Week 6

Fundamentals of Group Actions

6.1 Examples of Group Actions

10/31:

- Today: A number of interesting group actions.
- **Left action** (of G on X): A group action of the form $g \cdot x$ (as opposed to $x \cdot g$).
- Let G be a group, and let $X = G$. Take $g \cdot x = gx$.
  - Axiom confirmation.
    1. $e \cdot x = ex = x$.
    2. $g \cdot (h \cdot x) = ghx = gh \cdot x$.
  - Let $e \in X$. Then $\text{Orb}(e) = X$. In particular, this means that the action is transitive.
  - $\text{Stab}(x) = \{g \in G \mid gx = x\} = \{e\}$ for $x \in X$ arbitrary, in general.
  - $\ker = \{e\}$. This also follows from the above. Thus, the action is faithful.
- Corollary: Let G be a finite group. Then G is isomorphic to a subgroup of S_n for some n. We may take $n = |G|$.
  - Construction: We invoke the proposition from last lecture. In particular, we know that the action $G \circlearrowright G$ implies the existence of a homomorphism $\phi : G \to S_G$ defined by $g \mapsto \psi_g$.
  - The map in the above construction has trivial kernel. By the FIT, $G/\ker \cong \operatorname{im}\phi$. Combining these results, we obtain $G \cong G/\ker \cong \operatorname{im}\phi \leq S_n$.
  - Applying this construction to S_3, we deduce that $S_3 \leq S_6$.
- $\text{SO}(2) \cong \mathbb{R}/\mathbb{Z} \cong \mathbb{Q}/\mathbb{Z} \oplus \mathbb{Q}^\infty$.
  - In infinite cases, you usually want to consider some other topological things that disappear in the finite case.
- Let G be a group and take $X = G$ again. We can also consider $g \cdot x = gxg^{-1}$.
  - Axioms.
    1. $e \cdot x = exe^{-1} = x$.
    2. $g \cdot (h \cdot x) = ghxh^{-1}g^{-1} = (gh)x(gh)^{-1} = gh \cdot x$.
  - $\text{Orb}(e) = \{e\}$; not transitive if $|G| > 1$.
  - Let $x \in X$. Then $\text{Orb}(x)$ is the conjugacy class of x.
  - $\text{Stab}(x) = C_G(x)$.
  - $\ker = Z(G)$. Thus, the group action is faithful iff the center is trivial. Abelian implies not faithful.

- A nice thing about these constructions is that they cast other constructions we've encountered in the more general language of group actions.
- **Right actions** are even nastier than left cosets and right cosets, so Calegari will not mention them again.
  - $g \cdot x = x \cdot g^{-1}$ and $g \cdot (h \cdot x) = (x \cdot h^{-1}) \cdot g^{-1}$.
- Let $G = G$, X be the subgroups of G. $g \cdot H = gHg^{-1}$.
  - Note that $H \leq G$ does indeed imply that $gHg^{-1} \leq G$. In particular, ...
    - H is nonempty (contains at least e), so $gHg^{-1} \supset \{geg^{-1}\}$ is nonempty;
    - $gh_1g^{-1}, gh_2g^{-1} \in gHg^{-1}$ imply that $gh_1g^{-1}gh_2g^{-1} = g(h_1h_2)g^{-1} \in gHg^{-1}$;
    - $ghg^{-1} \in gHg^{-1}$ has inverse $gh^{-1}g^{-1} \in gHg^{-1}$.
  - Axioms (entirely analogous to the last example).
  - $\text{Orb}(H)$ is the "conjugates" of H.
  - $\text{Stab}(H) = N_G(H)$.
  - ker $=$?. We know that $Z(G) \subset$ ker. The conclusion is that there is not a nice definition for the kernel other than the intersections of the stabilizers/normalizers.
    - ...
    - If any $H \triangleleft G$ is normal, and $x \in G$ had order 2, then $\langle x \rangle \triangleleft G$, meaning that $gxg^{-1} \in \langle x \rangle$, i.e., $x \in Z(G)$, so this rules out D_8??
- Fix G and $H \leq G$. Let $X = G/H$ (not assuming $H \triangleleft G$, so we know that G/H is the set of left cosets but it is not a group in general). Define $g \cdot xH = gxH$.
  - We have $g \cdot xhH = gxhH$.
  - Orbit: $\text{Orb}(eH) = X$.
  - Stabilizer: $\text{Stab}(eH) = H$.
    - $\text{Stab}(gH) = gHg^{-1}$.
    - This is because $(ghg^{-1})gH = ghH = gH$.
    - Go to the more general case $G \circlearrowright X$, $\text{Stab}(x) = H$. Then $gHg^{-1} \subset \text{Stab}(g \cdot x)$??
  - Transitive: Yes (see orbits).
  - Faithful: If H is normal, no. If H contains a normal subgroup, no. Maybe yes.
  - Kernel: If H is normal, then ker $= H$. In general, ker $= \bigcap_{g \in G} gHg^{-1}$ (the largest normal subgroup of H).
- Takeaway: General constructions allow us to see things we've already done.
- Next time: The most useful theorem of the course, that provides lots of information on relations between objects.

