Lecture 13

Recall the following definition from Lec. 11

Definition A cycle of length 2 is called a transposition.

We'll soon see that it is advantageous to write any permutation as a product of transpositions. So we first prove,

Theorem 1 Any cycle of length $r \geq 2$ can be written as a product of transpositions.

Proof Before proving this let's understand what the theorem is saying. Suppose we have a cycle $(1\,2\,3\,4\,5)$. We want to write it as a product of transpositions. How do we do this?

First of all we know that $1 \longrightarrow 2$, so we write (12). This is a transposition in which $1 \rightarrow 2$ and rest all the elements are fixed.

Now we want to multiply it with another transpositions so that we should move forward in expressing (12345). Since 1 is already mapped to 2 $\Rightarrow$ now we should worry about $2 \rightarrow 3$.

A naive guess would be to write (23). But observe that overall we'll have $(23)(12)$ which is telling us that $1 \rightarrow 3$ as first $1 \rightarrow 2$ (from (12)) and then $2 \rightarrow 3$ (from (23)) which is wrong. This can be remedied easily by writing $(13)(12)$ as now this is telling us that $1 \rightarrow 2$ (as $2 \rightarrow 2$ in (13)) and $2 \rightarrow 3$ (as $2 \rightarrow 1$ in (12) and $1 \rightarrow 3$ in (13)).

So we have got $1 \to 2$, $2 \to 3$ part in (12345). Now we want to take care of $3 \to 4$. This again can be taken care by multiplying (14) to $(13)(12)$. So finally we'll get

$$(12345) = (15)(14)(13)(12)$$

But there was nothing special about (12345). In fact, if we start with any cycle $(a_1, a_2, \dots, a_k)$ Then it can be written, using the same procedure as above, as

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

which completes the proof of the theorem.

$\boxed{\text{ph}}$

Theorem 2 Any $\sigma \in S_n$ can be written as a product of transpositions.

Proof Consider the identity $\epsilon \in S_n$. Then

$$\epsilon = (12)(12)$$

as $|(12)| = 2 \Rightarrow \epsilon$ can be written as a product of transpositions. Now the Theorem follows from Theorem 1 above and Theorem 1 in Lec. 12.

$\blacksquare$

Exercise Consider $(123)(456) \in S_8$. Write this as a product of transpositions.

Let's come back to the example in the proof of Theorem 1.

$$(12345) = (15)(14)(13)(12)$$

You can check that

$$(12345) = (45)(35)(25)(15)$$

Also, $(12345) = (45)(25)(12)(25)(23)(13)$

so, a permutation can be written as a product of transpositions in more than one way.

So what's the advantage?

Notice that the number of transpositions being used in all the representations of (12345) is even.

In fact, try to check the same thing for any other permutation and the number of transpositions required will be either even or odd. We'll prove this below, but first a Lemma.

Lemma If $\epsilon = \beta_1 \beta_2 \cdots \beta_r$ where β_i's are transpositions $\Rightarrow$ r is even.

Proof First of all $r \neq 1$ as a transposition $\neq$ identity. If $r = 2$, we are done. So suppose $r > 2$ and we proceed by induction, i.e., we know that if the # of transpositions is less than r then they are even. We want to show that r is even.

Let's look at $\beta_{r-1}\beta_r$, i.e. the rightmost 2 transpositions. Suppose $\beta_r = (ab)$. Then there are 4 choices for $\beta_{r-1}\beta_r$

1) $\beta_{r-1}\beta_r = (ab)(ab)$

2) $\beta_{r-1}\beta_r = (ac)(ab)$

3) $\beta_{r-1}\beta_r = (bc)(ab)$

4) $\beta_{r-1}\beta_r = (cd)(ab)$.

Case 1 If $\beta_{r-1}\beta_r = (ab)(ab) = \epsilon \Rightarrow$ we get
$\epsilon = \beta_1 \dots \beta_{r-2} \Rightarrow$ by Principle of Mathema-

-tical induction $r-2$ is even $\Rightarrow$ r is even.

Case 2 We are in any of the three cases above. The goal is to write them in such a way so that 'a' appears in the 1st spot of the left-most transposition. More precisely, write

$$(ac)(ab) = (ab)(bc) \quad \text{or}$$
$$(bc)(ab) = (ac)(cb) \quad \text{or}$$
$$(cd)(ab) = (ab)(cd)$$

So we can write $\epsilon = \beta_1\beta_2\dots\beta_{r-2}(ab)(bc)$ or $\epsilon = \beta_1\beta_2\dots\beta_{r-2}(ac)(cb)$ or $\epsilon = \beta_1\dots\beta_{r-2}(ab)(cd)$.

Repeat the same procedure with $\beta_{r-2}\beta_{r-1}$, then $\beta_{r-3}\beta_{r-2}$ ... $\beta_1\beta_2$.

Just like above we either get $(r-2)$ transpo-

-sitions $\Rightarrow$ r-even or $\epsilon =$ product of r transpositions with the only 'a' occuring on the first spot in the leftmost transposition, i.e.,

$$\epsilon = (ab)\beta_2 \cdots \beta_r$$

Now if LHS is $\epsilon \Rightarrow \beta_2$ must be (ab) otherwise $a \to b$ on the RHS but $a \to a$ in ϵ $\Rightarrow \epsilon = \beta_3 \cdots \beta_r$ which are $(r-2)$ transpositions $\Rightarrow r-2$ is even $\Rightarrow r =$ even.

$\boxed{//}$

Theorem 3 If $\sigma \in S_n$ can be written as a product of transpositions in more than one ways then the # of transpositions in the decomposition is either always even or always odd.

Proof Suppose $\sigma = \beta_1 \cdots \beta_r$ and $\sigma = \alpha_1 \cdots \alpha_s$. Then

$$\beta_1 \beta_2 \cdots \beta_r = \alpha_1 \alpha_2 \cdots \alpha_s$$

$$\Rightarrow \quad \epsilon = \alpha_1 \alpha_2 \cdots \alpha_s \beta_r^{-1} \beta_{r-1}^{-1} \cdots \beta_1^{-1}$$

now inverse of a transposition is the transposition itself (as $(ab)(ab) = \epsilon \Rightarrow (ab)^{-1} = (ab)$).

$$\Rightarrow \quad \epsilon = \alpha_1 \alpha_2 \cdots \alpha_s \beta_r \beta_{r-1} \cdots \beta_1$$

$\Rightarrow$ $r + s$ = even from the Lemma above

$\Rightarrow$ either both r and s are even or both are odd.

////

This theorem motivates the following definition.

Definition Even and odd permutation

A permutation that can be expressed as a product of an even number of transpositions is called an even permutation.

A permutation that can be expressed as a product of an odd number of transpositions is called an odd permutation.

So the Lemma is telling us that the identity permutation is an even permutation and Theorem 3 is telling us that the definition is unambiguous.

Theorem 4 The set of even permutations in S_n forms a subgroup of S_n called the alternating group on n symbols and is denoted by A_n.

Proof. Exercise.

We end with finding the order of A_n.

Theorem 5 For $n > 1$, $|A_n| = \frac{n!}{2}$.

Proof Exercise.

Hint :- Prove that the number of even permutations in S_n = the number of odd permuations in S_n.

So $\#(\text{even permutations}) + \#(\text{odd permutations}) = n!$

$\Rightarrow \; 2\,\#(\text{even permutations}) = n!$

$\Rightarrow \; |A_n| = \dfrac{n!}{2}$

$\square$