

# 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 (abhijitm@uchicago.edu). His office hours will always be in JCL 267<sup>[1]</sup>. 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<sup>[2]</sup>. 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.

---

<sup>1</sup>JCL is John Crerar Library.

<sup>2</sup>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  $\sigma$  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 pigeonhole 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  $\sigma$ , there exists  $\sigma^{-1}$ . 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  $A$ ,  $2 \rightarrow 3 \rightarrow 5 \rightarrow 9 \rightarrow 17 \rightarrow 33 \rightarrow 14 \rightarrow 27 \rightarrow 2$ .
- 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  $G \times G \rightarrow G$ .

- **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  $(G, *)$ .

- 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.,  $\phi : \text{cube} \rightarrow \text{cube}$ .
  - 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  $M : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ .
  - We want it to preserve angles, i.e., orthogonality. Thus, we should assert  $MM^T = I$ .
  - We also want it to preserve orientation. Then we should have  $\det(M) = 1$ .
- **Cu:** The cube group.
- Does the permutation of faces determine  $M$ ?
  - Yes.
  - Furthermore, if we know where  $e_1, e_2$  go, then the fact that orientation and orthogonality are preserved implies that we know where  $e_3$  goes. Thus,  $M$  is determined by two (adjacent) faces.

- An upper bound on  $|\text{Cu}|$ .
  - Send  $e_1$  to one of 6 faces and send  $e_2$  to one of the 5 remaining faces (so  $|\text{Cu}| \leq 6 \cdot 5 = 30$ ).
  - Send  $e_1$  to one of 6 faces and send  $e_2$  to one of the four remaining *adjacent* faces (so  $|\text{Cu}| \leq 6 \cdot 4 = 24$ ).
  - And, in fact,  $|\text{Cu}| = 24$ .
- Moreover, since the rotations of the cube are determined by permutations of the faces, we can map  $\text{Cu} \hookrightarrow S_6$ . Additionally, composing any permutations of the faces is the same as composing any permutations of  $S_6$ , i.e.,  $\phi$  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  $\text{Cu}$  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  $\text{Cu} \rightarrow S_4$ . We now just need to prove it's bijective.
  - Let  $v_1, v_2, v_3, v_4$  be the vertexes of one face. Then  $-v_1, \dots, -v_4$  are the vertexes of the opposite face, and the line from each  $v_i$  to  $-v_i$  is a diagonal of the cube. To prove that the function is bijective, we will show that different elements of  $\text{Cu}$  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.

---

<sup>3</sup>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  $\text{SO}(3)$ . Thus, we need only prove that the second set is exactly  $\text{SO}(3)$ . 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

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

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

Without going into detail, the orientation issue further restricts us to  $\text{SO}(3)$ . □

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