International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Group Action and Sylow Theorems with Applications

Vedansh Rathore[1], Ashish Kumar[2], Chinta Mani Tiwari[3]

[1]Student, MSOS, Maharishi University of Information Technology, Lucknow, U.P., India
[2,3]Faculty, MSOS, Maharishi University of Information Technology, Lucknow, U.P., India

Abstract:
This dissertation explores the concepts of Group Actions and Sylow Theorems in finite group theory and highlights their importance in understanding the structure of groups. The study begins with the basic ideas of groups, subgroups, cyclic groups, and permutation groups, followed by a detailed explanation of group actions through orbits, stabilizers, and conjugacy classes. It further examines Sylow's First, Second, and Third Theorems, which help in determining the existence, number, and properties of prime power subgroups in finite groups. The dissertation also discusses applications of these theorems in classifying finite groups and analyzing their internal structure. Examples such as symmetric, cyclic, dihedral, and alternating groups are included to explain the concepts clearly. Overall, this work emphasizes the significance of group actions and Sylow theorems as important tools in modern abstract algebra.

Keywords: Group Theory, Group Actions, Sylow Theorems, Finite Groups, Abstract Algebra

Introduction:

Group theory is one of the most important branches of modern mathematics and plays a significant role in understanding algebraic structures and symmetry. It provides a systematic way to study mathematical objects through operations that satisfy specific rules. The concept of a group is widely applied in different areas such as geometry, physics, chemistry, computer science, and cryptography. In mathematics, group theory helps in analyzing patterns, transformations, and symmetries that occur in various structures.

A group is a set combined with an operation that satisfies four important properties: closure, associativity, identity, and inverse. Based on these properties, different types of groups such as cyclic groups, permutation groups, and abelian groups are studied. Understanding the structure of groups is important because it helps mathematicians classify and analyze complex mathematical systems. Subgroups, normal subgroups, quotient groups, and homomorphisms are some fundamental concepts used to investigate the internal structure of groups.

Among the important topics in group theory are Group Actions and Sylow Theorems, which provide powerful methods for studying finite groups. A group action describes how the elements of a group interact with or transform the elements of a set while preserving its structure. Through concepts such as orbits, stabilizers, and conjugacy classes, group actions help explain symmetry and simplify the study of algebraic systems. These ideas are useful not only in abstract algebra but also in combinatorics, geometry, and representation theory.

Sylow Theorems, introduced by the Norwegian mathematician Ludwig Sylow, are fundamental results in finite group theory. These theorems provide information about the existence, number, and conjugacy of

subgroups whose order is a power of a prime number, known as Sylow p-subgroups. The First Sylow Theorem guarantees the existence of such subgroups, the Second Sylow Theorem explains their conjugate relationship, and the Third Sylow Theorem gives conditions on their number. These results are highly useful in determining the structure and classification of finite groups.

This dissertation focuses on the study of Group Actions and Sylow Theorems along with their applications in finite group theory. By exploring theoretical concepts and examples involving cyclic, symmetric, dihedral, and alternating groups, this work aims to provide a better understanding of subgroup structures and symmetry. Overall, the study highlights the importance of these concepts as essential tools in modern abstract algebra.

Methodology:

This work is based on a theoretical and analytical study of finite group theory, with special emphasis on Group Actions and Sylow Theorems. The study begins with the collection and review of standard books, research papers, journals, and mathematical references related to abstract algebra and finite groups. Fundamental concepts such as groups, subgroups, cyclic groups, normal subgroups, conjugacy classes, and permutation groups are studied in detail. The methodology further includes the analytical examination of group actions through orbits, stabilizers, class equations, and conjugation actions. Sylow's First, Second, and Third Theorems are explored using theorem-based proofs and logical derivations. Various examples involving symmetric groups, dihedral groups, cyclic groups, and quaternion groups are used to illustrate theoretical concepts. Applications of group actions and Sylow theorems in classifying finite groups and understanding subgroup structures are also discussed to establish their significance in modern algebra.

Theorem 1 (Fundamental theorem)

Let G be a group and let X be a set, If X is a G-set, then the action of G on X induces a homomorphism $\phi : G \to S_X$. Any homomorphism $\phi : G \to S_X$ induces an action of G onto X.

