The Sylow Theorems

Recall that the Lagrange Theorem says that orders of subgroups divide order of group; but **not the converse**. We did discover that there were subgroups for each divisor if G is cyclic or if G is abelian[1]... But, this isn't true in general.[2] Time to investigate!

The three Sylow Theorems extend our characterizations of cyclic and abelian groups to general groups! We prove these by analyzing a series of group actions on sets. Begin with the standard group action of G on itself by conjugation $G \circlearrowright G$ by $g \cdot x = gxg^{-1}$.

Notation. Recall the following notation involving conjugation.

- $Z(G) = \{x \in G \mid gx = xg \text{ all } g \in G\}$ is the **center** of the group G.
  This is the **fixed point set**[3] of G under the conjugation action $X_G = \{x \in G \mid gxg^{-1} = x \text{ all } g \in G\}$.
- $C(x_i) = \{g \in g \mid gx_i = x_i g\}$ is the **centralizer** of the element x_i.
  This is the **stabilizer subgroup** of x_i under the conjugation action, G_{x_i}.
- $[G : C(x_i)]$ is the **index** of the centralizer (stabilizer) subgroup.
  This is the number of cosets of $C(x_i)$, which is equal to the **size of the orbit** of x_i under conjugation.
- Partitioning X into orbits, applying the Orbit-Stabilizer Theorem, and converting to this language yields the **class equation**. We will use this in our first two proofs.

$$\begin{aligned} |X| &= |X_G| + |Gx_1| + \cdots + |Gx_k| && \text{(Orbit Partition)} \\ &= |X_G| + [G : G_{x_1}] + \cdots + [G : G_{x_k}] && \text{(Orbit-Stabilizer Thm)} \\ |G| &= |Z(G)| + [G : C(x_1)] + \cdots + [G : C(x_k)] && \text{(Class Equation)} \end{aligned}$$

For great examples applying this, review the proofs of the following propositions (given previously).

Proposition. *If the order of G is p^n, then G has nontrivial center, $Z(G) \neq \{e\}$.*

Proposition. *If the order of G is p^2, then G is abelian.*

Our first step will be to finally prove the full Cauchy theorem! The proof will look similar to the proofs of the previous propositions, as well as the upcoming proof of the 1st Sylow theorem.[4]

Theorem [Cauchy]. *If the order of G is divisible by prime p, then G contains a subgroup of order p.*

Note. This is equivalent to G containing an element of order p, because a subgroup of order p must by cyclic (since p is prime).

Proof by strong induction on $|G|$. Fix a prime p dividing $|G|$. If $|G| = p$, then there is nothing to show. Suppose that the statement is true for all orders $< |G|$ divisible by p, and consider the class equation.

$$|G| = |Z(G)| + [G : C(x_1)] + \cdots + [G : C(x_k)]$$

[1] You can extract this from the classification of finite abelian groups. I should have assigned this as homework.

[2] Recall the counter-example: A_4 has order $4!/2 = 12$, but has no subgroup of order 6.

[3] Which happens to be a subgroup in this case.

[4] Cauchy's original proof of this was 9 pages long. Our proof is considerably shorter because we've carefully built the tools and structures needed during the past weeks.

If p divides the order of one of the centralizer subgroups $C(x_i)$ then we are done by the induction hypothesis. Otherwise p divides the index $\big[G : C(x_i)\big]$ for each x_i; since $\big|G\big| = \big[G : C(x_i)\big] \cdot \big|C(x_i)\big|$ by the Lagrange Theorem. In this case, p must divide $\big|Z(G)\big|$; since it divides $\big|G\big|$ on the left of the class equation and every other term on the right of the class equation. Once again, this completes the proof by the induction hypothesis. □

In particular we now have a proof of the following statement even for non-abelian groups G.

Corollary. $|G| = p^n$ *if and only if* G *is a* p*-group (i.e. all elements have order given by a power of* p*).*

Example. The symmetric group S_6 has order $6! = 5 \cdot 3^2 \cdot 2^4$. So it has subgroups of order 5, 3, and 2. The Sylow Theorems (up next) will tell us further information about the 2- and 3-group structure.

Cauchy's theorem tells us about the *smallest* p-subgroup contained in G. Sylow's first theorem extends this to all p-subgroups in G.

