The Insolvability of the Quintic by Radicals

- A Galois Theoretic Journey -

By Takaya Ueno

1 The Quest to Solving Polynomials

One of the most familiar concepts in mathematics that many have come across is the study of polynomial equations. Whilst solving them may seem routine today, this was certainly not the case in the past. From ancient Babylonian tablets to the birth of modern algebra, one of the central quests in mathematics has been to solve polynomial equations—a pursuit that revealed deep and beautiful connections across the mathematical world.

Consider the general quadratic equation

$$ax^2 + bx + c = 0$$

This has a well-known solution using the quadratic formula. Methods for solving such equations date back as early as 1600BC in Babylon, where early mathematicians—often priests—developed techniques for solving specific forms of quadratics [6]. However, it is important to note that the quadratic formula as we know it today, did not mean the same to the Babylonians. Take for example $x^2 + bx = c$ and $x^2 - bx = c$. In modern day algebra, these problems are equivalent since the coefficient of x can be positive or negative. However, the two were considered distinct at the time since negative numbers were not conceptually accepted or geometrically meaningful at the time [4].

In fact, it wasn't until the 9th century when Muḥammad ibn Mūsā al-Khwārizmī presented a more systematic approach to solving quadratic equations algebraically. Later, in 1637, the French mathematician René Descartes (1637) gave the quadratic formula in symbolic form in his work *La Géométrie*, which famously connected algebra and geometry. [4]. The familiar formula:

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

is thus the product of many centuries of mathematical development.

With the quadratic equation more or less settled, attention naturally turned to cubic and quartic equations. In the 16th century, Italian mathematicians such as Scipione del Ferro, Niccolò Tartaglia, and Gerolamo Cardano developed a method for solving the general cubic equation. Moreover, another Italian, Lodovico Ferrari, a student of Cardano, discovered a way to solve quartic equations [1, 6]. These formulas, while important, are far more complicated than the quadratic formula and are rarely used in practice. Still, they all share one key feature: they rely on extracting roots—a method now known as *solving by radicals.*

Given this historical trend, many believed it was just a matter of time before someone would find a general formula for the quintic—those of degree five. Yet, despite many creative attempts, no such formula emerged.

In 1799, Paolo Ruffini published a proof claiming the impossibility to solve the general fifth-degree polynomial with radicals, but this proof lacked the rigor required for full acceptance and thus left doubts on his conclusion [2]. Mathematicians seek for breakthroughs, and this as a side effect, left most mathematicians to lose interest as an impossibility proof seemed to lead nowhere. Despite this, it was still a step forward even though it was not appreciated in his time [6]. It was not until 1824 that the Norwegian mathematician Niels Henrik Abel, at just 22 years of age, provided a complete proof that the general quintic equation cannot be solved by radicals. This result is now known as the **Abel-Ruffini Theorem**[3].

At first, it seemed like the end of the story. But mathematicians weren't satisfied with simply knowing *that* something was impossible—they wanted to understand *why.* What determines whether a polynomial is solvable? What deeper structures govern this?

This is where Évariste Galois enters the picture. A brilliant young French mathematician, Galois introduced the idea that the solvability of a polynomial is fundamentally tied to the symmetries of its roots. His work developed a revolutionary framework that linked field and group theory, which we now call Galois theory. At its core, the principle is as follows:

A polynomial is solvable by radicals if and only if its Galois group is solvable

This insight not only explained why the quintic is not solvable, but also laid the foundations and created a new area of mathematics we now call **abstract algebra**.

In the following chapters, we aim to build the necessary tools to understand this deep and beautiful connection between symmetry and solvability.

Note: The next sections begin directly with field theory and assumes sufficient mathematical maturity and understanding of groups and rings, including irreducibility and minimal polynomials. While it is still possible to follow along by occasionally stepping back and reading upon definitions, as this paper is a non-rigorous and surface level expository, it is worth studying groups and rings first before diving into fields and ultimately, Galois theory.

2 Fields and Extensions

To understand Galois theory, we begin with the algebraic structures that describe how numbers, or more generally algebraic elements, behave under certain operations. In particular, we are interested in a structure called **fields** and how they can be extended to include new elements such as the roots of polynomials.