Proof.

We define $\phi : G \to S_X$ by $(\phi(a))(x) = ax$, $a \in G$, $x \in X$. Clearly $\phi(a) \in S_X$, $a \in G$. Let $a,b \in G$. Then $(\phi(ab))(x) = (ab)x = a(bx) = a((\phi(b))(x)) = (\phi(a))((\phi(b))(x) = (\phi(a)\phi(b))(x)$ for all $x \in X$.

Hence, $\phi(ab) = \phi(a)\phi(b)$. Define $a \star x = (\phi(a))(x)$; that is, $ax = (\phi(a))(x)$.Then $(ab)x = (\phi(ab))(x) = (\phi(a)\phi(b))(x) = (\phi(a)(\phi(b)(x))) = \phi(a)(bx) = a(bx)$. Also, $ex = (\phi(e))(x) = x$. Hence, X is a G-set.

Theorem 2 (Cayley's theorem)

Let G be a group. Then G is isomorphic into the symmetric group S_G. Proof. By Theorem.1 there exists a homomorphism. $\phi : G \to S_G$,

where $(\phi(a))(x) = ax$, $a \in G$, $x \in G$. Suppose $\phi(a)$ is the identity element in S_G. Then for all $x \in G$, $(\phi(a))(x) = x$. This implies $ax = x$ for all $x \in X$, and hence $a = e$, the identity in G. Therefore, ϕ is injective.

Example for A_3 (Order 3): The even permutations in S_3 are e and the 3cycles (1 2 3) and (1 3 2). The cycle structure of (1 2 3) has distinct odd lengths (a single cycle of length 3). The centralizer of (1 2 3) in S_3 is $\langle(1\ 2\ 3)\rangle = \{e,(1\ 2\ 3),(1\ 3\ 2)\}$, which contains only even permutations.

Thus, the conjugacy class of (1 2 3) in S_3, $\{(1\ 2\ 3),(1\ 3\ 2)\}$, remains a single conjugacy class in A_3. The conjugacy classes of A_3 are $\{e\}$, $\{(1\ 2\ 3),(1\ 3\ 2)\}$.

Example for A_4 (Order 12): The even permutations in S_4 have cycle structures (1, 1, 1, 1), (2, 2), and (3,1).
(1, 1, 1, 1): {e}, size 1.
(2, 2): {(1 2)(3 4),(1 3)(2 4),(1 4)(2 3)}. The centralizer in S_4 contains even and odd permutations, so this remains a single class of size 3 in A_4.
(3, 1): {(1 2 3),(1 3 2),(1 2 4),(1 4 2),(1 3 4),(1 4 3),(2 3 4),(2 4 3)}. These are 3-cycles. The conjugacy class of a 3-cycle in S_4 has size 8 and consists of even permutations.
The centralizer of (1 2 3) in S_4 is ⟨(1 2 3)⟩, containing only even permutations.
Thus, the S_4 conjugacy class splits into two classes of size 4 in A_4: {(123),(134),(142), and {(1 3 2),(1 2 4),(1 4 3),(2 3 4)}. The conjugacy classes of A_4 have sizes 1, 3, 4, 4.

Theorem (First Sylow Theorem)
Let G be a finite group, and let p be a prime. If $p^m \mid |G|$, then G has a subgroup of order p^m.
Proof. We prove the theorem by induction on n = |G|. If n = 1, the result is obvious. So let us assume that the result holds for all groups of orders less than n.
If the order of the center of G is divisible by p, then it follows from Cauchy's theorem for abelian groups3 that the center of G contains an element a of order p. The cyclic group C generated by a is clearly normal in G, and the quotient group G/C has order n/p, which is divisible by p^{m-1}. Therefore, by the induction hypothesis, G/C contains a subgroup H/C of order p^{m-1}, proving the theorem in this case.
Now consider the case when the order of the center is not divisible by p.The class equation of G is

$$n = |G| = |Z(G)| + \sum_a [G : N(a)]$$

where summation runs over one element from each conjugate class having more than one element. Now p | n, but p ∤ |Z(G)|. Hence, p | [G : N(a)] for some a ∈ G, a /∈ Z(G). This implies that $p^m \| |N(a)|$ and |N(a)| < |G|.
By the induction hypothesis N(a) has a subgroup of order p^m, and this yields the required subgroup of G.

