MATH 25700 (Honors Basic Algebra I) Notes

Steven Labalme

January 2, 2023

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 $\sigma^1, \ldots, \sigma^{52!+1}$, 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 $1, 27, 2, 28, \ldots, 26, 52$.
  - B does the same thing as A but with the first card off of the 27-52 pile. The final order is $27, 1, 28, 2, \ldots, 52, 26$.
- 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., $\phi : \text{cube} \to \text{cube}$.
  - 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 |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 $-v_1, \ldots, -v_4$ 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 $\langle x, y\rangle = x^T y$, this means we want

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

  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!

1.6 Chapter 0: Preliminaries

From Dummit and Foote (2004).

Basics

12/4:

- Frequently used notation defined at the beginning of the textbook.
- Know the basics of set theory.
  - Definitions given for: **Subset**, **Cartesian product**, $\mathbb{Z}$[4], $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$.
  - Additional important terms are defined below.
- **Order** (of a set A): The number of elements of A (provided A is a finite set). *Also known as* **cardinality**. *Denoted by* $\boldsymbol{|A|}$.
- $\mathbb{Z}^+, \mathbb{Q}^+, \mathbb{R}^+$ denote the positive nonzero elements of $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, respectively.
- **Function** (from A to B). *Also known as* **map**. *Denoted by* $\boldsymbol{f : A \to B}$, $\boldsymbol{A \xrightarrow{f} B}$.
  - Additional function-adjacent definitions not defined below: **Domain**, **codomain**, **composition**, **injection**, **surjection**, **bijection**, **bijective correspondence**, and **restriction**.
- **Value** (of f at a): *Denoted by* $\boldsymbol{f(a)}$.
  - Implication: We apply functions on the left throughout the book.
- $\boldsymbol{f : a \mapsto b}$, $\boldsymbol{a \mapsto b}$, $\boldsymbol{f(a) = b}$ are all used interchangeably to describe the action of f on **elements**.
  - The middle one is used only when f is understood from the context.
- If f is not specified on elements but defined by a rule, we must check that it is **well-defined** for each element in its domain.

[4] The German word for numbers is "Zahlen."

- **Image** (of A under f): The following subset of B (the codomain of f). *Also known as* **range**. *Denoted by* $\boldsymbol{f(A)}$. *Given by*
$$f(A) = \{b \in B \mid b = f(a),\ a \in A\}$$
- **Preimage** (of $C \subset B$ under f): The following subset of A (the domain of f). *Also known as* **inverse image**. *Denoted by* $\boldsymbol{f^{-1}(C)}$. *Given by*
$$f^{-1}(C) = \{a \in A \mid f(a) \in C\}$$
- **Fiber** (of f over b): The preimage of $\{b\}$ under f.
  - f^{-1} is not, in general, a function since the fibers of f generally contain many elements, i.e., many elements of A in general map to the same B.
- **Left inverse** (of f): A function $g : B \to A$ such that $g \circ f : A \to A$ is the identity map on A.
- **Right inverse** (of f): A function $h : B \to A$ such that $f \circ h : B \to B$ is the identity map on B.
- **2-sided inverse** (of f): A function $g : B \to A$ such that $f \circ g$ is the identity map on B and $g \circ f$ is the identity map on A. *Also known as* **inverse**.
  - Implied to be unique by part (3) of Proposition 1.
- Relating properties of functions.

  Proposition 1. Let $f : A \to B$.

  1. f is injective iff f has a left inverse.
  2. f is surjective iff f has a right inverse.
  3. f is a bijection iff f has a 2-sided inverse.
  4. If A, B satisfy $|A| = |B|$, then $f : A \to B$ is bijective iff f is injective iff f is surjective.
- **Permutation** (of a set A): A bijection from A to itself.
- **Extension** (of g to B): The function $f : B \to C$ where $A \subset B$, $g : A \to C$, and $f|_A = g$.
  - Extensions need not exist nor be unique.
- **Representative** (of an equivalence class): Any element of the equivalence class.
  - Additional relation-adjacent terms: **Binary relation**, **reflexive**, **symmetric**, **transitive**, **equivalence relation**, **equivalence class**, **equivalent** (elements), and **partition**.
- The notions of an equivalence relation and a partition of A are the same.

  Proposition 2. Let A be a nonempty set.

  1. If $\sim$ defines an equivalence relation on A, then the set of equivalence classes of $\sim$ form a partition of A.
  2. If $\{A_i \mid i \in I\}$ is a partition of A, then there is an equivalence relation on A whose equivalence classes are precisely the sets A_i, $i \in I$.
- Assumed familiarity with induction proofs.

Properties of the Integers

- Many of the properties stated herein will be familiar from elementary arithmetic.
  - We state them now because we will need them in Part I (Group Theory).
  - However, we delay proofs until Chapter 8, when we prove them in the more general context of ring theory.
  - To avoid circular reasoning, the proofs in Chapter 8 will not rely on any result from Part I, so the full logical structure of this book is Ring Theory and then Group Theory, but it is presented the other way around for pedagogical purposes.
- **Well Ordering** (of $\mathbb{Z}$): Any nonempty subset $A \subset \mathbb{Z}^+$ contains a **minimal element** m satisfying $m \leq a$ for all $a \in A$.
- ***a* divides *b***: Two numbers $a, b \in \mathbb{Z}$ with $a \neq 0$ such that $b = ac$ for some $c \in \mathbb{Z}$. *Denoted by* $\boldsymbol{a \mid b}$.
  - If a doesn't divide b, then we write $\boldsymbol{a \nmid b}$.
- **Greatest common divisor** (of $a, b \in \mathbb{Z} \setminus \{0\}$[5]): The unique positive integer d satisfying
  1. $d \mid a$ and $d \mid b$. (d is a *common* divisor of a, b.)
  2. If $e \mid a$ and $e \mid b$, then $e \mid d$. (d is the *greatest* common divisor of a, b.)

  Also known as **g.c.d.** *Denoted by* $\boldsymbol{(a, b)}$.
- **Relatively prime** (numbers): Two numbers $a, b \in \mathbb{Z} \setminus \{0\}$ for which $(a, b) = 1$.
- **Least common multiple** (of $a, b \in \mathbb{Z} \setminus \{0\}$): The unique positive integer l satisfying
  1. $a \mid l$ and $b \mid l$. (l is a *common* multiple of a, b.)
  2. If $a \mid m$ and $b \mid m$, then $l \mid m$. (l is the *least* common multiple of a, b.)

  Also known as **l.c.m.**
- "The connection between the greatest common divisor d and the least common multiple l of two integers a and b is given by $dl = ab$" (Dummit & Foote, 2004, p. 4).
- **Division Algorithm**: If $a, b \in \mathbb{Z} \setminus 0$, then there exist unique $q, r \in \mathbb{Z}$ such that

$$a = qb + r \qquad\qquad 0 \leq r < |b|$$

- **Quotient**: The number q in the above definition.
- **Remainder**: The number r in the above definition.
- **Euclidean Algorithm**: A procedure for finding the greatest common divisor of two integers a and b by iterating the Division Algorithm. *Given by*

$$\begin{aligned} a &= q_0 b + r_0 \\ b &= q_1 r_0 + r_1 \\ r_0 &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n \\ r_{n-1} &= q_{n+1} r_n \end{aligned}$$

  This yields $(a, b) = r_n$.

[5] Dummit and Foote (2004) prefers the notation $\mathbb{Z} - \{0\}$ for set differences, but I will stick with what I know.

Proof. Existence of r_n: $|b| > |r_0| > |r_1| > \cdots |r_n|$ is a decreasing sequence of strictly positive integers and such a sequence cannot continue indefinitely.

The rest of the proof comes later. □

- Example of applying the Euclidean Algorithm given.
- (a, b) is a $\mathbb{Z}$-linear combination of a, b: In particular, there exist $x, y \in \mathbb{Z}$ such that

$$(a, b) = ax + by$$

Proof. Exploit the Euclidean Algorithm. Use the second-to-last line to write (a, b) in terms of r_{n-1}, r_{n-2}:

$$r_n = r_{n-2} - q_n r_{n-1}$$

Then use $r_{n-1} = r_{n-3} - q_{n-1} r_{n-2}$ to express r_n in terms of r_{n-2}, r_{n-3}. Go back and back until we express r_n in terms of a, b, and then combine terms. □

- Notes on the above result.
  - Previous example expanded to apply here.
  - Either x or y will be negative.
  - x and y are not unique. The general solution is known, though (see Exercise 0.2.4 and Chapter 8).
- **Prime** (number $p \in \mathbb{Z}^+$): A number $p \in \mathbb{Z}^+$ for which $p > 1$ and the only positive divisors of p are 1 and p.
- **Composite** (number $n \in \mathbb{Z}^+$): A number $n \in \mathbb{Z}^+$ for which $n > 1$ and n is not prime.
- Examples given.
- If p is a prime and $p \mid ab$ for some $a, b \in \mathbb{Z}$, then $p \mid a$ or $p \mid b$.
  - This property can be used to define the primes (see Exercise 0.2.3).
- **Fundamental Theorem of Arithmetic**: If $n \in \mathbb{Z}$ and $n > 1$, then n can be factored uniquely into the product of primes, i.e., there are distinct primes $p_1, p_2, \ldots, p_s$ and positive integers $\alpha_1, \alpha_2, \ldots, \alpha_s$ such that

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$$

  - This decomposition is unique.
- Let a, b be positive integers such that

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s} \qquad b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_s^{\beta_s}$$

are their prime factorizations (we let $\alpha_i, \beta_j \geq 0$ so that we can express both as the product of the same primes). Then

$$\gcd(a, b) = p_1^{\min(\alpha_1, \beta_1)} p_2^{\min(\alpha_2, \beta_2)} \cdots p_s^{\min(\alpha_s, \beta_s)}$$
$$\operatorname{lcm}(a, b) = p_1^{\max(\alpha_1, \beta_1)} p_2^{\max(\alpha_2, \beta_2)} \cdots p_s^{\max(\alpha_s, \beta_s)}$$

- **Euler φ-function**: The function $\varphi : \mathbb{Z}^+ \to \mathbb{Z}^+$ where $\varphi(n)$ is defined to be the number of positive integers $a \leq n$ such that $(a, n) = 1$.
  - If p prime, then $\varphi(p) = p - 1$.
  - If p prime and $a \geq 1$, then $\varphi(p^a) = p^a - p^{a-1} = p^{a-1}(p - 1)$.

- If $(a, b) = 1$, then $\varphi(ab) = \varphi(a)\varphi(b)$.
- If $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$, then

$$\begin{aligned}\varphi(n) &= \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \cdots \varphi(p_s^{\alpha_s}) \\ &= p_1^{\alpha_1 - 1}(p_1 - 1)p_2^{\alpha_2 - 1}(p_2 - 1) \cdots p_s^{\alpha_s - 1}(p_s - 1)\end{aligned}$$

- φ is used for many functions throughout the text, so when we wish to indicate the Euler φ-function, we do so explicitly.

Exercises

3. Prove that if n is composite, then there are integers a, b such that $n \mid ab$ but $n \nmid a$ and $n \nmid b$.

4. Let a, b, N be fixed integers with a, b nonzero, and let $d = (a, b)$. Suppose x_0, y_0 are particular solutions to $ax + by = N$ (i.e., $ax_0 + by_0 = N$). Prove that for any integer t, the integers

$$x = x_0 + \frac{b}{d}t \qquad\qquad y = y_0 - \frac{a}{d}t$$

are also solutions to $ax + by = N$ (this is, in fact, the general solution).

$\mathbb{Z}/n\mathbb{Z}$: The Integers Modulo n

- Fix $n \in \mathbb{Z}^+$.
- Define $\sim$ on $\mathbb{Z}$ by $a \sim b \iff n \mid (b - a)$.
  - We can prove that $\sim$ is an equivalence relation.
  - If $a \sim b$, we write $a \equiv b \pmod{n}$[6].
- **Congruence class** (of a mod n): The equivalence class of a mod n. *Also known as* **residue class**. *Denoted by* $\bar{\boldsymbol{a}}$. *Given by*

$$\begin{aligned}\bar{a} &= \{a + kn \mid k \in \mathbb{Z}\} \\ &= \{a, a \pm n, a \pm 2n, a \pm 3n, \dots\}\end{aligned}$$

  - There are n distinct equivalence classes mod n, namely $\bar{0}, \bar{1}, \dots, \overline{n-1}$, and collectively referred to as the **integers modulo n**.
  - The congruence classes differ for different n, so always be sure to fix n before discussing them.
- **Integers modulo n**: The set of equivalence classes under this equivalence relation. *Also known as* **integers mod n**. *Denoted by* $\mathbb{Z}/n\mathbb{Z}$[7]
- **Reducing a mod n**: The process of finding the equivalence class mod n of some integer a.
  - Also frequently refers to finding the **least residue** of a mod n.
- **Least residue** (of a mod n): The smallest nonnegative number congruent to a mod n.
- **Modular arithmetic** (on $\mathbb{Z}/n\mathbb{Z}$): The addition and multiplication operations defined by

$$\bar{a} + \bar{b} = \overline{a + b} \qquad\qquad \bar{a} \cdot \bar{b} = \overline{ab}$$

for all $\bar{a}, \bar{b} \in \mathbb{Z}/n\mathbb{Z}$.

[6] "a is congruent to b mod n."
[7] The motivation for this notation will become clear in the discussion of quotient groups and quotient rings.

  - In other words, take a representative element of both residue classes, add or multiply them, and then take the class containing the product to be the sum (resp. product).

- Example given to hint at the well-definedness of modular arithmetic.

- Proof that modular arithmetic is well-defined.

  Theorem 3. The operations of addition and multiplication on $\mathbb{Z}/n\mathbb{Z}$ defined above are both well-defined, that is, they do not depend on the choices of representatives for the classes involved. More precisely, if $a_1, a_2 \in \mathbb{Z}$ and $b_1, b_2 \in \mathbb{Z}$ with $\overline{a_1} = \overline{b_1}$ and $\overline{a_2} = \overline{b_2}$, then $\overline{a_1 + a_2} = \overline{b_1 + b_2}$ and $\overline{a_1 a_2} = \overline{b_1 b_2}$, i.e., if

  $$a_1 \equiv b_1 \pmod{n} \qquad a_2 \equiv b_2 \pmod{n}$$

  then

  $$a_1 + a_2 \equiv b_1 + b_2 \pmod{n} \qquad a_1 a_2 \equiv b_1 b_2 \pmod{n}$$

  Proof. Given. □

- Further comments on equivalence classes and the integers mod n.

  - Preview: Adding equivalence classes by their representatives is a special case of a more general construction (that of a **quotient**).
  - We should be familiar with manipulating equivalence classes from studying $\mathbb{Q}$ rigorously.
  - We should be familiar with modular arithmetic from timekeeping: 8 hours after 5:00 AM? Must be 13h00, but $13 \equiv 1 \pmod{1}2$ so 1:00 PM.
  - We do need to be able to think of equivalence classes as elements that can be manipulated in their own right. But it is important to remember that these *are* still equivalence classes at the end of the day.
  - Useful application of modular arithmetic: Computing the last two digits of 2^{1000} using the integers modulo 100.

- **$(\mathbb{Z}/n\mathbb{Z})^\times$**: The collection of residue classes which have a multiplicative inverse in $\mathbb{Z}/n\mathbb{Z}$. *Given by*

  $$(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid \exists\ \bar{c} \in \mathbb{Z}/n\mathbb{Z} : \bar{a} \cdot \bar{c} = \bar{1}\}$$

- An alternate form for $(\mathbb{Z}/n\mathbb{Z})^\times$.

  Proposition 4. $(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid (a, n) = 1\}$.

  Proof. See Exercises 0.3.10-0.3.14. □

- Further comments on $(\mathbb{Z}/n\mathbb{Z})^\times$.

  - The set given in Proposition 4 is well-defined since if $(a, n) = 1$, then we clearly have $(a+qn, n) = 1$ as well.
  - Explicit example given: $(\mathbb{Z}/9\mathbb{Z})^\times$.
  - Computing the multiplicative inverse of $\bar{a}$: Let $(a, n) = 1$. Then the Euclidean algorithm generates integers x, y such that $ax + ny = 1$. But this implies that $ax = 1 + (-y)n$, i.e., $ax \equiv 1 \bmod n$. Therefore, $\bar{a} \cdot \bar{x} = \bar{1}$, so $\bar{x}$ is the multiplicative inverse of $\bar{a}$.

Exercises

10. Prove that the number of elements of $(\mathbb{Z}/n\mathbb{Z})^\times$ is $\varphi(n)$ where φ denotes the Euler φ-function.

11. Prove that if $\bar{a}, \bar{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$, then $\bar{a} \cdot \bar{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$.

12. Let $n \in \mathbb{Z}$, $n > 1$, and let $a \in \mathbb{Z}$, $1 \leq a \leq n$. Prove that if a, n are not relatively prime, then there exists an integer b with $1 \leq b < n$ such that $ab \equiv 0 \pmod{n}$ and deduce that there cannot be an integer c such that $ac \equiv 1 \pmod{n}$.

13. Let $n \in \mathbb{Z}$, $n > 1$, and let $a \in \mathbb{Z}$, $1 \leq a \leq n$. Prove that if a, n are relatively prime, then there exists an integer c with such that $ac \equiv 1 \pmod{n}$ [use the fact that the g.c.d. of two integers is a $\mathbb{Z}$-linear combination of the integers].

14. Conclude from the previous two exercises that $(\mathbb{Z}/n\mathbb{Z})^\times$ is the set of elements $\bar{a}$ of $\mathbb{Z}/n\mathbb{Z}$ with $(a, n) = 1$ and hence probe Proposition 4. Verify this directly in the case $n = 12$.

1.7 Chapter 1: Introduction to Groups

From Dummit and Foote (2004).

A Word on Group Theory

12/5:

- History of and motivation for group theory and abstract algebra in general.
- Power of the abstract approach:
  - Results for a number of examples are obtained from a single result for the abstraction.
  - General theorems allow specific theorems of interest to be recovered as a special case, while more broadly illustrating the connections between related results.
- **Groups** were abstracted from extremely old problems in algebraic equations, number theory, and geometry, all of which were found to have related solutions.
  - Examples given.
- "One of the essential characteristics of mathematics is that after applying a certain algorithm or method of proof, one then considers the scope and limits of the method. As a result, properties possessed by a number of interesting objects are frequently abstracted and the question raised; can one determine *all* the objects possessing these properties? Attempting to answer such a question also frequently adds considerable understanding of the original objects under consideration" (Dummit & Foote, 2004, p. 13).
- "It is important to realize, with or without the historical context, that the reason the abstract definitions are made is because it is useful to isolate specific characteristics and consider what structure is imposed on an object having these characteristics" (Dummit & Foote, 2004, p. 15).
  - Structure of algebraic objects is a major and recurring theme throughout the text.

Basic Axioms and Examples

- Goal: Introduce the algebraic structure studied in Part I and give some examples.
- **Binary operation** (on a set G): A function from $G \times G$ to G. *Denoted by* $\star$.
  - Additional binary operation-adjacent definitions: **Associative**, **commutative** (binary operation).
- Examples of commutative/noncommutative and associative/nonassociative operations given.

