23 Proofs and Applications of the Sylow Theorems

23.1 Review

Last time, we introduced the Sylow theorems. While they may be a lot to take in, the main takeaway is how general the Sylow theorems are. When provided with **any** finite group, we automatically already know that there exist certain p-subgroups[79] that must be conjugate, and additionally there is a strong constraint on the possible number of such subgroups.

The applications for C_{15} and C_{10} discussed last lecture demonstrate how powerful these theorems can be.

We restate the theorems briefly here:

Theorem 23.1 (Sylow Theorems)
Let G be a finite group where

$$|G| = n = p^e m$$

and $\gcd(p, m) = 1$. The three parts of the theorem follow:

1. Recall that a Sylow p-subgroup is a subgroup $H \leq G$ such that $|H| = p^e$. The first theorem states that there always exists a Sylow p-subgroup.
2. Given any $K \leq G$ where $|K| = p^f$, there exists some $g \in G$ such that $gKg^{-1} \leq H$.
3. The number of Sylow p-subgroups is a factor of m and congruent to 1 mod p.

23.2 Application: Decomposition of Finite Abelian Groups

One application of the Sylow theorems is the decomposition of finite abelian groups.

Consider a finite *abelian* group G such that the prime factorization of the order is

$$|G| = p_1^{e_1} \cdots p_r^{e_r}.$$

Then we know that we have a Sylow subgroup H_i such that

$$|H_i| = p_i^{e_i}$$

for each of these primes. Since G is abelian, conjugating a group produces the same group, so by Sylow II, these (abelian) subgroups H_i are **unique** for each prime.

Theorem 23.2
Every abelian group G is isomorphic to a product of groups of prime power order.

Using that G is abelian, if we take the product

$$H_1 \times \cdots \times H_r,$$

we can construct a homomorphism[80]

$$\begin{aligned} f : H_1 \times \cdots \times H_r &\longrightarrow G \\ (x_1, \ldots, x_r) &\longmapsto x_1 + \cdots + x_r. \end{aligned}$$

Lemma 23.3
The homomorphism f is an isomorphism.

[79] The size is the largest power of p that divides $|G|$

[80] Because G is abelian, we use $+$ as the group operation.

Proof. First, f is a homomorphism because G is abelian and the terms will commute when verifying the homomorphism property. It is necessary that G is abelian. [81] Next, we know that $\mathrm{im}(f)$ is a subgroup of G and also contains a copy of H_i for all i[82]:

$$H_i \leq \mathrm{im}(f) \leq G$$

for all i. Thus, $p_i^{e_i}$ divides $|\mathrm{im}(f)|$ for each i, and since they are relatively prime, the product

$$\prod p_i^{e_i}$$

divides $|\mathrm{im}(f)|$. This forces the image to be the same order as $|G|$, and thus they must be the same. We can conclude that f is surjective. Both the domain and image of f have the same size, so it is also injective and an isomorphism. □

As a result, the study of finite abelian groups can be reduced to studying abelian p-groups. These are completely understood, and will potentially be covered more in 18.702! In contrast, non-abelian groups are complicated and not well understood.

23.3 Proof of Sylow Theorems

The main idea to prove all of these theorems is to find a useful action of G on a set and exploit it. This is a continuation of what we have been doing in the last few weeks, in geometric situations with symmetries as well as with the conjugation action of G on itself. The striking part about these three proofs is that unlike rotational symmetries of the cube, where there are lots of sets to think about, such as vertices and faces and so on, here, there is no prior knowledge about G, and the only group action we have for any arbitrary group is G acting on itself, and not much else.

Theorem 23.4 (Sylow I)
Given G such that

$$|G| = n = p^e \cdot m,$$

where p^e is the largest power of p (that is, $\gcd(p, m) = 1$), then there exists a subgroup $H \leq G$ such that

$$|H| = p^e.$$

Proof of Sylow I. Take G such that

$$|G| = p^e \cdot m.$$

Let S be the subsets of G of size p^e and let n be the order of G. By basic combinatorics, there are $\binom{n}{p^e}$ such subsets, so

$$|S| = \binom{n}{p^e}.$$

Let G act on S by left translations: given an element $g \in G$ and a subset $U \in S$, we map

$$U \longmapsto gU.$$

Our eventual goal is to find a subgroup of G of size p^e by looking at stabilizers, as they are always subgroups of G. We find the size of a stabilizer by trying to find an orbit of size m, as we then know that the stabilizer will be order p^e.[83] We begin with some lemmas. The first lemma provides information about the size of the set modulo p.

[81] Essentially, since G is abelian, there is really only one way to "combine" the Sylow p-subgroups. When $|G| = 10$ for a non-abelian group, we saw that the Sylow subgroups for 2 and 5 could combine in a different way to make D_{10}.

[82] Take $H_1 \times \{1\} \times \cdots \{1\}$ to get $H_1 \leq \mathrm{im}(f)$, for example.

[83] The product of the size of an orbit and the size of the stabilizer is the size of the group G, which here is $m \cdot p^e$.

Lemma 23.5

Where $n = |G| = m \cdot p^e$, we have that

$$|S| = \binom{n}{p^e} \neq 0 \pmod{p}.$$

Furthermore,

$$\binom{n}{p^e} \equiv m \pmod{p}.$$

Sketch of Proof. The proof is not particularly relevant to group theory and can be proved by expanding the binomial coefficient and showing that the number of powers of p in the numerator is the same as the denominator. Alternatively, one could expand $(1+x)^n$ and look at it modulo p. □

To reiterate, S consists of **all** subsets of G of size p^e, and these subsets do not have to be subgroups.

