Q)$.

(iii) **Existence of identity :**

Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} : ad - bc = 1 \in SL(2,Q)$.

be an arbitrary,

and $$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in SL(2,Q).$$

then $$AI = IA = A \in SL(2,Q)$$

Since A is arbitrary, therefore $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is the identity of SL (2, Q).

(iv) Existence of inverse :

Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, and $B = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$

thus $A \in SL(2,Q)$ if $ad - bc = 1$

and $B \in SL(2,Q)$ if $ad - bc = 1$

Now $$AB = \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

$$= \begin{bmatrix} ad - bc & -ab + ba \\ cd - cd & -bc + ad \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$= I$$

Also $$BA = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

$$= \begin{bmatrix} ad - bc & bd - bd \\ -ac + ac & -bc + ad \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$= I$$

Therefore $\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$ is the inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ since $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is an arbitrary element of SL(2, Q), therefore we can obtain inverse in the same manner for every element of SL (2, Q).

(v) **Commutative property :**

We know that for any $A, B \in SL(2,Q)$

$$|A| = 1 \ , \ |B| = 1$$

Therefore by the property of non singular matrices

$$|AB| = |A| \, . \, |B| = |B| \, . \, |A| = |BA|$$

But $|AB| = |BA|$ does not imply $AB = BA$.

e.g. if $$AB = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \& \ BA = \begin{bmatrix} x & y \\ z & t \end{bmatrix}.$$

Thus $AB = BA$ means $a = x, \ b = y, \ c = z, \ d = t.$

Which is not necessary for every $A, B, \in SL(2, Q)$.

Hence, SL (2, Q) is a group with respect to multiplication of matrices but SL(2, Q) is not an abelian group.

Example 4.2. *Show that* $SL(2, Z_p) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : ad - bc = 1, \right.$ $\left. \forall\ a,b,c,d \in Z_p \right\}$ *is a group. Is* $SL(2, Z_p)$ *is abelian group?*

Sol. Closure property :

Let $$A = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} : a_1 d_1 - b_1 c_1 = 1, a_1, b_1, c_1, d_1 \in Z_p$$

$$B = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} : a_2 d_2 - b_2 c_2 = 1, a_2, b_2, c_2, d_1 \in Z_p$$

Then $$AB = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$$

$$= \begin{bmatrix} a_1 a_2 + b_1 c_2 & a_1 b_2 + b_1 d_2 \\ c_1 a_2 + d_1 c_2 & c_1 d_2 + d_1 d_2 \end{bmatrix}$$

Where all $a_1 a_2 + b_1 c_2, a_1 b_2 + b_1 d_2$ etc. are under modulop.

Further from the property of matrices multiplication and determinant

$$|AB| = |A| \,.\, |B| = 1.1 = 1.$$

Therefore $AB \in SL(2, Z_p)$.

(ii) Associative property : The multiplication of matrices is always associative.

Therefore $A(BC) = (AB)C \forall A, B, C \in SL(2, Z_p)$

(iii) Existence of identity :

Let $$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL(2, Z_p)$$

with $ad - bc = 1$ SL (2, Zp)

as both $|I| = 1$ and $0, 1 \in Z_p$

Now $AI = IA = A$

Since A is arbitrary so that is true for all A.

i.e. $$AI = IA = A \ \forall\ A \in SL(2, Z_p).$$

(iv) **Existence of inverse :**

Let $$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL(2, Z_p)$$

and $$B = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \in SL(2, Z_p)$$

When matrix entries are from Z_p, we use modulo p arithmatic to compute determinants, matrix products, and inverses.

To illustrate the case $SL(2, Z_5)$, consider the element $A = \begin{bmatrix} 3 & 4 \\ 4 & 4 \end{bmatrix}$.

$|A| = -4 = 1 \bmod 5$, and inverse of A is $\frac{1}{2}\begin{bmatrix} +4 & -4 \\ -4 & 3 \end{bmatrix}$.

where $-\frac{1}{4}\begin{bmatrix} -4 & -4 \\ -4 & 3 \end{bmatrix} = \begin{bmatrix} 4 & 1 \\ 1 & 3 \end{bmatrix}$.

Note that $\begin{bmatrix} 3 & 4 \\ 4 & 4 \end{bmatrix}\begin{bmatrix} 4 & 1 \\ 1 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

when the arithmatic modulo 5 is done.

(v) **Commutative property :** The commutative property does not hold in SL(2, Zp) as |AB| = |BA| does not implies that AB = BA under modulo 5 for both addition and multiplication.

Hence SL(2, Zp) is a non abeliang group.

Example 4.3. *Show that* $SL(2, R) = \left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} : ad - bc = 1, \forall\, a,b,c,d \in R\right\}$ *is a group. Is SL(2, R) an abelian group?*

Sol. To show that SL(2, R) is a group with respect to multiplication of matrices we need the following properties

(i) **Closure property :**

Let $$A = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \& B = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} \in SL(2, R)$$

Thus $a_1 d_1 - b_1 c_1 = 1 \;\&\; a_2 d_2 - b_2 c_2 = 1$

i.e. A and B are non singular.

$\therefore$ $|AB| = |A| \,.\, |B| = 1.1 = 1$

So $AB \in SL(2, R)$ and therefore

$AB \in SL(2, R) \;\forall\; A, B \in SL(2, R)$

(ii) Associative property : The multiplication of matrices is always associative i.e. $A(BC) = (AB)C \ \forall \ A, B, C \in SL(2, R)$

(iii) Existence of identity :

Let $$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in SL(2, R)$$

Thus for every $$A = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \in SL(2, R)$$

$$AI = IA = A.$$

Therefore I is identity of $SL(2, R)$.

(iv) **Existence inverse :**

Let $$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL(2, R)$$

& $$B = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \in SL(2, R)$$

Now $$AB = \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \begin{bmatrix} ad - bc & -ab + ba \\ cd - cd & -bc + ad \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

$$BA = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

$$= \begin{bmatrix} ad - bc & bd - bd \\ -ac + ac & -bc + ad \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$= I$$

Therefore $\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$ is the inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$. Since $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is an arbitrary element of SL(2, R), therefore we can obtain inverse in the same manner for every element of SL(2, R).

Since all the required property of a group are satisfied, therefore $SL(2, R)$ is a group with respect to multiplication of matrices. However SL(2, R) is not an abelian group as the commutative property is not satisfied.

Since, $|AB| = |BA|$ does not implies that $AB = BA$.

(ii) Associative property : The multiplication of matrices is always associative. i.e. $A(BC) = (AB)C \ \forall \ A, B, C \in SL(2, R)$

(iii) Existence of identity :

Let $$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in SL(2, R)$$

Thus for every $$A = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \in SL(2, R)$$

$$AI = IA = A.$$

Therefore I is identity of $SL(2, R)$.

(iv) Existence inverse :

Let $$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL(2, R)$$

& $$B = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \in SL(2, R)$$

Now $$AB = \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \begin{bmatrix} ad - bc & -ab + ba \\ cd - cd & -bc + ad \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

$$BA = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

$$= \begin{bmatrix} ad - bc & bd - bd \\ -ac + ac & -bc + ad \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$= I$$

Therefore $\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$ is the inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$. Since $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is an arbitrary element of SL(2, R), therefore we can obtain inverse in the same manner for every element of SL(2, R).

Since all the required property of a group are satisfied, therefore $SL(2, R)$ is a group with respect to multiplication of matrices. However $SL(2, R)$ is not an abelian group as the commutative property is not satisfied.

Since, $|AB| = |BA|$ does not implies that $AB = BA$.

Example 4.4. *Show that*

$$SL(2, C) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a,b,c,d \in C \ \& \ ad - bc = 1 \right\}$$ *is non obelian is group.*

Sol. To show that SL(2, C) is a group with respect to multiplication of matrices we need the following properties :-

(i) **Closure property :** Let $A = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$ & $B = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$

$\in SL(2, C)$, then $a_1 d_1 - b_1 c_1 = 1, a_2 d_2 - b_2 c_2 = 1$ and a_1, b_1, c_1, d_1 are complex numbers

i.e. A and B are non singular matrices.

$$\therefore \quad |AB| = |A| \,.\, |B|$$
$$= 1.1$$
$$= 1$$

$$\therefore \quad AB \in SL(2, C).$$

Since A, B are arbitrary, therefore

$AB \in SL(2, C) \forall \ A, B. \in SL(2, C)$.

(ii) **Associative property :** The multiplication of matrices is always associative.

(iii) **Existence of identity :** Let $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in SL(2, C)$

and let $A = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \in SL(2, C)$ be arbitrary.

Then $$AI = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a_1 + 0 & 0 + b_1 \\ c_1 + 0 & 0 + d_1 \end{bmatrix}$$

$$= \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} = A$$

also $$IA = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$$

$$= \begin{bmatrix} a_1 + 0 & b_1 + 0 \\ c_1 + 0 & d_1 + 0 \end{bmatrix}$$

$$= \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} = A$$

i.e. $AI = IA = A \ \forall \ A \in SL(2, C)$.

