On the Insolvability of the Quintic

A more accessible approach (subtitle wip)

Emerald (Emmy) Gu

MAT315 Essay (Draft)

November 10, 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:

- Linear Diophantine equations are polynomials of one degree in two variables:
$$ax + by - c = 0$$
- 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:
$$x^n + y^n - z^n = 0$$
- Fermat's *Little* Theorem, and more generally Euler's Theorem, is a statement about polynomials of a particular degree, modulo some value (ok, this is pushing it):
$$g^{p-1} \equiv 1 \bmod p \qquad g^{\varphi(n)} \equiv 1 \bmod n$$

When we discuss these topics, we're really discussing these polynomials. But more specifically, we care about the *solutions* to these polynomials, moreso than the polynomials themselves. Thus, it is only natural to ask - when, in general, do we have solutions to any given polynomial, and if they exist - what are they? some mention of solns in $\mathbb{Z}$ vs $\mathbb{R}$ here?

2 Problem Statement

Throughout this course (MAT315) and in number theory as a whole, we typically care about integer solutions the most. One way to find integer solutions is to find *all* the solutions in general, then reduce/pick out 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:

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

Slightly lesser known is the longer cubic formula, which is usually broken into parts when written:

TODO

There's even a quartic formula for degree 4 polynomials, which is too long and involved to be included in this essay. However, we claim that this does not continue any further.

Claim 2.2

We claim that there is no closed-form formula or expression for the roots of $p(x)$, only using the operations of

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

that is, addition, subtraction, multiplication, division, n-th powers, and n-th roots for any integer n.

Throughout this essay, we will examine the history of this problem, learn what worked, what didn't, and why, and see how to generalize this to higher degree polynomials.

i think that section needs some massaging still

II History

3 Existence

short-ish stint about history of quadratic formula (pre-fta) and fundamental theorem of arithmetic here. antiquity of quadratic formula, fta first statements, early discussion, who made attempts and when.

4 Closed-form expressions

history of motivation for cubic since its interesting, key steps of derivations for lower deg polynomials. particular attention/emphasis on the depressed and resolvent polynomials, initial suggestions of inductive method

5 Symmetry of roots

focus on the "symmetry" of the roots wrt permutation and how it shows up in the above derivations. discussion of how we could generalize to 5th degree, motivation for using algebra

III Prerequisite Algebra

6 Basic Group Theory

groups, subgroups, normal subgroups, (high-level) quotient groups. fields, sequences / trees of (sub)groups, solvable groups.

7 name tba

connection between groups and (roots of) polynomials, field extensions, automorphisms as permutations.

want to keep the "algebra" approach to a minimum, preferring a high-level, intuition-based story over a bunch of group theory theorems and terminology where possible

IV Proof of the Statement

8 Proving the claim

to add

9 Higher Degrees

brief segment about applying this to higher degree polynomials

10 Comparison to lower degrees

compare to degree 4, short examination of how the previous argument of the symmetry of roots manifests in the proof

V Bibliography