Week 7

Group Action Applications: A_5 and the Sylow Theorems

7.1 Actions of A_5

11/7:

- Classifying subgroups of $G = A_5 \cong$ Do.
- Let $H \leq G$. We must have $|H|\,\big|\,|G|$ by Lagrange's theorem.
  - Thus, if $H \leq A_5$, we must have
  $$|H| \in \{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}$$
- A good place to start is with orders of H that correspond to cyclic subsets.
- In particular, let's start with subgroups of the form $\langle(**)(**)\rangle$, which all have order 2.
  - Are such groups conjugate?
  - To prove that two groups of the form $\langle(**)(**)\rangle$ are conjugate, it will suffice to show that their generators are conjugate (since the only other element — the identity — will naturally be conjugate to itself).
  - Let $x, y \in A_5$ be arbitrary elements of the form $(**)(**)$. Then there exists $g \in S_5$ such that $gxg^{-1} = y$.
  - But is $g \in A_5$? If $g \in A_5$, then we are done. If $g \notin A_5$, then can we find an element $g' \in A_5$ such that $g'xg'^{-1} = y$?
  - First, note that if $gxg^{-1} = y = g'xg'^{-1}$, then
  $$\begin{aligned} g^{-1}(gxg^{-1})g' &= g^{-1}(g'xg'^{-1})g' \\ x(g^{-1}g') &= (g^{-1}g')x \end{aligned}$$
  Thus, $g^{-1}g' \in C_{S_5}(x)$, or $g' = gh$ for some $h \in C_{S_5}(x)$.
    - If $g \notin A_5$ and we want $g' \in A_5$, then we must have $h \notin A_5$.
      - Intuitively, this means that if g is the product of an odd number of permutations and we want $g' = gh$ to be the product of an even number of permutations, h had better be a product of an odd number of permutations as well.
      - More formally, consider G/A_5. If $g \in gA_5 \neq A_5$ and we want $g' \in g'A_5 = A_5$, then by homomorphically mapping gA_5 to $1 \in \mathbb{Z}/2\mathbb{Z}$ and A_5 to $0 \in \mathbb{Z}/2\mathbb{Z}$, we must have $h \in gA_5$ to get $gh \in A_5$.
    - Regardless, this example motivates the following two propositions, which we can use to resolve the original conjugacy question.

  - By Proposition 1, since $x \sim y$ in S_5 and $C_{S_5}(x) \not\subset A_5$ (take the first transposition in $(**)(**)$; for example, know that (12) commutes with (12)(34)), we know that $x \sim y$ in A_5.
  - Therefore, there are 15 subgroups of the form $\langle (**)(**) \rangle$, all of which are conjugate in A_5.

- Proposition 1: Let $x \sim y$ in S_n. Then if $C_{S_n}(x) \not\subset A_n$, then $x \sim y$ in A_n.

  Proof. Since $x \sim y$ in S_n, there exists $g \in S_n$ such that $gxg^{-1} = y$. If $g \in A_n$, then we are done. Now suppose $g \notin A_n$. Since $C_{S_n}(x) \not\subset A_n$, there exists $h \in C_{S_n}(x)$ such that $hxh^{-1} = x$ and $h \notin A_n$. Since $g, h \notin A_n$, we have that $gh \in A_n$. Additionally, we have that

$$(gh)x(gh)^{-1} = g(hxh^{-1})g^{-1} = gxg^{-1} = y$$

  Therefore, $x \sim y$ in A_n, as desired. $\square$

- Proposition 2: If $C_{S_n}(x) \subset A_n$ and $\sigma x \sigma^{-1} = y$, then $x \sim y$ in A_n iff $\sigma \in A_n$.

