Week 4

Normal Subgroups: Motivation and Properties

4.1 Quotient Groups

10/17: - Notational confusion regarding $\mathbb{Z}/10\mathbb{Z}$.
  - Let $G = \mathbb{Z}$ and $H = 10\mathbb{Z}$ (the multiples of 10).
  - A few of the cosets are as follows:

$$\begin{aligned}H &= \{\dots,-20,-10,0,10,20,30,\dots\}\\ 1+H &= \{\dots,-19,-9,1,11,21,31,\dots\}\\ 2+H &= \{\dots,-18,-8,2,12,22,32,\dots\}\end{aligned}$$

  - Evidently, $|\mathbb{Z}/10\mathbb{Z}| = 10$.
  - Yet $\mathbb{Z}/10\mathbb{Z}$ is also the notation for the cyclic group of order 10.
  - This notation is not an error, but reveals something deep: We can make the set of cosets into a group and define addition by

$$(a+10\mathbb{Z}) + (b+10\mathbb{Z}) = (a+b+10\mathbb{Z})$$

    More specifically, we can define an isomorphism between the two definitions of $\mathbb{Z}/10\mathbb{Z}$ via $a+H \mapsto a$ for $a = 0,\dots,9$.

- This example motivates the following goal.
- Goal: Make G/H, which is a set, into a group.
  - This set needs a binary operation. It makes natural sense to define the binary operation as follows.

$$xH * yH = xyH$$

  - We then need an identity coset, inverse cosets, and associativity.
    - The identity is H.
    - The inverse of xH is $x^{-1}H$.
    - Associativity of G/H follows from the associativity of G (which tells us that $(ab)c = a(bc)$). More specifically,

$$\begin{aligned}aH *_H (bH *_H cH) &= aH *_H (b *_G c)H\\ &= a *_G (b *_G c)H\\ &= (a *_G b) *_g cH\\ &= (a *_G b)H *_H cH\\ &= (aH *_H bH) *_H cH\end{aligned}$$

- Calegari's impromptu explanation of associativity drives home that he really is very good at drilling down to the core of an idea and working with it. He really has a very similar mind to mine.
- Something else we need to investigate: Equivalence classes, and defining functions on equivalence classes.
  - We need to make sure that functions are defined the same regardless of how you label the equivalence classes.
  - Consider the set of names.
    - Say we define equivalency classes based on all names which share the same first letter.
    - Then we define a function F on the equivalency classes based on the last letter.
    - But then [Frank] = [Fen] will be mapped to two different elements of the alphabet, so F is not well-defined.
  - Thus, for our example, we need to guarantee that if $x, x' \in xH$, then $xH * yH = x'H * yH$.
- Check: Independence of choice.
  - Suppose we relabel $x \mapsto xh$ and $y \mapsto yh$. We need
$$xhyh' = xyh''$$
for some $h'' \in H$.
    - Note that x, y, h, h' are all fixed; h'' is the only free thing (i.e., is what we're looking for).
  - Algebraically manipulating the above implies that we want
$$h'' = y^{-1}hyh'$$
  - Thus, we know that $h'' \in G$, but we need to make sure that $h'' \in H$. Alternatively, we want $y^{-1}hy = h''(h')^{-1} \in H$.
  - An example where $y^{-1}hy$ is not in H: $G = S_3$, $H = \langle(1,2)\rangle$, $h = (1,2)$, $y = (1,3)$, $yhy^{-1} = (2,3)$.
- Why did $\mathbb{Z}/10\mathbb{Z}$ work? Because it was abelian, so conjugacy cancelled $y^{-1}hy = y^{-1}yh = h$.
  - We could restrict ourselves entirely to abelian groups, but can we be more general?
- What should we require of G/H?
  - The canamonical map of sets $\phi : G \to G/H$ is given by $\phi(x) = xH$.
  - We should require that ϕ is a homomorphism (i.e., that the group structure of G is preserved for G/H).
  - See how $xH * yH = xyH$ is analogous to $\phi(x)\phi(y) = \phi(xy)$.
- Let's suppose $\phi : G \to G/H$ is a homomorphism.
  - Then $\phi(g) = eH$ implies that $g \in H$, i.e., $\ker\phi = H$.
  - Realization: An alternate way to do HW3, Q2b would have been in terms of quotient groups: In that case, $G/H \cong S_{26}$, and the following proposition would give us the surjectivity and kernel requirements.
- Lemma: Let ϕ be a homomorphism from G to another group. Let $K = \ker\phi \subset G$. Then K has the following property, which is not true for all subgroups but is for kernels: If $x \in K$ and $g \in G$, then $gxg^{-1} \in K$.