Theorem [Sylow 1]. *If the order of* G *is divisible by* p^k*, then* G *contains a subgroup of order* p^k*.*

Note. This is **not** equivalent to G containing **an element** of order p^k. Even for abelian groups we saw that $\mathbb{Z}_2 \times \mathbb{Z}_2$ has order 2^2 but contains no element of order 2^2.

Proof by induction on $\big|G\big|$. Fix the prime p dividing $\big|G\big|$. If $\big|G\big| = p$ then there is nothing to show. Suppose the statement is true for all orders $< \big|G\big|$ divisible by p, and consider the class equation.

$$\big|G\big| \;=\; \big|Z(G)\big| \;+\; \big[G : C(x_1)\big] \;+\; \cdots \;+\; \big[G : C(x_k)\big]$$

If p does not divide an index $\big[G : C(x_i)\big]$ for some i, then the Lagrange Theorem $\big|G\big| = \big[G : C(x_i)\big] \cdot \big|C(x_i)\big|$ would imply that p^k divides the centralizer $C(x_i)$, and we would be done by the induction hypothesis.

Otherwise, p must divide $Z(G)$ because it divides the left side of the class equation and all indexes on the right side of the class equation. By Cauchy's theorem, this means the center $Z(G)$ has an element g of order p. Consider $G \diagup \langle g \rangle$ (we can make this quotient because $\langle g \rangle$ is in the center of G, so it commutes with everything). Applying the Lagrange Theorem,

$$\big|G\big| \;=\; \Big|G \diagup \langle g \rangle\Big| \cdot \big|\langle g \rangle\big| \;=\; \Big|G \diagup \langle g \rangle\Big| \cdot p$$

Since p^k divides $\big|G\big|$, $p^{(k-1)}$ divides $\Big|G \diagup \langle g \rangle\Big|$. Thus the induction hypothesis yields an order $p^{(k-1)}$ subgroup $H < G \diagup \langle g \rangle$. By the 1st Isomorphism Theorem, $q^{-1}H < G$ has order p^k. □

Example. The symmetric group S_6 has order $\big|S_6\big| = 2^4 \cdot 3^2 \cdot 5$, so the First Sylow Theorem guarantees the existence of subgroups of orders 2^4, 2^3, 2^2, 2 and 3^2, 3 and 5.
However, the First Sylow Theorem does not give any insight into the existence (or non-existence) of subgroups of composite orders like 6, 10, or 15. In fact, there are no subgroups of order 10 or 15, as we'll show later.

Next we want to compute how many subgroups are contained in G. For this analysis, we'll need the following lemma about the number of fixed points for group actions of p-groups. We use this to show that there must be fixed points. This is simple, but actually **very powerful**.

Lemma [Fixed-Point Lemma]. *If a* p*-group* P *acts on a set* X*, then the number of* P*-fixed points is congruent mod* p *to the number of elements,* $\big|X_P\big| \equiv \big|X\big| \pmod{p}$*.*

Proof. Similar to the class equation, write $\left|X\right|$ as a sum over orbits and apply the Orbit-Stabilizer Theorem to convert size of orbits to index of stabilizer subgroups.

$$\left|X\right| \;=\; \left|X_P\right| \;+\; \left[P : P_{x_1}\right] \;+\; \cdots \;+\; \left[P : P_{x_r}\right]$$

If $\left|P\right| = p^k$ then all of the indexes on the right of this equation must be multiples of p (because they are greater than 1 and divide $\left|P\right| = p^k$). Reducing mod p gives the desired equation. □

We'll make critical use of the Fixed-Point Lemma to prove the 2nd and 3rd Sylow Theorems. There is also a famous proof of Cauchy's Theorem using the Fixed-Point Lemma by J. McKay in 1959. Curious students should look it up – it is **quite** clever.

Now we can show that p-subgroups form a lattice ordered by inclusion. At the top of this lattice, containing all other p-subgroups, are the p-subgroups of maximal order. (This same proof structure will be repeated to prove the 2nd Sylow Theorem.)

Proposition. *If $\left|G\right| = m\,p^n$ where p does not divide m and $H < G$ is a subgroup of order p^k then $H < P$ for some subgroup P of order p^n.*

Proof. By the 1st Sylow Theorem, G has a subgroup P of order p^n. Let $X = \left\{\text{cosets of } P \text{ in } G\right\}$ and consider the action of H on X by left multiplication. The Lagrange Theorem tells us that $\left|X\right| = m$.