6.2 Orbit-Stabilizer Theorem

11/2:

- We will have a take-home open-book final. Should take you a couple hours or a little more to do, but we'll have more time than that. Don't Google answers or collaborate. We'll have more practice problems (and 50% of the exam will be on that sheet); if we do every problem on the sheet, we'll certainly get an A.
- We will cover all theoretical material by Thanksgiving and then spend the rest of the time exploring applications.
- Today: The most fundamental theorem of the class.

- Let G be a group acting on a set X.
- Theorem (Orbit-Stabilizer Theorem): Let $x \in X$ be arbitrary. Then

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

Proof. We will break up G and count it in two different ways. Let $x \in X$ be arbitrary and consider $\operatorname{Orb}(x)$. By definition, $\operatorname{Orb}(x)$ is the set of all y such that $g \cdot x = y$ for some $g \in G$. Equivalently, every $g \in G$ maps x to some $y \in \operatorname{Orb}(x)$. Thus, we can partition G into sets of g that map x to a particular y, knowing that every g must send it to some y. Symbolically,

$$G = \bigsqcup_{y \in \operatorname{Orb}(x)} \{g \mid g \cdot x = y\}$$

Each of the sets over which we sum above is equal to $g \cdot \operatorname{Stab}(x)$ (the left coset of the stabilizer by g). Thus, for each $y \in \operatorname{Orb}(x)$, we contribute $|g \cdot \operatorname{Stab}(x)|$ to $|G|$. Symbolically,

$$|G| = \sum_{\operatorname{Orb}(x)} |g \cdot \operatorname{Stab}(x)| = \sum_{\operatorname{Orb}(x)} |\operatorname{Stab}(x)| = |\operatorname{Orb}(x)| \cdot |\operatorname{Stab}(x)|$$

as desired. □

- Examples:
  - Let $H \leq G$, $X = G/H$. Then G acts on X by left multiplication. Taking $x = H$ in particular, we have that

    $$|G| = |G/H| \cdot |H|$$

    and we recover Lagrange's theorem as a special case of the O-S theorem.
  - $G = S_n$, $X = [n]$.
    - Then $S_n = \{\sigma(1) = 1\} \cup \{\sigma(1) = 2\} \cup \cdots \cup \{\sigma(1) = n\}$. This is analogous to the proof strategy decomposition.
  - G acts on G by conjugation.
    - Take $g \in G$. Then $\operatorname{Orb}(g) = \{g\}$, i.e., the conjugacy class of g, and $\operatorname{Stab}(g) = C_G(g)$. Therefore, we have the below corollary.
  - $G = S_n$.
    - Let $g = (1, \dots, k)$ for $2 \leq k \leq n$. Recall that $|\{g\}| = n!/(n-k)!k$. Thus, $|C_{S_n}(g)| = (n-k)! \cdot k$.
    - Alternatively, we can derive the order of this centralizer directly: $C_{S_n}(g) = \langle g \rangle \times S_{n-k}$, i.e., all powers of the k-cycle and everything that's disjoint. $\times$ denotes the direct product.
  - $G = S_4$, $g = (12)(34)$.
    - $|\{g\}| = 3$, so $|C_G(g)| = 8$.
    - Here $C_G(g) = D_8$. Visualize a square with vertices clockwise (1,4,2,3).
  - $G = S_6$, $g = (16)(25)(34)$.
    - We have that $|\{g\}| = 6!/2^3 \cdot 3! = 15$, so $|C_{S_6}(g)| = 48$. The centralizer is the set of all elements satisfying $\sigma(i) + \sigma(7 - i) = 7$.
    - Moreover, there is an injective homomorphism from $\widetilde{\text{Cu}} \hookrightarrow S_6$ whose image is exactly the centralizer of (16)(25)(34). Moreover, it follows that $C_{S_6}(g) \cong S_4 \times S_2$.
    - Let $h = (16)$. Then $|\{h\}| = |\{g\}| = 15$. Does there exist an automorphism of S_6 to S_6 which sends $h \to g$? No: $S_2 \times S_4 \cong C_{S_6}(h)$ and $C_{S_6}(g) \cong S_2 \times S_4$.
- Corollary: We have that

$$|G| = |\{g\}| \cdot |C_G(g)|$$

- $\widetilde{\textbf{Cu}}$: The set of all orthogonal symmetries of the cube (i.e., including reflections).
  - There is an isomorphism between $\text{Cu} \times \mathbb{Z}/2\mathbb{Z}$ and $\widetilde{\text{Cu}}$ defined by $(g, 1) \mapsto g$ and $(g, -1) \mapsto -g$. The reverse function is $g \mapsto (g \cdot \deg g, \deg g)$.
  - $\widetilde{\text{Cu}}$ acts on 6 faces.
- The pace will be this fast through Thanksgiving.

