Galois Theory

An Introduction

Khalid Hourani

Wednesday April 28, 2010

Contents

A natural question which arises in the study of algebra is whether we can express the roots of a polynomial in terms of its coefficients. For example, you can solve the general degree 2 polynomial by means of completing the square:

$$Ax^2 + Bx + C = 0$$
$$x^2 + \frac{B}{A}x + \frac{C}{A} = 0$$

letting $b = \frac{B}{A}$ and $c = \frac{C}{A}$:

$$x^2 + bx + c = 0$$
$$x^2 + bx + \frac{b^2}{4} + c = \frac{b^2}{4}$$
$$(x + \frac{b}{2})^2 + c = \frac{b^2}{4}$$
$$(x + \frac{b}{2})^2 = \frac{b^2}{4} - c$$
$$x + \frac{b}{2} = \pm\sqrt{\frac{b^2}{4} - c}$$

which yields the well known result, *The Quadratic Formula*:

$$x = \frac{-b \pm \sqrt{b^2 - 4c}}{2} = \frac{-B \pm \sqrt{B^2 - 4AC}}{2A}$$

as the roots of the quadratic equation $Ax^2 + Bx + C$. We then wonder if a similar method would derive solutions for higher order equations. *Solving by radicals* is the process of finding a polynomial's roots in terms of its coefficients using only addition, subtraction, multiplication, division and taking nth roots. We shall later derive the solution for the general degree 3 polynomial in this fashion (by what is called *Cardano's method*). But disappointingly, solving by radicals only works for general polynomials of degrees 3 and 4; there is no solution by radicals for the roots of the general polynomial of degree 5 or higher.

In this paper, we develop the basic theory of Galois, which beautifully relates fields and groups, and answers the question of which polynomials we can solve by radicals.

1 Extension Fields

Recall trying to solve the equation $x^2 + 1 = 0$ in an elementary algebra class. Most likely, the reader was told that there is no solution, because there is no real number whose square is -1. The fact that no real number squares to -1 is true. On the other

hand, one later learns that this polynomial has a solution. Usually, they are given the solution in a very informal setting, and simply told that the number, i whose square is -1 is "imaginary." By *adjoining* i to $\mathbb{R}$, we get a new field, $\mathbb{C}$. In this section, we formalize this notion of adjoining elements to solve polynomials, but rather than work over $\mathbb{R}$, we work over a general field F.

Definition. Let F and K be fields with F a subfield of K. Then K is an *extension field*, or *field extension*, of F. We denote this K/F (not to be confused with the quotient ring K/F). If L is a field extension of F and K is a field extension of L, then L is an *intermediate field* or *intermediate extension*.

We will frequently refer to field extensions as simply extensions.

1.1 Theorem. *Let F be a field with extension K. Then K is a vector space over F.*

We leave the proof of this theorem to the reader.

Definition. Let F be a field with extension K. The *degree of the extension*, or *degree of K over F*, denoted $[K : F]$, is the dimension of K as a vector space over F. K is called a *finite extension* of F if $[K : F]$ is finite.

1.2 Theorem. *If F is a field with finite extension K and K has finite extension L, then L is a finite extension of F and $[L : F] = [L : K][K : F]$.*

Proof. Suppose $[K : F] = m$ and $[L : K] = n$. Then there is an m-element basis of K/F and an n-element basis of L/K, say $k_1, k_2, \ldots, k_m$ and $l_1, l_2, \ldots, l_n$ respectively. We consider the set $\beta = \{k_i l_j | 0 \leq i \leq m, 0 \leq j \leq n\}$, and proceed to show that it is a basis. First, we show that β spans L:

Take $l \in L$. Since $l_1, l_2, \ldots, l_n$ is a basis for L/K,

$$l = a_1 l_1 + a_2 l_2 + \ldots + a_n l_n$$

for some $a_1, a_2, \ldots, a_n$ in K. Since $k_1, k_2, \ldots, k_m$ is a basis for K/F,

$$\begin{aligned} a_1 &= f_{11} k_1 + f_{21} k_2 + \ldots + f_{m1} k_m \\ a_2 &= f_{12} k_1 + f_{22} k_2 + \ldots + f_{m2} k_m \\ &\vdots \\ a_n &= f_{1n} k_1 + f_{2n} k_2 + \ldots + f_{mn} k_m \end{aligned}$$

where each $f_{ij} \in F$. Thus,

$$\begin{aligned} l = {} & f_{11} k_1 l_1 + f_{21} k_2 l_1 + \ldots + f_{m1} k_m l_1 \\ & + f_{12} k_1 l_2 + f_{22} k_2 l_2 + \ldots + f_{m2} k_m l_2 \\ & \vdots \\ & + f_{1n} k_1 l_n + f_{2n} k_2 l_n + \ldots + f_{mn} k_m l_n \end{aligned}$$

is a linear combination of elements in β. So β spans L.

We now show that β is linearly independent. Suppose

$$\begin{aligned} 0 = {} & f_{11}k_1l_1 + f_{21}k_2l_1 + \ldots + f_{m1}k_ml_1 \\ & + f_{12}k_1l_2 + f_{22}k_2l_2 + \ldots + f_{m2}k_ml_2 \\ & \vdots \\ & + f_{1n}k_1l_n + f_{2n}k_2l_n + \ldots + f_{mn}k_ml_n \end{aligned}$$

for some f_{ij} in F. We can group this expression:

$$\begin{aligned} 0 = {} & (f_{11}l_1 + f_{12}l_2 + \ldots + f_{1n}l_n)k_1 \\ & + (f_{21}l_1 + f_{22}l_2 + \ldots + f_{2n}l_n)k_2 \\ & \vdots \\ & + (f_{m1}l_1 + f_{m2}l_2 + \ldots + f_{mn}l_n)k_m \end{aligned}$$

Since $k_1, k_2, \ldots, k_m$ is a basis, these coefficients must all be 0. Thus

$$\begin{aligned} 0 &= f_{11}l_1 + f_{12}l_2 + \ldots + f_{1n}l_n \\ 0 &= f_{21}l_1 + f_{22}l_2 + \ldots + f_{2n}l_n \\ &\vdots \\ 0 &= f_{m1}l_1 + f_{m2}l_2 + \ldots + f_{mn}l_n \end{aligned}$$

Similarly, since $l_1, l_2, \ldots, l_n$ is a basis, these coefficients are all 0, i.e. $f_{ij} = 0$ for all i, j. So the set β is linearly independent.

Thus, β is a basis. Since $|\beta| = mn$, we have $[L : F] = mn = [L : K][K : F]$. □

This gives the following useful corollary:

1.3 Corollary. *If F is a field with finite extension K, and K has finite extension L, then $[K : F]$ and $[L : K]$ divide $[L : F]$.*

For instance, if $[L : F]$ is prime, there can be no proper intermediate fields between F and L.

Definition. Let F be a field with extension K. An element $k \in K$ is said to be *algebraic over F* if there exists a polynomial $p(x)$ with coefficients in F so that $p(k) = 0$. In this case, we say k *solves* $p(x)$ or k *satisfies* $p(x)$. k is *algebraic of degree n* if k satisfies a polynomial with coefficients in F of degree n but no nonzero polynomial of degree less than n. An element which is not algebraic is called *transcendental*.

Definition. Let F be a field and let k be an element of an extension field, K, of F. The field $F(k)$, called F *adjoined with k*, is the intersection of all intermediate extensions of F containing k, and is therefore the smallest subfield of K containing F and k.

1.4 Theorem. *Let F be a field with extension K. The element $k \in K$ is algebraic of degree n over F if and only if $[F(k) : F] = n$.*

Proof. Suppose first that $[F(k) : F] = n$. Then the $n+1$ elements $1, k, k^2, \ldots, k^n$ are all in $F(k)$[1], so they are linearly dependent. Therefore, there exist $\alpha_0, \alpha_1, \ldots, \alpha_n \in F$, not all 0, so that $\alpha_0 + \alpha_1 k + \ldots + \alpha_n k^n = 0$. Then k is clearly algebraic over F.

We now show that $1, k, \ldots, k^{n-1}$ is a basis of $F(k)$. Let j be the smallest integer so that $\alpha_j \neq 0$ in the above relation. If $j = n$, we are finished, for then k^n is in the span of $1, k, \ldots, k^{n-1}$ trivially, for which it follows that k^m is also in the span of $1, k, \ldots, k^{n-1}$ for all m. Then $1, k, \ldots, k^{n-1}$ is an n-element spanning set of a $F(k)$, and is therefore a basis. If $j \leq n-1$, then k^{j+1} is in the span of $1, k, \ldots, k^j$ by multiplying the relation $\alpha_0 + \alpha_1 k + \ldots + \alpha_j k^j = 0$ by k. Similarly, for all m, multiplying through by k^{j-m} shows that k^m is in the span of $1, k, \ldots, k^j$, and so $1, k, \ldots, k^j$ spans $F(k)$. Since $F(k)$ is a degree n vector space over F, this forces $j \geq n-1$. But $j \leq n-1$, and so $j = n-1$. Again we have that $1, k, \ldots, k^{n-1}$ is an n-element spanning set of $F(k)$, which is a basis.