  Proof. Since $\phi(x) = e$, we have that
$$\phi(gxg^{-1}) = \phi(g)\phi(x)\phi(g^{-1}) = \phi(g)\phi(g^{-1}) = e$$
□

- **Normal** (subgroup): A subgroup H of G such that for all $x \in H$ and $g \in G$, $gxg^{-1} \in H$. *Denoted by* $\boldsymbol{H \trianglelefteq G}$, $\boldsymbol{H \triangleleft G}$.
  - We often write gHg^{-1}.
- Example: As per the lemma, $\ker \phi$ is a normal subgroup.
- Example: If G be abelian, then every $H \trianglelefteq G$.
- Lemma: A subset $H \subset G$ is normal iff
  1. H is a subgroup.
  2. H is a union of some number of conjugacy classes.
- Proposition: Let G be a group and $H \triangleleft G$. Then G/H is a group under the multiplication

  $$xH * yH = xyH$$

  and the map $\phi : G \to G/H$ is a surjective homomorphism with kernel H.

  Proof. We want to show that $xhyh' = xyh''h'$. We can do so via multiplying the following by x on the left and h' on the right:

  $$\begin{aligned} hy &= (yy^{-1})hy \\ &= y(y^{-1}hy) \\ &= yh'' \end{aligned}$$

  Note that we get from the second to the third line above because H is a normal subgroup, i.e., conjugates of its elements are elements of it. This implies the desired result. □
- Example: Let $G = \mathbb{Z}$, $H = 10\mathbb{Z}$, and $G/H = \mathbb{Z}/10\mathbb{Z}$.
- Example: Let $G = G$ and $H = \{e\}$.
  - H is normal since it's a subgroup and it's a union of conjugacy classes.
  - In this case, $G/H \cong G$.
- Example: $G = \mathrm{O}(2)$ and $H = \mathrm{SO}(2)$.
  - G is not abelian here.
  - From HW1, the cosets are $H = \{\text{rotations}\}$ and $\{\text{reflections}\}$.
  - The cosets are H and sH for some reflection $s \in \mathrm{O}(2) \setminus \mathrm{SO}(2)$.
  - What the group structure tells us here is that rotation $\circ$ reflection is like even $\times$ odd numbers.
  - $G/H \cong \mathbb{Z}/2\mathbb{Z}$ here.
- An equivalent formulation of normality.
- Proposition: $H \triangleleft G$ iff the left cosets coincide with the right cosets, i.e.,

  $$gH = Hg$$

  Proof. Suppose first that $H \triangleleft G$. Use a bidirectional inclusion argument. Let $gh \in gH$. Then

  $$gh = ghg^{-1}g = h'g \in Hg$$

  where h' may or may not equal h, but we know it is an element of H by the definition of normal subgroups. The argument is symmetric in the other direction.

  Now suppose $gH = Hg$. Let $h \in H$. Then there exist $h, h' \in H$ such that $gh = h'g$. Therefore, $ghg^{-1} = h' \in H$. □

- This is a nice resolution of left and right cosets.
  - It tells us when they're the same, and when they're different.
- Implication: If $H \triangleleft G$, then

$$xH \cdot yH = x(Hy)H = x(yH)H = xyHH = xyH$$

- Midterm next week.

4.2 Blog Post: Normal Groups, Quotient Groups

From Calegari (2022).

