SIMPLICITY OF $A_n$

KEITH CONRAD

1. Introduction

A finite group is called simple when it is nontrivial and its only normal subgroups are the trivial subgroup and the whole group.

For instance, a finite group of prime order is simple, since it in fact has no non-trivial proper subgroups at all (normal or not). A finite abelian group $G$ not of prime order is not simple: let $p$ be a prime factor of $|G|$, so $G$ contains a subgroup of order $p$, which is normal since $G$ is abelian and is proper since $|G| > p$. Thus, the abelian finite simple groups are the groups of prime order.

When $n \geq 3$ the group $S_n$ is not simple since it has the normal subgroup $A_n$ of index 2.

Theorem 1.1. For $n \geq 5$, the group $A_n$ is simple.

This is due to Camille Jordan [6, p. 66] in 1870. The special case $n = 5$ goes back to Galois. The restriction $n \geq 5$ is optimal, since $A_4$ is not simple: it has the normal subgroup $\{(1), (12)(34), (13)(24), (14)(23)\}$. The group $A_3$ is simple, since it has order 3, and the groups $A_1$ and $A_2$ are trivial.

We will give five proofs of Theorem 1.1. Section 2 includes some preparatory material and later sections give the proofs of Theorem 1.1. In the final section, we give a quick application of the simplicity of alternating groups and some references for further proofs not treated here.

2. Preliminaries

We need three lemmas, two about alternating groups and one about symmetric groups on $n$ letters for $n \geq 5$.

Lemma 2.1. For $n \geq 3$, $A_n$ is generated by 3-cycles. For $n \geq 5$, $A_n$ is generated by permutations of type (2, 2).

Proof. That the 3-cycles generate $A_n$ for $n \geq 3$ has been seen earlier in the course. To show permutations of type (2, 2) generate $A_n$ for $n \geq 5$, it suffices to write each 3-cycle $(abc)$ in terms of such permutations. Pick $d, e \notin \{a, b, c\}$. Then note

$$(abc) = (ab)(de)(de)(bc).$$

The 3-cycles in $S_n$ are all conjugate in $S_n$, since permutations of the same cycle type in $S_n$ are conjugate. Are 3-cycles conjugate in $A_n$? Not when $n = 4$: (123) and (132) are not conjugate in $A_4$. But for $n \geq 5$ we do have conjugacy in $A_n$.

Lemma 2.2. For $n \geq 5$, all 3-cycles in $A_n$ are conjugate in $A_n$.
Proof. We show every 3-cycle in \( A_n \) is conjugate within \( A_n \) to \((123)\). Let \( \sigma \) be a 3-cycle in \( A_n \). It can be conjugated to \((123)\) in \( S_n \):

\[
(123) = \pi \sigma \pi^{-1}
\]

for some \( \pi \in S_n \). If \( \pi \in A_n \) we’re done. Otherwise, let \( \pi' = (45)\pi \), so \( \pi' \in A_n \) and

\[
\pi' \sigma \pi'^{-1} = (45)\pi \sigma \pi^{-1}(45) = (45)(123)(45) = (123).
\]

\[\square\]

**Example 2.3.** The 3-cycles \((123)\) and \((132)\) are not conjugate in \( A_4 \). But in \( A_5 \) we have

\[
(132) = \pi(123)\pi^{-1}
\]

for \( \pi = (45)(12) \in A_5 \).

Most proofs of the simplicity of the groups \( A_n \) are based on Lemmas 2.1 and 2.2. The basic argument is this: show each nontrivial normal subgroup \( N \triangleleft A_n \) contains a 3-cycle, so \( N \) contains every 3-cycle by Lemma 2.2, and therefore \( N \) is \( A_n \) by Lemma 2.1.

The next lemma will be used in our fifth proof of the simplicity of alternating groups.

**Lemma 2.4.** For \( n \geq 5 \), the only nontrivial proper normal subgroup of \( S_n \) is \( A_n \). In particular, the only subgroup of \( S_n \) with index 2 is \( A_n \).

**Proof.** The last statement follows from the first since every subgroup of index 2 is normal.

Let \( N \triangleleft S_n \) with \( N \neq \{(1)\} \). We will show \( A_n \subset N \), so \( N = A_n \) or \( S_n \).

