INSOLVABILITY OF THE QUINTIC

IAN PORTEOUS

ABSTRACT. Most of us remember a time when we were forced to memorize the quadratic equation. Given enough time and dedication, we may also have seen the formula for the roots of the general third degree polynomial. This appears to put us on a trend. That given enough time and dedication, we can produce a formula or algorithm for finding the roots of a polynomial of any degree. Well, unfortunately (or fortunately if you've ever found the roots of a fourth degree polynomial by hand), this process breaks down at the fifth degree. This paper will outline the argument that leads to this surprising result.

1. INTRODUCTION

To begin this journey, we will go through some background information that will help us along our path. Firstly, let us recall the explicit formula for the quadratic formula. If $f(x) = ax^2 + bx + c$ is a polynomial with real coefficients and $a \neq 0$, then the roots of $f(x)$ are given by $x = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$. Note that if $b^2 - ac < 0$, then these roots are not real numbers. This leads directly to the idea of "extending" the field of real numbers to include new "imaginary" numbers. This idea leads to one of the main notions we will be working with, namely the idea of field "extensions." This process will be made explicit several sections from now.

Since we have an equation to find the roots of a degree two polynomial, it make sense to ask: can we find equations to that give the roots of higher degree polynomials? Based off the work of Cardano and others, the answer is yes, to a point. They were able to figure out methods for finding the roots of the general cubic and quartic polynomials, but the formula for the general quintic polynomial escaped them. Here is where Galois' theory comes in. The main focus of his study was to establish a connection between group theory and field theory. We will later go through the details of this connection, which will ultimately prove that there is no formula for the roots of the general quintic.

2. Background Material

In this paper we will be using some concepts from abstract algebra, such as groups, polynomial rings, ideals, and fields. We quickly review some of the relevant definitions.

Definition 2.1. A **group** is a set G together with an associative binary operation $*$ on G satisfying the following axioms:

(1) there exists an element $e \in G$, called the **identity** of G, such that for all $a \in G$ we have $a * e = e * a = a$; and
(2) for each $a \in G$ there is an element $a^{-1} \in G$, called the **inverse** of a, such that $a * a^{-1} = a^{-1} * a = e$.

We say the group is **abelian** if $a * b = b * a$ for all $a, b \in G$.

Definition 2.2. A **ring** is a set R together with two binary operations, usually denoted $+$ and $\cdot$, such that:

(1) R is an abelian group under $+$;
(2) the operation $\cdot$ is associative; and
(3) the distributive laws hold, i.e., for every $a, b, c \in R$ one has:
 (a) $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$; and
 (b) $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$.

We say the ring is **commutative** if the operation $\cdot$ is commutative, i.e., if $a \cdot b = b \cdot a$ for all $a, b \in R$. We say the ring **has unity** if there is an identity for the operation $\cdot$. All of the rings we consider will be commutative rings with unity. We will denote the additive identity by 0 and the multiplicative identity by 1.

Definition 2.3. Given a ring R, the **polynomial ring** in the variables $x_1, x_2, \ldots, x_n$ with coefficients in R is denoted $R[x_1, x_2, \ldots, x_n]$ and is defined inductively by $R[x_1, x_2, \ldots, x_n] = R[x_1, x_2, \ldots, x_{x_1}][x_n]$

Less formally, this gives a polynomial in n variables with coefficients that come from a given ring.

Definition 2.4. An **ideal** in a commutative ring R is a subset $I \subseteq R$ satisfying the following properties:

(1) I is a subgroup of R under $+$; and
(2) for every $r \in R$ and $i \in I$, one has $ri \in I$.

A proper ideal is **maximal** if it is maximal under inclusion, i.e., if the only ideals containing it are itself and the entire ring.

Definition 2.5. A **field** is a commutative ring with unity in which every nonzero element is a **unit**, i.e., has a multiplicative inverse.

Example 2.6. The set of integers, $\mathbb{Z}$, is a ring but not a field. The set of rational numbers, $\mathbb{Q}$, is a field. The setsb of real and complex numbers, denoted $\mathbb{R}$ and $\mathbb{C}$, respectively, are both fields.

3. Irreducible Polynomials and the Extensions that Love Them

3.1. **Field Extensions.**

To begin the process of figuring out why a general quintic polynomial has no formula for its roots, we must start here, with irreducible polynomials and field extensions. We begin with the idea of "extending" a field:

Definition 3.1. If K is a field containing a subfield F, then K is said to be an **extension field** (or **field extension**) of F. This is often denoted K/F. We may sometimes refer to F as the **base field** for the extension.