11/12:

- Mostly direct review of what was covered in class.
- Outline.
  - What constraints must we put on H to make G/H a group?
  - Defining multiplication on G/H by $xH \cdot yH = xyH$ gives us an identity, inverses, and associativity, but the multiplication is not necessarily well defined, i.e., we do not necessarily have $xh \cdot yh' = xyh''$ for all $x, y \in G$.
  - In particular, if $\psi : G \to G/H$ is a group homomorphism, then $h \in \ker\psi = H$ should make $\psi(ghg^{-1}) = e$, i.e., $ghg^{-1} \in H$.
  - This motivates our definition of **normal** subgroups as those subgroups having the property that $ghg^{-1} \in H$ for all $h \in H$.
  - Indeed, if H is normal, then

$$xhyh' = x(yy^{-1})hyh' = xy\underbrace{(y^{-1}hy)h'}_{\in H}$$

    as desired.
  - Consequence: H is normal in G iff $gH = Hg$ for all $g \in G$.
- Example where G/H is not a group: Let $G = S_3$ and $H = \langle(12)\rangle$. Suppose G/H is a group. Then, for example,

$$(13)H = \{(13), (123)\} = (123)H$$

  It follows that

$$H = (13)^2H = (13)H \cdot (13)H = (123)H \cdot (123)H = (123)^2H = (132)H$$

  a contradiction. Therefore, G/H is not a group.
- Example where G/H is a group: Let $G = S_4$ and $H = \{e, (12)(34), (13)(24), (14)(23)\}$. Note that H is isomorphic to the Klein 4-group. H is normal since it contains two complete conjugacy classes. We can visualize the homomorphism $\phi : G \to G/H$ as the related homomorphism from the full cube group to the permutations of opposite faces. Note that each element of H when acting on the diagonals does not permute pairs of opposite faces, as expected.

4.3 First Isomorphism Theorem

10/19:

- Last time:
  - If $K \lhd G$, then the map $\phi : G \to G/K$ defined by $g \mapsto gK$ is a surjective homomorphism with kernel K.
- Today: Understand a general surjective homomorphism $\phi : G \twoheadrightarrow H$ with kernel $K \lhd G$.

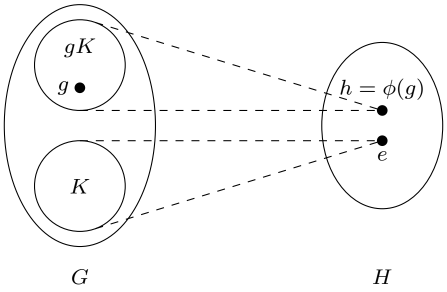

Figure 4.1: Visualizing a surjective homomorphism.

  - In general, we know that $K \mapsto \{e\}$.
  - Since ϕ is surjective, every $h \in H$ equals $\phi(g)$ for some $g \in G$.
  - More broadly, $gK \mapsto \{h\}$.
  - Can you get more elements than those in gK that map to h? Perhaps elements of Kg or KgK? Well since K is normal, $kg = gk$.
  - Thus, all surjective homomorphisms have the same general structure.
    - In particular, they all map disjoint cosets to single elements.
    - Alternatively, we can take the perspective that they send every element to their coset with the kernel.
- Lemma: If $\phi : G \to H$ is a surjective homomorphism, $h \in H$, $\phi(g) = h$, and $K = \ker\phi$, then $\phi^{-1}(h) = gK$.

  Proof. Suppose $g' \in \phi^{-1}(h)$. Suppose $g' = gx$ (we do know that such an x exists in G; in particular, choose $x = g^{-1}g'$). Then
  $$\phi(g') = \phi(gx) = \phi(g)\phi(x)$$
  Since $\phi(g') = h = \phi(g)$, we have by the cancellation lemma that
  $$e = \phi(x)$$
  i.e., $x \in K$. Therefore, $g' \in gK$, as desired. □

- We can define a bijection $\tilde{\phi} : G/K \mapsto H$ defined by $gK \mapsto \phi(g)$.
- Claim: $\tilde{\phi}$ is an isomorphism of groups.

  Proof. Need to check that $\tilde{\phi}$ is a homomorphism, surjective, and injective. We also need to check that it is well-defined (we did this with our picture).

  Surjective: Let $h \in H$ be arbitrary. Then $h = \phi(g)$. It follows that $h = \tilde{\phi}(gK)$.