(iv) Existence of inverse :

Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL(2, C)$

Now $AB = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \begin{bmatrix} ad - bc & -ab + ba \\ cd - cd & -bc + ad \end{bmatrix}$

$$= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

Also, $BA = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix}$

$$= \begin{bmatrix} ad - bc & bd - bd \\ -ac + ac & -bc + ad \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Since A and B are arbitrary, therefore

$$AB = BA = I \ \forall \ A, B \in SL(2, C),$$

Since all the properties of a group are satisfied SL(2, C) is a group with respect to multiplication of matrices. Although SL (2, C) is not an abelian group as

$$|AB| = |BA| \Rightarrow BA = BA.$$

i.e. SL (2, C) is not commutative.

5. Generalized Linear Groups :

The set of all 2 × 2 matrices with non zero determinant and entries from Q (rationals), R (reals), C complex numbers or Zp (p is a prime) is called generalised linear group of 2 × 2 matrices over Q, R, C or Zp respectively. If the entries are from F, where F is any of the above, we denote this group by GL(2, F).

i.e. (i) $GL(2, Q) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : ad - bc \neq 0, \forall \ a, b, c, d \in Q \right\}$

(ii) $GL(2, R) = \left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} : ad - bc \neq 0, \forall\ a, b, c, d \in R\right\}$

(iii) $GL(2, C) = \left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} : ad - bc \neq 0, \forall\ a, b, c, d \in C\right\}$

(iv) $GL(2, Z_p) = \left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} : ad - bc \neq 0, \forall\ a, b, c, d \in Zp\right\}$

Example 5.1. *Prove that*

$GL(2, Q) = \left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} : ad - bc \neq 0, \forall\ a, b, c, d \in Q\right\}$ *is a group. Is* $GL(2, Q)$ *an abelian group?*

Sol. We have $GL(2, Q) = \left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} : ad - bc \neq 0, a, b, c, d \in Q\right\}$.

Now to discuss that GL(2, Q) is a group with respect to multiplication of matrices, we need to verify the following properties :

(i) Closure property :

Let $A = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}, B = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} \in GL(2, Q)$

then $a_1 d_1 - b_1 c_1 \neq 0$ and $a_2 d_2 - b_2 c_2 \neq 0$

i.e. matrices A and B are non-singular matrices.

therefore, by the property of non-singular matrices

$$|AB| = |A| \,.\, |B| \neq 0$$

(as if $|A| \neq 0, |B| \neq 0$, then $|A| \,.\, |B| \neq 0$).

so $$AB \in GL(2, Q).$$

Since A, B are arbitrary matrices, therefore

$$AB \in GL(2, Q), \forall\ A, B\ \forall\ GL(2, Q).$$

(ii) Associative property : The multiplication of matrices is always associative.

i.e. $$A(BC) = (AB)\, C\ \forall\ A, B, C \in GL(2, Q).$$

(iii) Existence of identity :

Let $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, and $A = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \in GL(2, Q).$

Thus $AI = IA = A.$

Since A is arbitrary, therefore

$$AI = IA = A \ \forall \ A \in GL(2, Q).$$

(iv) Existence of inverse :

Let $$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL(2, Q).$$

Thus $ad - bc \neq 0$

Now, if we take

$$B = \begin{bmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix} \in GL(2, Q)$$

We can obtain

$$AB = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix}$$

$$= \begin{bmatrix} \frac{ad}{ad-bc} - \frac{bc}{ad-bc} & \frac{-ab}{ad-bc} + \frac{ab}{ad-bc} \\ \frac{cd}{ad-bc} - \frac{cd}{ad-bc} & \frac{-bc}{ad-bc} + \frac{ad}{ad-bc} \end{bmatrix}$$

$$= \begin{bmatrix} \frac{ad-bc}{ad-bc} & 0 \\ 0 & \frac{ad-bc}{ad-bc} \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

Also

$$BA = \begin{bmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

$$= \begin{bmatrix} \frac{da}{ad-bc} - \frac{bc}{ad-bc} & \frac{db}{ad-bc} - \frac{bd}{ad-bc} \\ \frac{-ac}{ad-bc} + \frac{ac}{ad-bc} & \frac{-bc}{ad-bc} + \frac{ad}{ad-bc} \end{bmatrix}$$

$$= \begin{bmatrix} \frac{ad-bc}{ad-bc} & 0 \\ 0 & \frac{ad-bc}{ad-bc} \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

Therefore, $AB = BA = I$

Hence B is the inverse of A.

Since all the properties of a group are satisfied, therefore GL(2, Q) is a group. although GL(2, Q) is not abelian as matrices multiplication not necessarity commutative.

Example 5.2. *Show that* $GL(2,R) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : ad - bc \neq 0, \forall\, a,b,c,d \in R \right\}$ *is a non abelian group.*

Sol. To show that $GL(2, R) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : ad - bc \neq 0, \forall\, a,b,c,d \in R \right\}$ *is a* non abelian group with respect to multiplication of matrices, we need the following properties :

(i) **Closure property :**

Let $$A = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \text{ and } B = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} \in GL(2,R)$$

thus $|A| \neq 0 \;\&\; |B| \neq 0$, therefore

$$|AB| = |A| \,.\, |B|$$
$$\neq 0.$$

this implies that $AB \in GL(2,R)$.

Since A and B are arbitrary so $AB \in GL(2,R)\ \forall A, B \in GL(2,R)$.

(ii) **Associative property :** The multiplication of matrices is always associative.

(iii) **Existence of identity :**

Let $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, and $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL(2, R)$ be arbitrary, then

$$AI = \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a+0 & 0+b \\ c+0 & d+0 \end{bmatrix}$$

$$= \begin{bmatrix} 0+a & 0+b \\ 0+c & 0+d \end{bmatrix}$$

$$= \begin{bmatrix} a & b \\ c & d \end{bmatrix} = A$$

Since A is arbitrary, then $AI = IA = A \; \forall \; A \in GL(2, R)$

(iv) Existence of inverse :

Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL(2, R)$, then $ad - bc \neq 0$,

Now, if we take $$B = \begin{bmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-b} \end{bmatrix} \in GL(2, R)$$

$$= \begin{bmatrix} \frac{ad}{ad-bc} - \frac{bc}{ad-bc} & \frac{-ab}{ad-bc} + \frac{ab}{ad-bc} \\ \frac{cd}{ad-bc} - \frac{cd}{ad-bc} & \frac{-bc}{ad-bc} + \frac{ad}{ad-bc} \end{bmatrix}$$

$$= \begin{bmatrix} \frac{ad-bc}{ad-bc} & 0 \\ 0 & \frac{ad-bc}{ad-bc} \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$BA = \begin{bmatrix} \frac{d}{ad-bc} & -\frac{b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

Therefore
Hence B
(v) Con
$\forall A, B \in GL$
as

Exam

$a, b, c, d \in$
ces.
Sol. T
Exam

$Zp) = \{\{[$

is multip
Sol.
plicatior
(i) (

Let

an

$|A$

$$= \begin{bmatrix} \frac{ad}{ad-bc} - \frac{bc}{ad-bc} & \frac{bd}{ad-bc} - \frac{bd}{ad-bc} \\ \frac{-ac}{ad-bc} + \frac{ac}{ad-bc} & \frac{-bc}{ad-bc} + \frac{ad}{ad-bc} \end{bmatrix}$$

$$= \begin{bmatrix} \frac{ad-bc}{ad-bc} & 0 \\ 0 & \frac{ad-bc}{ad-bc} \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Therefore $AB = BA = I.$

Hence B is the inverse of A.

(v) **Commutative property :** we know that in general $AB \neq BA$ $\forall A, B \in GL(2, R)$

as $|AB| = |BA| \not\Rightarrow AB = BA.$

Example 5.3. *Show that* $GL(2,C) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : ad - bc \neq 0, \text{ and } a,b,c,d \in C \right\}$ *is a non abelian group with respect to multiplication of matrices.*

Sol. Take R= C in example 5.2.

Example 5.4. *Show that GL(2, Zp) is a non abelian group, where GL (2,* $Zp) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : ad - bc \neq 0, \text{ and } a,b,c,d \in Zp \right\}$ *and the binary composition is multiplication of matrices.*

Sol. To show that GL(2, Zp) is a non abelian group with respect to multiplication of matrices, we need to verify the following properties -

(i) **Closure property :**

Let $A = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \in GL(2, Zp)$

and $B = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} \in GL(2, Zp)$, then

$|A| \neq 0, |B| \neq 0$ over modulo p (arithmatic used to calculate determinants).

Therefore $|AB| \neq 0$, $\forall\ A, B \in GL(2, Zp)$ and so $AB \in GL(2, Zp)$.

(ii) **Associative property :** The multiplication of matrices is always associative.

(iii) **Existence of identity :**

Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL(2, Zp)$ be arbitrary

then

if we take $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in GL(2, Zp)$

We observe $AI = IA = A\ \forall A \in GL(2, Zp)$.

(iv) **Existence of inverse :**

Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL(2, Zp)$, be arbitrary.