Lemma 23.6

Suppose we have a subset $U \in S$[a], which is a subset of G. Also, let H be a subgroup of G that stabilizes U. Then, $|H|$ divides $|U|$.

[a] Note that U is an element of S but is itself also a subset of G, so $U \subset G$.

Proof. Since H stabilizes U, for any $h \in H$, we know $hU = U$. In other words, for each $u \in U$, we have

$$Hu \subset U.$$

Equivalently, for each $u \in U$, the corresponding right coset of H is a subset of U. This implies that the right cosets partition U. Since the cosets have the same size, we know that $|H|$ divides $|U|$. □

With these lemmas in hand, we can continue with the proof of the main theorem. The first lemma tells us that $|S| \neq 0 \pmod{p}$. We know that the orbits partition S, so

$$|S| = |O_1| + \cdots + |O_r|.$$

Since p does not divide the LHS, there must exist an orbit θ where

$$\gcd(p, |\theta|) = 1.$$

Let the size of θ be $|\theta| = k$.

Now, consider some element u of θ. By the counting formula, we also know that

$$|G| = |\theta| \cdot |\mathrm{Stab}(u)|.$$

And so $p^e m = k|\mathrm{Stab}(u)|$ and $p^e \mid |\mathrm{Stab}(u)|$ because $\gcd(k, p) = 1$. By the second lemma, $|\mathrm{Stab}(u)|$ divides $|u| = p^e$.

Thus,

$$|\mathrm{Stab}(u)| = p^e$$

and we have found a Sylow p-group. □

The proof of the second Sylow theorem is similar.

Theorem 23.7 (Sylow II)
There are two parts; part a) is what is usually referred to as the second Sylow theorem.

(a) Given $H \leq G$, where H is a Sylow p-subgroup, any other Sylow $p-$subgroup $H' \leq G$ is conjugate to H; i.e. there exists g such that $H' = gHg^{-1}$.

(b) Given any subgroup $K \leq G$ such that $|K| = p^d$, for any Sylow subgroup H, there exists g such that $gKg^{-1} \leq H$.[a]

[a] Notice that $|K|$ does not have to be the maximal prime power, and can have order smaller than $|H|$. **Every** prime power order subgroup, up to conjugation, sits inside a Sylow subgroup.

Proof of Sylow II. We approach this proof similarly, finding a nice set and an action on it. Fix H to be a Sylow subgroup. Our set is $X = G/H$, the left cosets of H. The index of H is the same as $|X|$, so $|X| = m$.

Let K be the subgroup we want to show is a subgroup of H up to conjugation, where $|K| = p^f$. We will look at how K acts on X by left translation, the mapping:

$$k(aH) \longmapsto kaH.$$

We decompose into orbits, $|X| = |O_1| + \cdots + |O_r|$. Note that these orbits are with respect to the action of K, not the action of G, as that would be transitive and we'd only have one orbit. We have that $|O_i|$ divides $|K| = p^f$, but p does not divide m. Thus this orbit decomposition can only work if some orbit O has size 1. In other words, there exists some coset aH that is fixed by all $k \in K$. Then,

$$\begin{aligned} kaH &= aH \\ a^{-1}kaH &= H \\ a^{-1}ka &\in H \\ a^{-1}Ka &\leq H \end{aligned}$$

which is what we needed to show. □

A lot of the work done in these proofs are choosing some set and action, then looking at the orbits and seeing what we can do what them. The third proof is similar.

Theorem 23.8 (Sylow III)
The number of Sylow p-subgroups of G divides

$$m = \frac{n}{p^e}$$

and is congruent to 1 modulo p.

Proof of Sylow III. Our set will be Y as the set of Sylow p-subgroups of G. We will be trying to find the size of Y. G acts on Y by conjugation, $H \longmapsto gHg^{-1}$. By Sylow II, there is only one orbit. Pick a Sylow subgroup $H \in Y$. Then

$$|G| = |\text{Stab}(Y)||\text{orbit}(H)| = |Y||\text{Stab}(Y)|.$$

This already tells us that $|Y|$ divides $|G| = n$, but we can say more.

The stabilizer here has a name, the *normalizer* of H. It turns out that $H \leq \text{Stab}(H)$ because for all $h \in H$, $hHh^{-1} = H$. So $|\text{Stab}(H)|$ is divisible by $p^e = |H|$. The counting formula then says that $|G| = p^e m = |Y| \cdot (p^e \cdot \text{stuff})$ which implies that $|Y|$ divides m.

The last part is showing that $|Y| \equiv 1 \pmod{p}$. We now use the action of H on Y by conjugation.

Fact 23.9
Suppose we have another Sylow subgroup $H' \in Y$, H' is fixed by H if and only if $H = H'$. In other words, under the action of H, there is only one fixed point.

By looking at orbits, there is only one orbit of size 1 because there is only one fixed point. The rest are powers of p because the size of H is a power of p. Thus the decomposition into orbits looks like

$$Y = 1 + p + \cdots + p^2 + \cdots + p^3 + \cdots \equiv 1 \pmod{p}.$$

Proof of fact. If we look at the stabilizer/normalizer, $\mathrm{Stab}_G(H') = N(H')$, we know that $H \le N(H')$ because H' is fixed by H, and that $H' \le N(H')$ by what we said above about normalizers.

Now $N(H')$ is a subgroup of G as well, so the largest power of p that divides $N(H')$ can only be p^e. So H and H' are Sylow subgroups of $N(H')$ as well. By Sylow II on $N(H')$, there exists $n \in N(H')$ such that $nH'n^{-1} = H$. But then by the definition of N, $nH'n^{-1} = H'$, and so $H = H'$. □

Given this fact, we are done with the third proof. □