RUDIMENTARY GALOIS THEORY

JACK LIANG

Abstract. This paper introduces basic Galois Theory, primarily over fields with characteristic 0, beginning with polynomials and fields and ultimately relating the two with the Fundamental Theorem of Galois Theory. This paper then applies Galois Theory to prove Galois's Theorem, describing the relationship between the Galois groups of polynomials and their solvability by radicals.

Contents

1. Introduction

In this paper, we will explore Galois Theory in an attempt to relate field extensions with groups. This will ultimately be used to find the connection between the solvability of polynomials and the solvability of their Galois groups. We will assume a basic knowledge of algebra, primarily in the areas of groups and fields, however, not much beyond the basic definitions is necessary for the purposes of this paper. Much of the beginning sections of this paper is useful for developing intuition about polynomials and fields- while some of the early theorems may not directly be necessary for understanding Galois Theory, such theorems were included because it makes the application of some of the later theorems easier. The middle section of this paper is devoted to proving the Fundamental Theorem of Galois Theory, which I have broken into two parts because of its length. The final section is a very useful application of Galois Theory.

I have chosen to include several fairly lengthy examples because I believe that reading the theorems is not sufficient for understanding Galois Theory, rather, it is the worked out examples that are the greatest learning tool. Note that some lemmas necessary to prove certain theorems are asserted, particularly in the final section of the paper. Whenever an assertion was made, I was sure to include a note explaining why the assertion was necessary.

2. Basic Algebra and Polynomials

Definition 2.1 (Primitive and Monic Polynomials): A polynomial with coefficients in a unique factorization domain is **primitive** if the greatest common divisor of its coefficients is 1, and a polynomial is **monic** if its leading coefficient is 1.

Definition 2.2 (Irreducible and Separable Polynomial): Given a field F, a polynomial $p(x)$ with coefficients in F of degree $d \geq 1$ is **irreducible** if there exists no factorization $p(x) = f(x)g(x)$ for nonconstant $f, g \in F[x]$. A polynomial with coefficients is **separable** if its roots are distinct and in the algebraic closure of F.

Theorem 2.3 (Gauss' Lemma): The product of two primitive polynomials is itself primitive.

Proof: Proof by contradiction: Suppose f and g are primitive, but their product fg is not. This implies that there exists a prime p that divides all of the coefficients of fg. Because f and g are primitive, not all their coefficients are divisible by p. Let $a_r x^r$ and $b_s x^s$ be the terms of greatest power in f and g respectively that have coefficients not divisible by p.

Consider the coefficient of the x^{r+s} term in fg. Its value is given by

$$\sum_{r+s=i+j} a_i b_j.$$

Note that for $i = r$ and $j = s$ that $a_i b_j$ is not divisible by p, as neither a_r or b_s are divisible by p. However, as $a_r x^r$ and $b_s x^s$ are the first terms in f and g respectively not divisible by p, for $i > r$ we have that p divides a_i and thus divides $a_i b_j$ and for $i < r$ we have that $j > s$ and thus that p divides b_j, implying that p divides $a_i b_j$. Thus, every other term in the sum is divisible by p, so the sum cannot be divisible by p. This contradicts the fact that every coefficient in fg is divisible by p. Thus, fg must be primitive.

□

Lemma 2.4: Every polynomial $f \in \mathbb{Q}[x]$ can be uniquely factored up to a unit in $\mathbb{Z}$ as $f = cf_0$, where $c \in \mathbb{Q}$ and f_0 is a primitive integer polynomial.

Proof: We can see that $mf \in \mathbb{Z}[x]$ if we set m equal to the least common multiple of the denominators of the coefficients of f. If we now factor out the greatest common divisor of the remaining coefficients we can see that $mf = nf_0$, with f_0 being primitive. Thus, $f = \frac{m}{n} f_0$, which proves existence.

Now suppose that $cf_0 = df_1$, with $c, d \in \mathbb{Q}$ and f_0, f_1 primitive. Multiply by the least common multiple of the denominators of c and d to get $c' f_0 = d' f_1$, with $c', d' \in \mathbb{Z}$. It must be true that c' is the greatest common divisor of the coefficients of $c' f_0$, analogously, d' is the greatest common divisor of the coefficients in $d' f_1$. This implies that $c' = \pm d'$, which implies that $f_0 = \pm f_1$, which proves uniqueness up to a unit of $\mathbb{Z}$.

Theorem 2.5 (Corollary to Gauss' Lemma): If a primitive polynomial $p(x) \in \mathbb{Z}[x]$ cannot be factored as a product of two nonconstant polynomials, then $p(x)$ cannot be factored as such in $\mathbb{Q}[x]$.

Proof: Proof by contradiction. Assume that a primitive polynomial $f \in \mathbb{Z}[x]$ cannot be factored as a product of two nonconstant polynomials in $\mathbb{Z}$ but can be written $f = gh$, where $g, h \in \mathbb{Q}[x]$ and both ∂g and ∂h are greater than zero. By the previous lemma, we can see that $g = c_1 g_0$ and $h = c_2 h_0$, with $c_1, c_2 \in \mathbb{Q}$ and g_0, h_0 primitive in $\mathbb{Z}$. By Gauss's Lemma, we can see that $g_0 h_0$ is primitive in $\mathbb{Z}$. Thus, $f = c_1 c_2 g_0 h_0$. However, it must be true that $c_1 c_2$ is equal to the greatest common denominator of the coefficients of f, which is 1 because f is primitive. Thus, we can see that $g_0 h_0 = f$ is a nonconstant factorization of f in $\mathbb{Z}[x]$, a contradiction. Thus, f is irreducible in $\mathbb{Q}$.

□

The Corollary to Gauss' Lemma results in the following , which is a useful way to determine whether or not polynomials are irreducible in $\mathbb{Q}$.

Theorem 2.6 (Eisenstein's Criterion): Let polynomial $f \in \mathbb{Z}[x]$ be $f(x) = a_0 + a_1 x + ... + a_n x^n$. If there exists a prime p such that p divides $a_0, a_1 ... a_{n-1}$, p^2 does not divide a_0, and p does not divide a_n, then f is irreducible over $\mathbb{Q}$.

