"Sylow's theorem on finite groups and their applications"

Dissertation submitted to the Department of Mathematics in partial fulfillment of the requirement for the award of the degree of Master of Science in Mathematics

Mahapurusha Srimanta Sankaradeva Viswavidyalaya

Department of Mathematics

Submitted By:

Bandana Bayan

Roll No: MAT-21/23

Registration No: MSSV-0023-101-000391

Department of Mathematics MSSV, Nagaon

Under The Guidance:

Dr. Raju Bordoloi, HOD

Department of Mathematics, MSSV, Nagaon

Certificate

This is to certify that the dissertation entitled **"Sylow's theorem on finite groups and their application"**, submitted by **Bandana Bayan**, Roll No. **MAT-21/23**, Registration No. **MSSV-0023-101-000391**, in partial fulfillment for the award of the degree of **Master of Science in Mathematics**, is a bonafide record of original work carried out under my supervision and guidance.

To the best of my knowledge , the work has not been submitted earlier to any institution for the award of any degree or diploma.

Dr. Raju Bordoloi
HOD
Department of Mathematics
MAHAPURUSHA SRIMANTA SANKARDEVA VISWAVIDYALAYA

Date: Signature of Guide

Place:

Declaration

I, **Bandana Bayan**, hereby declare that the dissertation titled **"Sylow's theorems on finite groups and their application"**, submitted to the Department of Mathematics, **MAHAPURUSHA SRIMANTA SANKARDEVA VISWAVIDYALAYA**, is a record of original work carried out by me under the supervision of **Dr. Raju Bordoloi**, Associate Professor.

This work has not been submitted earlier to any other institution or university for the award of any degree or diploma.

Place:

Date: Roll No.: MAT-21/23

Acknowledgement

First and foremost, I would like to express my sincere gratitude to my guide, **Dr. Raju Bordoloi**, Associate Professor, Department of Mathematics, MAHAPURUSHA SRIMANTA SANKARDEVA VISWAVIDYALAYA, for his valuable guidance, continuous support, and encouragement throughout the course of this dissertation.

I also extend my heartfelt thanks to the faculty members of the Department of Mathematics for their constant academic support and the friendly learning environment they provided.

I am deeply grateful to my family and friends for their unwavering moral support and motivation throughout my academic journey. Their encouragement gave me the strength to successfully complete this work Lastly, I thank all those who directly or indirectly helped me during this poject.

Place: Date: Roll No : MAT-21/23

Table of Contents

Chapter 1

General Introduction

In this work, we aim to provide a comprehensive introduction to Sylow's theorems and explore their applications. Our primary objective is to present these fundamental results in group theory in such a way that a reader does not require any prior familiarity with advanced concepts like double cosets in a group. Although the notion of double cosets is often employed by many mathematicians to prove Sylow's theorems, we wish to demonstrate that one can successfully understand and prove these theorems by relying only on a few elementary yet powerful ideas from group theory, such as orbits and stabilizers.

Throughout this exposition, we have observed that numerous mathematicians prefer to state Sylow's second theorem in the following succinct form:

Any two Sylow p-subgroups of a finite group G are conjugate to each other.

While this is indeed a popular formulation, in this work we choose to present Sylow's second theorem in a more general and robust form. This approach will naturally allow the commonly stated version to emerge as a straightforward corollary of our main result.

To ensure that this work remains self-contained and accessible, we have included all necessary preliminary definitions and supporting results, which are provided in the form of lemmas. This careful inclusion allows readers to traverse the entire journey from the foundational concepts to the culmination in Sylow's theorems without encountering any obstacles.

In essence, we have taken great care to emphasize the clarity and precision of our exposition. Our intent is that the presentation of these significant results does not merely appear as a vague reflection in a distorted mirror, but rather stands out as a crystal-clear narrative, readily comprehensible to anyone who wishes to delve into this elegant segment of group theory.

Pre-requisites

Here we would like to state a few definitions and a few important results which will, in turn, ensure a smooth journey during the proofs of Sylow's theorems. Once again, we wish to emphasize that we shall endeavor to reach our intended goal without invoking the concept of double cosets in a group.

1.1 Historical Background of Sylow's Theorem

The story of Sylow's Theorem is deeply intertwined with the evolution of group theory — a central pillar of modern algebra that grew out of the quest to understand the solvability of polynomial equations. This historical journey spans over a century and involves contributions from many remarkable mathematicians, each building upon the work of their predecessors.

1. Early Roots: Permutations and Equations

The earliest seeds of group theory were planted at the end of the 18th century, when mathematicians investigated the solutions to polynomial equations. Joseph-Louis Lagrange (1736–1813) explored how the permutations of the roots could reveal symmetries and inherent limitations, laying an informal foundation for what would become group theory. His investigations into "resolvents" implicitly depended on analyzing how the roots permute under different substitutions.

Augustin-Louis Cauchy (1789–1857) extended these ideas by rigorously studying permutations. Cauchy is often credited with providing the first formal treatment of permutations and proving foundational results like Cauchy's Theorem, which states that if a prime divides the order of a group, then the group contains an element of that prime order. This directly anticipated part of Sylow's work.

2. Galois and the Birth of Group Theory

The breakthrough came with the young French mathematician Évariste Galois (1811–1832). While investigating when polynomial equations could be solved by radicals, Galois formalized the notion of a group of permutations — now known as the Galois group — that captures the symmetries of the roots. He famously connected the solvability of polynomial equations to the structure of these groups.

Tragically, Galois was killed at just 20 years old, and his manuscripts remained largely unpublished for over a decade. It was only through the efforts of Joseph Liouville, who published Galois's memoirs in 1846, that these revolutionary ideas began to influence the mathematical community.

Galois's work shifted the focus from solving specific equations to studying the underlying algebraic structures — laying the cornerstone for abstract group theory.

3. The Formalization of Groups

By the mid-19th century, group theory had become a subject in its own right. Arthur Cayley (1821–1895) played a pivotal role by defining a group abstractly as a set with a binary operation satisfying closure, associativity, the existence of an identity, and inverses. In 1854, he proved that every finite group is isomorphic to a group of permutations, a result now known as Cayley's Theorem, cementing the deep connection between abstract groups and permutation groups.

Meanwhile, Camille Jordan (1838–1922) was developing his influential *Traité des Substitutions et des Équations Algébriques* (1870), which thoroughly explored permutation groups and normal subgroups — further paving the way for Sylow's insights.

4. Sylow and His Theorems

Within this rapidly advancing field emerged Peter Ludwig Mejdell Sylow (1832–1918), a Norwegian mathematician who spent most of his career teaching at secondary schools rather than in universities. Despite being somewhat isolated from the European centers of mathematical activity, Sylow made one of the most profound contributions to group theory.

In his seminal 1872 paper, *"Théorèmes sur les groupes de substitutions,"* published in *Mathematische Annalen*, Sylow established three fundamental results concerning finite groups, now collectively known as Sylow's Theorems. These theorems address the existence, conjugacy, and count of subgroups whose orders are powers of a prime, called Sylow p-subgroups.

Informally, Sylow's Theorems state:

1. If $|G| = p^n m$ where p is a prime not dividing m, then G has a subgroup of order p^n.
2. Any two Sylow p-subgroups of G are conjugate to each other.
3. The number of Sylow p-subgroups is congruent to 1 modulo p and divides m.

These results powerfully generalized earlier theorems such as Cauchy's and provided a robust toolkit for understanding the internal structure of finite groups.

5. Spread and Impact

Although Sylow himself wrote relatively few mathematical papers, his theorems were quickly recognized for their depth and significance. Jordan incorporated Sylow's results

into his own work, helping to disseminate them widely across Europe. Later mathematicians such as William Burnside, Emil Artin, and Richard Brauer built upon Sylow's foundation to develop the rich classification theorems of finite group theory.

By the early 20th century, Sylow's Theorems had become indispensable tools in algebra. They were instrumental in analyzing finite simple groups — groups without nontrivial normal subgroups — and in establishing critical results about the uniqueness and properties of groups of various orders. Indeed, many approaches to classifying finite groups begin by applying Sylow's Theorems to determine possible subgroup structures.

6. A Lasting Legacy

Today, Sylow's Theorems are a cornerstone of any course in abstract algebra. Their elegant blend of existence proofs, counting arguments, and conjugacy considerations exemplifies the power of group-theoretic methods. Beyond pure mathematics, Sylow's ideas have far-reaching applications in areas such as crystallography, quantum mechanics, coding theory, and combinatorics — wherever the concept of symmetry and group actions arises.

