Chapter 1

An Introduction to The Sylow Theorems

Final Project Paper for Abstract Algebra I by Nathan Holt

1.1 Introduction

Last year, I read an article on the internet entitled something along the lines of "10 Most Important Mathematics Theorems." Many of these I had come across in my previous schoolwork, such as The Fundamental Theorem of Calculus, The Binomial Theorem, and Dirichlet's Theorem. There were two theorems that I had never heard of that were labeled under the "Group Theory" section: Lagrange's Theorem, and the Sylow Theorems. I read the brief description attached to them, and having no experience with group theory yet, didn't understand a word of it. In our Algebra class, we discussed Lagrange's Theorem, and even kind of used the result from the beginning of class without knowing it had a name or how to prove it. But we never touched on the Sylow Theorems. Since I'm a student that got accepted into the master's program for math, and plans on continuing my studies in Abstract Algebra, I thought it might be good to take this opportunity to learn the Sylow Theorems.

In this paper I will describe the Sylow Theorems precisely, state the results and consequences of the theorems, and then attempt some practice problems.

1.2 Preliminary Definitions

It's important to make clear the terminology I plan on using in this paper. (I'm also putting this section here for my own benefit; this vocabulary wasn't used in class).

Definition 1.2.1. Given a group G such that $|G| = p^k m$, then $H \leq G$ is a Sylow p-subgroup of G given that $|H| = p^k$. It's worth noting that this is

maximal in the sense that it has an order of the highest prime power of p.

Definition 1.2.2. The multiplicity of a prime factor is the exponent it is raised to in the prime factorization decomposition. For example: $60 = 2^2 \times 3 \times 5$, so the multiplicity of 2 is 2, whereas the multiplicity of 3 and 5 are 1.

Definition 1.2.3. Given a group G with subgroups H and K, H and K are conjugate to each other if there exists and element $g \in G$ such that $gHg^{-1} = K$.

1.3 The Sylow Theorems for Finite Groups

The Sylow Theorems are actually three main theorems, so I will state each of them here.

Theorem 1. For every prime factor p of $|G|$ with multiplicity n, there exists a Sylow p-subgroup of G, which has order p^n

Theorem 2. Given a finite group G and a prime number p, all Sylow p-subgroups of G are conjugate to each other.

Theorem 3. Let p be a prime factor of $|G|$ with multiplicity n, so the order of G can be expressed as $p^n m$, where $n > 0$ and n does not divide m. Then the total number of Sylow p-subgroups of G is congruent to 1 (mod 4) and also divides m.

I won't attempt to prove these, as the proofs are readily available online. Instead, I will take them as fact and apply them.

1.4 Consequences of the Theorems

The first apparent consequence is that a subgroup H of G that has order p^n, is a Sylow p-subgroup of G. This is simply writing the first theorem in the opposite direction. You are given a subgroup H, and can find a group G that will satisfy it being a Sylow p-subgroup.

The second consequence is less obvious. If the number of Sylow p-subgroups is 1, then the p-subgroup must be normal.

Proof. Let G be a group with a subgroup H that has a unique order - no other subgroups of G have the same order.

Now let $g \in G$. From class, we know that if $H \leq G$, then $gHg^{-1} \leq G$. Furthermore, we know that $|gHg^{-1}| = |H|$. However, we stated that H was the only subgroup of G with this order. This means that $H = gHg^{-1}$. This implies that H must be normal.

Applying this lemma to our Sylow p-subgroup, since there is only one subgroup with order p^n, it must be normal. □

1.5 All Groups of Order 15 Are Cyclic

A cool application of the Sylow Theorems is to show that groups of certain orders must be cyclic, or have a certain number of subgroups of a given order. Let's work out an example.

Proof. Let G be an arbitrary group of order 15. The prime factorization of this is: $|G| = 3 \times 5$. By the first Sylow Theorem, we are guaranteed the existence of a Sylow 3-subgroup and a Sylow 5-subgroup.

