

Week 7

Group Action Applications: A_5 and the Sylow Theorems

7.1 Actions of A_5

- 11/7:
- Classifying subgroups of $G = A_5 \cong \text{Do}$.
 - Let $H \leq G$. We must have $|H| \mid |G|$ 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 $h x h^{-1} = x$ and $h \notin A_n$. Since $g, h \notin A_n$, we have that $gh \in A_n$. Additionally, we have that

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

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 $x \sim x, x \approx x^2, x \approx x^3$, 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,

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

as desired. \square

- $x^2 \sim x^3$ in A_5 as well.
- $(abcd)$ 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 $|\text{Orb}(x)| = 1$.
- Since $4 = |H| = |\text{Orb}(x)| \cdot |\text{Stab}(x)|$ and $5 \equiv 1 \pmod{2}$. 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 $A_5 \rightarrow S_d$?? As A_5 has no normal subgroups. If $d = 2, 3, 4, \dots$? If $d = 5$, then $A_5 \rightarrow S_5 \rightarrow S_5/A_5$. But really $A_5 \rightarrow S_5 \rightarrow S_5/A_5 \cong \mathbb{Z}/2\mathbb{Z}$.
- 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 Blog Post: Actions of the Dodecahedral Group

From Calegari (2022).

11/26:

- Recall that in HW2, we found a faithful action $\text{Do} \curvearrowright 5$ inscribed cubes. This yielded an injective homomorphism $\text{Do} \rightarrow S_5$ identifying Do with an order 60 subgroup. Moreover, this subgroup was necessarily A_5 since it is of order 60 and hence normal. Therefore,

$$\text{Do} \cong A_5$$

- Herein, we seek to classify all transitive actions of Do .
- **Equivalent** (group actions): Two group actions $G \curvearrowright X$ and $G \curvearrowright Y$ for which there exists a bijection $\phi : X \rightarrow Y$ satisfying

$$\phi(g \cdot x) = g \cdot \phi(x)$$

for all $g \in G$ and $x \in X$.

- Because of the following theorem, to classify all transitive actions of Do , it will actually only be necessary to classify the conjugacy classes of the subgroups of G !

- Theorem: The transitive actions of a group G up to equivalence are in bijection to the conjugacy classes of the subgroups of G .

Proof. To prove this claim, we will first define a map f from the set of transitive actions of G to the set of conjugacy classes of the subgroups of G , and a map g from the set of conjugacy classes of the subgroups of G to the set of transitive actions of G . We will then check that f, g are well-defined, and that $g = f^{-1}$. Let's begin.

Define...

1. f by the rule, "take X a set with a transitive action to the conjugacy class of $H = \text{Stab}(x)$ for some $x \in X$;"
2. g by the rule, "take the conjugacy class of $H \leq G$ to $G \curvearrowright X = G/H$ by left multiplication."

To prove that f is well-defined, it will suffice to show that if $G \curvearrowright X$ and $G \curvearrowright Y$ transitive are equivalent, then $H = \text{Stab}(x)$ for an arbitrary $x \in X$ and $H' = \text{Stab}(y)$ for an arbitrary $y \in Y$ satisfy $H = \sigma H' \sigma^{-1}$ for some $\sigma \in G$. Suppose $G \curvearrowright X$ and $G \curvearrowright Y$ transitive are equivalent. Then there exists a bijection $\phi : X \rightarrow Y$ which preserves the group action. Let $H = \text{Stab}(x)$ for some $x \in X$ arbitrary, and $H' = \text{Stab}(y)$ for some $y \in Y$ arbitrary. Since $G \curvearrowright Y$ is transitive, $\phi(x) = \sigma \cdot y$ for some $\sigma \in G$. We choose this σ to be our σ . To confirm that $H = \sigma H' \sigma^{-1}$, we will verify that $\sigma H' \sigma^{-1} \subset H$ and that $|\sigma H' \sigma^{-1}| = |H|$. Let $\sigma h' \sigma^{-1} \in \sigma H' \sigma^{-1}$ be arbitrary. Before we show that $\sigma h' \sigma^{-1} \cdot x = x$ (and hence $\sigma h' \sigma^{-1} \in \text{Stab}(x) = H$), we prove one preliminary result. Indeed, we can show that like ϕ , ϕ^{-1} also preserves the group action:

