Simplicity of the alternating group A_n for $n \geq 5$

Sachin Kumar
University of Waterloo, Faculty of Mathematics

Abstract

In this essay, we will provide the required background (in form of *claims*) to prove that the alternating group A_n is simple for $n \geq 5$.

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

Proof. We will prove our following claims (which build a background for our proof):

Claim 1. For $n \geq 3$, A_n is generated by 3-cycles. For $n \geq 5$, A_n is generated by the permutations of type $(2, 2)$.

Proof of Claim 1. The identity (1) is (123)(132), which is a product of 3-cycles. Now pick an non-identity element of A_n, say σ and write it as a product of transpositions in S_n:

$$\sigma = \tau_1 \tau_2 \cdots \tau_r$$

The left side has sign 1 and the right side has sign $(-1)^r$, so r is even. Therefore, we can collect the products of the right into successive transpositions $\tau_i \tau_{i+1}$, where $i = 1, 3, \ldots$ is odd . We will now show every product of two transpositions in S_n is a product of two 3-cycles, so σ is a product of 3-cycles.

Case 1: τ_i and τ_{i+1} are equal. Then $\tau_i \tau_{i+1} = (1) = (123)(132)$, so we can replace $\tau_i \tau_{i+1}$ with a product of two 3-cycles.

Case 2: τ_i and τ_{i+1} have exactly one element in common. Let the common element be a, so we can write $\tau_i = (ab)$ and $\tau_{i+1} = (ac)$, where $b \neq c$. Then,

$$\tau_i \tau_{i+1} = (ab)(ac) = (acb) = (abc)(abc)$$

so we can replace $\tau_i \tau_{i+1}$ with a product of two 3-cycles.

Case 3: τ_i and τ_{i+1} have no element in common. This means τ_i and τ_{i+1} are disjoint, so we can write $\tau_i = (ab)$ and $\tau_{i+1} = (cd)$ where a, b, c, d are distinct, so $n \geq 4$. Then

$$\tau_i \tau_{i+1} = (ab)(cd) = (ab)(bc)(bc)(cd) = (bca)(adb) = (abc)(bcd)$$

so we can replace $\tau_i \tau_{i+1}$ with a product of two 3-cycles.

To show for $n \geq 5$ that A_n is generated by permutations of type $(2, 2)$, it suffices to write each 3-cycle (abc) in terms of such permutations. Pick $d, e \notin \{a, b, c\}$, we can do this since $n \geq 5$. Then note

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

and the permutations $(ab)(de)$ and $(de)(bc)$ have type $(2, 2)$, since a, b, c, d, e are distinct. □

Claim 2. For $n \geq 5$, all 3-cycles in A_n are conjugate in A_n.

Proof of Claim 2. We show every 3-cycle in A_n is conjugate within A_n to (123). Let σ 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

$$\pi'\sigma\pi'^{-1} = (45)\pi\sigma\pi^{-1}(45) = (45)(123)(45) = (123)$$

Hence proved. $\square$

Claim 3. When $n \geq 5$, each non-trivial σ in A_n has a conjugate $\sigma' \neq \sigma$ such that $\sigma(i) = \sigma'(i)$ for some i.

Proof of Claim 3. Let r be the longest length of a disjoint cycle in σ. By replacing σ with a conjugate permutation, which is also in A_n and has the effect of just relabeling the numbers form 1 to n when σ permutes in them, so we can assume the disjoint r-cycle in σ is $(12\dots r)$ and then we can write

$$\sigma = (12\dots r)\pi$$

where $(12\dots r)$ and π are disjoint.

If $r \geq 3$, let $\tau = (345)$ and $\sigma' = \tau\sigma\tau'$. 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 q.

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

If $r = 2$ and σ is a product of 2 disjoint transpositions, write $\sigma = (12)(34)$ after relabeling. Let $\tau = (132)$ and $\sigma' = \tau\sigma\tau' = (13)(24)$. Then $\sigma' \neq \sigma$ and they both fix at 5. $\square$

Now, we will prove that A_n is a simple group for $n \geq 5$. Let's consider the case, where $n = 5$. We want to show the only normal subgroups of A_5 are $\{(1)\}$ and A_5. Let $N \lhd A_5$ with $|N| > 1$. We will show N contains a 3-cycle. It follows that $N = A_n$ by *Claim 1* and *Claim 2.* Pick $\sigma \in N$ with $\sigma \neq (1)$. The cycle structure of σ is $(abc), (ab)(cd)$, or $(abcde)$, where different letters represent different numbers. Since, we want to show N contains a 3-cycles, we may suppose σ has the second and third cycle type. In the second case, N contains

$$((abe)(ab)(cd)(abe)^{-1})(ab)(cd) = (be)(cd)(ab)(cd) = (aeb)$$

In the third case, N contains,

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

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

Now, lets consider the case, where $n > 5$. For $1 \leq i \leq n$, let A_n act in the natural way on $\{1, 2, \dots, n\}$ 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, i.e., build out of 3 numbers other than i. Let $N \lhd A_n$ be a non-trivial normal subgroup. We want to show that $N = A_n$. Pick $\sigma \in N$ with $\sigma \neq \{(1)\}$. By *Claim 3.*, there is a conjugate σ' of σ 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 $N \lhd A_n$. 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, $N \lhd A_n$ 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 σ 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, $N = A_n$. $\square$