Proof: Proof by contradiction. Assume that f satisfies the named criteria, but is reducible in $\mathbb{Q}[x]$. It follows from the contrapositive of the Corollary to Gauss' Lemma that f can be factored as the product of two nonconstant polynomials in $\mathbb{Z}[x]$. Let $f = gh = (b_0 + b_1 x + ... + b_j x^j)(c_0 + c_1 x + ... + c_k x^k)$. By assumption, p divides a_0, so p divides $b_0 c_0$. However, because p^2 does not divide $b_0 c_0$, p divides either b_0 or c_0, but not both. Without loss of generality, let p divide c_0.

The leading coefficient a_n is not divisible by p, so p does not divide either b_j or c_k. Consider the first coefficient not divisible by p in h, and denote it c_i. If $i < n$, then p divides a_i.

Consider $a_i = b_0 c_i + b_1 c_{i-1} + ... + b_i c_0$. This makes $b_0 c_i = a_i - (b_1 c_{i-1} + ... + b_i c_0)$. However, each $c_0 ... c_{i-1}$ must be divisible by p, and a_i is also divisible by p, so $b_0 c_i$ is divisible by p. This is a contradiction, as neither b_0 nor c_i is divisible by p.

□

Definition 2.7 (Ideals): An **ideal** I of ring R is a subset such that if $a, b \in I$ then $a - b \in I$ and $ab \in I$. An ideal is a **proper ideal** if $I \neq R$. An ideal is a **prime ideal** if $ab \in I$ implies that $a \in I$ or $b \in I$. A **principal ideal** is an ideal generated by one element, i.e., the prinicple ideal for an element $a \in R$ is the set $\{ra \mid r \in R\}$ and is typically denoted (a).

Definition 2.8 (Quotient Rings): The **cosets** of an ideal I in a ring R are sets in the form $r + I = \{r + s \mid s \in I\}$. A **quotient ring** is the set of equivalence classes between cosets.

Example 2.9: The quotient ring $\mathbb{R}[x]/(x^2 + 1)$ we have that $x^2 + 1 \equiv 0$, or, that $x \equiv \pm i$. In this way, the set of equivalence classes for this ring is naturally isomorphic to $\mathbb{C}$, as they are all written in the form $[a + bi]$.

The previous example leads us to think about fields similar to $\{a + bi \mid a, b \in \mathbb{R}\} = \mathbb{C}$. Note that we did not need to let a and b be in $\mathbb{R}$, we could have just

as easily let them be in $\mathbb{Q}$ and gotten a comparable result. This brings us to the following definition.

Definition 2.10 (Field Extensions): A field E is known as a **field extension** of another field F if F is a subfield of E. We write E/F to indicate that E is a field extension of F. We can create a field extensions from a given field by **adjoining** an element, which is denoted by $F(\alpha)$ (read "F adjoin α"). Here, $F(\alpha)$ is the smallest extension of F that contains α. Note that we can also adjoin lists of elements, for example, $F(\alpha_1, \alpha_2)$ is the smallest extension of F that contains both α_1 and α_2. We call an extension **simple** if it is generated by one element.

Example 2.11: Consider the field $\mathbb{Q}[x]/(x^2 - 2)$. Following a similar process as before, we can see that this field is isomorphic to $\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} \mid a, b \in \mathbb{Q}\} \subset \mathbb{R}$. Here, we see that $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{R} \subset \mathbb{C}$. In this case, $\mathbb{R}$ and $\mathbb{C}$ are field extensions of $\mathbb{Q}(\sqrt{2})$ whereas $\mathbb{Q}$ is a subfield of $\mathbb{Q}(\sqrt{2})$. Visually:

$$\begin{tikzcd}
\mathbb{C} \arrow[d, dash] \\
\mathbb{R} \arrow[d, dash] \\
\mathbb{Q}(\sqrt{2}) \arrow[d, dash] \\
\mathbb{Q}
\end{tikzcd}$$

3. Fields and Field Extensions

Definition 3.1 (Algebraic and Transcendental): Let E/F be a field extension and let $\alpha \in E$. We call α **algebraic** over F if α is a root of some polynomial in $F[x]$. If α is not a root of any polynomial, we call α **transcendental**. We call the field extension E/F algebraic if every $\alpha \in E$ is algebraic over F.

Definition 3.2 (Degree): The **degree** of a field extension E/F is equal to the dimension of E viewed as a vector space over F. If the degree of E/F, denoted by $[E : F]$, is finite, then E/F is considered to be a **finite field extension**.

Example 3.3: Returning to our previous example of the field created by $\mathbb{Q}(\sqrt{2})$, we can see that when viewing $\mathbb{Q}(\sqrt{2})$ as a vector space over $\mathbb{Q}$ the dimension of such a vector space is 2 (because 1 and $\sqrt{2}$ form a basis). Thus, $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

However, we know that there exist infinitely many transcendentals in $\mathbb{R}$ over $\mathbb{Q}$, thus, $[\mathbb{R} : \mathbb{Q}]$ is not finite.

Finally, we can see that $\mathbb{C}$ as a vector space over $\mathbb{R}$ has a dimension of 2 (as 1 and i form a basis), thus, $[\mathbb{C} : \mathbb{R}] = 2$.

We will now attempt to gain some intuition about the degree of a field extension. The following lemma and theorem connect degrees of field extensions to degrees of polynomials.

Lemma 3.4: If F is a field, then $F[x]$ is a principal ideal domain (all ideals are generated by a single element).

Proof: Let $I \subset F[x]$ be an ideal. We wish to show that I is generated by one element. If $I = 0$, clearly, I is generated by the element 0. If $I \neq 0$, then let $p \in F[x]$ be a non-zero polynomial of minimal degree; we will prove that p generates I i.e., $I = (p)$.

Consider some $g \in I$. We can divide g by p using the division algorithm to yield $g = qp + r$, for a particular quotient q and remainder r of degree strictly less than that of p. However, we can see that $r = g - qp \in I$, so making p minimal forces r to be 0. Thus, $g = qp \in (p)$. Because $g \in I$ was arbitrary, $I = (p)$.

Lemma 3.5: Let E/F be a field extension and let $p(x) \in F[x]$ be a monic irreducible polynomial with $\alpha \in E$ as a root. Then $\partial p \leq \partial f$ for every $f(x) \in F[x]$ with α as a root and $p(x)$ is, up to factors of constants, the only polynomial in $F[x]$ with degree ∂p that has α as a root. Note that this $p(x)$ is known as the **minimal polynomial** for α.