Pick \( \sigma \in N \) with \( \sigma \neq (1) \). That means there is an \( i \) with \( \sigma(i) \neq i \). Pick \( j \in \{1,2,\ldots,n\} \) so \( j \neq i \) and \( j \neq \sigma(i) \). Let \( \tau = (ij) \). Then

\[
\sigma \tau \sigma^{-1} \tau^{-1} = (\sigma(i) \sigma(j))(ij).
\]

Since \( \sigma(i) \neq i \) or \( j \) and \( \sigma(i) \neq \sigma(j) \) (why?), the 2-cycles \((\sigma(i) \sigma(j))\) and \((ij)\) are unequal, so their product is not the identity. That shows \( \sigma \neq \tau \sigma \).

Since \( N \triangleleft S_n \), \( \sigma \tau \sigma^{-1} \tau^{-1} \) lies in \( N \). By construction, \( \sigma(i) \neq i \) or \( j \). If \( \sigma(j) \neq i \) or \( j \), then \((\sigma(i) \sigma(j))(ij)\) has type \((2,2)\). If \( \sigma(j) = i \) or \( j \), then \((\sigma(i) \sigma(j))(ij)\) is a 3-cycle. Thus \( N \) contains a permutation of type \((2,2)\) or a 3-cycle. Since \( N \triangleleft S_n \), \( N \) contains all permutations of type \((2,2)\) or all 3-cycles. In either case, this shows (by Lemma 2.1) that \( N \supset A_n \). \[\square\]

**Remark 2.5.** There is an analogue of Lemma 2.4 for the “countable” symmetric group \( S_\infty \) consisting of all permutations of \( \{1,2,3,\ldots\} \). A theorem of Schreier and Ulam (1933) says the only nontrivial proper normal subgroups of \( S_\infty \) are \( \cup_{n \geq 1} S_n \) and \( \cup_{n \geq 1} A_n \), which are the subgroup of permutations fixing all but a finite number of terms and its subgroup of even permutations.

**Remark 2.6.** By Lemma 2.4, for \( n \geq 5 \) each homomorphic image of \( S_n \) not isomorphic to \( S_n \) has order 1 or 2. So there is no surjective homomorphism \( S_n \to \mathbb{Z}/m \) for \( m \geq 3 \).

**Theorem 2.7.** For \( n \geq 5 \), no subgroup of \( S_n \) has index strictly between 2 and \( n \). Moreover, each subgroup of index \( n \) in \( S_n \) is isomorphic to \( S_{n-1} \).

**Proof.** Let \( H \) be a proper subgroup of \( S_n \) and let \( m := [S_n : H] \), so \( m \geq 2 \). If \( m = 2 \) then \( H = A_n \) by Lemma 2.4. If \( m < n \) then we will show \( m = 2 \). The left multiplication action of \( S_n \) on \( S_n/H \) gives a group homomorphism

\[
\varphi: S_n \to \text{Sym}(S_n/H) \cong S_m.
\]

By hypothesis \( m < n \), so \( \varphi \) is not injective. Let \( K \) be the kernel of \( \varphi \), so \( K \subset H \) and \( K \) is non-trivial. Since \( K \triangleleft S_n \), Lemma 2.4 says \( K = A_n \) or \( S_n \). Since \( K \subset H \), we get \( H = A_n \) or \( S_n \), which implies \( m = 2 \). Therefore we can’t have \( 2 < m < n \).
Now let $H$ be a subgroup of $S_n$ with index $n$. Consider the left multiplication action of $S_n$ on $S_n/H$. This is a homomorphism $\ell: S_n \to \text{Sym}(S_n/H)$. Since $S_n/H$ has order $n$, $\text{Sym}(S_n/H)$ is isomorphic to $S_n$. The kernel of $\ell$ is a normal subgroup of $S_n$ that lies in $H$ (why?). Therefore the kernel has index at least $n$ in $S_n$. Since the only normal subgroups of $S_n$ are 1, $A_n$, and $S_n$, the kernel of $\ell$ is trivial, so $\ell$ is an isomorphism. What is the image $\ell(H)$ in $\text{Sym}(S_n/H)$? Since $gH = H$ if and only if $g \in H$, $\ell(H)$ is the group of permutations of $S_n/H$ that fixes the “point” $H$ in $S_n/H$. The subgroup fixing a point in a symmetric group isomorphic to $S_n$ is isomorphic to $S_{n-1}$. Therefore $H \cong \ell(H) \cong S_{n-1}$. \qed

Theorem 2.7 is false for $n = 4$: $S_4$ contains the dihedral group of order 8 as a subgroup of index 3. An analogue of Theorem 2.7 for alternating groups will be given in Section 8; its proof will use the simplicity of the alternating groups.

