# GALOIS THEORY
# TOPIC VIII
# ALGEBRAIC FIELD EXTENSIONS

PAUL L. BAILEY

## 1. Field Extensions

**Definition 1.** A *field extension* $E/F$ consists of a field $E$ which contains a field $F$. We call $F$ the *base field* of the extension.

For example, $\mathbb{C}/\mathbb{R}$, $\mathbb{C}/\mathbb{Q}$, and $\mathbb{R}/\mathbb{Q}$ are field extensions.

**Definition 2.** Let $E/F$ be a field extension and let $A \subset E$.

The subring of $E$ generated by $F \cup A$ is denoted $F[A]$. This is the intersection of all subrings of $E$ which contain $F$ and $A$.

The subfield of $E$ generated by $F \cup A$ is denoted $F(A)$. This is the intersection of all subfields of $E$ which contains $F$ and $A$. Extend this notation as follows:

- If $A = \{\beta\}$ is a singleton, we may write $F[\beta]$ to mean $F[A]$;
- If $A = \{\beta\}$ is a singleton, we may write $F(\beta)$ to mean $F(A)$;
- If $A = \{\beta_1, \dots \beta_r\}$ is finite, we may write $F[\beta_1, \dots, \beta_r]$ to mean $F[A]$;
- If $A = \{\beta_1, \dots \beta_r\}$ is finite, we may write $F(\beta_1, \dots, \beta_r)$ to mean $F(A)$.

For example $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2}\}$. In this case, $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}]$. Also, $\mathbb{Q}[\sqrt{2}]/\mathbb{Q}$ is a field extension.

If $E/F$ is a field extension and $\beta \in E$, then

$$F[\beta] = \{f(\beta) \mid f \in F[x]\}.$$

**Definition 3.** The *degree* of the extension $E/F$, denoted $[E : F]$, is the dimension of $E$ as a vector space over $F$.

For example, $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$.

**Proposition 1.** *Let $F \subset K \subset E$ be fields. Then*

**(a)** $[K : F] = 1$ *if and only if* $K = F$.
**(b)** $[K : F] = [E : F]$ *if and only if* $K = E$.

**Definition 4.** Let $E$ be a field which contains a field $F$.

We say that $f \in F[x]$ *annihilates* $\beta \in E$ is $f(\beta) = 0$.

We say that $\beta \in E$ is *algebraic* over $F$ if $f(\beta) = 0$ for some nonzero $f \in F[x]$.

We say that $\beta \in E$ is *transcendental* over $F$ if it is not algebraic over $F$. In this case, the only polynomial which annihilates $\beta$ is the zero polynomial.

Typically, if the base field $F$ is not specifically mentioned, it is assumed to be $\mathbb{Q}$. For example, $\sqrt{2}$ and $\sqrt[3]{2 + \sqrt{5}}$ are algebraic, but Hadlock shows (§1.7) that $\pi$ is transcendental. It is also known that $e$ is transcendental, and in fact, the cardinality of the transcendental numbers exceeds that of the algebraic numbers.

---

*Date*: December 4, 2006.

## 2. Minimum Polynomials

**Proposition 2.** *Let $E/F$ be a field extension and let $\beta \in E$ be algebraic over $F$. Then there exists a unique monic polynomial $f \in F[x]$ of minimal degree which annihilates $\beta$. Every nonzero polynomial which annihilates $\beta$ is a multiple of $f$.*

*Proof.* Let

$$D = \{d \in \mathbb{Z} \mid d = \deg(f) \text{ for some nonzero } f \in F[x] \text{ with } f(\beta) = 0\}.$$

Since $\beta$ is algebraic, $D$ is a nonempty set of positive integers, and so has a minimum element, say $d$. Let $f \in F[x]$ with $d = \deg(f)$ and $f(\beta) = 0$.

Recall that a polynomial is *monic* if the leading coefficient is one. If we divide by the leading coefficient of $f$, we obtain a polynomial which is monic and still has $\beta$ as a root; thus we may assume that $f$ is monic. Thus, $f$ is a monic polynomial of minimal degree which annihilates $\beta$.

