IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Sylow theorems and their applications

Rameez Ahmad Dar.

Research scholar of Desh Bhagat University, Mandi Gobindgarh, Punjab.

Dr.Rama kumari, Professor of Desh Bhagat University, Mandi Gobindgarh, Punjab.

ABSTRACT: In this paper, we will discuss the concept of group and we will discuss the different groups like as dihedral group and the order of alternative groups, symmetric group, quaternion group etc. The sylow theorems are three powerful theorems. In modern algebra which helps us to show that group of certain order is not simple.

Key words: Groups, cyclic Groups, finite groups, simple groups, subgroups, normal subgroups and sylow p-subgroups.

Introduction

when studying group theory one notice almost immediately that groups of prime power orders are great significance, with Cauchy's , Lagrange's and Sylow 's theorems being three good examples of this. The study of these so called p-groups, where p is prime number, can for example be used to give a clear understanding of other groups as being compositions of different p-groups.

The sylow theorems are collection of theorems named after the Norwegian mathematician Pater Ludwig sylow (1872) that give detailed information about the number of subgroups of fixed order that given finite groups contains, the sylow theorems forms a fundamental part of finite group theory and have important application of finite simple group. Further this theorem also asserts of Lagrange's theorem.

Definition 1: Let X be a non empty set and $*$ is any operation. Then (X,$*$) is said to group if
(1) *Closure property :* $\forall$ a , $b\epsilon$ X, then the element a$*$b$\in X$

(2) *Associative property* : $(a*b)*c = a*(b*c)$ $\forall$ a, b, c $\in$ X
(3) *Identity :* $\exists$ e $\in G$ such that $e*a = a = a*e$ $\forall$ aϵG

(4) *Inverses:* for each a ϵ G there exists an inverse element $a^{-1} \epsilon\, G$ *such that* $a^{-1}a = aa^{-1} = e$

Theorem 1.1 :- let G be a group, if G has exactly one element of order one, then this element is unique.

Proof :- let $a, b \in G$ such that o (a) = 1 and o (b) = 1

If o (a) = 1 then a = e ...... (1)

If o (b) = 1 then b = e .... (2)

From equation (1) and (2), we get

a = b

Then G has unique element of order one.

Definition 2 :

A group G is said to be Abelian group if $ab = \mathrm{ba}\ \forall\ \mathrm{a, b} \in \mathrm{G}$

Theorem 2.1 :- if every element of group G has self inverse then G is Abelian group.

With the help of theorem 2.1, one can show that K_4 $(klein\ four\ group)$ is an Abelian group

Solution We know that $K_4 = \{e, a\ , b, ab | a^2 = e, b^2 = e, ab = ba\}$

Now $e \in K_4\ then\ e^{-1} = e\ ,$

$a \in K_4\ such\ that\ a^2 = e\ then\ a^{-1} = a$

And similarly $b \in K_4 such\ thatb^2 = e\ then\ b^{-1} = b$

Now $ab \in K_4 \Rightarrow (ab)^{-1} = b^{-1}a^{-1} = ba = ab$

$\Rightarrow (ab)^{-1} = ab$

Then every element of K_4 has self inverse

∴ By above theorem K_4 is an Abelian group

Definition 3 : A group G is said to be a finite group if the set G has a finite number of elements. In this case, the number of elements is called the order of G, denoted by $O(G)$

Definition 4: Let G be a group and $a \epsilon G$ then order of element $a \epsilon G$ is the least positive integer n such that $a^n = e$ and is denoted by $O(a) = n. if$ then a is said to have a finite order

If no such n exists for a then $O(a) = \infty$ then a is said to have infinite order

The order of elements in Z_6 is evaluated as follows

Solution: Z_6 is finite group of order 6 with identity zero, then $o(0) = 1$,

$$1 \in Z_6 \ such\ that \quad 6.1 = 0\ then\ o(1) = 6$$

$$2 \in Z_6\ such\ that\ 3.2 = 0\ then\ o(2)$$

$$3 \in Z_6\ such\ that\ 2.3 = 0\ then\ o(3) = 2,$$

$$4 \in Z_6\ such\ that\ 3.4 = 0\ then\ o(4) = 3\ ,\ and$$

$$5 \in Z_6\ such\ that\ 6.5 = 0\ then\ o(5) = 6$$

Therefore, Z_6 has one element of order 1, one element of order 2, two elements of order 3 and two elements of order 6

The order of elements of Q_4 (Quaternion group of order 8) is evaluated as follows:

