AMP-Algebra
Lecture 5

Permutation (Symmetric) Groups.

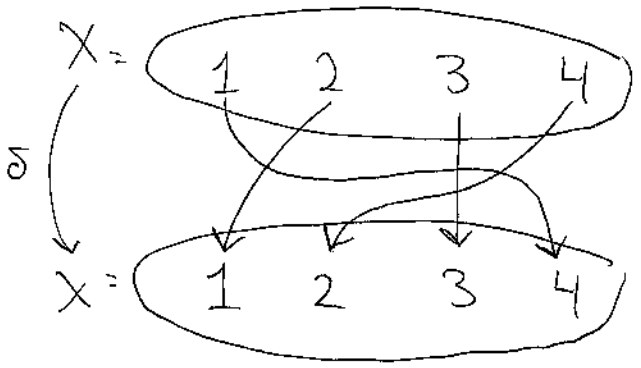
So we've already talked about a bunch of examples of groups last week. $\langle \mathbb{Z}, + \rangle$, $\langle \mathbb{Q}^\times, \cdot \rangle$ with $\cdot$, all the groups of order up to 7, the finite cyclic groups $\mathbb{Z}_n$, the dihedral groups, the Rubik's cube group. Today we're going to talk about another important example of groups, called the symmetric groups.

To build such a group, we'll start with an example. Remember a permutation of a set X is a "rearrangement" of the order of the elements in that set. You can equivalently think of a permutation σ as a bijective function $X \xrightarrow{\sigma} X$.

"Sigma"

τ is "tau"

For example, say $X = \{1, 2, 3, 4\}$. A permutation σ of X might look like



OR $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$

The notation on the right is nice and sparse, and we'll use it until we invent a better notation later.

So a permutation is a bijection from a set X to itself. We did an exercise involving this $\ddot{\smile}$.

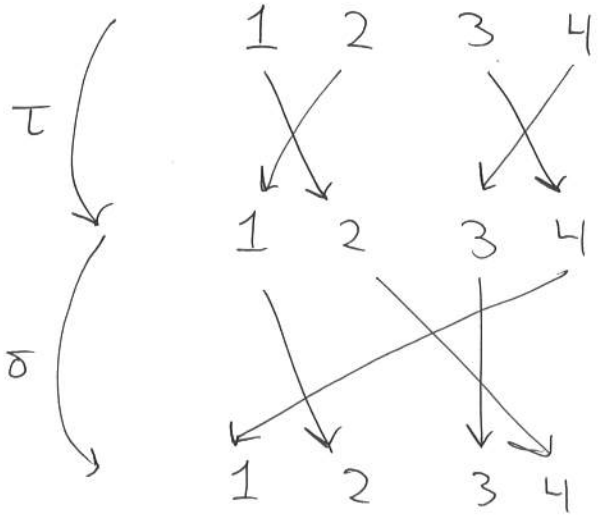
Recall that ~~a composite~~ if you have two bijective functions $\sigma: X \to X$ and $\tau: X \to X$, then their composite will also be a bijection $\sigma \circ \tau: X \to X$. This suggests we could use this as a binary operation on the set of all such permutations...

... but let's do an example first before we formalize things. Let σ and τ be permutations of the set $\{1,2,3,4\}$ given by

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

Since these are functions, we'll write them down in the usual order that we compose functions. So $\sigma \circ \tau = \sigma\tau$ means "do tau first, then do sigma."

Let's write down $\sigma \circ \tau$.



so $\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$

Practice: Write down $\tau \circ \sigma$.

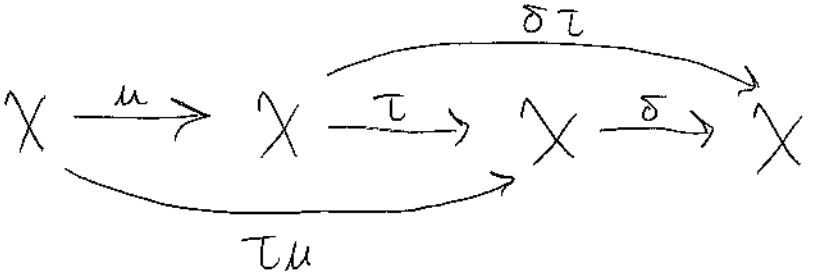
You'll notice that $\sigma\tau \neq \tau\sigma$. This means that this operation of composing permutations is not commutative. But these permutations can form a group. Let S_n denote the set of all permutations of a set with n elements (so like $\{1, 2, \ldots, n\}$).

THEOREM — The set S_n is a group under the operation of function composition, and is called the symmetric group on n letters.

