Math 417 – Eighth Day

Bruce Reznick
University of Illinois at Urbana-Champaign

September 11, 2020

We're first going to talk about the general symmetric group S_n and then go back to a much more detailed examination of S_3.

Okay. I have to start with an embarrassing confession.

I gave you the multiplication of permutations as I was taught it and I told you that there are books in which it can go in different directions.

Well, I looked up *Fraleigh*, and **he does it the other way**, and I'm going to follow him. So I'm going to redo the examples from yesterday. I think it's less confusing for me to fix about 30 minutes of class than for you to have to correct the book every time you read it.

Definition. Fix an integer $n \geq 2$ and consider permutations of $\{1, \ldots, n\}$.

We write S_n for the set of permutations of $\{1, \ldots, n\}$ with the operation $\circ$ as defined so that, if $\sigma, \pi \in S_n$, then $\sigma \circ \pi$ operates right to left, with $i \mapsto \pi(i) \mapsto \sigma(\pi(i))$: $(S_n, \circ)$ is called the *n-th symmetric group* or *the symmetric group on n letters*.

In other words, it is consistent with functional notation, but you do the second permutation first and then apply the first permutation.

First, from Tuesday night, recall

$$\sigma = \begin{pmatrix} 12345 \\ 32514 \end{pmatrix}, \qquad \rho = \begin{pmatrix} 12345 \\ 43512 \end{pmatrix};$$

we define $(\sigma \circ \rho)(i) = \sigma(\rho(i))$ so

$$\begin{aligned}
\rho(1) = 4 \quad \sigma(4) = 1 &\implies (\sigma \circ \rho)(1) = 1, \quad 1 \mapsto 4 \mapsto 1; \\
\rho(2) = 3 \quad \sigma(3) = 5 &\implies (\sigma \circ \rho)(2) = 5, \quad 2 \mapsto 3 \mapsto 5; \\
\rho(3) = 5 \quad \sigma(5) = 4 &\implies (\sigma \circ \rho)(3) = 4, \quad 3 \mapsto 5 \mapsto 4; \\
\rho(4) = 1 \quad \sigma(1) = 3 &\implies (\sigma \circ \rho)(4) = 3, \quad 4 \mapsto 1 \mapsto 3; \\
\rho(5) = 2 \quad \sigma(2) = 2 &\implies (\sigma \circ \rho)(5) = 2, \quad 5 \mapsto 2 \mapsto 2;
\end{aligned}$$

$$\implies \sigma \circ \rho = \begin{pmatrix} 12345 \\ 15432 \end{pmatrix} = (1)(25)(34),$$

Similarly, $(\rho \circ \sigma)(i) = \rho(\sigma(i))$ so

$$\begin{aligned}
\sigma(1) = 3 \quad \rho(3) = 5 &\implies (\rho \circ \sigma)(1) = 5, \quad 1 \mapsto 3 \mapsto 5;\\
\sigma(2) = 2 \quad \rho(2) = 3 &\implies (\rho \circ \sigma)(2) = 3, \quad 2 \mapsto 2 \mapsto 3;\\
\sigma(3) = 5 \quad \rho(5) = 2 &\implies (\rho \circ \sigma)(3) = 2, \quad 3 \mapsto 5 \mapsto 2;\\
\sigma(4) = 1 \quad \rho(1) = 4 &\implies (\rho \circ \sigma)(4) = 4, \quad 4 \mapsto 1 \mapsto 4;\\
\sigma(5) = 4 \quad \rho(4) = 1 &\implies (\rho \circ \sigma)(5) = 1, \quad 5 \mapsto 4 \mapsto 1;
\end{aligned}$$

$$\implies \rho \circ \sigma = \binom{12345}{53241} = (15)(23)(4)$$

These are just the reverses of what we had earlier.