Definition 2.1 A **field** $(F, +, \cdot)$ is a triple consisting of a set F with a binary operation $+, \cdot : F \times F \to F$ such that it is a commutative ring in which every non-zero element has a multiplicative inverse. That is, $F^\times = F \setminus \{0\}$ and for all $a \in F^\times$, there exists $a^{-1} \in F$ such that $aa^{-1} = 1$

Fields generalize the arithmetic properties of $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$, and are the natural setting in which polynomials are studied.

Remark. our definition of a ring assumes the existence of a multiplicative identity 1. Some authors take commutative rings to possibly lack the identity.

Example 2.2 A common example of a field (and one that we will see all the time) is the set of rational numbers $\mathbb{Q}$. We can verify this using the ring axioms, in addition to checking if there exists a multiplicative inverse for all elements in $\mathbb{Q}$. To build on this example, consider $\mathbb{Q}(\sqrt{2}) := \left\{a + \sqrt{2}b \mid a, b \in \mathbb{Q}\right\}$. Since a field requires the existence of multiplicative inverses, consider $\frac{1}{a+\sqrt{2}b}$, then we have:

$$\frac{1}{a+\sqrt{2}b}\cdot\frac{a-\sqrt{2}b}{a-\sqrt{2}b}=\frac{a-\sqrt{2}b}{a^2-2b^2}=\frac{a}{a^2-2b^2}-\frac{\sqrt{2}b}{a^2-2b^2}\in\mathbb{Q}(\sqrt{2})$$

Thus we have that $\mathbb{Q}(\sqrt{2})$ is a field.

Definition 2.3 Let F be a field. A field E is a **field extension** of F, denoted $E:F$, if F is a subfield of E or more generally, F is isomorphic to a subfield of E. The **degree** of $E:F$ is written $[E:F]=\dim_F E$.

Let us unpack this definition. Earlier, we observed that $\mathbb{Q}$ is an example of a field. The central idea of a field extension is to start with a field like $\mathbb{Q}$ and construct a new field E that contains the roots of polynomials not solvable in $\mathbb{Q}$. For example, 2 is a rational number and so it is contained in the field $\mathbb{Q}$. However, $\sqrt{2}$ is not in $\mathbb{Q}$ as it is an irrational number. What we can do instead, is to **adjoin** this by extending $\mathbb{Q}$ into a larger field that contains $\sqrt{2}$. That is, define $\mathbb{Q}(\sqrt{2})$, read $\mathbb{Q}$ adjoined $\sqrt{2}$, as the smallest field containing both $\mathbb{Q}$ and $\sqrt{2}$. We thus have the following definition:

Definition 2.4 If α is an element that is not in F, the smallest field containing both F and α is called a **simple extension**, denoted $F(\alpha)$. That is, $F(\alpha)$ contains all of F, contains α and is the smallest field doing so.

Observe that $\mathbb{Q}(\sqrt{2})$ is a field and thus is closed under the specified operations. In particular, elements such as $1+\sqrt{2}$ and $\frac{5}{\sqrt{2}}$ are contained in $\mathbb{Q}(\sqrt{2})$.

We can continue this extension of fields as follows. Consider the element $\sqrt{3}$. This is not an element in $\mathbb{Q}(\sqrt{2})$ and so we can again adjoin this and thus have a new extension $\mathbb{Q}(\sqrt{2},\sqrt{3})$. We now have a chain of field extensions:

$$\mathbb{Q}\subseteq\mathbb{Q}(\sqrt{2})\subseteq\mathbb{Q}(\sqrt{2},\sqrt{3})$$

To summarize, we can think of this as building the field up in three steps. First, start with $\mathbb{Q}$, then adjoin $\sqrt{2}$ to $\mathbb{Q}$, which consists of all the elements of the form $a+b\sqrt{2}$ with $a,b\in\mathbb{Q}$. Finally, within that field, adjoin $\sqrt{3}$, forming $\mathbb{Q}(\sqrt{2},\sqrt{3})$ which consists of all expressions of the form $a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$ with $a,b,c,d\in\mathbb{Q}$.

Having constructed a field extension, we now turn to understanding its degree.

Definition 2.5 The **degree** of a field extension $E:F$, denoted $[E:F]$, is the dimension of E as a vector space over F.

