Sylow’s Subgroup Theorem

Tharatorn Supasiti

February 2, 2010

Note: This is not my work. Most comes from Suzuki [2] and Wilkins [3].

1 Introduction

In finite group theory, one of the most influential ideas is the notion of Sylow $p$-subgroup. It was used to classify many groups of finite order. Despite original intentions to use it with finite group, it was extended to study Lie group, which inspires recent development in $p$-compact group.

Here, we will discuss some aspects of Sylow’s Subgroup Theorem. In particular, the focus is on a finite group with the intention to study simple groups. The main results in this article are the First and the Second Sylow Theorems.

**Theorem 1.1 (First Sylow Theorem):** Let $G$ be a finite group with an order $p^k m$, where $m$ and $p$ are coprime. Then there exists a Sylow $p$-subgroup in $G$.

**Theorem 1.2 (Second Sylow Theorem):** Let $G$ be a finite group with an order $p^k m$, where $m$ and $p$ are coprime.

1. Any $p$-subgroup of $G$ is contained in a Sylow $p$-subgroup of $G$. Hence, any two Sylow $p$-subgroups of $G$ are conjugate.
2. The number $n_p$ of Sylow $p$-subgroup divides $|G|$ and $n_p \equiv 1 \mod p$.

These will be used to show that the only finite simple group of order less than 60 is cyclic of prime order. A basic knowledge in group theory is assumed throughout this article. In particular, many proofs will involve the concept of group actions. They should illustrate one of the most important techniques in group theory.

2 Structure of $p$-Groups

To motivate the subject, let at the group of order 9. Figure 1 demonstrates a typical group of order $p^k$, where $p$ is prime. In studying a group, one would often try to divide a group into a set of smaller objects, called subgroups, in the hope that we might be able to piece together these subgroups to form an overall picture of the group of interest.
One characteristics highlighted in Figure 1 is a subgroup of order 3 (or \( p \) in general). In fact, there are 4 subgroups of order 3 in this group (exercise: find them all). Further investigation will yield a conclusion that this subgroup is in fact normal, and the group is abelian. With this information, one might conclude that this group is isomorphic to either \( \mathbb{Z}_3 \oplus \mathbb{Z}_3 \) or \( \mathbb{Z}_9 \). The fact that there is no element of order 9 then tells us that this group is isomorphic to \( \mathbb{Z}_3 \oplus \mathbb{Z}_3 \).

\[
\begin{array}{cccccccccc}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\
1 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\
2 & 2 & 5 & 9 & 3 & 1 & 7 & 8 & 6 & 4 \\
3 & 3 & 9 & 6 & 8 & 4 & 1 & 2 & 5 & 7 \\
4 & 4 & 3 & 8 & 7 & 9 & 5 & 1 & 2 & 6 \\
5 & 5 & 1 & 4 & 9 & 2 & 8 & 6 & 7 & 3 \\
6 & 6 & 7 & 1 & 5 & 8 & 3 & 9 & 4 & 2 \\
7 & 7 & 8 & 2 & 1 & 6 & 9 & 4 & 3 & 5 \\
8 & 8 & 6 & 5 & 2 & 7 & 4 & 3 & 9 & 1 \\
9 & 9 & 4 & 7 & 6 & 3 & 2 & 5 & 1 & 8 \\
\end{array}
\]

Figure 1: Multiplication table of a group of order 9

Our aim in this article will be to study the structure of \( p \)-group and then try to draw that structure from an arbitrary finite group. From this point onward, let \( p \) be some fixed prime number.

**Definition 2.1.** A finite group is called \( p \)-group if its order is \( p^k \) for some \( k \geq 1 \).

First, we should observe that by Lagrange’s theorem, any subgroup \( H \) of \( p \)-group \( G \) must also be a \( p \)-group. Further, if \( H \) is normal in \( G \) then the quotient is also a \( p \)-group. Now, we will study \( p \)-group by looking at its action on sets.