Emerging from modest circumstances, Sylow's work has profoundly shaped the landscape of modern algebra. His theorems stand as a testament to how foundational insights can illuminate vast swaths of mathematics and continue to inspire exploration to this day.

1.2 Definitions and Concepts

1. **Operation:**
   In mathematics, a *binary operation* on a set is a calculation that combines two elements of the set (called operands) to produce another element of the set. More formally, it is an operation whose arity is two, and whose two domains and one codomain are (subsets of) the same set. Examples include the familiar elementary arithmetic operations of addition, subtraction, multiplication, and division. Other instances are easily found in other branches of mathematics, e.g., vector addition, matrix multiplication, and conjugation in groups.

2. **Group Representations:**
   In the mathematics of representation theory, *group representations* express abstract groups in terms of linear transformations of vector spaces; more specifically, they provide a means to represent group elements as matrices such that the group operation can be represented by matrix multiplication. Representations of groups are significant since they enable many group-theoretic problems to be solved in terms of problems in linear algebra, which is more easily understood. They are significant in physics too, since, for instance, they give the way the symmetry group of a physical system influences the solutions of equations for that system.

3. **Abelian Groups:**
   In abstract algebra, an *abelian group*, also referred to as a *commutative group*, is a group where the product of applying the group operation to two group elements is independent of the order in which they are written (the axiom of commutativity). That is, for all a, b in the group,

$$a \cdot b = b \cdot a.$$

4. Algebraic Structure

In mathematics, and particularly in abstract algebra, the expression *algebraic structure* typically means a set (referred to as *carrier set* or *underlying set*) with one or more finitary operations defined on it that satisfies a list of axioms.

5. Axioms

An *axiom* or *postulate*, as defined in classic philosophy, is a statement (in mathematics often represented in symbolic form) that is so clear or well-established that it is accepted

uncontroversially or unconditionally. The axiom can therefore be adopted as the premise or starting point for other reasoning or arguments, typically in logic or in mathematics.

The term derives from Greek *axioma* "that which is thought worthy or fit" or "that which commends itself as evident."

6. Symmetry

Symmetry (from Greek *symmetria* "agreement in dimensions, due proportion, arrangement") in common usage means a feeling of fair and lovely proportion and balance.

In mathematics, "symmetry" has a more specific meaning: that an object is unchanged by a transformation, like reflection, but also including other transforms as well. While these two definitions of "symmetry" can usually be distinguished, they are connected, so here they are discussed together.

Mathematical symmetry can be seen with respect to the flow of time; as a spatial relation; through geometric transformations including scaling, reflection, and rotation; through other types of functional transformations; and as part of abstract objects, theories, models, language, music, and even knowledge itself.

7. Lie Groups

A *Lie group* is a group that is also a differentiable manifold, having the property that the group operations are compatible with the smooth structure. Lie groups are named after Sophus Lie, who founded the theory of continuous transformation groups.

8. Poincaré Groups

The *Poincaré group*, named in honor of Henry Poincaré (1906), was originally defined by Minkowski (1908) as the group of Minkowski space-time isometries. It is a ten-generator non-abelian Lie group of fundamental significance in physics.

9. Cosets

In mathematics, if G is a group, H is a subgroup of G, and g is an element of G, then

(a) $gH = \{gh : h \in H\}$ is the *left coset* of H in G with respect to g, and

(b) $Hg = \{hg : h \in H\}$ is the *right coset* of H in G with respect to g.

(c) Only if H is normal will the set of right cosets and the set of left cosets of H coincide, which is one definition of normality of a subgroup.

Though obtained from a subgroup, cosets are not typically themselves subgroups of G, only subsets.

10. Trivial Group

A *trivial group*, in mathematics, is a group with only one element. All these groups are isomorphic to each other, and hence one frequently refers to *the* trivial group.

The only member of the trivial group is the identity element and therefore it is most often written as such: 0, 1, or e depending on context. If the group operation is represented by $*$ then it satisfies

$$e * e = e.$$

11. Even Permutation

In algebra, an *even permutation* is a permutation which is derivable from an even number of two-element swaps. That is, a permutation for which the permutation symbol equals $+1$.

12. Dihedral Group

In group theory, a *dihedral group* is the group of symmetries of a regular polygon which contains the rotations and reflections of such polygon. It is represented by D_n and has order $2n$.

13. Generalized Dihedral Group

The *generalized dihedral group* is defined in group theory for any abelian group H, as the semidirect product of H and $\mathbb{Z}_2$ with $\mathbb{Z}_2$ acting on H by inverting elements. It is represented by $E_n(H)$ and has order $2n$.

14. Dicyclic Group

In group theory, the *dicyclic group* of any integer $n > 1$ is defined to be the subgroup of the unit quaternions generated by

$$\langle a, x \mid a^{2n} = 1, x^2 = a^n, x^{-1}ax = a^{-1} \rangle.$$

It is called Dic_n and has order $4n$. The quaternion group occurs when $n = 2$.

15. General Affine Group

In the theory of groups, the *general affine group* of any affine space over a field K is the group of all invertible affine transformations from the space into itself. It is denoted by $G(n, K)$ where $n \in \mathbb{N}$ and K is a field.

1.3 Aim and Objectives

The aim and objective of this study is to gain a deep insight into the term *Finite Groups* with the help of Sylow's theorems. It also seeks to provide a historical overview of group theory, along with definitions, terms, and concepts used throughout the study of group theory.

Additionally, we will examine the types and classifications of groups, the theorems that support the study, examples that illustrate these theorems, and the real-life implications of the concept.

Chapter 2

Preliminaries

2.1 Basic Group Theroy

In mathematics, a *group* refers to an algebraic structure that includes a set of elements, together with an operation that combines them in a unique manner. This combination of the set of elements assists in the creation of a third element.

To be part of a group, the elements must obey four laws, referred to as the *group axioms*. These include closure, associativity, and invertibility. For instance, the collection of integers along with the addition operation forms a group.

The definition of a group, however, has a more general character and possesses far broader applications compared to the example stated above. This allows complicated groups in abstract algebra and elsewhere to be treated in a versatile manner while maintaining their inherent structure.

Groups are rooted in the same principles as symmetry. A symmetry group encodes symmetrical properties of a geometrical object. Any transformation set done with the aid of an operation will not change the structure of the object.

Symmetry Groups and Group Theory

Group axioms form a very abstract structure that generalizes far beyond trivial examples. This abstraction of the groups makes them very powerful and flexible, and they find application in every corner of mathematics and science. For example, group theory enables us to handle sophisticated structures in abstract algebra and beyond, controlling them systematically and flexibly while retaining their intrinsic properties.

One of the most important relationships of group theory is with symmetry. Groups are closely associated with symmetry since they are able to capture and encode symmetrical properties of mathematical or physical objects. A *symmetry group* is a mathematical group where elements are symmetry operations (such as rotations, reflections, or translations), and whose group operation is equivalent to applying these symmetry transformations one after the other.

Technically, any collection of transformations which can be performed on an object without altering its underlying structure (and which satisfy the group axioms: closure, associativity, identity, and inverses) is a symmetry group.

Types of Symmetry Groups

There are some significant types of symmetry groups which occur often in mathematics and physics:

- **Lie groups:**
  These are groups that are also smooth manifolds, i.e., they have a smoothly varying structure on which calculus may be done. Lie groups are very important in applied physics, especially for defining continuous symmetries like space rotations that underlie much of the laws of physics (e.g., conservation laws by Noether's theorem).

- **Point groups:**
  These sets are comprised of symmetry operations that fix at least one point. They find especial utility in crystallography and molecular chemistry for the description of the symmetries of molecules and crystal structures. Point groups assist researchers in comprehending how molecules interact, their vibrational modes, and their absorption of light.

- **Poincaré groups:**
  These are the spacetime symmetry groups in special relativity theory. The Poincaré group is a combination of the rotations, translations, and Lorentz boosts (mixing space and time coordinates) and is very important for modern physics, particularly for the investigation of particle physics and the construction of relativistic quantum field theories.

Practical Example

A straightforward example of a symmetry group is the set of rotations of a square about its center. This set, under the operation of successive rotations, forms a group because:

- Combining two rotations results in another rotation (*closure*).
- The grouping of operations does not matter (*associativity*).
- Doing nothing (the identity rotation) is a symmetry (*identity element*).
- Every rotation has an inverse rotation that undoes it (*inverse element*).

