II.5. Sylow’s Theorems

Groups in this section are all finite groups.

(5.1) **Definition:** Let $G$ be a group and $p$ be a prime. A (sub)group $H$ with $|H| = p^a$ is called a $p$-(sub)group. A maximal $p$-subgroup of $G$ is a **Sylow $p$-subgroup** of $G$. The set of all Sylow $p$-subgroups of $G$ is $\text{Syl}_p(G)$, and $n_p = |\text{Syl}_p(G)|$.

(5.2) (Lemma 5.5) Let $H$ be a $p$-group of $G$. Then

$$[N_G(H) : H] = [G : H] \text{(mod } p).$$

**Proof:** Let $\mathcal{L}$ be the left cosets of $H$ in $G$, and let $H$ act on $\mathcal{L}$ by $h(xH) = (hx)H$. Then $\mathcal{L}$ is an $H$-set. Note that $|\mathcal{L}| = [G : H]$, and note that $\forall h \in H, x \in G$,

$$hxH = xH \iff x^{-1}hxH = H \iff x^{-1}hx \in H \iff x \in N_G(H).$$

Hence the number of fixed points of this action is $|\mathcal{L}_H| = [N_G(H) : H]$. Since $|H| = p^n$, by (4.7), $[N_G(H) : H] = [\mathcal{L}_H] \equiv [G : H] \text{(mod } p).$

(5.2a) (Cor 5.6) Let $H$ be a $p$-subgroup of a finite group $G$. If $p$ divides $[G : H]$, then $N_G(H) \neq H$.

(5.3) **The First Sylow Theorem** (Thm 5.7) Let $G$ be a group of order $p^am$, where $a > 0$ and where $p$ is a prime not dividing $m$. Then

(i) $G$ contains a subgroup of order $p^i$ for each $i$ where $0 \leq i \leq a$,

(ii) every subgroup $H$ of $G$ of order $p^i$ is a normal subgroup of a subgroup of order $p^{i+1}$ for $1 \leq i < a$.

**Proof:** (i) By induction on $a$. Clearly $G$ has a subgroup of order 1. Suppose that $H$ is a subgroup of order $p^i$ for some $0 \leq i < a$. Since $i < a$, $p$ divides $p^{a-i}m = [G : H]$.

By (5.2a), $|N_G(H) : H| > 0$. Since $H \subseteq N_G(H)$, the group $N_G(H)/H$ has $p$ as a factor, and so by Cauchy’s Theorem (4.8), $N_G(H)/H$ has a subgroup $K'$ of order $p$. Let $K = \{k \in N_G(H)|kH \in K'\}$. Then $K$ is the inverse image of a homomorphism, and so $K \leq N(G) \leq G$. Since $|K : H| = |K'| = p$, $|K| = p^{i+1}$.

(ii) Note that in (i), $H \leq K \leq N_G(H)$. Since $H \subseteq N_G(H)$, $H \subseteq K$.

(5.4) **The Second Sylow Theorem** (Thm 5.9) Let $G$ be a finite group and let $P_1, P_2 \in \text{Syl}_p(G)$.
Then there is some \( g \in G \) such that \( P_1 = gP_2g^{-1} \).

**Proof:** (The trick here is to let one \( (P_2, \text{say}) \) act on the left cosets of the other \( (P_1) \).)

Let \( L \) be the collection of left cosets of \( P_1 \), and let \( P_2 \) act on \( L \) by

\[
\forall y \in P_2, y(gP_1) = (yg)P_1.
\]

The fixed points: By (4.7), \(|L_{P_2}| \equiv |L| \pmod{p} \). Since \( P_1 \in Syl(G) \), \(|L| = |G : P_1| \) is not divisible by \( p \). Hence \(|L_{P_2}| > 0 \). Let \( zP_1 \in L_{P_2} \). Then

\[
\forall y \in P_2, y(zP_1) = zP_1 \implies z^{-1}P_2z \leq P_1 \implies z^{-1}P_2z = P_1,
\]

where the last equality follows by counting. Finally, set \( g = z^{-1} \).

(5.5) **The Third Sylow Theorem** (Thm 5.10) If \(|G| = p^n m < \infty \) (where \( p \) is a prime) and if \( n_p = |Syl_p(G)| \), then

\[
\text{both } n_p \equiv 1 \pmod{p} \text{ and } n_p|m.
\]

**Proof:** **Action 1:** Fix \( Q \in Syl_p(G) \). Let \( Q \) act on \( Syl_p(G) \) by conjugation:

\[
\forall x \in Q \text{ and } \forall P \in Syl_p(G), x(P) = xPx^{-1}.
\]

The fixed points: By (1.6b), \(|(Syl_p(G))_Q| \equiv |Syl_p(G)| \pmod{p} \).

\[
(Syl_p(G))_Q = \{P \in Syl_p(G)|xPx^{-1} = P, \forall x \in Q\} = \{P \in Syl_p(G)|Q \leq N_G(P)\},
\]

and so \( P, Q \in Syl_p(N(P)) \). Apply 2nd Sylow Theorem to \( N_G(P) \), there is a \( g \in N_G(P) \) such that \( Q = gPg^{-1} = P \), (the last equality follows from \( g \in N_G(P) \). Thus \( (Syl_p(G))_Q = \{Q\} \).

By (4.7), \( n_p = |Syl_p(G)| \equiv |(Syl_p(G))_Q| = 1 \pmod{p} \).

**Action 2:** Let \( G \) act on \( Syl_p(G) \) by conjugation. By (5.4), the action is transitive, and so \( G_P = Syl_p(G) \) is the only orbit. By (4.4), \( n_p = |Syl_p(G)| = |G : G_P| \) and so by Lagrange’s theorem, \( n_p \) divides \(|G|\).