Solution: we know that $Q_4 = \{\pm 1, \pm i, \pm j, \pm k \mid ij = -ji = k, jk = -kj = j, ki = -ik = j\}$ is group with identity 1 then $O(1) = 1$

$$-1 \in Q_4\ such\ that\ (-1)^2 = 1\ then\ O(-1) = 2,$$

$$i \in Q_4\ such\ that\ (i)^4 = 1\ then\ O(i) = 4,$$

$$-i \in Q_4\ \ such\ that\ (-i)^4 = 1\ then\ O(-i) = 4,$$

Similarly, $O(j) = 4,\ O(-j) = 4,\ O(k) = 4,\ and\ O(-k) = 4$

Then Q_4 has one element of order 1, one element of order 2 and six element of order 4

Definition 5: A group G is said to be a cyclic group if ∋ element $a \epsilon G$ such that every element of G is generated by 'a' that is $G = < a >$ such that

$G =< a > = \{\mathrm{a}^{\mathrm{n}} \setminus n \epsilon \mathrm{z}\}$, Then element a is called generator of G

Definition 6 : Let $\varphi \neq H \subseteq G$,H is subgroup of G if H is itself group with operation of G.

Proper subgroup: Let H be subgroup of G and H ≠ ***G*** is called a proper subgroup of G, while as H = G and H = {e} is called improper subgroup of G.

Dihedral ($\boldsymbol{D_n}$): it is denoted by D_n. And defined by

$D_n = \{x^i . y^j | x^2 = e, y^n = e, xy = y^{-1}x, i = 0,1\ and\ j = 0,1,2, \dots n-1\}\ and\ O(D_n) = 2n$

Example of dihedral group

$$D_4 = \{R_0, R_{90}, R_{180}, R_{270}, H, V, D, \dot{D}\}$$

The dihedral group D_4 is the symmetry group of the square.

Let S=ABCD be the square.

The various mappings of S are:

The identity mapping R_0, the rotations are R_{90}, R_{180}, R_{270} around the centre of S anticlockwise respectively

The reflections H and V are reflections in the x and y axis respectively.

The reflection D in the diagonal through vertices A and C

The reflection Ḋ in the diagonal through vertices B and D

Lagrange's theorem: The order of any subgroup of a finite group divides the order of a group.

Example: H=<R_{90}> is subgroup of a group $G = D_4$ such that O (H) = 4 and O $(D_4) =$ 8

Therefore, by Lagrange's theorem

O (H) / O (G) =4/8

Remark: if d does not divides order of G; Then G has no subgroup of order d.

Example: Q_4 is a group of order 8 and 6 does not divides 8, And then Q_4 has no subgroup of order 6.

Converse of Lagrange's theorem need not be true

That is if d /O (G) then G has may or may not be subgroup of order d.

Example:

$G = A_4$ Then $O(A_4) = 12$ and 6/ O (A_4) but A_4has no element of order 6 or A_4 has no subgroup of order 6.

Definition 7 :A subgroup H of group G is said to be normal subgroup of G if $\forall\ x \in G\ and\ \forall\ h \in H\ such\ that\ \ x\,H\,x^{-1} \in H$

Preposition 3:

If $xHx^{-1} \in H \quad \forall\, h \in H \;\; and\, \forall\, x \in G$

Then $xHx^{-1} \subseteq$ H $\forall\, x \in G$ and H $\subseteq xHx^{-1}$

From above two equations we get

$$xH\,x^{-1} = H$$

This implies $xH = Hx\, \forall\, x \in G$

Then every left coset of H in G is right coset of H in G

That is $xH = Hx\, \forall\, x \in G$ iff H is normal subgroup of G.

Definition 8: A group G is said to be simple group if G has exactly two normal subgroups H= {e} and H=G.

Example: $\boldsymbol{A_5}$ has exactly two normal subgroups then $\boldsymbol{A_5}$ is simple group.

Theorem 8.1: If G is group of prime order p then G is always simple.

Solution: if G is group of prime order p then G $\approx Z_p$ and Z_p has $\tau(p)$ normal subgroups then G has exactly two normal subgroups

Then G is simple group.

Note: the number of positive divisors of n is denoted by $\tau(n)$.

If n=1 then $\tau(1) = 1$.If n>1 then $n = {p_1}^{r_1}.{p_2}^{r_2} \dots {p_k}^{r_k}$

$\Rightarrow \tau(n) = ({p_1}^{r_1}.{p_2}^{r_2} \dots {p_k}^{r_k}) = (r_1 + 1)(r_2 + 1) \dots (r_k + 1)$

Example: $Z_{15}$is cyclic group of order 15 and Z_{15} has exactly $\tau(15) = \tau(3)\tau(5) = (1 + 1)(1 + 1) = 4$ normal subgroups

$\Rightarrow$ Z_{15} is not simple group.

