Proceedings of Science and Mathematics
Faculty of Science,
Universiti Teknologi Malaysia

Volume 34, 2026, page 38-45

A Comparison of the Solvability of the Symmetric Group in Two Different Proofs of the Abel-Ruffini Theorem

Muhammad Ehsan Mohd Hamzah[a], Supian Mat Salleh[b], Wan Heng Fong[a*]
[a]Department of Mathematical Sciences, Faculty of Science, Universiti Teknologi Malaysia, Johor Bahru, Johor, Malaysia
[b]Department of Computational and Theoretical Sciences, Kulliyyah of Science, International Islamic University Malaysia, Kuantan, Pahang, Malaysia
*Corresponding author: fwh@utm.my

Abstract

The solvability of polynomial equations has been a central problem in mathematics for many years. A classical theorem is the Abel-Ruffini theorem, which states that there is no formula by radicals that solves a general quintic equation. One well-known proof of this theorem uses Galois theory, which was developed by Évariste Galois before his death in 1832. A more recent proof by Vladimir Arnold was published in 1974, which approaches the problem using topology. This research aims to find all possible subnormal series and derived series of the symmetric group S_n for $n \leq 5$. Then, this paper seeks to find relations between the two proofs based on their methodologies. Some properties of commutators and normal subgroups are presented, which are utilized to find the main results of this research. From these properties, it is shown that there exists a subnormal series of S_n that is equivalent to its derived series for $n \leq 5$. Finally, it is proven that the definitions of a solvable group used in both proofs are equivalent. These results suggest that the two proofs share a common condition for a polynomial to be solvable by radicals.

Keywords: Galois theory, topology, commutator, subnormal series, derived series

Introduction

In mathematics, a central problem which has existed for millennia is solving polynomial equations. The general formula for quadratic, cubic, and quartic equations were well known during the Renaissance era [1]. Throughout the 18th century, many attempts were made to produce a formula to solve the general quintic equation. It was finally proven in 1826 by Neils Henrik Abel that no formula exists for the solutions to the general quintic equation using only the arithmetic operations and finite number of nth roots [2]. This theorem is now known as the Abel-Ruffini theorem, which was a very significant result in mathematics at the time.

Not long after Abel's proof was published, the theorem was proven again by Évariste Galois before his death in 1832 using methods which are now known as Galois theory [1]. Galois theory combines group theory and field theory to analyze the group of permutations of the solutions to polynomials. Over a century later, the Russian mathematician Vladimir Arnold found another proof which was first published by his student Alekseev in 1976 in Russian and in English in 2004 [3]. Arnold's proof uses complex analysis, topology, and properties of commutators, removing the need of Galois theory. The exposition of Arnold's proof was first conducted by Żołądek [4] who explained the same proof presented by Arnold in a more concise manner. A more simplified explanation of the proof was made by Ramond [2] who made use of permutations of a polynomial's solutions and loops in the complex plane.

In this research, the subnormal series and derived series of the symmetric group S_n for $n \leq 5$ are found and compared since they are used in the proofs by Galois and Arnold, respectively. In addition, the relation between the proofs by Galois and Arnold is determined. This research first states some properties of commutator subgroups for any group G and S_n, which are related to normal subgroups and factor groups. From these properties, the subnormal series and derived series of S_n for $n \leq 5$ are determined and compared. Finally, the two definitions of a solvable group used in both proofs are proven to be equivalent.

This paper is organized as follows: Section 1 reviews the two proofs and the past studies done on Arnold's proof. Section 2 presents some preliminary concepts used for this research. In Section 3, the main results of the research are presented as propositions and a theorem. Finally, Section 4 gives concluding remarks and summarizes the outcomes of the research.

Preliminaries

In this section, some important definitions and properties that are applied in this research are presented. The definition of a solvable group used in Galois's proof of the Abel-Ruffini theorem is stated as follows.