  Injective: Show that $\ker\tilde{\phi} = \{eK\}$. Let $gK \in \ker\tilde{\phi}$. Then $\phi(g) = \tilde{\phi}(gK) = e$. Thus, $g \in K$. Therefore, $gK = eK$, as desired.

Homomorphism: Check $\tilde{\phi}(xK)\tilde{\phi}(yK) = \tilde{\phi}(xyK)$. Since $\tilde{\phi}(zK) = \phi(z)$, we have the desired property. Explicitly,

$$\tilde{\phi}(xyK) = \phi(xy) = \phi(x)\phi(y) = \tilde{\phi}(xK)\tilde{\phi}(yK)$$

□

- Takeaway: All surjective homomorphisms are somewhat the same.
- Generalize:
- Let $\phi : G \to H$ be a homomorphism.
  - We know that $G \twoheadrightarrow \operatorname{im}\phi \hookrightarrow H$. Essentially, we can break up any homomorphism into the composition of a surjective homomorphism onto the image and an injective homomorphism into H.
- Theorem (FIT: First Isomorphism Theorem): To every homomorphism ϕ there corresponds an isomorphism $\tilde{\phi} : G/\ker\phi \to \operatorname{im}\phi$ such that

$$\tilde{\phi}(g \cdot \ker\phi) = \phi(g)$$

$$\begin{tikzcd}
 & g \arrow[r, mapsto] & \phi(g) & \\
g \arrow[dddr, mapsto] & G \arrow[r, two heads, "\phi"] \arrow[dd] & \operatorname{im}\phi \arrow[r, hook] & H \\
 & & \phi(g) & \\
 & G/\ker\phi \arrow[uur, "\tilde{\phi}"', "\sim"] & & \\
 & g \cdot \ker\phi \arrow[uur, mapsto] & &
\end{tikzcd}$$

Figure 4.2: First isomorphism theorem.

  - The triangle is **commutative**. This means that sending g along both paths gets you to the same result.
  - The way to understand normal subgroups is to understand the homomorphisms.
- $N \subset G$ is normal if
  1. N is a subgroup.
  2. N is normal, i.e., N is a union of conjugacy classes.
  3. $e \in N$.
  4. $|h|\,\big|\,|G|$ (Lagrange).
- 3-4 both follow from 1. They are not sufficient conditions for normality, but they can put restrictions on what is normal and make the computation easier.
- Examples.
  - Let $\phi : \mathbb{Z} \to H$ send $1 \mapsto h$ and $k \mapsto h^k$ (see Figure 4.3).
    - $\operatorname{im}\phi = \langle h \rangle$.
    - $\ker\phi = n\mathbb{Z}$ where $|h| = n$; if $|h| = \infty$, then $\ker\phi = \{0\}$.
    - The FIT tells us that there is a map from $\mathbb{Z}$ to $\mathbb{Z}/n\mathbb{Z}$ to $\langle h \rangle$ to H. The first map sends $k \mapsto k + n\mathbb{Z}$ and the second sends $k + n\mathbb{Z} \mapsto h^k$.
  - Let $G = S_3$.

$$\begin{tikzcd}
\mathbb{Z} \arrow[r] \arrow[d, two heads] & H \\
\mathbb{Z}/n\mathbb{Z} \arrow[r, "\sim"] & \langle h \rangle \arrow[u, hook] \\
k + n\mathbb{Z} \arrow[r, mapsto] & h^k
\end{tikzcd}$$

Figure 4.3: An example of the FIT.

        - The conjugacy classes are
$$\{e\} \qquad \{(1,2),(1,3),(2,3)\} \qquad \{(1,2,3),(1,3,2)\}$$
        - Thus, the only possible normal subgroup N is
$$H = \{e\} \cup (xxx) = \langle (1,2,3) \rangle$$
            - $e \in N$ eliminates union 2,3; Lagrange eliminates union 1,2 (which has order 4).
    - Let $G = S_4$.
        - The conjugacy classes are
$$e \qquad (xx) \qquad (xxx) \qquad (xxxx) \qquad (xx)(xx)$$
        - The number of elements of the above form is
$$1 \qquad 6 \qquad 8 \qquad 6 \qquad 3$$
        - The divisors of $|S_4| = 24$ are 1,2,3,4,6,8,12,24.
            - 1 is possible; no way to get 2,3; 4 is possible; 6,8 are impossible; 12,24 are possible.
            - The 4 example is
$$K = \langle e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3) \rangle$$

