Advanced Algebra I

SYLOW THEOREMS

We are now ready to prove Sylow theorems. The first theorem regards the existence of $p$-subgroups in a given group. The second theorem deals with relation between $p$-subgroups. In particular, all Sylow $p$-subgroups are conjugate. The third theorem counts the number of Sylow $p$-subgroups.

**Theorem 0.1** (First Sylow theorem). Let $G$ be a finite group of order $p^nm$ (where $(n, m) = 1$). Then there are subgroups of order $p^i$ for all $0 \leq i \leq n$.

Furthermore, for each subgroup $H_i$ of order $p^i$, there is a subgroup $H_{i+1}$ of order $p^{i+1}$ such that $H_i \triangleleft H_{i+1}$ for $0 \leq i \leq n - 1$.

In particular, there exist a subgroup of order $p^n$, which is maximal possible, called Sylow $p$-subgroup. We recall the useful lemma which will be used frequently.

**Lemma 0.2.** Let $G$ be a finite $p$-group. Then $|S| \equiv |S_0| \pmod{p}$.

proof of the theorem. We will find subgroup of order $p^i$ inductively. By Cauchy’s theorem, there is a subgroup of order $p$. Suppose that $H$ is a subgroup of order $p^i$. Consider the group action that $H$ acts on $S = G/H$ by translation. One show that $xH \in S_0$ if and only if $x \in N_G(H)$. Thus $|S_0| = |N_G(H)/H|$. If $i < n$, then $|S_0| \cong |S| \cong 0 \pmod{p}$.

By Cauchy’s theorem, the group $N_G(H)/H$ contains a subgroup of order $p$. The subgroup is of the form $H_1/H$, hence $|H_1| = p^{i+1}$. Moreover, $H \triangleleft H_1$.

**Example 0.3.** If $G$ is a finite $p$-group of order $p^n$, then one has a series of subgroups $\{e\} = H_0 < H_1 < \ldots < H_n = G$ such that $|H_i| = p^i$ and $H_i \triangleleft H_{i+1}, H_{i+1}/H_i \cong \mathbb{Z}_p$. In particular, $G$ is solvable.

**Definition 0.4.** A subgroup $P$ of $G$ is a Sylow $p$-subgroup if $P$ is a maximal $p$-subgroup of $G$.

If $G$ is finite of order $p^nm$ then a subgroup $P$ is a Sylow $p$-subgroup if and only if $|P| = p^n$ by the proof of the first theorem.

**Theorem 0.5** (Second Sylow theorem). Let $G$ be a finite group of order $p^nm$. If $H$ is a $p$-subgroup of a $G$, and $P$ is any Sylow $p$-subgroup of $G$, then there exists $x \in G$ such that $xHx^{-1} < P$. 

\[\square\]
Proof. Let $S = G/P$ and $H$ acts on $S$ by translation. Thus by the Lemma, one has $|S_0| \equiv |S| = m(\mod p)$. Therefore, $S_0 \neq \emptyset$. One has
\[ xP \in S_0 \iff h xP = xP \quad \forall h \in H \iff x^{-1}hx < P. \]
\[ \square \]

An immediately but important consequence is that two Sylow $p$-subgroups are conjugate.

**Theorem 0.6 (Third Sylow theorem).** Let $G$ be a finite group of order $p^n m$. The number of Sylow $p$-subgroups divides $|G|$ and is of the form $kp + 1$.

**Proof.** Let $S$ be the conjugate class of a Sylow $p$-subgroup $P$ (this is the same as the set of all Sylow $p$-subgroups). We consider the action that $G$ acts on $S$ by conjugation, then the action is transitive. Hence $|S| \mid |G|$.

Furthermore, we consider the action $P \times S \to S$ by conjugation. Then
\[ Q \in S_0 \iff xQx^{-1} = Q \quad \forall x \in P \iff P < N_G(Q). \]

Both $P, Q$ are Sylow $p$-subgroup of $N_G(Q)$ and therefore conjugate in $N_G(Q)$. However, $Q < N_G(Q)$, $Q$ has no conjugate other than itself. Thus one concludes that $P = Q$. In particular, $S_0 = \{P\}$. By the Lemma, one has $|S| = 1 + kp$. \[ \square \]

**Example 0.7.** Group of order 200 must have normal Sylow subgroups. Hence it’s not simple. (let $r_p :=$ number of Sylow $p$-subgroups. Then $r_5 = 1$).

**Example 0.8 (Classification of groups of order $2p \ (p \neq 2)$).** Let $G$ be a group of order $2p$. If it’s abelian, then it’s cyclic by fundamental theorem of abelian groups plus Chinese remainder theorem. Let’s suppose that it’s non-abelian.

There are elements $a, b$ of order $p, 2$ respectively. By Sylow theorem, $r_p = 1$, hence the subgroup $\langle a \rangle$ is normal. Then one notices that $G = \langle a \rangle \langle b \rangle$ for $\langle a \rangle \cap \langle b \rangle = \{e\}$. Moreover, $bab^{-1} = a^k$ for some $k$. One has
\[ a = b^2ab^{-2} = a^{k^2}. \]

It follows that $k = 1, -1$. If $k = 1$, then $G$ is abelian. Thus we assume that $k = -1$. This gives the group $D_p := \langle a, b | a^p = b^2 = e, ab = ba^{-1} \rangle$.

**Proposition 0.9.** If $H, K \triangleleft G$ and $H \cap K = \{e\}, HK = G$, then $G \cong H \oplus K$.

**Proposition 0.10.** Let $G$ be a group of order $pq$, with $p > q$ distinct primes. If $q \mid p - 1$, then $G$ is cyclic. If $q \mid p - 1$ then either $G$ is cyclic or there is a unique model of non-abelian group up to isomorphism.
(Which is a "semi-direct" of two cyclic groups, or called a metacyclic groups in this case)