  Proof. Suppose first that $x \sim y$ in A_n. Then $gxg^{-1} = y$ for some $g \in A_n$. Then as per the above, $gxg^{-1} = \sigma x \sigma^{-1}$ implies that $g^{-1}\sigma \in C_{S_n}(x)$. Thus, $\sigma = gh$ for some $h \in C_{S_n}(x) \subset A_n$. But since $g, h \in A_n$, we must have $\sigma \in A_n$, too.

  Now suppose that $\sigma \in A_n$. Then since $\sigma x \sigma^{-1} = y$, $x \sim y$ in A_n as desired. $\square$

- Now we discuss subgroups of the form $\langle (***) \rangle$.
  - Let x be an arbitrary element of A_5 of the form $(***)$. In particular, suppose $x = (abc)$ for $a, b, c \in [5]$.
  - Then $(de) \in C_{S_5}(x)$, where $d, e \in [5]$ are the other two elements that are not already represented by a, b, c.
  - Moreover, (de) will be in the centralizers of both x and x^2.
  - There are $\binom{5}{2} = 10$ subgroups of the form we're discussing (20 generators/elements of the form $(***)$, though).
  - Suppose we have two subgroups $\langle x \rangle, \langle y \rangle$ of the form being discussed. We know that $\langle x \rangle, \langle y \rangle$ are conjugate in S_5. But since $C_{S_5}(x) \not\subset A_5$ again as per the above, we know the groups are conjugate in A_5.
  - Therefore, there are 10 subgroups of the form $\langle (***) \rangle$, all of which are conjugate in A_5.

- Now we discuss subgroups of the form $\langle (*****) \rangle$.
  - We know that $|C_{S_5}((12345))| \cdot |\{(12345)\}| = 120$. Additionally, only a power of (12345) commutes with it in this case, so the first term is 5. Thus, the second must be 24.
    - In sum, we have showed that there are 24 elements conjugate to (12345) in S_5.
    - Another way we could show this is by counting all of the 5-cycles and knowing that they are all conjugate as 5-cycles. Indeed, there are $4! = 24$ 5-cycles.
  - Claim: In A_5, $|x| = 5$ implies $x \sim x$, $x \nsim x^2$, $x \nsim x^3$, and $x \sim x^4 = x^{-1}$.

    Proof. We know that $|x| = 5$. Thus, let $x = (abcde)$.

    By the above statements on $C_{S_5}((12345))$, we know that $C_{S_5}(x) \subset A_5$. Thus, by proposition 2, $gxg^{-1} = x'$ iff $g \in A_n$. Thus,

$$\begin{aligned}
exe^{-1} = x &\implies x \sim x \\
[(bc)(cd)(de)]x[(bc)(cd)(de)]^{-1} = (bced)(abcde)(bced)^{-1} = (acebd) &\implies x \nsim x^2 \\
(bdec)(abcde)(bdec)^{-1} = (adbec) &\implies x \nsim x^3 \\
[(be)(cd)](abcde)[(be)(cd)]^{-1} = (aedcb) &\implies x \sim x^4 = x^{-1}
\end{aligned}$$