### 2.1 Actions of \( p \)-groups

**Lemma 2.1:** Let \( G \) be a \( p \)-group with a \( G \)-action on a finite set \( X \). If \( |X| \not\equiv 0 \mod p \), there exists \( x \in X \) which is invariant under \( G \)-action.

**Proof.** First, observe that \( X \) is a disjoint union of orbits;

\[
x = O_1 \sqcup \ldots \sqcup O_m.
\]

Since the cardinality of \( |O_i| \) is equal to the index of the stabilizer \( Stab(x_i) \) for some \( x_i \in O_i \), we have that \( |O_i| = p^{k_i} \) for some power \( k_i \geq 0 \). Now, if \( k_i > 0 \) for all \( 0 \leq i \leq m \), then \( p \) divides
\(|X|\), contradicting the hypothesis. So, there is some \(i\) such that \(|O_i| = \{x_i\}\). That is, \(x_i\) is fixed by all elements of \(G\).

**Corollary 2.2:** Suppose that a \(p\)-group \(H\) acts on a \(p\)-group \(G\) by automorphisms. If \(G \neq \{e\}\), then there exists a non-trivial element of \(G\) that is \(H\)-invariant.

**Proof.** Let \(X = G - \{e\}\), and apply Lemma 2.1.

**Corollary 2.3:** Let \(G\) be a \(p\)-group, then the centre of \(G\) is non-trivial.

**Proof.** Consider \(G\)-action on \(G\) itself by conjugation. By Corollary 2.2, there exists non-trivial \(z \in G\) such that \(g \cdot z = gzg^{-1} = z\) for all \(g \in G\). Hence, \(1 \neq z \in Z(G)\) as required.

### 2.2 Subgroups of \(p\)-groups

Corollary 2.3 and the fact that \(Z(G)\) is a normal subgroup in \(G\) imply that \(Z(G)\) is a non-trivial abelian \(p\)-group. Observe that every subgroup of \(Z(G)\) is normal. Suppose that it doesn’t contain any proper non-trivial subgroup, then it must be a cyclic of order \(p\). Otherwise, by induction, there exists a normal subgroup of order \(p\). We have just proved the following lemma.

**Lemma 2.4:** Let \(G\) be a \(p\)-group. Then, there is a normal subgroup of order \(p\) that is contained in the centre of \(G\).

**Theorem 2.5:** Let \(G\) be a \(p\)-group and \(H\) be a proper subgroup of \(G\). Then there exists a subgroup \(K\) such that \(H \triangleleft K\) and \(K/H \cong C_p\).

**Proof.** We will prove this by induction on order of \(G\). By Corollary 2.3, \(Z(G)\) is non-trivial and normal, so \(HZ(G)\) is a subgroup of \(G\). If \(HZ(G) = H\), then \(Z(G) \subseteq H\). So the image of \(H\) under quotient is a subgroup in \(G/Z(G)\). Since \(|G/Z(G)| < |G|\), by induction step there exists a subgroup \(K'\) containing \(HZ(G)\). Take \(K = \{g \in G \mid gZ(G) \in K'\}\).

Suppose that \(HZ(G) > H\). If \(g \in HZ(G)\), then we can write \(g\) as \(hz\), with \(h \in H\) and \(z \in Z(G)\). Notice that \(hzhz^{-1}h^{-1} = hHz^{-1}h^{-1} = hHh^{-1} = H\). So, \(H \triangleleft HZ(G)\). By Lemma 2.4, there exists a normal subgroup \(K'\) of order \(p\) in \(HZ(G)/H\). Take \(K\) to be the preimage of \(K'\).

