Term Paper

Zehao Li

March 2025

Abstract

This paper presents and proves Sylow's theorems, fundamental results in group theory that describe the number and structure of p-subgroups of finite groups.

1 Introduction

Group theory is a fundamental area of abstract algebra, and Sylow's theorems provide key insights into the existence and number of subgroups of prime power order in finite groups. These theorems are essential in classification problems and play a crucial role in various algebraic applications.

Lagrange's theorem states that the order of any subgroup of a finite group G divides the order of G. However, it does not guarantee the existence of subgroups of a specific order. Sylow's theorems refine this result by ensuring the existence of subgroups whose orders are prime powers and by describing their conjugacy properties and counting formulae. These theorems provide a deeper understanding of the subgroup structure of finite groups and are essential in the classification of groups.

2 Background Knowledge

Before stating Sylow's theorems, we introduce some fundamental concepts in group theory.

2.1 Conjugacy Class

Definition 1. *Let G be a group and let $a \in G$. The conjugacy class of a in G is defined as the set:*

$$Cl(a) = \{gag^{-1} \mid g \in G\}.$$

Two elements $a, b \in G$ are conjugate if there exists some $g \in G$ such that $b = gag^{-1}$.

2.2 Sylow p-Subgroup

Definition 2. *Let G be a finite group, and let p be a prime divisor of $|G|$. If p^k divides $|G|$ and p^{k+1} does not divide $|G|$, then any subgroup of G of order p^k is called a* ***Sylow p-subgroup*** *of G.*

2.3 Normalizer

Definition 3. *Let G be a group and H be a subgroup of G. The normalizer of H in G, denoted by $N_G(H)$, is defined as the set of all elements $g \in G$ such that conjugation by g leaves H invariant, i.e.,*

$$N_G(H) = \{g \in G \mid gHg^{-1} = H\}.$$

In other words, $N_G(H)$ consists of all the elements of G that, when conjugating any element of H, result in an element that still lies in H.

3 Statement of Sylow's Theorems

Theorem 1 (Sylow's First Theorem)**.** *Let G be a finite group, and let p be a prime. If p^k divides $|G|$, then G has at least one subgroup of order p^k.*

Theorem 2 (Sylow's Second Theorem)**.** *Let H be a subgroup of a finite group G such that $|H|$ is a power of a prime p. Then H is contained in some Sylow p-subgroup of G.*

Theorem 3 (Sylow's Third Theorem)**.** *Let p be a prime and let G be a group of order $p^k m$, where p does not divide m. Then the number n of Sylow p-subgroups of G satisfies:*

$$n \equiv 1 \pmod{p}, \quad \text{and} \quad n \mid m.$$

Furthermore, any two Sylow p-subgroups of G are conjugate.

4 Proof of Sylow's Theorems

4.1 Proof of Sylow's First Theorem

Lemma 4. *Let G be a finite group and let $a \in G$. Then,*

$$|cl(a)| = |G : C(a)|,$$

where $cl(a)$ denotes the conjugacy class of a in G and $C(a) = \{g \in G \mid ga = ag\}$ is the centralizer of a.

Proof. Consider the action of G on itself by conjugation, that is, for any $g \in G$ and $a \in G$, define

$$g \cdot a = gag^{-1}.$$

Under this action, the orbit of a is exactly the conjugacy class $\mathrm{cl}(a)$. By the Orbit-Stabilizer Theorem, we have

$$|\mathrm{cl}(a)| = \frac{|G|}{|\mathrm{Stab}(a)|},$$

where $\mathrm{Stab}(a)$ is the stabilizer of a under conjugation. Notice that

$$\mathrm{Stab}(a) = \{g \in G \mid gag^{-1} = a\} = C(a).$$

Therefore,

$$|\mathrm{cl}(a)| = \frac{|G|}{|C(a)|} = |G : C(a)|.$$

□

Lemma 5. *Let G be a finite group, and let $Z(G)$ be the center of G. The class equation of G is given by:*

$$|G| = |Z(G)| + \sum_{a \in Conj(G)} |G : C(a)|,$$

where the sum runs over one element a from each conjugacy class of G.

