

Why No Quintic Formula Exists: A No Galois Theory Approach

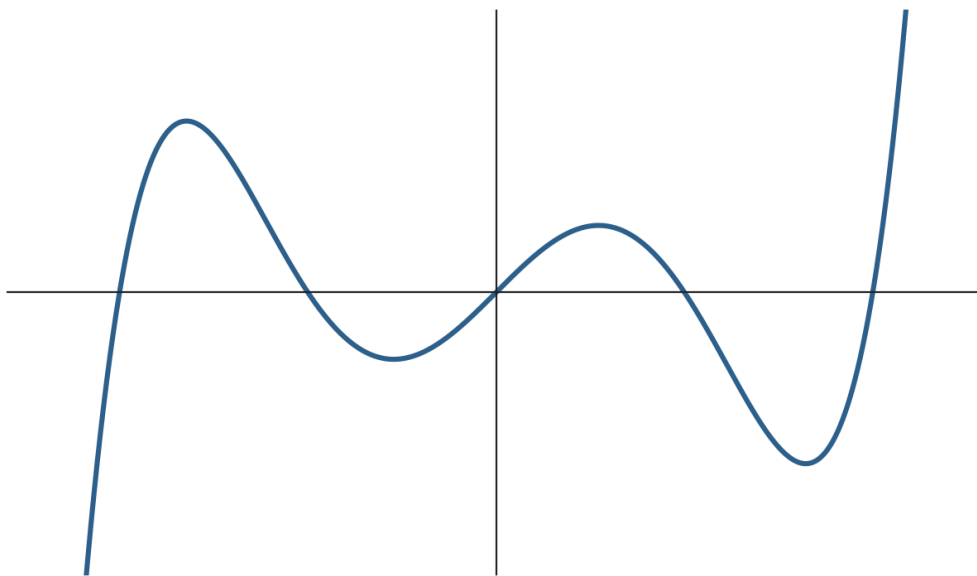
Udai Thenua

Contents

1	Introduction	2
2	Permutations of Roots	3
3	Multivaluedness	5
4	Loops and More Permutations	6
5	Radical Expressions and Nested Roots	8
6	Commutators	9
7	The Quintic	11

1 Introduction

The quadratic formula has been known for centuries, and by the 1700s mathematicians had found similar formulas for cubics and quartics. Yet no such formula exists for the quintic. This essay aims to explain, without the use of Galois Theory, why no such quintic formula can exist by making use of Vladimir Arnold's 1963 topological proof of the Abel-Ruffini theorem which links directly to the insolubility of the quintic. Please ensure that this pdf is opened in Adobe Acrobat or another pdf viewer that supports animations.



2 Permutations of Roots

The Fundamental Theorem of Algebra tells us a degree n polynomial has n roots, counting repeated roots.¹

Definition 2.1. A polynomial of degree n is called **separable** if it has n distinct roots.

Throughout this essay we'll focus only on separable polynomials as repeated roots do not affect the overall argument.

Let's look at a generic quintic again:

$$p(z) = az^5 + bz^4 + cz^3 + dz^2 + ez + f.$$

We know this must have five roots z_1, z_2, z_3, z_4, z_5 , so it can be written as

$$p(z) = (z - z_1)(z - z_2)(z - z_3)(z - z_4)(z - z_5).$$

However, we could equally write that

$$p(z) = (z - z_2)(z - z_1)(z - z_4)(z - z_3)(z - z_5)$$

or indeed any rearrangement, and the polynomial would remain unchanged. This means that a polynomial does not distinguish between its roots. Any permutation of $z_1, z_2, \dots, z_5$ produces exactly the same quintic.

This means that, despite starting with the exact same coefficients a, b, c, d, e, f , there is no algebraic reason to prefer one ordering of the roots over any other — all $5!$ orderings describe the same polynomial:

$$(z_1, z_2, z_3, z_4, z_5), \quad (z_1, z_5, z_4, z_3, z_2), \quad \text{etc.}$$

Why is this a problem, though? Surely we can just choose a certain order of roots and proceed? Unfortunately, there is no natural way to simply pick a certain order of roots, and this is one of the main difficulties behind finding formulae for solving polynomial equations.

By moving a polynomial around in a continuous way and returning to where we started, we are able to permute the roots while the polynomial itself remains unchanged. Let's first consider a simple example:

$$z^3 = 8.$$

¹If you want some intuition as to why this is true, then this pdf should help.