Remark 2.8. That $S_n$ has no subgroup with index strictly between 2 and $n$ when $n \geq 5$ is due to Bertrand [1, p. 129] with an incomplete proof that relied on “Bertrand’s postulate” that there is a prime strictly between $n$ and $2n - 2$ for $n \geq 4$. He checked there is such a prime for $n$ up to 3 million and it was proved in general by Chebyshev several years later.

Corollary 2.9. Let $F$ be a field. If $f \in F[X_1, \ldots, X_n]$ and $n \geq 5$, the number of different polynomials we get from $f$ by permuting its variables is either 1, 2, or at least $n$.

Proof. Letting $S_n$ act on $F[X_1, \ldots, X_n]$ by permutations of the variables, the polynomials we get by permuting the variables of $f$ is the $S_n$-orbit of $f$. The size of this orbit is $|S_n : H|$, where $H = \text{Stab}_f = \{\sigma \in S_n : \sigma f = f\}$. By Theorem 2.7, this index is either 1, 2, or at least $n$. \qed

Corollary 2.9 is not true when $n = 4$. Here is a counterexample.

Example 2.10. In $F[X_1, X_2, X_3, X_4]$, let $f = X_1X_2 + X_3X_4$. Its $S_4$-orbit has 3 values:

\[
X_1X_2 + X_3X_4, \quad X_1X_3 + X_2X_4, \quad X_1X_4 + X_2X_3.
\]

3. FIRST PROOF

Our first proof of Theorem 1.1 is based on the one in [3, pp. 149–150].

We begin by showing $A_5$ is simple.

Theorem 3.1. The group $A_5$ is simple.

Proof. We want to show the only normal subgroups of $A_5$ are $\{(1)\}$ and $A_5$. This will be done in two ways.

Our first method involves counting the orders of the conjugacy classes. There are 5 conjugacy classes in $A_5$, with representatives and orders as indicated in the following table.

<table>
<thead>
<tr>
<th>Rep</th>
<th>(1)</th>
<th>(12345)</th>
<th>(21345)</th>
<th>(12)(34)</th>
<th>(123)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Order</td>
<td>1</td>
<td>12</td>
<td>12</td>
<td>15</td>
<td>20</td>
</tr>
</tbody>
</table>

If $A_5$ has a normal subgroup $N$, then $N$ is a union of conjugacy classes – including $\{(1)\}$ – whose total size divides 60. However, no sum of the above numbers that includes 1 is a factor of 60 except for 1 and 60. Therefore $N$ is trivial or $A_5$.

For the second proof, let $N \triangleleft A_5$ with $|N| > 1$. We will show $N$ contains a 3-cycle. It follows that $N = A_n$ by Lemmas 2.1 and 2.2.
Pick $\sigma \in N$ with $\sigma \neq (1)$. The cycle structure of $\sigma$ is $(abc), (ab)(cd)$, or $(abcde)$, where different letters represent different numbers. Since we want to show $N$ contains a 3-cycle, we may suppose $\sigma$ has the second or third cycle type. In the second case, $N$ contains


In the third case, $N$ contains

$$( (abc)(abcde)(abc)^{-1})(abcde)^{-1} = (adebc)(aedcb) = (abd).$$

Therefore $N$ contains a 3-cycle, so $N = A_5$. \hfill \Box

**Lemma 3.2.** When $n \geq 5$, each nontrivial $\sigma$ in $A_n$ has a conjugate $\sigma' \neq \sigma$ such that $\sigma(i) = \sigma'(i)$ for some $i$.

For example, if $\sigma = (12345)$ in $A_5$ then $\sigma' = (345)(345)^{-1} = (12453)$ has the same value at $i = 1$ as $\sigma$ does.

**Proof.** Let $\sigma$ be a non-identity element of $A_n$. Let $r$ be the longest length of a disjoint cycle in $\sigma$. Relabelling, we may write

$$\sigma = (12\ldots r)\pi,$$

where $(12\ldots r)$ and $\pi$ are disjoint.

If $r \geq 3$, let $\tau = (345)$ and $\sigma' = \tau \sigma \tau^{-1}$. Then $\sigma(1) = 2, \sigma'(1) = 2, \sigma(2) = 3$, and $\sigma'(2) = 4$. Thus $\sigma' \neq \sigma$ and both take the same value at 1.

If $r = 2$, then $\sigma$ is a product of disjoint transpositions. If there are at least 3 disjoint transpositions involved, then $n \geq 6$ and we can write $\sigma = (12)(34)(56)(\ldots)$ after relabelling. Let $\tau = (12)(35)$ and $\sigma' = \tau \sigma \tau^{-1}$. Then $\sigma(1) = 2, \sigma'(1) = 2, \sigma(3) = 4$, and $\sigma'(3) = 6$. Again, we see $\sigma' \neq \sigma$ and $\sigma$ and $\sigma'$ have the same value at 1.