Theorem 2.6 (Tower Law) If $F\subseteq K\subseteq E$ are fields, then

$$[E:F]=[E:K]\cdot[K:F]$$

This is a powerful theorem when dealing with radical extensions and ultimately helps to analyze the structure of roots in relation to their symmetry.

Example 2.7 Consider the example we saw earlier with $\mathbb{Q}(\sqrt{2},\sqrt{3})$. We now compute the degree of the full extension:

$$[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]=[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})]\cdot[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]$$

Since $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$, the minimal polynomial of $\sqrt{3}$ over $\mathbb{Q}(\sqrt{2})$ is $x^2 - 3$ which is irreducible. Therefore,

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2,\ [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \implies [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$$

Remark. This example shows how we can construct larger fields via a tower of simple extensions. Such towers are precisely the kind used when expressing solutions by radicals. For each step in the chain corresponds to adjoining a root — square root, cube root etc.

To summarize, we generalize this by the following chain of extensions.

$$F \xrightarrow{\sqrt[n]{\text{root in } F}} F_1 \xrightarrow{\sqrt[n]{\text{root in } F_1}} \cdots \xrightarrow{\sqrt[n]{\text{root in } F_{k-1}}} F_k$$

We reach a point where we have an extended field F_k that contains all the roots of some polynomial $f(x)$.

3 Splitting Fields and Galois Extensions

In the previous chapter, we learned how to construct field extensions by adjoining roots of polynomials. Now, we want to understand what it means for a polynomial to fully split — that is, to find a field where all of its roots live. This motivates the concept of a **splitting field**. From there, we define a special kind of field extension called the **Galois extension**, which plays a central role in Galois theory as expected.

Definition 3.1 Let $f(x)$ be a polynomial over F. A field extension $E : F$ is a splitting field of $f(x)$ over F if:

1. $f(x)$ splits into a product of linear factors over E, meaning it can be written as $f(x) = a(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha - n)$ with $\alpha_i \in E$.

2. E is the smallest field containing F and all of the roots α_i.

Example 3.2 Consider the polynomial $x^2 - 2$ over $\mathbb{Q}$. This does not split in $\mathbb{Q}$ since $\sqrt{2} \notin \mathbb{Q}$. However, if we work over $\mathbb{Q}(\sqrt{2})$ instead, we have:

$$x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$$

which works since $\pm\sqrt{2}$ is a root in $\mathbb{Q}(\sqrt{2})$. We have that the polynomial splits completely in $\mathbb{Q}(\sqrt{2})$ and since this field is generated by adjoining $\sqrt{2}$, it is the smallest such field. Therefore, $\mathbb{Q}(\sqrt{2})$ is the splitting field of $x^2 - 2$ over $\mathbb{Q}$.

It is worth noting that every non-constant polynomial in $F[x]$ has a splitting field, and although it may not be unique as a set, any two splitting fields of the same polynomial over the same base field are isomorphic over F. This allows us to meaningfully talk about the splitting field of a polynomial. Moreover, to study the structure of these fields further, especially with how roots relate to one another, we need two important properties of field extensions: **normality** and **separability**.

Definition 3.3 Let $E : F$ be a field extension. Then:

1. $E : F$ is **normal** if every irreducible polynomial in $F[x]$ that has at least one root in E splits completely in E.

2. $E : F$ is **separable** if every element of E is the root of a separable polynomial over F, meaning the polynomial has no repeated roots.

Corollary 3.4 For a field with characteristic 0, such as $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$, all irreducible polynomials are automatically separable, thus separability is guaranteed.

Definition 3.5 A **Galois extension** is a field extension that is both normal and separable.

Example 3.6 For example, $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ is Galois since it is separable, because $x^2 - 2$ has distinct roots and it is normal since $x^2 - 2$ splits completely in $\mathbb{Q}(\sqrt{2})$.

So far, we have done quite a lot on constructing fields that contain the roots of polynomials. As mentioned in the first chapter, this topic is very dense and it may be difficult to keep up without the prerequisites such as group and ring theory. Additionally, what I am laying out here is a surface level foundational concept leading up to Galois theory and a lot of rigor has been omitted to avoid side tracking from our main goal, that is the insolvability of the quintic.

With that aside, we now move onto the study of the symmetries of the roots, that is, the automorphisms of the splitting field that fixes the base field. This motivates our next goal: to define the **Galois group** of a field extension, which captures how the roots of a polynomial can be permuted without changing the base field. This group will ultimately connect field theory with group theory.