Also we can show that if $O(G_1) > 1$ *and* $O(G_2) > 1$ *then* $G_1 \times G_2$ *is not simple*

Solution: we already know that with help of above theorem that $G_1 \times \{e_2\}$ *and* $\{e_1\} \times G_2$ are the normal subgroups of $G_1 \times G_2$ other than H= {e} and $H = G_1 \times G_2$ then $G_1 \times G_2$ is not simple.

Definition 9: if $O(G) = p^n$. Where p is prime number, Then G is called p-group

Example: if G is group of order 64 then $O(G) = 64 = 2^6$ is called 2-subgroup.

Sylow p-subgroup of a finite group (p- SSG): if 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 sylow p-subgroup

Example: let $O(G) = 60.$ *and* $2^2/O(G)$ but 2^2does not divides O (G) then the subgroup of order $\mathbf{2^2} = \mathbf{4}$ is called 2-ssg

Cauchy's theorem for finite Abelian groups: suppose G is a finite Abelian group and p /O (G), where p is a prime number. Then their exists $\boldsymbol{a}(\neq \boldsymbol{e}) \in \boldsymbol{G}$ such that $\boldsymbol{a^p} = \boldsymbol{e}$.if G is finite abelian group and a positive integer k divides O(G).then G contains a subgroup of order k.

Sylow first theorem

If G is finite group and p^n / $O(G)$ then G has subgroup of order p^n.

Example: if G is finite group of order 10.then G has subgroup of order 5 and 25.

Solution: Since $O(G) = 100.$ *then* $5/O(G)$ then G has subgroup of order 5

Now $5^2/O(G)$ then G has subgroup of order 5^2.

Theorem: let $G = S_{20}$ (symmetric group of order 20!), then find the order of 7-sylow subgroups in G.

Proof $G = S_{20}$ then $O(S_{20}) = 20!$

=1.2.3.4.5.6.7.8...13.14.15....20

$=7^2(1.2.3 \ldots 6.8 \ldots .13.2.15 \ldots 20)$

$=7^2.m$ where m =1.2...6.8.....13.2.15...20 and gcd (7, m) =1

Now $7^2/O(S_{20})$ but 7^{2+1} does not divides $O(S_{2o})$. then S_{20} has 7-sylow subgroup of order $7^2 = 49$.

Theorem: let $G = A_{20}(alternative\ group\ of\ order\ \frac{20!}{2})$ and H is 7-sylow subgroup of A_{20}. Then show that $O(H) = 49$ and any 7-sylow subgroup of S_{20} is subset of A_{20}.

Proof: G = A_{20} and O (A_{20})= $\frac{20!}{2}$

$$=\frac{1.2.3 \ldots 6.7.8 \ldots\ldots 13.14.15 \ldots 20}{2}$$

$$=\frac{7^2(1.2.3 \ldots 6.8 \ldots 13.2.14 \ldots 20)}{2}$$

$=7^2.m$ *and* $\gcd(m, 7) = 1$

Now $7^2/O(A_{20)}$ But 7^{2+1} does not divides $O(A_{20})$.

Then order of 7-sylow subgroup in A_{20} is $7^2 = 49$. Which implies O (H) =49.

Thus 7-sylow subgroup in S_{20} is same 7-sylow subgroup in A_{20}.

Then any 7-sylow subgroup of $S_{20}$is subset of A_{20}.

Sylow 2nd theorem:

Let G be a finite group then any two p-sylow subgroups of G are conjugate.

That is let H and K are two p-sylow subgroups of G then there exists $x \in G$ such that $K = xHx^{-1}$.

Theorem: let $G = S_3$ (symmetric group of order 3!). Then show that any two 2-sylow subgroups of $\boldsymbol{S_3}$ are conjugate.

Proof: let $G = S_3$ then O $(S_3) = 6 = 2 \times 3$.

Then 2/O (S_3) then 2^{1+1}does not divide $O(S_3)$ then S_3 has 2-sylow subgroup of order 2. That is the subgroup of order 2 is 2-sylow subgroup of S_3.

Now 2-sylow sub group of S_3 are $H_1 = \{ I, (1,2)\},\ H_2 = \{I, (1,3)\}, \quad and\ H_3 = \{I, (2,3)\}$.

Next, we will show that $H_2\ and\ H_3$ are conjugate.