Thus $ad - bc \neq 0$ while the arithmatic done by (ad – bc) modulo p. If we take B in the light of A to obtain its inverse as

$$B = \begin{bmatrix} \frac{d}{ad-bc} & -\frac{b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix} \in GL(2, Zp)$$

We can obtain

$$AB = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix}$$

$$= \begin{bmatrix} \frac{ad}{ad-bc} - \frac{bc}{ad-bc} & \frac{-ab}{ad-bc} + \frac{ab}{ad-bc} \\ \frac{cd}{ad-bc} - \frac{cd}{ad-bc} & \frac{-bc}{ad-bc} + \frac{ad}{ad-bc} \end{bmatrix}$$

$$= \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} \frac{ad-bc}{ad-bc} & 0 \\ 0 & \frac{ad-bc}{ad-bc} \end{bmatrix}$$

Similarly

Hence B i
multiplication
(v) Comm

that
6. Group
Exampl
$ij = -ji = k, j$
group of ord

Sol. We

where

Compo
multiplicati

1	
−1	
i	
$-i$	
j	
$-j$	
k	
$-k$	

(i) (
element
(ii)
bers and
(iii)
Sin

the
(iv

$$= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

Similarly $$BA = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

Hence B is the inverse of A provided we interpret division by ad – bc as multiplication by inverse of (ad – bc) modulo-p

(v) **Commulative property :** We know that in general

$|AB| = |BA|$ does not implies that $AB = BA$, therefore GL(2, Zp) is not commutative.

6. Group of quanternians :

Example 6.1. *The set* $G = \{\pm 1, \pm i, \pm j, \pm k\}$, *where* $i^2 = j^2 = k^2 = -1$ *and* $ij = -ji = k, jk = kj = i, ki = -ik = j, ij \neq ji$ *etc. is a non-abelian multiplication group of order 8.*

Sol. We have $G = \{1, -1, i, -i, i, -j, k, -k\}$,

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

Composition table : following composition is based on the composition multiplication.

	1	−1	i	$-i$	j	$-j$	k	$-k$
1	1	−1	i	$-i$	j	$-j$	k	$-k$
−1	−1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	−1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	−1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	−1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	−1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	−1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	−1

(i) **Closure property :** Since all the entries in the composition table are elements of set G, therefore closure property is verified.

(ii) **Associative property :** Since all the elements of G are complex numbers and we know that complex numbers are associative.

(iii) **Existence of identity :**

Since $1 \in G$, and for all $a \in G$

$$a.1 = 1.a = a$$

therefore 1 is the identity element of G.

(iv) **Existence of inverse :** From the composition table we see that the

inverse of 1 is 1, inverse of -1 is -1, inverse of i is $-i$, inverse of j is $-j$ and inverse of k is $-k$.

(v) **Commutativity :** Since $ij \neq ji$, $jk \neq kj$, etc, therefore the commutative property does not hold in G.

Hence G is a non abelian group.

7. U(n) the group of all positive integers less than n and relatively prime to n.

An integer a has a multiplicative inverse modulo n if and only if a and n are relatively prime. So, for each $n > 1$, we define U(n) to be the set of all positive integers less than n and relatively prime to a. U(n) is a group under multiplication modulo-n.

Example 7.1 *For $n = 10$, we have $U(n) = \{1, 3, 7, 9\}$. Show that U(10) is an abelian group.*

Sol. Composition Table

.	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

(i) **Closure property :** Since all the entries in the composition table are elements of U(10). Therefore U(10) is closed with respect to multiplication of positive integers less than 10 and relatively prime to 10.

(ii) **Associativity :** Since the multiplication of integers is always associative, therefore the multiplication of positive integers less than n and relatively prime to n are associative.

(iii) **Existence of identity :**

Since $1 \in U(10)$, and $\forall\ a \in U(10)$

$$a.1 = 1.a = a$$

Therefore 1 is the identity element of U(10).

(iv) **Existence of inverse :** from the composition table we see that the inverse of 1 is 1, inverse of 3 is 7, inverse of 7 is 3, inverse of 9 is 9.

(v) **Commutative property :** From the composition table we see that

Ist row = Ist Column
IInd row = IInd Column
IIIrd row = IIIrd Column
IVth row = IVth Column.

Therefore, commutative property hold in U(10). Finally, we conclude that U(10) is an abelian group.

8. Miscellaneous Examples

Example 1. *For a fixed point (a, b) in R^2, define $T_{a,b} : R^2 \to R^2$. by $(x, y) \to (x + a, y + b)$. Then $T(R^2) = \{T_{a,b} : a, b \in R\}$ is an abelian group with respect to*

the composition of functions.

Sol. We have $T : R^2 \to R^2$ defined as

$T_{a,b}(x, y) = (x + a, y + b)$ for fixed $a, b \in R$, and $(x, y) \in R^2$.

Now, to prove that $T(R^2) = \{T_{a,b} : a, b \in R\}$ is an abelian group, we need the following properties–

(i) **Closure property :**

Let $T_{a,b}$ and $T_{c,d}$ be two arbitrary elements of $T(R^2)$. Thus

$$\begin{aligned} T_{a,b}\, T_{c,d}(x, y) &= T_{a,b}(x + c, y + d) \\ &= (x + c + a, y + d + b) \\ &= (a + c + x, b + d + y) \\ &= T_{a+c,\, b+d}(x, y) \end{aligned}$$

i.e., $T_{a,b}\, T_{c,d} = T_{a+c,\, b+d} \quad \forall\, T_{a,b}, T_{c,d} \in T(R^2)$

(ii) **Associative property :**

The composition of functions is always associative.

i.e. for any $T_{a,b}, T_{c,d}, T_{e,f} \in T(R^2)$

$$(T_{a,b} \cdot T_{c,d}) \cdot T_{e,f} = T_{a,b} \cdot (T_{c,d} \cdot T_{e,f})$$

(iii) **Existence of identity :**

For any $T_{a,b} \in T(R^2)$, $\exists$ a nuique $T_{0,0} \in T(R^2)$ such that

$$T_{a,b} \cdot T_{0,0} = T_{0,0} \cdot T_{a,b} = T_{a,b}.$$

Therefore, $T_{0,0}$ is identity element of $T(R^2)$.

(iv) **Existence of inverse :**

For every $T_{a,b} \in T(R^2)$, $\exists\, a\, T_{-a,-b} \in T(R^2)$ such that

$T_{a,b} \cdot T_{-a,-b} = T_{-a,-b} T_{a,b} = T_{0,0}$ Therefore $T_{-a,-b}$ is the inverse of $T_{a,b}$.

(v) **Commutativity :**

For any two $T_{a,b} \in T(R^2)$ and $T_{c,d} \in T(R^2)$

$$T_{a,b} \cdot T_{c,d} = T_{c,d} \cdot T_{a,b}$$

as

$$\begin{aligned} T_{a,b} \cdot T_{c,d}(x, y) &= T_{a,b}(x + c, y + d) \\ &= (x + c + a, y + d + b) \\ &= (x + a + c, y + b + d) \end{aligned}$$

$(\because a + c = c + a\ \forall a, c \in R,\ b + d = d + b\ \forall\, b, d \in R)$

$$\begin{aligned} &= T_{c,d} \cdot (x + a, y + b) \\ &= T_{c,d} \cdot T_{a,b}. \end{aligned}$$

Example 2. *Find the inverse of the element* $\begin{bmatrix} 2 & 6 \\ 3 & 5 \end{bmatrix}$ *in* $GL(2, z_{11})$.

Sol. We have

$$A = \begin{pmatrix} 2 & 6 \\ 3 & 5 \end{pmatrix}, \text{ then } A^{-1} = \frac{-1}{8}\begin{bmatrix} 5 & -6 \\ -3 & 2 \end{bmatrix}$$

as

$$A^{-1} = \frac{1}{|A|} adj(A)$$

Now, in $GL(2, z_{11})$, we see that

$$-8 = -8 + 11 = 3$$

We can also make other elements multiple of 3.

i.e.

$$5 = 5 + 11 = 16 + 11 = 27$$
$$-6 = -6 + 11 = 5 + 11 = 16 + 11 = 27$$
$$-3 = -3 + 11 = 8 + 11 = 19 + 11 = 30$$
$$2 = 2 + 11 = 13 + 11 = 24$$

Therefore

$$A^{-1} = -\frac{1}{8}\begin{bmatrix} 5 & -6 \\ -3 & 2 \end{bmatrix} = \frac{1}{3}\begin{bmatrix} 27 & 27 \\ 30 & 24 \end{bmatrix}$$

$$= \begin{pmatrix} 9 & 9 \\ 19 & 8 \end{pmatrix}$$

Example 3. *Prove by an example that the generalised linear group GL(2, R) is non abelian.*

Sol. Let $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$

and $B = \begin{pmatrix} 5 & 6 \\ 7 & 8 \end{pmatrix}$

where $|A| = -2, \ |B| = -2$

$$AB = \begin{pmatrix} 19 & 22 \\ 43 & 51 \end{pmatrix}, \ BA = \begin{pmatrix} 23 & 24 \\ 31 & 46 \end{pmatrix}$$

therefore $AB \neq BA$ although $|AB| = 4, |BA| = 4$.

