Lecture 11

(11.0) Recall S_n = group of permutations of $\{1, \dots, n\}$

$$|S_n| = n!$$

The aim of today's lecture is to prove:

- existence of sign: $S_n \longrightarrow \{\pm 1\}$ group hom.
- simplicity of A_n (for $n \geq 5$).

(11.1) Some easy facts about S_n.

Definition (r-cycle) $\gamma = (i_1, \dots, i_r) \in S_n$ if

$$\gamma(i_1) = i_2 \; ; \; \gamma(i_2) = i_3 \; ; \; \dots \; ; \; \gamma(i_{r-1}) = i_r \; ; \; \gamma(i_r) = i_1$$

$$\gamma(j) = j \quad \forall \; j \in \{1, \dots, n\} \setminus \{i_1, \dots, i_r\}$$

In other words, for γ acting on the set $X = \{1, \dots, n\}$ there is one orbit containing r elements and $n-r$ orbits each with only one element ($X^\gamma = X - \{i_1, \dots, i_r\}$).

The order of an r-cycle is r.

Prop. Let $\pi \in S_n$ and $\gamma = (i_1, \dots, i_r)$ be an r-cycle.

Then $\pi\gamma\pi^{-1} = (\pi(i_1), \ldots, \pi(i_r))$

Proof. An easy direct verification. Let $j = \pi(k) \in X$.

$k \in \{i_1, \ldots, i_r\}$; say $k = i_s$. Then $\pi\gamma\pi^{-1}(j) = \pi(i_{s+1})$. ($\uparrow$ mod r)

$k \notin \{i_1, \ldots, i_r\}$. Then $\pi\gamma\pi^{-1}(j) = \pi(k) = j$ □

Cor. (i) Disjoint cycles commute.

(ii) Every $\pi \in S_n$ can be written (uniquely up to reordering) as a product of disjoint cycles.

$$\pi = \gamma_1 \cdots \gamma_\ell : \begin{cases} \text{each } \gamma_j \text{ is an } r_j\text{-cycle} \\ \text{mutually disjoint (hence commuting)} \\ \sum_{j=1}^{\ell} r_j = n \end{cases}$$

$$\text{ord}(\pi) = \text{l.c.m.}\ (r_1, \ldots, r_\ell)$$

One usually orders $\{r_1, \ldots, r_\ell\}$ is a decreasing order.

The resulting sequence of numbers is called a <u>partition of n</u>

$$\text{Partitions of } n = \left\{ \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_\ell > 0 \text{ such that } \lambda_1 + \cdots + \lambda_\ell = n \right\}$$

(iii) Conjugacy classes in S_n $\longleftrightarrow$ Partitions of n

$\Downarrow$

$\{$ permutations with cycle lengths $\lambda_1, \dots, \lambda_\ell$ $\}$ $\longleftrightarrow$ $(\lambda_1 \geq \dots \geq \lambda_\ell)$

$\|$

Conjugates of $(1, 2, \dots, \lambda_1)(\lambda_1+1, \dots, \lambda_1+\lambda_2)\cdots$

(11.2) Cycles of length 2 are called <u>transpositions</u>.

There are $\binom{n}{2}$ transpositions in S_n; namely

$\{(a\ b) : 1 \leq a < b \leq n\}$.

For $1 \leq i \leq n-1$, $s_i = (i\ i+1)$ are often called simple transpositions.

Proposition. Every permutation can be written as a product of (simple) transpositions. (<u>NOT</u> disjoint).

Remark: not uniquely, e.g.

$$(1\ 3) = (12)(23)(12) = (23)(12)(23)$$

Proof. It is enough to prove this for an r-cycle (by Cor (11.1) (ii))

$$(a_1\ a_2 \cdots a_r) = (a_1\ a_2)\ (a_2\ a_3) \cdots (a_{r-1}\ a_r)$$

Now we claim that every transposition can be written in terms of simple transpositions. We argue by induction on $b-a$, for a transposition $(a\ b)$. $b-a = 1$ means it is simple. $[a < b]$

Otherwise $(a\ b) = (b-1\ b)\ (a\ b-1)\ (b-1\ b)$

and the claim follows by induction. □

(11.3) Theorem. Let $\pi \in S_n$ and assume there are two ways of writing π as a product of transpositions

$$\pi = \tau_1 \cdots \tau_p = \tau_1' \cdots \tau_q'$$

Then $p \equiv q \pmod 2$.

Proof. For any permutation $\sigma \in S_n$, write σ as product of disjoint cycles (unique up to reordering these mutually commuting cycles).

$$\sigma = \sigma_1 \cdots \sigma_\ell \qquad \sigma_j \text{ is an } r_j\text{-cycle.}$$

Define $N(\sigma) = \sum_{j=1}^{\ell} (r_j - 1)$

Now for $\pi \in S_n$, if $\pi = \tau_1 \cdots \tau_p$ is a way of writing π as a product of transpositions.

