Abel-Ruffini Explained

Sam Lowe

February 2, 2022

1 Introduction

Definition 1.1 (Expressability in Radicals)**.** We call a number **expressible in radicals** if we can write it just using $+, -, \times, \div$, and $\sqrt[n]{}$.

We want to express the roots of a polynomial in radicals. Consider the solution to a quadratic polynomial $ax^2 + bx + c$:

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

This formula is a little intimidating[1], but we can still express the two roots in radicals nonetheless.

You may notice that $\sqrt{}$ is odd man out – it's generally harder to work with and introduces irrational numbers into our calculations. If we could simply black box quantities $\sqrt{b^2 - 4ac}$ as a single unknown – let's call it Δ – then we could write the formula for the roots of a quadratic in terms of a, b, c, and Δ as

$$\frac{-b \pm \Delta}{2a}$$

This formula only uses $+, -, \times$, and $\div$ – no roots needed!

[1] Not as bad as the formulas for 3rd and 4th degree polynomials — those are atrocious!

What is it about quadratic polynomials that lets us write down their roots like this, but doesn't let us write down the roots of 5th degree polynomials, or polynomials of a higher degree?

After all, I can make a degree 5 polynomial with five "nice" numbers as roots:

$$(x-2)(x+3)(x-1)(x+5)(x-4)$$

and make a degree 2 polynomial by multiplying two "ugly" numbers as roots:

$$(x-e)(x+\pi i)$$

neither of which can be expressed in radicals.

They key is to realize that we can always express the roots of degree 2 polynomials *in terms of their coefficients*. The coefficients of the polynomial have a special relation with their roots — that relationship is given by the quadratic formula — that allows us to write down the two roots with just a, b, c, fractions, and the operations $+, -, \times, \div$, and $\sqrt[n]{}$.

Even though I can take a particular polynomial and write down its roots in terms of its coeffiecients using only those operations, *I can't write a general, catch-all formula that works for every degree five polynomial.* This document exists to answer the question:

Why not?

2 Polynomial Equations: A Short History

Polynomial equations have been studied going back for millenia. Babylonians tablets as late as 1600BCE had formulas for solving certain kinds of polynomials; the Egyptian Berlin Papyrus dating from roughly the same period also contains solutions to quadratic polynomials. Chinese mathematicians had formulas

Gerolamo Cardano (1501-1576)

The **Abel-Ruffini Theorem**, the theorem that explains why no quintic formula exists, is the prize that we seek, and we're going to take a tour.

Niels Henrik Abel (1802-1829)

Paolo Ruffini (1765-1822)

Evariste Galois (1811-1832)

Galois uncovered a deep connection between objects in abstract algebra, called **the Galois correspondence**, and used this to develop the theories that underpins the modern proof of Abel-Ruffini. To honor his contribution, this field of study now bares his name: **Galois theory**.

Abel-Ruffini Theorem is the prize that we seek, and we're going to take a tour through Galois theory to uncover it.

A professor of mine called Abel-Ruffini an irreducibly complex result, and it does require a lot of machinery to do justice. However, a lot of the concepts that we discover and build upon on the way — groups, fields, roots of unity, and the Galois correspondence — are profound and fascinating results. By the end of the journey, many mathematicians find these ideas to be more enticing than Abel-Ruffini itself, which is then presented as an immediate corollary of a deeper theory.

I'm going to hide some of the details that aren't necessary for someone who's only interested in Abel-Ruffini and isn't as interested in learning a lot of jargon or seeing some theorems in a completely general form that isn't relevant. That being said, I'm going to try to do some of the big ideas that we encounter on the way justice in the hopes that it provides a new way of thinking about things or a peek at the manifold beauty of mathematics.

3 Prerequisites

3.1 Sets

3.2 Euler's Number *e*, Complex Numbers, and the Complex Plane

Euler's number is perhaps the most important number in mathematics.

Its value 2.718...

Besides showing up in the solution to hundreds of differential equations — formulas that describe change —

While the real numbers form a number *line*, the complex numbers form a number *plane*.

4 Fields

These four operations are the standard operations in **fields**.

If you're working in a space where there's a reasonable notion of addition, subtraction, multiplication, and division, chances are you're working in a field.

Example 4.1. The **rational numbers** — the set of fractions — denoted $\mathbb{Q}$ (for $\mathbb{Q}$uotient), are a field.

Example 4.2. The **real numbers** $\mathbb{R}$ — the whole number line, including numbers like π that can't be written as a fraction, are a field.

Example 4.3. The **complex numbers** $\mathbb{C}$ — the set of all real and imaginary numbers are a field.

One example of a

If we could just "extend" $\mathbb{Q}$ by also adding $\Delta = \sqrt{b^2 - 4ac}$ into it, then we could express the roots of a quadratic polynomial entirely in terms of $+, -, \times, \div$, and $\sqrt{}$.

5 Field Extension

Field extensions are our first

5.1 Splitting Fields

Definition 5.1 (Splitting Field)**.** The **splitting field** F of a polynomial is f is a field that contains every root of f. In other words, F is the splitting field of a polynomial f if we can write

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$$

and each root α is a member of F.