Let $x = (1,2) \in S_3$ such that $xH_2x^{-1} = (1,2)H_2(1,2)^{-1}$

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

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

$$= \{I, (2, 3)\} = H_3$$

$\Rightarrow H_3 = (1,2)H_2(1,2)^{-1}, (1,2) \in S_3$

then H_2 *and* H_3 Are conjugates

Example: show that H= {I, (1, 2)} and K= {I, (2, 3)} are conjugates?

Solution: let $x = (1,3) \in S_3$

Such that (1, 3) K$(1,3)^{-1} = (1,3)\{I, (2,3)\}(1,3)^{-1}$

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

$$= \{I, (1, 2) = H$$

Then H and K are conjugates.

Sylow 3rd theorem

Let G be a finite group and p, a prime number such that p/O(G).Then number of p-sylow subgroups is of the form to1+pk, where k is some non-negative integer such that 1+pk/O(G).

Example: if $O(G) = 14$. then sylow subgroups of order 7 in G can be calculated as.

Solution: $O(G) = 14 = 2 \times 7$.

Now 7^1/O (G) But 7^{1+1} does not divides O (G)

Then the subgroups of order 7 are 7-sylow subgroup.

Then $n_7 = 1 + pk$

Put k=0, then $n_7 = 1\ and 1/O(G)$ then $n_7 = 1$.

Put k=1 then $n_7 = 8$ but 8 does not divides O (G).then $n_7 = 8$ is not possible for 7-sylow subgroup of G

Put k=2 then $n_7 = 15\ But$ 15/O (G) then $n_7 = 15$ are not possible for 7-sylow subgroup of G

Similarly k =3, 4, 5, 6... Are not possible for 7-sylow subgroup of G

Then $n_7 = 1$ then G has unique subgroup of order 7`

Theorem: if O (G) =21. Then the number of subgroups of order 3 in G can be calculated as

proof: O (G)=21 =3×7 then 3^1/O(G) but 3^{1+1} does not divides O(G), then subgroups of order 3 is 3-sylow subgroups of G.

Then $n_3 = 1 + 3k$ such that 1+3k/O (G)

Put k=0, then $n_3 = 1$ and 1/O (G). Then $n_3 = 1$ is possible for 3-sylow subgroup of G

Put k=1 then $n_3 = 4$ but 4does not divides O (G), then $n_3 = 4$ is not possible for 3-sylow subgroup of G

Put k=2 then $n_3 = 7$ and 7/O (G) then $n_3 = 7$ is possible for 3-sylow subgroup of G.

Put k=3 then $n_3 = 10$ but 10 does not divides O (G), then $n_3 = 10$ is not possible for 3-sylow subgroup of G

Similarly, k=4, 5, 6 ...are not possible for 3-sylow subgroups of G.

Then $n_3 = 1$ or $n_3 = 7$ is possible for 3-sylow subgroup of order 3 of G.

Theorem: Group G has unique p-sylow subgroup if and only if p-sylow subgroup is normal.

Theorem: if order of group G is 12.then the subgroup of order 3 is normal?

Proof: since $O(G) = 12 = 2^2 \times 3$ then 3/ O (G) But 3^{1+1} does not divide O (G). Then G has 3-sylow subgroup of order 3.

Now $n_3 = 1 + 3k$ - - - - (1)

Put k=0 then $n_3 = 1\ and 1/O(G)$

Then $n_3 = 1$ is possible for 3-sylow subgroup

Put k=1 then $n_3 = 4\ and\ 4/O(G)$

Then $n_3 = 4$ is also possible for 3-sylow subgroup

Then $n_3 = 1\ and\ n_3 = 4$ both are possible for 3-sylow subgroup of G

Then the subgroup of order 3 of G may or may not be normal

Theorem: if order of group G is 39 and G is non-abelian, then find number of normal subgroups of G.

Proof; O (G) = 39 = 3×13 and G is non-abelian group. Then G has one subgroup of order one, 13 subgroups of order 3, 1 subgroup of order 13 and 1 subgroup of order 39.

Since H= {e} and H=G is always normal subgroups of G, then the subgroups of order 1 and 39 are normal subgroups of G.

Subgroups of order 3:

3/O (G) but 3^{1+1} does not divides O (G), then the subgroups of order 3 is 3-sylow subgroups of G.

Then $n_3 = 1 \; and \; n_3 \; = 13$ both are possible for 3-sylow subgroup

Then 3-sylow subgroup of G is not unique.

Then 3-sylow subgroup of G is not normal.

Subgroups of order 13:

13/ O (G), but 13^{1+1}does not divides O (G).then the subgroup of order 13 is 13 –sylow subgroup of G.

