Supplement. The Alternating Groups $A_n$
are Simple for $n \geq 5$

Note. Recall that a group is *simple* if it is nontrivial and has no proper nontrivial normal subgroups. In this supplement, we follow the hints of Fraleigh in Exercise 15.39 and prove that $A_n$ is simple for $n \geq 5$.

**Theorem 15.15.** The alternating group $A_n$ is simple for $n \geq 5$.

**Proof.** (Exercise 15.39.)

(a) For $n \geq 3$, $A_n$ contains every 3-cycle.

Proof. Recall that $A_n$ contains all even permutations (those permutations that are a product of an even number of transpositions). Since the 3-cycle $(a, b, c) = (a, c)(a, b)$ (remember to read from right to left), then every 3-cycle is an even permutation and hence is in $A_n$. □

(b) For $n \geq 3$, $A_n$ is generated by the 3-cycles.

Proof. Let $\sigma \in A_n$. Then $\sigma$ is a product of an even number of permutations, say

$$\sigma = (a_1, b_1)(c_1, d_1)(a_2, b_2)(c_2, d_2) \cdots (a_k, b_k)(c_k, d_k)$$

where these $a_i, b_i, c_i, d_i$ for $i = 1, 2, \ldots, k$ may not be distinct. Now we consider the pairs of transpositions in terms of repeated elements. (1) If for some $j$, $a_j, b_j, c_j, d_j$ are distinct, then $(a_j, b_j)(c_j d_j) = (a_j, c_j, b_j)(a_j, c_j, d_j)$. (2) If for some $j$, $a_j, b_j, d_j$ are distinct, but $a_j = c_j$, then

$$(a_j, b_j)(c_j, d_j) = (a_j, b_j)(a_j, d_j) = (a_j, b_j, c_j).$$
(3) If for some \( j \), \( a_j = c_j \) and \( b_j = d_j \) then

\[
(a_j, b_j)(c_j, d_j) = (a_j, b_j)(a_j, b_j) = \iota,
\]

the identity permutation, and this pair of transpositions can be eliminated from the representation of \( \sigma \) in terms of the \( k \) pairs of transpositions.

These three types of pairs of transpositions are the only types possible (remember, \( a_j \neq b_j, c_j \neq d_j \), and the order in a transposition is irrelevant). So each pair of transpositions in the representation of \( \sigma \) given above can be (1) replaced with a product of two 3-cycles, (2) replaced with a single 3-cycle, or (3) omitted from the product (respectively). Therefore, \( \sigma \) can be written as a product of 3-cycles and the 3-cycles generate \( A_n \). \( \square \)

(c) Let \( r \) and \( s \) be distinct fixed elements of \( \{1, 2, \ldots, n\} \) for \( n \geq 3 \). Then \( A_n \) is generated by the \( n \) “special” 3-cycles of the form \( (r, s, i) \) for \( 1 \leq i \leq n, i \neq r, i \neq s \).

Proof. Let \( r \) and \( s \) be given. Then a 3-cycle in the generating set of \( A_n \) as given in (b) may (1) contain neither \( r \) nor \( s \) and be of the form \( (a, b, c) \), (2) contain \( r \) only and be of the form \( (r, a, b) \), (3) contain \( s \) only and be of the form \( (s, a, b) \), or (4) contain both \( r \) and \( s \) and be of the form \( (r, s, a) \) or be of the form \( (s, r, a) \).

Following the hint:

\[
(r, s, a)^2(r, s, c)(r, s, b)^2(r, s, a) = (a, b, c)
\]

\[
(r, s, b)(r, s, a)^2 = (r, a, b)
\]

\[
(r, s, b)^2(r, s, a) = (s, a, b)
\]

\[
(r, s, a) = (r, s, a)
\]

\[
(r, s, a)^2 = (s, r, a).
\]
So every possible 3-cycle in $A_n$ can be written as a product of 3-cycles of the form $(r, s, i)$ where $r$ and $s$ are given and $1 \leq i \leq n$. □

(d) Let $N$ be a normal subgroup of $A_n$ for $n \geq 3$. If $N$ contains a 3-cycle, then $N = A_n$.