- **Closed** (subset $H \subset G$ under $\star$): A subset $H \subset G$ such that $a \star b \in H$ for all $a, b \in H$, where $\star$ is a binary operation on G.
  - Alternatively, we can require that $\star|_H$ be a binary operation on H.
  - $\star$ associative/commutative on G implies $\star|_H$ associative/commutative on H.
- If $\star$ is an associative (respectively, commutative) binary operation on G and $\star|_H$ is a binary operation on $H \subset G$, then $\star$ is associative (respectively, commutative) on H as well.
- **Group**: An ordered pair $(G, \star)$ where G is a set and $\star$ is a binary operation on G satisfying the following axioms:
  (i) *Associativity*: $(a \star b) \star c = a \star (b \star c)$ for all $a, b, c \in G$.
  (ii) *Identity*: There exists an element $e \in G$ such that for all $a \in G$, $a \star e = e \star a = a$.
  (iii) *Inverses*: For all $a \in G$, there exists an element $a^{-1} \in G$ such that $a \star a^{-1} = a^{-1} \star a = e$.
- **Abelian** (group): A group $(G, \star)$ such that for all $a, b \in G$, $a \star b = b \star a$. *Also known as* **commutative**.
- Informally, we may call G a group under $\star$ or, if $\star$ is clear from context, G alone a group.
- **Finite group**: A group G for which G is a finite set.
- Axiom (ii) implies that G is nonempty.
- Examples of groups given (and justified).
  1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.
  2. $(\mathbb{Q} \setminus \{0\})^\times$, $(\mathbb{R} \setminus \{0\})^\times$, $(\mathbb{C} \setminus \{0\})^\times$, $(\mathbb{Q}^+)^\times$, $(\mathbb{R}^+)^\times$.
  3. A vector space under vector addition.
  4. $\mathbb{Z}/n\mathbb{Z}$.
  5. $(\mathbb{Z}/n\mathbb{Z})^\times$.
  6. **Direct product** of groups $(A, \star)$ and $(B, \diamond)$.
- **Direct product** (of $(A, \star)$ and $(B, \diamond)$): The group $A \times B$ whose elements are those in the Cartesian product
$$A \times B = \{(a, b) \mid a \in A,\ b \in B\}$$
and whose operation is defined component-wise by
$$(a_1, b_1)(a_2, b_2) = (a_1 \star a_2, b_1 \diamond b_2)$$
- Basic properties of groups.

  Proposition 5. Let G be a group under the operation $\star$.
  1. The identity of G is unique.
  2. For each $a \in G$, a^{-1} is uniquely determined.
  3. $(a^{-1})^{-1} = a$ for all $a \in G$.
  4. $(a \star b)^{-1} = (b^{-1}) \star (a^{-1})$.
  5. **Generalized associative law**: For any $a_1, \ldots, a_n \in G$, the value of $a_1 \star \cdots \star a_n$ is independent of how the expression is bracketed.

  Proof. Given. □

- Further notational simplification:

$$\star \mapsto \cdot \qquad a \cdot b \mapsto ab \qquad (ab)c \mapsto abc \qquad e \mapsto 1 \qquad \underbrace{xx \cdot x}_{n \text{ times}} \mapsto x^n \qquad (x^{-1})^n \mapsto x^{-n} \qquad x^0 \mapsto 1$$

  - Note that the operation we're using for a given group can alter the above.
  - For example, when the operation is $+$, we let $e \mapsto 0$, $x + \cdots + x$ (n times) be written as nx, $-a - a - \cdots - a$ (n times) be written as $-nx$, and $0x = 0$.

- Cancellation lemma.

  Proposition 6. Let G be a group and let $a, b \in G$. The equations $ax = b$ and $ya = b$ have unique solutions for $x, y \in G$. In particular, the left and right cancellation laws hold in G, i.e.,

  1. If $au = av$, then $u = v$;
  2. If $ub = vb$, then $u = v$.

  Proof. Given. □

- Corollary: Either $ab = e$ or $ba = e$ implies $b = a^{-1}$ directly; we don't have to verify the other if we only know one.

- Corollary: Either $ab = a$ or $ba = a$ implies $b = e$.

  - Related to the previous one.

- **Order** (of x): The smallest positive integer n such that $x^n = 1$. *Denoted by* $\boldsymbol{|x|}$.

  - We say x is of order n.
  - If no such n exists, the order of x is defined to be infinity and x is said to be of infinite order.
  - Note that $|\cdot|$ means different things in the contexts $|g|$ and $|G|$ (so be careful), but the uses are naturally related since the order of g is equal to the cardinality of the set of all its (distinct) powers (see Proposition 8).

- Examples.

  - $|g| = 1$ iff $g = e$.
  - Others given.

- **Multiplication table** (of a finite group): The $n \times n$ matrix whose i, j entry is the group element $g_i g_j$, where $G = \{g_1, \ldots, g_n\}$ and $g_1 = e$. *Also known as* **group table**.

  - Contains all group information, but is a computationally and visually unwieldy object. Does not easily reveal deeper relations.
  - Analogy: A multiplication table is like having a list of the distances between every US city; what would be far more useful is a map with such distances labeled on it.

- A goal going forward: Develop a better visualization of the internal structure of groups.

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	
$\mathbb{Z}/n\mathbb{Z}$	$\{0, 1, \ldots, n-1\}$	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		

⟶

	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*

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

  - 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:

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

  - 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 $\{1, \ldots, n\}$ 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 $a_1, \ldots, a_k$ are distinct elements of $[n]$. *Denoted by* $\boldsymbol{(a_1, a_2, \ldots, a_k)}$.

- 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.

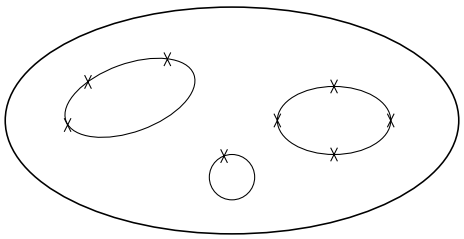


Figure 2.2: Decomposing σ into disjoint cycles.

- 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

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

  □

  (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

$$\begin{matrix} 1 & 3 \\ 2 & 4 \\ 3 & 2 \\ 4 & 1 \end{matrix}$$

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,

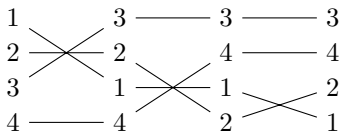


Figure 2.3: Generating S_n with 2-cycles.

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

- S_n is also generated by

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

  - 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 $\tau = (1,2,\ldots,n)$. 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 $p(n)$.

2.6 Chapter 1: Introduction to Groups

From Dummit and Foote (2004).

Dihedral Groups

12/5:
- **Dihedral group**: A group whose elements are symmetries of regular planar figures.
- D_{2n} denotes the group of symmetries of a regular n-gon for $n \geq 3$.
- **Symmetry**: Any rigid motion which can be effected by taking a copy of a shape, moving this copy in any fashion in 3 space, and then placing the copy back on the original so that it exactly covers it.
- Describe symmetries mathematically by labeling the vertices of a regular n-gon from $1, \ldots, n$ and mapping each symmetry s to the unique corresponding permutation σ of $\{1, \ldots, n\}$.
  - Make it a group by letting function composition be the group operation. (Function composition is naturally associative.)
- Note that $|D_{2n}| = 2n$.

  - "Since symmetries are rigid motions, one sees that once the position of the ordered pair of vertices 1,2 has been specified, the action of the symmetry on all remaining vertices is completely determined" (Dummit & Foote, 2004, p. 24).
  - Thus, there are $n \cdot 2$ possible rigid motions (sending vertex one to any of the n options, and then vertex two to one of the 2 adjacent positions).

- The elements of D_{2n} are the n rotations by $2\pi i/n$ about the center of the n-gon, and the n reflections about the n lines of symmetry (which may come in one type or two; see Figure 3.2).

- Abstracting D_{2n}: Fix a regular n-gon centered at the origin in the xy-plane and label the vertices consecutively from 1 to n in a clockwise manner. Let r be the rotation clockwise about the origin through $2\pi/n$ radians. Let s be the reflection about the line of symmetry through vertex 1 and the origin. Then

  1. $1, r, r^2, \ldots, r^{n-1}$ are distinct and $r^n = 1$, so $|r| = n$.
  2. $|s| = 2$.
  3. $s \neq r^i$ for any i.
  4. $sr^i \neq sr^j$ for all $0 \leq i,\ j \leq n-1$ with $i \neq j$, so
  $$D_{2n} = \{1, \ldots, r^{n-1}, s, \ldots, sr^{n-1}\}$$
  In other words, each element of D_{2n} can be written uniquely in the form $s^k r^i$ for some $k = 0, 1$ and $0 \leq i \leq n-1$.
  5. $rs = sr^{-1}$. Thus, r, s do not commute so D_{2n} is non-abelian.
  6. $r^i s = sr^{-i}$ for all $0 \leq i \leq n$. This indicates how to commute s with powers of r.

- Relations (1), (2), and (6) allow us to simplify any product of two elements $s^{i_1} r^{i_2} s^{i_3} r^{i_4} \cdots$ to a product of the form $s^i r^j$.

- Note that r, s in the above example are **generators**, which will only be rigorously introduced later but are useful now and thus used informally.
  - Detailed discussion: Section 2.4. Rigorous treatment (with **free groups**): Section 6.3.

- **Generators** (of G): A subset $S \subset G$ with the property that every element in G can be written as a (finite) product of elements of S and their inverses.
  - We write $G = \langle S \rangle$ and say that "G is generated by S" or "S generates G."
  - Examples: $\mathbb{Z} = \langle 1 \rangle$ and $D_{2n} = \langle r, s \rangle$.
  - Later: We need not include the inverses of the elements of S as generators.

- **Relation** (in G): An equation in a general group G that the generators satisfy.
  - Example: In D_{2n}, we have $r^n = 1$, $s^2 = 1$, and $rs = sr^{-1}$. These relations have the additional property that *any* other relation may be deduced from them (since we can determine exactly when two group elements are equal using these), motivating the following.

- **Presentation** (of G): The set S of generators of G along with the relations $R_1, \ldots, R_m$, where each R_i is an equation in the elements from $S \cup \{1\}$, such that any relation among the elements of S can be deduced from these. *Denoted by* $G = \langle \boldsymbol{S \mid R_1, \ldots, R_m} \rangle$.
  - Example: $D_{2n} = \left\langle r, s \mid r^n = s^2 = 1,\ rs = sr^{-1} \right\rangle$. This is far easier to work with than the motivating geometric description.
  - Limitations of presentations: It may be difficult (or impossible) to tell from a given presentation when two elements of the group are equal, what the order is, or even whether a group is finite or infinite.

- Dummit and Foote (2004) list examples and works with **collapsing** presentations, i.e., ones in which some important relations are consequences of others.
  - Dummit and Foote (2004) deduce that $X_{2n} = \langle x, y \mid x^n = y^2 = 1,\ xy = yx^2 \rangle$ has order at most 6, even though this is highly counterintuitive.
  - Groups with two generators and a relation $x^n = y^2 = 1$ have order *at most* $2n$, but may collapse much more, even down to the trivial group. D_{2n} has order $2n$ because we know by independent (geometric) means that such a group exists; finding such "lower bound" groups for other presentations can be much harder.
  - More on group presentations in Section 6.3.

Symmetric Groups

- **Symmetric group** (on the set Ω): The group $(S_\Omega, \circ)$, where S_Ω is the set of all bijections from a nonempty set Ω to itself and $\circ$ is function composition. *Also known as* **permutations** (of Ω).
  - We write $\sigma \in S_\Omega$ and let $1 \in S_\Omega$ be the identity function defined by $1(a) = a$ for all $a \in \Omega$.
  - If $\Omega = [n]$, then we denote S_Ω by S_n.
- **Symmetric group** (of degree n): The symmetric group on the set $\{1, 2, \ldots, n\}$. *Denoted by* $\boldsymbol{S_n}$.
  - Section 1.6: The structure of S_Ω depends only on the cardinality of Ω, i.e., if $|\Omega| = n$, then S_Ω "looks like" S_n.
  - S_n will be studied in its own right and used to illustrate/motivate general group theory often throughout the text.
- $|S_n| = n!$.
  - Derivation for this presented as well.
- **Cycle**: A string of integers which represents the element of S_n which cyclically permutes these integers (and fixes all other integers).
  - The cycle $(a_1\ a_2\ \ldots\ a_m)$ is the permutation which sends a_i to a_{i+1} for all $1 \leq i \leq m-1$ and sends a_m to a_1.
- **Cycle decomposition** (of σ): The product of all cycles describing part of the action of σ. *Given by*

$$(a_1\ a_2\ \ldots\ a_{m_1})(a_{m_1+1}\ a_{m_1+2}\ \ldots\ a_{m_2})\ldots(a_{m_{k-1}+1}\ a_{m_{k-1}+2}\ \ldots\ a_{m_k})$$

- Cycle decomposition algorithm (proof in Chapter 4):
  1. To start a new cycle, pick the smallest element of $[n]$ which has not yet appeared in a previous cycle — call it a (if you are just starting, choose $a = 1$); begin the new cycle: "$(a$".
  2. Read off $\sigma(a)$ from the given description of σ — call it b. If $b = a$, close the cycle with a right parenthesis (without writing b down); this completes a cycle — return to step 1. If $b \neq a$, write b next to a in this cycle: "$(a\ b$".
  3. Read off $\sigma(b)$ from the given description of σ — call it c. If $c = a$, close the cycle with a right parenthesis to complete the cycle — return to step 1. If $c \neq a$, write c next to b in this cycle: "$(a\ b\ c$". Repeat this step using the number c as the new value for b until the cycle closes.
  4. Remove all cycles of **length** 1.

- Example:

$$\begin{array}{llll} \sigma(1) = 12 & \sigma(2) = 2 & \sigma(3) = 3 & \sigma(4) = 1 \\ \sigma(5) = 11 & \sigma(6) = 9 & \sigma(7) = 5 & \sigma(8) = 10 \\ \sigma(9) = 6 & \sigma(10) = 4 & \sigma(11) = 7 & \sigma(12) = 8 \end{array}$$

  becomes

$$\sigma = (1\ 12\ 8\ 10\ 4)(5\ 11\ 7)(6\ 9)$$

- **Length** (of a cycle): The number of integers which appear in it.
- ***t*-cycle**: A cycle of length t.
- **Disjoint** (cycles): Two cycles that have no numbers in common.
- The convention of removing all cycles of length 1 makes it so that any cyclic decomposition essentially represents a bijection on the infinite set $\mathbb{N}$, not just $[n]$; in particular, σ can be though of as a function $\sigma : \mathbb{N} \to \mathbb{N}$.
  - Thus, $\sigma \in S_n$ is represented by the same cycle decomposition when it's an element of S_m, $m \geq n$.
  - The cycle decomposition for the identity element of S_n is taken to be 1.
- For any $\sigma \in S_n$, the cyclic decomposition of σ^{-1} is obtained by writing the numbers in each cycle of the cycle decomposition of σ in reverse order.
  - Continuing with the above example, $\sigma^{-1} = (4\ 10\ 8\ 12\ 1)(7\ 11\ 5)(9\ 6)$.
- Dummit and Foote (2004) covers computing products of cycle decompositions.
- S_n is a non-abelian group for all $n \geq 3$.
- Disjoint cycles commute.
- We can permute the disjoint cycles in a cycle decomposition and rotate (cyclically permute) the elements of a given cycle without affecting the identity of the cycle decomposition.
  - Convention: Smallest number written first in a cycle, and cycle containing the smallest number written first.
  - Thus, a cycle decomposition is "the *unique* way of expressing a permutation as a product of disjoint cycles (up to rearranging its cycles and cyclically permuting the numbers within each cycle)" (Dummit & Foote, 2004, p. 32).
- The order of a permutation is the l.c.m. of the lengths of the cycles in its cycle decomposition.

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 $x_1, x_2, \cdots \in G$. We can let $H = \langle x_1, x_2, \ldots \rangle$, i.e., H is the group **generated** by $x_1, x_2, \ldots$. In other words, H is the set of all finite products $x_1, x_1^{-1}, x_2, x_2^{-1}, \ldots$.
  - 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* $\mathbf{im}\,\boldsymbol{\phi}$.
- **Kernel** (of ϕ): The subset of H containing all $h \in H$ such that $\phi(h) = e_G$. *Denoted by* $\mathbf{ker}\,\boldsymbol{\phi}$.
- 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 numbers. The index of H in G 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

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

- **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* $\boldsymbol{D_{2n}}$.
- 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 $(1, 2, \ldots, n)$.
  - 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 $e, r, r^2, \ldots, r^{n-1}$.
  2. The elements $s, sr, sr^2, \ldots, sr^{n-1}$.

  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

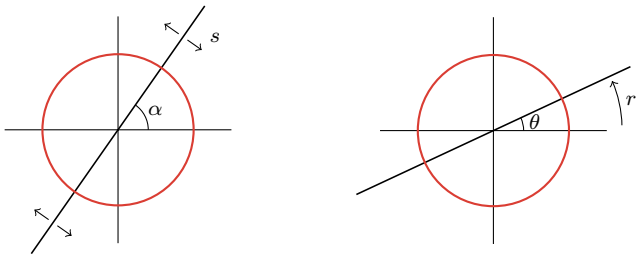
$$rs = sr^{-1}$$

– 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

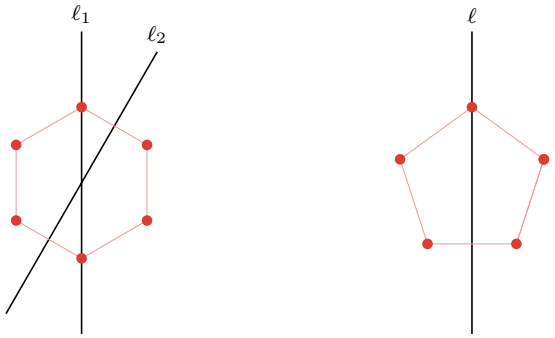
$$gsr^ig^{-1} = r^jsr^ir^{-j} = sr^{-j}r^ir^{-j} = sr^{i-2j}$$

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

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

    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,
  $$gh = gh' \iff h = h'$$
  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. □

3.8 Chapter 1: Introduction to Groups

From Dummit and Foote (2004).

Matrix Groups

12/5:

- Used for illustrative purposes in Part I, and studied in detail with vector spaces later on.
- **Field**: A set F together with two binary operations $+$ and $\cdot$ on F such that $(F, +)$ is an abelian group with identity 0, $(F - \{0\}, \cdot)$ is an abelian group, and the following **distributive law** holds:
  $$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$
  for all $a, b, c \in F$.
  - The "smallest" mathematical structure in which we can perform all the arithmetic operations $+$, $-$, $\times$, and $\div$ (division by nonzero elements).
  - Fields will be studied more thoroughly later; for now, it suffices to know $\mathbb{Q}$, $\mathbb{R}$, and the finite fields $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ for p prime.
- $\boldsymbol{F^\times}$: The set $F - \{0\}$ where F is a field.
- Linear algebra (vector space theory, matrices and linear transformations, and determinants) over $\mathbb{R}$ is true *mutatis mutandis*[2] over an arbitrary field F.
- **General linear group of degree n**: The set of all $n \times n$ matrices, where $n \in \mathbb{Z}^+$, whose entities come from the field F and whose determinant is nonzero. *Denoted by* $\boldsymbol{GL_n(F)}$.
  - We can compute the determinant $\det(A)$ of a matrix A with entries in F using the same formulas applied when $F = \mathbb{R}$.
  - The product of two matrices A, B with entries in F is also computed by using the familiar formula.
  - $\det(AB) = \det(A) \cdot \det(B)$ implies that for $A, B \in GL_n(F)$ (i.e., $\det(A) \neq 0 \neq \det(B)$), AB will also have nonzero determinant and hence $AB \in GL_n(F)$ as well. Thus, $GL_n(F)$ is closed under matrix multiplication.

[2] Def: Making the necessary adjustments while not affecting the main point.

  - $\det(A) \neq 0$ still implies the existence of A^{-1}.
  - Compute inverses can be done with the same familiar adjoint formula.

- Useful results (proven in Part III).
  - If F is a field and $|F| < \infty$, then $|F| = p^m$ for some prime p and integer m.
  - If $|F| = q < \infty$, then $|GL_n(F)| = (q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1})$.

Exercises

The next exercise introduces the **Heisenberg group** over the field F and develops some of its basic properties. When $F = \mathbb{R}$, this group plays an important role in quantum mechanics and signal theory by giving a group theoretic interpretation (due to H. Weyl) of Heisenberg's Uncertainty Principle. Note also that the Heisenberg group may be defined more generally, for example, with entries in $\mathbb{Z}$.