Definition 2.1 [5] Solvable Group (used in Galois's proof)
A group G is called solvable if there exists a finite series of subgroups of G, called a subnormal series given by

$$G = G_n \geq G_{n-1} \geq \cdots \geq G_1 \geq G_0 = \{e\},$$

where G_i is a normal subgroup in G_{i+1}, such that G_{i+1}/G_i is abelian for $i = 0, 1, \ldots, n-1$.

Arnold's proof used the concept of a commutator and the commutator subgroup. The definitions of a commutator of two elements and the commutator subgroup are stated as follows.

Definition 2.2 [3] Commutator of Two Elements of a Group, Commutator Subgroup
Let a and b be any two elements of a group G. Then the commutator of a and b, denoted by $[a, b]$, is the product $aba^{-1}b^{-1}$. The subgroup generated by the commutators in G is called the commutator subgroup of G, denoted by $[G, G]$.

The following definition of a solvable group is used in Arnold's proof, which utilizes the series of commutator subgroups.

Definition 2.3 [2] Solvable Group (used in Arnold's proof)
A group G is called solvable if there exists a series of commutator subgroups, called a derived series given by

$$G^{(0)} = G, G^{(1)} = \left[G^{(0)}, G^{(0)}\right], G^{(2)} = \left[G^{(1)}, G^{(1)}\right], \ldots, G^{(i+1)} = \left[G^{(i)}, G^{(i)}\right]$$

for $i = 1, 2, 3, \ldots$ such that $G^{(n)} = \{e\}$ is the trivial group for some positive integer n.

Lastly, the following propositions give some properties of the symmetric group S_n and the alternating group A_n.

Proposition 2.1 [5]
For all n, the alternating group A_n has index two in the symmetric group S_n, which implies that A_n is a normal subgroup of S_n.

Proposition 2.2 [5]
The alternating group A_n is generated by 3-cycles for $n \geq 3$.

Proposition 2.3 [5]
Two elements in the symmetric group S_n are conjugate in S_n if and only if they have the same cycle type.

Main Results
Both proofs of the Abel-Ruffini theorem use different definitions of a solvable group which are applied to the symmetric group S_n. Galois's proof uses the subnormal series while the Arnold's proof uses the derived series. In this research, the subnormal series and derived series for S_n are determined and compared.

The normal subgroups of S_n are first identified. For $n = 1$, the case is trivial since $S_1 = \{e\}$ is the trivial group whose only normal subgroup is itself. Therefore, the only subgroup in the subnormal series of S_1 is itself. For S_2, the only proper subgroup is $\{e\}$, which has index two in S_2. Thus, $\{e\}$ is normal in S_2. Therefore, the subnormal series of S_2 is $\{e\} \lhd S_2$. For S_3, there are five proper subgroups: $\{e\}, \langle(1\ 2)\rangle, \langle(1\ 3)\rangle, \langle(2\ 3)\rangle$, and $\langle(1\ 2\ 3)\rangle$. The subgroup $\langle(1\ 2\ 3)\rangle$ is isomorphic to A_3, which is a normal subgroup of S_3 by Proposition 2.1. The only normal subgroup of A_3 is $\{e\}$. Therefore, the subnormal series of S_3 is $\{e\} \lhd A_3 \lhd S_3$.

It is less straightforward to determine the subnormal series of S_4. According to Sulaiman [6], there are 30 subgroups of S_4. The largest proper subgroup is A_4, and by Proposition 2.1, it is a normal subgroup of S_4. The proper nontrivial subgroups of A_4 are isomorphic to $\mathbb{Z}_2$, A_3, and V, where

$$V = \{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

is the Klein four-group. Moreover, the Klein four-group V is a normal subgroup of A_4 [5]. The proper normal subgroups of V are $\mathbb{Z}_2$ and $\{e\}$. Therefore, there are two possible subnormal series of S_4:

$$\{e\} \lhd V \lhd A_4 \lhd S_4 \quad \text{and} \quad \{e\} \lhd \mathbb{Z}_2 \lhd V \lhd A_4 \lhd S_4.$$

The group S_5 has one proper nontrivial normal subgroup, namely A_5. The alternating group A_5 is famously known to be a simple group [5]. Therefore, the only subnormal series of S_5 is $\{e\} \lhd A_5 \lhd S_5$.