$$\begin{aligned} g \cdot \phi(x) &= \phi(g \cdot x) \\ \phi^{-1}(g \cdot y) &= \phi^{-1}(\phi(g \cdot \phi^{-1}(y))) \\ \phi^{-1}(g \cdot y) &= g \cdot \phi^{-1}(y) \end{aligned}$$

With this result, we have that

$$\begin{aligned} \sigma h' \sigma^{-1} \cdot x &= \sigma \cdot (h' \cdot (\sigma^{-1} \cdot x)) \\ &= \sigma \cdot (h' \cdot (\sigma^{-1} \cdot \phi^{-1}(\sigma \cdot y))) \\ &= \sigma \cdot (h' \cdot \phi^{-1}(\sigma^{-1} \cdot (\sigma \cdot y))) \\ &= \sigma \cdot (h' \cdot \phi^{-1}(y)) \\ &= \sigma \cdot \phi^{-1}(h' \cdot y) \\ &= \sigma \cdot \phi^{-1}(y) \\ &= \phi^{-1}(\sigma \cdot y) \\ &= x \end{aligned}$$

as desired. As to the second statement we wish to verify, since ϕ is a bijection, $|X| = |Y|$. Thus, by the Orbit-Stabilizer theorem and the transitivity of both group actions,

$$|H| = |\text{Stab}(x)| = \frac{|G|}{|\text{Orb}(x)|} = \frac{|G|}{|X|} = \frac{|G|}{|Y|} = \frac{|G|}{|\text{Orb}(y)|} = |\text{Stab}(y)| = |H'|$$

Since conjugate groups have the same order, $|H'| = |\sigma H' \sigma^{-1}|$. Therefore, by transitivity,

$$|H| = |\sigma H' \sigma^{-1}|$$

as desired.

To prove that g is well-defined, it will suffice to show that $H \leq G$ and $\sigma H \sigma^{-1} \leq G$ map to equivalent transitive group actions. First off, since all actions of a group on its quotient groups are transitive as per the previous lecture, we know that we are mapping subgroups to *transitive* group actions of G .

Additionally, let $X = G/H$ and $Y = G/\sigma H\sigma^{-1}$. To confirm that $G \curvearrowright X$ and $G \curvearrowright Y$ are *equivalent*, it will suffice to find a bijection $\phi : X \rightarrow Y$ that preserves the action. Define $\phi : X \rightarrow Y$ by

$$\phi(\gamma H) = (\gamma\sigma^{-1})\sigma H\sigma^{-1} = \gamma H\sigma^{-1}$$

To confirm that ϕ is well-defined, it will suffice to verify that $\phi(\gamma H) = \phi(\gamma h H)$ for all $\gamma \in G$, $h \in H$. Let $\gamma \in G$, $h \in H$ be arbitrary. Then

$$\phi(\gamma h H) = \gamma h H\sigma^{-1} = \gamma H\sigma^{-1} = \phi(\gamma H)$$

as desired. ϕ is naturally bijective since it takes as input γH for all $\gamma \in G$ (i.e., all cosets of H) and produces as output $(\gamma\sigma^{-1})\sigma H\sigma^{-1}$ (i.e., all cosets of $\sigma H\sigma^{-1}$ since all $\gamma\sigma^{-1}$'s are distinct by the Sudoku lemma). To confirm that ϕ preserves the group action, it will suffice to verify that $\phi(g \cdot \gamma H) = g \cdot \phi(\gamma H)$ for all $g \in G$ and $\gamma H \in X$. Let $g \in G$ and $\gamma H \in X$ be arbitrary. Then

$$\phi(g \cdot \gamma H) = \phi(g\gamma H) = g\gamma H\sigma^{-1} = g\gamma\sigma^{-1}\sigma H\sigma^{-1} = g \cdot \gamma\sigma^{-1}\sigma H\sigma^{-1} = g \cdot \phi(\gamma H)$$

as desired.