Since the normaliser \(N_G(H)\) is, by definition, the largest subgroup of \(G\) such that \(H \triangleleft N_G(H)\), by the theorem above, \(N_G(H) \geq H\), so it is strictly larger than the subgroup \(H\). The second consequence of this theorem is; by repeatedly applying the theorem, one obtain a sequence

\(\{e\} = H_0 \triangleleft H_1 \triangleleft \ldots \triangleleft H_n = G,\)

where \(H_i/H_{i-1} \cong C_p\). In fact, we must have \(|G| = p^n\). In general, if the condition on the quotient is removed, a sequence

\(\{e\} = H_0 \triangleleft H_1 \triangleleft \ldots \triangleleft H_n = G,\)
is called subnormal series. The quotient \( H_i / H_{i-1} \) is called the factor groups. The group \( G \) is called polycyclic if there exists a normal series

\[
\{e\} = H_0 \lhd H_1 \lhd \ldots \lhd H_n = G,
\]
such that \( H_i / H_{i-1} \) is cyclic.

Alternatively, if a \( p \)-group \( G \) is non-trivial, then by Corollary 2.3, the centre \( Z(G) \) is non-trivial \( p \)-group. Suppose that \( G/Z(G) \) is non-trivial \( p \)-group. Apply the same corollary, we can conclude that \( Z(G/Z(G)) \) is non-trivial. Define a subgroup \( Z_2(G) \) of \( G \) to be the subgroup with image of \( Z(G/Z(G)) \) under quotient, so \( Z_2/Z \cong Z(G/Z(G)) \). If \( Z_2 \neq G \), we can play the same game again to get the next term.

**Definition 2.2.** For any group \( G \), define a series of subgroups \( Z_i \) for \( i = 0, 1, 2, \ldots \) as follows. Define \( Z_0 = \{e\} \). For \( i > 0 \), \( Z_i \) is the subgroup of \( G \) corresponding to \( Z(G/Z_{i-1}) \). The sequence

\[
\{e\} = Z_0 < Z_1 < \ldots,
\]
is called the upper central series of \( G \). The term \( Z_i \) is called \( i \)-th centre of group \( G \). A group \( G \) is called nilpotent if \( Z_m = G \) for some integer \( m \).

As noted before, the subgroup \( Z_i \) satisfies \( Z_i / Z_{i-1} \cong Z(G/Z_{i-1}) \). Now, by repeat applications of Lemma 2.3, we can conclude that the following:

**Theorem 2.6:** Any \( p \)-group is nilpotent and polycyclic.

In general, nilpotent property coincides with polycyclic property, when the group is finitely generated. In general, however, nilpotent group is not polycyclic.

### 3 Sylow’s Subgroup Theorem

**Definition 3.1.** Let \( G \) be a finite group and let \( p \) be a prime dividing the order \( |G| \) of \( G \). A \( p \)-subgroup of \( G \) is a subgroup of order \( p^k \) for some \( k \). A Sylow \( p \)-subgroup \( S \) is a \( p \)-subgroup of \( G \) such that \( p \nmid |G|/|S| \).

That is, Sylow \( p \)-group is a \( p \)-subgroup in \( G \) with order \( p^k \), where \( k \) is the largest possible for which \( p^k \) divides \( |G| \). Observe also that if \( S \) is a Sylow \( p \)-group, then its conjugate \( gSg^{-1} \) is a Sylow \( p \)-group as well. The next theorem is the most fundamental theorem in finite group theory.

**Theorem 3.1** (First Sylow Theorem): Let \( G \) be a finite group with order \( p^km \), where \( m \) and \( p \) are coprime. Then there exists a Sylow \( p \)-subgroup in \( G \).

Before proving this theorem, we need the following observation about finite group. Notice that \( G - Z(G) \) is a disjoint union of conjugacy classes. Suppose that \( G - Z(G) \) has \( r \) conjugacy classes. Denote \( n_i \) as a cardinality of the \( i \)-th conjugacy class. So, we must have that

\[
|G| = |Z(G)| + n_1 + n_2 + \ldots + n_r.
\]
This equation is called the class equation of the group $G$. Observe that $n_i > 1$ for all $i$. Suppose the otherwise. Let $h$ be the element in that conjugacy class. Then $ghg^{-1} = h$ for all $g \in G$. So, by definition of the centre, $h \in Z(G)$.

