A_n is Simple for $n \geq 5$

Sarah Baker, Charlie Heil, Sooraj Soman, Braden Stillmaker

November 2024

Contents

1 Introduction **1**

2 Preliminary Lemmas **1**
Lemma 1 . . . 1
Lemma 1.1 . . . 2
Lemma 1.2 . . . 2
Lemma 1.3 . . . 2
Lemma 2 : A_5 and A_6 are simple . . . 2

3 A_n is simple for $n > 6$ **3**

References **4**

1 Introduction

We will show that A_n is simple for $n \geq 5$. A group is simple when it is nontrivial and there are no normal subgroups besides the trivial group and the group itself. To say n must be greater than 5, we first must look at A_1 through A_4. We know A_1 and A_2 are trivial and therefore not simple groups. Next, A_3 is simple because it has order 3, but A_4 has a normal subgroup, {(1), (1 2)(3 4), (1 3)(2 4), (1 4)(2 3)}, and as a result is not a simple group.

This proof was written by Évariste Galois in the early 1800's. The motivation for Galois to write this proof was to explain the insolvability of quintic functions. This proof has become a fundamental part of group theory. It was Camille Jordan that officially published the proof in his book, "Traité des substitutions et des équations algébriques" [**?**]. Many other mathematicians, such as Leonard Dickson, made advancements in understanding simple groups based on this proof [2].

We will prove that A_n is simple for $n \geq 5$ by first proving five lemmas, then the theorem.

2 Preliminary Lemmas

Lemma 1. *For $n \geq 3$, A_n is generated by 3-cycles.*

Proof. The identity $e = (1) = (1\ 2\ 3)(1\ 3\ 2)$ is a product of 3-cycles. Let σ be a non identity element in A_n, $\sigma = \tau_1\tau_2...\tau_r$ where σ is a product of transpositions.

We know that $\text{sign}(\sigma) = 1$ and $\text{sign}(\tau_1\tau_2...\tau_r) = (-1)^r$, thus r must be even.

Now, write the right side as successive transpositions, $\tau_i\tau_{i+1}$, where i is odd. Now, we will look at each case of transposition products in S_n:

Case 1: τ_i and τ_{i+1} are equal.

We see that $\tau_i\tau_{i+1} = (1) = (123)(132)$. Therefore, $\tau_i\tau_{i+1}$ is the 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 let $\tau_i = (ab)$ and $\tau_{i+1} = (ac)$ where $b \neq c$. From this we have $\tau_i\tau_{i+1} = (ab)(ac) = (acb) = (abc)(abc)$. Therefore, $\tau_i\tau_{i+1}$ is the product of two 3-cycles.

Case 3: τ_i and τ_{i+1} are disjoint.

Let $\tau_i = (ab)$ and $\tau_{i+1} = (cd)$. Then $\tau_i\tau_{i+1} = (ab)(cd) = (ab)(bc)(bc)(cd) = (bca)(cdb) = (abc)(bcd)$. Therefore, $\tau_i\tau_{i+1}$ is the product of two 3-cycles. □

Lemma 1.1. *Conjugacy is an equivalence relation.*

Proof. Let $g_1, g_2, g_3, x_1, x_2 \in G$ be arbitrary.

$g_1 = eg_1e^{-1}$, so conjugacy is reflexive.

If $g_1 = x_1g_2x_1^{-1}$, then $g_2 = x_1^{-1}g_1(x_1^{-1})^{-1}$, so conjugacy is symmetric.

If $g_1 = x_1g_2x_1^{-1}$ and $g_2 = x_2g_3x_2^{-1}$, then $g_1 = x_1(x_2g_3x_2^{-1})x_1^{-1} = (x_1x_2)g_3(x_1x_2)^{-1}$, so conjugacy is transitive.

