Galois Theory and the Insolvability of the Quintic Equation

Daniel Franz

1. Introduction

Polynomial equations and their solutions have long fascinated mathematicians. The solution to the general quadratic polynomial $ax^2 + bx + c = 0$ is the well known quadratic formula:

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

This solution was known by the ancient Greeks and solutions to general cubic and quartic equations were discovered in the 16th century. The important property of all these solutions is that they are solutions "by radicals"; that is, x can be calculated by performing only elementary operations and taking roots. After solutions by radicals were discovered for cubic and quartic equations, it was assumed that such solutions could be found polynomials of degree n for any natural number n. The next obvious step then was to find a solution by radicals to the general fifth degree polynomial, the quintic equation. The answer to this problem continued to elude mathematicians until, in 1824, Niels Abel showed that there existed quintics which did not have a solution by radicals. During the time Abel was working in Norway on this problem, in the early 18th century, Evariste Galois was also investigating solutions to polynomials in France. Galois, who died at the age of 20 in 1832 in a duel, studied the permutations of the roots of a polynomial, and used the structure of this group of permutations to determine when the roots could be solved in terms of radicals; such groups are called solvable groups. In the course of his work, he became the first mathematician to use the word "group" and defined a normal subgroup. His work forms the foundations of what is now known as Galois theory, a theory that bridges field theory and group theory by giving a correspondence between certain subfields of fields and subgroups of permutations.

We will begin by recalling some useful information about algebraic extensions of fields, and then cover some useful definitions and results from field theory. Galois theory will then be explored, culminating in the Fundamental Theorem of Galois theory. Finally we will use this result to prove Galois's result that a polynomial is solvable by radicals if and only if its Galois group is solvable. This will allow us to show that the general quintic equation cannot be solved by radicals.

2. Field Theory

We begin with some review by recalling some definitions and theorems concerning field extensions. This material is covered at the undergraduate level and some results will not be proved here. Rather, the material provides the necessary basic level of knowledge required to discuss Galois Theory.

Let F be a field. A field E is a *field extension* of F if F is a subfield of E. An element α is *algebraic over* F if α is the root of some polynomial $f(x) \in F[x]$. If α is algebraic over F, then the *minimal polynomial of* α is the monic polynomial of minimal degree that has α as a root. A field extension K over F is an *algebraic extension* if every element of K is algebraic over F. We will use the notation E/F to denote that E is a field extension of a field F. This notation is unrelated to quotient groups or rings; it is simply an easy way to refer to E as an extension of F.

The field extensions we are interested in are those created by adjoining algebraic elements to a base field. If F is a field and α is algebraic over F, then $F(\alpha)$ is an algebraic extension over F. Also, $F(\alpha)$ is the smallest field containing F and α. One can adjoin any finite number of elements that are algebraic over F to F to create an algebraic extension. Any extension created this way is an algebraic field extension over F. A proof that $F(\alpha_1, \cdots, \alpha_n)$ is an algebraic extension over F if the α_i are algebraic over F can be found on page 283 of [2].

One of the more interesting and useful aspects of field extensions is that they can be treated as vector spaces over the base field. That is, if E is an extension of a field F, then E is a vector space over F, with the elements of F serving as scalars and the elements of E serving as vectors. A vector space has finite dimension if it has a finite basis. If V is a vector space over F and has finite dimension, then the number of elements in a basis of V is the *dimension of* V *over* F. If E is an extension field over F and has finite dimension n over F as a vector space, then E is a *finite extension over* F and the *degree of* E *over* F is $[E : F] = n$. The following theorem allows us to easily construct a basis of any extension of the form $F(\alpha)$ when α is algebraic over F. A proof of the theorem can be found on page 280 in [2].

Theorem 2.1. *If the degree of the minimal polynomial for* α *is* n*, then a basis of* $F(\alpha)$ *as a vector space over* F *is* $\{1, \alpha, \cdots, \alpha^{n-1}\}$.

The next theorem presents a very useful property concerning degrees of field extensions. The proof closely follows the proof of Theorem 31.4 on pages 283-284 of [2].

Theorem 2.2. *If E/F and K/E are each finite extensions, then $[K : F] = [K : E][E : F]$.*

Proof. Let $B_E = \{\alpha_1 \cdots, \alpha_n\}$ be a basis for E as a vector space over F, and let $B_K\{\beta_1, \cdots, \beta_m\}$ be a basis for K as a vector space over E. We wish to show that the set $B = \{\alpha_i\beta_j : 1 \leq i \leq n, 1 \leq j \leq m\}$ is a basis for K over F, so that $[K : F] = mn = [K : E][E : F]$. We begin by showing that the elements of B span K over F.

Let $\gamma \in K$. Then since B_K is a basis for K over E,

$$\gamma = \sum_{j=1}^{m} b_j\beta_j,$$

where $b_j \in E$ for each j. Since B_E is a basis for E over F, for each b_j

$$b_j = \sum_{i=1}^{n} a_{ij}\alpha_i,$$

where $a_{ij} \in F$ for each i, j. Thus we can write γ as

$$\gamma = \sum_{j=1}^{m} \left(\sum_{i=1}^{n} a_{ij}\alpha_i \right) \beta_j = \sum_{j=1}^{m} \sum_{i=1}^{n} a_{ij}(\alpha_i\beta_j).$$

Therefore any element of K can be written as a linear combination, with coefficients in F, of the elements in the set B, so the elements of B span K over F.

We now show the elements of B are independent. Suppose

$$0 = \sum_{j=1}^{m} \sum_{i=1}^{n} c_{ij}(\alpha_i\beta_j) = \sum_{j=1}^{m} \left(\sum_{i=1}^{n} c_{ij}\alpha_i \right) \beta_j$$

for some elements $c_{ij} \in F$. Notice that for each j, $\sum_{i=1}^{n} c_{ij}\alpha_i \in E$. Since the elements of B_K are independent over E, we must have

$$\sum_{i=1}^{n} c_{ij}\alpha_i = 0$$

for each j. But the elements of B_E are independent over F, so $c_{ij} = 0$ for each i and j. Therefore the elements of B are independent over F, so they form a basis for K over F, proving the theorem. □

Notice that the proof of the theorem above gives us an easy way to find a basis for K over F if we know the bases of K over E and E over F. If $\{\alpha_1, \cdots, \alpha_n\}$ is a basis for K over E and $\{\beta_1, \cdots, \beta_m\}$ is a basis for E over F, then $\{\alpha_i\beta_j : 1 \leq i \leq n, 1 \leq j \leq m\}$ is a basis for K over F. This is very convenient and, when paired with Theorem 2.1

allows us to construct a basis for any finite extension. To see this, let F be a field and consider a finite extension $E = F(\alpha_1, \cdots, \alpha_n)$. We can create E by first adjoining α_1 to F to form $F(\alpha_1)$, and then adjoining α_2 to form $F(\alpha_1)(\alpha_2) = F(\alpha_1, \alpha_2)$, and repeating this process until we reach $F(\alpha_1, \cdots, \alpha_n)$. Theorem 2.1 gives us bases for $F(\alpha_1)$ over F and $F(\alpha_1, \alpha_2)$ over $F(\alpha_1)$, and the proof of Theorem 2.2 gives us a way to construct a basis for $F(\alpha_1, \alpha_2)$ over F. Continuing in this fashion, we can construct a basis for E over F which will be the set of pairwise products of all the basis elements for the individual extensions. This is a very useful result and will be used to construct bases of finite extensions when necessary.

We cite the following theorem without proof, and use it and the results cited or proved before this as our foundation for exploring Galois Theory. The proof can be found on page 519 in [1].

Theorem 2.3. *Let $\phi : F \to F'$ be a field isomorphism. Let $p(x) \in F[x]$ be an irreducible polynomial, and let $p'(x) \in F'[x]$ be the irreducible polynomial obtained by applying ϕ to the coefficients of $p(x)$. Let α be a root of $p(x)$ and let β be a root of $p'(x)$. Then there is an isomorphism $\sigma : F(\alpha) \to F(\beta)$ such that $\sigma(\alpha) = \beta$ and σ restricted to F is ϕ. Thus σ can be viewed as an extension of ϕ.*

Suppose the minimal polynomial of α is $h(x) \in F[x]$. By definition $F(\alpha)$ contains α, but it is not guaranteed to contain the other roots of $h(x)$. For example, suppose $\alpha = \sqrt[3]{2}$. Then $h(x) = x^3 - 2 \in \mathbb{Q}[x]$. Letting $\omega = (-1+\sqrt{-3})/2$,a primitive third root of unity, the other two roots of $h(x)$ are $\omega\sqrt[3]{2}$ and $\omega^2\sqrt[3]{2}$, neither of which are in $\mathbb{Q}(\alpha)$, since they are complex. However, the extension $\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$ does contain all the roots of $h(x)$, since it contains $\sqrt{-3}$ in addition to $\sqrt[3]{2}$. As we will show later, no proper subfield of $\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$ contains all the roots of $h(x)$. Fields with this property are of great importance in Galois theory and are called splitting fields, which we now define. An extension field E of a field F is a *splitting field* of some polynomial $f(x) \in F[x]$ if $f(x)$ factors completely into linear factors in E and does not factor completely in any proper subfield of E. When this is the case, we say that $f(x)$ splits completely in E. A splitting field E of $f(x)$ is minimal in the sense that E is a subfield of every field containing F and all the roots of $f(x)$. We now show that there exists a splitting field for every $f(x) \in F[x]$.

Theorem 2.4. *Let F be a field. If $f(x) \in F[x]$, then there exists an extension K of F which is a splitting field for $f(x)$.*

Proof. We proceed by induction on the degree n of $f(x)$ to show that there exists an extension field E containing all the roots of $f(x)$. If $n = 1$, then clearly $E = F$ since $f(x)$ is a linear polynomial in this case. Now assume that for any polynomial $f(x)$ of degree $k-1$, there exists an extension E of F containing all the roots of $f(x)$. Let $f(x) \in F[x]$ have degree k. If all the irreducible factors of $f(x)$ have degree 1, then $E = F$. Otherwise, at least one irreducible factor $p(x)$ has degree at least 2. Let α be a root of $p(x)$. Then $E_1 = F(\alpha)$ contains α, so $f(x)$ factors as $(x-\alpha)f_1(x)$ in E_1, where $f_1(x)$ is degree $k-1$. Then by the inductive hypothesis, there exists an extension E of E_1 in which $f_1(x)$ factors completely. Thus E contains all the roots of $f(x)$.

Now let K be the intersection of all subfields of E containing F and the roots of $f(x)$ and note that $K \leq E$. We show that K is a splitting field of $f(x)$ over $F[x]$. Clearly K contains F and all the roots of $f(x)$, so K is a field extension of F and $f(x)$ factors completely in to linear factors in K. We now show that the only subfield of K that contains F and all the roots of $f(x)$ is K. Let $K_1 \leq K$ such that K_1 contains F and all the roots of F and let $k \in K$. Then by definition of K, k is in every subfield of E that contains F and the roots of $f(x)$. Since $K_1 \leq K \leq E$, K_1 is a subfield of E that contains F and all the roots of $f(x)$, so $k \in K_1$. Thus $K \subset K_1$, so $K = K_1$. Thus no proper subfield of K contains F and the roots of $f(x)$, so K is a splitting field for $f(x)$. □

This shows that every $f(x) \in F[x]$ has a splitting field, but could $f(x)$ have multiple non-isomorphic splitting fields? The following result on extending isomorphisms will help show that splitting fields of a polynomial are unique up to isomorphism, so that we can speak of the splitting field of $f(x)$.

Theorem 2.5. *Let $\phi : F \to F'$ be a field isomorphism. Let $f(x) \in F[x]$ be a polynomial and let $f'(x) \in F'[x]$ be obtained by applying ϕ to the coefficients of $f(x)$. Let E be a splitting field for $f(x)$ over F and let E' be a splitting field for $f'(x)$ over F'. Then ϕ extends to an isomorphism $\sigma : E \to E'$, so that σ restricted to F is ϕ.*

Proof. We again proceed by induction on the degree n of $f(x)$. If $n = 1$, then $E = F$ and $E' = F'$, so $\sigma = \phi$. Now assume the theorem holds for $n = k-1$. Let $f(x) \in F[x]$ have degree k. If $f(x)$ splits completely in F, then again $E = F$ and $E' = F'$, giving $\sigma = \phi$, so assume the contrary. Then $f(x)$ has some irreducible factor $p(x)$ with degree at least 2, which ϕ maps to an irreducible factor $p'(x)$ of $f'(x)$. Let $\alpha \in E$ be a root of $p(x)$ and $\beta \in E'$ be a root of $p'(x)$. Then by Theorem 2.3,

ϕ extends to an isomorphism $\phi' : F(\alpha) \to F'(\beta)$ in which $\phi'(\alpha) = \beta$. In $F(\alpha)$, $f(x)$ factors as $f(x) = (x - \alpha)f_1(x)$, and in $F'(\beta)$, $f'(x)$ factors as $f'(x) = (x - \beta)f_1'(x)$, where $f_1(x), f_1'(x)$ have degree $k - 1$.