Next, some properties of the commutator subgroup, which are needed to find the derived series of S_n, are presented. The following proposition is an important property of the commutator subgroup of abelian groups.

Proposition 3.1
If a group G is abelian, then its commutator subgroup is the trivial group $\{e\}$.

Proof. Since G is abelian, then for all elements $a, b \in G$, the commutator of a and b is

$$\begin{aligned}[a,b] &= aba^{-1}b^{-1} \\ &= aa^{-1}bb^{-1}\end{aligned}$$

$$= e.$$

Thus, all commutators in G is the identity element. Therefore, $[G, G] = \{e\}$. ■

Another important fact is that the derived series of any group is unique, which is stated in Proposition 3.2.

Proposition 3.2

The commutator subgroup of any group is unique, and thus the derived series of any group is unique.

Proof. Let G be a group and let $[G, G]$ be the subgroup generated by all the commutators $[a, b]$ in G where $a, b \in G$. By definition, this is the smallest subgroup containing every commutator in G and all their products. Since the subgroup generated by a subset of a group is unique, the commutator subgroup $[G, G]$ is unique.

The derived series is defined recursively by

$$G^{(0)} = G, G^{(i+1)} = \left[G^{(i)}, G^{(i)}\right] \text{ for } i = 0, 1, 2, \dots .$$

Since each commutator subgroup is unique for each group in the series of subgroups, it follows by induction that the derived series of any group G is also unique. ■

A useful property of the commutator subgroup of the symmetric group S_n is that it is equal to the alternating group A_n, as shown in the next proposition.

Proposition 3.3

For any n, the commutator subgroup of the symmetric group S_n is the alternating group A_n, i.e., $[S_n, S_n] = A_n$.

Proof. The property holds for $n = 1$ since $S_1 = A_1 = \{e\}$. For S_2, since it is an abelian group, by Proposition 3.1, $[S_2, S_2] = \{e\}$. In addition, $A_2 = \{e\}$ since the identity permutation is the only even permutation of two elements. Thus, the property holds for $n = 2$. Generally, for all n, $[S_n, S_n]$ consists of even permutations, thus, $[S_n, S_n] \leq A_n$. Now let $n \geq 3$. For the proof that $A_n \leq [S_n, S_n]$, let a, b, and c be distinct elements. Then any 3-cycle can be written as a commutator of transpositions (applying the transpositions from right to left):

$$(a\, b\, c) = (a\, c\, b)^2 = (a\, c)(c\, b)(a\, c)(c\, b).$$

Since A_n is generated by 3-cycles by Proposition 2.2, the elements of A_n can be written as commutators. Thus, $A_n \leq [S_n, S_n]$ and therefore, $[S_n, S_n] = A_n$. ■

The following properties are significant in that they are used to find the commutator subgroup of A_4 and the relationship between the two definitions of a solvable group.

Proposition 3.4

For any group G, the commutator subgroup $G^{(1)} = [G, G]$ is a normal subgroup of G.