If $r = 2$ and $\sigma$ is a product of 2 disjoint transpositions, write $\sigma = (12)(34)$ after relabelling. Let $\tau = (132)$ and $\sigma' = \tau \sigma \tau^{-1} = (13)(24)$. Then $\sigma' \neq \sigma$ and they both fix 5. \hfill \Box

Now we prove Theorem 1.1.

**Proof.** We may suppose $n \geq 6$, by Theorem 3.1. For $1 \leq i \leq n$, let $A_n$ act in the natural way on $\{1, 2, \ldots, n\}$ and let $H_i \subset A_n$ be the subgroup fixing $i$, so $H_i \cong A_{n-1}$. By induction, each $H_i$ is simple. Note each $H_i$ contains a 3-cycle (build out of 3 numbers other than $i$).

Let $N \triangleleft A_n$ be a nontrivial normal subgroup. We want to show $N = A_n$. Pick $\sigma \in N$ with $\sigma \neq (1)$. By Lemma 3.2, there is a conjugate $\sigma'$ of $\sigma$ such that $\sigma' \neq \sigma$ and $\sigma(i) = \sigma'(i)$ for some $i$. Since $N$ is normal in $A_n$, $\sigma' \in N$. Then $\sigma^{-1}\sigma'$ is a non-identity element of $N$ that fixes $i$, so $N \cap H_i$ is a non-trivial subgroup of $H_i$. It is also a normal subgroup of $H_i$ since $N \triangleleft A_n$. Since $H_i$ is simple, $N \cap H_i = H_i$. Therefore $H_i \subset N$. Since $H_i$ contains a 3-cycle, $N$ contains a 3-cycle and we are done.

Alternatively, we can show $N = A_n$ when $N \cap H_i$ is non-trivial for some $i$ as follows. As before, since $N \cap H_i$ is a non-trivial normal subgroup of $H_i$, $H_i \subset N$. Without referring to 3-cycles, we instead note that the different $H_i$’s are conjugate subgroups of $A_n$: $\sigma H_i \sigma^{-1} = H_{\sigma(i)}$ for $\sigma \in A_n$. Since $N \triangleleft A_n$ and $N$ contains $H_i$, $N$ contains every $H_{\sigma(i)}$ for all $\sigma \in A_n$. Since $\sigma(i)$ can be an arbitrary element of $A_n$ as $\sigma$ varies in $A_n$, $N$ contains every $H_i$. Every permutation of type $(2,2)$ is in some $H_i$ since $n \geq 5$, so $N$ contains all permutations of type $(2,2)$. Every permutation in $A_n$ is a product of permutations of type $(2,2)$, so $N \supset A_n$. Therefore $N = A_n$. \hfill \Box
4. Second proof

Our next proof is taken from [8, p. 108]. It does not use induction on \( n \), but we do need to know \( A_6 \) is simple at the start.

**Theorem 4.1.** The group \( A_6 \) is simple.

**Proof.** We follow the first method of proof of Theorem 3.1. Here is the table of conjugacy classes in \( A_6 \).

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Order</td>
<td>1</td>
<td>40</td>
<td>40</td>
<td>45</td>
<td>72</td>
<td>72</td>
<td>90</td>
</tr>
</tbody>
</table>

A tedious check shows no sum of these orders, which includes 1, is a factor of \( 6!/2 \) except for the sum of all the terms. Therefore the only non-trivial normal subgroup of \( A_6 \) is \( A_6 \). \( \Box \)

Now we prove the simplicity of \( A_n \) for larger \( n \) by reducing directly to the case of \( A_6 \).

**Proof.** Since \( A_5 \) and \( A_6 \) are known to be simple by Theorems 3.1 and 4.1, pick \( n \geq 7 \) and let \( N \triangleleft A_n \) be a non-trivial subgroup. We will show \( N \) contains a 3-cycle.