Example 5.1. Consider the polynomial x^2+1. This polynomial doesn't have real roots, so $\mathbb{R}$ is *not* the splitting field of $x^2 + 1$. However, $\mathbb{C}$ is: both the roots of x^2+1, $\pm i$, are contained in $\mathbb{C}$, so we can write $x^2+1 = (x+i)(x-i)$.

Example 5.2. The polynomial x^2-2 has roots $\pm\sqrt{2}$, so $\mathbb{Q}$ is not its splitting field because its roots are irrational. $\mathbb{Q}(\sqrt{2})$ and $\mathbb{R}$ are both splitting fields for $x^2 - 2$.

As an aside,

Theorem 1 (Fundamental Theorem of Algebra)**.** $\mathbb{C}$ *is its own splitting field.*

5.2 Field Automorphisms

6 Groups

These sets of automorphisms possess, in an abstract way, a fascinating symmetry. When mathematicians want to talk about symmetry, we usually describe them by talking about **groups**, which are sets of objects that posses symmetry.

The operation determines whether the a set is a group or not; a set may or may not be a group depending on what operation we're manipulating it with, even though the actual objects we're working with are the same. The next two examples illustrate this nicely:

Example 6.1. The integers under addition are a group.

Example 6.2. The integers under multiplication is *not* a group, because not every number has a multiplicative inverse!

Example 6.3. The positive real numbers under multiplication is a group.

Example 6.4. Every field is a group under the operation of addition.

Example 6.5. Every vector space is a group under vector addition.

Example 6.6. The integers mod n (written $\mathbb{Z}/n\mathbb{Z}$) is a group under modular arithmetic.

Group theory is one of the deepest and most profound areas of mathematics; it describes the fundamental rules of symmetry, and the possible kinds of symmetry. It has applications to computer science, biology, engineering, chemistry, linguistics, and many more fields. Wherever there is symmetry, there are groups; and wherever there are groups, there is symmetry.

In fact, the **axiom of choice** is equivalent to the statement "For every set, there exists an operation giving that set a group structure."

6.1 The Roots of Unity

My favorite example of a group is called the **n^{th} roots of unity**, which are the roots of the polynomial $x^n - 1$.

Example 6.7. The second roots of unity are the roots of $x^2 - 1$, which are 1 and -1.

Example 6.8. The third roots of unity are the roots of $x^3 - 1$, which are

Example 6.9. The fourth roots of unity are the roots of $x^4 - 1$, which are 1, -1, i, and $-i$.

If you look at the complex plane, you'll see that the n^{th} roots of unity form a regular n-gon on the unit circle. This way, you can see how the roots are symmetric.

6.2 Cyclotomic Extensions

7 How Groups Interact

7.1 Quotient Groups

Definition 7.1. A group G is called **simple** if it doesn't have any normal subgroups N with $1 < \#N < \#G$.

7.2 Direct Product Groups

If you have two groups, is there a way to combine them to get more groups?

7.3 Galois Groups

When an automorphism group is as large as possible — that is to say, when the roots it contains are as self-symmetric as possible — we call the automorphism group a **Galois group** for emphasis.

[2]

7.4 Solvable Groups

What property do Galois groups have to possess for their associated polynomials to be solvable in radicals? A group with property is called **solvable**:

Definition 7.2 (Solvable Group)**.** We call a group G solvable if

7.5 The Galois Correspondence

8 Abel-Ruffini

We've covered all the ground that we need to, so it's time to put all this information together!

Theorem 2 (Abel-Ruffini)**.** *A polynomial $f(x)$ in a field F[3] is solvable in radicals if and only if the Galois group of its splitting field is solvable.*

Proof. (Forward Direction). Assume f is separable.

First, let's start with a polynomial f that's solvable in radicals and then prove that the Galois group of its splitting field is solvable. Let's call f's splitting field K and its Galois group $\mathrm{Gal}(K/F)$.

[2] You may sometimes hear mathematicians talk about the **Galois group of a polynomial**, which is just short for "the Galois group of a polynomial('s splitting field)." This abbreviation is nice, but it's extra terminology to remember, so I won't be using it.

[3] In a field F of characteristic not dividing $\deg(f)$!

If α is any root of f, then α is expressible in radicals, so by our proposition (Dummit properties of solvable groups) there exists a Galois extension L_α/F containing α such that $\mathrm{Gal}(L_\alpha/F)$ is solvable.

Then the composite L of all the L_α over all roots α of f is also Galois over F, and its Galois group is a subgroup of the direct product of the $\mathrm{Gal}(L_\alpha/F)$ by our results on the Galois groups of composite extensions.

Since the direct product of a solvable group is solvable, and subgroups of solvable groups are solvable, that means the Galois group of L/F is solvable.

Since L contains all roots of f, it contains K, and so by the fundamental theorem of Galois theory $G = \mathrm{Gal}(K/F)$ is a quotient of $\mathrm{Gal}(L/F)$. Thus G is a quotient of solvable group, hence is solvable. □

Proof. (Reverse Direction). Suppose G is solvable with chain $G = G_0 \geq G_1 \geq G_k = \{e\}$ such that G_{i+1} is normal in G_i and G_i/G_{i+1} is a cycle of order n_i.

By the fundamental theorem of Galois theory, the corresponding fixed fields $F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_k = K$ such that K_{i+1}/K_i is Galois with cyclic Galois group of order n_i.

If we let E □