MATH 25700 (Honors Basic Algebra I) Notes

Steven Labalme

October 24, 2022

Weeks

List of Figures

List of Tables

Week 1

Motivating Group Theory

1.1 Groups as Shuffles

9/28:

- Office hours will be pooled between the two sections.
  - Our section's TA is Abhijit Mudigonda (abjihitm@uchicago.edu). His office hours will always be in JCL 267[1]. The times are...
    - Monday: 12:30-2:00 (OH).
    - Wednesday: 1:30-2:30 (PS).
    - Thursday: 12:30-2:00 (OH).
  - The other section's TA is Ray Li (rayli@uchicago.edu). His office hours will always be in Eck 17[2]. The times are...
    - Tuesday: 5:00-7:00 (OH).
    - Thursday: 4:00-5:00 (OH).
    - Thursday: 5:00-6:00 (PS).
- Textbook: Abstract Algebra. Download the PDF from LibGen.
- Weekly HW due on Monday at the beginning of class. Submit online or in person. There is a webpage w/ all the homeworks, but don't do them all at once because they're subject to change.
- Notes on math and math pedagogy.
  - There's a tendency to say here's an object, here's its properties, etc.
  - But this is not historically accurate or motivated. Calegari really gets it! Math is motivated by abstracting examples.
  - Let's not just define a group, but start with an example. This week, we will give examples of groups. In later weeks, we will establish the axiomatic framework that is really only there to understand these examples.
  - Don't stare at the page blankly waiting for inspiration when doing homework; think of examples first and test out your intuition on them to actually understand what the question means.
  - There are some hard problems; work with each other, but acknowledge our collaborators.
  - In-class midterm; final will be take-home. Calegari doesn't like timed exams.
- Today's example: Shuffling.
  - 52 cards; can be shuffled.

[1] JCL is John Crerar Library.

[2] Eckhart basement.

- Number of shuffles:

$$|\text{shuffles}| = 52! \approx 8 \times 10^{67}$$

- Properties of shuffles.
  - **Distinguished shuffle**: e, the identity shuffle, where you do nothing.
  - Shuffle once; shuffle again. The composition of two shuffles is another shuffle.
  - If you repeat the *same* shuffle enough times, the cards will come back to the same order.
    - Let σ be a shuffle, and $n \in \mathbb{N}$. Does there exist n such that

$$\sigma^n = \underbrace{\sigma \circ \cdots \circ \sigma}_{n \text{ times}} = e$$

    - Proving this: By the piegeonhole principle, if you have $\sigma^1, \dots, \sigma^{52!+1}$, then we have repeats a, b with $52! + 1 \geq a > b \geq 1$ such that $\sigma^a = \sigma^b$. This statement is weaker than we want, though.
    - We need more tools. A shuffle is a bijection/permutation. Thus, for every σ, there exists σ^{-1}. This allows us to do this:

$$\begin{aligned}\sigma^a &= \sigma^b\\ \sigma^{-b} \circ \sigma^a &= \sigma^{-b} \circ \sigma^b\\ \sigma^{a-b} &= e\end{aligned}$$

    - This implies a bound! We get that $n \leq 52!$, so $a - b \leq 52!$.
- Define two shuffles: A and B.
  - A splits the deck into two halves (cards 1-26 and 27-52) and stacks (from the top down) the first card off of the 1-26 pile, then the first card off of the 27-52 pile, then the second card off of the 1-26 pile, then the second card off of the 27-52 pile, etc. The final order is $1, 27, 2, 28, \dots, 26, 52$.
  - B does the same thing as A but with the first card off of the 27-52 pile. The final order is $27, 1, 28, 2, \dots, 52, 26$.
- Computation shows that $A^8 = e$ and $B^{52} = e$.
  - For A, $2 \to 3 \to 5 \to 9 \to 17 \to 33 \to 14 \to 27 \to 2$.
  - For B, we can do the same thing but obviously the cycle is much longer.
- We shouldn't necessarily have an intuition for this right now, but in doing more examples, Calegari certainly believes we can develop it.
- First HW problem (due Friday). Can, just by using combinations of A and B, we generate any possible shuffle? Hint: Develop your intuition on a smaller value of 52.

- I really like Calegari. Very nice, relatable, not demeaning.
- **Binary operation** (on G): A map from $G \times G \to G$.
- **Group**: A mathematical object consisting of a set G and a binary operation $*$ on G satisfying the following properties.
  1. There exists an identity element $e \in G$ such that $e \times g = g \times e = g$ for all $g \in G$.
  2. For any $g \in G$, there exists $h \in G$ such that $h * g = g * h = e$.
  3. (Associativity) For any $g_1, g_2, g_3 \in G$, $g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3$.

  Denoted by $\boldsymbol{(G, *)}$.
- In the cards example, the elements of G are the shuffles and $*$ is the composition operation between two shuffles.

- Aside on shuffles: For bijections, $h(g(x)) = x$ implies $g(h(y)) = y$.
  - Proof: Let $x = h(y)$ — we can do this since h is a bijection. Then since $h(g(h(y))) = h(y)$ and h is injective, $g(h(y)) = y$. This works for all y.
- The set of shuffles, together with composition, does form a group.
- Theorem: If G is a group such that $|G| < \infty$, then any $g \in G$ has finite **order**, i.e., there exists n such that $g^n = e$.
- Lemma:
  1. The identity e is unique.
     - Let e_1, e_2 be identities. Then
       $$e_1 = e_1 * e_2 = e_2$$
  2. Inverses are unique.
     - Let h, h' be inverses of g. Then
       $$h = e * h = (h' * g) * h = h' * (g * h) = h' * e = h'$$
- Proving examples is easier, but these aren't that hard.
- If you understand everything about S_5, you'll understand everything about this course.

1.2 Blog Post: What is Group Theory About?

From Calegari (2022).

10/24:
- Many great ideas on how mathematics should be taught.
  - Example: "A natural mathematical question is: How do we quantify this symmetry? This is unlike mathematical questions you might be used to, like ”what is 2^{10}“ or ”what is $\int_{-1}^{1} \sqrt{1 - x^2}$,“ but it is actually reflective of what real mathematicians do."
- A terrific intuitive motivation for group theory.
- Using symmetry to put constraints on physical laws.
  - Suppose we want to understand the gravitational attraction between two particles $\mathbf{x}, \mathbf{y}$ in $\mathbb{R}^3$.
  - The gravitation pull F has a certain magnitude which depends on the positions of the two particles, i.e.,
    $$F(\mathbf{x}, \mathbf{y}) = F(x_1, x_2, x_3, y_1, y_2, y_3)$$
  - However, "our conception of this force is that it shouldn't depend on how we are labeling the coordinates," i.e., the force should be invariant under translation. Thus,
    $$F(\mathbf{x}, \mathbf{y}) = F(\mathbf{x} - \mathbf{y}, \mathbf{0}) = F(x_1 - y_1, x_2 - y_2, x_3 - y_3, 0, 0, 0)$$
  - Going further, the force should not depend on the direction, but only the distance between the two particles. Thus,
    $$F(\mathbf{x}, \mathbf{y}) = H(|\mathbf{x} - \mathbf{y}|)$$
  - Thus, we see that through only consideration of symmetry, we have put strong constraints on how the force of gravity may behave.
- Review of the riffle shuffle stuff from class.

1.3 Blog Post: The Axioms of a Group

From Calegari (2022).

- Relevant section from Dummit and Foote (2004): 1.1.
- Review of the content covered in class, plus the cancellation lemma (from the 10/3 lecture).
- Note that the cancellation lemma for groups is stronger than the one for the real numbers.
  - In $\mathbb{R}$, we have $xy = xz$ implies $y = z$ or $x = 0$, but the latter case doesn't happen in groups.
  - One consequence of this observation is that $\mathbb{R}$ under numerical multiplication does not form a group.

1.4 The Cube Group

9/30:

- Can't download `.tex` file for homework?
  - Calegari will check it.
- Detail on the homework?
  - Up to your level of confidence in what you think is clear to be true.
  - The problem is not about doing linear algebra; it's about finding some facts about linearly algebraic objects.
  - Concentrate on the new geometry of the situation.
  - Project confidence to the grader that you know what you're doing.
- The symmetries of the cube.
  - Rotational symmetries.
  - Rigid transformation.
  - Preserves lengths, angles, and lines.
  - A map from the cube to itself, i.e., ϕ : cube $\to$ cube.
  - No scaling allowed.
  - Reflectional symmetries are *not* going to be allowed for today; we will insist that the orientation is also preserved for now.
  - We want the set of all rotations and compositions of rotations. (Are compositions of rotations also rotations? We'll answer later. Yes they are.)
- Symmetries should be composable: If you compose two symmetries, you should get a third one.
  - In other words, we want the symmetries to form a group.
- We want to fix the center of the cube at the origin. Thus, a symmetry can be a linear map $M : \mathbb{R}^3 \to \mathbb{R}^3$.
  - We want it to preserve angles, i.e., orthogonality. Thus, we should assert $MM^T = I$.
  - We also want it to preserve orientation. Then we should have $\det(M) = 1$.
- **Cu**: The cube group.
- Does the permutation of faces determine M?
  - Yes.
  - Furthermore, if we know where e_1, e_2 go, then the fact that orientation and orthogonality are preserved implies that we know where e_3 goes. Thus, M is determined by two (adjacent) faces.