Let \( \sigma \) be a non-identity element of \( N \). It moves some number. By relabelling, we may suppose \( \sigma(1) \neq 1 \). Let \( \tau = (ijk) \), where \( i,j,k \) are not 1 and \( \sigma(1) \in \{i,j,k\} \). Then \( \tau \sigma \tau^{-1}(1) = \tau(\sigma(1)) \neq \sigma(1) \), so \( \tau \sigma \tau^{-1} \neq \sigma \). Let \( \varphi = \tau \sigma \tau^{-1} \sigma^{-1} \), so \( \varphi \neq (1) \). Writing

\[
\varphi = (\tau \sigma \tau^{-1}) \sigma^{-1},
\]

we see \( \varphi \in N \). Now write

\[
\varphi = \tau (\sigma \tau^{-1} \sigma^{-1}),
\]

Since \( \tau^{-1} \) is a 3-cycle, \( \sigma \tau^{-1} \sigma^{-1} \) is also a 3-cycle. Therefore \( \varphi \) is a product of two 3-cycles, so \( \varphi \) moves at most 6 numbers in \( \{1, 2, \ldots, n\} \). Let \( H \) be the copy of \( A_6 \) inside \( A_n \) corresponding to the even permutations of those 6 numbers (possibly augmented to 6 arbitrarily if in fact \( \varphi \) moves fewer numbers). Then \( N \cap H \) is non-trivial (it contains \( \varphi \)) and it is a normal subgroup of \( H \). Since \( H \cong A_6 \), which is simple, \( N \cap H = H \). Thus \( H \subset N \), so \( N \) contains a 3-cycle. \( \Box \)

5. Third proof

Our next proof is by induction, and uses conjugacy classes instead of Lemma 3.2. It is based on [11, §2,3].

**Lemma 5.1.** If \( n \geq 6 \) then every non-trivial conjugacy class in \( S_n \) and \( A_n \) has at least \( n \) elements.

The lower bound \( n \) in Lemma 5.1 is actually quite weak as \( n \) grows. But it shows that the size of each non-trivial conjugacy class in \( S_n \) and \( A_n \) grows with \( n \).

**Proof.** For \( n \geq 6 \), pick \( \sigma \in S_n \) with \( \sigma \neq (1) \). We want to look at the conjugacy class of \( \sigma \) in \( S_n \), and if \( \sigma \in A_n \) we also want to look at the conjugacy class of \( \sigma \) in \( A_n \), and our goal in both cases is to find at least \( n \) elements in the conjugacy class.

**Case 1:** The disjoint cycle decomposition of \( \sigma \) includes a cycle with length greater than 2. Without loss of generality, \( \sigma = (123\ldots)\ldots \).
For $3 \leq k \leq n$, fix a choice of $\ell \not\in \{1, 2, 3, k\}$ (which is possible since $n \geq 5$) and let $\alpha_k = (2k\ell)$ and $\beta_k = (3k\ell)$. Then $\alpha_k \sigma \alpha_k^{-1}$ has the effect $1 \to 1 \to 2 \to k$ and $\beta_k \sigma \beta_k^{-1}$ has the effect $1 \to 1 \to 2 \to 2$ and $2 \to 2 \to 3 \to k$. This tells us that the conjugates

$$\alpha_3 \sigma \alpha_3^{-1}, \ldots, \alpha_n \sigma \alpha_n^{-1}, \beta_3 \sigma \beta_3^{-1}, \ldots, \beta_n \sigma \beta_n^{-1}$$

are all different from each other: the conjugates by the $\alpha$’s have different effects on 1, the conjugates by the $\beta$’s have different effects on 2, and a conjugate by an $\alpha$ is not a conjugate by a $\beta$ since they have different effects on 1. Since these conjugates are different, the number of conjugates of $\sigma$ is at least $2(n-2) > n$. Because $\alpha_k$ and $\beta_k$ are 3-cycles, if $\sigma \in A_n$ then these conjugates are in the $A_n$-conjugacy class of $\sigma$.

Case 2: The disjoint cycle decomposition of $\sigma$ only has cycles with length 1 or 2. Therefore without loss of generality $\sigma$ is a transposition or a product of at least 2 disjoint transpositions.

If $\sigma$ is a transposition, then its $S_n$-conjugacy class is the set of all transpositions $(ij)$ where $1 \leq i < j \leq n$, and the number of these permutations is $\binom{n}{2} = \frac{n^2-n}{2}$, which is greater than $n$ for $n \geq 6$.

If $\sigma$ is a product of at least 2 disjoint transpositions, then without loss of generality $\sigma = (12)(34)\ldots$, where the terms in $\ldots$ don’t involve 1, 2, 3, or 4.