Proof. Let $a, b, g \in G$ and $x = aba^{-1}b^{-1} \in G$ be a commutator in G. Then gxg^{-1} is a commutator in G since

$$gxg^{-1} = gaba^{-1}b^{-1}g^{-1}$$

$$\begin{aligned} &= (gag^{-1})(gbg^{-1})(ga^{-1}g^{-1})(gb^{-1}g^{-1}) \\ &= (gag^{-1})(gbg^{-1})(gag^{-1})^{-1}(gbg^{-1})^{-1}. \end{aligned}$$

Suppose $k = x_1x_2 \cdots x_n \in G^{(1)}$ where each x_i is a commutator in G. Then the conjugation of a product of commutators is a product of commutators:

$$\begin{aligned} gkg^{-1} &= gx_1x_2 \cdots x_ng^{-1} \\ &= (gx_1g^{-1})(gx_2g^{-1}) \cdots (gx_ng^{-1}). \end{aligned}$$

Thus, $gG^{(1)}g^{-1} \subseteq G^{(1)}$. Therefore, $G^{(1)}$ is a normal subgroup of G. ■

From Proposition 3.4, the factor group $G/G^{(1)}$ can be formed since $G^{(1)}$ is normal in G. This factor group is abelian, which is an important property for this research.

Proposition 3.5

Let G be a group and let $G^{(1)}$ be the commutator subgroup of G. Then the factor group $G/G^{(1)}$ is abelian.

Proof. Let $g, h \in G$ and $G^{(1)} = N$. Then $(gN)(hN)(g^{-1}N)(h^{-1}N) = (ghg^{-1}h^{-1})N$. The product $ghg^{-1}h^{-1}$ is a commutator, so $ghg^{-1}h^{-1} \in N$. Thus, $(ghg^{-1}h^{-1})N = N = eN$. Consequently,

$$\begin{aligned} (gN)(hN)(g^{-1}N)(h^{-1}N) &= eN \\ (gN)(hN)(gN)^{-1}(hN)^{-1} &= eN \\ (gN)(hN) &= eN(hN)(gN) \\ (gN)(hN) &= (hN)(gN). \end{aligned}$$

Hence, the product of cosets commute. Therefore, $G/N = G/G^{(1)}$ is an abelian group. ■

Lastly, the following property is a partial converse of Proposition 3.5, which states that an abelian factor group G/N implies that the commutator subgroup of G is a subgroup of N.

Proposition 3.6

Let G be a group and N be a normal subgroup of G such that G/N is abelian. Then $G^{(1)} \leq N$ where $G^{(1)}$ is the commutator subgroup of G.

Proof. Let $g, h \in G$. Since G/N is abelian, then

$$\begin{aligned} (gN)(hN) &= (hN)(gN) \\ (gN)(hN)(gN)^{-1}(hN)^{-1} &= N \\ (ghg^{-1}h^{-1})N &= N, \end{aligned}$$

which implies that $ghg^{-1}h^{-1} \in N$. Since g and h are arbitrary and N is a subgroup, N contains the products of all commutators in G. Therefore, $G^{(1)} \leq N$. ■

With all the necessary properties of commutator subgroups stated, the derived series of S_n for $n \leq 5$ can be determined. The derived series is trivial for S_1, which only has $\{e\}$ in its series. The symmetric group S_2 is abelian, so its commutator subgroup is $\{e\}$ by Proposition 3.1. Thus, the derived series of S_2 is S_2 and $\{e\}$. For S_3, its commutator subgroup is A_3 by Proposition 3.3. The alternating group A_3 is an abelian group, hence by Proposition 3.1, its commutator subgroup is $\{e\}$. Thus, the derived series of S_3 is S_3, A_3, and $\{e\}$.

For S_4, its commutator subgroup is A_4 by Proposition 3.3. The next proposition states the commutator subgroup of A_4.

Proposition 3.7
The commutator subgroup of A_4 is the Klein four-group V.