6.3 Blog Post: The Orbit-Stabilizer Theorem, Cayley's Theorem

From Calegari (2022).

11/13:
- Lemma: Let $G \circlearrowright X$ and let $x \in X$. Let $y \in \text{Orb}(x)$, i.e., let there exist $\sigma \in G$ such that $y = \sigma \cdot x$. Then
  1. $\text{Stab}(y) = \sigma \cdot \text{Stab}(x) \cdot \sigma^{-1}$.

     Proof. Let $H := \text{Stab}(x)$. We use a bidirectional inclusion argument.
     Suppose first that $\sigma h \sigma^{-1} \in \sigma H \sigma^{-1}$. Then

     $$\sigma h \sigma^{-1} \cdot y = \sigma h \cdot (\sigma^{-1} \cdot y) = \sigma h \cdot x = \sigma \cdot (h \cdot x) = \sigma \cdot x = y$$

     so $\sigma h \sigma^{-1} \in \text{Stab}(y)$, as desired.
     Now suppose that $g \in \text{Stab}(y)$. An analogous argument to the above shows that $\sigma^{-1} g \sigma \in \text{Stab}(x)$, so $g = \sigma h \sigma^{-1} \in \sigma H \sigma^{-1}$, as desired. □

  2. The set of elements $g \in G$ such that $g \cdot x = y$ is exactly the coset $\sigma \cdot \text{Stab}(x)$.

     Proof. As before, let $H := \text{Stab}(x)$ and proceed via a bidirectional inclusion argument.
     Suppose first that $\sigma h \in \sigma H$. Then

     $$\sigma h \cdot x = \sigma \cdot (h \cdot x) = \sigma \cdot x = y$$

     so σh is in the first set, as desired.
     Now suppose that $g \cdot x = y$. Since $\sigma \cdot x = y$ as well by hypothesis, it follows by transitivity that

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

     This implies that $\sigma^{-1} g \in H$, i.e., that $g \in \sigma H$, as desired. □
- This lemma further justifies the following step we took when proving the Orbit-Stabilizer Theorem in class: Equating each $\{g \mid g \cdot x = y\} = \sigma \, \text{Stab}(x)$.
- Further comments on $G \circlearrowright G/H$ (H a subgroup).
  - Why the action is well-defined.
    - $g \cdot xhH = gxhH = gxH = g \cdot xH$.
    - What saves the day here is that we're combining an unambiguous term (g) with our ambiguous term (xH) instead of trying to combine two ambiguous terms (e.g., xH and yH).
  - An example where the action is faithful.
    - Let $G = S_n$ and $H = \{\sigma \mid \sigma(1) = 1\} \cong S_{n-1}$.
    - Note that if $\sigma \in H$, then $(1, k)\sigma(1, k)^{-1}$ sends $\sigma(k) = k$.

  - Thus,
    $$\ker = \bigcap_{g\in G} gHg^{-1} \subset \bigcap_{k=1,\dots,n}(1,k)H(1,k)^{-1} = \{e\}$$
    so the action is faithful, here.
- When $H = \{e\}$, $G \circlearrowright G/H$ is entirely analogous to left multiplication within the group: $g\cdot x = gx$.

- Lemma: $G \circlearrowright G$ by left multiplication is faithful.

  Proof. To prove this result, we will actually prove the stronger result that $\text{Stab}(x) = \{e\}$ for all $x \in G$, from which it will follow that $\ker = \bigcap_{x\in G}\text{Stab}(x) = \{e\}$. We have this stronger result by the cancellation lemma since
  $$\begin{aligned} g\cdot x &= x \\ gx &= ex \\ g &= e \end{aligned}$$
  for all $g \in \text{Stab}(x)$. $\square$

- Corollary (Cayley's Theorem): If $|G| = n$, then $G \leq S_n$.

  Proof. From the construction $G \circlearrowright G$ via left multiplication, we get a homomorphism $\phi : G \to S_G$ as per the Proposition in Lecture 5.2. Since this action is faithful (by the lemma), this homomorphism is an injection. This implies that $G \cong \operatorname{im}\phi \leq S_G \cong S_n$, as desired. $\square$

- Implication: Even without knowing anything about G, we can get useful information by considering its actions on a set.

