Lecture 20: odd and even permutation. Order of a permutation.

Wednesday, November 19, 2014
9:15 AM

<u>Theorem</u>. If $\tau_1 \circ \cdots \circ \tau_r = \tau_1' \circ \cdots \circ \tau_s'$ and τ_i, τ_j' are transpositions (2-cycles), then $r \equiv s \pmod 2$.

<u>Pf</u>. $\tau_1 \circ \cdots \circ \tau_r = \tau_1' \circ \cdots \circ \tau_s' \Rightarrow$

$$\tau_1 \circ \cdots \circ \tau_r \circ \tau_s' \circ \cdots \circ \tau_1' = \mathrm{id}.$$

It is enough to show: identity cannot be written as a product of odd many transpositions.

[If we show this, then $2 \mid r+s \Rightarrow r \overset{2}{\equiv} s$.]

So suppose $\tau_1'' \circ \cdots \circ \tau_\ell'' = (1)$ for some transpositions τ_i''.

We introduce a process which at each step changes a decomposition of (1) to transpositions to another such decomp. <u>without changing the parity</u> of the number transpositions.

Our goal is to end up with <u>zero</u> transposition, to conclude that $2 \mid \ell$. To this end, it is enough to <u>get rid</u> of all the numbers that can appear in the transpositions:

all the numbers that can appear in the transpositions:

if no number $1 \le a \le n$ appears among the transpositions, there is NO transposition !

<u>First</u>. Move all the transpositions that have a to the left.

$$(y,z)(a,x) = (a,x)(y,z)$$

$$(x,y)(a,x) = (a,y)(x,y)$$

<u>Second</u>. Reduce the number appearance of a.

$$(a,x)(a,x) = (1)$$

$$(a,x)(a,y) = (a,y)(y,x)$$

<u>Third</u> When the process stopped, there is no a left: If there are two a's we can use 2^{nd} step (after moving them to left if needed.)

If there is only one a, then

$$(1) = (a,x)\,\sigma \qquad \text{s.t. } \sigma(a) = a$$

$\Rightarrow \quad a = (a,x)\,\sigma\,[a] = x$ which is a contradiction $\square$

<u>Def</u> ① A permutation is called <u>odd</u> if it can be written a product of <u>odd many transpositions</u>. Otherwise it is called <u>even</u>.

② The sign $\mathrm{sgn}(\sigma)$ of a permutation is

$$\mathrm{Sgn}(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ is even} \\ -1 & \text{if } \sigma \text{ is odd}. \end{cases}$$

<u>Cor.</u> $\mathrm{sgn} : S_n \to \{\pm 1\}$ is a group homomorphism. I.e.

① $\mathrm{sgn}(\sigma_1 \sigma_2) = \mathrm{sgn}(\sigma_1)\,\mathrm{sgn}(\sigma_2)$

② $\mathrm{sgn}(\sigma^{-1}) = \mathrm{sgn}(\sigma)^{-1} = \mathrm{sgn}(\sigma)$.

<u>Pf</u>. By the definitions we have $\mathrm{sgn}(\tau_1 \cdots \tau_\ell) = (-1)^\ell$ if τ_i's are transpositions.

In particular, if $\sigma_1 = \tau_{11} \cdot \tau_{12} \cdot \ldots \cdot \tau_{1n_1}$

and $\sigma_2 = \tau_{21} \cdot \tau_{22} \cdot \ldots \cdot \tau_{2n_2}$,

where τ_{ij}'s are transpositions, then

$$\operatorname{sgn}(\sigma_1\sigma_2) = \operatorname{sgn}(\tau_{11}\cdot\dots\cdot\tau_{1n_1}\cdot\tau_{21}\cdot\dots\cdot\tau_{2n_2})$$

$$= (-1)^{n_1+n_2} = (-1)^{n_1}\cdot(-1)^{n_2}$$

$$= \operatorname{sgn}(\tau_{11}\cdot\dots\cdot\tau_{1n_1})\cdot\operatorname{sgn}(\tau_{21}\cdot\dots\cdot\tau_{2n_2})$$

$$= \operatorname{sgn}(\sigma_1)\cdot\operatorname{sgn}(\sigma_2).$$

If $\sigma = \tau_1\cdot\dots\cdot\tau_\ell$, then $\sigma^{-1} = \tau_\ell^{-1}\cdot\dots\cdot\tau_1^{-1}$

$$= \tau_\ell\cdot\dots\cdot\tau_1$$

$$\operatorname{sgn}(\sigma) = \operatorname{sgn}(\tau_1\cdot\dots\cdot\tau_\ell)$$

$$= (-1)^\ell$$

$$= \operatorname{sgn}(\tau_\ell\cdot\dots\cdot\tau_1)$$

$$= \operatorname{sgn}(\sigma^{-1}).$$ □

<u>Def/Cor.</u> $A_n := \{\sigma\in S_n \mid \sigma \text{ is even}\}$ is a subgroup of S_n. And it is called the alternating group on n elements.

