Math 113 Supplement on Permutation Groups

1 A brief history

As early as 200BC, mathematicians have studied structures that we now call groups: structures, symmetries, numbers, permutations and more. But it was not until the mid-1800s that someone noticed that collections of symmetries, of numbers and of other operations have something in common and gave that something a name. This was British mathematician Arthur Cayley (1821-1895), the first to write down something that looks like our modern definition of a "group"[1].

Cayley's observation did not come out of nowhere. A whole family of mathematicians were working on problems involving groups – although mostly groups of permutations – and moving towards higher and higher degrees of abstraction. French mathematician Évariste Galois (1811-1832)[2] was the first to use the word "group" (groupe in French) to describe a group of permutations. Other major contributors were Augustin-Louis Cauchy, C. F. Gauss, and Felix Klein, who worked on groups of symmetries. And once the notion of "group" had been defined, there was an explosion of interest in creating a unified theory and extending the concept to cover broader and broader areas of mathematics.

The symmetric groups S_n (recall that S_n is the group of permutations of n objects) are particularly important. Historically, they were the objects of study that inspired the modern definition of a group. And as we saw in class, every finite group can be thought of as a kind of a permutation group. (Precisely, for any finite group, there is at least one subgroup of some symmetric group S_n that is structurally the same as the finite group.) So understanding symmetric groups is one way to get at an understanding of all finite groups.

2 More on the mathematics of permutation groups *a.k.a* Course Notes Section 12b

Our treatment of groups of permutations is a little different than that in the official course notes. What follows is a summary of what we did beyond what is covered in the book, for your reference. You should read and understand sections 12.1 and 12.2 in the book before working through the content here. Section 12.3 in the book is optional and won't be covered in class or on the midterm.

Let's start with the theorem we mentioned in the history above: that all groups can be understood as groups of permutations. This theorem was discovered and proved by Cayley, the mathematician who first defined group.

[1] Pop quiz: the definition is...

[2] You'll notice that Galois died at the age of 20. He was fighting a duel and lost. The man led a somewhat colorful life and produced a remarkable amount of mathematics in a remarkably short time, pioneering what is now called Galois theory.

2.1 Writing groups using permutations

Theorem 2.1 (Cayley)**.** Any finite group is structurally the same as a subgroup of some permutation group.

As we did in class, we will not give a complete proof of this theorem, but we will explain *how* to make a group of permutations that corresponds to a given finite group. We leave it to you to check some examples for verification and ponder *why* this method works.

Here is how to do it. Start with the multiplication table for your group. For example:

×	I	A	B	C	D	E
I	I	A	B	C	D	E
A	A	B	I	E	C	D
B	B	I	A	D	E	C
C	C	D	E	I	B	A
D	D	E	C	A	I	B
E	E	C	D	B	A	I

Remember that our convention for the multiplication table says that you the *column* first and then the *row*. Next, assign a number to each element of your group, and write this down in the table. If we do $I \leftrightarrow 1$, $A \leftrightarrow 2$, etc, we get:

×	I	A	B	C	D	E
I	I_1	A_2	B_3	C_4	D_5	E_6
A	A_2	B_3	I_1	E_6	C_4	D_5
B	B_3	I_1	A_2	D_5	E_6	C_4
C	C_4	D_5	E_6	I_1	B_3	A_2
D	D_5	E_6	C_3	A_2	I_1	B_3
E	E_6	C_4	D_5	B_3	A_2	I_1

Finally, to figure out what permutation goes with which element, read the row of numbers across and write this below 1 2 3 4 5 6. In our example, we find that:

I corresponds to $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$

A corresponds to $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 6 & 4 & 5 \end{pmatrix}$

B corresponds to $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 5 & 6 & 4 \end{pmatrix}$ and so on.

If we do the permutation BA (first A, then B), we get the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$.

That's I, which is BA in the multiplication table for the group. So our correspondence works out – when you multiply two elements and then take the corresponding permutation, that's the same thing as "multiplying" the two corresponding permutations.

Practice Problem 12b.0 What are the permutations corresponding to C, D and E? Check that the permutations corresponding to C and A multiply together (in the right order, as CA) to give the permutation corresponding to E.

Question 2.2. Why does this always work out? Can you think of a reason?

NOTE: this scheme will only work if you make multiplication go column first and then row! (otherwise I think we'd have to read the columns going down, instead of the rows going across to get the numbers we need to use in our permutations)

Practice Problem 12b.1 Follow the procedure above for the group with four elements with the multiplication table given at the bottom of page 272 in the course notes. You will get a subgroup of S_4 that is structurally the same as that group. Check that multiplication works on at least two different examples of elements (e.g. since $HR^2 = V$, check that if you do the permutation corresponding to R^2 followed by the one corresponding to H, then you get the permutation corresponding to V. Then choose two other elements).

2.2 Generators for S_n

A special kind of permutation is a *transposition*. This is the result of switching two adjacent numbers and doing nothing else. We write it down by writing down the two numbers. For example,

$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 4 & 3 & 5 & 6 \end{pmatrix}$ is a transposition and we call it (34)

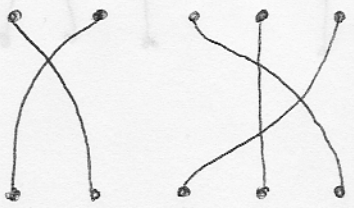
Practice Problem 12b.2 Prove that there are exactly $n-1$ transpositions in S_n

We will show that *any* permutation can be made by putting together a bunch of permutations. One way to think about this is as follows: suppose that you have a line-up of heavy objects that you want to rearrange in a different order. In fact, they are so heavy that you can only move an object past *one* other before you have to put it down and rest for a moment before picking it up again or moving anything else. In other words, you can only do one transposition at a time. Provided that you are allowed to take as many breaks as you want, is it possible to put the objects into any order you want? Sure – this is one case where patience is all you need!