Proof. Firstly, it is claimed that V is a normal subgroup of A_4. This is because the non-identity permutations in V are of the form $(i\ j)(k\ l)$ for distinct elements i, j, k, and l. By Proposition 2.3, conjugation of any permutation in S_4 (and therefore in V) does not change the permutation's cycle type. Thus, V is a normal subgroup of A_4. The order of A_4 is 12 while the order of V is four. Hence, $A_4/V \cong \mathbb{Z}_3$, which is an abelian group. Hence, by Proposition 3.6, the commutator subgroup $A_4^{(1)}$ is a subgroup of V. Furthermore, since A_4 is nontrivial and contains even permutations, there exists permutations $(i\ j)(k\ l) \in A_4^{(1)}$. Hence, V is a subgroup of $A_4^{(1)}$. Therefore, $A_4^{(1)} = V$. ■

Since the Klein four-group V is abelian, its commutator subgroup is $\{e\}$ by Proposition 3.1. Therefore, the derived series of S_4 is S_4, A_4, V, and $\{e\}$.

For the group S_5, its commutator subgroup is A_5 by Proposition 3.3. The commutator subgroup of A_5 is itself, which is a significant result in Arnold's proof that a general quintic formula does not exist [2]. This is proven in the next proposition.

Proposition 3.8
The commutator subgroup of the alternating group A_5 is itself, i.e., $[A_5, A_5] = A_5$.

Proof. Let a, b, c, d, and e be five distinct elements. The group A_5 is a product of 3-cycles by Proposition 2.2. Then the commutator of any 3-cycles in A_5 is

$$\begin{aligned}[(a\ d\ c),(c\ b\ e)] &= (c\ b\ e)^{-1}(a\ d\ c)^{-1}(c\ b\ e)(a\ d\ c)\\ &= (b\ c\ e)(a\ c\ d)(c\ b\ e)(a\ d\ c)\\ &= (c\ e\ d) \in [A_5, A_5].\end{aligned}$$

The 3-cycle $(c\ e\ d)$ is arbitrary. Hence, the commutator of any 3-cycle in A_5 is also a 3-cycle. Since A_5 is a product of 3-cycles, then $[A_5, A_5] = A_5$. ■

This result implies that the derived series of S_5 terminates at A_5. Hence, the only subgroups in the derived series of S_5 are S_5 and A_5.

Thus, all the subnormal series and derived series of S_n for $n \leq 5$ are determined. Table 1 summarizes the findings thus far, showing the comparison of the two types of series for each S_n.

Table 1: All subnormal series and derived series of the symmetric group S_n for $n \leq 5$.

Group	Subnormal Series	Derived Series
S_1	$\{e\}$	$\{e\}$
S_2	$\{e\} \lhd S_2$	$S_2, \{e\}$
S_3	$\{e\} \lhd A_3 \lhd S_3$	$S_3, A_3, \{e\}$

S_4	$\{e\} \lhd V \lhd A_4 \lhd S_4$ and $\{e\} \lhd \mathbb{Z}_2 \lhd V \lhd A_4 \lhd S_4$	$S_4, A_4, V, \{e\}$
S_5	$\{e\} \lhd A_5 \lhd S_5$	S_5, A_5

From Table 1, there is a subnormal series of the symmetric group S_n for $n \leq 5$ that is identical to the group's derived series. Despite being defined differently, the resulting series exhibit similar structure in these cases. This suggests that there is a relationship between the two proofs of the Abel-Ruffini theorem. This pattern gives motivation for comparing the two definitions of the solvability of any group.

Next, a lemma is given to help show the equivalence of the two definitions of a solvable group, which states that commutator subgroups preserve subgroup relations.

Lemma 3.1

Let H be a subgroup of a group G. Then $[H,H]$ is a subgroup of $[G,G]$.

Proof. The group $[H,H]$ contains elements that are generated by the commutators in H which are also commutators in G. Hence, $[H,H]$ is a subgroup of $[G,G]$. ■

Lastly, it is shown in Theorem 3.1 that Definition 2.1 and Definition 2.3 are equivalent by using the properties of commutator subgroups. Theorem 3.1 is the main result of this research.

Theorem 3.1

A group G is solvable if either of the following statements is true:

(i) There exists a subnormal series of G,

$$G = G_k \trianglerighteq G_{k-1} \trianglerighteq \cdots \trianglerighteq G_1 \trianglerighteq G_0 = \{e\},$$

such that G_{i+1}/G_i is abelian for $i = 0, 1, \dots, k-1$.