4 Galois Groups and Correspondence

In this section, we shift our focus on understanding how the roots of polynomial ”moves” within the splitting field. These movements are governed by the symmetries of the field, which in essence is captured by the Galois group.

Definition 4.1 Let $E : F$ be a field extension. The **Galois group** denoted $\mathrm{Gal}(E : F)$ is the group of all field automorphisms of E that fix every element of F. In other words, each element $\theta \in \mathrm{Gal}(E : F)$ is a bijective map $\theta : E \to E$ such that:

1. $\theta(a + b) = \theta(a) + \theta(b)$

2. $\theta(ab) = \theta(a)\theta(b)$

3. $\theta(a) = a$ for all $a \in F$.

Mathematically, we can write this as follows:

$$\mathrm{Gal}(E : F) := \{\theta : E \to E \mid \theta \text{ is a ring isomorphism and } \theta(a) = a, \ \forall a \in F\}$$

Intuitively, this group describes how the elements of E, especially the roots of polynomials, can be permuted without disturbing the base field F.

Example 4.2 Consider the extension $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$, in which $\mathbb{Q}(\sqrt{2})$ is the splitting field of $x^2 - 2$ and its roots are $\pm\sqrt{2}$. The Galois group, $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}) : \mathbb{Q})$, has two automorphisms.

1. The identity map θ_1, which sends every element to itself,

$$\theta_1(\sqrt{2}) = \sqrt{2}, \quad \theta_1(a + b\sqrt{2}) = a + b\sqrt{2}$$

2. A map θ_2 sending $\sqrt{2} \mapsto -\sqrt{2}$, fixing all elements of $\mathbb{Q}$.

$$\theta_2(\sqrt{2}) = -\sqrt{2}, \quad \theta_2(a + b\sqrt{2}) = a - b\sqrt{2}$$

These two automorphisms form a group under composition. The group table (also known as the Cayley table) is:

$\circ$	θ_1	θ_2
θ_1	θ_1	θ_2
θ_2	θ_2	θ_1

Now consider $\mathbb{Z}/2\mathbb{Z}$. This group consists of elements $\{0, 1\}$ with addition $\pmod 2$, and this group's Cayley table is:

$+ \pmod 2$	0	1
0	0	1
1	1	0

Now define a group isomorphism:

$$\phi : \mathrm{Gal}(\mathbb{Q}(\sqrt{2}) : \mathbb{Q}) \longrightarrow \mathbb{Z}/2\mathbb{Z}$$

by $\phi(\theta_1) = 0$ and $\phi(\theta_2) = 1$.

Since ϕ preserves the group structure and is a bijection, we can conclude that

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{2}) : \mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$$

and therefore, the Galois group above is isomorphic to the cyclic group of order 2. The Galois group reflects the symmetries of the roots, in this case, the only symmetry is flipping $\sqrt{2} \leftrightarrow -\sqrt{2}$. This leads us to the **Fundamental Theorem of Galois Theory**, which sets up a one-to-one inclusion-reversing correspondence between intermediate fields, $F \subseteq K \subseteq E$ and subgroups $H \leq \mathrm{Gal}(E : F)$.

Definition 4.3 Let $E : F$ be a Galois extension, and $G = \mathrm{Gal}(E : F)$. There exists a bijection:

$$\begin{aligned} \{L \mid E : L : F\} &\leftrightarrow \{H \mid H \leq G\} \\ L &\longmapsto Gal(E : L) \\ E^H &\longleftarrow H \end{aligned}$$

Since the previous example regarding $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}) : \mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$ has only two subgroups: the full group and the trivial group, we take a look at more interesting example.

Example 4.4 Consider $\mathbb{Q}(\omega, t)$ where $\omega = e^{\frac{2\pi i}{3}}$ and $t = \sqrt{3}$. For simplicity I will omit a few proofs regarding separability and splitting fields, although I encourage you to verify the following yourself.