- More on $G \circlearrowright G$ by conjugation.
  - Since $|G| = |\{g\}| \cdot |C_G(g)|$, we can calculate the orders of centralizers. From the order, we can often get even more specific information.
  - Consider $G = S_n$.
    - If $g = (1, 2, \dots, n)$, then $|\{g\}| = (n-1)!$ and $C_G(g) = n!/(n-1)! = n$. This combined with the fact that g commutes with g implies that
      $$C_{S_n}((1,2,\dots,n)) = \langle(1,2,\dots,n)\rangle$$
    - If $g = (1, 2, \dots, k)$, then $|\{g\}| = n!/k(n-k)!$ so $|C_{S_n}(g)| = k\cdot(n-k)!$. Naturally, $g \in C_{S_n}(g)$, but so are all elements which fix $1, 2, \dots, k$ and shuffle $k+1, k+2, \dots, n$. Thus,
      $$C_{S_n}((1,2,\dots,k)) = \mathbb{Z}/k\mathbb{Z} \times S_{n-k}$$
    - Let g have cycle shape corresponding to the partition $a_1n_1 + a_2n_2 + \cdots$ where $n_1 > n_2 > \cdots$ denote cycle lengths and the a_i denote the corresponding multiplicity. We can deduce that the centralizer has order $\prod n_i^{a_i}a_i!$.
      It follows from the fact that disjoint cycles commute that g commutes with each component cycle, i.e., if $g = \cdots(a_1,\dots,a_k)\cdots$, then g and $(a_1,\dots,a_k)$ commute. g therefore also commutes with all powers of each component cycle. Going even further, g commutes with all products of all powers of each component cycle, i.e., if $g = (a_1,\dots,a_k)(b_1,\dots,b_\ell)(c_1,c_2,\dots)\cdots$, then
      $$C_{S_n}(g) \supset \langle(a_1,\dots,a_k),(b_1,\dots,b_\ell),(c_1,c_2,\dots),\dots\rangle$$
      The group on the right above is isomorphic to $\prod(\mathbb{Z}/n_i\mathbb{Z})^{a_i}$ and thus has order $\prod n_i^{a_i}$.
      What are the other elements in the centralizer that account for the $\prod a_i!$ term?? Is it the products of the powers of the cycles??

  - How many elements $g \in G$ make $g \cdot x = y$ true?
    - Equivalent to asking how many $g \in G$ make $gxg^{-1} = y$.
    - Relating to before, this will be a coset of the centralizer (we need a particular solution, and then we can compose it with all homogeneous solutions).

- More on $G \circlearrowright X$ (X is the set of subsets of G).
  - Let H be a subgroup. Since $\text{Orb}(H)$ is the conjugates of H and $\text{Stab}(H) = N_G(H)$, we have by the Orbit-Stabilizer Theorem that the number of subgroups of G conjugate to H is equal to $|G|/|N_G(H)| = [G : N_G(H)]$.

6.4 Group Actions on the Quotient Group

11/4:

- Let $G \supset H$ and $X = G/H$. Consider a group action $G \circlearrowright X$ defined by $g \cdot xH = gxH$ that is transitive.
- Recall that $xH = yH$ iff $x = yh$ for some $h \in H$ iff $y^{-1}x \in H$.
- Example: Consider $G = S_4$ and $H = D_8 = \langle (1234), (13) \rangle$.
- Let $A = H$, $B = (123)H$, $C = (123)^2 H$ be the three elements of $X = G/H = S_4/D_8$.
- We define a homomorphism $\phi : S_4 \to S_X = S_{\{A,B,C\}}$ by

$$\phi(\sigma) = \begin{cases} A & \mapsto \sigma A \\ B & \mapsto \sigma B \\ C & \mapsto \sigma C \end{cases}$$

  - Example: $\phi(123) = (ABC)$.
  - Example: $\phi(1234)$ is the element of $S_{\{A,B,C\}}$ that sends $A \mapsto (1234)H = H = A$, $B \mapsto (1234)(123)H = (1324)H = C$, and $C \mapsto (1234)(132)H = (14)H = B$. Thus, $\phi(1234) = (BC)$.
  - Let $x = (14)$ and $y = (123)$. Then $y^{-1}x = (321)(14) = (1432) = (1234)^{-1} \in H$, so $xH = yH$.

- Investigating $\ker \phi$.
  - $\phi((13)(24)) = (BC)^2 = e$. Thus, $(13)(24) \in \ker$ and it follows that everything conjugate to it is as well.
  - By the FIT, $S_4/\ker\phi \cong S_3$ so $|\ker\phi| = 4$.
  - Thus, $\ker\phi = \{e, (12)(34), (13)(24), (14)(23)\}$.

- Investigating the stabilizers on X.
  - $\text{Stab}(A) = H$.
    - Naturally, every $h \in H$ makes $hH = H$.
  - $\text{Stab}(B) = \text{Stab}((123)H) = (123)H(123)^{-1}$.
    - This is because any $(123)h(123)^{-1} \in (123)H(123)^{-1}$ makes

$$(123)h(123)^{-1}(123)H = (123)hH = (123)H$$

  - It follows by similar logic that $\text{Stab}(C) = (132)H(132)^{-1}$.

- Is something about H special in determining this action?
  - Suppose you take $H' = (123)H(123)^{-1}$. Is $G \circlearrowright G/H'$ the same action? The cosets of H' are $(123)H'$ and $(132)H'$. Let $A' = (132)H'$, $B' = H'$, and $C' = (123)H'$.

