Week 8

Applications of the Sylow Theorems

8.1 Sylow III and Examples

11/14:

- Last time:
  - Sylow I: p-Sylow subgroups exist.
  - Sylow II: p-Sylow subgroups are unique up to conjugation. Moreover, if $Q \subset G$ is a p-group, then $Q \subset gPg^{-1}$ with the same g.
  - We proved Sylow II by taking $H \subset G$, and separately taking $P \subset G$ to be p-Sylow. In this case, there exists $g \in G$ such that $H \cap gPg^{-1}$ is a p-Sylow of H. If $H = Q$, then $Q \cap gPg^{-1} = Q$.
    - More on this??
- Alternate proof of Sylow II.

  Proof. We attack the first claim (equality for p-Sylows) in three steps; we will not prove the second claim (containment for p-groups) herein. Step 1 defines a useful group action, allowing us to apply relevant theorems from that domain later on. Step 2 proves the existence of a fixed point of said group action, which will be intimately related to the final element g by which we conjugate P to make it equal Q. Step 3 relates this element g to the desired result. Let's begin.

  Let X denote the set of all p-Sylows of G. By Sylow I, X is nonempty. Thus, we may choose $P, Q \in X$ (note that P, Q are not necessarily distinct). Define $G \curvearrowright G/P$ by left multiplication. Restrict the group action to Q (i.e., restrict the function $\cdot : G \times G/P \to G/P$ to $Q \times G/P$).

  Since $|G| = p^n k$ and $|P| = p^n$, we have that $\gcd(|G/P|, p) = 1$. Thus, $|G/P|$ is not divisible by p, so $|G/P| \mod p \not\equiv 0 \mod p$. Additionally, since Q is a p-group (by definition as a p-Sylow), we have from the proposition in Lecture 7.2 that $\text{Fixed}(G/P) \equiv |G/P| \mod p$. This combined with the previous result reveals that $\text{Fixed}(G/P)$ is nonempty. As such, we may choose $gP \in \text{Fixed}(G/P)$.

  By definition, Q stabilizes gP, i.e.,

  $$QgP = gP$$
  $$g^{-1}QgP = P$$

  where the latter equation above is a simple rearrangement of the first, but can be interpreted to mean that $g^{-1}Qg$ stabilizes P. Thus, if $g^{-1}qg \in g^{-1}Qg$, we have $(g^{-1}qg)p_1 = p_i$ for some $i = 1, \ldots, p^n$, and hence $q = g(p_i p_1^{-1})g^{-1} \in gPg^{-1}$. Therefore, $Q \subset gPg^{-1}$. Since $|P| = |Q|$, we additionally have that $Q = gPg^{-1}$, as desired. □

- Sylow III. The first is existence, the second is uniqueness, and then there's this one (divisibility and congruence).

- Theorem (Sylow III — divisibility and congruence): Let P be a p-Sylow, and let n_p denote the number of p-Sylows of G. Then

  1. Let $N = N_G(P)$. Then $n_p = |G|/|N| = [G : N]$. In particular, n_p divides $|G|$.

     Proof. To prove a claim which expresses $|G|$ in terms of the product of two other numbers, we should think about using the Orbit-Stabilizer theorem. To do so, we need a group action. In particular, a group action by conjugation could be useful because we have a normalizer involved. With this motivation mentioned, let's begin.

     Let X be the set of p-Sylows of G. Define $G \circlearrowright X$ by conjugation. By the Orbit-Stabilizer theorem,

     $$|\operatorname{Stab}_G(P)| \cdot |\operatorname{Orb}(P)| = |G|$$

     Since the group action is by conjugation, we have by the definition of the stabilizer and the normalizer that

     $$\operatorname{Stab}_G(P) = \{g \in G \mid gPg^{-1} = P\} = N_G(P) = N$$

     According to Sylow II, every p-Sylow (every element of X) is conjugate to every other via some element of G. Thus, since our group action is conjugation, the group action is transitive and $\operatorname{Orb}(P) = X$. Thus,

     $$|\operatorname{Orb}(P)| = |X| = n_p$$

     Therefore, substituting the previous two results into the preceding one, we have that

     $$\begin{aligned} |N| \cdot n_p &= |G| \\ n_p &= |G|/|N| = [G : N] \end{aligned}$$

     as desired. □

  2. $n_p \equiv 1 \mod p$.

