



CSIR-NET

Council of Scientific & Industrial Research

MATHEMATICAL SCIENCE

VOLUME - III



INDEX

1. Caylays theorem	1
2. Ring theory	32
3. Ideal value	80
4. Ring homomorphism	102
5. Integral domain	120
6. Polynomial ring	135

Cayley's Theorem:

Every finite group of order n is isomorphic to some subgroup of S_n .

$$f: S_n \longrightarrow A_{n+2}.$$

$$f(\sigma) = \begin{cases} \sigma & : \sigma \text{ is even.} \\ \sigma(n+1, n+2) & \sigma \text{ is odd.} \end{cases}$$

clearly f is 1-1 homo.

$$S_n \cong f(S_n) < A_{n+2}.$$

" S_n is isomorphic to some subgp of A_{n+2} ."

(A_{n+3}, A_{n+4}, \dots)

Thus every group of order n is isomorphic to some subgp of $A_{n+2}, A_{n+3}, A_{n+4}, \dots$

Generalized Cayley's Theorem (G.C.T)

If G is finite group and G has proper subgroup of index n . (say H) then $\exists \phi: G \xrightarrow{\text{homo}} S_n$

s.t that

$$\ker \phi \subseteq H$$

**
Corollary

Let p be the smallest prime divisor of order of G and if there exist a subgp of index p (say H) then H is normal in G .

Index Theorem:

If G is a finite group and G has proper subgroup of index n and $o(G) \nmid n!$
 $\Rightarrow G$ can not be simple.

G is finite, ...
 and $\text{ind}_G H = n$.

By C.T.

$$\phi: G \rightarrow S_n$$

s.t. $\ker \phi \subseteq H$.

if $\ker \phi = \{e\}$.

By F.T.H.

$$G \cong \phi(G) < S_n$$

$$\Rightarrow o(G) \mid n!$$

$$q \nmid o(G) \nmid n!$$

$$\Rightarrow \ker \phi \neq \{e\}$$

$$\text{And } \ker \phi \neq G \quad (\because \ker \phi \subseteq H)$$

$\ker \phi$ is proper normal subgroup of G .

$\Rightarrow G$ can not be simple gp

Example:-

$$o(G) = 108 = 2^2 \cdot 3^3$$

$$H < G \text{ and } o(H) = 3^3$$

$$\text{ind}_G H = 4$$

$$o(G) \nmid 4!$$

$$\Rightarrow 108 \nmid 4!$$

$\Rightarrow G$ can not be simple gp.

Example: $-o(a) = 24 = 2 \cdot 3 \cdot 2$
 $H < G$ and $o(H) = 2^3$

$$\text{ind}_G H = 3.$$

$$24 \neq 3!$$

$\Rightarrow G$ can not be simple.

Embedding Theorem:

If G is finite simple group and G has a proper subgroup of index n then G is isomorphic to some subgroup of A_n .

If G is finite simple group and $\text{ind}_G H = n$.

By G.C.T
 $\exists \phi: G \xrightarrow{\text{hom.}} S_n$

$$\text{ker } \phi \subseteq H.$$

$$\text{ker } \phi = \{e\}.$$

$$\text{ker } \phi = G \quad \text{X.}$$

$$\therefore \text{ker } \phi = \{e\}.$$

By F.T.H.

$$G \cong \phi(G) < S_n.$$

subgroup $\phi(G)$ contains exactly half even and half odd.

$$K = \{ \sigma : \sigma \text{ is even} \}$$

clearly $K < \phi(G)$

$$\text{ind}_G H = \frac{o(\phi(G))}{o(K)} = 2.$$

$$\Rightarrow K \trianglelefteq \phi(H)$$

$\phi(H)$ can't be simple

But $G \cong \phi(H)$ ($\because G$ is simple)
 ~~\times~~

$\therefore \phi(H)$ contains all even permutations

$$G \cong \phi(H) \text{ and } o(G) \mid n!/2$$

Corollary. If G is finite group and has a proper subgp of index n and $o(G) \nmid n!/2$

$\Rightarrow G$ can not be simple.

Corollary \therefore

If G is a finite group and has a proper subgp of index < 5 . then G can not be simple

Case-I

$$\text{ind}_G H = 2$$

$H \triangleleft G$.

$\Rightarrow G$ can not be simple.