We now show that E is a splitting field for $f_1(x)$ over $F(\alpha)$. Since E is a splitting field for $f(x)$ over F, E contains all the roots of $f(x)$, so E contains all the roots of $f_1(x)$. If any proper subfield of E contains $F(\alpha)$ and the roots of $f_1(x)$, then it contains F and all the roots of $f(x)$, since $F(\alpha)$ contains F and α. But E is a splitting field for $f(x)$ over F, so no proper subfield of E contains F and all the roots of $f(x)$. Hence no proper subfield of E contains $F(\alpha)$ and the roots of $f_1(x)$. Thus E is a splitting field for $f_1(x)$ over $F(\alpha)$. A similar argument shows that E' is a splitting field for $f_1'(x)$ over $F'(\beta)$. We can now apply the induction hypothesis to extend ϕ_1 to an isomorphism $\sigma : E \to E'$. Since ϕ_1 itself is an extension of ϕ, we see that σ is an extension of ϕ, as the diagram below shows.

$$\begin{array}{ccccc} \sigma: & E & \longrightarrow & E' \\ & | & & | \\ \phi': & F(\alpha) & \longrightarrow & F'(\beta) \\ & | & & | \\ \phi: & F & \longrightarrow & F' \end{array}$$

□

The uniqueness of splitting fields follows easily. Let $F = F'$ and take ϕ as the identity isomorphism. Then if E and E' are two splitting fields for some $f(x) \in F[x]$, E and E' are isomorphic by the theorem just proved.

We now construct some splitting fields. We said before that the splitting field for $f(x) = x^3 - 2$ is $\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$; we now show this is true. Recall that $\omega = (-1 + \sqrt{-3})/2$ is a primitive third root of unity and that the roots of $x^3 - 2$ are $\sqrt[3]{2}, \omega\sqrt[3]{2}$, and $\omega^2\sqrt[3]{2}$. The splitting field K for $f(x)$ contains all three roots and thus contains ω, the quotient of the first two roots. Thus K contains $\sqrt{-3}$. Since $\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$ is the smallest extension of $\mathbb{Q}$ containing $\sqrt[3]{2}$ and $\sqrt{-3}$, we see that $K = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$.

The splitting field of $x^2 - 2$ is just $\mathbb{Q}(\sqrt{2})$, since the roots of $x^2 - 2$ are $\sqrt{2}$ and $-\sqrt{2}$. Note that by Theorem 2.2, $[\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3}) : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3 \cdot 2 = 6$ and $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, so in each case the degree of the splitting field for a polynomial of degree n over $\mathbb{Q}$ was $n!$. This is in fact the maximum possible degree. If we have $f(x) \in F[x]$ with degree n, then we can adjoin one root of $f(x)$ at a time and obtain the splitting field after adjoining all n roots. If

F_1 is the first extension constructed this way, then $[F_1 : F] \leq n$. Over F_1, $f(x)$ now has at least one linear factor, so the next root adjoined is from a polynomial of degree $n-1$, so if F_2 is this next extension, $[F_2 : F_1] \leq n-1$, so that $[F_2 : F] \leq n(n-1)$. Continuing in this fashion, we see that $[F_n : F] \leq n!$.

This bound is not always achieved, however. Consider $f(x) = x^4 + 4 \in \mathbb{Q}[x]$. Then $f(x)$ is not irreducible, as it factors to $f(x) = (x^2 + 2x + 2)(x^2 - 2x + 2)$. These factors are irreducible, and the four roots of $f(x)$ are $\pm 1 \pm i$. Hence the splitting field for $f(x)$ is $\mathbb{Q}(i)$, and since i is a root of $x^2 - 1$, $\mathbb{Q}(i)$ is of degree 2 over $\mathbb{Q}$, considerably less than $4! = 24$.

As another example, consider $f(x) = (x^2-3)(x^2-5) \in \mathbb{Q}[x]$. Clearly $f(x)$ has roots $\pm\sqrt{3}, \pm\sqrt{5}$, so the splitting field is $\mathbb{Q}(\sqrt{3}, \sqrt{5})$, which has degree 4 over $\mathbb{Q}$. We have exhibited two degree 4 polynomials over $\mathbb{Q}$ which have splitting fields with different degrees over $\mathbb{Q}$, each less than 4!, so care must be taken when determining the splitting field of a polynomial.

We now make two more definitions before moving on to Galois Theory. Let $f(x) \in F[x]$ and let E be the splitting field of $f(x)$. Then $f(x)$ is *separable* if it has distinct roots in E, so that viewed as an element in $E[x]$, $f(x)$ can be written as a product of distinct linear factors. A field K is *separable over* F if every element $k \in K$ is the root of a separable polynomial over F. Since every $k \in K$ is a root of its minimal polynomial in $F[x]$, an equivalent definition is that K is separable over F if the minimal polynomial of every $k \in K$ is separable. Note that the base field of a polynomial $f(x)$ is unimportant when determining if it is separable, since it is the roots of $f(x)$ in the splitting field E of $f(x)$ that determine whether or not $f(x)$ is separable.

The polynomial $x^4+4 \in \mathbb{Q}[x]$ is separable because as shown above, it has roots $\pm 1 \pm i$ in $\mathbb{Q}(i)$. The polynomial $x^2 - 4x + 4 = (x-2)^2 \in \mathbb{Q}[x]$ is not separable because it has only one distinct root, $x = 2$.

Splitting fields and separable field extensions are very important in Galois Theory. Splitting fields are nice because they allow us to work in a field that contains all the roots of a polynomial, and if the splitting field is separable, all these roots are distinct. As we will see in the next section, this gives the optimal situation for permutations of roots of a polynomial, which is of great interest in Galois Theory.

3. Galois Theory

In this section we introduce the concepts of Galois Theory and prove results that lead up to the Fundamental Theorem of Galois Theory, which will be proved in the next section.

We begin with some definitions. An *automorphism* of a field K is an isomorphism of K with itself. The theorem below shows that the set of automorphisms of a field K is a group under function composition; we call this group the "automorphism group of K" and denote it by $\mathrm{Aut}(K)$. An automorphism σ *fixes* an element $k \in K$ if $\sigma(k) = k$. If $F \subset K$ and $\sigma(a) = a$ for all $a \in F$, then σ *fixes* F. If K is an extension of F, then $\mathrm{Aut}(K/F)$ is the set of automorphisms of K that fix F. The theorem below shows that $\mathrm{Aut}(K/F)$ is in fact a group.

Theorem 3.1. *Let K be a field, let $F \subset K$, and let $\mathrm{Aut}(K)$ be the set of automorphisms of K. Then $\mathrm{Aut}(K)$ is a group under function composition and $\mathrm{Aut}(K/F)$ is a subgroup of $\mathrm{Aut}(K)$.*

Proof. Clearly the identity function is an automorphism, so $1 \in \mathrm{Aut}(K)$. If $\sigma \in \mathrm{Aut}(K)$, then since σ is an automorphism, σ^{-1} exists and is also an automorphism, so $\sigma^{-1} \in \mathrm{Aut}(K)$. Since function composition is associative, $\mathrm{Aut}(K)$ is a group.

To show $\mathrm{Aut}(K/F)$ is a subgroup of $\mathrm{Aut}(K)$, note that since 1 fixes all of K, in particular it fixes F, so $1 \in \mathrm{Aut}(K/F)$. If $\sigma, \tau \in \mathrm{Aut}(K/F)$ then since they each fix F, the composition $\sigma\tau$ also fixes F, so $\sigma\tau \in \mathrm{Aut}(K/F)$. Finally, if σ fixes F then σ^{-1} also fixes F so $\sigma^{-1} \in \mathrm{Aut}(K/F)$. Hence $\mathrm{Aut}(K/F)$ is a subgroup of $\mathrm{Aut}(K)$. □

Let E be the splitting field of some $f(x) \in F[x]$ and let $\phi : F \to F$ be the identity map. Then the isomorphism $\sigma : E \to E$ which extends ϕ that is guaranteed to exist by Theorem 2.5 is an automorphism of E which fixes F, so $\sigma \in \mathrm{Aut}(E/F)$. The action of σ on E is defined by its action on roots of irreducible factors of $f(x)$. As we show below, if $p(x)$ is an irreducible factor of $f(x)$, σ permutes the roots of $p(x)$ and can thus be viewed as a permutation of the roots of $p(x)$. This is an important property of elements of $\mathrm{Aut}(E/F)$, in fact of elements of $\mathrm{Aut}(K/F)$ for any extension K/F, and we make this statement precise in the following theorem.

Theorem 3.2. *Let K be an extension of a field F, let $\sigma \in \mathrm{Aut}(K/F)$, and let $\alpha \in K$ be algebraic over F. Then any polynomial in $F[x]$ having α as a root also has $\sigma(\alpha)$ as a root.*

Proof. Suppose α is a root of $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in F[x]$, so that $f(\alpha) = 0$. Then since σ is a field isomorphism,

$$\sigma(f(\alpha)) = \sigma(a_n)\sigma(\alpha)^n + \cdots + \sigma(a_1)\sigma(\alpha) + \sigma(a_0) = \sigma(0) = 0.$$

But σ fixes F, so $\sigma(a_i) = a_i$ for $0 \leq i \leq n$. Thus

$$a_n\sigma(\alpha)^n + \cdots a_1\sigma(\alpha) + a_0 = 0,$$

so $f(\sigma(\alpha)) = 0$, and thus $\sigma(\alpha)$ is a root of $f(x)$. □

By this theorem and the comments preceding it we see that any $\sigma \in \mathrm{Aut}(K/F)$ can be associated with a permutation of the roots of some polynomial in $F[x]$. Note that this was only possible because σ fixed F. This is one of the key observations of Galois Theory. What we have done is associated a group, $\mathrm{Aut}(K/F)$, with the subfield F of K. Just as the subfield F gave rise to $\mathrm{Aut}(K/F)$, a subgroup of $\mathrm{Aut}(K)$ can give rise to a subfield of K, as shown in the theorem below.

Theorem 3.3. *Let H be a subgroup of $\mathrm{Aut}(K)$ and let F be the subset of K fixed by H. Then F is a subfield of K.*

Proof. Let H be a subgroup of $\mathrm{Aut}(K)$ and let F be the subset of K fixed by H. Let $\sigma \in H$ and $a, b \in F$. Then $\sigma(a) = a$ and $\sigma(b) = b$, so $\sigma(a \pm b) = \sigma(a) \pm \sigma(b) = a \pm b$, $\sigma(ab) = \sigma(a)\sigma(b) = ab$ and $\sigma(a^{-1}) = a^{-1}$, where we are using the fact that σ is a field automorphism and thus both addition and multiplication preserving. Thus $a \pm b, ab, a^{-1} \in F$ since they are fixed by σ, so F is closed under addition and multiplication and contains multiplicative inverses. Also, every automorphism must fix 1, so $1 \in F$. Hence F is a subfield of K. □

Let K be a field and let $H \subset \mathrm{Aut}(K)$. By Theorem 3.3 the subset of K fixed by H is a field. We denote this field by K_H and call it the *fixed field of H*.

The diagrams below illustration the relationship between subgroups of $\mathrm{Aut}(K/F)$ and the fixed fields of these subgroups.

$$\begin{array}{ccc} K & \longrightarrow & \mathrm{Aut}(K) \\ \cup| & & \vee| \\ F & \longrightarrow & \mathrm{Aut}(K/F) \end{array} \qquad \begin{array}{ccc} K & \longleftarrow & \mathrm{Aut}(K) \\ \cup| & & \vee| \\ K_H & \longleftarrow & H \end{array}$$

This association between subgroups of $\mathrm{Aut}(K/F)$ and the their fixed fields is inclusion reversing, as the following theorem shows.

Theorem 3.4. *If $F_1 \subset F_2$ are both subfields of K, then $\mathrm{Aut}(K/F_2) \leq \mathrm{Aut}(K/F_1)$. If $H_1 \leq H_2 \leq \mathrm{Aut}(K)$, then $K_{H_2} \subseteq K_{H_1}$.*

Proof. Assume $F_1 \subset F_2$ and that F_1, F_2 are subfields of K. Let $\sigma \in \mathrm{Aut}(K/F_2)$. Then σ fixes F_2, so since $F_1 \subseteq F_2$, σ fixes F_1, so $\sigma \in \mathrm{Aut}(K/F_1)$. Hence $\mathrm{Aut}(K/F_2) \leq \mathrm{Aut}(K/F_1)$.