    as desired. $\square$

  - $x^2 \sim x^3$ in A_5 as well.
  - $(abced)$ and $(acebd)$ are conjugate by $(bce) \in A_5$.
  - Six subgroups, all conjugate.
  - All of the subgroups are conjugate, but not all of the elements are conjugate?
- Consider $K = \{e, (12)(34), (13)(24), (14)(23)\} \triangleleft A_4 \subset A_5$.
- Consider a transitive group action from A_5 to $X = \{\text{cong of } K\}$.
- $\text{Stab}(K) = N_{A_5}(K) \supset A_4$.
- By O.S. trm, $X = |A_5|/|A_4| = 5$.
- Let $H \subset A_5$ have $|H| = 4$.
- We want to show that H fixes a point. Equivalently, we want to find $x \in \{1,2,3,4,5\}$ such that $|\operatorname{Orb}(x)| = 1$.
- Since $4 = |H| = |\operatorname{Orb}(x)| \cdot |\operatorname{Stab}(x)|$ and $5 \equiv 1 \mod 2$. Thus, there is a fixed point.
- Thus, there are 15 cyclic subgroups of order 4 like K, and they are all conjugate.
- $H \leq A_5$ has index d iff there is a transitive action and puts A_5/H. Induces a map from $A_5 \to S_d$?? As A_5 has no normal subgroups. If $d = 2, 3, 4, \ldots$?? If $d = 5$, then $A_5 \to S_5 \to S_5/A_5$. But really $A_5 \to S_5 \to S_5/A_5 \cong \mathbb{Z}/2\mathbb{Z}$.
- The hard ones are 6, 10, or 12.
- Consider a subgroup of A_5 of order 6. Must be $\mathbb{Z}/6\mathbb{Z}$ or S_3. These groups have subgroups of order 3. If we have this, it must be a subgroup of $S_3 \times S_2 \cap A_5$. Important: $\langle (1,2,3) \rangle$ and $(1,2)(4,5)$.
- Same analysis for subgroups of order 10. Subsets of order 1,2,5,10. (12) orbits include...
- Table with sets.
- If we spend a couple of hours understanding this example in complete detail, that will be very helpful for the final.

7.2 p-Groups

11/9:

- ***p*-group**: A finite group of order p^m, where p is prime and $m \geq 1$. *Denoted by* $\boldsymbol{P}$.
- Example: If $|P| = p$, then $P \cong \mathbb{Z}/p\mathbb{Z}$.
- **Fixed point** (of X under $G \circlearrowright X$): A point $x \in X$ for which $|\operatorname{Orb}(x)| = 1$.
- Proposition: Let $P \circlearrowright X$ where P is a p-group. Then the number of fixed points is congruent to $|X|$ mod p.

  Proof. Let $x \in X$ be arbitrary. By the Orbit-Stabilizer theorem,

  $$p^m = |P| = |\operatorname{Orb}(x)| \cdot |\operatorname{Stab}(x)|$$

  If x is a fixed point, then $|\operatorname{Orb}(x)| = 1$. However, if x is not a fixed point, then we have by the above that no nontrivial element has order less than p and hence $|\operatorname{Orb}(x)| \equiv 0 \mod p$.

  As we know,

  $$X = \bigsqcup \text{Orbits} = \{\text{Fixed points}\} \sqcup \{\text{Non-trivial orbits}\}$$

  Therefore, $|X|$ is equal to the number of fixed points plus the sum of the magnitudes of the other orbits. But since the magnitudes of the other orbits are all multiples of p as per the above, we have that $|X|$ is congruent to the number of fixed points mod p. The desired result readily follows. $\square$

- Corollary: If $|X| \not\equiv 0 \mod p$, then there exists at least one fixed point.
- **Center** (of G): The set of elements in G that commute with every element of G. *Denoted by* $\boldsymbol{Z(G)}$. *Given by*

$$Z(G) = \{g \in G \mid gx = xg \; \forall \; x \in G\}$$

- Proposition: Let P be a p-group, and $Z := Z(P)$ be the center of P. Then Z is a non-trivial normal subgroup.

  Proof. To prove that Z is normal, it will suffice to show that for all $x \in Z$ and $g \in G$, $gxg^{-1} \in Z$. Let $x \in Z$ and $g \in G$ be arbitrary. Then since $x \in Z$, $gx = xg$, i.e., $gxg^{-1} = x \in Z$, as desired.

