

The Sylow Theorems and their Applications

Rameez Ahmad Dar*

Department of Mathematics, Kulgam, India

Abstract: In this article we will discuss some applications of Sylow theorem and briefly we will go through the converse of langranges theorem on finite groups.

Keywords: Groups, cyclic group, Simple group, Sylow subgroup.

1. Introduction

In mathematics, specifically in the field of the finite group theory, the sylow theorems are collection of theorems named after the Norwegian mathematician Pater Ludwig Sylow (1872) that give detailed information about the number of sub groups of fixed order that given finite group contains, the Sylow theorems forms a fundamental part of finite group theory and have important application of finite simple group

The sylow theorem form a fundamental part of group theory and have an implications on finite simple groups. Further this theorems also asserts of langrange's theorem

2. Introductory definitions

1) Definition 1

Cyclic subgroup; Let G be a group with $a \in G$, then $\langle a \rangle = \{a^n, n \in \mathbb{Z}\}$ is subgroup of G is called the cyclic subgroup generated by a and a is called Generator.

2) Definition 2

Order of an element and group; Let G be a group and $a \in G$. The Order of an element $a \in G$ is the least positive integer n such that $a^n = e$ and is denoted by $o(a)$. If no such n exists for a then order of $o(a) = \infty$

Also the number of elements of G is called the order of group G denoted by $o(G)$

E.g. $G = [z, +]$ then order of $G = \infty$

$G = [Zn, +]$ then order of $G = n$

3) Definition 3

Let G be a group, if $a \in G$, we say $b \in G$ is conjugate of 'a' denoted $a \sim b$ if there exists some $x \in G$ such that $xax^{-1} = b$

- \sim is an equivalence relation on G

4) Definition 4

- Given a group and a subgroup N of G . We say that N is normal subgroup of G if it is closed with respect to conjugation that is for any $a \in N$ and $x \in G$, we have that $xax^{-1} \in N$

5) Definition 5

P group –if order of G is equal to p^n then G is called p -group
 E.g. if $o(G) = 64 = 2^6$ is called 2-group

- G be a group and K is P -SSG of G then for all $g \in G$

the conjugate gKg^{-1} of K is also a P -SSG

- **Langrange's theorem;** if G is a finite group and H is a sub group of G then $o(H)$ divides $o(G)$
- $H = \langle R90 \rangle$ is a subgroup of $D4$ such that $o(H) = 4$ then by Langrange's theorem, $o(H)/o(D4) = 4/8$

If d does not divides order of G then G has no subgroup of order d

Eg. 5 does not divides $o(Z14)$ then $Z14$ has no subgroup of order 5.

B. Converse of Langranges Theorem

i.e., if d divides $o(G)$ then G may or may not have a subgroup of order d

Proof; we will prove that the converse of langrange's theorem need not be true with the help of following example

We know that $o(A4) = 12$ and $6 / o(A4)$. Now we show that $A4$ has no subgroup of order 6

$A4 = \{ e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), (1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 4), (2\ 3\ 4), (4\ 3\ 2), (4\ 3\ 1), (4\ 2\ 1), (3\ 2\ 1) \}$ and

$O(A) = 12$ and $A4$ has elements of order 1, 2 and 3. Let H is subgroup of $A4$ of order 6 then $H \approx Z6$ or $S3$. if $H \approx Z6$ then H has elements of order 6, since H is subgroup of $A4$ then $A4$ has elements of order 6. But $A4$ has no element of order greater than 3 then H is not isomorphic to $Z6$

If $H \approx S3$, then H has 1 element of order 1, 3 elements of order 2, and 2 elements of order 3

$H = \{ e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), a, a^{-1} \}$, where $a \in A4$ and $o(a) = 3$

Now $H' = \{ e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3) \}$ subset of H

Now we will show that H' is group with operation of $A4$.

	E	(12)(34)	(13)(24)	(14)(23)
E	E	(12)(34)	(13)(24)	(14)(23)
(12)(34)	(12)(34)	e	(14)(23)	(13)(24)
(13)(24)	(13)(24)	(14)(23)	E	(12)(34)
(14)(23)	(14)(23)	(13)(24)	(12)(34)	E

Then H' is group of order 4, H' is subgroup of H .