- An upper bound on $|\text{Cu}|$.
  - Send e_1 to one of 6 faces and send e_2 to one of the 5 remaining faces (so $|\text{Cu}| \leq 6 \cdot 5 = 30$).
  - Send e_1 to one of 6 faces and send e_2 to one of the four remaining *adjacent* faces (so $|\text{Cu}| \leq 6 \cdot 4 = 24$).
  - And, in fact, $|\text{Cu}| = 24$.
- Moreover, since the rotations of the cube are determined by permutations of the faces, we can map $\text{Cu} \hookrightarrow S_6$. Additionally, composing any permutations of the faces is the same as composing any permutations of S_6, i.e., ϕ is an **injective homomorphism** to a **subgroup** of S_6.
- We can also think about permuting the vertices.
  - 3 vertices (chosen correctly) form a basis of $\mathbb{R}^3$.
  - Thus, since there are 8 vertices, we have another map from $\text{Cu} \hookrightarrow S_8$.
  - Since we can map the first vertex to any of eight and the second to only one of three adjacent vertices, the order is $8 \cdot 3 = 24$[3].
- We now have both Cu and S_4 with order 24. Are they isomorphic?
  - One characteristic of a cube that numbers four are its four diagonals. This induces a function from $\text{Cu} \to S_4$. We now just need to prove it's bijective.
  - Let v_1, v_2, v_3, v_4 be the vertexes of one face. Then $-v_1, \dots, -v_4$ are the vertexes of the opposite face, and the line from each v_i to $-v_i$ is a diagonal of the cube. To prove that the function is bijective, we will show that different elements of Cu map to different elements of S_4.
  - Let A and B be actions on the cube group such that

$$\begin{aligned} Bv_1 &= \pm Av_1 \\ Bv_2 &= \pm Av_2 \\ Bv_3 &= \pm Av_3 \\ Bv_4 &= \pm Av_4 \end{aligned}$$

  - Taking $C = A^{-1}B$ means that

$$\begin{aligned} Cv_1 &= \pm v_1 \\ Cv_2 &= \pm v_2 \\ Cv_3 &= \pm v_3 \\ Cv_4 &= \pm v_4 \end{aligned}$$

  - If $Cv_1 = v_1$, it implies that $Cv_i = v_i$ for $i = 2, 3, 4$.
  - Thus, A and B are distinct?

1.5 Blog Post: Symmetries of the Cube

From Calegari (2022).

10/24:

- Motivating the definition of symmetries of the cube.
- From our intuition, symmetries can be of the form...
  1. Rotations in lines passing through the origin.
  2. Linear maps which preserve distances, angles, and orientation.

[3] We have gotten the order a different way. Deep connection to prime factorization? Edges would be $2 \cdot 12$!

- Claim: These two sets are the same.

  Proof. From HW1, the first set is SO(3). Thus, we need only prove that the second set is exactly SO(3). To begin, we will concentrate only on distances and angles.

  Let $\langle x,y\rangle$ denote the Euclidean inner product of $x,y\in\mathbb{R}^3$. Since $\langle x,y\rangle = |x||y|\cos(\theta)$, the set of all linear maps that preserve distances and angles is equal to the set of all linear maps M satisfying

  $$\langle Mx,My\rangle = \langle x,y\rangle$$

  Since $\langle x,y\rangle = x^Ty$, this means we want

  $$\begin{aligned}(Mx)^T(My) &= x^Ty\\ x^TM^TMy &= x^Ty\\ M^TM &= I\end{aligned}$$

  It follows that we want all $M\in\mathrm{O}(3)$.

  Without going into detail, the orientation issue further restricts us to SO(3). □

- Calegari subtly gives away the $f(n)+f(53-n)=53$ from the homework in this post!

Week 2

Group Theory Foundations

2.1 Groups of Low Order

10/3:

- Calegari: Nothing in particular to know for missing Friday; Adi will get me notes.
- Having explored examples, today, we're coming back down to earth to flex our axiomatic muscles.
- Distinguishing sets and binary operations.

Group	G	$*$	?
S_n	shuffles	composition	cards
$\mathrm{O}(n)$ and $\mathrm{SO}(n)$	(sp) orthogonal matrices	composition	vectors?
$\mathbb{Z}$	integers	addition	
$\mathbb{Z}/n\mathbb{Z}$	$\{0,1,\dots,n-1\}$	addition modulo n	

Table 2.1: Elements of a group.

  - Be careful not to confuse the shuffles and the cards; the cards are something else curious but are *not* the elements of the group.
  - Notice that $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ are **commutative** groups, but the shuffles (for $n > 1$) and $\mathrm{O}(n)$ are not.
  - Note that S_2, $\mathrm{O}(1)$, and $\mathbb{Z}/2\mathbb{Z}$ are all isomorphic groups.
- **Commutative** (group): A group such that for all $x, y \in G$, $x * y = y * x$. *Also known as* **Abelian**.
- Lemma (Cancellation Lemma): Let $x, y, z \in G$. Then $xy = xz$ implies $y = z$ and $yx = zx$ implies $y = z$.

Proof. We have that

$$\begin{aligned} x * y &= x * z \\ x^{-1} * (x * y) &= x^{-1} * (x * z) && \text{Inverses exist} \\ (x^{-1} * x) * y &= (x^{-1} * x) * z && \text{Associativity} \\ e * y &= e * z \\ y &= z \end{aligned}$$

as desired.

The proof of the second statement is symmetric. □

  - This will be Calegari's only proof from the axioms directly.

- **Multiplication table** (for G): A table with all elements of G on the top and the side, and all binary products in it.
  - The total number of binary operations is n^{n^2}?
  - To check that a group is a group, we can write out its multiplication table and confirm pointwise that the group axioms are satisfied. However, there are also many ways to speed this process up.
  - An example of a multiplication table can be found on the right in Figure 2.1.
- **Trivial group**: The only group with $|G| = 1$, i.e., $G = \{e\}$.
- A group of $|G| = 2$ has the form $G = \{e, x\}$ where we must have $x = x^{-1}$.
  - We can find this by inspection or invoke the **Sudoku Lemma**.
  - Thus, all groups of order 2 are isomorphic.
- Lemma (Sudoku Lemma): Fix $x \in G$. Then

  $$\{xg \mid g \in G\} = G = \{gx \mid g \in G\}$$

  Proof. There exists g such that $xg = y$ for x, y fixed: Choose $g = x^{-1}y$.

  y only occurs once: If $xg = y$ and $xg' = y$, transitivity and the cancellation lemma imply $g = g'$. □

  - In layman's terms, in every row and column of the multiplication table, each element of G occurs exactly once.
- Playing Sudoku, we can show that all groups of order 3 are isomorphic.

	e	x	y
e	e	x	y
x	x		
y	y		

$\longrightarrow$

	e	x	y
e	e	x	y
x	x	y	e
y	y	e	x

Figure 2.1: Playing Sudoku for $|G| = 3$.

  - Start from the left table above.
  - Notice that row 3 has a y and column 2 has an x, so by the Sudoku Lemma, e must be the element in row 3, column 2.
  - Then column 2 has e, x in it, so the entry in row 2, column 2 must by y.
  - Then row 2 has x, y in it, so the entry in row 2, column 3 must be e.
  - Then row/column 3 both have e, y in them, so the entry in row 3, column 3 must be x.
- However, we cannot play Sudoku in the same way with groups of order 4. In fact, there are multiple groups of order 4.
  - Two cases: (1) $x^2 \neq e$ so WLOG let $x^2 = y$, and (2) $a^2 = e$ for $a = x, y, z$.
    - Case 1 is isomorphic to $\mathbb{Z}/4\mathbb{Z}$.
    - Case 2 is isomorphic to the **direct product** of $\mathbb{Z}/2\mathbb{Z}$ with itself, also known as the **Klein 4-group**.
  - This should not come as a surprise: We've already encountered the very different groups S_4 and $\mathbb{Z}/24\mathbb{Z}$ of order 24.