Let $C_i$ be the $i$-th conjugacy class. The group $G$ acts on $C_i$ by conjugation $g \in G : h \in C_i \mapsto ghg^{-1}$. If $h \in C_i$, then the stabiliser $\text{Stab}(h)$ is subgroup in $G$ satisfying $|G| = |\text{Orb}(h)||\text{Stab}(h)| = n_i|\text{Stab}(h)|$. The stabiliser $\text{Stab}(h)$ is called the centraliser $C(h)$ of $h$.

Let $G$ be a finite group with the order $|G| = p^km$. Suppose $p^k$ does not divide the order of any proper subgroup of $G$. If $h \in C_i$, then $C(h)$ is a proper subgroup of $G$ and therefore $p^k \nmid |C(h)|$. As $|G| = n_i|C(h)|$, this implies that $p|n_i$. Therefore, the class equation tells us that $p|Z(G)$. So we have proved the following lemma.

**Lemma 3.2**: Let $G$ be a finite group with order $|G| = p^km$. Either $p^k$ divides the order of some proper subgroup of $G$ or $p$ divides the order of the centre $Z(G)$.

Now, we are ready to prove Sylow Subgroup theorem.

**Proof of Theorem 3.1**. We will prove this by induction on the order of $G$. We may assume that $p^k$ does not divide the order of any proper subgroup of $G$. Otherwise, by induction step, a Sylow $p$-subgroup of such subgroup is also a Sylow $p$-group of $G$. So, by Lemma 3.2, $p$ divides $|Z(G)|$ and thus either;

- $|Z(G)| = p^lm'$ for some $l < k$ and $m'|m$; or
- $Z(G) = G$.

In the latter case, $G$ is abelian, so we can use classification of abelian groups to find a Sylow $p$-subgroup.

In the first case, by induction step, there is a $p$-subgroup $H \leq Z(G)$ with $|H| = p^l$. Observe that $H$ is normal in $G$ and thus $G/H$ is well-defined. Further, $|G/H| = p^{k-l}m < |G|$, and hence there is a $p$-subgroup $H'$ with $|H'| = p^{k-l}$. The preimage $K = \{g \in G \mid gH \in H'\}$ is a subgroup of $G$ with $|K| = |H'||H'| = p^k$. Therefore, the subgroup $K$ is the desired Sylow $p$-subgroup.

**Corollary 3.3** (Cauchy’s Theorem): Let $G$ be a finite group such that $p$ divides $|G|$. Then, $G$ contains an element of order $p$.

**Theorem 3.4** (Second Sylow Theorem): Let $G$ be a finite group with order $p^km$, where $m$ and $p$ are coprime.

1. Any $p$-subgroup of $G$ is contained in a Sylow $p$-subgroup of $G$. Hence, any two Sylow $p$-subgroups of $G$ are conjugate.
2. The number $n_p$ of Sylow $p$-subgroup divides $|G|$ and $n_p \equiv 1 \mod p$.

**Proof.** Let $H$ be a $p$-subgroup of $G$ and $S_p$ be a Sylow $p$-subgroup of $G$. Let $C$ be a set of $S_p$-left cosets. The group $G$ acts on $C$ by left multiplication. This induces $H$-action on $C$. Observe that $|C| = m$, and $p \nmid m$. So, by Lemma 2.1, there exists $g \in G$ such that $hgS_p = gS_p$ for all $h \in H$. Therefore $g^{-1}Hg \subseteq S_p$, thus $H \subseteq gS_pg^{-1}$ for some $g \in G$. Let $H$ be the other Sylow $p$-subgroup to show the second assertion.