By Lagrange's theorem $o(H')/o(H) \Rightarrow 4/6$ but 4 does not divides 6 then supposition is wrong

Hence $A4$ has no subgroup of order 6

C. Definition Simple group

A group G is said to be simple group if G has exactly two normal subgroups $H = \{e\}$ and $H = G$

- Q If G is group of order P then G is always simple
 Hint; if $o(G) = P$ then $G \approx Zp$ and Zp has $t(p)$ normal

*Corresponding author: rahirameez1995@gmail.com

sub groups then G has exactly two normal sub groups then G is simple

- Q if G is cyclic group then G is simple
Hint; need not, we will prove this with the help of the example

Let $G = Z_{15}$ is cyclic group and Z_{15} has exactly $\tau(15) = \tau(3 \times 5) = (1+1)(1+1) = 4$ normal subgroups

Then $G = Z_{15}$ is not simple

e.g. is $G = Z_4 \times D_6$ simple

solution ; we know that $Z_4 \times \{Ro\}$ is normal subgroup of $Z_4 \times D_6$ other than $H = \{e\}$ and $H = Z_4 \times D_6$

then $Z_4 \times D_6$ is not simple

- note ; if $o(G_1) > 1$ and $o(G_2) > 1$ then $G_1 \times G_2$ is not simple

Hint ; $G_1 \times \{e_2\}$ is normal subgroup of $G_1 \times G_2$ other than $H = e$ and $H = G$ then $G_1 \times G_2$ is not simple

D. Cauchy's theorem for finite group

If G is a finite group and P is a prime number such that P divides $o(G)$ then there exist an element 'a' different from 'e' such that $a^P = e$ i.e. $o(a) = P$

- Remark ; If G is a finite group and P is a prime number such that P divides $o(G)$ then there exist an element 'a' different from 'e' such that $a^P = e$ i.e. $o(a) = P$
- Then G has element of order P ,
- Then G has a cyclic sub group of order P and the number of elements of order P in G is equal to the multiple of $\phi(P)$

Example if $O(G) = 100$ and $5/o(G)$ then G has elements and then number Of elements of order 5 = $\phi(5) = 4$

- If $o(G) > 1$ and G is finite then G has subgroup of order P
- Solution; If $o(G) > 1$ then there exists a prime number P such that $P/o(G)$ then by Cauchy's theorem G has elements of order p

Then $H = \langle a \rangle$ is a subgroup of G order P then G has subgroup of order P.

E. Main point of sylow theorem

Motivation for the sylow theorems comes from attempting to determine the validity of the converse of Lagrange's theorem. To review Lagrange's theorem says that the order of any subgroup H of some group G will divide the order of G. The converse of this could then be that if there exists $n \in \mathbb{N}$ such that $n/O(G)$ then G has some subgroup H such that $o(H) = n$. The first sylow theorem serves to determines when this converse actually holds and classifies various sub group of group G based on order. The second and third sylow theorems classifies the relations between the some of the subgroups of G that are equal in size.

1) Sylow's Ist theorem

Let G be a group .If P is a prime number and p^n divides $o(G)$ then (G) has a subgroup of order p^n

e.g. if $o(G) = 100$ then G has subgroup of order 5 and 25

Hint order of G =100 and $5/o(G)$ then G has subgroup of order 5

$5^2/o(G)$ then G has subgroup of order $5^2 = 25$

2) P -sylow's subgroup or P-SSG

Let G be a finite group and $p^n /o(G)$ but p^{n+1} does not divides $o(G)$ then the subgroup of order p^n is called p-sylow subgroup or P-SSG

Example; let $o(G) = 60$ then $2^2/o(G)$ but 2^{2+1} does not divides $o(G)$ then the subgroup of order $2^2 = 4$ is called 2-sylow subgroup or 2-SSG