Proof: By Lemma 3.4, $F[x]$ is a principal ideal domain. Let I be the set defined by $I = \{f(x) \in F[x] \mid f(\alpha) = 0\}$. It is trivial to show that I is an ideal. Let f be an element of I. We can see that because p is irreducible, its only monic divisors are 1 and p. However, $1 \notin I$, as α is not a solution to the polynomial 1, so the generator for the ideal must be p. Thus, p divides f, so $\partial p \leq \partial f$.

Now let $q(x)$ be a monic polynomial in I such that $\partial q = \partial q$. We can see that $p - q$ is a polynomial in I with degree less than ∂p. However, if $p - q \neq 0$, then we would have a polynomial of degree less than the degree of p with α as a solution, contradicting the first part of the proof. Thus, $p - q = 0$, or, all polynomials with degree equal to p that have α as a root are equal to p.

□

Theorem 3.6: Let $p(x) \in F[x]$ be an irreducible polynomial of degree d. Then the field $E = F[x]/(p(x))$ is a field extension of F with degree d.

Proof: Consider the ideal generated by $p(x)$, which we will call I and some $\alpha \in E$ which is a root of p. We will prove that $\{1, \alpha, \alpha^2 ... \alpha^{d-1}\}$ is a basis for the vector space E with respect to F.

To prove linear independence, suppose that $c_0 + c_1\alpha + ... + c_{d-1}\alpha^{d-1} = 0$. This means that there exists a polynomial of degree $d - 1$ with alpha as a root, contradicting the lemma. Thus, it must be true that all such c are 0, thus, $\{1, \alpha ... \alpha^{d-1}\}$ are linearly independent.

To prove that $\{1, \alpha, ... \alpha^{d-1}\}$ span E, note that every $g \in E$ has the form $f + I$. By the division algorithm for polynomials, we see that $f(x) = q(x)p(x) + r(x)$, with $\partial r < \partial p$. Thus, $f(x) + I = r(x) + I$. Evaluating at α, we can see that $\{1, \alpha ... \alpha^{d-1}\}$ spans $r(\alpha) + I$. Thus, every polynomial in E is in the span of $\{1, \alpha, ... \alpha^{d-1}\}$.

Because $\{1, \alpha, ...\alpha^{d-1}\}$ are linearly independent and span E, they form a basis for E. Thus, the degree of $E/F = |\{1, \alpha...\alpha^{d-1}\}| = d$.

□

Theorem 3.7 (Tower Theorem): If $F \subset E \subset D$ are fields and $[D : E]$ and $[E : F]$ are finite, then $[D : F]$ is also finite with degree equal to $[E : F] \cdot [D : E]$.

Proof: Let the degree of $[E : F] = n \in \mathbb{N}$ and $[D : E] = m \in \mathbb{N}$. Consider bases $a_1...a_n$ for E over F and $b_1...b_m$ for D over E.

We will demonstrate that the basis $a_i b_j$ for $1 \leq i \leq n$ and $1 \leq j \leq m$ form a basis of $n \cdot m$ elements for D over F. To prove linear independence, suppose there exist α_{ij} such that

$$\sum_{i=1}^{n} \sum_{j=1}^{m} \alpha_{ij} a_i b_j = 0.$$

We will prove that all α_{ij} must be equal to zero. However, we can write this as

$$\sum_{j=1}^{m} \left(\sum_{i=1}^{n} \alpha_{ij} a_i \right) b_j.$$

Because all b_j are linearly independent (because they form a basis for D over E), we know that each coefficient of each b_j term is equal to zero, or, that

$$\sum_{i=1}^{n} \alpha_{ij} a_i = 0 \text{ for all } 1 \leq i \leq n.$$

However, we know that all a_i are linearly independent as they form a basis for E over F, so it must be true that all such $\alpha_{ij} = 0$. Thus, the elements of our set $\{a_i b_j \mid 1 \leq i \leq n \text{ and } 1 \leq i \leq m\}$ are linearly independent.

To prove that our chosen set spans D, consider some $d \in D$. Because $b_1...b_m$ span D as a vector space over E, we can write

$$d = \beta_1 b_1 + ... + \beta_m b_m = \sum_{j=1}^{m} \beta_j b_j.$$

Because $a_1...a_n$ span E as a vector space over F, we can write each β_j as

$$\beta_j = \alpha_{1j} a_1 + \alpha_{2j} a_2 + ... + \alpha_{nj} a_n = \sum_{i=1}^{n} \alpha_{ij} a_i.$$

Substituting, we see that

$$d = \sum_{j=1}^{m} \left(\sum_{i=1}^{n} \alpha_{ij} a_i \right) b_j = \sum_{i=1}^{n} \sum_{j=1}^{m} \alpha_{ij} a_i b_j,$$

which is a linear combination of our basis vectors. Thus, D is spanned by our set.

Thus, the set $\{a_i b_j \mid 1 \leq i \leq n \text{ and } 1 \leq i \leq m\}$ is linearly independent and spans D, so the dimension of D as a vector space over F is $n \cdot m$. Thus, $[D : F] = n \cdot m = [E : F] \cdot [D : E]$.

□

4. Galois Theory

Definition 4.1 (Galois Group): Let E/F be a finite field extension. Then the **Galois Group** denoted by $\mathrm{Gal}(E/F)$ is the set

$$\{\sigma : E \to E \mid \sigma \text{ is an automorphism with } \sigma(a) = a \text{ for all } a \in F\}.$$

As suggested, the Galois Group is a group under the operation given by composition and is a finite group.

Example 4.2: Consider the field extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$. Trivially, we see that the identity map $i_{\mathbb{Q}(\sqrt{2})}$, which maps $a + b\sqrt{2}$ to $a + b\sqrt{2}$ is a member of the Galois Group. Furthermore, we see that the map σ which maps $a+b\sqrt{2}$ to $a-b\sqrt{2}$ is also in the Galois Group, as all $\sigma(x) = x$ for all $x \in \mathbb{Q}$.

We can also see that the set of automorphisms that fix $x \in \mathbb{Q}$ need to map $\sqrt{2}$ to $\pm\sqrt{2}$, thus, these are the only two elements in the Galois Group. So $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{i_{\mathbb{Q}(\sqrt{2})}, \sigma\}$.

