Math 322, Lecture 5, 21/9/2014

Last time: $S_X = \{ \sigma: X \rightarrow X \mid \sigma \text{ bijective} \}$

$S_n = S_{3,2,\ldots,n}$

$r$-cycle $(i_1, i_2, \ldots, i_r)$ is the map $\rho(c) = \{ \begin{array}{ll}
    i_{j+1} & \text{if } c = i_j, \ j < r \\
    i_r & \text{if } i = i_j, \ j \neq r
\end{array}$

Every $\sigma \in S_n$ is of the form $\sigma = \prod K_j$, $K_j$ disjoint cycles, unique up to reordering.

Proof: For $i, j \in \{1, 2, \ldots, n\}$ set $i \leftrightarrow j$ if $i = c^{k_j}(j)$ for some $k \in \mathbb{Z}$

Check:
1. is an equivalence relation
2. each class is $\sigma$-invariant: if $i \in$ class, $\sigma(i)$ also true
3. Define cycle $\sigma$ by restricting $\sigma$ to classes

Example: $(1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 7) \\
(6 \ 3 \ 2 \ 1 \ 5 \ 7 \ 4)$

Today:
1. sign of a permutation
2. linear groups

Odd and even permutations

Lemma: Every permutation is a product of 2-cycles ("transpositions")

[$\text{the transpositions generate } S_n$]
Pf: let \( \sigma \in S_n \) be a counterexample of minimal support. 
\( \sigma \neq \text{id} \) (\( \text{id} = (1) \)) so \( \text{supp}(\sigma) \neq \emptyset \). Say \( i \in \text{supp}(\sigma) \) 
Consider permutation \( \tau = (i \ \sigma(i)) \sigma \) (apply \( \sigma \), swap \( i, \sigma(i) \)) 
\( \neq \sigma(i) \) since \( i \in \text{supp}(\sigma) \) 
If \( j \notin \text{supp}(\sigma) \) then \( j \neq i, j \neq \sigma(i) \) so \( \tau(j) = (i \ \sigma(i))(\sigma(j)) = (i \ \sigma(i))(j) = j \) 
also, \( \tau(i) = (i \ \sigma(i))(\sigma(i)) = i \) so \( i \notin \text{supp}(\tau) \) 
so \( \text{supp}(\tau) \subseteq \text{supp}(\sigma) \setminus \{i\} \) 
so \( \tau \) is a product of transpositions: \( \tau = \prod \beta \). 
Then \( (i \ \sigma(i)) \cdot \sigma = \prod \beta \). 
Then \( (i \ \sigma(i))^2 \sigma = (i \ \sigma(i)) \cdot \prod \beta \)
\( (\text{let } \beta = (i \ \sigma(i)) = 1 \) then let \( \tau = \beta \sigma \), for \( j \notin \text{supp}(\sigma) \), \( \tau(j) = j \) 

PF: know \( \sigma \in S_n \) is a product of cycles enough to show each cycle is a product of transpositions. 
By induction: \( (i_1, \ldots, i_r) = (i_1, i_2) (i_2, i_3) (i_3, i_4) \cdots (i_{r-1}, i_r) \) 

Def: The alternating group \( A_n \) is the set of \( n \)-elements that are the product of an even number of transpositions (those permutations are said to be "even")

Remark: If \( \sigma, \tau \in A_n \), so do \( \sigma \tau, \sigma^{-1} \) (concatenate or reverse even products keeps them even)
Lemma: Let $1 \leq k \leq n$ then in $S_n$

$$(a, a_k)(a, \ldots, a_n) = (a, \ldots, a_{k-1})(a_k \ldots a_n)$$

(if $k = 1$ or $a_k$ is the identity)

$$(a, a_k)(a, \ldots, a_{k-1})(a_k \ldots a_n) = (a, \ldots, a_n)$$

Pf: 1st by direct evaluation

2nd follows by multiplying by $(a, a_k)$ on left, using $(a, a_k)^2 = id$

Def: For $\sigma \in S_n$, let $\sigma = \prod_{j=1}^{t} k_j$ be the cycle decomposition of $\sigma$ (add a 1-cycle for each fixed point)

Set $sgn(\sigma) = (-1)^{n-t}$ call it the sign of $\sigma$.

Key lemma: Let $\tau$ be a transposition. Then

$$sgn(\tau \sigma) = -sgn(\sigma)$$

Pf: Say $\tau = (a, a_k)$ either, $a, b a_k$ both in same cycle for $\tau$ or they are in different cycles (if only one, assume its $k_1$, if two assume its $k_1, k_2$)

Lem: previous lemma: in either case, # of cycles in $\tau \sigma$ changes by one

(in case 1, $\tau \sigma = (a, \ldots, a_{k-1})(a_k \ldots a_n)(k_2 k_3 \ldots k_t$)

2. $\tau \sigma = (a, \ldots, a_n \cdot k_3 k_4 \ldots k_t$)
Thm: For all \( \sigma, \tau \in S_n \), have \( \text{sgn}(\sigma \tau) = \text{sgn}(\sigma) \text{sgn}(\tau) \).

[Interpretation: map \( \text{sgn} : S_n \to \mathbb{Z}/2\mathbb{Z} \) respects multiplication.]

Pf: By lemma showed \( \text{sgn}(\tau \sigma) = \text{sgn}(\tau) \text{sgn}(\sigma) \) if \( \tau \) is a transposition.

Set \( H = \{ \tau \in S_n : \text{sgn}(\tau \sigma) = \text{sgn}(\tau) \text{sgn}(\sigma) \} \).

We know \( H \) contains all transpositions. Also, if \( \tau, \tau_1 \in H \) then \( \tau, \tau_1 \in H \) because for all \( \sigma \):

\[
\text{sgn}(\tau_1 \tau \sigma) = \text{sgn}(\tau_1 \tau_2 \sigma) = \text{sgn}(\tau_1) \text{sgn}(\tau_2 \sigma) = \uparrow \uparrow \text{sgn}(\tau_1) \text{sgn}(\tau_2) \text{sgn}(\sigma) = \text{sgn}(\tau_1 \tau_2) \text{sgn}(\sigma).
\]

But every element of \( S_n \) is a product of transpositions, so \( H = S_n \).

Cor.: Suppose \( \sigma = \prod_{j=1}^{S} \tau_j \), \( \tau_j \) are transpositions.

Then \( \text{sgn}(\sigma) = \text{sgn}(\prod_{j=1}^{S} \tau_j) = \prod_{j=1}^{S} \text{sgn}(\tau_j) = (-1)^S \).

So parity of \( S \) depends only on \( \sigma \).

Cor: \( \#A_n = \frac{1}{2} \#S_n \).

Pf: Let \( \tau \) be a transposition. Then \( \tau \) multiplies \( A_n \) by \( S_n \). \( A_n \) multiplies \( S_n \) by \( A_n \).

Eq: Saw that \( n \)-cycle has \( \text{sgn}(-1) \).

Show \( A_n \) is generated by \( 3 \)-cycles (\( n \geq 3 \)).