On the Disjoint Cycle Decomposition of a Permutation

R. C. Daileda

For $n \in N$, the *permutation group on n symbols* is usually defined to be

$$S_n = \text{Perm}(\{1, 2, 3, \ldots, n\}),$$

the group operation being composition of functions. The fact that every member of S_n can be written as a product of disjoint cycles is essential to understanding the group theoretic structure of S_n, but the proofs presented in many textbooks are notoriously tedious and difficult to understand. It turns out that if we slightly generalize the statement "every member of S_n can be written as a product of disjoint cycles," it's possible to give a relatively short inductive proof. The key observation is that the notion of a *cycle* makes sense in the group $\text{Perm}(S)$ for *any* nonempty set S.

Theorem 1. *For any nonempty finite set S, every $\sigma \in \text{Perm}(S)$ can be written as a product of disjoint cycles.*

Proof. We induct on $|S|$. Since the only permutation of a singleton set is the identity, which can be written as a 1-cycle, there is nothing to prove when $|S| = 1$. Now suppose $n > 1$ and that every member of $\text{Perm}(S')$ can be written as a product of disjoint cycles, whenever $1 \leq |S'| < n$. Let $|S| = n$ and choose $\sigma \in \text{Perm(S)}$. There is nothing to prove if σ is the identity, so we may assume that $\sigma(x) \neq x$ for some $x \in S$.

Consider the set

$$H = \{k \in \mathbb{Z} \,|\, \sigma^k(x) = x\}.$$

It is easy to see that $H < \mathbb{Z}$. Since $\text{Perm}(S)$ is a finite group, σ has finite order $m \geq 1$, so that $\sigma^m(x) = \text{id}(x) = x$. Therefore $m \in H$ and H is nontrivial. This means that $H = r\mathbb{Z}$ for some $r \in \mathbb{N}$. Since $\sigma(x) \neq x$, $1 \notin H$ which implies $r \geq 2$.

Let $k, \ell \in \mathbb{Z}$ and suppose that $\sigma^k(x) = \sigma^\ell(x)$. Then $\sigma^{k-\ell}(x) = x$ and hence $k-\ell \in H = r\mathbb{Z}$. That is, $k \equiv \ell \pmod r$. This implies that

$$x, \sigma(x), \sigma^2(x), \ldots, \sigma^{r-1}(x)$$

are pairwise distinct members of S, since the exponents $0, 1, 2, \ldots, r-1$ are all distinct mod r. It follows that

$$\tau = (x \ \sigma(x) \ \sigma^2(x) \cdots \sigma^{r-1}(x))$$

represents an r-cycle in $\text{Perm}(S)$.

Now consider $\sigma' = \tau^{-1}\sigma$. For any $0 \leq k \leq r-1$ we have

$$\sigma'(\sigma^k(x)) = (\tau^{-1}\sigma)(\sigma^k(x)) = \tau^{-1}(\sigma^{k+1}(x)) = \sigma^k(x),$$

by the definition of τ. So σ' fixes $x, \sigma(x), \sigma^2(x), \ldots, \sigma^{r-1}(x)$ and can therefore be viewed as a permutation of the set $S' = S \setminus \{x, \sigma(x), \sigma^2(x), \ldots, \sigma^{r-1}(x)\}$. If $S' = \varnothing$, then σ' is the identity and $\sigma = \tau$ is an r-cycle. Otherwise $1 \leq |S'| < |S|$ and the inductive hypothesis implies that $\sigma' = \tau_1 \cdots \tau_k$ for some disjoint cycles $\tau_1, \ldots, \tau_k$ in $\mathrm{Perm}(S')$. Since τ is a cycle disjoint from any cycle in $\mathrm{Perm}(S')$, it follows that $\sigma = \tau\sigma' = \tau\tau_1 \cdots \tau_k$ expresses σ as a product of disjoint cycles. Since σ was an arbitrary (nonidentity) member of $\mathrm{Perm}(S)$, the result now follows by mathematical induction.

□