From the Fixed-Point Lemma we know that $\left|X_H\right| \equiv \left|X\right| \pmod{p}$. In particular, $\left|X_H\right| \neq 0$ because $m \not\equiv 0 \pmod{p}$. Thus at least one coset of P must be fixed by all of H!

If gP is a coset fixed by all of H, then $h(gP) = (gP)$ for all $h \in H$. Rearranging yields $g^{-1}hgP = P$; so $g^{-1}hg \in P$ and thus $h \in gPg^{-1}$. Since this is true for all $h \in H$, we have $H \subset gPg^{-1}$. Therefore gPg^{-1} is the desired subgroup of order p^n. □

We want to focus on these "top" subgroups of order p^n since they contain all of the others.

Definition. A **Sylow p-subgroup** of G is a subgroup of maximal order p^n.

Example. If G has order $2^3 \cdot 3^2 \cdot 5$, then the subgroups of order 2^3, 3^2, and 5 are Sylow subgroups.

To investigate Sylow p-subgroups, we switch our group action slightly – from conjugation on elements $(g \cdot x = gxg^{-1})$ to conjugation on subgroups $(g \cdot H = gHg^{-1})$. First, note that we can use conjugation to make new Sylow p-subgroups from old ones!

Proposition. *Every conjugate of a Sylow p-subgroup is also a Sylow p-subgroup.*

Proof. We've already shown that conjugation takes subgroups to subgroups. Conjugation also preserves order, since $gag^{-1} = gbg^{-1}$ if and only if $a = b$. □

The Second Sylow Theorem says that, not only are all conjugates of a Sylow p-subgroup themselves Sylow p-subgroups... these are **the only** Sylow p-subgroups.

Theorem [Sylow 2]. *The Sylow p-subgroups of G are conjugates of each other.*

Proof. Given Sylow p-subgroups P and Q let $X = \left\{\text{cosets of } P\right\}$ and consider the action of Q on X by multiplication $q \cdot gP = (qg)P$.

By the Fixed-Point Lemma, $\left|X_Q\right| \equiv \left|X\right| \pmod{p}$. But $\left|X\right|$ is the number of cosets of P, which is relatively prime to p because P had maximal order p^n. Thus there is a coset gP which is fixed by all $q \in Q$.

If gP is a coset fixed by all of Q, then $q(gP) = (gP)$ for all $q \in Q$. Rearranging yields $g^{-1}qgP = P$; so $g^{-1}qg \in P$ and thus $q \in gPg^{-1}$. Since this is true for all $q \in Q$, we have $Q \subset gPg^{-1}$. But Q and gPg^{-1} have the same size, so they must be equal. □

We're about to count the number of Sylow p-subgroups. We begin the count by noting a condition for there to be **only one** subgroup.

Proposition. *A Sylow p-subgroup of G is normal if and only if it is the only Sylow p-subgroup.*

Proof. ($\Rightarrow$) If P is a normal Sylow p-subgroup, then $gPg^{-1} = P$ for all $g \in G$. By the 2^{nd} Sylow Theorem, all Sylow subgroups have this form; so P is the only one.

($\Leftarrow$) Conjugates of Sylow subgroups are Sylow subgroups. So if there is only one Sylow subgroup P, then $gPg^{-1} = P$ for all $g \in G$. Thus P is normal. □

Consider the conjugation action of G on $X = \{\text{Sylow } p\text{-subgroups of } G\}$. We will count Sylow p-subgroups using the Orbit-Stabilizer Theorem. The stabilizer subgroups of the conjugation action have another name.

Definition. The **normalizer** of a subgroup $H < G$ is $N(H) = \{g \in G \mid gHg^{-1} = H\}$.
These are the stabilizer subgroups G_H of $G \circlearrowright \{\text{subgroups of } G\}$ by conjugation.

The normalizer satisfies a universal property. It is the largest subgroup with $H \lhd N(H)$. Now we are ready for the 3^{rd} Sylow Theorem!

