22 The Sylow Theorems

22.1 Review

Last time, we discussed the conjugacy classes of symmetric and alternating groups.

22.2 Motivation

The Sylow theorems are a set of related theorems describing the subgroups of prime power order of a given finite group. They are very powerful, since they can apply to any finite group, and play an important role in the theory of finite groups.

To motivate the Sylow theorems, recall the following basic theorem.

Theorem 22.1
If G is finite, and H is a subgroup of G, then $|H|$ divides $|G|$.

In fact, we can ask if the reverse is also true: given a factor of $|G|$, is there a subgroup of that size? It turns out that it it **not** true.

Example 22.2 (Counterexample)
For $G = A_4$, $|G| = 12$, but it turns out that there is no subgroup of order 6.[a]

[a] As an exercise, try showing this using the class equation!

So there is not always such a subgroup.

Guiding Question
Can we add constraints so that some form of reverse of Theorem 22.1 is true? When must there be a subgroup of a particular size?

The next theorem is quite surprising and powerful: it turns out that the reverse is true for prime powers. If $d = p^k$, a prime power dividing $|G|$, then there must exist a subgroup where $|H| = p^k$.

22.3 The First Sylow Theorem

The three Sylow theorems, which will be stated in this lecture and proved in the next, formalize and elaborate on this idea of studying subgroups of prime power order.

Note 22.3
For today's lecture, we use e to denote the largest exponent of p such that $p^e \mid |G|$ and we use 1 to denote the identity element instead. Also, n will always refer to $|G|$.

The first Sylow theorem states that there is always a prime power order subgroup.

Theorem 22.4 (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

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

Such a subgroup is called a **Sylow p-subgroup**. It has maximal prime power order within G.

Definition 22.5
Let G be a group such that $|G| = n = p^e m$ such that $\gcd(p, m) = 1$. Then a subgroup $H \leq G$ such that $|G| = p^e$ is called a **Sylow $p-$subgroup**.

Let's see an application of this powerful theorem.

Example 22.6
Consider $G = S_4$. Since $|S_4| = 24 = 8 \cdot 3$, Sylow I states that there is a subgroup of order 8. In fact, we can take

$$H = \langle (12), (34), (13)(24) \rangle.$$

Another example is the dihedral group.

Example 22.7
For $G = D_5$, we have $|D_5| = 10 = 2 \cdot 5$. So there must be subgroups of size 5 and 2. A subgroup generated by a rotation

$$\langle \rho_{2\pi/5} \rangle \text{ has order 5.}$$

A subgroup generated by any reflection

$$\langle \text{reflection} \rangle \text{ has order 2.}$$

Looking at this theorem now, it may be hard to appreciate. One reason this theorem is relevant now is that the proof is a very nice application of the theory on group actions and orbits. Moreover, this theorem is one that applies extremely generally. We have mostly been studying explicit groups such as the dihedral groups or symmetric groups in this class, but the Sylow theorems apply to **any** finite group. When given an unfamiliar group, the Sylow theorems provide footholds and crevices, like in climbing a cliff, to start off with and to learn more about the groups. Sylow I gives lots of interesting subgroups that play off of each other, depending on the different factors of the size of the group G.

We can get a useful corollary for free.

Corollary 22.8
If p divides $|G|$, there exists an element $x \in G$ with order p.

For example, if $|G| = 14$, it must have at least one element of order 7.

Proof of Corollary 22.8. Using Sylow I, there exists a subgroup $H \leq G$ such that $|H| = p^e$, where $e \geq 1$. Pick some $y \in H$. Then,

$$\langle y \rangle = C_{p^f},$$

some cyclic group with order dividing p^e. Taking

$$x = y^{p^{k-1}}$$

provides an element of order p. □

22.4 The Second Sylow Theorem

The first Sylow theorem states that a Sylow p-subgroup, a subgroup of maximal size p^e dividing $|G|$, **exists**. In fact, we can say a lot more about what these subgroups look like.

Theorem 22.9 (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.

Evidently, conjugating a Sylow subgroup will result in a Sylow subgroup (since they have the same size), and Sylow II states that **all** the Sylow subgroups arise in this way.

Note that the second part is stronger, since $|K|$ can be a prime power smaller than $|H|$, and implies the first part by applying b) to $K = H'$. The second part states that given **any** prime power subgroup $K \leq G$ and **any** Sylow subgroup $H \leq G$, it is possible to conjugate K to make it land in H.

Student Question. *Is the converse of part a) true? If H is a Sylow p-subgroup, is gHg^{-1} also a Sylow p-subgroup?*

Answer. *The converse is essentially automatically true. In order to be a Sylow p-subgroup, the only requirement is being a subgroup of a certain size, and conjugating by an element evidently produces a subgroup of the same size. The impressive part is that given two arbitrary Sylow p-subgroups, they must in fact be conjugate!*

Sylow II confirms our intuition for reflections in dihedral groups.