     Proof. Congruence should make us think, "fixed points." In this argument, we will pick up where we left off, using the same group action defined in the proof of part 1 to express the claim in the language of fixed points. We will then deduce that this latter claim is true, proving the original claim. Let's begin.

     Restrict the action from part 1 to P. This may mean that $P \circlearrowright X$ is no longer transitive, but this will not cause any issues. Moving on, we know by the closure of subgroups that $gPg^{-1} = P$ for any $g \in P$; thus, P is a fixed point of $P \circlearrowright X$. It follows by the proposition from Lecture 7.2 that $\operatorname{Fixed}_P(X) \equiv |X| \mod p$, and hence $n_p = |X| \equiv \operatorname{Fixed}_P(X) \mod p$. Thus, we are done if we can show that $\operatorname{Fixed}_P(X) = 1$, i.e., that P is the only fixed point of X under $P \circlearrowright X$.

     Let $Q \in \operatorname{Fixed}_P(X)$ be arbitrary; we seek to prove that $Q = P$. Define $N := N_G(Q)$. By definition, $Q \subset N$. Additionally, $P \subset N$: Since $Q \in \operatorname{Fixed}_P(X)$, $gQg^{-1} = g \cdot Q = Q$ for all $g \in P$. Hence P, Q are both p-Sylows of N (the order of p dividing $|N|$ certainly [by Lagrange's Theorem] divides the order of p dividing $|G|$). By Sylow II, any two p-Sylows are conjugate, so there exists $n \in N$ such that $nQn^{-1} = P$. Additionally, since $Q \triangleleft N$ by HW4 Q3c, we have that $nQn^{-1} = Q$. Therefore, by transitivity, $P = Q$, as desired. □

- We are now done with proving the Sylow theorems. Make sure you have nice copies written out!
  - Perhaps before the final, I should take all important proofs from the quarter and make "proof outlines" in my review sheet, giving the tricks and motivation in as concise a format as possible but still allowing me to deduce the rest of the proof for myself. This could be a great exercise!
- The arguments that we've used thus far in this class are mostly combinatorical with a bit of number theory sprinkled in.
- Before going into applications of the Sylow theorems, we present an example that's good to keep in mind.

- Let $G = S_p$ for some $p \in \mathbb{N}$ prime.
  - S I: Yes, G has a p-Sylow, namely $P = \langle (1, 2, \ldots, p) \rangle$.
  - S II: Any p-cycles are conjugate to one another.
  - Intuitive derivation of the value of n_p: n_p is the number of elements of order p[1] divided by $p-1$[2]. Thus,
$$n_p = \frac{p!}{p(p-1)} = (p-2)!$$
  - S III: $(p-2)! \equiv 1 \mod p$.
    - We obtain a related statement from **Wilson's theorem**: $(p-1)! \equiv -1 \mod p$.
  - S III: $|N| = |N_G(P)| = p(p-1)$.
  - This result combined with $P \triangleleft N$: $|N/P| = p - 1$.
- Theorem (Wilson's theorem): A natural number $p > 1$ is prime iff
$$(p-1)! \equiv -1 \mod p$$
- **Affine group** (of order p): The following group, which consists of permutations given by affine maps. *Denoted by* $\mathbf{Aff}_p$. *Given by*
$$\mathrm{Aff}_p = S_{\mathbb{Z}/p\mathbb{Z}}$$
  - We send $x \in \mathbb{Z}/p\mathbb{Z}$ to $ax + b \in \mathbb{Z}/p\mathbb{Z}$.
  - Injective:
$$\begin{aligned} ax + b &= ay + b \\ a(x - y) &\equiv 0 \mod p \\ x &= y \end{aligned}$$
  - We also need to check that Aff_p is actually a subgroup. The group operation...
  - An affine map is the sum of a linear transformation and a translation. Thus,
$$A(ax + b) + B = Aax + Ab + B$$
    so
$$(a, b)(A, B) = (aA, Ab + B)$$
  - We claim that $P = \langle X \to X + 1 \rangle$ is a subgroup??
  - In particular, $P \triangleleft \mathrm{Aff}_p \leq N$.
  - Thus, $\mathrm{Aff}_p = N_{S_p}(\langle (1, 2, \ldots, p) \rangle)$. This is a nice new group to have.
  - We have $P : \mathrm{Aff}_p \to (\mathbb{Z}/p\mathbb{Z})^*$ defined by $\langle x \mapsto x + b \rangle$. $x \mapsto ax + b$ goes to a in the codomain, $Ax + B$ maps to A, and $aAx + \cdots$ maps to aA.
  - Remark: If $q | p - 1$ is prime, then $(\mathbb{Z}/p\mathbb{Z})^*$ has an element of order q (Sylow). Call it σ. Then $\langle \sigma \rangle \leq (\mathbb{Z}/p\mathbb{Z})^*$.
- Theorem: Let p, q be primes such that $p > q$. Then either...
  1. $p \equiv 1 \mod q$ and there exists a nonabelian group of order pq that is a subset of Aff_p.
  2. $p \not\equiv 1 \mod q$ and all groups of order pq are isomorphic to $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}/pq\mathbb{Z}$.