Theorem (Second Sylow Theorem):-Let G be a finite group of order $p^r m$, where p > 0 is a prime number, r,m ∈ N and gcd(p,m) = 1. Then any two Sylow p-subgroups of G are conjugate, and hence are isomorphic.
Proof. Let H and K be two Sylow p-subgroups of G. Let $L_H := \{aH \mid a \in G\}$ be the set of all left cosets of H in G. Since G is finite, so is the set L_H. Define a map $\sigma : K \times L_H \to L_H$ by $\sigma(b,aH) = (ba)H$, $\forall (b,aH) \in K \times L_H$. If $aH = a'H$, for some $a,a' \in G$, then $(ba)^{-1}(ba') = a^{-1}b^{-1}ba' = a^{-1}a' \in H$, and hence $(ba)H = (ba')H$, for all b ∈ K. Therefore, the map σ is well-defined. It is easy to check that σ is a left action of K on L_H. Th e subset of all elements of L_H with singleton K-orbits is given by

$$\begin{aligned} L_{H,0} &:= \{aH \in L_H \mid baH = aH, \forall b \in K\} \\ &= \{aH \in L_H \mid aba^{-1} \in H, \forall b \in K\} \\ &= \{aH \in L_H \mid aKa^{-1} \subseteq H\} \\ &= \{aH \in L_H \mid aKa^{-1} = H\}, \end{aligned}$$

since both H and K are finite Sylow p-subgroups of G, they have the same cardinality. Since K is a finite p-group, considering the class equation for L_H associated to the K-action σ on it, we have

$$|L_H| \equiv |L_{H,0}| \pmod{p}.$$

Since H is a Sylow p-subgroup of G, we see that $p \nmid [G : H]$. Therefore, $|L_H| = [G : H] \not\equiv 0 \pmod p$, which implies $|L_{H,0}| \not\equiv 0 \pmod p$. In particular, $|L_{H,0}| \geq 1$, and hence there exists $a \in G$ such that $aKa^{-1} = H$. Since for any $a \in G$, the conjugation by a map

$$c_a : G \to G, \quad c_a(g) = aga^{-1}, \quad \forall g \in G,$$

is an automorphism of G, we conclude that any two Sylow p-subgroups of G are isomorphic. This completes the proof.

Theorem (Third Sylow Theorem)

Let G be a finite group of order $p^r m$, where $p > 0$ is a prime number, $r,m \in N$ and $\gcd(p,m) = 1$. Let n_p be the number of Sylow p-subgroups of G. Then $n_p \equiv 1 \pmod p$, for some $k \in N \cup \{0\}$, and $n_p \mid m$.

Proof. Let $X = Syl_p(G)$ be the set of all Sylow p-subgroups of G.

Note that $X \not= \emptyset$ by Sylow's first theorem.

Let $P \in X$. Note that P acts on X by conjugation:$P \times X \to X$, $(a,Q) \mapsto aQa^{-1}$.

Let $X_0 := \{Q \in X \mid aQa^{-1} = Q, \forall a \in P\}$.

For $Q \in X_0$ to be arbitrary, $aQa^{-1} = Q$, for all $a \in P$, we have $P \subseteq N_G(Q)$.

Let both P and Q be Sylow p-subgroups of G contained in $N_G(Q)$.

By Sylow's second theorem3.2 applied to $N_G(Q)$, P and Q are conjugate in $N_G(Q)$.

Therefore, there exists $n \in N_G(Q)$ such that $nQn^{-1} = P$. But $n \in N_G(Q)$ implies $nQn^{-1} = Q$. Hence $P = Q$, and hence $X_0 = \{P\}$ is singleton. By Lemma3.1 we have $|X| \equiv |X_0| \pmod p$, and hence $n_p = |X| \equiv 1 \pmod p$, for some $k \in N \cup \{0\}$.