$\Rightarrow n_{13} = 1 + 13k$

Put k=0 then $n_{13} = 1 \; and \; 1/O(G)$ then $n_{13} = 1$ is possible for 13-sylow subgroup.

Similarly k=1, 2, 3 . . . are not possible for 13-sylow subgroup of G.

Now 13-sylow subgroup of G is unique.

Therefore, 13-sylow subgroup of G is normal.

Then G has unique normal subgroup of order 13.

∴ G has exactly three normal subgroups, one of order 1, one of order 13 and one of order 39.

Theorem: if G is Abelian group of order 40. Then number of subgroups of order 8 in G can be calculated as

Proof: we have $O(G) = 40 = 2^3 \times 5$ and G is Abelian group.

Now $2^3/$O (G), but 2^{3+1} does not divides O (G). Then G has 2-sylow subgroup of order 8

$\Rightarrow n_2 = 1 \; and \; n_2 = 5$ both are possible for 2-sylow subgroup of order 8.}

Since G is abelian then 2-sylow subgroup of G is normal.

Then 2-sylow subgroup of G is unique.

Then G has unique subgroup of order 8.

Theorem: show that the subgroups of order 2 are not normal in $\boldsymbol{S_3}${symmetric group of order 3!}.

Proof: let $G = S_3$ then O (G) = 6 = 2×3. ⇒ 2/O (G) but 2^{1+1} does not divides O (G).

Then the subgroup of order2 is 2-sylow subgroup of G and $\boldsymbol{S_3}$ has 3 subgroup of order 2.

Then 2-sylow subgroup of S_3 is not normal.

Then the subgroups of order 2 of S_3 are not normal.

Theorem: show that the subgroup of order 4 of A_4 is normal subgroup of A_4.

Proof: $O(A_4) = \frac{4!}{2} = 2^2 \times 3. \Rightarrow 2^2/O(A_4)$ but 2^{2+1} does not divides $O(A_4)$.

Then the subgroup of order 4 of A_4 is 2-sylow subgroup of A_4.

$\{n_2 = 1 + 2k$. Then $n_2 = 1$ *and* $n_2 = 3$ both are possible for 2-sylow subgroup of $A_4\}$

Since A_4 have exactly 3 elements of order 2 and no element of order 4.

Then A_4 has unique subgroup of order 4.

Then the subgroups of order 4 or 2-sylow subgroup of A_4 is unique.

Then 2-sylow subgroup of A_4 is normal.

Therefore, the subgroup of order 4 of A_4

Conclusion

(1) Every group has exactly one element of order one and this element is unique

(2) Symmetric group of order 20! has sylow 7-subgroup of order 7^2

(3) Sylow 7-subgroup of symmetric group of order 20! Is same as sylow 7-subgroup of alternative group of order $\frac{20!}{2}$

(4) Any two sylow 2-subgroups of symmetric group of order 6 are conjugate.

(5) Group of order 14 has unique sylow 7- subgroup of order 7.

(6) If G is non-abelian group of order 39 then G has exactly three normal subgroups of order 1, 13 and 39.

(7) Any sylow 2-subgroups of order 2 are not normal in symmetric group of order 6.

(8) The subgroups of order 4 is normal subgroup of alternative group of 12

Reference

(1) "Contemporary abstract algebra" by Joseph A. Gallian. ISBN-1305887859, 9781305887855.

(2) "A course in Abstract Algebra" by V.K. Khanna and S.K.

(3) Bhambri, second edition, Vikas publication House Pvt. limit,1999,0 "Abstract Algebra" by I.N.Hersterin, ISBN 70698675X, 9780706986754

(4) "A first court in Abstract Algebra"(7th edition) by- J.B.Fraleigh, IBSN-13:9780201763904

(5) "Abstract Algebra"(3rd edition) by David S.Dummit ,Richard M.Foote,ISBN-9780471433347-10;0471368792

(6) Concard K. Consequences of the sylow theorems. Available at http://www.math.uconn.edu/kconrad/blurds/grouptheory/sylowapp.pdf

(7) Fang, J.(1963).Abstract Algebra. Schaum publishing company.

(8) McKiernan, J sylow's theorem and application , http://math.mit,edu/mckernan/teaching/12-13/spring/18.703/L13.pdf

(9) J. Farleigh, A first course in Abstract Algebra, Addison- Wesley publishing company, Redding, MA (1968).

(10) W. Keith Nicholson, Introduction to abstract Algebra: forth edition. John wiley and sons INC, Hoboken, Nj(2012)

(11) Idelhaj, A. (2016). The sylow theorem and their applications. Available at http://math.uchicago.edu/may/REU2016/REUPapers/Idelhaj.pdf