This symmetry group encodes all the rotational symmetries of the square.

2.2 Definitions and Notations

Here we present the basic definitions, notations, and conventions used in this dissertation. These are the building blocks of the language for describing and applying the Sylow theorems.

Definition 2.2.1 (Group)

A **group** is a set G with a binary operation (usually written multiplicatively) that satisfies:

1. **Closure:** $ab \in G$ for all $a, b \in G$.
2. **Associativity:** $(ab)c = a(bc)$ for all $a, b, c \in G$.
3. **Identity:** There exists $e \in G$ such that $ae = ea = a$ for all $a \in G$.
4. **Inverses:** For each $a \in G$, there exists $a^{-1} \in G$ such that $aa^{-1} = a^{-1}a = e$.

If $ab = ba$ for all $a, b \in G$, then G is called **abelian**.

Example

- $(\mathbb{Z}, +)$ is an abelian group.
- S_3, the symmetric group on three symbols, is non-abelian.

—

Definition 2.2.2 (Order of Group and Element)

The **order** of a group G is $|G|$, the cardinality of G.

The **order** of an element $g \in G$, written $\text{ord}(g)$, is the smallest positive integer n such that $g^n = e$.

—

Definition 2.2.3 (Subgroup, Normal Subgroup, Quotient Group)

A **subgroup** H of G is a subset which is itself a group using the operation of G. Notation: $H \leq G$.

A **normal subgroup** N is such that $gNg^{-1} = N$ for all $g \in G$. Notation: $N \triangleleft G$.

For $N \triangleleft G$, the set of cosets G/N is the **quotient group**.

—

Definition 2.2.4 (Index)

The **index** $[G : H]$ is the number of different left cosets of H in G.

—

Definition 2.2.5 (p-group and Sylow p-subgroup)

A p**-group** is a group with order p^n, with p a prime.

If $|G| = p^k m$ with $p \nmid m$, then a subgroup of order p^k is called a **Sylow** p**-subgroup**.

—

Definition 2.2.6 (Orbit and Stabilizer)

Suppose a group G acts on a set X.

- The **orbit** of an element $x \in X$ is

$$\mathrm{Orb}_G(x) = \{g \cdot x : g \in G\}.$$

- The **stabilizer** of x is

$$\mathrm{Stab}_G(x) = \{g \in G : g \cdot x = x\}.$$

Example If S_3 acts on $X = \{1, 2, 3\}$ by permutations, then

$$\mathrm{Orb}_{S_3}(1) = \{1, 2, 3\}$$

since any element can be mapped to any position, and

$$\mathrm{Stab}_{S_3}(1) = \{\mathrm{id}, (2\,3)\},$$

the permutations that fix 1.

—

Orbit-Stabilizer Theorem

If G acts on X, then for any $x \in X$,

$$|\,\mathrm{Orb}_G(x)| = [G : \mathrm{Stab}_G(x)],$$

and

$$|G| = |\,\mathrm{Orb}_G(x)| \cdot |\,\mathrm{Stab}_G(x)|.$$

—

Definition 2.2..7 (Counting Sylow p-subgroups)

Let G be a finite group and p a prime dividing $|G|$. Then:

- The number of Sylow p-subgroups is denoted by n_p.
- By the third Sylow theorem, n_p satisfies:

$$n_p \equiv 1 \pmod{p} \quad \text{and} \quad n_p \mid m$$

  where $|G| = p^k m$ and $p \nmid m$.

Example In S_3,

$$|S_3| = 6 = 2 \cdot 3.$$

We have

$$n_3 \equiv 1 \pmod{3}, \quad n_3 \mid 2.$$

Thus $n_3 = 1$ or 2. By checking the subgroups, there is exactly 1 Sylow 3-subgroup (order 3), so $n_3 = 1$.

A **group** is a set G with a b

2.3 Important Results Used

This chapter brings together the fundamental results that underpin the proofs and discussions of Sylow's theorems and their various applications. These theorems and propositions form a core toolkit for analyzing the structure of finite groups.

2.3.1 Lagrange's Theorem

If G is a finite group and H is a subgroup of G, then the order of H divides the order of G, i.e.,

$$|H| \mid |G|.$$

This also gives the index formula

$$[G : H] = \frac{|G|}{|H|}.$$

Example In S_3, every subgroup of order 2 (for instance, generated by a transposition) divides 6.

2.3.2 Cauchy's Theorem

If a prime p divides the order of G, then there exists an element in G of order p. This result is crucial for establishing the existence of elements of prime order, which is a necessary step before constructing Sylow p-subgroups.

2.3.3 Class Equation

For a finite group G, the class equation decomposes the group according to conjugacy:

$$|G| = |Z(G)| + \sum_i [G : C_G(x_i)],$$

where $Z(G)$ denotes the center of G, and $C_G(x_i)$ is the centralizer of a representative x_i from each non-central conjugacy class.

This equation is frequently used, for instance, to prove the existence of nontrivial centers in certain p-groups.

2.3.4 Orbit-Stabilizer Theorem

Suppose G acts on a set X, and let $x \in X$. Then

$$|G| = |\operatorname{Orb}_G(x)| \cdot |\operatorname{Stab}_G(x)|.$$

This theorem is a fundamental tool for counting arguments in group theory.

2.3.5 First Sylow Theorem (Existence)

If $|G| = p^k m$ where p is a prime and $p \nmid m$, then G contains at least one subgroup of order p^k, known as a Sylow p-subgroup.

2.3.6 Second Sylow Theorem (Conjugacy)

All Sylow p-subgroups of G are conjugate to one another. Thus, under the internal symmetries of G, these subgroups are essentially indistinguishable.

2.3.7 Third Sylow Theorem (Counting)

Let n_p denote the number of Sylow p-subgroups of G. Then

$$n_p \equiv 1 \pmod{p}, \quad n_p \mid m.$$

These conditions place strict constraints on the possible number of Sylow p-subgroups.

2.3.8 Consequence for Normality

If $n_p = 1$, then the unique Sylow p-subgroup is normal in G. This follows immediately since all Sylow p-subgroups are conjugate, and having only one forces it to be invariant under conjugation.

Chapter 3

3.1. Sylow Theorems

3.1.1. Introduction

One of the main problems in finite group theory is to understand how the order of a group governs its subgroup structure. While Lagrange's theorem tells us that the order of any subgroup divides the order of the group, it does not guarantee the existence of a subgroup of a particular divisor order. For example, a group of order 12 might or might not possess a subgroup of order 6.

However, when we focus on subgroups whose orders are powers of primes, we have an exceptionally powerful set of results: the *Sylow theorems*. These theorems not only ensure the existence of such subgroups, but also describe how they are conjugate to each other and impose restrictions on their number.

These theorems, formulated by the Norwegian mathematician Ludwig Sylow in the 19th century, form a cornerstone in the study of finite groups.

3.1.2. First Sylow Theorem Statement

We now present the first Sylow theorem, which primarily addresses the existence of subgroups of a given prime power order.

Theorem 0.1 (First Sylow Theorem)**.** *Let G be a finite group with*

$$|G| = p^k m$$

where p is a prime, k is a non-negative integer, and p does not divide m. Then G contains a subgroup of order p^k.

Any such subgroup is called a Sylow p-subgroup *of G.*

3.1.3. Proof of the First Sylow Theorem

There are several ways to prove this theorem, including using counting arguments with group actions. Here, we provide a version that employs the group action on subsets, often called the "Cauchy-Frobenius technique."

Proof. **Step 1: Considering subsets of appropriate size.**

Let X be the set of all subsets of G that contain exactly p^k elements, that is,

$$X = \{S \subseteq G \mid |S| = p^k\}.$$

The total number of such subsets is given by

$$|X| = \binom{|G|}{p^k} = \binom{p^k m}{p^k}.$$

By a standard property of binomial coefficients, since p does not divide m, it follows that p does not divide $\binom{p^k m}{p^k}$. Thus, $|X|$ is not divisible by p.

Step 2: Group action on these subsets.

Now let G act on X by left translation:

$$g \cdot S = \{gs \mid s \in S\}, \quad \text{for } g \in G, S \in X.$$

By the Orbit-Stabilizer theorem, X decomposes into a disjoint union of orbits, and hence

$$|X| = \sum_i |\text{Orb}_i|.$$

Step 3: Analysis of orbit sizes.