11. Let

$$H(F) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \middle| \, a, b, c \in F \right\}$$

be the **Heisenberg group** over F. Let

$$X = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \qquad Y = \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix}$$

be elements of $H(F)$.

(a) Compute the matrix product XY and deduce that $H(F)$ is closed under matrix multiplication. Exhibit explicit matrices such that $XY \neq YX$ (so that $H(F)$ is always non-abelian).

(b) Find an explicit formula for the matrix inverse X^{-1} and deduce that $H(F)$ is closed under inverses.

(c) Prove the associative law for $H(F)$ and deduce that $H(F)$ is a group of order $|F|^3$. (Do not assume that matrix multiplication is associative.)

(d) Find the order of each element of the finite group $H(\mathbb{Z}/2\mathbb{Z})$.

(e) Prove that every nonidentity element of the group $H(\mathbb{R})$ has infinite order.

The Quaternion Group

- **Quaternion group**: The group defined as follows. *Denoted by* $\boldsymbol{Q_8}$. *Given by*

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$$

where the product $\cdot$ is described by

$$1 \cdot a = a \cdot 1 = a \qquad \text{for all } a \in Q_8$$
$$(-1) \cdot (-1) = 1$$
$$(-1) \cdot a = a \cdot (-1) = -a \qquad \text{for all } a \in Q_8$$

$$i \cdot i = j \cdot j = k \cdot k = -1$$

$i \cdot j = k$	$j \cdot k = i$	$k \cdot i = j$
$j \cdot i = -k$	$k \cdot j = -i$	$i \cdot k = -j$

- Associativity can be tediously checked by explicit computation, or by less computational means later on.

- Q_8 is a non-abelian group of order 8.

Homomorphisms and Isomorphisms

- Goal: Quantify when two groups "look the same."
  - We say this happens when there exists an **isomorphism** between them. We'll first define a **homomorphism**, though. This latter concept we'll discuss in much greater detail later.
- **Homomorphism**: A map $\varphi : G \to H$ such that the following equality holds for all $x, y \in G$, where $(G, \star)$ and $(H, \diamond)$ are groups.
$$\varphi(x \star y) = \varphi(x) \diamond \varphi(y)$$
  - Without explicit group operations, we have the form $\varphi(xy) = \varphi(x)\varphi(y)$. This form will commonly show up, but it is important to remember the distinction between group operations.
  - Intuitively, a map is a homomorphism if it "respects the group structures of its domain and codomain" (Dummit & Foote, 2004, p. 37).
- **Isomorphism**: A bijective homomorphism.
  - If an isomorphism exists from G to H, we write that G and H are **isomorphic**, are of the same **isomorphism type**, and that $\boldsymbol{G \cong H}$.
  - Intuitively, such a map implies that G and H are the same group; the elements have simply been relabeled from one to the other.
- The existence of an isomorphism between two groups implies that any property of G that can be derived from the group axioms also holds for H, and vice versa.
- Isomorphisms formally justify writing all group actions as $\cdot$ since groups $(G, \star)$ and $(G, \cdot)$ where $\star, \cdot$ are defined the same are isomorphic.
- $\cong$ is an equivalence relation.
- **Isomorphism class**: An equivalence class of a nonempty collection $\mathcal{G}$ of groups under $\cong$.
- $\exp : \mathbb{R} \to \mathbb{R}^+$ defined by $\exp(x) = \mathrm{e}^x$ is an isomorphism from $(\mathbb{R}, +)$ to $(\mathbb{R}^+, \times)$.
  - $\mathrm{e}^{x+y} = \mathrm{e}^x \mathrm{e}^y$.
- $|\triangle| = |\Omega| \iff S_\triangle \cong S_\Omega \iff |S_\triangle| = |S_\Omega|$.
- We will define new notions of isomorphisms for other algebraic structures (e.g., rings, fields, vector spaces, etc.).
- **Classification theorem**: A theorem stating what properties of a structure specify its isomorphism type.
  - Finding classification theorems is a central problem in mathematics.
  - A general classification theorem would assert that if G is an object with some structure (such as a group) and G has property $\mathcal{P}$, then any other similarly structured object (group) X with property $\mathcal{P}$ is isomorphic to G.
- Example: Any non-abelian group of order 6 is isomorphic to S_3.
  - Utility: Allows us to obtain $D \cong S_3$ and $GL_2(\mathbb{F}_2) \cong S_3$ without having to find explicit maps between said groups.
- **Classification**: A theorem stating what properties of a structure specify that it is isomorphic to one of more than one distinct objects.
  - Less specific conclusions, but simpler property $\mathcal{P}$ to check compared to a classification theorem.
- Example: Any group of order 6 is isomorphic to S_3 or $\mathbb{Z}/6\mathbb{Z}$.

  - We don't get an isomorphism type, but we can check "$|G| = 6$" more easily than "$|G| = 6$ and non-abelian."

- Conditions that allow us to rule out two groups G, H being isomorphic: If $\varphi : G \to H$ is an isomorphism, then

  1. $|G| = |H|$.
  2. G is abelian iff H is abelian.
  3. For all $x \in G$, $|x| = |\varphi(x)|$.

- "Let G be a finite group of order n for which we have a presentation and let $S = \{s_1, \ldots, s_m\}$ be the generators. Let H be another group and $\{r_1, \ldots, r_m\}$ be elements of H. Suppose that any relation satisfied in G by the s_i is also satisfied in H when each s_i is replaced by r_i. Then there is a unique homomorphism $\varphi : G \to H$ which sends $s_i \mapsto r_i$" (Dummit & Foote, 2004, pp. 38–39).

  - If $\{r_1, \ldots, r_m\}$ generate H, then φ is surjective. If in addition $|G| = |H| < \infty$, then φ is injective, and φ is an isomorphism.
  - Intuitively, we can map the generators of G to any elements of H and obtain a homomorphism provided that the relations in G are still satisfied.

- Examples:

  - Let $k \geq 3$ be such that $k \mid n$. Then since $a^k = 1$ implies $a^n = 1$, and we can obtain a homomorphism $\varphi : D_{2n} \to D_{2k}$.
  - Mapping $r \in D_6$ to (1 2 3) $\in S_3$ and $s \in D_6$ to (1 2) $\in S_3$ yields an isomorphism.

- Corresponding statement from vector spaces: Let V, W be vector spaces and S a basis for V. Then we can specify $T : V \to W$ a linear transformation by its action on S. If $\dim W = \dim V$ and $T(S)$ spans W, then T is a vector space isomorphism.

Group Actions

- **Group action** (of a group G on a set A): A map $\cdot : G \times A \to A$ such that $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$ for all $g_1, g_2 \in G$ and $a \in A$, and such that $1 \cdot a = a$ for all $a \in A$.

- Let G act on A, and for each $g \in G$, define $\sigma_g : A \to A$ by $\sigma_g(a) = g \cdot a$. Then

  1. For each fixed $g \in G$, σ_g is a permutation of A;

     Proof. We prove that σ_g has a two-sided inverse; it follows that σ_g is a permutation by Proposition 1. Let $g \in G$ be arbitrary. Then by Axiom (iii), there exists g^{-1}. Therefore,

     $$\begin{aligned}(\sigma_{g^{-1}} \circ \sigma_g)(a) &= \sigma_{g^{-1}}(\sigma_g(a)) \\ &= g^{-1} \cdot (g \cdot a) \\ &= (g^{-1} \cdot g) \cdot a \\ &= 1 \cdot a \\ &= a\end{aligned}$$

     We can prove something similar in the other direction. □

  2. The map from G to S_A defined by $g \mapsto \sigma_g$ is a homomorphism.

     Proof. Let $\varphi : G \to S_A$ be defined by $\varphi(g) = \sigma_g$ for all $g \in G$. To prove that φ is a homomorphism, it will suffice to show that $\varphi(g_1 \cdot g_2) = \varphi(g_1) \circ \varphi(g_2)$ for all $g_1, g_2 \in G$. To verify the equality

of functions, we must show that for all $a \in A$, $\varphi(g_1 \cdot g_2)(a) = (\varphi(g_1) \circ \varphi(g_2))(a)$. Let a be an arbitrary element of A. Then

$$\begin{aligned}\varphi(g_1 \cdot g_2)(a) &= \sigma_{g_1 \cdot g_2}(a) \\ &= (g_1 \cdot g_2) \cdot a \\ &= g_1 \cdot (g_2 \cdot a) \\ &= g_1 \cdot \sigma_{g_2}(a) \\ &= \sigma_{g_1}(\sigma_{g_2}(a)) \\ &= (\sigma_{g_1} \circ \sigma_{g_2})(a) \\ &= (\varphi(g_1) \circ \varphi(g_2))(a)\end{aligned}$$

□

- Intuitively, a group action of G on A means that every element $g \in G$ acts as a permutation on A in a manner consistent with the group operations in G.
- **Permutation representation** (associated to the group action $\cdot$): The homomorphism $\varphi : G \to S_A$ defined by $\varphi(g)(a) = \sigma_g(a) = g \cdot a$ for all $g \in G$, $a \in A$.
- **Left** (action): A group action where the elements of G act on the elements of A from the left.
  - Group actions, as we have defined them, are left actions.
- **Right** (action): A group action where the elements of G act on the elements of A from the right.
- **Trivial action**: The group action defined by $g \cdot a = a$ for all $g \in G$, $a \in A$.
  - G is said to **act trivially** on A.
  - The associated permutation representation is the **trivial homomorphism**.
- **Trivial homomorphism**: The homomorphism $\varphi : G \to H$ sending all $g \in G$ to $1 \in H$.
- **Faithful** (group action): A group action for which distinct elements of G induce distinct permutations of A.
  - The associated permutation representation is injective.
- **Kernel** (of a group action): The set of $g \in G$ that fix all elements of A.
- Examples:
  - If V is a vector field taken over F, then scalar multiplication can be described as the action of $F^\times$ on V.
  - S_A acts on A by $\sigma \cdot a = \sigma(a)$; the associated permutation representation is the identity map from S_A to itself.
  - D_{2n} acts on $[n]$ in a manner consistent with the geometric picture. This action is faithful (since, geometrically, distinct symmetries induce distinct permutations of the vertices).
  - The **left regular action** of G on itself. This action is faithful (by the cancellation lemma).
  - Further examples appear in the exercises.
- **Left regular action** (of G on itself): The group action where $A = G$ defined by $g \cdot a = ga$, i.e., where the group operation is left multiplication within the group. *Also known as* **left translation** [when G is additive and thus $a \mapsto g + a$].

3.9 Chapter 2: Subgroups

From Dummit and Foote (2004).

Definition and Examples

- Two way of unraveling the structure of an axiomatically defined mathematical object are to study subsets of the object that satisfy the same axioms, and to study quotients (which, roughly speaking, collapse one group onto a smaller one).
  - Here, we study subgroups and quotient groups. Later, we will study subrings and quotient rings of a ring, subspaces and quotient spaces of a vector space, etc.
- **Subgroup** (of G): A nonempty subset $H \subset G$ that is closed under products and inverses. *Denoted by* $\boldsymbol{H \leq G}$.
  - In other words, we require that $x^{-1} \in H$ for all $x \in H$, and $xy \in H$ for all $x, y \in H$.
  - Alternatively, a subgroup of $(G, \cdot)$ is a subset of G that is a group in its own right under $\cdot$.
  - It is possible for a subset $H \subset G$ to have the structure of a group with respect to some operation other than the one on G (e.g., $(\mathbb{Q}, +)$ and $(\mathbb{Q} \setminus \{0\}, \times)$), but we do not refer to this subset as a *subgroup*.
  - Any equation in the elements of H may be viewed as an equation in the elements of G. Consequences:
    - Every subgroup must contain 1, the identity of G.
    - The inverse of $x \in G$ is the same as the inverse of $x \in H$, i.e., x^{-1} is indeed unambiguous notation.
- $H \leq G$ and $H \neq G$ imply $H < G$.
- Examples of groups and some of their subgroups given.
- **Trivial subgroup**: The subgroup $H = \{1\}$. *Denoted by* $\mathbf{1}$.
- $\leq$ is transitive: $K \leq H \leq G \implies K \leq G$.
- Let G be a group.

  Proposition 7 (The Subgroup Criterion)**.** A subset $H \subset G$ is a subgroup iff

  1. $H \neq \emptyset$;
  2. For all $x, y \in H$, $xy^{-1} \in H$.

  Furthermore, if H is finite, then it suffices to check that H is nonempty and closed under multiplication.

  Proof. Given. □

Centralizers and Normalizers, Stabilizers and Kernels

- Goal: Introduce important families of subgroups for an arbitrary group G.
- Let A be a nonempty subset of G.
- **Centralizer** (of A in G): The set defined as follows. *Denoted by* $\boldsymbol{C_G(A)}$. *Given by*

$$C_G(A) = \{g \in G \mid gag^{-1} = a \ \forall \ a \in A\}$$

  - $C_G(A)$ is the set of all elements in G which commute with every element of A, since $gag^{-1} = a$ is an equivalent condition to $ga = ag$.
  - If $A = \{a\}$, we write $C_G(a)$ instead of $C_G(\{a\})$.
    - In this case, $a^n \in C_G(a)$ for all $n \in \mathbb{Z}$.
- $C_G(A) \leq G$.

Proof. Use the subgroup criterion (Proposition 7).

Criterion 1: Since $1a1^{-1} = 1a1 = a$ for all $a \in A$, $1 \in C_G(A)$. Thus, $C_G(A)$ is nonempty.

Criterion 2: Let $x, y \in C_G(A)$ be arbitrary. To prove that $xy^{-1} \in C_G(A)$, it will suffice to show that for all $a \in A$, $(xy^{-1})a(xy^{-1})^{-1} = a$. Let a be an arbitrary element of A. Since $x, y \in C_G(A)$, we know that $xax^{-1} = a$ and $yay^{-1} = a$. It follows from the latter condition via multiplication on the left by y^{-1} and multiplication on the right by y that $a = y^{-1}ay$. Combining the last two results, we have that

$$\begin{aligned}(xy^{-1})a(xy^{-1})^{-1} &= x(y^{-1}ay)x^{-1} \\ &= xax^{-1} \\ &= a\end{aligned}$$

as desired. □

- Examples.
  - $C_{Q_8}(i) = \{\pm 1, \pm i\}$.
- **Center** (of G): The set defined as follows. *Denoted by* $\boldsymbol{Z(G)}$. *Given by*

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

  - Observe that $Z(G) = C_G(G)$.
  - Thus, $Z(G) \leq G$ by the above argument.
- **Normalizer** (of A in G): The set defined as follows, where $gAg^{-1} = \{gag^{-1} \mid a \in A\}$. *Denoted by* $\boldsymbol{N_G(A)}$. *Given by*

$$N_G(A) = \{g \in G \mid gAg^{-1} = A\}$$

  - $g \in C_G(A)$ implies $g \in N_G(A)$.
  - Thus, $C_G(A) \leq N_G(A)$.
  - We can prove $N_G(A) \leq G$ analogously to how we proved $C_G(A) \leq G$.
- Examples.
  - G abelian implies $C_G(A) = Z(G) = N_G(A) = G$ for all $A \subset G$.
  - Let $A = \{1, r, r^2, r^3\}$ be the rotational subgroup of D_8. Then $C_{D_8}(A) = A$, $N_{D_8}(A) = D_8$, and $Z(D_8) = \{1, r^2\}$.
  - Let $A = \{1, (1\ 2)\}$ be a subgroup of S_3. Then $C_{S_3}(A) = N_{S_3}(A) = A$ and $Z(S_3) = 1$.
- We deduce that the fact that the normalizer, centralizer, and center are subgroups is a special case of a more general result about group actions (this will be discussed further in Chapter 4).
- Define the following two subgroups of G for an arbitrary group action.
- **Stabilizer** (of s in G): The set defined as follows. *Denoted by* $\boldsymbol{G_s}$. *Given by*

$$G_s = \{g \in G \mid g \cdot s = s\}$$

  - $G_s \leq G$. Dummit and Foote (2004) proves this.
  - "Notice how the steps take to prove G_s is a subgroup are the same as those to prove $C_G(A) \leq G$ with axiom (1) of an action taking the place of the associative law" (Dummit & Foote, 2004, p. 51).
- **Kernel** (of the action of G on S): The set defined as follows. *Given by*

$$\{g \in G \mid g \cdot s = s \ \forall \ s \in S\}$$

  - The kernel is a subgroup of G as well.

- **Power set** (of A): The set of all subsets of A, where A is any set. *Denoted by* $\boldsymbol{\mathcal{P}(G)}$.
- Consider the action of G on $S = \mathcal{P}(G)$ by conjugation, i.e., $g \cdot B = gBg^{-1}$.
  - By definition, $N_G(A) = G_s$ where $s = A \in S$. Thus, the stabilizer being a subgroup implies that the normalizer is a subgroup of G.
- Consider the action of $N_G(A)$ on A by conjugation, i.e., $g \cdot a = gag^{-1}$.
  - By definition, $C_G(A)$ is the kernel of this action. Thus, the kernel being a subgroup implies that the centralizer is a subgroup of the normalizer, which in turn is a subgroup of G.
- Consider the action of G on $S = G$ by conjugation, i.e., $g \cdot s = gsg^{-1}$.
  - By definition, $Z(G)$ is the kernel of this action. Thus, the kernel being a subgroup implies that the center is a subgroup of G.

Cyclic Groups and Cyclic Subgroups

- One type of subgroup of G is to pick $x \in G$ and let H be the set of all integer powers of x, guaranteeing closure under inverses and products. We study groups like H in this section.
- **Cyclic** (group): A group H that can be generated by a single element, i.e., there is some element $x \in H$ such that $H = \{x^n \mid n \in \mathbb{Z}\}$ (where, as usual, the operation is multiplication).
  - Additive notation: $H = \{nx \mid n \in \mathbb{Z}\}$.
  - We write $H = \langle x \rangle$ and say "H is **generated** by x (and x is a **generator** of H)."
  - A cyclic group may have more than one generator (e.g., we have $H = \langle x \rangle = \langle x^{-1} \rangle$ since $(x^{-1})^n = x^{-n}$ and as n runs over all integers so does $-n$).
  - Cyclic groups are abelian.
- Examples:
  - Rotational subgroup of D_{2n}.
  - $(\mathbb{Z}, +)$.
- Relating the order of H and its generator x.

  Proposition 8. If $H = \langle x \rangle$, then $|H| = |x|$ (where if one side of this equality is infinite, so is the other). More specifically,

  1. If $|H| = n < \infty$, then $x^n = 1$ and $1, x, x^2, \ldots, x^{n-1}$ are all the distinct elements of H;
  2. If $|H| = \infty$, then $x^n \neq 1$ for all $n \neq 0$ and $x^a \neq x^b$ for all $a \neq b \in \mathbb{Z}$.

  Proof. Given. □

- Important note on the above proof: The Division Algorithm is used to reduce arbitrary powers of a generator in a finite cyclic group to the "least residue" powers.
  - The use of this algorithm suggests a similarity between finite cyclic groups and groups of the form $\mathbb{Z}/n\mathbb{Z}$. Theorem 10 will formalize this notion, noting that a finite cyclic group H and $\mathbb{Z}/n\mathbb{Z}$ are the same up to isomorphism as long as $n = |H|$.
  - Before we can prove this, though, we need another proposition.
- Properties of $|x|$ given that $x^n = x^m = 1$.

Proposition 9. Let G be an arbitrary group, let $x \in G$, and let $m, n \in \mathbb{Z}$. If $x^n = 1$ and $x^m = 1$, then $x^d = 1$ where $d = (m, n)$. In particular, if $x^m = 1$ for some $m \in \mathbb{Z}$, then $|x|$ divides m.

Proof. If $d = (m, n)$, then by the Euclidean Algorithm, there exist integers r, s such that $d = mr + ns$. Thus,

$$x^d = x^{mr+ns} = (x^m)^r (x^n)^s = 1^r 1^s = 1$$

as desired.