Example 4. *Let p and q be distinct primes. Suppose that H is a proper subset of the integers and H is a group under addition that contains exactly three elements of the set $\{p, p+q, pq, p^q, q^p\}$. Determine which of the following are the three elements in H.*

(i) $H = \{p, pq, p^q\}$
(ii) $H = \{pq, p^q, q^p\}$
(iii) $H = \{p + q, pq, p^q\}$
(iv) $H = \{p, p + q, pq\}$
(v) $H = \{p, p^q, q^p\}$

Sol. (i) Let $H = \{p, pq, p^q\}$. Since H is group under addition, therefore according to closure property

if $p \in H$, *then* $p + p + \ldots\ldots + p$ (q times) $\in H$

i.e. $p(\underbrace{1+1\ldots\ldots+1}_{q \text{ times}}) \in H$

i.e. $pq \in H$

again $p \in H$, then $p + p + \ldots\ldots + p$ (p times) $\in H$

i.e. $p(\underbrace{1+1\ldots\ldots+1}_{p \text{ times}}) \in H$

i.e. $p.p \in H$

i.e. $p^2 \in H$

Now, as $p^2 \in H, p^2 + p^2 - + p^2$ (p times) $= p^2 \in H$

Similarly $p^{q-1} + p^{q-1} - + p^{q-1}$ (p times)

i.e. $p^{q-1}(\underbrace{1+1+\ldots\ldots+1}_{p \text{ times}}) = p^{q-1}.p^1 = p^q \in H$

therefore, H is a group with $\{p, pq, p^q\}$, under addition, with $p, pq, p^q \in H$.

(ii) $H = \{p^q, p^q, q^p\}$

if $p \in H$, then $p + p + \ldots\ldots + p$ (q times) $= pq \in H$.

Also $p \in H$, $p^2 \in H$, $p^{q-1} \in H$,

$p^{q-1} + p^{q-1} \ldots\ldots + p^{q-1}$ (p times) $\in H$

i.e. $p^{q-1}(\underbrace{1+1+\ldots\ldots+1}_{p \text{ times}}) = p^{q-1}p = p^q \in H$.

Now if $q \in H$, then $p^q \in H$ (similar as above)

then $p \in H, q \in H \Rightarrow p+q \in H$ which is not an element of H.

Therefore, either $p \in H$ or $q \in H$.

i.e. if $p \in H$ and $q \notin H$, then $p^q \notin H$

Hence, H is not a group under addition.

Therefore, we conclude that $H = \{pq, p^q, q^p\}$ is not a group under addition.

(iii) H = $\{p + q, pq, p^q\}$

let $p \in H$, then $pq \in H$, (as above)

also $p \in H$, then $p^q \in H$ (as above)

Now, its $q \notin H$, $p \in H \Rightarrow p+q \notin H$,

therefore, H is not a group with three elements $p + q$, pq, p^q.

(iv) $H = \{p, p + q, pq\}$

Let $p \in H$, then $pq \in H$ (as above)

But if $q \notin H$, $p \in H$ does not implies that $p+q \in H$.

Therefore, set H with elements p, $p + q$, pq does not form a group with respect to addition.

(v) $H = \{p, p^q, q^p\}$

Let $p \in H$, then $p^q \in H$ (as above)

But if $q \notin H$, $q^p \notin H$. (closure property does not hold)

Example 5. *(A) Show that the set {5, 15, 25, 35} is a group with respect to multiplication modulo 40.*

(B) What is the identity element of this group?

(C) Can you see any relationship between this group and U(8)?

Sol. Let G = {5, 15, 25, 35}, with composition multiplication modulo 40.

Now, to show that G is an abelian group, we firstly make the following composition table

$\odot_{40}$	5	15	25	35
5	25	35	5	15
15	35	25	15	5
25	5	15	25	35
35	15	5	35	25

(i) Closure property : Since all the entries in the composition table are elements of G, therefore closure property is verified.

(ii) Associative property : Since elements of G are natural numbers and we know that natural numbers and associative with respect to multiplication.

i.e. $$a(bc) = (ab)c \quad \forall\, a,b,c \in G.$$

(iii) Existence of identity : from the composition table, we see that

$25.a = a.25 = a \quad \forall\, a \in G.$

Therefore $25 \in G$ is the identity element of G.

(iv) Existence of inverse : From the composition table, we see that

$(5)^{-1} = 5$, $(15)^{-1} = 15$, $(25)^{-1} = 25$, $(35)^{-1} = 35$

i.e. all the elements of G are self inverse.

(v) Commutative property : From the composition table, we see that

Ist row = Ist column, IInd row = IInd column.

IIIrd row = IIIrd column, IVth row = IV column.

i.e. the transpose of the composition table is same as the composition

table.

Hence G is an abelian group.

(B) 25 is the identity element of this group.

as $25 \,.\, a = a.25 = a \;\forall\, a \in G.$

(C) $G = \{5x : x \in U(8)\}$, where U(8) is an abelian group of positive integers relatively prime to 8 and less than 8 with 1 as identity element. From the composition table of U(8), we observe that

$\odot_8$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

the inverse of 1, 3, 5, 7 in U(8) are 1, 3, 5, 7 resp. Hence we observe that both G and U(8) contains elements which are self inverse.

Example 6. *Prove that the set of all 3 × 3 matrices with real entries of the form*

$$G = \left\{ A : A = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}, a,b,c \in R \right\}$$

is a group with respect to multiplication of matrices. [This group is sometimes called the Heisenberg group after the nobel prize-winning physist Werner Heisenberg is infimately related to the Heisenberg uncertainty principle, of Quantum physics.]

Sol. (i) Closure Property :

Let $$A = \begin{bmatrix} 1 & a_1 & b \\ 0 & 1 & c_1 \\ 0 & 0 & 1 \end{bmatrix}, B = \begin{bmatrix} 1 & a_2 & b_2 \\ 0 & 1 & c_2 \\ 0 & 0 & 1 \end{bmatrix}$$

$$AB = \begin{bmatrix} 1 & a_1 & b_1 \\ 0 & 1 & c_1 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & a_2 & b_2 \\ 0 & 1 & c_2 \\ 0 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & a_1 + a_2 & b_1 + b_2 + a_1 c_2 \\ 0 & 1 & c_1 + c_2 \\ 0 & 0 & 1 \end{bmatrix} \in G$$

Since A, B are arbitrary, therefore $AB \in G \; \forall \; A, B \in G$.

(ii) Associativity : The multiplication of matrices is always associative,

i.e. $(AB)\,C = A(BC) \quad \forall \; A, B, C \in G.$

(iii) Existence of identity :

For every $A = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$, $\exists$ a unique matrix called

$I = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ (the identity matrix) such

that $AI = IA = A.$

(iv) Existence of inverse :

For every $A = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$, $\exists$ a unique matrix B in G such

that $AB = BA = I$, where B is called the inverse of A. We can obtain easily

$$B = \frac{1}{|A|}\text{adj}\,(A) = \begin{pmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix} \in G.$$

(v) Commutativity :

Let $A = \begin{bmatrix} 1 & a_1 & b_1 \\ 0 & 1 & c_1 \\ 0 & 0 & 1 \end{bmatrix}$

and $B = \begin{bmatrix} 1 & a_2 & b_2 \\ 0 & 1 & c_2 \\ 0 & 0 & 1 \end{bmatrix}$

Then $AB = \begin{bmatrix} 1 & a_1 + a_2 & b_1 + b_2 + a_1 c_2 \\ 0 & 1 & c_1 + c_2 \\ 0 & 0 & 1 \end{bmatrix}$

and $$BA = \begin{bmatrix} 1 & a_1 + a_2 & b_1 + b_2c_1 + b_2 \\ 0 & 1 & c_1 + c_2 \\ 0 & 0 & 1 \end{bmatrix}$$

Thus $$AB \neq BA$$

Hence G is a non abelian group.

Example 4. *Let* $G = \left\{ \begin{bmatrix} a & a \\ a & a \end{bmatrix} : a \in R, a \neq 0 \right\}$. *Show that* G *is a group under matrix multiplication.*

Sol. Colsure property :

Let $$A = \begin{bmatrix} a & a \\ a & a \end{bmatrix}, B = \begin{bmatrix} b & b \\ b & b \end{bmatrix} \in G \text{ be arbitrary}$$

thus $$AB = \begin{bmatrix} a & a \\ a & a \end{bmatrix}\begin{bmatrix} b & b \\ b & b \end{bmatrix} = \begin{bmatrix} 2ab & 2ab \\ 2ab & 2ab \end{bmatrix} \in G$$

Since A, B are arbitrary.