To prove that $g = f^{-1}$, it will suffice to show that $f \circ g$ is the identity on the set of conjugacy classes of the subgroups of G and $g \circ f$ is the identity on the set of transitive actions of G .

Tackling $f \circ g$: Let $H \leq G$ be arbitrary. Then g takes H to the action of G on G/H by left multiplication, and f takes G/H back to $\text{Stab}(\gamma H)$ for some $\gamma H \in G/H$. We now need only confirm that $\text{Stab}(\gamma H)$ is conjugate to H . But since $\text{Stab}(\gamma H) = \gamma H\gamma^{-1}$ by last lecture, we have the desired result.

Tackling $g \circ f$: Let X be an arbitrary set on which G acts transitively. Then f takes X to the conjugacy class of $H = \text{Stab}(x)$ for some $x \in X$, and g takes H back to the (transitive) action of G on G/H by left multiplication. To prove that these two actions are equivalent, it will suffice to find a bijection $\phi : G/H \rightarrow X$ that preserves the action. Define $\phi : G/H \rightarrow X$ by

$$\phi(gH) = g \cdot x$$

where x is the same element of X used to define H . To confirm that ϕ is well-defined, it will suffice to verify that $\phi(gH) = \phi(ghH)$ for all $g \in G$, $h \in H$. Let $g \in G$, $h \in H$ be arbitrary. But since $h \in \text{Stab}(x)$, we have that

$$\phi(ghH) = gh \cdot x = g \cdot (h \cdot x) = g \cdot x = \phi(gH)$$

as desired. To confirm that ϕ is bijective, it will suffice to verify that ϕ is injective and surjective. For injectivity, we have that

$$\begin{aligned}\phi(gH) &= \phi(g'H) \\ g \cdot x &= g' \cdot x\end{aligned}$$

so $g^{-1}g' \in \text{Stab}(x) = H$. But this implies that $g' = gh$ for some $h \in H$, meaning that

$$g'H = ghH = gH$$

as desired. For surjectivity, since $G \curvearrowright X$ is transitive, there exists $g \in G$ for which $g \cdot x = x'$ for all $x' \in X$. Therefore, for any $x' \in X$, $gH \in G/H$ satisfies

$$\phi(gH) = g \cdot x = x'$$

as desired. To confirm that ϕ preserves the group action, it will suffice to verify that $\phi(\gamma \cdot gH) = \gamma \cdot \phi(gH)$ for all $\gamma \in G$ and $gH \in G/H$. Let $\gamma \in G$ and $gH \in G/H$ be arbitrary. Then

$$\phi(\gamma \cdot gH) = \phi(\gamma gH) = \gamma g \cdot x = \gamma \cdot (g \cdot x) = \gamma \cdot \phi(gH)$$

as desired. □

- Calegari reviews the isomorphism between $D_5 \cong I_c$.
- Subgroups of A_5 with distinct conjugacy classes.
 1. The trivial subgroup.
 2. The cyclic group $\langle (12)(34) \rangle$ of order 2.
 3. The cyclic group $\langle (123) \rangle$ of order 3.
 4. The Klein 4-group $\langle (12)(34), (13)(24), (14)(23) \rangle$ of order 4.
 5. The cyclic group $\langle (12345) \rangle$ of order 5.
 6. The group $\langle (123), (23)(45) \rangle \cong S_3 \cong D_6$ of order 6.
 7. The dihedral group $D_{10} = \langle (12345), (25)(34) \rangle$ of order 10.
 8. The group $A_4 = \langle (123), (124) \rangle$ of order 12.
 9. The group A_5 of order 60.
- Notes on the above.
 - These are actually *all* of the subgroups of A_5 .
 - All of the above subgroups have different orders. Thus, there is a unique equivalence class of transitive actions on this group for a given set X with

