Spring 2018/MA 434 **Group Project 4: The Sylow Theorems**

1. Introduction

Let G be a finite group of order $n = |G|$.

(1) Give an example of a group G, and a number a which divides n, such that G does not have any elements of order a.

The Sylow (pronounced SEE-low) theorems concern the case when a is a power of a prime. Henceforth, assume that p is a prime and that $n = p^r m$ where p does not divide m. A group whose order is a non-zero power of a prime p is a p**-group**.

Theorem (First Sylow Theorem)**.** *G has a subgroup of order p^r.*

A subgroup of order p^r is called a **Sylow subgroup** of G. Another way of phrasing this is that a subgroup $H < G$ is a Sylow subgroup if and only if $|H|$ is a non-zero power of a prime and $|G|/|H|$ is not divisible by that prime. Notice that any subgroup conjugate to a Sylow subgroup is a Sylow subgroup.

The second Sylow theorem relates the Sylow subgroups of G to Sylow subgroups of its subgroups.

Theorem (Second Sylow Theorem)**.** *Suppose that $K < G$ is a subgroup such that p divides $|K|$. Then there exists $g \in G$ such that $K \cap (gHg^{-1})$ is a Sylow subgroup of K.*

How many different Sylow subgroups are there?

Theorem (Third Sylow Theorem)**.** *Let s denote the number of Sylow p-subgroups of G. Then s divides m and s is congruent to 1 modulo p.*

2. The proof of the First Sylow Theorem

We need the following lemma.

Lemma 2.1. Let $G \curvearrowright G$ by left multiplication and let $U \subset G$. Let $\mathrm{stab}(U)$ be the subgroup of G consisting of all $g \in G$ such that $gu \in U$ if and only if $u \in U$. Then $|\mathrm{stab}(U)|$ divides $|U|$.

Our proof is based on Prop. 3.6 from Artin's *Algebra.*

Proof. Observe that $\mathrm{stab}(U) \curvearrowright U$ by left multiplication. Thus, U is the union of orbits under this group action. For $u \in U$, let $\mathrm{orb}(u)$ denote the orbit of U under the action by $\mathrm{stab}(U)$. Thus, there exists elements $u_1, \ldots, u_k$ with disjoint orbits, so that $U = \bigcup_{i=1}^{k} \mathrm{orb}(u_i)$. In particular,

$$|U| = |\mathrm{orb}(u_1)| + \cdots + |\mathrm{orb}(u_k)|.$$

For $i \in \{1, \ldots, k\}$, observe

$$\mathrm{orb}(u_i) = \{u \in U : \exists h \in \mathrm{stab}(U) \text{ s.t. } hu_i = u.\}$$

But this is exactly the definition of the *right* coset of $\mathrm{stab}(U)$ by the element $u_i \in U$. That is,

$$\mathrm{orb}(u_i) = (\mathrm{stab}(U))u_i.$$

Standard facts say that all cosets of stab(U) in G have the same number of elements as stab(U). Consequently,

$$|\operatorname{orb}(u_i)| = |\operatorname{stab}(U)|.$$

Thus, $|U|$ is a multiple of $|\operatorname{stab}(U)|$. □

(1) Prove that if G acts on a set S, then G also acts on the power set $\mathscr{P}(S)$. Furthermore, prove that G acts on the set $\mathscr{S}$ of all subsets of S of cardinality p^r. In what follows, we'll take $G = S$ and the group action to be left multiplication.

(2) Let $N = \binom{n}{p^r}$. This is the cardinality of $\mathscr{S}$. Prove that N is not divisible by p.

(3) Prove that there is an orbit for the action of G on $\mathscr{S}$ whose cardinality is not divisible by p. Let $U \in \mathscr{S}$ be an element of the orbit.

(4) Prove that stab(U) has order p^r. This concludes the proof of the theorem, as stabilizers are subgroups.

3. The proof of the Second Sylow Theorem

Let $H < G$ be a Sylow p-subgroup of G. We must show the intersection of some conjugate of H with the subgroup K is a Sylow p-subgroup of K.

(1) Let $S = G/H$ (the set of left cosets of H in G). Prove that the action of G on itself by left multiplication induces an action of G on S.

(2) Prove that G acts transitively on S. (That is, for every $gH, g'H \in S$, there exists $a \in G$ such that $a(gH) = g'H$.)

(3) Recall that $H \in S$. Prove that $H = \operatorname{stab}(H)$.

(4) For $g \in G$, prove that the $\operatorname{stab}(gH) = gHg^{-1}$.

(5) Explain why p and the cardinality of S are relatively prime.

(6) Consider the action of K on S which is the restriction of the action of G on S. Let $\mathscr{O}$ be the set of orbits produced by this action. Prove that there exists $O \in \mathscr{O}$ such that the order of O is relatively prime to p.

(7) Let $o \in O$. Prove that stab(o) is the subgroup we are looking for.

4. The proof of the Third Sylow Theorem

(1) Use the second Sylow theorem to prove that the Sylow p-subgroups of G are all conjugate.

(2) Let H be a Sylow p-subgroup and let $N(H)$ be its normalizer. That is,

$$N(H) = \{g \in G : gHg^{-1} = H\}.$$

Recall that $N(H)$ is a subgroup of G. Prove that s (the number of Sylow p-subgroups of G) is equal to $[G : N(H)]$.

(3) Prove that s divides $m = [G : H]$.

(4) Let $\mathscr{U} = \{H_1, H_2, \dots, H_s\}$ be the set of Sylow p-subgroups of H. Let N_i be the normalizer of H_i. Let H act on U by conjugation. Prove that $|\operatorname{orb}(H_i)| = 1$ if and only if $H < N_i$.

(5) Prove that if $|\mathrm{orb}(H_i)| = 1$, then H_i is normal in N_i. Conclude (using (1)) that $H = H_i$.

(6) Show that if $|\mathrm{orb}(H_i)| \neq 1$, then $|\mathrm{orb}(H_i)|$ is divisible by p.

(7) Prove that s is congruent to 1 mod p.

5. Some relatively easy applications

(1) Prove that if G is a finite group with order divisible by p, then G has an element of order p. (Use Sylow 1.)

(2) Prove that there are exactly two isomorphism classes of groups of order 6. (Use Sylow 1)

(3) Prove that every group of order 15 is cyclic. (Use Sylow 3.) (Hint: Show that if $|G| = 15$, then $G \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.)

(This project is based on material from Michael Artin's *Algebra*.)