Now we prove that

Theorem: Every two ways of decomposing a permutation π into transpositions have the same parity

Proof: Suppose $\pi = \tau_r \tau_{r-1} \cdots \tau_2 \tau_1 = \sigma_s \sigma_{s-1} \cdots \sigma_2 \sigma_1$

Obs1: $C(\tau_i) = \underbrace{(n-2)}_{} + 1 = n-1$

$\uparrow$
(n−2) size one cycles

Obs2: As we multiply $\tau_1, \tau_2, \cdots$ etc we add or delete cycles one at a time

$\Rightarrow$ Say we go up g times
go down h times

$\Rightarrow C(\pi) = C(\tau_1) + g - h = (n-1) + g - h$

Obs3 Note $g + h = r - 1$

so putting together $r = 1 + g + h = 1 + g + (n - 1 + g - C(\pi))$
$= n - C(\pi) + 2g$

Same thinking can be done with σ's, $s = n - C(\pi) + 2g'$

$\Rightarrow r - s = 2(g - g') \Rightarrow r \equiv s \pmod 2$

$\Rightarrow$ same parity

NOTE: $n - C(\pi)$ has same parity as r (or s)
This is useful to compute parity

Definition: We say a permutation is EVEN (or ODD) depending if the number of transpositions in any of its decompositions.

The **sign** of a permutation π, $sgn(\pi) = (-1)^r$
where $r = \#$ of transpositions in any of its decompositions

Definition: The set of all EVEN permutations is A_n = ALTERNATING GROUP

This is an important example of a SUBGROUP of S_n

Definition; We say $H \subseteq S_n$ is a subgroup of permutations if

(a) H is closed under composition
(b) $id \in H$
(c) if $\pi \in H \Rightarrow \pi^{-1} \in H$.

Lemma: The Alternating Group (deserves its name!) is a subgroup

proof: The composition of even permutations is even Because

$sgn(\pi\sigma) = sgn(\pi) sgn(\sigma)$
$sgn(id) = 1 \Rightarrow id$ is even

Finally $sgn(\pi\pi^{-1}) = id \Rightarrow$ if π even π^{-1} even as well.

Proposition; For even n, half of the permutations in S_n are even, half are odd

proof $\longrightarrow$

proof: let $\pi_1, \pi_2, \ldots, \pi_m$ are all EVEN permutations.

Pick any transposition. Note that $\tau\pi_i \neq \tau\pi_j$

$\Rightarrow \tau\pi_1, \tau\pi_2, \ldots, \tau\pi_m$ are all ODD permutations

Now any odd permutation is image of this map

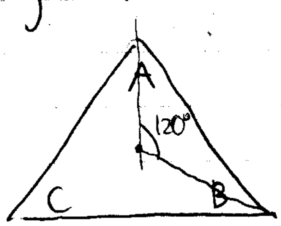
σ odd, $\tau^{-1}\sigma = \pi_j$ for some $j \Rightarrow \sigma = \tau\pi_j$

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

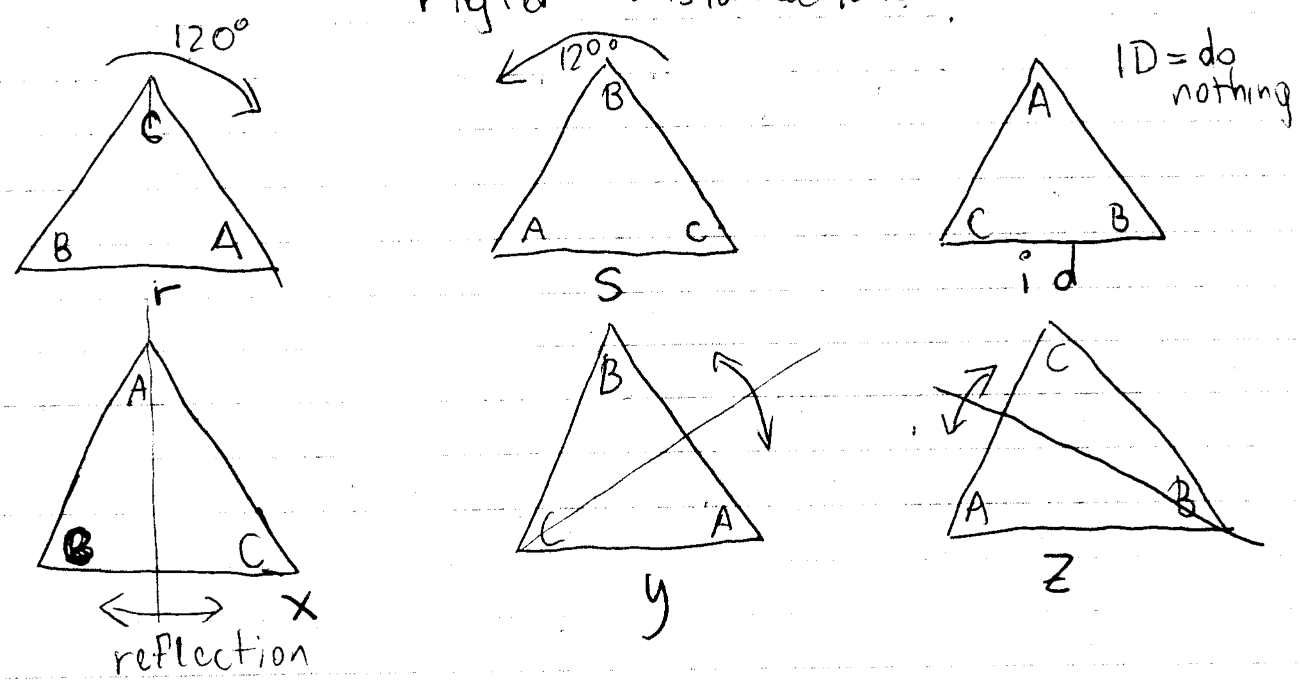
FROM NOW ON WE ARE DYING TO FIND MORE EXAMPLES OF SUBGROUPS OF PERMUTATIONS!