Definition 4.3 (Splitting Fields and Fixed Fields): A **splitting field** of $f(x) \in F[x]$ is the smallest field extension E/F in which $f(x)$ can decompose into linear factors. Let a subset of automorphisms on a field E be called G. Then the **fixed field** E^G is defined by all elements fixed by every automorphism in G, i.e., $E^G = \{\alpha \in E \mid \sigma(\alpha) = \alpha \text{ for all } \sigma \in G\}$.

The following theorem will demonstrate that finite separable extensions are generated by one element, which in turn will help prove a theorem useful for developing some primary intuition about the Galois Group and its relation with fields between E and F, where E/F is a field extension. Such fields K with $F \subset K \subset E$ are called **intermediate fields**.

Theorem 4.4 (Theorem of the Primitive Element): Let $F \subset E = F(\alpha_1 ... \alpha_n)$ be a finite extension, with each α_i being separable over F. Then there exists $\gamma \in E$ that has the property that $F(\gamma) = E$. This γ is called the **primitive element**. Note that for the sake of simplicity, this proof will be written for fields of characteristic 0, however, this theorem applies for finite fields as well.

Proof: Let $E = F(\alpha_1 ... \alpha_n)$, with each α_i being separable over F. We will inductively prove that there exist $a_1 ... a_n \in F$ such that $F(a_1\alpha_1 + ... + a_n\alpha_n) = E$.

Base case: n=2. Let $E = F(\alpha_1, \alpha_2)$, and consider the minimal polynomials $f, g \in F[x]$ for α_1 and α_2 respectively. Note that f and g are both separable over F. Let the degree of f be $\partial f = n$ and the degree of g be $\partial g = m$. Because f and g are separable, there exist distinct roots $f_1 ... f_n$ of f and $g_1 ... g_m$ of g. Let $\alpha_1 = f_1$ and $\alpha_2 = g_1$.

Because F is infinite by assumption, we can see that there exists $k \in F$ such that $\alpha_1 + k\alpha_2 \neq f_i + kg_j$ for $1 \leq i \leq n$ and $2 \leq j \leq m$. We will prove that $F(\alpha_1 + k\alpha_2) = E$.

Obviously, $F(\alpha_1 + k\alpha_2) \subset E$. To prove the other direction, we must show that α_1 and α_2 are both contained in $F(\alpha_1 + k\alpha_2)$, which will be sufficient to

show that $F(\alpha_2 + k\alpha_2)$ generates E. First consider α_2. Note that the greatest common divisor of g and $f(\alpha_1 + k\alpha_2 - kx) \in F(\alpha_1 + k\alpha_2)[x]$ must be a polynomial of degree of at least one. This is true, because else, there would exist polynomials $f', g' \in F(\alpha_1 + k\alpha_2)[x]$ such that $gg' + f'f(\alpha_1 + k\alpha_2 - kx) = 1$. However, evaluating this at $x = \alpha_2$ yields $(0)g' + (0)f' = 1$, or, $0 = 1$, clearly a contradiction. So there exists $h = \gcd(f(\alpha_1 + k\alpha_2 - kx), g)$ such that $\partial h \geq 1$.

We can see that if $\partial h > 1$, we have that there exists some root of g not equal to α_2 that is also a root of $f(\alpha_1 + k\alpha_2 - kx)$, however, this contradicts our construction of k above. Thus, $\partial h = 1$. In particular, $h = x - \alpha_2$, as it must have α_2 as a root. We know that $h \in F(\alpha_1 + k\alpha_2)[x]$, so $\alpha_2 \in F(\alpha_1 + k\alpha_2)$. Thus, we can clearly also see that $\alpha_1 = (\alpha_1 + k\alpha_2) - k \cdot \alpha_2 \in F(\alpha_1 + k\alpha_2)$, so we have that $F(\alpha_1 + k\alpha_2) = F(\alpha_1, \alpha_2)$.

Inductive step: Let $n = m > 2$. By the inductive hypothesis, we can see that $E = F(\alpha_1 ... \alpha_m)$. By assumption, we can find some γ_0 such that $F(\alpha_1 ... \alpha_{m-1}) = F(\gamma_0)$. Thus, we see that $E = F(\gamma_0, \alpha_m)$. However, for the $n = 2$ case we have already demonstrated that a field generated by two elements can be generated by a primitive element, γ. Thus, we have found the desired primitive element by the base case. By the inductive hypothesis, our proof is complete.

□

Theorem 4.5: If E is the splitting field of a separable polynomial f in $F[x]$, then the Galois group of $F \subset E$ has cardinality $|\mathrm{Gal}(E/F)| = [E : F]$.

Proof: First, we will prove that $E = F(\alpha_1 ... \alpha_n)$, with $\alpha_1 ... \alpha_n$ being the roots of f. We have that E is the smallest field with $F(\alpha_1 ... \alpha_n) \subset E$ because F splits in E. Each α_i is clearly separable over F. By the Theorem of the Primitive Element, there exists $\gamma \in E$ that is separable over F such that $E = F(\gamma)$. Let g be the minimal polynomial for γ.

By Theorem 3.5, because g is the minimal polynomial for γ and $E = F(\gamma)$, we can see that $[E : F] = \partial g \equiv d$. We must now demonstrate that $\mathrm{Gal}(E/F)$ has d elements.

Because g is the minimal polynomial for γ with degree d, there exists $\gamma = \gamma_1, \gamma_2 ... \gamma_d$ distinct roots of g contained in E. Because E is the splitting field over F, there exist automorphisms σ_i such that $\sigma_i(\gamma) = \gamma_i$ for $1 \leq i \leq d$. Note that in this case, σ_1 is the identity, while each of the others simply permutes the roots of g. Thus, there exist at least d elements in the Galois group.

To show that there exist no other such elements in the Galois group, we can see that any σ in the Galois group must send γ to one of the other roots. This is equivalent to the permutations listed above. Thus, there are no additional elements in the Galois group, so $|\mathrm{Gal}(E/F)| = d = [E : F]$.

□

Theorem 4.6: The following conditions are equivalent for a finite field extension E/F with Galois group $G = \mathrm{Gal}(E/F)$.

(1) $F = E^{\mathrm{Gal}(E/F)}$.
(2) Every irreducible polynomial $p(x) \in F[x]$ with one root in E is separable and has all its roots in E.
(3) E is a splitting field of some separable polynomial $f(x) \in F[x]$.

A finite extension E/F is called **Galois** if it satisfies any of the previous equivalent conditions.