And we did this in class on Wednesday.

$$\mu_1 = \binom{123}{132} = (1)(23), \qquad \mu_2 = \binom{123}{321} = (13)(2),$$

Thinking about these as functions, and $(\mu_1 \circ \mu_2)(i) = \mu_1(\mu_2(i))$, so we do μ_2 first:

$$(\mu_1 \circ \mu_2)(1) = \mu_1(\mu_2(1)) = \mu_1(3) = 2$$
$$(\mu_1 \circ \mu_2)(2) = \mu_1(\mu_2(2)) = \mu_1(2) = 3$$
$$(\mu_1 \circ \mu_2)(3) = \mu_1(\mu_2(3)) = \mu_1(1) = 1$$
$$\implies \mu_1 \circ \mu_2 = \binom{123}{231} = \rho_1$$

Similarly,

$$(\mu_2 \circ \mu_1)(1) = \mu_2(\mu_1(1)) = \mu_2(1) = 3$$
$$(\mu_2 \circ \mu_1)(2) = \mu_2(\mu_1(2)) = \mu_2(3) = 1$$
$$(\mu_2 \circ \mu_1)(3) = \mu_2(\mu_1(3)) = \mu_2(2) = 2$$
$$\implies \mu_1 \circ \mu_2 = \binom{123}{312} = \rho_2$$

So the product of each flip is a rotation, but they are different rotations: $\mu_1 \circ \mu_2 \neq \mu_2 \circ \mu_1$.

And from the worksheet

$$\rho_2 = \begin{pmatrix} 123 \\ 312 \end{pmatrix} = (132), \qquad \mu_2 = \begin{pmatrix} 123 \\ 321 \end{pmatrix} = (13)(2)$$

So $\mu_2 \circ \rho_2$ takes $1 \mapsto 3 \mapsto 1$, $2 \mapsto 1 \mapsto 3$ and $3 \mapsto 2 \mapsto 2$ and

$$\mu_2 \circ \rho_2 = \begin{pmatrix} 123 \\ 132 \end{pmatrix} = (1)(23) = \mu_1$$

Similarly, $\rho_2 \circ \mu_2$ takes $1 \mapsto 3 \mapsto 2$, $2 \mapsto 2 \mapsto 1$ and $3 \mapsto 1 \mapsto 3$ and

$$\rho_2 \circ \mu_2 = \begin{pmatrix} 123 \\ 213 \end{pmatrix} = (12)(3) = \mu_3$$

I owe you a fresh example. Suppose $n = 4$ and

$$\sigma(1) = 2, \sigma(2) = 4, \sigma(3) = 1, \sigma(4) = 3;\ \sigma = \binom{1234}{2413} = (1243),$$

$$\pi(1) = 4, \pi(2) = 1, \pi(3) = 3, \pi(4) = 2;\ \pi = \binom{1234}{4132} = (142)(3).$$

Then

$$\begin{aligned}
\sigma(1) = 2 \quad \pi(2) = 1 &\implies (\pi \circ \sigma)(1) = 1, \quad 1 \mapsto 2 \mapsto 1;\\
\sigma(2) = 4 \quad \pi(4) = 2 &\implies (\pi \circ \sigma)(2) = 2, \quad 2 \mapsto 4 \mapsto 2;\\
\sigma(3) = 1 \quad \pi(1) = 4 &\implies (\pi \circ \sigma)(3) = 4, \quad 3 \mapsto 1 \mapsto 4;\\
\sigma(4) = 3 \quad \pi(3) = 3 &\implies (\pi \circ \sigma)(4) = 3, \quad 4 \mapsto 3 \mapsto 3;
\end{aligned}$$

$$\implies$$

$$\pi \circ \sigma = \binom{1234}{1243} = (1)(2)(34).$$

THEOREM: The symmetric group S_n is a group of order $n!$.

PROOF: First, how many elements are there in S_n? There are n choices for $\sigma(1)$, and we know that there are $n-1$ choices for $\sigma(2)$ (because it can't equal $\sigma(1)$) and then $n-2$ choices for $\sigma(3)$ (because it can't equal $\sigma(1)$ or $\sigma(2)$), etc., so altogether, there are $n \cdot (n-1) \cdot (n-2) \cdots = n!$ possible permutations, and $|S_n| = n!$.