Proof. Consider the conjugacy class of an element $a \in G$. If $a \in Z(G)$, then $\mathrm{Cl}(a) = \{gag^{-1} \mid g \in G\} = \{agg^{-1} \mid g \in G\} = \{a\}$.

Observe that the group G is partitioned into disjoint conjugacy classes. Therefore, we can express the order of G as the sum of the sizes of its conjugacy classes:

$$|G| = \sum_{a \in G} |\,\mathrm{Cl}(a)|.$$

We classification all a into $Z(G)$ with

$$|\mathrm{cl}(a)| = 1,$$

and a from each conjugacy class not contained in $Z(G)$ with

$$|\mathrm{cl}(a)| = |G : C(a)|,$$

Thus, the order of G can be rewritten as

$$|G| = |Z(G)| + \sum_{a \in \mathrm{Conj}(G)} |G : C(a)|,$$

where the sum runs over one representative a from each conjugacy class not contained in $Z(G)$.

□

[Sylow's First Theorem] Let G be a finite group, and let p be a prime. If p^k divides $|G|$, then G has at least one subgroup of order p^k.

Proof. We prove the theorem by induction on $|G|$.

Base Case: When $|G| = 1$, the group G is trivial. Since p^k divides 1 only if $k = 0$ (because $p^0 = 1$), the unique subgroup G itself has order 1. Hence, the base case is trivial true for the theorem.

Inductive Hypothesis: Assume that for every group K with $|K| < |G|$, if p^k divides $|K|$, then K contains a subgroup of order p^k.

Now consider the group G with $|G| > 1$ and suppose p^k divides $|G|$. We consider two cases:

Case (a): *There exists a proper subgroup H of G such that p^k divides $|H|$.* By the inductive hypothesis, H contains a subgroup of order p^k. Since H is a subgroup of G, this subgroup is also a subgroup of G, and the theorem holds in this case.

Case (b): *Every proper subgroup H of G has order not divisible by p^k.* In this case, no proper subgroup of G has order divisible by p^k. We now use the class equation of G.

The class equation is:

$$|G| = |Z(G)| + \sum_{a \notin Z(G)} |G : C(a)|,$$

where the sum is taken over one representative from each conjugacy class not contained in $Z(G)$.

By the lemma, For any $a \in Z(G)$the conjugacy class of a is

$$|\operatorname{Cl}(a)| = |\{a\}| = 1,$$

For any $a \notin Z(G)$,

$$|\mathrm{cl}(a)| = \frac{|G|}{|C(a)|} = |G : C(a)|.$$

Since p^k divides $|G|$ but, by assumption, p^k does not divide the order of any proper subgroup (including each $C(a)$ with $a \notin Z(G)$), it follows that $|G : C(a)|$ is divisible by p^k for each $a \notin Z(G)$.

Thus, every term in the sum

$$\sum_{a \notin Z(G)} |G : C(a)|$$

is divisible by p^k. Since p^k divides $|G|$, it follows that p divides

$$|Z(G)| = |G| - \sum_{a \notin Z(G)} |G : C(a)|.$$

In particular, $|Z(G)| \geq p$.

Since $Z(G)$ is an abelian subgroup of G and p divides $|Z(G)|$, by the Fundamental Theorem of Finite Abelian Groups (or Cauchy's Theorem for abelian groups), there exists an element $x \in Z(G)$ of order p. Note that x is central in G, so the subgroup $\langle x \rangle$ is normal in G.

Consider the factor group $G/\langle x \rangle$. Its order is

$$|G/\langle x \rangle| = \frac{|G|}{p}.$$

Since p^k divides $|G|$, it follows that p^{k-1} divides $|G/\langle x \rangle|$. By the inductive hypothesis, $G/\langle x \rangle$ contains a subgroup of order p^{k-1}. Let $H/\langle x \rangle$ be such a subgroup, where H is a subgroup of G. Then

$$|H| = |\langle x \rangle| \cdot |H/\langle x \rangle| = p \cdot p^{k-1} = p^k.$$

Thus, H is a subgroup of G of order p^k.