Case-II

$$\text{ind}_G H = 3.$$

Suppose G is simple

$$G \cong K < A_3.$$

$$\text{ind}_G H = 3.$$

$$o(G) = 3 \cdot o(K).$$

$$o(G) \geq 6$$

$$o(K) \geq 6$$

$$K < A_3. \quad \times$$

G can not be simple.

$$\text{ind}_q^n = 4$$

subgroup G is simple.

$$G \cong K \subset A_4.$$

$$o(G) \geq 8.$$

$$o(K) \geq 8.$$

$$\text{and } o(K) \mid 12$$

$$\Rightarrow o(K) = 12.$$

$$\therefore A_4 = K$$

$$G \cong A_4 \quad \times \quad (\because A_4 \text{ is not simple})$$

G is cannot be simple.

Example:-

$$G = A_5.$$

$$o(G) = 60$$

$$A_5 = \text{simple.}$$

Possible orders of subgrp $\rightarrow 1, 2, 3, 4, 5, 6, 10, 12$

$$18, 20, 30, 60$$

$\times \quad \times \quad \times \quad \checkmark$

Through out possible orders of proper subgrp $\rightarrow 12$.

Note: If G is simple group of order 60 then G is isomorphic to A_5 .

Sylow rule

p-group:-

A group G is said to be p-group if $\forall g \in G, \exists n \in \mathbb{N}$ s.t. $o(g) = p^n$.

Example:- Q_8 is 2-group.

(i) $(P(n), \Delta)$ is 2-group.

(ii) $Z_7 \times Z_7$ is 7-group.

(iii) $H = \left\{ \frac{m}{2^n} + Z : m \in Z, n \in \mathbb{N} \cup \{0\} \right\}$

2-group

$G = \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} : a, b, c \in Z_p \right\}$

$o(G) = p^3$, G is non-abelian group.

$\therefore G$ is p-group.

$o(Z(G)) = p$.

Note:- A finite group is said to be p-group.

iff $o(G) = p^n$ for some $n \in \mathbb{N}$.

p-Sylow's Subgroup (p-SSG).

Let H be subgroup of G s.t. $o(H) = p^m$.

and $p^{m+1} \nmid o(G)$ then the subgroup of order p^m is defined as p-SSG.

Example:- $o(G) = 108 = 2^2 \cdot 3^3$
 order of 2-SSG = 2^2
 order of 3-SSG = 3^3

Theorem:-

$$\begin{aligned} \text{order of } GL(n, \mathbb{Z}_p) &= (p^n - p^{n-1})(p^{n-1} - p^{n-2}) \dots (p - 1) \\ &= p^{n-1} p^{n-2} \dots p^2 p \\ &= (p-1)(p-1) \dots (p-1) \\ &= p^{\sum_{k=1}^{n-1} k} \cdot R. \end{aligned}$$

$\text{order of } p\text{-SSG} = p^{\sum_{k=1}^{n-1} k}$

$\therefore \text{order of } p\text{-SSG in } GL(n, \mathbb{Z}_p) = \text{order of } p\text{-SSG in } SL(n, \mathbb{Z}_p) = p^{\sum_{k=1}^{n-1} k}$

Example:- No. of 5-SSG of S_6 is

- (i) 16 (ii) 6 (iii) 36 (iv) 4

$$\begin{aligned} &= 7 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = 2^4 \cdot 3^2 \cdot 5 \\ &= 720 \end{aligned}$$

120

$$\begin{array}{r} 81 \overline{) 720} \\ 81 \overline{) 720} \end{array}$$

order of 6-SSG in $S_6 = 5$.

$$\begin{aligned} \text{No. of 8-SSG in } S_6 &= \frac{6 \times 4 \times 3 \times 2}{4} \\ &= 36 \end{aligned}$$

Normalizer of a subgroup:-

Let $H \leq G$.

Then normalizer of H is defined as

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

clearly $N(H) \leq G$.

Properties

(i) $H \triangleleft N(H)$

(ii) $H \triangleleft G \iff N(H) = G$.

(iii) If $H \triangleleft K$ then $K \leq N(H)$

(iv) $\frac{|G|}{|N(H)|} = [G : N(H)] = \text{ind}_G N(H)$, G is finite.

Sylow's First Theorem:

If $p^a \mid |G|$ then \exists at least one subgroup of order p^a .

Example: $|G| = 108 = 2^2 \cdot 3^3$.

