3. The Symmetric and Alternating groups

The symmetric group acts on the set $S = \{1, 2, \ldots, n\}$. Fix $\sigma \in S_n$. The cyclic group $\langle \sigma \rangle$ also acts on $S$.

Let $T_1, T_2, \ldots, T_k$ be the orbits of this action.

Define permutation $\sigma_1, \sigma_2, \ldots, \sigma_k$ as follows:

- $\sigma_i$ acts as $\sigma$ does on $T_i$, but as the identity on $T_j$ ($j \neq i$).

Clearly:

- $\sigma = \sigma_1 \sigma_2 \cdots \sigma_k$
- $\sigma_1, \sigma_2, \ldots, \sigma_k$ all pairwise commute (since $T_i$'s are pairwise disjoint).

Consider $T_i$:

\[ S \xrightarrow{\sigma} \sigma S \xrightarrow{\sigma^2} \sigma^2 S \cdots \xrightarrow{\sigma^{k-1}} \sigma^{k-1} S \xrightarrow{\sigma^k} \sigma^k S = S \]

- A permutation that permutes $T \leq S$ cyclically and fixes everything else is a $k$-cycle. (where $|T| = k$).

We write this as $\phi = (s \ \sigma s \ \sigma^2 s \ \cdots \ \sigma^{k-1} s)$. Example: $\phi = (1 \ 3 \ 5 \ 2 \ 4)$ is a 5-cycle. We write it as $\phi = (1 \ 3 \ 5 \ 2 \ 4)$, or $\phi = (3 \ 5 \ 2 \ 4 \ 1)$, etc.
If cycles $\phi_1$ and $\phi_2$ permute the elts of $T_1 \cap T_2$ and if $T_1 \cap T_2 = \emptyset$, then $\phi_1$ and $\phi_2$ are disjoint cycles.

Clearly, disjoint cycles commute.

**Prop 3.1** If $\sigma \in S_9$, then $\sigma$ can be expressed as a product of disjoint cycles, uniquely up to order.

Usually we don't write cycles.

E.g., $\sigma = (1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 7 \ 8 \ 9) \in S_9$.

Orbits on $\{1, \ldots, 9\}$ are $\{1,2,7,3\}, \{3\}, \{4,5,6,8,9\}$.

Write $\sigma = (127)(45869)$.

**Note:**
- If $\sigma$ is a $k$-cycle, then $|\sigma| = k$.
- If $\sigma = \sigma_1 \sigma_2 \ldots \sigma_m$, all disjoint, then $|\sigma| = \text{lcm}(|\sigma_1|, \ldots, |\sigma_m|)$.
- If e.g., $\sigma = (1 \ 2 \ 3 \ 4 \ 5)$, then $\sigma^{-1} = (5 \ 4 \ 3 \ 2 \ 1)$.

A 2-cycle is called a transposition.

Every cycle (and hence elt of $S_n$) can be written as a product of transpositions, e.g.

$$(1 \ 2 \ 3 \ \cdots \ k) = (1 \ k)(1 \ k-1) \cdots (1 \ 3)(1 \ 2)$$

**Note:** Read right-to-left (function composition).
We say an $S_n$ is even if it can be written as a product of an even number of transpositions, otherwise call it odd.

Note: $\sigma_1, \sigma_2$ even $\Rightarrow \sigma_1 \sigma_2$ even

$\sigma_1, \sigma_2$ odd $\Rightarrow \sigma_1 \sigma_2$ even.

Define $f: S_n \rightarrow \{1, -1\}$, $f(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ is even} \\ -1 & \text{if } \sigma \text{ is odd} \end{cases}$

Check: $f$ is a homomorphism.

$\ker f \leq S_n$, $\ker f = \{ \text{even permutations} \}$ is the alternating group, denoted $A_n$.

Prop 3.2: If $n \geq 2$, then $[S_n : A_n] = 2$.

Proof: It suffices to show that $F: S_n \rightarrow \{1, -1\}$ is surjective, because then, $S_n/A_n \cong \{1, -1\}$, so by FHT, $|S_n/A_n| = [S_n : A_n] = |\{1, -1\}| = 2$.

Claim: $(12)$ is odd (i.e., it cannot be written as an even # of transpositions).

If it were even, then we could write $1 = (ab) \cdots$.

Write $1 = (ab) \cdots$ when “a” appears a min’l # of times.

Note: $a \neq b$, so “a” appears at least once more

$(ac)(dc) = (ad)(cd)$. Thus we may “move” “a” to the left, and assume that $1 = (ab)(ac) \cdots$.
Since # of a's is minimal, b = c.

But \((ab)(ac) = (ac)(bc)\), also contradicting minimality.

Then (12) is odd. \(\square\)

**Exercise:** Let \((a_1, a_2, \ldots, a_k) \in S_n\) be a \(k\)-cycle. Then
\[
\tau(a_1, a_2, \ldots, a_k)\tau^{-1} = (\tau a_1, \tau a_2, \ldots, \tau a_k).
\]

Way to think about this. Let \([n] = \{1, 2, \ldots, n\}\).

Then the following diagram commutes

\[
\begin{array}{ccc}
[n] & \xrightarrow{(a_1, a_2, \ldots, a_k)} & [n] \\
\tau & & \tau \\
\downarrow & & \downarrow \\
[n] & \xrightarrow{(\tau a_1, \tau a_2, \ldots, \tau a_k)} & [n]
\end{array}
\]

Write \(\sigma \in S_n\) as a product of disjoint cycles.

