More on Cycles

Definition: An element f of the symetric group on n letters S_n is called a *cycle* if there are elements $i_1, \dots, i_m \in \{1, \dots, n\}$ (here m can be any number between 1 and n) such that:

1. $f(i_1) = i_2,\ f(i_2) = i_3, \dots, f(i_{m-1}) = i_m$, and $f(i_m) = i_1$; and
2. $f(i) = i$ for all other $i \in \{1, \dots, n\}$ not equal to any i_j.

The number m is called the *length* of the cycle f.

Recall that we used the notation $(i_1, \dots, i_m)$ for such a permutation, but this wasn't unique.

For example, $(1, 4, 6)$ is a cycle of length three, but can also be written $(4, 6, 1)$ and $(6, 1, 4)$.

Notice that the identity function is a cycle of length 1, and technically can be written as (1), (2), or even (i) for any number i.

We can view a cycle graphically by considering an m-sided polygon with vertices labelled clockwise $i_1, \dots, i_m$. Then we can think of the cycle $(i_1, \dots, i_m)$ as a clockwise rotation of the polygon.

What happens if we rotate the polygon m times? What happens when we compose a cycle of length m with itself m times?

Notation: For any permutation $f \in S_n$ (not just cycles), let

$$f^m = \underbrace{f \circ f \circ \cdots \circ f}_{m \text{ times}}.$$

Lemma: If f is a cycle of length m, then $f^m = (1)$, the identity function. Moreover, m is the smallest positive integer for which this is true.

Proof: Suppose f is a cycle of length m, say $f(i_1) = i_2, \ldots, f(i_{m-1}) = i_m$ and $f(i_m) = i_1$. We see that $f^j(i_1) = i_{j+1}$ for all positive integers j with $j \leq m-1$. (Note in particular that f^j is not the identity function if $j < m$, since $f^j(i_1) \neq i_1$ if $j < m$.) Then $f^m(i_1) = f \circ f^{m-1}(i_1) = f(i_m) = i_1$.

More generally, $f^j(i_l) = i_{j+l}$ for all positive integers j with $j \leq m - l$. So $f^{m-l+1}(i_l) = f \circ f^{m-l}(i_l) = f(i_m) = i_1$ and $f^m(i_l) = f^{l-1} \circ f^{m-l+1}(i_l) = f^{l-1}(i_1) = i_l$.

Thus, $f^m(i_l) = i_l$ for $l = 1, \ldots, m$. Also, $f^m(i) = i$ for all i not equal to $i_1, \ldots, i_m$. This shows that f^m is the identity function.

If f is a cycle of length m, what does the collection $f, f^2, \ldots, f^m$ look like algebraically? In other words, what does the composition table look like?

Example: Suppose f is the cycle of length 3, or "3-cycle" for short(er), (1,4,6). Then

$$f^2 = (1,4,6)(1,4,6) = (1,6,4), \qquad f^3 = f \circ f^2 = (1,4,6)(1,6,4) = (1)$$

and

$$f^2 \circ f^2 = f^3 \circ f = f.$$

This last line used a few things. What, specifically, did we use?