  - It follows that $A' = (132)(123)H(123)^{-1} = A(123)^{-1}$, $B' = (123)H(123)^{-1} = B(123)^{-1}$ and $C' = (123)(123)H(123)^{-1} = C(123)^{-1}$.
  - Conclusion: Take H, gHg^{-1}. Let A be a left coset of H. Then Ag^{-1} is a left coset of gHg^{-1}.
  - First, a coset (like A) is the set of all elements that send x to y.
  - Suppose $g \cdot x = z$. Then the coset is Ag^{-1}??
- Take G and $H = \{e\}$, $G \circlearrowright G$ the left matrices??
- Another example: Let $G = S_3 = \{e, (123), (123)^2, (12), (12)(123), (12)(123)^2\}$.
- Again, we can define a homomorphism $\phi : G \to S_G$. Call the above elements of S_3 A-F, respectively, as listed above.
  - Example: $\phi(123) = (ABC)(DFE)$.
  - Example: $\phi(12) = (AD)(BE)(CF)$.
- Let $|g| = k$, e.g., $g^{k=1}$ is distinct.
  - x, gx and $g^{k-1}x$ all distinct.
  - The cycle class of $\phi(g)$ is all k-cycles where $k = |g|\,\big|\,|G|$.
  - The remark here is that if $|g| = k$, not only are $e, \dots, g^{k-1}$ distinct, but $x, \dots, g^{k-1}x$ are distinct.
- Exotic automorphism of S_6.
- Take S_5, and let X be the set of subgroups of S_5 of order 5. We may also call this the subgroups generated by 5-cycles.
- Let S_5 act on X by conjugation.
- The action is transitive.
- $|X| = 24/4 = 6$.
  - There are $\binom{5}{5}(5-1)! = 24$ elements of order 5, i.e., 5-cycles in S_5.
  - Each subgroup of S_5 of order 5 contains 4 distinct 5-cycles and e.
  - These remarks imply the above result.
- Therefore, we get a map $\phi : S_5 \to S_X$.
- Take $P = \langle (12345) \rangle$.
  - We have
$$\text{Stab}(P) = \{g \in G \mid g \cdot P = P\} = \{g \in G \mid gPg^{-1} = P\} = N_{S_5}(P)$$
  - Since the action is transitive, $\text{Orb}(P) = X$. Thus, by the Orbit-Stabilizer theorem,
$$|N_{S_5}(P)| = \frac{|G|}{|X|} = \frac{120}{6} = 20$$
- $\ker\phi = \{\{e\}, A_5, S_5\}$.
- By the FIT, $\{S_5, \mathbb{Z}/2\mathbb{Z}, e\}$. We can't have order ?? so we eliminate e, we can't have order 5 so we eliminate $\mathbb{Z}/2\mathbb{Z}$. Thus, the only thing is S_5. It's doing too many interesting things to have such a small image.
- We obtain an injective map from S_5 to S_6. Why do it in such a strange way? Because it also has the property that its image acts transitively on six points.

- Remark: You can restrict to $A_5 \to S_6$, and we've seen this before where $A_5 \cong$ Do and S_6 is the pairs of opposite faces.

- So what we say is that we have an **exotic** subgroup S_5 inside S_6.
- Let's call S_5, H now. $[S_6 : H] = 6$. Thus, we have $S_6 \circlearrowright S_6/H$ by left multiplication. This action is transitive. $\mathrm{Stab}(H) = H$.
- $\psi : S_6 \to S_{S_6/H}$.
- $\ker\psi = \{1, A_6, S_6\}$, $\mathrm{im}\,\psi = \{S_6, \mathbb{Z}/2\mathbb{Z}, e\}$ where we know once again that the latter two can't happen.
- So we get $\psi : S_6 \to S_{S_6/H} \cong S_6$ is exotic??
  - H under this map maps to a boring S_5.
  - We know that we're sending a whole bunch of shit around (see picture).
- There will be a blog post on all of this nonsense.
- Future: Groups of order 5, groups of prime order, the Sylow theorems, and simple groups.

6.5 Blog Post: Actions of Symmetric Groups and Aut(S_6)

From Calegari (2022).

11/13:
- Lemma: $G \circlearrowright X$ is transitive iff G has a subgroup of index $n = |X|$.

  Proof. Suppose first that G acts transitively on some set X. Pick an $x \in X$ — we will prove that $H = \mathrm{Stab}(x)$ is the desired subgroup of index n. We know H is a subgroup since it's a stabilizer. Additionally, it has index n since by the Orbit-Stabilizer Theorem and the transitivity of $G \circlearrowright X$, we have that
  $$[G : H] = |G|/|H| = |\operatorname{Orb}(x)| = |X| = n$$
  Now suppose that G has a subgroup H of index n. Choosing $X = G/H$, we have that $G \circlearrowright X$ is transitive. ☐

- S_n canonically acts on $[n]$, but it can act on other sets as well.
- Lemma: If S_n acts transitively on a set X of size m, then one of the following holds.
  1. $m = 1$.
  2. $m = 2$ and $\mathrm{Stab}(x) = \mathrm{Stab}(y) = A_n$, where x, y are the 2 elements of X.
  3. $n = 4$ and $m = 3$ or $m = 6$.
  4. $m \geq n$ and the action of S_n is faithful, that is, the map $S_n \to S_m$ is injective.

