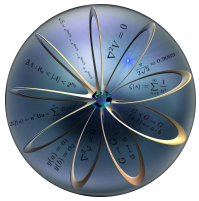

planetmath.org

Math for the people, by the people.

every permutation has a cycle decomposition

Canonical name	EveryPermutationHasACycleDecomposition
Date of creation	2013-03-22 16:48:39
Last modified on	2013-03-22 16:48:39
Owner	rspuzio (6075)
Last modified by	rspuzio (6075)
Numerical id	10
Author	rspuzio (6075)
Entry type	Proof
Classification	msc 03-00
Classification	msc 05A05
Classification	msc 20F55

In this entry, we shall show that every permutation of a finite set can be factored into a product of disjoint cycles. To accomplish this, we shall proceed in two steps.

We begin by showing that, if f is a non-trivial permutation of a set $\{x_i \mid 1 \leq i \leq n\}$, then there exists a cycle $(y_1, \ldots y_m)$ where

$$\{y_i \mid 1 \leq i \leq m\} \subseteq \{x_i \mid 1 \leq i \leq n\}$$

and a permutation g of $\{x_i \mid 1 \leq i \leq n\}$ such that $f = (y_1, \ldots y_m) \circ g$ and $g(y_i) = y_i$.

Since the permutation is not trivial, there exists z such that $f(z) \neq z$. Define a sequence inductively as follows:

$$z_1 = z$$
$$z_{k+1} = f(z_k)$$

Note that we cannot have $z_{k+1} = z_k$ for any k. This follows from a simple induction argument. By definition $f(z_1) = f(z) \neq z = z_1$. Suppose that $f(z_k) \neq z_k$ but that $f(z_{k+1}) = z_{k+1}$. By definition, $f(z_k) = z_{k+1}$. Since f is a permutation, $f(z_k) = z_{k+1}$ and $f(z_{k+1}) = z_{k+1}$ imply that $z_k = z_{k+1}$, so $z_k = f(z_k)$, which contradicts a hypothesis. Hence, if $f(z_k) \neq z_k$, then $f(z_{k+1}) \neq z_{k+1}$ so, by induction, $f(z_k) \neq z_k$ for all k.

By the pigeonhole principle, there must exist p and q such that $p < q$ but $f(z_p) = f(z_q)$. Let m be the least integer such that $f(z_p) = f(z_{p+m})$ but $f(z_p) \neq f(s_{p+k})$ when $k < m$. Set $y_k = z_{k+p}$. Then we have that $(y_1, \ldots y_m)$ is a cycle.

Since f is a permutation and $\{y_i \mid 1 \leq i \leq m\}$ is closed under f, it follows that

$$\{x_i \mid 1 \leq i \leq n\} \setminus \{y_i \mid 1 \leq i \leq m\}$$

is also closed under f. Define g as follows:

$$g(z) = \begin{cases} z & z \in \{y_i \mid 1 \leq i \leq m\} \\ f(z) & z \in \{x_i \mid 1 \leq i \leq n\} \setminus \{y_i \mid 1 \leq i \leq m\} \end{cases}$$

Then it is easily verified that $f = (y_1, \ldots y_m) \circ g$.

We are now in a position to finish the proof that every permutation can be decomposed into cycles. Trivially, a permutation of a set with one element can be decomposed into cycles because the only permutation of a set with one

element is the identity permutation, which requires no cycles to decompose. Next, suppose that any set with less than n elements can be decomposed into cycles. Let f be a permutation on a set with n elements. Then, by what we have shown, f can be written as the product of a cycle and a permutation g which fixes the elements of the cycle. The restriction of g to those elements z such that $g(z) \neq z$ is a permutation on less than n elements and hence, by our supposition, can be decomposed into cycles. Thus, f can also be decomposed into cycles. By induction, we conclude that any permutation of a finite set can be decomposed into cycles.