Proof: We will prove that the first statement implies the second, the second implies the third, and the third implies the first, demonstrating equivalence.

$1 \implies 2$: Consider an irreducible polynomial p such that there exists $\alpha \in E$ with $p(\alpha) = 0$. Then, $F(\alpha)$ is isomorphic to the quotient field of $F[x]/(p(x))$. Thus, there must be exactly e embeddings from $F(\alpha)$ into the algebraic closure of F, where e is the number of distinct roots of p in the algebraic closure of F.

Suppose that there exist e' embeddings with image inside E. Then $[E : F] = |\mathrm{Gal}(E/F)| \leq e' \cdot [E : F(\alpha)]$. Thus, $[F(\alpha) : F] \leq e'$ by the Tower Theorem, so the degree of $\partial p \leq e'$. However, it must be true that $e' \leq \partial p$, because p has at most ∂p distinct roots and thus can have at most ∂p embeddings. Thus, $\partial p = e'$. Thus, we can see that $e = e'$ and $e = \partial p$, which implies that p is separable and has all of its roots in E.

$2 \implies 3$: Consider some $\alpha_1 \in E$ such that $\alpha_1 \notin F$. Because E/F is finite, α_1 must be algebraic over F, thus, there exists an irreducible polynomial $p_1(x) \in F[x]$ with α_1 as a root. By assumption, p_1 is separable; let K_1 be its splitting field. If $K_1 = E$, the third condition is satisfied.

If not, consider another $\alpha_2 \in E$ with $\alpha_2 \notin F$. Repeating the process above, find irreducible $p_2 \in F[x]$ with α_2 as a root. The new polynomial $p_1 p_2 \in F[x]$ will have both α_1 and α_2 as roots, let K_2 be the splitting field of $p_1 p_2$, again, if $K_2 = E$ we have satisfied the third condition.

This process will terminate after a finite number of iterations because the degree of E/F is finite, thus, repeating this process a total of $[E : F] = n$ times will produce a polynomial $p_1 p_2 ... p_n \in F[x]$ whose splitting field is E.

$3 \implies 1$: By Theorem 4.5, $|\mathrm{Gal}(E/F)| = [E : F]$. We will now prove that that $|\mathrm{Gal}(E/F)| = [E : E^{\mathrm{Gal}(E/F)}]$.

Consider $\sigma_1 ... \sigma_n \in \mathrm{Gal}(E/F)$. Clearly, $[E : E^{\mathrm{Gal}(E/F)}] \leq n = |\mathrm{Gal}(E/F)|$. Furthermore, each authomorphism in the Galois group will fix exactly one such field, resulting in a vector space of exactly n dimensions for E over $E^{\mathrm{Gal}(E/F)}$. Thus, $|\mathrm{Gal}(E/F)| = [E : E^{\mathrm{Gal}(E/F)}]$.

This implies that $[E : F] = [E : E^{\mathrm{Gal}(E/F)}]$. By definition, $F \subset E^{\mathrm{Gal}(E/F)}$, so we must have that $F = E^{\mathrm{Gal}(E/F)}$.

$\square$

Corollary 4.7: If E/F is Galois, and there exists K such that $F \subset K \subset E$, then E/K is also Galois.

Proof: If $F \subset E$ is Galois, then E is the splitting field of a particular separable polynomial $f \in F[x]$. Because $F \subset K$, when we consider $f \in K[x]$, we can see that E must still be the splitting field of f. Thus, E/K is also Galois.

Theorem 4.8 (Fundamental Theorem of Galois Theory, part 1): Let $F \subset E$ be a normal extension. Then for any intermediate field $F \subset K \subset E$, we have that E/K is Galois and its Galois group $\mathrm{Gal}(E/K)$ is a subgroup of $\mathrm{Gal}(E/F)$. Also, $[\mathrm{Gal}(E/F) : \mathrm{Gal}(E/K)] = [K : F]$.

Proof: We can see that if $F \subset E$ is Galois, then $K \subset E$ is also Galois by Theorem 4.6. We have that $K = E^{\mathrm{Gal}(E/K)}$ by Theorem 4.6.

Because $K \subset E$ and $F \subset E$ are both Galois, we can see by Theorem 4.5 that $|\mathrm{Gal}(E/K)| = [E : K]$ and $\mathrm{Gal}(E/F)| = [E : F]$. Using the Tower Theorem, we see that $[E : F] = [K : F] \cdot [E : K]$. Thus

$$[K : F] = \frac{[E : F]}{[E : K]} = \frac{|\mathrm{Gal}(E : F)|}{|\mathrm{Gal}(E : K)|} = [\mathrm{Gal}(E/F) : \mathrm{Gal}(E/K)].$$

□

Theorem 4.9 (Fundamental Theorem of Galois Theory, part 2): Let $F \subset E$ be a Galois extension. Then the maps between the set of intermediate fields $F \subset K \subset L$ and the set of subgroups $H \subset \mathrm{Gal}(E/F)$ given by

$$K \mapsto \mathrm{Gal}(E/K) \text{ and } H \mapsto E^H$$

are one to one and are inverses of each other. This correspondence reverses inclusions.

Furthermore, if a subfield K corresponds to a subgroup H under these maps, then K is Galois over F if and only if H is normal in $\mathrm{Gal}(E/F)$, and when this happens, there is a natural isomorphism

$$\mathrm{Gal}(E/F)/H \cong \mathrm{Gal}(K/F).$$

Proof: To prove that the maps are inverses of eacth other and reverse inclusions, consider the compositions of the maps. First, we have that

$$K \mapsto \mathrm{Gal}(E/K) \mapsto E^{\mathrm{Gal}(E/K)},$$

however, because E/K is Galois by Corollary 4.7, we have that $E^{\mathrm{Gal}(E/K)} = K$. Thus:

$$K \mapsto \mathrm{Gal}(E/K) \mapsto K.$$

Analogously, we have that

$$H \mapsto E^H \mapsto \mathrm{Gal}(E/E^H),$$

however, again, by the Fundamental Theorem of Galois Theory we have that $\mathrm{Gal}(E/E^H) = H$. Thus:

$$H \mapsto E^H \mapsto H.$$

This demonstrates that the two maps are inverses of each other. We can also see that the fixed field generated by a larger H is smaller than the fixed field generated

by a smaller H because a larger subfield of the Galois group fixes less elements in F. Thus, we can see that these inverses reverse inclusions, i.e.,

$$K_1 \subset K_2 \subset E \implies \mathrm{Gal}(E/K_1) \supset \mathrm{Gal}(E/K_2).$$

□

Note that the final portion of the previous proof was omitted because it relied on two lengthy lemmas- for complete proofs consult *Galois Theory* by David A. Cox under the section "Normal Subgroups and Normal Extensions". The proof should follow naturally from the theorems in this section.