- $S_3 / \langle (1,2,3) \rangle \cong \mathbb{Z}/2\mathbb{Z}$.
- S_4/K is a group of order 6.
- The first instance corresponds to some map from $S_3 \to S_2$.
    - You can get an isomorphism from S_3 to D_6.
    - The surjective map sends rotations to the identity and reflections to the nonidentity element.
    - By the FIT, $S_3 / \langle (1,2,3) \rangle \cong S_2$.
        - Yes, if you know enough about the quotient group, you can think about its properties. But it's easier to use the FIT.
- We constructed a map $S_4 \to \text{Cu} \to S_3$. If $N = \ker$, by the FIT, $S_4/N \cong S_3$.
    - As per the above example, we need to take $N = K$ here.
- Example: $G = \text{O}(2)$.
    - The normal subgroups of O(2) are $\{e\}$, $\{r, r^{-1}\}$, and {reflections}.
    - If $N \lhd \text{O}(2)$ contains a reflection, then $N = \text{O}(2)$.
    - Let $N \subset \text{SO}(2)$ be such that $|N| = k$, i.e., N is generated by the rotation of $2\pi k/N$. What is $\text{O}(2)/N$? You can think of SO(2) as a rotation in $\mathbb{R}$. Thus, $\mathbb{R}/2\pi\mathbb{Z} \cong \text{O}(2)$. Thus, $\text{SO}(2)/N \cong \text{SO}(2)$.
- Next time: Replace S_4 with S_5.
- The midterm is most likely Wednesday next week.
    - The midterm will not be on Monday, but it could test stuff covered next Monday.
- Read the blog post on dihedral groups and the other blog posts I've missed!

4.4 Blog Post: The First Isomorphism Theorem

From Calegari (2022).

11/12:

- Again, a fairly straight review of class.
- Implication of the FIT: The image of *any* homomorphism ϕ is naturally (i.e., isomorphic to) the quotient group of $G/\ker\phi$.
- A direct statement and proof of the FIT is given.
- Example: We can use the FIT to prove that $S_4/K \cong S_3$, which would be painful to verify by hand.
- "First" Isomorphism Theorem?
  - There are other isomorphism theorems, but since they are all consequences of the first, Calegari recommends we only memorize the first.
- Theorem (Second Isomorphism Theorem): Let G be a group, H a subgroup, and N a normal subgroup of G. Then there is an isomorphism

$$H/(H \cap N) \cong HN/N$$

- What this means:
  - $HN = \{hn \mid h \in H,\ n \in N\}$.
  - HN is a subgroup of G since

$$(hn)_1(hn)_2 = h_1n_1h_2n_2 = h_1(h_2h_2^{-1})n_1h_2n_2 = \underbrace{h_1h_2}_{\in H}\underbrace{(h_2^{-1}n_1h_2)n_2}_{\in N}$$

  - Since $e \in H$, $N \subset HN$. Moreover, $N \triangleleft HN$ since $N \triangleleft G$.
  - $H \cap N$ is normal in H: If $n \in H \cap N$ and $h \in H$, then $hnh^{-1} \in N$ since $N \triangleleft G$; $hnh^{-1} \in H$ since $n, h \in H$; and therefore, $hnh^{-1} \in H \cap N$.
- If we now define a map $\phi(h(H \cap N)) = hN$, we can easily prove that it is well-defined, surjective, injective, and a homomorphism.
- Calegari can't really think of any applications of the SIT, so he recommends we forget it and just view the proof as another exercise in thinking about the constructions we introduced in building up to the FIT.
- Why normal subgroups are interesting:
  - The FIT asserts that any homomorphism of groups $\phi : G \to H$ can be understood by understanding (1) the subgroups of H (one of which will be $\operatorname{im}\phi$) and (2) the quotients G/K of G.
  - These problems can be studied individually.
  - Thus, to understand maps among the S_n for example which we're often interested in, we should study these two things.
- Union of conjugacy classes and $e \in N$ / Lagrange lemma.