To show that any other polynomial which annihilates $\beta$ is a multiple of $f$, suppose that $g \in F[x]$ with $g(\beta) = 0$. By the division algorithm, $g = fq + r$ for some $q, r \in F[x]$, where $\deg(r) < \deg(f)$. Then

$$0 = g(\beta) = f(\beta)q(\beta) + r(\beta) = 0 + r(\beta) = r(\beta);$$

thus $r(\beta) = 0$, and since $f$ has minimal degree among nonzero polynomials which have $\beta$ as a root, we must have $r = 0$. Then $g = fq$.

To show that $f$ is unique, suppose that $g$ is another monic polynomial of minimal degree which annihilates $\beta$. Then $g$ is a multiple of $f$, so $g = fq$ for some $q$. But since $\deg(f) = \deg(g)$, we must have $\deg(q) = 0$, so $q$ is a constant. Since $f$ is monic, the leading coefficient of $g = fq$ is $q$; now since $g$ is monic, we must have $q = 1$. Thus $g = f$. □

**Definition 5.** Let $E/F$ be a field extension and let $\beta \in E$ be algebraic over $F$.

The *minimum polynomial* of $\beta$ over $F$, denoted $\min(\beta/F)$, is the unique monic polynomial of minimal degree which annihilates $\beta$.

The *degree* of $\beta$ over $F$, denoted $\deg(\beta/F)$, is the degree of $\min(\beta/F)$.

**Proposition 3.** *Let $E/F$ be a field extension and let $\beta \in E$ be algebraic over $F$. Let $f \in F[x]$ be a monic polynomial which annihilates $\beta$. Then $f$ is the minimum polynomial of $\beta$ if and only if $f$ is irreducible.*

*Proof.* Let $f$ be the minimum polynomial of $\beta$ and let $g$ be a monic irreducible polynomial which annihilates $\beta$; it suffices to show that $f = g$. Now $g$ is a multiple of $f$ by Proposition 2, so $g = af$; but since $g$ is irreducible, so either $a$ or $f$ is a constant. But $f$ is nonzero and annihilates $\beta$, so it is not constant; thus $a$ is constant. Since $f$ is monic, $a$ is the leading coefficient of $g = af$. Since $g$ is monic, $a = 1$, and $f = g$. □

## 3. Primitive Extensions

**Definition 6.** Let $E/F$ be a field extension. We say that $E/F$ is a *primitive extension* if $E = F[\beta]$ for some $\beta \in F$ which is algebraic over $F$. In this case, we call $\beta$ a *primitive element* for $E/F$.

**Proposition 4.** *Let $E/F$ be a field extension and let $\beta \in E$. Then*

$$F[\beta] = \{\gamma \in E \mid \gamma = g(\beta) \text{ for some } g \in F[x]\}.$$

*Proof.* Since $F[\beta]$ contains $F$ and $\beta$ and is closed under addition and multiplication, it must contain $g(\beta)$ for every $g \in F[x]$. But $\{g(\beta) \mid g \in F[x]\}$ is itself a ring, since it is closed under addition and multiplication. □

**Proposition 5.** *Let $E/F$ be a field extension and let $\beta \in F$ be algebraic over $F$. Then*

$$F[\beta] = \{\gamma \in E \mid \gamma = g(\beta) \text{ for some } g \in F[x] \text{ with } \deg(g) < \deg(\beta/F)\}.$$

*Proof.* In light of the Proposition 4, it suffices to show that for every $h \in F[x]$ there exists $g \in F[x]$ with $\deg(g) < \deg(\beta/F)$ such that $h(\beta) = g(\beta)$. This will follow from the division algorithm.

Let $f = \min(\beta/F)$. Then $h = fq + r$ for some $q, r \in F[x]$ where $\deg(r) < \deg(f)$. Thus $h(\beta) = f(\beta)q(\beta) + r(\beta) = 0 \cdot q(\beta) + r(\beta) = r(\beta)$. Set $g = r$. □

**Proposition 6.** *Let $E/F$ be a field extension and let $\beta \in E$. Then $\beta$ is algebraic over $F$ if and only if $F[\beta]$ is a field.*

*Proof.* We prove both directions of the implication; clearly, we may assume $\beta \neq 0$.