There are subgroups of order = 2

$$= 4$$

$$= 3$$

$$= 3^2$$

$$= 3^3.$$

Application:-

$$|G| = p^n, \quad n \neq 1$$

By cyclic 1st Theorem,

$$\exists H < G \text{ s.t. } |H| = p^{n-1}$$

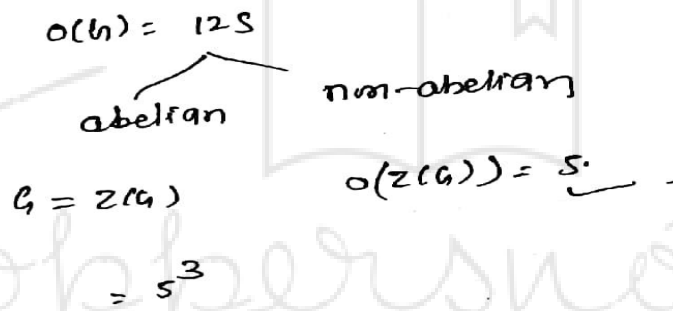
$$\text{ind}_G H = p$$

$$\Rightarrow H \triangleleft G \quad \text{By (G.C.T.)}$$

$\Rightarrow G$ can't be simple.

Problem:- Let G be a group of order 125, which of the following statements are necessarily true.

- i) G has a non-trivial abelian subgroup ✓
- (ii) $Z(G)$ is proper subgroup. ✗
- (iii) $Z(G)$ has order 5. ✗
- (iv) There is a subgroup of order 25. ✓



By 1st Sylow's Theorem -
 There is a subgroup = 5
 = 25.

Sylow's second Theorem:

All p -SSG are conjugate.

* Corollary:-

p -SSG is unique iff p -SSG is normal.

Sylow's 3rd Theorem :-

$$\text{No. of } p\text{-SSG} = 1 + kp \mid \frac{O(G)}{p^m}$$

where p^m is order of p -SSG

$$k = 0, 1, 2, 3, \dots$$

Example:-

$$o(G) = 56$$

$$\text{order of 2-SSG} = 23$$

$$\text{order of 7-SSG} = 7.$$

$$\begin{aligned} \text{No. of 2-SSG} &= 1 + 2k \mid 7 \\ &= 1, 7 \end{aligned}$$

$$\begin{aligned} \text{No. of 7-SSG} &= 1 + 7k \mid 8 \\ &= 1, 8. \end{aligned}$$

Case-I

$$\text{No. of 7-SSG} = 1.$$

\Rightarrow 7-SSG is unique.

\Rightarrow 7-SSG is normal.

\Rightarrow G cannot be simple.

Case-II

$$\text{No. of 7-SSG} = 8$$

$$H_1, H_2, \dots, H_8.$$

$$o(H_i) = 7.$$

total no. of elements of order 7 = $6 \times 6 = 42$.

\Rightarrow 2-SSG is unique.

\Rightarrow 2-SSG is normal.

\Rightarrow G can not be simple.

Hence $o(G) = 56$ can not be simple group.

Example:- $O(n) = 2 \times 3 \times 5$.

order 2-SSG = 2

order 3-SSG = 3

order 5-SSG = 5

No. of 2-SSG = $1 + 2k \mid 15$
 $= 1, 3, 5, 15$.

No. of 3-SSG = $1 + 3k \mid 10$
 $= 1, 10$

No. of 5-SSG = $1 + 5k \mid 6$
 $= 1, 6$

suppose No. of 3-SSG = 10

No. of 5-SSG = 6

H_1, H_2, \dots, H_{10} are 3-SSG.

$O(H_i) = 3$

total no. of elements of order 3 = $2 \times 10 = 20$

K_1, K_2, \dots, K_6 are 5-SSG.

$O(K_i) = 5$.

total no. of elements order 5 = $4 \times 6 = 24$

total no. of elements of order 3 and 5
 $= 20 + 24 = 44$

~~X~~

Either $2 - 2 > 1$ or $2 - 2 < 1$
 $\Rightarrow G$ can't be simple.