Therefore $$AB \in G \ \forall \ A, B \in G.$$

Associative property : Matrices multiplication is always associntive. Therefore

$$(AB)C = A(BC) \ \forall \ A, B, C \in G.$$

Existence of identity : For any $A = \begin{bmatrix} a & a \\ a & a \end{bmatrix} \in G$, $\exists$ **unique**

$I = \begin{bmatrix} ½ & ½ \\ ½ & ½ \end{bmatrix} \in G$ **such that**

$$AI = \begin{bmatrix} a & a \\ a & a \end{bmatrix}\begin{bmatrix} ½ & ½ \\ ½ & ½ \end{bmatrix} = \begin{bmatrix} \frac{a}{2}+\frac{a}{2} & \frac{a}{2}+\frac{a}{2} \\ \frac{a}{2}+\frac{a}{2} & \frac{a}{2}+\frac{a}{2} \end{bmatrix} = \begin{bmatrix} a & a \\ a & a \end{bmatrix} = A,$$

$$\text{Also } IA = \begin{bmatrix} ½ & ½ \\ ½ & ½ \end{bmatrix}\begin{bmatrix} a & a \\ a & a \end{bmatrix} = \begin{bmatrix} \frac{a}{2}+\frac{a}{2} & \frac{a}{2}+\frac{a}{2} \\ \frac{a}{2}+\frac{a}{2} & \frac{a}{2}+\frac{a}{2} \end{bmatrix} = \begin{bmatrix} a & a \\ a & a \end{bmatrix} = A$$

therefore $AI = IA = A$, $\forall \ A \in G$. Matrix I is called the identity of G.

and $$BA = \begin{bmatrix} 1 & a_1+a_2 & b_1+b_2c_1+b_2 \\ 0 & 1 & c_1+c_2 \\ 0 & 0 & 1 \end{bmatrix}$$

Thus $AB \neq BA$

Hence G is a non abelian group.

Example 4. *Let* $G = \left\{ \begin{bmatrix} a & a \\ a & a \end{bmatrix} : a \in R, a \neq 0 \right\}$. *Show that G is a group under matrix multiplication.*

Sol. Colsure property :

Let $A = \begin{bmatrix} a & a \\ a & a \end{bmatrix}, B = \begin{bmatrix} b & b \\ b & b \end{bmatrix} \in G$ *be arbitrary.*

thus $$AB = \begin{bmatrix} a & a \\ a & a \end{bmatrix}\begin{bmatrix} b & b \\ b & b \end{bmatrix} = \begin{bmatrix} 2ab & 2ab \\ 2ab & 2ab \end{bmatrix} \in G$$

Since A, B are arbitrary.

Therefore $AB \in G \ \forall \ A, B \in G.$

Associative property : Matrices multiplication is always associative.

Therefore $$(AB)C = A(BC) \ \forall \ A, B, C \in G.$$

Existence of identity : For any $A = \begin{bmatrix} a & a \\ a & a \end{bmatrix} \in G$, $\exists$ unique

$I = \begin{bmatrix} ½ & ½ \\ ½ & ½ \end{bmatrix} \in G$ such that

$$AI = \begin{bmatrix} a & a \\ a & a \end{bmatrix}\begin{bmatrix} ½ & ½ \\ ½ & ½ \end{bmatrix} = \begin{bmatrix} \frac{a}{2}+\frac{a}{2} & \frac{a}{2}+\frac{a}{2} \\ \frac{a}{2}+\frac{a}{2} & \frac{a}{2}+\frac{a}{2} \end{bmatrix} = \begin{bmatrix} a & a \\ a & a \end{bmatrix} = A,$$

Also $$IA = \begin{bmatrix} ½ & ½ \\ ½ & ½ \end{bmatrix}\begin{bmatrix} a & a \\ a & a \end{bmatrix} = \begin{bmatrix} \frac{a}{2}+\frac{a}{2} & \frac{a}{2}+\frac{a}{2} \\ \frac{a}{2}+\frac{a}{2} & \frac{a}{2}+\frac{a}{2} \end{bmatrix} = \begin{bmatrix} a & a \\ a & a \end{bmatrix} = A$$

therefore $AI = IA = A, \ \forall \ A \in G.$ Matrix I is called the identity of G.

Existence of inverse :

For every $A = \begin{bmatrix} a & a \\ a & a \end{bmatrix} \in G, \exists$ a unique matrix

$B = \begin{bmatrix} 1/4a & 1/4a \\ 1/4a & 1/4a \end{bmatrix} \in G$, called the inverse of A.

We observe $AB = BA = I$.

Since $AB = \begin{bmatrix} a & a \\ a & a \end{bmatrix}\begin{bmatrix} 1/4c & 1/4a \\ 1/4a & 1/4a \end{bmatrix}$

$= \begin{bmatrix} 1/4+1/4 & 1/4+1/4 \\ 1/4+1/4 & 1/4+1/4 \end{bmatrix}$

$= \begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix} = I$ *(identity of G).*

Similarly $BA = \begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix} = I$

Therefore B is the inverse of A.

Hence G is a group under multiplication.

Example 8. *Define a group. Prove that the set* $G = \left\{\begin{bmatrix} a & a \\ a & a \end{bmatrix} : a \in R, a \neq 0\right\}$ *is a group under multiplication. Is it an infinite abelian group? (D.U. Sem. 3)*

Sol. Hint : for definition see page no. 10. The set G is a group under multiplication (see Ex. 7). G is an infinite abelian group as

$G = \left\{\begin{bmatrix} a & a \\ a & a \end{bmatrix} : a \in R, a \neq 0\right\}$ is set of matrices of order 2 × 2 with $a \in R, a \neq 0$. Since R is infinite set of real numbers, therefore G is an infinite set. Now, for the commutativity.

Let

$$A = \begin{bmatrix} a & a \\ a & a \end{bmatrix} \in G, \quad B = \begin{bmatrix} b & b \\ b & b \end{bmatrix} \in G$$

Thus $AB = \begin{bmatrix} a & a \\ a & a \end{bmatrix}\begin{bmatrix} b & b \\ b & b \end{bmatrix} = \begin{bmatrix} 2ab & 2ab \\ 2ab & 2ab \end{bmatrix} = \begin{bmatrix} 2ba & 2ba \\ 2ba & 2ba \end{bmatrix}$

$= \begin{bmatrix} b & b \\ b & b \end{bmatrix}\begin{bmatrix} a & a \\ a & a \end{bmatrix} = BA.$ (as, $ab = ba \ \forall \ a,b \in R$)

Thus $AB = BA \ \forall \ A, B \in G$.

Hence G is an abelian group.

Delhi Univ
B.Sc. (Phys
Pape
(Admis

Time : 3 Hours

Attempt any two parts from

1. (a) Define a group and
$G = \left\{\begin{pmatrix} a & a \\ a & a \end{pmatrix} : a \in$
is a group under m

(b) Let G be a group,
tre of the group (

(c) Consider the ele
If we view A =
order of A?

2. (a) Prove that Z_{30} i
indicating their

(b) Prove that the
cyclic.

(c) (i) Define an
mine whe

(ii) Let α and
mutation.

3. (a) State Lagrang
Justify your a

(b) Suppose G is
Prove that eve

(c) Define a norm
normal subgr

4. (a) Define an ide
of a ring is an

Existence of inverse :

For every $A = \begin{bmatrix} a & a \\ a & a \end{bmatrix} \in G$, $\exists$ a unique matrix

$$B = \begin{bmatrix} \frac{1}{4a} & \frac{1}{4a} \\ \frac{1}{4a} & \frac{1}{4a} \end{bmatrix} \in G, \text{ called the inverse of } A.$$

We observe $AB = BA = I$.

Since
$$AB = \begin{bmatrix} a & a \\ a & a \end{bmatrix}\begin{bmatrix} \frac{1}{4a} & \frac{1}{4a} \\ \frac{1}{4a} & \frac{1}{4a} \end{bmatrix}$$
$$= \begin{bmatrix} \frac{1}{4} + \frac{1}{4} & \frac{1}{4} + \frac{1}{4} \\ \frac{1}{4} + \frac{1}{4} & \frac{1}{4} + \frac{1}{4} \end{bmatrix}$$
$$= \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix} = I \text{ (identity of } G\text{)}.$$

Similarly $BA = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix} = I$

Therefore B is the inverse of A.
Hence G is a group under multiplication.

Example 8. *Define a group. Prove that the set* $G = \left\{ \begin{bmatrix} a & a \\ a & a \end{bmatrix} : a \in R, a \neq 0 \right\}$ *is a group under multiplication. Is it an infinite abelian group? (D.U. Sem. 3)*

Sol. Hint : for definition see page no. 10. The set G is a group under multiplication (see Ex. 7). G is an infinite abelian group as

$G = \left\{ \begin{bmatrix} a & a \\ a & a \end{bmatrix} : a \in R, a \neq 0 \right\}$ is set of matrices of order 2 × 2 with $a \in R, a \neq 0$. Since R is infinite set of real numbers, therefore G is an infinite set. Now, for the commutativity.

