Finding (or not) Formulas for Polynomial Roots

MA294 Final Project

Adam Godel

April 27, 2026

Introduction

A problem of great interest when considering the analysis of polynomials is the ability to determine the existence of a formula identifying their roots, and, if a formula exists, identifying it. This is what Galois theory allows us to show, through its connection of group theory and field theory using field automorphisms.

An ***automorphism*** of a group G or a ring R is an isomorphism with itself. It is not hard to see that the set of automorphisms forms a group. Let F be a field and let E be a field extension of F. We will denote the full group of automorphisms of E by $\mathrm{Aut}(E)$. We define the ***Galois group*** of E over F to be the group of automorphisms that fix F elementwise; that is,

$$G(E/F) = \{\sigma \in \mathrm{Aut}(E) : \sigma(\alpha) = \alpha \text{ for all } \alpha \in F\}.$$

If $f(x)$ is a polynomial in $F[x]$ and E is the splitting field of $f(x)$ over F, then we define the Galois group of $f(x)$ to be $G(E/F)$.

Galois groups are a very powerful tool. It turns out that we can pretty easily make a connection between the permutation groups and the roots of a polynomial, and this is what we will use to power our investigation of polynomial formulas.

Proposition 1. *Let E be a field extension of F and $f(x)$ be a polynomial in $F[x]$. Then any automorphism in $G(E/F)$ defines a permutation of the roots of $f(x)$ that lie in E.*

Proof. We adopt the proof from [1]. Let

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

and suppose that $\alpha \in E$ is a zero of $f(x)$. Then for $\sigma \in G(E/F)$,

$$\begin{aligned} 0 &= \sigma(0) \\ &= \sigma(f(\alpha)) \\ &= \sigma(a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n) \\ &= a_0 + a_1\sigma(\alpha) + a_2[\sigma(\alpha)]^2 + \cdots + a_n[\sigma(\alpha)]^n; \end{aligned}$$

therefore, $\sigma(\alpha)$ is also a zero of $f(x)$. □

This background will suffice to define a property we will call "solvability by radicals" which will allow us to find exactly what we want: a general method to determine the roots of certain polynomials.

Solvability by Radicals

By the end of this section, we will have re-derived the quadratic formula using the language of Galois theory as well as showing that there must exist general cubic and quartic formulas. In short, this is our guiding question: does there exist a formula for the roots of an n-degree polynomial using only addition, subtraction, multiplication, division, and the extraction of nth roots?

An extension field E over a field F is an ***extension by radicals*** if there exists a chain of subfields

$$F = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_r = E$$

such for $i = 1, 2, \ldots, r$, we have $F_i = F_{i-1}(\alpha_i)$ and $\alpha_i^{n_i} \in F_{i-1}$ for some positive integer n_i. In other words, the extension field is an extension of our base field adjoining some number of extra radicals.

A polynomial $f(x)$ is ***solvable by radicals*** over F if the splitting field K of $f(x)$ over F is contained in an extension of F by radicals. In determining if a polynomial is solvable by radicals, it turns out we can make a much stronger statement than Proposition 1.

Let's first return to groups, though. A ***subnormal series*** of a group G is a finite sequence of subgroups

$$G = H_n \supset H_{n-1} \supset \cdots \supset H_1 \supset H_0 = \{e\},$$

where H_i is a normal subgroup of H_{i+1}. A group G is ***solvable*** if it has a subnormal series $\{H_i\}$ such that all the factor groups H_{i+1}/H_i are abelian.

This gives us the language we need to express our main theorem.

Theorem 1. *Let $f(x)$ be in $F[x]$, where $\operatorname{char} F = 0$. $f(x)$ is solvable by radicals if and only if the Galois group of $f(x)$ over F is solvable.*

Proof. I leave the proof to the references. The forward direction is proven by Theorem 23.3.4 of [1] while the reverse direction is proven in [2]. □

This theorem allows us to assess the existence of a general polynomial formula for a given degree. Now let's build up the facts we need to show existence of general polynomial formulas.