Theorem:- $O(G) = p \cdot q$, $p < q$, and $p \nmid q-1$
 then G is cyclic.

order of p -SSG = p

order of q -SSG = q .

$$\text{No. of } q\text{-SSG} = 1 + qk \mid p$$

$$\begin{aligned} \text{No. of } p\text{-SSG} &= 1 + pk \mid q \\ &= 1, q \end{aligned}$$

suppose No. of p -SSG = q .

$$1 + pk = q$$

$$p \cdot k = q - 1$$

$$\Rightarrow p \mid q - 1 \quad \times$$

\therefore No. of p -SSG = 1

let H be p -SSG and K be q -SSG.

$$H \triangleleft G, \quad K \triangleleft G.$$

$$O(H) = p, \quad O(K) = q.$$

$$H \cap K = \{e\}.$$

$\exists a \in G$ and $b \in G$ s.t.

$$H = \langle a \rangle \quad \text{and} \quad K = \langle b \rangle.$$

In particular, $ab = ba$.

$$\langle a \rangle \cap \langle b \rangle = \{e\}$$

$$\begin{aligned} o(ab) &= \text{l.c.m.}(o(a), o(b)) \\ &= pq = o(G) \end{aligned}$$

$\Rightarrow G$ is cyclic group.

Application:-

$$o\left(\frac{G}{Z(G)}\right) \neq pq, \quad p < q \text{ and } p \nmid q-1.$$

Example $o(G) = 60 = 2^2 \times 3 \times 5$.

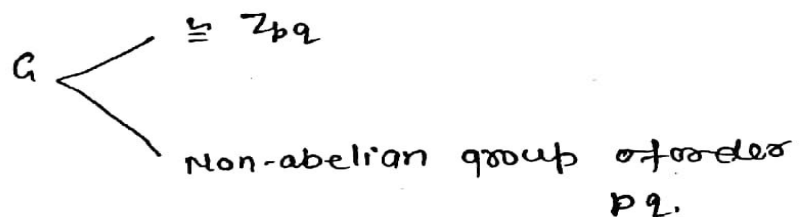
$$o(Z(G)) = 4.$$

$$o\left(\frac{G}{Z(G)}\right) = 15 \quad \checkmark$$

$o(Z(G))$ can not be four.

Theorem :-

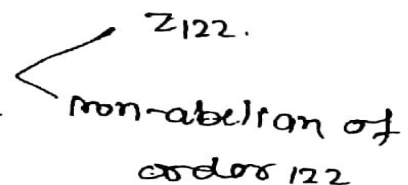
$$o(G) = p \cdot q, \quad p < q \text{ and } p \nmid q-1$$



Problem :- The total of no of non-isomorphic groups of order 122 is

- (a) 2 (b) 1 (c) 61 (d) 4

$$o(G) = 122 = 2 \times 61$$



Problem :- Let $G = D_8$...
 order can:

- (a) $2S$ \times (b) $5S$ \checkmark (c) $12S$ \checkmark (d) $3S$ \times

Example:- Every group of order 30 has cyclic subgp of order 15.

$$O(G) = 30 = 2 \times 3 \times 5$$

$$\text{No. of 3-SS } G = 11 \cdot 0$$

$$\text{No. of 5-SS } G = 1 \cdot 6$$

Case-I

$$\text{No. of 3-SS } G = 1$$

$$\text{No. of 5-SS } G = 6$$

Let H be 3-SS and $O(H) = 3$
 $H \triangleleft G$.

Let K be 5-SS and $O(K) = 5$.

We know that $H \triangleleft G, K \leq G$.

$$\Rightarrow HK < G$$

$$O(HK) = 15$$

Case-II

up to isomorphism: group of order 30.

- Z_{30} - abelian
- D_{15} \rightarrow Non-abelian
- $S_3 \times Z_5$ \rightarrow Non-abelian
- $D_8 \times Z_3$ \rightarrow Non-abelian.

$S_5 \times S_7$ S_6
 No subgroup order is cyclic.

$$\frac{720}{3 \times 2} = 12$$

Theorem: Every group of order pqr can't be simple.

$\frac{7!}{30 \times 2}$

$$|G| = pqr, \quad p < q < r.$$

$$\text{order of } p\text{-Syl} = p$$

$$\text{order } q\text{-Syl} = q$$

$$\text{order } r\text{-Syl} = r$$

$$\begin{aligned} \text{No. of } p\text{-Syl} &= (1 + kp) \mid qr \\ &= 1, r, q, qr \end{aligned}$$

$$\begin{aligned} \text{No. of } q\text{-Syl} &= (1 + kq) \mid pr \\ &= 1, r, pr \end{aligned}$$

$$\begin{aligned} \text{No. of } r\text{-Syl} &= (1 + kr) \mid pq \\ &= 1, pq. \end{aligned}$$

$$\text{Suppose no. of } p\text{-Syl} = q$$

$$\text{no. of } q\text{-Syl} = r$$

$$\text{no. of } r\text{-Syl} = pq.$$