Lecture 21:

Last time: we proved that a permutation is either
even or odd but $\boxed{\text{not}}$ both.

product of an even # of transpositions

product of an odd number of transpositions.

"alternating group"

Def: $A_n \leq S_n$ is the subgroup of even permutations.

Ex: $(123) = (12)(23)$ is even

$(1234) = (12)(23)(34)$ is odd.

$(12\ldots k)$ is even if k is odd.
odd if k is even.

Remark: $|A_n| = \dfrac{n!}{2}$

why?: Consider the map $f: A_n \to O \subset S_n$
given by $f(\sigma) = (12)\sigma$ where O is the
subset (not subgroup) of odd permutations.
f is a bijection since it has an inverse
$f^{-1}(\sigma) = (12)\sigma$ because $f \circ f^{-1}(\sigma) = (12)(12)\sigma$
$= \sigma$
$f^{-1} \circ f(\sigma) = (12)(12)\sigma = \sigma$.

So # of even permutations is equal to the # of odd
permutations $|A_n| = |O|$. So $|A_n| = \dfrac{|S_n|}{2} = n!/2$

15-Puzzle:

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

. 16 is empty.

. each time you slide a square in the place of 16, swapping its number with 16.

Say somebody gave us a 15-puzzle with 14 and 15 swapped. Is it possible to get the puzzle back to original order by sliding the squares?

No. Consider the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & \dots & 13 & 14 & 15 & 16 \\ 1 & 2 & 3 & 4 & \dots & 13 & \underline{15} & \underline{14} & 16 \end{pmatrix} = \sigma_0$

we want to apply transpositions involving 16 to it and get the identity. ← "sliding squares to empty space".

But since 16 must go back to the end, every sequence of transpositions we apply will be even.

Hence we can only apply odd permutations.

So we can only do $\tau \cdot \sigma_0 \neq 1$ ← even permutation

τ: even # of transpositions.

σ_0: odd permutation

Tidbits:

- Cayley's theorem (in earlier lecture notes) in more detail.

Every finite group is isomorphic to a subgroup of S_n for some n.

proof: Let G be finite Let $\cancel{\#}(S_n =) S_G$ permutations of the set G without the binary operation.

$n = |G|$

be the S_n we are considering.

define $\varphi : G \longrightarrow S_G$ by

$$\varphi(g) = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ gg_1 & gg_2 & \cdots & gg_n \end{pmatrix}$$

$\varphi(g) \in S_G$ ($\varphi(g)$ is an isomorphism)

because $(\varphi(g) \circ \varphi(g^{-1}))(g_i) = gg^{-1}g_i = g_i$

so $\varphi(g) \circ \varphi(g^{-1}) = id$

Same for $\varphi(g^{-1}) \circ \varphi(g)$ so $\varphi(g)$ has an inverse.

- φ is a homomorphism:

$$\varphi(g) \circ \varphi(h) = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ gg_1 & gg_2 & \cdots & gg_n \end{pmatrix} \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ hg_1 & hg_2 & \cdots & hg_n \end{pmatrix}$$

$$= \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ ghg_1 & ghg_2 & \cdots & ghg_n \end{pmatrix} = \varphi(gh).$$

- φ is injective:

Suppose $\varphi(g) = \varphi(h)$, then $\varphi(g)(g_1) = \varphi(h)(g_1)$

$$gg_1 = hg_1$$

so $g = h$.

We are done by the following lemma.

Lemma: Let $\varphi: G \to K$ be a group homomorphism. Then, for every subgroup $H \subset G$, $\varphi(H)$ is a subgroup.

proof: We need to show that:

- $e \in \varphi(H)$. True since $\varphi(e) = e$.
- $\varphi(H)$ is closed under the group operation. True since $\varphi(h_1) \cdot \varphi(h_2) = \varphi(h_1 h_2)$
- $\varphi(H)$ is closed under taking inverses: True since $\varphi(h)^{-1} = \varphi(h^{-1})$.

$\square$