Now Assume $H_1 \leq H_2 \leq \mathrm{Aut}(K)$ and let $a \in K_{H_2}$. Then a is fixed by every element of H_2, so since $H_1 \leq H_2$, a is fixed by every element of H_1. Hence $a \in K_{H_1}$, so $K_{H_2} \subseteq K_{H_1}$. □

The diagrams below illustrate Theorem 3.4.

$$\begin{array}{ccccc} F_2 & \longrightarrow & \mathrm{Aut}(K/F_2) & K_{H_2} & \longleftarrow & H_2 \\ \cup| & & \wedge| & \cap| & & \vee| \\ F_1 & \longrightarrow & \mathrm{Aut}(K/F_1) & K_{H_1} & \longleftarrow & H_1 \end{array}$$

We now examine some examples of the interactions between subgroups of $\mathrm{Aut}(K)$ and their fixed fields F. We first give an example of finding $\mathrm{Aut}(K/F)$ given a fixed field F. Let $K = \mathbb{Q}(\sqrt{3}, \sqrt{5})$, which as we saw before is the splitting field of $(x^2-3)(x^2-5)$ over $F = \mathbb{Q}$. The elements of $\mathrm{Aut}(K/F)$ are completely determined by their actions on the basis elements of K, which in this case are $\sqrt{3}$ and $\sqrt{5}$. Define σ by $\sigma(\sqrt{3}) = \sqrt{3}$ and $\sigma(\sqrt{5}) = -\sqrt{5}$, and define τ by $\tau(\sqrt{3}) = -\sqrt{3}$ and $\tau(\sqrt{5}) = \sqrt{5}$. Then $\sigma, \tau \in \mathrm{Aut}(K/F)$ and $\sigma^2 = \tau^2 = 1$. Also, $\sigma\tau = \tau\sigma$, since each maps the two basis elements to their negatives. Note that an automorphism θ of K that mapped $\sqrt{3}$ to $\sqrt{5}$ and vice versa would not be in $\mathrm{Aut}(K/F)$ because $\theta(3) = \theta(\sqrt{3})^2 = 5$, so that θ does not fix F. We could also have used Theorem 3.2, which would have denied θ membership in $\mathrm{Aut}(K/F)$ because it mapped $\sqrt{3}$ to a root of a different minimal polynomial. Since any element of $\mathrm{Aut}(K/F)$ permutes the roots of each minimal polynomial, the elements we have found so far comprise the whole group, so we have $\mathrm{Aut}(K/F) = \{1, \sigma, \tau, \sigma\tau\}$, which is isomorphic to the Klein-4 group since the square of each element is the identity. Note that $|\mathrm{Aut}(K/F)| = [K : F] = 4$.

As discussed above, one can also start with a subgroup H of $\mathrm{Aut}(K)$ and find the fixed field K_H. Suppose $K = \mathbb{Q}(\sqrt[3]{2})$. The minimal polynomial of $\sqrt[3]{2}$ is $x^3 - 2$. The other two roots of $x^3 - 2$ are complex and thus not in K. Hence the only element of $\mathrm{Aut}(K)$ is the identity isomorphism. Thus $\mathrm{Aut}(K/\mathbb{Q}) = \mathrm{Aut}(K)$, so the fixed field of $\mathrm{Aut}(K/\mathbb{Q})$ is in fact the entire field K, not $\mathbb{Q}$. Note that the reason K is the fixed field of $\mathrm{Aut}(K/\mathbb{Q})$ is that $\mathrm{Aut}(K)$ does not contain enough automorphisms. This in turn is due to the fact that K only contains one root of $x^3 - 2$.

Now let $K = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$, the splitting field of $x^3 - 2$. Then K contains all three roots of $x^3 - 2$, so $\mathrm{Aut}(K)$ contains more than the identity automorphism. Specifically, $\mathrm{Aut}(K)$ contains the automorphism σ defined by $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$ and $\sigma(\sqrt{-3}) = -\sqrt{-3}$. Note that σ maps $\sqrt{-3}$

to a root of its irreducible polynomial x^2+3 and σ maps $\sqrt[3]{2}$ to a root of its irreducible polynomial x^3-2. Also notice that $\sigma^2=1$. Then $H=\langle\sigma\rangle=\{1,\sigma\}$ is a subgroup of $\mathrm{Aut}(K)$. Every element in K can be written uniquely in the form $a+b\sqrt[3]{2}+c\sqrt[3]{4}+d\sqrt{-3}+e\sqrt[3]{2}\sqrt{-3}+f\sqrt[3]{4}\sqrt{-3}$, by the comments following Theorem 2.2. Thus, elements in K_H satisfy $\sigma(a+b\sqrt[3]{2}+c\sqrt[3]{4}+d\sqrt{-3}+e\sqrt[3]{2}\sqrt{-3}+f\sqrt[3]{4}\sqrt{-3})=a+b\sqrt[3]{2}+c\sqrt[3]{4}+d\sqrt{-3}+e\sqrt[3]{2}\sqrt{-3}+f\sqrt[3]{4}\sqrt{-3}$, so that $a+b\sqrt[3]{2}+c\sqrt[3]{4}+d\sqrt{-3}+e\sqrt[3]{2}\sqrt{-3}+f\sqrt[3]{4}\sqrt{-3}=a+b\sqrt[3]{2}+c\sqrt[3]{4}-d\sqrt{-3}-e\sqrt[3]{2}\sqrt{-3}-f\sqrt[3]{4}\sqrt{-3}$. Thus we have $d=e=f=0$, so the elements of K that are fixed by σ are exactly the elements of the form $a+b\sqrt[3]{2}+\sqrt[3]{4}$. This is the field $\mathbb{Q}(\sqrt[3]{2})$, so $K_H=\mathbb{Q}(\sqrt[3]{2})$.

Note that another element of $\mathrm{Aut}(K)$ is τ, defined by $\tau(\sqrt[3]{2})=\omega\sqrt[3]{2}$ and $\tau(\sqrt{-3})=\sqrt{-3}$. Then $H'=\langle 1,\tau,\tau^2\rangle$ is another subgroup of $\mathrm{Aut}(K)$. It is clear that the fixed field of H' is $\mathbb{Q}(\sqrt{-3})$. We can now compute $\mathrm{Aut}(K/\mathbb{Q})$. Notice that $\sigma(\omega)=\omega^2$ since $\sigma(\sqrt{-3})=-\sqrt{-3}$, so $\sigma\tau(\sqrt[3]{2})=\sigma(\omega\sqrt[3]{2})=\omega^2\sqrt[3]{2}$. Also, $\sigma\tau(\sqrt{-3})=\sigma(\sqrt{-3})=-\sqrt{-3}$. Similar computations show that $\tau\sigma(\sqrt[3]{2})=\omega\sqrt[3]{2}$ and $\tau\sigma(\sqrt{-3})=-\sqrt{-3}$. We now have six distinct automorphisms: $1,\sigma,\tau,\tau^2,\sigma\tau,\tau\sigma$. We will show shortly that because K is a splitting field of a separable polynomial in $\mathbb{Q}$, $|\mathrm{Aut}(K/\mathbb{Q})|=[K:\mathbb{Q}]=6$, so $\mathrm{Aut}(K/\mathbb{Q})=\{1,\sigma,\tau,\tau^2,\sigma\tau,\tau\sigma\}$. We can now see that $\mathrm{Aut}(K/\,\mathbb{Q}\,(\sqrt[3]{2}))=H$ and $\mathrm{Aut}(K/\,\mathbb{Q}\,(\sqrt{-3}))=H'$, so that in these two cases, the fixed field of $\mathrm{Aut}(K/F)$ is in fact F.

The next theorem will be used to show that splitting fields of separable polynomials in F give the maximum number of automorphisms that fix F.

Theorem 3.5. *Let F be a field and let E be the splitting field of some separable polynomial $f(x)\in F[x]$. Let $\phi:F\to F'$ be a field isomorphism that maps $f(x)$ to $f'(x)\in F'[x]$ with splitting field E'. Then ϕ can be extended to an isomorphism $\sigma:E\to E'$ in exactly $[E:F]$ ways.*

Proof. Proceed by induction on the degree n of $f(x)$. If $n=1$, then $E=F$ so $\phi=\sigma$. Thus there is $1=[E:F]$ way to extend ϕ. Now assume the theorem holds for polynomials with degree $n-1$ and assume $f(x)$ has degree n. Clearly if $f(x)$ splits completely in F, $E=F$ and there is only one way to extend ϕ. So assume that $f(x)$ has some irreducible factor $p(x)$ with a root α that is not in F. Then $p(x)$ is mapped to $p'\in F'[x]$ which is a factor of $f'(x)$ and has a root β that is not in F. By Theorem 2.5, ϕ extends to an isomorphism $\sigma:E\to E'$. This isomorphism restricted to $F(\alpha)$ is $\theta:F(\alpha)\to F'(\beta)$, whose action is defined by $\theta(\alpha)=\beta$. Now, α can be mapped to any

root of $p'(x)$ and still maintain θ as an isomorphism. Since $f(x)$ is separable, it has distinct roots, so $p(x)$ has distinct roots, as does its image $p'(x)$. Thus there are $[F'(\beta) : F'] = [F(\alpha) : F]$ choices for $\theta(\alpha)$, and thus $[F(\alpha) : F]$ possible isomorphisms θ. Over $F(\alpha)$, $f(x)$ factors as $f = (x - \alpha)g$, where $g(x)$ has degree $n - 1$. Since E is the splitting field of $g(x)$ as well, we can apply the induction hypothesis and see that θ can be extended to σ in $[E : F(\alpha)]$ ways. Therefore there are $[E : F(\alpha)][F(\alpha) : F] = [E : F]$ ways to extend ϕ to an isomorphism $\sigma : E \to E'$. □

Letting F be a field and applying Theorem 3.5 with ϕ as the identity automorphism and $E = E'$ as the splitting field of some separable $f(x) \in F[x]$, we see that $|\mathrm{Aut}(E/F)| = [E : F]$, since every extension of ϕ is an automorphism of E that fixes F. Note that we obtain $|\mathrm{Aut}(E/F)| = [E : F]$ because $f(x)$ was separable over E; if $f(x)$ is not separable then $|\mathrm{Aut}(E/F)| < [E : F]$. The case where $|\mathrm{Aut}(E/F)| = [E : F]$ is of primary interest in Galois Theory, and thus merits the following definition.

A finite extension K/F is a *Galois extension* and K is *Galois over* F if $|\mathrm{Aut}(K/F)| = [K : F]$. Using this definition, every splitting field of a separable polynomial in $F[x]$ is Galois over F. When K is Galois over F we denote $\mathrm{Aut}(K/F)$ by $\mathrm{Gal}(K/F)$. We can also discuss the Galois group of a separable polynomial. The Galois group of a separable polynomial is simply the Galois group of its splitting field, which is guaranteed to be Galois over the base field of the polynomial by the above comments.

There are several equivalent ways of defining Galois extensions, and they are presented in the next theorem. The fourth property was used as our definition, and we have already seen that splitting fields over separable polynomials satisfy this. The other two properties help give a nice sense as to the properties of a Galois extension.

Theorem 3.6. *Let K/F be a finite extension. The following properties are equivalent.*

(1) *K is the splitting field over F of a separable polynomial.*

(2) *The fixed field of $Aut(K/F)$ is F.*

(3) *Every irreducible polynomial in $F[x]$ with a root in K is separable and splits completely in K.*

(4) $[K : F] = |\mathrm{Aut}(K/F)|$.

Proof. We first prove (1) implies (4) and (2). Let K be the splitting field over F of some separable polynomial $f(x) \in F[x]$. Then $[K : F] = |\mathrm{Aut}(K/F)|$ by the discussion following Theorem 3.5, so we have (1) implies (4). Let F' be the fixed field of $\mathrm{Aut}(K/F)$. Then K is the splitting field of $f(x)$ over F' as well, since clearly $F \subseteq F'$. Thus $[K : F'] = |\mathrm{Aut}(K/F')|$. Note that since $\mathrm{Aut}(K/F)$ fixes F', $\mathrm{Aut}(K/F) \subseteq \mathrm{Aut}(K/F')$. Also, because $F \subseteq F'$, $Aut(K/F') \subseteq Aut(K/F)$ by Theorem 3.4. Thus $\mathrm{Aut}(K/F) = \mathrm{Aut}(K/F')$, so $[K : F] = [K : F']$, and since $[K : F] = [K : F'][F' : F]$ by Theorem 2.2, $[F' : F] = 1$, so $F' = F$. Thus F is the fixed field of $\mathrm{Aut}(K/F)$.

