Lecture 4: transpositions, more properties of cycles

Summary:
We explore transpositions and their importance in permutation theory. We prove that the order of a permutation is the least common multiple of its disjoint cycle lengths. We show that every permutation can be written as a product of transpositions. We prove that the number of transpositions needed to write a permutation is either always even or always odd, establishing the concept of parity. We define even and odd permutations and provide examples of writing permutations as products of transpositions.

Topics Covered: even permutation, odd permutation, order of a permutation, parity of a permutation, transposition

Proposition: If $\sigma \in S_n$ is a product of disjoint cycles of lengths $l_1, \ldots, l_z$, then the order of σ is the least common multiple of $l_1, \ldots, l_z$.

This is the smallest positive integer k such that $l_i \mid k$ for all $i \in [z]$.

Consider these permutations

$$\sigma = (1,2)(3,4,5)$$

$$\pi = (1,2)(3,4,5,6)$$

Note that

$$(1,2)(1,2) = (1)(2)$$

Definition: A cycle of the form (a_1, a_2) is called a transposition.

Proposition: Every $\sigma \in S_n$ can be written as a product of transposition.

Proof: Since $\sigma \in S_n$ is a product of disjoint cycles, it suffices to prove the above claim for a cycle $(a_1, \ldots, a_k)$.

Note that

$$(a_1, \ldots, a_k) = (a_{k-1}, a_k) \ldots (a_3, a_k)(a_2, a_k)(a_1, a_k)$$

We can also write it as

$$(a_1, \ldots, a_k) = (a_1, a_2)(a_2, a_3) \ldots (a_{k-1}, a_k)$$

Both ways show that the cycle $(a_1, \ldots, a_k)$ can be written as a product of transpositions.

> The goal is to show that all of these complex permutations can be constructed using tiny building blocks.

Example: Try writing $(1,2,3,4)$ as a product of three transpositions.

$$(1,2,3,4) = (1,2)(2,3)(3,4)$$

Theorem: If $\sigma \in S_n$ is written as a product of transpositions in two ways, then the number of transpositions in both cases is either both even or both odd. That is to say that the parity of the number of transpositions remains the same.

Proof: Assume to the contrary that for some $\sigma \in S_n$ and transpositions $\tau_1, \ldots, \tau_{2m}, \delta_1, \ldots, \delta_{2n+1}$ we have

$$\sigma = \tau_1 \ldots \tau_{2m} = \delta_1 \ldots \delta_{2n+1}$$

We can write σ^{-1} as follows:

$$\sigma^{-1} = \tau_{2m}^{-1} \ldots \tau_1^{-1}$$

But, note that each $\tau_i^{-1} = \tau_i$, since τ_i is a transposition, and a transposition is its own inverse.

$$\implies \sigma^{-1} = \tau_{2m} \ldots \tau_1$$

Similarly, we have

$$\sigma^{-1} = \delta_{2n+1}.\ldots\delta_1$$

So, we have that

$$\mathrm{id} = \sigma\sigma^{-1} = \underbrace{\tau_1.\ldots\tau_{2m}\delta_{2n+1}.\ldots\delta_1}_{\text{odd number of transpositions}}$$

Thus, we have a way of writing the identity on an odd number of transpositions. Suppose k is the smallest positive odd number for which the product of k transpositions is the id. We see that $k \geq 3$.

$$\sigma = \rho_1.\ldots\rho_k$$

We let $\rho_1 = (a, b)$.

Note that a must appear in some ρ_i for $i > 1$, because otherwise a would get stuck and wouldn't map to a in id.

Among the products $\rho_1.\ldots\rho_k = \mathrm{id}$, let this expression have the fewest $\rho_1(a, \star)$ of a's in transposition (at least two a's we know from above!)

Let ρ_i with $i > 1$ be the leftmost such that $\rho = (a, c)$.

a, u, v, v distinct

$$(u, v)(a, r) = (a, r)(u, v)$$

$$(u, v)(a, u) = (a, u)(u, v)$$

$$\underbrace{(a, b)}_{\rho_1}.\ldots\underbrace{(a, c)}_{\rho_i}$$

Using relation $\star$, we have

$$\mathrm{id} = (a, c)(a, c')\rho'_3.\ldots\rho'_k$$

In the case that $b = c' \implies \mathrm{id} = \rho'_3.\ldots\rho'_k$, so we can write id as a product of $k-2$ transpositions, which is a contradiction to the minimality of k.

In the case that $b \neq c' \implies$

$$\mathrm{id} = (a, c')(b, c')\rho_3.\ldots\rho'_k$$

Which contradicts that we picked transpositions with the least number of a's.

So, in either case, we've reached a contradiction. So, we conclude that the lengths of the products of transpositions must have the same length.

$$QED$$

Definition: A permutation $\sigma \in S_n$ is called even when it can be written as a product of an even number of transpositions. A permutation $\sigma \in S_n$ is called odd when it can be written as a product of an odd number of transpositions. This notion is well-defined, as proven above.

Examples:

id is even. You can write it as $(1, 2)(1, 2)$. You can also write it as the empty composition!

(a_1, a_2, a_3) is even, you can write it as $(a_1, a_2)(a_2, a_3)$.