Continuation Symmetric Groups

Cycle notation: An efficient notation for writting elements σ of S_n.

A **cycle** is a string of integers which cyclically permutes these integers (and fixes all other integers). Let $a_i \in X_n$. The cycle $(a_1\ a_2\ \cdots\ a_m) \in S_n$ is the permutation sending a_i to a_{i+1}, $1 \leq i \leq m-1$, a_m to a_1, and a_i to a_i, $i \notin \{1,2,\ldots,m\}$.

$$\begin{tikzcd} a_1 \arrow[r] & a_2 \arrow[r] & \cdots \arrow[r] & a_m \arrow[lll, bend left] \end{tikzcd} \qquad \underset{i \notin \{1,2,\ldots,m\}}{a_i \longrightarrow a_i}$$

Ex: Let $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 6 & 5 & 3 \end{pmatrix} \in S_6$. We will leave out the first row and write the cycles $\alpha = (1\ 2)(3\ 4\ 6)$. ⚠ We omit the elements that are fixed.

Def: (1) A cycle of the form $(a_1\ a_2 \cdots a_m) \in S_n$ is called a cycle of length m or m-cycle.

(2) A 2-cycle is called a transposition.

Composition in cycle notation: Move through cycles from right to left.

Ex: Let $\alpha = (1\ 3)(2\ 7)(4\ 5\ 6)$ and $\beta = (1\ 2\ 3\ 7)(6\ 4\ 8)$ in S_8

$$\alpha\beta = (1\ 3)\ (2\ 7)\ (4\ 5\ 6)\ (1\ 2\ 3\ 7)\ (6\ 4\ 8) = (1\ 7\ 3\ 2)\ (4\ 8)\ (5\ 6)$$

2 7   1 2

1 3   1   7

Def: Two cycles are disjoint if they have no number in common.

Explicitly ⇝ α and β in S_n are disjoint if for all $k \in X_n$

$$\alpha(k) = k \quad \text{implies} \quad \beta(k) \neq k.$$

$$\alpha \text{ fixes } k \quad \Rightarrow \quad \beta \text{ moves } k$$

Theorem 13: If $\alpha, \beta \in S_n$ are disjoint, then $\alpha\beta = \beta\alpha$.

Proof: Exercise.

Theorem 14: Any nonidentity permutation $\pi \in S_n$ $(n \geq 2)$ can be uniquely expressed (up to the order of the factors) as a product of disjoint cycles of length at least 2.

Proof: By induction on n.

Basis step: Suppose $n = 2$. Now $|S_2| = 2$ and the nonidentity element of S_2 is $\alpha = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$. Now $\alpha = (1\ 2)$, i.e., α is a cycle. Thus, the theorem is true for $n = 2$.

Inductive hypothesis: Suppose that the theorem is true for all S_k such that $2 \leq k < n$.

Inductive step: Suppose $n > 2$. We show that the result is true for n.

Let π be a nonidentity element of S_n. Now $\pi^i(1) \in X_n$ for all integers i, $i \geq 1$. Therefore, $\{\pi(1), \pi^2(1), \ldots, \pi^i(1), \ldots\} \subseteq X_n$. Because X_n is a finite set, we must have $\pi^l(1) = \pi^m(1)$ for some integers l and m such that $l > m \geq 1$. This implies that $\pi^{l-m}(1) = 1$. Let us write $j = l - m$. Then $j > 0$ and $\pi^j(1) = 1$. Let i be the smallest positive integer such that $\pi^i(1) = 1$. Let

$$A = \{1, \pi(1), \pi^2(1), \ldots, \pi^{i-1}(1)\}.$$

Then all elements of the set A are distinct. Let $\tau \in S_n$ be the permutation defined by

$$\tau = (1\ \pi(1)\ \pi^2(1)\ \cdots\ \pi^{i-1}(1)),$$

i.e., τ is a cycle. Let $B = X_n \backslash A$. If $B = \emptyset$, then π is a cycle. Suppose $B \neq \emptyset$. Let $\sigma = \pi|_B$. If σ is the identity, then π is a cycle. Suppose that σ is not the identity. Now by the induction hypothesis, σ is a product of disjoint cycles on B, say, $\sigma = \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_r$. Now for $1 \leq i \leq r$, define π_i by

$$\pi_i(a) = \begin{cases} \sigma_i(a) \text{ if } a \in B \\ a \text{ if } a \notin B. \end{cases}$$

Then $\pi_1, \pi_2, \ldots, \pi_r$ and τ are disjoint cycles in S_n. It is easy to see that $\pi = \pi_1 \circ \pi_2 \circ \cdots \circ \pi_r \circ \tau$. Thus, π is a product of disjoint cycles.

To prove the uniqueness, let $\pi = \pi_1 \circ \pi_2 \circ \cdots \circ \pi_r = \mu_1 \circ \mu_2 \circ \cdots \circ \mu_s$, a product of r disjoint cycles and also a product of s disjoint cycles, respectively. We show that every π_i is equal to some μ_j and every μ_k is equal to some π_t. Consider π_i, $1 \leq i \leq r$. Suppose $\pi_i = (i_1 i_2 \ldots i_l)$. Then $\pi(i_1) \neq i_1$. This implies that i_1 is moved by some μ_l. By the disjointness of the cycles, there exists unique μ_j, $1 \leq j \leq s$, such that i_1 appears as an element in μ_j. By reordering, if necessary, we may write $\mu_j = (i_1\ c_2\ \ldots\ c_m)$. Now

$$
\begin{array}{ccccccccccc}
i_2 & = & \pi_i(i_1) & = & \pi(i_1) & = & \mu_j(i_1) & = & c_2 & & \\
i_3 & = & \pi_i(i_2) & = & \pi(i_2) & = & \pi(c_2) & = & \mu_j(c_2) & = & c_3 \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
i_l & = & \pi_i(i_{l-1}) & = & \pi(i_{l-1}) & = & \pi(c_{l-1}) & = & \mu_j(c_{l-1}) & = & c_l.
\end{array}
$$

If $l < m$, then $i_1 = \pi_i(i_l) = \pi(i_l) = \pi(c_l) = \mu_j(c_l) = c_{l+1}$, a contradiction. Thus, $l = m$. Hence, $\pi_i = \mu_j$ for some j, $1 \leq j \leq s$. Similarly, every $\mu_k = \pi_t$ for some t, $1 \leq t \leq r$. ■

Corollary 15: Let $n \geq 2$. Any permutation σ of S_n can be expressed as a product of transpositions.

Proof: In view of Thm 14, it suffices to show that every m-cycle can be expressed as a product of transpositions.

Observe that $1 = (1) = (1\ 2)(1\ 2)$ and for $m \geq 2$

$$(a_1\ a_2 \cdots a_m) = (a_1\ a_m)(a_1\ a_{m-1}) \cdots (a_1\ a_2)$$

where $\{a_1, a_2, \dots, a_m\} \subseteq X_n$.

⚠ The representation as product of transpositions is not unique:

$$(1\ 2\ 3) = (1\ 3)(1\ 2) \quad \text{and} \quad (1\ 2\ 3) = (2\ 1)(2\ 3).$$

Def: Let $\sigma \in S_n$. Suppose $\sigma = \tau_1 \tau_2 \cdots \tau_m$ where τ_i, $1 \le i \le m$, is a tranposition.

If m is even, then σ is called an even permutation; otherwise σ is called an odd permutation.

Q: How do we know σ does not have even and odd decompositions at the same time?

A: We don't know! We'll need to show that is not possible. See Q1, PS7.