To prove (2) implies (3), assume that the fixed field of $\mathrm{Aut}(K/F)$ is F, so that any $u \in K \setminus F$ is moved by some element of $\mathrm{Aut}(K/F)$. Let $u \in K \setminus F$ and let $f(x)$ be the minimal polynomial of u. Then the image of u under the elements of $\mathrm{Aut}(K/F)$ are also roots of $f(x)$. Let $u_1 = u, u_2, \cdots, u_m$ be the distinct images of u by the elements of $\mathrm{Aut}(K/F)$. Then the polynomial $g(x) = (x - u_1) \cdots (x - u_m)$ remains fixed under the mapping of any $\sigma \in \mathrm{Aut}(K/F)$, since each σ just permutes the u_i's. Since the fixed field of $\mathrm{Aut}(K/F)$ is F, only elements of F are fixed by every $\sigma \in \mathrm{Aut}(K/F)$. Thus, since $g(x)$ is fixed by all $\sigma \in \mathrm{Aut}(K/F)$, all the coefficients of $g(x)$ must be in F, so $g(x) \in F[x]$. Also, since each u_i is distinct, $g(x)$ is separable. Since u is a root of $g(x)$, $g(x)$ is a multiple of $f(x)$, the minimal polynomial of u, so $f(x)$ is separable and splits completely in K.

We now show that (3) implies (1). Assume (3) is true. Then since K/F is a finite extension, $K = F(\alpha_1, \cdots, \alpha_n)$ for some $\alpha_1, \cdots, \alpha_n \in K$. Let $f_i(x) \in F[x]$ be the minimal polynomial of α_i in F. By (3), each $f_i(x)$ is separable and splits completely in K, so $f(x) = f_1(x)f_2(x) \cdots f_n(x)$ splits completely in K and is separable if the $f_i(x)$'s are distinct. If they are not, let $g(x)$ be $f(x)$ with any common factors removed, so that $g(x)$ is separable over K. Since $f(x)$ splits completely in K, K contains the roots of each $f_i(x)$, so K contains all the roots of $g(x)$, so that $g(x)$ splits completely in K. Now suppose that some subfield E of K contains F and all the roots of $g(x)$. Then E contains $\alpha_1, \cdots, \alpha_n$, so $F(\alpha_1, \cdots, \alpha_n) \subset E$. Thus $K \subset E$, so $E = K$. Hence no proper subfield of K contains all the roots of $g(x)$, so K is the splitting field of $g(x)$ over F. Hence K is the splitting field over F of a separable polynomial.

We have now shown that (1), (2), and (3) are equivalent and that (1) implies (4). All that remains to be shown is that (4) implies (1). Assume $[K : F] = |\mathrm{Aut}(K/F)|$. Let F' be the fixed field of $\mathrm{Aut}(K/F)$. Then as shown in the proof that (1) implies (2), $\mathrm{Aut}(K/F) = \mathrm{Aut}(K/F')$ and thus F' is the fixed field of $\mathrm{Aut}(K/F')$. Since (2) implies (1), K is

the splitting field over F' of some separable polynomial $f(x) \in F'[x]$. Since we have already shown that (1) implies (4), we have $[K : F'] = |\mathrm{Aut}(K/F')|$. But $|\mathrm{Aut}(K/F)| = |\mathrm{Aut}(K/F')|$, so $[K : F'] = [K : F]$. By Theorem 2.2, $[K : F] = [K : F'][F' : F]$, so $[F' : F] = 1$. Since $F \subseteq F'$, $F = F'$. Hence F is the fixed field of $\mathrm{Aut}(K/F)$. We have already shown that (2) implies (1), so K is the splitting field over F of a separable polynomial, completing the proof. □

The next theorem shows that if H is a subgroup of $\mathrm{Aut}(K)$, then K/K_H is always a Galois extension. This theorem will also be helpful in proving the Fundamental Theorem in the next section.

Theorem 3.7. *Let K be a field extension of F, and let $H = \{\sigma_1 = 1, \sigma_2, \cdots, \sigma_n\}$ be a subgroup of $\mathrm{Aut}(K)$, with $|H| = n$, and let $F = K_H$. Then $[K : F] = |H| = n$.*

Proof. We first show that $[K : F] \leq n$. Suppose $[K : F] > n$. Then there are $n + 1$ elements of K that are linearly independent over F, denoted $\alpha_1, \cdots, \alpha_{n+1}$. Consider the system of equations

$$\begin{aligned} \sigma_1(\alpha_1)x_1 + \sigma_1(\alpha_2)x_2 + \cdots + \sigma_1(\alpha_{n+1})x_{n+1} &= 0 \\ &\vdots \\ \sigma_n(\alpha_1)x_1 + \sigma_n(\alpha_2)x_2 + \cdots + \sigma_n(\alpha_{n+1})x_{n+1} &= 0 \end{aligned}$$

This is a system of n equations in $n + 1$ unknowns, so some nontrivial solution exists. Since σ_1 is the identity automorphism, the first equation is

$$\alpha_1 x_1 + \cdots + \alpha_{n+1}x_{n+1} = 0,$$

so if $(a_1, \cdots, a_{n+1}) \in F^{n+1}$ were a nontrivial solution, then

$$\alpha_1 a_1 + \cdots + \alpha_{n+1}a_{n+1} = 0,$$

contradicting the linear independence of $\alpha_1, \cdots \alpha_{n+1}$. Hence any nontrivial solution $(a_1, \cdots, a_{n+1})$ contains a term $a_i \in K \setminus F$ for some i, $1 \leq i \leq n + 1$.

Choose a solution of the system of equations with the minimal number r of nonzero terms, and renumber the variables if necessary so that the nonzero terms are the first r terms of the solution, so that the solution is of the form $(\beta_1', \cdots, \beta_r', 0, \cdots 0)$. Since the equations are homogeneous, we can divide each term of the solution by β_1' and still have a solution. Consider the solution $(1, \beta_2, \cdots, \beta_r, 0, \cdots 0)$, which is the solution $(\beta_1', \cdots, \beta_r', 0, \cdots 0)$ with each term divided by β_1'. As discussed earlier, there is some β_i such that $\beta_i \notin F$. Assume without loss of generality that $i = 2$. Then since $\beta_2 \notin F$, the fixed field of H, there

is some $\sigma_j \in H$ such that $\sigma_j(\beta_2) \neq \beta_2$. Applying σ_j to the equations with the solution substituted in give the following system of equations:

$$\begin{aligned} \sigma_j(\sigma_1(\alpha_1))\sigma_j(1) + \sigma_j(\sigma_1(\alpha_2))\sigma_j(\beta_2) + \cdots + \sigma_j(\sigma_1(\alpha_r))\sigma_j(\beta_r) &= 0 \\ &\vdots \\ \sigma_j(\sigma_n(\alpha_1))\sigma_j(1) + \sigma_j(\sigma_n(\alpha_2))\sigma_j(\beta_2) + \cdots + \sigma_j(\sigma_n(\alpha_r))\sigma_j(\beta_r) &= 0 \end{aligned}$$

Since H is a group, $\{\sigma_j\sigma_1, \cdots, \sigma_j\sigma_n\} = H = \{\sigma_1, \cdots, \sigma_n\}$. Hence we can replace each $\sigma_j\sigma_i$ with the corresponding σ_k, $1 \leq i, k \leq n$ and rearrange the equations to obtain the system

$$\begin{aligned} \sigma_1(\alpha_1) + \sigma_1(\alpha_2)\sigma_j(\beta_2) + \cdots + \sigma_1(\alpha_r)\sigma_j(\beta_r) &= 0 \\ &\vdots \\ \sigma_n(\alpha_1) + \sigma_n(\alpha_2)\sigma_j(\beta_2) + \cdots + \sigma_n(\alpha_r)\sigma_j(\beta_r) &= 0 \end{aligned}$$

Hence $(1, \sigma_j(\beta_2), \cdots, \sigma_j(\beta_r), 0, \cdots, 0)$ is also a solution. Since the system of equations is homogeneous, the difference of two solutions is also a solution, so $(0, \beta_2 - \sigma_j(\beta_2), \cdots, \beta_r - \sigma_j(\beta_r), 0, \cdots, 0)$ is a solution. But since $\sigma_j(\beta_2) \neq \beta_2$, this solution is nontrivial, and it has fewer than r nonzero terms. Thus it contradicts the minimality of the solution we chose at the beginning. Therefore $[K : F]$ does not have $n+1$ linearly independent elements, so $[K : F] \leq n$.

We now show $[K : F] \geq n$. Notice that $H \subseteq \mathrm{Aut}(K/F)$ since every automorphism in H fixes F, so $|H| \leq |\mathrm{Aut}(K/F)|$. But every element of $K \setminus F$ is mapped to a different element by some automorphism in H, which is also in $\mathrm{Aut}(K/F)$, so K/F satisfies property 2 in Theorem 3.6. Hence $n = |H| \leq |\mathrm{Aut}(K/F)| = [K : F]$, so $[K : F] \geq n$. Therefore $[K : F] = n$. □

The following corollaries will also be useful in proving the Fundamental theorem in the next section. The follow almost immediately from Theorem 3.7.

Corollary 3.8. *Let K/F be a finite extension. Then $|\mathrm{Aut}(K/F)| \leq [K : F]$, with equality if F is the fixed field of $\mathrm{Aut}(K/F)$.*

Proof. Let F_1 be the fixed field of $\mathrm{Aut}(K/F)$. Then by Theorem 3.7, $|\mathrm{Aut}(K/F)| = [K : F_1]$. Clearly $F \subseteq F_1$, so $[K : F] = |\mathrm{Aut}(K/F)|[F_1 : F]$, and thus $|\mathrm{Aut}(K/F)| \leq [K : F]$. If F is the fixed field of $\mathrm{Aut}(K/F)$, then by Theorem 3.6, $|\mathrm{Aut}(K/F)| = [K : F]$. □

Corollary 3.9. *Let H be a finite subgroup of $\mathrm{Aut}(K)$ and let $F = K_H$. Then $\mathrm{Aut}(K/F) = H$.*

Proof. Since F is fixed by all the elements in G, $G \subseteq \mathrm{Aut}(K/F)$, so $|G| \leq |\mathrm{Aut}(K/F)|$. By Theorem 3.7, $|G| = [K : F]$, and by the corollary above, $|\mathrm{Aut}(K/F)| \leq [K : F]$, so $|G| \leq |\mathrm{Aut}(K/F)| \leq [K : F] = |G|$. Therefore $|G| = |\mathrm{Aut}(K/F)|$, so $G = \mathrm{Aut}(K/F)$. □

Before we proceed to the Fundamental Theorem, we make two more definitions. If E_1 and E_2 are subfields of E, then the *composite field* of E_1 and E_2, denoted E_1E_2, is the smallest subfield of E that contains E_1 and E_2. Similarly, if H_1 and H_2 are subgroups of H, then $\langle H_1, H_2\rangle$, the group generated by H_1 and H_2, is the smallest subgroup of H containing H_1 and H_2. We are now ready to move on to the Fundamental Theorem, which provides a connection between subfields of a field extension K/F that contain F and subgroups of $\mathrm{Aut}(K/F)$ when K/F is Galois.

4. Fundamental Theorem of Galois Theory

We are now ready to prove the Fundamental Theorem of Galois Theory.

Theorem 4.1. *(Fundamental Theorem of Galois Theory) Let K/F be a Galois extension and let $G = \mathrm{Gal}(K/F)$. Then there exists a bijection λ between the subfields of K containing F and the subgroups of G defined as follows. If E is a subfield of K containing F, then $\lambda(E)$ is the subgroup of G that fixes E, and if H is a subgroup of G, then $\lambda^{-1}(H)$ is the subfield of K fixed by H. This bijection has the following properties concerning $H, H_1, H_2 \in G$ and subfields E, E_1, E_2 of K containing F:*

(1) *If $\lambda(E_1) = H_1$ and $\lambda(E_2) = H_2$, then $E_1 \subseteq E_2$ if and only if $H_2 \leq H_1$.*

(2) *If $\lambda(E) = H$, then $[K : E] = |H|$ and $[E : F] = (G : H)$, the index of H in G.*

(3) *K/E is always a Galois extension, with Galois group $\mathrm{Gal}(K/E) = \lambda(E)$.*

(4) *E/F is a Galois extension if and only if $\lambda(E) = H$ is a normal subgroup of G. When this is the case, $\mathrm{Gal}(E/F)$ is isomorphic to the factor group G/H.*

(5) *If $\lambda(E_1) = H_1$ and $\lambda(E_2) = H_2$, then $\lambda(E_1 \cap E_2) = \langle H_1, H_2\rangle$ and $\lambda(E_1E_2) = H_1 \cap H_2$. Thus the lattice of subgroups of G is the inverse of the lattice of subfields of K that contain F.*

Proof. We begin by showing λ^{-1} is one to one and onto. Suppose $\lambda^{-1}(H_1) = \lambda^{-1}(H_2) = E$. Then E is the fixed field of H_1 and of H_2, so by Corollary 3.9, $\mathrm{Aut}(K/E) = H_1$ and $\mathrm{Aut}(K/E) = H_2$, so $H_1 = H_2$.