  Proof. By the Proposition from Lecture 5.2, $S_n \circlearrowright X$ corresponds to a homomorphism $\phi : S_n \to S_m$. By the Lemma from Lecture 4.1, $\ker\phi \triangleleft S_n$. Additionally, since $\mathrm{im}\,\phi$ acts transitively on X, $|\mathrm{im}\,\phi| \geq m$. We now divide into cases.

  If $\ker\phi = S_n$, then all S_n can do is fix elements. Thus, if it is to move every element in X to every other element in X, we must have only one element in X, i.e., $m = 1$. An alternate way of proving this would be by noting that $\ker\phi = S_n$ implies $\mathrm{Stab}(x) = S_n$ for all $x \in X$, implying by the Orbit-Stabilizer Theorem and transitivity that
  $$1 = |S_n|/|S_n| = |\operatorname{Orb}(x)| = |X| = m$$

If $\ker\phi = A_n$, then we must have

$$2 = |S_n|/|A_n| = |\operatorname{Orb}(x)| = |X| = m$$

As to the other part of the proof, we know that $\operatorname{Stab}(x) \supset \ker\phi = A_n$. However, since $\operatorname{Stab}(x)$ is a subgroup, the only subgroup of S_n larger than A_n is S_n itself, and there exists $\sigma \in S_n$ that takes $\sigma \cdot x = y$ (i.e., $\sigma \notin \operatorname{Stab}(x)$), we know that $\operatorname{Stab}(x) = A_n$, as desired. An analogous result holds for $\operatorname{Stab}(y)$.

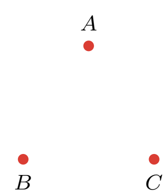
If $n = 4$ and $\ker\phi = K$, then we can think of some of the 24 elements of S_4 acting on X to shuffle things around differently, but many of the elements doing the same thing. In particular, if we want to look at just the distinct actions, it is probably better to take the perspective of each coset in S_4/K acting on X. But $S_4/K \cong \operatorname{im}\phi \cong S_3$, so what we really have here is a case of S_3 acting transitively on some number of elements. By the Orbit-Stabilizer Theorem,

$$6 = |S_3| = |\operatorname{Orb}(x)| \cdot |\operatorname{Stab}(x)| = |X| \cdot |\operatorname{Stab}(x)| = m \cdot |\operatorname{Stab}(x)|$$

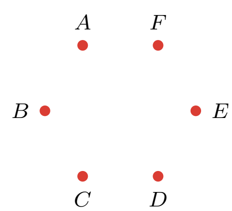
Thus, m must divide 6. It follows that $m = 1, 2, 3, 6$. The cases where $m = 1, 2$ have already been dealt with, so the only new cases worth mentioning additionally here are $m = 3, 6$. For some more intuition here, recall that

$$S_3 = \{e, (123), (132), (12), (13), (23)\}$$

and picture Figure 6.1.



(a) Three points.



(b) Six points.

Figure 6.1: Transitive actions of S_3.

The transitive action of S_3 on three points is, respectively,

$$\{e, (ABC), (ACB), (AB), (AC), (BC)\}$$

Notice that this action obeys the compatibility property, and sends A (for example) to every element. We represent the elements of S_3 as $120°$ rotations and reflections to move the points around. Essentially, we compare S_3 to D_6 The transitive action of S_3 on six points is, respectively,

$$\{e, (ACE)(BDF), (AEC)(BFD), (AB)(CF)(DE), (AD)(BC)(EF), (AF)(BE)(CD)\}$$

This action also obeys the compatibility property, i.e., we did not choose $60°$ rotations as we could have if we were dealing with $\mathbb{Z}/6\mathbb{Z}$ but instead chose $120°$ rotations again, coupled with the three reflections that don't fix any points. Essentially, we compare S_3 with $D_6 \leq D_{12}$, again.

The last case is $\ker\phi = \{e\}$. In this case, ϕ is injective (and thus the action is faithful) and we must have $m \geq |S_n| = n!$. □

- Let's now investigate the case $m \geq n$ more closely.
- Example: S_n acts transitively on the set X of unordered pairs of points from 1 through n.
  - X contains elements like $(1, 4) = (4, 1)$.