Now, since $1, k, \ldots, k^{n-1}$ is a basis, it is linearly independent. In particular, if $\alpha_0 + \alpha_1 k + \ldots + \alpha_{n-1} k^{n-1} = 0$, then $\alpha_0 = \alpha_1 = \ldots = \alpha_{n-1} = 0$, so k is algebraic of degree n.

Suppose now that k is algebraic of degree n over F. Suppose $p(x) \in F[x]$ is a degree n polynomial which k satisfies, i.e. $p(k) = 0$. Suppose $p(x) = f(x)g(x)$ for some polynomials $f(x)$ and $g(x)$, then $p(k) = f(k)g(k) = 0$, so $f(k) = 0$ or $g(k) = 0$. Without loss of generality, say $f(k) = 0$. Since k is algebraic of degree n, $\deg f(x) \geq n$. Then $\deg p(x) = \deg f(x) + \deg g(x) = n$. This forces $\deg f(x) = n$, $\deg g(x) = 0$. Thus, $p(x)$ is irreducible.

Consider the surjective map $\phi : F[x] \to F(k)$ given by $f(x) \mapsto f(k)$. This is clearly a ring homomorphism, and the kernel of ϕ is the set of polynomials which k satisfies, i.e. $\ker(\phi) = \{f(x) \in F[x] | f(k) = 0\}$. $p(x)$ is an element of lowest degree in $\ker(\phi)$ and, since $F[x]$ is a principal ideal domain, $\ker(\phi) = (p(x))$, the ideal generated by $p(x)$. Since p is irreducible, $(p(x))$ is maximal, and therefore $F[x]/(p(x))$ is a field. By the **First Isomorphism Theorem for Rings**, $F[x]/(p(x))$ is isomorphic to $F(k)$. Notice that $[F[x]/(p(x)) : F] = n$, and, since $F(k)$ is isomorphic to $F[x]/(p(x))$, $[F(k) : F] = n$. □

The theorem above is the most important result of this section. For example, since we know $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, we know that $\sqrt{2}$ is algebraic of degree 2 over $\mathbb{Q}$ without needing to construct a polynomial which $\sqrt{2}$ solves. The above theorem also yields the following corollary.

1.5 Corollary. *If F is a field with extension K, and $a, b \in K$ are algebraic over F, then $a \pm b$, ab and a/b (if $b \neq 0$) are algebraic over F. In other words, the set $\{k \in K | k$ is algebraic over $F\}$ forms a field.*

[1]Recall that $F(k)$ is a field. Since $k \in F(k)$, all powers of k must be in $F(k)$.

Proof. By **Theorem 1.4**, $F(a)$ and $F(b)$ are finite extensions. Let $L = F(a)$ and $M = L(b)$. By **Theorem 1.2**, $[M : F] = [M : L][L : F]$, so M is a finite extension of F. M clearly contains $a \pm b$, ab and a/b, and by **Theorem 1.4**, these elements are algebraic. □

Definition. Let F be a field. The extension K of F is an *algebraic extension of* F if every element of K is algebraic over F.

1.6 Theorem. *If F is a field with algebraic extension K and K has algebraic extension L, then L is an algebraic extension of F.*

Proof. For any $u \in L$, u is algebraic over K, since L is an algebraic extension of K. Thus, there exist $k_0, k_1, \ldots, k_n \in K$ so that $k_0 + k_1 u + \ldots + k_n u^n = 0$. Let $M = F(k_0, k_1, \ldots, k_n)$. Since K is algebraic over F, each k_i is algebraic, and, by **Theorem 1.4**, M is a finite extension of F. Further, u is algebraic over M, since it satisfies a polynomial with coefficients in M, so $M(u)$ is a finite extension of M. By **Theorem 1.2**, $[M(u) : F] = [M(u) : M][M : F]$ is finite, so $M(u)$ is a finite extension of F. Therefore, u is algebraic over F. □

In particular, given a field F and an element x which is algebraic over F, an element algebraic over $F(x)$ is algebraic over F. For example, we know that $\sqrt{2}$ is algebraic over $\mathbb{Q}$. Since $\sqrt[4]{2}$ solves $x^2 - \sqrt{2}$ over $\mathbb{Q}(\sqrt{2})$, $\sqrt[4]{2}$ is algebraic over $\mathbb{Q}$.

A natural question to ask is whether every extension of a field F is algebraic, i.e. if there actually exist transcendental elements in some field extension of F. Luckily, we can show their existence by proving that $\mathbb{R}$ is *not* a finite extension of $\mathbb{Q}$. To see this, suppose F is a finite extension of $\mathbb{Q}$, say $\{f_1, f_2, \ldots, f_n\}$ is a basis of $F/\mathbb{Q}$. Then $F = \{\sum_{i=1}^{n} q_i f_i | q_i \in \mathbb{Q}\}$. This set is clearly countable. Since $\mathbb{R}$ is uncountable, it is not a finite extension of $\mathbb{Q}$.

2 Roots of Polynomials

In the previous section, we discussed elements of an extension K of a field F which are algebraic. We proceed in the opposite direction; rather than discuss which elements satisfy polynomials in $F[x]$, we discuss finding an extension of F so that a particular $p(x) \in F[x]$ has a root.

Definition. Let F be a field. If $p(x) \in F[x]$ then an element k lying in some extension field of F is called a *root of* $p(x)$ if $p(k) = 0$.

2.1 Lemma (The Remainder Theorem)**.** *If $p(x) \in F[x]$ and if K is an extension of F, then for any element $k \in K$, $p(x) = (x - k)q(x) + p(k)$ where $q(x) \in K[x]$ and where deg $q(x) =$ deg $p(x) - 1$.*

Proof. Since K is an extension of F, $K[x]$ obviously contains $F[x]$, so $p(x) \in K[x]$. By the division algorithm, there exists a polynomial $q(x) \in K[x]$ so that $p(x) = (x-k)q(x)+r(x)$ for some $r(x) \in K[x]$ with $r(x) \equiv 0$ or $\deg r(x) < \deg (x-k) = 1$. In either case, $r(x)$ is constant. Further, $p(k) = (k-k)q(k) + r(k) = r(k)$. Thus, $p(x) = (x-k)q(x) + p(k)$. Finally, $\deg p(x) = \deg (x-k) + \deg q(x)$, so $\deg q(x) = \deg p(x) - 1$. □

2.2 Corollary. *If $k \in K$ is a root of $p(x) \in F[x]$, then $(x-k)|p(x)$.*

Proof. By **Lemma 2.1**, $p(x) = (x-k)q(x)+p(k) = (x-k)q(x)$, so $(x-k)|p(x)$. □

2.3 Lemma. *If $p(x)$ has degree n over a field, then there are at most n roots of $p(x)$ in any extension of F.*

Proof. We begin by induction on the degree of n. If $p(x)$ is degree 0, then it has no roots in F. Suppose that, for all $k \leq n-1$ if $\deg p(x) = k$, then $p(x)$ has at most k roots in any extension of F. Suppose now that $p(x)$ is degree n over F, and let K be any extension of F. Suppose now that $k \in K$ is a root of $p(x)$ of multiplicity m. Then $(x-k)^m|p(x)$, hence $p(x) = (x-k)^m q(x)$ for a degree $n-m$ polynomial $q(x) \in K[x]$. Further, since m is the largest power of $x-k$ which divides $p(x)$, $x-k$ does not divide $q(x)$. Further, if $w \neq k$ is a root of $p(x)$, then $p(w) = 0 = (w-k)^m q(w)$, so w is a root of $q(x)$. By the induction hypothesis, we have at most $n-m$ such elements $w \in K$. Thus, there are at most $n-m+m = n$ roots of $p(x)$ in K. □

This theorem agrees with our intuition, for we would like a polynomial of degree n to have exactly n roots. We've shown it has no more than n roots. Later, we will show that there is an extension in which it has exactly n roots.

2.4 Theorem. *If $p(x) \in F[x]$ has degree $n \neq 0$ and is irreducible over F, then there is an extension K of F such that $[K:F] = n$ and $p(x)$ has a root in K.*

Proof. Since $p(x)$ is irreducible, we have that $V = (p(x))$ is maximal in $F[x]$, so $\overline{K} = F[x]/(p(x))$ is a field. Let $\phi : F[x] \to \overline{K}$ be given by $q(x) \mapsto q(x) + V$. Let $\overline{F} = \phi(F)$ denote the image of F under ϕ. Then $\overline{F}$ is isomorphic to F and $\overline{K}$ is an extension of $\overline{F}$.