For the second part, we consider the conjugation action of G on X. Since any two Sylow p-subgroups of G are conjugate by Sylow's second theorem (Theorem 2.14.11), we see that X has only one G-orbit, i.e., $X = Orb_G(P) = \{aPa^{-1} \mid a \in G\}$,for any Sylow p-subgroup P of G. Since the stabilizer of $P \in X$ is $G_P = \{a \in G \mid aPa^{-1} = P\} = N_G(P)$, the normalizer of P in G, by the Orbit-Stabilizer Theorem, we have

$$\begin{aligned} n_p = |X| &= [G : N_G(P)] \\ &= \frac{|G|}{|N_G(P)|} \\ &= \frac{p^r m}{|N_G(P)|}. \end{aligned}$$

Since $P \subseteq N_G(P) \subseteq G$, we have $|P| = p^r$ divides $|N_G(P)|$, so $|N_G(P)| = p^r \cdot |N_G(P)|_m$, where $|N_G(P)|_m$ divides m. Thus,

$$n_p = \frac{p^r m}{p^r |N_G(P)|_m} = \frac{m}{|N_G(P)|_m}$$ and hence $n_p \mid m$. This completes the proof.

Applications Of Sylow Theorems

1) Groups of Order 15

Let $|G| = 15 = 3^1 \cdot 5^1$. By Sylow's Third Theorem:

The number of Sylow 3-subgroups, n_3, satisfies $n_3 \equiv 1 \pmod 3$ and $n_3 \mid 5$.

The only possibility is $n_3 = 1$.

The number of Sylow 5-subgroups, n_5, satisfies $n_5 \equiv 1 \pmod 5$ and $n_5 \mid 3$. The only possibility is $n_5 = 1$.

Since $n_3 = 1$, the Sylow 3-subgroup P_3 is normal in G. Similarly, the Sylow 5subgroup P_5 is normal in G. As $|P_3| = 3$ and $|P_5| = 5$ are coprime, $P_3 \cap P_5 = \{e\}$, and $G \tilde{=} P_3 \times P_5 \tilde{=} Z3 \times Z5 \tilde{=} Z15$. Thus, any group of order 15 is cyclic.

2) Groups of Order 21

Let $|G| = 21 = 3^1 \cdot 7^1$. By Sylow's Third Theorem:

The number of Sylow 7-subgroups, n_7, satisfies $n_7 \equiv 1 \pmod 7$ and $n_7 \mid 3$, implying $n_7 = 1$. The Sylow 7-subgroup $P_7 \tilde{=} Z7$ is normal.

The number of Sylow 3-subgroups, n_3, satisfies $n_3 \equiv 1 \pmod 3$ and $n_3 \mid 7$, implying $n_3 = 1$ or $n_3 = 7$.

If $n_3 = 1$, the Sylow 3-subgroup $P_3 \tilde{=} Z3$ is also normal, and $G \tilde{=} P_3 \times P_7 \tilde{=} Z21$ (cyclic). If $n_3 = 7$, there exists a non-abelian group of order 21, a semidirect product of Z7 by Z3.

3) **Groups of Order 30** are Not Simple

Let $|G| = 30 = 2 \times 3 \times 5$. By Sylow's Third Theorem:

$n_5 \equiv 1 \pmod 5$ and $n_5 \mid 6 \Rightarrow n_5 = 1$ or 6.

$n_3 \equiv 1 \pmod 3$ and $n_3 \mid 10 \Rightarrow n_3 = 1$ or 10.

$n_2 \equiv 1 \pmod 2$ and $n_2 \mid 15 \Rightarrow n_2 = 1,3,5,$ or 15.

If G were simple, $n_5 \neq 1$ (so $n_5 = 6$) and $n_3 = 1$/ (so $n_3 = 10$). The $6\times(5-1) = 24$ elements of order 5 and $10\times(3-1) = 20$ elements of order 3, plus the identity, would require 24+20+1 = 45 elements, exceeding the order of G. Thus, G cannot be simple.

Lemma- Let G be a finite group and let N be a normal subgroup of G. If $x \in G$ and $\gcd(o(x),|G/N|) = 1$, then $x \in N$.