Proof. Let $(r, s, a)$ be the 3-cycle in $N$ and let $b \in \{1, 2, \ldots, n\}$ where $b \neq r$ and $b \neq s$. Then $(a, b)(r, s) \in A_n$ since this is an even permutation. Also,

$$((a, b)(r, s))^{-1} = (r, s)^{-1}(a, b)^{-1} = (r, s)(a, b) \in A_n$$

since $A_n$ is a group. Since $N$ is a normal subgroup, then by Theorem 14.13,

$$((a, b)(r, s))(r, s, a)((r, s)(a, b))^{-1} = (a, b)(r, s)(r, s, a)(r, s)(a, b) = (r, s, b) \in N.$$  

Since $b$ is an arbitrary element of $\{1, 2, \ldots, n\}$ (other than the restriction $b \neq r$, $b \neq s$), then $N$ contains all of the “special” 3-cycles of part (c). Therefore, by part (c), $N = A_n$. □

(e) Let $N$ be a nontrivial normal subgroup of $A_n$ for $n \geq 5$. Then one of the following cases must hold. In each case, $N = A_n$.

Case I. $N$ contains a 3-cycle.

Case II. $N$ contains a product of disjoint cycles, at least one of which has length greater than 3.

Case III. $N$ contains a disjoint product of the form $\sigma = \mu(a_4, a_5, a_6)(a_1, a_2, a_3)$ (where $\mu \in A_n$).

Case IV. $N$ contains a disjoint product of the form $\sigma = \mu(a_1, a_2, a_3)$ where $\mu$ is a product of an even number of disjoint 2-cycles.

Case V. $N$ contains a disjoint product $\sigma$ of the form $\sigma = \mu(a_3, a_4)(a_1, a_2)$ where $\mu$ is a product of an even number of disjoint 2-cycles.
Proof. To see why at least one of Case I–V must hold, we consider writing the elements of $N$ as *disjoint* products of cycles (which can be done by Theorem 9.8). Case II describes the situation in which there is a permutation which is the product of disjoint cycles, at least one of which has length greater than 3. So if Case II does not hold, then all elements of $N$ can be written as a disjoint product of cycles of lengths 2 and 3 (we omit cycles of length 1—i.e., fixed points). Case V covers the case where $N$ contains a permutation consisting of no 3-cycles and a bunch of 2-cycles (i.e., transpositions). Case I covers the case where $N$ contains a permutation consisting of a single 3-cycle alone. Case IV covers the case where $N$ contains a permutation consisting of a single 3-cycle and a bunch of 2-cycles. Case III covers the case where $N$ contains a permutation consisting of two or more 3-cycles. Therefore, in terms of decompositions of permutations into disjoint cycles and with an eye towards 3-cycles, if Case II does not hold, then at least one of Case I, III, IV, or V must hold.

Now we explore Cases I–V to show that each implies that $N = A_n$ and therefore that $A_n$ has no proper nontrivial normal subgroup for $n \geq 5$ (that is, $A_n$ is simple for $n \geq 5$).

**Case I.** If $N$ contains a 3-cycle, then by part (d), $N = A_n$ and $A_n$ is simple (in fact, this holds for $n \geq 3$).

**Case II.** If $N$ contains a permutation of the form $\sigma = \mu(a_1, a_2, \ldots, a_r)$ where $r > 3$ and $\mu$ contains none of $a_1, a_2, \ldots, a_r$, then $(a_1, a_2, a_3)\sigma(a_1, a_2, a_3)^{-1} \in N$ since $N$ is a normal subgroup (by Theorem 14.13). So

$$\sigma^{-1} \left( (a_1, a_2, a_3)\sigma(a_1, a_2, a_3)^{-1} \right) = (a_r, \ldots, a_2, a_1)\mu^{-1}(a_1, a_2, a_3)\mu(a_1, a_2, \ldots, a_r)(a_3, a_2, a_1)$$
\[ A_n \text{ is Simple for } n \geq 5 \]

Supplement

\[ \mu^{-1}(a_r, \ldots, a_2, a_1)(a_1, a_2, a_3)(a_1, a_2, \ldots, a_r)(a_3, a_2, a_1) \]

since \( \mu \) and \( \mu^{-1} \) are disjoint from the other cycles

\[ = (a_r, \ldots, a_2, a_1)(a_1, a_2, a_3)(a_1, a_2, \ldots, a_r)(a_3, a_2, a_1) = (a_1, a_3, a_r) \in N. \]

So \( A_n \) contains a 3-cycle and by part (d) \( N = A_n \) and \( A_n \) is simple (in fact, this holds for \( n \geq 4 \)).