Then \(\sigma\) has **cycle-type** \((k_1, k_2, \ldots, k_n)\), where

\(k_i = \#\) of \(i\)-cycles.

**Example:** \(\sigma = (1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 7 \ 8 \ 9) = (1 \ 2 \ 7 \ 3 \ 5 \ 8 \ 9 \ 1 \ 4) = (1 \ 2 \ 7)(3 \ 5 \ 8 \ 9)(1 \ 4)\)

has cycle-type \((1, 0, 1, 0, 1, 0, 0, 0, 0)\).

Prop 2.3: If \(\sigma \in S_n\), then all elts of \(C(\sigma)\) have the same cycle-type.
Cor: If \( n \geq 3 \), then \( Z(S_n) = 1 \).

Prop 3.4: If \( n \geq 5 \), then all 3-cycles are conjugate in \( A_n \).

Proof: Let \((ijk)\) be any 3-cycle. Then
\[
(ijk) = \sigma(123)\sigma^{-1}
\]
for some \( \sigma \in S_n \).

If \( \sigma \in A_n \), we're done.

If \( \sigma \not\in A_n \), then \( \tau = \sigma(45) \).

Then \( \tau(123)\tau^{-1} = \sigma(45)(123)(45)\sigma^{-1} = \sigma(123)\sigma^{-1}(ij4) \). \( \square \)

Prop 3.5: If \( n \geq 3 \), then \( A_n \) is generated by 3-cycles.

Proof: Let \( i, j, k \) be distinct.
\[
(ijk)(ikj) = (i)(kj), \quad \text{and} \quad (ij)(km) = (jmk)(ikj). \quad \square
\]

Def: A group \( G \) is simple if its only normal subgroups are 1 and \( G \).

By Lagrange's theorems, if \( |G| = p \), then \( G \) is simple.

Thm 3.6: If \( n \neq 4 \), then \( A_n \) is simple.

Proof: \( A_1, A_2, A_3 \) are clearly simple.

Suppose \( n \geq 5 \), and say \( 1 \neq H \triangleleft A_n \).

Goal: Show \( H \) contains a 3-cycle
(We then by Prop 3.4, \( H \) contains all 3-cycles, and by Prop 3.5, \( H = A_n \)).
**Cor:** If $n \geq 3$, then $Z(S_n) = 1$.

**Prop 3.4:** If $n \geq 5$, then all 3-cycles are conjugate in $A_n$.

**Pf:** Let $(ijk)$ be any 3-cycle. Then

$$(ijk) = \sigma(123)\sigma^{-1} \text{ for some } \sigma \in S_n.$$  

If $\sigma \in A_n$, we're done.

If $\sigma \notin A_n$, then $\tau = \sigma(45)$.

Then

$$\tau(123) \tau^{-1} = \sigma(45)(123)(45)\sigma^{-1} = \sigma(123)\sigma^{-1} = (i,j,k).$$

**Prop 3.5:** If $n \geq 3$, then $A_n$ is generated by 3-cycles.

**Pf:** Let $i, j, k, m$ be distinct.

$$(ij)(ik) = (ikj), \text{ and } (ij)(km) = (jmk)(ikj).$$

**Def:** A group $G$ is **simple** if its only normal subgroups are 1 and $G$.

By Lagrange's theorem, if $|G| = p$, then $G$ is simple.

**Thm 3.6:** If $n \neq 4$, then $A_n$ is simple.

**Pf:** $A_1, A_2, A_3$ are clearly simple.

Suppose $n \geq 5$, and say $1 \neq H \triangleleft A_n$.

**Goal:** Show $H$ contains a 3-cycle

(But then by Prop 3.4, $H$ contains all 3-cycles, and by Prop 3.5, $H = A_n$).
Pick prime $p = |H|$, and an elt $\sigma \in H$ of order $p$ (which exists due to Cauchy).

Then, $\sigma$ is a product of $k$ disjoint $p$-cycles, for some $k$.

If $p = 3$, and $k = 1$, we're done.

Otherwise, there are 4 cases:

Case 1: $p > 3$. Say $\sigma = (a_1, a_2, \ldots, a_p)$... Then

$$\sigma(a_1, a_2, a_3) \sigma^{-1}(a_1, a_2, a_3) = (a_2, a_3, a_4)(a_1, a_3, a_2) = (a_1, a_2, a_3) \in H.$$

Case 2: $p = 3$, $k > 1$. Say $\sigma = (a_1, a_2, a_3)(a_4, a_5, a_6)$...

$$\sigma(a_1, a_2, a_4) \sigma^{-1}(a_1, a_2, a_4) = (a_2, a_3, a_5)(a_1, a_4, a_2) = (a_1, a_4, a_3, a_5, a_2).$$

We're back in Case 1.

Case 3: $p = 2$, $k = 2m > 2$, and some letter $a_5$ is fixed by $\sigma$.

Say $\sigma = (a_1, a_2)(a_3, a_4)...

\sigma(a_1, a_2, a_5) \sigma^{-1}(a_1, a_2, a_5) = (a_2, a_1, a_5)(a_1, a_5, a_2) = (a_1, a_2, a_5) \in H.$

Case 4: $p = 2$, $k = 2m > 2$, $\sigma$ fixes nothing.

Say $\sigma = (a_1, a_2)(a_3, a_4)(a_5, a_6)...

\sigma(a_1, a_2, a_5) \sigma^{-1}(a_1, a_5, a_2) = (a_2, a_1, a_6)(a_1, a_5, a_2) = (a_1, a_5)(a_2, a_6) \in H.$

We're back in Case 3. \[ \square \]