4 Cycle decomposition in cyclic groups (09/27)

Theorem 4.1 (Cycle decomposition)**.** *Let $f \in S_n$ be an element of S_n. Then, for some $1 \leqslant r \leqslant n$ there are r pairwise disjoint cycles $(a_{11} \cdots a_{1,k_1}), (a_{21} \cdots a_{2,k_2}), \ldots, (a_{r1}, \ldots, a_{r,k_r})$ such that*

$$f = (a_{11} \cdots a_{1,k_1}) \cdots (a_{r1} \cdots a_{r,k_r}).$$

Proof. As $\{1, \ldots, n\}$ is finite, there is some smallest $k \geqslant 1$ for which $f^{(k)}(1) = 1$. Then, $(1\, f(1)\, f(f(1) \cdots f^{(k-1)}(1))$ is a cycle of length k. Let this be $(a_{11} \cdots a_{1,k_1})$. Let a_{21} be the first element in $\{1, \ldots, n\}$ not in the cycle $(a_{11} \cdots a_{1,k_1})$ and consider the cycle generated by a_{21}, say $(a_{21} \cdots a_{2,k_2})$. This is a disjoint cycle. Continue on in this way until every element of $\{1, \ldots, n\}$ appears in a cycle. $\square$

Remark 4.2. As cycles of length 1 all correspond to the identity element of S_n it is standard to omit them from the final cycle decomposition of f. The cycle decomposition of f is unique up to cyclically rotating the terms in the cycles (Remark 3.9) and reordring the cycles themselves (Lemma 3.10).

Example 4.3. If $f = (a_{11} \cdots a_{1,k_1}) \cdots (a_{r1} \cdots a_{r,k_r})$ is a decomposition of f into disjoint cycles, then the order of f is the least common multiple of $k_1, \ldots, k_r$. For example, if $f = (1\,12\,8\,10\,4)(2\,13)(5\,11\,7)(6\,9)$, then $|f| = 30$.

Recall the following definition from last time.

Definition 4.4. A **transposition** is a cycle $(a\,b)$ of length 2. If $f = (a\,b)$, then $f^2 = e$, so $f^{-1} = f$.

Lemma 4.5. *Every element $f \in S_n$ can be written as a product of transpositions.*

Proof. Using cycle decomposition, it is enough to prove the result for cycles. Thus, assume that $f = (a_1 \cdots a_k)$. Then, $f = (a_1\, a_2) \circ (a_2\, a_3) \circ \cdots \circ (a_{k-1}\, a_k)$. Indeed, for a_i with $1 \leqslant i \leqslant k-1$, it us unchanged except by $(a_i\, a_{i+1})$, which sends it to a_{i+1}. For a_k, $(a_{k-1}\, a_k)$ sends it to a_{k-1}, then $(a_{k-2}\, a_{k-1})$ sends it to a_{k-2}. This continues until finally $(a_1\, a_2)$ sends the result to a_1. $\square$

Example 4.6. Write down the cycle decomposition of each element of S_3 and compute the order of each element. See Table 1 for the solution.

e	1
$(1\,2)$	2
$(1\,3)$	2
$(2\,3)$	2
$(1\,2\,3)$	3
$(1\,3\,2)$	3

Table 1: The cycle decompositions and orders of the $6 = 3!$ elements of S_3.

Example 4.7. If $f = (a_{11} \cdots a_{1,k_1}) \cdots (a_{r1} \cdots a_{r,k_r})$ is a decomposition of f into disjoint cycles, then the order of f is the least common multiple of $k_1, \ldots, k_r$. For example, if $f = (1\,12\,8\,10\,4)(2\,13)(5\,11\,7)(6\,9)$, then $|f| = 30$.

Example 4.8 (Dummit–Foote, Exercise 1.3.1)**.** One way to write down permutations is using a kind of matrix notation: the permutation $f \in S_5$ given by

$$1 \mapsto 3 \quad 2 \mapsto 4 \quad 3 \mapsto 5 \quad 4 \mapsto 2 \quad 5 \mapsto 1$$

can be written efficiently as

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix},$$

which is just a lookup table. The cycle decomposition of f is $f = (1\,3\,5)(2\,4)$. If we consider

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 4 & 1 \end{pmatrix},$$

which has cycle decomposition $g = (1\,5)(2\,3)$, then we can compute the cycle decompositions

$$\begin{aligned} f^2 &= (1\,5\,3) \\ fg &= (2\,5\,3\,4) \\ gf &= (1\,2\,4\,3) \\ g^2 f &= f = (1\,3\,5)(2\,4). \end{aligned}$$

4.1 Exercises

Exercise 4.1. Justify Example 4.7. Fix pairwise commuting elements $f_1, \ldots, f_r$ of a group G, i.e., elements such that $f_i f_j = f_j f_i$ for all $1 \leqslant i, j \leqslant r$. Prove that if each f_i has finite order n_i, then $f = f_1 \cdots f_r$ has order the least common multiple of $f_1, \ldots f_r$.

Exercise 4.2. By Lemma 4.5, every element $f \in S_n$ can be written as a product of transpositions. Suppose that $f = g_1 \circ \cdots \circ g_k$ where $g_1, \ldots, g_k$ are transpositions. We say that f is **even** if k is even and we say that f is **odd** if k is odd. Show that this is well-defined by proving that if $f = h_1 \circ \cdots \circ h_m$ is another way of writing f as a product of transpositions, then $k \equiv m \mod 2$.

Exercise 4.3. Let $f = (a_1 \ \cdots \ a_k)$ be a cycle. Show that f is even if k is odd and that f is odd if k is even.

Exercise 4.4. Write down the cycle decomposition of each element of S_4 and compute the order of each element.

Exercise 4.5 (Dummit–Foote, Exerice 1.3.2)**.** Let

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 13 & 2 & 15 & 14 & 10 & 6 & 12 & 3 & 4 & 1 & 7 & 9 & 5 & 11 & 8 \end{pmatrix}$$

and

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 14 & 9 & 10 & 2 & 12 & 6 & 5 & 11 & 15 & 3 & 8 & 7 & 4 & 1 & 13 \end{pmatrix}$$

be two elements of S_{15}. Find cycle decompositions for f, g, f^2, $f \circ g$, $g \circ f$, and $g^2 \circ f$.