Notice that $\overline{K}$ is a degree n extension of $\overline{F}$, for $1+V, x+V, \ldots, x^{n-1}+V$ is a basis of $\overline{K}$. Further, $\phi(p(x)) = p(x+V)$, for if $p(x) = a_0 + a_1 x + \ldots + a_n x^n$, then

$$\begin{aligned}
\phi(p(x)) &= \phi(a_0) + \phi(a_1 x) + \ldots + \phi(a_n x^n) \\
&= \phi(a_0) + \phi(a_1)\phi(x) + \ldots + \phi(a_n)\phi(x)^n \\
&= (a_0 + V) + (a_1 + V)(x+V) + \ldots + (a_n + V)(x+V)^n \\
&= (a_0 + V) + (a_1 x + V) + \ldots + (a_n x^n + V) \\
&= p(x+V)
\end{aligned}$$

However, since $p(x) \in V$, $\phi(p(x)) = p(x+V) = 0$, so $x+V$ is a root of $\phi(p(x)) \in \overline{K}$.

Identifying $p(x)$ with its image $p(x+V)$, and F with its image $\overline{F}$, $p(x)$ has a root in some extension K isomorphic to $\overline{K}$. □

An immediate corollary of this theorem is that *any* polynomial has a root in some extension. In particular:

2.5 Corollary. *If $p(x) \in F[x]$ is a degree n polynomial, then there is a finite extension K of F such that $p(x)$ has a root in K and $[K : F] \leq n$.*

Proof. If $q(x)$ is an irreducible factor of $p(x)$, then $q(x)$ has a root in some finite extension K of F with $[K : F] \leq \deg q(x) \leq n$. □

2.6 Theorem. *If $p(x) \in F[x]$ is a degree n polynomial, then there is a extension K of F so that p has n roots in K and $[K : F] \leq n!$.*

Proof. By the above corollary, there is a extension K_0 of F such that $p(x)$ has a root $k_0 \in K_0$ and $[K_0 : F] \leq n$. Then $p(x) = (x - k_0)q(x)$ for some $q(x) \in K_0[x]$ of degree $n - 1$. Similarly, there is an extension K_1 of K_0 so that $q(x)$ has a root $k_1 \in K_1$ and $[K_1 : K_0] \leq n - 1$. Continuing this process, there is an extension K_n such that $p(x)$ has n roots and

$$[K_n : F] = [K_n : K_{n-1}][K_{n-1} : K_{n-2}] \dots [K_1 : K_0][K_0 : F] \leq 1 \cdot 2 \dots \cdot (n-1) \cdot n = n! \ \square$$

By **Lemma 2.3**, a polynomial in $F[x]$ of degree n has at most n roots in any extension field. Thus, a polynomial of degree n has *exactly* n roots in the sense that there is an extension K of F such that $p(x)$ has n roots, and if K' is an extension of K, $p(x)$ has no roots in $K' - K$. Applying **Corollary 2.2**, if $p(x) \in F[x]$ has degree n, there is an extension K of degree at most $n!$ so that $p(x) = \alpha(x - r_1)(x - r_2) \dots (x - r_n)$ for some $r_1, r_2, \dots, r_n \in K$. That is, $p(x)$ *splits* into linear factors. This allows us to define a "minimal" extension of F.

Definition. If $p(x) \in F[x]$ is a degree n polynomial, a finite extension K of F is called a *splitting field* if $p(x)$ can be written as the product of linear factors over K, but not over any proper subfield of K.

2.7 Lemma. *Let F and F' be fields and $\tau : F \to F'$ be an isomorphism. Let $\tau(a) = a'$ for all $a \in F$. Then*

(i) *$\tau^* : F[x] \to F'[x]$ given by*

$$a_0 + a_1 x + \dots + a_n x^n \mapsto a_0' + a_1' x + \dots + a_n' x^n$$

defines an isomorphism from $F[x]$ to $F'[x]$.

(ii) *Let $\tau^*(f(x)) = f'(x)$ for all $f(x) \in F[x]$. There is an isomorphism $\tau^{**} : F[x]/(f(x)) \to F'[x]/(f'(x))$ such that $\tau^{**}(a + (f(x))) = a' + (f'(x))$ for all $a \in F$.*

We leave this proof to the reader. For the next two theorems, we shall refer to F, F', τ, τ^* and and τ^{**} as in the above lemma.

2.8 Theorem. *If $p(x) \in F[x]$ is irreducible and k is a root of $p(x)$, then $F(k)$ is isomorphic to $F'(w)$, where w is a root of $p'(t)$. Further, we can choose the isomorphism ϕ so that $\phi(k) = w$ and $\phi(x) = x$ for all $x \in F$.*

Proof. Suppose K is some extension of F with $k \in F$ and $p(k) = 0$. Letting $M = \{f(x) \in F[x] | f(k) = 0\}$, we have that M is an ideal of $F[x]$, and since $p(x)$ is irreducible, $M = (p(x))$. As in **Theorem 1.4**, let $\psi : F[x] \to F(k)$ be the surjective map $\psi(p(x)) = p(k)$. Moreover $\ker(\psi) = M = (p(x))$. By **The First Isomorphism Theorem for Rings**, $F[x]/(p(x))$ is isomorphic to $F(k)$ by the isomorphism $\psi^*(f(x) + M) = f(k)$. Further, $\psi^*(x + M) = k$.

By **Lemma 2.7**, since $p(x)$ is irreducible in $F[x]$, $p'(x)$ is irreducible in $F'[x]$, and so the same argument shows that there is an isomorphism θ^* from $F'[x]/(p'(x))$ to $F'(w)$ where w is a root of $p'(x)$ and $\theta^*(x + M) = w$. By part **(ii)** of **Lemma 2.7**, the isomorphism $\tau^{**} : F[x]/(p(x)) \to F'[x]/(p'(x))$ maps $x + (p(x))$ to $x + (p'(x))$ and satisifes $\tau^{**}(a + p(x)) = a' + (p'(x))$ for all $a \in F$. Notice that

$$F(k) \xrightarrow{(\psi^*)^{-1}} \frac{F[x]}{(p(x))} \xrightarrow{\tau^{**}} \frac{F'[x]}{(p'(x))} \xrightarrow{\theta^*} F'(w)$$

and so composing these isomorphisms gives us an isomorphism $\sigma : F(k) \to F'(w)$. Letting $(p'(x)) = M'$,

$$\sigma(k) = \theta^*(\tau^{**}(\psi^{*-1}(k))) = \theta^*(\tau^{**}(x + M)) = \theta^*(x + M') = w$$

Similarly, for any $a \in F$, $\sigma(a) = a'$. □

A special case of this is when $F = F'$. Then

2.9 Corollary. *If $p(x) \in F[x]$ is irreducible with roots a, b, then $F(a)$ is isomorphic to $F(b)$ by an isomorphism which takes a to b and fixes every element of F.*

2.10 Theorem. *Any splitting fields K and K' of the polynomials $f(x) \in F[x]$ and $f'(x) \in F'[x]$ are isomorphic by an isomorphism ϕ with $\phi(a) = a'$ and for all $a \in F$. In particular, setting $F = F'$, K and K' are isomorphic by an isomorphism which is the identity on F.*

Proof. We induct on the degree of the extension K of F. If $[K : F] = 1$, then $K = F$, and so $f(x)$ splits into linear factors over $F[x]$. By **Lemma 2.7**, $f'(x)$ splits into linear factors over $F'[x]$, so $K' = F'$. Then the isomorphism τ from F to F' is trivially an isomorphism from K to K' which fixes every element of F.

Suppose that, for all $k \leq n - 1$, and any field F_0, if $[K : F_0] \leq k$, then K is isomorphic to K' by an isomorphism which maps a to a' for all $a \in F_0$. If $[K : F] = n$, then $f(x)$ has an irreducible factor $p(x)$ of degree $r > 1$. Let $p'(x)$ be the corresponding irreducible factor of $p(x)$. Since K is the splitting field of F, $f(x)$ has all of its roots in K, and so $p(x)$ has all of its roots in K. Say $k \in K$ is such that

$p(k) = 0$, then By **Theorem 1.4**, $[F(k) : F] = r$. Similarly, there is a $k' \in K'$ so that $p'(k') = 0$, and by **Theorem 2.8**, there is an isomorphism σ from $F(k)$ to $F'(k')$ so that $\sigma(a) = a'$ for all $a \in F$. Observe that

$$[K : F(k)] = \frac{[K : F]}{[F(k) : F]} = \frac{n}{r} < n$$

Notice that K is a splitting field for $f(x) \in F(k)[x]$, for no proper subfield of E can split $f(x)$ by definition. Similarly, E' is the splitting field of $f'(x) \in F(k')[x]$. By the induction hypothesis there is an isomorphism $\phi : K \to K'$ so that $\phi(a) = a'$ for all $a \in F(k)$. Then ϕ is an isomorphism from K to K' with $\phi(a) = a'$ for all $a \in F \subseteq F(k)$. □

Thus, we can talk about *the* splitting field of $f(x)$, in the sense that the splitting field is unique up to isomorphism.

3 More About Roots

Definition. If $f(x) = a_0 + a_1x + \ldots + a_nx^n$ in $F[x]$, the *formal derivative of* $f(x)$, denoted $f'(x)$, is given by

$$f'(x) = a_1 + 2a_2x + 3a_3x^2 + \ldots + na_nx^{n-1}$$

We denote by $f^{(n)}(x)$ the *nth derivative of* $f(x)$ defined recursively by

$$f^{(0)}(x) = f(x)$$
$$f^{(n)}(x) = (f^{(n-1)}(x))'$$

We use the term formal derivative to avoid talking about limits. In $\mathbb{R}$, the derivative given by

$$f'(x) = \lim_{h \to 0} \frac{f(x+h) - f(x)}{h}$$

agrees with the formal derivative. On the other hand, it is difficult to make sense of the idea of a limit in a general field, and so we make use of the formal derivative to avoid this problem.

3.1 Lemma. *For any $f(x), g(x) \in F[x]$ and any $a \in F$*

(i) $(f(x) + g(x))' = f'(x) + g'(x)$

(ii) $(af(x))' = af'(x)$

(iii) $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$

Proof. We leave the proofs of part **(i)** and **(ii)** to the reader. For part **(iii)**, we need only show that $(p(x)q(x))' = p'(x)q(x) + p(x)q'(x)$ for the case $p(x) = x^m$, $q(x) = x^n$, after which **(i)** and **(ii)** show this for any polynomials $p(x)$ and $q(x)$. Then

$$(x^m x^n)' = (x^{m+n})' = (m+n)x^{m+n-1} = mx^{m-1}x^n + nx^{n-1}x^m = (x^m)'x^n + x^m(x^n)' \quad \square$$

These results agree with the results learned from calculus, but one must tread carefully, for many results learned in calculus do not hold for formal derivatives over general fields. For example, in calculus one learned that the derivative of a function is 0 if and only if it is constant. This is not true for the formal derivative: in $\mathbb{Z}/p\mathbb{Z}$, where p is prime, the derivative of x^p is $px^{p-1} = 0$.

3.2 Lemma. *$p(x) \in F[x]$ has a multiple root if and only if $p(x)$ and $p'(x)$ have a nontrivial (i.e. positive degree) common factor.*

Proof. Let K be the splitting field of $p(x)$ over F. Suppose that $p(x)$ has a root of multiplicity $m > 1$. Then $p(x) = (x-a)^m q(x)$ for some $q(x) \in K[x]$. It is easy to verify that

$$p'(x) = (x-a)^m q'(x) + m(x-a)^{m-1}q(x)$$

and so $p(x)$ and $p'(x)$ are both divisible by $x - a$.

Suppose, now that $p(x)$ has no multiple roots. Then

$$p(x) = a(x-r_1)(x-r_2)\dots(x-r_n)$$

for some distinct $r_1, r_2, \dots, r_n \in K$. Denote

$$a(x-r_1)(x-r_2)\dots(x-r_{i-1})(x-r_{i+1})\dots(x-r_n)$$

by $\frac{p}{x-r_i}(x)$. Then

$$p'(x) = \frac{p}{x-r_1}(x) + \frac{p}{x-r_2}(x) + \dots + \frac{p}{x-r_n}(x)$$

And so we have $p'(r_i) = \frac{p}{x-r_i}(r_i) \neq 0$. $\square$

3.3 Corollary. *If $f(x) \in F[x]$ is irreducible, then*

(1) *If the characteristic of F is 0, then $f(x)$ has no multiple roots*

(2) *If the characteristic of F is $p \neq 0$, then $f(x)$ has a multiple root only if $f(x) = g(x^p)$ for some $g(x) \in F[x]$.*

Proof. Suppose $f(x)$ has a multiple root. Then $f(x)$ and $f'(x)$ have a nontrivial common factor by **Lemma 3.2**. Since $f(x)$ is irreducible, this implies $f(x)|f'(x)$. However, $f'(x)$ has degree less than $f(x)$, and so $f'(x)$ must be 0. If the characteristic of F is 0, this forces $f(x)$ to be constant, in which case it has no roots. This is a contradiction, and so it cannot have a multiple root. On the other hand, if F has characteristic p, this forces $f(x) = g(x^p)$. $\square$

This does not rule out the fact that some irreducible polynomials in a field of characteristic $p \neq 0$ will have multiple roots. For example, if F has characteristic 2, and v is transcendental over F, then letting $K = F(v)$, we see that $x^2 - v$ is irreducible[2] and that its derivative is given by $2t = 0$, and so it has multiple roots.

3.4 Corollary. *If F is a field of characteristic $p \neq 0$, then the polynomial $x^{p^n} - x \in F[x]$ has n distinct roots.*

Proof. The derivative of $x^{p^n} - x$ is $p^n x^{p^n - 1} - 1 = -1$. Thus, $x^{p^n} - x$ and its derivative share no common factors, so $x^{p^n} - x$ has no multiple roots. □

Definition. An extension K of F is a *simple extension* if $K = F(k)$ for some $k \in K$.

3.5 Theorem. *If F is of characteristic 0 and if a, b are algebraic over F, then there exists a $c \in F(a, b)$ so that $F(a, b) = F(c)$.*

Proof. Let $p(x)$ and $q(x)$ be irreducible polynomials of degree m and n, respectively, corresponding to a and b, respectively. Say K is an extension of F so that $p(x)$ and $q(x)$ both split completely. By **Corollary 3.3**, $p(x)$ and $q(x)$ have distinct roots, say $a, a_1, \ldots, a_{m-1}$ and $b, b_1, \ldots, b_{n-1}$ respectively. If $a_i + \lambda_{ij} b_j = a + \lambda_{ij} b$, then $\lambda_{ij} = \frac{a_i - a}{b - b_j}$. Since F has characteristic 0, it has infinitely many elements, so take $v \neq \lambda_{ij}$ for all i, j. Then $a + bv \neq a_i + b_j v$ for all i, j. Letting $c = a + bv$, we have that $F(c) \subseteq F(a, b)$.

Observe that $q(x) \in F[x] \subseteq F(c)[x]$. If $f(x) = p(c - vx) \in F(c)[x]$, then $f(b) = p(c - bv) = p(a) = 0$, so $f(x)$ and $g(x)$ have $x - b$ has a common factor in $F[c]$. In fact, $x - b$ is the greatest common divisor of $f(x)$ and $g(x)$, i.e. $(f(x), g(x)) = (x - b)$, for if b_i is another root of $g(x)$, then $f(b_i) = p(c - vb_i) \neq 0$ since $c - vb_i \neq a_i$ for all i. Thus, $x - b \in F(c)[x]$, so $b \in F[c]$. Further, since $a = c - bv$, $a \in F[c]$. In other words, $F(a, b) \subseteq F(c)$. This gives $F(a, b) = F(c)$. □

3.6 Corollary. *If F is a field of characteristic 0, and if $a_1, a_2, \ldots, a_n$ are algebraic over F, then there is a $c \in F(a_1, a_2, \ldots, a_n)$ such that $F(c) = F(a_1, a_2, \ldots, a_n)$.*

Proof. We induct on n, the number of algebraic elements a_i over F. The case $n = 2$ has been shown by **Theorem 3.5**. Suppose that, for $n - 1$ elements, there exists a c_0 such that $F(a_1, a_2, \ldots, a_{n-1}) = F(c)$. Then, for n elements, $F(a_1, a_2, \ldots, a_n) = F(a_1, a_2, \ldots, a_{n-1})(a_n) = F(c_0, a_n) = F(c)$. □

4 The Elements of Galois Theory

Given a polynomial $p(x)$ over a field F, there is a corresponding group, called the *Galois group* of $p(x)$. This section developes the notion of a Galois group, and culminates in the Fundamental Theorem of Galois Theory, which beautifully relates subfields of a polynomial's splitting field to subgroups of its Galois group.

[2]The proof of this follows the same procedure as the proof that $\sqrt{2}$ is irrational.

4.1 Theorem. *Suppose F is a field and $\sigma_1, \sigma_2, \ldots, \sigma_n$ are distinct automorphisms of F. If*

$$a_1\sigma_1(x) + a_2\sigma_2(x) + \ldots + a_n\sigma_n(x) = 0 \text{ for all } x \in F$$

then

$$a_1 = a_2 = \ldots = a_n = 0$$

Proof. Suppose that

$$a_1\sigma_1(x) + a_2\sigma_2(x) + \ldots + a_n\sigma_n(x) = 0 \text{ for all } x \in F \tag{1}$$

If $n = 1$, we are done, for then $a_1\sigma_1(x) = 0$, and so $a_1 = 0$, for the permutation σ_1 is not identically 0. If $n > 1$, then, since the automorphisms are distinct, we have that $\sigma_1(c) \neq \sigma_n(c)$ for some $c \in F$. By way of contradiction, suppose not all a_i are 0. Without loss of generality, suppose in fact that no a_i are 0, and that the minimum number of nonzero terms in relation (1) is n, i.e. that

$$b_1\sigma_1(x) + b_2\sigma_2(x) + \ldots + b_m\sigma_m(x) \equiv 0 \text{ implies } m \geq n$$

Since $cx \in F$, by (1)

$$a_1\sigma_1(cx) + a_2\sigma_2(cx) + \ldots + a_n\sigma_n(cx) = 0$$

Since σ_i are automorphisms, we have

$$a_1\sigma_1(c)\sigma_1(x) + a_2\sigma_2(c)\sigma_2(x) + \ldots + a_n\sigma_n(c)\sigma_n(x) = 0 \tag{2}$$

Multiplying (1) by $\sigma_1(c)$ and subtracting the result from (2) yields

$$b_2\sigma_2(x) + b_3\sigma_3(x) + \ldots + b_n\sigma_n(x) = 0$$

where $b_i = a_i(\sigma_i(c) - \sigma_1(c))$. This is a relation of fewer than n terms, which contradicts the minimality of n. Thus,

$$a_1 = a_2 = \ldots = a_n = 0$$ □

Definition. If G is a group of automorphisms of K, then the *fixed field* of G is the set of $a \in K$ such that $\phi(a) = a$ for all $\phi \in G$.