Now let E be a subfield of K containing F. Since K/F is a Galois extension, by Theorem 3.6, K is the splitting field of some separable polynomial $f \in F[x]$. We can view $f(x)$ as an element in $E[x]$, in which case K is still the splitting field and $f(x)$ is still separable, so by Theorem 3.6, K/E is a Galois extension and E is the fixed field of $\mathrm{Aut}(K/E)$. Hence λ^{-1} is onto.

Property (1) is simply a restatement of Theorem 3.4.

By Theorem 3.7, $[K : E] = |H|$ and $[K : F] = |G|$, since E is the fixed field of H and F is the fixed field of G. Since $[K : F] = [K : E][E : F]$ by Theorem 2.2, we have $(G : H) = |G|/|H| = [K : E][E : F]/[K : E] = [E : F]$.

We now prove property (3). If E is a subfield of K containing F, then because λ is a bijection, $E = \lambda^{-1}(H) = K_H$ for some $H \leq G$. By Corollary 3.9, $\mathrm{Aut}(K/E) = H$, so E is the fixed field of $\mathrm{Aut}(K/E)$. Hence K/E is a Galois extension with Galois group $\mathrm{Gal}(K/E) = H = \lambda(E)$.

To prove (4), let E/F be a Galois extension and let $\lambda(E) = H$. Let $u \in E$. Then by Theorem 3.6, the minimal polynomial $p(x) \in F[x]$ of u splits completely in E. Since $\sigma \in G$ implies $\sigma(u)$ is also a root of $p(x)$, $\sigma(u) \in E$ for all $\sigma \in G$. Hence $\sigma|_E$ is an automorphism of E for all $\sigma \in G$. Thus the map $\theta : G \to \mathrm{Gal}(E/F)$, defined by $\theta(\sigma) = \sigma|_E$, is well defined. It is also clearly a homomorphism. The kernel of θ is the set of elements of G that are the identity automorphism when restricted to E. This is just the set of automorphisms of K that fix E, so the kernel of θ is H. Thus H is a normal subgroup of G. By the Fundamental Homomorphism Theorem, $G/H \cong \theta[G]$. By (2), $(G : H) = [E : F] = |\mathrm{Gal}(E/F)|$, so $|G/H| = |\mathrm{Gal}(E/F)|$. Hence $|\theta[G]| = |\mathrm{Gal}(E/F)|$, so $\theta[G] =\mathrm{Gal}(E/F)$. Therefore G/H is isomorphic to $\mathrm{Gal}(E/F)$.

Now let $\lambda(E) = H$ be a normal subgroup of G. Let $\sigma \in H$ and $\theta \in G$. Then $\delta = \theta^{-1}\sigma\theta \in H$ and $\theta\delta = \sigma\theta$. Assume $u \in E$. Then $\delta(u) = u$ since $\delta \in H$, so $\sigma(\theta(u)) = \theta(\delta(u)) = \theta(u)$. Hence $\theta(u)$ is fixed by σ, so since σ was chosen arbitrarily, $\theta(u)$ is fixed by H. Since E is the fixed field of H, $\theta(u) \in E$ for all $\theta \in G$, $u \in E$, so $\theta|_E$ is an automorphism of E. Let $\theta, \tau \in G$. We now show that $|\mathrm{Gal}(E/F)| = (G : H)$ by showing that $\theta|_E = \tau|_E$ if and only if $\theta\tau^{-1} \in H$. Assume $\theta|_E = \tau|_E$. Then for all $u \in E$, $\theta(\tau^{-1}(u)) = \theta(\theta^{-1}(u)) = u$, so $\theta\tau^{-1} \in H$. If $\theta\tau^{-1} \in H$, then for all $u \in E$, $\theta(\tau^{-1}(u)) = u$, so $\tau^{-1}(u) = \theta^{-1}(u)$, and hence $\tau(u) = \theta(u)$. Thus each distinct automorphism of E corresponds to a

coset of H, so $|\mathrm{Gal}(E/F)| = (G : H)$. By (2), $[E : F] = (G : H)$, so $|\mathrm{Gal}(E/F)| = [E : F]$. Therefore E/F is a Galois extension.

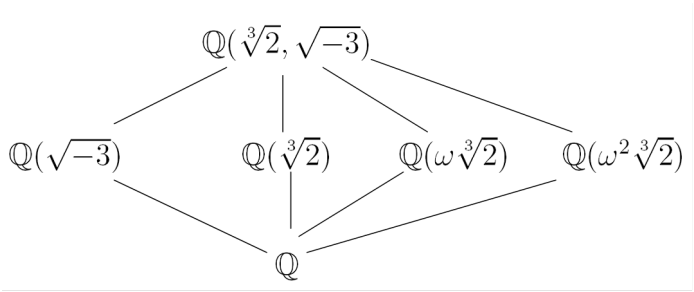
We now prove (5). Let $\lambda(H_1) = E_1$ and $\lambda(H_2) = E_2$. We show $\lambda^{-1}(\langle H_1, H_2\rangle) = E_1 \cap E_2$. Let $u \in \lambda^{-1}(\langle H_1, H_2\rangle)$. Then in particular u is fixed by H_1 and by H_2, so $u \in E_1 \cap E_2$. Now let $u \in E_1 \cap E_2$. Then u is fixed by H_1 and H_2, so it is fixed by any composition of automorphisms in H_1 and H_2. Thus $u \in \lambda^{-1}(\langle H_1, H_2\rangle)$, so $\lambda^{-1}(\langle H_1, H_2\rangle) = E_1 \cap E_2$.

We now prove that $\lambda(E_1E_2) = H_1 \cap H_2$. Let $\sigma \in H_1 \cap H_2$. Then σ fixes E_1 and E_2, so σ fixes any algebraic combination of elements in E_1 and E_2. Thus $\sigma \in \lambda(E_1E_2)$. Now let $\sigma \in \lambda(E_1E_2)$. Then σ must fix E_1 and E_2 individually, so $\sigma \in H_1 \cap H_2$. Thus $\lambda(E_1E_2) = H_1 \cap H_2$. $\square$

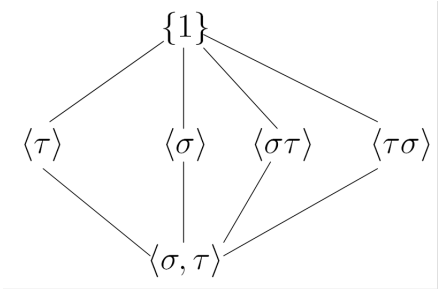
We now give an example of an application of Fundamental Theorem. Let $K = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$. Then K is the splitting field of $x^3 - 2$ over $\mathbb{Q}$, so $K/\mathbb{Q}$ is a Galois extension and $|\mathrm{Aut}(K/\mathbb{Q})| = [K : \mathbb{Q}] = 6$. This justifies our claim in the example preceding Theorem 3.5 that $\mathrm{Aut}(K/\mathbb{Q}) = \{1, \sigma, \tau, \tau^2, \sigma\tau, \tau\sigma\}$, since we found six distinct elements of $\mathrm{Aut}(K/\mathbb{Q}) = \mathrm{Gal}(K/\mathbb{Q})$. By the Fundamental Theorem, the subgroups of $\mathrm{Gal}(K/\mathbb{Q})$ are in a 1-1 correspondence with the subfields of K that contain $\mathbb{Q}$. We now demonstrate this, as well as the property that the subgroup diagram of $\mathrm{Gal}(K/\mathbb{Q})$ is the inversion of the subfield diagram of $K/\mathbb{Q}$.

Recall that in the example preceding Theorem 3.5 we determined that with $H_1 = \langle\sigma\rangle$ and $H_2 = \langle\tau\rangle$, the corresponding fixed fields are $K_{H_1} = \mathbb{Q}(\sqrt[3]{2})$ and $K_{H_2} = \mathbb{Q}(-\sqrt{-3})$. Note that $\mathrm{Gal}(K/\mathbb{Q})$ has two other subgroups: $H_3 = \langle\sigma\tau\rangle$ and $H_4 = \langle\tau\sigma\rangle$, each of order two. By Theorem 3.2 each element of $\mathrm{Gal}(K/\mathbb{Q})$ maps roots of x^2+3 to roots of x^2+3 and roots of x^3-2 to roots of x^3-2. Since the action of an element in $\mathrm{Gal}(K/\mathbb{Q})$ is completely determined by its action on these roots, to find fixed fields we must determine which roots of these polynomials are fixed by a subgroup of $\mathrm{Gal}(K/\mathbb{Q})$. To find K_{H_3}, recall that we showed $\sigma\tau(\sqrt[3]{2}) = \omega^2\sqrt[3]{2}$ and $\sigma\tau(\sqrt{-3}) = -\sqrt{-3}$. Hence $\sigma\tau(\omega) = \omega^2$, so $\sigma\tau(\omega\sqrt[3]{2}) = \omega\sqrt[3]{2}$ and $\sigma\tau(\omega^2\sqrt[3]{2}) = \sqrt[3]{2}$. Therefore the only root of $x^2 + 3$ or $x^3 - 2$ that is fixed by $\sigma\tau$ is $\omega\sqrt[3]{2}$, so $K_{H_3} = \mathbb{Q}(\omega\sqrt[3]{2})$. We perform the same procedure to find K_{H_4}. We have already determined that $\tau\sigma(\sqrt[3]{2}) = \omega\sqrt[3]{2}$ and $\tau\sigma(\sqrt{-3}) = -\sqrt{-3}$. Thus $\tau\sigma(\omega) = \omega^2$, so $\tau\sigma(\omega\sqrt[3]{2}) = \sqrt[3]{2}$ and $\tau\sigma(\omega^2\sqrt[3]{2}) = \omega^2\sqrt[3]{2}$, giving $K_{H_4} = \mathbb{Q}(\omega^2\sqrt[3]{2})$.

The Fundamental Theorem tells us that we have now found all the subfields of K that contain $\mathbb{Q}$. This is an important result, as finding all subfields of a given field is generally difficult. We can now illustrate the last property of the Fundamental Theorem. Below is the diagram of subfields of K that contain $\mathbb{Q}$.



We see below the subgroup diagram of $\mathrm{Gal}(K/\mathbb{Q})$, inverted. Notice that each subgroup corresponds to its fixed field in the diagram above.



The Fundamental Theorem also allows us to easily prove the following results concerning Galois extensions.

Theorem 4.2. *Let K/F be a Galois extension and let F'/F be any extension. Then KF'/F is a Galois extension and its Galois group is isomorphic to a subgroup of* $\mathrm{Gal}(K/F)$.

Proof. Since K/F is a Galois extension, by Theorem 3.6 K is the splitting field over F of a separable polynomial $f(x) \in F[x]$. Now consider $f(x)$ as a polynomial in $F'[x]$. Clearly the composite field KF' contains the roots of $f(x)$ and F'. Let E be a subfield of KF' that contains F' and the roots of $f(x)$. Then E contains F as well, so since K is the splitting field of $f(x)$ over F, $K \subset E$. Since $F' \subset E$ as well, $KF' \subset E$. Hence $E = KF'$, so KF' is the splitting field of $f(x)$ over F'. Thus by Theorem 3.6 KF'/F' is a Galois extension.

Consider the map $\phi : \mathrm{Gal}(KF'/F') \to \mathrm{Gal}(K/F)$ given by $\phi(\sigma) = \sigma_K$. We showed in the proof of property (4) of the Fundamental Theorem that this map is well defined. Since it is clear that for any $\sigma, \tau \in \mathrm{Gal}(KF'/F')$, $\sigma\tau|_K = \sigma|_K\tau|_K$, ϕ is a homomorphism. The kernel of ϕ is $\ker\phi = \{\sigma \in \mathrm{Gal}(KF'/F') : \sigma|_K = 1\}$. Thus, $\ker\phi$ contains the automorphisms of KF' that fix both F' and K. Clearly, this is just the identity automorphism, so $\ker\phi = \{1\}$, and hence ϕ is 1-1. Thus $\mathrm{Gal}(KF'/F')$ is isomorphic to $\phi[\mathrm{Gal}(KF'/F')]$, a subgroup of $\mathrm{Gal}(K/F)$. $\square$

We now show that intersections and composites of Galois extensions are also Galois extensions.