$\mathbb{Q}(\omega, \sqrt{3})$ is the splitting field of the polynomial $f(x) = (x^2 - x + 1)(x^2 - 3) \in \mathbb{Q}[x]$ and by the tower law, since $\omega \notin \mathbb{Q}(\sqrt{3})$ and $\sqrt{3} \notin \mathbb{Q}(\omega)$, the fields are linearly disjoint over $\mathbb{Q}$. Thus,

$$[\mathbb{Q}(\omega, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] \cdot [\mathbb{Q}(\omega) : \mathbb{Q}] = 4$$

This shows us that the size of the Galois group $|G| = 4$, and since we are looking for a group that is isomorphic to this, it must be that whatever this group is, is of size 4.

In order to differentiate this, we must determine the behavior of $\theta \in G$. In particular, any θ is determined by its values on $\sqrt{3}$ and ω. Moreover, $\theta(t) \in \left\{\pm\sqrt{3}\right\}$ and $\theta(\omega) \in \{\omega, \omega^5 = \omega^{-1}\}$. Since $|G| = 4$, all possibilities must occur and $G = \{\theta_1, \theta_2, \theta_3, \theta_4\}$ where:

$$\begin{array}{ll} \theta_1 : t \mapsto t,\ \omega \mapsto \omega & \theta_2 : t \mapsto -t,\ \omega \mapsto \omega \\ \theta_3 : t \mapsto t,\ \omega \mapsto \omega^{-1} & \theta_4 : t \mapsto -t,\ \omega \mapsto \omega^{-1} \end{array}$$

Computing the order of each element, we see that each element is of order 2. For example if you apply θ_2 twice, we have the following:

$$\theta_2^2(t) = \theta_2(\theta_2(t)) = t$$

In other words, applying the operation twice gives the element you initially started with. There is one group in particular that is of size 4 and each element has order 2, which would be the the Klein 4-group, often denoted V_4 or $C_2 \times C_2$. Thus, we can conclude that $G \cong C_2 \times C_2$.

To wrap this example up, we use the Galois correspondence to essentially build a subgroup lattice to show all the subgroups and its correspondent fields. To put it simply, we analyze each θ and determine what elements are being fixed. For example, θ_2 fixes ω since t is being mapped to $-t$. Additionally, θ_3 fixes t since t is being mapped to itself but ω is being mapped to its inverse. Given that $C_2 \times C_2$ have the elements $\{e, a, b, ab\}$ where e is just the identity element, we have the following:

$$\begin{aligned} H_1 = \{\theta_1\} &\implies \text{Fix}(H_1) = \mathbb{Q}(\omega, t) \\ H_2 = \{\theta_2\} &\implies \text{Fix}(H_2) = \mathbb{Q}(\omega) \\ H_3 = \{\theta_3\} &\implies \text{Fix}(H_3) = \mathbb{Q}(t) \\ H_4 = \{\theta_4\} &\implies \text{Fix}(H_4) = \mathbb{Q}(i) \text{ since } i = \frac{\omega - \omega^{-1}}{t} \in \mathbb{Q}(\omega, t) \end{aligned}$$

By fixing G to be $\mathbb{Q}$, we can create the following subgroup lattice:

$$\begin{tikzcd}
& G \leftrightarrow \mathbb{Q} \arrow[dl, no head] \arrow[d, no head] \arrow[dr, no head] & \\
H_2 \leftrightarrow \mathbb{Q}(\omega) \arrow[dr, no head] & H_3 \leftrightarrow \mathbb{Q}(\sqrt{3}) \arrow[d, no head] & H_4 \leftrightarrow \mathbb{Q}(i) \arrow[dl, no head] \\
& H_1 \leftrightarrow \mathbb{Q}(\omega, t) &
\end{tikzcd}$$

It's difficult to grasp this concept in the beginning, and I suppose the bigger question is, what does this do exactly? It feels as though we have moved so far away from the initial question on polynomials. How does this relate to the question of whether a polynomial can be solved using just radicals? This is a valid point and one that I got myself thinking when I was first introduced to this concept. The beauty of all of this is that what seems to be completely disconnected topics, has a way of coming together and answering those questions.

5 The General Quintic and the Role of S_5

Definition 5.1 A finite group G is **solvable** if there exists a chain of subgroups

$$\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$$

such that each $G_i \trianglelefteq G_{i+1}$ is normal and the quotient G_{i+1}/G_i are abelian (in fact, cyclic of prime order).