- **Direct product**: The group whose set is the Cartesian product of the sets of groups $A = (A, *_A), B = (B, *_B)$, and whose operation is coordinate-wise multiplication. *Given by*

$$G = A \times B \qquad\qquad (a, b) *_G (a', b') = (a *_A a', b *_B b')$$

  - We can prove that $e = (e_A, e_B)$, that $(a, b)^{-1} = (a^{-1}, b^{-1})$, and that associativity holds.
  - We have that

$$|G| = |A| \cdot |B|$$

- There is only one group of order 5.
- Examples of groups of order 6: S_3, $\mathbb{Z}/6\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$, $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.
  - Are there any two groups which are distinct?
    - S_3 is not commutative, but the others are, so it is distinct from them.
    - $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$ and $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ are the same because order doesn't matter in the construction of the direct product.
    - $\mathbb{Z}/6\mathbb{Z}$ and the two direct products are the same because they both have elements of order 6 (i.e., a one-element generator). The cycles are:

$$\begin{aligned}
1^1 &= 1 &&= 1 & \qquad (1,1)^1 &= (1,1) &&= (1,1)\\
1^2 &= 1+1 &&= 2 & (1,1)^2 &= (1+1, 1+1) &&= (2,0)\\
1^3 &= 2+1 &&= 3 & (1,1)^3 &= (2+1, 0+1) &&= (0,1)\\
1^4 &= 3+1 &&= 4 & (1,1)^4 &= (0+1, 1+1) &&= (1,0)\\
1^5 &= 4+1 &&= 5 & (1,1)^5 &= (1+1, 0+1) &&= (2,1)\\
1^6 &= 5+1 &&= 0 & (1,1)^6 &= (2+1, 1+1) &&= (0,0)\\
1^7 &= 0+1 &&= 1 & (1,1)^3 &= (0+1, 0+1) &&= (1,1)
\end{aligned}$$

  - These are the only two groups of order 6.
- Continuing on, there is only 1 group with $|G| = 2047$ (which is "mostly prime" — connection between primes and number of groups?), but there are 1,774,274,116,992,170 groups of $|G| = 2048 = 2^{11}$.
- Conclusion: The arithmetic of $|G|$ has an impact on the structure of G.

2.2 The Symmetric Group

10/5:

- **Symmetric group** (on n letters): The set of all bijections from the set of numbers $\{1, \dots, n\}$ to itself, whose operation is function composition. *Denoted by* $\boldsymbol{S_n}$.
  - Convention: Denote elements of S_n not by f but by σ, τ.
  - $\sigma\tau$ means do τ first and then σ.
  - $|S_n| = n!$.
- One of the first challenges we encounter when defining new objects is a notational one.
  - We could define a function with a table, but cycle notation is easier.
- ***k*-cycle**: The bijection

$$m \mapsto \begin{cases} a_{i+1} & m = a_i,\ i \neq k\\ a_1 & m = a_k\\ m & m \neq a_i \end{cases}$$

  in S_n, where $a_1, \dots, a_k$ are distinct elements of $[n]$. *Denoted by* $\boldsymbol{(a_1, a_2, \dots, a_k)}$.

- If σ is a k-cycle, then the order of σ is k.
- There are k ways to write down the same k-cycle.
  - For example, $(i,j)=(j,i)$ and $(a,b,c)=(b,c,a)=(c,a,b)$.
- All 1-cycles are the identity e.
- Combinatorics: How many k-cycles are there in S_n?
  - $k=1$: Just one – (e).
  - $k=2$: $\binom{n}{2}$.
  - $k=3$: $\binom{n}{3}\cdot 2$.
    - ➢ We must first choose 3 of the n possible elements to be manipulated by the k-cycle.
    - ➢ But then we can send a_1 to a_2 or a_3, so that's an additional two choices beyond just a selection of 3 elements. Once we send a_1 to a_2 or a_3, the rest of the cycle is determined, so we need not augment any more.
  - k: $\binom{n}{k}\cdot(k-1)! = \frac{n!}{(n-k)!k}$.
    - ➢ As before, we must choose k of the n possible elements to be manipulated by the k-cycle.
    - ➢ However, here, there are $k-1$ possibilities to which we can send a_1, so we need to multiply by that. Once we've determined $\sigma(a_1)$, there are $k-2$ possibilities to which we can send $\sigma(a_1)$. This pattern naturally continues, and we end up needing to correct $\binom{n}{k}$ by $(k-1)!$.

- Proposition: Every $\sigma\in S_n$ can be written as a product/composition of disjoint cycles. Moreover, disjoint cycles commute.

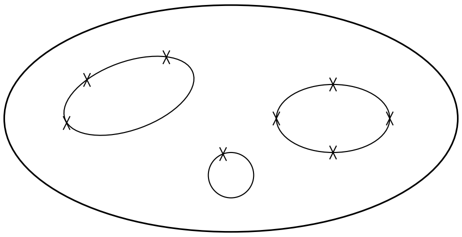


Figure 2.2: Decomposing σ into disjoint cycles.

  - The idea behind this proposition is that every element will cycle back to itself eventually, and you can't get to elements of one cycle if you're not in the cycle (so all cycles are disjoint).
  - Every permutation can be visualized by ordering the n letters in a set in $\mathbb{R}^2$ and connecting all disjoint cycles (think a circle full of oriented circles/loops/cycles).

- Composing cycles. See what the right one does and then the left one. Canonically, start with 1.
- Proposition: The cycle decomposition of σ is unique up to...
  - The ordering of the disjoint cycles;
  - Cycle permutations of each cycle;
  - Include/exclude 1-cycles.

  Moreover, $|\sigma|$ is the least common multiple of the cycle lengths.

- How many elements in S_6 have a cycle shape that looks like $(x,x)(x,x)(x,x)$?
  - It is
$$\frac{6!}{2^3\cdot 3!}=15$$
  - Rationale: See PSet 2, Q1a.

- The cycle decompositions of all elements in S_4.

$(1,2,3,4)$	$(1,2,3)$	$(1,2)$	$(1,2)(3,4)$	e
$(1,2,4,3)$	$(1,3,2)$	$(1,3)$	$(1,3)(2,4)$	
$(1,3,2,4)$	$(1,2,4)$	$(1,4)$	$(1,4)(2,3)$	
$(1,3,4,2)$	$(1,4,2)$	$(2,3)$		
$(1,4,2,3)$	$(1,3,4)$	$(2,4)$		
$(1,4,3,2)$	$(1,4,3)$			
	$(2,3,4)$			
	$(2,4,3)$			

Table 2.2: S_4 cycle decompositions.

- **Conjugate** (elements x, y): Two elements $x, y \in G$ a group for which there exists $g \in G$ such that $y = g \cdot x \cdot g^{-1}$. *Denoted by* $\boldsymbol{x \sim y}$.
- Lemma: Conjugacy is an equivalence relation.
  (I) $x \sim x$.

  Proof. $x = exe^{-1}$. □

  (II) If $y \sim x$, then $x \sim y$.

  Proof. Take

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

□

  (III) If $x \sim y$ and $y \sim z$, then $x \sim z$.

  Proof. Suppose $y = gxg^{-1}$ and $z = hyh^{-1}$. Then

$$z = hgxg^{-1}h^{-1} = (hg)x(hg)^{-1}$$

□

- **Conjugacy class** (of x): A subset of G containing all $g \in G$ which are conjugate to a certain $x \in G$. *Denoted by* $\boldsymbol{C(x)}$. *Given by*

$$C(x) = \{g \in G \mid g \sim x\}$$

- Straightforward: Not necessarily obvious, but there's nothing really tricky going on.
  - The joke about the mathematician who says something is obvious, someone asks why?, he thinks for 20 minutes, and then says it's obvious.
- Why is conjugacy important?
  - In linear algebra, we've seen it with similar matrices.
    - Same linear map in a different basis is the same as conjugating the matrix of the map in one basis with the change of basis matrix.
  - Conjugacy tells us that a set of objects are, in some way, the same.

2.3 Blog Post: The Symmetric Group

From Calegari (2022).

10/24:

- Relevant section from Dummit and Foote (2004): 1.3.
- Review from class plus more details on the riffle shuffle problem.

2.4 Conjugacy

10/7:

- You can request one extension per quarter on homework (possibly more if you have a really good reason) for sickness, etc., no questions asked. Email your TA to secure this extension.
- Last time, we began covering conjugacy.
  - Conjugacy classes.
  - Conjugacy defines an equivalence relation on G.
  - $G = \bigsqcup$ conjugacy classes[1].
- More on conjugacy today.
- The conjugacy class of e is $\{e\}$.
- If $y = gxg^{-1}$, then $y^k = gx^kg^{-1}$.
- Proposition: $y \sim x$ implies $|y| = |x|$.

