Orders of Permutations

The purpose of this handout is to prove the following theorem, which is stated in Exercise 8.10(a) in Saracino's textbook.

Theorem. Let $n \geq 1$, and let $f \in S_n$ be a permutation. Suppose that $f = f_1 f_2 \cdots f_m$ is a product of disjoint cycles $f_1, f_2, \ldots, f_m \in S_n$. Then the order of f is given by

$$o(f) = \operatorname{lcm}(o(f_1), o(f_2), \ldots, o(f_m)).$$

Note 1. Recall that $f \in S_n$ means that f is a one-to-one and onto function $f : X \to X$, where X is the set $X = \{1, 2, \ldots, n\}$. Similarly, each $f_i \in S_n$ is also a one-to-one and onto function $f_i : X \to X$.

Also, recall that the binary operation on S_n is composition. So the formula $f = f_1 f_2 \cdots f_m$ in the statement of the theorem really means $f = f_1 \circ f_2 \circ \cdots \circ f_m$.

Note 2. Recall that a *cycle* (of length r) in S_n is a permutation of the form $g = (x_1, x_2, \ldots, x_r)$, where $x_1, \ldots, x_r \in X$ are *distinct* elements of $X = \{1, 2, \ldots, n\}$. (A cycle of length r is sometimes also called an r-*cycle*.)

It is a fact that if $g \in S_n$ is a cycle of length r, then the order of g is $o(g) = r$. (This is the content of Exercise 8.4 in Saracino's book.)

For example, $g = (1, 6, 4) \in S_7$ is a 3-cycle. It is the bijective function from $X = \{1, 2, 3, 4, 5, 6, 7\}$ to itself with $g(1) = 6$ and $g(6) = 4$ and $g(4) = 1$, and with $g(x) = x$ for every other x.

That is, g may be written in long form as $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 2 & 3 & 1 & 5 & 4 & 7 \end{pmatrix}$, and we have $o(g) = 3$.

Note 3. Recall that two cycles $f_1 = (x_1, x_2, \ldots, x_r)$ and $f_2 = (y_1, y_2, \ldots, y_s)$ are said to be *disjoint* if the items $x_1, \ldots, x_r$ that appear in the cycle notation for f_1 do not overlap at all with the items $y_1, \ldots, y_s$ that appear in the cycle notation for f_2.

For example, $(1, 6, 4)$ and $(2, 7)$ are disjoint cycles. On the other hand, the cycles $(1, 6, 4)$ and $(4, 5)$ are not disjoint.

More generally, we say that multiple cycles $f_1, \ldots, f_m$ are disjoint if **no two of them** share an item in common; that is, if every single pair f_i, f_j of different cycles in this list are disjoint.

Note 4. Many permutations are **not** cycles. In fact, when n gets to be at least 7, *most* elements of S_n are not cycles.

For example, $f = (1, 6, 4)(2, 7) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 7 & 3 & 1 & 5 & 4 & 2 \end{pmatrix}$ is *not* a cycle. Applying f means rotating the three items $\{1, 6, 4\}$ are rotated amongst themselves, while separately, the two items $\{2, 7\}$ are switched back and forth.

By Note 2 above, the orders of the two disjoint cycles making up f are $o((1, 6, 4)) = 3$ and $o((2, 7)) = 2$. Therefore, the Theorem above says that $o(f) = \operatorname{lcm}(3, 2) = 6$.

I would suggest you try to intuitively understand why this conclusion makes sense, as follows: $f_1 = (1, 6, 4)$ returns everyone to start every 3 iterations, and $f_2 = (2, 7)$ does so every 2 iterations. So the first iteration when *both* of them return everybody to start is the 6th, i.e., the lcm of 3 and 2.

Before proving the Theorem, we need the following result, which is Exercise 8.8 in Saracino:

Lemma. Let $f_1, f_2 \in S_n$ be disjoint cycles. Then they commute; that is, $f_1 f_2 = f_2 f_1$.

Proof of Lemma. Write $X = \{1, 2, \ldots, n\}$. By hypothesis, we have $f_1 = (x_1, x_2, \ldots, x_r)$ and $f_2 = (y_1, y_2, \ldots, y_s)$ for some $x_1, \ldots, x_r, y_1, \ldots, y_s \in X$ all distinct from one another.

Given an arbitrary $t \in X$, we must show $f_1 \circ f_2(t) = f_2 \circ f_1(t)$. [This is what it means for the two functions $f_1 \circ f_2 : X \to X$ and $f_2 \circ f_1 : X \to X$ to be equal.] We consider three cases.