- Q; find order of q-SSG in $GL_n[Fq]$

Hint; if $G = GL_n[Fq]$ then we know that $o(GL_n[Fq]) = (q^n - q^{n-1})(q^n - q^{n-2}) \dots (q^n - 1) = q^{n-1}(q-1) q^{n-2}(q^2-1) \dots (q^n - 1) = q^{(n-1)+(n-2)+\dots+2+1}(q-1)(q^2-1) \dots q^{n-1} = q^{n(n-1)/2} \cdot m$

where $m = (q-1)(q^2-1) \dots (q^{n-1}-1)$ and $\gcd(q, m) = 1$

Now $q^{n(n-1)/2}$ divides $o(GL_n\{fq\})$ but $q^{\frac{n(n-1)}{2}+1}$ does not divides $o(GL_n\{fq\})$

Then $GL_n\{fq\}$ has q-SSG of $q^{n(n-1)/2}$

- Remark; order of q-SSG in $GL_n\{fq\}$ is same as order of q-SSG in $SL_n\{fq\}$

Note: If H is subgroup of G and $x \in G$ then its conjugate that is $xHx^{-1} = \{xhx^{-1} / h \in H\}$ is subgroup of G

Soln; let G be group and H is subgroup of G and $e \in H$ then $xhx^{-1} = xex^{-1} \in xHx^{-1}$

Then $e = xex^{-1} \in xHx^{-1}$ then it is non empty subset of G

Now let $a = xHx^{-1}$ then $a = \{h\} \in H$

$b \in xHx^{-1}$ then $b = xh_2x^{-1}, h_2 \in H$ such that $ab^{-1} = (xh_1x^{-1})(xh_2x^{-1})^{-1} = xh_1h_2^{-1}x^{-1} = xh'x^{-1} \in xHx^{-1}$,

then xHx^{-1} is a subgroup of G

Sylow 2 theorem:

Any two P-SSG of G are conjugate that is H and K are two P-SSG of G then there exists $x \in G$ such that $K = xHx^{-1}$

- ❖ Example Show that any two 2-SSG of S_3 are conjugate

Solution; $G = S_3 = \{e, (1 2), (1 3), (2 3), (1 2 3), (1 3 2)\}$

$O(S_3) = 6 = 2 \times 3, 2/o(G)$ but 2^2 does not divides $o(G)$ then $G = S_3$ has 2-SSG of order 2

That is subgroup of order 2 of S_3 is 2-SSG

2-SSG of S_3 are $H_1 = \{e, (1 2)\}, H_2 = \{e, (1 3)\}, H_3 = \{e, (2 3)\}$

Now show that H_2 and H_3 are conjugate, let $x = (1 2) \in S_3$ such that $(1 2)H_2(1 2)^{-1} = \{(1 2)h_2(1 2)^{-1} / h_2 \in H_2\}$ Now show that H_2 and H_3 are conjugate, let $x = (1 2) \in S_3$ such that $(1 2)H_2(1 2)^{-1} = \{(1 2)h_2(1 2)^{-1} / h_2 \in H_2\}$

$= (1 2)\{e, (1 3)\}(1 2)^{-1} = \{e, (2 3)\} = H_3$ then $H_3 = (1 2)H_2((1 2)^{-1})$

Then H_2 and H_3 are conjugate

3) Sylow 3 theorem

If G be a finite group the number of (P-SSG) or p-sylow subgroup in G is equal to $1 + PK$ such that $1 + PK / o(G)$ that is $np = 1 + PK$ such that $1 + PK / o(G)$ where $K = 0, 1, 2, \dots$

- Example if $O(G) = 21$ then find number of subgroups of Order 3 in G

Solution if $o(G) = 21 = 3 \times 7$, then $3/o(G)$ but 3^2 does not divides $O(G)$ then the subgroup of order 3 is 3-SSG then $n_3 = 1 + 3K$ such that $1 + 3K$ divides $O(G)$