We divide into two cases for the second assertion ($m = 0$ and $m \neq 0$). If $m = 0$, then clearly $|x|$ divides $0 = m$, as desired. On the other hand, if $m \neq 0$, then we continue. Let $d = (m, |x|)$. By the first part, $x^d = 1$. By definition, $0 < d \leq |x|$. But since $|x|$ is the smallest positive integer such that $x^{|x|} = 1$, we must have $d = |x|$. Thus, by the definition of d, $d \mid m$ so $|x| \mid m$. □

- Cyclic group structure.

  Theorem 10. Any two cyclic groups of the same order are isomorphic. More specifically,

  1. If $n \in \mathbb{Z}$ and $\langle x \rangle$ and $\langle y \rangle$ are both cyclic groups of order n, then the map

     $$\begin{aligned} \varphi : \langle x \rangle &\to \langle y \rangle \\ x^k &\mapsto y^k \end{aligned}$$

     is well defined and is an isomorphism.

     Proof. To prove that φ is well defined, it will suffice to show that if $x^r = x^s$, then $\varphi(x^r) = \varphi(x^s)$. Let $x^r = x^s$. Then $x^{r-s} = 1$. Thus, by Proposition 9, $n \mid r - s$. It follows that $r - s = nt$, i.e., that $r = nt + s$ for some $t \in \mathbb{Z}$. Consequently,

     $$\varphi(x^r) = \varphi(x^{tn+s}) = y^{tn+s} = (y^n)^t y^s = y^s = \varphi(x^s)$$

     as desired.

     To prove that φ is an isomorphism, it will suffice to show that it is a homomorphism and a bijection. The following shows that φ is a homomorphism.

     $$\varphi(x^a x^b) = \varphi(x^{a+b}) = y^{a+b} = y^a y^b = \varphi(x^a)\varphi(x^b)$$

     As to proving that φ is a bijection, we have by hypothesis that $\langle x \rangle$ and $\langle y \rangle$ are finite groups of the same order, and we know that φ is a surjection since each y^k is the image of an x^k. These two facts prove that it is a bijection by Proposition 1. □

  2. If $\langle x \rangle$ is an infinite cyclic group, the map

     $$\begin{aligned} \varphi : \mathbb{Z} &\to \langle x \rangle \\ k &\mapsto x^k \end{aligned}$$

     is well defined and is an isomorphism.

     Proof. φ is automatically well-defined since $\mathbb{Z}$ is well-defined (i.e., there is no ambiguity in the representation of elements in the domain).

     By Proposition 8, $a \neq b$ implies $x^a \neq x^b$ for all distinct $a, b \in \mathbb{Z}$. Thus, φ is injective. By the definition of a cyclic group, φ is surjective. Thus, it is bijective. Additionally, laws of exponents prove that it is a homomorphism, as above. □

- **Cyclic group of order n**: The cyclic group of order n written multiplicatively. *Denoted by* $\boldsymbol{Z_n}$.
  - We liken Z_n more to $\langle r \rangle \leq D_{2n}$ than $\mathbb{Z}/n\mathbb{Z}$ so that we can use multiplication as the group operation.

- Up to isomorphism, Z_n is the unique cyclic group of order n.
- We will occasionally say "let $\langle x \rangle$ be the infinite cyclic group written multiplicatively," but we do not introduce any special notation for this; indeed, we always use $\mathbb{Z}$ (additively) to *represent* the infinite cyclic group.

- How to determine all generators for a given cyclic group H.

  Proposition 11. Let G be a group, let $x \in G$, and let $a \in \mathbb{Z} \setminus \{0\}$.

  1. If $|x| = \infty$, then $|x^a| = \infty$.

     Proof. Suppose for the sake of contradiction that $|x^a| = m < \infty$. Then $x^{am} = (x^a)^m = 1$ and $x^{-am} = ((x^a)^m)^{-1} = 1^{-1} = 1$. Thus, since either am or $-am$ is a positive integer (neither are 0 since $a \neq 0 \neq m$), $|x| = \pm am < \infty$, a contradiction. □

  2. If $|x| = n < \infty$, then $|x^a| = \frac{n}{(n,a)}$.

     Proof. Given. □

  3. In particular, if $|x| = n < \infty$, and a is a positive integer dividing n, then $|x^a| = \frac{n}{a}$.

     Proof. Given. □

  Proposition 12. Let $H = \langle x \rangle$.

  1. Assume $|x| = \infty$. Then $H = \langle x^a \rangle$ iff $a = \pm 1$.
  2. Assume $|x| = n < \infty$. Then $H = \langle x^a \rangle$ iff $(a, n) = 1$. In particular, the number of generators of H is $\varphi(n)$ (where φ is Euler's φ-function).

  Proof. Given. □

- Example of applying Proposition 12.
  - $\varphi(12) = 4$, so we should not be surprised to find that there are four residue classes $\bar{a}$ mod n with $(a, n) = 1$: Namely, these are $\bar{1}$, $\bar{5}$, $\bar{7}$, and $\bar{11}$. Thus, these four residue classes are the generators of $\mathbb{Z}/12\mathbb{Z}$.

- Complete subgroup structure of a cyclic group.

  Theorem 13. Let $H = \langle x \rangle$ be a cyclic group.

  1. Every subgroup of H is cyclic. More precisely, if $K \leq H$, then either $K = 1$ or $K = \langle x^d \rangle$, where d is the smallest positive integer such that $x^d \in K$.
  2. If $|H| = \infty$, then for any distinct nonnegative integers a, b, $\langle x^a \rangle \neq \langle x^b \rangle$. Furthermore, for every integer m, $\langle x^m \rangle = \langle x^{|m|} \rangle$, where $|m|$ denotes the absolute value of m, so that the nontrivial subgroups of H corresponds bijectively with the integers in $\mathbb{Z}^+$.
  3. If $|H| = n < \infty$, then for each positive integer a dividing n, there is a unique subgroup H of order a. This subgroup is the cyclic group $\langle x^d \rangle$, where $d = n/a$. Furthermore, for every integer m, $\langle x^m \rangle = \langle x^{(n,m)} \rangle$, so that the subgroups of H correspond bijectively with the positive divisors of n.

  Proof. Given. □

- Example:
  - We can use Proposition 12 and Theorem 13 to list all the subgroups of $\mathbb{Z}/n\mathbb{Z}$ for any given n. Continuing with $n = 12$, for instance, we have

- $\mathbb{Z}/12\mathbb{Z} = \langle\bar{1}\rangle = \langle\bar{5}\rangle = \langle\bar{7}\rangle = \langle\overline{7}\rangle$ (order 12).
- $\langle\bar{2}\rangle = \langle\overline{10}\rangle$ (order 6).
- $\langle\bar{3}\rangle = \langle\bar{9}\rangle$ (order 4).
- $\langle\bar{4}\rangle = \langle\bar{8}\rangle$ (order 3).
- $\langle\bar{6}\rangle$ (order 2).
- $\langle\bar{0}\rangle$ (order 1).

– The inclusions between the subgroups are given by

$$\langle\bar{a}\rangle \leq \langle\bar{b}\rangle \quad \Longleftrightarrow \quad (b, 12) \mid (a, 12), \quad 1 \leq a, b \leq 12$$

- Example: Centralizers and normalizers of cyclic groups.

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 $\times$ 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 $K \triangleleft G$, 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 $K \triangleleft G$.

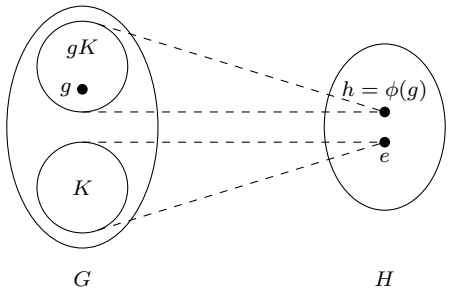


Figure 4.1: Visualizing a surjective homomorphism.

  - 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

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

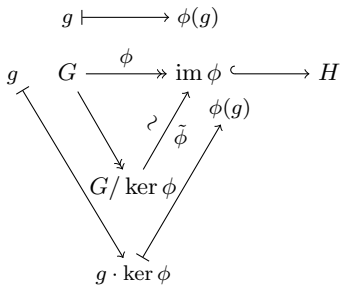


Figure 4.2: First isomorphism theorem.

  - 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 $G = S_3$.

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & H \\ \downarrow & & \uparrow \\ \mathbb{Z}/n\mathbb{Z} & \xrightarrow{\sim} & \langle h \rangle \\ k + n\mathbb{Z} & \longmapsto & h^k \end{array}$$

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 $N \triangleleft \text{O}(2)$ 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

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

  - 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 $H \triangleleft S_n$. We know that if $(xxx) \in H$, then $A_n \triangleleft H$.

  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 $\ker\phi \triangleleft S_n$, 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.

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 $A_n \triangleleft K$, 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

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

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

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

  It follows that

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

  as desired.

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

σ contains exactly two 2-cycles: 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.

σ contains three or more 2-cycles: 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.

Week 5

Applications and Generalizations

5.1 Special Normal Subgroups

10/24:

- Last time: If $H \triangleleft S_n$, $n \neq 4$, then $H = \{e\}, S_n, A_n$. If $n = 4$, H can also equal $\{e\} \cup \{(xx)(xx)\}$.
- Theorem: Let $n \neq 4$. Then the only normal subgroups of A_n are the identity and A_n.
  - Let $H \triangleleft A_n \triangleleft S_n$. From this, you could propose concluding that since we know all normal subgroups of S_n, and H is less than or equal to A_n, we know that $H = \{e\}, A_n$.
  - Issue: $\triangleleft$ is not transitive. Conjugacy classes change depending on where you're sitting.
  - Consider A, B, C: If $A \triangleleft B \triangleleft C$, then is $A \triangleleft C$?
  - This theorem is on HW5.
  - Counterexample:

$$A = \langle (1,2)(3,4) \rangle \qquad B = \{e\} \cup \{(xx)(xx)\} \qquad C = S_4$$

    - This is not so far from the simplest example.
  - Calegari reemphasizes that, "if you understand everything about S_4, then you understand everything in this class."
- We know that if $H \leq A_4$, then $|H| \big| 12$ by Lagrange's theorem.
- Claim: A_4 has no subgroups of order 6.
  - If H has index 2, then $H \triangleleft A_4$. This was a HW problem.
  - Thus, we can try to understand conjugacy classes in A_n. Whereas in S_n, we have a beautifully simple way to characterize all conjugacy classes, we do not have that in A_n. For example, $(1,2,3)$ and $(1,3,2)$ are not conjugate. $(2,3)(1,2,3)(2,3) = (1,3,2)$. $(1,2)(1,2,3)(1,2) = (2,1,3)$. $(1,3)(1,2,3)(1,3) = (3,2,1)$. But none of these transpositions are in A_n.
  - There are four conjugacy classes in A_4.

$$\{e\} \quad \{(12)(34),(13)(24),(14)(23)\} \quad \{(123),(243),(134),(142)\} \quad \{(132),(234),(143),(124)\}$$

    - Note that if $x, y \in A_4$ are of order 3, either $x \sim y$ or $x \sim y^{-1}$.
  - In A_5, all 3-cycles are conjugate; in A_4, they're not.
  - The sizes of the conjugacy classes in A_4 are $1 + 4 + 4 + 3$. That's enough to prove that there is no subgroup of order 6.
  - Alternate proof.

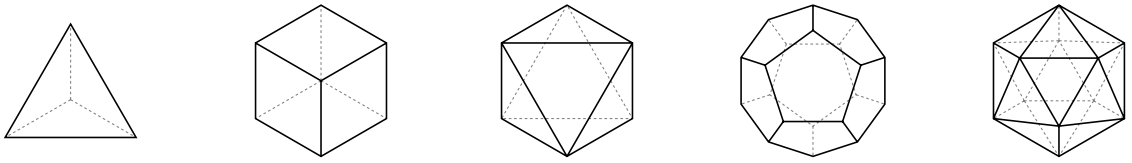
Proof. Suppose for the sake of contradiction that A_4 has a normal subgroup H of index 2. Then by the proposition from Lecture 4.1, there exists a surjective homomorphism from $A_4 \to A_4/H$. Additionally, since $|A_4/H| = 2$ and there is only one group of order 2, $A_4/H \cong \mathbb{Z}/2\mathbb{Z}$. Thus, there exists a surjective homomorphism $\phi : A_4 \to \mathbb{Z}/2\mathbb{Z}$.

We know that every alternating group (including A_4) is generated by 3-cycles. Let σ be an arbitrary 3-cycle generator of A_4. We know that $\phi(\sigma) = 0$ or $\phi(\sigma) = 1$. If $\phi(\sigma) = 1$, then

$$0 = \phi(e) = \phi(\sigma^3) = 3\phi(\sigma) = 1 +_2 1 +_2 1 = 1$$

which clearly cannot happen. Thus, $\phi(\sigma) = 0$. Consequently, the image of all of the generators of A_4 under ϕ is 0. But this implies that $\phi(A_4) = \{0\} \subsetneq \mathbb{Z}/2\mathbb{Z}$, contradicting our hypothesis that ϕ is surjective. □

- Here ends the material that will be covered on the midterm.
- We now move on to something we will come back to later.
- A_n in nature for $n = 4, 5$.



(a) Tetrahedron. (b) Cube. (c) Octahedron. (d) Dodecahedron. (e) Icosahedron.

Figure 5.1: The platonic solids.

  - Recall the cube group Cu.
  - The cube is an example of a **platonic solid**.
  - Other examples: Tetrahedron, octahedron, icosahedron, and dodecahedron. We define corresponding symmetry groups Te, Oc, Do, and Ic.
  - Consider the tetrahedral group to start.
    - Since any rigid motion permutes the vertices, we have a map $\text{Te} \hookrightarrow S_4$. Moving 2 vertices fixes the rest. Thus, $\text{Te} \leq S_4$. Therefore, $|\text{Te}| = 12$ so $\text{Te} \cong A_4$.
  - We determined in HW2 that...
    - $\text{Do} \hookrightarrow S_5$ and $|\text{Do}| = 60$. Thus, $\text{Do} \cong A_5$.
  - Consider the octahedron.

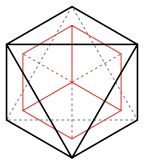


Figure 5.2: Inscribing a cube in an octahedron.

    - $|\text{Oc}| = 6 \cdot 4 = 24$. Rationale: Fix one vertex anywhere and then fix another (the other one can only take on the four adjacent positions, though); the positions of the rest are determined from these two.
    - Let's look at fixing opposite faces. This does give an injective map to S_4, and it follows that $\text{Oc} \cong S_4$.

        - Relation between Oc and Cu. We can inscribe a cube in the octahedron by connecting each vertex of the cube to the midpoint of one of the faces of the octahedron and vice versa. Thus, we get maps Oc $\to$ Cu, leading to Oc $\cong$ Cu.
    - We can similarly inscribe a dodecahedron in an icosahedron.
    - Thus, the cube and the octahedron have the same symmetry, and the dodecahedron and icosahedron have the same symmetry.
- **Platonic solid**: A solid geometric shape in three dimensions for which the faces, edges, and vertices are all indistinguishable.
    - We will study the platonic solids in more depth later.
- Problem: What symmetries can objects in $\mathbb{R}^3$ have?
    - Rephrase: What are the finite subgroups of SO(3)?
    - An octagon is Calegari's favorite polygon.
    - An octagonal prism has much the same symmetry in $\mathbb{R}^3$ as an octagon does in $\mathbb{R}^2$. This leads to $D_{2n} \leq \mathrm{SO}(3)$.
        - Recall the map from the blog post.
    - We also have $\mathbb{Z}/n\mathbb{Z} \leq D_{2n}$.
- It follows that the groups $\mathbb{Z}/n\mathbb{Z}$, D_{2n}, A_4, S_4, and S_5 occur as finite subgroups of SO(3).
- Theorem: All finite subgroups of SO(3) are on this list. Moreover, all related versions are conjugate.
    - This is a companion theorem to the theorem that there are only five platonic solids.
    - Neither theorem implies the other, but they are related.
- Infinite subgroups of SO(3): O(2), SO(3), SO(2).
- This theorem will be completely evident by the end of the course.
- You can either use this theorem to understand A_4, A_5, or use an understanding of A_4, A_5 to rationalize this theorem.
- Points to the main focus of the class: Understanding groups not just based on writing down elements but by their action on a certain set. This is the focus of the second half of the course.
- Midterm: 50 mins, closed book, Wednesday. Final exam must be in-person by department rules, but Calegari is fighting for us. Calegari is hoping that the midterm should not be a speed test.
    - Trying to test our skills, not our ability to memorize stuff.
    - How to do well: Learn group theory.
- The quaternion group.
    - A 4D vector space where you define a noncommutative product. If you just take 8 specific quaternions, the group of order 8 is distinct from D_8 but related.

5.2 Group Actions

10/28:

- Let G be a group and X be a set.
- **Group action** (of G on X): A map $\cdot : G \times X \to X$ satisfying the following. *Denoted by* $\boldsymbol{G \circlearrowright X}$.
    1. For all $g, h \in G$ and $x \in X$, $g \cdot (h \cdot x) = gh \cdot x$.
    2. For all $x \in X$, $e \cdot x = x$.

- Note that condition 2 does not follow from condition 1, and an "inverse condition" follows from both.
  - In particular, condition 1 relates certain elements of the domain of the group action but does not relate any elements of the domain to elements of X (as condition 2 does).
  - The inverse condition $g^{-1} \cdot (g \cdot x) = g \cdot (g^{-1} \cdot x) = x$ follows from conditions 1-2 via

$$g^{-1} \cdot (g \cdot x) = g^{-1}g \cdot x = e \cdot x = x = e \cdot x = gg^{-1} \cdot x = g \cdot (g^{-1} \cdot x)$$

- Example: If G is any group and X is any set, we may define a group action by $g \cdot x = x$ for all $g \in G$ and $x \in X$.
- Lemma: Let $G \curvearrowright X$ and $g \in G$. Define $\psi_g : X \to X$ by $x \mapsto g \cdot x$. Then ψ_g is a bijection.

  Proof. Injectivity:

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

  Surjectivity: Given $x \in X$, we want y such that $\psi_g(y) = x$. Choose $y = g^{-1} \cdot x$. □

- This allows us to recast group actions into the following equivalent form.
- Let X be a set and S_X be the set of all bijections from $X \to X$ under composition. Note that if $|X| = n$, then $S_X \cong S_n$.
- Proposition: An action G on the set X is equivalent to a homomorphism from G to S_X defined by $g \mapsto \psi_g$.

  Proof. A statement of the proposition that makes it more clear what exactly it is we want to prove is, "there exists an action $\cdot : G \times X \to X$ iff there exists a homomorphism $\phi : G \to X$ defined by $g \mapsto \psi_g$." Let's begin.

  Suppose first that $\cdot : G \times X \to X$ is group action of G on X. Define $\phi : G \to S_X$ by $g \mapsto \psi_g$. To prove that ϕ is a homomorphism, it will suffice to show that $\phi(gh) = \phi(g) \circ \phi(h)$ for all $g, h \in G$. Let $g, h \in G$ be arbitrary. Then by condition 1, we have for any and all $x \in X$ that

$$\begin{aligned} g \cdot (h \cdot x) &= gh \cdot x \\ \psi_g(\psi_h(x)) &= \psi_{gh}(x) \\ [\psi_g \circ \psi_h](x) &= \psi_{gh}(x) \\ [\phi(g) \circ \phi(h)](x) &= [\phi(gh)](x) \end{aligned}$$

  Therefore, $\phi(gh) = \phi(g) \circ \phi(h)$, as desired.