First we need an identity element. Let e be defined so that $e(j) = j$ for all j; that is, $e = \begin{pmatrix} 12 \dots n \\ 12 \dots n \end{pmatrix} = (1)(2)\cdots(n)$. Then it should be clear that for every $\sigma \in S_n$, $\sigma \circ e = e \circ \sigma = \sigma$.

Next we need inverses, and here we use functional inverses. For $\sigma \in S_n$, define ρ by $\sigma(i) = j \implies \rho(j) = i$, that is, $\rho(j) = \sigma^{-1}(j)$ *as a function*. Then $\sigma \circ \rho$ takes $j \mapsto i \mapsto j$, and similarly for $\rho \circ \sigma$. That is, $\sigma \circ \rho = \rho \circ \sigma = e$, and so $\rho = \sigma^{-1}$.

The last thing we have to check is associativity, and this is ugly. We need to show that

$$(\sigma_1 \circ \sigma_2) \circ \sigma_3 = \sigma_1 \circ (\sigma_2 \circ \sigma_3).$$

Let's work through the definition. For $i \in \{1, \dots, n\}$,

$$((\sigma_1 \circ \sigma_2) \circ \sigma_3)(i) = (\sigma_1 \circ \sigma_2)(\sigma_3(i)) = \sigma_1(\sigma_2(\sigma_3(i)))$$
$$(\sigma_1 \circ ((\sigma_2 \circ \sigma_3))(i) = \sigma_1((\sigma_2 \circ \sigma_3)(i)) = \sigma_1(\sigma_2(\sigma_3(i))),$$

so they're equal, because taking functions is associative. Yes, this is tedious, but we only have to do this once, and now we can say we have a group. □

A bit about how to find inverses in practice. Let's recall σ:

$$\sigma(1) = 2,\ \sigma(2) = 4,\ \sigma(3) = 1,\ \sigma(4) = 3;\ \sigma = \binom{1234}{2413} = (1243).$$

If as a function, $\rho = \sigma^{-1}$, then we can just reverse this:

$$\rho(2) = 1,\ \rho(4) = 2,\ \rho(1) = 3,\ \rho(3) = 4;\ \Longleftrightarrow$$
$$\rho(1) = 3,\ \rho(2) = 1,\ \rho(3) = 4,\ \rho(4) = 2,$$

or take the matrix for σ, flip it over and then rearrange columns:

$$\rho = \binom{2413}{1234} = \binom{1234}{3142}$$

Or take the cycles and just run them in reverse. If, previously, under a permutation, we had $a_1 \to a_2 \cdots \to a_n \to a_1$, then in the inverse we have $a_1 \leftarrow a_2 \cdots \leftarrow a_n \leftarrow a_1$, so (1243) becomes (3421) or (1342).

It's also worth mentioning that $S_1 = \{(1)\}$ is just the trivial group and $S_2 = \{(1)(2), (12)\}$ is a cyclic group of order 2. We're about to spend a lot of time with S_3. There is something we can say generally about symmetric groups.

THEOREM If $n \geq 3$, then S_n is not abelian.

PROOF All we need to show is that there are always $\alpha, \beta \in S_n$ so that $\alpha \circ \beta \neq \beta \circ \alpha$. Consider these two transpositions:

$$\alpha(1) = 2, \alpha(2) = 1; k \in \{3, 4, \dots, n\} \implies \alpha(k) = k,$$
$$\beta(1) = 3, \beta(3) = 1; k \in \{2, 4, \dots, n\} \implies \beta(k) = k,$$

In other words, $\alpha = (12)$ switches $\{1, 2\}$ and leaves everything else alone and $\beta = (13)$ switches $\{1, 3\}$ and leaves everything else alone. These are both elements of S_n for $n \geq 3$.