Being reflexive, symmetric, and transitive, conjugacy is an equivalence relation. □

Lemma 1.2. *For $n \geq 5$, all 3-cycles in A_n are conjugate in A_n.*

Proof. Given a 3-cycle (abc),

$$(123) = (1a)(2b)(3c)(abc)(3c)(2b)(1a) = ((1a)(2b)(3c))(abc)((1a)(2b)(3c))^{-1}.$$

If $(1a)(2b)(3c)$ is in A_n, (abc) and (123) are conjugate in A_n. Otherwise,

$$\begin{aligned}(123) &= (45)(123)(45)\\ &= (45)((1a)(2b)(3c))(abc)((1a)(2b)(3c))^{-1}(45)\\ &= ((45)(1a)(2b)(3c))(abc)((45)(1a)(2b)(3c))^{-1}\end{aligned}$$

so (abc) and (123) are conjugate in A_n. In either case, we find all 3-cycles are conjugate in A_n to (123) and thus to each other. □

Lemma 1.3. *For $n \geq 5$, the conjugate of all 3-cycles in A_n are 3-cycles.*

Proof. Consider $\tau, \sigma \in A_n$, where τ is a 3-cycle (abc). Given $x \in \{a, b, c\}$,

$$\sigma\tau\sigma^{-1}(\sigma(x)) = \sigma(\tau(x)).$$

Thus σ contains the cycle $(\sigma(a)\sigma(b)\sigma(c))$. It remains to show that elements of $\{1, 2, ..., n\} \setminus \{\sigma(a), \sigma(b), \sigma(c)\}$ remain fixed under $\sigma\tau\sigma^{-1}$. Consider such an element n. σ is bijective and $\sigma^{-1}(\{\sigma(a), \sigma(b), \sigma(c)\}) = \{a, b, c\}$, so $\sigma^{-1}(n) \notin \{a, b, c\}$. Thus τ fixes $\sigma^{-1}(n)$ and $\sigma\tau\sigma^{-1}(n) = \sigma\sigma^{-1}(n) = n$, completing the proof. □

Lemma 2. *A_5 and A_6 are simple.*

Proof. If N is a normal subgroup of A_n, the conjugacy classes in A_n contained in N partition N since conjugacy is an equivalence relation and given $\sigma \in N$, $\sigma \in \{\pi\sigma\pi^{-1} \mid \pi \in A_n\} \subseteq N$. The conjugacy classes of A_5 and A_6 are given in Table 1 and Table 2, respectively.

Table 1: A_5 Conjugacy Classes

Representative	e	(12345)	(21345)	(12)(34)	(123)
Order	1	12	12	15	20

Table 2: A_6 Conjugacy Classes

Representative	e	(123)	(123)(456)	(12)(34)	(12345)	(23456)	(1234)(56)
Order	1	40	40	45	72	72	90

By Lagrange's theorem, any subgroup of A_5 or A_6 must have an order dividing 60 or 360 respectively. However, if N is a normal subgroup of A_5 or A_6, its order must be the sum of distinct entries including 1 (since N contains e) in the corresponding tables. However, the only such orders possible are 1 and 60, so N must be either trivial or non-proper. Thus A_5 and A_6 are simple. □

3 A_n is simple for $n > 6$

Proof. Suppose $N \trianglelefteq A_n$ be a non-trivial subgroup for $n > 6$. Let σ be a non-identity element of N, i.e., $\sigma(l) \neq l$ for some $l \in \{1, 2, \cdots, n\}$. Let $\tau = (i\ j\ k)$ where $i, j, k \neq l$ and $\sigma(l) \in \{i, j, k\}$. Then,

$$\begin{aligned} \tau\sigma\tau^{-1}(l) &= \tau(\sigma(l)) \neq \sigma(l) \\ \therefore \quad \tau\sigma\tau^{-1} &\neq \sigma \end{aligned} \tag{1}$$

Let $\mu = \tau\sigma\tau^{-1}\sigma^{-1}$ then $\mu \neq (1)$ since $\tau\sigma\tau^{-1} \neq \sigma$. Also, $\tau\sigma\tau^{-1} \in N$ since $\tau \in A_n$ and $\sigma \in N \trianglelefteq A_n$.

$$\sigma, \tau\sigma\tau^{-1} \in N \implies \mu = (\tau\sigma\tau^{-1})\sigma^{-1} \in N \tag{2}$$

Now,

$$\mu = \tau\sigma\tau^{-1}\sigma^{-1} = \tau(\sigma\tau^{-1}\sigma^{-1}) \tag{3}$$