  To prove that Z is non-trivial, we make use of the previous proposition. Let $P \circlearrowright P$ by conjugation. We first prove that $Z(P)$ is exactly the set of fixed points of P. If $x \in P$ is a fixed point, then $pxp^{-1} = x$ for all p, so $x \in Z(P)$. In the other direction, if $x \in Z(P)$ normal, then by the definition of the center, $pxp^{-1} = x$ for all $p \in P$. Thus, $|Z(P)|$ is equal to the number of fixed points of P, and hence $|Z(P)| \equiv |P| \mod p \equiv 0 \mod p$. Thus, we could have $|Z(P)| = 0$, but since $e \in Z(P)$, we must instead have $|Z(p)| \geq p$. Therefore, $Z(P)$ is nontrivial. $\square$

- We get from this proposition an outline for "classifying" p-groups. We will do this inductively on k. Here are the steps.
  1. Understand Abelian p-groups.
  2. Understand all p-groups of order $|p^k|$.
  3. Let $|P| = p^{k+1}$. Then by the above, $Z \triangleleft P$. If $Z = P$, use 1. If $Z \neq P$, then $|Z|$ and $|P/Z|$ divide p^k, so we can use 2.
- Goal: Knowing Z and G/Z, try to find all possible G.
- Classification for $k = 2$.
  1. Abelian groups. By Lagrange's theorem, there are two possibilities: There exists x with $|x| = p^2$, and there exists x with $|x| = p$.
     (a) G has an element of order p^2, and hence $G \cong \mathbb{Z}/p^2\mathbb{Z}$.
     (b) There exists $x \in G$ such that $|x| = p$. Let $y \in G \setminus \langle x \rangle$. Then $y^p = e$. Thus, $G = \langle x, y \rangle$. $x^p = e = y^p$ and $xy = yx$. Thus, $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.
  2. Suppose G is not abelian. Z still has a nontrivial center, though, and hence any proper nontrivial subgroup of G is necessarily isomorphic to $\mathbb{Z}/p\mathbb{Z}$ for the $k = 2$ case. Thus, the only possible pair $(Z, G/Z)$ is $(Z, G/Z) = (\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p\mathbb{Z})$. But then $G/Z \cong \mathbb{Z}/p\mathbb{Z}$ is cyclic, so by HW4 Q5, G is abelian, a contradiction. Therefore, $G \cong \mathbb{Z}/p^2\mathbb{Z}$ or $(\mathbb{Z}/p\mathbb{Z})^2$, hence abelian.
- (Partial) classification for $k = 3$.
  1. Abelian groups: $\mathbb{Z}/p^3\mathbb{Z}$, $\mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, and $(\mathbb{Z}/p\mathbb{Z})^3$.
  2. Possible pairs $(Z, G/Z)$:

$$(\mathbb{Z}_{p^2}, \mathbb{Z}_p)^\times \qquad (\mathbb{Z}_p, \mathbb{Z}_{p^2})^\times \qquad (\mathbb{Z}_p^2, \mathbb{Z}_p)^\times \qquad (\mathbb{Z}_p, \mathbb{Z}_p^2)^\times$$

  G/Z cyclic implies the same contradiction, so the only possibility is $Z = \mathbb{Z}_p$ and $G/Z = (\mathbb{Z}_p)^2$.
- Does the trend of no nonabelian groups continue for higher powers? No — for $|G| = 2^3 = 8$, both D_8 and Q (the Quaternion group) are nonabelian counterexamples.
  - Case 1: All elements in G have order 2.
    - G is abelian: If $x, y \in G$ are arbitrary, then