Consider the set $M = \{gS_pg^{-1} \mid g \in G\}$ of conjugates of a Sylow $p$-subgroup $S_p$. Note that $M$ is the set of all Sylow $p$-subgroups. Let $n_p = |M|$. Clearly, $n_p$ divides $|G|$. Let $S_p$ acts on
\[ M' = M \setminus \{ S_p \} \] by conjugation. This is a well-defined action. For if there exists \( s \in S_p \) such that \( sgS_p g^{-1}s^{-1} = S_p \), then \( gS_p g^{-1} = S_p \).

We claim that there is no \( S_p \)-invariant element in \( M' \). Suppose not. Then, there exists \( g \notin \text{Stab}(S_p) \), such that \( sgS_p g^{-1}s^{-1} = gS_p g^{-1} \) for all \( s \in S_p \). Thus, \( S_p \neq g^{-1}S_p g \subseteq \text{Stab}(S_p) \) for all \( g \). Since \( g^{-1}S_p g \) is another Sylow \( p \)-subgroup of \( \text{Stab}(S_p) \), there is \( s \in \text{Stab}(S_p) \) such that
\[
g^{-1}S_p g = sS_p s^{-1} \iff S_p = gsS_p g^{-1}.
\]

So, \( gs \in \text{Stab}(S_p) \) and hence \( g \), contradicting hypothesis.

By Lemma 2.1, \( n_p - 1 = |M'| \equiv 0 \mod p \) and hence \( n_p \equiv 1 \mod p \). \( \square \)

Since Sylow’s Theorem is so fundamental in finite group theory, we will show an alternative proof. It will demonstrate how one can obtain information from group action on a set if one choose the set cleverly.

**Alternative proof of the First Sylow Theorem.** We will prove by induction on the order of \( G \). Let \( \Omega \) be a set of all subsets of \( G \) of size \( p^k \). The group \( G \) acts on \( \Omega \) naturally by left multiplication. Observe that \( |\Omega| = \binom{p^m}{p^k} \) and hence \( p \nmid |\Omega| \) (check). Suppose that for each \( \omega \in \Omega \), \( p^k \nmid \text{Stab}(\omega) \). This implies that \( p \mid \text{Orb}(\omega) \). Since \( |\Omega| \) is equal to the sum of distinct orbits, we have \( p \) divides \( |\Omega| \), which is absurd. So, there exists \( \omega \in \Omega \) such that \( p^k \mid \text{Stab}(\omega) \).

If \( \text{Stab}(\omega) \) is a proper subgroup of \( G \), then by induction, we are done. Otherwise \( \text{Stab}(\omega) = G \supset \omega \). Therefore, \( \omega \) is a subgroup of \( G \) of order \( p^k \). \( \square \)

**Corollary 3.5:** Let \( G \) be a finite group with order \( p^k m \), where \( m \) and \( p \) are coprime. If \( m = q \neq 1 \mod p \) for prime \( q \), then the Sylow \( p \)-subgroup is normal.

4 Some Properties of Sylow \( p \)-subgroup

**Proposition 4.1:** Let \( H \) be a \( p \)-subgroup of a group \( G \). If \( H \) is a Sylow \( p \)-subgroup of \( N_G(H) \), then it is a Sylow \( p \)-subgroup of \( G \).

**Proof.** Suppose not. By Theorem 3.4, there is a Sylow \( p \)-subgroup \( S_p \) in \( G \) that strictly contains \( H \). By Theorem 2.5, we have \( N_G(H) \supseteq N_{S_p}(H) > H \). But that contradicts the fact that \( H \) is a Sylow \( p \)-subgroup of \( N_G(H) \) as \( N_{S_p}(H) \) is also another \( p \)-subgroup.

**Theorem 4.2:** Let \( H \) be a normal subgroup of a group \( G \), and let \( S_p \) be a Sylow \( p \)-subgroup of \( G \). Then, the intersection \( S_p \cap H \) is a Sylow \( p \)-subgroup of \( G \).

