Simplicity of $A_n$ continued.

Last time we saw $A_5$ is simple. We almost, but did not quite, prove the following in the course of the proof:

**Lemma.** Any two 3-cycles are conjugate in $A_n$, $n \geq 5$.

**Proof.** We will show any 3-cycle $(a \, b \, c)$ is conjugate to $(1 \, 2 \, 3)$.

Let $x_1, \ldots, x_{n-3}$ be s.t. $x_1, x_2, x_3, \ldots, x_{n-3}$ = $1, \ldots, n^3$.

Let $\sigma \in \text{Sym}(n)$ be the permutation

$$
\begin{pmatrix}
0 & 2 & 3 & 4 & 5 & \ldots & 0 \\
0 & 0 & 0 & 0 & 0 & \ldots & 0 \\
0 & 0 & 0 & 0 & 0 & \ldots & 0 \\
0 & 0 & 0 & 0 & 0 & \ldots & 0 \\
0 & 0 & 0 & 0 & 0 & \ldots & 0 \\
\end{pmatrix}
$$
Let \( \gamma = (4 \\ 5) \)
and set \( \gamma = 0 \).

\[
\begin{array}{ccccccc}
1 & 2 & 3 & 4 & 5 & \cdots & n \\
0 & 0 & 0 & 0 & 0 & \cdots & 0 \\
0 & 0 & 0 & 0 & 0 & \cdots & 0 \\
0 & 0 & 0 & 0 & 0 & \cdots & 0 \\
0 & 0 & 0 & 0 & 0 & \cdots & 0 \\
0 & 0 & 0 & 0 & 0 & \cdots & 0 \\
0 & 0 & 0 & 0 & 0 & \cdots & 0 \\
0 & 0 & 0 & 0 & 0 & \cdots & 0 \\
\end{array}
\]

we have

\[
6 (123) 6^{-1} = (a \\ b \\ c)
\]

and

\[
\gamma (123) \gamma^{-1} = (a \\ b \\ c)
\]

But either 6 or \( \gamma \) is even, so one way or the other \((123)\) and
\((a \\ b \\ c)\) are conjugate in \( \text{An} \).

Next, we have:

**Lemma:** \( \text{An} \) is generated by 3 cycle

for \( n \geq 5 \).
Let \( G \in S_n \). Then \( G \) is a product of an even number of transpositions:
\[
G = (y_1, y_2) \cdot \ldots \cdot (y_{2k-1}, y_{2k})
\]

It suffices to show each product of transpositions is a product of 3 cycles.
Let \( \alpha, \beta \) be 2 transpositions.

If \( \alpha = \beta \) then
\[
\alpha \cdot \beta = 1 = (1 \ 2 \ 3)^3 \quad \checkmark
\]

If \( \alpha = (a \ b) \) and \( \beta = (b \ c) \) for \( a, b, c \) distinct
\[
\alpha \cdot \beta = (a \ b \ c) \quad \checkmark
\]

If \( \alpha = (a \ b) \) and \( \beta = (c \ d) \) for \( a, b, c, d \) distinct
\[
\alpha \cdot \beta = (a \ b \ c) (b \ c \ d) \quad \checkmark
\]

Let's introduce a small amount of abstraction. If \( \phi : X \to Y \) is a
A bijection \( f: S_\infty \rightarrow S_\infty \)
\( \phi \rightarrow \phi^{-1} \phi \)
\( f \Rightarrow x \rightarrow x \)

if \( |x| = n < \infty \) then we have

\( X = \frac{1}{m} x_1, \ldots, x_m \) for some elements \( x_1, x_\infty \) and have a bijection

\( \frac{1}{m} x_1, \ldots, x_m \rightarrow \frac{1}{m} x_1, \ldots, x_m \)
\( i \rightarrow x_i \)

Giving an iso
\( S_\infty \Rightarrow S_n \)

Setting \( A_{\infty} := \{ s \in S_\infty \mid F_\phi(s) \in A_n \} \)

\( = F_\phi^{-1}(A_n) \)

de\'line, the algebraic group of \( A_\infty \), which
is isomorphic to $A_n : F_p : A_x \to A_n$.

Thus $A_n$ is simple for $n \geq 6$.

**Proof**

We have already proven this in the case $n=5$.

We will prove the result by induction.

Suppose $n \geq 6$ and $A_j$ is simple if $5 \leq j < n-1$.

Let $N \leq A_n$, $N \neq 1$. All 3 cycles are conjugate in $A_n$ and $A_n$ is generated by 3-cycles, so if $N$ contains one (hence all) 3-cycles, $N = A_n$, which is what we want.

So it suffices to show $N$ contains some 3-cycle.
An acts on \( S_1, S_2, \ldots, S_n \) in the natural way, let \( H_i \leq A_n \) be the stabilizer of \( r \in S_i \), \( \cdots \in S_n \).

Then \( H_i \cong A_{n-1} \) (\( H_i \cong A_{n-1} \), \( X = S_1, S_2, \ldots, S_n \)).

So \( H_i \) is simple by induction.

Now \( N N H_i \triangleleft H_i \).

Thus either \( N N H_i = H_i \) or \( N N H_i = 1 \).

If \( N N H_i = 2H_i \), then \( N \) contains a 3-cycle (\( \sigma \), \( H_i \cong A_{n-1} \), \( \sigma \sigma \sigma ) \) so it suffices to show \( N N H_i \neq 1 \).

Let \( 6 \neq \sigma \in N \).

Claim 6 is conjugate to some \( 6^c \neq 6 \) with \( 6(\epsilon) = 6^c(\epsilon) \) for some \( \epsilon \).

Pf of claim: Let \( r \) be the longest length
of a disjoint cycle in $\mathcal{G}$.

$G = (\alpha_1, \ldots, \alpha_r)$ with

disjoint.

Case 1 $r \geq 3$. Consider $g = (\alpha_3, \alpha_4, \alpha_5)$ and

set $g^c = g \circ g^{-1}$

$g^c (\alpha_2) = \alpha_4$ but $g (\alpha_2) = \alpha_3$

so $G \neq G^c$ but $6 (\alpha_2) = 6^c (\alpha_2) \neq \alpha_3$

Case 2 $r = 2, \Rightarrow G$ is a product of

transpositions.

If $G = (\alpha_1, \alpha_2)(\beta_1, \beta_2)$ is a product of

2 transpositions, take

$g = (\alpha_1, \beta_1, \alpha_2)$

$g \circ g^{-1} = (\alpha_1, \beta_1, \alpha_2)(\alpha_2, \beta_2) \neq G$ but

both fix any element of

$\beta_1, \ldots, \alpha_2 \in \mathcal{G} \setminus \{\alpha_1, \beta_1, \alpha_2\}$. \]
Suppose \( S = (x_1 x_2) (B_1 B_2) (x_1 x_2) (\ldots) \) is a product of at least 3 transpositions.

Set \( S' = g S g^{-1} \) for \( g = (x_1 x_2) (B_1 B_2) \)

- \( S'(x_1) = S(x_1) \)
- \( S'(B_1) = B_2 + S(B_1) \)

So, from the claim \( S, S' \in N \) with \( S^{-1} S' \neq id \) and \( S^{-1} S' (i) = i \)

Then \( S^{-1} S' \in N \cap H \), which finishes the proof.

Q.E.D.