**Case III.** If \( N \) contains a permutation of the form \( \sigma = \mu(a_4, a_5, a_6)(a_1, a_2, a_3) \) where \( \mu \) contains none of \( a_1, a_2, a_3, a_4, a_5, a_6 \), then \( (a_1, a_2, a_4)\sigma(a_1, a_2, a_4)^{-1} \in N \) since \( N \) is a normal subgroup (by Theorem 14.13). So

\[ \sigma^{-1}((a_1, a_2, a_4)\sigma(a_1, a_2, a_4)^{-1}) \]

\[ = (a_3, a_2, a_1)(a_6, a_5, a_4)\mu^{-1}(a_1, a_2, a_4)\mu(a_4, a_5, a_6)(a_1, a_2, a_3)(a_4, a_2, a_1) \]

\[ = (a_3, a_2, a_1)(a_6, a_5, a_4)(a_1, a_2, a_4)(a_4, a_5, a_6)(a_1, a_2, a_3)(a_4, a_2, a_1) \]

since \( \mu \) and \( \mu^{-1} \) are disjoint from the other cycles

\[ = (a_1, a_4, a_2, a_6, a_3) \in N. \]

So \( N \) contains a cycle of length greater than 3 and by Case II, \( N = A_n \) and \( A_n \) is simple (notice this case requires \( n \geq 6 \)).

**Case IV.** If \( N \) contains a permutation of the form \( \sigma = \mu(a_1, a_2, a_3) \) where \( \mu \) contains none of \( a_1, a_2, a_3 \), and is a product of disjoint 2-cycles, then

\[ \sigma^2 = \mu(a_1, a_2, a_3)\mu(a_1, a_2, a_3) \]

\[ = \mu^2(a_1, a_2, a_3)(a_1, a_2, a_3) \text{ since } \mu \text{ is disjoint from the 3-cycles} \]

\[ = (a_1, a_2, a_3)(a_1, a_2, a_3) \text{ since } \mu^2 = \iota \text{ because } \mu \text{ is a product of disjoint 2-cycles} \]

\[ = (a_1, a_3, a_2) \in N. \]
Case V. If $N$ contains a permutation of the form $\sigma = \mu(a_3, a_4)(a_1, a_2)$ where $\mu$ contains none of $a_1, a_2, a_3, a_4$ and $\mu$ is a product of an even number of disjoint 2-cycles, then $(a_1, a_2, a_3)\sigma(a_1, a_2, a_3)^{-1} \in N$ since $N$ is a normal subgroup (by Theorem 14.13). So

$$\sigma^{-1}((a_1, a_2, a_3)\sigma(a_1, a_2, a_3)^{-1})$$

$$= (a_1, a_2)(a_3, a_4)\mu^{-1}(a_1, a_2, a_3)\mu(a_3, a_4)(a_1, a_2)(a_3, a_2, a_1)$$

$$= (a_1, a_2)(a_3, a_4)(a_1, a_2, a_3)(a_3, a_4)(a_a, a_2)(a_3, a_2, a_1)$$

since $\mu$ and $\mu^{-1}$ are disjoint from the other cycles

$$= (a_1, a_3)(a_2, a_4) = \alpha \in N.$$ 

Let $\beta = (a_1, a_3, i) = (a_1, i)(a_3, a_1) \in A_n$ for some $i$ different from $a_1, a_2, a_3, a_4$ (so we need $n \geq 5$ here). Since $N$ is a normal subgroup and $\alpha \in N$ then $\beta^{-1}\alpha\beta \in N$ by Theorem 14.13. So

$$(\beta^{-1}\alpha\beta)\alpha = (i, a_3, a_1)(a_1, a_3)(a_2, a_4)(a_1, a_3, i)(a_1, a_3)(a_2, a_4) = (a_1, a_3, i) \in N.$$ 