**Proof.** First, \( S_p \cap H \) is a \( p \)-subgroup in \( H \). Observe that \( [H : S_p \cap H] = [S_p H : S_p] \). Since \( S_p \) is a Sylow \( p \)-subgroup of \( G \), it is also for \( S_p \cap H \). So, \( [S_p H : S_p] \) is prime to \( p \). Hence \( S_p \cap H \) is a Sylow \( p \)-subgroup of \( H \).

Note that \( S_p H / H \cong S_p / (S_p \cap H) \), so \( S_p H / H \) is a \( p \)-subgroup of \( G / H \). Now, \( [G / H : S_p H / H] = [G : S_p H] \) which is prime to \( p \), so \( S_p H / H \) is a Sylow \( p \)-subgroup of \( G / H \). \( \square \)

**Theorem 4.3:** Let \( H \) be a normal subgroup of a group \( G \). If \( S_p \) is a Sylow \( p \)-subgroup of \( H \), then \( G = N_G(S_p) H \).
Proof. Let \( S^g \) be \( S_p \) conjugated by \( g \). As \( H \) is normal in \( G \), \( S^g \) is in \( H \) and therefore by Theorem 3.4 it is conjugate to \( S_p \). So, there is \( h \in H \), such that \( S^h = S^g \). Let \( n = gh^{-1} \). Observe that \( S^n = S_p \), so \( n \in N_G(S_p) \). As \( g = nh \), we have \( G = N_S(S_p)H \).

\[ \square \]

5 Some Applications of Sylow’s Theorem

The following theorems will be useful in the classification of finite simple group.

Theorem 5.1: Let \( p \) and \( q \) be prime numbers, where \( p < q \) and \( q \neq 1 \mod p \). Then, any group \( G \) of order \( pq \) is cyclic.

Proof. By Theorem 3.1, there are Sylow \( p \)-subgroups and Sylow \( q \)-subgroups. Let \( S_i \) denote a Sylow \( i \)-subgroup. By Corollary 3.5, \( S_p \) is normal. As \( q > p \), so \( p \neq 1 \mod q \), \( n_q \) must be 1, so \( S_q \) is normal. Now \( S_p \cap S_q \) is a subgroup of both \( S_p \) and \( S_q \). By Lagrange’s Theorem, \( S_p \cap S_q = \{e\} \).

Let \( g \in S_p \) and \( h \in S_q \). Then \( h^{-1}g^{-1}h^{-1} \in S_p \) and \( gh^{-1} \in S_q \) as both are normal subgroups of \( G \). So, \( gh^{-1}h^{-1} \in S_p \cap S_q = \{e\} \) and hence \( S_p \) commutes with \( S_q \). A function \( \phi : S_p \oplus S_q \to G \) which sends \( (g,h) \mapsto gh \) is a homomorphism. This function is injective. For if \( gh = e \), then \( g = h^{-1} \) and thus \( g \in S_p \cap S_q \). Now, as \( \phi \) is an injective homomorphism between two finite groups of the same order, it follows that \( \phi \) is surjective. Therefore, \( G \cong S_p \oplus S_q \).

First, any group of order prime must be cyclic. Let 1 be the generator of a cyclic group. Then, the order of \( (1,1) \in S_p \oplus S_q \) must divide \( pq \). So, it must either be 1, \( p \), \( q \), or \( pq \). Clearly it is not 1. Observe that \( (1,1)^p = (p, p) = (e, p) \neq e_G \). Similarly for \( (1,1)^q \), so the order of \( (1,1) \) must be \( pq \). Therefore, \( S_p \oplus S_q \) is generated by \( (1,1) \) and thus \( G \) is cyclic.

\[ \square \]

Theorem 5.2: Any group of order \( 2p \), where \( p \) is prime greater than 2 is either cyclic or isomorphic to a dihedral group \( D_{2p} \).