If $K=0$ then $n_3=1$ and $1/O(G)$ then $n_3=1$ is possible

If $K=1$ then $n_3=4$ and 4 does not divide $O(G)$ then $n_3=4$ is not possible

If $k=2$ then $n_3=7$ and 7 divides $O(G)$ then $n_3=7$ is possible

If $k=3$ then $n_3=10$ but 10 does not divide $n_3=10$ is not possible

Similarly $K=4,5,\dots$ are not possible for 3-SSG

Then $n_3=1$ and $n_3=7$ are possible for 3-SSG

- Note; G has unique p -sylow subgroup or p -SSG iff P -SSG is normal

Hint ; let H is P -SSG of G of order p^n and p -SSG is unique , since H is p -SSG of order p^n then p^n divides order of G but p^{n+1} does not divide order of G . now H is subgroup of G then $XHX^{-1}, x \in G$ is a subgroup of G and $O(XHX^{-1}) = o(H) = p^n$ but p^{n+1} does not divide $o(G)$. Since G has a unique P -SSG then $xHX^{-1} = H$ for all $x \in G$ then H is normal sub group of G

Conversely, Let P -SSG is normal. Let H and k are two P -SSG of (G) then by Sylow's 2 theorem there exist $x \in G$ such that $K = XHX^{-1}$ (1)

Since P -SSG is normal then $XHX^{-1} = H$ for all $x \in G$ (2)

From 1 and 2 we get

$K = H$ then G has unique P -SSG

Example: if $O(G) = 40 = 2^3 \times 5$ and G is abelian now $2^3/o(G)$ but 2^{3+1} does not divide $O(G)$ then G has 2-SSG of order 8, since G is abelian then 2-SSG of G is normal then 2-SSG is unique then G has unique subgroup of order 8

Note: if $o(G) = Pq$, $P < q$ and G is abelian then G is cyclic

Hint; $O(G) = pq$ and G is abelian

$P/o(G)$ but p^{1+1} does not divide $o(G)$ then the subgroup of order p is P -SSG. Since G is abelian then P -SSG is normal then P -SSG is unique,

Then G has exactly 1 subgroup of order P . Then number of elements of order P in $G = \phi(P) = P-1$ now $q/o(G)$ but q^{1+1} does not divide $o(G)$ then subgroup of order q is q -SSG since G is abelian then q -SSG is normal then q -SSG is unique, then number of elements of order $q = \phi(q) = q-1$ and G has exactly one element of order 1

Total number of elements of order 1, p and q in $G = 1 + p - 1 + q - 1 = P + q - 1 < pq = o(G)$.

Then G has elements of order other than 1, P and q

G has elements of order pq then G is cyclic then $G \approx Z_{pq}$

- Q ; if $o(G) = 39$ and G is non abelian then find the number of normal subgroup in G

Solution; $o(G) = 3 \times 13$ and G is non abelian then G has one subgroup of order 1, 13 subgroups of order 3, one subgroup of order 13 and one subgroup of order 39

Since $H = \{e\}$ and $H = G$ is always normal subgroups of G then subgroups of order 1 and 39 are normal subgroups

Normal subgroups of order 3; $3/o(G)$ but 3^{1+1} does not divide $o(G)$ then the subgroup of order 3 is 3-SSG and 3-SSG is not unique Then 3-SSG is not normal .

Subgroups of order 13;

$13/o(G)$ but 13^{1+1} does not divide $o(G)$ then the subgroup of order 13 is 13-SSG

Now 13-SSG of G is unique then it is normal

Then G has unique normal subgroup of order 13

Then total number of normal subgroups in $G = 1 + 1 + 1 = 3$

3. Conclusion

- Converse of Lagrange's theorem need not be true.
- If G is finite group and prime no. p divides order of G then Group G has elements of order p .
- A cyclic group need not be simple.
- Order of q -sylow subgroups in general linear matrix group over finite field F_q is $q^{n(n-1)/2}$.
- Group G has unique p -sylow subgroup if p -sylow subgroup is normal.
- If G is abelian and $O(G) = pq$, $p < q$ then G is cyclic.
- If G is non abelian group and $O(G) = 39$ then G has 3 normal subgroups.

References

- J. A. Gallian, "Contemporary Abstract Algebra," ISBN-1305887859, 9781305887855
- V. K. Khanna and S. K. Bhambri, "A Course in Abstract Algebra."
- D. S. Dummit, and R. M. Foote, "Abstract Algebra," 3rd Edition, ISBN-9780471433347 -10:0471368792
- W. K. Nicholson, "Introduction to Abstract Algebra," 4th Edition, John Wiley and Son's INC, Hoboken N. J, 2012.