Lecture 20: More counting, First Sylow Theorem

Chit-chat 20.1. Last time, we saw that the orbit-stabilizer theorem answered some non-trivial questions for us: How big is the symmetry group of the tetrahedron?—for instance. Recall that the theorem says that for any group acting on a set X, and for any $x \in$X, there is a bijection $G\ G_x \cong \mathcal{O}_x$. In particular, if the group G is finite, we have

$$|\mathcal{O}_x| = |G|/|G_x|.$$

These kinds of counting theorems are great in math. They're like "lay-ups" in basketball; they're the easiest shots you can take. Once you reduce a hard problem to just counting, you're in business.

In the proof of Lagrange's Theorem, we used the reasoning that any set is a union of its orbits. Hence given a group action of G on a finite set X, we can conclude

$$|X| = \sum_{\text{orbits}} |\mathcal{O}_x|.$$

Let's use this observation some more. The above equation is called the *counting formula*.

Definition 20.2. Let p be a prime number. A finite group G is called a *p-group* if

$$|G| = p^n$$

for some integer $n \geq 1$. I.e., if its order is a power of p.

Definition 20.3. Let G act on a set X. $x \in X$ is called a *fixed point* of the group action if $gx = x$ for all $g \in G$.

Proposition 20.4. Fix a p-group G. Fix a finite set X whose order is not divisible by p. Then any action of G on X must have at least one fixed point.

Example 20.5. So if someone claims to you that they have a p-group acting on the tetrahedron, you can look at the induced action of G on the set of vertices of the tetrahedron. If p is anything other than 2, you know that this group action fixes at least one vertex.

PROOF. By the orbit-stabilizer theorem, any orbit $\mathcal{O}_x$ has order dividing the order of the group G. Hence we have that $|\mathcal{O}_x|$ has to equal p^k for some $k \geq 0$. Note that we must prove that $|\mathcal{O}_x| = p^0 = 1$ for some $x \in X$ to exhibit a fixed point.

Such an x must exist—otherwise, each $\mathcal{O}_x$ is equal to p^k for $k \geq 1$, hence each $\mathcal{O}_x$ is divisible by p. Then the righthand side of the counting formula

$$|X| = \sum_{\text{orbits}} \mathcal{O}_x$$

is divisible by p. But by assumption, $|X|$ cannot be divisible by p. Hence $\mathcal{O}_x$ must be 1. $\square$

Here's anotherr application:

Proposition 20.6. Let G be a p-group. Then G has non-trivial center (i.e., its center must contain more than just the identity element).

Chit-chat 20.7. Throughout, we let Z stand for the center of G.

PROOF. Consider the conjugation action of G on itself. The orbits of this action are precisely the conjugacy classes of G. Hence the counting formula reads

$$|G| = \sum_{\text{conjugacy classes}} |[x]|$$

where $[x]$ is the conjugacy class of x—it is the set of all elements of the form gxg^{-1} for some $g \in G$. At this point, I asked the class to prove the rest of the theorem as an exercise. I gave a hint: When does $|[x]| = 1$?

The answer to the hint is that $|[x]| = 1$ if and only if x is in the center of G. For if the only element in $\mathcal{O}_x$ is x itself, this means $gxg^{-1} = x$ for all $g \in G$—this of course implies that $gx = xg$.

Finally, we know that $1_G \in G$ is always in the center of G, so the counting formula reads

$$|G| = 1 + \sum_{\text{conjugacy classes} \neq [1_G]} |[x]|.$$

If $|[x]| \geq 2$ for all $x \neq 1_G$, then the righthand side is not divisible by p—for it would be a summation of the form

$$1 + \sum_{\text{various } k \geq 1} p^k.$$

This is a contradiction since $|G|$ is only divisible by p. Hence there must be some $x \neq 1_G$ for which $|[x]| = 1$; that is, there must be some $x \neq 1_G$ in the center. $\square$

This has a great corollary.

Corollary 20.8. Any group of order p^2 is abelian.

Chit-chat 20.9. This is highly non-trivial. For instance, imagine proving by hand that a group of order 49 must be abelian.

Chit-chat 20.10. We knew that every group of order p is abelian, since it must be cyclic. This is the next power up.

Proof. The center of G is a subgroup, so by Lagrange's Theorem, we must have $|Z| = 1, p$, or p^2 since these are the only divisors of p^2.

On the other hand, the proposition tells us that $|Z| \neq 1$, so it must be p or p^2.

Assume $|Z| = p$. We will yield a contradiction. For fixing $x \in G, \notin Z$, let us examine the stabilizer of x under the conjugation action of G. This, we called the centralizer of x last time, and we denote it $Z(x)$. It is the set of all $y \in G$ for which $xy = yx$.

Since the stabilizer of a group action is always a subgroup, by Lagrange's theorem, we know that $|Z(x)|$ must divide p^2. On the other hand, $Z \subset Z(x)$ since any element of the center (by definition) commutes with x. Moreover, $x \in Z(x)$ since x commutes with itself. This proves that $|Z| <_{\neq} |Z(x)|$, so $|Z(x)|$ must be a number bigger than p dividing p^2. We conclude $|Z(x)| = p^2$.

But this means every element of G commutes with x. Hence x must be in the center. $\square$

Chit-chat 20.11. So this strategy of just "counting" has paid off great dividends. Let's milk it for all we've got. One beautiful outcome of all this milking is *Sylow's theorems*. We'll state just the first one today.

Let p divide $|G|$. We write

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

where p^e is the largest power of p dividing $|G|$. In particular, $gcd(m, p) = 1$.

Definition 20.12. Then a *Sylow p-subgroup*, or *p-Sylow subgroup*), is a subgroup $H \subset G$ such that $|H| = p^e$. In other words, it is a subgroup is the biggest subgroup with size a power of p.

Chit-chat 20.13. So if there are many different primes p that divide $|G|$, we can try to look for a Sylow p-subgroup for each of these p. As of this comment, we have no idea if there even existence, nor how many there may be inside of G.

Example 20.14. Let $G = S_3$. Then since $6 = 3 \cdot 2$, a Sylow 3-subgroup is a subgroup of order 3 inside G. THhre is a unique one, given by $H =$

$\{\mathrm{id}, (123), (132)\}$. There are three Sylow 2-subgroups: $\{id, (12)\}, \{\mathrm{id}, (13), \}, \{\mathrm{id}, (23)\}$.

Theorem 20.15. Let p divide $|G|$. Then there exists a Sylow p-subgroup of G.

Corollary 20.16. Let p divide $|G|$. Then there exists an element $x \in G$ of order p.

Chit-chat 20.17. You may not have considered this corollary before. By Lagrange, we know that any element $x \in G$ must divide the order of $|G|$. But given a number dividing $|G|$, is it obvious that there should (or shouldn't) be an element of a specified order p for a prime dividing G?

PROOF. Since p divides G, $|H| \geq 2$. So we can choose an element $x \in H$ such that $x \neq 1_G$. Moreover, the order of x must divide $|H|$ by Lagrange's theorem. Thus

$$x^{p^k} = 1_G$$

for some $k \geq 1$. Just let $y = x^{p^{k-1}}$. Then $y^p = 1_G$. $\square$

Next time, we'll state the other Sylow Theorems, and prove a few things.