Proof. Let $o(x) = r$ and $|G/N| = s$. Then there exist integers $a,b \in Z$ such that $ar + bs = 1$. Therefore, $Nx = (Nx)^{ar+bs} = (Nx^r)^a(Nx^s)^b = N^a(Nx^s)^b = (Nx^s)^b = N^b = N$. Hence, $x \in N$.

The Group A_5 is Simple

Proof. A_5 is a group of order 60. By Cauchy's theorem, A_5 has elements of order 2, 3 and 5.

Any element of order 5 in A_5 is of the form $(x_1x_2x_3x_4x_5)$, where $x_1,\ldots,x_5$ are distinct.

Thus, there are $(5 \times 4 \times 3 \times 2 \times 1)/5 = 24$ elements of order 5 in A_5.

Any element of order 3 in A_5 is of the form $(x_1x_2x_3)$, where x_1,x_2,x_3 are distinct.

Thus, there are $(5 \times 4 \times 3)/3 = 20$ elements of order 3 in A_5.

Any element of order 2 in A_5 is of the form $(x_1x_2)(x_3x_4)$, where x_1,x_2,x_3,x_4 are distinct.

Thus, there are $\frac{1}{2} \times \frac{5\times4}{2} \times \frac{3\times2}{2} = 15$ elements of order 2 in A_5.

Let $N \lhd A_5$ and $|N| > 1$.

Then by Lagrange's theorem $|N| = 2,3,4,5,6,10,12,15,20$ or 30.

- If $|N| = 5,10,15$ or 20, then $\gcd(5,|G/N|) = 1$. By Lemma 4.1,4.3 N has all elements of order 5, and so $|N| \geq 24$, a contradiction.
- If $|N| = 3,6$ or 12, then $\gcd(3,|G/N|) = 1$. By Lemma 4.1,4.3 N has all elements of order 3, and so $|N| \geq 20$, a contradiction.
- If $|N| = 4$ or 12, then $\gcd(2,|G/N|) = 1$. By Lemma 4.1,4.3 N has all elements of order 2, and so $|N| > 15$, a contradiction.
- If $|N| = 30$, then $|G/N| = 2$, and so by Lemma 4.1,4.3 N has all elements of order 5 as well as all elements of order 3. Thus, $|N| \geq 24 + 20 = 44$, a contradiction.

Now the only possibility is that $|N| = 2$ so for this Let $|N| = 2$ and $G = A_5/N$. Then $|G| = 30$.

Now either Sylow 5-subgroup or Sylow 3-subgroup of G is normal.
Otherwise, G will have six Sylow 5-subgroups or ten Sylow 3-subgroups, each of order 3.
Therefore, $|G| \geq 6 \times 4 + 10 \times 2 = 44$, a contradiction.
Thus, G has a subgroup S such that $S \lhd G$ and $|S| = 3$ or 5.
The inverse image H of S under the canonical epimorphism $A_5 \rightarrow G$ is a normal subgroup of A_5, and $|H| = 6$ or 10. This is a contradiction.
Hence, A_5 is simple.