Theorem 4.3. *Let K_1 and K_2 be Galois extensions of a field F. Then $K_1 \cap K_2$ and K_1K_2 are both Galois over F.*

Proof. Let $p(x) \in F[x]$ be an irreducible polynomial with a root $\alpha \in K_1 \cap K_2$. Then $\alpha \in K_1$, so since K_1/F is Galois, all the roots of $p(x)$ are in K_1, by Theorem 3.6. Similarly, all the roots of $p(x)$ are in K_2 since $\alpha \in K_2$ and K_2/F is Galois. Thus all the roots of $p(x)$ are in $K_1 \cap K_2$, so by Theorem 3.6, $K_1 \cap K_2$ is a Galois extension of F.

Since K_1 and K_2 are Galois over F, by Theorem 3.6 K_1 is the splitting field of a separable polynomial $f(x) \in F[x]$ and K_2 is the splitting field of a separable polynomial $g(x) \in F[x]$. Let $h(x) \in F[x]$ be fg with duplicate factors removed, so that $h(x)$ is separable. Then the splitting field of $h(x)$ is the smallest field containing all the roots of $f(x)$ and $g(x)$, so it is K_1K_2. Thus K_1K_2 is the splitting field of a separable polynomial in $F[x]$, so by Theorem 3.6, K_1K_2 is Galois over F. □

It is often desirable to work in a Galois extension, so that we can use the Fundamental Theorem. The theorem below allows us to extend any extension E of a field F to a minimal Galois extension of F, so that we can work with elements of E in a Galois extension.

Corollary 4.4. *Let E/F be a separable finite extension. Then E is contained in an extension K which is Galois over F and is minimal in the sense that any other Galois extension of F containing E contains F.*

Proof. Suppose $E = F(\alpha_1 \cdots, \alpha_n)$. For $1 \leq i \leq n$, let L_i be the splitting field over F of the minimal polynomial of α_i. Since E is a separable extension, each of the minimal polynomials is separable, so each L_i is Galois over F. Then by Theorem 4.3 the composite L of all the $L_i's$ is Galois over F. Clearly $E \subset L$, so E is contained in a Galois extension of F. Let K be the intersection of all such extensions of F. Then by Theorem 4.3 K is Galois over F, and clearly K is contained in any other Galois extension of F containing E. □

The field K in the corollary above is called the *Galois closure* of E over F.

5. Insolvability of the Quintic

We are now ready to apply the material we have developed to show that quintic polynomial equations are, in general, not solvable by radicals. We first investigate the Galois groups of polynomials in more detail and describe what is meant by a "general" polynomial.

Recall that if $f(x) \in F[x]$ is a separable polynomial with splitting field E, then the Galois group of $f(x)$ is $\mathrm{Gal}(E/F)$. If $f(x)$ has roots $\alpha_1, \cdots, \alpha_n$, then by Theorem 3.2, each $\sigma \in \mathrm{Gal}(E/F)$ acts as a permutation of the roots of $f(x)$ and thus defines a unique permutation on $\{1, \cdots, n\}$. Thus $\mathrm{Gal}(E/F)$ can be identified with a subgroup of S_n. Going back to the example of the Galois extension $K/\mathbb{Q}$ with $K = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$, denote the roots of $x^3 - 2$ by $\alpha_1 = \sqrt[3]{2}$, $\alpha_2 = \omega\sqrt[3]{2}$, and $\alpha_3 = \omega^2\sqrt[3]{2}$. Then associating the elements of $\mathrm{Gal}(K/\mathbb{Q})$ with their permutations of the roots, which were found in the example following the proof of the Fundamental Theorem, we obtain $\sigma = (2, 3)$ and $\tau = (1, 2, 3)$. Repeating this for the other elements of $\mathrm{Gal}(K/\mathbb{Q})$ gives $\tau^2 = (1, 3, 2)$, $\sigma\tau = (1, 3)$, and $\tau\sigma = (1, 2)$, so that $\mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to S_3. As this example shows, working with the permutation equivalents of elements of a Galois group can be computationally simpler.

Let $x_1, x_2, \cdots, x_n$ be indeterminates. The *elementary symmetric functions* $s_1, s_2, \cdots s_n$ are defined by

$$\begin{aligned} s_1 &= x_1 + x_2 + \cdots x_n \\ s_2 &= x_1x_2 + x_1x + 3 + \cdots + x_2x_3 + x_2x_4 + \cdots + x_{n-1}x_n \\ &\vdots \\ s_n &= x_1x_2 \cdots x_n. \end{aligned}$$

The *general polynomial of degree* n is the polynomial $f(x) = (x - x_1)(x - x_2)\cdots(x - x_n)$, the roots of which are the indeterminates $x_1, x_2, \cdots, x_n$. Notice that $(x-x_1)(x-x_2)\cdots(x-x_n) = x^n - s_1x^{n-1} + s_2x^{n-2} + \cdots + (-1)^n s_n$. Thus $f(x) \in F(s_1, \cdots, s_n)$, and clearly $F(x_1, \cdots, x_n)$ is the splitting field of $f(x)$ over $F(s_1, \cdots, s_n)$, so $F(x_1, \cdots, x_n)$ is a Galois extension of $F(s_1, \cdots, s_n)$. We now show that $F(s_1, \cdots, s_n)$ is in fact the fixed field of S_n.

Theorem 5.1. *Let $x_1, \cdots, x_n$ be indeterminates, and let $s_1, \cdots, s_n$ be the elementary symmetric functions. Then the fixed field of S_n acting on $K = F(x_1, \cdots, x_n)$ is $F(s_1, \cdots, s_n)$.*

Proof. First note that any $\sigma \in S_n$ acts on $F(x_1, \cdots, x_n)$ by permuting the subscripts of the x_i, so σ is an automorphism of $F(x_1, \cdots, x_n)$ for all $\sigma \in S_n$, and thus $S_n \subset \mathrm{Aut}(F(x_1, \cdots, x_n))$.

Let $\sigma \in S_n$. Then clearly each s_i, $1 \leq i \leq n$ is fixed by σ since the symmetric functions remain unchanged by permutations of the subscripts of the x_i. Hence $F(s_1, \cdots, s_n) \subset K_{S_n}$. By the Fundamental Theorem, $[K : K_{S_n}] = |S_n| = n!$. Since K is the splitting field of the separable polynomial $(x - x_1) \cdots (x - x_n)$ over $F(s_1, \cdots, s_n)$, $[K : F(s_1, \cdots, s_n)] = n!$ by the comments following Theorem 2.5. Therefore $F(s_1, \cdots, s_n) = K_{S_n}$, the fixed field of S_n. □

We can also begin with a polynomial $f(x) = x^n - s_1 x^{n-1} + \cdots + (-1)^n s_n$ over the field $F(s_1, \cdots, s_n)$, where $s_1, \cdots, s_n$ are indeterminates. If we let $x_1, \cdots, x_n$ be the roots of $f(x)$, then we see that $s_1, \cdots, s_n$ are the elementary symmetric functions in terms of $x_1, \cdots, x_n$, and that $x_1, \cdots, x_n$ are also indeterminates. Since $x_1, \cdots, x_n$ are indeterminates, $f(x)$ is separable, so the Galois group of $f(x)$ is $\mathrm{Gal}(F(x_1, \cdots, x_n)/F(s_1, \cdots, s_n))$, since $F(x_1, \cdots, x_n)$ is the splitting field of $f(x)$ over $F(s_1, \cdots, s_n)$, as discussed earlier. By Theorem 5.1, this Galois group is in fact S_n. We restate this result in the form of the following theorem.

Theorem 5.2. *If $s_1, \cdots, s_n$ are indeterminates, the polynomial $x^n - s_1 x^{n-1} + \cdots + (-1)^n s_n$ over $F(s_1, \cdots, s_n)$ is the general polynomial of degree n and is separable with Galois group S_n.*

We are now ready to discuss solving for the roots of polynomials by radicals. First, some definitions.

Let K/F be a field extension. Then K/F is a *simple radical extension* if $K = F(\sqrt[n]{a})$ for some $a \in F$, where $\sqrt[n]{a}$ is any root of $x^n - a \in F[x]$. Also, K/F is *cyclic* and K is a *cyclic extension* of F if K/F is a Galois extension and $\mathrm{Gal}(K/F)$ is a cyclic group. Note that in saying K/F is cyclic, we are referring to the Galois group of K/F being cyclic. For the remainder of the paper, if $a \in F$, F a field, then $\sqrt[n]{a}$ refers to any root of $x^n - a \in F[x]$, as in the definition of simple radical extensions. Also, for simplicity, any base field F will be assumed to have characteristic zero. The following theorems will also be valid if the base field does not have characteristic dividing any of the orders of roots that are taken in the field. The next two theorems provide a connection between simple radical extensions and cyclic extensions when the base field F contains the appropriate roots of unity. Specifically, they show that if F contains the appropriate roots of unity, cyclic extensions are equivalent to simple radical extensions. The proofs closely follow those of Propositions 36 and 37 on pages 625-626 of [1].

Theorem 5.3. *Let F be a field which contains the n^{th} roots of unity. If $a \in F$, then $F(\sqrt[n]{a})$ is a cyclic extension of F and $[F(\sqrt[n]{a}) : F]$ divides n.*

Proof. Since F contains the n^{th} roots of unity, $K = F(\sqrt[n]{a})$ is the splitting field over F for $x^n - a$. Thus K/F is a Galois extension by Theorem 3.6. Now, if $\sigma \in \mathrm{Gal}(K/F)$, then σ maps $\sqrt[n]{a}$ to a root of $x^n - a$, so $\sigma(\sqrt[n]{a}) = \zeta_\sigma \sqrt[n]{a}$ for some n^{th} root of unity ζ_σ. Let $\theta : \mathrm{Gal}(K/F) \to U_n$, where U_n is the group of n^{th} roots of unity, be defined by $\theta(\sigma) = \zeta_\sigma$. Since F contains the n^{th} roots of unity, $U_n \subset F$, so U_n is fixed by $\mathrm{Gal}(K/F)$. Thus, if $\sigma, \tau \in \mathrm{Gal}(K/F)$,

$$\begin{aligned} \sigma\tau(\sqrt[n]{a}) &= \sigma(\zeta_\tau \sqrt[n]{a}) \\ &= \zeta_\tau \sigma(\sqrt[n]{a}) \\ &= \zeta_\tau \zeta_\sigma \sqrt[n]{a} = \zeta_\sigma \zeta_\tau \sqrt[n]{a}. \end{aligned}$$

Hence $\zeta_{\sigma\tau} = \zeta_\sigma \zeta_\tau$, so $\theta(\sigma\tau) = \theta(\sigma)\theta(\tau)$. Thus θ is a homomorphism. The kernel of θ is the set of $\sigma \in \mathrm{Gal}(K/F)$ satisfying $\sigma(\sqrt[n]{a}) = 1 \cdot \sqrt[n]{a}$, so the kernel is just the set containing the identity automorphism, so θ is one-to-one. Thus $\mathrm{Gal}(K/F)$ is in one-to-one correspondence with a subgroup of U_n, which is cyclic, so $\mathrm{Gal}(K/F)$ is cyclic and $|\mathrm{Gal}(K/F)|$ divides n. Since $|\mathrm{Gal}(K/F)| = [K : F]$ by the Fundamental Theorem, $[K : F]$ also divides n. □

Theorem 5.4. *Let K be a cyclic extension of degree n over a field F which contains the n^{th} roots of unity. Then $K = F(\sqrt[n]{a})$ for some $a \in F$.*

Proof. Since K is a cyclic extension, $\mathrm{Gal}(K/F)$ has some generator σ, with $\sigma^n = 1$. For $\alpha \in K$ and ζ an n^{th} root of unity, define

$$(\alpha, \zeta) = \alpha + \zeta\sigma(\alpha) + \cdots + \zeta^{n-1}\sigma^{n-1}(\alpha).$$

Then, since the n^{th} roots of unity are in F and thus fixed by σ,

$$\sigma((\alpha, \zeta)) = \sigma(\alpha) + \zeta\sigma^2(\alpha) + \cdots + \zeta^{n-1}\sigma^n(\alpha).$$

Since $\zeta^n = 1$ in U_n and $\sigma^n = 1$ in $\mathrm{Gal}(K/F)$, we can rewrite $\sigma((\alpha, \zeta))$ as

$$\begin{aligned} \sigma((\alpha, \zeta)) &= \sigma(\alpha) + \zeta\sigma^2(\alpha) + \cdots + \zeta^{-1}\alpha \\ &= \zeta^{-1}(\alpha + \zeta\sigma(\alpha) + \zeta^2\sigma^2(\alpha) + \cdots + \zeta^{n-1}\sigma^{n-1}(\alpha)) \\ &= \zeta^{-1}(\alpha, \zeta). \end{aligned}$$

Thus $\sigma((\alpha, \zeta)^n) = \sigma((\alpha, \zeta))^n = \zeta^{-n}(\alpha, \zeta)^n = (\alpha, \zeta)^n$, so $(\alpha, \zeta)^n$ is fixed by σ. Since σ generates $\mathrm{Gal}(K/F)$, $(\alpha, \zeta)^n$ is thus fixed by $\mathrm{Gal}(K/F)$, so $(\alpha, \zeta)^n = a$ for some $a \in F$.