EXAMPLES OF GROUPS OF PERMUTATIONS

A) Symmetries of an Equilateral triangle:



Think of it as a flat piece of cardboard we label the corners, what are the permutations coming rigid transformations?



EXAMPLE: 15-PUZZLE

A =

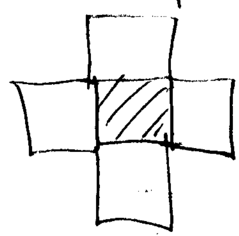
1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

? can one do moves and **get** NO why?

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

= B

Physical move slide square down or up, left or right to the empty space.



Each move gives a TRANSPOSITION of the 16 symbols (empty square counted as a symbol)

Definition: Let P_{15} = { set of all permutations one can have by a product composition of finitely moves that leave the ▨ block back in original position.

Lemma: This is a subgroup of permutations.

proof: id is in P_{15} = do nothing

if $\pi \in P_{15}$ $\quad \pi = \sigma_s \sigma_{s-1} \cdots \sigma_1$ ← legal 15-puzzle transpositions

Each move can be undone!

$$\sigma_1^{-1} \cdots \sigma_{s-1}^{-1} \sigma_s^{-1}$$

if $\pi, \gamma \in P_{15} \Rightarrow \pi \circ \gamma \in P_{15}$ because we can pick up to where we left off.

Lemma: All permutations inside Π_5 are even

why? (you move ▨ back to where it began)

So impossible to go from A to B because of lemma, B is an odd permutation.

IN FACT one can prove

Theorem: Every even permutation of the 15-puzzle initial configuration is reachable

$\Rightarrow P_{15} = A_{15}$

Definition: We say that a finite set of permutations $\pi_1, \dots \pi_r$ GENERATES a subgroup of permutations S if $\forall \gamma \in S, \quad \gamma = \pi_{i_1} \pi_{i_2} \cdots \pi_{i_\ell}$

Example: A_n is generated by id, pairs of transpositions,

Lemma: 3-cycles generate A_n (well 3-cycles + id)

why? $(a,b)(c,d) = (a,b,c)(a,d,c)$

$(a,b)(b,c) = (a,c,b)$

$(a,b)(a,b) = id$

Lemma: (In Homework): A 3-cycle is consecutive if it is of the form $(k, k+1, k+2)$. The consecutive 3-cycles and the identity generate A_n

proof: By induction on n. True for $n \le 4$

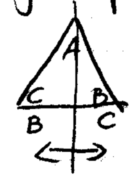
Assume true for $n-1$ take A_n. By induction

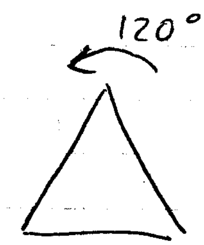
Definition: Let $H \leq G$ be a subgroup
The LEFT COSET of H with respect to $g \in G$

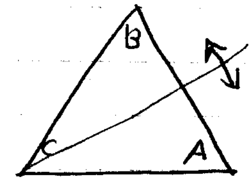
$$gH = \{ x \in G \mid x = gh \,,\ h \in H \}$$

Lemma: Any coset of a finite subgroup H of a finite group has the same cardinality as H

Why? suppose $gh_1 = gh_2 \Rightarrow h_1 = h_2$
$\Rightarrow$ One element inside gH for each element of H.

Example: Let G be the group of symmetries of $\triangle$. Let $H = \{ id,$  $\}$

What are the left cosets?
H, sH, yH where $s =$ 

$y =$ 

NOTE: Group G can be written as
$$G = H \cup sH \cup yH$$
(Spend time checking this!)
in class.

Do table of Multiplication!

⟶ SEE ⟶

Theorem: If H is a subgroup of a finite group and xH, yH are two left cosets then either

(a) $xH = yH$ OR (b) $xH \cap yH = \phi$

proof: Suppose $xh_1 = yh_2$ $h_1, h_2 \in H$

we prove that $xH = yH$, first $xH \subseteq yH$

$\Rightarrow xh = (y h_2 h_1^{-1})h = y(h_2 h_1^{-1} h) \in yH$

(Clearly $yH \subseteq xH$ has same argument) $\blacksquare$

HENCE The COSETS of H partition the group G

Corollary: (Lagrange's theorem) If G is a finite group of order n, and H is a subgroup of G

$\Rightarrow$ order(H) | order(G)

proof: Since the left cosets of H partition G

$$G = \bigcup y_i H \quad \{y_1, \ldots y_k\} \text{ coset representative}$$

$$y_i H \neq y_j H.$$

$\Rightarrow$ Order(G) = $K \cdot$ Order(H).

Corollary: Given a permutation π $\langle \pi \rangle = \{id, \pi, \pi^2, \pi^3, \ldots\}$ = all powers of π.

This is a subgroup of S_n $\Rightarrow$ Order(π) = Order$(\langle\pi\rangle)$

To conclude this part of the course we do example:

<u>Example</u>: What are the subgroups of A_4

<u>Answer</u>: possible orders are 1, 2, 3, 4, 6, 12

The elements of A_4 are

$$A_4 = \left\{ \begin{array}{l} id, \ (12)(34), \ (13)(24), \ (14)(23), \\ (1,2,3), \ (132), (124), (142), (134), (143), (2,3,4) \\ (2,4,3) \end{array} \right\}$$