$$xy = xey = x(xy)^2y = xxyxyy = x^2yxy^2 = eyxe = yx$$

  - There are, of course, the other abelian groups as well. We now focus on the other case, and specifically its nonabelian forms.
  - Case 2: There exists $g \in G$ with $|g| = 4$.
    - $g^2 \neq e$.
    - We also assume that G is not abelian.
    - $[G : \langle g \rangle] = 2$, so $\langle g \rangle \lhd G$.
    - Let $h \in G \setminus \langle g \rangle$. If $|h| = 8$, then $G \cong \mathbb{Z}/8\mathbb{Z}$. But G is not abelian, so this cannot be the case.
    - Hence $|h| = 2$ or $|h| = 4$.
    - If $|h| = 4$, then $h^2 \notin \langle g \rangle$ implies $G/\langle g \rangle \cong \mathbb{Z}/2\mathbb{Z}$ (another abelian case we are not interested in). Similarly, $h^2 \in \langle g \rangle$ implies $h^2 = g^2$. Thus, either $h^2 = e$ or $h^2 = g^2$.
    - Since $\langle g \rangle \lhd G$, $hgh^{-1} \in \langle g \rangle$. It follows since the powers of hgh^{-1} are as distinct as the powers of g that $\langle g \rangle = \langle hgh^{-1} \rangle$. Thus, we either have $hgh^{-1} = g$ or $hgh^{-1} = g^{-1}$. In the first case, $hg = gh$, so $G = \langle g, h \rangle$ is abelian, and we are not interested.
    - If $g^4 = e = h^4$, then $G = Q$ and $hg = g^{-1}h$.
    - If $g^4 = e = h^2$, then $G = D_8$ and $hg = g^{-1}h$.

- We now investigate the case where p is odd and $G = p^3$. Let $Z = \mathbb{Z}/p\mathbb{Z}$ and $G/Z = (\mathbb{Z}/p\mathbb{Z})^2$.
  - Consider a surjection $G \twoheadrightarrow G/Z$. Choose $x \mapsto (1, 0)$ and $y \mapsto (0, 1)$.
  - Let $x^p, y^p, xyx^{-1}y^{-1} \in Z$.
  - If $xy = yx$, then $G = \langle x, y, Z \rangle$ is abelian.
  - Suppose $xy = yxz$ for some $z \in Z$ nontrivial.
  - Case 1: All $g \in G$ have order p. Then
$$G = \{y^b x^a z^c \mid 0 \leq a, b, c \leq p - 1\}$$
  - We have that
$$y^b x^a z^c (y^B x^A z^C) = y^b x^a y^B x^A z^{c+C} = y^{b+B} x^{a+A} z^{c+C+aB}$$
    since $xy = yxz$??
  - This gets into $\mathrm{GL}_3(\mathbb{F}_p)$, the group of 3×3 invertible matrices over the field of numbers 0 to p under addition mod p. In particular,
$$\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & A & C \\ 0 & 1 & B \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a + A & c + c + aB \\ 0 & 1 & b + B \\ 0 & 0 & 1 \end{pmatrix}$$

- p-groups and their orders for different values of p, m.

	p	p^2	p^3	p^4
2	1	2	$3+2$	14
3	1	2	$3+2$	15
5	1	2	$3+2$	15
7	1	2	$3+2$	15

Table 7.1: $|P|$ for various p, m values.

- Another perspective.
  - Consider $x^p = e = y^p$, $xy = yxz$, $z^p = e$, and $z \in Z(P)$.
  - Then
$$(xy)^p = y^p x^p z^{1+\cdots+p} = z^{p(p+1)/2}$$
  - If p is odd, then $z^{p(p+1)/2} = e$ implies $(xy)^p = e$ *except* when $p = 2$.

7.3 Sylow I-II

11/11:

- ***p*-Sylow**[1]: A subgroup $P \leq G$ of order $|P| = p^n$ for some prime p and $n \in \mathbb{N}$, where G is a finite group of order $|G| = p^n \cdot k$ for $\gcd(p,k) = 1$.
- Theorem (Sylow I — Existence): Let G be a finite group with order divisible by p. Then G has a p-Sylow subgroup.

  Proof. Let X be the set of all subsets (not subgroups!) of G of order p^n. Define $G \circlearrowright X$ by left multiplication. Then if $S = \{s_1, \dots, s_{p^n}\} \in X$, we have for instance that

  $$g \cdot S = gS = \{gs_1, \dots, gs_{p^n}\}$$

  We now investigate the properties of $\operatorname{Stab}(S)$; we will eventually prove that there exists an S for which $\operatorname{Stab}(S)$ is the desired p-Sylow. Let's begin.

