Recall we defined • normal subgrp $N \triangleleft G$ last time.
• quotient grp G/N

Fundamental Homomorphism Theorem (for grps.)

Given $f: G_1 \to G_2$ a grp homorphism, then.

$$G_1 / \mathrm{Ker}(f) \simeq \mathrm{Im}(f) \subseteq G_2$$

Recall $\mathrm{Ker}(f)$ is $\{ g \in G_1 \mid f(g) = \underbrace{e}_{\in G_2} \}$

Pf: We need to construct a grp isomorphism between $G_1/\mathrm{Ker}(f)$ and $\mathrm{Im}(f)$.

The map $\tilde{f}$ is clearly the choice, the point is to show $\tilde{f}$ is indeed an isomorphism (which means $\tilde{f}$ is injective and surjective).

$$\tilde{f}: G_1/\mathrm{Ker}(f) \longrightarrow \mathrm{Im}(f)$$
$$g_1 \cdot \mathrm{Ker}(f) \longrightarrow f(g_1)$$

$\tilde{f}$ is well-defined : $f(g_1) \overset{\text{goal}}{=} f(g_1 \cdot h) \quad \forall\, h \in \mathrm{Ker}(f)$

$$\underset{f \text{ being grp homomorphism}}{=} f(g_1) \cdot f(h) \overset{f(h)=e}{=} f(g_1)$$

$\tilde{f}$ is injective : it suffices to show that $\mathrm{Ker}(\tilde{f}) = \{e\} \subseteq G_1/\mathrm{Ker}(f)$.

if $\tilde{f}(g \cdot \mathrm{Ker}(f)) = e \in G_2$

then $f(g) = e \in G_2 \Leftrightarrow g \in \mathrm{Ker}(f) \Leftrightarrow$

$g \cdot \mathrm{Ker}(f) = e \in G_1/\mathrm{Ker}(f)$

$\tilde{f}$ is surjective : clearly because the target grp is $\mathrm{Im}(f)$

$\square$.

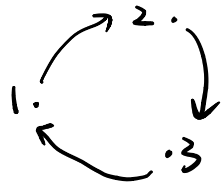
Definition of Alternating grp

Previously we consider elements in S_n as

- a map bijective betwen $\{1, \cdots, n\} \to \{1, \cdots, n\}$
- permutation of n letters.

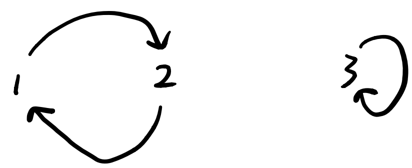
eg.

$\sigma: \begin{matrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 \end{matrix}$



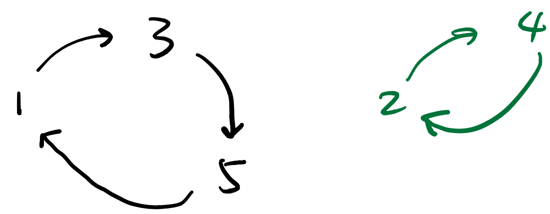
cycle

$\tau: \begin{matrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{matrix}$



transposition

$\begin{matrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 4 & 5 & 2 & 1 \end{matrix}$



$(1\ 3\ 5)(2\ 4)$

Claim: Elements in S_n can be written as a product of disjoint cycles.

Pf: Fix $\sigma \in S_n$.

We define "$\sim$" a relation among the letters.

$i \sim j \iff \exists k \in \mathbb{Z},\ \sigma^k(i) = j$

We claim $\sim$ is an equivalence relation.

$\sim$ is reflexsive : $i \sim i$ since $\sigma^{ord(\sigma)} = e$

i.e. choose $k = \mathrm{ord}(\sigma)$ in S_n.

$\sim$ is symmetric: $i \sim j \Rightarrow j \sim i$

if $\sigma^k(i) = j$ then $\sigma^{-k}(j) = i$.

$$\sigma^{-k}(j) = \sigma^{\mathrm{ord}(\sigma)-k}(j)$$

$\sim$ is transitive: $i \sim j$ $j \sim s \Rightarrow i \sim s$

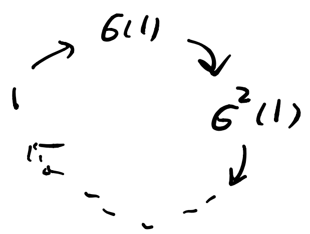
$\sigma^{k_1}(i) = j$ $\sigma^{k_2}(j) = s$ then

$\sigma^{k_1+k_2}(i) = s$.

Then $\sim$ gives a partition of elements in $\{1, \cdots, n\}$.

We claim each equivalence class is a cycle.

$[1]$: the equivalence class of 1. Denote c to be the size of equivalence class.



It suffices to show that the number of elements in $[1]$ equal to the minimal positive integer k s.t. $\underline{\sigma^k(1) = 1}$.

$[1] = \{ \sigma^n(1) \mid n \in \mathbb{Z} \}$

$= \{ \sigma^n(1) \mid 1 \leq n \leq k \}$.

$\forall n = q \cdot k + r$

$\sigma^n(1) = \sigma^{q \cdot k + r}(1) = \sigma^r(1)$

So $[1]$ has size at most k.

Actually $[1]$ has size equal to k. because.

$\sigma^i(1) \neq \sigma^j(1)$ for $i \neq j < k$.