(5.6) **Sylow’s Theorem** (A combined statement) Let \( G \) be a group of order \( p^n m \), where \( p \) is a prime not dividing \( m \).

(i) \( Syl_p(G) \neq \emptyset \), and if \( H \) is a \( p \)-subgroup of \( G \) such that \(|G : H| \equiv 0 \pmod{p} \), then there exists a \( p \)-subgroup \( H' \) of \( G \) such that \(|H' : H| = p \).

(ii) If \( P \) is a Sylow \( p \)-subgroup of \( G \) and \( Q \) is a \( p \)-subgroup of \( G \), then there exists \( g \in G \) such that \( Q \leq gPg^{-1} \). In particular, any two Sylow \( p \)-subgroups of \( G \) are conjugate in \( G \).

(iii) The number of Sylow \( p \)-subgroups \( n_p \equiv 1 \pmod{p} \) and \( n_p|m \).
5A. Theorems on Sylow $p$-groups

In this section, we make the following assumptions: $|G| = p^am$ for some prime $p$, where integers $a > 0$ and $m$ satisfies $(m,p) = 1$.

(5A.1) Suppose that $P \in Syl_p(G)$, and $N \leq G$ such that $N_G(P) \leq N$. Then $N_G(N) = N$.

**Proof:** It suffices to show that $N_G(N) \subseteq N$. \(\forall x \in N_G(N), Q = xPx^{-1} \in Syl_p(G)\). Since $x \in N_G(N)$ and $P \leq N$, then $Q = xPx^{-1} \leq xNx^{-1} = N$, and so $P, Q \in Syl_p(N)$. By 2nd Sylow Theorem, \(\exists y \in N, \text{ such that } P = yQy^{-1} = (yx)P(yx)^{-1}\). It follows that \(yx \in N_G(P) \subseteq N\). But $y \in N$, and so $x \in N$.

(5A.2) Suppose that $H = H_1 \cap H_2$ is maximal in the set of \(\{H, \cap H_j : H_i, H_j \text{ are distinct members in } Syl_p(G)\}\). Let $N = N_G(H)$. Then

(i) If $K \in Syl_p(N)$, then there exists exactly one $P \in Syl_p(G)$ such that $K = P \cap N$.

(ii) If $P \in Syl_p(G)$ such that $H \leq P$, then $P \cap N \in Syl_p(N)$.

(iii) If $K_1, K_2 \in Syl_p(N)$ are two distinct members, then $K_1 \cap K_2 = H$.

(iv) If $K \in Syl_p(N)$, then $N_K(K) = N \cap N_G(P)$ for some $P \in Syl_p(G)$ such that $H \leq P$.

(v) $|N : H| > 1$, and every Sylow $p$-subgroup of $N$ contains $H$ properly.

(vi) $|Syl_p(N)| > 1$.

**Proof:** Since $H \neq H_1$, then $N \neq N_{H_1}(H) \subseteq H_1 \cap N$. Therefore, there exists a $K \in Syl_p(N)$ such that $H_1 \cap H \leq K$. By 1st Sylow Theorem, there exists a $P \in Syl_p(G)$ such that $K \leq P$. Since

\[N \neq H_1 \cap N \leq P \cap H_1,\]

We must have $H_1 = P$, and so $P \cap N = H_1 \cap N$ (this proves (i) and (ii)).

Let $K_1, K_2 \in Syl_p(N)$ be two distinct members, and let $K \in Syl_p(N)$ be a member such that $H \leq K$. By 2nd Sylow Theorem, there exists $z \in N$ such that $K_1 = zKz^{-1}$.

Since $z \in N = N_G(H)$ and since $H \leq K$, $H = zHz^{-1} \leq zKz^{-1} = K_1$. Similarly, $H \leq K_2$. Therefore, $H \leq H_1 \cap H_2$. By (iv) (just shown above), there exist $P_1, P_2 \in Syl_p(G)$ such that $K_1 = P_1 \cap N$. Therefore, $H \subseteq P_1 \cap P_2$. By the maximality of $H$, $H = P_1 \cap P_2 = K_1 \cap K_2$. This proves (iii).

Let $K = H_1 \cap N$. Then by checking the definition for normalizer, we have $K \triangleleft N_G(H_1) \cap N$. If for any $x \in N$, $xKx^{-1} = K$, then $K \subseteq xH_1x^{-1}, \forall x \in N$, and so by (iv), $H_1 = xH_1x^{-1}$.
It follows that \( x \in N_G(H_1) \cap N = K \). This would imply that

\[
H_1 \cap N = K = N_G(H_1) \cap N = N_N(K).
\]

This proves (iv) with \( P = H_1 \).

Note that \( H_1 \in \text{Syl}_p(G) \) and that \( H \subseteq H_1 \) but \( H \neq H_1 \). Thus \( [N : H] \equiv [G : H] \equiv 0 \mod p \) (See (5.2) in the preceding section), and so \( [N : H] > 1 \). This proves the first half of (v).

Recall that \( H = H_1 \cap H_2 \). Let \( K_1 = H_1 \cap N \) and \( K_2 = H_2 \cap N \). By (ii), \( K_1, K_2 \in \text{Syl}_p(N) \). By (i), \( K_1 \neq K_2 \). Therefore, \( |\text{Syl}_p(N)| > 1 \). This proves (vi).

Let \( K \in \text{Syl}_p(N) \). By (vi), we can find another \( K' \in \text{Syl}_p(N) - \{K\} \). By (iii), \( H = K \cap K' \). This proves the later half of (v).