($\Rightarrow$) Suppose that $\beta$ is algebraic over $F$; it suffices to show that $F[\beta]$ contains the inverse of each nonzero element in it.

Let $f = \min(\beta/F)$, and let $\gamma \in F[\beta]$ be nonzero; then $\gamma = g(\beta)$ for some $g \in F[x]$ with $\deg(g) < \deg(f)$. Since $f$ is irreducible and $\deg(g) < \deg(f)$, we must have $\gcd(f, g) = 1$. By the Euclidean algorithm for polynomials, there exist $s, t \in F[x]$ such that $fs + gt = 1$. These are polynomials, so we can evaluate them at $\beta$ to obtain $f(\beta)s(\beta) + g(\beta)t(\beta) = 1$. Since $f(\beta) = 0$, this produces $g(\beta)t(\beta) = 1$. Thus $t(\beta)$ is the inverse of $g(\beta) = \gamma$.

($\Leftarrow$) Suppose that $F[\beta]$ is a field. We know that $F[\beta] = \{g(\beta) \mid g \in F[x]\}$. Thus, since $\beta^{-1} \in F[\beta]$, then $\beta^{-1} = g(\beta)$ for some $g \in F[x]$. Thus $\beta g(\beta) - 1 = 0$, so $xg(x) - 1$ is a polynomial over $F$ which annihilates $\beta$. □

Note that this proof in *constructive*; it tells us how to find the inverse.

**Proposition 7.** *Let $E/F$ be a field extension and let $\beta \in F$ be algebraic over $F$. Let $d = \deg(\beta/F)$. Then $B = \{1, \beta, \ldots, \beta^{n-1}\}$ is a basis for $F[\beta]$ as a vector space over $F$. Consequently, $[F[\beta] : F] = \deg(\beta/F)$.*

*Proof.* By Proposition 5, $B$ spans $F[\beta]$; thus we only have to show that the set $B$ is linearly independent. Let $a_1, \ldots, a_n \in F$ such that

$$\sum_{i=0}^{n-1} a_i \beta^i = 0.$$

Let $g(x) = \sum_{i=0}^{n-1} a_i x^i$; now this is a polynomial of degree less that the degree of $\beta$ over $F$ which annihilates $\beta$, so it is the zero polynomial. Thus $a_i = 0$ for all $i$, proving independence. □

## 4. Finite Extensions

**Definition 7.** Let $E/F$ be a field extension. We say that $E/F$ is a *finite extension* if $E$ has a finite basis as a vector space over $F$.

**Proposition 8** (Product of Degrees Formula)**.** *Let $E/F$ and $K/E$ be finite extensions. Then $K/F$ is a finite extension, and*

$$[K : F] = [K : E][E : F].$$

*Proof.* Let $\{u_1, \ldots, u_m\}$ be a basis for $E/F$ and let $\{v_1, \ldots, v_n\}$ be a basis for $K/E$. Set

$$B = \{u_i v_j \mid i = 1, \ldots, m \text{ and } j = 1, \ldots, n\};$$

we claim that $B$ is a basis for $K/F$.

Let $x \in K$. Then there exist $a_1, \ldots, a_n \in E$ such that $x = a_1 v_1 + \cdots + a_n v_n$. But for $j = 1, \ldots, n$ there exist $b_{1,j}, \ldots, b_{m,j} \in F$ such that $a_i = b_{1,i} u_1 + \cdots + b_{m,i} u_m$, so that $x = \sum_j \sum_i b_{i,j} u_i v_j$. Thus $B$ spans $K/F$, and $K/F$ is finite.

