Sylow Theorem

Liming Pang

1 Sylow Theorem

Definition 1. $p$ is a prime and $G$ is a group whose order is divisible by $p$. A subgroup $H$ of $G$ is a {p-subgroup} if $|H| = p^r$ for some positive integer $r$.

Definition 2. $G$ is a group such that $|G| = p^e m$, where $p$ is a prime, $e$ is a positive integer and $p$ doesn’t divide $m$. A subgroup $H$ of $G$ is a {Sylow p-subgroup} if $|H| = p^e$.

Theorem 3. (Sylow Theorem) $G$ is a group such that $|G| = p^e m$, where $p$ is a prime, $e$ is a positive integer and $p$ doesn’t divide $m$. Then;

(i). There exists a Sylow $p$-subgroup of $G$

(ii). If $H$ is a Sylow $p$-group of $G$ and $K$ is a $p$-group of $G$, then there exists $g \in G$ such that $K \subseteq gHg^{-1}$

(iii). The number of Sylow $p$-subgroups divides $m$ and congruent to 1 modulo $p$.

Corollary 4. All the Sylow $p$-subgroups are conjugate to each other, and a Sylow $p$-subgroup is a normal subgroup of $G$ if and only it is the only Sylow $p$-subgroup of $G$.

We will prove this significant theorem in the next section, and we will first see some applications instead.

Example 5. We will show that any group of order 15 is isomorphic to $\mathbb{Z}/15\mathbb{Z}$.

If $G$ is a group of order $15 = 3 \times 5$, it will have Sylow 3-subgroups and Sylow 5-subgroups, i.e. subgroups of order 3 and order 5. (This can also be seen from the Cauchy’s Theorem). The number of Sylow 3-subgroups divides 5 and is congruent to 1 modulo 3, so it has to be 1, which then implies this
unique Sylow 3-subgroup is a normal subgroup of $G$, and call it $H$. Similarly, we can show that there is a unique Sylow 5-subgroup of $G$ that is a normal subgroup, and call it $K$. Since 3 and 5 are primes, we know $H \cong \mathbb{Z}/3\mathbb{Z}$ and $K \cong \mathbb{Z}/5\mathbb{Z}$.

$|H| = 3$ and $|K| = 5$ implies $|H \cap K| = 1$, so $H \cap K = \{1\}$.

$|HK| = \frac{|H| \times |K|}{|H \cap K|} = \frac{3 \times 5}{1} = 15 = |G|$, so $HK = G$

and together with the fact $H,K$ are normal subgroups of $G$, we conclude $G \cong H \times K \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/15\mathbb{Z}$.

**Example 6.** We will show that any group of order 224 is not simple.

If $|G| = 224 = 2^5 \times 7$, then it has Sylow 2-subgroup of order 32 and Sylow 7-subgroup of order 7. The number of Sylow 2-subgroups divides 7 and is congruent to 1 modulo 2, so it may be 1 or 7.

If the number of Sylow 2-subgroups is 1, then this unique Sylow 2-subgroup is a proper normal subgroup, so $G$ is not simple.

If the number of Sylow 2-subgroups is 7, let $S$ be the set of all Sylow 2-subgroups, and $G$ acts on $S$ by conjugation, and this group action corresponds to a homomorphism

$$\Phi : G \longrightarrow S_7$$

$\Phi$ is not the trivial homomorphism, since the action is transitive, which implies the action is not the trivial action. Also $\Phi$ cannot be injective, since $|G| = 2^5 \times 7$ does not divide $|S_7| = 7!$. So ker $\Phi$ is neither $G$ nor $\{1\}$, we conclude ker $\Phi$ is a proper normal subgroup of $G$, so $G$ is not simple.

## 2 Proof of Sylow Theorem

**Lemma 7.** If $n = p^e m$ where $p$ is a prime, $e > 1$ and $p$ doesn’t divide $m$, then $p$ does not divide $\binom{n}{p^e}$, which the number of ways to choose $p^e$ elements from a set of $n$ elements.

**Lemma 8.** $G$ is a group and $k$ is a positive integer with $k \leq |G|$. $S$ is the set of all subsets of cardinality $k$ of $G$. $G$ has an action on $S$ by left multiplication:

$$g \cdot \{x_1, ..., x_k\} = \{gx_1, ..., gx_k\}$$

and for this action, $|G_U|$ divides $k$ for any $U \in S$. 

2
Proof. It is easy to see \( g \{ x_1, ..., x_k \} = \{ gx_1, ..., gx_k \} \) defines a group action, so we leave this part as an exercise.

To show \( G_U \) divides \( k \), it suffices to show \( U \) is a disjoint union of some right cosets of \( G_U \) in \( G \), since all the right cosets of \( G_U \) in \( G \) are disjoint and have the same number of elements.