If an orbit has size divisible by p, it contributes a multiple of p to the sum. Given that $|X|$ itself is not divisible by p, there must exist at least one orbit whose size is not divisible by p. In fact, the only possibility is an orbit of size 1.

Step 4: Existence of a fixed subset under the action.

An orbit of size 1 implies that for such a subset S, we have

$$g \cdot S = S \quad \text{for all } g \in G_S,$$

where G_S denotes the stabilizer of S. Using standard arguments (often involving normalizers), one deduces that this leads to a subgroup of G of order p^k.

Alternate approach:

Alternatively, one may build such a subgroup inductively on k, applying Cauchy's theorem to find elements of order p and gradually constructing a p-group.

Thus, there exists a subgroup of G of order p^k.

□

Examples

Example 0.2. Let $|G| = 12 = 2^2 \cdot 3$. By the First Sylow theorem:

- There exists a subgroup of order 4 (a Sylow 2-subgroup).
- There exists a subgroup of order 3 (a Sylow 3-subgroup).

Example 0.3. Let $|G| = 28 = 2^2 \cdot 7$. By the First Sylow theorem:

- There exists a subgroup of order 4.
- There exists a subgroup of order 7.

3.2. Second Sylow Theorem

3.2.1. Introduction

Although the First Sylow theorem guarantees us that there exist subgroups of order p^k (where p^k is the greatest power of p dividing the group order), it says nothing about how these subgroups relate to one another. The Second Sylow theorem answers this question by asserting that all such subgroups are conjugate in the group. This means essentially that they are all "the same up to the group's internal symmetry."

3.2.2. Statement of the Second Sylow Theorem

Theorem 0.4 (Second Sylow Theorem)**.** *Let G be a finite group and let p be a prime that divides $|G|$. Then any two Sylow p-subgroups of G are conjugate.*

If P and Q are Sylow p-subgroups of G,
then there exists some $g \in G$ such that $Q = gPg^{-1}$.

This has an important consequence:

> Any p-subgroup of G (that is, a subgroup whose order is a power of p) is contained in some Sylow p-subgroup of G.

3.2.3. Proof of the Second Sylow Theorem

The proof exploits the theory of group actions, in particular the notion of the group acting on the coset set, and then uses a counting argument (sometimes referred to as the orbit-stabilizer or class equation technique).

Proof. Step 1: Setup group action.

Let P be a Sylow p-subgroup of G. Let H be any p-subgroup of G. (We could take H to be another Sylow p-subgroup in the strongest possible sense, but the argument applies to any p-subgroup.)

Consider the action of H on the set of left cosets G/P by left multiplication:

$$h \cdot (gP) = (hg)P$$

for all $h \in H$, $gP \in G/P$.

Step 2: Counting fixed points.

Let us consider the set of fixed points under this action:

$$\text{Fix} = \{gP \in G/P : h \cdot (gP) = gP \quad \text{for all } h \in H\}.$$

This means

$$hgP = gP \quad \Longleftrightarrow \quad g^{-1}hg \in P \quad \text{for all } h \in H.$$

Step 3: Using the counting argument.

Now by general principles of counting orbits, because $|H|$ is a power of p, and the number of elements in G/P is $|G : P|$, which is *not divisible by* p (since $|P|$ is the largest power of p dividing $|G|$), it follows that:

the total number of fixed points modulo p equals the total number of elements modulo p,

hence there must be at least one fixed point.

Formally, using the class equation (or the Cauchy-Frobenius lemma), we conclude there exists a coset gP fixed by H.

Step 4: Conjugation into P.

So there is some $g \in G$ such that

$$g^{-1}Hg \subseteq P.$$

In particular, if H itself was a Sylow p-subgroup, then its order equals $|P|$, forcing

$$g^{-1}Hg = P.$$

Thus,

$$H = gPg^{-1}.$$

Hence, every Sylow p-subgroup is conjugate to P.

□

3.3. Sylow's Third Theorem

3.3.1. Statement of the theorem

Theorem 0.5 (Sylow's Third Theorem)**.** *Let G be a finite group of order*

$$|G| = p^k m,$$

where p is a prime, $k \geq 1$, and $p \nmid m$. Let n_p denote the number of Sylow p-subgroups of G. Then:

1. *n_p divides m, i.e. $n_p \mid m$,*
2. *$n_p \equiv 1 \pmod{p}$.*

This theorem imposes sharp restrictions on the number of Sylow p-subgroups of G. Often, these conditions uniquely determine n_p, which becomes a powerful tool for classifying finite groups.

3.3.2. Proof of the theorem

Proof. We divide the proof into two parts.

1. Divisibility condition

Let P be a Sylow p-subgroup of G. By definition, $|P| = p^k$. Consider the normalizer $N_G(P) = \{g \in G : gPg^{-1} = P\}$. By the orbit-stabilizer theorem, applied to the action of G on the set $\mathcal{S}$ of all Sylow p-subgroups by conjugation, we have

$$n_p = [G : N_G(P)] = \frac{|G|}{|N_G(P)|}.$$

Since $P \leq N_G(P)$, we may write $|N_G(P)| = p^k t$ for some integer t, yielding

$$n_p = \frac{p^k m}{p^k t} = \frac{m}{t}.$$

Thus, n_p divides m.

2. Congruence condition

We now show that $n_p \equiv 1 \pmod{p}$. Consider the action of P on $\mathcal{S}$ by conjugation:

$$x \cdot Q = xQx^{-1}, \quad x \in P,\ Q \in \mathcal{S}.$$

A Sylow p-subgroup Q is fixed under this action precisely when $xQx^{-1} = Q$ for all $x \in P$, i.e. $P \leq N_G(Q)$. But since $|P| = |Q|$ and both are Sylow p-subgroups, it follows that $P = Q$.

Hence, the only Sylow p-subgroup fixed by this action is P itself. Thus,

$$|\mathrm{Fix}(P)| = 1.$$

By the class equation for this action,

$$|\mathcal{S}| = |\mathrm{Fix}(P)| + \sum(\text{sizes of other orbits}),$$

where each orbit other than the fixed point has size divisible by p. Therefore,

$$n_p = |\mathcal{S}| \equiv |\mathrm{Fix}(P)| \equiv 1 \pmod{p}.$$

This completes the proof. □

3.3.3. Remarks

Remark 0.6. This theorem is remarkably restrictive. For instance, if $|G| = 28 = 2^2 \cdot 7$, then the number of Sylow 7-subgroups must both divide 4 and satisfy

$$n_7 \equiv 1 \pmod{7}.$$

The only possibility is $n_7 = 1$, showing there is a unique Sylow 7-subgroup, which must then be normal. This highlights the power of Sylow's third theorem in studying the structure of finite groups.

Chapter 4

More Applications

Last chapter, I have given the Sylow's theorem, which constitutes a strong foundation of the concept of classification of finite groups, and I have used the theorem to describe how to prove if a group is simple, possesses normal subgroup and is abelian. In this chapter, we will further apply Sylow's theorem to cyclic groups, groups of certain order (which has been chosen at random with no special interest other than to show again how the Sylow's theorem operates), and non-trivial normal subgroups.

4.1. Application of Sylow's theorem to characterizing cyclic groups

Theorem 0.7. *Let G be a group with prime order p, then G is cyclic.*

Proof. Let $g \in G$, where $g \neq e$. We wish to prove that $\langle g \rangle = G$. We know from Lagrange's theorem that any subgroup of G has order dividing p, that is, either order 1 or p. The subgroup $\langle g \rangle$ contains at least two elements, which are g and e, where $g \neq e$. Thus, $\langle g \rangle$ has order p. Therefore, this subgroup generates the whole group. □

Theorem 0.8. *Suppose that p and q are primes with $p < q$ and that $q \not\equiv 1 \pmod{p}$. Then every group of order pq is cyclic.*

Proof. Suppose that G is a group of order pq with $p < q$ and $q \not\equiv 1 \pmod{p}$.

From Cauchy's theorem, we have that G contains an element a of order p and an element b of order q. Let $P = \langle a \rangle$ and $Q = \langle b \rangle$. These subgroups are of order p and q and are, respectively, the p-Sylow and q-Sylow subgroups of G.

By applying the Sylow theorems, we will demonstrate that P and Q are both normal subgroups of G.