Example 4.10: Consider the polynomial $x^3 - 2 \in \mathbb{Q}[x]$. Clearly, the splitting field for this polynomial is $\mathbb{Q}(\omega, \sqrt[3]{2})$, where ω is the third root of unity. We construct the following field diagram to illustrate the relationship between $\mathbb{Q}$ and its extension:

$$\begin{tikzcd}
 & & \mathbb{Q}(\omega, \sqrt[3]{2}) \arrow[dll, dash] \arrow[dl, dash] \arrow[dr, dash] \arrow[drr, dash] & & \\
\mathbb{Q}(\omega) \arrow[drr, dash] & \mathbb{Q}(\sqrt[3]{2}) \arrow[dr, dash] & & \mathbb{Q}(\omega\sqrt[3]{2}) \arrow[dl, dash] & \mathbb{Q}(\omega^2\sqrt[3]{2}) \arrow[dll, dash] \\
 & & \mathbb{Q} & &
\end{tikzcd}$$

We can see that any element $\sigma \in \mathrm{Gal}(\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q})$ has the following properties:

$$\sigma(\omega) \in \{\omega, \omega^2\} \text{ and } \sigma(\sqrt[3]{2}) \in \{\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}\}.$$

This thus shows us explicitly the 6 elements in our Galois group. We know that there must be six elements because $[\mathbb{Q}(\omega, \sqrt[3]{2}) : \mathbb{Q}] = 6$.

Consider $\sigma_1 : \mathbb{Q}(\omega, \sqrt[3]{2}) \to \mathbb{Q}(\omega, \sqrt[3]{2})$ such that $\sigma_1(\omega) = \omega$ and $\sigma_1(\sqrt[3]{2}) = \omega\sqrt[3]{2}$. Now consider $\sigma_2 : \mathbb{Q}(\omega, \sqrt[3]{2}) \to \mathbb{Q}(\omega, \sqrt[3]{2})$ such that $\sigma_2(\omega) = \omega^2$ and $\sigma_2(\sqrt[3]{2}) = \sqrt[3]{2}$. Note that these two automorphisms characterize all permutations of the roots of $x^3 - 2$ in that σ_1 sends $\sqrt[3]{2}$ to $\omega\sqrt[3]{2}$ to $\omega^2\sqrt[3]{2}$ and back, while σ_2 sends $\omega\sqrt[3]{2}$ to $\omega^2\sqrt[3]{2}$ and back.

Now, note that σ_1 and σ_2 generate subgroups of the Galois group $\mathrm{Gal}(\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q})$. For instance, compositions of σ_1 form a cycle with three elements, the identity, σ_1, and σ_1^2, while compositions of σ_2 form a cycle of two elements, the identity and σ_2.

Composing both σ_1 and σ_2, we see that $\sigma_1\sigma_2$ forms a cycle with 2 elements similar to σ_2, as does $\sigma_1^2\sigma_2$. Each of these is a **cyclic group** (the group itself is denoted by $\langle\sigma\rangle$) and is isomorphic to $\mathbb{Z}/n\mathbb{Z}$, for $n = 3$ for σ_1 and $n = 2$ for the rest.

$$\begin{tikzcd}
 & \{identity\} \arrow[dl, dash] \arrow[d, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\langle\sigma_1\rangle \arrow[dr, dash] & \langle\sigma_2\rangle \arrow[d, dash] & \langle\sigma_1^2\sigma_2\rangle \arrow[d, dash] & \langle\sigma_1\sigma_2\rangle \arrow[dl, dash] \\
 & \mathrm{Gal}(\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q}) &
\end{tikzcd}$$

Now notice the correspondence between $\mathbb{Q}(\omega)$ and $\langle\sigma_1\rangle$; when $a + b\sqrt[3]{2} + c\omega + d\sqrt[3]{2}^2 + e\omega\sqrt[3]{2} + f\omega\sqrt[3]{2}^2 + g\omega^2\sqrt[3]{2} + h\omega^2\sqrt[3]{2}^2$ undergoes the permutation σ_1, the only terms that remain fixed are a and $c\omega$. The field generated by $\{a + c\omega \mid a, c \in \mathbb{Q}\}$ is clearly $\mathbb{Q}(\omega)$. If we repeat this process, we see that $\mathbb{Q}(\sqrt[3]{2})$ corresponds with σ_2, $\mathbb{Q}(\omega\sqrt[3]{2})$ corresponds with $\sigma_1^2\sigma_2$, and $\mathbb{Q}(\omega^2\sqrt[3]{2})$ corresponds with $\sigma_1\sigma_2$.

This demonstrates the Fundamental Theorem of Galois Theory, as we have established a connection between subgroups of $\mathrm{Gal}(\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q})$ and the intermediate fields between $\mathbb{Q}$ and $\mathbb{Q}(\omega, \sqrt[3]{2})$.

5. An Application of Galois Theory

We will now apply Galois Theory to the solvability of polynomials by radicals, that is to say, determining whether or not the roots to a polynomial can be written using only some combination of $+$, $-$, $\times$, $\div$ and $\sqrt[n]{}$. To answer this question simply, no, in general polynomials of degree greater than 4 cannot be written in this way; the proof of this is perhaps one of the most important applications of Galois Theory. In the following section, all fields will have characteristic 0.

Definition 5.1 (Galois Closure): Let E be a field extension of F. A field $L \supset E$ is a **Galois Closure** of E/F if L/F is Galois and no proper subfield of L containing E is Galois over F.

We will now introduce the idea of solvable groups and radical extensions. In general, we will apply solvable groups to Galois groups and radical extensions to the fields with which the Galois groups are related to by the Fundamental Theorem of Galois Theory.

Definition 5.2 (Solvable Groups): A finite group G is solvable if there exist subgroups

$$\{e\} = G_n \subset G_{n-1} \subset ... \subset G_0 = G$$

such that, for $1 \leq i \leq n$ we have that G_i is normal in G_{i-1} and $[G_{i-1} : G_i]$ is prime.