The three roots of this polynomial are:

$$2, \quad 2e^{\frac{2\pi i}{3}}, \quad 2e^{\frac{4\pi i}{3}},$$

which lie, equally spaced, on a circle of radius 2 in the complex plane. We can vary this equation by multiplying the right hand side by some $e^{i\theta}$. Consider

$$z^3 = 8e^{i\theta}.$$

As θ increases, $8e^{i\theta}$ rotates around a circle of radius 8, changing the equation continuously. This means that the roots must also change continuously².

What's important here is that, as θ increases and $8e^{i\theta}$ rotates, each root also rotates around the origin, but only at one third the rate of $8e^{i\theta}$. Consequently, even as $8e^{i\theta}$ completes one full revolution around the circle as θ increases from $0 \rightarrow 2\pi$, each root only completes a third of a rotation around the circle, meaning that each root has moved into a new position previously occupied by another root (as the roots are equally spaced around the circle). The roots have been *cyclically permuted*, despite the equation remaining the same. This helps show that there is no natural way to order the roots of a polynomial - we can continue rotating the right hand side in order to cyclically permute the roots without changing the original equation.

Figure 1: As $8e^{i\theta}$ makes one full revolution around the origin, the roots of $z^3 = 8e^{i\theta}$ move continuously. When the equation returns to $z^3 = 8$, the roots have been cyclically permuted.

If roots can be permuted this way, how do formulas like the quadratic formula separate them? It all comes down to *multivaluedness*.

²We used a similar sort of idea related to continuity earlier when explaining the Fundamental Theorem of Algebra.

3 Multivaluedness

When we solve a polynomial equation, we want to find all the values for which an equality holds. For example, let's consider the following quadratic:

$$z^2 = 4.$$

This equation does not have one solution, but two:

$$z = \pm 2.$$

More generally, if we consider a quadratic of the form

$$z^2 = a,$$

we find that it has two solutions:

$$z = \pm \sqrt{a}.$$

However, what do we really mean when we write $\sqrt{a}$? Let's take $a = e^{2\pi it}$. When $t = 0$,

$$\sqrt{e^{2\pi i0}} = \sqrt{e^0} = \sqrt{1} = 1.$$

Yet, when $t = 1$,

$$\sqrt{e^{2\pi i1}} = \sqrt{e^{2\pi i}} = e^{\pi i} = -1.$$

Therefore, despite the input being identical ($e^0 = e^{2\pi i} = 1$), the two evaluations give different values. This means that no continuous, single-valued square root can exist over the entire complex plane. If it did, then continuity would force $\sqrt{e^{2\pi i0}} = \sqrt{e^{2\pi i1}}$, but we know that this is not true.

Therefore, although we write $\sqrt{a}$ as if it represents just a single value, there is no natural way to choose one value of $\sqrt{a}$ consistently as a varies over the **entire** complex plane³. Informally, this is what we mean by multivaluedness.

The quadratic formula

$$z = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

handles this multivaluedness through its $\pm$. The $\pm$ accounts for both roots regardless of which branch the value of $\sqrt{b^2 - 4ac}$ is taken from. Any valid formula must account for all permutations of roots, and in this case, the $\pm$ suffices as a quadratic has $2! = 2$ possible permutations.

³It is important to note that we can define square roots consistently over smaller regions in the complex plane, but we cannot do this consistently over the entire complex plane

4 Loops and More Permutations

In order to prove that there exists no algebraic quintic formula, we need to somehow show that not all permutations of roots are able to arise from radical expressions, and that the quintic involves these ‘forbidden’ permutations. To do this, let’s take a look at how permutations arise when we vary the coefficients of a polynomial.

Definition 4.1. Let $\mathcal{F}_n$ denote the set of all monic (meaning the coefficient of the highest degree term is 1) separable polynomials of degree n .

This means that each point in the coefficient space belonging to $\mathcal{F}_n$ corresponds to a polynomial

$$p(z) = z^n + a_1 z^{n-1} + a_2 z^{n-2} + \cdots + a_0$$

with n distinct roots. This means as we move through $\mathcal{F}_n$, the roots also move continuously.

A **loop** in coefficient space is a continuous path in $\mathcal{F}_n$ which begins and ends at the same polynomial. A loop is essentially a more general version of what we did earlier when we permuted the roots of the cubic $z^3 = 8e^{i\theta}$ by varying θ from 0 to 2π . Instead of simply revolving in a circle, we are now able to permute the roots of a polynomial by moving in any continuous manner before eventually returning to the original point corresponding to our original polynomial. Formally:

Definition 4.2. A **loop** in coefficient space is a continuous map

$$\gamma: [0, 1] \rightarrow \mathcal{F}_n$$

such that $\gamma(0) = \gamma(1)$.

Figure 2: As the loop is traced in the coefficient space, the roots of the corresponding polynomial are permuted in the complex plane.