4.5 The Alternating Group

10/21:
- Today, we continue our investigation of normal subgroups.
- Recall our conditions for normal subgroups that we can check first as constraints before doing the formal evaluation.
- Normal subgroups of S_5.

(x)	1	$\subset H$
(xx)	10	X
(xxx)	20	
$(xxxx)$	30	X
$(xxxxx)$	24	$\subset H$
$(xx)(xx)$	15	$\subset H$
$(xx)(xxx)$	20	

Table 4.1: Counting S_5 cycle decompositions.

  - $H = \{e\}, S_5$ are normal subgroups.
  - $|H| = 11$. Nope.
  - $|H| = 16$. Nope.
  - Let's change strategy: Divisors of 120 that are greater than 16 are 120, 60, 40, 30, 24, and 20.
  - Can't hit 20, 24, 30.
  - Possibility 1: $H = \{e\} \cup \{(xx)(xx)\} \cup \{(xxxxx)\}$.
  - We know that the $\subset H$ subgroups must be included if we want to get a multiple of 10 greater than 40.
  - Possibility 2: $H = \{e\} \cup \{(xx)(xx)\} \cup \{(xxxxx)\} \cup \{(xxx)\}$.
  - Possibility 3: $H = \{e\} \cup \{(xx)(xx)\} \cup \{(xxxxx)\} \cup \{(xxx)(xx)\}$.
  - Which of these, if any, are subgroups of S_5?
  - We know that the X'ed out subgroups cannot be included because they generate S_5.
  - n-cycles imply 3-cycles since

$$(n, n-1, \dots, 4, 2, 3, 1) \cdot (1, 2, 3, 4, \dots, n) = (1, 3, 2)$$

  - Thus, we lose 1 and 3.
  - It follows that if $H \triangleleft S_5$ is proper and nontrivial, then $|H| = 60$ and H equals possibility 2, or there is no such H.
  - We now show that possibility 2 is a group and apply a construction more general than technically necessary but it will be useful later.
  - We've already seen possibility 2: It's the symmetries of the dodecahedron $D_0 \subset S_5$ from the homework.
  - Thus, the only proper subgroup of S_5 is this one (which we will later equate to a group called A_5).

- **Alternating** (group of order n): The set of all $g \in S_n$ that can be written as the product of an even number of transpositions. *Denoted by* $\boldsymbol{A_n}$.
- A_n is a subgroup:
  - $e = \tau\tau^{-1}$.

  - Product of an even number of 2-cycles: Add an even number of 2 cycles to an even number of 2-cycles; still have an even number.
  - Inverse is same length: $\sigma = \tau_1 \cdots \tau_{2k}$; $\sigma^{-1} = \tau_{2k}^{-1} \cdots \tau_1^{-1}$.

- Proposition: Either A_n is normal of index 2, $|A_n| = n!/2$, or $A_n = S_n$.
- Claim: Let $\sigma \in S_n \setminus A_n$ be such that $\sigma = \tau_1 \cdots \tau_{2k+1}$. Then $S_n = A_n \cup \sigma A_n$.

  Proof. Let $g \in S_n$ be arbitrary. We divide into two cases. If g is the product of an even number of transpositions, then $g \in A_n$. If g is the product of an odd number of transpositions, then $\sigma^{-1}g$ is the product of an even number of transpositions, i.e., $g\sigma^{-1} \in A_n$. But this implies that $g \in \sigma A_n$, as desired. □

- Define C_n to be the set of all $g \in S_n$ that is a product of a multiple of three 2-cycles. This is just equal to S_n because $(a, b) = (a, b)(a, b)(a, b)$, so it contains all 2-cycles, so it generates S_n.
- So we want to prove that A_n preserves a property (some invariant) that general elements of the symmetric group of not.
- Let $n \geq 2$. There are $\binom{n}{2}$ pairs $\{i, j\}$ in $[n]$. We now take the product of all ordered pairs, or all ordered pairs where $i > j$. This is equal to 1 if $\sigma(i) > \sigma(j)$ and equal to -1 if $\sigma(i) < \sigma(j)$. All 2-cycles swap an odd number of things around. We can thus take

$$\prod_{i>j} \frac{\sigma(i) - \sigma(j)}{i - j}$$

  - This leads to an argument, but we wanna give a slick argument.