  Proof. Suppose $|y| = k$, i.e., $y^k = e$. By the above statement, we know that $y^k \sim x^k$. Since $y^k = e$, it follows that $e \sim x^k$. Thus, x^k is in the conjugacy class of e. But since the conjugacy class of e is $\{e\}$, this means that $x^k = e$, as desired. □

- Conjugacy in S_n, $n \geq 2$.
  - Each $x \in S^n$ has a cycle decomposition

$$x = (a_1, \dots, a_k)(b_1, \dots, b_m)(c_1, \dots) \cdots$$

  - We want to investigate the properties of gxg^{-1} for an arbitrary $g \in S_n$. Ideally, we'd like to express it in a form related to x.
  - Trick: Apply gxg^{-1} to $g(a_1)$. Then

$$gxg^{-1}(g(a_1)) = gx(a_1) = g(a_2)$$

  - It follows by induction that

$$gxg^{-1} = (g(a_1), \dots, g(a_k))(g(b_1), \dots, g(b_m))(g(c_1), \dots) \cdots$$

  - Now suppose that $m \neq g(a_i), g(b_j), g(c_k), \dots$. Then

$$g^{-1}(m) \notin \{a_1, \dots, a_k, b_1, \dots, b_m, c_1, \dots\}$$

    It follows since x is the identity on such elements that $x(g^{-1}(m)) = g^{-1}(m)$. Therefore, since all functions involved are bijections,

$$[gxg^{-1}](m) = g[x(g^{-1}(m))] = g(g^{-1}(m)) = m$$

[1] $\bigsqcup$ denotes a **disjoint union**. Think of the *disjoint* union of sets as a union of sets that happen to be disjoint, the same way a *direct* sum of subspaces is a sum of subspaces that happen to be linearly independent.

  - It follows that gxg^{-1} has the same **cycle shape**.

- **Shape** (of $g \in S_n$): The partition of n given by the lengths of the cycles in the cycle decomposition of g in decreasing order. *Also known as* **cycle shape**, **partition**.

S_4	4-cycle	3-cycle	Product of 2-cycles	1-cycles
Cycle decomposition	(x,x,x,x)	$(x,x,x)(x)$	$(x,x)(x,x)$	$(x)(x)(x)(x)$
Shape	4	$3+1$	$2+2$	$1+1+1+1$

Table 2.3: Shape of elements in S_4.

- Claim: $x, y \in S_n$ are conjugate iff they have the same cycle shape.

  Proof. We will do a proof by example that illustrates the idea of the generalized proof.

  Let

$$x = (1,2,3)(4,5,6)(7,10) \qquad\qquad y = (2,3)(4,1,5)(6,9,10)$$

  Note that both have the same cycle shape: $3+3+2+1+1$. We now use a two-step process to define a g such that $y = gxg^{-1}$.

  Step 1: Including 1-cycles, line both x and y up so they "match."

x	$(\ 1$	2	$3\ )(\ 4$	5	$6\ )(\ 7$	$10\ )(\ 8\ )(\ 9\ )$
y	$(\ 4$	1	$5\ )(\ 6$	9	$10\ )(\ 2$	$3\ )(\ 7\ )(\ 8\ )$
gxg^{-1}	$(g(1)$	$g(2)$	$g(3))(g(4)$	$g(5)$	$g(6))(g(7)$	$g(10))(g(8))(g(9))$

  Step 2: We want $y = gxg^{-1}$. Thus, take g to be the map which sends every entry in gxg^{-1} to the entry of y directly above it. For example, we want $g(1) = 4$, $g(2) = 1$, $g(3) = 5$, ... Noting that $g(1) = 4$, $g(4) = 6$, $g(6) = 10$, ..., we realize that g can actually be written as the following cycle.

$$g = (1,4,6,10,3,5,9,8,7,2)$$

  □

- Follow ups.
  - How many different g's satisfy $y = gxg^{-1}$?
    - Depends on the number of ways y can be matched up with x.
    - The above manner obviously works.
    - However, we can rotate the elements in both 3-cycles three ways, and the elements of the 2-cycle two ways, so that's $3 \cdot 3 \cdot 2 = 18$ g's right there.
    - Additionally, we can swap the place of the 3-cycles and the 1-cycles entirely, so thats an additional $2 \cdot 2$ times as many ways.
    - All told, there are $3 \cdot 3 \cdot 2 \cdot 2 \cdot 2 = 72$ possible g's.
    - See HW2, Q1a for a treatment of an analogous problem.
  - Counting the size of conjugacy classes.
    - Suppose G is an abelian group. Then if $y = gxg^{-1}$, $y = gg^{-1}x = x$, so the size of the conjugacy class of any $x \in G$ is 1.
    - For this reason, the elements of $\mathbb{Z}/n\mathbb{Z}$ and of SO(2) are conjugate only to themselves.
    - However, we get something different for O(2). Here, we can prove that the conjugacy class of every rotation r is $\{r, r^{-1}\}$, and that all reflections are in the same conjugacy class[2].

[2] This is fundamentally related to the structure of point groups in inorganic chemistry! Remember that in C_{5v}, for instance, C_5, C_5^4 are conjugate, C_5^2, C_5^3 are conjugate, and all reflections get lumped together.

  - ➢ Let r denote a rotation, and s denote a reflection.
  - ➢ Suppose $x = r$. Then

$$\begin{aligned} e &= (sr)^2 \\ &= srsr \\ r^{-1} &= srs \\ &= srs^{-1} \end{aligned}$$

    where we have HW1, Q2d(i) to justify the first equality and the fact that every reflection is it's own inverse[3] to justify the last equality.
  - ➢ On the other hand, suppose $x = s$. Then if r is any rotation,

$$\begin{aligned} srsr &= e \\ rsr &= s^{-1} \\ rsrr^{-2} &= s^{-1}r^{-2} \\ rsr^{-1} &= sr' \end{aligned}$$

    where r' denotes r^{-2} to express the main takeaway: that s is conjugate to itself times any rotation (for r' arbitrary, we may choose $r = (r')^2$). In other words, since all reflections are related by some rotation, all reflections are, indeed, in the same conjugacy class.

- Generators of S_n, $n \geq 3$.
- Lemma: The set of 2-cycles generates S_n.

  Proof. It only requires $n - 1$ swaps between pairs of elements to get to any permutation. For example, to get to

$$\begin{array}{ccc} 1 & & 3 \\ 2 & \mapsto & 4 \\ 3 & & 2 \\ 4 & & 1 \end{array}$$

  we can swap 1 and 3 (so $1 \mapsto 3$), then 2 and 4 (so $2 \mapsto 4$), then "3" and "4" (so $3 \mapsto 2$ and $4 \mapsto 1$). More graphically,

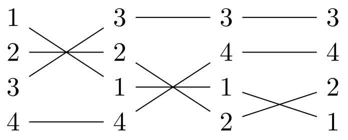


Figure 2.3: Generating S_n with 2-cycles.

  The idea is we fix the first element and then work down the list. □

- S_n is also generated by

$$\{(1,2),(2,3),(3,4),\dots,(n-1,n)\} \qquad \{(1,2),(1,3),(1,4),\dots,(1,n)\}$$

  - Both of these sets have cardinality $n - 1$.
- As we can see from the above. . .

[3] Intuitively, applying any reflection twice yields the original object.

  - If we generate S_n with all 2-cycles, the generator set has cardinality $\frac{n}{2}(n-1)$;
  - If we generate S_n with all elementary 2-cycles, the generator set has cardinality $n-1$.
- But we can do even better: Let $\sigma = (1,2)$ and $\tau = (1,2,\dots,n)$. Then any

$$(k,k+1) = \tau^{k-1}\sigma\tau^{-(k-1)}$$

  - Indeed, we can see that using the RHS above, $k \mapsto 1 \mapsto 2 \mapsto k+1$ and $k+1 \mapsto 2 \mapsto 1 \mapsto k$. Every other element receives the identity treatment, as we can confirm.

2.5 Blog Post: Conjugacy

From Calegari (2022).

