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 $G \circlearrowright G/P$ 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.,

  $$\begin{aligned} QgP &= gP \\ g^{-1}QgP &= P \end{aligned}$$

  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 $i = 1, \dots, p^n$, 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. $\square$

- 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 $P = \langle (1, 2, \dots, p) \rangle$.
  - 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* $\mathbf{Aff}_{\boldsymbol{p}}$. *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:
$$\begin{gathered} ax + b = ay + b \\ a(x - y) \equiv 0 \mod p \\ x = y \end{gathered}$$
  - 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, $\mathrm{Aff}_p = N_{S_p}(\langle (1, 2, \dots, p) \rangle)$. 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. ... $\square$

- 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.