For $5 \leq k \leq n$, let $\alpha_k = (12)(3k), \beta_k = (13)(2k)$, and $\gamma_k = (1k)(23)$. Then $\alpha_k \sigma \alpha_k^{-1}$ has the effect

$$1 \to 2 \to 1 \to 2, \ 2 \to 1 \to 2 \to 1, \ k \to 3 \to 4 \to 4,$$

$\beta_k \sigma \beta_k^{-1}$ has the effect

$$1 \to 3 \to 4 \to 4, \ 3 \to 1 \to 2 \to k, \ k \to 2 \to 1 \to 3,$$

and $\gamma_k \sigma \gamma_k^{-1}$ has the effect

$$2 \to 3 \to 4 \to 4, \ 3 \to 2 \to 1 \to k, \ k \to 1 \to 2 \to 3.$$

The conjugates of $\sigma$ by the $\alpha$’s are different from each other since they take different elements to 4, the conjugates of $\sigma$ by the $\beta$’s are different from each other since they take different elements to 3, and the conjugates of $\sigma$ by the $\gamma$’s are different from each other since they take different elements to 3. Conjugates of $\sigma$ by an $\alpha$ and a $\beta$ are different since they send 1 to different places, conjugates of $\sigma$ by an $\alpha$ and a $\gamma$ are different since they send 2 to different places, and conjugates of $\sigma$ by a $\beta$ and a $\gamma$ are different since they send different elements to 4 (1 for the $\beta$’s and 2 for the $\gamma$’s). In total the number of conjugates of $\sigma$ we have written down (which are all conjugates by 3-cycles, hence they are conjugates in $A_n$ if $\sigma \in A_n$) is $3(n-4)$, and $3(n-4) \geq n$ if $n \geq 6$.

Now we prove Theorem 1.1.

**Proof.** We argue by induction on $n$, the case $n = 5$ having already been settled by Theorem 3.1. Say $n \geq 6$. Let $N < A_n$ with $N \neq \{(1)\}$. Since $N$ is normal and non-trivial, it contains non-identity conjugacy classes in $A_n$. By Lemma 5.1, each non-identity conjugacy class in $A_n$ has size at least $n$ when $n \geq 6$. Therefore, by counting the trivial conjugacy class and a non-trivial conjugacy class in $N$, we see $|N| \geq n + 1$.

Using a wholly different argument, we now show that $|N| \leq n$ if $N \neq A_n$, which will be a contradiction. Pick $1 \leq i \leq n$. Let $H_i \subset A_n$ be the subgroup fixing $i$, so $H_i \cong A_{n-1}$. In particular, $H_i$ is a simple group by induction. Notice each $H_i$ contains a 3-cycle.

The intersection $N \cap H_i$ is a normal subgroup of $H_i$, so simplicity of $H_i$ implies $N \cap H_i$ is either $\{(1)\}$ or $H_i$. If $N \cap H_i = H_i$ for some $i$, then $H_i \subset N$. Since $H_i$ contains a 3-cycle,
N does as well, so $N = A_n$ by Lemmas 2.1 and 2.2. (This part resembles part of our first proof of simplicity of $A_n$, but we will now use Lemma 5.1 instead of Lemma 3.2 to show the possibility that $N \cap H_i = \{1\}$ for all $i$ is absurd.)

Suppose $N \neq A_n$. Then, by the previous paragraph, $N \cap H_i = \{1\}$ for all $i$. Therefore each $\sigma \neq (1)$ in $N$ acts on $\{1, 2, \ldots, n\}$ without fixed points (otherwise $\sigma$ would be a non-identity element in some $N \cap H_i$). That implies each $\sigma \neq (1)$ in $N$ is completely determined by the value $\sigma(1)$: if $\tau \neq (1)$ is in $N$ and $\sigma(1) = \tau(1)$, then $\sigma \tau^{-1} \in N$ fixes 1, so $\sigma \tau^{-1}$ is the identity, so $\sigma = \tau$.

There are only $n - 1$ possible values for $\sigma(1) \in \{2, 3, \ldots, n\}$, so $N - \{1\}$ has size at most $n - 1$, hence $|N| \leq n$. We already saw from Lemma 5.1 that $|N| \geq n + 1$, so we have a contradiction. \hfill \Box

6. Fourth proof

Our next proof, based on [4, p. 50], is very computational.

Proof. Let $N \triangleleft A_n$ be a non-trivial normal subgroup. We will show $N$ contains a 3-cycle.

Pick $\sigma \in N$, $\sigma \neq (1)$. Write

$$\sigma = \pi_1 \pi_2 \cdots \pi_k,$$

where the $\pi_j$’s are disjoint cycles. In particular, they commute, so we can relabel them at our convenience. Eliminate all 1-cycles from the product.