These prime-order quotients reflect how you can "disassemble" the group using radical operations. In Galois theory, this means: **a polynomial is solvable by radicals if and only if its Galois group is a solvable group**, which is exactly what was stated in the first chapter. Naturally, primes appear as the order of the building blocks of the group (which is fascinating in itself but more on this on another day).

Let's revisit some earlier examples and see how primes govern solvability:

- For $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}) : \mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$, the group has order 2, a prime, and is solvable trivially. That is,

$$S_2 \xrightarrow{2} e$$

- For $\mathrm{Gal}(\mathbb{Q}(\omega, \sqrt{3}) \colon \mathbb{Q}) \cong C_2 \times C_2$, every subgroup has index 2, again a prime, and thus it is solvable.

In fact we can start from some symmetric group S_n whose elements are all the bijections from the set to itself, and observe the chain of subgroups to see that the degree of each pair is in fact a prime.

Example 5.2 Consider the symmetric group on 3 elements, S_3. We have the following chain:

$$S_3 \to C_3 \to e$$

S_3 is the symmetric group with order 6, since $|S_n| = n!$. C_3 is the cyclic group of order 3, which is normal in S_3. Thus we have $[S_3 : C_3] = 2$ and $[C_3 : \{e\}] = 3$. Each step is prime, so it is a solvable group. This corresponds to a cubic polynomial like $x^3 - 2$, which is solvable by radicals.

Example 5.3 Now lets consider a generic quartic polynomial such as $x^4 - 1$. The Galois group is S_4 or really any subgroup of it with an order of less than $4! = 24$. One possible composition would be:

$$S_4 \to A_4 \to C_2 \times C_2 \to C_2 \to e$$

Now lets compute the quotients.

$$[S_4 : A_4] = 2,\ [A_4 : C_2 \times C_2] = 3,\ [C_2 \times C_2 : C_2] = 2,\ [C_2 : \{e\}] = 2$$

All composition factors are of prime order, and hence it is solvable. This means that degree 4 polynomials are solvable by radicals in general.

It is easier to see now where we are heading. By utilizing the Galois groups, its correspondence and the definition of solvability, we have determined that there is an underlying reason as to why there is a general formula for quadratic, cubic and quartic polynomials. Now what happens when we apply the same to the general quintic?

The typical Galois group of a degree-5 polynomial is S_5, the symmetric group on 5 elements. S_5 has a normal subgroup, that is the alternating group A_5, so we can compute this.

$$[S_5 : A_5] = 2$$

So far there are no issues, since 2 is a prime. However, A_5 is simple and non-abelian and also has order 60. If a group is simple, then it has no non-trivial normal subgroups. Which means that the only normal subgroups of A_5 are itself and the trivial group $\{e\}$. Thus, we have the following chain:

$$S_5 \xrightarrow{2} A_5 \xrightarrow{60} \{e\}$$

And so the right hand side of the chain has quotient group A_5 which is non-abelian, not of prime order and not a cyclic group of prime order. This violate the requirement for a solvable group, which demands that each quotient in the series be abelian and of prime order, like $\mathbb{Z}/p\mathbb{Z}$ where p is prime.

Furthermore, this occurs with degree-6 and higher polynomials as well, where for S_6 we have:

$$S_6 \xrightarrow{2} A_6 \xrightarrow{360} \{e\}$$

which again, violates the requirement for what it means to be solvable.

This is precisely where Galois theory stands out. It doesn't just say that you can't solve the quintic by radicals, but rather it explains why; the Galois group is not solvable, the composition factors contain non-abelian simple groups like A_5 and the prime factor chains stops working. At the end of the day, it is not really the polynomial that is difficult, but rather the symmetries of its roots that become too entangled with just square and cube roots.

This complex journey from field extensions to Galois groups reveals a remarkable unity between algebra and symmetry, something that is present in various fields within mathematics. What began as a fairly elementary question of "can I solve this equation?" led to the abstract but precise nature of group theory.

When it can be solved, we obtain the familiar radical formulas for quadratics, cubics and quartics. When we can't, we discover that the obstacle lies not necessarily in our ability to compute, but in the fundamental nature of algebraic symmetries. This is the essence of Galois theory: a classification of solvability through symmetry.

