PERMUTATION GROUPS

L. MARIZZA A BAILEY

1. Review

We have already learned that a permutation of a set, S, is a bijective function from S to itself.
How can we reconcile this definition with our preconceived notion of permutation?
We normally think of permutations as a rearrangement of the elements of a set.
How is this a bijective function?
Let us consider an example.
Suppose we would like to rearrange the elements in the set $\{1, 2, 3, 4, 5\}$.
Then we could send 1 to 2^{nd} place and 2 to 4^{th} place,

$$3 \to 5 \ , \ 5 \to 1 \text{ and } 4 \to 3$$

This could be modeled by the bijective function

$$f(1) = 2 \ , \ f(2) = 4 \ , \ f(3) = 5 \ , \ f(4) = 3 \ , \ f(5) = 1 \ .$$

We have learned previously that the set of all bijective functions from a set S to itself is a group under composition.
If the set, S, is finite of cardinality n, then we call the group of permutations of S, S_n.
Since a set of S of cardinality n is isomorphic to $\{1, 2, 3, 4, \ldots, n\}$ in the category of sets, we usually consider S_n to be the group of permutations on the set $\{1, 2, 3, 4, \ldots, n\}$.

2. Cycle Notation

A very common notation used for permutations is called cycle notation.
For example, the permutation above can be written as $f = (1\ 2\ 4\ 3\ 5)$.
We read this as 1 goes to 2, 2 goes to 4, 4 goes to 3, 3 goes to 5 and 5 goes back to 1.
One of the main reasons we would like to write permutations in cycle notation is for convenience.
If a point is fixed by a permutation, meaning $f(x) = x$, then we eliminate it from the notation.

Date: November 24, 2014.

Example 1. The permutation $\sigma = (13)(25)$ in S_5 is missing the number 4. This is because
$\sigma(1) = 3$
$\sigma(2) = 5$
$\sigma(3) = 1$
$\sigma(4) = 4$
$\sigma(5) = 2$
As you can see (13)(25) saves us a lot of writing.

Also note that it is convention that in each cycle we start with the smallest number. This allows us to identify which cycles are describing the same permutation immediately. If we wrote (31)(52), it would take us a second or two to realize that this permutation is the same as (13)(25).

Another very important reason, is that we can easily compose permutations which share a number that isn't fixed. Although we call composition of permutations when they are written in cycle notation *multiplication*, for simplicity, it is still composition. It is for this reason that I like to "multiply" permutations right to left.

Example 2. (132)(345)(4678)(245) can be simplified by the following algorithm
We start with 1. This makes it easier for us to start each cycle with the smallest number, following convention.
The only cycle that moves 1 is the left most cycle, so $1 \to 3$.
Next we see where 3 goes, so that we can continue the cycle.
3 appears in the second to left most cycle, and that cycle send $3 \to 4$.
Also, the left most cycle fixes 4, so

$$\begin{aligned}(132)(345)(4678)(245)3 &= (132)(345)(4678)3\\ &= (132)(345)3\\ &= (132)4\\ &= 4\end{aligned}$$

To continue the cycle, we must follow 4 now.

$$\begin{aligned}(132)(345)(4678)(245)4 &= (132)(345)(4678)5\\ &= (132)(345)5\\ &= (132)3\\ &= 2\end{aligned}$$

Now to see where 2 goes,

$$\begin{aligned}(132)(345)(4678)(245)2 &= (132)(345)(4678)4\\ &= (132)(345)6\\ &= (132)6\\ &= 6\end{aligned}$$

But this is taking too long, so let us try to follow the progress of 6 from right to left.
(132)(345)(4678)(245) sends 6 to itself, then to 7, then 7 is fixed in the rest of

the cycles.
Now we will summarize our progress, so far; (13426 . . . , but we aren't done yet.
6 goes to 7, which is fixed, yielding (134267.
And 7 goes to 8 which is fixed, yielding (1342678.
8 goes to 4, which goes to 5 and is then fixed, so (13426785
And finally, 5 goes to 2 which goes to 1, so (13426785).

3. Disjoint Cycle Decomposition

Why would we want to do all of this work to multiply cycles with number in common?
Why not leave them alone?
Well, multiplying cycles with numbers in common produces the product of cycles with no numbers in common.
These are called *disjoint cycles.*
Every permutation in S_n can be written as a product of disjoint cycles.
To see this we recall that $\alpha \in S_n$ means that α is a bijective function from $\{1, 2, 3, \ldots, n$ to itself.

Definition 1 (orbit)**.** The orbit of $x \in \{1, 2, 3, \ldots n\}$ under α to be $O_\alpha(x) = \{\alpha^k(x) \mid k \in \mathbb{Z}\}$ be the set of all numbers to which all possible powers of α send x.

For example, if $\alpha = (123)(45)$, then the orbit of 3 under α, $O_\alpha(3) = \{3, 1, 2\}$, and $O_\alpha(1) = \{1, 2, 3\}$.

In fact, given any $x \in \{1, 2, 3, \ldots n\}$, $O_\sigma(x)$ will be finite for all σ.
Furthermore, for any bijective function from a finite set to itself, the orbit of any element will consist of exactly those elements in the cycle.

Next we will see that if $y \notin O_f(x)$, then $O_f(y) \cap O_f(x) = \varnothing$.
In the space provided below, compute the orbit of each element in the permutation given in the example above.

Now to prove this in general. Suppose $z \in O_f(x) \cap O_f(y)$.
Then $f^k(x) = z$, and $f^m(y) = z$.
Since f is bijective, then f^{-1} exists.
In particular, $f^{-m}(z) = y$.
Therefore, $f^{-m} \circ f^k(x) = f^{-m}(z) = y$.
But $f^{-m} \circ f^k = f^{k-m}$ is a integral power of f, which means y is in the orbit of x. This is a contradiction.