Example 5.3: Consider the groups $\{e\} \subset \{e, (123)(132)\} \subset \{e, (12)(13)(23)(123)(132)\}$, perhaps better known as $\{e\} \subset A_3 \subset S_3$. Each subgroup is clearly normal in the next, and $[A_3 : \{e\}] = 3$ and $[S_3 : A_3] = 2$, which are both primes. Thus, the group S_3 is solvable. Furthermore, all finite Abelian groups are solvable- the proof of this has been excluded for space purposes but follows from Cauchy's Theorem.

Definition 5.4 (Radical Extensions): A field extension E/F is **radical** if there exist fields $F = F_0 \subset F_1 \subset ... \subset F_n = E$ such that, for $1 \leq i \leq n$, we have

$$F_i = F_{i-1}(\sqrt[m_i]{k_i}),\ k_i \in F_{i-1}.$$

We call a field extension $F \subset E$ **solvable** or **solvable by radicals** if there exists a field extension $F \subset E \subset L$ such that $F \subset L$ is radical.

Example 5.5: Consider the field extension $\mathbb{Q}(\sqrt{2}+\sqrt{6})$ over $\mathbb{Q}$. This field, despite not seeming it, is actually radical. We can see that $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$ is obviously a radical extension.

To prove that that $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2}+\sqrt{6})$ is radical, we will prove that $\mathbb{Q}(\sqrt{2})(\sqrt{3})$ is equal to $\mathbb{Q}(\sqrt{2}+\sqrt{6})$. Consider $\sqrt{2}+\sqrt{6} \in \mathbb{Q}(\sqrt{2}+\sqrt{6})$. We can see that $\left(\sqrt{2}+\sqrt{6}\right)^2 = 2+6+2\sqrt{12} = 8+4\sqrt{3}$. Thus, we can see that $\sqrt{3} \in \mathbb{Q}(\sqrt{2}+\sqrt{6})$.

Furthermore, $\sqrt{2} = \frac{\sqrt{2}+\sqrt{6}}{1+\sqrt{3}}$, so $\sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{6})$. Thus, we can see that $\mathbb{Q}(\sqrt{2})(\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{6})$.

Thus, $\mathbb{Q}(\sqrt{2}+\sqrt{6})$ is radical, as it is formed by adjoining $\sqrt{2}$ to $\mathbb{Q}$, and then adjoining $\sqrt{3}$ to $\mathbb{Q}(\sqrt{2})$.

Due to the length of the lemmas required to prove the following theorem, some assertions will be made. I have made a note next to each assertion of a lemma, most can be found in *Galois Theory* by David Cox. I will list the lemmas here as a series of facts, and refer to them in the proof of Galois's Theorem by the fact number.

- Fact 1: If $F \subset E$ is separable and radical, then its Galois closure is also radical.
- Fact 2: Suppose that $F \subset K \subset E$ is a tower of fields, with $F \subset K$ and $F \subset E$ being Galois. Then $\mathrm{Gal}(E/K)$ is a normal subgroup of $\mathrm{Gal}(E/F)$ and there exists an isomorphism between $\mathrm{Gal}(E/F)/\mathrm{Gal}(E/K)$ and $\mathrm{Gal}(K/F)$.
- Fact 3: Let G be a finite group and H a normal subgroup. Then G is solvable if and only if H and G/H are.
- Fact 4: If $F \subset K_1 \subset E$ and $F \subset K_2 \subset E$ and $F \subset K_1$ is radical, then $K_2 \subset K_1K_2$ is also radical.
- Fact 5: Let $F \subset E$ be a Galois extension and ω be a primitive m^{th} root of unity. Then $F \subset E(\omega)$ and $F(\omega) \subset E(\omega)$ are both Galois and the following are equivalent:
  (1) $\mathrm{Gal}(E/F)$ is solvable.
  (2) $\mathrm{Gal}(E(\omega)/F)$ is solvable.
  (3) $\mathrm{Gal}(E(\omega)/F(\omega))$ is solvable.
- Fact 6: Suppose that $F \subset E$ is a Galois extension and $\mathrm{Gal}(E/F)$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ for some prime p. Then if F contains the pth primitive root of unity then there exists some $\alpha \in E$ such that $E = F(\alpha)$ and $\alpha^p \in F$.

Theorem 5.6 (Galois's Theorem): Let $F \subset E$ be a Galois extension. Then $F \subset E$ is a solvable extension if and only if $\mathrm{Gal}(E/F)$ is a solvable group.

Proof: $F \subset E$ is solvable $\implies$ $\mathrm{Gal}(E/F)$ is a solvable group: suppose that $F \subset E$ is a solvable extension, i.e., F is contained in some radical extension K.

The Galois Closure of F contained in K, which we will call M, is also radical over F by Fact 1.

Note that if $\mathrm{Gal}(M/F)$ is solvable, then by Fact 2 there exists an isomorphism between $\mathrm{Gal}(E/F)$ and $\mathrm{Gal}(M/F)/\mathrm{Gal}(M/E)$. By Fact 3 we would then get that, $\mathrm{Gal}(E/F)$ is solvable. Thus, we must only prove that $\mathrm{Gal}(M/F)$ is solvable, which allows us to assume that $F \subset E$ is radical and Galois.

If we assume that $F \subset E$ is radical and Galois, adjoining the mth primitive root of unity ω to both F and E would mean that the resulting extension $F(\omega) \subset E(\omega)$ is also radical by Fact 4. By Fact 5 this extension is also Galois. Thus, if we can show that $\mathrm{Gal}(E(\omega)/F(\omega))$ is solvable, then by Fact 5 we will have shown that $\mathrm{Gal}(E/F)$ is solvable. Thus, we now assume that F contains any m^{th} root of unity.