But first, we want to determine the order of ab. We do this by raising ab to the power n. From the table of elements of $\langle ab \rangle$, we obtain that $\langle ab \rangle$ has elements of order pq. But we desire to exclude the possibilities of double counting the same elements.

Suppose that

$$a^i b^j = a^k b^\ell,$$

then we obtain

$$a^{i-k} = b^{\ell-j}.$$

Now, $a^{i-k} \in P$ and $b^{\ell-j} \in Q$. We know that $\text{ord}(a^{i-k}) \mid p$ and $\text{ord}(b^{\ell-j}) \mid q$.

Because p and q are coprime, the only element common to both subgroups is the identity. That is,

$$a^{i-k} = e = b^{\ell-j}.$$

Therefore $i = k$ and $\ell = j$. Then since $\gcd(p, q) = 1$, we have $\operatorname{lcm}(p, q) = pq$. As $|G| = pq$, this means that G is cyclic.

By Sylow's theorem (3), $n_p \mid q$ and $n_p \equiv 1 \pmod{p}$. So, the only options are $n_p = 1$ or q. As $q \not\equiv 1 \pmod{p}$ (by assumption), we have $n_p = 1$, so P is the unique p-Sylow subgroup and hence normal in G.

Similarly, by Sylow's theorem (3), $n_q \mid p$ and $n_q \equiv 1 \pmod{q}$. The only possibilities are $n_q = 1$ or p. As $1 < n_q < q$ is not possible, the congruence condition on n_q forces $n_q = 1$. Hence Q is the unique q-Sylow subgroup and thus normal in G. □

Remark 0.9. Using Lagrange's theorem, it can be proved that any group of prime order is cyclic.

Theorem 0.10. *A group with no more than one subgroup of any order is cyclic.*

Proof. The proof has two steps: we first show the theorem holds for groups of prime-power order and then apply Sylow's first theorem to conclude the general case from the prime-power case.

Step 1: Let $|G| = p^k$ where p is prime and $k \geq 1$, and suppose G has at most one subgroup of each order. To demonstrate that G is cyclic, let g be an element of G with maximum order. We wish to show that $\langle g \rangle = G$.

Choose any $h \in G$, so h has order a power of p by Lagrange's theorem. Suppose g has order p^m and h has order p^n, so $n \leq m$. Then p^n divides p^m, so there is a subgroup of the cyclic group $\langle g \rangle$ with order p^n.

Explicitly, this subgroup is

$$\left\langle g^{p^{m-n}} \right\rangle.$$

Also, $\langle h \rangle$ has order p^n, so by our hypothesis that G has at most one subgroup of each size, we must have

$$\langle h \rangle \subseteq \langle g \rangle,$$

so $h \in \langle g \rangle$. Therefore $G \subseteq \langle g \rangle$, and thus $\langle g \rangle = G$.

Step 2: Now let G be a finite group with at most one subgroup of each order. Therefore $n_p = 1$ for all primes p dividing $|G|$, meaning each p-Sylow subgroup is unique and hence normal.

For different primes p and q dividing $|G|$, the elements of the p-Sylow and q-Sylow subgroups commute, because otherwise their generated subgroup would have more than one subgroup of the same order, violating our hypothesis.

By Step 1, the p-Sylow subgroup of G is cyclic. Select a generator g_p of the p-Sylow subgroup of G. The order of g_p is the size of the p-Sylow subgroup.

These g_p's commute as p varies, and their orders are relatively prime. Thus, the order of the product of the g_p's is the product of the sizes of the Sylow subgroups of G. This product of sizes is $|G|$, so G is cyclic. □

4.2 Application of Sylow's theorem to Symmetric groups S_4, S_5 and Alternating groups A_4, A_5

Theorem 0.11 (Theorem 4.4)**.** *The group A_4 has 3 subgroups of order 4 and 4 subgroups of order 3, while S_4 has 3 subgroups of order 8 and 4 subgroups of order 3.*

Proof. From prime factorization, we have

$$|A_4| = 12 = 2^2 \cdot 3.$$

Let n_2 and n_3 be the number of 2-Sylow and 3-Sylow subgroups respectively.

By Sylow's theorem:

$$n_2 \mid 3 \quad \text{and} \quad n_2 \equiv 1 \pmod 2,$$

so $n_2 = 1$ or 3. Since there are more than one transpositions in A_4, we have $n_2 \neq 1$. Thus, $n_2 = 3$.

Similarly,

$$n_3 \mid 4 \quad \text{and} \quad n_3 \equiv 1 \pmod 3,$$

so $n_3 = 1$ or 4. The number of 3-cycles (abc) in A_4 is 8, and these appear in inverse pairs, hence we have 4 subgroups of order 3.

Thus, A_4 contains 3 subgroups of order 4 and 4 subgroups of order 3.

Next, for

$$|S_4| = 24 = 2^3 \cdot 3,$$

let n_2 and n_3 denote the number of 2-Sylow and 3-Sylow subgroups respectively.

By Sylow's theorem,

$$n_2 \mid 3 \quad \text{and} \quad n_2 \equiv 1 \pmod 2,$$

so $n_2 = 1$ or 3. There are more than one transpositions in S_4, so $n_2 \neq 1$, giving $n_2 = 3$.

Similarly,

$$n_3 \mid 8 \quad \text{and} \quad n_3 \equiv 1 \pmod 3,$$

so $n_3 = 1$ or 4. There are 8 3-cycles (abc) in S_4, which form 4 subgroups of order 3.

Therefore, both S_4 and A_4 have 4 subgroups of order 3, while A_4 has 3 subgroups of order 4 and S_4 has 3 subgroups of order 8. □

Theorem 0.12. *(Theorem 4.5)*
The groups S_5 and A_5 both have 10 subgroups of order 3 and 6 subgroups of order 5.

Proof. Each element of odd order in a symmetric group is an even permutation, so the 3-Sylow and 5-Sylow subgroups of S_5 are contained in A_5. Hence, it is enough to discuss

A_5. By the prime factorization, we have

$$|A_5| = 60 = 2^2 \cdot 3 \cdot 5.$$

The 3-Sylow subgroups are of order 3 and the 5-Sylow subgroups are of order 5.

From Sylow's theorem, we know that

$$n_3 \mid 20 \quad \text{and} \quad n_3 \equiv 1 \pmod 3,$$

so $n_3 = 1, 4$, or 10.

A_5 contains 20 3-cycles (abc), and these appear in inverse pairs, so there are

$$\frac{20}{2} = 10$$

subgroups of order 3. Thus $n_3 = 10$.

Now for the 5-Sylow subgroups, we have

$$n_5 \mid 12 \quad \text{and} \quad n_5 \equiv 1 \pmod 5,$$

so n_5 is 1 or 6. As A_5 has at least two distinct subgroups of order 5 (for example, the subgroups generated by (12345) and by (21345) are distinct), we see that $n_5 > 1$ and thus $n_5 = 6$. □

4.3 Non-trivial normal subgroups

The implications of the Sylow theorems here are instances where the order of G requires G to possess a nontrivial normal subgroup (often, but not necessarily, a normal Sylow subgroup).

Let us start by first introducing a lemma:

Lemma 0.13 (Lemma 4.1)**.** *If G possesses k subgroups of order p, then G has $k(p-1)$ elements of order p.*

Proof. We have that G has k subgroups, each of order p, with the identity element $\{e\}$ belonging to each of them. This provides

$$k(p-1)$$

elements of order p.

Next, we need to rule out the possibility that any non-identity element belongs to the intersection of two distinct subgroups of G.

Suppose H and K are two distinct subgroups of G. We assert that

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

By Lagrange's theorem, if $H \cap K \neq \{e\}$, then $H \cap K$ must be a nontrivial subgroup of both H and K. Since $|H| = |K| = p$ and p is a prime, the only nontrivial subgroup they could have would be of order p, which would imply

$$H = K,$$

contradicting our assumption that they are distinct.

Thus, the intersection of any two distinct subgroups of order p is trivial, and so G contains exactly

$$k(p-1)$$

elements of order p. □

Theorem 0.14. *Suppose $|G| = 20$ or 100, then G possesses a normal 5-Sylow subgroup.*

Proof. Let $|G| = 20$. Then by factorization into primes, we obtain

$$20 = 2^2 \cdot 5.$$

By Sylow's theorem (specifically the third Sylow theorem), we have

$$n_5 \mid 4 \quad \text{and} \quad n_5 \equiv 1 \pmod 5.$$

Therefore, $n_5 = 1$.