Let's look at $\alpha \circ \beta$ and $\beta \circ \alpha$. I should look at 1, 2, 3 and $k \geq 4$ separately when we compute $\alpha(\beta(i))$ and $\beta(\alpha(i))$:

$$\begin{aligned}
\beta(1) = 3 \quad \alpha(3) = 3 &\implies (\alpha \circ \beta)(1) = 3, \quad 1 \mapsto 3 \mapsto 3; \\
\beta(2) = 2 \quad \alpha(2) = 1 &\implies (\alpha \circ \beta)(2) = 1, \quad 2 \mapsto 2 \mapsto 1; \\
\beta(3) = 1 \quad \alpha(1) = 2 &\implies (\alpha \circ \beta)(3) = 2, \quad 3 \mapsto 1 \mapsto 2; \\
\beta(k) = k \quad \alpha(k) = k &\implies (\alpha \circ \beta)(k) = 3, \quad k \mapsto k \mapsto k; \\
&\implies \alpha \circ \beta = (132)(4) \cdots (n).
\end{aligned}$$

$$
\begin{array}{llll}
\alpha(1) = 2 & \beta(2) = 2 \implies & (\beta \circ \alpha)(1) = 2, & 1 \mapsto 2 \mapsto 2; \\
\alpha(2) = 1 & \beta(1) = 3 \implies & (\beta \circ \alpha)(2) = 3, & 2 \mapsto 1 \mapsto 3; \\
\alpha(3) = 3 & \beta(3) = 1 \implies & (\beta \circ \alpha)(3) = 1, & 3 \mapsto 3 \mapsto 1; \\
\alpha(k) = k & \beta(k) = k \implies & (\beta \circ \alpha)(k) = 3, & k \mapsto k \mapsto k;
\end{array}
$$

$$\implies \beta \circ \alpha = (123)(4) \cdots (n).$$

The two calculations is very similar, but notice that $\beta \circ \alpha$ is like $\alpha \circ \beta$ if we just switched the 2 and the 3.

Since $(132) \ne (123)$, it follows that $(12) \circ (13) \ne (13) \circ (12)$ and S_n is not abelian. □

The argument generalizes. Suppose i, j, k are different elements of $\{1, 2, \ldots, n\}$. Then $(ij) \circ (ik) = (ikj)$.

Let's review what we've seen of S_3:

$$\rho_0 = \begin{pmatrix} 123 \\ 123 \end{pmatrix} = (1)(2)(3), \quad \rho_1 = \begin{pmatrix} 123 \\ 231 \end{pmatrix} = (123),$$
$$\rho_2 = \begin{pmatrix} 123 \\ 321 \end{pmatrix} = (132), \quad \mu_1 = \begin{pmatrix} 123 \\ 132 \end{pmatrix} = (1)(23),$$
$$\mu_2 = \begin{pmatrix} 123 \\ 321 \end{pmatrix} = (13)(2), \quad \mu_3 = \begin{pmatrix} 123 \\ 213 \end{pmatrix} = (12)(3).$$

We also know that ρ_0 is the identity element, $\{\rho_0, \rho_1, \rho_2\}$ form a cyclic group of order 3 and $\mu_j^2 = \rho_0$ for $j = 1, 2, 3$.

We've argued by looking at whether the triangle is flipped, we've seen that $\rho_i \circ \rho_j$ will be some ρ_k and $\rho_i \circ \mu_j$ or $\mu_i \circ \rho_j$ will be some μ_k. Unless we know the answer, the subscript is mysterious. This is enough to fill in 18 of the 36 places of the multiplication table.