10/22:

- x,y are conjugate implies $|x| = |y|$, but $|x| = |y|$ does not imply x,y are conjugate.
  - Example: $(1,2)$ and $(1,2)(3,4)$ in S_4 are not conjugate (their cycle shapes differ) but they are both of order 2.
- $\boldsymbol{p(n)}$: The number of possible partitions of $\sigma \in S_n$.
- Growth rate of $|n|$ and $p(n)$.
  - We have

$$p(n) \sim \frac{1}{4n\sqrt{3}} \exp\left(\pi\sqrt{\frac{2n}{3}}\right)$$

    - ■ $\sim$ means that the ratio of the two numbers converges to 1 as $n \to \infty$.
  - We also have that

$$|n| = n! \sim n^n \mathrm{e}^{-n}\sqrt{2\pi n}$$

  - Since

$$\log n! \sim n\log n \qquad\qquad \log p(n) \sim Cn^{1/2}$$

    for some explicit C, we know that $|n|$ grows much faster than $p(n)$.

Week 3

Types of Subgroups and Group Functions

3.1 Subgroups and Generators

10/10: - Defining **subgroups**.
    - Let $G = (G, *)$ be a group, and let $H \subseteq G$ be a subset.
    - What properties do we want H to satisfy to consider it a "subgroup?"
        - H should inherit the binary operation from G.
        - H should be closed under multiplication using said binary operation.
        - H should be nonempty.
        - H should contain the inverses of every element — this is automatic if G is finite since the inverse of an element g of order n is g^{n-1} and $g^{n-1} \in H$ by closure under multiplication.
        - H should also be associative; we also inherit this for free from G.
- Easy way to construct a subgroup.
    - Let G be a group, and let $x_1, x_2, \dots \in G$. We can let $H = \langle x_1, x_2, \dots \rangle$, i.e., H is the group **generated** by $x_1, x_2, \dots$. In other words, H is the set of all finite products $x_1, x_1^{-1}, x_2, x_2^{-1}, \dots$.
    - This construction does give you all possible subgroups, but when you write it down, it's very hard to say what group you get.
- Example: If you have $H \subset G$ a subgroup, then $H = \langle h|_{h \in H} \rangle$.
- **Cyclic** (group): A group G for which there exists $g \in G$ such that $G = \langle g \rangle$.
- Examples:
    - If $1 < n < \infty$, then $\mathbb{Z}/n\mathbb{Z} = \langle 1 \rangle$.
    - However, the generator isn't always unique — $\mathbb{Z}/7\mathbb{Z} = \langle 3 \rangle$.
    - If G is generated by an element, it's also generated by its inverse. For example, $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$.
- Proposition: Let G be a cyclic group. It follows that
    1. If $|G| = \infty$, then G is isomorphic to $\mathbb{Z}$;
    2. If $|G| = n < \infty$, then G is isomorphic to $\mathbb{Z}/n\mathbb{Z}$.

Proof. Assertion 1: Let $G = \langle g \rangle$. Then

$$G = \{\dots, g^{-2}, g^{-1}, e, g, g^2, g^3, \dots\}$$

Now suppose for the sake of contradiction that $g^a = g^b$ for some $a, b \in \mathbb{Z}$. Then $g^{a-b} = e$, so $|G| \leq a-b$, a contradiction. Therefore, $G = \{G^{\mathbb{Z}}\}$. In particular, we may define $\phi : \mathbb{Z} \to G$ by $k \mapsto g^k$. This map has the property that $a + b \mapsto g^a g^b$, i.e., $\phi(a)\phi(b) = \phi(ab)$[1].

Assertion 2: Let $G = \langle g \rangle$. Then

$$G = \{e, g, g^2, \dots, g^{n-1}\}$$

Now suppose for the sake of contradiction that $g^a = g^b$. Then $g^{a-b} = e$, so $|G| \leq a - b < n$, a contradiction. Therefore, we may once again define $\phi : \mathbb{Z}/n\mathbb{Z} \to G$ as above. Note that $a + b \mapsto g^{(a+b) \mod n}$. This is still a homomorphism, though. □

- Claim: Any subgroup of a cyclic group is also cyclic.
- Example: $G = \mathbb{Z}$, $H = \langle 2002, 686 \rangle$.
  - $H = \{2002x + 686y \mid x, y \in \mathbb{Z}\}$.
  - To say that H is cyclic is to say that it is equal to the integer multiples of some $d \in \mathbb{Z}$, i.e., there exists d such that $G = \{zd \mid z \in \mathbb{Z}\}$.
  - We can take $d = \gcd(2002, 686)$.
  - (Nonconstructive) proof: Let d be the smallest positive integer in H. Suppose for the sake of contradiction that $md + k$ is in the group for some $1 \leq k < d$. Then adding $-d$ m times, we get that $k \in H$, a contradiction since we assumed d was the smallest positive integer in H.
- Let $G = \langle x, y \rangle$ be a group that is generated by two elements. Find a subgroup $H \subset G$ such that H *must* be generated by more than 2 elements.
  - Let's work with $S_n = \langle (1, 2, \dots, n), (1, 2) \rangle$.
  - The subgroup $H = \langle (1, 2), (3, 4), (5, 6) \rangle$ will work.
    - $H = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
    - Suppose $H = \langle a, b \rangle$. We can get e, a, b, ab. But because everything commutes, we can rearrange any product to $a^i b^j$ and cancel.
- When you want to answer questions like, "Is $\mathbb{Z}/180180\mathbb{Z}$ a subgroup of S_n for some n," you need some more information on the structure of S_n.
- Group **presentations** allow us to describe a group really easily. Seems useful at first but isn't really.

3.2 Blog Post: Subgroups

From Calegari (2022).

10/24:

- Relevant section from Dummit and Foote (2004): 2.1.
- **Subgroup**: A subset H of a group G for which the binary operation $\cdot$ on G restricts to a binary operation (which we can also call $\cdot$) on H and $(H, \cdot)$ is a group.
- Lemma: $H \subset G$ iff the following three conditions are satisfied.
  1. H is nonempty.
  2. H is closed under multiplication, that is, if $x, y \in H$, then $x \cdot y \in H$.
  3. H has inverses, that is, if $x \in H$, then $x^{-1} \in H$.

  Proof. Calegari gives a totally rigorous proof of this. □
- Rigorous definitions of the notation x^n as well as proving that the usual properties of exponents hold.

[1] We all know that this is a **homomorphism**; Calegari just doesn't want to call it that yet.

3.3 Homomorphisms

10/12:

- We've studied groups a lot at this point. But as with vector spaces, we don't have a complete theory of groups until we consider maps between them.
- Today: Homomorphisms.
- Let H, G be groups.
- What qualities do we want a map of groups to have?
  - Maps between vector spaces preserve linearity, so maps between groups should probably preserve the group operation.
  - Bijection? As with linear maps, the bijective case is interesting, but we don't want to be this restrictive.
  - In fact, that first quality is the only one we want.
- **Homomorphism**: A map $\phi : H \to G$ of sets such that $\phi(x *_H y) = \phi(x) *_G \phi(y)$.
- Lemma: Let $\phi : H \to G$ be a homomorphism. Then...
  1. $\phi(e_H) = e_G$.
  2. $\phi(x^{-1}) = \phi(x)^{-1}$.

  Proof. Claim 1:

$$\begin{aligned} e_G\phi(x) = \phi(x) &= \phi(xe_H) = \phi(x)\phi(e_H) \\ e_G &= \phi(e_H) \end{aligned}$$

  Claim 2:

$$e_G = \phi(e_H) = \phi(xx^{-1}) = \phi(x)\phi(x^{-1})$$

□

- **Image** (of ϕ): The subset of G such that for all $h \in H$, $\phi(h) = g$. *Denoted by* $\textbf{im}\,\boldsymbol{\phi}$.
- **Kernel** (of ϕ): The subset of H containing all $h \in H$ such that $\phi(h) = e_G$. *Denoted by* $\textbf{ker}\,\boldsymbol{\phi}$.
- Lemma:
  1. $\operatorname{im}\phi \subset G$ is a subgroup.
  2. $\ker\phi \subset H$ is a subgroup.

  Proof. Claim 1: We know that $\phi(e_H) = e_G$, so

$$\operatorname{im}\phi \neq \emptyset$$

  as desired. Next, let $g_1, g_2 \in \operatorname{im}\phi$. Suppose $g_1 = \phi(h_1)$ and $g_2 = \phi(h_2)$. Then since H is closed under multiplication as a subgroup, $h_1h_2 \in H$. It follows that

$$g_1g_2 = \phi(h_1)\phi(h_2) = \phi(h_1h_2) \in \operatorname{im}\phi$$

  as desired. Lastly, let $g \in \operatorname{im}\phi$. Suppose $g = \phi(h)$. Then since H is closed under inverses as a subgroup, $h^{-1} \in H$. It follows that

$$g^{-1} = \phi(h)^{-1} = \phi(h^{-1}) \in \operatorname{im}\phi$$

  as desired.