(ii) The derived series of G,

$$G^{(0)} = G, G^{(1)} = [G,G], \dots, G^{(i+1)} = \left[G^{(i)}, G^{(i)}\right]$$

for $i = 1, 2, 3, \dots$, terminates at some positive integer n such that $G^{(n)} = \{e\}$.

Proof. Suppose there exists a series of subgroups as stated in (i). It is proven by induction that $G^{(i)} \leq G_{k-i}$. This is true for $i = 0$ since $G^{(0)} = G = G_k$. Assume $G^{(i)} \leq G_{k-i}$. Then by Lemma 3.1,

$$G^{(i+1)} = \left[G^{(i)}, G^{(i)}\right] \leq [G_{k-i}, G_{k-i}].$$

Since G_{k-i}/G_{k-i-1} is abelian, by Proposition 3.6, $[G_{k-i}, G_{k-i}] \leq G_{k-i-1}$. Thus, $G^{(i+1)} \leq G_{k-i-1}$, which completes the induction. Since $G_0 = \{e\}$, then $G^{(n)} = \{e\}$ for some positive integer n. Therefore, the series of subgroups as stated in (ii) exists.

Conversely, suppose the series of subgroups as stated in (ii) exists. By Proposition 3.4, $G^{(i+1)}$ is a normal subgroup in $G^{(i)}$ for $i = 0, 1, \dots, n-1$. Furthermore, each $G^{(i)}/G^{(i+1)}$ is abelian by Proposition 3.5. Therefore, there exists a series of subgroups $G = G^{(0)} \trianglerighteq G^{(1)} \trianglerighteq \cdots \trianglerighteq G^{(n)} = \{e\}$ where each $G^{(i)}/G^{(i+1)}$ is abelian for $i = 0, 1, \dots, n-1$, which is the series of subgroups stated in (i). ■

The result above explains how the proofs of the Abel-Ruffini theorem by Galois and Arnold reach the same conclusion. In both proofs, the criterion for the solvability of polynomials by radicals is based on similar series of subgroups of S_n. Despite the different construction of subgroup series used in each proof, the subgroups obtained proved to be identical.

Conclusion

In summary, the results of this research show some similarities in the construction of series of subgroups used in the two proofs of the Abel-Ruffini theorem. The subgroups in the derived series of S_n for $n \leq 5$ are found to be identical to the subgroups in the subnormal series. The definitions of a solvable group used in the two proofs were then proven to be equivalent, which explains that the identical subgroups found in the subnormal series and derived series are not just a coincidence. This relation suggests that some problems in Galois theory can be solved using topological methods as Arnold achieved in his proof. Further research can be carried out to explore more of these relations.

Acknowledgement

The authors would like to express sincere gratitude to all who have contributed throughout this research.

References

[1] Kiernan, B. M. (1971). The Development of Galois Theory from Lagrange to Artin. *Archive for History of Exact Sciences*, *8*(1), 40–154.

[2] Ramond, P. (2022). Abel-Ruffini’s Theorem: Complex but Not Complicated. *The American Mathematical Monthly*, *129*(3), 231–245.

[3] Alekseev, V. B. (2004). *Abel’s Theorem in Problems and Solutions: Based on the lectures of Professor V. I. Arnold*. Kluwer Academic Publishers.

[4] Żołądek, H. (2000). The Topological Proof of Abel-Ruffini Theorem. *Topological Methods in Nonlinear Analysis*, *16*, 253–265.

[5] Judson, T. W. (2023). *Abstract Algebra: Theory and Applications* (2023 ed.). Orthogonal Publishing L3c.

[6] Sulaiman, R. (2012). Subgroups Lattice of Symmetric Group S_4. *International Journal of Algebra*, *6*(1), 29–35.