Practice Problem 12b.3 Convince yourself that you really can rearrange the objects using this strategy

Another way to show this is by drawing permutations as *braids*.

Definition 2.3. A braid with n strands is a diagram with n dots in a top row, n dots in a bottom row, and a line (called a *strand*) connecting each top dot to a single bottom dot. Here is an example with 5 strands:

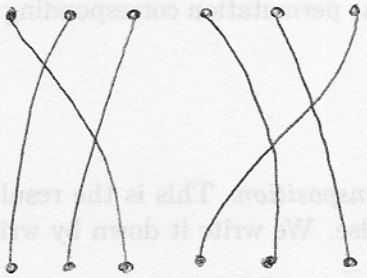


You could make a physical model of a braid out of strings.

A braid is a way of writing down a permutation. Remember, our notation

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

tells you how to do a rearrangement by saying "1 goes to the third position", "2 goes to the first position", etc. Now we'll say "1 goes to the third position" instead by drawing a strand from the 1st dot at the top to the third dot at the bottom. Similarly, "2 goes to the first position" is indicated by a strand connecting the 2nd dot at the top to the first dot at the bottom. Thus, the permutation written down above gives this braid:



You can also go backwards: if you have a picture of a braid, just follow the strings down to see what permutation it corresponds to. If the string from the first dot at the top goes to the 5th dot at the bottom, you should write a 5 underneath the 1.

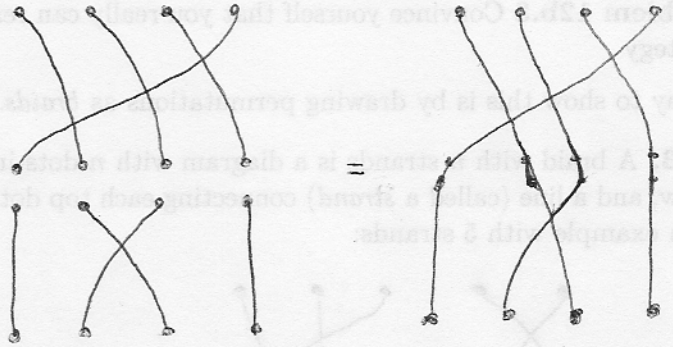
Problem 2.4 (Practice Problem 12b.4). What permutation is represented by the braid on 5 strands in the example right below Definition 2.3?

You can simulate doing one permutation followed by another by drawing the braid for one permutation right underneath the braid for the other.

For example:

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

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



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

Practice Problem 12b.5 Why does this method work to show you what happens when you do one permutation after the other?

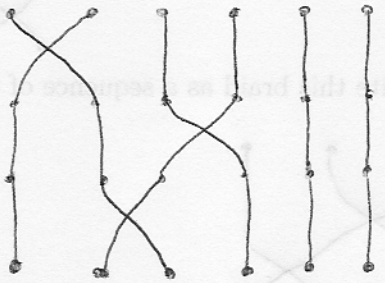
With braids, a transposition is just an instruction to cross one strand over an adjacent one:

(23) =

So to write a permutation as a sequence of transpositions, we need to give instructions for crossing neighboring strands one at a time. If you had physical strings, this is exactly what you would do to make the "braid": pick up two side by side strands, one strand in each hand, and cross them. Then pick up another pair of side by side strands and cross them.

this is the same as (34)

Here is the result of doing (12) then (43) and then (32) to a braid with 6 strands:

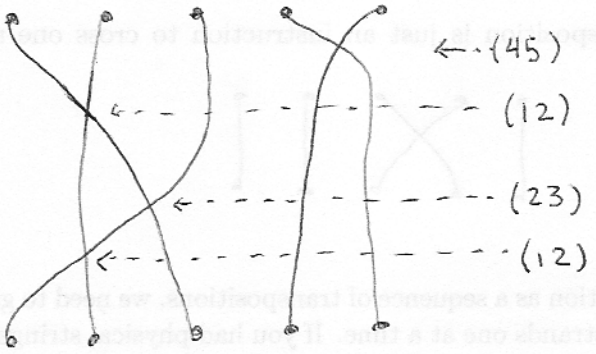


We see that we get the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 2 & 5 & 6 \end{pmatrix}$, which is exactly what we get if we multiply the three transpositions

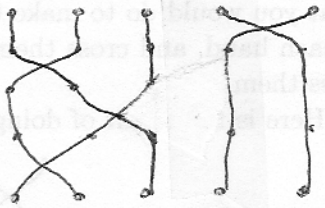
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 4 & 5 & 6 \end{pmatrix}$$
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 4 & 3 & 5 & 6 \end{pmatrix}$$
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 2 & 4 & 5 & 6 \end{pmatrix}$$

using the old method.

If you have a picture of a braid, you can also go backwards and see what transpositions make it up, by reading the string-crossings from top to bottom. Here is an example.



A nicer picture:



Practice Problem 12b.6 Write this braid as a sequence of transpositions: