On the Insolvability of the Quintic

With a focus on intuition

Emerald (Emmy) Gu

MAT315 Essay

December 2, 2025

Contents

I Introduction

1 Motivation

Often in math do we come across and work with polynomials. They're simple, easy to understand, and widely applicable across many areas of study. For instance, we've seen polynomials a number of times within our course:

- Pythagorean triples are integer solutions to a polynomial of two degrees in three variables:
$$x^2 + y^2 - z^2 \ = \ 0$$
- The problem of the sum of two squares is similar:
$$a^2 + b^2 - n \ = \ 0$$
- Fermat's Last Theorem famously generalizes the Pyhthagorean triples:
$$x^n + y^n - z^n \ = \ 0$$

When we discuss these topics, we're really discussing the solutions to these polynomials. Thus, we can ask: in general, when do we have solutions to any given polynomial, and if they exist - what are they?

2 Problem Statement

Because we typically care about integer solutions, one strategy is to find *all* solutions, real or complex, then select integer solutions. We'll take this approach for solutions to polynomials.

Before we can worry about finding solutions, we need to know they exist. Thankfully:

Theorem 2.1: Fundamental Theorem of Algebra

A polynomial of degree n has n complex roots, with multiplicity.

From high school, we know there's a quadratic equation to find roots of a quadratic polynomial:

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

There's also a cubic and even a quartic formula for degree 4 polynomials, which are omitted for their length. However, we claim that there are no more.

Claim 2.2

There is no closed-form equation for the roots of a degree 5 polynomial with rational coefficients, using only the following operations:

$$+ \qquad - \qquad \times \qquad \div \qquad \sqrt[n]{\cdot}$$

that is, addition, subtraction, multiplication, division, and n-th roots (also known as *radicals*) for any integer n.

This is a very general statement, and is difficult to precisely describe mathematically. However, note that the existence of a closed-form equation of the roots of a given degree polynomial indicates that the roots of *any* polynomial of the same degree can be written in precisely that form. Thus, for it to be false in the case of the quintic, it suffices to find even a single quintic whose roots cannot be expressed using the above operations. In other words, we aim to prove the slightly stronger theorem:

Theorem 2.3: Abel-Ruffini Theorem

There exists a polynomial of degree 5 whose roots cannot be written in radicals.

Throughout this essay, we will examine some of the history of this problem, and examine where the modern proof comes from.

II History

3 Closed-form expressions

The general method which was used to derive the quartic equation is largely similar to the derivation for the cubic equation; the discoverer, Ferrari in 1540, was in fact a student of Cardano at the time, and adapted the latter's argument to construct the quartic. We examine the method published by Cardano, which is due to del Ferro and Tartaglia.

Given a polynomial $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0$, we can always divide by a_n to make the polynomial monic; this makes it easier to work with. Thus, all polynomials from here forward will be monic without loss of generality.

Consider a quadratic $x^2 + ax + b = (x-r)(x-s)$. Observe that:

$$(x-r)(x-s) \;=\; x^2 - (r+s)x + rs \;=\; x^2 + ax + b$$

This means that for any quadratic $x^2 + ax + b$ with roots r and s, we always have that $a = -(r+s)$ and $b = rs$. This property generalizes to higher degree polynomials; in the case of the cubic, we have:

$$x^3 + ax^2 + bx + c = (x-r_1)(x-r_2)(x-r_3) \implies \begin{cases} a = -(r_1 + r_2 + r_3) \\ b = r_1 r_2 + r_2 r_3 + r_1 r_3 \\ c = -r_1 r_2 r_3 \end{cases}$$

These equations of the coefficients in terms of the roots are known as **Vieta's Formulas**. Named after their discoverer François Viète in the 16th century for positive roots, the method may have been known as early as the 12th century.

Let $P(x) = x^3 + ax^2 + bx + c$ be a cubic polynomial. We use the above formulas to construct a quadratic $r(x)$ such that the roots of $P(x)$ can be derived from the roots of $r(x)$. To see how, first apply a change of variables $x = y - \frac{b}{3a}$:

$$P\left(y - \frac{b}{3a}\right) \;=\; \left(y - \frac{b}{3a}\right)^3 + a\left(y - \frac{b}{3a}\right)^2 + b\left(y - \frac{b}{3a}\right) + c \;=\; y^3 + my + n$$

The act of performing such a change of variables to eliminate the term of second-highest degree is known as **depressing the polynomial** - in this case, a cubic. Let $Q(y) := y^3 + my + n$; note that m and n are in terms of a, b, and c. Suppose a root $y = w + z$ is expressed as a sum of two numbers. Then:

$$\begin{aligned} (w+z)^3 &= w^3 + 3w^2z + 3wz^2 + z^3 = w^3 + z^3 + 3wz(w+z) \\ \implies & (w+z)^3 - 3wz(w+z) - (w^3+z^3) = 0 \end{aligned}$$

Since $y = w + z$, then:

$$\begin{cases} m &= -3wz \\ n &= -(w^3+z^3) \end{cases} \implies \begin{cases} w^3+z^3 &= -n \\ w^3z^3 &= \frac{-m^3}{27} \end{cases}$$

We then apply Vieta's formulas to construct a quadratic with roots w^3, z^3:

$$R(x) := x^2 + nx - \frac{m^3}{27} = 0 \qquad w^3, z^3 = \frac{-n}{2} \pm \sqrt{\frac{n^2}{4} + \frac{m^3}{27}}$$

Recalling that $y = w + z$ is a root of $Q(y)$, we thus obtain a root given as:

$$y = \sqrt[3]{\frac{-n}{2} + \sqrt{\frac{n^2}{4} + \frac{m^3}{27}}} + \sqrt[3]{\frac{-n}{2} - \sqrt{\frac{n^2}{4} + \frac{m^3}{27}}}$$

The other two roots can be obtained by taking different possible values of w, z as the cube root, and using the earlier constraint that $m = -3wz$.

In general, $R(x)$ is called the **resolvent** of $p(x)$, because it is a polynomial of smaller degree whose roots we can use to obtain the roots of $p(x)$. Since m, n are solely in terms of the coefficients a, b, c of $p(x)$, the pre-existing quadratic formula thus makes finding roots for a cubic quite straightforward.

4 Symmetry of roots

In 1770 and 1771, Lagrange generalized the above work by finding a connection between finding a resolvent of a polynomial and a *discrete Fourier transform* of the roots. While we do not need to know what a DFT is, the key insight lies with what we will refer to as “almost symmetric expressions”.

Definition 4.1

A **symmetric** expression on n variables is an expression whose value does not change upon any permutation of the n variables.

An **almost symmetric** expression is an expression which takes on a limited number of different values.

For instance, consider $a^2b + b^2c + c^2a$. This is not a symmetric expression, however it only has two algebraically distinct values:

$$a^2b + b^2c + c^2a \qquad a^2c + c^2b + b^2a$$

Any permutation of a, b, c which does not fix any of the letters will yield the expression on the left. On the other hand, any permutation which fixes exactly one of the letters will yield the expression on the right. Thus, $a^2b+b^2c+c^2a$ is an expression in 3 variables with 2 algebraically distinct values. There is also one in 4 variables with 3 algebraically distinct values:

$$(a+b)(c+d) \qquad (a+c)(b+d) \qquad (a+d)(b+c)$$

In general, Lagrange’s key insight was to take a depressed polynomial of degree n, and find an almost symmertic expression in n variables with $n-1$ algebraically distinct values. This would allow him to construct a resolvent polynomial and a system of equations which connected it to the original polynomial. For instance, given a quartic $p(x)$ with roots a, b, c, d:

$$\begin{cases} (a+b)(c+d) = A \\ (a+c)(b+d) = B \\ (a+d)(b+c) = C \\ a+b+c+d = 0 \end{cases} \qquad \longrightarrow \qquad r(x) := (x-A)(x-B)(x-C) = 0$$

Since the roots of $r(x)$ can be found with the cubic equation, and by the system of equations are also written in terms of the roots of $q(x)$, and since those can be written in terms of the coefficients of $q(x)$, this provided a method of solving the quartic. Note the last condition that $a + b + c + d = 0$ comes from depressing the quartic.