Theorem 4.3. *Every possible permutation of the roots of a separable polynomial can be induced by a loop in $\mathcal{F}_n$.*

To show that this is true, we need to show that any swap of two roots (a **transposition**) can be induced by a loop, as every permutation is simply a composition of transpositions.

Figure 3: A transposition can be induced by moving two roots, z_i and z_j , along non-intersecting paths in root space so that they swap places. This swap produces a loop in coefficient space and, as every permutation is a composition of transpositions, it follows that any permutation can be induced by a loop.

Therefore any formula for an n -th degree polynomial must account for all $n!$ permutations of its roots.

5 Radical Expressions and Nested Roots

A **formula involving radicals** is an expression built only using the operations $+$, $-$, $\times$, $\div$ and n -th roots. Okay, so how can we actually prove that some permutations cannot arise from formulas involving radicals? Well, first it may be useful to figure out what kind of permutations **can** arise from formulas involving radicals.

When we solve equations using radicals, we use multivalued operations such as square roots, cube roots, and so on. The multivalued nature of these radicals, as discussed earlier, naturally introduces permutations. From earlier, we know that taking a square root introduces the following permutation:

$$(z_1, z_2) \mapsto (z_2, z_1).$$

What about a cube root? Let's consider

$$z^3 = a.$$

If we vary a around a loop that winds once around the origin in $\mathbb{C}$, we find that each root rotates around the origin and, when a returns to its starting value, the roots are permuted cyclically:

$$(z_1, z_2, z_3) \mapsto (z_2, z_3, z_1).$$

This can be generalised to any n -th degree root. The n -th roots of $re^{i\theta}$ are $r^{1/n}e^{i(\theta+2\pi k)/n}$ for $k = 0, 1, \dots, n-1$. As θ increases by 2π , i.e., as a completes one loop around the origin, each root's phase increases by $2\pi/n$, shifting it exactly into the next root's position. This is a cyclic permutation of the n values, exactly as we saw earlier in the example of $z^3 = 8e^{i\theta}$.

By combining cyclic permutations from different radicals, **nested** radicals can induce permutations unreachable by any single n -th root. For example, applying a swap (square root)

$$(z_1, z_2, z_3) \mapsto (z_2, z_1, z_3)$$

followed by a cube root

$$(z_2, z_1, z_3) \mapsto (z_1, z_3, z_2),$$

gives $(z_1, z_2, z_3) \mapsto (z_1, z_3, z_2)$, which neither radical could produce alone.

But can we generate *all* permutations by using nested roots? To answer this, we need to understand what happens when we apply multiple permutations in different orders.

6 Commutators

Suppose we have two loops in a coefficient space, γ_1 and γ_2 , that are both based at the same polynomial (meaning that they start at the same point). Let's suppose that

$$\gamma_1: (z_1, z_2, z_3) \mapsto (z_2, z_1, z_3)$$

and

$$\gamma_2: (z_1, z_2, z_3) \mapsto (z_2, z_3, z_1).$$

If we apply γ_1 , followed by γ_2 , we get:

$$(z_1, z_2, z_3) \mapsto (z_2, z_1, z_3) \mapsto (z_1, z_3, z_2).$$

Yet, if we apply γ_2 , followed by γ_1 , we get:

$$(z_1, z_2, z_3) \mapsto (z_2, z_3, z_1) \mapsto (z_3, z_2, z_1).$$

Therefore, it is clear that γ_1 and γ_2 do not commute, and so the order in which we apply loops matters. Combining operations in different orders produces different outcomes. In order to isolate this difference, we use a **commutator**.

Definition 6.1. The *commutator* of two loops γ_1, γ_2 (both based at the same polynomial) is defined as

$$[\gamma_1, \gamma_2] = \gamma_1 \gamma_2 \gamma_1^{-1} \gamma_2^{-1}.$$

Intuitively, the commutator constructs a new loop by going around γ_1 , then γ_2 , before going backwards around γ_1 , then backwards around γ_2 ⁴. If the loops commute, then the process cancels out and we return to the original configuration with no effect on the roots. If the loops do not commute, then the commutator produces a new, nontrivial permutation. For instance, with γ_1 and γ_2 as above:

$$(z_1, z_2, z_3) \xrightarrow{\gamma_1} (z_2, z_1, z_3) \xrightarrow{\gamma_2} (z_1, z_3, z_2) \xrightarrow{\gamma_1^{-1}} (z_3, z_1, z_2) \xrightarrow{\gamma_2^{-1}} (z_2, z_3, z_1),$$

and so the commutator $[\gamma_1, \gamma_2]$ induces the nontrivial permutation $(z_1, z_2, z_3) \mapsto (z_2, z_3, z_1)$.