  Now suppose that $\phi : G \to S_X$ is a homomorphism defined by $g \mapsto \psi_g$. Define $\cdot : G \times X \to X$ by $g \cdot x = [\phi(g)](x)$. To prove that $\cdot$ is a group action, it will suffice to show that for all $g, h \in G$ and $x \in X$, $g \cdot (h \cdot x) = gh \cdot x$ and $e \cdot x = x$. Let $g, h \in G$ and $x \in X$ be arbitrary. Then

$$g \cdot (h \cdot x) = g \cdot \psi_h(x) = [\psi_g \circ \psi_h](x) = [\phi(g) \circ \phi(h)](x) = [\phi(gh)](x) = \psi_{gh}(x) = gh \cdot x$$

  and

$$e \cdot x = \psi_e(x) = x$$

  as desired. □

- You need to be careful with what the set is and what the group is; $x \cdot y$ probably doesn't make any sense (unless you start to get into cases where X is a group, too).
- **Kernel** (of a group action): The set of all $g \in G$ such that $g \cdot x = x$ for all $x \in X$.
  - The kernel is a (normal) subgroup of G.
  - We know this since it is equivalent to the kernel of the homomorphism described by the above proposition.
- **Faithful** (group action): A group action for which the kernel is trivial, i.e., $\ker = \{e\}$.
  - Such a group action is "faithful" because it is telling the whole story, i.e., not leaving out any information, i.e., mapping everything to everything.
  - The trivial group action is an example of a group action that isn't faithful.
- **Orbit** (of $x \in X$): The set of $g \cdot x$ for all $g \in G$. *Denoted by* $\mathbf{Orb}(\boldsymbol{x})$.
  - A subset of X.
  - Everywhere you can get to from your starting point x.
- **Transitive** (group action): A group action for which $\mathrm{Orb}(x) = X$ for some (any) $x \in X$.
  - In what way is a transitive group action *transitive*??
- **Stabilizer** (of $x \in X$): The set of all $g \in G$ for which $g \cdot x = x$. *Denoted by* $\mathbf{Stab}(\boldsymbol{x})$.
  - A subgroup of G.
- The kernel is a subgroup of the stabilizer. More specifically,
$$\ker = \bigcap_{x \in X} \mathrm{Stab}(x)$$
  - This is because the elements of the stabilizer fix *some* $x \in X$, whereas the elements of the kernel fix *all* $x \in X$.
- Orbits are equivalence relations, i.e., $x \in \mathrm{Orb}(x)$ and $x \in \mathrm{Orb}(y)$ imply that $\mathrm{Orb}(x) = \mathrm{Orb}(y)$.
  - In particular,
$$X = \bigsqcup \mathrm{Orbits}$$
- Let $G = S_n$ and $X = [n]$.
- Let $G = \mathrm{Cu}$.
- Examples.

G	X	$\lvert X\rvert$	Transitive	Faithful	Kernel	$\mathrm{Stab}(x)$	$\lvert\mathrm{Stab}(x)\rvert$
Cu	Faces	6	✓	✓	$\{e\}$	$\mathbb{Z}/4\mathbb{Z}$ (rotations by 90°)	4
	Vertices	8	✓	✓	$\{e\}$	$\mathbb{Z}/3\mathbb{Z}$	3
	Edges	12	✓	✓	$\{e\}$	$\mathbb{Z}/2\mathbb{Z}$	2
	Diagonals	4	✓	✓	$\{e\}$	$S_3 \cong D_6$	6
	Pairs of opposite faces	3	✓	X	Rotations by 180°, in particular, $\lvert K\rvert = 4$	D_8	8
	Inscribed tetrahedra	2	✓	X	A_4	A_4	12
	Ed ∪ Fac	18	X	✓	$\{e\}$	$\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z}$	4 or 2

Table 5.1: Examples of group actions.

  - The last two rows we filled out by first asserting transitivity, A_4, and 12; and edges union faces, not transitive.
- On Monday, we will look into group actions where the geometry is not so convenient.

5.3 Blog Post: Group Actions

From Calegari (2022).

11/13:

- Motivating group actions.
  - We now address the "?" category in Table 2.1.
  - $G = S_{52}$ is an incredibly huge group, yet it seems pretty manageable since we can write down any element and multiply two or more by hand, for instance, without too much difficulty. Why is this group with 52! elements so manageable? It seems like it has something to do with the set X of 52 numbers that S_{52} "moves around."
  - Similarly, $G = \mathrm{GL}_n(\mathbb{R})$ denotes the group of $n \times n$ invertible matrices but this set is made more manageable by understanding its action on $X = \mathbb{R}^n$.
  - In both cases, G acts on X in some sense. Elements of G form bijective maps $g : X \to X$. Moreover, the group product corresponds to function composition.
  - Question: Can we find a suitable X for any group G?
  - Hint: Look at Cu. There are several sets on which Cu acts, each of which leads to a greater understanding of the group, itself.
  - Conclusion: In general, there will be many *different* X that we will want to consider, even when G is the symmetric group.
- $g \cdot (h \cdot x) = gh \cdot x$ is called a **compatibility property**.
- Covers the Lemma and Proposition from class.
- Examples of group actions.
  - The trivial group action (see class notes).
  - If $G = \mathrm{Cu}$ and X is the set of inscribed tetrahedra, pairs of opposite faces, diagonals, faces, or edges, we get homomorphisms from G to S_2, S_3, S_4, S_6, and S_{12}, respectively. Going even further, we can let X be the disjoint union of the set of edges and faces to obtain a homomorphism from G to S_{18}.
  - Consider $G = \mathrm{SO}(3)$ and $X = \mathbb{R}^3$ or $X = S^2$ (the unit 2-sphere).
  - Consider $G = S_n$ and $\sigma = \{1, 2, \ldots, n\}$.

Week 6

Fundamentals of Group Actions

6.1 Examples of Group Actions

10/31:

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

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

6.2 Orbit-Stabilizer Theorem

11/2:

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

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

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

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

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

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

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

as desired. □

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

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

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

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

From Calegari (2022).

11/13:

- Lemma: Let $G \curvearrowright X$ and let $x \in X$. Let $y \in \mathrm{Orb}(x)$, i.e., let there exist $\sigma \in G$ such that $y = \sigma \cdot x$. Then

  1. $\mathrm{Stab}(y) = \sigma \cdot \mathrm{Stab}(x) \cdot \sigma^{-1}$.

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

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

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

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

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

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

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

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

     This implies that $\sigma^{-1} g \in H$, i.e., that $g \in \sigma H$, as desired. □

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

- Thus,
$$\ker = \bigcap_{g\in G} gHg^{-1} \subset \bigcap_{k=1,\dots,n} (1,k)H(1,k)^{-1} = \{e\}$$
so the action is faithful, here.

– When $H = \{e\}$, $G \circlearrowright G/H$ is entirely analogous to left multiplication within the group: $g\cdot x = gx$.

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

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

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

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

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

- More on $G \circlearrowright G$ by conjugation.

– Since $|G| = |\{g\}| \cdot |C_G(g)|$, we can calculate the orders of centralizers. From the order, we can often get even more specific information.

– Consider $G = S_n$.

■ If $g = (1, 2, \dots, n)$, then $|\{g\}| = (n-1)!$ and $C_G(g) = n!/(n-1)! = n$. This combined with the fact that g commutes with g implies that
$$C_{S_n}((1,2,\dots,n)) = \langle (1,2,\dots,n)\rangle$$

■ If $g = (1, 2, \dots, k)$, then $|\{g\}| = n!/k(n-k)!$ so $|C_{S_n}(g)| = k\cdot(n-k)!$. Naturally, $g \in C_{S_n}(g)$, but so are all elements which fix $1, 2, \dots, k$ and shuffle $k+1, k+2, \dots, n$. Thus,
$$C_{S_n}((1,2,\dots,k)) = \mathbb{Z}/k\mathbb{Z} \times S_{n-k}$$

■ Let g have cycle shape corresponding to the partition $a_1n_1 + a_2n_2 + \cdots$ where $n_1 > n_2 > \cdots$ denote cycle lengths and the a_i denote the corresponding multiplicity. We can deduce that the centralizer has order $\prod n_i^{a_i} a_i!$.
It follows from the fact that disjoint cycles commute that g commutes with each component cycle, i.e., if $g = \cdots(a_1,\dots,a_k)\cdots$, then g and $(a_1,\dots,a_k)$ commute. g therefore also commutes with all powers of each component cycle. Going even further, g commutes with all products of all powers of each component cycle, i.e., if $g = (a_1,\dots,a_k)(b_1,\dots,b_\ell)(c_1,c_2,\dots)\cdots$, then
$$C_{S_n}(g) \supset \langle (a_1,\dots,a_k),(b_1,\dots,b_\ell),(c_1,c_2,\dots),\dots\rangle$$
The group on the right above is isomorphic to $\prod(\mathbb{Z}/n_i\mathbb{Z})^{a_i}$ and thus has order $\prod n_i^{a_i}$.
What are the other elements in the centralizer that account for the $\prod a_i!$ term?? Is it the products of the powers of the cycles??

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

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

6.4 Group Actions on the Quotient Group

11/4:

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

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

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

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

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

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

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

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

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

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

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

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

From Calegari (2022).

11/13:

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

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

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

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

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

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

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

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

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

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

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

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

and picture Figure 6.1.

(a) Three points. (b) Six points.

Figure 6.1: Transitive actions of S_3.

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

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

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

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

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

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

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

  - We have the
$$m = |X| = \binom{n}{2} = \frac{n(n-1)}{2}$$
  - This yields maps from $S_4 \to S_6$, $S_5 \to S_{10}$, and $S_6 \to S_{15}$, for example.
  - Still not entirely sure how we define the group action??

- We now characterize $\mathrm{Aut}(S_n)$ almost completely.
- Lemma: Suppose $n \neq 6$. Let $S_n \curvearrowright X$ transitively, where $|X| = n$. Then (after possibly relabeling the set X) the action is precisely the "usual" action of S_n on $X = \{1, 2, \ldots, n\}$.

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

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

  Proof. This proof is constructive.

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

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

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

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

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

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

  so

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

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

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

  so

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

- Therefore, the exotic subgroup is given by

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

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

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

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

  - Note that G is a relabeling of the exotic subgroup H of S_6 with the numbers $1,\dots,6$.
- Lemma: The map $\psi : S_6 \to S_6$ induced by the action of S_6 on S_6/G by left multiplication is an automorphism which is not inner. In particular, this automorphism takes the conjugacy class (xx) to the conjugacy class $(xx)(xx)(xx)$ and, as we shall also see, the conjugacy class $(xxxxxx)$ to the conjugacy class $(xxx)(xx)$.

  Proof. This is a slick proof by contradiction.

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

isomorphism, we must also have $|\{\psi((xx))\}| = 15$. Thus, either $\psi(\{(xx)\}) = \{(xx)\}$ or $\psi(\{(xx)\}) = \{(xx)(xx)(xx)\}$.

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

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

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

Proof. This is an explicit construction.

Return later for the details.

We conclude that

$$\psi((1,2)) = (a,b)(c,d)(e,f) = (1,2)(3,4)(5,6)$$
$$\psi((1,2,3,4,5,6)) = (b,f)(c,e,d) = (2,6)(3,5,4)$$

□

Week 7

Group Action Applications: A_5 and the Sylow Theorems

7.1 Actions of A_5

11/7:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

    as desired. □

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

7.2 Blog Post: Actions of the Dodecahedral Group

From Calegari (2022).

11/26:
- Recall that in HW2, we found a faithful action Do $\circlearrowright$ 5 inscribed cubes. This yielded an injective homomorphism Do $\to S_5$ identifying Do with an order 60 subgroup. Moreover, this subgroup was necessarily A_5 since it is of order 60 and hence normal. Therefore,

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

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

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

  for all $g \in G$ and $x \in X$.
- Because of the following theorem, to classify all transitive actions of Do, it will actually only be necessary to classify the conjugacy classes of the subgroups of G!

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

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

Define...

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

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

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

With this result, we have that

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

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

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

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

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

as desired.

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

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

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

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

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

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

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

as desired.

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

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

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

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

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

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

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

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

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

$$g'H = ghH = gH$$

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

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

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

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

as desired. □

- Calegari reviews the isomorphism between Do $\cong$ Ic.
- Subgroups of A_5 with distinct conjugacy classes.
  1. The trivial subgroup.
  2. The cyclic group $\langle (12)(34) \rangle$ of order 2.
  3. The cyclic group $\langle (123) \rangle$ of order 3.
  4. The Klein 4-group $\langle (12)(34), (13)(24), (14)(23) \rangle$ of order 4.
  5. The cyclic group $\langle (12345) \rangle$ of order 5.
  6. The group $\langle (123), (23)(45) \rangle \cong S_3 \cong D_6$ of order 6.
  7. The dihedral group $D_{10} = \langle (12345), (25)(34) \rangle$ of order 10.
  8. The group $A_4 = \langle (123), (124) \rangle$ of order 12.
  9. The group A_5 of order 60.
- Notes on the above.
  - These are actually *all* of the subgroups of A_5.
  - All of the above subgroups have different orders. Thus, there is a unique equivalence class of transitive actions on this group for a given set X with
$$|X| = 60, 30, 20, 15, 12, 10, 6, 5, 1$$
- Since A_5 has no non-trivial normal subgroups to act as kernels, all actions save the final one below will be faithful.
- Actions of the dodecahedral group:
  1. The action on the "one" dodecahedron.
  2. The action on the five inscribed cubes.
  3. The action on the six pairs of opposite faces of the dodecahedron.
     (a) Equivalently, the action on the six pairs of opposite diagonals of the icosahedron.
  4. The action on the ten pairs of opposite vertices of the dodecahedron.
     (a) Equivalently, the action on the ten pairs of opposite faces of the icosahedron.
  5. The action on the twelve faces of the dodecahedron.
     (a) Equivalently, the action on the twelve vertices of the icosahedron.
  6. The action on the fifteen pairs of opposite edges of the dodecahedron.
     (a) Equivalently, the action on the fifteen pairs of opposite edges of the icosahedron.
  7. The action on the twenty vertices of the dodecahedron.
     (a) Equivalently, the action on the twenty faces of the icosahedron.
  8. The action on the thirty edges of the dodecahedron.
     - Equivalently, the action on the thirty edges of the icosahedron.
  9. The action of the group on itself by left multiplication.

7.3 p-Groups

11/9:

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

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

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

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

  As we know,

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

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

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

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

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

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

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

- We get from this proposition an outline for "classifying" p-groups. We will do this inductively on k. Here are the steps.
  1. Understand Abelian p-groups.
  2. Understand all p-groups of order $|p^k|$.
  3. Let $|P| = p^{k+1}$. Then by the above, $Z \triangleleft P$. If $Z = P$, use 1. If $Z \neq P$, then $|Z|$ and $|P/Z|$ divide p^k, so we can use 2.
- Goal: Knowing Z and G/Z, try to find all possible G.
- Classification for $k = 2$.
  1. Abelian groups. By Lagrange's theorem, there are two possibilities: There exists x with $|x| = p^2$, and there exists x with $|x| = p$.

   (a) G has an element of order p^2, and hence $G \cong \mathbb{Z}/p^2\mathbb{Z}$.
   (b) There exists $x \in G$ such that $|x| = p$. Let $y \in G \setminus \langle x \rangle$. Then $y^p = e$. Thus, $G = \langle x, y \rangle$. $x^p = e = y^p$ and $xy = yx$. Thus, $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.
2. Suppose G is not abelian. Z still has a nontrivial center, though, and hence any proper nontrivial subgroup of G is necessarily isomorphic to $\mathbb{Z}/p\mathbb{Z}$ for the $k = 2$ case. Thus, the only possible pair $(Z, G/Z)$ is $(Z, G/Z) = (\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p\mathbb{Z})$. But then $G/Z \cong \mathbb{Z}/p\mathbb{Z}$ is cyclic, so by HW4 Q5, G is abelian, a contradiction. Therefore, $G \cong \mathbb{Z}/p^2\mathbb{Z}$ or $(\mathbb{Z}/p\mathbb{Z})^2$, hence abelian.

- (Partial) classification for $k = 3$.
  1. Abelian groups: $\mathbb{Z}/p^3\mathbb{Z}$, $\mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, and $(\mathbb{Z}/p\mathbb{Z})^3$.
  2. Possible pairs $(Z, G/Z)$:

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

  G/Z cyclic implies the same contradiction, so the only possibility is $Z = \mathbb{Z}_p$ and $G/Z = (\mathbb{Z}_p)^2$.

- Does the trend of no nonabelian groups continue for higher powers? No — for $|G| = 2^3 = 8$, both D_8 and Q (the Quaternion group) are nonabelian counterexamples.
  - Case 1: All elements in G have order 2.
    - G is abelian: If $x, y \in G$ are arbitrary, then

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

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

- We now investigate the case where p is odd and $G = p^3$. Let $Z = \mathbb{Z}/p\mathbb{Z}$ and $G/Z = (\mathbb{Z}/p\mathbb{Z})^2$.
  - Consider a surjection $G \twoheadrightarrow G/Z$. Choose $x \mapsto (1, 0)$ and $y \mapsto (0, 1)$.
  - Let $x^p, y^p, xyx^{-1}y^{-1} \in Z$.
  - If $xy = yx$, then $G = \langle x, y, Z \rangle$ is abelian.
  - Suppose $xy = yxz$ for some $z \in Z$ nontrivial.
  - Case 1: All $g \in G$ have order p. Then

$$G = \{y^b x^a z^c \mid 0 \leq a, b, c \leq p - 1\}$$

  - We have that

$$y^b x^a z^c (y^B x^A z^C) = y^b x^a y^B x^A z^{c+C} = y^{b+B} x^{a+A} z^{c+C+aB}$$

  since $xy = yxz$??

- This gets into $\mathrm{GL}_3(\mathbb{F}_p)$, the group of 3×3 invertible matrices over the field of numbers 0 to p under addition mod p. In particular,

$$\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & A & C \\ 0 & 1 & B \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+A & c+c+aB \\ 0 & 1 & b+B \\ 0 & 0 & 1 \end{pmatrix}$$

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

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

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

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

7.4 Blog Post: *p*-Groups

From Calegari (2022).

11/27:

- Mostly review of lecture.
- Claim (by Lagrange): Any subgroup of a p-group P is also a p-group. The order of any element of P is a power of p.
- **Fixed points** (of X under $G \circlearrowright X$): The set of all fixed points of X. *Denoted by* **Fixed(X)**.
- Theorem:
$$|\operatorname{Fixed}(X)| \equiv |X| \mod p$$
- Example: Let $X = P$ and $P \circlearrowright P$ by left multiplication. Then $|P| \mod p = p^m \mod p = 0 \mod p$. This squares with the fact that by the Sudoku lemma, P has no fixed points ($|P| > 1$ by definition since the smallest prime number is 2), so $|\operatorname{Fixed}(P)| = 0 \equiv 0 \mod p$.
- Following up on the center being a non-trivial normal subgroup, we have the following corollary.
- More on $\mathrm{GL}_3(\mathbb{F}_p)$.
  - Let $P \subset \mathrm{GL}_3(\mathbb{F}_p)$ be the set of matrices of the following form.
$$\begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix}$$
  - P is non-abelian since the operation is matrix multiplication, which is not commutative.
  - $|P| = p^3$ since we have 3 free entries in the matrix, each of which can take on p values.

– Every matrix in P is invertible (and hence an element of $\mathrm{GL}_3(\mathbb{F}_p)$) since the determinant for such an upper triangular matrix is the product of the diagonal entries and hence $1 \neq 0$.