Claim. $p \equiv N(\pi) \pmod 2$

Theorem follows from this claim.

Proof of Claim: Note that we have the following identity

$\forall\, k, l \geq 0$; $(a\, c_1\, c_2 \cdots c_k\, b\, d_1 \cdots d_l) = (ab)(b\, d_1 \cdots d_l)(a\, c_1 \cdots c_k)$

$$\Rightarrow N((a\,b)\cdot\sigma) = \begin{cases} N(\sigma)+1 & \text{if } a, b \text{ lie in same cycle of } \sigma \\ N(\sigma)-1 & \text{o/w} \end{cases}$$

Now we can prove the claim by induction on p.

$p=0$. $\Rightarrow \pi = e$ and $N(e) = 0$.

$p>1$. Let $\pi' = \tau_1 \pi = \tau_2 \cdots \tau_p$. By induction

$$N(\pi') \equiv p-1 \pmod 2$$

But $N(\pi') = N(\pi) \pm 1$. So we get $N(\pi) \equiv p \pmod 2$ □

Cor. We have a group hom. uniquely determined by

$$\text{sign}((a\,b)) = -1 \;;\; \text{sign}: S_n \longrightarrow \{\pm 1\}$$

(11.4) $A_n := \mathrm{Ker}(\mathrm{sign})$

Note: $A_2 = \{e\}$; $A_3 \simeq \mathbb{Z}/3\mathbb{Z}$ $(= \langle (123) \rangle)$

Lemma. (i) For $n \geq 3$, A_n is generated by 3-cycles.

(ii) For $n \geq 5$, all 3-cycles are conjugate to each other in A_n.

Proof (i) Since $(a\ b\ c) = (a\ b)(b\ c)$ is even, it is in A_n. Conversely every $\sigma \in A_n$ can be written as even number of transpositions, hence in terms of 3-cycles because:

$$(a\ c)(a\ c) = e$$
$$(a\ c)(a\ b) = (a\ b\ c)$$
$$(a\ b)(c\ d) = (a\ b\ c)(b\ c\ d)$$

(ii) Let $(a_1\ a_2\ a_3)$ and $(b_1\ b_2\ b_3)$ be two 3-cycles.
We know $\exists\ \gamma \in S_n$ s.t. $\gamma(a_1\ a_2\ a_3)\gamma^{-1} = (b_1\ b_2\ b_3)$.
If γ is even, there is nothing to prove. If γ is odd, pick $c, d \notin \{b_1, b_2, b_3\}$ (since $n \geq 5$). Then $(c \neq d)$

$$[(c\ d)\gamma]\ (a_1\ a_2\ a_3)\ [\gamma^{-1}(c\ d)] = (b_1\ b_2\ b_3)$$

$[(c\ d)\gamma]$ ↑ even $\in A_n$.

□

(11.5) Theorem. A_n is simple for $n \geq 5$.

Proof. Let $K \triangleleft A_n$ (normal), $K \neq \{e\}$. Let us choose $\sigma \in K$ $(\sigma \neq e)$ for which $X^\sigma = \{x \in \{1, \dots, n\} : \sigma(x) = x\}$ ("x") has maximum cardinality.

Claim. σ is a 3-cycle.

So K has a 3-cycle in it. As it is normal, it contains all 3-cycles (Lemma 11.4 (ii)) and hence $K = A_n$ (Lemma 11.4 (i)).

Proof of the claim. Write σ as a product of disjoint cycles.

- σ has a cycle of length ≥ 3.

  $\sigma = (a_1\ a_2\ a_3 \dots) \dots$. If $\sigma = (a_1\ a_2\ a_3)$ we are done.

Otherwise, there are a_4, a_5 s.t. $\sigma(a_4) \neq a_4$, $\sigma(a_5) \neq a_5$.

Let $\tau = (a_3\ a_4\ a_5)$ and $\sigma' = \tau\sigma\tau^{-1}\sigma^{-1} \in K$.

Check: $X^{\sigma'} \supset X^\sigma$ and $a_2 \in X^{\sigma'}$, $a_2 \notin X^\sigma$

$\Rightarrow |X^{\sigma'}| > |X^\sigma|$ contradiction.

- All cycles in σ are transpositions (at least 2)

  $\sigma = (a\ b)(c\ d) \dots$

Take $k \notin \{a, b, c, d\}$ (as $n \geq 5$ such k exists).

$\tau := (c\ d\ k)$ $\quad \sigma' := \tau \sigma \tau^{-1} \sigma^{-1} \in K$

Check: $X^{\sigma'} \supset X^{\sigma} \setminus \{k\}$; $a, b \in X^{\sigma'}$; $a, b \notin X^{\sigma}$

Again we get $|X^{\sigma'}| > |X^{\sigma}|$ a contradiction. □