Similarly, let $|G| = 100$. Then by prime factorization,

$$100 = 2^2 \cdot 5^2.$$

From here, the proof follows similarly by applying Sylow's theorem to show $n_5 = 1$, hence G has a normal 5-Sylow subgroup. □

Theorem 0.15. *Suppose $|G| = 12$. Then G contains a normal 2-Sylow or 3-Sylow subgroup.*

Proof. From Sylow's theorem, we have

$$n_2 \mid 3 \implies n_2 = 1 \text{ or } 3,$$

and

$$n_3 \mid 4, \quad n_3 \equiv 1 \pmod 3 \implies n_3 = 1 \text{ or } 4.$$

We shall prove that $n_2 = 1$ or $n_3 = 1$.

Suppose $n_3 \neq 1$, so $n_3 = 4$. Because the 3-Sylows are of size 3, by Lemma 4.1, G has

$$n_3 \cdot 2 = 8$$

elements of order 3. Thus the number of remaining elements is

$$12 - 8 = 4.$$

A 2-Sylow subgroup has size 4, and hence occupies these remaining elements. Therefore, $n_2 = 1$.

For instance, the alternating group A_4 has $n_2 = 1$ and $n_3 = 4$, whereas the dihedral group D_6 has $n_2 = 3$ and $n_3 = 1$. □

4.4 Application to classifying finite groups

We will now use all the ideas that have been constructed to classify groups of finite order from 1 to 25 and demonstrate the uniqueness and existence of such groups.

The classification will first be ordered by prime orders, which are the easier cases, and then orders that behave in a similar manner will follow.

The group of order 1 is the trivial group (the identity element), and there is only one such finite group. This is obvious, so we will not discuss it further.

Theorem 0.16. *Suppose that G is a group of prime order p. Then up to isomorphism, there is exactly one group of finite order p.*

Proof. From Algebra II and Theorem 4.1, we have that a group of prime order is cyclic. Therefore, the only option is the cyclic group $\mathbb{Z}_p$. This establishes the uniqueness of $\mathbb{Z}_p$.

Also, the group $\mathbb{Z}_n$ is a familiar object from Algebra II and in mathematics in general. Therefore, this covers finite groups of order $2, 3, 5, 7, 11, 13$. □

Theorem 0.17. *Let G be any group of order 4. Then up to isomorphism, there are exactly two groups of order 4, namely $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$.*

Proof. For the uniqueness of these groups, we construct them by examining their multiplication tables explicitly.

The strategy is to multiply the elements with each other. Eventually, there is nothing left to determine unless we assume, for some element $a \in G$, that either $a \cdot a = b$ or $a \cdot a = e$. Proceeding this way, we obtain tables that correspond to $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$.

This demonstrates that there cannot be any group of order 4 other than these two up to isomorphism.

For example, if we assume $a \cdot a = e$, we get a table of the form:

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

On the other hand, if we assume $a \cdot a = b$, we obtain a table like:

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

For existence, both groups $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$ are well-known and clearly exist. □

Theorem 0.18. *Let p and q be primes with $p > q$.*

1. *If $q = p - 1$, then every group of order pq is isomorphic to the cyclic group $\mathbb{Z}_{pq}$.*
2. *If $q \mid (p-1)$, then up to isomorphism, there are precisely two distinct groups of order pq: the cyclic group $\mathbb{Z}_{pq}$ and a non-abelian group K generated by elements c and d such that $|c| = p$ and $|d| = q$ and satisfying the relation*

$$dc = c^s d$$

where $s \not\equiv 1 \pmod{p}$ and $s^q \equiv 1 \pmod{p}$.

Proof. Let G be a group of order pq.

Step 1: Existence of elements of orders p and q.
By Cauchy's theorem, there exist elements $a, b \in G$ such that $|a| = p$ and $|b| = q$.

Step 2: Sylow p-subgroups.
Let n_p be the number of Sylow p-subgroups. Then:

$$n_p \equiv 1 \pmod{p} \quad \text{and} \quad n_p \mid q.$$

Since $p > q$, the only possibility is $n_p = 1$. Thus, the unique Sylow p-subgroup is normal in G. Denote it by $\langle a \rangle = S$.

Step 3: Factor group and generation.
Consider G/S, which has order q. Thus G/S is cyclic, say generated by bS. It follows

that every element of G can be written in the form $b^i a^j$. By repeated application of group relations (cf. Hungerford I.2.8 and I.6.13), we can write any element as a product $a^i b^j$.

Step 4: Sylow q-subgroups.
Let n_q be the number of Sylow q-subgroups. Then

$$n_q \equiv 1 \pmod{q}, \quad n_q \mid p.$$

So $n_q = 1$ or $n_q = p$.

Case 1: $n_q = 1$.
Then $\langle b \rangle$ is also normal in G. Thus G is the internal direct product:

$$G \cong \langle a \rangle \times \langle b \rangle.$$

Since $\gcd(|\langle a \rangle|, |\langle b \rangle|) = \gcd(p, q) = 1$, the group is cyclic of order pq. Hence

$$G \cong \mathbb{Z}p \times \mathbb{Z}_q \cong \mathbb{Z}pq.$$

Case 2: $n_q = p$ (possible if $q \mid (p-1)$).
Then $\langle a \rangle$ is normal, but $\langle b \rangle$ is not. By theorem I.3.4(v) (Hungerford), we have

$$bab^{-1} = a^r$$

where $r \not\equiv 1 \pmod{p}$ (else G would be abelian). Iterating gives

$$b^i a b^{-i} = a^{r^i}.$$

Taking $i = q$,

$$a = b^q a b^{-q} = a^{r^q}$$

so $r^q \equiv 1 \pmod{p}$.

Step 5: Constructing K.
By number theory, $X^q \equiv 1 \pmod{p}$ has exactly q solutions. Since $r \not\equiv 1$, its minimal power is q, and $\{1, r, r^2, \ldots, r^{q-1}\}$ exhausts the solutions. We can relabel b to $b_1 = b^t$ for suitable t so that

$$b_1 a b_1^{-1} = a^s$$

where $s = r^t \not\equiv 1$ but still $s^q \equiv 1 \pmod{p}$. Thus $G = \langle a, b_1 \rangle$ with relations

$$|a| = p, \quad |b_1| = q, \quad b_1 a = a^s b_1.$$

This is precisely the presentation of the non-abelian group K.

Step 6: Isomorphism.
Define $\varphi : G \to K$ by

$$\varphi(a^i b_1^j) = c^i d^j.$$

This is well-defined, respects multiplication by similar calculations using the relations, and is bijective, thus an isomorphism.

Conclusion:
Thus, up to isomorphism, there are exactly two groups of order pq when $q \mid (p-1)$: the cyclic group $\mathbb{Z}_{pq}$ and the non-abelian group K as constructed.

□

Theorem 0.19 (4.10)**.** *Suppose p is an odd prime. Then every group of order $2p$ is isomorphic either to the cyclic group $\mathbb{Z}_{2p}$ or the dihedral group D_p.*

Proof. This follows directly by applying Theorem 4.9 with $q = 2$. If G is not cyclic, then the conditions on s in Theorem 4.9 imply that

$$s \equiv -1 \pmod{p}.$$

Thus G is generated by elements c and d such that

$$|c| = p, \quad |d| = 2, \quad \text{and} \quad dc = c^{-1}d.$$

Therefore, by Theorem I.6.13 (Hungerford), $G \cong D_p$, the dihedral group of order $2p$. □

Remark. Theorems 4.9 and 4.10 together classify groups of order $6, 10, 14$ and 15 completely.

Theorem 0.20 (4.11)**.** *Let G be a group of order p^2 where p is prime. Then up to isomorphism, there exist precisely two groups of order p^2: the cyclic group $\mathbb{Z}_{p^2}$ and a non-cyclic group which is the direct product $\mathbb{Z}_p \times \mathbb{Z}_p$.*

Proof. We first prove that every group of order p^2 is abelian.

Let $Z(G)$ denote the center of G. By group theory (Algebra II), $Z(G)$ is a subgroup of G. By Lagrange's theorem, $|Z(G)|$ divides $|G| = p^2$. Thus,

$$|Z(G)| \in \{1, p, p^2\}.$$

Case 1: $|Z(G)| = 1$.
This is impossible by Corollary II.5.4 (Hungerford), which states that the center of a nontrivial p-group is nontrivial.