Proof. From the First Sylow Theorem, a group \( G \) contains Sylow subgroups, \( S_2 \) and \( S_p \). The Second Sylow Theorem asserts that \( S_p \) must be normal, since \( 2 \neq 1 \mod p \). Any group of order prime must be cyclic. Let \( x \) and \( y \) be generators of \( S_2 \) and \( S_p \) respectively. Note that \( x = x^{-1} \) and \( xyx^{-1} = y_k \in S_p \) for some \( k < p \) as \( S_p \) is normal. Then

\[ y = x^{-1}y^kx = xy^kx^{-1} = (xyx^{-1})^k = y^{k^2} \]

So, \( p \mid k^2 - 1 \) as the order of \( y \) is \( p \). Observe that \( k^2 - 1 = (k - 1)(k + 1) \). If \( p \mid k - 1 \), then \( k = 1 \), and \( S_2 \) commutes with \( S_p \). A similar argument to the proof of Theorem 5.1 shows that \( G \) is cyclic. If \( p \mid k + 1 \), then \( k = p - 1 \). This is precisely the presentation of a dihedral group as \( x, y \) generate \( G \).

\[ \square \]

Theorem 5.3: Let \( p \) and \( q \) be prime numbers with \( p < q \), and let \( d \) be the smallest number such that \( p^d \equiv 1 \mod q \). Then, any group of order \( p^k q \) where \( 1 \leq k < d \) contains a normal subgroup of order \( q \). If \( |G| = p^d q \), then either \( G \) contains a normal subgroup of order \( q \) or a normal subgroup of order \( p^d \).

Proof. The first assertion is a direct application of the First and the Second Sylow Theorems.
Suppose that \(|G| = p^d q^e\). The First Sylow Theorem asserts that \(G\) contains a Sylow \(q\)-subgroup \(S_q\). The Second Sylow theorem tells us that the number of such subgroups is congruent to 1 mod \(q\). The hypothesis implies that \(n_q = 1\) or \(p^d\). If \(n_q = 1\) then \(S_q\) is normal and we are done. So, we may assume that \(n_q = p^d\). Suppose that \(S_q\) and \(S'_q\) are two Sylow \(q\)-subgroups. By applying Lagrange’s Theorem, we can concluded that \(S_q \cap S'_q = \{e\}\). It follows that each element of order \(q\) is in exactly one of Sylow \(q\)-subgroups. Then, the number of elements of order \(q\) is \(p^d(q - 1)\). That leaves \(p^d\) elements of other order. By the First Sylow Theorem, \(G\) contains a Sylow \(p\)-subgroup \(S_p\) of order \(p^d\). Notice that the order of any element of \(S_p\) cannot be a multiple of \(q\). So, there is only one Sylow \(p\)-subgroup. The Second Sylow Theorem implies that \(S_p\) is normal.

6 Finite Simple Groups

Definition 6.1. A non-trivial group \(G\) is simple if the only proper normal subgroup is a trivial subgroup.

One of the greatest challenge in the 20th century is the classification of finite simple groups. Sylow’s Subgroup Theorems can be use to prove the following statement:

Any finite simple group of order less than 60 is cyclic of prime order.

Cyclic groups of prime order less than 60 are those of order

\[
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59
\]

It is an easy exercise to show that any group of order prime must be cyclic and simple. For other groups, we will begin by considering the consequences of theorems from the previous section.

- **Theorem 5.2**: A group of order \(2p\) is either cyclic or isomorphic to a dihedral group. In either case, Sylow \(p\)-subgroup is normal. It follows that there is no simple group of order \(6, 10, 14, 22, 26, 34, 38, 46,\) or \(58\).

- **Theorem 5.3**: There is no simple group of order \(12, 15, 20, 21, 28, 33, 35, 39, 40, 44, 45, 51, 52, 55, 56,\) or \(57\).