Many of us are familiar with this notion, though we may have seen it under a different guise. Take the polynomial $f(x) = x^2 + 1$. A root of $f(x)$ corresponds to a solution to the equation $x^2 + 1 = 0$. We very quickly find that this has no solutions in $\mathbb{R}$, since $r^2 \geq 0$ for every real number r. Thus, the polynomial $f(x) = x^2 + 1$ is **irreducible** over $\mathbb{R}$, i.e., cannot be factored into two polynomials of smaller degree in $\mathbb{R}[x]$. This leads us to two possibilities. The first is to get rid of this equation and pretend it never happened. Alternatively, we can figure out a way to make this work, i.e., a way to "extend" or "enlarge" our field to include a root of $f(x)$.

Following the second option, we introduce a new "number" which we label i with the defining property that it is a root of the polynomial $f(x) = x^2 + 1$, i.e., $i^2 + 1 = 0$. (For this reason, the number i is sometimes denoted $\sqrt{-1}$.) We then form the smallest set of elements that contains $\mathbb{R}$, this new number i, and is also a field. This ultimately leads to the field of complex numbers, $\mathbb{C}$. Every number in $\mathbb{C}$ is of the form $a+bi$ where $a, b \in \mathbb{R}$. Note that if we let $b = 0$, we get our familiar real numbers back. Viewed as a vector space over $\mathbb{R}$, the field $\mathbb{C}$ is two dimensional. We say the extension $\mathbb{C}/\mathbb{R}$ is an extension of **degree** two. The idea of using dimension of one field as a vector space over another becomes wildly important later.

It is now appropriate to ask the following:

Question. Given some field F and some nonconstant irreducible polynomial $p(x) \in F[x]$, can we come up with some field extension of F that contains a root of $p(x)$?

It turns out we can. That is, there exists a field K containing (an isomorphic copy of) F in which $p(x)$ is a root. The process by which we create this field is fairly straightforward. We let $K = F[x]/(p(x))$, where $(p(x))$ the ideal in $F[x]$ generated by the irreducible polynomial $p(x)$. Since $p(x)$ is irreducible in $F[x]$, by basic facts in ring theory the ideal $(p(x))$ in $F[x]$ is maximal, and as taking the quotient by a maximal ideal produces a field (another basic fact in ring theory), we have that K is a field. It is straightforward to check that there is a copy of F in this new field, namely the (image of) the constant polynomials.

3.2. **Algebraic Field Extensions.** Now, we move onward to the topic of algebraic extensions.

Definition 3.2. Suppose K/F is a field extension. We say an element $\alpha \in K$ is **algebraic over** F if α is is the root of some nonzero polynomial in $F[x]$.

It turns out that if α is algebraic over F then there is a unique monic irreducible polynomial in $F[x]$ that has α as a root. We call this polynomial the **minimal polynomial** of α over F and denote it $m_{\alpha,F}(x)$.

We can also generate a field by a single element, in a way reminiscent of generating a subgroup of a group. If we have a field extension K/F, then the **field generated by** α **over** F is the smallest subfield of K that contains F and α. We denote this field by $F(\alpha)$.

Since degrees of extensions plays such a major role in what is to come, it is worth noting the following result:

Theorem 3.3. *Suppose K/F is a field extension and $\alpha \in K$ is algebraic over F. Then $F(\alpha) \cong F[x]/(m_{\alpha,F}(x))$ and furthermore, we have $[F(\alpha) : F] = \deg(m_{\alpha,F}(x))$.*

The degree of $F(\alpha)$ over F is called the **degree of** α **over** F, and denoted $\deg_F(\alpha)$.

