Week 1

???

1.1 Understandig Groups as Shuffles

9/28:
- Office hours will be pooled between the two sections.
  - Our section's TA is Abhijit Mudigonda (abjihitm@uchicago.edu). His office hours will always be in JCL 267[1]. The times are...
    - Monday: 12:30-2:00 (OH).
    - Wednesday: 1:30-2:30 (PS).
    - Thursday: 12:30-2:00 (OH).
  - The other section's TA is Ray Li (rayli@uchicago.edu). His office hours will always be in Eck 17[2]. The times are...
    - Tuesday: 5:00-7:00 (OH).
    - Thursday: 4:00-5:00 (OH).
    - Thursday: 5:00-6:00 (PS).
- Textbook: Abstract Algebra. Download the PDF from LibGen.
- Weekly HW due on Monday at the beginning of class. Submit online or in person. There is a webpage w/ all the homeworks, but don't do them all at once because they're subject to change.
- Notes on math and math pedagogy.
  - There's a tendency to say here's an object, here's its properties, etc.
  - But this is not historically accurate or motivated. Calegari really gets it! Math is motivated by abstracting examples.
  - Let's not just define a group, but start with an example. This week, we will give examples of groups. In later weeks, we will establish the axiomatic framework that is really only there to understand these examples.
  - Don't stare at the page blankly waiting for inspiration when doing homework; think of examples first and test out your intuition on them to actually understand what the question means.
  - There are some hard problems; work with each other, but acknowledge our collaborators.
  - In-class midterm; final will be take-home. Calegari doesn't like timed exams.
- Today's example: Shuffling.
  - 52 cards; can be shuffled.

[1]JCL is John Crerar Library.
[2]Eckhart basement.

- Number of shuffles:
$$|\text{shuffles}| = 52! \approx 8 \times 10^{67}$$
- Properties of shuffles.
  - **Distinguished shuffle**: e, the identity shuffle, where you do nothing.
  - Shuffle once; shuffle again. The composition of two shuffles is another shuffle.
  - If you repeat the *same* shuffle enough times, the cards will come back to the same order.
    - Let σ be a shuffle, and $n \in \mathbb{N}$. Does there exist n such that
$$\sigma^n = \underbrace{\sigma \circ \cdots \circ \sigma}_{n \text{ times}} = e$$
    - Proving this: By the piegeonhole principle, if you have $\sigma^1, \dots, \sigma^{52!+1}$, then we have repeats a, b with $52! + 1 \geq a > b \geq 1$ such that $\sigma^a = \sigma^b$. This statement is weaker than we want, though.
    - We need more tools. A shuffle is a bijection/permutation. Thus, for every σ, there exists σ^{-1}. This allows us to do this:
$$\begin{aligned} \sigma^a &= \sigma^b \\ \sigma^{-b} \circ \sigma^a &= \sigma^{-b} \circ \sigma^b \\ \sigma^{a-b} &= e \end{aligned}$$
    - This implies a bound! We get that $n \leq 52!$, so $a - b \leq 52!$.
- Define two shuffles: A and B.
  - A splits the deck into two halves (cards 1-26 and 27-52) and stacks (from the top down) the first card off of the 1-26 pile, then the first card off of the 27-52 pile, then the second card off of the 1-26 pile, then the second card off of the 27-52 pile, etc. The final order is $1, 27, 2, 28, \dots, 26, 52$.
  - B does the same thing as A but with the first card off of the 27-52 pile. The final order is $27, 1, 28, 2, \dots, 52, 26$.
- Computation shows that $A^8 = e$ and $B^{52} = e$.
  - For A, $2 \to 3 \to 5 \to 9 \to 17 \to 33 \to 14 \to 27 \to 2$.
  - For B, ??
- We 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.