Now suppose that $\sum_{i,j} b_{i,j} u_i v_j = 0$. By the linear independence of the $v_j$'s, we have that $\sum_i b_{i,j} u_i = 0$ for $j = 1, \ldots, n$, and so by the linear independence of the $u_i$'s, each $b_{i,j} = 0$. Thus $B$ is linearly independent and is therefore a basis. Since $|B| = mn$, $K/F$ has dimension $mn$, so $[K : F] = [K : E][E : F]$. □

**Proposition 9** (Product of Degrees Inequality)**.** *Let $E/F$ be a field extension and let $\beta_1, \ldots, \beta_n \in E$ be algebraic over $F$. Let $L = F[\beta_1, \ldots, \beta_n]$. Then $L/F$ is finite, and*

$$[L : F] \leq \prod_{i=1}^{n} [F[\beta_i] : F].$$

*Proof.* Let $K = F[\beta_1, \ldots, \beta_{n-1}]$; by induction, we assume that

$$[K : F] \leq \prod_{i=1}^{n-1} [F[\beta_i] : F].$$

Let $f$ be the minimum polynomial of $\beta_n$ over $F$. Then the coefficients of $\beta_n$ are in $K$, so view $f \in K[X]$. Since $f(\beta_n) = 0$, $\beta_n$ is algebraic over $K$, and the minimum polynomial of $\beta_n$ over $K$ is a factor of $f$. In particular, the degree of this minimum polynomial is less than or equal to $\deg(f) = [F[\beta_n] : F]$. Thus

$$[L : F] = [K[\beta_n] : K][K : F] \leq [F[\beta_n] : F] \prod_{i=1}^{n-1} [F[\beta_i] : F] = \prod_{i=1}^{n} [F[\beta_i] : F].$$

□

## 5. Algebraic Extensions

**Definition 8.** Let $E/F$ be a field extension. We say that $E/F$ is an *algebraic extension* if every element of $E$ is algebraic over $F$.

**Proposition 10.** *Let $E/F$ be a finite extension.*
*Then $E/F$ is an algebraic extension.*

*Proof.* Let $\beta \in E$; we wish to show that $\beta$ is algebraic over $F$.

Since $E/F$ is finite, it has a finite dimension, say $[E : F] = n$. Then any set of $n+1$ elements of $E$ is linearly dependent over $F$. Thus the set $\{1, \beta, \ldots, \beta^n\}$ is linearly dependent over $F$, so there exists a nontrivial dependence relation from this set. That is, there exist $a_0, a_1, \ldots, a_n \in F$, not all zero, such that

$$\sum_{i=0}^{n} a_i \beta^i = 0.$$

If we set $f(x) = \sum_{i=0}^{n} a_i x^i$, we obtain a nonzero polynomial in $F[x]$ which annihilates $\beta$. Thus, $\beta$ is algebraic over $F$. □

We are now ready to prove §1.5 Theorem 8 from Hadlock without matrix computations, determinants, and the theory of eigenvalues.

**Proposition 11.** *Let $E/F$ be a field extension and let $\alpha, \beta \in E$ be nonzero and algebraic over $F$. Then $\alpha + \beta$, $\alpha\beta$, $-\beta$, and $\beta^{-1}$ are algebraic over $F$.*

*Proof.* Let $L = F[\alpha, \beta]$. By Proposition 9, $[L : F] \leq [F[\alpha] : F][F[\beta] : F] < \infty$, so $L/F$ is a finite extension. By Proposition 10, $L/F$ is an algebraic extension, so every element of $L$ is algebraic over $F$. Clearly $\alpha + \beta \in L$ and $\alpha\beta \in L$, so they are algebraic over $F$. Moreover, since $\beta$ is algebraic over $F$, $F[\beta]$ is a field, and $F[\beta]/F$ is a finite extension, and therefore is an algebraic extension. Since $-\beta$ and $\beta^{-1}$ are in $F[\beta]$, they are algebraic over $F$. □

**Corollary 1.** *Let $\mathbb{A} = \{z \in \mathbb{C} \mid z \text{ is algebraic over } \mathbb{Q}\}$. Then $\mathbb{A}$ is a subfield of $\mathbb{C}$.*

## 6. Splitting Extensions

**Definition 9.** Let $E/F$ be a field extension and let $f \in F[x]$.

We say that $f$ *splits* over $E$ if $f$ is a product of linear factors in $E[x]$.