Example 3.4. As a quick example of this idea, we will look at the minimal polynomial for $\sqrt{2}$ over $\mathbb{Q}$. It might seem too easy to guess that the given polynomial would be $f(x) = x^2 - 2$ is the minimal polynomial, but that is exactly the case. Clearly, the polynomial has two roots $x = \pm\sqrt{2}$. Then, a basic number theory proof will show that $\sqrt{2} \notin \mathbb{Q}$, which forces $f(x)$ to be irreducible in $\mathbb{Q}[x]$. It follows that $\sqrt{2}$ is degree 2 over $\mathbb{Q}$ and thus, $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

It is worth noting that if α is an element of an extension of degree n over F, then α satisfies a polynomial of degree at most n over F;

conversely, if α is the root of a polynomial of degree n in $F[x]$, then the degree of $F(\alpha)$ over F is at most n. We note one last result about degrees of field extensions:

Theorem 3.5 (The Tower Law)**.** *If $F \subseteq K \subseteq L$ are fields, then $[L : F] = [L : K][K : F]$. In particular, if L/F is a finite extension and $F \subseteq K \subseteq L$, then $[K : F]$ divides $[L : F]$.*

Example 3.6. Suppose we wish to look at the field $\mathbb{Q}(\sqrt{2}, \sqrt{5})$ as an extension over $\mathbb{Q}$. Now, we can see that $\sqrt{5}$ is degree 2 over $\mathbb{Q}$ (since its minimal polynomial is $m_{\sqrt{5},\mathbb{Q}}(x) = x^2 - 5$, which is of degree 2). Then the degree of the extension $\mathbb{Q}(\sqrt{2}, \sqrt{5})/\mathbb{Q}(\sqrt{2})$ is 2 if $x^2 - 5$ is irreducible in $\mathbb{Q}(\sqrt{2})$, i.e., if it doesn't have a root in $\mathbb{Q}(\sqrt{2})$. So, it makes sense to now check if $x^2 - 5$ has a root in $\mathbb{Q}(\sqrt{2})$. Suppose $\sqrt{5} \in \mathbb{Q}(\sqrt{2})$. Then we would have $\sqrt{5} = a + b\sqrt{2}$ for some $a, b \in \mathbb{Q}$. Squaring both sides gives $5 = (a^2 + b^2) + 2ab\sqrt{2}$. This then gives us three possibilities. If $ab \neq 0$, solving this for $\sqrt{2}$ we find that $\sqrt{2} = \frac{5-a^2-b^2}{2ab} \in \mathbb{Q}$, a contradiction. Now, if $b = 0$, then $5 = a^2$ or $a = \sqrt{5}$, another contradiction. Lastly, if $a = 0$, then $\sqrt{5} = \sqrt{2}b$, solving for b we find that $b = \sqrt{10}$, a contradiction since $\sqrt{10} \notin \mathbb{Q}$. We can now conclude $[\mathbb{Q}(\sqrt{2}, \sqrt{5}) : \mathbb{Q}] = 4$. Furthermore, to absolutely finish this problem off, we note that $\{1, \sqrt{2}, \sqrt{5}, \sqrt{10}\}$ is a basis for $\mathbb{Q}(\sqrt{2}, \sqrt{5})$ as a vector space over $\mathbb{Q}$.

Remark 3.7. Fun side note: this same process can be used to quickly determine if certain compass and straightedge constructions are possible–including some that were unsolved for thousands of years. It turns out that if $\alpha \in \mathbb{R}$ can be constructed (as a length) by a series of compass and straightedge constructions, then $[F(\alpha) : F] = 2^k$ for some $k \in \mathbb{Z}^+ \cup \{0\}$. For example, consider the famous problem of "doubling the cube," which asks: using only compass and straightedge, can we construct a cube with exactly double the volume of a given cube? Assuming we begin with a unit cube, this is the same thing as constructing $\sqrt[3]{2}$ over $\mathbb{Q}$. By an argument similar to the one in the previous example, we can show that $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, and so $\sqrt[3]{2}$ cannot be constructed with a straightedge and compass. We cannot double the cube.

3.3. **Splitting Fields.** We next consider the concept of "splitting fields."

Definition 3.8. A polynomial $f(x)$ **splits** (or **splits completely**) in $K[x]$ if it factors completely into linear factors in $K[x]$, i.e., the field K contains all of the roots of $f(x)$.

Definition 3.9. Given a polynomial $f(x) \in F[x]$, a field extension K/F is a **splitting field extension** for $f(x)$ over F if $f(x)$ splits completely in $K[x]$ and K is the smallest field extension of F over which $f(x)$ splits completely.

It turns out that if K/F is a splitting field extension for $f(x)$, then $K = F(\alpha_1, \dots, \alpha_n)$, where the α_i are the roots of $f(x)$.