The significance of Lagrange's work was in showing that the existence of formulas for 2nd, 3rd, and 4th degree polynomials in fact stems from a single idea. Although unknown at the time, Lagrange's work is a special case of a broader fact:

Theorem 4.2

Given a polynomial $p(x)$, any symmetric polynomial in terms of the roots of $p(x)$ can be written as a polynomial in terms of the coefficients of $p(x)$.

This theorem would later be dubbed the **Fundamental Theorem of Symmetric Polynomials**.

However, Lagrange struggled to continue his work to degree 5 and beyond - he could not find an almost symmetric expression in 5 variables with 4 algebraically distinct values. More specifically, whenever he tried to construct a resolvent to the quintic, it would always end up with a degree *higher* than 5. This ultimately led him to consider the existence of the quintic in the negative.

III Proof of the Statement

5 Prerequisite Algebra

The modern proof of non-existence uses the language of Galois theory; in this section, we'll highlight why. We will be assuming some familiarity with fields and elementary group theory.

When discussing the existence of roots of a polynomial, we want to clarify which field is being discussed. For instance, every polynomial has n roots in $\mathbb{C}$ (with multiplicity), but this is not the case in $\mathbb{R}$.

The field of interest for this proof is $\mathbb{Q}$. This is because we care about solutions to polynomials, and $\mathbb{R}$ has "too much information" - it contains (almost) all transcendental numbers, and every non-negative real number has an n-th root.

We use **field extensions** over $\mathbb{Q}$ to examine our polynomials, because this allows us to control the obtainable elements within our field. In particular, we know when a root can be written with the operations we care about. A **splitting field** of a polynomial is a field extension over which the polynomial factors into linear terms.

Given an extension L/K, its **Galois group** is the group $\mathrm{Aut}(L/K)$ of automorphisms of the extension L/K. This is the group of permutations over L/K. The extension is a **Galois extension** if all $\varphi \in \mathrm{Aut}(L/K)$ fix K. Equivalently, the extension is the splitting field of a (separable) polynomial.

A **solvable group** is a series of normal subgroups

$$\{e\} = G_1 \triangleleft G_2 \triangleleft \cdots \triangleleft G_n$$

such that each factor group G_{k+1}/G_k is abelian. The motivation for this definition actually comes from Galois theory itself, and encapsulates a property we will see in the proof itself.

6 Proving the claim

We finish this essay with the proof of the claim.

Let $p(x)$ be a degree 5 polynomial with rational coefficients; suppose its roots can be written using radicals, and WLOG are distinct. Consider the splitting field $\mathbb{Q}[\alpha_1, \ldots, \alpha_n]$ of $p(x)$. We construct a tower of field extensions as follows:

Write out each of the roots of p. For visual purposes, consider $\sqrt[5]{1+3\sqrt[3]{10}}$. Let β_1 be any of the "innermost" radicals of the root, in this case $\sqrt[3]{10}$. Start by adjoining β_1 to $\mathbb{Q}$. Then, iteratively adjoin the next radical $\beta_k = \sqrt[n]{x}$ where $x \in \mathbb{Q}[\beta_1, \ldots, \beta_{k-1}]$.

At each step, if the extension is not Galois, then first adjoin the n-th roots of unity, followed by the desired radical. For instance, in the case of $\sqrt[3]{2}$:

$$\mathbb{Q} \longrightarrow \mathbb{Q}[e^{2\pi i/3}] \longrightarrow \mathbb{Q}[e^{2\pi i/3}, \sqrt[3]{2}]$$

Thus, the extension at each step is the splitting field of a polynomial, and therefore is Galois. After this process, $\mathbb{Q}[\beta_1, \ldots, \beta_m]$ contains all the roots of $p(x)$, so we can draw the diagram shown in Figure 1.

Now, consider any three consecutive extensions A, B, C as in Figure 2, where G, N, L are the Galois groups of C/A, C/B, and B/A respectively. First, we claim that $N \triangleleft G$.