We say that $E/F$ is a *splitting extension*, or that $E$ is a *splitting field* for $f$ over $F$, if $f$ splits over $E$ and $E$ is generated over $F$ by the roots of $f$. That is,

**(a)** $f(x) = \prod_{i=1}^{n} c(x - \alpha_i)$ for some $c \in F$ and $\alpha_1, \ldots, \alpha_n \in E$, and
**(b)** $E = F[\alpha_1, \ldots, \alpha_n]$.

The first key fact about splitting extensions is that they exist. This is typically shown using the ring theoretical concept of ideals, but in this case, the proof boils down to the following construction.

**Proposition 12.** *Let $F$ be a field and let $f \in F[x]$. Then there exists a field $E$ containing $F$ and an element $\beta \in E$ such that $f(\beta) = 0$.*

*Proof.* Without loss of generality, $f$ is irreducible over $F$. Define an equivalence relation on $F[x]$ by

$$g \equiv h \quad \Leftrightarrow \quad f \mid (g - h);$$

that is, two polynomials are equivalent if and only if their difference is divisible by $f$. For $g \in F[x]$, the *equivalence class* of $g$ is

$$\overline{g} = \{h \in F[x] \mid g \equiv h\}.$$

Let $E = \{\overline{g} \mid g \in F[x]\}$. Distinct constant polynomials (elements of $F$) are not equivalent to each other; identify $F$ with the set of equivalence classes of constant polynomials, so that $a \in F$ implies $\overline{a} = a$, and $E$ contains $F$.

Define addition and multiplication on $E$ by $\overline{g} + \overline{h} = \overline{g + h}$, and $\overline{gh} = \overline{g}\overline{h}$. Using the fact that $f$ divides $g - h$, one may show that these operations are well-defined, and in fact, $\overline{E}$ together with these operations is a field.

Note that if $g \in F[x]$, divide $g$ by $f$ to obtain $g = fq + r$, where $q, r \in F[x]$ and $\deg(r) < \deg(f)$. Then $\overline{g} = \overline{r}$. In particular, $\overline{f} = 0$.

We now have a field $E$ which contains the field $F$, and $E/F$ is a field extension. So, if $g \in F[x]$, we may evaluate $g$ at an element $\overline{h} \in E$, and obtain some other element in $E$ which is, in fact, the equivalence class of the composition $g \circ h$.

Consider the polynomial $g(x) = x$; let $\overline{x}$ denote its equivalence class. Set $\beta = \overline{x}$, and consider what happens when we evaluate the polynomial $f$ at the element $\beta$. Let $f(x) = \sum_{i=0}^{n} a_i x^i$ with coefficients $a_i \in F$; now $\overline{a_i} = a_i$, so

$$f(\beta) = f(\overline{x}) = \sum_{i=0}^{n} a_i \overline{x}^i = \sum_{i=0}^{n} \overline{a_i}\overline{x^i} = \overline{\sum_{i=0}^{n} a_i x^i} = \overline{f} = 0.$$

Thus $\beta$ is a root of $f$ in $E$. □

**Proposition 13.** *Let $F$ be a field and let $f \in F[x]$. Then there exists a field $E$ which is a splitting field of $f$ over $F$.*

*Proof.* By induction, we may assume that splitting fields exist for polynomials of degree less than that of $f$. Apply the above proposition to obtain a field $K$ which contains a root $\beta$ of $f$. Let $h \in K[x]$ be given by $h(x) = x - \beta$. Now $f, h \in K[x]$, and $h$ divides $f$, so $f = hq$ for some $q \in K[x]$. Since $\deg(q) < \deg(f)$, there exists a field $E$ which is a splitting field of $q$ over $K$. Clearly, $E$ is a splitting field of $f$ over $F$. □

## 7. Multiple Roots

We wish to show that if $E/F$ is a field extension and $\alpha, \beta \in E$ are algebraic over $F$, then there exists $\gamma \in F$ which is algebraic over $F$ such that $F[\alpha, \beta] = F[\gamma]$. Unfortunately, this is not true in complete generality; it is, however, true if $E$ is a subfield of $\mathbb{C}$. There are two properties of $\mathbb{C}$ which we need for the proof. The first is that any subfield of $\mathbb{C}$ is infinite, and the second is that irreducible polynomials over $\mathbb{C}$ do not have multiple roots; this leads to the abstract definition of separability. We now outline the proof of this fact; the astute reader will ask where the fact that the coefficients are complex numbers is being used.