Example 3.10. We have seen that a splitting field extension of $f(x) = x^2+1$ over $\mathbb{R}$ is the field $\mathbb{C}$. If we look at the same irreducible polynomial over $\mathbb{Q}$, a splitting field extension is $\mathbb{Q}(i)$.

Definition 3.11. A field K is **algebraically closed** if every polynomial with coefficients in K also has a root in K.

Definition 3.12. Given a field F, an algebraic closure of F is a field $\overline{F}$ that is algebraic over F and such that every polynomial $f(x) \in F[x]$ splits completely over $\overline{F}$

We note that for any field F there exists an algebraically closed field K containing F, and that such a field extension of F contains an algebraic closure of F.

Theorem 3.13. *The field $\mathbb{C}$ is algebraically closed.*

It follows that $\mathbb{C}$ contains algebraic closures of any of its subfields. It turns out that $\overline{\mathbb{R}} = \mathbb{C}$, while $\overline{\mathbb{Q}}$ is a proper subfield of $\mathbb{C}$.

3.4. **Separable Extensions.** As a last topic before moving onto the section on Galois theory, we will need to set up some definitions for different types of extensions.

Definition 3.14. An irreducible polynomial in $F[x]$ is **separable over** F if it has no multiple roots (in an algebraic closure of F). An element α that is algebraic over F is **separable over** F if its minimal polynomial $m_{\alpha,F}(x)$ is separable over F.

These will be the types of extensions with which we will be working. We can extend this definition to fields in the following way:

Definition 3.15. A field extension K/F is said to be **separable** if every element of K is separable over F, i.e., the root of a separable polynomial over F.

4. The Goal of Galois

The subject at hand, Galois Theory, is named after a French mathematician, Evariste Galois, who tragically died at age 20 as a result of a duel. In the possibly-apocryphal story, he supposedly wrote down the foundations for the theory that would bear his name the night before a duel that would ultimately lead to his death. The big realization in this manuscript was that the algebraic solution to a polynomial is related the group of permutations associated to the roots of the polynomial. In other words, there is a fundamental connection between group theory and field theory. This connection between the two is what we now refer to as Galois theory. In order to properly begin the study of Galois groups and their associated extensions; we must first build our dictionary.

4.1. **Automorphism Groups.**

We need to recall several things from group theory in order to get started, the first of which will be the automorphism groups.

Definition 4.1. An isomorphism of a field K with itself is called an **automorphism** of K. We will denote the set of all automorphisms of K by $\text{Aut}(K)$. This set is a group under the operation of composition.

An automorphism $\sigma \in \text{Aut}(K)$ is said to **fix** an element $\alpha \in K$ if $\sigma(\alpha) = \alpha$. For a field extension K/F, we let $\text{Aut}(K/F)$ denote the subset of all automorphisms $\sigma \in \text{Aut}(K)$ that fix every element in F. It is easily verified that $\text{Aut}(K/F)$ is a subgroup of $\text{Aut}(K)$.

Here is a rather useful fact:

Lemma 4.2. *Suppose K/F is a field extension and $\alpha \in K$ is algebraic over F. Then for every $\sigma \in \text{Aut}(K/F)$, the element $\sigma(\alpha)$ is a root of the minimal polynomial for α over F.*

The proof for this goes as follows. Suppose $m_{\alpha,F}(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$. Then α satisfies the equation $\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0 = 0$. Now, applying the automorphism σ we find:

$$\sigma(\alpha^n) + \sigma(a_{n-1}\alpha^{n-1}) + \ldots + \sigma(a_1\alpha) + \sigma(a_0) = \sigma(0) = 0.$$

Since σ is a multiplicative morphism, this becomes:

$$(\sigma(\alpha))^n + \sigma(a_{n-1})(\sigma(\alpha))^{n-1} + \ldots + \sigma(a_1)(\sigma(\alpha)) + \sigma(a_0) = 0.$$

By assumption, σ fixes all the elements of F, so $\sigma(a_i) = a_i$ for $i = 0, 1, \ldots, n-1$. So

$$(\sigma\alpha)^n + a_{n-1}(\sigma\alpha)^{n-1} + \ldots + a_1(\sigma\alpha) + a_0 = 0.$$

This shows that $\sigma(\alpha)$ is the root of the same polynomial over F as α, which completes our proof.

The above lemma implies $\text{Aut}(K/F)$ permutes the roots of the irreducible polynomials in $F[x]$.