⁴Often permutations are applied from right to left, but for the sake of simplicity we will apply these permutations from left to right.

Figure 4: The commutator loop is obtained by following γ_1 , then γ_2 , then reversing γ_1 , and finally reversing γ_2 . This results in a permutation of roots.

The key property of commutator loops is that their *net winding*⁵ around the origin is always zero. As the commutator ‘reverses’ around every path it takes, any winding caused by an individual permutation cancels out. Therefore, for any continuous function f of the coefficients, $\sqrt[n]{f([\gamma_1, \gamma_2](t))}$ is consistently defined along the entire loop, i.e., the output value of the n -th root remains constant even after traversing the entire commutator loop.

Although each individual radical returns to its starting value along a commutator loop, the roots may still be permuted. The formula outputs a fixed complex number, i.e., 4, but after the loop, that value may now correspond to a different root z_3 rather than z_1 . Therefore, despite the roots being permuted, the value of the radical has remained the same.

A formula with a single layer of radicals can only induce permutations arising from commutators. For a cubic, only 3 of the 6 permutations are able to be induced this way, and so at least one level of nesting is required, as taking commutators of commutators allows us to reach all 6. The question is: does this work for quintics?

⁵*Net winding* here refers to the total number of times that a curve loops around the origin. An clockwise loop adds +1 to the net winding, while an anticlockwise loop adds -1 to the net winding. As an example, a curve with net winding 1 around the origin would result in a sign change (as seen with $\sqrt{e^{2\pi it}}$).

7 The Quintic

We know there are $5! = 120$ permutations of five roots, and a formula with no nested radicals can only induce permutations that are themselves commutators of permutations. It turns out that exactly 60 of the 120 possible permutations can be expressed this way, and so we immediately can conclude that we need at least a single level of nesting to account for the remaining permutations⁶.

Now, let's allow one level of nesting. This means that our formula can use commutators of commutators, and so we ask: of the 60 permutations reachable using a single commutator, which new permutations become reachable by taking commutators of those 60 reachable permutations? Surprisingly, it turns out that we reach no new permutations. Taking commutators of any two of the 60 reachable permutations always produces one of the same 60 permutations. This means that, no matter how many layers of nesting you apply (i.e., how many commutators of commutators of commutators... you take), we will never be able to 'escape' those same 60 permutations. A formula with a trillion levels of nesting will induce the same permutations as a formula with just a single level! This is the main difference between the quintic and the cubic we looked at earlier. For a cubic, the process of taking commutators through nested radicals does eventually reach all 6 permutations, which is why a cubic formula exists.

Yet, by Theorem 4.1, every one of the 120 permutations can be induced by some loop in $\mathcal{F}_5$. Let's assume a quintic formula with N levels of nesting exists. For any N , a formula with N levels of nesting can only reach the same 60 permutations - never all 120. This is a contradiction, as for a valid formula to exist, it must be able to induce all 120 permutations. Therefore, we can conclude that

Theorem 7.1. *There exists no formula for solving a general quintic built out of the operations $+$, $-$, $\times$, $\div$ and any finite number of nested radicals.*

We have *not* shown that all quintic equations are unsolvable. For example, the quintic

$$z^5 - 1 = 0$$

has roots at $z = e^{\frac{2\pi ik}{5}}, k = 0, 1, 2, 3, 4$ ⁷. Instead, we have shown that no *general* quintic formula using finitely many nested radicals can solve every quintic, in the way the quadratic formula solves every quadratic.

⁶The easiest way to do this is through trial-and-error, which avoids using Galois Theory. There are $120^2 = 14400$ possible commutators of two permutations, and calculating all of these can be done using a python script.

⁷If you're interested in why this works, look up 'roots of unity'!

References

- [1] L. Goldmakher, *Arnold's Elementary Proof of the Insolvability of the Quintic*, Williams College. Available at <https://web.williams.edu/Mathematics/lg5/394/ArnoldQuintic.pdf>
- [2] H. Zoladek, *The Topological Proof of the Abel–Ruffini Theorem*, Topological Methods in Nonlinear Analysis, Vol. 16, No. 2 (2000), pp. 253–265. Available at <https://projecteuclid.org/journals/topological-methods-in-nonlinear-analysis/volume-16/issue-2/The-topological-proof-of-Abel-Ruffini-theorem/tmna/1471875703.pdf>
- [3] B. Katz, *Why There's No Quintic Formula* [Video], YouTube, 2013. Available at <https://www.youtube.com/watch?v=RhpVSV6iCko>
- [4] Wikipedia, *Abel–Ruffini Theorem*. Available at https://en.wikipedia.org/wiki/Abel%E2%80%93Ruffini_theorem