Proof Remember that to prove something is a group we're gotta check three things:

- Is the operation associative?
- Does the set contain an identity element with respect to the operation?
- Does every element of the set have an inverse element in the set with respect to the operation?

First, associativity. Suppose you have three permutations of a finite set X named σ, τ, and μ.



I hope it's clear that $\sigma(\tau\mu) = (\sigma\tau)\mu$. I.e. that writing down $\sigma\tau\mu$ is NOT ambiguous. To prove this symbolically, take $x \in X$ and note that

$$(\sigma(\tau\mu))(x) = \sigma((\tau\mu)(x)) = \sigma(\tau(\mu(x))) = \cdots$$

$$\cdots = (\sigma\tau)(\mu(x)) = ((\sigma\tau)\mu)(x) \quad \checkmark$$

The identity permutation is the permutation that "does nothing." It must leave everything fixed. So it's just the identetity function.

$$e = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}. \quad \checkmark$$

Finally, for any permutation δ, can we find its inverse δ^{-1} that takes the set "back to e"? Yes! The permutation δ is a bijective function, so it has an inverse function σ^{-1}. ✓ □

The proof is done, but just as an illustrative example of the inverse of a permutation, consider:

$$\delta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$$

The inverse σ^{-1} will be the permutation that sends 2 back to 1, 4 back to 2, 3 to 3, and 1 back to 4.

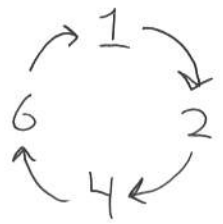
$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}.$$

Break for practice and rest.

Let's introduce another notation for permutations that helps us study and describe the symmetric group. We won't get too far into it, but it'll help to see it briefly now.

For a set $X = \{1, 2, \ldots, n\}$, a <u>cyclic</u> permutation of X takes some subset of X and permutes that subset in a cyclic fashion. For example

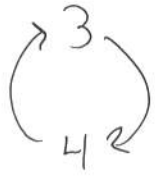
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 6 & 5 & 1 \end{pmatrix} \in S_6$$



$(1\ 2\ 4\ 6)$

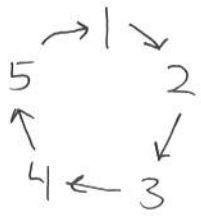
is a cyclic permutation. These are cyclic permutations too

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} \in S_4$$



$(3\ 4)$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} \in S_5$$

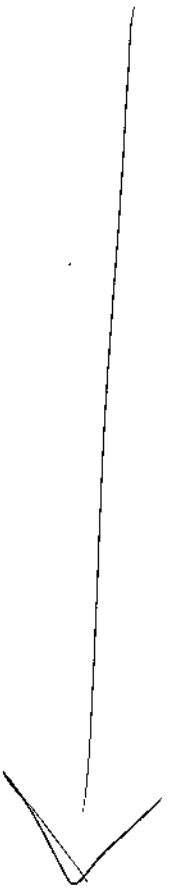


$(1\ 2\ 3\ 4\ 5)$

For cyclic permutations, we can denote them with a more terse notation as written in blue on the previous page.

PROPOSITION – Every permutation can be written as a product of cyclic permutations.

We won't prove this, but hopefully an example will help you see that it's true.



Define a cycle first!

For example let

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 2 & 4 & 3 & 1 \end{pmatrix}.$$

and look at what τ does to 2 upon repeated application

$$2 \xrightarrow{\tau} \tau(2) \xrightarrow{\tau} \tau(\tau(2)) \xrightarrow{\tau} \cdots$$

$$2 \xrightarrow{\tau} 5 \xrightarrow{\tau} 3 \xrightarrow{\tau} 2$$

Because our set, $\{1, 2, 3, 4, 5, 6\}$ is finite, we must eventually get back where we started. This completes a cycle α that is a factor of τ. We want to introduce more natural notation for this cycle, so we'll use $\alpha = (2\ 5\ 3)$.

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 2 & 4 & 3 & 6 \end{pmatrix}$$

But α doesn't touch the other numbers 1, 4, or 6. Looking back at τ and seeing what τ does to 1, we get another cyclic factor of τ, $\beta = (1\ 6)$.

Then 4 remains fixed under τ, so the cycle it generates is only (4), which as a factor of τ is the identity map. So we have

Disjoint on letters so they commute!

$$\tau = \alpha\beta \quad (= \beta\alpha)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 2 & 4 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 2 & 4 & 3 & 6 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 2 & 3 & 4 & 5 & 1 \end{pmatrix}$$

$$\tau = (2\,5\,3)(1\,6).$$

This is, at least, more convenient to write a permutation this way. And in fact, via the process we followed in the example, every permutation can be written as a product of ~~these transpositions~~ disjoint cycles this way.