Case 1: Some $\pi_i$ has length at least 4. Relabelling, we can write

$$\pi_1 = (12\cdots r)$$

with $r \geq 4$. Let $\varphi = (123)$. Then $\varphi \sigma \varphi^{-1} \in N$ and

$$\varphi \sigma \varphi^{-1} = \varphi \pi_1 \varphi^{-1} \pi_2 \cdots \pi_k = \varphi \pi_1 \varphi^{-1} \pi_1^{-1} \sigma = (123) (123 \cdots r) (132) (r \cdots 21) \sigma = (124) \sigma,$$

so $(124) = \varphi \sigma \varphi^{-1} \sigma^{-1} \in N$.

Case 2: Each $\pi_i$ has length $\leq 3$, and at least two have length 3 (so $n \geq 6$). Without loss of generality, $\pi_1 = (123)$ and $\pi_2 = (456)$. Let $\varphi = (124)$. Then

$$\varphi \sigma \varphi^{-1} = \varphi \pi_1 \pi_2 \varphi^{-1} \pi_3 \cdots \pi_k = \varphi \pi_1 \pi_2 \varphi^{-1} \pi_1^{-1} \pi_1^{-1} \sigma = (124) (123) (456) (142) (465) (132) \sigma = (12534) \sigma,$$

so $\varphi \sigma \varphi^{-1} \sigma^{-1} = (12534) \in N$. Now run through Case 1 with this 5-cycle to find a 3-cycle in $N$.

Case 3: Exactly one $\pi_i$ has length 3, and the rest have length $\leq 2$. Without loss of generality, $\pi_1 = (123)$ and the other $\pi_i$’s are 2-cycles. Then $\sigma^2 = \pi_1^2$ is in $N$, and $\pi_1^2 = (132)$.
Case 4: All $\pi_i$’s are 2-cycles, so necessarily $k > 1$. Write $\pi_1 = (12)$ and $\pi_2 = (34)$. Let $\varphi = (123)$. Then
\[
\varphi \sigma \varphi^{-1} = \varphi \pi_1 \pi_2 \varphi^{-1} \pi_3 \cdots \pi_k = \varphi \pi_1 \pi_2 \varphi^{-1} \pi_2^{-1} \pi_1^{-1} \sigma = (123)(12)(34)(132)(34)(12) \sigma = (13)(24)\sigma,
\]
so
\[
\varphi \sigma \varphi^{-1} \sigma^{-1} = (13)(24) \in N.
\]
Let $\psi = (135)$. Then
\[
\]
so $N$ contains a 3-cycle. \qed

7. Fifth proof

Our final proof is taken from [10, p. 295]. Let $N \triangleleft A_n$ with $N$ not $\{1\}$ or $A_n$. We will study $N$ as a subgroup of $S_n$. By Lemma 2.4, $N$ is not a normal subgroup of $S_n$. This means the normalizer of $N$ inside $S_n$ is a proper subgroup, which contains $A_n$, so

\[(7.1) \quad A_n = N_{S_n}(N).
\]

For a transposition $\tau$ in $S_n$, $\tau \not\in N_{S_n}(N)$ by (7.1), so $\tau N \tau^{-1} \neq N$. Since $N \triangleleft A_n$ and $\tau N \tau^{-1}$ is a subgroup of $A_n$, the product set $N \cdot \tau N \tau^{-1}$ is a subgroup of $A_n$. We have the chain of inclusions
\[
N \cap \tau N \tau^{-1} \subset N \subset N \cdot \tau N \tau^{-1} \subset A_n,
\]
where the first and second are strict.

We will now show, for each transposition $\tau$ in $S_n$, that

\[(7.2) \quad N \cap \tau N \tau^{-1} \triangleleft S_n, \quad N \cdot \tau N \tau^{-1} \triangleleft S_n.
\]

The proof of (7.2) is a bit tedious, so first let’s see why (7.2) leads to a contradiction.

It follows from (7.2) and Lemma 2.4 that

\[(7.3) \quad N \cap \tau N \tau^{-1} = \{(1)\}, \quad N \cdot \tau N \tau^{-1} = A_n
\]

for all transpositions $\tau$ in $S_n$. By (7.3), $|A_n| = |N| \cdot |\tau N \tau^{-1}| = |N|^2$, so $n! = 2|N|^2$. This tells us $|N|$ must be even, so $N$ has an element, say $\sigma$, of order 2. Then $\sigma$ is a product of disjoint 2-cycles. There is a transposition $\rho$ in $S_n$ that commutes with $\sigma$: just take for $\rho$ one of the transpositions in the disjoint cycle decomposition of $\sigma$. Then
\[
\sigma = \rho \sigma \rho^{-1} \in N \cap \rho N \rho^{-1}.
\]

From (7.3), using $\rho$ for the arbitrary $\tau$ there, $N \cap \rho N \rho^{-1}$ is trivial, so we have a contradiction. Another way of reaching a contradiction from the equation $n! = 2|N|^2$ uses Bertrand’s postulate (Remark 2.8), which implies $n!/2$ can’t be a perfect square since it is divisible once by a prime between $n!/4$ and $n!/2$.