In fact, G not need be a group of automorphisms, only a set. However, the fixed field of a set S of automorphisms is the same as the fixed field of the group generated by S, and so we define G to be a group.

4.2 Lemma. *The fixed field of G is a subfield of K.*

Proof. Denote by F the fixed field of K. If $a, b \in F$, then $\phi(a) = a$ and $\phi(b) = b$ for all $\phi \in G$. Then $\phi(a + b) = \phi(a) + \phi(b) = a + b$ for all $\phi \in G$, so $a + b \in F$. Similarly, $\phi(ab) = \phi(a)\phi(b) = ab$, so $ab \in F$. Further, $1 \in F$ because every automorphism fixes 1. □

Definition. Let F be a field with extension K. The *Group of Automorphisms of K relative to F*, denoted $G(K, F)$ is the set of all automorphisms of K which fix all elements of F.

4.3 Lemma. *$G(K, F)$ is a group under function composition. In particular, it is a subgroup of $Aut(K)$.*

Proof. Notice that the identity automorphism acts as the identity with respect to function composition. Further, if $\phi \in G(K, F)$, ϕ fixes all elements of F, and so ϕ^{-1} clearly fixes all elements of F. Thus $\phi^{-1} \in G(K, F)$. Moreover, if ϕ_1, ϕ_2 fix all elements of F, their composition fixes all elements of F, so their composition is in $G(K, F)$. Therefore, $G(K, F)$ is a group. □

Before proceeding with more theory, we consider a few examples in which we explicitly find $G(K, F)$ for given fields K and F.

Examples.

(1) $G(\mathbb{C}, \mathbb{R})$ is the set of automorphisms which satisfy $\phi(x) = x$ for all $x \in \mathbb{R}$. Notice that $\phi(i)^2 = \phi(i^2) = \phi(-1) = -1$ and so $\phi(i) = \pm i$. It follows that $\phi(z) = z$ and $\phi(z) = \overline{z}$ are the only automorphisms of $\mathbb{C}$ which fix $\mathbb{R}$, and so $G(\mathbb{C}, \mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$.

(2) $G(\mathbb{Q}(\sqrt{2}), \mathbb{Q})$ is the set of automorphisms of $\mathbb{Q}(\sqrt{2})$ which fix $\mathbb{Q}$. If ϕ is an automorphism of $\mathbb{Q}(\sqrt{2})$ which fixes $\mathbb{Q}$, then $\phi(\sqrt{2})^2 = \phi(\sqrt{2}^2) = \phi(2) = 2$, and so the only elements of $G(\mathbb{Q}(\sqrt{2}), \mathbb{Q})$ are $\phi(x) = x$ and $\phi(a + b\sqrt{2}) = a - b\sqrt{2}$. This group is also isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

(3) Consider $G(\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q})$. Every element in $\mathbb{Q}(\sqrt[3]{2})$ is of the form $a_0 + a_1\sqrt[3]{2} + a_2(\sqrt[3]{2})^2$ for rational a_0, a_1, a_2. If ϕ is an automorphism of $\mathbb{Q}(\sqrt[3]{2})$ which fixes $\mathbb{Q}$, then $\phi(\sqrt[3]{2})^3 = \phi(\sqrt[3]{2}^3) = \phi(2) = 2$, and so $\phi(\sqrt[3]{2})$ is a cube root of 2. However, there is only one real cubed root of 2, which foces $\phi(x) = x$ for all x, so $G(\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}) \cong \{1\}$. In particular, the fixed field of $G(\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q})$ is $\mathbb{Q}(\sqrt[3]{2})$.

4.4 Theorem. *If K is a finite extension of F, then $G(K, F)$ is a finite group and $|G(K, F)| \leq [K : F]$.*

Proof. Let $[K : F] = n$ and let $k_1, k_2, \ldots, k_n$ be a basis of K/F. Take $\sigma_1, \sigma_2, \ldots, \sigma_{n+1}$ to be $n + 1$ elements (not necessarily distinct) of $G(K, F)$. The system of equations

$$\begin{aligned} x_1\sigma_1(k_1) + x_2\sigma_2(k_1) + \ldots + x_{n+1}\sigma_{n+1}(k_1) &= 0 \\ x_1\sigma_1(k_2) + x_2\sigma_2(k_2) + \ldots + x_{n+1}\sigma_{n+1}(k_2) &= 0 \\ &\vdots \\ x_1\sigma_1(k_n) + x_2\sigma_2(k_n) + \ldots + x_{n+1}\sigma_{n+1}(k_n) &= 0 \end{aligned}$$

must have a nontrivial solution, for there are n equations in $n+1$ unknowns. Say $a_1, a_2, \ldots, a_{n+1}$ is this solution, i.e. some $a_j \neq 0$ and

$$a_1\sigma_1(k_i) + a_2\sigma_2(k_i) + \ldots + a_{n+1}\sigma_{n+1}(k_i) = 0 \tag{1}$$

for all i. For any $t \in K$, we can write $t = \alpha_1 k_1 + \alpha_2 k_2 + \ldots + \alpha_n k_n$. Multiplying (1) by α_i and adding all such equations, we see that

$$a_1\sigma_1(t) + a_2\sigma_2(t) + \ldots + a_{n+1}\sigma_{n+1}t = 0$$

But not all a_i are 0! Applying the contrapositive of **Lemma 4.1**, this implies that the σ_i are *not* all distinct. In particular, there are at most n such σ_i, which proves the theorem. □

Definition. The elements

$$\begin{aligned} s_1 &= x_1 + x_2 + \ldots + x_n \\ s_2 &= \sum_{i<j} x_i x_j \\ s_3 &= \sum_{i<j<k} x_i x_j x_k \\ &\vdots \\ s_n &= x_1 x_2 \ldots x_n \end{aligned}$$

in $F[x_1, x_2, \ldots, x_n]$ are the *symmetric functions in* $x_1, x_2, \ldots, x_n$.

This is motivated by the fact that

$$(x - x_1)(x - x_2)\ldots(x - x_n) = x^n - s_1x^{n-1} + s_2x^{n-2} + \ldots + (-1)^n s_n$$

which can be verified by induction on n. Notice that this function is symmetric in $x_1, x_2, \ldots, x_n$. We call this polynomial the *General Polynomial of degree* n.

4.5 Lemma. *The symmetric functions* $s_1, s_2, \ldots, s_n$ *in* $x_1, x_2, \ldots, x_n$ *are symmetric in* $x_1, x_2, \ldots, x_n$, *i.e. given any* $\sigma \in S_n$,

$$s_i(x_1, x_2, \ldots, x_n) = s_1(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x(\sigma_n))$$

We leave the proof of this lemma to the reader.

Definition. The *field of symmetric rational functions in* $x_1, x_2, \ldots, x_n$, S, is the fixed field of $F(x_1, x_2, \ldots, x_n)$ relative to S_n, i.e. the set of all $f \in F(x_1, x_2, \ldots, x_n)$ such that $\sigma(f) = f$ for all $\sigma \in S_n$.