- **Lemma 2.4**: Obviously, if a group \(G\) is of prime order, then that normal subgroup is itself. But if \(|G| = p^k\), where \(k > 1\), this lemma implies that there is a non-trivial normal subgroup of \(G\). So, there is no simple group of order \(4, 8, 9, 16, 25, 27, 32,\) or \(49\).

This leaves the groups of order \(18, 24, 30, 36, 42, 48, 50,\) and \(54\) to be verified. To do this, we need the following lemma.

**Lemma 6.1**: Let \(G\) be a group with a subgroup \(H\) of index \(n\). Then there exists a normal subgroup \(N \leq H\), such that \(|G : N| = n!\). In particular, any subgroup of index 2 is normal.

**Proof.** Consider a group \(G\) acting on a set of \(H\)-left cosets. This induces a homomorphism from \(G\) to a symmetric group \(S_n\). Note that the kernel \(K\) is a subgroup of \(H\) since any element in \(K\) must fix \(H\). So, \(K\) is the desired subgroup. The second assertion is true by Lagrange’s Theorem.
Corollary 6.2: Let $G$ be a group with a subgroup $H$ of index $n$. If $n! < |G|$, then the group $G$ is not simple.

Proof. If $n! < |G|$, $H$ contains a normal subgroup $N$ which is non-trivial. □

A simple application of the First Sylow Theorem shows that groups of order 18, 24, 36, 48, 50, and 54 have subgroups of order 2, 3, 4, 3, 2, and 2 respectively. Apply Corollary 6.2 to conclude that there is no simple group of order 18, 24, 36, 48, 50, and 54. This leaves groups of order 30 and 42.

If the order of a group $G$ is 30 = $2 \times 3 \times 5$, then First Sylow Theorem implies that $G$ contains Sylow $p$-subgroups $S_5$ and $S_3$. Suppose that $S_5$ and $S_3$ are not normal in $G$. Then $n_5 = 6$ and $n_3 = 10$. If $S_5'$ is another Sylow 5-subgroup, then $S_5 \cap S_5'$ is a proper subgroup. By Lagrange’s Theorem, we can conclude that $S_5 \cap S_5' = \{e\}$ as $|S_5| = 5$. So, Any element of order 5 must be in exactly one of these subgroups. Similar conclusion can be made about $S_3$. So, the total number of element with order 3 or 5 is $6 \times 4 + 10 \times 2 = 44 > 30$. So, at least one of $S_3$ or $S_5$ must be normal. A group of order 30 is not simple.

If the order of the group is 42 = $6 \times 7$, then by the First Sylow Theorem, $G$ contains a subgroup of order 7. The Second Sylow Theorem forces $n_7$ to be 1. Thus, $S_7$ is normal in $G$. A group of order 42 is not simple.

There is a simple group of order 60 which is not cyclic.

Definition 6.2. An alternating group of degree $n$ is a subgroup of a symmetric group $S_n$ consisting of all even permutation.

Despite the suggestion that alternating group is a group, one still need to check that it is actually a group. Indeed, identity is an even permutation; any product of even permutations will give an even permutation; and the inverse of even permutation is an even permutation. Denote $A_n$ an alternating group of degree $n$. We will sketch a proof that alternating group of degree 5 is simple. In fact the proof can be applied to any alternating group of degree $n \geq 5$. The detail can be found in de La Harpe’s book [1].

Sketch of proof.

Step 1: Show that $A_n$ is generated by cycles of order 3.
Step 2: Show that if a normal subgroup $N$ of $A_n$ contains a cycle of length 3, then $N = A_n$.
Step 3: Show that any normal subgroup of $A_{n \geq 5}$ contains a cycle of length 3. □

References


[3] David Wilkins. Part ii: Topics in group theory. Lecture notes for course 311 (Abstract algebra), as it was taught at Trinity College, Dublin, 2005.