From the third Sylow Theorem, we know that the number of Sylow 3-subgroups is congruent to 1 (mod 3), and also divides 15. The only value that satisfies this is 1. This means that there is only one Sylow 3-sugroup of G. A similar argument is applied towards the number of Sylow $5-subgroups$. We know that it is congruent to 1 (mod 5), and also divides 15. The only value satisfying this is 1. Thus, there is only one Sylow 5-subgroup.

From the "Consequences of the Theorems" section, we know that any subgroup of order 3 or 5 is a Sylow 3-subgroup or Sylow 5-subgroup respectively. (Any subgroup of order 3 or 5 is account for already in the number of $3-subgroups$ and $5-subgroups$).

So we know that G has one subgroup of order 3, and one subgroup of order 5. Furthermore, we know based on the definition, that both of these subgroups must be normal. From a theorem we learned in class, since the intersection of these two subgroups must be trivial ($H \cap K = \{e\}$), we know that $G = H \times K$.

This means that G is the direct product of the groups H and K, meaning that it is the cyclic group of order 15. This proves that the only group of order 15 is the cyclic group of order 15 (or isomorphic to it). □

1.6 Wilson's Theorem

Last semester I took Number Theory. In that class, we proved Wilson's Theorem using a bunch of things we'd learned up to that point, including Fermat's Little Theorem, modular arithmetic, and polynomial manipulations. To be honest, it always felt very clunky and not at all beautiful. But, I see that the Sylow Theorems offer a simple, elegant way to prove Wilson's Theorem.

Wilson's Theorem states that a number p is prime if and only if the following holds:

$$(p-1)! \equiv -1 \pmod{p}$$

Now let's prove this using the Sylow Theorems.

Proof. Let p be a prime number. Now consider the symmetric group S_p, which has $(p-1)!$ elements of order p: the p-cycles. Since each of the Sylow p-subgroups contains $p-1$ p-cycles, it is apparent that there are $(p-2)!$ Sylow p-subgroups total. From here we will apply the third of the Sylow Theorems:

$$(p-1)! \equiv -(p-2)! \equiv -1 \pmod{p}$$

□

This is a much simpler proof, and I'm confident I could recreate this proof for a test if asked (unlike the old proof I learned).

1.7 Practice Problems

Problem: Show that there is no simple group of order 200.

Proof. The prime factorization of $200 = 2^3 \times 5^2$. Thus, we can conclude that the number of Sylow 5-subgroups is congruent to 1 mod 5 and a divisor of 8 by the third Sylow Theorem. The only solution to this is 1, so there is only one Sylow 5-subgroup. This is a nontrivial normal subgroup since it's the only 5-subgroup (previously discussed in paper). This means that the group of order 200 is not simple. □

Problem: Find a 2-Sylow subgroup and a 3-Sylow subgroup of S_4.

Proof. S_4 has an order of $4! = 24 = 3 \times 2^3$. Thus, we know that a Sylow 2-subgroup will have an order of 2^3, and a Sylow 3-subgroup will have an order of 3. So, let us consider the following subgroups: G generated by (1234) and (13) and H generated by (123). G has an order of 8, and is thus a Sylow 2-subgroup. H has an order of 3, and is thus a Sylow 3-subgroup. □

1.8 Conclusion

I understand why the Sylow Theorems are a big deal - they give us a way to better classify subgroups, and thus the groups themselves, allowing us to make conclusions about the kinds of subgroups a group has. It also helped illustrate Wilson's Theorem in a simple proof - which I wouldn't have guessed had anything to do with group theory, since I associated it with a bunch of messy proofs (and the number theory at RIT is taught without any number theory, although we do discuss certain groups such as Z_n and U_n).

I feel relatively competent with understanding and applying the Sylow Theorems now, although all of the practice problems seemed very repetitive. There are probably more advanced applications of the Sylow Theorems that I hadn't uncovered. But maybe we'll discuss that in Algebra II.