Lemma 1. *Let $f(x)$ be in $F[x]$, where $\operatorname{char} F = 0$ and $\deg f = n$, and let E be a splitting field of $f(x)$. The Galois group of $f(x)$ over F is a subgroup of S_n.*

Proof. The fact that elements in $G(E/F)$ will be permutations in S_n follows directly from Proposition 1. It is evident that $e \in G(E/F)$ and for every $\sigma \in G(E/F)$, $\sigma^{-1} \in G(E/F)$, since these will retain the fixing of all elements in F. Let $\sigma, \tau \in G(E/F)$. We can see that for any $\alpha \in F$, $(\tau \circ \sigma)(\alpha) = \alpha$, so $\tau \circ \sigma \in G(E/F)$. Therefore, all three group properties have been fulfilled. □

Lemma 2. *S_n is solvable if and only if $n \leq 4$.*

Proof. S_2 is clearly solvable as it only contains two elements. S_3 is solvable since the subnormal series

$$S_3 \supset A_3 \supset \{e\}$$

has abelian factor groups, as $S_3/A_3 \cong \mathbb{Z}_2$ and $A_3/\{e\} \cong A_3$. For S_4, we can see that

$$S_4 \supset A_4 \supset \{e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\} \supset \{e\}$$

has abelian factor groups. However, for $n \geq 5$, the series

$$S_n \supset A_n \supset \{e\}$$

has a nonabelian factor group, as A_n is simple for $n \geq 5$, meaning any subnormal series has to pass through $A_n \supset \{e\}$. Therefore, S_n is solvable for $n \leq 4$ but not for $n \geq 5$. □

Proposition 2. *Every quadratic, cubic, and quartic polynomial is solvable by radicals.*

Proof. This follows directly from Theorem 1, Lemma 1, and Lemma 2. □

Since we have resolved the problem of existence, let's turn to the question of finding the actual formulas. I will show a derivation of the quadratic formula; the cubic and quartic formulas can be derived similarly, but they are markedly more complicated, indicated by the much larger size of their splitting fields. To get a clue of where to start, let's examine the splitting field of the quadratic.

Lemma 3 (Discriminant)**.** *Let F be a field such that* $\operatorname{char} F \neq 2$*. The splitting field of $f(x) = ax^2 + bx + c$ is $F(\sqrt{\alpha})$, where $\alpha = b^2 - 4ac$.*

Proof. We can observe that $f(x)$ will have the same splitting field as the monic polynomial $g(x) = x^2 + \frac{b}{a}x + \frac{c}{a}$. Now consider $y = x + \frac{b}{2a}$. We can see that

$$g(x) = \left(y - \frac{b}{2a}\right)^2 + \frac{b}{a}\left(y - \frac{b}{2a}\right) + \frac{c}{a} = y^2 - \frac{b^2 - 4ac}{4a^2} = y^2 - \frac{\alpha}{4a^2}$$

Hence the roots of $g(x)$ satisfy $y^2 = \frac{\alpha}{4a^2}$. We can observe that the denominator will remain in the field when the square root is taken, so we just need to adjoin the square root of the numerator. Therefore, the splitting field of $g(x)$, and thus $f(x)$, is $F(\sqrt{\alpha})$. □

We can clearly see that if $\sqrt{\alpha} \in F$, the splitting field of $f(x)$ is just F, while if $\sqrt{\alpha} \notin F$, its splitting field is $F(\sqrt{\alpha})$. This maps cleanly onto our perception of the discriminant in $\mathbb{R}$. If $\sqrt{\alpha} \in \mathbb{R}$, then the quadratic has real roots, and if $\sqrt{\alpha} \notin \mathbb{R}$, we need to work over the complex numbers, i.e. adjoin some complex number to our field of real numbers.

We can build off of this radical adjoining, in this case of the discriminant of the quadratic, to get the actual quadratic formula.

Theorem 2 (Quadratic Formula)**.** *Let F be a field such that* $\operatorname{char} F \neq 2$*. The roots of $f(x) = ax^2 + bx + c$ satisfy $x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$.*

Proof. Let $r_1 \in F(\sqrt{\alpha})$ be a root of $f(x)$, so $ar_1^2 + br_1 + c = 0$. We know that $r_1 = u + v\sqrt{\alpha}$, where $u, v \in F$. From Proposition 1, we know that $r_2 = u - v\sqrt{\alpha}$ will also be a root of $f(x)$, since this is an automorphism in the Galois group of $f(x)$. Therefore, we know that

$$f(x) = a(x - r_1)(x - r_2) = a\big(x - (u + v\sqrt{\alpha})\big)\big(x - (u - v\sqrt{\alpha})\big) = a\big((x - u)^2 - v^2\alpha\big).$$

This expands to $f(x) = ax^2 - 2aux + a(u^2 - v^2\alpha)$. We can see that $u = -\frac{b}{2a}$, and

$$a\left(\frac{b^2}{4a^2} - v^2\alpha\right) = c \implies av^2\alpha = \frac{\alpha}{4a} \implies v^2 = \frac{1}{4a^2},$$

so $v = \pm\frac{1}{2a}$. Hence

$$r = u + v\sqrt{\alpha} = -\frac{b}{2a} \pm \frac{1}{2a}\sqrt{\alpha} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

□

The process is very similar, just much more tedious, for the cubic and quartic formulas, giving us essentially as general a description as possible of the roots of all polynomials up to degree 4. This turns out to be impossible for certain polynomials that are degree 5 or above.