Example 4.3. If we look at the field $\mathbb{Q}(\sqrt{5})$, then for every $\sigma \in \mathrm{Aut}(\mathbb{Q}(\sqrt{5})/\mathbb{Q})$ we have $\sigma(\sqrt{5}) = \pm\sqrt{5}$, since these are the two roots of $m_{\sqrt{5},\mathbb{Q}}(x) = x^2 - 5$. In fact, since $\sqrt{5}$ generates $\mathbb{Q}(\sqrt{5})$ we also have that every $\sigma \in \mathrm{Aut}(\mathbb{Q}(\sqrt{5})/\mathbb{Q})$ is determined entirely by where it maps $\sqrt{5}$, so the previous observation implies that there are only two distinct elements in $\mathrm{Aut}(\mathbb{Q}(\sqrt{5})/\mathbb{Q})$, namely the identity morphism and the automorphism that maps $\sqrt{5}$ to $-\sqrt{5}$.

4.2. **Subgroups and Intermediate Extensions.** Suppose H is a subgroup of $\mathrm{Aut}(K/F)$. Let K^H denote the collection of the elements in K fixed by H. It is readily verified this is a subfield of K containing F. We call this the **fixed field** of H. So, to each subgroup of $\mathrm{Aut}(K/F)$ we can associate an intermediate field extension $F \subseteq K^H \subseteq K$.

Conversely, suppose $F \subseteq E \subseteq K$ is an intermediate field extension. One can easily check that $\mathrm{Aut}(K/E)$ is a subgroup of $\mathrm{Aut}(K/F)$. We call this the **fixing subgroup** of the intermediate extension. So, to each intermediate field extension of K/F we can associate a subgroup of $\mathrm{Aut}(K/F)$.

Observe that these associations are inclusion reversing: if we have intermediate extensions $F \subseteq E_1 \subseteq E_2 \subseteq K$, then $\mathrm{Aut}(K/E_2) \leq \mathrm{Aut}(K/E_1)$; similarly if $H_1 \leq H_2 \leq \mathrm{Aut}(K/F)$, then $K^{H_2} \subseteq K^{H_1}$.

It turns out that these associations, between intermediate field extensions and subgroups, are particularly nice when the original extension is particularly nice.

Definition 4.4. We say a finite field extension K/F is **Galois** if $[K : F] = |\,\mathrm{Aut}(K/F)|$.

As a final note before moving on to an example and the major theorem, we will present several facts involving Galois extensions.

1. If K is the splitting field over F of a separable polynomial $f(x) \in F[x]$, then K/F is Galois. In that case, we call $\mathrm{Aut}(K/F)$ the **Galois group of** $f(x)$ **over** F.
2. Conversely, if K/F is a (finite) Galois extension, then K is the splitting field over F for some separable polynomial $f(x) \in F[x]$.
3. If K/F is a (finite) Galois extension, then every irreducible polynomial $f(x) \in F[x]$ that has a root in K is separable and has *all* its roots in K.

Example 4.5. Here is an example of a process similar to Example 4.3, but with some extra steps. We will look at the extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ This is definitely Galois over $\mathbb{Q}$ since this is splitting field for the polynomial $f(x) = (x^2 - 2)(x^2 - 3)$. Thus, an automorphism $\sigma \in \mathrm{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ is completely determined by how it acts on the generators $\sqrt{2}$ and $\sqrt{3}$, which must be mapped to $\pm\sqrt{2}$ and $\pm\sqrt{3}$ respectively. We will define two automorphisms explicitly by the following:

$$\sigma(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6}$$

and

$$\tau(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6}.$$

Then we find that $\sigma^2(\sqrt{2}) = \sigma(\sigma(\sqrt{2})) = \sigma(-\sqrt{2}) = \sqrt{2}$ and $\sigma^2(\sqrt{3}) = \sqrt{3}$, so we see that $\sigma^2 = 1$. We similarly see that $\tau^2 = 1$. We can now compute the automorphism $\sigma\tau$:

$$\sigma\tau(\sqrt{2}) = \sigma(\tau(\sqrt{2})) = \sigma(\sqrt{2}) = -\sqrt{2}$$

and similarly,

$$\sigma\tau(\sqrt{3}) = \sigma(\tau(\sqrt{3})) = \sigma(-\sqrt{3}) = -\sqrt{3}.$$

Now, since both these automorphisms have order 2 in the Galois group, we find that $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) = \{1, \sigma, \tau, \sigma\tau\}$. Since this group is made up of two 2-cycles, we can conclude that the Galois group is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

5. The Main Theorem of Galois Theory

In an ideal world, we would have a bijective correspondence between the intermediate field extensions (as seen in the last example) and the subgroups of the automorphism group. If K/F is Galois, it turns out this is exactly the case. Before stating the main theorem, We note that for a Galois extension K/F, the group of automorphisms $\mathrm{Aut}(K/F)$ is called the **Galois group** of K/F and denoted $\mathrm{Gal}(K/F)$.