[1] Recall that this is $p!/p$, since there are p options for the first entry, $p - 1$ for the second, on and on down to 1, but there are also p ways to write said element.

[2] Each p-Sylow P contains $p - 1$ distinct p-cycles.

Proof. ... □

- Misc notes: According to S III...
  - $|G| = pq$ and $n_p \equiv 1 \mod p$. Either $n_p = 1$ or $n_p = q \equiv 1 \mod p$, implying $q > p$, a contradiction.
  - Alternatively, $G \cong P_p \times P_q$. $n_q = 1$ or $n_q = p$. If $p \not\equiv 1 \mod q$, then $n_q = 1$. We end up with $P_p \trianglelefteq G$ and $P_q \trianglelefteq G$, which implies that $P_p \cap P_q = \{e\}$. Therefore, P_p and P_q commute.
- First example: 15; the first composite number for which $p, q > 2$ (and thus the structure is not covered by our previous analysis).
- We still haven't completely classified groups of order pq; sometimes there's one, sometimes there's more. We will look at these groups in greater detail next lecture.

8.2 Groups of Order *pq*

11/16:

- Classifying groups of order $|G| = 2p$ for $p > 2$ prime.
- By Sylow I, there exists a p-Sylow P_p and a 2-Sylow P_2.
  - Since $[G : P_p] = 2$, HW4 Q6 implies that P_p is normal.
    - Alternate strategy: By SyIII, $n_p \equiv 1 \mod p$ and $n_p = |G|/|N| = |G|/|P| = 2p/p = 2$. Thus, $n_p = 1$ or $n_p = 2$. These facts combine to say that $n_p = 1$ and $P_p \trianglelefteq G$.
  - By Lagrange's Theorem, we must have $P_p = \langle x \rangle$ and $P_2 = \langle y \rangle$ for some $x, y \in G$.
  - $x^p = e = y^2$.
  - $G = \langle x, y \rangle$.
- The elements have order 1, 2, p or $2p$ by Lagrange.
- Since $\langle x \rangle$ is normal, it follows that

$$\begin{aligned} y \langle x \rangle y^{-1} &= \langle x \rangle \\ yxy^{-1} &\in \langle x \rangle \\ yxy^{-1} &= x^k \end{aligned}$$

  where the x, y used throughout are the previously referenced generators (not any sort of arbitrary variable).
- Goal: Put constraints on k.
- $k \equiv 0 \mod p$ iff $x = e$.
  - If $k \equiv 0 \mod p$, then $yxy^{-1} = x^k = e$, so $x = y^{-1}y = e$.
  - If $x = e$, then $x^k = yey^{-1} = e$, so we must have $k \equiv 0 \mod p$.
- A preview of something we will shortly prove.
  - There are two groups of order $2p$: D_{2p} and $\mathbb{Z}/2p\mathbb{Z}$.
  - In the latter, $k = 1$.
    - Since $\mathbb{Z}/2p\mathbb{Z}$ is abelian, the conjugate of any element is itself. Thus, $yxy^{-1} = x^1$.
  - In the former, $k = -1$ (if conjugating by a reflection??).
    - Recall the multiplication rule $rs = sr^{-1}$, from which we can deduce that $srs^{-1} = r^{-1}$.
    - Note that it is proper to use s analogously to y and r analogously to x since reflections (s) have order 2 like y and rotations (r) can have much higher orders (e.g., p).