Let $\varphi \in G$ be an automorphism. Since C/A is Galois, then φ fixes elements in A. Recall B is constructed by adjoining A with particular roots of a polynomial f. Let $x \in B$ be a root of f. Notice:

$$f(x) = \sum_{i=0}^{n} a_i x^i = 0 \implies f(\varphi(x)) = \varphi(f(x)) = 0$$

So φ sends roots of f to roots of f, or in other words, $\varphi(B) = B$.

Now, let $\psi \in N$. Consider $(\varphi \circ \psi \circ \varphi^{-1})(b)$ for some $b \in B$:

$$\varphi^{-1}(b) \in B \implies \varphi(\psi(\varphi^{-1}(b))) = \varphi(\varphi^{-1}(b)) = b$$

In other words, we see that $\varphi \circ \psi \circ \varphi^{-1}$ fixes B, and thus must be an element of N.

Next, we claim that $L = G/N$ is a quotient group.

Since $N \triangleleft G$, the group G/N is well-defined. Note that any automorphism on B can be extended to an automorphism on C, and as previously shown, automorphisms on C restrict to automorphisms on B. If $\varphi_1, \varphi_2 \in G$ agree on B, then $\varphi_1 \varphi_2^{-1}$ is the identity on L, so $\varphi_1 \varphi_2^{-1} \in N$. It then follows that $L = G/N$.

Returning to our original diagram in Figure 1, recall that $\mathbb{Q}[\beta_1, \ldots, \beta_m]/\mathbb{Q}$ is Galois. Then it is the splitting field of some polynomial f with coefficients in $\mathbb{Q}$, but then for all $1 \leq k \leq m$, notice $\mathbb{Q}[\beta_1, \ldots, \beta_m]/\mathbb{Q}[\beta_1, \ldots, \beta_k]$ is also Galois using the same polynomial f. Therefore, every extension shown in Figure 3 is Galois.

The extensions shown on the left sides being Galois requires a slight amount of additional work, but the details are roughly similar to our prior construction. Due to length, they have been omitted.

Consider the groups $G_0, \ldots, G_m$ as labeled above. From our previous work, we can conclude that $G_{k+1} \triangleleft G_k$ and G_k/G_{k+1} is abelian for each k. In other words, we have the following series:

$$G_m \triangleleft G_{m-1} \triangleleft \cdots \triangleleft G_2 \triangleleft G_1 \triangleleft G_0 = G$$

where each composition factor is abelian. Therefore, we can conclude that G is solvable. By the fourth isomorphism theorem (also known as the correspondence/lattice theorem), it follows that G/N is solvable as well. Since G/N

is determined by our original $p(x)$, we have proven that if $p(x)$ is solvable by radicals, then the Galois group of its splitting field is necessarily solvable.

It now suffices to find a quintic for which the Galois group of its splitting field is *not* solvable. Indeed, consider:

$$p(x) \ = \ x^5 - x - 1$$

This polynomial has Galois group S_5, the proof for which is omitted. We claim that S_5 is not a solvable group; indeed, a composition series is given by:

$$\{e\} \ \triangleleft \ A_5 \ \triangleleft \ S_5$$

The composition factors are thus A_5 and $\mathbb{Z}_2$, and by the Jordan-Holder theorem, any composition series of S_5 necessarily has A_5 as a composition factor. However, A_5 is not abelian, so S_5 is not solvable, concluding our proof.

IV Figures

This section contains the figures referenced in the proof. It is recommended to have two copies of this file open simultaneously to make viewing the figures in-context easier.