Theorem 5.1 (Main Theorem of Galois Theory)**.** *Suppose K/F is a (finite) Galois extension. Let $G = \mathrm{Gal}(K/F)$. The correspondence described above gives a bijection between the intermediate extensions of K/F and the subgroups of G. Moreover, the following properties hold:*

(1) if E_1 and E_2 are intermediate field extensions corresponding to subgroups H_1 and H_2 of G, respectively, then $E_1 \subseteq E_2$ if and only if $H_2 \leq H_1$;

(2) for each subgroup $H \leq G$, we have $[K : K^H] = |H|$ and $[K^H : F] = [G : H]$ (the index of H in G);

(3) for every $H \leq G$ the extension K/K^H is Galois and $\mathrm{Gal}(K/K^H) = H$;

(4) for every intermediate extension E, the fixed field of $\mathrm{Aut}(K/E)$ *is exactly E;*

(5) if E is an intermediate extension of K/F, then E/F is Galois if and only if $\mathrm{Aut}(K/E)$ *is a normal subgroup of G; and lastly*

(6) if E_1 and E_2 are intermediate extensions corresponding to subgroups H_1 and H_2 of G, then the intersection $E_1 \cap E_2$ corresponds to the group $\langle H_1, H_2 \rangle$ generated by H_1 and H_2 and the composite field E_1E_2 corresponds to the intersection $H_1 \cap H_2$.

We will graciously omit the proof for this, lest we turn this rather short paper into a never-ending monster. We will however, do a quick example illustrating how the Galois group can be used to compute minimal polynomials.

Example 5.2. Let's look at the minimal polynomial over $\mathbb{Q}$ for the element $\alpha = \sqrt{3} + \sqrt{5}$. Observe first that α is certainly contained in the Galois extension $\mathbb{Q}(\sqrt{3}, \sqrt{5})/\mathbb{Q}$. The Galois group of this extension is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$, as shown above. Since the Galois group permutes the roots of any irreducible polynomial with coefficients in $\mathbb{Q}$, we can quickly compute that the roots of $m_{\alpha,\mathbb{Q}}(x)$ will be $\pm\sqrt{3}\pm\sqrt{5}$. We then compute the minimal polynomial by cleaning up the equation: $[x-(\sqrt{3}+\sqrt{5})][x-(\sqrt{3}-\sqrt{5})][x-(-\sqrt{3}+\sqrt{5})][x-(-\sqrt{3}-\sqrt{5})]$, this will eventually reduce down to $x^4 - 16x^2 + 4$. It can be shown that this is in fact the minimal polynomial for α over $\mathbb{Q}$.

Note that we can also now determine the Galois group for the polynomial $f(x) = x^4 - 16x^2 + 4$ over $\mathbb{Q}$. To do so, we must look at how the Galois group of the larger extension acts on the roots of $f(x)$. In this case it is rather simple, in that one sees that none of the roots are fixed by the Galois group of the larger extension, so that $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, and hence the Galois group of $f(x)$ is the Galois group of our original extension.

As a final remark before moving onto the ending result, we note that the Galois group of a polynomial of degree n is always (isomorphic to) a subgroup of S_n, corresponding to how the Galois group permutes the roots.