– P is closed under inversion since

$$\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -x & -y+xz \\ 0 & 1 & -z \\ 0 & 0 & 1 \end{pmatrix}$$

– P is closed under multiplication since

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+x & b+y+az \\ 0 & 1 & c+z \\ 0 & 0 & 1 \end{pmatrix}$$

– Exercises:

1. If $p \geq 3$, then every non-trivial element of P has order p. In particular, knowing that every element of a group P satisfies $x^p = e$ does not imply that P is abelian unless $p = 2$, in which case we did prove that such a group is abelian.
2. What are the order four elements in P when $p = 2$?
3. The center $Z(P)$ is the subgroup of order p containing all elements of the form

$$\begin{pmatrix} 1 & 0 & * \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Moreover, we have $P/Z = (\mathbb{Z}/p\mathbb{Z})^2$. In fact, I claim that if P is any non-abelian group of order p^3, then $P/Z = (\mathbb{Z}/p\mathbb{Z})^2$ has to be true. Since P is not abelian, we can't have $Z = P$. We also know since P is a p-group that Z is non-trivial. Finally, we can't have $|Z| = p^2$ since then P/Z would be cyclic and then (by HW4 Q5 again) $P = Z$, which is a contradiction. Finally, even when $|Z| = p$, we can't have $P/Z \cong \mathbb{Z}/p^2\mathbb{Z}$ since that still implies by HW4 Q5 that P is cyclic and thus $P = Z$, another contradiction.

4. When $p = 2$, is this group the dihedral group D_8 or the quaternion group Q? (It is one of these groups — see the claim below.)

– Claim: There are exactly 5 groups of order p^3, three of which are abelian and two of which are not. When $p > 2$, the non-abelian groups of order p^3 are distinguished by whether all elements in P have order dividing p or not. When $p = 2$, the two non-abelian groups are D_8 and Q.

Proof. No proof given. □

– Exercise: Can you construct the other non-abelian group of order p^3 which has an element of order p^2?

7.5 Sylow I-II

11/11:

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

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

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

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

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

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

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

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

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

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

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

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

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

- Example: Let $G = S_p$.
  - $|G| = p! = p \cdot k$.
  - Need to find a subgroup of order p.
  - $P = \langle (1, 2, \ldots, p) \rangle$ is a p-Sylow of G.
- Example: Let $G = S_4$.
  - Pick $p = 2$ so that $|G| = 24 = 2^3 \cdot 3$.
  - Need to find a subgroup of order 8.
  - We can choose $D_8 \leq S_4$.
- Theorem (Sylow II — Uniqueness up to conjugation): Fix P a p-Sylow.
  1. If $Q \subset G$ is a p-Sylow, then $Q = gPg^{-1}$ for some $g \in G$.
  2. If $Q \subset G$ is a p-group, then $Q \subset gPg^{-1}$ for some $g \in G$.

Proof. Ask in office hours?? □

Week 8

Applications of the Sylow Theorems

8.1 Sylow III and Examples

11/14:

- Last time:
  - Sylow I: p-Sylow subgroups exist.
  - Sylow II: p-Sylow subgroups are unique up to conjugation. Moreover, if $Q \subset G$ is a p-group, then $Q \subset gPg^{-1}$ with the same g.
  - We proved Sylow II by taking $H \subset G$, and separately taking $P \subset G$ to be p-Sylow. In this case, there exists $g \in G$ such that $H \cap gPg^{-1}$ is a p-Sylow of H. If $H = Q$, then $Q \cap gPg^{-1} = Q$.
    - More on this??
- Alternate proof of Sylow II.

  Proof. We attack the first claim (equality for p-Sylows) in three steps; we will not prove the second claim (containment for p-groups) herein. Step 1 defines a useful group action, allowing us to apply relevant theorems from that domain later on. Step 2 proves the existence of a fixed point of said group action, which will be intimately related to the final element g by which we conjugate P to make it equal Q. Step 3 relates this element g to the desired result. Let's begin.

  Let X denote the set of all p-Sylows of G. By Sylow I, X is nonempty. Thus, we may choose $P, Q \in X$ (note that P, Q are not necessarily distinct). Define $G \curvearrowright G/P$ by left multiplication. Restrict the group action to Q (i.e., restrict the function $\cdot : G \times G/P \to G/P$ to $Q \times G/P$).

  Since $|G| = p^n k$ and $|P| = p^n$, we have that $\gcd(|G/P|, p) = 1$. Thus, $|G/P|$ is not divisible by p, so $|G/P| \mod p \not\equiv 0 \mod p$. Additionally, since Q is a p-group (by definition as a p-Sylow), we have from the proposition in Lecture 7.2 that $\text{Fixed}(G/P) \equiv |G/P| \mod p$. This combined with the previous result reveals that $\text{Fixed}(G/P)$ is nonempty. As such, we may choose $gP \in \text{Fixed}(G/P)$.

  By definition, Q stabilizes gP, i.e.,

  $$QgP = gP$$
  $$g^{-1}QgP = P$$

  where the latter equation above is a simple rearrangement of the first, but can be interpreted to mean that $g^{-1}Qg$ stabilizes P. Thus, if $g^{-1}qg \in g^{-1}Qg$, we have $(g^{-1}qg)p_1 = p_i$ for some $i = 1, \ldots, p^n$, and hence $q = g(p_i p_1^{-1})g^{-1} \in gPg^{-1}$. Therefore, $Q \subset gPg^{-1}$. Since $|P| = |Q|$, we additionally have that $Q = gPg^{-1}$, as desired. □

- Sylow III. The first is existence, the second is uniqueness, and then there's this one (divisibility and congruence).

- Theorem (Sylow III — divisibility and congruence): Let P be a p-Sylow, and let n_p denote the number of p-Sylows of G. Then

  1. Let $N = N_G(P)$. Then $n_p = |G|/|N| = [G : N]$. In particular, n_p divides $|G|$.

     Proof. To prove a claim which expresses $|G|$ in terms of the product of two other numbers, we should think about using the Orbit-Stabilizer theorem. To do so, we need a group action. In particular, a group action by conjugation could be useful because we have a normalizer involved. With this motivation mentioned, let's begin.

     Let X be the set of p-Sylows of G. Define $G \circlearrowright X$ by conjugation. By the Orbit-Stabilizer theorem,

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

     Since the group action is by conjugation, we have by the definition of the stabilizer and the normalizer that

     $$\operatorname{Stab}_G(P) = \{g \in G \mid gPg^{-1} = P\} = N_G(P) = N$$

     According to Sylow II, every p-Sylow (every element of X) is conjugate to every other via some element of G. Thus, since our group action is conjugation, the group action is transitive and $\operatorname{Orb}(P) = X$. Thus,

     $$|\operatorname{Orb}(P)| = |X| = n_p$$

     Therefore, substituting the previous two results into the preceding one, we have that

     $$\begin{aligned} |N| \cdot n_p &= |G| \\ n_p &= |G|/|N| = [G : N] \end{aligned}$$

     as desired. □

  2. $n_p \equiv 1 \mod p$.

     Proof. Congruence should make us think, "fixed points." In this argument, we will pick up where we left off, using the same group action defined in the proof of part 1 to express the claim in the language of fixed points. We will then deduce that this latter claim is true, proving the original claim. Let's begin.

     Restrict the action from part 1 to P. This may mean that $P \circlearrowright X$ is no longer transitive, but this will not cause any issues. Moving on, we know by the closure of subgroups that $gPg^{-1} = P$ for any $g \in P$; thus, P is a fixed point of $P \circlearrowright X$. It follows by the proposition from Lecture 7.2 that $\operatorname{Fixed}_P(X) \equiv |X| \mod p$, and hence $n_p = |X| \equiv \operatorname{Fixed}_P(X) \mod p$. Thus, we are done if we can show that $\operatorname{Fixed}_P(X) = 1$, i.e., that P is the only fixed point of X under $P \circlearrowright X$.

     Let $Q \in \operatorname{Fixed}_P(X)$ be arbitrary; we seek to prove that $Q = P$. Define $N := N_G(Q)$. By definition, $Q \subset N$. Additionally, $P \subset N$: Since $Q \in \operatorname{Fixed}_P(X)$, $gQg^{-1} = g \cdot Q = Q$ for all $g \in P$. Hence P, Q are both p-Sylows of N (the order of p dividing $|N|$ certainly [by Lagrange's Theorem] divides the order of p dividing $|G|$). By Sylow II, any two p-Sylows are conjugate, so there exists $n \in N$ such that $nQn^{-1} = P$. Additionally, since $Q \triangleleft N$ by HW4 Q3c, we have that $nQn^{-1} = Q$. Therefore, by transitivity, $P = Q$, as desired. □

- We are now done with proving the Sylow theorems. Make sure you have nice copies written out!
  - Perhaps before the final, I should take all important proofs from the quarter and make "proof outlines" in my review sheet, giving the tricks and motivation in as concise a format as possible but still allowing me to deduce the rest of the proof for myself. This could be a great exercise!
- The arguments that we've used thus far in this class are mostly combinatorical with a bit of number theory sprinkled in.
- Before going into applications of the Sylow theorems, we present an example that's good to keep in mind.

- Let $G = S_p$ for some $p \in \mathbb{N}$ prime.
  - S I: Yes, G has a p-Sylow, namely $P = \langle (1, 2, \ldots, p) \rangle$.
  - S II: Any p-cycles are conjugate to one another.
  - Intuitive derivation of the value of n_p: n_p is the number of elements of order p[1] divided by $p-1$[2]. Thus,
$$n_p = \frac{p!}{p(p-1)} = (p-2)!$$
  - S III: $(p-2)! \equiv 1 \mod p$.
    - We obtain a related statement from **Wilson's theorem**: $(p-1)! \equiv -1 \mod p$.
  - S III: $|N| = |N_G(P)| = p(p-1)$.
  - This result combined with $P \triangleleft N$: $|N/P| = p - 1$.
- Theorem (Wilson's theorem): A natural number $p > 1$ is prime iff
$$(p-1)! \equiv -1 \mod p$$
- **Affine group** (of order p): The following group, which consists of permutations given by affine maps. *Denoted by* $\mathbf{Aff}_p$. *Given by*
$$\mathrm{Aff}_p = S_{\mathbb{Z}/p\mathbb{Z}}$$
  - We send $x \in \mathbb{Z}/p\mathbb{Z}$ to $ax + b \in \mathbb{Z}/p\mathbb{Z}$.
  - Injective:
$$\begin{aligned} ax + b &= ay + b \\ a(x - y) &\equiv 0 \mod p \\ x &= y \end{aligned}$$
  - We also need to check that Aff_p is actually a subgroup. The group operation...
  - An affine map is the sum of a linear transformation and a translation. Thus,
$$A(ax + b) + B = Aax + Ab + B$$
    so
$$(a, b)(A, B) = (aA, Ab + B)$$
  - We claim that $P = \langle X \to X + 1 \rangle$ is a subgroup??
  - In particular, $P \triangleleft \mathrm{Aff}_p \leq N$.
  - Thus, $\mathrm{Aff}_p = N_{S_p}(\langle (1, 2, \ldots, p) \rangle)$. This is a nice new group to have.
  - We have $P : \mathrm{Aff}_p \to (\mathbb{Z}/p\mathbb{Z})^*$ defined by $\langle x \mapsto x + b \rangle$. $x \mapsto ax + b$ goes to a in the codomain, $Ax + B$ maps to A, and $aAx + \cdots$ maps to aA.
  - Remark: If $q | p - 1$ is prime, then $(\mathbb{Z}/p\mathbb{Z})^*$ has an element of order q (Sylow). Call it σ. Then $\langle \sigma \rangle \leq (\mathbb{Z}/p\mathbb{Z})^*$.
- Theorem: Let p, q be primes such that $p > q$. Then either...
  1. $p \equiv 1 \mod q$ and there exists a nonabelian group of order pq that is a subset of Aff_p.
  2. $p \not\equiv 1 \mod q$ and all groups of order pq are isomorphic to $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}/pq\mathbb{Z}$.

[1] Recall that this is $p!/p$, since there are p options for the first entry, $p - 1$ for the second, on and on down to 1, but there are also p ways to write said element.

[2] Each p-Sylow P contains $p - 1$ distinct p-cycles.

Proof. ... □

- Misc notes: According to S III...
  - $|G| = pq$ and $n_p \equiv 1 \mod p$. Either $n_p = 1$ or $n_p = q \equiv 1 \mod p$, implying $q > p$, a contradiction.
  - Alternatively, $G \cong P_p \times P_q$. $n_q = 1$ or $n_q = p$. If $p \not\equiv 1 \mod q$, then $n_q = 1$. We end up with $P_p \trianglelefteq G$ and $P_q \trianglelefteq G$, which implies that $P_p \cap P_q = \{e\}$. Therefore, P_p and P_q commute.
- First example: 15; the first composite number for which $p, q > 2$ (and thus the structure is not covered by our previous analysis).
- We still haven't completely classified groups of order pq; sometimes there's one, sometimes there's more. We will look at these groups in greater detail next lecture.

8.2 Groups of Order *pq*

11/16:

- Classifying groups of order $|G| = 2p$ for $p > 2$ prime.
- By Sylow I, there exists a p-Sylow P_p and a 2-Sylow P_2.
  - Since $[G : P_p] = 2$, HW4 Q6 implies that P_p is normal.
    - Alternate strategy: By SyIII, $n_p \equiv 1 \mod p$ and $n_p = |G|/|N| = |G|/|P| = 2p/p = 2$. Thus, $n_p = 1$ or $n_p = 2$. These facts combine to say that $n_p = 1$ and $P_p \trianglelefteq G$.
  - By Lagrange's Theorem, we must have $P_p = \langle x \rangle$ and $P_2 = \langle y \rangle$ for some $x, y \in G$.
  - $x^p = e = y^2$.
  - $G = \langle x, y \rangle$.
- The elements have order 1, 2, p or $2p$ by Lagrange.
- Since $\langle x \rangle$ is normal, it follows that

$$\begin{aligned} y \langle x \rangle y^{-1} &= \langle x \rangle \\ yxy^{-1} &\in \langle x \rangle \\ yxy^{-1} &= x^k \end{aligned}$$

  where the x, y used throughout are the previously referenced generators (not any sort of arbitrary variable).
- Goal: Put constraints on k.
- $k \equiv 0 \mod p$ iff $x = e$.
  - If $k \equiv 0 \mod p$, then $yxy^{-1} = x^k = e$, so $x = y^{-1}y = e$.
  - If $x = e$, then $x^k = yey^{-1} = e$, so we must have $k \equiv 0 \mod p$.
- A preview of something we will shortly prove.
  - There are two groups of order $2p$: D_{2p} and $\mathbb{Z}/2p\mathbb{Z}$.
  - In the latter, $k = 1$.
    - Since $\mathbb{Z}/2p\mathbb{Z}$ is abelian, the conjugate of any element is itself. Thus, $yxy^{-1} = x^1$.
  - In the former, $k = -1$ (if conjugating by a reflection??).
    - Recall the multiplication rule $rs = sr^{-1}$, from which we can deduce that $srs^{-1} = r^{-1}$.
    - Note that it is proper to use s analogously to y and r analogously to x since reflections (s) have order 2 like y and rotations (r) can have much higher orders (e.g., p).

- Another (redundant??) possibility: $yx^iy^{-1} = yx^{ik}y^{-1}$.
- We now prove that there are only two groups of order $2p$.
- Conjugating x by y twice gives us

$$x = exe = y^2xy^{-2} = y(yxy^{-1})y^{-1} = yx^ky^{-1} = (yxy^{-1})^k = (x^k)^k = x^{k^2}$$

  - Comparing exponents, we have $k^2 \equiv 1 \mod p$.
  - This is equivalent to $(k^2-1) \equiv 0 \mod p$, which in turn is equivalent to $(k+1)(k-1) \equiv 0 \mod p$.
  - It follows that $k \equiv \pm 1 \mod p$.
- Now we must consider each case in turn.
- If $k = 1$, then G is abelian, i.e., $G = P_p \times P_2$.
  - Example: $\mathbb{Z}/2p\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.
  - We'll see a lot of this breaking up of groups next quarter.
  - Calegari alludes to the **Chinese remainder theorem**.
- Theorem (Chinese remainder theorem): Let m, n be relatively prime positive integers. For all integers a, b, the pair of congruences

$$\begin{aligned} x &\equiv a \mod m \\ y &\equiv b \mod m \end{aligned}$$

  has a solution, and this solution is uniquely determined modulo mn.
- If $k = -1$, then $yx = x^{-1}y$.

	x^i	x^iy
x^j	x^{i+j}	$x^{i+j}y$
x^jy	$x^{j-i}y$	x^{j-i}

Table 8.1: Multiplication table for $|G| = 2p$ and $k = -1$.

  - We still have that $x^p = 1$.
  - We want to show based on this multiplication rule that we really have the dihedral group. Once we have this, there's at most one group it could possibly be. Since D_{2p} is such a group, then they must be isomorphic.
  - To do so, we show that the rule determines the multiplication table (see Table 8.1 above).
  - Thus, there is at *most* one group.
  - But since D_{2p} exists, there is also at *least* one group.
  - Therefore, if $k = -1$, we must have $G \cong D_{2p}$.
- Proposition: Let $|G| = 2n$, $n > 2$. If $x \in G$ and $|x| = n$, $|y| = 2$, $yx = x^{-1}y$ implies $G \cong D_{2n}$.

  Proof. The multiplication table is uniquely determined (analogous to the above argument). □
- Remark about $D_4 = K$, where K is the Klein 4-group??
- We now move on to $|G| = pq$, where $p > q$ are both prime.
- Applying S III, we get n_p equals 1 or q and is congruent to 1 mod p, and n_q equals 1 or p and is congruent to 1 mod q.

  - Thus, $n_p = 1$ always and $n_q = 1$ unless $p = 1 \mod q$.

- If $|G| = pq$ and$p > 2$, $p \not\equiv 1 \mod q$, then $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$.
- Case where $|G| = q$ and $p \equiv 1 \mod q$. Then $P_p = \langle x \rangle$ and $P_q = \langle y \rangle$, so $P_p \trianglelefteq G$. This is another (strange??) application of S III.
  - Using what we have here, we know that $yxy^{-1} = x^k$, $k \not\equiv 0 \mod p$. $k = 1$ implies G is abelian and $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$.
  - Now we just need to conjugate x by y, q times over: $x = y^q x y^{-q} = x^{k^q}$. Thus, $k^q \equiv 1 \mod p$.
  - Unlike when $q = 2$, we could factor then. Now we've got a more difficult problem; can't factor it.
  - Does there exist q satisfying the above property? If so, how many are there?
  - Think about this as an identity in the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ which has order $p - 1$. We can thus deduce by Lagrange that $q|p - 1$.
  - Sylow I: There exists η of order q such that $\eta, \eta^2, \eta^3, \ldots, \eta^{q-1}$ all have order p.
  - We could argue that $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic (and in fact it is), but here's something else: We have that $k^q - 1 = (k-1)(k-\eta)\cdots(k-\eta^{q-1})$. This is factoring polynomials mod p (weird for now, but very commonplace next quarter).
  - Fix η. Then $yxy^{-1} = x^{\eta^2}$.
- Claim I: This determines the multiplication table; $\langle x \rangle \subset G$. The right cosets $\langle x \rangle, \langle x \rangle y, \ldots, \langle x \rangle y^{q-1}$. $G/P_p \cong \mathbb{Z}/q\mathbb{Z}$. If we have all of the elements of the form $x^i y^j$, do we know how to multiply these together? In particular, can we determine how to write

$$x^i y^j x^a y^b = x^r y^s$$

  We have that $yx = x^{\eta^i} y$, so the multiplication table is determined. This implies that there is at most $q - 1$ nonabelian groups.
- Now we have

$$\begin{aligned} yxy^{-1} &= x^{\eta^i} \\ y^2 xy^{-1} &= x^{\eta^{2i}} \\ &\vdots \\ y^r xy^{-r} &= x^{\eta^{ri}} \end{aligned}$$

  Thus, $\eta^{ri} = \eta$. Therefore, $y_i = y^r$ so $yxy^{-1} = x^\eta$, so there is at most 1 non abelian group.
- But, P a p-Sylow of S_p and $N = N_{S_p}(P)$ and $C = C_{S_p}(P)$ gives us $|N| = p(p-1)$ and $|C| = p$ so that $N/C = (\mathbb{Z}/p\mathbb{Z})^\times$. We now take the preimage in N so that $\langle y, x \rangle = G$. $|G| = pq$. Then P, G abelian would imply $G \subset C$, but this is not possible since G ahs pq and C has p, so G is not abelian.
- Example $21 = 7 \cdot 3$. $2^3 \equiv 1 \mod 7$. Then we take $\mathbb{Z}/7\mathbb{Z} \to \mathbb{Z}/7\mathbb{Z}$ so we take $x \mapsto x + a$, $x \mapsto 2x + a$, $x \mapsto 4x + a$, on and on where a is a constant. There are 21 such maps.
- If $\eta^1 = 1 \mod p$, then the affine maps from $\mathbb{Z}/p\mathbb{Z}$ to $\mathbb{Z}/p\mathbb{Z}$ send $x \mapsto \eta^i x + b$.
- If we call $\sigma = x + 1$ and and $\tau = x \to x\eta$, then $x \mapsto x + \eta = \sigma\eta$.
- The set of affine maps has both $\mathbb{Z}/p\mathbb{Z}$ and $(\mathbb{Z}/p\mathbb{Z})^\times$ as subsets.
- If we think about the groups we've classified, we've classified $1, p, p^2, p^3, pq$. p^3 just a bit, though. Limit to this strategy: The prime factorizations are so simple that we get immediate and very restrictive information about the p-Sylow subgroups (e.g., the biggest one is normal). This can't occur indefinitely because we will eventually get to cases like A_5 of order 60, for example, which has no normal subgroups.