Let

$$A = \begin{bmatrix} a & a \\ a & a \end{bmatrix} \in G, \quad B = \begin{bmatrix} b & b \\ b & b \end{bmatrix} \in G$$

$$\text{Thus } AB = \begin{bmatrix} a & a \\ a & a \end{bmatrix}\begin{bmatrix} b & b \\ b & b \end{bmatrix} = \begin{bmatrix} 2ab & 2ab \\ 2ab & 2ab \end{bmatrix} = \begin{bmatrix} 2ba & 2ba \\ 2ba & 2ba \end{bmatrix}$$

$$= \begin{bmatrix} b & b \\ b & b \end{bmatrix}\begin{bmatrix} a & a \\ a & a \end{bmatrix} = BA. \quad (\text{as, } ab = ba \ \forall\, a,b \in R)$$

Thus $AB = BA \ \forall\ A, B \in G$.

Hence G is an abelian group.

Existence of inverse :

For every $A = \begin{bmatrix} a & a \\ a & a \end{bmatrix} \in G$, $\exists$ a unique matrix

$$B = \begin{bmatrix} 1/4a & 1/4a \\ 1/4a & 1/4a \end{bmatrix} \in G,$$ called the inverse of A.

We observe $AB = BA = I$.

Since $$AB = \begin{bmatrix} a & a \\ a & a \end{bmatrix}\begin{bmatrix} 1/4a & 1/4a \\ 1/4a & 1/4a \end{bmatrix}$$

$$= \begin{bmatrix} 1/4 + 1/4 & 1/4 + 1/4 \\ 1/4 + 1/4 & 1/4 + 1/4 \end{bmatrix}$$

$$= \begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix} = I \text{ (identity of } G\text{)}.$$

Similarly $$BA = \begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix} = I$$

Therefore B is the inverse of A.

Hence G is a group under multiplication.

Example 8. *Define a group. Prove that the set* $G = \left\{ \begin{bmatrix} a & a \\ a & a \end{bmatrix} : a \in R, a \neq 0 \right\}$ *is a group under multiplication. Is it an infinite abelian group? (D.U. Sem. 3)*

Sol. Hint : for definition see page no. 10. The set G is a group under multiplication (see Ex. 7). G is an infinite abelian group as

$G = \left\{ \begin{bmatrix} a & a \\ a & a \end{bmatrix} a \in R, a \neq 0 \right\}$ is set of matrices of order 2×2 with $a \in R, a \neq 0$. Since R is infinite set of real numbers, therefore G is an infinite set. Now, for the commutativity

Let

$$A = \begin{bmatrix} a & a \\ a & a \end{bmatrix} \in G, \quad B = \begin{bmatrix} b & b \\ b & b \end{bmatrix} \in G$$

Thus $$AB = \begin{bmatrix} a & a \\ a & a \end{bmatrix}\begin{bmatrix} b & b \\ b & b \end{bmatrix} = \begin{bmatrix} 2ab & 2ab \\ 2ab & 2ab \end{bmatrix} = \begin{bmatrix} 2ba & 2ba \\ 2ba & 2ba \end{bmatrix}$$

$$= \begin{bmatrix} b & b \\ b & b \end{bmatrix}\begin{bmatrix} a & a \\ a & a \end{bmatrix} = BA \quad (\because ab = ba \ \forall\ a, b \in R)$$

Thus $AB = BA \ \forall\ A, B \in G$.

Hence G is an abelian group.

Existence of inverse :

For every $A = \begin{bmatrix} a & a \\ a & a \end{bmatrix} \in G, \exists$ a unique matrix

$B = \begin{bmatrix} 1/4a & 1/4a \\ 1/4a & 1/4a \end{bmatrix} \in G$, called the inverse of A.

We observe $AB = BA = I$.

Since $AB = \begin{bmatrix} a & a \\ a & a \end{bmatrix}\begin{bmatrix} 1/4c & 1/4a \\ 1/4a & 1/4a \end{bmatrix}$

$$= \begin{bmatrix} 1/4 + 1/4 & 1/4 + 1/4 \\ 1/4 + 1/4 & 1/4 + 1/4 \end{bmatrix}$$

$$= \begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix} = I \text{ (identity of } G\text{)}.$$

Similarly $BA = \begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix} = I$

Therefore B is the inverse of A.

Hence G is a group under multiplication.

Example 8. *Define a group. Prove that the set* $G = \left\{ \begin{bmatrix} a & a \\ a & a \end{bmatrix} : a \in R, a \neq 0 \right\}$ *is a group under multiplication. Is it an infinite abelian group? (D.U. Sem. 3)*

Sol. Hint : for definition see page no. 10. The set G is a group under multiplication (see Ex. 7). G is an infinite abelian group as

$G = \left\{ \begin{bmatrix} a & a \\ a & a \end{bmatrix} : a \in R, a \neq 0 \right\}$ is set of matrices of order 2 × 2 with $a \in R, a \neq 0$. Since R is infinite set of real numbers, therefore G is an infinite set. Now, for the commutativity.

Let

$$A = \begin{bmatrix} a & a \\ a & a \end{bmatrix} \in G, \quad B = \begin{bmatrix} b & b \\ b & b \end{bmatrix} \in G$$

Thus $AB = \begin{bmatrix} a & a \\ a & a \end{bmatrix}\begin{bmatrix} b & b \\ b & b \end{bmatrix} = \begin{bmatrix} 2ab & 2ab \\ 2ab & 2ab \end{bmatrix} = \begin{bmatrix} 2ba & 2ba \\ 2ba & 2ba \end{bmatrix}$

$$= \begin{bmatrix} b & b \\ b & b \end{bmatrix}\begin{bmatrix} a & a \\ a & a \end{bmatrix} = BA. \text{ (as, } ab = ba \ \forall\ a, b \in R)$$

Thus $AB = BA \ \forall\ A, B \in G$.

Hence G is an abelian group.

Delhi University Examination Paper
B.Sc. (Physical Science)/III Sem. - 2011
Paper–MAPT-303 : Algebra
(Admission of 2010 and onwards)

Time : 3 Hours

Maximum Marks : 75

Attempt any two parts from each question. All questions are compulsory.

Unit-I

1. (a) Define a group and prove that the set

$$G = \left\{ \begin{pmatrix} a & a \\ a & a \end{pmatrix} : a \in R, a \neq 0 \right\}$$

is a group under matrix multiplication. Is it an infinite abelian group? 6

(b) Let G be a group. Prove that $Z(G) = \bigcap_{a \in G} C(a)$ where Z(G) is the centre of the group G and C(a) is the centralizer of 'a' in G. 6

(c) Consider the element $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ in SL (2, R). What is the order of A?

If we view $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ as a member of $SL(2, Z_p)$ (p-prime), what is the order of A? 6

2. (a) Prove that Z_{30} is a cyclic group. Write down all the subgroups of Z_{30} indicating their orders. 6

(b) Prove that the group (Q, +) of rational numbers under addition is not cyclic. 6

(c) (i) Define an odd permutation and an even permutation and determine whether the permutation (1256743) is odd or even.

(ii) Let α and β belong to S_n. Prove that $\alpha^{-1}\beta^{-1}\alpha\beta$ is an even permutation.

3. (a) State Lagrange's Theorem for finite groups. What about the converse? Justify your answer by giving some example. 6

(b) Suppose G is a group with order $|G| = pq$, where p and q are prime. Prove that every proper subgroup of G is cyclic. 6

(c) Define a normal subgroup of a group G and prove that SL(2, R) is a normal subgroup of GL(2, R). 6

Unit II

4. (a) Define an ideal of a ring R and prove that intersection of two ideals of a ring is an ideal but union is not so. 6½

Section III

3+4½

Q. 1. Define $g : R \to R$ by
$g(x) = 2x$, when x is rational and $g(x) = x + 3$, when x is irrational.
Show that g is continuous at $x = 3$ and discontinuous everywhere else.

Q. 2. Show that the function $f(x) = \frac{1}{x^2}$ is uniformly continuous on $A = [1, \infty]$ but is not uniformly continuous on $B = (0, \infty)$. 3½+4

Q. 3. (a) Obtain Maclaurin series expansion of :
(i) $f(x) = \sin x, x \in R$ (ii) $f(x) = (1 + x)^m, x \in R$ and $m \in N$.
(b) Use mean value theorem to prove :
$|\sin x - \sin y| \leq |x - y|$ for all x, y in R. 5+2½

Section IV

Q.1. State Schwarz's and Young's theorems. Show that for function :

$$f(x,y) = \begin{cases} \frac{x^2y^2}{x^2+y^2}, & (x,y) \neq (0,0) \\ 0, & (x,y) = (0,0) \end{cases}$$

$f_{xy}(0,0) = f_{yx}(0,0)$,
but the conditions of Schwarz's and Young's theorems are not satisfied. 2+5½

Q. 2. Show that the function f, where

$$f(x,y) = \begin{cases} \frac{xy}{\sqrt{x^2+y^2}}, & x^2+y^2 \neq 0 \\ 0, & x = y = 0 \end{cases}$$

is continuous, possesses partial derivatives but is not differentiable at the origin. 3+1½+3

Q. 3. (a) Expand $x^2y + 3y - 2$ in powers of $x - 1$ and $y + 2$.
(b) Find all the maxima and minima of the function given by : 4+3½
$f(x,y) = x^3 + y^3 - 63(x + y) + 12xy$.