Conclusion: In either case, G has a subgroup of order p^k. Therefore, by the principle of mathematical induction, Sylow's First Theorem is proved. □

4.2 Proof of Sylow's Second Theorem

Lemma 6. *Let K be a Sylow p-subgroup of a finite group G, if $x \in N(K)$ and the order of x is a power of p, then $x \in K$*

Proof. Since $x \in N(K)$, we consider the coset xK in the quotient group $N(K)/K$. The cyclic subgroup generated by this coset is given by:

$$\langle xK \rangle \subseteq N(K)/K.$$

By assumption, the order of x is a power of p, which implies that the order of $\langle xK \rangle$ is also a power of p.

By the Correspondence Theorem, there exists a subgroup H of $N(K)$ such that:

$$K \subseteq H \quad \text{and} \quad H/K = \langle xK \rangle.$$

Since the order of H/K is a power of p, the order of H is:

$$|H| = |K| \cdot |\langle xK \rangle|,$$

which is also a power of p.

However, K is a Sylow p-subgroup of G, meaning that K is the largest p-subgroup in G. Since H is a p-subgroup containing K, and K is of the largest possible order, it follows that:

$$H = K.$$

Thus, H/K is the trivial subgroup, meaning that:

$$xK = K.$$

This implies that $x \in K$, completing the proof. □

[Sylow's Second Theorem] Let H be a subgroup of a finite group G such that $|H|$ is a power of a prime p. Then H is contained in some Sylow p-subgroup of G.

Proof. Let K be a Sylow p-subgroup of G, and let $\mathcal{C} = \{K_1, K_2, \ldots, K_n\}$ be the set of all conjugates of K in G, where $K = K_1$. Since conjugation is an automorphism of G, each element K_i in $\mathcal{C}$ is also a Sylow p-subgroup of G.

Next, let $S_{\mathcal{C}}$ denote the group of all permutations on the set $\mathcal{C}$. For each $g \in G$, define the permutation $f_g \in S_{\mathcal{C}}$ by

$$f_g(K_i) = gK_ig^{-1}.$$

It is easy to verify that each f_g is indeed a permutation of $\mathcal{C}$, and so we define a map $T : G \to S_{\mathcal{C}}$ by

$$T(g) = f_g.$$

Since

$$f_{gh}(K_i) = (gh)K_i(gh)^{-1} = g\left(hK_ih^{-1}\right)g^{-1} = f_g\left(f_h(K_i)\right),$$

we have $T(gh) = T(g)T(h)$, so T is a homomorphism.

Now, let H be any subgroup of G whose order is a power of p, i.e., $|H| = p^m$ for some m. Since T is a homomorphism, the image $T(H)$ is a p-subgroup of $S_{\mathcal{C}}$ since the property of the homomorphism.

Then, by the Orbit-Stabilizer Theorem, for each $K_i \in \mathcal{C}$, the size of the orbit of K_i under the action of $T(H)$, denoted by $\mathrm{orb}_{T(H)}(K_i)$, divides $|T(H)|$ and hence is a power of p.

Next, we consider the condition under which $|\mathrm{orb}_{T(H)}(K_i)| = 1$. If this condition holds, then for every $g \in H$,

$$f_g(K_i) = gK_ig^{-1} = K_i.$$

This means $H \subseteq N(K_i)$, the normalizer of K_i in G. By the lemma proved, the only elements of $N(K_i)$ that are powers of p are those that are contained in K_i itself. Therefore, if $H \subseteq N(K_i)$ and H is a p-group, it follows that $H \subseteq K_i$.