Case 2: $|Z(G)| = p$.
Then by the index formula,

$$|G/Z(G)| = \frac{|G|}{|Z(G)|} = \frac{p^2}{p} = p.$$

Thus $G/Z(G)$ is of prime order and hence cyclic. But if $G/Z(G)$ is cyclic and $Z(G) < G$, then G cannot be abelian (as an abelian group would have itself as center), yielding a contradiction.

Case 3: $|Z(G)| = p^2$.
Then $Z(G) = G$, showing that G is abelian.

Now, since G is a finite abelian group of order p^2, the fundamental theorem of finitely generated abelian groups together with Theorem II.2.1 (Hungerford) implies that

$$G \cong \mathbb{Z}m_1 \times \mathbb{Z}m_2 \times \cdots \times \mathbb{Z}_{m_t}$$

where $m_1 \mid m_2 \mid \cdots \mid m_t$ and $m_1 m_2 \cdots m_t = p^2$.

For $|G| = p^2$, this yields only two possibilities up to isomorphism:

$$G \cong \mathbb{Z}_{p^2} \quad \text{or} \quad G \cong \mathbb{Z}_p \times \mathbb{Z}_p.$$

Example: For $p = 3$, the groups of order $9 = 3^2$ up to isomorphism are

$$\mathbb{Z}_9 \quad \text{and} \quad \mathbb{Z}_3 \times \mathbb{Z}_3.$$

□

Theorem 0.21 (4.12)**.** *Let G be a group of order pq where p and q are primes such that $p < q$ and $q \not\equiv 1 \pmod{p}$. Then, up to isomorphism, there exists only one group of order pq.*

Proof. To prove uniqueness, we illustrate with the case where $|G| = 15$, since 15 is the smallest such order and is the only group order under consideration in this thesis that satisfies these characteristics.

From Proposition 3.1, together with the condition $n_5 = 1$, and applying Theorems 3.3 and 4.2, we deduce that there exists a normal subgroup of G. Consequently, G must be cyclic.

Therefore, there is only one group of finite order 15 up to isomorphism, namely

$$G \cong \mathbb{Z}_{15}.$$

This completes the classification of groups of order 15. □

Theorem 0.22 (4.13)**.** *Suppose G is a group of order 8. Then, up to isomorphism, there are precisely five groups of order 8.*

Proof. To establish the uniqueness, we begin by noting from Hungerford's theorem that any finite abelian group G is isomorphic to

$$\mathbb{Z}m_1 \oplus \mathbb{Z}m_2 \oplus \cdots \oplus \mathbb{Z}_{m_t}$$

where $m_1 > 1$ and $m_1 \mid m_2 \mid \cdots \mid m_t$.

Since $8 = 2 \cdot 2 \cdot 2 = 2 \cdot 4$, we have three possible decompositions for the abelian case:

Case 1: $m_1 = 2, m_2 = 2, m_3 = 2$. Then $m_1 \mid m_2 \mid m_3$ holds, and thus

$$G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2.$$

Case 2: $m_1 = 2, m_2 = 4$. Here, $m_1 \mid m_2$ and $m_1 > 1$, so

$$G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_4.$$

Case 3: Simply

$$G \cong \mathbb{Z}_8.$$

Next, by Proposition II.6.3 (Hungerford), there exist (up to isomorphism) exactly two distinct non-abelian groups of order 8: the quaternion group Q_8 and the dihedral group D_4.

Non-isomorphism of Q_8 and D_4: We establish $Q_8 \ncong D_4$ by counting elements of order 2. Specifically, Q_8 has exactly one element of order 2, whereas D_4 has five elements of order 2. Thus, they cannot be isomorphic.

Existence of these non-abelian groups: Let G be a non-abelian group of order 8. Since G cannot have every non-identity element of order 2 (otherwise it would be abelian), there exists an element $a \in G$ of order 4. Then $\langle a \rangle$ is a subgroup of index 2 and is therefore normal in G.

Let $b \in G \setminus \langle a \rangle$. Since $\langle a \rangle$ is normal, we have

$$bab^{-1} \in \langle a \rangle = \{1, a, a^2, a^3\}.$$

Because G is non-abelian, $bab^{-1} \neq a$. Thus, it must be that

$$bab^{-1} = a^{-1}.$$

Now consider b^2. Since $|G : \langle a \rangle| = 2$, we have $b^2 \in \langle a \rangle$. Thus,

$$b^2 \in \{1, a, a^2, a^3\}.$$

Given b has order 2 or 4, we must have $b^2 = 1$ or $b^2 = a^2$.

Case 1: $a^4 = 1$, $b^2 = 1$, and $bab^{-1} = a^{-1}$. Then, by Theorem I.6.13 (Hungerford), we conclude

$$G \cong D_4.$$

Case 2: $a^4 = 1$, $b^2 = a^2$, and $bab^{-1} = a^{-1}$. Then, by Theorem I.4.14 (Hungerford),

$$G \cong Q_8.$$

Thus, up to isomorphism, there are exactly five groups of order 8:

$$\mathbb{Z}_8, \quad \mathbb{Z}_4 \oplus \mathbb{Z}_2, \quad \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2, \quad D_4, \quad Q_8.$$

□

Theorem 0.23 (4.14)**.** *Suppose G is a group of order 12. Then, up to isomorphism, there are precisely five groups of finite order 12.*

Proof. To establish uniqueness, we begin with Theorem II.2.1, which gives the condition for G to be isomorphic to a direct sum of cyclic groups:

$$G \cong \mathbb{Z}m_1 \oplus \mathbb{Z}m_2 \oplus \cdots \oplus \mathbb{Z}_{m_t}$$

where $m_1 > 1$ and $m_1 \mid m_2 \mid \cdots \mid m_t$.

We factor 12 in two ways:

$$12 = 2 \cdot 6 = 3 \cdot 4.$$

Only $12 = 2 \cdot 6$ satisfies the required divisibility conditions. Thus we have two cases to consider.

Case 1: $m_1 = 2, m_2 = 6$. Since $m_1 \mid m_2$ and $m_1 > 1$, it follows that

$$G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_6.$$

Case 2: Direct product:

$$G \cong \mathbb{Z}_{12}.$$

Next, by Proposition II.6.4 (Hungerford), there exist, up to isomorphism, precisely three different non-abelian groups of order 12: the dihedral group D_6, the alternating

group A_4, and a group T with generators a, b satisfying

$$|a| = 6, \quad b^2 = a^3, \quad bab^{-1} = a^{-1}.$$

Existence of T: Let T be a non-abelian group of order 12. The non-identity elements of T have either order 2 or 6. If $g^2 = 1$ for all $g \in T$, then T is abelian. Thus, some $a \in T$ must have order 6. Then $\langle a \rangle$ is of index 2 and therefore normal in T.

Taking $b \in T \setminus \langle a \rangle$, since $\langle a \rangle$ is normal,

$$bab^{-1} \in \langle a \rangle = \{1, a, a^2, a^3, a^4, a^5\}.$$

Because T is non-abelian, $bab^{-1} \neq a$. Thus,

$$bab^{-1} = a^{-1}.$$

Moreover, since $|T/\langle a \rangle| = 2$, we have $b^2 \in \langle a \rangle$, so

$$b^2 \in \{1, a, a^2, a^3, a^4, a^5\}.$$

Given the possible orders of b, we deduce that

$$b^2 = 1 \quad \text{or} \quad b^2 = a^3.$$

Thus $T = \langle a, b \rangle$ with presentations:

$$a^6 = 1, \quad b^2 = a^3, \quad bab^{-1} = a^{-1} \quad \Longrightarrow \quad T.$$

Alternatively,

$$a^6 = 1, \quad b^2 = 1, \quad bab^{-1} = a^{-1} \quad \Longrightarrow \quad D_6.$$

Non-isomorphism of T, A_4, D_6: We show no two of T, A_4, D_6 are isomorphic. Comparing element orders, D_6 has an element (a 60° rotation) of order 6, while A_4 has no element of order 6. In fact, no element in S_4 has order 6, so $D_6 \ncong A_4$.

For a non-abelian group G of order 12, by Sylow's theorem, G has a Sylow 3-subgroup P of order 3, and $|G : P| = 4$.

By Proposition II.4.8 (Hungerford), there exists a homomorphism

$$f : G \to S_4$$

with kernel $K \subseteq P$. Thus $K = P$ or $K = \{e\}$.

