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.

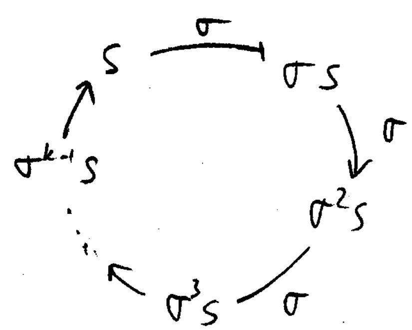
Let $T_1, T_2, \ldots, T_k$ be the orbits of this action.

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

σ_i acts as σ 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:



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

We write this as $\phi = (s \;\; \phi s \;\; \phi^2 s \; \ldots \; \phi^{k-1} s)$.

Example: $\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}$ is a 5-cycle. We write it as $\phi = (1\,3\,5\,2\,4)$, or $\phi = (3\,5\,2\,4\,1)$, etc.

If cycles ϕ_1 and ϕ_2 permute the elts of T_1 & T_2 and if $T_1 \cap T_2 = \emptyset$, then ϕ_1 & ϕ_2 are <u>disjoint</u> cycles.

Clearly, disjoint cycles commute.

<u>Prop 3.1</u> If $\sigma \in S_n$, then σ can be expressed as a product of disjoint cycles, uniquely up to order.

Usually we don't write 1-cycles.

e.g., $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 7 & 3 & 5 & 8 & 9 & 1 & 6 & 4 \end{pmatrix} \in S_9$.

$\langle\sigma\rangle$-orbits on $\{1,\dots,9\}$ are $\{1,2,7\}$, $\{3\}$, $\{4,5,6,8,9\}$

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

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

A 2-cycle is called a <u>transposition</u>.

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 $\sigma \in S_n$ is <u>even</u> if it can be written as a product of an even number of transpositions, otherwise call it <u>odd</u>.

<u>Note</u>: σ_1, σ_2 even $\Rightarrow$ $\sigma_1\sigma_2$ even

σ_1, σ_2 odd $\Rightarrow$ $\sigma_1\sigma_2$ even.

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

<u>Check</u>: f is a homom.

$\ker f \trianglelefteq S_n$, $\ker f = \{\text{even permutations}\}$ is the <u>alternating group</u>, denoted A_n.

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

<u>Pf</u>: It suffices to show that $f: S_n \longrightarrow \{1,-1\}$ is surjective, because then, $S_n/A_n \cong \{1,-1\}$, so by FIT, $|S_n/A_n| = [S_n : A_n] = |\{1,-1\}| = 2$.

<u>Claim</u>: (12) is odd (ie, it <u>cannot</u> be written as an even # of transpositions).

If it were even, then we could write $1 = \underbrace{(ab)\cdots\cdots}_{\text{odd }\#}$.

Write $1 = (ab)\cdots$ where "a" appears a mini'l # of times

<u>Note</u>:
- $a \neq b$, so "a" appears at least once more
- $(dc)(ac) = (ad)(cd)$. Thus we may "move" "a" to the left, and assume that $1 = (ab)(ac)\cdots$

Since # of a's is minimal, $b \neq c$.

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

Thus (12) is odd. $\square$

<u>Exercise</u>: Let $(a_1 a_2 \dots a_k) \in S_n$ be a k-cycle. Then

$$\tau (a_1 a_2 \dots a_k) \tau^{-1} = (\tau a_1 \, \tau a_2 \dots \tau a_k).$$

Way to think about this. Let $[n] = \{1, 2, \dots, n\}$.

Then the following diagram commutes

$$\begin{tikzcd}
{[n]} \arrow[r, "(a_1 a_2 \dots a_k)"] \arrow[d, "\tau"'] & {[n]} \arrow[d, "\tau"] \\
{[n]} \arrow[r, "(\tau a_1 \, \tau a_2 \dots \tau a_n)"'] & {[n]}
\end{tikzcd}$$

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

Then σ has <u>cycle-type</u> $(k_1, k_2, \dots, k_n)$, where

k_i = # of i-cycles.

<u>Example</u>: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 7 & 3 & 5 & 8 & 9 & 1 & 6 & 4 \end{pmatrix} = (127)(45869)$

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

<u>Prop 3.3</u>: If $\sigma \in S_n$, then all elts of $Cl(\sigma)$ 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.

Pf: Let $(i\,j\,k)$ be any 3-cycle. Then

$(i\,j\,k) = \sigma(1\,2\,3)\sigma^{-1}$ for some $\sigma \in S_n$.

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

If $\sigma \notin A_n$, then $\tau = \sigma(4\,5)$.

Then $\tau(1\,2\,3)\tau^{-1} = \sigma(4\,5)(1\,2\,3)(4\,5)\sigma^{-1} = \sigma(1\,2\,3)\sigma^{-1} = (i\,j\,k)$ ✓

$\square$

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

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

$(i\,j)(i\,k) = (i\,k\,j)$, and $(i\,j)(k\,m) = (j\,m\,k)(i\,k\,j)$. $\square$

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

By Lagrange's thm, 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 $1 \neq H \lhd A_n$.

Goal: Show H contains a 3-cycle

(B/c 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 $(i\,j\,k)$ be any 3-cycle. Then

$(i\,j\,k) = \sigma(1\,2\,3)\sigma^{-1}$ for some $\sigma \in S_n$.

If $\sigma \in A_n$, we're done.
If $\sigma \notin A_n$, then $\tau = \sigma(4\,5)$.
Then $\tau(1\,2\,3)\tau^{-1} = \sigma(4\,5)(1\,2\,3)(4\,5)\sigma^{-1} = \sigma(1\,2\,3)\sigma^{-1} = (i\,j\,k)$ ✓

□

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

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

$(i\,j)(i\,k) = (i\,k\,j)$, and $(i\,j)(k\,m) = (j\,m\,k)(i\,k\,j)$. □

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

By Lagrange's thm, 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
(b/c then by Prop 3.4, H contains all 3-cycles, and by Prop 3.5, $H = A_n$).

$\boxed{6}$

Pick prime $p \mid |H|$, and an elt $\sigma \in H$ of order p (which exists due to Cauchy).

Then, σ 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:

<u>Case 1</u>: $p>3$. Say $\sigma = (a_1\ a_2 \dots a_p)\cdots$ Then

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

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

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

We're back in Case 1.

<u>Case 3</u>: $p=2$, $k=2m \geq 2$, and some letter a_5 is fixed by σ.

Say $\sigma = (a_1 a_2)(a_3 a_4)\cdots$

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

<u>Case 4</u>: $p=2$, $k=2m \geq 2$, σ fixes nothing.

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

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

We're back in Case 3. $\square$