  - We have the
$$m = |X| = \binom{n}{2} = \frac{n(n-1)}{2}$$
  - This yields maps from $S_4 \to S_6$, $S_5 \to S_{10}$, and $S_6 \to S_{15}$, for example.
  - Still not entirely sure how we define the group action??
- We now characterize $\text{Aut}(S_n)$ almost completely.
- Lemma: Suppose $n \neq 6$. Let $S_n \circlearrowright X$ transitively, where $|X| = n$. Then (after possibly relabeling the set X) the action is precisely the "usual" action of S_n on $X = \{1, 2, \dots, n\}$.

  Proof. Relabeling the elements if necessary, we find that the action corresponds to a homomorphism $\phi : S_n \to S_X \cong S_n$. Since $m = n \geq n$, the above Lemma tells us that the action is faithful, implying that ϕ is injective. But since ϕ maps a set to itself, its bijectivity follows from its injectivity, so ϕ is an automorphism. Thus, by HW5-Q1 and the hypothesis that $n \neq 6$, ϕ is a conjugation. Since relabeling the elements of X also changes the homomorphism precisely by a conjugation, we may relabel the elements of X to make ϕ the identity. □

- We now address $\text{Aut}(S_6)$.
- Before we do this, though, we must learn a bit more about S_5.
- Lemma: $S_5 \circlearrowright X$ transitively, where $|X| = 6$. The corresponding map $\phi : S_5 \to S_6$ realizes S_5 as a transitive subgroup of S_6.

  Proof. This proof is constructive.

  Let X be the set of all subgroups of S_5 of order 5. Since 5 is prime, every subgroup of order 5 is generated by a 5-cycle. Moreover, every subgroup of order 5 contains four distinct 5-cycles and e. Thus, since there are $(5-1)! = 24$ 5-cycles in S_5 and four distinct 5-cycles per subgroup, there are $24/4 = 6$ subgroups of order 5 in X. As we know, S_5 acts on S_5/X by coset conjugation; this combined with the fact that all subgroups in X are conjugate to each other (since all 5-cycles are conjugate to each other) implies that $S_5 \circlearrowright S_5/X$ transitively, as desired. □

- Additional comments on this **exotic** subgroup of S_6.
  - Every $S_{n-1} \leq S_n$, but this typically involves fixing some $i \in n$ and permuting everything else. The fact that this subgroup doesn't fix anything but is truely transitive makes it somewhat unique and, perhaps, a bit "exotic."
- An explicit formulation for the exotic subgroup of S_6.
  - We begin by writing down all elements of X. To do so, we use the fact that within each subgroup of order 5, there will be a unique element such that $\sigma(1) = 2$[1].
$$\begin{aligned}
A &= \langle (1,2,3,4,5) \rangle \\
B &= \langle (1,2,3,5,4) \rangle \\
C &= \langle (1,2,4,3,5) \rangle \\
D &= \langle (1,2,4,5,3) \rangle \\
E &= \langle (1,2,5,3,4) \rangle \\
F &= \langle (1,2,5,4,3) \rangle
\end{aligned}$$

[1]Reason why this is true: Consider $(1,3,5,4,2)$, for example. It sends $1 \mapsto 3$. Continuing on, $(1,3,5,4,2)^2$ will send $1 \mapsto 3 \mapsto 5$, i.e., will send the leftmost element to the one two away. Continuing on, since every number appears once, we will eventually raise $(1,3,5,4,2)$ to a power such that 1 gets sent far enough down the cycle to make it to 2; in this case, $(1,3,5,4,2)^4$ does the trick as it sends $1 \mapsto 3 \mapsto 5 \mapsto 4 \mapsto 2$.

  - It follows since S_5 is generated by $(1,2,3,4,5)$ and $(1,2)$ and $\phi : S_5 \to S_X$ is a homomorphism that the image of these two elements under ϕ generates the exotic subgroup of $S_X \cong S_6$. We compute these images presently.
  - Compute $\phi((1,2,3,4,5))$. We have that

$$\begin{aligned}
[\phi((1,2,3,4,5))](A) &= (1,2,3,4,5)A(1,2,3,4,5)^{-1} = \langle(2,3,4,5,1)\rangle = \langle(1,2,3,4,5)\rangle = A \\
[\phi((1,2,3,4,5))](B) &= (1,2,3,4,5)B(1,2,3,4,5)^{-1} = \langle(2,3,4,1,5)\rangle = \langle(1,2,4,5,3)\rangle = D \\
[\phi((1,2,3,4,5))](C) &= (1,2,3,4,5)C(1,2,3,4,5)^{-1} = \langle(2,3,5,4,1)\rangle = \langle(1,2,3,5,4)\rangle = B \\
[\phi((1,2,3,4,5))](D) &= (1,2,3,4,5)D(1,2,3,4,5)^{-1} = \langle(2,3,5,1,4)\rangle = \langle(1,2,5,4,3)\rangle = F \\
[\phi((1,2,3,4,5))](E) &= (1,2,3,4,5)E(1,2,3,4,5)^{-1} = \langle(2,3,1,4,5)\rangle = \langle(1,2,4,3,5)\rangle = C \\
[\phi((1,2,3,4,5))](F) &= (1,2,3,4,5)F(1,2,3,4,5)^{-1} = \langle(2,3,1,5,4)\rangle = \langle(1,2,5,3,4)\rangle = E
\end{aligned}$$