Insolvability of the Quintic

We now shift our focus to examine the insolvability of certain quintic (and higher degree) polynomials. If we can find a quintic polynomial with S_5 as its Galois group, then we're done. First, though, it will help us to get a slightly better handle of subgroups of permutation groups.

Lemma 4. *If p is prime, then any subgroup of S_p that contains a transposition and a cycle of length p must be all of S_p.*

Proof. We adopt the proof from [1]. Let G be a subgroup of S_p that contains a transposition σ and a cycle τ of length p. We may assume that $\sigma = (1\,2)$. The order of τ is p and τ^n must be a cycle of length p for $1 \leq n < p$. Therefore, we may assume that $\mu = \tau^n = (1, 2, i_3, \ldots, i_p)$ for some n, where $1 \leq n < p$. Noting that $(1\,2)(1, 2, i_3, \ldots, i_p) = (2, i_3, \ldots, i_p)$ and $(2, i_3, \ldots, i_p)^k(1\,2)(2, i_3, \ldots, i_p)^{-k} = (1\,i_k)$, we can obtain all the transpositions of the form $(1\,n)$ for $1 \leq n < p$. However, these transpositions generate all transpositions in S_p, since $(1\,j)(1\,i)(1\,j) = (i\,j)$. The transpositions generate S_p. □

Now let's look at an example quintic polynomial to analyze its solvability.

Proposition 3. *$f(x) = x^5 - 6x^3 - 27x - 3 \in \mathbb{Q}[x]$ is not solvable by radicals.*

Proof. By Eisenstein's criterion with $p = 3$, we know that $f(x)$ is irreducible. By examining the plot of the polynomial, we can pretty easily see that it has three distinct real roots. Since the other two roots are complex conjugates, we can define an automorphism flipping the complex sign and hence, letting K be the splitting field of $f(x)$, we know that $G(K/\mathbb{Q})$ contains a transposition. For any real root $\alpha \in f(x)$, we know that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$, so $G(K/\mathbb{Q})$ must contain a cycle of length 5, and therefore, $G(K/\mathbb{Q}) = S_5$. Since S_5 is not solvable, $f(x)$ is not solvable by radicals. □

Hence we have shown that a quintic polynomial is not solvable by radicals. We conclude by briefly discussing how a higher degree polynomial that is not solvable by radicals can be derived. We just want to find a polynomial that is irreducible and has the entire permutation group for its degree as its Galois group, which for prime degrees just means that we need to find a transposition and a cycle of length p.

Proposition 4. *There exists a polynomial of degree 7 in $\mathbb{Q}[x]$ that is not solvable by radicals.*

Proof. We will reverse engineer a polynomial of degree 7 based on our requirements. Let's pick $p = 7$ for Eisenstein's criterion, and let's drop all even-degree terms to make our analysis easier. It turns out we can actually choose to drop another coefficient too, and work with a template like $f(x) = x^7 + 7a_5x^5 + 7a_1x + 7$. We then just need to select a_5 and a_1 so that the polynomial has five real roots. We can simply test out values, analyzing $f'(x) = 7x^6 + 35a_5x^4 + 7a_1$, and can see easily that $a_5 = -2$ and $a_1 = 3$ is an example of a working configuration. Since $f(x) = x^7 - 14x^5 + 21x + 7$ has five real roots, we can use the complex conjugation automorphism to show that the Galois group of $f(x)$ contains a transposition, and since for any real root $\alpha \in f(x)$, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 7$, the Galois group of $f(x)$ contains a 7-cycle, and thus is S_7. Therefore, $f(x)$ is not solvable by radicals. □

Conclusion

We introduced the powerful tool of Galois groups, defined solvability by radicals, showed that all polynomials of degree 4 or lower are solvable by radicals, and showed that some polynomials of degree 5 or higher are not solvable by radicals and how to construct them.

References

[1] T. W. Judson, *Abstract Algebra: Theory and Applications*, 2025 ed.

[2] E. Artin, *Galois Theory: Lectures Delivered at the University of Notre Dame* (Notre Dame Mathematical Lectures, No. 2). Dover, Mineola, NY, 1997.