Now let ζ be a primitive n^{th} root of unity. By the above argument, for $i \geq 0$, $\sigma^i((\alpha,\zeta)) = \sigma((\alpha,\zeta))^i = \zeta^{-i}(\alpha,\zeta)$. For $i < n$, $\zeta^i \neq \zeta$ since ζ is a primitive root of unity, so σ^i does not fix (α,ζ) for any $i < n$. Thus (α,ζ) is not fixed by any nontrivial subgroup of $\mathrm{Gal}(K/F)$, so by the Fundamental Theorem (α,ζ) is not in any proper subfield of K that contains F. Hence $[K : F((\alpha,\zeta))] = 1$ and $F((\alpha,\zeta)) \subseteq K$ since $(\alpha,\zeta) \in K$, so $K = F((\alpha,\zeta))$. Since $(\alpha,\zeta)^n = a$ for some $a \in F$, $K = F(\sqrt[n]{a})$. □

We now make precise the notion of solving by radicals. Let α be algebraic over F. Then α can be *solved for in terms of radicals* if α is in a field K that can be obtained from F by successive simple radical extensions, so that

$$F = K_0 \subset K_1 \subset \cdots \subset K_s = K,$$

where for $i = 0, 1, \cdots, s-1$, $K_{i+1} = K_i(\sqrt[n_i]{a_i})$ for some $a_i \in K_i$. In this expression, $\sqrt[n_i]{a_i}$ is some root of the polynomial $x^{n_i} - a_i \in K_i[x]$. The field K is called a *root extension* of F. We refer to the extensions K_{i+1}/K_i as the *intermediate extensions* of K. Finally, a polynomial $f(x) \in F[x]$ can be *solved by radicals* if all its roots can be solved for in terms of radicals.

This definition makes sense because if we start with $\alpha \in K$, we can rewrite α in terms of elements of the field one step down in the chain and radicals of these elements. We can repeat this process until we are working in F and have α written in terms of elements of F and radicals, or multiple radicals, of elements in F. As an example of constructing a root extension K, suppose $F = \mathbb{Q}$ and $\alpha = \sqrt{3 + \sqrt[3]{52}}$. Then $K_0 = \mathbb{Q}$ and $K_1 = K_0(\sqrt[3]{a_0})$, where $a_0 = 52$. We then let $K_2 = K_1(\sqrt{a_1})$, where $a_1 = 3 + \sqrt[3]{52} \in K_1$. Since $\alpha \in K_2$, we have $K_2 = K$, so K_2 is a root extension of F which contains α.

An arbitrary root extension containing α is not necessarily useful, but given that α is in some root extension of F, we can find a root extension of F containing α that has very nice properties. First we need the following lemma concerning composites of root extensions.

Lemma 5.5. *If K and K' are both root extensions of F, then KK' is a root extension of F. Additionally, if K and K' each have cyclic intermediate extensions, then KK' has cyclic intermediate extensions.*

Proof. Let K and K' be root extensions of F. Then there are chains of subfields

$$\begin{aligned} F &= K_0 \subset K_1 \subset \cdots \subset K_{s-1} \subset K_s = K \\ F &= K'_0 \subset K'_1 \subset \cdots \subset K'_{t-1} \subset K'_t = K' \end{aligned}$$

with K_{i+1}/K_i and K'_{j+1}/K'_j simple radical extensions for $0 \leq i \leq s-1$, $0 \leq j \leq t-1$. Consider the chain of subfields

$$F = K_0 \subset K'_1K_0 \subset K'_1K_1 \subset \cdots \subset K'_1K_s = K'_1K \subset K'_2K \subset \cdots \subset K'_tK = K'K.$$

Then K'_1K_{i+1}/K'_1K_i and $K'_{j+1}K/K'_jK$ are all simple radical extensions for $0 \leq i \leq s-1$, $0 \leq j \leq t-1$. Hence $K'K$ is a root extension of F.

Now assume K and K' are both root extensions of F with the same subfields as above, with the additional assumption that K_{i+1}/K_i and K'_{j+1}/K'_j are cyclic extensions for $0 \leq i \leq s-1$, $0 \leq j \leq t-1$. Consider the root extension KK' with the same chain of subfields as above. Let $i \in \mathbb{N}$ such that $0 \leq i \leq s-1$. Since K_{i+1}/K_i is Galois and K'_1K_i is an extension of K_i, $K_{i+1}K_iK'_1 = K_{i+1}K'_1$ is a Galois extension of K'_1K_i by Theorem 4.2 and $\mathrm{Gal}(K_{i+1}K'_1/K'_1K_i)$ is a subgroup of $\mathrm{Gal}(K_{i+1}/K_i)$. Since K_{i+1}/K_i is a cyclic extension, $\mathrm{Gal}(K_{i+1}/K_i)$ is cyclic, so $\mathrm{Gal}(K_{i+1}K'_1/K'_1K_i)$ is cyclic and hence $K_{i+1}K'_1/K'_1K_i$ is a cyclic extension. A similar argument shows that for each j with $1 \leq j \leq t-1$, $K'_{j+1}K/K'_jK$ is a cyclic extension. Thus all the intermediate extensions of KK' are cyclic. □

We now show that we can extend any root extension of F to a Galois root extension of F which has cyclic intermediate extensions. Working in such a root extension will allow us to use the Fundamental Theorem to maximum effect.

Lemma 5.6. *If α is an element of a root extension of F, then α is in a root extension K which is Galois over F and for which each extension K_{i+1}/K_i is cyclic.*

Proof. Let F be a field and suppose α is an element of a root extension K of F. Then their exist fields K_i, $0 \leq i \leq s$, such that

$$F = K_0 \subset K_1 \subset \cdots \subset K_s = K$$

and such that K_{i+1} is a simple radical extension of K_i for $1 \leq i \leq s-1$. Let L be the Galois closure of K over F. This closure exists by Corollary 4.4. We first show that for any $\sigma \in \mathrm{Gal}(L/F)$, $\sigma(K)$ is a root extension of F. Consider the chain of subfields

$$F = \sigma(K_0) \subset \sigma(K_1) \subset \cdots \subset \sigma(K_s) = \sigma(K).$$

Let i be such that $0 \leq i \leq s-1$. Then K_{i+1} is a simple radical extension of K_i, so $K_{i+1} = K_i(\sqrt[n_i]{a_i})$ for some $a_i \in K_i$, $n_i \in \mathbb{N}$. Note that $\sigma(\sqrt[n_i]{a_i})$ is a root of $x^{n_i} - \sigma(a_i) \in \sigma(K_i)[x]$, so if we can show that $\sigma(K_{i+1}) = \sigma(K_i)(\sigma(\sqrt[n_i]{a_i}))$, then we will have shown that $\sigma(K_{i+1})$ is

a simple radical extension of $\sigma(K_i)$. Let $y \in \sigma(K_{i+1}) = \sigma(K_i(\sqrt[n_i]{a_i}))$. Then $y = \sigma(z)$ for some $z \in \sigma(K_i(\sqrt[n_i]{a_i}))$, with

$$z = \sum_{j=0}^{n_i-1} b_j \sqrt[n_i]{a_i^j},$$

where $b_j \in K_i$, since $\{1, \sqrt[n_i]{a_i}, \sqrt[n_i]{a_i^2}, \cdots, \sqrt[n_i]{a_i^{n-1}}\}$ is a basis for $K_i(\sqrt[n_i]{a_i})$ over K. Then

$$y = \sigma(z) = \sum_{j=0}^{n_i-1} \sigma(b_j)\sigma(\sqrt[n_i]{a_i^j}),$$

so $y \in \sigma(K_i)(\sigma(\sqrt[n_i]{a_i}))$.

Now let $y \in \sigma(K_i)(\sigma(\sqrt[n_i]{a_i}))$. Then

$$\begin{aligned} y &= \sum_{j=0}^{n_i-1} \sigma(b_j)\sigma(\sqrt[n_i]{a_i^j}) \\ &= \sigma(\sum_{j=0}^{n_i-1} b_j \sqrt[n_i]{a_i^j}) \\ &= \sigma(z) \end{aligned}$$

for some $z \in K_i(\sqrt[n_i]{a_i})$. Thus $y \in \sigma(K_{i+1})$. Therefore $\sigma(K_{i+1}) = \sigma(K_i)(\sigma(\sqrt[n_i]{a_i}))$, so $\sigma(K_{i+1})$ is a simple radical extension of $\sigma(K_i)$. Hence $\sigma(K)$ is a root extension of F.

Since the composite of root extensions is a root extension by Lemma 5.5, the composite of all the fields $\sigma(K)$ for each $\sigma \in \mathrm{Gal}(K/F)$ is a root extension of F. The argument below shows that this composite is actually L, which is Galois over F, so that α is in a Galois root extension of F.

Let E be the composite of all the fields $\sigma(K)$ for $\sigma \in \mathrm{Gal}(L/F)$. Since $\sigma(K) \subset L$ for each σ, $E \subset L$, since E is the smallest field containing each $\sigma(K)$. To show that $L \subset E$, we will show that E/F is Galois. Since L is the minimal field that is Galois over F, this implies $L \subset E$.

Let $H = \mathrm{Aut}(L/E)$. To show E/F is Galois, we show that H is normal in $\mathrm{Gal}(L/F)$ and apply property 4 of the Fundamental Theorem of Galois Theory. To this end let $\phi \in \mathrm{Gal}(L/F)$ and let $\tau \in H$. Let $a \in E$. Then a can be written in the terms of sums and products of elements of the form $\sigma_i(k)$, where $\sigma_i \in \mathrm{Gal}(L/F)$ and $k \in K$. Since $\phi^{-1}\sigma_i \in \mathrm{Gal}(L/F)$ for each $\sigma_i \in \mathrm{Gal}(L/F)$, $\phi^{-1}(a) \in E$, so $\tau(\phi^{-1}(a)) = \phi^{-1}(a)$, since τ fixes E. Thus $\phi\tau\phi^{-1}(a) = \phi\phi^{-1}(a) = a$, so $\phi\tau\phi^{-1}$ fixes E. Therefore $\phi\tau\phi^{-1} \in H$, so $\phi H\phi^{-1} = H$, and thus H is normal in

$\mathrm{Gal}(L/F)$. Then by property 4 of the Fundamental Theorem, E is a Galois extension of F. By the minimality of L, we have $L \subset E$. Therefore $L = E$.

Now let K be a Galois root extension of F with subfields K_i, $0 \leq i \leq s$, where each simple radical extension is obtained by adjoining $\sqrt[n_i]{a_i}$. Let F' be the field obtained by adjoining the n_i-th roots of unity to F for each i. Note that F' is the splitting field of $(x^{n_1} - 1) \cdots (x^{n_s} - 1)$ over F, so F'/F is Galois. Thus, by Theorem 4.3, KF' is Galois over F. Consider the chain of subfields

$$F \subset F' = F'K_0 \subset F'K_1 \subset \cdots \subset F'K_s = F'K$$

in which K_{i+1}/K_i is a simple radical extension for $0 \leq i \leq s-1$ because K is a root extension of F. Thus $F'K_{i+1}/F'K_i$ is a simple radical extension for $0 \leq i \leq s-1$. Since $F'K_i$ contains the n_i-th roots of unity, $F'K_{i+1}$ is a cyclic extension over $F'K_i$ for $0 \leq i \leq s-1$ by Theorem 5.3.

We now show that F' is a root extension of F with each intermediate extension cyclic. Let ω_{n_i} be a primitive n_i-th root of unity for $0 \leq i \leq s-1$. Then $F' = F(\omega_{n_0}, \cdots, \omega_{n_{s-1}})$. Any $\sigma \in \mathrm{Gal}(F'/F)$ maps each ω_{n_i} to a power of ω_{n_i}, and the action of σ is completely determined by its action on each ω_{n_i}. For any $a, b \in \mathbb{N}$, $(\omega_{n_i}^a)^b = (\omega_{n_i}^b)^a$. Thus, if $\sigma, \tau \in \mathrm{Gal}(F'/F)$ such that $\sigma(\omega_{n_i}) = \omega_{n_i}^a$ and $\tau(\omega_{n_i}) = \omega_{n_i}^b$, then $\sigma\tau(\omega_{n_i}) = \tau\sigma(\omega_{n_i})$. Since this is true for $0 \leq i \leq s-1$, $\sigma\tau = \tau\sigma$, so $\mathrm{Gal}(F'/F)$ is abelian.