S_3	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	$\mu_?$	$\mu_?$	$\mu_?$
ρ_2	ρ_2	ρ_0	ρ_1	$\mu_?$	$\mu_?$	$\mu_?$
μ_1	μ_1	$\mu_?$	$\mu_?$	ρ_0	$\rho_?$	$\rho_?$
μ_2	μ_2	$\mu_?$	$\mu_?$	$\rho_?$	ρ_0	$\rho_?$
μ_3	μ_3	$\mu_?$	$\mu_?$	$\rho_?$	$\rho_?$	ρ_0

We know a few more things that have been worked out in class yesterday, and corrected today. For example, we showed that $\mu_1 \circ \mu_2 = \rho_1$ and $\mu_2 \circ \mu_1 = \rho_2$, and from the worksheet $\rho_2 \circ \mu_2 = \mu_3$ and $\mu_2 \circ \rho_2 = \mu_1$. Let's put these in (in red for the lecture, though it won't show up in the end of the week document.)

S_3	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	$\mu_?$	$\mu_?$	$\mu_?$
ρ_2	ρ_2	ρ_0	ρ_1	$\mu_?$	μ_3	$\mu_?$
μ_1	μ_1	$\mu_?$	$\mu_?$	ρ_0	ρ_1	$\rho_?$
μ_2	μ_2	$\mu_?$	μ_1	ρ_2	ρ_0	$\rho_?$
μ_3	μ_3	$\mu_?$	$\mu_?$	$\rho_?$	$\rho_?$	ρ_0

There are still 14 question marks, but I claim that we are actually done, provided we remember the rules that elements in all rows and columns have to be different.

Let's look at $\rho_2 \circ \mu_1$.

It can't be ρ_2, ρ_0, ρ_1 or μ_3, because they already appear in the row, and it can't be μ_1, because it's already in the column, so *without any calculation!* we know that $\rho_2 \circ \mu_1 = \mu_2$ – it's the only choice left.

S_3	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	$\mu_?$	$\mu_?$	$\mu_?$
ρ_2	ρ_2	ρ_0	ρ_1	μ_2	μ_3	$\mu_?$
μ_1	μ_1	$\mu_?$	$\mu_?$	ρ_0	ρ_1	$\rho_?$
μ_2	μ_2	$\mu_?$	μ_1	ρ_2	ρ_0	$\rho_?$
μ_3	μ_3	$\mu_?$	$\mu_?$	$\rho_?$	$\rho_?$	ρ_0

Looking at the same row now forces is to see that $\rho_2 \circ \mu_3 = \mu_1$, because it's the only element left!

S_3	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	$\mu_?$	$\mu_?$	$\mu_?$
ρ_2	ρ_2	ρ_0	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	$\mu_?$	$\mu_?$	ρ_0	ρ_1	$\rho_?$
μ_2	μ_2	$\mu_?$	μ_1	ρ_2	ρ_0	$\rho_?$
μ_3	μ_3	$\mu_?$	$\mu_?$	$\rho_?$	$\rho_?$	ρ_0

Since the columns are different, we can fill out the ρ_1 row, and this completes the $\rho \circ \mu$ block. Identical reasoning lets us fill out the $\mu \circ \rho$ block as well, leaving only $\mu \circ \mu$, which is by now really forced.

You might enjoy copying this table and trying to finish it on your own.

Maybe not.

Here's the full version; also on p.79 of the book.

S_3	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_3	μ_1	μ_2
ρ_2	ρ_2	ρ_0	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	ρ_0	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	ρ_0	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	ρ_0

As a check, let's do $\mu_3 \circ \rho_1$:

$$\mu_3 \circ \rho_1 = \begin{pmatrix} 123 \\ 213 \end{pmatrix} \circ \begin{pmatrix} 123 \\ 231 \end{pmatrix} \implies 1 \mapsto 2 \mapsto 1, \quad 2 \mapsto 3 \mapsto 3,$$

$$3 \mapsto 1 \mapsto 2, \implies \mu_3 \circ \rho_1 = \begin{pmatrix} 123 \\ 132 \end{pmatrix} = \mu_1.$$

It's *not* necessary to memorize the table! Just know the names of the elements of S_3 and how to multiply them.