- Another (redundant??) possibility: $yx^iy^{-1} = yx^{ik}y^{-1}$.
- We now prove that there are only two groups of order $2p$.
- Conjugating x by y twice gives us

$$x = exe = y^2xy^{-2} = y(yxy^{-1})y^{-1} = yx^ky^{-1} = (yxy^{-1})^k = (x^k)^k = x^{k^2}$$

  - Comparing exponents, we have $k^2 \equiv 1 \mod p$.
  - This is equivalent to $(k^2-1) \equiv 0 \mod p$, which in turn is equivalent to $(k+1)(k-1) \equiv 0 \mod p$.
  - It follows that $k \equiv \pm 1 \mod p$.
- Now we must consider each case in turn.
- If $k = 1$, then G is abelian, i.e., $G = P_p \times P_2$.
  - Example: $\mathbb{Z}/2p\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.
  - We'll see a lot of this breaking up of groups next quarter.
  - Calegari alludes to the **Chinese remainder theorem**.
- Theorem (Chinese remainder theorem): Let m, n be relatively prime positive integers. For all integers a, b, the pair of congruences

$$\begin{aligned} x &\equiv a \mod m \\ y &\equiv b \mod m \end{aligned}$$

  has a solution, and this solution is uniquely determined modulo mn.
- If $k = -1$, then $yx = x^{-1}y$.

	x^i	x^iy
x^j	x^{i+j}	$x^{i+j}y$
x^jy	$x^{j-i}y$	x^{j-i}

Table 8.1: Multiplication table for $|G| = 2p$ and $k = -1$.

  - We still have that $x^p = 1$.
  - We want to show based on this multiplication rule that we really have the dihedral group. Once we have this, there's at most one group it could possibly be. Since D_{2p} is such a group, then they must be isomorphic.
  - To do so, we show that the rule determines the multiplication table (see Table 8.1 above).
  - Thus, there is at *most* one group.
  - But since D_{2p} exists, there is also at *least* one group.
  - Therefore, if $k = -1$, we must have $G \cong D_{2p}$.
- Proposition: Let $|G| = 2n$, $n > 2$. If $x \in G$ and $|x| = n$, $|y| = 2$, $yx = x^{-1}y$ implies $G \cong D_{2n}$.

  Proof. The multiplication table is uniquely determined (analogous to the above argument). □
- Remark about $D_4 = K$, where K is the Klein 4-group??
- We now move on to $|G| = pq$, where $p > q$ are both prime.
- Applying S III, we get n_p equals 1 or q and is congruent to 1 mod p, and n_q equals 1 or p and is congruent to 1 mod q.

  - Thus, $n_p = 1$ always and $n_q = 1$ unless $p = 1 \mod q$.

- If $|G| = pq$ and$p > 2$, $p \not\equiv 1 \mod q$, then $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$.
- Case where $|G| = q$ and $p \equiv 1 \mod q$. Then $P_p = \langle x \rangle$ and $P_q = \langle y \rangle$, so $P_p \trianglelefteq G$. This is another (strange??) application of S III.
  - Using what we have here, we know that $yxy^{-1} = x^k$, $k \not\equiv 0 \mod p$. $k = 1$ implies G is abelian and $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$.
  - Now we just need to conjugate x by y, q times over: $x = y^q x y^{-q} = x^{k^q}$. Thus, $k^q \equiv 1 \mod p$.
  - Unlike when $q = 2$, we could factor then. Now we've got a more difficult problem; can't factor it.
  - Does there exist q satisfying the above property? If so, how many are there?
  - Think about this as an identity in the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ which has order $p - 1$. We can thus deduce by Lagrange that $q|p - 1$.
  - Sylow I: There exists η of order q such that $\eta, \eta^2, \eta^3, \ldots, \eta^{q-1}$ all have order p.
  - We could argue that $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic (and in fact it is), but here's something else: We have that $k^q - 1 = (k-1)(k-\eta)\cdots(k-\eta^{q-1})$. This is factoring polynomials mod p (weird for now, but very commonplace next quarter).
  - Fix η. Then $yxy^{-1} = x^{\eta^2}$.
- Claim I: This determines the multiplication table; $\langle x \rangle \subset G$. The right cosets $\langle x \rangle, \langle x \rangle y, \ldots, \langle x \rangle y^{q-1}$. $G/P_p \cong \mathbb{Z}/q\mathbb{Z}$. If we have all of the elements of the form $x^i y^j$, do we know how to multiply these together? In particular, can we determine how to write

$$x^i y^j x^a y^b = x^r y^s$$

  We have that $yx = x^{\eta^i} y$, so the multiplication table is determined. This implies that there is at most $q - 1$ nonabelian groups.
- Now we have

$$\begin{aligned} yxy^{-1} &= x^{\eta^i} \\ y^2 xy^{-1} &= x^{\eta^{2i}} \\ &\vdots \\ y^r xy^{-r} &= x^{\eta^{ri}} \end{aligned}$$

  Thus, $\eta^{ri} = \eta$. Therefore, $y_i = y^r$ so $yxy^{-1} = x^\eta$, so there is at most 1 non abelian group.
- But, P a p-Sylow of S_p and $N = N_{S_p}(P)$ and $C = C_{S_p}(P)$ gives us $|N| = p(p-1)$ and $|C| = p$ so that $N/C = (\mathbb{Z}/p\mathbb{Z})^\times$. We now take the preimage in N so that $\langle y, x \rangle = G$. $|G| = pq$. Then P, G abelian would imply $G \subset C$, but this is not possible since G ahs pq and C has p, so G is not abelian.
- Example $21 = 7 \cdot 3$. $2^3 \equiv 1 \mod 7$. Then we take $\mathbb{Z}/7\mathbb{Z} \to \mathbb{Z}/7\mathbb{Z}$ so we take $x \mapsto x + a$, $x \mapsto 2x + a$, $x \mapsto 4x + a$, on and on where a is a constant. There are 21 such maps.
- If $\eta^1 = 1 \mod p$, then the affine maps from $\mathbb{Z}/p\mathbb{Z}$ to $\mathbb{Z}/p\mathbb{Z}$ send $x \mapsto \eta^i x + b$.
- If we call $\sigma = x + 1$ and and $\tau = x \to x\eta$, then $x \mapsto x + \eta = \sigma\eta$.
- The set of affine maps has both $\mathbb{Z}/p\mathbb{Z}$ and $(\mathbb{Z}/p\mathbb{Z})^\times$ as subsets.
- If we think about the groups we've classified, we've classified $1, p, p^2, p^3, pq$. p^3 just a bit, though. Limit to this strategy: The prime factorizations are so simple that we get immediate and very restrictive information about the p-Sylow subgroups (e.g., the biggest one is normal). This can't occur indefinitely because we will eventually get to cases like A_5 of order 60, for example, which has no normal subgroups.

- If we think about our progress (classifying groups of low order up to 4), then going upwards, the first group we can't do is of order $12 = 2 \cdot 2 \cdot 3$. This is like A_4, which is not too bad but all the same, $n_3 = 1, 4$, $n_2 = 1, 3$. If $n_3 = 4$, then we have an action of G on the 3 Sylow's, giving a transitive map from G to S_4. Thus, the stabilizer has size 3.
- $n_3 = 1$, so $G = P_3 \times P_2$. $n_3 = 1$ and $n_2 = 3$, so $G \times S_3$. Since there is such an explosion of groups, this is not the optimal strategy. Thus, ...
- We may do a review session of the 25 practice problems over Twitch with him playing speedtest.
- At this point, we have the tools to do every outgoing homework problem, save the last one of the last psets on symmetry groups.

8.3 Symmetries in Three-Space

11/18:

- Classify the finite subgroups of SO(3).
- We can take any regular n-gon and think of $D_{2n} \subset \mathrm{O}(2) \subset \mathrm{SO}(2)$.
- Five platonic solids: Te, Cu, Oc, Do, and Ic.
- Cu and Oc are paired and Do and Ic are paired. Te $\cong A_4$, Cu $\cong$ Oc $\cong S_4$, and Do $\cong$ Ic $\cong A_5$.
- Theorem: Let $G \subset \mathrm{SO}(3)$ be a finite group. Then G is conjugate to one of these groups.
- Let $g \in \mathrm{SO}(3)$, $g \neq e$. The only fixed points of g lie on a line ℓ which contains the origin 0.
- We have a group action $\mathrm{SO}(3) \circlearrowright S^2 = \{v \mid \|v\| = 1\}$. Consider $G \circlearrowright S^2$. Any $g \neq e$ has exactly 2 fixed points which we may call $\{\pm u\}$ for some u.
- Thus, $|\operatorname{Stab}(x)| = 1$ for all but finitely many points $x \in S^2$.
- Claim:

$$\sum_{x \in S^2} |\operatorname{Stab}(x) - 1|$$