Section V

Q. 1. Prove that a bounded function f is Riemann integrable in the interval $[a, b]$ iff for every $\epsilon > 0$, there exists a partition P such that : 7½
$U(P, f) - L(P, f) < \epsilon$.

Q. 2. Compute $\int_{-1}^{1} f(x)dx$ where $f(x) = |x|$. 7½

Q. 3. (a) Prove that if P is a partition of $[a, b]$ and f is a bounded function on $[a, b]$, then :
$m(b - a) \leq L(P, f) \leq U(P, f) \leq M(b - a)$
where $m = \inf \{f(x) : a \leq x \leq b\}$. and $M = \sup \{f(x) : a < x \leq b\}$.
(b) Show that the function :
$f : [1, 2] \to R$ defined by $f(x) = 6x + 5, x \in [1, 2]$
is Riemann integrable on [1, 2] and find the value of $\int_{1}^{2} f(x)dx$. 3+4½

DELHI UNIVERSITY EXAMINATION PAPERS

B.A./B.Sc. (Hons)/II – 2007

MATHEMATICS – Unit V

(Algebra-II)

Time : 2 Hours *Maximum Marks : 38*

Attempt any one question from each Section.

Section A

1. (*a*) Prove that a finite semi-group in which both the cancellation laws hold, is a group. Does the conclusion hold, if the semi-group is infinite ? Justify.

(*b*) Let G be the group of 2×2 matrices over the set of real numbers of the form $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, (where $ad \neq 0$) , under matrix multiplication and $N = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \text{ a real number} \right\}$. Prove that N is a normal subgroup of G. 4

(*c*) Prove that a finite group of composite order has at least one non-trivial subgroup. 3

2. (*a*) (*i*) If G is a group of even order, then prove that is has an element, $a \neq e$ satisfying $a^2 = e$.

(*ii*) If H is a normal subgroup of G with index m, then prove that $g^m \in H$, for all $g \in G$. 5

(*b*) If G is a finite cyclic group and m is a positive integer such that $m \mid o(G)$, then show that G contains a subgroup of order m. 3

(*c*) Using the result : $o(HK) = \dfrac{o(H) \cdot o(K)}{o(H \cap K)}$ for any two finite subgroups H and K of a group G prove that, if $o(H) > \sqrt{o(G)}$ and $o(K) > \sqrt{o(G)}$, then $H \cap K \neq \{e\}$. 3

Section II

3. (*a*) Show that a finite cyclic group of order n is isomorphic to the quotient group $\dfrac{Z}{(b)}$, where $\langle Z, + \rangle$ is the additive-group of integers. 3

(*b*) Show that the smallest subgroup of S_n (the symmetric group of order n), containing (12) and (123..... n) is S_n. 3

(*c*) If H and K are two normal subgroups of a group G and $H \subseteq K$ then prove that : $\dfrac{G}{K} \cong \dfrac{(G/H)}{(K/H)}$. 4

4. (*a*) Let H and K be two subgroups of a group G and K is normal in G. Prove that : 4

(*i*) $H \cap K$ is normal in H ; (*ii*) $\dfrac{HK}{K} \cong \dfrac{H}{H \cap K}$.

(*b*) Show that the multiplicative group $W = \{1, -1\}$, is a homomorphic image of S_n, (the symmetric group of degree n). Deduce that A_n, the set of all even permutations, is a normal subgroup of S_n. 4

(*c*) Let G be a group and $f: G \to G$ be such that $f(x) = x^{-1}$, $\forall\, x \in G$, is a homomorphism. Prove that G is an Abelian group. 2

Section III

5. (*a*) Define class equation of a finite group G. Write down all the conjugate classes of S_4 and hence check the class equation for S_4, the symmetric group of degree 4. 3½

(*b*) Let G be a finite Abelian group of order n and m be a positive integer co-prime to n. Prove that :

$$T: G \to G$$

defined by $T(x) = x^m$, for all $x \in G$, is an isomorphism. 2½

(*c*) Let G be a finite group. If $a \in G$ has exactly two conjugates, then prove that G has a non-trivial normal subgroup. 3

6. (*a*) Find two elements in A_5 which are conjugate in S_5 but not conjugate in A_5. 3

(*b*) Prove that the number of conjugate classes in S_n is $p(n)$, the number of partitions of n. Verify the result for S_3, the symmetric group of degree 3. 3

(*c*) Find the number of automorphisms of an infinite cyclic group. 3

Section IV

7. (*a*) State all the Sylow's theorem. Find all the Sylow subgroups of A_4, the alternative group of degree four. 3

(*b*) If A and B are two finite cyclic groups of order m and n such that $A \times B$ is also cyclic of order mn, then prove that m and n are relatively prime. 3

(*c*) Let G be a group and $H = \{(g, g) : g \in G\}$. Prove that H is a subgroup of $G \times G$. Also prove that H is normal in $G \times G$ if and only if G is an Abelian group. 3

8. (*a*) Prove that a group of order 28 in which a Sylow 4-subgroup is normal, is abelian. 3

(*b*) Show that a group of order 4 is either cyclic or is an internal Direct product of two cyclic/subgroups of order 2 each. 3

(*c*) Show that S_3, (the symmetric group of degree 3), can not be written as an Internal Direct Product of two non-trivial subgroups. 3

B.A./B.Sc. (Hons.)/II – 2008
Mathematics – Unit V (Algebra II)

Time : 2 Hours *Maximum Marks : 38*

Attempt any one question from each Section.

Section I

1. (*a*) Show that the set I of all integers with binary operation, defined as $a \cdot b = a + b + 1$, $\forall\, a, b \in I$ is an abelian group. 3

   (*b*) Show that a semi group G is a group if and only if for any $a, b \in G$, the equations $a \cdot x = b$ and $y \cdot a = b$ have solutions in G. 4

   (*c*) A non-empty subset H of a group G is a subgroup of G if and only if $ab^{-1} \in H$ for all $a, b \in H$. 3

2. (*a*) If H and K are two subgroups of a group G, then $H \cup K$ is a subgroup of G if and only if either $H \subset K$ or $K \subset H$. 3

   (*b*) Find the order of each of the elements of the group : $G = \{1, -1, i, -i\}$ where $i = \sqrt{-1}$. 2

   (*c*) State and prove Langrange's Theorem for finite groups. 5

Section II

3. (*a*) If f is a homomorphism of G onto G' with kernel K, then show that : $\frac{G}{K} = G'$. 4

   (*b*) Prove that a group G is abelian if and only if the mapping $f: G \to G$, given by $f(x) = x^{-1}$, is a homomorphism. 2

   (*c*) Show that the permutations (12) and (123 . . . n) generate the permutation group S_n. 4

4. (*a*) Let H be a subgroup of a group G, $S = \{Hx : x \in G\}$, then prove that there is a homomorphism θ of G onto $A(S)$ such that Ker θ is the largest normal subgroup of G contained in H. 5

   (*b*) List all the elements of A_4, where A_4 denotes the set of all even permutations in S_4. 2

   (*c*) Show that A_4 has no subgroup of order 6. 3

Section III

5. (*a*) For any group G prove that : $I(G) = \frac{G}{Z}$, where $I(G)$ is the group of inner automorphisms of G and Z is the centre of G. 3

   (*b*) Find Aut(G), if G is an infinite cyclic group. 3

(c) If $O(G) = p^n$, where p is a prime number, then $O[Z(G)] > 1$, where $Z(G)$ is the centre of G. 3

6. (a) If G is a finite abelian group in a positive integer such that m divides $O(G)$, then show that G contains a subgroup of order m. 3

(b) Find the number of conjugate classes of a non-abelian group of order p^3, p being a prime number. 3

(c) If $O(G) = p^n$, p a prime number, and if $N \neq (e)$ is a normal subgroup of G, prove that $N \cap Z \neq (e)$, where Z is the center of G. 3

Section IV

7. (a) If $O(G) = p^n$, p-prime, and H is a subgroup of G of order p^{n-1}, then show that H is a normal subgroup of G. 4

(b) What are Sylow p-groups ? State Sylow's 3rd theorem and discuss the number and nature of Sylow subgroups of a group of order 30. 5

8. (a) Show that G is an internal direct product of its normal subgroups $H_1 H_2 \ldots H_n$ if and only if :

(i) $G = H_1 H_2 \ldots H_n$

(ii) $H_i \cap (H_1 H_2 \ldots H_{i-1} H_{i+1} \ldots H_n) = \{e\}$ for $i = 1, 2, \ldots n$. 5

(b) Show that a group of order 4 is either cyclic or is an internal direct product of two cyclic subgroups each of order 2. 4

B.A./B.Sc. (Hons.)/II – 2009
Mathematics – Unit V (Algebra II)

e : 2 Hours

Maximum Marks : 38

Attempt any one question from each Section.