Claim 2: We know that $\phi(e_H) = e_G$, so

$$\ker\phi \neq \emptyset$$

as desired. Next, let $g_1, g_2 \in \ker\phi$. Then

$$e_G = e_G e_G = \phi(g_1)\phi(g_2) = \phi(g_1 g_2)$$

so $g_1 g_2 \in \ker\phi$, as desired. Lastly, let $g \in \ker\phi$. Then

$$e_G = \phi(e_H) = \phi(gg^{-1}) = \phi(g)\phi(g^{-1}) = e_G\phi(g^{-1}) = \phi(g^{-1})$$

□

- Examples:

H	G	ϕ	$\operatorname{im}\phi$	$\ker\phi$
H	G	$\phi(h) = e$	$\{e\}$	H
$H \leq G$	G	inclusion	H	$\{e\}$
$\mathbb{Z}$	$\mathbb{Z}/n\mathbb{Z}$	$k \mapsto k \mod n$	$\mathbb{Z}/n\mathbb{Z}$	$n\mathbb{Z}$
$\mathrm{O}(n)$	$\mathbb{R}^*$	det	$\{\pm 1\}$	$\mathrm{SO}(n)$
$\mathrm{GL}_n\mathbb{R}$	$\mathbb{R}^*$	det	$\mathbb{R}^*$	$\mathrm{SL}_n\mathbb{R}$

Table 3.1: Examples of images and kernels.

  - The first example shows that there is always at least one homomorphism between two groups.
  - $\mathbb{R}^*$ is the group of nonzero real numbers with multiplication as the group operation.
  - The $\mathrm{O}(n)$ example expresses the fact that $\det(AB) = \det(A)\det(B)$, i.e., that the determinant is a homomorphism.
    - The kernel is $\mathrm{SO}(n)$ since 1 is the multiplicative identity of $\mathbb{R}^*$ and all matrices in $\mathrm{SO}(n) \subset \mathrm{O}(n)$ get mapped to 1 by the determinant.
  - $\mathrm{GL}_n\mathbb{R}$ is the set of all $n \times n$ invertible matrices over the field $\mathbb{R}$.

- **Isomorphism**: A bijective homomorphism from $H \to G$.
  - If an isomorphism exists between H and G, we say, "H is isomorphic to G."

- Lemma: H is isomorphic to G implies G is isomorphic to H.

Proof. $\phi : H \to G$ a bijection implies the existence of $\phi^{-1} : G \to H$. Claim: This is an isomorphism. We can formalize the notion, or just think of ϕ as relabeling elements of H and ϕ^{-1} as unrelabeling them. □

- Lemma: A homomorphism $\phi : H \to G$ is **injective** iff $\ker\phi = \{e_H\}$.

Proof. Suppose ϕ is injective. We know that $\phi(e_H) = e_G$ from a previous lemma; this implies that $e_H \in \ker\phi$. Now let $x \in \ker\phi$ be arbitrary. Then $\phi(x) = e_G = \phi(e_H)$. But since ϕ is injective, we have that $x = e_H$. Thus, we have proven that $e_H \in \ker\phi$, and any $x \in \ker\phi$ is equal to e_H; hence, we know that $\ker\phi = \{e_H\}$, as desired.

Now suppose that $\ker\phi = \{e_H\}$. Let $\phi(x) = \phi(y)$. It follows that

$$\phi(xy^{-1}) = \phi(x)\phi(y^{-1}) = \phi(x)\phi(y)^{-1} = \phi(x)\phi(x)^{-1} = e_G$$

But this implies that

$$xy^{-1} = e_H$$
$$x = y$$

as desired. □

- Problem: Is there a surjective homomorphism $\phi : S_5 \to S_4$?
  - Proposal 1: Send 5-cycles to the identity and everything else to itself.
  - Proposal 2: "Drop 5" $(1,2)(3,4,5) \mapsto (1,2)(3,4)$.
    - Counterexample: $(1,2,3,4,5) \mapsto (1,2,3,4)$.
  - Proposal 3: If it doesn't do something to everything, send it to e.
- Lemma: Let $\phi : H \mapsto G$ be a homomorphism. If $|h| = n$, then $|\phi(h)|$ divides n, i.e., n is a multiple of $|\phi(h)|$.

  Proof. If $h^n = e$, then $\phi(h^n) = e = \phi(h)^n$. □
- Equipped with this lemma, let's return to the previous problem.
  - Suppose for the sake of contradiction that such a surjective homomorphism ϕ exists.
  - Consider a 5-cycle $h \in S_5$; obviously, $|h| = 5$.
  - It follows by the lemma that $\phi(h) \in S_4$ has order which divides 5. But since the maximum order of an element in S_4 is 4, this means that $|\phi(h)| = 1$, so $\phi(h) = e$.
- If one 5-cycle maps to the identity, then all of their products must, too.
- What can map to an order 3 element in S_4?
- If $\psi(g) = (1,2,3)$, then $|g|$ is divisible by 3.
- In fact, no surjective map exists!
- In order for homomorphisms to exist, there must be some reason. If there aren't any (nontrivial ones), proving this can be easy.
- Now consider $S_4 \mapsto S_3$.
  - 4-cycles to e or 2-cycles.
  - 3-cycles to 3-cycles.
- Idea: $S_4 \cong \text{Cu} \cong S_3$.
  - 3 pairs of opposite faces and 4 diagonals.

3.4 Blog Post: Homomorphisms and Isomorphisms

From Calegari (2022).

10/24:

- Relevant section from Dummit and Foote (2004): 1.7.
- Additional homomorphism examples:
  - Let Cu be the cube group. Then the action of this group on vertices, faces, edges, diagonals, and pairs of opposite faces gives homomorphisms $\psi : \text{Cu} \to S_n$ for $n = 8, 6, 12, 4, 3$, respectively.
  - Let $G = \mathbb{Z}/6\mathbb{Z}$ and $H = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Then $\psi : G \to H$ sending $n \mod 6 \mapsto (n \mod 2, n \mod 3)$ is a homomorphism.
- Lemma: If $\psi : G \to H$ is an injection, then $\tilde{\psi} : G \to \text{im}(\psi)$ is an isomorphism.

3.5 Cosets

10/14:

- Asking, "what's the intuition for this question?" in OH.
  - Calegari: Intuition is borne of experience. You get intuition from grubby computations, and then you finally recognize the structure. If you don't know what's going on, it's good to struggle. Start with the simplest possible example and then struggle until you develop intuition.
- Last time, we discussed the fact that there is no surjective homomorphism from $S_5 \to S_4$, but there is a surjective homomoprhism from $S_4 \to S_3$. How about the case $S_{n+1} \to S_n$ for arbitrary n?
- Teaser theorem: Let $n > m$ and $\phi : S_n \twoheadrightarrow S_m$. Then
  1. $m = 1$.
  2. $m = 2$.
  3. $m = 3$.
- Think about the problem of maps from $G \to \Gamma$, where Γ is another group. What we know:
  - Let $K = \ker \phi$. Recall that ϕ is injective iff $\ker \phi = \{e\}$. But there is some additional structure: If $\phi(g) = x$, then $\phi(gK) = x$ where $gK = \{gk \in G \mid k \in K\}$. Another way of phrasing this: If $\phi(g') = x$, then $g' = gk$ for some $k \in K$.
  - This motivates the following definition.
- **Left coset**: The set defined as follows, where $g \in G$ and H is a subgroup of G. *Denoted by* $\boldsymbol{gH}$. *Given by*

$$gH = \{gh \mid h \in H\}$$

  - You can define cosets for H a subset (not a subgroup) of G, but we will not be interested in these cases.
- Claim: Let $x, y \in G$ be arbitrary. Then either $xH \cap yH = \emptyset$ or $xH = yH$.
- Example: $G = S_3$, $H = \langle e, (1,2) \rangle$.

g	gH
e	$\{e, (1,2)\}$
$(1,2)$	$\{e, (1,2)\}$
$(1,3)$	$\{(1,3), (1,2,3)\}$
$(1,2,3)$	$\{(1,3), (1,2,3)\}$
$(2,3)$	$\{(2,3), (1,3,2)\}$
$(1,3,2)$	$\{(2,3), (1,3,2)\}$

Table 3.2: Cosets of $\langle e, (1,2) \rangle$ in S_3.

  - Observations: Cosets are pairwise disjoint. $x \in gH$ implies $xH = gH$.
- $\boldsymbol{G/H}$: The set of all left cosets of H in G.
- Proposition:
  1. Any two cosets in G/H are either (i) the same or (ii) disjoint.
  2. All $g \in G$ lie in a unique coset (in particular, gH).
  3. $|gH| = |H|$.