We will now prove that $\mathrm{Gal}(E/F)$ is solvable, thus completing the first direction of this proof. Because, by assumption, $F \subset E$ is radical, there exists subfields $F = F_0 \subset F_1 \subset ... \subset F_n = E$ such that, for $1 \leq i \leq n$ we get that $F_i = F_{i-1}(\sqrt[m_i]{k_i})$, with $k_i \in F_{i-1}$. By the above, we can also say that F_i contains a primitive m_i^{th} root of unity, which we will call ω_i. Note that $1, \omega_i, \omega_i^2 ... \omega_i^{m_i - 1}$ are distinct m_i^{th} roots of unity. Thus, we can see that the solutions to the polynomial

$$x^{m_1} - k_i \in F_{i-1}[x]$$

are

$$1 \cdot \sqrt[m_i]{k_i},\ \omega_i \cdot \sqrt[m_i]{k_i} ...\ \omega_i^{m-1} \cdot \sqrt[m_i]{k_i}.$$

Because $\omega_i \in F \subset F_{i-1}$, we can see that

$$F_{i-1}(1 \cdot \sqrt[m_i]{k_i},\ \omega_i \cdot \sqrt[m_i]{k_i} ...\ \omega_i^{m-1} \cdot \sqrt[m_i]{k_i}) = F_{i-1}(\sqrt[m_i]{k_i})$$

which demonstrates that F_{i-1} is Galois. We can also clearly see that the Galois Group for the extension $F_{i-1} \subset F_i$ is cyclic, as the group is generated by the element that maps $1 \cdot \sqrt[m_i]{k_i} \mapsto \omega_i \cdot \sqrt[m_i]{k_i}$. Thus, we have proven that $F_{i-1} \subset F_i$ is Galois and has a cyclic Galois Group.

Now consider the subgroups $G_i = \mathrm{Gal}(E/F_i) \subset \mathrm{Gal}(E/F)$. By the fundamental theorem of Galois Theory, the Galois correspondence is inclusion-reversing, thus, we get that

$$\{identity\} = \mathrm{Gal}(E/E) = G_n \subset G_{n-1} \subset ... \subset G_1 \subset G_0 = \mathrm{Gal}(E/F).$$

Because F_{i-1} is an intermediate field of the Galois extension $F \subset E$, we see that $F_{i-1} \subset E$ must be Galois. By our previous proof, we can see that $F_{i-1} \subset F_i$ is also Galois. Thus, by Fact 2, we see that G_i is normal in G_{i-1}, which means that G_{i-1}/G_i is Abelian. Because Abelian groups are solvable, we know by induction on i we can see that it must be true that $\mathrm{Gal}(F_n/F_0) = \mathrm{Gal}(E/F)$ is solvable.

$\mathrm{Gal}(E/F)$ is solvable $\implies$ $F \subset E$ is solvable: Let ω be the mth root of unity, where $m = |\mathrm{Gal}(E/F)|$. By Fact 5, $\mathrm{Gal}(E(\omega)/F(\omega)) \equiv G'$ is solvable.

By Fact 2, we can construct an isomorphism between $\mathrm{Gal}(E/F)$ and $\mathrm{Gal}(E(\omega)/F)/\mathrm{Gal}(E(\omega)/E)$, which stems from the homomorphism $\mathrm{Gal}(E(\omega)/F)$ to $\mathrm{Gal}(E/F)$ which restricts some automorphism of $E(\omega)$ to just E. Because $G' \subset \mathrm{Gal}(E(\omega)/F)$, there exists a homomorphism $G' \to \mathrm{Gal}(E/F)$ with the same restriction on $E(\omega)$. Obviously, the kernel of this map is the identity (as elements

of the kernel must be the identity on both E and $F(\omega)$, which cannot occur unless the element itself is the identity), thus, the map is injective. To prove surjectivity, suppose σ maps E to E and fixes F. Define $\overline{\sigma}$, which maps $E(\omega)$ to $E(\omega)$ and sends ω to itself. This would imply that $\overline{\sigma}/E = \sigma$, so $\overline{\sigma} \in G'$. Thus, the map is bijective.

Let p be a prime that divides m. Because ω is the mth primitive root of unity, $\omega^{m/p} \in F(\omega)$ must be the primitive p^{th} root of unity. Thus, we can see that $F(\omega)$ has a primitive p^{th} root of unity for every prime p dividing q, as p is arbitrary.

Because G' is solvable, there exist subgroups $\{identity\} \subset G_{n-1} \subset ... \subset G_1 \subset G'$ that satisfy the definition of solvable groups. Because the Galois correspondence is inclusion reversing, there exist fields $F(\omega) = E^{G'} \subset F(\omega)_1 \subset ... \subset F(\omega)_{n-1} \subset E$. Because G_i is normal in G_{i-1}, we can say that there exists an isomorphism between G_{i-1}/G_i and $\mathrm{Gal}(F(\omega)_i/F(\omega)_{i-1})$.

Because by the definition of a solvable group $[G_{i-1} : G_i]$ is prime, we can see that there exists an isomorphism between $\mathrm{Gal}(F(\omega)_i/F(\omega)_{i-1})$ and a cyclic group with $|\mathrm{Gal}(F(\omega)_i/F(\omega)_{i-1})|$ elements.

We can thus see that $F(\omega)_{i-1} \subset F(\omega)_i$ is a Galois extension that has a Galois group that is isomorphic to a cyclic group with a prime number p of elements and contains the pth root of unity. By Fact 6, $F(\omega)_i = F(\omega)_{i-1}(\sqrt[p]{x})$ for some $x \in F(\omega)_{i-1})$. Thus, we can see that $F(\omega) \subset E(\omega)$ is radical.

We also can see that $F \subset F(\omega)$ is radical (as $\omega^m = 1$), and as $E \subset E(\omega)$ is radical for the same reason, we can conclude that $F \subset E$ is radical. Thus, $F \subset E$ is solvable by radicals.

□

This result demonstrates to us that there cannot exist a generalized quintic (or above) formula because S_5, or any greater symmetric group, do not have solvable Galois groups. Note that the Galois groups of quintics are subgroups of S_5, thus, any quintic with a Galois group equal to S_5 (among many others) cannot be solved using only $+, -, \times, \div$, and $\sqrt[n]{}$ because S_5 is not solvable.

Acknowledgements. I would like to thank my mentor Yiwen Zhou for his guidance and his help with developing an intuition regarding group theory and Galois groups. His help made it possible for me not only to learn the material but also to work with it in a way that helped me understand it . I would also like to thank my other mentor, Sergei Sagatov, as well as Peter May and the other organizers of the REU for this opportunity to study interesting and advanced mathematics.

References

[1] Cox, David A. Galois Theory. John Wiley and Sons INC. 2004.
[2] Rotman, Joseph. Galois Theory. Springer. 1991.
[3] Lang, Serge. Graduate Texts in Mathematics: Algebra. Springer. 2000.