Math 122 – Lecture 17 Notes

Last Time

- **Cauchy's Theorem:** If G is a finite group and $p \mid |G|$, then G contains an element of order p.
- We proved Cauchy's Theorem for p-groups (commutative case).
- We formulated the **First Sylow Theorem:** If G is finite and $|G| = p^k n$ with $\gcd(p, n) = 1$, then there exists a subgroup $H \leq G$ with $|H| = p^k$. Such a subgroup H is called a **Sylow p-subgroup**.

$\Rightarrow$ Sylow's Theorem generalizes Cauchy's Theorem.

Goal for Today

Our first goal is to prove the **First Sylow Theorem**.

1 Examples

Example 1.1. Let $G = S_3$ and $p = 3$. Then $|H| = 3$ and we can take $H = \langle (1\,2\,3) \rangle$.

Example 1.2. Let $G = S_4$ and $p = 2$. Then $|H| = 8$, and one Sylow 2-subgroup is $H = D_8 \subseteq S_4$.

2 Proof of the First Sylow Theorem

We proceed by strong induction on $|G|$.

Case 1: $p \mid |Z(G)|$

Then $Z(G)$ contains a subgroup of order p by Cauchy's Theorem (since $Z(G)$ is abelian).

Let $N \subseteq Z(G)$ be such a subgroup of order p. Then consider the quotient $\overline{G} = G/N$, which satisfies $|\overline{G}| = p^{k-1} n$.

By the inductive hypothesis, there exists a subgroup $\overline{H} \subseteq \overline{G}$ of order p^{k-1}. Then the preimage $H = \pi^{-1}(\overline{H})$ under the quotient map

$$\pi : G \to \overline{G}$$

is a subgroup of G with

$$|H| = p \cdot |\overline{H}| = p^k.$$

Thus H is a Sylow p-subgroup of G.

Case 2: $p \nmid |Z(G)|$

Write the class equation:

$$|G| = |Z(G)| + \sum_{i=1}^{r} [G : C_G(x_i)],$$

where $x_1, \ldots, x_r$ are representatives of the noncentral conjugacy classes. Since $p \mid |G|$ but $p \nmid |Z(G)|$, there must exist some i such that $p \nmid [G : C_G(x_i)]$. Hence $|C_G(x_i)| = p^k \cdot m$ for some m not divisible by p.

Then $C_G(x_i)$ is a proper subgroup of G (since x_i is noncentral). By induction, there exists $H \leq C_G(x_i)$ with $|H| = p^k$. Thus H is a Sylow p-subgroup of G.

3 Non-uniqueness of Sylow Subgroups

We know that G contains at least one Sylow p-subgroup $H \leq G$, but H is not necessarily unique.

Example 3.1. Let $G = S_4$, $p = 2$. Then one Sylow 2-subgroup is $H = \langle (2\,4), (1\,4)(2\,3) \rangle \cong D_8$. However, another is $H' = \langle (1\,2), (1\,3)(2\,4) \rangle$. These are different Sylow 2-subgroups.

4 Conjugacy of Sylow Subgroups

Claim 4.1. *Any two Sylow p-subgroups of G are conjugate.*

Proof. Continuing the example $G = S_4$, $p = 2$, we can verify that if $g = (1\,3\,4)$, then

$$g(2\,4)g^{-1} = (1\,2), \qquad g(1\,4)(2\,3)g^{-1} = (1\,3)(2\,4),$$

so $gHg^{-1} = H'$.

In general, the **Second Sylow Theorem** states that if $H \leq G$ is a Sylow p-subgroup, then:

(a) If $H' \leq G$ is another Sylow p-subgroup, there exists $g \in G$ such that $H' = gHg^{-1}$.

(b) If $K \leq G$ is any p-subgroup, then $K \subseteq gHg^{-1}$ for some $g \in G$.

□

Proof Idea for (b)

Consider the group action $G \curvearrowright G/H$ given by left multiplication: $g \cdot aH = gaH$. Let $X = G/H$. Then $|X| = |G|/|H| = n$, so $p \nmid |X|$.

Now let $K \leq G$ be a p-subgroup acting on X by left multiplication. We use the following lemma.

Lemma 4.1. *If a p-group K acts on a finite set X and $p \nmid |X|$, then there exists $x \in X$ fixed by all elements of K; i.e., $K_x = K$.*

Proof. By the orbit–stabilizer theorem,

$$|X| = \sum_i [K : K_{x_i}],$$

where the sum is taken over orbit representatives x_i. If $p \nmid |X|$, then at least one term must also not be divisible by p, so $[K : K_{x_i}] = 1$, meaning $K_{x_i} = K$. Thus $x = x_i$ is fixed by K. □

Hence, there exists $x = gH \in X$ such that $K \subseteq gHg^{-1}$. This proves part (b) of the Second Sylow Theorem.

5 Consequences and the Third Sylow Theorem

Theorem 5.1 (Third Sylow Theorem)**.** *Let $|G| = p^k n$ with $\gcd(p, n) = 1$, and let S be the number of Sylow p-subgroups of G. Then:*

$$S \mid n \quad \textit{and} \quad S \equiv 1 \pmod{p}.$$

Example 5.1. If $G = S_3$ and $p = 3$, then there is only one Sylow 3-subgroup, $\langle (1\,2\,3) \rangle$, so $S = 1$.

If $G = S_4$ and $p = 2$, then there are $S = 3$ Sylow 2-subgroups, and indeed $3 \equiv 1 \pmod{2}$.

Sketch of Proof. Let X be the set of all Sylow p-subgroups of G, and let G act on X by conjugation: $g \cdot H = gHg^{-1}$. This action is transitive by the Second Sylow Theorem.

Fix $H \in X$. Then the stabilizer of H in this action is

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

the normalizer of H in G. By the orbit–stabilizer theorem,

$$|X| = [G : G_H] = \frac{|G|}{|N_G(H)|}.$$

Since $H \subseteq N_G(H)$ and $|H| = p^k$, we can write

$$|N_G(H)| = p^k m',$$

where $m' \mid n$. Thus $|X| = n/m'$, so $S = |X| \mid n$.

To see that $S \equiv 1 \pmod{p}$, consider the restriction of the conjugation action to H itself. Then H fixes itself under conjugation, and by a counting argument (using the class equation for the action), the number of fixed points is congruent to $1 \pmod{p}$. Hence $S \equiv 1 \pmod{p}$. □

Summary

- Every finite group G of order $p^k n$ (with $\gcd(p, n) = 1$) has a Sylow p-subgroup.
- All Sylow p-subgroups are conjugate.
- The number S_p of Sylow p-subgroups divides n and satisfies $S_p \equiv 1 \pmod{p}$.