Proof. Claim 1: Let $C_1, C_2 \in G/H$. We divide into two cases ($C_1 \cap C_2 = \emptyset$ and $C_1 \cap C_2 \neq \emptyset$). In the first case, C_1, C_2 are disjoint, as desired. In the latter case, they are not disjoint, so we need to prove that they are the same. Suppose $g \in C_1 \cap C_2$. Let $C_1 = \gamma H$. We will prove that $gH = \gamma H$ via a bidirectional inclusion argument. It will follow by similar logic that $gH = C_2$, from which transitivity will imply that $C_1 = gH = C_2$, as desired. Let's begin. Let $x \in gH$. Then $x = gh$ for some $h \in H$. Additionally, we know that $g \in \gamma H$ by hypothesis, so $g = \gamma h'$ for some $h' \in H$. It follows by combining the last two equations that $x = \gamma h'h$. But since $h'h \in H$, $x \in \gamma H$ as desired. A symmetric argument works in the other direction.

Claim 2: We know that $g \in gH$ since $e \in H$ and $g = ge$. Additionally, if $g \in \gamma H$, we have by part (1) that $\gamma H = gH$, so g does lie in a *unique* coset.

Claim 3: Suppose there exist $h, h' \in H$ such that $gh = gh'$. Then $h = h'$ by the cancellation lemma. Thus, every distinct $h \in H$ induces a distinct $gh \in gH$. Therefore, $|gH| = |H|$, as desired. □

- Notice that so far, general statements we've made about groups have been very easy to prove; it's only in particular instances that things become tricky.
- Decomposition of a group into equivalence classes: Cosets and conjugacy both do this.
- Corollary: Let H be a subgroup of G. Then

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

Proof. Sketch: Partition G into cosets, each of order $|H|$. But there are $|G/H|$ of these. Thus, the number of elements in G is $|G/H| \cdot |H|$. □

- **Index** (of H in G): The number of cosets into which H partitions G. *Denoted by* $[\boldsymbol{G : H}]$. *Given by*

$$[G : H] = |G/H|$$

- If $|G| < \infty$, then $[G : H] = |G|/|H|$. If $|G| = \infty$, then we can still define the concept $|G/H|$, but we don't have a nice formula for it.
- Example: Let $G = \mathbb{Z}$ and $H = 2\mathbb{Z}$ (i.e., H is the set of even integers). Then the orbits are all even and all odd nunbers. The index is 2??
- Theorem (Lagrange):
  1. Let G be a finite group, $H \subset G$. Then $|H|$ divides $|G|$.
  2. Let G be a finite group. Let $g \in G$. Then $|g|$ divides $|G|$.
- Example: Let p be prime. If $|G| = p$, then $G \cong \mathbb{Z}/p\mathbb{Z}$.

Proof. Take $g \in G$ such that $g \neq e$. By Lagrange's theorem, $|g|$ divides p. But this means that $|g| = 1$ or $|g| = p$. But it's not the first case because $g \neq e$. Thus, $G = \langle g \rangle \cong \mathbb{Z}/p\mathbb{Z}$, as desired. □

- **Right coset**: The set defined as follows, where $g \in G$ and H is a subgroup of G. *Denoted by* $\boldsymbol{Hg}$. *Given by*

$$Hg = \{hg \mid h \in H\}$$

- $\boldsymbol{H/G}$: The set of all right cosets of H in G.
- The theories of left and right cosets are very similar, but they are not entirely equivalent.
  - For example, $H = \langle e, (1,2) \rangle$ implies

$$(1,3)H = \{(1,3), (1,2,3)\} \qquad H(1,3) = \{(1,3), (1,3,2)\}$$

3.6 Blog Post: Dihedral Groups

From Calegari (2022).

10/24:

- Moving on from the cube group as a subset of SO(3), we can talk about 2-dimensions.
- In 2-dimensions, we choose to admit both rotations and reflections of a given geometric object.
  - This is because reflections in 2D are equal to rotations in 3D. Mathematically, there is a homomorphism $\psi : \mathrm{O}(2) \to \mathrm{SO}(3)$ given by

$$A \mapsto \left(\begin{array}{cc|c} \multicolumn{2}{c|}{\multirow{2}{*}{A}} & 0 \\ & & 0 \\ \hline 0 & 0 & \det(A) \end{array}\right)$$

- **Dihedral group**: The subgroup of O(2) consisting of elements which preserve the regular n-gon ($n \geq 3$) centered at the origin. *Denoted by* D_{2n}.
- We can study $D_{2n} \subset S_n$ by labeling the vertices of the n-gon from 1 through n.
  - Similarly to in the cube group, any two nonopposite vertices are linearly independent, and the transformation is uniquely determined by any two such vertices.
  - In particular, we can move vertex 1 anywhere we want (say m), but then since vertex 2 must remain a neighbor, it can either move to $m \pm 1$ (addition modulo n).
  - Thus, we get an injective homomorphism from $D_{2n} \to S_n$.
- We can write down the elements of D_{2n} explicitly in terms of S_n. For example...
  - A rotation r of $2\pi/n$ is sent to $(1, 2, \dots, n)$.
  - A reflection s through the edge connecting 1 and n is sent to $(1, n)(2, n-1)(3, n-2)\cdots$.
    - Note that depending on whether n is odd or even (i.e., depending on the **parity** of n), s may or may not (respectively) fix one vertex.
- We can easily write out all of the elements of D_{2n} and the multiplication table; this is rather rare.
- Lemma: The elements of D_{2n} are as follows.
  1. The powers of r, given by $e, r, r^2, \dots, r^{n-1}$.
  2. The elements $s, sr, sr^2, \dots, sr^{n-1}$.

  The multiplication table is given by

$$\begin{aligned} r^i \cdot r^j &= r^{i+j} \\ sr^i \cdot r^j &= sr^{i+j} \\ r^i \cdot sr^j &= sr^{-i+j} \\ sr^i \cdot sr^j &= r^{-i+j} \end{aligned}$$

- All rotations are distinct.
- All elements sr^i are distinct: If $sr^i = r^j$, then $s = r^{j-i}$, but r is a reflection not a rotation.
- To check the multiplication table, we use the identity

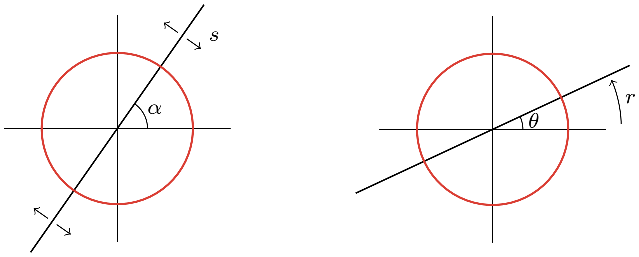
$$rs = sr^{-1}$$

- This identity has the alternate form

$$srs = s^{-1}rs = r^{-1}$$

since s has order 2.

- Claim: The above identity is true for any rotation and reflection.



(a) Reflection. (b) Rotation.

Figure 3.1: Commuting rotations and reflections.

Proof. Let's consider the plane to be the complex plane, and represent points on the unit circle using the complex numbers $z = \mathrm{e}^{i\gamma}$. In this case, we have that

$$s : \mathrm{e}^{i\gamma} \mapsto \mathrm{e}^{i(2\alpha-\gamma)} \qquad r : \mathrm{e}^{i\gamma} \mapsto \mathrm{e}^{i(\gamma+\theta)} \qquad r^{-1} : \mathrm{e}^{i\gamma} \mapsto \mathrm{e}^{i(\gamma-\theta)}$$

It follows that for any $\mathrm{e}^{i\gamma}$ on the unit circle,

$$[srs](\mathrm{e}^{i\gamma}) = [sr](\mathrm{e}^{i(2\alpha-\gamma)}) = s(\mathrm{e}^{i(2\alpha-\gamma+\theta)}) = \mathrm{e}^{i(2\alpha-(2\alpha-\gamma+\theta))} = \mathrm{e}^{i(\gamma-\theta)} = r^{-1}(\mathrm{e}^{i\gamma})$$

meaning that

$$srs = r^{-1}$$

as desired. □

- The identity $r^i \cdot sr^j = sr^{-i+j}$ follows inductively.
- Lemma: The conjugacy classes of D_{2n} are as follows.

1. The identity.
2. If $n = 2m$, the element r^m.
3. For all other $0 < m < n$, the pair $\{r^m, r^{-m}\}$.
4. If n is odd, then all reflections are conjugate.
5. If $n = 2m$, then the reflections divide into two conjugacy classes of size m, consisting of elements of the form sr^{2i} and sr^{2i+1}, respectively.