Example 22.10
For D_{2n}, every subgroup of size 2 is generated by a reflection, and Sylow II indicates that all the reflections are conjugate.

22.5 The Third Sylow Theorem

The last Sylow theorem indicates the number of these (conjugate) subgroups.

Theorem 22.11 (Sylow III)
The number of Sylow p-subgroups of G divides

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

and is congruent to 1 modulo p.

This theorem seems kind of weird, but is actually very useful.

Example 22.12
Consider D_5 and $p = 2$. The number of Sylow $2-$subgroups is 5, which does divide $10/2$ and is congruent to 1 modulo 2.

The first Sylow theorem indicates **existence** of Sylow subgroups, the second Sylow theorem indicates that all Sylow subgroups are related by **conjugation**, and the third provides strong (and kind of funky) constraints on the **number** of such subgroups.

22.6 Applications of the Sylow Theorems

Now, we can look at a few different applications of these theorems, and we will see how powerful they are.

Example 22.13
Consider any group G such that

$$|G| = 15 = 5 \cdot 3.$$

By Sylow III, for $p = 5$, the number of Sylow 5-groups divides $3 = 15/5$, and is equal to 1 mod 5. In particular, the only possibility is

$$\#\text{Sylow 5-groups} = 1.$$

So there is a unique $H \leq G$ such that $|H| = 5$. Since there is only one subgroup of size 5, Sylow II indicates that $gHg^{-1} = H$. That is, H is normal: the Sylow theorems indicate automatically that there is a normal subgroup of size 5.

For $p = 3$, Sylow III states that the number of Sylow 3−subgroups divides 5 and is 1 mod 3, so it is also 1. Thus, there exists some unique $K \trianglelefteq G$ such that $|K| = 3$.

Moreover, $H \cap K = \{1\}$, since $H \cong C_5$ and $K \cong C_3$. Nontrivial elements of H have order 5, while elements of K have order 3, so they intersect only at the identity. So the Sylow theorems give, for free, nonintersecting normal subgroups of size 5 and 3 for **every single** group of size 15. That is quite impressive!

Recall the notion of a **product group**.[76]

Definition 22.14
The **product group** $H \times K$ is

$$H \times K = \{(h, k) : h \in H, k \in K\}$$

where

$$(h, k) \cdot (h', k') = (hh', kk').$$

The product group is the group given by coordinate-wise multiplication. We claim that in Example 22.15, a group of order 15 must be isomorphic to a product of groups of order 3 and order 5.

Proposition 22.15 (Example 22.15)
Where $|H| = 5$ and $|K| = 3$,

(a) the two subgroups commute: for $h \in H$ and $k \in K$, $hk = kh$;

(b) $H \times K \cong G$.

Once $H \times K \cong G$, then we know that any group of order 15 is isomorphic to $C_5 \times C_3$.

Proof. Part b) follows from part a).

(a) For the first claim, since K is normal, $hkh^{-1} \in K$, and thus, multiplying on the right by an element of K,

$$hkh^{-1}k^{-1} \in K.$$

Similarly, $kh^{-1}k^{-1} \in H$, since H is normal, but then

$$hkh^{-1}k^{-1} \in H.$$

Thus, $hkh^{-1}k^{-1} \in H \cap K = \{1\}$, and since the intersection was just 1, so $hkh^{-1}k^{-1} = 1$, and so

$$hk = kh.$$

(b) Consider the mapping

$$\begin{aligned} f : H \times K &\longrightarrow G \\ (h, k) &\longmapsto hk. \end{aligned}$$

[76] This was discussed on the homework.

We claim that this is a homomorphism. In particular,

$$f((h,k)\cdot(h',k')) = f((hh',kk')) = hh'kk' = hkh'k' = f((h,k))\cdot f((h',k')),$$

where the second-to-last step comes from H and K commuting.

In general, if we take two arbitrary subgroups and take this function, this would **not** be a group homomorphism! It was extremely important that H and K commute, which is true since they are both normal.

Next, we must check that f is in fact an isomorphism. Since H and K have trivial intersection, $hk = 1$ only when $h = 1$ and $k = 1$, so the kernel is

$$\begin{aligned}\ker(f) &= \{h,k : hk = 1 \in G\}\\ &= \{(1,1)\}.\end{aligned}$$

Since the kernel is trivial, f is injective. In addition, $|H\times K| = |G| = 15$, and so f must be bijective and thus an isomorphism.