It remains to check the two conditions in (7.2). In both cases, we show the subgroups are normalized by $A_n$ and by $\tau$, so the normalizer contains $\langle A_n, \tau \rangle = S_n$. 

First consider $N \cap \tau N \tau^{-1}$. It is clearly normalized by $\tau$. Now pick $\pi \in A_n$. Then $\pi N \pi^{-1} = N$ since $N \lhd A_n$, and

$$\pi(\tau N \tau^{-1})\pi^{-1} = \tau(\tau^{-1} \pi \tau) N (\tau^{-1} \pi^{-1} \tau) \tau^{-1} = \tau N \tau^{-1}$$

(7.4)

since $\tau^{-1} \pi \tau \in A_n$. Therefore

$$\pi(N \cap \tau N \tau^{-1})\pi^{-1} = \pi N \pi^{-1} \cap \pi \tau N \tau^{-1} \pi^{-1} = N \cap \tau N \tau^{-1},$$

so $A_n$ normalizes $N \cap \tau N \tau^{-1}$.

Now we look at $N \cdot \tau N \tau^{-1}$. Pick an element of this product, say

$$\sigma = \sigma_1 \tau \sigma_2 \tau^{-1},$$

where $\sigma_1, \sigma_2 \in N$. Then, since $N \lhd A_n$,

$$\tau \sigma \tau^{-1} = \tau \sigma_1 \tau \sigma_2 \tau^{-2} = \tau \sigma_1 \tau \sigma_2 \in \tau N \tau^{-1} \cdot N = N \cdot \tau N \tau^{-1},$$

which shows $\tau$ normalizes $N \cdot \tau N \tau^{-1}$.

Now pick $\pi \in A_n$. To see $\pi$ normalizes $N \cdot \tau N \tau^{-1}$, pick $\sigma$ as before. Then

$$\pi \sigma \pi^{-1} = \pi \sigma_1 \pi^{-1} \cdot \pi (\tau \sigma_2 \tau^{-1}) \pi^{-1}.$$

The first factor $\pi \sigma_1 \pi^{-1}$ is in $N$ since $N \lhd A_n$. The second factor is in $\pi \tau N \tau^{-1} \pi^{-1}$, which equals $\tau N \tau^{-1}$ by (7.4).

8. Concluding Remarks

The standard counterexample to the converse of Lagrange’s theorem is $A_4$: it has order 12 but no subgroup of index 2. For $n \geq 5$, the groups $A_n$ also have no subgroup of index 2, since each index-2 subgroup of a group would be normal and $A_n$ is simple.

In fact, something stronger is true.

**Corollary 8.1.** For $n \geq 5$, each proper subgroup of $A_n$ has index at least $n$.

This is an analogue of Theorem 2.7, but its proof is more sophisticated.

**Proof.** Let $H$ be a proper subgroup of $A_n$, with index $m > 1$. Consider the left multiplication action of $A_n$ on $A_n/H$. This gives a group homomorphism

$$\varphi: A_n \to \text{Sym}(A_n/H) \cong S_m.$$

Let $K$ be the kernel of $\varphi$, so $K \subset H$ (why?) and $K \lhd A_n$. By simplicity of $A_n$, $K$ is trivial. Therefore $A_n$ injects into $S_m$, so $(n!/2) \mid m!$, which implies $n \leq m$. \(\square\)

The lower bound of $n$ is sharp since $[A_n : A_{n-1}] = n$. Corollary 8.1 is false for $n = 4$: $A_4$ has a subgroup of index 3.

**Remark 8.2.** What the proof of Corollary 8.1 shows more generally is that if $G$ is a finite simple group and $H$ is a subgroup with index $m > 1$, then there is an embedding of $G$ into $S_m$, so $|G| \mid m!$. With $G$ fixed, this divisibility relation puts a lower bound on the index of a proper subgroup of $G$.

A reader who wants to read more proofs that $A_n$ is simple for $n \geq 5$ can see [5, pp. 247-248] or [7, pp. 32-33] for another way of showing a non-trivial normal subgroup contains a 3-cycle, or see [2, §1.7] or [9, pp. 295–296] for a proof based on the theory of highly transitive permutation groups.
References