**Definition 10.** Let $E/F$ be an algebraic field extension.

Let $f \in F[x]$ and let $\beta \in E$. We say that $\beta$ is a *multiple root* of $f$ if $(x - \beta)^2$ is a factor of $f$ over $F[\beta]$.

A polynomial is said to have distinct roots if it does not have multiple roots. To prove that polynomials over subfields of $\mathbb{C}$ have no multiple roots, we use the derivative of the polynomial. Note that, for polynomials, the derivative may be defined in a completely formal (algebraic) way.

**Definition 11.** Let $f \in \mathbb{C}[x]$. If $f(x) = \sum_{i=0}^{n} a_i x^i$, where $a_i \in F$, define the *derivative* of $f$ is the polynomial $f' \in \mathbb{C}[x]$ given by $f'(x) = \sum_{i=0}^{n-1} (i+1) a_{i+1} x^i$.

**Proposition 14** (Product Rule)**.** *Let $f, g \in \mathbb{C}[x]$. Then $(fg)' = fg' + f'g$.*

*Proof.* Assign coefficients to $f$ and $g$, compute the product and take the derivative to obtain $(fg)'$. Then compute $fg' + f'g$, and compare coefficients. □

**Proposition 15.** *Let $f \in \mathbb{C}[x]$, and let $r_1, \ldots, r_n$ be the (not necessarily distinct) roots of $f$, so that $f(x) = \prod_{i=1}^{n} (x - r_i)$. Then*

$$f'(x) = \sum_{i=1}^{n} \prod_{j \neq i} (x - r_j).$$

*Proof.* This follows from the product rule and induction. □

**Proposition 16.** *Let $f \in \mathbb{C}[x]$, and let $\beta \in \mathbb{C}$ with $f(\beta) = 0$. Then $\beta$ is a multiple root of $f$ if and only if $f'(\beta) = 0$.*

*Proof.* Let $r_1, \ldots, r_n$ be the (not necessarily distinct) roots of $f$; we have

$$f'(x) = \sum_{i=1}^{n} \prod_{j \neq i} (x - r_j).$$

Since $\beta$ is a root of $f$, $\beta = r_k$ for some $k$. Then $\beta$ is a root of $\prod j \neq i (x - r_j)$, so long as $i \neq k$. Thus $\beta$ is a root of $f'$ if and only if $\beta$ is a root of $\prod_{j \neq k} (x - r_j)$, and this happens only if $\beta = r_j$ for some $j \neq k$, in which case $\beta$ is a multiple root, since $\beta = r_j$ and $\beta = r_k$. □

**Proposition 17.** *Let $f \in \mathbb{C}[x]$ be irreducible over a subfield $F \subset \mathbb{C}$. Then $f$ has no multiple roots.*

*Proof.* Without loss of generality, $f$ is monic. Let $\beta$ be a root of $f$. Since $f$ is irreducible, it is the minimum polynomial of $\beta$. Thus no nonzero polynomial of lower degree annihilates $\beta$. Thus, $\beta$ is not a root of $f'(x)$, so $\beta$ is not a multiple root of $f$. □

## 8. Separable Extensions

**Definition 12.** Let $E/F$ be an algebraic field extension.

If $f \in F[x]$, we say that $f$ is *separable* if $f$ has $\deg(f)$ distinct roots in a splitting field for $f$ over $F$.

We say that $E/F$ is *separable* if for every $\beta \in E$, the minimum polynomial of $\beta$ over $F$ is separable.

**Proposition 18.** *Let $E/F$ be a finite separable extension. Let $\alpha, \beta \in E$ be algebraic over $F$. Then there exists $\gamma \in E$ which is algebraic over $F$ such that*

$$F[\gamma] = F[\alpha, \beta].$$

*Proof.* Assume that $F$ is infinite; the proof for the finite case is handled separately, and we will not discuss this here.