Proof. Consider the rotation r^i and, more specifically, gr^ig^{-1} for $g \in D_{2n}$. We divide into two cases. If g is a rotation, then it commutes with r^i. Thus,

$$gr^ig^{-1} = r^igg^{-1} = r^i$$

If g is a reflection, then since the inverse of a reflection is itself and $r^{j+i}s = sr^{-i-j}$, we have that

$$gr^ig^{-1} = sr^jr^i(sr^j)^{-1} = sr^{j+i}sr^j = ssr^{-i-j}r^j = r^{-i}$$

Therefore, the only elements in the conjugacy class of r^i are r^i and r^{-i}. This validates claims 1-3, above.

Now consider the reflection sr^i and, more specifically, gsr^ig^{-1} for $g \in D_{2n}$. Once again, we divide into two cases. If g is a rotation, then

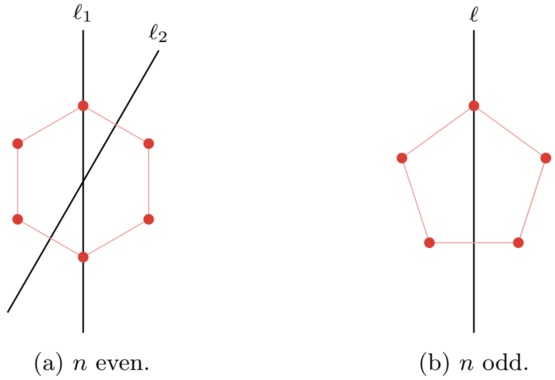
$$gsr^ig^{-1} = r^jsr^ir^{-j} = sr^{-j}r^ir^{-j} = sr^{i-2j}$$

If g is a reflection, then since $sr^is = r^{-i}$ as proven above, we have that

$$gsr^ig^{-1} = sr^jsr^isr^j = sr^j(sr^is)r^j = sr^jr^{-i}r^j = sr^{2j-i}$$

Therefore, either way, sr^i is only conjugate to reflections with the same parity of a power of a rotation. If n is odd, then we will be able to get to all reflections using different values of j, but if n is even, then we will only be able to get to half at a time. This validates claims 4-5, above. □

- Geometric intuition for the relation between the reflection conjugacy classes and n.



(a) n even. (b) n odd.

Figure 3.2: Reflection conjugacy classes for n even or odd.

  - If n is even, there are two "flavors" of reflection: Those in which the line of reflection passes through two opposite vertices (e.g., ℓ_1 in Figure 3.2a), and those in which the line of reflection passes through the midpoints of two opposite edges (e.g., ℓ_2 in Figure 3.2a).
  - If n is odd, all lines of reflection pass through one vertex and through the middle of the opposite edge (e.g., ℓ in Figure 3.2b).

3.7 Blog Post: Cosets and Lagrange's Theorem

From Calegari (2022).

10/24:

- **Left coset**: The following subset of G, where $g \in G$ and H is a subgroup of G. *Denoted by* $\boldsymbol{gH}$, $[\boldsymbol{g}]$. *Given by*

$$[g] = gH = \{gh \mid h \in H\}$$

- Additional coset examples:
  - If $H = G$, then $[g] = gH = G$ for any $g \in G$.
  - If $H = \{e\}$, then $[g] = gH = \{e\}$ for any $g \in G$.
  - If $G = \mathbb{Z}$ and $H = 10\mathbb{Z}$, then

$$[7] = \{\dots, -13, -3, 7, 17, 27, 37, 47, \dots\} = [17] = [-3]$$

    for instance.
- Calegari does want us to attempt to prove the claims in the blog by ourselves.

- Calegari offers two proofs of the fact claim that either $xH \cap yH = \emptyset$ or $xH = yH$.
- Lemma: If $g \in G$ is arbitrary, then there is a bijection between H and gH.

  Proof. The bijection is given by $h \mapsto gh$; the fact that this is a bijection follows from the cancellation lemma. Explicitly,

  $$gh = gh' \quad \Longleftrightarrow \quad h = h'$$

  and gh in the codomain is mapped to by h in the domain. □

- Theorem: There is an equality

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

  for all subgroups H of G, where when $|G| = \infty$ the above statement is interpreted to mean that at least one of the quantities on the RHS is also infinite.

  Proof. We count the elements of G in two ways. The first is to say that there are $|G|$ elements in G. The second is to say that $G = \bigcup_{g \in G} gH$. But by the previous lemma, $|gH| = |H|$ so the size of G is the product of the size of each coset $|H|$ and the number of cosets $|G/H|$. Therefore, via transitivity, we have the desired result. □

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 cananonical 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 × 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 First Isomorphism Theorem

10/19:

- Last time:
  - If $K \triangleleft G$, 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 $K \triangleleft G$.

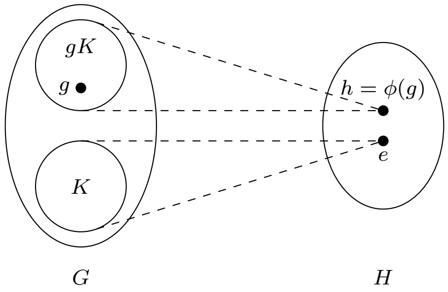


Figure 4.1: Visualizing a surjective homomorphism.

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

$$\begin{tikzcd}
 & g \arrow[rr, mapsto] & & \phi(g) & & \\
g \arrow[ddrr, mapsto] & G \arrow[rr, two heads, "\phi"] \arrow[dr] & & \operatorname{im}\phi \arrow[rr, hook] & & H \\
 & & G/\ker\phi \arrow[ur, "\tilde{\phi}"', "\sim"] & & \phi(g) & \\
 & & g\cdot\ker\phi \arrow[urr, mapsto] & & &
\end{tikzcd}$$

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.

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

Figure 4.3: An example of the FIT.

- Examples.
  - Let $\phi:\mathbb{Z}\to H$ send $1\mapsto h$ and $k\mapsto h^k$.
    - $\operatorname{im}\phi=\langle h\rangle$.
    - $\ker\phi=n\mathbb{Z}$ 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 $G=S_3$.
    - The conjugacy classes are

      $$\{e\}\qquad\qquad \{(1,2),(1,3),(2,3)\}\qquad\qquad \{(1,2,3),(1,3,2)\}$$

    - 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

      $$e\qquad\qquad (xx)\qquad\qquad (xxx)\qquad\qquad (xxxx)\qquad\qquad (xx)(xx)$$

    - The number of elements of the above form is

      $$1\qquad\qquad 6\qquad\qquad 8\qquad\qquad 6\qquad\qquad 3$$

    - 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: $G = \mathrm{O}(2)$.
  - The normal subgroups of $\mathrm{O}(2)$ are $\{e\}$, $\{r, r^{-1}\}$, and $\{\text{reflections}\}$.
  - If $N \lhd \mathrm{O}(2)$ contains a reflection, then $N = \mathrm{O}(2)$.
  - Let $N \subset \mathrm{SO}(2)$ be such that $|N| = k$, i.e., N is generated by the rotation of $2\pi k/N$. What is $\mathrm{O}(2)/N$? You can think of $\mathrm{SO}(2)$ as a rotation in $\mathbb{R}$. Thus, $\mathbb{R}/2\pi\mathbb{Z} \cong \mathrm{O}(2)$. Thus, $\mathrm{SO}(2)/N \cong \mathrm{SO}(2)$.
- 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!

4.3 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 $\sigma \in S_n/A_n$ 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 $g\sigma^{-1}$ 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

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

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

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

$$\begin{aligned}(a,b)(c,d) &= (c,a,d)(a,b,c)\\ (a,b)(a,c) &= (a,c,b)\\ (a,b)(a,b) &= e\end{aligned}$$

3: If $H \triangleleft S_n$, then $(xxx) \in H$ implies $A_n \triangleleft H$. Case 1: $\sigma \in H$ with $\sigma = (xxx \cdots x)(xx)(xxx)$... Case 2: $\sigma = (xx)(xx) \cdots (xx)$ (σ is a product of disjoint two cycles; "the only thing left"). Subcase 0: (ab) implies $H = S_n$. Subcase 1: $(ab)(cd)$. Multiply by $(a,b)(c,e)$ gives (c,e,d). Subcase 2: $(a,b)(c,d)(e,f) \cdots$. Not changing anything else. 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. We can now get it to (a,d,e). 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 $\ker\phi \triangleleft S_n$, 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.

References

Calegari, F. (2022). *Group theory* [Accessed 2022-10-24.]. https://www.galoistheory2020.com/2022/

Dummit, D. S., & Foote, R. M. (2004). *Abstract algebra* (third). John Wiley and Sons.