- Here's a trick that's a bit subtle.
- Work in $\mathbb{R}^n$; think about the standard basis of orthonormal vectors. Represent S_n as a subset of $O(n)$ (the subset of all permutation matrices with one 1 in every row and column and zeroes everywhere else) and then compose it with the determinant map to get to ± 1. This is a homomorphism. It sends all 2-cycles to -1. So the things that are all products of an even number of 2-cycles, we send to 1. Check Dummit and Foote (2004) for more details.
- Theorem: Assume $n \geq 2$.
  1. A_n is generated by 3-cycles.
  2. A_n is generated by k-cycles where k is odd.
  3. If $n \geq 5$, then the only proper normal subgroup of S_n is A_n.

  Proof. $1 \Rightarrow 2$: If $k \geq 3$ and odd, take

$$(k, \ldots, 2, 3, 1)(1, 2, \ldots, k) = (1, 3, 2)$$

  Note: $(1, \ldots, k) = (1, 2)(1, 3) \cdots (1, k)$.

  1: A_n is generated by all products of two 2-cycles. Three cases:

$$(a, b)(c, d) = (c, a, d)(a, b, c)$$
$$(a, b)(a, c) = (a, c, b)$$
$$(a, b)(a, b) = e$$

  3: We want $H \lhd S_n$. We know that if $(xxx) \in H$, then $A_n \lhd H$.

  Case 1: $\sigma \in H$ with $\sigma = (xxx \cdots x)(xx)(xxx) \ldots$ (i.e., at least one component k-cycle satisfies $k \geq 3$). Implies that we can generate a three cycle by the n-cycles implies 3-cycles approach.

Case 2: $\sigma = (xx)(xx)\cdots(xx)$ (σ is a product of disjoint two cycles; "the only thing left" after case 1). Subcase 0: $\sigma = (ab)$. Implies $H = S_n$. Subcase 1: $\sigma = (ab)(cd)$. Multiply by $(a,b)(c,e)$ to get (c,e,d). Subcase 2: $\sigma = (a,b)(c,d)(e,f)\cdots$. Choose $(a,c)(b,e)(d,f)$. Then $(a,b)(c,d)(e,f)\cdot(a,c)(b,e)(d,f) = (a,d,e)(b,f,c)$. We've reduced to the previous case at this point, i.e., we can now get it to (a,d,e). □

- Misc. notes:
  - When you have two things, you need that extra space of an e. If $n = 4$ it's false because there are other normal subgroups. Note that S_3 actually does work in this proof; it's just $n = 4$ that causes the issue.
- Corollary: Let $n \geq 5$. Let $\phi : S_n \to \Gamma$ be a homomorphism. Then 3 possible things occur.
  1. $\operatorname{im}\phi = \{e\}$.
  2. $\operatorname{im}\phi \cong \mathbb{Z}/2\mathbb{Z}$.
  3. $\operatorname{im}\phi \cong S_n$.

  Proof. By the FIT, $\operatorname{im}\phi \cong S_n/\ker\phi$. Since $\ker\phi \lhd S_n$, we have that $\ker\phi = S_n$, $\ker\phi = A_n$, or $\ker\phi = \{e\}$. These three cases correspond to possibilities 1-3, respectively. □
- This does imply the surjective homomorphism thing.
- Notes on the exam: The material in this class covered on Monday may be tested. Emphasis on it not being too long. He will not be able to avoid one "fun" small amount of credit problem. Look at the practice problems! Would not be as hard as the riffle shuffle problem. A boring problem is "do a computation" or "is it a subgroup? No: It violates Lagrange's theorem." A fun problem is more like some of the practice/HW problems.

4.6 Blog Post: Normal Subgroups of S_n

11/13:

- Lemma: If K is a proper normal subgroup of S_n and $n \geq 5$, then $K = A_n$.