Using lemma 1.3

$$\tau^{-1} \text{ is a 3-cycle} \implies -\sigma\tau^{-1}\sigma^{-1} \text{ is also a 3-cycle} \tag{4}$$

That means, $\mu = \tau(\sigma\tau^{-1}\sigma^{-1}) \in N$ is a product of two 3-cycles. Therefore, μ permutes at most 6 numbers in $\{1, \cdots, n\}$. Let H be the copy of A_6 inside A_n corresponding to the even permutations of these 6 numbers (augmented to 6 numbers arbitrarily if μ permutes fewer than 6 numbers), i.e., $H \cong A_6$. Since μ is a product of two 3-cycles, it is an even permutation on these 6 numbers. Therefore,

$$\begin{aligned} \mu \in H \quad \text{and} \quad \mu \in N \quad \textit{and} \quad \mu \neq (1) \\ \therefore \quad \mu \in N \cap H \implies N \cap H \text{ is non-trivial} \end{aligned} \tag{5}$$

Now, given $N \trianglelefteq A_n$ we have $gng^{-1} \in N$ for all $g \in A_n, n \in N$. For any $h \in H \leq A_n$ and $n \in N \cap H$,

$$\begin{aligned} h \in A_n \quad \text{and} \quad n \in N \quad \text{and} \quad N \trianglelefteq A_n \\ \therefore \quad hnh^{-1} \in N \end{aligned} \tag{6}$$

$$\begin{aligned} h^{-1} \in H \quad \text{and} \quad n \in H \\ \therefore \quad hnh^{-1} \in H \end{aligned} \tag{7}$$

From equations 6 and 7, $hnh^{-1} \in N \cap H$ for all $h \in H,\ n \in N \cap H$

$$\therefore \quad N \cap H \trianglelefteq H \tag{8}$$

Therefore, from equations 5 and 8, $N \cap H$ is non-trivial and $N \cap H \trianglelefteq H$. Since $H \cong A_6$ that is simple from the lemma 2, and therefore only contains the normal subgroups (1) and H. Therefore, $N \cap H \in \{(1), H\}$, and given that $N \cap H$ is nontrivial, $N \cap H = H$, and hence $H \subseteq N$.

A_6 contains all the even permutations of our 6 numbers and any 3-cycle is an even permutation. Therefore, A_6 contains 3-cycles. Then,

$$H \cong A_6 \implies H \text{ contains 3-cycles} \tag{9}$$
$$\therefore \quad H \subseteq N \implies N \text{ contains 3-cycles} \tag{10}$$

i.e., each non-trivial subgroup $N \trianglelefteq A_n$ contains a 3-cycle. Then, by lemma 1.3, N contains all 3-cycles. That means, using lemma 1, N contains all elements that generate A_n. Since $N \trianglelefteq A_n$, N must contain all the possible products of the elements that generate A_n. Therefore, N must contain every element of A_n. That means, $A_n \subseteq N$. Also, since $N \trianglelefteq A_n$ we have $N \subseteq A_n$. Combining both gives $N = A_n$, i.e., any non-trivial normal subgroup of A_n for $n > 6$ is A_n itself. □

4 Applications

The simplicity of A_n for $n \geq 5$ can be applied in showing the unsolvability of quintic polynomials. If the roots of a quintic may be found by a radical formula (such as the quadratic formula), then its Galois group is solvable. That is, there is a composition series $\{H_i\}$ of the Galois group such that H_{i+1}/H_i is abelian for all i. If there is a quintic with a Galois group isomorphic to S_5, then because $\{e\} < A_5 < S_5$ is a composition series, but A_n is simple for $n \geq 5$ as we have shown, so $A_5/\{e\}$ is not abelian. Thus the roots of such a quintic could not be found by a radical formula, which would mean that quintics (and, by extension, higher polynomials) cannot be, in general, solved by a radical formula as lower order polynomials can.

References

[1] Conrad, K. Simplicity of An.

[2] Judson, T. W. (2021). Abstract Algebra: Theory and Applications. Stephen F. Austin State University.

[3] Solomon, R. (2001). A brief history of the classification of the finite simple groups. Bulletin of the American Mathematical Society (New Series), 38(3), 315–352. https://doi.org/10.1090/S0273-0979-01-00934-0