6 Further Studies and A Historical Epilogue and

As mentioned in previous chapters, this paper alone does not contain nearly enough information to cover the density of abstract algebra; there is a reason why many textbooks going over groups, rings, fields and Galois theory are couple hundred pages long. However, even at this level, we were able to explore and witness something rather extraordinary. If you'd like, I suggest **Abstract Algebra by Dummit and Foote** as the study tool to learn abstract algebra from the ground up, or if you are already proficient, going through **Galois Theory by Ian Stewart**, which focuses more on what this paper went through, but with more rigor and problems to better understand the content. From here, one can go further in many directions; one may explore how these ideas extend into infinite extensions or the classification of finite simple groups, each of which deepens the role that symmetry plays in algebra. It is truly remarkable that a problem that had mathematicians working for centuries led to the formalization of what we now call abstract algebra, and how that in itself impacted other areas of mathematics such as cryptography, topology and more. To wrap this paper up, I thought it was best to include some historical context of certain mathematicians, not necessarily as problem solvers, but as theory builders—great minds who transformed a concrete question into abstract clarity.

6.1 Paolo Ruffini (1765 - 1822)

In 1799, an Italian polymath **Paolo Ruffini** published an attempt to prove the insolvability of the quintic in his two-volume book, *Teoria Generale delle Equazioni*, stating that the algebraic solution of general equations of degree greater than four is always impossible [6]. Hi method was partially group-theoretic, which was decades before the formalization of the introduction of a group. Ruffini attempted to analyze permutations of roots and deduce the impossibility of expressing them using only radicals [4].

Although his work was never truly appreciated during his time, due to it containing many gaps and flaws, he was the first to properly argue for the insolvability of the general quintic. Modern historians recognize his work as a precursor to later developments in Galois theory [7].

6.2 Niels Henrik Abel (1802 - 1829)

Two decades later, the Norwegian mathematician **Niels Henrik Abel** provided the first complete and rigorous proof that no general formula exists for solving fifth-degree equations by radicals. His 1824 publication gave a concice and general argument that transformed the discussion of solvability, now known as the **Abel-Ruffini** theorem [4].

However, Abel's life was far from glorious. His short life was marked by poverty and illnesses and he died of tuberculosis at the young age of 26. He left behind a body of work that would eventually take decades to be fully appreciated. In the modern day, the **Abel Prize** honors his legacy as one of the founders of modern algebra, and in fact, the abelian group is named after him.

6.3 Évariste Galois (1811 - 1832)

Galois made the decisive leap, asking: *what determines whether a polynomial is solvable by radicals?*

Galois introduced the concept of the Galois group, which reflects the symmetries among the roots of a polynomial. His insight was that a polynomial is solvable if and only if its Galois group is solvable. That is, if it can be decomposed into a sequence of simpler groups, each of prime order [6].

He was a radical political activist, as well as a mathematical one. Repeatedly rejected by academic institutions and imprisoned for revolutionary activity, he died in a duel at the age of 20. The night before, expecting his end, he wrote an extensive letter outlining his theory. While the theory itself required a lot of formalization in the coming decades, it became the foundation of what we now call **Galois theory** [5].

His work was more or less neglected until it was published by **Joseph Liouville**, fourteen year after Galois' death. Only then did the mathematical world begin to understand the magnitude of what Galois had accomplished during his short time on earth.

6.4 A Lasting Legacy

Where Ruffini asked the question, and Abel answered that question, Galois then revealed the structure behind it. It is important to note that there are many more mathematicians who had contributed in this field, but Galois theory does more than just prove the impossibility, it explains why and by doing so, it bridged the seemingly unrelated worlds of polynomials, symmetry and abstract algebra.

References

[1] Carl B. Boyer and Uta C. Merzbach. *A History of Mathematics*. John Wiley & Sons, 1991.

[2] David A. Cox. *Galois Theory*. John Wiley & Sons, 2012.

[3] Harold M. Edwards. *Galois Theory*. Springer, 1984.

[4] Victor J. Katz. *A History of Mathematics: An Introduction*. Addison-Wesley, Boston, MA, 3 edition, 2009.

[5] Laura Toti Rigatelli. *Evariste Galois, 1811–1832*. Birkhäuser, Boston, 1996.

[6] Ian Stewart. *Galois Theory*. Chapman and Hall/CRC, Boca Raton, FL, 5 edition, 2022.

[7] B.L. van der Waerden. *Modern Algebra*. Springer, 7 edition, 2006.