

# Week 2

???

## 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
$O(n)$ and $SO(n)$	(sp) orthogonal matrices	composition	vectors?
$\mathbb{Z}$	integers	addition	
$\mathbb{Z}/n\mathbb{Z}$	$\{0, 1, \dots, n-1\}$	addition modulo $n$	

Table 2.1: Elements of a group.

- Be careful not to confuse the shuffles and the cards; the cards are something else curious but are *not* the elements of the group.
- Notice that  $\mathbb{Z}$  and  $\mathbb{Z}/n\mathbb{Z}$  are **commutative** groups, but the shuffles (for  $n > 1$ ) and  $O(n)$  are not.
- Note that  $S_2$ ,  $O(1)$ , 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  $n^2$ ?
  - 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  $g = g'$ .  $\square$

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

	$e$	$x$	$y$
$e$	$e$	$x$	$y$
$x$	$x$		
$y$	$y$		

 $\longrightarrow$ 

	$e$	$x$	$y$
$e$	$e$	$x$	$y$
$x$	$x$	$y$	$e$
$y$	$y$	$e$	$x$

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

- Start from the left table above.
- Notice that row 3 has a  $y$  and column 2 has an  $x$ , so by the Sudoku Lemma,  $e$  must be the element in row 3, column 2.
- Then column 2 has  $e, x$  in it, so the entry in row 2, column 2 must be  $y$ .
- 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:

$1^1 = 1$	$= 1$	$(1, 1)^1 = (1, 1)$	$= (1, 1)$
$1^2 = 1 + 1 = 2$		$(1, 1)^2 = (1 + 1, 1 + 1) = (2, 0)$	
$1^3 = 2 + 1 = 3$		$(1, 1)^3 = (2 + 1, 0 + 1) = (0, 1)$	
$1^4 = 3 + 1 = 4$		$(1, 1)^4 = (0 + 1, 1 + 1) = (1, 0)$	
$1^5 = 4 + 1 = 5$		$(1, 1)^5 = (1 + 1, 0 + 1) = (2, 1)$	
$1^6 = 5 + 1 = 0$		$(1, 1)^6 = (2 + 1, 1 + 1) = (0, 0)$	
$1^7 = 0 + 1 = 1$		$(1, 1)^3 = (0 + 1, 0 + 1) = (1, 1)$	

- 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 Characteristics of the Symmetric Group

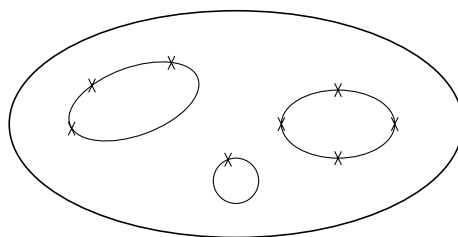
10/5:

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

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

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

- If  $\sigma$  is a  $k$ -cycle, then the order of  $\sigma$  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  $\sigma$  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  $\sigma$  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  $x \sim y$ .
- 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:** A subset of  $G$  containing all  $g \in G$  which are conjugate to a certain  $x \in G$ .
- 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.