It is pretty clear that the order of a cycle is the same as the cardinality of its orbit.
Since the cardinality of the orbit of any element in the cycle is the length of the cycle, then it is also clear that the order of a cycle is its length.

One immediate consequence of this method of writing permutations is that the disjoint cycles commute with each other.

Corollary 1. *Let $\alpha, \beta \in S_n$ be disjoint cycles. Then $\alpha\beta = \beta\alpha$.*

Proof 1. *To prove this we will break this up into two cases.*
Let $x \in \{1, 2, 3, \dots n\}$.
Case 1*: Suppose x is a fixed point of α and β.*
Then $\alpha\beta(x) = x = \beta\alpha(x)$.
Case 2*: Now suppose x is a fixed point of α, but $\beta(x) = y$.*
This means $\beta(x) = y$, then $y \in O_\beta(x)$ which means that y is in the cycle β.
Since β and α are disjoint, this means that y is also a fixed point of α.
Then $\alpha\beta(x) = \alpha(y) = y = \beta(x) = \beta\alpha(x)$.
Clearly, the same argument will occur if x is a fixed point of β but not α.
Since α and β are disjoint, there is no possibility that x will not be fixed by α and β.

One of the most useful consequences of disjoint cycle decomposition is that we can immediately identify the order of a permutation if it's written in disjoint cycle decomposition.

Lemma 1. *The order of a permutation in disjoint cycle decomposition is the least common multiple of the lengths of the disjoint cycles.*

Proof 2. *To see this, let's assume that $\alpha, \beta \in S_n$ be cycles such that* $\mathrm{ord}(\alpha) = m$ *and* $\mathrm{ord}(\beta) = k$.
Then for each element in $x \in S_n$, $\alpha^m(x) = x$ and $\beta^k(x) = x$, so, since disjoint cycles commute, $\alpha^{\mathrm{lcm}(k,m)}\beta^{\mathrm{lcm}(k,m)} = (\alpha\beta)^{\mathrm{lcm}(k,m)}(x) = x$ for all $x \in S_n$.
Since $(\alpha\beta)^r(x) = x$ for all $x \in S_n$ means that $m \mid r$ and $k \mid r$, then $\mathrm{lcm}(k.m) \mid r$.
Therefore, $\mathrm{lcm}(k, m) = \mathrm{ord}(\alpha\beta)$.

4. Exercises

Exercise 1. Find the order of each of the following permutations

(a) $(124)(357)$ _____

(b) $(1235)(24567)$ _____

(c) $(345)(245)$ _____

(d) $(14)(15)(16)(17)$ _____

Exercise 2. What are the possible orders of the elements in S_5? How many elements of each order are there?

Exercise 3. What is the inverse of the permutations $(12345)(678)$? _____

5. Transposition Decomposition

Another useful method of writing a permutation is using 2-cycles.
Every permutation can be written as a product of 2-cycles.
For example, $(1345) = (15)(14)(13) = (13)(34)(45)$.
Even the identity can be written as $e = (12)(12)$.
More importantly, although each permutation can be written in transposition decomposition in many different ways, since the identity is even, the parity of the number of transpositions will not change.
For example,

$$(1345) = (15)(14)(13) = (14)(15)(15)(14)(13)(34)(45) = (14)e(14)(13)(34)(45) = (13)(34)(45)$$

Note that in order to change the first transposition decomposition $(15)(14)(13)$ to the second, $(13)(34)(45)$, we needed to multiply by the inverse of (15) and (14), yielding an product of transpositions equal to the identity, times the intended transposition decomposition.
In other words, if $\beta \in S_n$ can be written as the product of transpositions $\beta = \tau_1\tau_2\tau_3\ldots\tau_n$ and β can also be written as the product of transpositions, $\beta = \gamma_1\gamma_2\gamma_3\ldots\gamma_k$ then those two transposition decompositions differ by the product of transpositions equal to the identity.

Definition 2. A permutation which can be written as an even number of transpositions is called an *even permutation*.
A permutation which can be written as an odd number of transpositions is called an *odd permutation*.

6. Exercises

Exercise 4. For each of the following permutations, identify them as even or odd.

- **(a)** (12345) _____
- **(b)** (123456) _____
- **(c)** $(123)(4567)$ _____
- **(d)** $(1235)(1267)$ _____
- **(e)** an even length cycle _____
- **(f)** an odd length cycle _____
- **(g)** the product of two odd permutations _____
- **(h)** the product of two even permutations _____
- **(j)** the product of an even permutation and an odd permutation _____
- **(k)** the inverse of an even permutation _____

Exercise 5. Show that the set of all even permutations forms a group, but the set of odd permutations does not. We call the group of even permutations in S_n, A_n.

Exercise 6. The ultimate goal of this exercise is to show that A_n is a normal subgroup of S_n.

(a) Find $|A_n|$.

(b) Find $[S_n : A_n]$

(c) Show that $\sigma A_n = A_n \sigma$ for all $\sigma \in S_n$.

(d) Show $A_n \triangleleft S_n$.

Exercise 7. Define a function $f : S_n \to \{-1, 1\}*$ from the permutation group of n elements to the multiplicative group of 1 and -1, by

$$f(\sigma) = \begin{cases} 1 & \sigma \in A_n \\ -1 & \sigma \notin A_n \end{cases}$$

Show that f is a homomorphism. How does this also show that $A_n \triangleleft S_n$.

Department of Mathematics, BASIS Scottsdale
E-mail address: marizza.bailey@basisscottsdale.org