If \( G_Ug \cap U \neq \emptyset \), then there exists \( g' \in G \) such that \( g' \in G_Ug \cap U \), so \( G_Ug = G_Ug' \). \( G_U \) is the stabiliser of \( U \), and \( g' \in U \), so \( G_Ug' \subseteq U \). We thus see \( U \) is a disjoint union of some right cosets of \( G_U \) in \( G \).

Lemma 9. \( \text{(Fixed Point Theorem)} \) \( G \) is a group acting on a set \( X \). \( |G| = p^k \), where \( p \) is a prime and \( k > 0 \). If \( p \) does not divide \( |X| \), then there exists a fixed point \( x \in X \) under this action, i.e. \( g.x = x \) for any \( g \in G \).

Proof. Suppose there is no fixed point. Then for any \( y \in X \), the orbit \( O(y) \) has size \( |O(y)| > 1 \), and \( |O(y)| = \frac{|G|}{|G_U|} = p^k |G_U|^{-1} \) so \( |O(y)| \) is a positive power of \( p \), in particular, \( p \) divides \( O(y) \).

\( X \) is the disjoint union of all the orbits, so it follows \( |X| \) is divisible by \( p \), contradiction. \( \square \)

Lemma 10. \( G \) is a group acting on \( X \). For any \( g \in G \), any \( x \in X \):

\[
G_{g.x} = gG_xg^{-1}
\]

Proof. \( h \in G_{g.x} \iff h.(g.x) = g.x \iff (hg).x = g.x \iff (g^{-1}hg).x = x \iff g^{-1}hg \in G_x \iff h \in gG_xg^{-1} \) \( \square \)

Now we shall begin the proof of Sylow Theorem.

2.1 Proof of (i)

We are going to show that \( G \) has a Sylow \( p \)-subgroup.

Let \( G \) act on \( S \), the set of all subsets of \( G \) with \( p^e \) elements. \( |S| = \binom{n}{p^e} \), and by Lemma 7, \( p \) does not divide \( |S| \), so there exists \( U \in S \) such that \( p \) does not divide \( |O(U)| \).

Applying the Counting Formula,

\[
|O(U)||G_U| = |G| = p^em
\]

so \( p \) not dividing \( |O(U)| \) implies \( p^e \) dividing \( |G_U| \)

if we apply Lemma 8, we get \( |G_U| \) divides \( p^e \) as well, so we conclude \( |G_U| = p^e \), and thus we have found a Sylow \( p \)-subgroup of \( G \).
2.2 Proof of (ii)

Let $H$ be a Sylow $p$-subgroup of $G$ and $K$ a $p$-subgroup of $G$, so $|H| = p^e$ and $|K| = p^r$ for some $1 \leq r \leq e$.

$G$ acts on $X = G/H$, the set of left cosets of $H$ in $G$, by left multiplication:

$$g \cdot xH = (gx)H$$

it is left as an exercise to show that $G_H = H$.

Now restrict the action to the subgroup $K$. $|K| = p^r$, and by Lagrange Theorem, $|X| = \frac{|G|}{|H|} = m$, which is not divisible by $p$. So we can apply Lemma 9, there exists a fixed point $gH \in X$ for this $K$-action on $X$, i.e. $K_{gH} = K$.

In particular, we get $K \subseteq G_H = gG_Hg^{-1} = gHg^{-1}$ by Lemma 10.

2.3 Proof of (iii)

Let $Y$ be the set of Sylow $p$-subgroups of $G$. By Corollary 4 (which is a consequence of (ii) and (ii) has been proved), $G$ acts on $Y$ by conjugation transitively.

Let $H \in Y$, then $G_H = \{g \in G | gHg^{-1} = H\} = N(H)$, the normaliser of $H$. We leave it as an exercise to show that $H$ is a normal subgroup of $N(H)$. In particular, $|H|$ divides $N(H)$, $\frac{|G|}{N(H)}$ divides $\frac{|G|}{|H|}$.

The Counting Formula implies $|Y| = |O(H)| = \frac{|G|}{|N(H)|}$, which divides $\frac{|G|}{|H|} = \frac{p^e}{p^r} = m$, i.e. $|Y|$ divides $m$.

Now we restrict the group action to the subgroup $H$, that is, let $H$ act on $Y$ by conjugation.

$H \subseteq N(H)$ implies $O(H) = \{H\}$, $|O(H)| = 1$. Note $|H| = p^e$, so the number of elements in any orbit divides $p^e$. We know $|Y|$ is the summation of the cardinality of all its orbits, so in order to show $|Y| \equiv 1$ (mod $p$), it suffices to show the number of elements in any orbit other than $\{H\}$ is more than one:

If $H' \in Y$ and $O(H') = \{H'\}$, then $H \subseteq N(H')$, we see both $H$ and $H'$ are Sylow $p$-subgroups of $N(H')$. But $H'$ is a normal subgroup in $N(H')$, which implies $H'$ is the only Sylow $p$-subgroup of $N(H')$, hence $H = H'$. So $\{H\}$ is the only orbit with one element.