- If we think about our progress (classifying groups of low order up to 4), then going upwards, the first group we can't do is of order $12 = 2 \cdot 2 \cdot 3$. This is like A_4, which is not too bad but all the same, $n_3 = 1, 4$, $n_2 = 1, 3$. If $n_3 = 4$, then we have an action of G on the 3 Sylow's, giving a transitive map from G to S_4. Thus, the stabilizer has size 3.
- $n_3 = 1$, so $G = P_3 \times P_2$. $n_3 = 1$ and $n_2 = 3$, so $G \times S_3$. Since there is such an explosion of groups, this is not the optimal strategy. Thus, ...
- We may do a review session of the 25 practice problems over Twitch with him playing speedtest.
- At this point, we have the tools to do every outgoing homework problem, save the last one of the last psets on symmetry groups.

8.3 Blog Post: The Sylow Theorems

From Calegari (2022).

11/28:

- Sylow I gives a partial converse to Lagrange's theorem.
  - Lagrange's theorem states, "If H is a subgroup of G, then $|H|$ divides $|G|$."
  - Sylow I states, "If $|G|$ is divisible by p^n, then G has a subgroup said order."
  - Recall that the full converse to Lagrange's theorem is not true: For example, $6|12$, but A_4 has no subgroup of order 6.
- In the proof of Sylow I, we define X as such because G acts **naturally** on X.
- Theorem (Sylow Theorems): Let G be a finite group with order divisible by p.
  1. *Sylow I*: Then G has a p-Sylow subgroup.
  2. *Sylow II*: Any two p-Sylows of G are conjugate. If $Q \subset G$ is any p-group, and P is any p-Sylow, then there exists a $g \in G$ such that $g^{-1}Qg \subset P$ and so $Q \subset gPg^{-1}$. Equivalently, some conjugate of Q is contained in P, and Q is contained in some conjugate of P.
  3. *Sylow III*: Let P be a p-Sylow, and let n_p denote the number of p-Sylows of G. Then...
     (a) $n_p \equiv 1 \mod p$;
     (b) If $N := N_G(P)$ is the normalizer of P in G, then $n_p = [G : N] = |G|/|N|$. In particular, $n_p \big| |G|$.
- Example: Take $G = S_4$ and $p = 2$.
  1. An example is $P = D_8$.
  2. Any two p-Sylows act on the square with four vertices; conjugation is equivalent to a relabeling of the vertices. Indeed, there are six 4-cycles in S_4, and each p-Sylow contains a unique pair $\{g, g^{-1}\}$ of 4-cycles. This leads into...
  3. $N_G(P) = P$, so there are $n_2 = [G : P] = 3$ such subgroups. Note that $n_2 \equiv 1 \mod 2$.
- Example: Take $G = S_4$ and $p = 3$.
  1. An example is $P = \langle (1, 2, 3) \rangle$.
  2. P acts on four vertices by shuffling three points. Conjugation decides which three points are shuffled.
  3. Since there are four possible choices of three points, it should not be surprising that $n_3 = 4 \equiv 1 \mod 3$. Another way of getting this answer is noticing that there are 8 elements of order 3 and each pair $\{g, g^{-1}\}$ gives a subgroup, so $n_3 = 8/2 = 4$. Either way, we end up with the result that $|N_G(P)| = 6$ and $N_G(P) = S_3$.

- Example: Take $G = S_5$ and $p = 5$.
  - We skip out on the part-by-part conclusion here to focus on something more interesting.
  - Here, we have $n_5 = 24/4 = 6 \equiv 1 \mod 5$ by S III. Let X be the set containing the 6 p-Sylows. Then the transitive action $G \circlearrowright X$ by conjugation yields the exotic transitive map from $S_5 \to S_6$.
- Restatement of the p, q classification theorem:
- Theorem: Let p, q be primes such that $p > q$. Then either...
  1. $p \equiv 1 \mod q$, in which case there are two possible groups, one abelian and one not. In either case, the p-Sylow subgroup is normal.
  2. $p \not\equiv 1 \mod q$, in which case there is a unique (abelian and cyclic) group of order pq.

8.4 Symmetries in Three-Space

11/18:

- Classify the finite subgroups of SO(3).
- We can take any regular n-gon and think of $D_{2n} \subset \mathrm{O}(2) \subset \mathrm{SO}(2)$.
- Five platonic solids: Te, Cu, Oc, Do, and Ic.
- Cu and Oc are paired and Do and Ic are paired. Te $\cong A_4$, Cu $\cong$ Oc $\cong S_4$, and Do $\cong$ Ic $\cong A_5$.
- Theorem: Let $G \subset \mathrm{SO}(3)$ be a finite group. Then G is conjugate to one of these groups.
- Let $g \in \mathrm{SO}(3)$, $g \neq e$. The only fixed points of g lie on a line ℓ which contains the origin 0.
- We have a group action $\mathrm{SO}(3) \circlearrowright S^2 = \{v \mid \|v\| = 1\}$. Consider $G \circlearrowright S^2$. Any $g \neq e$ has exactly 2 fixed points which we may call $\{\pm u\}$ for some u.
- Thus, $|\operatorname{Stab}(x)| = 1$ for all but finitely many points $x \in S^2$.
- Claim:
$$\sum_{x \in S^2} |\operatorname{Stab}(x) - 1|$$

Week 9

Simple Groups

9.1 Simple Groups I

11/28:

- **Simple** (group): A group G for which the only normal subgroups of G are G and itself, i.e., $H \triangleleft G$ implies $H = G$ or $H = \{e\}$.
  - Simple does not mean "easy" but means "cannot be broken up into pieces."
  - By analogy, think of atoms as indivisible.
  - If you have G and $H \triangleleft G$, you get H and G/H, and you can think of G as being made up of $H, G/H$. Together, these two groups convey quite a bit of information about G.
  - Warning: $H, G/H$ do *not* determine G; just a lot of information about it.
    - Example: Let $H = \mathbb{Z}/2\mathbb{Z}$ and $G/H = \mathbb{Z}/2\mathbb{Z}$. Then we could have $G = (\mathbb{Z}/2\mathbb{Z})^2$ or $G = \mathbb{Z}/4\mathbb{Z}$.
- Idea: If you want to classify all finite groups, you might start with all finite simple groups, knowing that finite nonsimple groups can in some way be described by its simple quotients and subgroups.
- Problem I (Classification): Classify all finite simple groups.
  - A bit like understanding all prime numbers first in order to understand all composite numbers.
- Problem II (Extension problem): Given A, B, understand all G such that $A \triangleleft G$ and $G/A \cong B$.
  - We can build back up to G with $A \times B$ or other ways.
  - We'll talk about this one less than problem I.
- Examples:
  - Let p be prime. Then $G = \mathbb{Z}/p\mathbb{Z}$ is a simple group.
    - Follows directly form Lagrange's theorem.
    - It's even stronger than simple; the only *subgroups* (let alone normal subgroups) of $\mathbb{Z}/p\mathbb{Z}$ are $\mathbb{Z}/p\mathbb{Z}$ and $\{e\}$.
  - Let $n \geq 5$ and let $G = A_n$. Then A_n is a simple group.
    - More interesting and intricate. Has many subgroups but the only *normal* ones are itself and the trivial one.
    - Note that A_3 is also simple, but cyclic and abelian as well, so it got classified with the above.
- What does it mean to classify simple groups?
  - Start by asking what are the simple groups of some particular order.
  - Start with groups of a certain factorization or those with small order.

  - In this series of lectures, we'll focus on groups of small order. Can we understand for order below 100, 200, or 300?
  - What's important: Less the classification, more the application of techniques we've used. Fancier techniques needed for bigger n.

- Things in math aren't always hard because the technique is hard; they're hard because knowing what technique to use is hard. This is the challenge here.
- The prime factorization of the order says a lot about the group and allows us to make various conclusions.
- Theorem: Let p be prime. Suppose that $|G| = p^n$. Then if G is simple, we have $|G| = p$ and $G \cong \mathbb{Z}/p\mathbb{Z}$.

  Proof. If G is a p-group, then $Z(G) \neq \{e\}$.

  Case 1: $G = Z(G)$, so G is abelian. Therefore, let $g \in G$ have order p and let $H = \langle g \rangle \neq \{e\}$. If G is simple, then $H = G$ and therefore $|G| = p$.

  Case 2: G is not abelian. Take $H = Z(G) \neq G$. We know that $Z(G) \triangleleft G$, so G is not simple, a contradition. □

- Takeaway: $|G| = 2$ is simple, but $|G| = 4, 8, 16, \ldots$ are all not simple.
- The general $p^i q^j$ case is very sophisticated, so we'll start simple.
- Lemma 1: Let $|G| = pq$ where p, q are distinct primes. Then G is not simple.

  Proof. Suppose for the sake of contradiction that G is simple with $|G| = pq$. WLOG, let $p > q$. WTS: One of the Sylow subgroups will be normal. The normal one is the one with greater order (motivation: D_{2n}; it's often useful to consider the p-Sylow subgroups for the largest p). What do we know? From the Sylow theorems, $n_p \cong 1 \mod p$ and $n_p \mid q$ (we know that $|N| = |G|/n_p = pq/n_p$, but since $n_p \equiv 1 \mod p$, $n_p \nmid p$, so it must be that $n_p \mid q$). $p > q$ implies $q \not\equiv 1 \pmod{p}$. Thus, $n_p = 1$. This is a contradiction: If there's only 1 p-Sylow subgroup, then that p-Sylow is normal (because all p-Sylows are conjugate, so one p-Sylow means its in its own conjugacy class). □

- We use a contradiction argument every time.
- Lemma 2: Let $|G| = pqr$. Then G is not simple.

  Proof. Strategy (again): Apply Sylow theorems and get information.

  WLOG, let $p > q > r$. We have that $n_p \equiv 1 \pmod{p}$ and $n_p \mid qr$. $n_p \in \{1, q, r, qr\}$. If $n_p \equiv 1 \pmod{p}$, the p-Sylow is normal in G, a contradiction. $q, r \not\equiv 1 \mod p$, so we eliminate those cases, too. One case left: qr. We thus deduce that $n_p = qr$.

  New technique: Because of these congruences, the number of p-Sylows cannot be really small (congruence obstructions). But we also know that it can't be too big. If there are that many elements of order p, we will crowd out the elements of other orders. We know that $n_q \equiv 1 \mod q$, and $n_q \mid pr$. $n_q = 1$ gives a contradiction. $n_q \not\equiv r$ because $n > r$. Thus, $n_q \in \{p, pr\}$. Doing the same thing for n_r, we get three possibilities: p, q, pr. Next step: Count elements. How many elements of order p are in G?

  Proposition: If $p \mid |G|$ exactly, then any two distinct p-Sylows have only trivial intersection. The number of $g \in G$ of order p is equal to $n_p(p-1)$.

  Because p exactly divides p, each p-Sylow is a subgroup of order p, but their intersection is a subgroup and thus has to divide the order (Lagrange's theorem). Thus, the order of the intersection is either 1 or p. Thus, all elements of order p lie in trivially intersecting p-Sylows. We count $p-1$ elements of order p for each p-Sylow (p minus the identity).

Thus, since $p \,||\, |G|$ in this case, we know that the number of $g \in G$ with $|g| = p$ is $n_p(p-1) = qr(p-1)$. The number of $g \in G$ with $|g| = q$ is $n_q(q-1) \geq p(q-1)$. The number of $g \in G$ with $|g| = r$ is $n_r(r-1) \geq q(r-1)$. Counting the number of elements and the identity, we get

$$qr(p-1) + p(q-1) + q(r-1) + 1 = qrp + pq - p - q + 1 = pqr + (p-1)(q-1) > pqr = |G|$$

a contradiction. □

- This has to fail eventually, though — we know A_5 is simple for instance, and it has prime factorization $2^2 \cdot 3 \cdot 5$, so pqr^2 can be simple.
- Thus, we now turn to other types of factorizations.
- Thus, consider variations of the two primes case.
- First, new technique.
- Lemma 3: Let $G \subset S_4$ is simple. Then $|G| = 2, 3$.

  Proof. If we have a homomorphism from a simple group to any other group, it is either trivial or injective (our group doesn't break up; it either injects fully or disappears completely). We know that $\ker \phi \triangleleft G$, so if G is simple, either $\ker \phi = \{e\}$ (injective) or $\ker \phi = G$ (trivial).

  We know that $A_4 \triangleleft S_4 \twoheadrightarrow S_4/A_4 \cong \mathbb{Z}/2\mathbb{Z}$. Now let $G \triangleleft S_4$. We can apply a homomorphism to get a map from $G \to S_4/A_4$. It follows by the above claim that the homomorphism is either trivial or injective.

  Let Γ be a group with $A \triangleleft \Gamma$. Let $\Gamma/A = B$. If $G \hookrightarrow \Gamma$ is simple, then either $G \hookrightarrow A$ or $G \hookrightarrow \Gamma/A = B$. Proof: We have $G \to \Gamma \to \Gamma/A = B$. Case 1: G injects into B, so we get the latter claim. Case 2: the map is trivial, so everything in G maps to the identity in $B = \Gamma/A$. Then $G \leq A$. So if we know how to divide our group up, we can make something of the pieces.

  Returning to our example, we have $A_r \triangleleft S_4$, $S_4/A_4 = \mathbb{Z}/2\mathbb{Z}$, so $G \hookrightarrow A_4$, $G \hookrightarrow \mathbb{Z}/2\mathbb{Z}$. In the latter case, it has order 2. We have $K \triangleleft A_4$ and $A_4/K \equiv \mathbb{Z}/3\mathbb{Z}$. So either $G \leq K$ or $G \leq \mathbb{Z}/3\mathbb{Z}$. The first one implies since $K = (\mathbb{Z}/2\mathbb{Z})^2$ that $G \triangleleft \mathbb{Z}/2\mathbb{Z}$. □
- Groups of order 2,3 are trivially simple, so it's kind of meaningless, but doesn't matter; the lemma still holds.
- We narrowed in on the case of S_4 in order to prove our next theorem.
- Lemma 4 (No small actions): Let G be a simple group, and suppose $G \curvearrowright X$ transitively, where $|X| = 2, 3, 4$. Then $|G| = 2, 3$.

  Proof. Given a transitive action, we get a homomorphism $G \to S_X$. Transitivity and $|X| \geq 2$ implies the homomorphism is nontrivial. But since G is simple, $G \hookrightarrow S_X$. But since $|X| \leq 4$, this means that $G \hookrightarrow S_4$. We now use Lemma 3. This means that $|G| = 2, 3$.

  See lemma 6 for the kind of group action we are talking about?? □
- Corollary: If $p \mid |G|$, p is prime, G is simple, $|G| \neq 2, 3, p$, then $n_p \neq 1, 2, 3, 4$.
- Next time: At the same time these videos release, there will be a blog post with the statements of these lemmas and maybe some words on them.

9.2 Office Hours (Abhijit)

- What do we need to know about the affine group of order p, as discussed in Lecture 8.1?
- Friday's office hours will be the last one unless Frank changes something. If the Twitch stream actually happens, Abhijit isn't sure what day it would be. Frank is currently traveling.
- HW8 2c requires 2d.
- Abhijit will email me more info on the A_5 question that he "beat a tactical retreat from."

9.3 Simple Groups II

11/30:

- Lemma 5: Assume $|G| = 2p^n, 3p^n, 4p^n$. p is a prime, and for mp^n, $m \neq p$. Then G is not simple.

  Proof. We again look at p-Sylows and how many are there. n_p must divide the order of the group and not divide p in these cases. Therefore, $n_p = 1, 2, 3, 4$, so as in Lemma 4, we have a very small set for G to act on. Thus, by Lemma 4, G is not simple. □

- Beefing this up a bit.

- Lemma 6: Assume $|G| = 5p^n$. Then G is not simple.

  Proof. Only interesting case: $n_p = 5$. In this case, we get an action of G on 5 points, namely the transitive action of G on the 5 p-Sylows by conjugation. Thus, we get an injective map $G \to S_5$, so $G \leq 5$ and has order $5p^n$. Additionally, since $n_p = 5 \equiv 1 \pmod{p}$, we know that $p = 2$. What else can we say? We now look at n_5. We know from Sylow III that $n_5 \equiv 1 \mod 5$ and $n_5 \mid (p^n = 2^n)$, so $2^n \geq 16$ (since $16 \equiv 1 \mod 5$ and 16 divides a power of 2). Thus, $|G|$ divides 16, but $|S_5| = 120$ which is not divisible by 16, a contradiction. □

- See again the procedure of "assume it's simple; derive a contradiction."

- Lemma 7: Assume $|G| = 6p^n$. Then G is not simple.

  Proof. We know that $n_p \mid 6$, so $n_p = 1, 2, 3, 6$. Lemma 4: $n_p = 6$. Sylow III: $n_p \equiv 1 \mod p$. Thus, $p = 5$. G acts on 6 p-Sylows, so we get an injective map from $G \hookrightarrow S_6$. How many powers of 5 can divide $|S_6|$? Only 5^1, so we must have $n = 1$. Thus, $|G| = 6 \cdot 5 = 30 = 5 \cdot 3 \cdot 2$. Applying Lemma 2 (3 distinct primes) finishes us off. □

- Lemma 8: Assume $|G| = 8p, 9p$. Then G is not simple.

  Proof. Look at n_p. $n_p = 1, 2, 4, 8$ in the first case; $n_p = 1, 3, 9$ in the second case. Lemma 4: Rule out $1, 2, 4$ and $1, 3$. Thus, $n_p = 8$ in the first case and $n_p = 9$ in the second case.

  First case: $n_p = 8$ and $n_p \equiv 1 \mod p$. We must have $p = 7$. Thus $|G| = 8 \cdot 7 = 56$. That's all we can get from the p-Sylow; now let's look at the 2-Sylow ($2^3 = 8$). $n_2 = 1, 7$. We apply the pqr too-many-elements style again. Number of elements of order 7 is $n_7(7-1) = 8 \cdot 6 = 48$. We have a group of 56 elements and 48 of them have order 7. So what's left? There are 8 elements left. But we know that the 2-Sylow has order 8, so let $P = G \setminus \{g \in G \mid |g| = 7\}$. Then $|P| = 8$. This implies that there is only one 2-Sylow, so $n_2 = 1$, meaning that the 2-Sylow is normal and giving us a contradiction. □

- Again, we only have a contradiction because we are assuming G is simple. If we don't assume G is simple, we have a perfectly valid mathematical derivation of the properties of a group of order $8p$.