Any Simple Group of Order 60 is Isomophic to A_5

Proof. Let G be a simple group of order 60. Then G has six Sylow 5-subgroups, each of order 5 and has either five or fifteen Sylow 2-subgroups, each of order 4. First suppose that G has five Sylow 2-subgroups.
Let P be a Sylow 2-subgroup of G.
Since Sylow 2-subgroups form single conjugacy class, so $[G : N_G(P)] = 5$.
Now assume that G has fifteen Sylow 2-subgroups. If any two of these subgroups intersect at {1}, then G has $15 \times 3 = 45$ nonidentity elements of 2-power order.
Also as G has six Sylow 5-subgroups, each of order 5, so G has 24 elements of order 5.
But then $|G| > 45 + 24 = 69$, a contradiction.
Therefore, if P and Q are any two Sylow 2-subgroups of G, then $P \cap Q \neq \{1\}$.
Since. $|\langle P, Q\rangle| = \frac{|P||Q|}{|P \cap Q|} = \frac{4 \times 4}{2} = 8$.
Now, if $x \in P \cap Q$ then $\langle P,Q\rangle \leq C_G(x)$ as P and Q are abelian.
Thus, $|C_G(x)| \geq 8$.
Also, as $P \leq C_G(x)$, $|C_G(x)|$ is a multiple of 4 and is a factor of 60.
Therefore, $|C_G(x)| = 12$ or 20. If $|C_G(x)| = 20$, then $|G : C_G(x)| = 3$, a contradiction (Since, if G is finite non -abelian simple group and H is a subgroup of G, then $|G : H| \geq 5$).
If $|C_G(x)| = 12$, then $|G : C_G(x)| = 5$.
We have thus shown that if G is simple group of order 60, then G has a subgroup of index 5.
By Theorem (Let H be a subgroup of a group G and let X be the set of all distinct left cosets of H in G. Then there is a homomorphism from G into S_X with its kernel lying in H. In particular, if G has a subgroup of index m, then there is a homomorphism from G to S_m.), there is a monomorphism $\theta : G \rightarrow S_5$.
Now $\theta(G) \leq S_5$ and $\theta(G) \cap A_5 \lhd A_5$.
Since A_5 is simple, either $\theta(G) \cap A_5 = \{1\}$ or $\theta(G) \cap A_5 = A_5$.
If $\theta(G) \cap A_5 = \{1\}$, then $|\theta(G)A_5| = \frac{|\theta(G)||A_5|}{|\theta(G) \cap A_5|} = \frac{60 \times 60}{1} = 3600$, a contradiction as $\theta(G)A_5 \leq S_5$.
Hence, $\theta(G) \cap A_5 = A_5$, that is, $\theta(G) = A_5$.

Conclusion:

In this paper, we have explored the fundamental concepts of group actions and Sylow's Theorems. We began by revisiting the basic terminologies of group theory to provide a solid foundation. Group actions were defined as a way to understand how groups operate on sets, leading to the study of orbits and stabilizers. We then transitioned into Sylow's Theorems, which provide critical insights into the structure of subgroups within finite groups. The interplay between these two areas was a focal point, particularly in demonstrating how group actions facilitate the proofs and applications of Sylow's Theorems. Through various examples, we illustrated the practical utility of these theoretical constructs in classifying groups

and uncovering their inherent symmetries. This thesis not only consolidates the theoretical underpinnings of group actions and Sylow's Theorems but also emphasizes their significance in advancing our comprehension of algebraic structures.

REFERENCES:

[1] P.B. Bhattacharya, S.K. Jain, S.R. Nagpaul,BASIC ABSTRACT ALGEBRA second edition, Cambridge University Press, New York, USA 1994.
[2] Abstract Algebra by David S. Dummit and Richard M. Foote, 3rd Edition, John Wiley & Sons, New York, 2004.
[3] Contemporary Abstract Algebra by Joseph A. Gallian, 9th Edition, Cengage Learning, Boston, 2017.
[4] Topics in Algebra by I. N. Herstein, 2nd Edition, Wiley Eastern Limited, New Delhi, 1975.
[5] Algebra by Michael Artin, 2nd Edition, Pearson Education, 2011.
[6] A First Course in Abstract Algebra by John B. Fraleigh, 7th Edition, Pearson Education, 2003.
[7] Finite Group Theory by Michael Aschbacher, Cambridge University Press, Cambridge, 2000.
[8] Algebra by Serge Lang, Revised 3rd Edition, Springer, New York, 2002.
[9] Introduction to Group Theory by O. J. Schmidt, Dover Publications, 1994.
[10] Groups and Symmetry by M. A. Armstrong, Springe
[11] Ramji Lal, Algebra 1 (Groups, Rings, Fields and Arithmetic), published by Springer, Singapore 2017.
[12] D. S. Malik, J. M. Mordeson and M. K. Sen, Fundamentals of Abstract Algebra, International series in pure and applied mathematics, McGraw-Hill, 1997.
[13] Vivek Sahai, Vikas Bist, Algebra fourth edition, Alpha Science International, Limited, 2018
[14] David S. Dummit, Richard M. Foote, Abstract Algebra Third edition illustrated, John Wiley & Sons, 2003
[15] Algebra by Thomas W. Hungerford, Springer-Verlag, New York, 1974.