Lecture 02

Melissa Zhang

MAT 150A

Participation Slip

1. Take a slip from the front of the room.
2. Write your full name on the top left corner.
3. Answer the following question. You are encouraged to discuss your answer with those around you.

Question (write solution on participation slip)

There are five seats in the a classroom, and five students. How many different ways are there to seat the students?

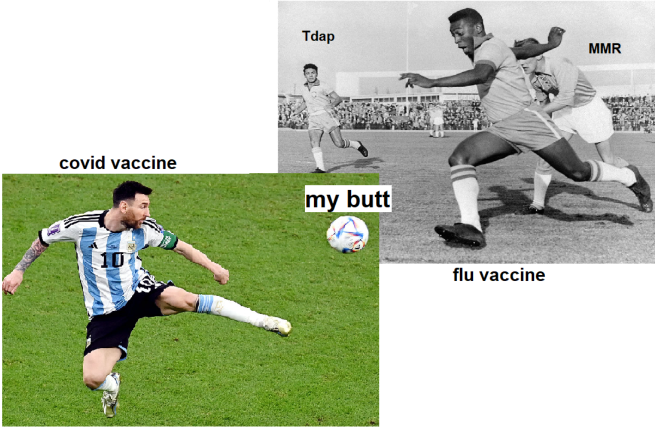
Advertisement

Directed Reading Program (DRP)

DRP is a program pairing undergraduates and graduate students to learn topics in math you will not find in standard classes. It is a way to get deeper into math studies in a fun and low-pressure setting. DRP can also serve as an initial step towards research, graduate school, and beyond! The program will start this fall and continue through the winter quarter. Mentors and mentees will generally have weekly meetings during the quarter. No prerequisites or background required.

Check out our website for more information and to sign up for the program by **Tuesday October 3** (`https://www.math.ucdavis.edu/~lstarkston/drp/`).

I'm dual-wielding vaccines today, and I'm pretty tired.



Recall from last time

Definition

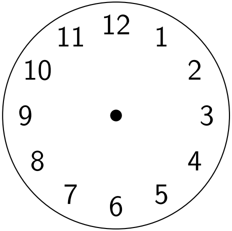
A **group** is a set G together with a law of composition $\circ$ that has the following properties:

- $\circ$ is associative: $(a \circ b) \circ c = a \circ (b \circ c)$ for all $a, b, c \in G$.
- G contains an identity element e such that $e \circ a = a$ and $a \circ e = a$ for all $a \in G$.
- Every element $a \in G$ has an inverse, i.e. an element b such that $a \circ b = e$ and $b \circ a = e$.

Example: $(\mathbb{Z}, +)$

- $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$
- $0 + n = n + 0 = n$
- $n + (-n) = (-n) + n = 0$

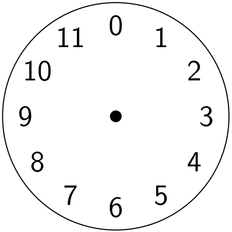
Another example: $(\mathbb{Z}/12\mathbb{Z}, +)$



- What does $+$ mean here?
- What are the elements, and what's the identity element?
- What is the inverse of 3?

- The notation $\mathbb{Z}/12\mathbb{Z}$ will make more sense later, when we talk about *cosets*.
- We usually write 0 instead of 12.

Cyclic groups



Definition

A group G is **cyclic** if it is *generated* by a single element,
i.e. there exists an element $\rho \in G$ such that every $g \in G$ is of the form $g = \rho^k$ for some $k \in \mathbb{Z}$.

Generators and Relations for $\mathbb{Z}/12\mathbb{Z}$

$\mathbb{Z}/12\mathbb{Z}$ is the “biggest” group generated by a single element ρ, subject to the relation $\rho^{12} = e$:

$$\mathbb{Z}/12\mathbb{Z} \cong \langle \rho \mid \rho^{12} = e \rangle.$$

(Generators and relations will be discussed more carefully after we learn about *normal subgroups*.)

Permutations

Definition

Let S be a set.
A **permutation** of S is a bijective map

$$p : S \to S.$$

Example

Let $[5] = \{1, 2, 3, 4, 5\}$.
Here is an example of a permutation p of [5]:

i	1	2	3	4	5
p(i)	3	5	4	1	2

Permutations

i	1	2	3	4	5
p(i)	3	5	4	1	2

Notation

For any $n \in \mathbb{N}$, let $[n]$ denote the set $\{1, 2, \ldots, n\}$.

Definition

The group of *all* permutations of $[n]$ is called the **symmetric group** and is denoted S_n.

Do not confuse this with *permutation groups*, which are *subgroups* of symmetric groups.

i	1	2	3	4	5
p(i)	3	5	4	1	2

Question

Consider our permutation $p \in S_5$ above.

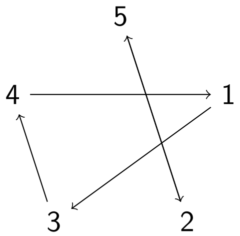
How does the permutation p^2 act on [5]?

Recall that $p^2 = p \circ p$. Write down a similar chart.

As always, discuss your answer with your classmates.

Cycle notation is an easier way to describe a permutation:

i	1	2	3	4	5
p(i)	3	5	4	1	2



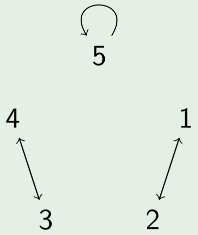
Cycle notation for p

$$p = (3\ 4\ 1)(2\ 5) = (1\ 3\ 4)(2\ 5) = (2\ 5)(1\ 3\ 4)$$

Cycle notation

Example

The cycle notation for the permutation $q \in S_5$



is $\mathbf{(1\ 2)(3\ 4)(5)}$.

We can also just write $q = (\mathbf{1}\ \mathbf{2})(\mathbf{3}\ \mathbf{4})$ if it's clear we're talking about an element of S_5.

$$p = (3\ 4\ 1)(2\ 5) \qquad q = (1\ 2)(3\ 4)$$

Practice

1. Write down p^2, p^3, and p^4 in cycle notation.
2. Write down qp and pq in cycle notation.

(Remember, qp means $q \circ p$.)

As always, discuss your answer with your classmates.

Permutation Matrices

We can represent permutations using *permutation matrices*.

Key idea: $[n] \cong \{e_1, e_2, \ldots, e_n\}$.

Example (cf. HW01)

Let $\sigma = (1\ 3\ 2) \in S_3$. We can represent σ as the linear transformation that sends each $e_i \mapsto e_{\sigma(i)}$:

$$\sigma \mapsto \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

You will study S_4 on HW01.

A set of generators for S_n

A standard deck of cards contains 52 cards (no jokers). A random $g \in S_{52}$ gives a permutation of the cards, i.e. one possible result from shuffling the cards.

A really slow way to shuffle cards is to do the following:

1. Pick a random pair of adjacent cards.
2. Swap them.
3. Repeat.

Transpositions generate S_n

A **transposition** is a permutation that swaps two adjacent indices:

$$\tau_i = (i \quad i+1) \qquad \text{for} \qquad 1 \leq i \leq n-1.$$

A set of generators for S_n

Transpositions generate S_n

A **transposition** is a permutation that swaps two adjacent indices:

$$\tau_i = (i \quad i+1) \qquad \text{for} \qquad 1 \leq i \leq n-1.$$

Example

How can we write $p = (3\ 4\ 1)(2\ 5)$ as a composition of transpositions?