Theorem [Sylow 3]. *If p divides $|G|$, then $\#\{\text{Sylow } p\text{-subgroups}\} \equiv 1 \pmod p$ and divides $|G|$.*

Proof. Let $X = \{\text{Sylow } p\text{-subgroups of } G\}$ and let P be some Sylow p-subgroup. Consider the action of P on X by conjugation. According to the Fixed-Point Lemma, $|X| \equiv |X_P| \pmod p$. We claim that the only Sylow subgroup fixed by conjugation by every element in P is P itself. This will show that $|X| \equiv 1 \pmod p$.

If Q is a Sylow subgroup with $xQx^{-1} = Q$ for all $x \in P$ then $P < N(Q)$. But $Q \lhd N(Q)$ so it is the **only** Sylow subgroup of $N(Q)$. Thus $P = Q$.

To show that $\#\{\text{Sylow } p\text{-subgroups}\}$ divides $|G|$, consider the conjugation action of all of G on $X = \{\text{Sylow } p\text{-subgroups of } G\}$. The Sylow p-subgroups are all conjugate, so there is only one orbit. Picking any Sylow subgroup P, the Orbit-Stabilizer Theorem says $|X| = [G : N(P)]$. Finish by recalling Lagrange's Theorem $[G : N(P)] \cdot |N(P)| = |G|$. □

Note that we actually showed $\#\{\text{Sylow } p\text{-subgroups}\} = [G : N(P)]$. We can use this to get a slightly stronger statement.

Corollary. *If $|G| = m\,p^n$ then $\#\{\text{Sylow } p\text{-subgroups}\}$ divides m.*

Proof. Let P be any Sylow p-subgroup. Recall that $\#\{\text{Sylow } p\text{-subgroups}\} = [G : N(P)]$.

Apply this to the triple $P \lhd N(P) < G$.

$$[G : P] = [G : N(P)] \cdot [N(P) : P]$$

The left-hand side is m and the right hand side is a multiple of $\#\{\text{Sylow } p\text{-subgroups}\}$. □

Example. We now have a short proof that the symmetric group S_5 doesn't contain a subgroup of order 15 even though 15 divides $|S_5| = 5! = 120$. Using Sylow to count subgroups, we can show that the only group of order 15 is the cyclic group $\mathbb{Z}_{15}$; but S_5 doesn't include any elements of order 15. [5]

Let G be a group of order 15. The number of Sylow 5-subgroups of G must divide the index $15/5 = 3$, but also be $\equiv 1 \pmod 5$. Thus there is only 1 subgroup of order 5. Similarly there

[5] The order of an element in S_n is the least common multiple of the lengths of its disjoint cycles – e.g. $(1\ 2)\,(3\ 4\ 5)$ has order $2 \cdot 3 = 6$. But $15 = 3 \cdot 5$ and $3 + 5 = 8$; so S_8 is the first symmetric group with an element of order 15.

is only 1 subgroup of order 3. When Sylow subgroups are unique, they are normal. Thus their product set is a subgroup, which must have order 15 by the Product Formula. Since G has order 15, $G \cong \mathbb{Z}_5 \times \mathbb{Z}_3 \cong \mathbb{Z}_{15}$.

Example. Wilson's theorem says p is prime if and only if $(p-1)! \equiv -1 \pmod{p}$.

The 3rd Sylow Theorem gives one direction of this statement. Consider the symmetric group S_p where p is prime. By Sylow 3,

$\#\{\text{Sylow } p\text{-subgroups}\} \equiv 1 \pmod{p}$.

However S_p has order $p!$ and p is prime, so the Sylow p-subgroups of S_p must be order $p^1 = p$ (and thus cyclic). Prime order subgroups are disjoint and each contain $(p-1)$ elements of order p, so

$\#\{\text{Sylow } p\text{-subgroups}\} = \#\{\text{elements of order } p\} \;/\; (p-1)$

But there are exactly $(p-1)!$ elements of order p in S_p, because p-cycles all must have the form $(1\ a_2\ a_3\ \ldots\ a_p)$ where $a_2, \ldots, a_p$ are a permutation of $2, \ldots, p$. So there are $(p-2)!$ Sylow p-subgroups and thus $(p-2)! \equiv 1 \pmod{p}$.

Therefore $(p-1)! = (p-1)\,(p-2)! \equiv -1 \pmod{p}$.