<u>Pf</u>. $(1)\in A_n$;

$$\sigma_1,\sigma_2\in A_n \Rightarrow \operatorname{sgn}(\sigma_1) = \operatorname{sgn}(\sigma_2) = 1$$

$$\Rightarrow \operatorname{sgn}(\sigma_1\sigma_2^{-1}) = \operatorname{sgn}(\sigma_1)\operatorname{sgn}(\sigma_2^{-1})$$

$$= \operatorname{sgn}(\sigma_1)\operatorname{sgn}(\sigma_2)^{-1}$$

$$= 1.$$

$$\Rightarrow \sigma_1 \sigma_2^{-1} \in A_n. \quad \blacksquare$$

<u>Proposition.</u> $[S_n : A_n] = 2 \Rightarrow |A_n| = n!/2$.
(if $n \geq 2$)

<u>Pf.</u> $(1,2) \notin A_n \Rightarrow (1,2) A_n \neq A_n$.

$$\sigma \notin A_n \Rightarrow \operatorname{sgn}(\sigma) = -1 \Rightarrow \operatorname{sgn}((1,2)\sigma) = (-1)(-1)$$
$$= 1.$$

$$\Rightarrow (1,2)\sigma \in A_n.$$

$$\Rightarrow (1,2) A_n = \sigma A_n.$$

$$\Rightarrow S_n/A_n = \{A_n, (1,2)A_n\}.$$

By Lagrange theorem, $|S_n| = |A_n| [S_n : A_n]$

$$\Rightarrow |A_n| = n!/2. \quad \square$$

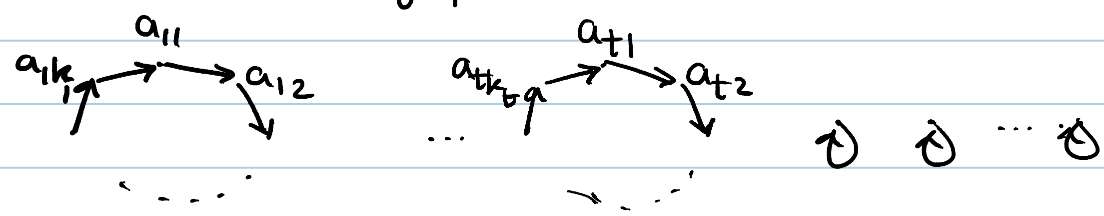
Let me finish by discussing the order of a permutation.

<u>Proposition.</u> Let $\sigma = c_1 \circ \cdots \circ c_t$ be the decomposition of σ to disjoint cycles. Then

$$o(\sigma) = \operatorname{lcm}(\ell(c_1), \ldots, \ell(c_t)).$$

Pf. We have proved that, if $c_i = (a_{i1}, a_{i2}, \dots, a_{ik_i})$,

then the Schreier graph of $\langle \sigma \rangle$ on $\{1, \dots, n\}$ is



And these also give us <u>the orbits</u> of this action.

$\Rightarrow$ $k_i \mid |\langle \sigma \rangle| = o(\sigma)$

$\Rightarrow$ $\operatorname{lcm}(k_1, \dots, k_t) \mid o(\sigma)$. I

On the other hand, since c_i's are disjoint, they commute. Thus $\sigma^d = c_1^d \circ \dots \circ c_t^d$.

$\Rightarrow$ if $d = \operatorname{lcm}(\ell(c_1), \dots, \ell(c_t))$, then

$c_i^d = (1) \Rightarrow \sigma^d = (1)$

$\Rightarrow o(\sigma) \mid \operatorname{lcm}(k_1, \dots, k_t)$. II

I, II $\Rightarrow$ ✓ ∎

Exp. How many elements of S_5 have order 3?

Solution. The size of <u>cycles</u> in the cyclic decomposition of such σ should be 3. They should add up to ≤ 5.

$\Rightarrow$ only a cycle of size 3

$\Rightarrow \quad 5 \times 4 \times 3 / 3 = 20.$

Exp. How many elements of S_6 have order 3?

Solution. As before it is either a 3-Cycle or a product of two disjoint 3-cycles.

There are $6 \times 5 \times 4 / 3 = 40$ 3-cycles

For any give 3-cycle $\underline{c}$, there are only two 3-cycles c' s.t. c and c' are disjoint.

$$\Rightarrow \left[\underbrace{(6 \times 5 \times 4 / 3)}_{\substack{\text{First} \\ \text{3-cycle}}} \underbrace{(2)}_{\substack{\text{Second} \\ \text{disjoint} \\ \text{3-cycle}}} \right] / \underbrace{2}_{\text{they commute}}$$

$$= 40$$

So overall there 80 such elements.