6. The Insolvability of the Quintic

Here we begin the push towards the insolvability of the quintic with a discussion of the Galois groups associated with polynomials. In order to make everything proceed as it should, we will define several notions, many of which will be familiar, but it will be beneficial for us to all use the same language. Firstly, we will refer to the **general polynomial**

of degree n as the polynomial $(x-x_1)(x-x_2)\cdots(x-x_n)$ which has roots $x_1, x_2, \ldots, x_n$. We will call a rational function $f(x_1, x_2, \ldots, x_n)$ **symmetric** if it is not changed by any permutation of the variables $x_1, x_2, \ldots, x_n$. Given indeterminates $x_1, x_2, \ldots, x_n$ we will define the **elementary symmetric functions** $s_1, s_2, \ldots, s_n$ as follows:

$$\begin{aligned} s_1 &= x_1 + x_2 + \ldots + x_n \\ s_2 &= x_1x_2 + x_1x_3 + \ldots + x_2x_3 + x_2x_4 + \ldots + x_{n-1}x_n \\ &\vdots \\ s_n &= x_1x_2\ldots. \end{aligned}$$

Perhaps the most important theorem in this section is the following:

Theorem 6.1. *The general polynomial $x^n - s_1x^{n-1} + s_2x^{n-2} + \ldots + (-1)^n s_n$ over the field $F(s_1, s_2, \ldots, s_n)$ is separable with Galois group (isomorphic to) S_n.*

This tells us that if we take a generic polynomial in degree n, its Galois group will be (isomorphic to) S_n. Recalling Cayley's Theorem, which states that every finite group is isomorphic to a subgroup of S_n, together with the Main Theorem of Galois Theory, we obtain:

Corollary 6.2. *Every finite group is isomorphic to the Galois group of some field extension.*

6.1. **Discriminants.** For the sake of being thorough, we will go through the definition of the discriminant and how it is used. However, we will not go into the general solutions for the roots of polynomials in degrees three and four.

Definition 6.3. Given elements $x_1, \ldots, x_n$, we define their **discriminant** to be

$$D = \prod_{i<j}(x_i - x_j)^2.$$

We define the discriminant of a polynomial to be the discriminant of the roots of the polynomial.

Example 6.4. As an explicit example, let us look at the polynomial $f(x) = x^2 - 2x - 15$. The discriminant will be given by $D = (\alpha - \beta)^2$ which we can relate to the elementary symmetric functions so that

$$D = s_1^2 - 4s_2 = (-a)^2 - 4(b) = a^2 - 4b = 4 + 60 = 64,$$

and since $64 \neq 0$ we can further establish that this polynomial is separable.

The usefulness of the discriminant lies in the fact that the Galois group of $f(x) \in F[x]$ is a subgroup of A_n if and only if the discriminant $D \in F$ is the square of an element of F. In other words, this is the case only when $\sqrt{D} \in F$. Now, we will look at the familiar case of polynomials of degree 2.

Given a polynomial, $f(x) = x^2 + ax + b$ with roots α, β, the discriminant is $D = (\alpha - \beta)^2$. Noting that $a = \alpha + \beta$ and $b = \alpha\beta$, we can rewrite the previous equality as $D = a^2 - 4b$. Note that $f(x)$ is separable exactly when $D \neq 0$. By our earlier remarks we know that the Galois group of $f(x)$ is (isomorphic to) a subgroup of S_2, and is a subgroup of A_2 (i.e., trivial) if $D = a^2 - 4b$ is a square in $\mathbb{Q}$, i.e., $\sqrt{a^2 - 4b} \in \mathbb{Q}$. That is all the possibilities for the Galois groups for this polynomial.

Now, we will avoid doing any of the computations of the roots of degree three and four polynomials, but it is worth mentioning several things about them. An analysis similar to the above (i.e., involving the discriminant) can be used to work out all of the possibilities for the Galois group. In those cases, an additional technique is needed, involving a construction known as the **resolvent**. The resolvent of $f(x)$ is a carefully constructed polynomial of one lower degree which has roots related to those of $f(x)$. In particular, knowledge about the resolvent gives information about $f(x)$. In particular, the Galois group of $f(x)$ can be deduced from information about the discriminant and the Galois group of the resolvent. Additionally, the roots of $f(x)$ can be reconstructed from the roots of the resolvent.

Several hundred years ago, it seemed to many that this process (for cubics and quartics) could be extended to handle polynomials of even higher degrees, and that coming up with new tricks would eventually lead to the solutions of the roots of the general quintic polynomial. Much to their consternation, however, none of their tricks panned out. The issue (as one may have guessed at this point) wasn't in a lack of a trick. The issue was in the Galois group related to the fifth degree (and higher) polynomial.

6.2. **Solvability.**

Lastly, we move onto the topic at hand. The insolvability of the quintic. We first need to decide what we mean to "solve" for the roots of a polynomial.