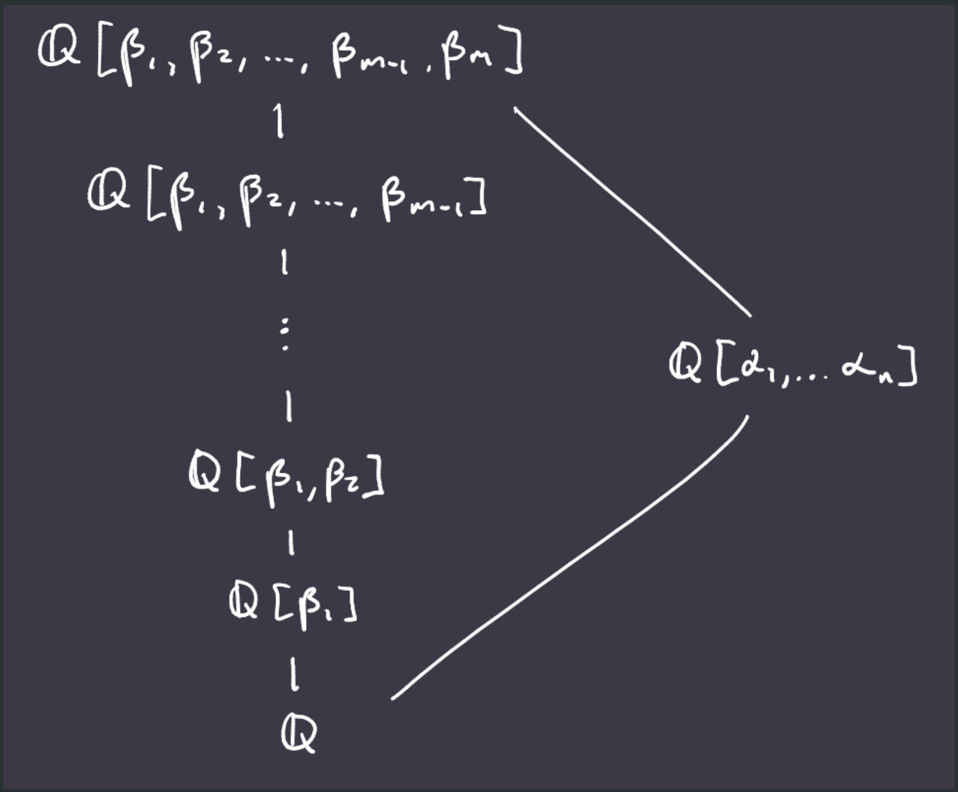
$\mathbb{Q}[\beta_1, \beta_2, \ldots, \beta_{m-1}, \beta_m]$
$\mathbb{Q}[\beta_1, \beta_2, \ldots, \beta_{m-1}]$
$\vdots$
$\mathbb{Q}[\alpha_1, \ldots \alpha_n]$
$\mathbb{Q}[\beta_1, \beta_2]$
$\mathbb{Q}[\beta_1]$
$\mathbb{Q}$

Figure 1.

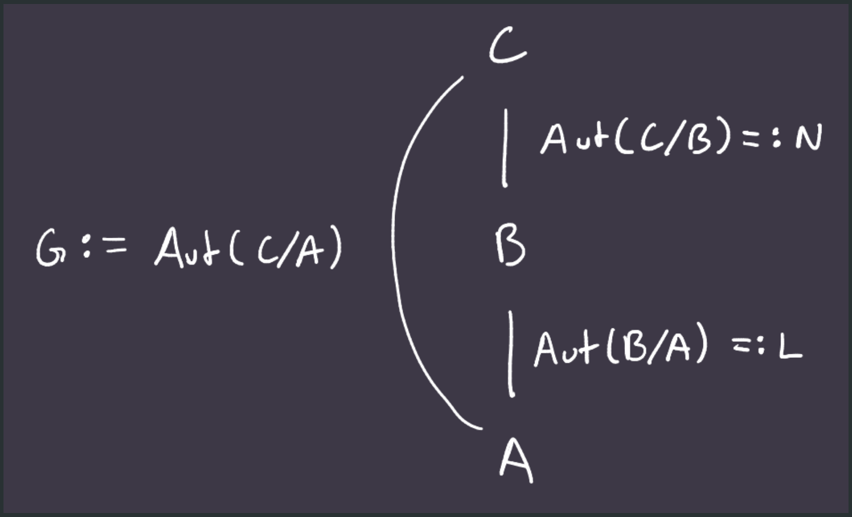

Figure 2.