  Proof. Let K be a proper normal subgroup of S_n for $n \geq 5$. To prove that $K = A_n$, it will suffice to show that K contains all 3-cycles since the 3-cycles generate A_n. Technically, this will only prove that $A_n \lhd K$, but since $[S_n : A_n] = 2$, if K a subgroup is larger than A_n, then Lagrange's theorem implies that K necessarily equals S_n and is thus no longer proper. Consequently, proving that every proper normal subgroup of S_n contains *at least* A_n will suffice to show that every proper normal subgroup of S_n is *at most* A_n.

  To show that K contains *all* 3-cycles, it will suffice to show that K contains *one* 3-cycle since as a normal subgroup of S_n, all conjugates of this 3-cycle will be 3-cycles as well and will be in the subgroup. Let's begin. Since K is proper, we know that $\{e\} \neq K \neq S_n$. Thus, there exists a nontrivial element $\sigma \in K$. We now divide into four cases, as follows.

  The cycle decomposition of σ contains at least one k-cycle where $k \geq 3$: Let

$$\sigma = (a_1, a_2, a_3, \dots, a_k)(b_1, b_2, \dots)(c_1, c_2, \dots)\cdots$$

  Being normal, K contains all conjugates of σ, notably including

$$\sigma' = (a_2, a_1, a_3, \dots, a_k)(b_1, b_2, \dots)(c_1, c_2, \dots)\cdots$$

  It follows that

$$\sigma'\sigma^{-1} = (a_1, a_2, a_3)$$

  as desired.

<u>σ is a 2-cycle</u>: Then all 2-cycles are present, and $K = S_n$, so we neglect this case.

<u>σ contains exactly two 2-cycles</u>: Let

$$\sigma = (a_1, a_2)(a_3, a_4)$$

Since $n \geq 5$, we may define

$$\sigma' = (a_1, a_5)(a_3, a_4)$$

Then

$$\sigma' \sigma^{-1} = (a_1, a_2, a_5)$$

as desired.

<u>σ contains three or more 2-cycles</u>: Let

$$\sigma = (a_1, a_2)(a_3, a_4)(a_5, a_6) \cdots$$

Choose

$$\sigma' = (a_1, a_3)(a_2, a_5)(a_4, a_6) \cdots$$

Then

$$\sigma' \sigma^{-1} = (a_1, a_5, a_4)(a_2, a_3, a_6) \cdots$$

and we have reduced to case 1. This yields the desired result. □

11/13:

- Corollary: If $n > m$ and $\psi : S_n \to S_m$ is a homomorphism, then either...
  1. The image is trivial.
  2. The image has order two.
  3. $n = 4$, $m = 3$, and the kernel is the Klein four group.

  Proof. By the FIT, ψ induces an isomorphism $\phi : S_n / \ker \psi \to \operatorname{im} \psi$. By the lemma from lecture 4.1, $\ker \psi$ is normal. Thus, by the above Lemma, either $\ker \psi = S_n$, $\ker \psi = A_n$, or $\ker \psi = \{e\}$ for $n \geq 5$. We can eliminate the last case immediately since $|S_m| < |S_n|$, meaning that ψ must have nontrivial kernel. As to the other two cases, the first one gives trivial image and the second one gives image of order two. If $n < 5$, then $n = 4, 3, 2, 1$. If $n = 4$ and $m = 3$, we can get to the first two cases, but we do also have the additional third case. If $m \leq 2$, then naturally only the first two cases are possible since $|S_m| \leq 2$ at that point. □

- Examples:
  - Prove that Te $\cong A_4$: We know that Te $\subset$ Cu $= S_4$. Since [Cu : Te] $= 2$, Te is normal. Thus, by the lemma, Te $\cong A_4$.
  - Prove that Do $\cong A_5$: Same argument that Do has index 2 in S_5.
- Reminder that conjugacy classes in A_n are not necessarily as nice as those in S_n.
  - Example: When $n = 3$, $\{e, (123), (132)\} = A_3 \cong \mathbb{Z}/3\mathbb{Z}$. $\{(123)\}$ in S_n includes (132) as well, but $\{(123)\}$ is a singleton set in A_5 since A_5 is abelian.