4.6 Theorem. *(Fundamental Theorem of Symmetric Polynomials) A polynomial $f(x_1, x_2, \ldots, x_n)$ in $F[x_1, x_2, \ldots, x_n]$ is symmetric if and only if it is a polynomial in $s_1, s_2, \ldots, s_n$, the symmetric functions in $x_1, x_2, \ldots, x_n$.*

Proof. We first define the *height* of a monomial $x_1^{k_1}x_2^{k_2}\ldots x_n^{k_n}$ to be $k_1 + 2k_2 + \ldots + nk_n$. We then define the height of any polynomial to be the maximum height of its monomial terms. Suppose f is a symmetric polynomial. We induct on the height of f. If f has height 0, then $f(x_1, x_2, \ldots, x_n) = a$ for some $a \in F$. Suppose that, for all $j < k$, if f has height j, f can be expressed as a polynomial in $s_1, s_2, \ldots, s_n$. If f has height k, with maximal height term $cx_1^{k_1}x_2^{k_2}\ldots x_n^{k_n}$, then g defined by

$$g(x_1, x_2, \ldots, x_n) = f(x_1, x_2, \ldots, x_n) - cs_1^{k_n - k_{n-1}}s_2^{k_{n-1}-k_{n-2}}\ldots s_{n-1}^{k_2-k_1}s_n^{k_1}$$

is a symmetric polynomial of height less than k, and so it can be expressed as a polynomial in $s_1, s_2, \ldots, s_n$. Thus, f can be expressed as a polynomial in $s_1, s_2, \ldots, s_n$. □

4.7 Corollary. *If S is the field of symmetric rational functions in $x_1, x_2, \ldots, x_n$, then $S = F(s_1, s_2, \ldots, s_n)$ where $s_1, s_2, \ldots, s_n$ are the symmetric functions in $x_1, x_2, \ldots, x_n$*

Proof. The symmetric rational functions $x_1, x_2, \ldots, x_n$ are of the form $\frac{p}{q}$ for p, q symmetric polynomials in $x_1, x_2, \ldots, x_n$. By **Theorem 4.6**, p and q are polynomials in $s_1, s_2, \ldots, s_n$. □

4.8 Theorem. *If $s_1, s_2, \ldots, s_n$ are the symmetric functions in $x_1, x_2, \ldots, x_n$, $P = F(x_1, x_2, \ldots, x_n)$ and $S = F(s_1, s_2, \ldots, s_n)$, then*

(1) *P is the splitting field over S of the polynomial $x^n - s_1x^{n-1} + \ldots + (-1)^n s_n$.*

(2) *$[P : S] = n!$*

(3) *$G(P, S) = S_n$*

Proof. **(1)** Notice that the polynomial $p(x) = x^n - s_1x^{n-1} + \ldots + (-1)^n s_n$ factors over P as $(x - x_1)(x - x_2)\ldots(x - x_n)$, so $p(x)$ splits over P. If $p(x)$ splits over a subfield of P, then this subfield contains $x_1, x_2, \ldots, x_n$, and so it would in fact be equal to P. Thus, $P = F(x_1, x_2, \ldots, x_n)$ is the splitting field of $p(x)$ over S.

(2) Observe first that $S_n \subseteq G(P, S)$, and by **Theorem 4.4**, $[P : S] \geq n!$. Moreover, since $p(x)$ is of degree n, by **Theorem 2.6**, $[P : S] \leq n!$, and so $[P : S] = n!$.

(3) Finally, since $S_n \subseteq G(P, S)$ and since $[P : S] = n!$, we have both that $|G(P, S)| \geq n!$ and $|G(P, S)| \leq n!$. Thus, $|G(P, S)| = n!$ Since S_n is contained in this group, and $|S_n| = n!$, $G(P, S) = S_n$. □

Definition. K is a *normal extension* of F if K is a finite extension of F such that F is the fixed field of $G(K, F)$.

4.9 Theorem. *Let K be a normal extension of F and let H be a subgroup of $G(K,F)$. If $K_H = \{x \in K | \phi(x) = x \text{ for all } \sigma \in H\}$ is the fixed field of H, then*

(1) $[K : K_H] = |H|$

(2) $H = G(K, K_H)$

Proof. **(1)** Since H fixes K_H, $H \subseteq G(K, K_H)$. By **Theorem 4.4**, $[K : K_H] \geq |H|$. By **Theorem 3.5**, there is an $k \in K$ such that $K_H(k) = K$, and so there is an irreducible polynomial $p(x)$ of degree $m = [K : K_h]$ with $p(k) = 0$ and no nontrivial lower degree polynomial which k satisfies. Let $H = \{\sigma_1, \sigma_2, \ldots, \sigma_h\}$ where $h = |H|$ and $\sigma_1 = \mathrm{Id}_K$. By **Lemma 4.5**, the symmetric functions

$$\begin{aligned} s_1 &= \sigma_1(a) + \sigma_2(a) + \ldots + \sigma_h(a) \\ s_2 &= \sum_{i<j} \sigma_i(a)\sigma_j(a) \\ &\vdots \\ s_h &= \sigma_1(a)\sigma_2(a)\ldots\sigma_h(a) \end{aligned}$$

of $\sigma_1(a), \sigma_2(a), \ldots, \sigma_h(a)$ are invariant under all $\sigma \in H$. By definition, then, $s_1, s_2, \ldots, s_n$ are elements of K_H. Moreover, $\sigma_1(a), \sigma_2(a), \ldots, \sigma_h(a)$ are roots of the polynomial

$$(x - \sigma_1(a))(x - \sigma_2(a))\ldots(x - \sigma_h(a)) = x^h - s_1x^{h-1} + \ldots + (-1)^h s_h$$

which is in $K_h[x]$. By **Theorem 4.4**, $[K : K_H] = m \leq h = |H|$, and so $[K : K_H] = |H|$. Finally, since $|H| = [K : K_H] \geq |G(K, K_H)|$, and since $H \subseteq G(K, K_H)$, $H = G(K, K_H)$. □

This yields the following very useful corollary.

4.10 Corollary. *If K is a normal extension of F, then $[K : F] = |G(K, F)|$.*

Proof. Letting $H = G(K, F)$, $K_H = F$ by the normality of K, and so $[K : F] = |G(K, F)|$. □

In order to characterize normal extensions, we need the following lemma.

4.11 Lemma. *Let K be the splitting field of $f(x) \in F[x]$ and let $p(x)$ be an irreducible factor of $f(x)$. If the roots of $p(x)$ are $k_1, k_2, \ldots, k_n$ then for all i there exists a $\sigma \in G(K, F)$, so that $\sigma(k_1) = k_i$.*

Proof. The roots of $p(x)$ are also roots of $f(x)$ and so they are in K. By **Theorem 2.8**, there is an isomorphism $\tau : F(k_1) \to F(k_i)$ taking k_1 to k_i and fixing every element in F. K is the splitting field of $f(x)$ considered as a polynomial over F, but similarly is the splitting field of $f(x) \in F(k_1)[x]$ and $f(x) \in F(k_i)[x]$. By **Theorem 2.10**, there is an automorphism σ of K with $\sigma(x) = \tau(x)$ for all $x \in F(k_1)$. Since τ fixes every element of F, $\sigma \in G(K, F)$ and $\sigma(k_1) = \tau(k_1) = k_i$. □

We now characterize normal extensions. For simplicity, we assume F is a field of characteristic 0 for the remainder of the section. While the results of this section have analogues in characteristic $p \neq 0$, they are beyond the scope of this work.

4.12 Theorem. *K is a normal extension of F if and only if K is the splitting field of some polynomial over F.*

Proof. Suppose that K is a normal extension of F. Then, by **Theorem 3.5**, $K = F(a)$ for some $a \in K$. We proceed to show that K is the splitting field of

$$p(x) = (x - \sigma_1(a))(x - \sigma_2(a)) \dots (x - \sigma_n(a)) = x^n - s_1 x^{n-1} + \dots + (-1)^n s_n$$

where $\sigma_1, \sigma_2, \dots, \sigma_n$ are the elements of $G(K, F)$ and $s_1, s_2, \dots, s_n$ are the corresponding symmetric functions. By **Lemma 4.5**, the s_i are invariant under all $\sigma \in G(K, F)$. Since K is normal, $s_1, s_2, \dots, s_n$ are in F. Thus, K splits $f(x)$ into a product of linear factors. Further, since a is a root of $p(x)$ and since $K = F(a)$, a is not in any proper subfield of K, so K is the splitting field of $p(x)$.

Suppose now that K is the splitting field of some polynomial $p(x)$ over F. We proceed by induction on the degree of K over F. In the case $[K : F] = 1$, $K = F$, in which case K is obviously a normal extension of F. Suppose that, for any pair of fields K_1, F_1 of degree less than k, that, whenever K_1 is a splitting field over F_1 of a polynomial in $F_1[x]$, K_1 is normal over F_1. Our induction step is to show that, if $[K : F] = k$, then K is a normal extension of F.

If $f(x)$ splits into linear factors factors over F, then $K = F$, and so we are done. So suppose that $f(x)$ has an irreducible factor $p(x) \in F[x]$ of degree $m > 1$. The m distinct roots $k_1, k_2, \dots, k_m$ of $p(x)$ all lie in K, and K is the splitting field of $f(x)$ considered as a polynomial over $F(k_1)$. Observe that

$$[K : F(k_1)] = \frac{[K : F]}{[F(k_1) : F]} = \frac{n}{m} < n$$

Therefore, by the induction hypothesis, K is a normal extension of $F(k_1)$.