    so

$$\phi((1,2,3,4,5)) = (B,D,F,E,C)$$

  - Compute $\phi((1,2))$. We have that

$$\begin{aligned}
[\phi((1,2))](A) &= (1,2)A(1,2)^{-1} = \langle(2,1,3,4,5)\rangle = \langle(1,2,5,4,3)\rangle = F \\
[\phi((1,2))](B) &= (1,2)B(1,2)^{-1} = \langle(2,1,3,5,4)\rangle = \langle(1,2,4,5,3)\rangle = D \\
[\phi((1,2))](C) &= (1,2)C(1,2)^{-1} = \langle(2,1,4,3,5)\rangle = \langle(1,2,5,3,4)\rangle = E \\
[\phi((1,2))](D) &= (1,2)D(1,2)^{-1} = \langle(2,1,4,5,3)\rangle = \langle(1,2,3,5,4)\rangle = B \\
[\phi((1,2))](E) &= (1,2)E(1,2)^{-1} = \langle(2,1,5,3,4)\rangle = \langle(1,2,4,3,5)\rangle = C \\
[\phi((1,2))](F) &= (1,2)F(1,2)^{-1} = \langle(2,1,5,4,3)\rangle = \langle(1,2,3,4,5)\rangle = A
\end{aligned}$$

    so

$$\phi((1,2)) = (A,F)(B,D)(C,E)$$

  - Therefore, the exotic subgroup is given by

$$H = \langle(A,F)(B,D)(C,E),(B,D,F,E,C)\rangle \subset S_6$$

  - It is highly nonobvious that H is transitive and a subgroup isomorphic to S_5, but it is true. However, it can be seen to some extent that it is transitive since the 5-cycle above rotates B-F around, and the other one allows A to be brought into the fold.

- There exists a labeling of the pairs of opposite faces in the dodecahedron such that the action of Do on said pairs induces a map from A_5 to a subgroup of the exotic subgroup of S_6 constructed above.
- We are now ready to construct an automorphism on S_6 that is not a conjugation, i.e., is not inner.
- Let

$$G = \langle(1,6)(2,4)(3,5),(2,4,6,5,3)\rangle \subset S_6$$

  - Note that G is a relabeling of the exotic subgroup H of S_6 with the numbers $1,\dots,6$.

- Lemma: The map $\psi : S_6 \to S_6$ induced by the action of S_6 on S_6/G by left multiplication is an automorphism which is not inner. In particular, this automorphism takes the conjugacy class (xx) to the conjugacy class $(xx)(xx)(xx)$ and, as we shall also see, the conjugacy class $(xxxxxx)$ to the conjugacy class $(xxx)(xx)$.

  Proof. This is a slick proof by contradiction.

  By HW5-Q1a, $\psi(\{(xx)\})$ is another conjugacy class. Additionally, since ψ is a homomorphism, the elements of this conjugacy class must also have order 2. Lastly, since $|\{(xx)\}| = 15$ and ψ is an isomorphism, we must also have $|\{\psi((xx))\}| = 15$. Thus, either $\psi(\{(xx)\}) = \{(xx)\}$ or $\psi(\{(xx)\}) = \{(xx)(xx)(xx)\}$.

Suppose for the sake of contradiction that $\psi(\{(xx)\}) = \{(xx)\}$. Then by HW5-Q1, ψ is an inner automorphism, and thus is given by conjugation. Let

$$\Sigma = \{1,2,3,4,5,6\} \qquad\qquad Y = S_6/G = \{G_1, G_2, G_3, G_4, G_5, G_6\}$$

This makes clear that the true nature of ψ is a map $\psi : S_\Sigma \to S_Y$. WLOG, let $G_1 := G$. Consider $\text{Stab}(G)$ as a subset of S_Y: Here, $\text{Stab}(G)$ (which we will call J) should be the set of all permutations on Y that don't move G_1 (i.e., that fix G_1). On the other hand, as a subset of S_Σ, $\text{Stab}(G) = G$. Since ψ is the map coming from the action, stabilizers should map to stabilizers (why??), so $\psi(G) = J$. It follows that $\psi^{-1}(J) = G$. Since J fixes a point and ψ (hence ψ^{-1}) is given by conjugation, $\psi^{-1}(J) = G$ fixes a point, too. But this contradicts the hypothesis that $G \circlearrowright \Sigma$ transitively. $\square$

Proof. This is an explicit construction.

Return later for the details.

We conclude that

$$\begin{aligned} \psi((1,2)) &= (a,b)(c,d)(e,f) = (1,2)(3,4)(5,6) \\ \psi((1,2,3,4,5,6)) &= (b,f)(c,e,d) = (2,6)(3,5,4) \end{aligned}$$

$\square$