Case 1: $t = x_i$ for some i. Then

$$f_1 \circ f_2(t) = f_1(f_2(x_i)) = f_1(x_i) = x_{i+1} = f_2(x_{i+1}) = f_2(f_1(x_i)) = f_2 \circ f_1(t),$$

where the second and and fourth equalities are because f_2 only moves the y_j's (and hence $f_2(x_i) = x_i$ and $f_2(x_{i+1}) = x_{i+1}$), and the third and fifth are because $f_1(x_i) = x_{i+1}$. Here, if $i = r$, we write x_{r+1} for x_1, which is what $f_1(x_r)$ is.

Case 2: $t = y_i$ for some i. Then

$$f_1 \circ f_2(t) = f_1(f_2(y_i)) = f_1(y_{i+1}) = y_{i+1} = f_2(y_i) = f_2(f_1(i_i)) = f_2 \circ f_1(t),$$

by similar reasoning, where this time in the case $i = s$, we write y_{s+1} for y_1.

Case 3: t is not any of the x_i's or y_i's. Then $f_1(t) = t$ and $f_2(t) = t$, so

$$f_1 \circ f_2(t) = f_1(f_2(t)) = f_1(t) = t = f_2(t) = f_2(f_1(t)) = f_2 \circ f_1(t).$$

QED Lemma

Proof of Theorem. Define $n_i = o(f_i)$, and $N = \operatorname{lcm}(n_1, \ldots, n_m)$. Our goal is to show $o(f) = N$. So define the following sets of positive integers:

$$S = \{k \geq 1 \,|\, f^k = e\} \quad \text{and} \quad T = \{k \geq 1 \,|\, n_i \text{ divides } k \text{ for each } i = 1, \ldots, m\}$$

By definition of order, we have $o(f) = \min S$; and by definition of lcm, we have $N = \min T$. Thus, it suffices to show that $S = T$.

Proving ($\supseteq$): By the Lemma, we know that for each $i \neq j$, we have $f_i f_j = f_j f_i$, i.e., the disjoint cycles f_i and f_j commute. Thus, for each integer $k \geq 1$, we have

$$f^k = (f_1 f_2 \cdots f_m)^k = f_1^k f_2^k \cdots f_m^k \qquad (\star)$$

[Technically, proving equation ($\star$) requires induction — probably in two steps, once on k and once on m — but I will skip that here.]

In particular, given any $k \in T$, since $n_i | k$ for each $i = 1, \ldots, m$, we therefore have

$$f^k = f_1^k f_2^k \cdots f_m^k = ee \cdots e = e,$$

and hence $k \in S$. QED ($\supseteq$)

Proving ($\subseteq$): Given any $k \in S$ and any $i = 1, \ldots, m$, we claim that $n_i | k$.

Write the cycle f_i as $f_i = (x_0, x_1, \ldots, x_{n_i - 1})$, where $x_0, \ldots, x_{n_i - 1} \in X = \{1, \ldots, n\}$ are all distinct.

By the Division Algorithm, there are integers $q, r \in \mathbb{Z}$ such that $k = qn_i + r$, with $0 \leq r \leq n_i - 1$. It suffices to prove that $r = 0$.

Observe that $f_i^k = f_i^{qn_i + r} = (f_i^{n_i})^q f_i^r = e^q f_i^r = f_i^r$, and hence $f_i^k(x_0) = f_i^r(x_0) = x_r$. Therefore, by equation ($\star$) and the fact that $f^k = e$, we have

$$\begin{aligned} x_0 = e(x_0) = f^k(x_0) &= f_1^k f_2^k \cdots f_{i-1}^k f_i^k f_{i+1}^k \cdots f_m^k(x_0) \\ &= f_1^k f_2^k \cdots f_{i-1}^k f_i^k(x_0) = f_1^k f_2^k \cdots f_{i-1}^k(x_r) = x_r, \end{aligned}$$

where the fourth and sixth equalities are because f_j fixes both x_0 and x_r for $j \neq i$, since the cycles f_i and f_j are disjoint. But because $0 \leq r \leq n_i - 1$ and because $x_0, \ldots, x_{n_i - 1}$ are all distinct, it follows from the above equation (which says $x_r = x_0$) that $r = 0$.

That is, $k = qn_i$, whence $n_i | k$. Since this is true for all $i = 1, \ldots, m$, it follows that $k \in T$, as desired. QED ($\subseteq$)

Since $S = T$, we have $o(f) = \min S = \min T = \operatorname{lcm}(n_1, \ldots, n_m)$ QED