Let $k \in K$ be left fixed by every automorphism $\sigma \in G(K, F)$. Since K is a normal extension of $F(k_1)$, every element of $G(K, F(k_1))$ fixes every element of F, and so $k \in F(k_1)$. Thus

$$k = a_0 + a_1 k_1 + a_2 k_1^2 + \dots + a_{m-1} k_1^{m-1} \tag{1}$$

for some $a_0, a_1, \dots, a_n \in F$. By **Lemma 4.11**, there is an automorphism $\sigma_i \in G(K, F)$ such that $\sigma_i(k_1) = k_i$. Since σ_i leaves k and all a_i fixed, applying it to (1) we see that

$$k = a_0 + a_1 k_i + a_2 k_i^2 + \dots + a_{m-1} k_i^{m-1} \text{ for } i = 1, 2, \dots, m \tag{2}$$

And so the polynomial $q(x) = (a_0 - k) + a_1 x + a_2 x^2 + \dots + a_{m-1} x^{m-1}$ has m distinct roots $k_1, k_2, \dots, k_m$. But the degree of $q(x)$ is $m - 1$, which forces the coefficients to be 0. In particular, $a_0 = k$, and so $k \in F$. Thus, the fixed field of $G(K, F)$ is F. $\square$

Definition. Let $f(x)$ be a polynomial in $F[x]$ and let K be its splitting field over F. The *Galois Group* of $f(x)$ is the group $G(K, F)$ of automorphisms of K which fix every element of F.

The following theorem establishes a deep connection between splitting fields and their corresponding Galois groups. Before proving it, we prove the following lemma.

4.13 Lemma. *Suppose K is the splitting field of F and T is an intermediate field, i.e. $F \subseteq T \subseteq K$. Then T is a normal extension of F if and only if for every $\sigma \in G(K, F)$, $\sigma(T) \subseteq T$.*

Proof. Let $G = G(K, F)$. By **Theorem 3.5**, $K = F(a)$ for some $a \in K$. If $\sigma(T) \subseteq T$, then $\sigma(a) \in T$. As shown in the proof for **Theorem 4.12**, this implies that T is the splitting field of

$$p(x) = \prod_{\sigma \in G} (x - \sigma(a))$$

which has coefficients in F. Thus, T is a normal extension of F.

On the other hand, if T is a normal extension of F, then $T = F(a)$ for some $a \in K$. By **Theorem 4.12**, the irreducible polynomial $p(x)$ which is solved by a has all of its roots in T. But, for any $\sigma \in G(K, F)$, $\sigma(a)$ is a root of $p(x)$, and so $\sigma(a) \in T$. Since $K = F(a)$, it follows that $\sigma(T) \subseteq T$. □

4.14 Theorem (Fundamental Theorem of Galois Theory)**.** *Let $f(x) \in F[x]$ have splitting field K and Galois group $G(K, F)$. If T is an intermediate field of K/F, then for any subgroup H of $G(K, T)$, let $K_H = \{x \in K | \sigma(x) = x \text{ for all } \sigma \in H\}$. Then*

(1) $T = K_{G(K,T)}$

(2) $H = G(K, K_H)$

(3) $[K : T] = |G(K, T)|$ *and* $[T : F] = [G(K, F) : G(K, T)]$

(4) *T is a normal extension of F if and only if $G(K, T)$ is a normal subgroup of $G(K, F)$.*

(5) *If T is a normal extension of F, then $G(T, F)$ is isomorphic to $G(K, F)/G(K, T)$.*

Proof.

(1) Since K is the splitting field of $f(x)$ over F, it is also the splitting field of $f(x)$ over T, and by **Theorem 4.12**, it is a normal extension of T. By definition, T is the fixed field of $G(K, T)$ and so $T = K_{G(K,T)}$.

(2) Since K is a normal extension of F, by **Theorem 4.9**, $H = G(K, K_H)$.

(3) Since K is normal over T, by **Theorem 4.9**, $[K : T] = |G(K,T)|$. Further, $|G(K,F)| = [K : F] = [K : T][T : F] = G(K,T)[T : F]$ and so

$$[T : F] = \frac{|G(K,F)|}{|G(K,T)|} = [G(K,F) : G(K,T)]$$

(4) Suppose T is a normal extension of F. Then, by **Lemma 4.13**, for any $\sigma \in G(K,F)$ and $t \in T$, $\sigma(t) \in T$. For any $\tau \in G(K,T)$, $\tau(\sigma(t)) = \sigma(t)$, and so $\sigma^{-1}\tau\sigma \in G(K,T)$. Thus, $G(K,T) \lhd G(K,F)$.

On the other hand, if $G(K,T) \lhd G(K,F)$, then for any $\sigma \in G(K,F)$ and $\tau \in G(K,T)$, $\sigma^{-1}\tau\sigma \in G(K,T)$, i.e. $\sigma^{-1}(\tau(\sigma(t))) = t$ for all $t \in T$. Therefore $\tau(\sigma(t)) = \sigma(t)$, and so $\sigma(t) \in T$. By **Lemma 4.13**, T is normal over F.

(5) Since T is a normal extension, for any $\sigma \in G(K,F)$, $\sigma(t) \in T$, and so we can restrict the automorphism to T. Call this automorphism σ^*. Since σ^* is an automorphism of T which leaves every element of F fixed, $\sigma^* \in G(T,F)$. Further, for any $\phi \in G(K,F)$, we have $(\phi \circ \sigma)^* = \phi^* \circ \sigma^*$, and so we can define the surjective homomorphism from $G(K,F)$ into $G(T,F)$ by

$$\sigma \mapsto \sigma^*$$

The kernel of this homomorphism is everything which maps to the identity automorphism of $G(T,F)$, i.e.

$$\{\phi \in G(K,F) | \phi(t) = t \text{ for all } t \in T\} = G(K,T)$$

and, by **The First Isomorphism Theorem**, $G(K,F)/G(K,T)$ is isomorphic to the image of this homomorphism. By **(3)**, the $|G(K,F)/G(K,T)| = [T : F]$. By **Theorem 4.9** $[T : F] = |G(T,F)]$, and so $|G(K,F)/G(K,T)| = |G(T,F)|$. Thus, $G(T,F)$ is isomorphic to $G(K,F)/G(K,T)$ □

4.15 Corollary. *Let $f(x) \in F[x]$ have splitting field K, and let G be the Galois group of $f(x)$. There is a one-to-one correspondence between subfields T of K containing F and subgroups of G.*

Proof. Part **(2)** of **Theorem 4.14** shows that any subgroup of G arises in the form $G(K,T)$, and so we can find a one-to-one correspondence between subfields T of K containing F and subgroups of G by

$$T \mapsto G(K,T)$$

which is clearly surjective. If $G(K,T_1) = G(K,T_2)$, then, by part **(1)**,

$$T_1 = K_{G(K,T_1)} = K_{G(K,T_2)} = T_2$$

so the map is injective. □

5 Solvability by Radicals

We now proceed to address what it means for a polynomial to be solvable by radicals, and why the general 5th degree polynomial is not solvable by radicals. But first, we derive the solution to the general 3rd degree polynomial using *Cardano's method*.

We would like to solve

$$x^3 + ax^2 + bx + c =$$

and so we set $x = t - a/3$ which yields the *depressed cubic*

$$t^3 + pt + q = 0$$

where

$$p = b - \frac{a^2}{3} \text{ and } q = c + \frac{2a^3 - 9ab}{27}$$

Now we introduce variables u and v such that $u + v = t$. By substitution, we have

$$u^3 + v^3 + (3uv + p)(u + v) + q = 0$$

If we require that $3uv + p = 0$, then, multiplying by u^3 and substituting $uv = -p/3$,

$$u^6 + qu^3 - \frac{p^3}{27} = 0$$

which is quadratic in u^3. Solving for u^3:

$$u^3 = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$$

and so

$$u = \sqrt[3]{-\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

Since $t = u + v$, $t = x + a/3$ and $v = -p/3u$, we have

$$x = -\frac{p}{3u} + u - \frac{a}{3}$$

While there are 6 possible values for u, the sign of the square root does not effect t, and so we have all 3 solutions. However, special care must be taken when p or q is 0.

We proceed by discussing the notion of a solvable group, and we establish the link between a polynomial which is solvable by radicals and a group which is solvable.

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

$$G = N_0 \geq N_1 \geq N_2 \geq \ldots \geq N_k = \{1\}$$

with $N_{i+1} \lhd N_i$ and N_i/N_{i+1} abelian for all i.

In order to formulate a concrete way to determine whether a group is solvable, we must define a special subgroup of a given group G, called the *commutator subgroup*, and establish some useful properties of this subgroup.

Definition. The *Commutator Subgroup* or *Derived Subgroup* of a group G, denoted G', is the group generated by the set $\{aba^{-1}b^{-1}|a, b \in G\}$. The *nth Commutator Subgroup*, denoted $G^{(n)}$, is defined recursively

$$G^{(0)} = G$$
$$G^{(n)} = G^{(n-1)'}$$

5.1 Lemma (Properties of the Commutator Subgroup)**.** *For any group G and any integer $n \geq 0$*

(i) $G^{(n)} \lhd G$

(ii) $G^{(n)}/G^{(n+1)}$ *is abelian*

(iii) *If* $H \leq G$, $H' \leq G'$

(iv) G/H *is abelian if and only if* $G' \leq H$

Proof.