$\mathrm{Gal}(F'/F)$ is finite, so we can write $\mathrm{Gal}(F'/F) = \langle \sigma_1, \cdots, \sigma_m \rangle$ for some $\sigma_1, \cdots, \sigma_m \in \mathrm{Gal}(F'/F)$. Then

$$\{1\} \subset \langle \sigma_1 \rangle \subset \cdots \subset \langle \sigma_1, \cdots, \sigma_m \rangle = \mathrm{Gal}(F'/F).$$

Letting $\lambda(\langle \sigma_1, \cdots, \sigma_i \rangle) = F_{m-i}$ be the fixed field of $\langle \sigma_1, \cdots, \sigma_i \rangle$, we see by the Fundamental Theorem that

$$F = F_0 \subset F_1 \subset \cdots \subset F_m = F'.$$

Since $\mathrm{Gal}(F'/F)$ is abelian, $\langle \sigma_1, \cdots, \sigma_{m-i-1} \rangle$ is normal in $\langle \sigma_1, \cdots, \sigma_{m-i} \rangle$ for $0 \leq i \leq m-1$. Then by the Fundamental Theorem, F_{i+1}/F_i is Galois and $\mathrm{Gal}(F_{i+1}/F_i) \cong \langle \sigma_1, \cdots, \sigma_{m-i} \rangle / \langle \sigma_1, \cdots, \sigma_{m-i-1} \rangle \cong \langle \sigma_{m-i} \rangle$, where the second isomorphism follows from an easy application of the Fundamental Homomorphism Theorem. Hence $\mathrm{Gal}(F_{i+1}/F_i)$ is cyclic for $0 \leq i \leq m-1$, so each F_{i+1}/F_i is a cyclic extension. Therefore $F'K$ is a root extension of F which is Galois over F with cyclic intermediate extensions. $\square$

Before we prove the main theorem of the section, we present one more definition.

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

$$1 = G_s \leq G_{s-1} \leq \cdots \leq G_0 = G$$

such that G_i/G_{i+1} is cyclic, $i = 0, 1, \cdots, s-1$.

The reader can refer to page 196 in [1] for proofs that subgroups and quotient groups of solvable groups are also solvable groups; we will use these facts in the following theorem.

Theorem 5.7. *The separable polynomial $f(x) \in F[x]$ can be solved by radicals if and only if its Galois group is solvable.*

Proof. Assume first that $f(x) \in F[x]$ is separable and can be solved by radicals. Then every root of $f(x)$ is contained in a root extension of F, so by Lemma 5.6, each root of $f(x)$ is contained in a root extension which is Galois over F with cyclic intermediate extensions. Let K be the composite of these root extensions. Then by Theorem 5.5, K is a Galois root extension over F with cyclic intermediate extensions. Thus we have

$$F = K_0 \subset K_1 \subset \cdots K_{s-1} \subset K_s = K,$$

with K_{i+1}/K_i a cyclic extension for each i, $0 \leq i \leq s-1$. For each i, let $G_i = \lambda(K_i)$, where λ is the the function in the Fundamental Theorem that maps a subfield of K to the subgroup of $\mathrm{Gal}(K/F)$ which fixes it. By the Fundamental Theorem, K/K_i is a Galois extension and $\mathrm{Gal}(K_{i+1}/K_i) \cong G_i/G_{i+1}$ if K_{i+1}/K_i is Galois. But K_{i+1}/K_i is cyclic, so it is Galois by definition of a cyclic extension. Thus $\mathrm{Gal}(K_{i+1}/K_i) \cong G_i/G_{i+1}$, and since K_{i+1}/K_i is a cyclic extension, its Galois group is cyclic, so G_i/G_{i+1} is cyclic. Because λ is inclusion reversing by the Fundamental Theorem,

$$\{1\} = G_s \leq G_{s-1} \leq \cdots \leq G_1 \leq G_0 = G.$$

Therefore G is solvable.

Now let E be the splitting field of $f(x)$ over F. Since K contains all the roots of $f(x)$, E is a subfield of K. Let $H = \lambda(E)$. Since E is the splitting field of a separable polynomial in $F[x]$, E is a Galois extension of F, so by the Fundamental Theorem $\mathrm{Gal}(E/F) \cong G/H$. Since $H \leq G$ and G is solvable, H is solvable, so the quotient group G/H is solvable. Hence $\mathrm{Gal}(E/F)$, the Galois group of $f(x)$, is solvable.

To prove the other direction, assume that the Galois group of $f(x)$ is solvable. Let K be the splitting field of $f(x)$ over F, with $G = \mathrm{Gal}(K/F)$ the Galois group of $f(x)$. Since G is solvable, there exists a chain of subgroups satisfying

$$\{1\} = G_s \leq G_{s-1} \leq \cdots \leq G_1 \leq G_0 = G$$

with G_i/G_{i+1} cyclic for $0 \leq i \leq s-1$. For each i, let $K_i = K_{G_i} = \lambda^{-1}(G_i)$ be the fixed field of G_i. Then by Property 1 of the Fundamental Theorem,

$$F = K_0 \subset K_1 \subset \cdots \subset K_{s-1} \subset K_s = K.$$

Let $i \in \mathbb{N}$ such that $0 \leq i \leq s-1$. Since K/K_i is Galois by the Fundamental Theorem, K_{i+1}/K_i is Galois if and only if G_{i+1} is a normal subgroup of G_i. Since G_i/G_{i+1} is a group, G_{i+1} is indeed normal in G_i, so K_{i+1}/K_i is a Galois extension. Also, $\mathrm{Gal}(K_{i+1}/K_i) \cong G_i/G_{i+1}$, a cyclic group, so K_{i+1} is a cyclic extension of K_i.

Let n_i be the degree of each extension K_{i+1}/K_i, and let F' be the extension of F containing all the n_i-th roots of unity for each i, $0 \leq i \leq s-1$. Then F' is Galois over F since F' is the splitting field of $(x^{n_0}-1)\cdots(x^{n_{s-1}}-1)$ with any duplicate factors removed. Also, F' can be obtained from F by adjoining a primitive n_i-th root of unity at each step, so that F' can be obtained from F by a chain of simple radical extensions. Now consider the chain of extensions

$$F \subset F' = F'K_0 \subset F'K_1 \subset \cdots \subset F'K_{s-1} \subset F'K_s = F'K.$$

Let $i \in \mathbb{N}$ such that $0 \leq i \leq s-1$. Since K_{i+1} is a Galois extension of K_i and $F'K_i$ is an extension of K_i, by Theorem 4.2, $F'K_iK_{i+1}/F'K_i$ is a Galois extension with Galois group isomorphic to a subgroup of $\mathrm{Gal}(K_{i+1}/K_i)$. Since $K_i \subset K_{i+1}$, $F'K_iK_{i+1} = F'K_{i+1}$, so $F'K_{i+1}/F'K_i$ is Galois. Also, since $\mathrm{Gal}(K_{i+1}/K_i)$ is cyclic and $\mathrm{Gal}(F'K_{i+1}/F'K_i) \leq \mathrm{Gal}(K_{i+1}/K_i)$, $\mathrm{Gal}(F'K_{i+1}/F'K_i)$ is cyclic. Thus $F'K_{i+1}/F'K_i$ is a cyclic extension. Letting $H = \mathrm{Gal}(F'K_{i+1}/F'K_i)$, we have $[F'K_{i+1} : F'K_i] = |H|$ by Theorem 3.6. Since H is isomorphic to a subgroup of $\mathrm{Gal}(K_{i+1}/K_i)$, $|H|$ divides $|\mathrm{Gal}(K_{i+1}/K_i)| = [K_{i+1} : K_i] = n_i$, using Theorem 3.6 again. Hence $F'K_{i+1}/F'K_i$ has degree m_i dividing n_i. Since F' contains the n_i-th roots of unity, F' also contains the m_i-th roots of unity. This is because any n_i-th root of unity raised to the power of n_i/m_i is an m_i-th root of unity. Thus $F'K_i$ contains the m_i-th roots of unity, so by Theorem 5.4, $F'K_{i+1}$ is a simple radical extension of $F'K_i$. Therefore $F'K$ is a root extension of F. Recall that K is the splitting field of $f(x)$, so $F'K$ contains all the roots of $f(x)$. Therefore $f(x)$ can be solved by radicals. □

Corollary 5.8. *The general polynomial equation of degree n cannot be solved by radicals for $n \geq 5$. Specifically, the general quintic polynomial equation cannot be solved by radicals.*

Proof. By Theorem 5.2, the general polynomial of degree n has Galois group S_n. For $n \geq 5$, the only nontrivial proper normal subgroup of S_n is A_n, which is simple. Since A_n is not cyclic, or even abelian, S_n is

not solvable. Thus by Theorem 5.7, the general polynomial of degree n is not solvable by radicals. $\square$

By Corollary 5.8, we have now accomplished our goal of showing that the general quintic polynomial equation is not solvable by radicals. In fact, we have proved a stronger result; for any $n \geq 5$, the general polynomial of degree n cannot be solved by radicals. This means that given a degree $n \geq 5$ polynomial, it is not guaranteed that we can find its exact solutions using only the elementary operations and radicals. This is not to say that no polynomial of degree 5 or higher cannot be solved by radicals; for instance, clearly $x^5 - 1$ has the fifth roots of unity as its zeros, and these can all be expressed in terms of radicals. Rather, there exists polynomials with solutions not expressible by radicals, and given a random polynomial of degree 5 or greater, this is likely to be the case. We now give an example of a quintic polynomial in $\mathbb{Q}[x]$ that is not solvable by radicals. This example is taken from page 629 of [1].

Let $f(x) = x^5 - 6x + 3 \in \mathbb{Q}[x]$. Using the Eisentein criteria, learned in undergraduate abstract algebra, with $p = 3$, we see that $f(x)$ is irreducible. Thus the splitting field E of $f(x)$ over $\mathbb{Q}$ is divisible by 5. By the Fundamental Theorem, $[E : \mathbb{Q}] = |\mathrm{Gal}(E/\mathbb{Q})|$, so the order of the Galois group of $f(x)$ is divisible by 5. By Cauchy's theorem, covered in undergraduate abstract algebra, $\mathrm{Gal}(E/\mathbb{Q})$ has an element σ of order 5, which must be a 5-cycle since $\mathrm{Gal}(E/\mathbb{Q}) \subset S_5$. By graphing $f(x)$ we observe that $f(x)$ has three real zeroes, and thus two complex roots. Thus the automorphism τ of E defined by complex conjugation fixes the three real roots and interchanges the two complex roots, so τ is a transposition in S_5. We now have a 5-cycle σ and a transposition τ in $\mathrm{Gal}(E/\mathbb{Q})$. For $i = -4, -3, \cdots, 3, 4$, $\sigma^{-i}\tau\sigma^i$ is a distinct transposition, so we see that $\langle \sigma, \tau \rangle$ contains all the transpositions in S_5. Since any element of S_5 can be written as a product of transpositions, we have $\langle \sigma, \tau, \rangle = S_5$. Since $\sigma, \tau \in \mathrm{Gal}(E/\mathbb{Q})$, $\mathrm{Gal}(E/\mathbb{Q}) = S_5$. Thus the Galois group of $f(x)$ is S_5, which is not solvable, so $f(x)$ is not solvable by radicals.

As the example shows, it can be somewhat difficult to show a polynomial has S_n as its Galois group. The easiest way is to confirm that generators of S_n are in the Galois group, but this is not always easy.

As we have seen, Galois Theory allows for an elegant correspondence between subgroups and subfields. In addition, Galois Theory lets us view field automorphisms as permutations of roots of irreducible polynomials, which is very useful. Finally, Galois Theory gave us the tools to prove the insolvability of the general quintic equation.

References

[1] Dummit, David S., and Richard M. Foote. *Abstract Algebra*. 3rd ed. Hoboken, NJ: John Wiley and Sons, Inc, 2004.

[2] Fraleigh, John B., *A First Course in Abstract Algebra*. 7th ed. Boston: Addison Wesley, 2003.

[3] MacLane, Saunders, and Garrett Birkhoff, *Algebra*. 2nd ed. New York: MacMillan Publishing Co., Inc., 1979

[4] Pinter, Charles C., *A Book of Abstract Algebra*. New York: McGraw Hill, 1982.