$$|X| = 60, 30, 20, 15, 12, 10, 6, 5, 1$$

- Since A_5 has no non-trivial normal subgroups to act as kernels, all actions save the final one below will be faithful.
- Actions of the dodecahedral group:
 1. The action on the “one” dodecahedron.
 2. The action on the five inscribed cubes.
 3. The action on the six pairs of opposite faces of the dodecahedron.
 - (a) Equivalently, the action on the six pairs of opposite diagonals of the icosahedron.
 4. The action on the ten pairs of opposite vertices of the dodecahedron.
 - (a) Equivalently, the action on the ten pairs of opposite faces of the icosahedron.
 5. The action on the twelve faces of the dodecahedron.
 - (a) Equivalently, the action on the twelve vertices of the icosahedron.
 6. The action on the fifteen pairs of opposite edges of the dodecahedron.
 - (a) Equivalently, the action on the fifteen pairs of opposite edges of the icosahedron.
 7. The action on the twenty vertices of the dodecahedron.
 - (a) Equivalently, the action on the twenty faces of the icosahedron.
 8. The action on the thirty edges of the dodecahedron.
 - Equivalently, the action on the thirty edges of the icosahedron.
 9. The action of the group on itself by left multiplication.

7.3 p -Groups

- 11/9:
- **p -group**: A finite group of order p^m , where p is prime and $m \geq 1$. Denoted by P .
 - Example: If $|P| = p$, then $P \cong \mathbb{Z}/p\mathbb{Z}$.
 - **Fixed point** (of X under $G \curvearrowright X$): A point $x \in X$ for which $|\text{Orb}(x)| = 1$.
 - Proposition: Let $P \curvearrowright X$ where P is a p -group. Then the number of fixed points is congruent to $|X| \pmod{p}$.

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

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

If x is a fixed point, then $|\text{Orb}(x)| = 1$. 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 $|\text{Orb}(x)| \equiv 0 \pmod{p}$.

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 $|X| \not\equiv 0 \pmod{p}$, 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 $Z(G)$. 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 $P \curvearrowright P$ 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 $|Z(P)| \equiv |P| \pmod{p} \equiv 0 \pmod{p}$. 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 $(Z, G/Z)$:

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

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

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

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

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 $\langle g \rangle \triangleleft G$.
 - 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 $\langle g \rangle \triangleleft G$, $hgh^{-1} \in \langle g \rangle$. 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 $\text{GL}_3(\mathbb{F}_p)$, 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

$$(xy)^p = y^p x^p z^{1+\dots+p} = z^{p(p+1)/2}$$

- If p is odd, then $z^{p(p+1)/2} = e$ implies $(xy)^p = e$ *except* when $p = 2$.

7.4 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 $G \curvearrowright X$ 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 $\text{Stab}(S)$; we will eventually prove that there exists an S for which $\text{Stab}(S)$ is the desired p -Sylow. Let's begin.

We will first show that $|\text{Stab}(S)| \leq p^n$. Pick a $g \in \text{Stab}(S)$. 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 $\text{Stab}(S)$ 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 ($|\text{Stab}(S)| = p^n$ for some S and $|\text{Stab}(S)| < p^n$ for all S). In the former case, we may choose $P = \text{Stab}(S)$ 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,

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

¹Sylow is pronounced "SIH-lohv."

Since $|\text{Stab}(S)| < p^n$, we know that $|\text{Stab}(S)| \not\equiv 0 \pmod{p^n}$. It follows that the largest power of p dividing $|\text{Stab}(S)|$ (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 $|\text{Stab}(S)|$ is not, we have that

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

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

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

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 $|G| = 24 = 2^3 \cdot 3$.
 - 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?? \square