□

We have shown that any group G of order 15 is

$$G \cong C_5 \times C_3.$$

There is only one group of size 15. In particular,

$$C_{15} = C_5 \times C_3.$$

Student Question. *How did we know that H and K were C_5 and C_3?*

Answer. *Any group of prime order is cyclic; we proved this in a previous lecture.*

There is only one group up to isomorphism of order 15. For higher order groups, finding the number of groups up to isomorphism can get tricky. The Sylow theorems make it much easier to start an argument for classifying different groups, since they can apply to any finite group.

For $n = 15$, there is only one isomorphism class.

Guiding Question
For groups such that $|G| = pq$, a product of two distinct primes, how many isomorphism classes of groups are there of size pq?

Let's think about $n = 10$.

Example 22.16
Consider a group G such that $|G| = 10 = 5\cdot 2$.

We know already that G is not unique; for example, D_5 and C_{10} both have order 10 but are non-isomorphic.

Proposition 22.17
There are two isomorphism classes: $G \cong C_5 \times C_2$, and $G \cong C_{10}$.

Proof. From Sylow III, the number of Sylow 5-groups divides 2 and is 1 modulo 5, so there is only one Sylow 5-group. So there is a normal subgroup $K \trianglelefteq G$ such that $|K| = 5$. Let $x \in K$ be a generator for K, so that

$$K = \langle x\rangle,$$

where $\operatorname{ord}(x) = 5$.

Take H to be some Sylow 2-group. Let $H = \langle y \rangle$, where the order of y is 2. Since K is normal and generated by x, $yxy^{-1} \in K$, so

$$yxy^{-1} = x^r$$

for some exponent $1 \leq r \leq 4$. Rearranged, we have

$$yx = x^r y.$$

As before, since K has elements of order 5 and H has elements of order 3, the intersection is trivial:

$$K \cap H = \{1\}.$$

This implies that the possible $x^i y^j$ are distinct from each other.[77]

Therefore, the group G is

$$G = \{x^i y^j : 0 \leq i \leq 4, 0 \leq j \leq 1\},$$

where all these elements are distinct. There are 10 such elements, so these elements must be the entire group G. The relations

$$x^5 = y^2 = 1$$

and

$$yx = x^r y$$

completely determine the group operation! The exponent r entirely controls which group of size 10 we have.

Which values of r work? Currently, we have that $1 \leq r \leq 4$, so there are **at most** four different isomorphism classes for G.

- If $r = 2$, then we would have
$$x = y^2 x = yyx = yx^2 y = x^4 y^2 = x^4,$$
by repeatedly using the relations $x^5 = y^2 = 1; yx = x^r y$. Here we have $x = x^4$, implying that $x^3 = 1$. This is a contradiction, since x had order 5. So $r = 2$ is impossible.
- In general, if $yx = x^r y$, then
$$x = y^2 x = \cdots = x^{r^2},$$
by running through the same calculations as above. So $x^{r^2-1} = 1$, and we must have $r^2 = 1 \bmod 5$. So $r = 3$ is impossible, since 9 is not 1 mod 5.
- For $r = 1$, then H and K commute by definition, and the same analysis as in 22.15 works, and we have
$$G = C_5 \times C_2,$$
which turns out to be isomorphic to C_{10}.
- For $r = 4$, we recognize these relations:
$$G = D_5.$$

For this example, we used the Sylow theorems to narrow down the possibilities, and simply looked through the possibilities to determine the isomorphism classes of groups of order 10.

For $n = 10$, because Sylow III did not restrict the number of 2-subgroups to be 1, only the 5-subgroup was necessarily normal, and so the analysis was more complicated and subtle than for $n = 15$. Since for $p = 2$, there could have been 1 or 5 subgroups (both these numbers divide $10/2 = 5$ and are congruent to 1 modulo 2), we were able to obtain less information about 2−subgroups.

□

In general, if $|G| = pq$, a product of two distinct primes, then

- if $q \neq 1 \mod p$, then $G = C_p \times C_q = C_{pq}$.

[77] Otherwise, if there are two nondistinct elements, we end up with $x^{i-i'} y^{j-j'} = 1$, implying that some element of K is the inverse of some element of H, which is not possible with a trivial intersection.

- if $q = 1 \mod p$, then $G = C_{pq}$ or a different non-abelian group.[78]

To prove this, we follow the same analysis as today. The first step is to look at the Sylow $p-$groups and the Sylow $q-$groups. In the first case, we argue that they are normal and commute, and we can show that $G \cong C_p \times C_q$. In the second case, using the relations, there end up only being two possibilities for r.

[78] For $p = 2$ and $q = 5$, the different non-abelian group is D_5.

Resource: Algebra I Student Notes

Fall 2021

Instructor: Davesh Maulik
Notes taken by Jakin Ng, Sanjana Das, and Ethan Yang