- Example: Let $G = A_4$. Then $|G| = 12 = 3 \cdot 2^2$, so $n_3 = 1, 2, 4$ and $n_3 \equiv 1 \mod 3$. The 3-Sylow in A_4 is not normal, so $n_p \neq 1$. $n_p \neq 2$ because $2 \not\equiv 1 \mod 3$. Thus, $n_3 = 4$ and therefore the number of elements of order 3 is $n_3(3-1) = 4 \cdot 2 = 8$. Thus, there are 12 elements A_4 minus 8 elements of order 3, so there are 4 elements left. These 4 elements compose the 2-Sylow, meaning that the 2-Sylow is normal. And here (where we're not assuming G is simple), that's fine!

- So far: Continuing to build up and rule out groups of certain (mostly prime) factorizations.

- This will not classify all simple groups, but if we start taking n to be small, we know the factorizations of small numbers tend to have a small number of prime factors. So can we classify all groups of small order? That's our task now.

- Lemma 9: If $|G| = 84, 126, 140, 156, 175, 189, 198, 200$, then G is not simple.

Proof. $84 = 7 \cdot 3 \cdot 2^2$. Sylow III: $n_7 \equiv 1 \mod 7$ and $n_7 \mid 12$, so $n_7 = 1$.
$126 = 7 \cdot 18$. Sylow III: $n_7 \equiv 1 \mod 7$, $n_7 \mid 18$ implies $n_7 = 1$.
$140 = 7 \cdot 20$. Sylow III: $n_7 \equiv 1 \mod 7$, $n_7 \mid 20$ implies $n_7 = 1$.
$189 = 7 \cdot 27$. Sylow III: $n_7 \equiv 1 \mod 7$, $n_7 \mid 27$ implies $n_7 = 1$.
$176 = 11 \cdot 16$. Sylow III: $n_{11} \equiv 1 \mod 11$, $n_{11} \mid 16$ implies $n_{11} = 1$.
$176 = 11 \cdot 18$. Sylow III: $n_{11} \equiv 1 \mod 11$, $n_{11} \mid 18$ implies $n_{11} = 1$.
$175 = 5^2 \cdot 7$. Sylow III: $n_5 \equiv 1 \mod 5$, $n_5 \mid 7$ implies $n_5 = 1$.
$200 = 5^2 \cdot 8$. Sylow III: $n_5 \equiv 1 \mod 5$, $n_5 \mid 8$ implies $n_5 = 1$.
$156 = 13 \cdot 12$. Sylow III: $n_{13} \equiv 1 \mod 13$, $n_{13} \mid 12$ implies $n_{13} = 1$. □

- A bit messy and *ad hoc*, but this covers the simple groups of certain orders we haven't covered so far.
  - If you do a random case for a small number, often it will be a bit like this.
- For a bunch of small numbers, we immediately get without any work from the Sylow theorems a normal p-Sylow.
  - We actually get these conclusions for any groups of these orders??
- This way of thinking lends itself to you generating your own problem; you basically choose a random number and look for a prime with $n_p = 1$.
- Two more exceptional cases.
- Lemma 10: If $|G| = 132$, then G is not simple.

Proof. $132 = 11 \cdot 12$, so $n_{11} = 1, 12$. If 1, we're done. If very large, we get that contradiction. The number of elements of order 11 is $n_{11}(11-1) = 12 \cdot 10 = 120$, so only 12 elements left. We now consider other primes. $11 \cdot 12 = 11 \cdot 3 \cdot 2^2$. $n_3 \equiv 1 \mod 3$, $n_3 \mid 44$. Thus, $n_3 = 1, 2, 4, 11, 22, 44$. If 1, we're done. 2,11,44 can't happen because of the congruence law. If $n_3 = 4$, apply Lemma 4. Thus, $n_3 = 22$, so the number of elements of order 3 is $n_3(3-1) = 22 \cdot 2 = 44$. $120 + 44 > 132$, so we win. □

- At this point, we've considered a bunch of easy general and special cases. At this point, let's look at the numbers under 200 we can rule out.
  - Calegari writes out all numbers from 1-200.
  - For the prime numbers, there is a simple group of that order.
  - Powers of primes, there is no simple group, so we can cross those off ($4 = 2^2, 8 = 2^3, 9 = 3^2, 16 = 2^4, 25 = 5^2, 27 = 3^3, 32 = 2^5, \dots$).
  - Products of two primes, there is no simple group ($6 = 2 \cdot 3, 10 = 2 \cdot 5, 15 = 3 \cdot 5, \dots$).
  - Products of three distinct primes, there is no simple group ($30 = 2 \cdot 3 \cdot 5, 42 = 2 \cdot 3 \cdot 7, \dots$).
  - Everything that's $2p^n, 3p^n, 4p^n$, there is no simple group ($12 = 3 \cdot 2^2, 18 = 2 \cdot 3^2, \dots$).
  - Everything that's $5p^n$, there is no simple group ($20 = 5 \cdot 2^2, 40 = 5 \cdot 2^3, \dots$).
  - Everything that's $6p^n$, there is no simple group (just $150 = 6 \cdot 5^2$). Only got one number with Lemma 7 :(
  - Everything that's $8p, 9p$, there is no simple group ($56 = 8 \cdot 7, 63 = 9 \cdot 7, 88 = 8 \cdot 11, 99 = 9 \cdot 11, \dots$).
  - Exceptional numbers done by hand: $84, 126, 132, 140, 156, 175, 189, 198, 200$.
- There are no simple groups of order 1 by definition, so the trivial group is not a simple group much the same way 1 is not a prime number.

- At this point, we have to acknowledge that this list left out numbers, so we have to see what's left and then work with it.
- First numbers up: 60 (there does happen to be a simple group of this order here — A_5), 72, 90.
  - Thus, if we have a simple group of order less than 100, it is of prime order or of order 60, 72, or 90 (note that we can still eliminate 72 and 90, but we haven't investigated them yet, so it's fair to include them here; not the most restrictive theorem, but a valid one all the same).
- Next numbers up: 112, 120, 144, 168, 180.
  - Calegari really does have quite a fast mind as he's doing prime factorizations by memory.
- Thus, using the lemmas, we've proven the following: A simple group of order at most 200 either has prime order, or order 60, 72, 90, 112, 120, 144, 168, or 180.

9.4 Simple Groups III

12/2:

- Proposition: Let G be a simple group of order $|G| \leq 200$. Then either $|G|$ is prime (in which case we know there is a unique simple group of said order) or $|G| \in \{72, 112, 60, 90, 120, 144, 180, 168\}$.
  - These numbers are not in increasing order; they are more or less in order of increasing difficulty.
- Case: $|G| = 72 = 3^2 \cdot 2^3$.

  Proof. $n_3 \equiv 1 \mod 3$ and $n_3 \mid 8$, so either $n_3 = 1, 4$. $n_3 = 1$ implies normal 3-Sylow; $n_3 = 4$ implies invoke Lemma 4. Therefore, G is not simple. □

- Reminder: If G is simple, then any homomorphism from it to another group must be either trivial or injective.
- Lemma 11: Let G be a simple group with a transitive action on a set of $n \geq 2$ points. Then $G \hookrightarrow A_n$ or $|G| = 2$.

  Proof. The action induces a homomorphism $G \to S_n$ which is nontrivial. Therefore, $G \hookrightarrow S_n$. Now we want to upgrade this map and restrict the range. Now suppose that the image is not in A_n. Then the composite map $G \to S_n \to S_n/A_n \cong \mathbb{Z}/2\mathbb{Z}$ is nontrivial. If $g \in A_n$, then $g \mapsto eA_n = A_n$. If $g \notin A_n$, then $g \mapsto gA_n$. This nontrivial map into $\mathbb{Z}/2\mathbb{Z}$ implies, since G is simple, that $G \hookrightarrow \mathbb{Z}/2\mathbb{Z}$, so $|G| = 2$. □

- Lemma 12: If $|G| = 112$, then G is not simple.

  Proof. $112 = 7 \cdot 2^4$. We can deduce that $n_7 \equiv 1 \mod 7$ and $n_7 \mid 16$, so $n_7 = 1, 8$. If $n_7 = 1$, we win, so let's consider $n_7 = 8$. 8 is pretty big, but not too big. It's in this annoying intermediate range. We deduce from this that there are $n_7(7-1) = 8 \cdot 6 = 48$ elements of order 7, which doesn't help much. Here, it's better to look at $n_2 = 1, 7$. If $n_2 = 1$, we win, so consider $n_2 = 7$. Then by Lemma 11, $G \hookrightarrow A_7$. $|G| = 112$ and $|A_7| = 2520$. But $|G| \nmid |A_7|$, contradicting Lagrange's Theorem. □

- Next up: 60, 90, 120, which we will consider all at once because they're all a bit similar. One preliminary lemma first, though.
- Lemma 13: Let $n \geq 5$ and $H \leq A_n$ of index $d > 1$. Then $d \geq n$ and if $d = n$, then $H \cong A_{n-1}$. In other words, there are no small-index subgroups and the smallest one is isomorphic to A_{n-1}.

Proof. A_n acts transitively on the cosets A_n/H (by left multiplication??), inducing a nontrivial map from $A_n \to S_d = S_{\{\text{cosets}\}}$. Since A_n is simple for $n \geq 5$, we get that $A_n \hookrightarrow A_d = A_{\{\text{cosets}\}}$ (by Lemma 11). The injection implies that $d \geq n$. Now assume that $d = n$. Then we have an isomorphism from A_n to $A_{\{\text{cosets}\}}$. What is $H \leq A_n$? How does H act on $A_{\{\text{cosets}\}}$? Well H stabilizes the coset H, so $H \hookrightarrow \text{Stab}(H)$. But the stabilizer of a point in the symmetric group is isomorphic to the symmetric group of one smaller size, and the same holds true in the alternating group, so $\text{Stab}(H) \cong A_{n-1}$. $[A_n : H] = n$ by hypothesis, so $|H| = (n!/2)/n = (n-1)!/2$. But since this is also $|A_{n-1}|$, we have an injection from H into a group of the same order, meaning that we have a bijection. In particular, $H \cong A_{n-1}$, as desired. □

- Comments on Lemma 13: ...
- Lemma 14: If G is simple and $|G| \in \{60, 90, 120\}$, then $G \cong A_5$. In particular, we rule out 90,120 and know that 60 must be the last number standing.

  Proof. $60 = 5 \cdot 12$, $90 = 5 \cdot 18$, $120 = 5 \cdot 24$. $n_5 \equiv 1 \mod 5$ and $n_5 \mid 12, 18, 24$ implies $n_5 = 1, 6$ (we can confirm that 11,16,21 are not factors). If $n_5 = 1$, we're done, so assume $n_5 = 6$. G acts on the 6 5-Sylow subgroups transitively, giving us $G \hookrightarrow A_6$ by Lemma 13. $[A_6 : G] = 6, 4, 3$ for 60,90,120. But by Lemma 13, $d \geq 6$, so contradiction for 90,120, and the latter part of the Lemma proves that $G \cong A_5$. □

- We have our first genuine simple group of nonprime order at this point, and we know that that group is unique and equal to A_5.
- Lemma 15: There is no simple group of order 144.

  Proof. Many of the arguments we've used thus far will play in, but in new and unexpected ways. We have $144 = 2^4 3^2$. $n_3 \equiv 1 \mod 3$ and $n_3 \mid 16$, so $n_3 = 1, 4, 16$. If $n_3 = 1$, we're done (normal 3-Sylow). If $n_3 = 4$, we apply Lemma 4. Thus, $n_3 = 16$. Number of elements of order 3: Issue — we no longer know that the intersections of the p-Sylows are trivial since $p^2 = 9$; we could have a subgroup of order 3 as the intersection.

  Case 1: $P \neq Q$ are 3-Sylows, WTS: $P \cap Q = \{e\}$. Number of elements of order 3 or 9 is $n_3 \cdot 8 = 16 \cdot 8 = 128$. This leaves $144 - 128 = 16$ elements. But since G has a 2-Sylow P_2 of order 16, so $G = P_2 \cup \{|g| = 3, 9\}$. Thus, $n_2 = 1$, so we have a normal subgroup, which is a contradiction.

  Case 2: There exist 3-Sylows P, Q such that $C = P \cap Q$ has $|C| = 3$. We can still gain some advantage since it's 3^2, not 3^n. Remark: If $|P| = 9$, then P is abelian. Recall that p-groups of order p^2 are abelian. What other constructions do we have for subgroups besides Sylows? Consider $N = N_G(C)$, where $C = P \cap Q$. $C \leq P$ and $C \leq Q$. But since P is abelian, then $P \subset N_G(C)$. Lagrange: $9 \mid N \mid 144$, so $N = 18, 36, 72, 144$. So we need 4 contradictions to finish this off. If $|N| = 144$, then $N = G$. But since $C \triangleleft N$, this means that $C \triangleleft G$, i.e., G has a normal subgroup and is not simple, a contradiction. If $N = 72, 36$, then $[G : N] = 2, 4$. Thus, G acts transitively on a set of size 2,4, so Lemma 4 eliminates these. Only possibility: $|N| = 18$. We know that $Q \subset N$ and $P \subset N$. By applying the Sylow theorems to N, we get that $n_3 \equiv 1 \mod 3$, $n_3 \mid 2$, so $n_3 = 1$, but N contains 2 distinct p-Sylows, a contradiction. □

- The case of 180 is quite similar.
- Lemma 16: There is no simple group of order 180.

  Proof. $180 = 5 \cdot 3^2 \cdot 2^2$. $n_5 \equiv 1 \mod 5$, so $n_5 = 1, 6, 36$. $n_5 \neq 1$. If $n_5 = 6$, then $G \hookrightarrow A_6$ and we get index 2, which is a contradiction by Lemma 13 (same contradiction as with 90,120). If $n_5 = 36$, then we get a number of elements of order 5 equal to $n_5(5-1) = 144$, leaving $180 - 144 = 36$ elements left to contain the 2-Sylows and 3-Sylows. But we get the same annoyance about whether or not they overlap.

$n_3 \mid 20$ and $n_3 \equiv 1 \mod 3$ yields $n_3 = 1, 4, 20$. $n_3 = 1$ is normal, 4 invokes lemma 4, so $n_3 = 20$.

Case 1: $P \cap Q = \{e\}$. Then the number of elements of order 3 or 9 is $n_3(9-1) = 160$. Contradiction (too many elements).

Case 2: $P \cap Q = C$, $|C| = 3$. Take $N = N_G(C)$. So once again, we have $9 \mid |N| \mid 180$ and $|N| > 9$. Thus, $|N| = 18, 36, 45, 90, 180$. $|N| = 180$ gives us $C \triangleleft G$ again. $|N| = 90, 45$ yields $[G : N] = 2, 4$ again. This leaves us with 18,36. We can't have 2 3-Sylows, so $|N| = 36$. Thus, $[G : N] = 5$. This induces $G \hookrightarrow A_5$, but G is too big; $G \not\leq A_5$, a contradiction. □

- Summary of what we've proven so far.
- Theorem: Let G be a simple group of order at most 200. Then either...
  1. $|G| =$ prime;
  2. $G \cong A_5$;
  3. $|G| = 168$ and $G \cong \mathrm{GL}_3(\mathbb{F}^2) \cong \mathrm{PSL}_2(\mathbb{F}_7)$.
- This is the limit of what we'll do; Calegari doesn't think it's worth the hour it'd take to do a full analysis of 168.
- A word on 168, though.
  - $168 = 2^3 \cdot 3 \cdot 7$.
  - Deduce that $n_7 = 8$. $n_2 = 1, 3, 7, 21$ so $n_2 = 7, 21$. $n_3 = 1, 2, 4, 7, 8, 14, 28, 56$ so $n_3 = 7, 28$ by Lemma 4 and the $1 \mod 3$ rule. But none of the remaining numbers are super easy to work with; we need normalizers and such.
  - Start with n_7 to learn that $G \hookrightarrow A_8$. We also know that $n_7 = [G : N]$, so $|N| = 21$. Let P be a 7-Sylow. Up to conjugation, we may as well take $P = \langle (1, 2, 3, 4, 5, 6, 7) \rangle \subset A_6$. Additionally, $N \subset N_{A_8}(\langle (1, 2, 3, 4, 5, 6, 7) \rangle)$ which has order 21.
  - More and more elaborate facts lead you to write down parts of the group in terms of elements of A_8.
  - The contradictions and computations we eventually get do get messy eventually.
  - The reason for this is because there *does* exist a simple group of order 168: We know that $\mathrm{SL}_2(\mathbb{F}_7)$ has an action on 8 points. The quotient $G = \mathrm{PSL}_2(\mathbb{F}_7)$ is a simple group of order 168.
  - There's another group $|\mathrm{GL}_3(\mathbb{F}^2)| = (2^3 - 1)(2^3 - 2)(2^3 - 2^2) = 168$. These two groups are isomorphic (this is completely opaque from the description, but it is true; there is an exotic isomorphism; it's like the story between the cube group and S_4?? This is a recurring theme in finite group theory).
  - Indeed, these two groups are the only one of 168.
- On the blog, Calegari will continue from 200 all the way up to 300.
- Particularly bad cases include more and more powers of 2 and 3.
- Theorem (Burnside's pq theorem): If $|G| = p^n q^m$, then G is not simple.
  - In other words, once you remove the cyclic group, any simple group has at least 3 prime factors dividing its factorization.
  - This theorem is beyond the scope of this course, but it could come up in an intro grad course on representations of groups.
- In our course, we've really been studying actions of G on finite sets, i.e., maps to symmetric groups.

  - Another natural thing we can do is consider the actions on vector spaces (specifically the basis of a vector space). This corresponds to a map from $G \to \mathrm{GL}_n(V)$. This is a rich theory and allows us to write out all the possible representations. Proving Burnside's pq theorem involves all of this plus algebraic number theory.

- Burnside's pq theorem came to prominence around 1900, so about 120 years back.
- Theorem (Feit-Thompson): If G is a simple group and $|G|$ is odd, then $|G|$ = prime.
  - From the 1960s.
  - This is the start of modern group theory.
  - It follows by the Sylow theorems that our group has an element of order 2. From here, we can start to think about the classification of all finite simple groups.
- Thus, not only do simple groups have to have at least 3 prime factors, they also have to have even order.
- The classification of finite simple groups was achieved 20-30 years after Feit-Thompson.
  - Thus, we now really understand all finite simple order.
  - This means that we can describe them by various lists that we know how to construct.
  - Examples: Cyclic groups of prime order, A_n ($n \geq 5$), $\mathrm{PSL}_n(\mathbb{F}_p)$ ($n \geq 3$ or $n = 2$ and $p \geq 5$).
  - Calegari goes over several more groups of Lie type. There are also 26 sporadic group types that don't really fit in any other category. One class called the Mathieu group. Simplest weird group: M_{11} of order $11 \cdot 10 \cdot 9 \cdot 8 = 7920$. There's also M_{12}, M_{23}, M_{24}. There are 26 of these leading up to a group M called the **monster group** (of order $\approx 8 \times 10^{53}$).
  - We have to be careful in saying that the monster group is scary just because it's so big; indeed, S_{52} is bigger. But the latter is understandable by its action on a relatively small set. S_{52} acts on a vector space of dimension 52. If you try to let M act on a vector space, the dimension is 196883.
  - Something better than this type of description is infinite groups. The most interesting infinite groups arise when you have topological considerations as well (e.g., continuity). This is why S_∞ is not the most interesting. We have orthogonal and unitary groups (these arise in physics often as infinite symmetry groups). Pure topology and spaces and symmetries are potential applications, too. We don't consider these in this course because these topics are so intertwined.
- Next quarter is ring theory, and last quarter is Galois theory.
- In group theory, you want to understand all finite groups. In ring theory, you don't want to classify rings; rather, you want to consider a bunch of simple rings that come up all the time, and you want to understand those very well.

9.5 Twitch Stream

12/3:

- 18a of the review sheet is true.
  - Orbit-Stabilizer Theorem: $|C| \cdot |\langle g \rangle| = |G|$. C is the centralizer. So we need to compute the size of the conjugacy class of the n-cycle. There are $n!/n$ of these. So $C = n$.
  - The centralizer is not the normalizer; the latter will be bigger.

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.