Let $f = \min(\alpha/F)$ and $g = \min(\beta/F)$. Let $r = \deg(f)$ and $s = \deg(g)$. Let $K/F$ be a splitting extension for $fg$; clearly, $K$ contains splitting fields for $f$ and $g$ over $F$. Since $E/F$ is separable, $f$ and $g$ have distinct roots in $K$. Let $a_1, \ldots, a_r$ be the distinct roots of $f$ in $K$, and let $b_1, \ldots, b_s$ be the distinct roots of $g$ in $K$.

Consider the polynomial

$$p(x) = \prod_{i=1}^{r} \prod_{j=1}^{s} \Big[ (a_i x + b_j) - (\alpha x + \beta) \Big].$$

This is a polynomial of degree $rs$ so it has at most $rs$ roots in $F$. Since $F$ is infinite, there exists $c \in F$ such that $p(c) \neq 0$.

Define $\gamma = \alpha c + \beta$; we will show that $\gamma$ is a primitive element for $F[\alpha, \beta]$ over $F$. Certainly $\gamma \in F[\alpha, \beta]$, so $F[\gamma] \subset F[\alpha, \beta]$. If we show that $\alpha \in F[\gamma]$, then $\beta = \gamma - \alpha c$ will also be in $F[\gamma]$, so then $F[\alpha, \beta] \subset F[\gamma]$. Thus it remains to show that $\alpha \in F[\gamma]$.

Let $h(x) = g(\gamma - cx)$; this is a polynomial over $F[\gamma]$. Also, $f(x)$ is a polynomial over $F[\gamma]$, so $\gcd(f, h)$ is a polynomial of $F[\gamma]$. We note that $h(\alpha) = g(\gamma - c\alpha) = g(\beta) = 0$; therefore $\alpha$ is a common root of $f$ and $h$, and $(x - \alpha)$ is a factor of $\gcd(f, h)$. If $\gcd(f, h)$ has another factor, then it has another linear factor over $K$; any other linear factor of $\gcd(f, h)$ must be of the form $(x - a)$, where $a$ is a root of $f$.

Since $\alpha$ is not a multiple root of $f$, the remaining linear factors of $f$ are of the form $(x - a_i)$, where $a_i \neq \alpha$. But if $(x - a_i)$ is a factor of $\gcd(f, h)$, then $(x - a_i)$ also divides $h(x)$, so $a_i$ is a root of $h$. Suppose this is the case; then $0 = h(a_i) = g(\gamma - ca_i)$, so $\gamma - ca_i = b_j$ for some $j$. Therefore $a_i c + b_j - \gamma = 0$, that is, $(a_i c + b_j) - (\alpha c + \beta) = 0$. In this case, $c$ is a root of $p(x)$, a contradiction.

Therefore, $\gcd(f, h) = (x - \alpha)$ is a polynomial over $F[\gamma]$, whence $\alpha \in F[\gamma]$. □

**Theorem 1** (Primitive Element Theorem)**.** *Let $E/F$ be a finite separable extension. Then there exists $\gamma \in E$ such that $E = F[\gamma]$.*

*Proof.* We may assume that $E$ is larger than $F$. By induction on the degree $[E : F]$, we may also assume that every proper subfield of $E$ which contains $F$ has a primitive element over $F$. Thus let $K$ be a maximal proper subfield of $E$ which contains $F$; then $K = F[\alpha]$ for some $\alpha \in K$. Let $\beta \in E \setminus F$; then $E = K[\beta]$, for otherwise, $K$ would not be maximal among proper subfields. Thus $E = F[\alpha, \beta]$. Now by the Primitive Element Theorem, there exists $\gamma \in E$ such that $F[\gamma] = F[\alpha, \beta]$. □

## 9. Ring Homomorphisms

**Definition 13.** A *ring homomorphism* is a function $\phi : R \to S$, where $R$ and $S$ are rings, which satisfies:

**(H0)** $\phi(1_R) = 1_S$;
**(H1)** $\phi(a + b) = \phi(a) + \phi(b)$;
**(H2)** $\phi(ab) = \phi(a)\phi(b)$.

**Example 1.** Let $n \in \mathbb{Z}$, $n \geq 2$. Then $\mathbb{Z}$ and $\mathbb{Z}_n$ are rings, and let $\xi = \xi_n$ be the residue map

$$\xi : \mathbb{Z} \to \mathbb{Z}_n \quad \text{given by} \quad a \mapsto \overline{a},$$

where $\overline{a}$ is the remainder when $a$ is divided by $n$. Then $\xi$ is a ring homomorphism.

