Lecture 12

In this lecture we'll prove several theorems about permutations and cycles.

Theorem 1 Let $\sigma \in S_n$. Then σ can be written as a cycle or as a product of disjoint cycles.

Proof The proof of this theorem is essentially the procedure of writing σ in the cycle notation which we saw in the last lecture.

We start with choosing any element $a_1 \in \{1, \dots, n\}$ and look at $\sigma(a_1) = a_2$ (say) and form $(a_1, a_2, \dots)$. Then we look at $\sigma(a_2) = a_3$. If $a_3 = a_1$ then we write (a_1, a_2) otherwise we write $(a_1, a_2, a_3 \dots)$. We carry on this procedure until we arrive at $\sigma(a_{m-1}) = a_1$.

We know this must happen because $\{1, 2, \dots, n\}$ is a finite set so we'll start getting repetitions. If we have exhausted all the elements of $\{1, 2, \dots, n\}$ then σ can be written as a cycle $(a_1, a_2, \dots, a_{m-1})$.

Otherwise, we pick any element b_1, not appearing in $(a_1, a_2, \dots, a_{m-1})$ and repeat the above procedure, i.e., we now form

$$(b_1, b_2, \dots, b_{k-1}).$$

Claim :- $(b_1, b_2, \dots, b_{k-1})$ will have no elements common with $(a_1, a_2, \dots, a_{m-1})$.

Proof of the claim Suppose $b_i = a_j$ for some i and j $\Rightarrow$ $\sigma^{i-1}(b_1) = \sigma^{j-1}(a_1)$

$\Rightarrow$ $b_1 = \sigma^{j-1-(i-1)}(a_1) = \sigma^{j-i}(a_1)$

$\Rightarrow$ $b_1 = a_t$ for some t which is a contradiction because b_1 was chosen so that it has not appeared in $(a_1, a_2, \ldots, a_{m-1})$.

Continuing this process, until we exhaust all the elements of A, σ will appear as

$$\sigma = (a_1, \ldots, a_{m-1})(b_1, \ldots, b_{k-1}) \cdots (c_1, \ldots, c_{n-1})$$

i.e., σ is written as a product of disjoint cycles.

$\boxed{///}$

We know that S_n, $\forall n \geq 3$ is non-abelian. But does any of it's elements commute?

<u>Theorem 2</u> (<u>Disjoint cycle commutes</u>)

Let $\alpha = (a_1, \ldots, a_m)$ and $\beta = (b_1, \ldots, b_k)$ be two disjoint cycles in S_n, i.e., they have no entries in common. Then $\alpha\beta = \beta\alpha$.

Proof This is left as an exercise. Just remember the group operation in S_n is composition of functions and $\alpha\beta$ and $\beta\alpha$ are bijective functions on $\{1, \ldots, n\}$.

$\blacksquare$

Theorem 3 (Order of any element in S_n)
Let $\sigma \in S_n$. Write σ as a product of disjoint cycles using Theorem 1. Then $\text{ord}(\sigma) =$ least common multiple of the length of the cycles.

Proof Let's first understand what are we trying to prove. If $\sigma = (a_1, \ldots, a_m)(b_1, \ldots, b_k)(c_1, \ldots, c_\ell)$
Then the Theorem is saying that

$$\text{ord}(\sigma) = \text{lcm}(m, k, \ell)$$

Let's prove this for any σ.

Observation 1 A cycle of length k has order k, i.e., if $(a_1, \dots, a_k)$ is a cycle then k is the least positive integer such that $(a_1 \cdots a_k)^k = \epsilon$, the identity permutation.

Verify the observation yourself.

Now suppose α is a cycle of length k and β is a cycle of length m which is disjoint from α. Let $l = \operatorname{lcm}(m, k)$. Then

$$\alpha^l = \beta^l = \epsilon, \text{ the identity permutation.}$$

Claim :- $\operatorname{ord}(\alpha\beta) = l$.

Proof of the claim Since α and β are disjoint, they commute $\Rightarrow$ $(\alpha\beta)^l = \alpha^l \beta^l = \epsilon$.

So we know from Lec. 10 that $\operatorname{ord}(\alpha\beta)$ say t, divides l, i.e., $t \mid l$. We want to prove $t = l$.

We have $(\alpha\beta)^t = \alpha^t \beta^t = \epsilon \Rightarrow \alpha^t = \beta^{-t}$.

But since α and β were disjoint so are

α^t and β^{-t}, so if they are equal then they must be the identity permutation ϵ because only then every symbol in α^t will be fixed by β^{-t} and vice-versa.

So $\alpha^t = \epsilon$ and $\beta^{-t} = \epsilon \Rightarrow \beta^t = \epsilon$.

$\Rightarrow$ $k \mid t$ and $m \mid t \Rightarrow l \mid t \Rightarrow t = l$.

So we proved the theorem in the case when σ is a single cycle or a product of two disjoint cycle. But from Theorem 1, σ can be written as a product of disjoint cycle and hence in a similar fashion, we can prove the theorem.

$\boxed{//}$

Before we move to any more theorems let's pause for a moment to appreciate the strength of Theorem 3.

Example 1 Suppose $\sigma \in S_8$ and can be written as $\sigma = (1\,2\,3)(5\,6)(4\,8)$

Note that $|S_8| = 8! = 40320$, so we know that $\operatorname{ord}(\sigma) \mid 40320$ but how to find it !!

Theorem 3 tells us that $\operatorname{ord}(\sigma) = \operatorname{lcm}(3,2,2)$ $= 6$, so simple.

Example 2 Consider S_7 whose order is 5040. We are interested in finding all the elements of order 3 in S_7. We know that if $\sigma \in S_7$ with $\operatorname{ord}(\sigma) = 3$, then in its cycle decompo-sition, it must have either one cycle of of length 3, say (a_1, a_2, a_3) or two cycles of lengths 3, say $(a_1, a_2, a_3)(a_4, a_5, a_6)$ as only in these cases the lcm will be 3.

In the (a_1, a_2, a_3) case there are $7.6.5$ choices but it is counting every element three times as e.g. (134), (341) and (413) are the same elements. So in S_7, the number of elements of the form $(a_1, a_2, a_3) = \frac{7.6.5}{3}$

$= 70.$

For elements of the form $(a_1, a_2, a_3)(a_4, a_5, a_6)$ there are $\frac{7.6.5}{3}$ choices for first and $\frac{4.3.2}{3}$

choices for the second. However, again every element is counted twice as $(a_1, a_2, a_3)(a_4, a_5, a_6)$ and $(a_4, a_5, a_6)(a_1, a_2, a_3)$ are the same element by Theorem 2. So in S_7, the number of elements of the form $(a_1, a_2, a_3)(a_4, a_5, a_6)$

$= \frac{70.8}{2} = 280.$

So, there are total $280 + 70 = 350$ elements of order 3 in S_7.

Exercise Find the number of elements of order 6 in S_7.

o ——————— x ——————— x ——————— o