(if $\sigma^i(1) = \sigma^j(1)$ then $\sigma^{i-j}(1) = 1$ contradict with k being the smallest integer s.t. $\sigma^k(1) = 1$)

$\square$.

Lemma. Elements in S_n can always be written as a product of transpositions.

transpositions means switch. 2 letters in n letters. $(i\ j) \in S_n$

eg. $(1\ 2\ 3) = \underbrace{(1\ 3)}_{\sigma_2} \circ \underbrace{(1\ 2)}_{\sigma_1}$

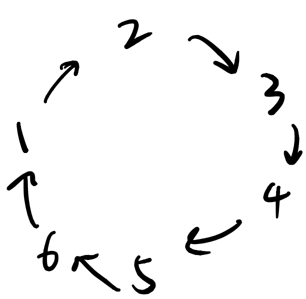
$1 \xrightarrow{\sigma_1} 2 \xrightarrow{\sigma_2} 2$

$2 \longrightarrow 1 \longrightarrow 3$

$3 \longrightarrow 3 \longrightarrow 1$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = (16) \circ (15) \circ (14) \circ (13) \circ (12)$$

a b c d e f (ad)(ac)(ab)



Any cycle can be written as a product of transpositions. Then any $\sigma \in S_n$ can be written as product of transpositions.

$\sigma = \underbrace{\sigma_1 \cdot \sigma_2 \cdots \sigma_m}$ where σ_i are disjoint cycles in S_n.

$= \prod_i \sigma_i$

$= \prod_i \prod_j \sigma_{ij}$ $\quad \sigma_{ij}$ are transpositions.

Rmk. σ_i and σ_j commute because they are disjoint.

but σ_{ij} and σ_{ik} might. not commute.

$$\sigma = \sigma \cdot \underbrace{(12)\cdot(21)}_{\overset{\shortparallel}{e}}$$

Lemma: Fix $\sigma \in S_n$. The number of transipositions in writing σ is either all even or all odd.

pf: We define an invariant of σ.

$$f(\sigma) := \#\{(i,j) \mid i<j,\ \sigma(i) > \sigma(j)\}$$

eg. $\sigma = (1\ 2\ 3)$ $\qquad f(\sigma) = 2$

$\sigma = (1\ 2)$ $\qquad f(\sigma) = 1$

$$\begin{matrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{matrix}$$

	$\xrightarrow{(123)}$		$\xrightarrow{(12)}$	
$(1,2)$	$2\ 3$	×	$2\ 1$	✓
$(1,3)$	$2\ 1$	✓	$2\ 3$	×
$(2,3)$	$3\ 1$	✓	$1\ 3$	×

We claim.

$$f((a_i\ a_j)\circ\sigma) \equiv f(\sigma)+1 \mod 2$$

To show this.

$$\begin{array}{lcccccccc}
 & 1 & 2 & \cdots & i & \cdots & j & \cdots & n \\
\sigma: \downarrow & & & & & & & & \\
 & a_1 & a_2 & \cdots & a_i & \cdots & a_j & \cdots & a_n. \\
(a_i\ a_j)\downarrow & & & & \downarrow & & \downarrow & & \\
 & a_1 & a_2 & \cdots & a_j & \cdots & a_i & \cdots & a_n
\end{array}$$

For (s_1, s_2) where $s_1 < s_2$ and $s_1, s_2 \notin \{i, j\}$, they stay the same. Only need to consider (k, i) and (k, j) and (i, k) (j, k).

① If $k < i$, then the contribution from (k, i) and (k, j) stays the same (since we just count whether $a_k < a_i$, $a_k < a_j$).

② Similarly for $k > j$. The contribution from (i, s) & (j, s) stays the same.

③ For $i < k < j$.

If $a_i < a_k < a_j$, then.

(i, k), (k, j) both do not contribute to $f(\sigma)$.

(i, k), (k, j) both contribute to $f((a_i\ a_j)\circ\sigma)$.

If $a_k < a_i < a_j$, then.

only (i, k) contribute for $f(\sigma)$

only (k, j) contribute to. $f((a_i\ a_j)\circ\sigma)$.

Depending on the ordering of a_i, a_k, a_j, (6 cases).

$\square$

This gives a map: $S_n \xrightarrow{g} \{0,1\} = \mathbb{Z}_2$

$$\sigma \longrightarrow f(\sigma) \bmod 2$$

It is a grp homomorphism since

$$g(\sigma_1 \circ \sigma_2) = g(\underbrace{\prod t_{1j}}_{n \text{ tran}} \circ \underbrace{\prod t_{2j}}_{m \text{ tran}})$$

$$= f(\underbrace{\prod t_{1j}}_{n \text{ tran}} \circ \underbrace{\prod t_{2j}}_{m \text{ tran}}) \bmod 2$$

$$= \# \text{transpositions} \bmod 2 = n+m \bmod 2$$

$$g(\sigma_1) + g(\sigma_2) = n + m \bmod 2.$$

Since $g((12)) = 1$ $g(e) = 0$. we also know g is surjective.

Def (Alternating Grp).

A_n is the subgrp of S_n that is $\ker(g)$.

Equivalently, A_n is also the subgrp consists of permutations σ s.t. $f(\sigma)$ is even.

Coro. A_n is a subgrp of S_n with index 2.