- If $K = \{e\}$, then f is injective and G is isomorphic to a subgroup of order 12 in S_4, which by Theorem I.6.8 (Hungerford) must be A_4.

- If $K = P$, then P is normal and the unique Sylow 3-subgroup. For any element c of order 3, we have

$$[G : C_G(c)] = 1 \text{ or } 2,$$

so $|C_G(c)| = 12$ or 6. Thus by Cauchy's theorem, there exists an element $d \in C_G(c)$ of order 2.

Therefore, all finite groups of order 12 up to isomorphism are:

$$\mathbb{Z}_2 \oplus \mathbb{Z}_6, \quad \mathbb{Z}_{12}, \quad D_6, \quad A_4, \quad T.$$

□

All groups which have been classified in this these are given in the table below:

Order of Group	**Number of Distinct Groups**
1	1
2	1
3	1
4	2
5	1
6	2
7	1
8	5
9	2
10	2
11	1
12	5
13	1
14	2
15	1

Chapter 5

Conclusion and Recommendations

5.1. Conclusion

One of the pillars of finite group theory, namely the Sylow theorems, and their deep implications to the classification of finite groups and the internal structure of groups of different orders have been investigated in this study. The Sylow theorems contain strong existence, count, and conjugacy theorems for subgroups of prime power order, and are now a standard tool in abstract algebra.

Throughout this thesis, we have discussed the three Sylow theorems at length:

1. **Sylow's first theorem** ensures the existence of subgroups of order p^k for any prime p dividing the group order, given p^k is the highest power of p dividing $|G|$.

2. **Sylow's second theorem** establishes that all Sylow p-subgroups are conjugate, resulting in an intrinsic uniformity in their distribution within the group.

3. **Sylow's third theorem** restricts and states the quantity of such subgroups, which says the number of Sylow p-subgroups divides $|G|$ and is congruent to 1 modulo p.

The power of these theorems has been beautifully illustrated through the classification of groups of small orders. To illustrate, when investigating groups of order 12 or 15, the Sylow theorems helped us eliminate some possibilities in structure, infer normality of subgroups, and even determine when a group had to be cyclic or had to have a direct product structure. In most situations, information about the numbers of Sylow p-subgroups served as the critical insight. For instance:

- If a Sylow p-subgroup is unique (i.e. there is only one up to isomorphism), then it must be normal, greatly simplifying analysis of the structure of the group.

- The limitations on the quantity of such subgroups often led directly to determining isomorphism classes of groups.

In addition, we examined non-trivial cases like the alternating group A_4, the dihedral groups D_n, and the quaternion group Q_8, all of which serve as instructive examples illustrating how the interaction of Sylow subgroups controls the nature of non-abelian groups. For example, in A_4, the fact that there are four Sylow 3-subgroups prevents these from being normal, and this impacts the normal subgroup structure of the group significantly.

Another important point is the great insight Sylow theory provides into how group orders factor into products of primes. Not by mere counting arguments does Sylow theory enable us to claim not just that certain subgroups must exist, but also that they conjugate in a well-behaved manner and that their counts obey strict arithmetic limitations. This underlies the whole process of classifying small finite groups.

Through the proofs and examples given, this thesis has pointed out how the Sylow theorems transform otherwise mysterious group structures into discernible patterns. Even outside of groups of small order, the Sylow theorems are key tools in many classical results, such as proving that simple non-abelian groups must be of large size, or that no simple group of order 30 exists.

5.2. Recommendations

From the findings of this study, a number of recommendations for future exploration and research become apparent.

1. **Push classification to higher orders.** This thesis focused mainly on groups of comparably small order to maintain the analysis tractable. A natural extension is to explore groups of order up to 20, 30, or beyond. As group order increases, new phenomena emerge, such as more intricate interactions among several distinct prime divisors. Such investigations would demand heavier combinatorial and group-action tools, but would uncover even greater structural richness.

2. **Study automorphism groups and subgroup lattices.** For every group categorized or built using Sylow theorems, knowledge of its automorphism group informs us about its internal symmetries. Similarly, a thorough depiction of the subgroup lattice explains how different subgroups connect through containment. This would enhance understanding of how Sylow subgroups behave not just in isolation but as part of the whole subgroup structure.

3. **Apply group actions to establish deeper results.** Group actions, such as orbit-stabilizer concepts, can provide alternative proofs of the Sylow theorems themselves, and enable more sophisticated classification. For instance, orbit counting can be employed to prove Cauchy's theorem and normalizer results closely related to Sylow theory. Investigating this path broadens the set of tools available for tackling challenging classification problems.

4. **Link to applications beyond pure group theory.** The Sylow theorems have profound implications not only in group theory but also in geometry, crystallography, and even chemistry in terms of symmetry groups of molecules. Exploring such connections would illustrate how abstract algebra predicts concrete patterns

in the physical world. Permutation groups, often studied via Sylow subgroups, govern counting symmetries in problems ranging from graph theory to error-correcting codes in combinatorics.

5. **Use computational tools.** Computer algebra systems such as GAP or MAGMA can compute Sylow subgroups and their numbers, as well as conjugacy classes, explicitly. Employing such software makes it possible to verify theoretical conclusions on concrete examples and to uncover interesting corner cases that might inspire new theoretical questions. Familiarity with computational experiments can therefore enrich and support theoretical insights.

6. **Investigate connections with the classification of finite simple groups.** On a larger scale, the Sylow theorems play key roles in the classification of all finite simple groups, one of the monumental achievements of 20th-century mathematics. While this topic lies well outside the scope of this thesis, future studies could explore how Sylow subgroups underpin decompositions of complex groups into simpler building blocks.

5.3. Closing thoughts

The study of Sylow theorems provides a striking demonstration of how compelling abstract consequences can impose global restrictions on group structures, regardless of how the groups are originally presented. They reveal deep arithmetic patterns within seemingly disparate algebraic objects and assist mathematicians in navigating complex classifications. Through the application of these theorems to diverse examples, we have witnessed not just their technical power but also the elegance with which they shape the landscape of finite groups.

Future research, whether on higher orders, automorphism structures, or applied settings, will likely continue this beautiful interplay between abstract algebra and concrete symmetry. Through such studies, we gain a better appreciation of how group theory—driven by results such as the Sylow theorems—acts as a unifying language for patterns both in mathematics and in the natural world.

Bibliography

[1] Andruskiewitsch, N., & Schneider, H. J. (2010). On the classification of finite-dimensional pointed Hopf algebras. *Annals of Mathematics*, 375–417.

[2] Barut, A. O., & Raczka, R. (1986). *Theory of group representations and applications* (Vol. 2). Singapore: World Scientific.

[3] Fang, J. (1963). *Abstract algebra*. Schaum Publishing Company.

[4] Foote, R. (2007). Mathematics and complex systems. *Science*, 318(5849), 410–412.

[5] Gallian, J. (2016). *Contemporary abstract algebra*. Cengage Learning Publisher.

[6] Gilmore, R. (2012). *Lie groups, Lie algebras, and some of their applications*. Courier Corporation.

[7] Gorenstein, D. (2013). *Finite simple groups: An introduction to their classification*. Springer Science & Business Media.

[8] Herstein, I.N. (1975). *Topics in Algebra*. John Wiley & Sons.

[9] Hungerford, T. W. (1980). *Algebra, Graduate Texts in Mathematics*, Volume 73. Springer.

[10] Jungnickel, D. (1992). On the Uniqueness of the Cyclic Group of Order n. *The American Mathematical Monthly*, 99(6), 545–547.

[11] Kleiner, I. (1986). The evolution of group theory: A brief survey. *Mathematics Magazine*, 59(4), 195–215.

[12] Lang, S. (2002). *Algebra, Graduate Texts in Mathematics*. Revised third edition. Springer-Verlag.

[13] Shockley, J. E. (1967). *Introduction to Number Theory*. New York: Holt, Rinehart and Winston, Inc.

[14] Solomon, R. (2001). A brief history of the classification of the finite simple groups. *Bulletin of the American Mathematical Society*, 38(3), 315–352.

[15] Upadhyay, S.K., & Kumar, S.D. (2011). Existence of a unique group of finite order. *arXiv preprint* arXiv:1104.3831.

[16] Wallace, D. A. (2012). *Groups, Rings and Fields*. Springer Science & Business Media.