Section I

(a) Let G be a semi-group. Suppose there exists $e \in G$ s.t., $a.e. = a \ \forall$ $a \in G$ and also $\exists\, a' \in G$ for each $a \in G$ s.t. $a \,.\, a' = e$. Show that G forms a group. 4

(b) If $G \neq (e)$ is a group such that it has no proper subgroups, then show that G must be cyclic and of prime order. 3

(c) Define order of an element of a group G. Prove that : $o(ab) = o(a) \,.\, o(b)$ where $ab = ba$ and $(o(a), o(b)) = 1$ for $a, b \in G$. 3

(a) Let R be the set of all real numbers. Let $a, b \in R$. Define the mapping $f_{a,b} : R \to R$ s.t. $f_{a,b}(x) = ax + b \ \forall\, x \in R$.
Let $G = \{f_{a,b} : a, b \in R, a \neq 0\}$. Prove that G is a group under composite of mappings. 4

(b) Show that (I, t) is cyclic while (Q, t) is not cyclic. Also if G is a finite group and H Δ G, then show that $\frac{G}{H}$ is also finite. Is the converse true ? Justify. 3

(c) If G is a finite group whose order is a prime number p, then show that G is cyclic. 3

Section II

(a) Let ϕ be a homomorphism of a group G into a group G'. Define kernel of ϕ and show that $K_\phi \,\Delta\, G$. 4

(b) Prove that a subgroup H of a group G is normal in G iff whenever $Ha \neq Hb$ then $aH \neq bH$ where $a, b \in G$. 3

(c) If H and K are subgroups of G and $K \,\Delta\, G$, show that: $\frac{HK}{K} \cong \frac{H}{H \cap K}$. 3

(a) If G is a finite group and $H \neq G$ is a subgroup of G s.t. $0(G) \nmid (i(H))!$, where $i(H)$ denotes the index of H in G, then H contains a non-trivial normal subgroup of G. 4

(b) Show that a group G is abelian iff the mapping $f : G \to G$ s.t. $f(x) = x^{-1} \ \forall\, x \in G$ is a homomorphism. 3

(c) Prove that $A_n \,\Delta\, S_n$ where A_n consists of all the even permutations of S_n. Also show that $o(A_n) = \frac{1}{2}\, o(S_n)$. 3

Section III

5. (*a*) Define class equation of a finite group G and use it to prove that if $o(G) = p^n$ where p is a prime number and $n \geq 1$ is an integer, then $o(Z(G)) > 1$. 6

(*b*) Prove that for any group G, the set of all automorphisms Aut G, of G, is a subgroup of the permutation group $A(G)$. 3

6. (*a*) Prove that for any group G, $\frac{G}{Z} \cong I(G)$; where $I(G)$ is the group of inner automorphisms of G and Z is the centre of G. 4

(*b*) Let G be a finite group. If $a \in G$ has exactly two conjugates, then prove that G has a non-trivial normal subgroup. 3

(*c*) Give *two* elements in A_5 which are conjugate in S_5, but not in A_5. 2

Section IV

7. (*a*) Show that a group G is the internal direct product of its normal subgroups $N_1, N_2, \ldots\ldots, N_r$ iff

(*i*) $G = N_1 N_2 \ldots\ldots N_r$

(*ii*) $N_i \cap \prod_{j \neq i} N_j = (e) \quad \forall \; i = 1, 2, \ldots\ldots, r.$ 5

(*b*) State all the Sylow's theorems. Find all Sylow subgroups of A_4, the alternating group of degree 4. 4

8. (*a*) If A and B are two finite cyclic groups of orders m and n respectively. Then $A \times B$ is cyclic iff $(m, n) = 1$. 5

(*b*) Let $o(G) = p, q$, where p and q are distinct prime numbers. Also $p < q$ and $p \nmid (q - 1)$. Prove that G is cyclic. 4

B.A./B.Sc. (Hons.)/II – 2010
MATHEMATICS–Unit V
(Algebra – II)

Time : 2 Hours *Maximum Marks : 38*

Attempt any one question from each Section.

Section I

1. (*a*) Prove that a semigroup G is a group if :
(*i*) there exists $e \in G$, such that $ea = a \ \forall \ a \in G$ and
(*ii*) for each $a \in G$, $\exists\ a' \in G$ such that $a'a = e$.
Give an example to show that the conclusion does not hold if the semigroup has left identity and every element has right inverse. 5

(*b*) Prove that S_n may be generated by the cycles $f = (12 \ldots\ldots n)$ and $g = (12)$. 3

(*c*) If H and K are two normal subgroups of a group G such that $o(H)$ and $o(K)$ are relatively prime, then prove that $hk = kh$ for all $h \in H$, $k \in K$. 2

2. (*a*) Define order of an element. Is order of every element of a finite group finite. Justify you answer. Give example of an infinite group in which every element is of finite order. 4

(*b*) Let G be a group that has exactly one non-trivial proper subgroup. Prove that G is a cyclic group of order p^2, where p is a prime. 3

(*c*) We know that "if H is a subgroup of K and K is a subgroup of G, then H is a subgroup of G". Is it true for normal subgroups ? Give reasons. 3

Section II

3. (*a*) If f is a homomorphism of G onto G' with kernel $f = K$, then prove that the set of all inverse images of $g' \in G'$ under f is K_g, where g is any particular inverse image of g' in G. 3

(*b*) Find all subgroups of $\frac{Z}{(18)}$, where Z is the group of integers under addition and (18) is the subgroup of Z consisting of all multiples of 18. 4

(*c*) State and prove Cayley's theorem. 4

4. (*a*) Prove that if H is any subgroup of S_n $(n \geq 2)$, then either all permutations in H are even or exactly half are even. 4

(*b*) Prove that $(R, +) \equiv (R^+, .)$ where $(R, +)$ is the group of real numbers under addition and $(R^+, .)$ is the group of positive real numbers under multiplication. 4

(*c*) Justify : The group Z_4 under addition modulo 4 is isomorphic to U_5 under multiplication modulo 5. Give two isomorphisms between them. 2

5. (a) Prove that $Aut(S_3) \equiv S_3$

(b) Define the class equation of a [illegible] order p^n, p a prime, has non-trivial cen[illegible] order p^2 is abelian.

6. (a) Let Z be the centre of a group G. Prove that $\frac{G}{2} \equiv I(G)$, where $I(G)$ is the group of all inner automorphisms of G.

(b) Prove that two cycles is S_n are conjugate iff they are of same length

Section IV

7. (a) Let G be a finite-p-group and $H \neq G$ be a subgroup of G. Prove that $\exists\, x \in G, x \notin H$ such that $x H x^{-1} = H$.

(b) Determine the non-isomorphic groups of order 6.

8. (a) Prove that a group of order p^2q, p, q primes, $p \neq q$ cannot be simple.

(b) Define internal and external direct product of groups. If G is integral direct product of its subgroups $H_1, H_2, \ldots\ldots, H_n$ then prove that $G \equiv H_1 \times H_2 \times \ldots\ldots \times H_n$.

Practical using Mathematica for Numerical Methods and Analysis II for B.Sc. (H) Maths. Sem-III, DC-I by Sandeep Kumar

Practical using Mathematica for Calculus I for B.Sc. (H) Maths. Sem-I by Sandeep Kumar & Honey Garg

Mathematics and Statistics for Life Sciences by Shah & Garg

Rings and Vector Spaces by Sudesh Shah

Linear Algebra & Calculus by Manmohan Singh Bhasin

Mathematics I for Chemistry by S.H. Raza, for B.Sc. (H) Semester-I

Mathematics II for Chemistry by S.H. Raza, for B.Sc. (H) Semester-3

Probability and Statistics by S.H. Raza, for B.Sc. (H) Maths.

GRAPH THEORY by Sandeep Kumar & Rahul Tomar

ALGEBRA

CALCULUS (Differential & Integral)

REAL ANALYSIS

MATHEMATICAL ANALYSIS

TWO DIMENSIONAL GEOMETRY

THREE DIMENSIONAL GEOMETRY

VECTOR CALCULUS

DIFFERENTIAL EQUATIONS.

STATISTICS

ABSTRACT ALGEBRA (Group Theory)

ABSTRACT ALGEBRA (Ring Theory)

LINEAR ALGEBRA

PARTIAL DIFFERENTIAL EQUATIONS

DYNAMICS (Mechanics-II)

ANALYSIS II (Metric Spaces)

PROBABILITY& MATH. STATISTICS

TOPICS IN REAL ANALYSIS For Physics (H), Sem.-3, Paper-PHHT-310

TOPICS IN ANALYSIS & STATISTICS For Phy. (H.), Sem.-4, Paper-PHHT-413

CALCULUS & GEOMETRY (Paper-MAPT 202) for II Sem. Phy.Sci.

ALGEBRA (MAPT 303) for III Semester B.Sc. IInd year, Physical Sciences

DIFFERENTIAL EQUATIONS, Paper-MAPT 404, Sem.-4, Phy. Sciences

REAL ANALYSIS, Paper-MAPT 505, Semester-5, Physical Sciences

MECHANICS, Paper-MAPT 606, Semester-6, Physical Sciences

ELEMENTS OF ANALYSIS (for Economics Hons.)

VARDHMAN PUBLICATIONS
EDUCATIONAL PUBLISHERS
98-UB, JAWAHAR NAGAR, DELHI-7 (Ph.: 23855542)
e-mail : vardhmanpublications@gmail.com