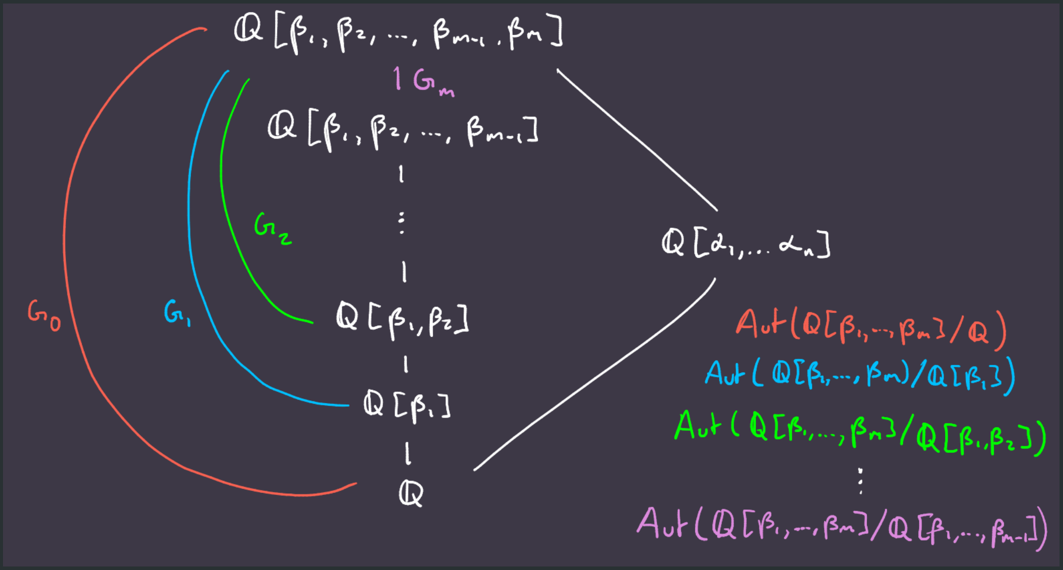
$\mathbb{Q}[\beta_1, \beta_2, \dots, \beta_{m-1}, \beta_m]$
G_m
$\mathbb{Q}[\beta_1, \beta_2, \dots, \beta_{m-1}]$
G_2
$\mathbb{Q}[\alpha_1, \dots \alpha_n]$
G_0
G_1
$\mathbb{Q}[\beta_1, \beta_2]$
$\mathbb{Q}[\beta_1]$
$\mathbb{Q}$
$\mathrm{Aut}(\mathbb{Q}[\beta_1, \dots, \beta_m]/\mathbb{Q})$
$\mathrm{Aut}(\mathbb{Q}[\beta_1, \dots, \beta_m]/\mathbb{Q}[\beta_1])$
$\mathrm{Aut}(\mathbb{Q}[\beta_1, \dots, \beta_m]/\mathbb{Q}[\beta_1, \beta_2])$
$\vdots$
$\mathrm{Aut}(\mathbb{Q}[\beta_1, \dots, \beta_m]/\mathbb{Q}[\beta_1, \dots, \beta_{m-1}])$

Figure 3.

V Bibliography

I'm not really sure how to format a bibliography for a math paper, so I apologize in advance.

References used:

- Why you can't solve quintic equations (Galois theory approach). Mathemaniac, Youtube. Retrieved December 2, 2025.

  `https://www.youtube.com/watch?v=zCU9tZ2VkWc`

- Grant Sanderson - Unsolvability of the Quintic. The Cartesian Cafe with Timothy Nguyen. Timothy Nguyen, Youtube. Retrieved December 2, 2025.

  `https://www.youtube.com/watch?v=aaW30_f2on0`

- Vieta's Formulas, Wikipedia. Retrieved December 2, 2025.

  `https://en.wikipedia.org/wiki/Vieta's_formulas`

- Joseph-Louis Lagrange, Wikipedia. Retrieved December 2, 2025.

  `https://en.wikipedia.org/wiki/Joseph-Louis_Lagrange`

- Cubic Equation, Wikipedia. Retrieved December 2, 2025.

  `https://en.wikipedia.org/wiki/Cubic_equation`

- The Fundamental Theorem on Symmetric Polynomials: History's First Whiff of Galois Theory. Ben Blum-Smith, Samuel Coskey. Retrieved December 2, 2025.

  `https://arxiv.org/abs/1301.7116`

- Abel-Ruffini Theorem. Retrieved December 2, 2025.

  `https://en.wikipedia.org/wiki/Abel%E2%80%93Ruffini_theorem`