(i) We first show that G' is normal in G. In particular, we show that, for any generating element $x = aba^{-1}b^{-1}$, $gaba^{-1}b^{-1}g^{-1} \in G'$. To see this, notice that

$$gaba^{-1}b^{-1}g^{-1} = gag^{-1}gbg^{-1}ga^{-1}gb^{-1}g^{-1}$$

Letting $c = gag^{-1}$, $d = gbg^{-1}$, then

$$gaba^{-1}b^{-1}g^{-1} = cdc^{-1}d^{-1} \in G'$$

We then induct on n: suppose that, for some k, $G^{(k)}$ is normal in G. Then $G^{(k+1)} = G^{(k)'}$. If $x \in G^{(k+1)}$, $x = aba^{-1}b^{-1}$ for some $a, b \in G^{(k)}$. For any $g \in G$, $c = gag^{-1}$, $d = gbg^{-1}$, $c^{-1} = ga^{-1}g^{-1}$ and $d^{-1} = gbg^{-1}$ are all in $G^{(k)}$ by the induction hypothesis. Further,

$$gxg^{-1} = cdc^{-1}d^{-1} \in G^{(k+1)}$$

so $G^{(k+1)} \lhd G$.

(ii) If $aG', bG' \in G/G'$, then $aG'bG' = abG' = ba(b^{-1}a^{-1}ab)G' = baG' = bG'aG'$, so G/G' is abelian. This is true for any group G; in particular, then, it is true for the group $G^{(n)}$ whose commutator is $G^{(n+1)}$.

(iii) Clearly, the commutators of H are commutators of G, and so the group generated by these commutators would be a subgroup of the group generated by the commutators of G.

(iv) If G/H is abelian, then, for any $g_1, g_2 \in G$, $g_1 g_2 g_1^{-1} g_2^{-1} H = H$, so $g_1 g_2 g_1^{-1} g_2^{-1} \in H$. On the other hand, if $G' \leq H$, then $g_1 g_2 g_1^{-1} g_2^{-1} H = H$, and so $g_1 H g_2 H = g_2 H g_1 H$. □

We've established some useful facts about the commutator subgroup, and these facts allow us to formulate an equivalent notion of solvability for groups, as in the following theorem.

5.2 Theorem. *A group G is solvable if and only if $G^{(k)} = \{1\}$ for some k.*

Proof. If $G^{(k)} = \{1\}$ for some k, then $G \geq G' \geq \ldots \geq G^{(k)} = \{1\}$ are normal subgroups of G with $G^{(k)}/G^{(k+1)}$ abelian by **Lemma 5.1**, so G is solvable. On the other hand, if G is solvable, say $G = N_0 \geq N_1 \geq \ldots \geq N_k = \{1\}$. Since N_{i+1}/N_i is abelian, $N'_{i+1} \leq N_i$ and so $G^{(k)} \leq N_k = \{1\}$. □

5.3 Corollary. *If H is the homomorphic image of a solvable group G, then H is solvable.*

Proof. Since H is the image of G, $H^{(k)}$ is the image of $G^{(k)} = \{1\}$, and so $H^{(k)} = \{1\}$. □

5.4 Theorem. *Suppose F is a field with all nth roots of unity for some particular n, and suppose $a \neq 0$ is in F. Let K be the splitting field of $x^n - a$ over F. Then*

(i) *$K = F(u)$ where u is any root of $x^n - a$*

(ii) *The Galois group of $x^n - a$ is abelian. In particular, it is cyclic.*

Proof. **(i)** Let ω be a primitive nth root of unity. Then $\omega, \omega^2, \ldots, \omega^{n-1}$ are not equal to 1, and so $x^n - a$ is solved by $u, \omega u, \omega^2 u, \ldots, \omega^{n-1} u$ for any root u of $x^n - a$. It is easy to see that these roots are distinct, and so the splitting field of $x^n - a$ is $F(u)$.

(ii) By **Lemma 4.11**, there is a map $\sigma \in G(K, F)$ with $\sigma(u) = \omega u$. Further, for any $\phi \in G(K, F)$, $\phi(u) = \omega^i u$ for some i. Therefore

$$\phi = \underbrace{\sigma \circ \sigma \circ \ldots \circ \sigma}_{i-\text{times}}$$

And so σ generates the Galois group of $x^n - a$. Therefore, the group is cyclic. □

Definition. An element α which is algebraic over F can be *expressed by radicals* or *solved for in terms of radicals* if α is an element of a field K which can be obtained by a succession of simple radical extensions

$$F = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_s = K$$

where $K_{i+1} = K_i(\sqrt[n_i]{a_i})$ for some $a_i \in K_i$, $i = 0, 1, \ldots, s-1$. Here $\sqrt[n_i]{a_i}$ denotes some root of the polynomial $x^{n_i} - a_i$. Such a field K is called a *root extension* of F. A polynomial $f(x) \in F[x]$ is *solvable by radicals* if all of its roots can be solved for in terms of radicals.

For simplicity, we proceed by assuming our base field F has characteristic 0, but these results all hold in a field whose characteristic does not divide the order of the roots that will be taken.

5.5 Lemma. *If $p(x)$ is solvable by radicals over F, there is a sequence of fields*

$$F = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_s = K$$

where $K_{i+1} = K_i(\sqrt[n_i]{a_i})$ such that K is normal over F and $p(x)$ splits over K.

We leave this proof to the reader.

5.6 Theorem. *If F contains all nth roots of unity for all n and $p(x) \in F[x]$ is solvable by radicals, then the Galois group of $p(x)$ is solvable.*

Proof. Suppose that $p(x)$ is solvable by radicals. By **Lemma 5.5**, there is a sequence of fields

$$F = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_s = K$$

where $K_{i+1} = K_i(\sqrt[n_i]{a_i})$ for some $a_i \in K_i$, $i = 0, 1, \ldots, s-1$, with K a normal extension of F. Then K is a normal extension of each K_i. Consider the chain

$$G(K, F) \supseteq G(K, K_1) \supseteq \ldots \supseteq G(K, K_{s-1}) \supseteq \{1\}$$

Since K is a normal extension of K_i, $G(K, K_i)$ is normal in $G(K, F)$ by **Theorem 4.14**. Further, by **Theorem 5.4**, $G(K_{i+1}, K_i)$ is abelian, and so must be the quotients $G(K, K_i)/G(K, K_{i-1})$. Thus, $G(K, F)$ is solvable.

Suppose now that $p(x)$ has splitting field L over F. Since $p(x)$ is solvable by radicals, it must be that $L \subseteq K$ for some K as above. Since L is a splitting field, it must be a normal extension of F, and so $G(K, L)$ is a normal subgroup of $G(K, F)$ by **Theorem 4.14** and $G(L, F)$ is isomorphic to $G(K, F)/G(K, L)$. Thus, $G(L, F)$ is the image of $G(K, F)$ under a homomorphism. By **Corollary 5.3**, since $G(K, F)$ is solvable, $G(L, F)$ is solvable. □

5.7 Theorem. *S_n is not solvable for $n \geq 5$.*

Proof. Take $a = (123)$, $b = (145)$. Then $aba^{-1}b^{-1} = (142) \in S_n'$. Since $S_n' \lhd S_n$, for any $(ijk) \in S_n$, take $\sigma \in S_n$ with $1 \mapsto i$, $4 \mapsto j$, $2 \mapsto k$, then $\sigma(142)\sigma^{-1} = (ijk) \in S_n'$. In other words, S_n' contains all 3-cycles. Similarly, $S_n^{(k)}$ contains all 3-cycles for all k, and so $S^{(k)} \neq \{1\}$ for any k. By **Lemma 5.2**, S_n is not solvable for $n \geq 5$. □

5.8 Corollary. *The general polynomial of degree $n \geq 5$ is not solvable.*

Proof. Recall that the general polynomial of degree $n \geq 5$ over a field F is the polynomial

$$p(x) = (x - x_1)(x - x_2)\dots(x - x_n) = x^n - a_1x^{n-1} + \dots + (-1)^n a_n$$

where $x_1, x_2, \dots, x_n$ are indeterminates over F and $a_1, a_2, \dots, a_n$ are the symmetric functions in $x_1, x_2, \dots, x_n$. By **Theorem 4.8**, this polynomial has Galois group S_n, which is not solvable for $n \geq 5$ by the above theorem. By **Theorem 5.5**, $p(x)$ is not solvable by radicals. □

This does not rule out the possibility of a particular degree $n \geq 5$ polynomial being solvable by radicals. For example, over $\mathbb{Q}$, the polynomial $x^6 + x^3 + 1$ is a degree 6 polynomial which is solvable by radicals! Simply take $y = x^3$, then solve $y^2 + y + 1 = 0$. Rather, **Corollary 5.8** rules out the possibility of a solution by radicals for the roots of a degree $n \geq 5$ polynomial over any field in terms of only its coefficients. This is due to the algebraic independence of the roots x_i of $p(x)$ in the general polynomial.