  We will first show that $|\operatorname{Stab}(S)| \leq p^n$. Pick a $g \in \operatorname{Stab}(S)$. By definition $gs_1 \in S$, so $gs_1 = s_i$ for some $i = 1, \dots, p^n$. It follows that $g = s_i s_1^{-1}$. Thus, every element of $\operatorname{Stab}(S)$ is of the form $s_i s_1^{-1}$, so there are at most p^n elements in the set (one for each i).

  We now divide into two cases ($|\operatorname{Stab}(S)| = p^n$ for some S and $|\operatorname{Stab}(S)| < p^n$ for all S). In the former case, we may choose $P = \operatorname{Stab}(S)$ to be our p-Sylow, and we are done. In the latter case, we can derive a contradiction, meaning that the former case is always true. To do so, let $S \in X$ be arbitrary. Note that by the Orbit-Stabilizer theorem,

  $$|\operatorname{Stab}(S)| \cdot |\operatorname{Orb}(S)| = |G| = p^n \cdot k \equiv 0 \mod p^n$$

  Since $|\operatorname{Stab}(S)| < p^n$, we know that $|\operatorname{Stab}(S)| \not\equiv 0 \mod p^n$. It follows that the largest power of p dividing $|\operatorname{Stab}(S)|$ (which we will call m) is less than n (note that it is possible that $m = 0$). But since $|G|$ is divisible by p^n and $|\operatorname{Stab}(S)|$ is not, we have that

  $$|\operatorname{Orb}(S)| = \frac{|G|}{|\operatorname{Stab}(S)|} = \frac{p^n \cdot k}{p^m \cdots} = p^{n-m} \cdots$$

  i.e., that $|\operatorname{Orb}(S)|$ has at least one power of p in its prime factorization. This implies that $|\operatorname{Orb}(S)| \equiv 0 \mod p$. But since $|\operatorname{Orb}(S)|$ is divisible by p for all S, $|X|$ must be, too (why??). However,

  $$|X| = \binom{p^n k}{p^n} = \frac{(p^n k)!}{(p^n k - p^n)! p^n!} = \frac{(p^n k)(p^n k - 1) \cdots (p^n k - p^n + 1)}{(p^n)(p^n - 1) \cdots 1} = \frac{p^n k}{p^n} \cdots \frac{p^n k - (p^n - 1)}{p^n - (p^n - 1)}$$

  We show that every power of p in the numerator above cancels with one in the denominator. In fact, we can do this term-by-term. Consider $p^n k - i$ and $p^n - i$ for some $i = 0, \dots, p^n - 1$. Let p^j be the largest power of p dividing i. Note that since $i < p^n$, we must have $j < n$. Thus, p^j will divide $p^n k$ and p^n, too, and hence the differences $p^n k - i$ and $p^n - i$ as well. This implies the desired result. Therefore, since there are no "excess" powers of p in the numerator above, $|X|$ is *not* divisible by p, a contradiction. $\square$

- Example: Let $G = S_p$.
  - $|G| = p! = p \cdot k$.
  - Need to find a subgroup of order p.
  - $P = \langle (1, 2, \dots, p) \rangle$ is a p-Sylow of G.
- Example: Let $G = S_4$.
  - Pick $p = 2$ so that $|G| = 24 = 2^3 \cdot 3$.

[1] Sylow is pronounced "SIH-lohv."

  - Need to find a subgroup of order 8.
  - We can choose $D_8 \leq S_4$.

- Theorem (Sylow II — Uniqueness up to conjugation): Fix P a p-Sylow.
  1. If $Q \subset G$ is a p-Sylow, then $Q = gPg^{-1}$ for some $g \in G$.
  2. If $Q \subset G$ is a p-group, then $Q \subset gPg^{-1}$ for some $g \in G$.

Proof. Ask in office hours?? □