Recall we defined a normal subgroup $N$ of $G$ last time.

### Fundamental Homomorphism Theorem (for groups)

Given $f: G_1 \to G_2$ a group homomorphism, then

$$\frac{G_1}{\ker(f)} \cong \text{Im}(f) \leq G_2$$

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

**pf:** We need to construct a group isomorphism between $\frac{G_1}{\ker(f)}$ and $\text{Im}(f)$.

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).

$$\tilde{f}: \frac{G_1}{\ker(f)} \to \text{Im}(f)$$

$$g_1 \cdot \ker(f) \rightarrow f(g_1)$$

$\tilde{f}$ is well-defined: $f(g_1) = f(g_1h)$ and $h \in \ker(f)$

$$\tilde{f} (g_1) = f(g_1) \cdot f(h) = f(g_1h) = f(g_1)$$

$f$ being group homomorphism

$\tilde{f}$ is injective: it suffices to show that $\ker(\tilde{f}) = \{e\} \leq G_1/\ker(f)$

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

then $f(g) = e \in G_2 \Rightarrow g \in \ker(f)$

$g \cdot \ker(f) = e \in G_1/\ker(f)$

$\tilde{f}$ is surjective: clearly because the target group is $\text{Im}(f)$.
Definition of Alternating Group

Previously we consider elements in \( S_n \) as
- a map bijective between \( \{1, \ldots, n\} \rightarrow \{1, \ldots, n\} \)
- permutation of \( n \) letters.

\[
\sigma : 
\begin{array}{c}
1 & 2 & 3 \\
\downarrow & \downarrow & \downarrow \\
2 & 3 & 1 \\
\end{array}
\xrightarrow{\sigma}
\begin{array}{c}
2 & 3 & 1 \\
\downarrow & \downarrow & \downarrow \\
1 & 2 & 3 \\
\end{array}
\]

\[ \sigma \text{ cycle} \]

\[
\tau : 
\begin{array}{c}
1 & 2 & 3 \\
\downarrow & \downarrow & \downarrow \\
2 & 1 & 3 \\
\end{array}
\xrightarrow{\tau}
\begin{array}{c}
1 & 2 & 3 \\
\downarrow & \downarrow & \downarrow \\
2 & 1 & 3 \\
\end{array}
\]

\[ \tau \text{ transposition} \]

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.

\[ \sim \text{ if } \exists k \in \mathbb{Z}, \ i \sim j \iff \sigma^k(i) = j \]

We claim \( \sim \) is an equivalence relation.

\( \sim \) is reflexive: \( i \sim i \) since \( \sigma^{\text{ord}(\sigma)}(i) = i \)
\[ \text{i.e. choose } k = \text{ord}(\sigma) \text{ in } S_n. \]

\[ \sim \text{ is symmetric: } i \sim j \implies j \sim i \]

\[ \text{if } \sigma^k(i) = j \text{ then } \sigma^{-k}(j) = i. \]

\[ \sigma \text{ is transitive: } i \sim j \sim s \implies i \sim s \]

\[ \sigma^k(i) = j \quad \sigma^{k_2}(j) = s \text{ then } \]

\[ \sigma^{k + k_2}(i) = s. \]

Then \( \sim \) gives a partition of elements in \( \{1, \ldots, n\} \).

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.

\[ \sigma^k(1) = 1. \]

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

\[ = \{ \sigma^n(1) \mid 1 \leq n \leq k \} \]

\[ \forall n = q \cdot k + r \]

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

so \([1]\) has size at most \( k \).

Actually \([1]\) has size equal to \( k \) because.
Lemma. Elements in $S_n$ can always be written as a product of transpositions.

**Proof.**

Elements in $S_n$ can always be written as a product of transpositions. Consider any cycle $(i_1 i_2 \ldots i_k)$.

Any cycle can be written as a product of transpositions. Then any element in $S_n$ can be written as a product of transpositions.
$6 = \prod_{i}^{m} 6_i$ where $6_i$ are disjoint cycles in $S_n$.

$= \prod_{i}^{m} 6_i$

$= \prod_{i} \prod_{j} 6_{ij}$ $6_{ij}$ are transpositions.

Rmk. $6_i$ and $6_j$ commute because they are disjoint.

but $6_{ij}$ and $6_{ik}$ might not commute.

$6 = 6 \cdot (12)(21)$

Lemma: Fix $6 \in S_n$. The number of transpositions in writing $6$ is either all even or all odd.

pf: We define an invariant of $6$.

$f(6) := \# \{(i,j) \mid i < j, \ 6(i) > 6(j)\}$

Ex. $6 = (1 \ 2 \ 3) \quad f(6) = 2$

$6 = (1 \ 2) \quad f(6) = 1$

$\begin{array}{ccc}
1 & 2 & 3 \\
2 & 1 & 3 \\
\end{array}$

$\begin{array}{ccc}
(1,2) & 2 & 3 & x & \checkmark \\
(1,3) & 2 & 1 & \checkmark & 23 x \\
(2,3) & 3 & 1 & \checkmark & 13 x \\
\end{array}$
We claim
\[ f((a_i, a_j) \circ s) \equiv f(s) + 1 \mod 2 \]

To show this, let
\[ s = a_1, a_2, \ldots, a_n. \]
\[ (a_i, a_j) \circ s = a_1, a_2, \ldots, a_j, a_i, a_{j+1}, \ldots, a_n. \]

For \((s_i, s_j)\), where \(s_i < s_j\) and \(s_i, s_j \in \{i, j\}\), they stay the same. Only need to consider \((k, i)\) and \((k, j)\) and \((i, k)\) and \((j, k)\).

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 \((i, s)\) and \((j, s)\) 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 \(f(s)\).
   \((i, k), (k, j)\) both contribute to \(f((a_i, a_j) \circ s)\).

   If \(a_k < a_i < a_j\), then.
   only \((i, k)\) contribute for \(f(s)\).
   only \((k, j)\) contribute to \(f((a_i, a_j) \circ s)\).

Depending on the order of \(a_i, a_k, a_j\), (6 cases).
This gives a map: $S_n \xrightarrow{g} \mathbb{Z}_2$. $\xi_0, 13 = \mathbb{Z}_2$

$$6 \rightarrow f(6) \mod 2$$

It is a grp homomorphism since

$$g(6_1 \circ 6_2) = g(\prod_{i,j}^{n \text{ tran}} t_{ij} \circ \prod_{i,j}^{m \text{ tran}} t_{ij})$$

$$= f(\prod_{i,j}^{n \text{ tran}} t_{ij} \circ \prod_{i,j}^{m \text{ tran}} t_{ij}) \mod 2$$

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

$$g(6_1) + g(6_2) = n + m \mod 2.$$ 

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

Def (Alternating Grp).

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

Equivalently, $A_n$ is also the subgroup consists of permutations $6$ s.t. $f(6)$ is even.

Coro. $A_n$ is a subgroup of $S_n$ with index 2.