

Even More on Cycles

We've seen cycles and looked at them both algebraically and geometrically. We've also seen permutations written (not uniquely!) as a composition of cycles. To a certain extent, the study of permutations can be reduced to the study of cycles, and is yet another nice example of equivalence relations.

Theorem: Every permutation in S_n can be written as a composition of disjoint cycles.

Two cycles are called *disjoint* if the numbers occurring in one do not occur in the other. For example $(1, 4, 5)$ and $(2, 3)$ are disjoint cycles, whereas $(1, 4, 5)$ and $(2, 3, 4)$ are not.

Proof: Let $\sigma \in S_n$. We first show that for some positive integer m , σ^m is the identity function. To see why, note that we actually counted the total number of permutations in S_n ; there are $n!$ of them. Thus, the permutations $\sigma, \sigma^2, \dots, \sigma^{n!+1}$ can't all be distinct; at least two of them must be the same permutation. Let's write $\sigma^i = \sigma^j$ where $1 \leq i < j \leq n! + 1$. There is a σ^{-1} in S_n , and one can easily check that $(\sigma^{-1})^i = (\sigma^i)^{-1}$. (We'll write σ^{-i} for this permutation.) Hence,

$$\iota = (\sigma^i)^{-1} \circ \sigma^i = \sigma^{-i} \circ \sigma^i = \sigma^{j-i}.$$

Now σ is a one-to-one and onto function from the set $\{1, 2, \dots, n\}$ to itself. Given two elements of this set, a and b , we say a is equivalent to b if $a = \sigma^i(b)$ for some positive integer i . We check that this is an equivalence relation. First, given any a we have $a = \iota(a) = \sigma^m(a)$ for some positive integer m as above, so $a \sim a$. Next, if a is equivalent to b , then $a = \sigma^i(b)$ for some positive integer i . Let m be as above. Note that $\sigma^{2m} = \sigma^{3m} = \dots$ are all equal to the identity function. Thus, there is a positive integer $j > i$ with $\sigma^j = \iota$. Then $\sigma^{j-i}(a) = \sigma^{j-i} \circ \sigma^i(b) = \sigma^j(b) = b$ and b is equivalent to a . Finally suppose $a \sim b$ and $b \sim c$; write $a = \sigma^l(b)$ and $b = \sigma^k(c)$ for some positive integers l and k . Then $a = \sigma^l \circ \sigma^k(c) = \sigma^{l+k}(c)$ and $a \sim c$.

This equivalence relation partitions the set $\{1, 2, \dots, n\}$ into equivalence classes. We show how each equivalence class gives us a cycle. Let $\{a_1, \dots, a_p\}$ be an equivalence class of p distinct

elements of $\{1, 2, \dots, n\}$ and consider the set

$$\{\sigma(a_1), \dots, \sigma^p(a_1)\}.$$

Certainly every element of this set is equivalent to a_1 , so that this set is a subset of our equivalence class. Let i be the least positive integer with $\sigma^i(a_1) = a_1$. Then we see that $\{\sigma(a_1), \dots, \sigma^i(a_1)\}$ is precisely the equivalence class containing a_1 , so that $i = p$ and

$$\{a_1, \dots, a_p\} = \{\sigma(a_1), \dots, \sigma^p(a_1)\}.$$

We associate this equivalence class with the p -cycle

$$(\sigma(a_1), \dots, \sigma^p(a_1)).$$

Since the equivalence classes partition $\{1, \dots, n\}$, the cycles we get in this manner are disjoint.

Finally, let $a \in \{1, \dots, n\}$. Then a is in exactly one equivalence class and occurs in exactly one of our disjoint cycles; say $a \sim b$ where $\tau = (\sigma(b), \dots, \sigma^p(b))$ is one of our cycles. Then by construction $a = \sigma^i(b)$ for some positive integer $i \leq p$ and $\sigma(a) = \sigma^{i+1}(b) = \tau(\sigma^i(b)) = \tau(a)$. Hence there is exactly one of our cycles τ in which a occurs, and $\sigma(a) = \tau(a)$. Since these cycles are disjoint, none of the others move a or $\tau(a)$, so that $\tau(a)$ is the same as applying the composition of all our cycles to a . In other words,

$$\sigma = \tau_1 \circ \dots \circ \tau_q,$$

where τ_1, \dots, τ_q are all our disjoint cycles corresponding to the q equivalence classes.

Note that we will likely see some one-cycles when we follow this construction. In fact, if we do this construction with the identity function, we get n equivalence classes with one element each, so n disjoint one-cycles. Of course, any one-cycle is just the identity function.

Another little tidbit is that, apparently, the order we compose the different cycles doesn't matter (since it never came up in the proof). But this is clear once we realize that disjoint cycles commute, i.e., $\tau \circ \rho = \rho \circ \tau$ for disjoint cycles τ and ρ .

By the way, the equivalence classes we used here are typically called *orbits*.