So $N$ contains a 3-cycle and by Case I, $N = A_n$ and $A_n$ is simple (this case holds for $n \geq 5$).

\[\blacksquare\]

**Note.** Alternating groups $A_n$ are of order $n!/2$ and are only defined for $n \geq 2$. When $n = 2$, $A_2 = \{e\}$ is the trivial group and so is not simple. When $n = 3$, $|A_3| = 3!/2 = 2$ and there is only one group (up to isomorphism) of order 3, so $A_3 \cong \mathbb{Z}_3$ and $A_3$ is also simple. For $n = 4$, Case V might apply, but Case V requires $n \geq 5$ in the proof that $A_n$ is simple. In fact, $A_4$ has a proper nontrivial normal subgroup of order 4 (namely, $N = \{1, (1, 3)(2, 4), (1, 4)(2, 3), (1, 2)(3, 4)\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$).
Note. A multiplication table for $A_4$ is given below. We follow the notation of *Schaum’s Outline of Theory and Problems of Group Theory* by Benjamin Baumslag and Bruce Chandler, NY: McGraw-Hill (1968). The table is broken up in a way as to reveal the cosets. The normal subgroup is $N = \{\iota, (1, 3)(2, 4), (1, 4)(2, 3), (1, 2)(3, 4)\} = \{\iota, \sigma_2, \sigma_5, \sigma_8\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. You can tell by the structure of the table that $A_4/N \cong \mathbb{Z}_3$.

$$
\begin{align*}
\iota &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} & \sigma_2 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} & \sigma_5 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} & \sigma_8 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \\
\tau_1 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} & \tau_2 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} & \tau_3 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} & \tau_4 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} \\
\tau_5 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} & \tau_6 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} & \tau_7 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} & \tau_8 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}
\end{align*}
$$

$$
\begin{array}{|c|c|c|c|c|c|c|c|}
\hline
 & \iota & \sigma_2 & \sigma_5 & \sigma_8 & \tau_1 & \tau_4 & \tau_5 & \tau_8 \\
\hline
\iota & \iota & \sigma_2 & \sigma_5 & \sigma_8 & \tau_1 & \tau_4 & \tau_5 & \tau_8 \\
\sigma_2 & \sigma_2 & \iota & \sigma_8 & \sigma_5 & \tau_1 & \tau_4 & \tau_5 & \tau_8 \\
\sigma_5 & \sigma_5 & \sigma_8 & \iota & \sigma_2 & \tau_1 & \tau_4 & \tau_5 & \tau_8 \\
\sigma_8 & \sigma_8 & \sigma_5 & \sigma_2 & \iota & \tau_1 & \tau_4 & \tau_5 & \tau_8 \\
\tau_1 & \tau_1 & \tau_8 & \tau_4 & \tau_5 & \tau_2 & \tau_6 & \tau_7 & \tau_3 \\
\tau_4 & \tau_4 & \tau_5 & \tau_1 & \tau_8 & \tau_2 & \tau_6 & \tau_7 & \tau_3 \\
\tau_5 & \tau_5 & \tau_4 & \tau_8 & \tau_1 & \tau_3 & \tau_7 & \tau_6 & \tau_2 \\
\tau_8 & \tau_8 & \tau_1 & \tau_5 & \tau_4 & \tau_6 & \tau_2 & \tau_3 & \tau_7 \\
\tau_2 & \tau_2 & \tau_3 & \tau_6 & \tau_7 & \iota & \sigma_5 & \sigma_8 & \sigma_2 \\
\tau_3 & \tau_3 & \tau_2 & \tau_7 & \tau_6 & \sigma_5 & \iota & \sigma_2 & \sigma_8 \\
\tau_6 & \tau_6 & \tau_7 & \tau_2 & \tau_3 & \sigma_8 & \sigma_2 & \iota & \sigma_5 \\
\tau_7 & \tau_7 & \tau_6 & \tau_3 & \tau_2 & \sigma_2 & \sigma_8 & \sigma_5 & \iota \\
\hline
\end{array}
$$

Revised: 1/10/2013