Definition 6.5. We say an element α which is algebraic over F can be **expressed by radicals** if α is an element of a field extension K/F that can be obtained by a succession of simple radical extensions:

$$F = K_0 \subset K_1 \subset \ldots \subset K_i \subset K_{i+1} \subset \ldots \subset K_s = K,$$

where $K_{i+1} = K_i(\sqrt[n_i]{a_i})$ for some $a_i \in K_i$ with $i = 0, 1, \ldots, s-1$. We say a polynomial $f(x) \in F[x]$ can be **solved by radicals** if all its roots can be expressed by radicals.

We have seen this process in action in the case where we looked at the polynomial $f(x) = x^2 - 2$, which gave us the solution $x = \pm\sqrt{2}$.

Observe that, by the fundamental theorem of Galois theory, the chain of subfields above will correspond exactly to a chain of subgroups in the opposite direction. This leads directly to a property of groups called **solvability**.

Definition 6.6. We say a group G is **solvable** if there is a chain of subgroups

$$\{1\} \trianglelefteq N_1 \trianglelefteq N_2 \trianglelefteq \cdots \trianglelefteq N_k = G,$$

which each N_i is normal in N_{i+1}, and each quotient N_{i+1}/N_i is cyclic.

It is perhaps not difficult to believe, then, that the following is true:

Theorem 6.7. *A polynomial can be solved by radicals if and only if its Galois group is a solvable group.*

This theorem is the final nail in the coffin for the solvability of the quintic. Since the equation for a general polynomial of degree n has a corresponding Galois group (isomorphic to) S_n, the general polynomial of degree 5 polynomial has Galois group (isomorphic to) S_5. (Note that a given, explicit quintic polynomial has Galois group (isomorphic to) a subgroup of S_5.) We next note that S_5 is not a solvable group. Indeed, it has only one nontrivial normal subgroup, namely A_5 (the alternating group on five elements). Now, A_5 is a simple, non-cyclic group, so A_5 is not a solvable group. (In fact, A_5 is the smallest non-solvable group.) Since every normal subgroup of a solvable group is solvable, it follows that S_5 is not a solvable group. Thus, the general quinctic polynomial cannot be solved by radicals.

This does not mean that specific fifth degree (or higher) polynomials cannot be solved by radicals. This simply states that there does not exist a general formula (involving only taking roots) for the roots of such a polynomial.

Example 6.8. As a final example, we will look at the polynomial $f(x) = x^5 - x - 1$. This polynomial has no linear factors as given by the Rational Roots Theorem. We will look at this polynomial over $\mathbb{F}_5$ to determine if it is irreducible. One can immediately check it has no roots in $\mathbb{F}_5$, and hence has no linear factors. Now suppose it is reducible, in which case it must have an irreducible quadratic factor, say $g(x)$. Then $\mathbb{F}_5[x]/(g(x)) \cong \mathbb{F}_5(\alpha) \cong \mathbb{F}_{25}$, where α is a root of $g(x)$.

Now, we have $\alpha^5 - \alpha - 1 = 0$. Rewriting, we obtain $\alpha^5 = \alpha + 1$. Recalling that every $z \in \mathbb{F}_{25}$ satisfies $z^{25} = z$, we then have

$$\alpha = \alpha^{25} = (\alpha^5)^5 = (\alpha + 1)^5 = \alpha^5 + 1 = (\alpha + 1) + 1 = \alpha + 2.$$

Thus, $0 = 2$ in $\mathbb{F}_{25}$, a contradiction. So our polynomial is irreducible over $\mathbb{F}_5$, which in turn allows us to conclude that it is irreducible over $\mathbb{Q}$. Lastly, we can verify that this polynomial has three real roots and two complex conjugate roots. The map complex conjugation then permutes the five roots, keeping three fixed and interchanging the two complex roots. This means there is an element in the Galois group that keeps three of the roots fixed and transposes the other two. It follows that the Galois group contains a transposition. It turns out that this is enough to guarantee the Galois group is (isomorphic to) S_5.

7. Conclusion

Through this we have seen how a seemingly simple question, whether or not there is a formula for finding the roots of the general quintic, has brought us to discovering a connection between two previously-unconnected algebraic structures. This connection not only answered the original question, but also gave us insight into abstract algebra in general. Using this connection, we have been able to answer many questions that have plagued mathematicians for hundreds, maybe thousands of years.