To complete the proof, we need to show that for some i, $|\mathrm{orb}_{T(H)}(K_i)| = 1$. Since elements of $N(K)$ conjugate K to itself, every left coset of $N(K)$ corresponds uniquely to a distinct conjugate gKg^{-1}. Hence, the number of distinct conjugates of K is precisely the number of left cosets of $N(K)$ in G, which is given by the index:

$$|C| = |G : N(K)|$$

, where $N(K)$ is the normalizer of K in G. We know that

$$|G : K| = |G : N(K)| \cdot |N(K) : K|,$$

and since $|G : N(K)| \cdot |N(K) : K|$ is not divisible by p, neither is $|C|$. Thus,$|C|$ is not divisible by p. Since $|C|$ is partitioned into orbits under the action of $T(H)$, and each orbit has size a power of p, if no orbit has size 1, then p must divide

each summand. This would imply that p divides $|C|$, which is a contradiction. Therefore, there must be at least one orbit of size 1. That is, there exists some $K_i \in |C|$ such that

$$|\operatorname{orb}_{T(H)}(K_i)| = 1,$$

which implies $H \subseteq N(K_i)$ and, by the restriction on p-elements in the normalizer, $H \subseteq K_i$.

Thus, every Sylow p-subgroup of G is conjugate to a Sylow p-subgroup of K. This completes the proof. □

4.3 Proof of Sylow's Third Theorem

[Sylow's Third Theorem] Let p be a prime and let G be a group of order $p^k m$, where p does not divide m. Then the number n of Sylow p-subgroups of G satisfies:

$$n \equiv 1 \pmod{p}, \quad \text{and} \quad n \mid m.$$

Furthermore, any two Sylow p-subgroups of G are conjugate.

Proof. Consider the group G with the same set of all conjugation C with proof before in Sylow's second theorem, for each $g \in G$ and $K_i \in C$, define

$$T(g)(K_i) = gK_ig^{-1}.$$

In particular, we already proved the orbits under the subgroup $T(K)$ (the image of K under this action). For each $K_i \in C$, the size of the orbit $\operatorname{orb}(K_i)$ is a power of p because the stabilizer of K_i in K has p-power order.

$$|\operatorname{orb}(K_1)| = 1,$$

Next, for every other K_i (with $i \neq 1$), the orbit size is a nontrivial power of p (i.e., at least p). Since the orbits partition C, we can write

$$n = 1 + p \cdot a,$$

for some nonnegative integer a. Hence, it follows that

$$n \equiv 1 \pmod{p}.$$

Then, We meed to show every Sylow p-subgroup is conjugate to K Assume, for contradiction, that there exists a Sylow p-subgroup H of G which is not in C. Then consider the action of H (via conjugation) on the set C. Since H is not conjugate to K, none of the orbits under this action has size 1; that is, each orbit has size divisible by p. Thus, the total number n (being the sum of the sizes of these orbits) would be divisible by p, implying

$$n \equiv 0 \pmod{p}.$$

This contradicts the result $n \equiv 1 \pmod{p}$. Therefore, every Sylow p-subgroup of G must be conjugate to K, meaning that all Sylow p-subgroups belong to C.

Furthermore, We try to prove $n \mid m$. Recall that by the Orbit-Stabilizer Theorem, the number n of Sylow p-subgroups equals the index of the normalizer $N(K)$ of K in G:

$$n = |G : N(K)|.$$

Since $|G| = p^k m$ and $|K| = p^k$ divides $|N(K)|$, it follows that

$$|N(K)| = p^k \ell,$$

for some integer ℓ dividing m. Consequently, we have

$$n = \frac{|G|}{|N(K)|} = \frac{p^k m}{p^k \ell} = \frac{m}{\ell},$$

which shows that n divides m.

Thus, we have established that:

1. $n \equiv 1 \pmod{p}$,
2. Every Sylow p-subgroup of G is conjugate (i.e., belongs to C),
3. n divides m.

This completes the proof of Sylow's Third Theorem. □

5 Conclusion

Sylow's theorems are powerful tools in group theory that describe the structure of finite groups, bridging group order with subgroup existence, making them indispensable tools in the study of finite group structures.

References

[1] Gallian, Joseph A. Contemporary Abstract Algebra. 7th ed., Houghton Mifflin, 2009.

[2] Dummit, David S., and Richard M. Foote. *Abstract Algebra*. John Wiley & Sons, 2004.