**Example 2.** Consider the function

$$\phi : \mathbb{C} \to \mathbb{C} \quad \text{given by} \quad z \mapsto= \overline{z},$$

where $\overline{z}$ is the complex conjugate of $z$. Then $\phi$ is a ring homomorphism.

**Proposition 19** (Properties of Ring Homomorphisms)**.** *Let $\phi : R \to S$ be a ring homomorphism. Then*

**(a)** *$\phi(0_R) = 0_S$;*
**(b)** *$\phi(-a) = -\phi(a)$ for all $a \in R$;*
**(c)** *if $a \in R$ is invertible, then so is $\phi(a)$, and $\phi(a^{-1}) = \phi(a)^{-1}$.*

*Proof.* Note that

$$\phi(0_R) = \phi(0_R + 0_R) = \phi(0_R) + \phi(0_R).$$

Thus $\phi(0_R) + \phi(0_R) = 0_S + \phi(0_R)$, and by the cancellation law of addition, $\phi(0_R) = 0_S$.

Now for $a \in R$,

$$\phi(a) + \phi(-a) = \phi(a - a) = \phi(0_R) = 0_S,$$

which shows that $\phi(-a)$ is an additive inverse of $\phi(a)$; by uniqueness of inverses, $\phi(-a) = -\phi(a)$.

Suppose that $a \in R$ is invertible. Then

$$\phi(a)\phi(a^{-1}) = \phi(aa^{-1}) = \phi(1_R) = 1_S,$$

which shows that the inverse of $\phi(a)$ is $\phi(a^{-1})$. □

**Proposition 20.** *Let $\phi : R \to S$ and $\psi : S \to T$ be ring homomorphisms. Then $\psi \circ \phi : R \to T$ is a ring homomorphism.*

*Proof.* Let $a, b \in R$. Then

$$(\psi \circ \phi)(a+b) = \psi(\phi(a+b)) = \psi(\phi(a)+\phi(b)) = \psi(\phi(a)) + \psi(\phi(b)) = (\psi \circ \phi)(a) + (\psi \circ \phi)(b),$$

and

$$(\psi \circ \phi)(ab) = \psi(\phi(ab)) = \psi(\phi(a)\phi(b)) = \psi(\phi(a))\psi(\phi(b)) = (\psi \circ \phi)(a)(\psi \circ \phi)(b).$$

□

**Proposition 21.** *Let $\phi : R \to S$ be a ring homomorphism. Then*

$$\phi(R) = \{s \in S \mid s = \phi(r) \text{ for some } r \in R\}$$

*is a subring of $S$.*

*Proof.* We verify the properties of a subring.

**(S0)** Since $\phi(1_R) = 1_S$, we have $1_S \in \phi(R)$.

**(S1)** and **(S2)** Let $r, s \in \phi(R)$. Then $r = \phi(a)$ and $s = \phi(b)$ for some $a, b \in R$. Now $a + b, ab \in R$, so $\phi(a + b), \phi(ab) \in \phi(R)$. But $\phi(a + b) = \phi(a) + \phi(b) = r + s$, and $\phi(ab) = \phi(a)\phi(b) = rs$. □

**Proposition 22.** *Let $E/F$ be a field extension, and let $\beta \in E$. Define a function*

$$\epsilon : F[x] \to E \quad \text{given by} \quad f \mapsto f(\beta).$$

*Then $\epsilon$ is a ring homomorphism, called the* evaluation map*, whose image is $F[\beta]$.*

*Proof.* The *definition* of polynomial addition in $F[x]$ we gave is that $f + g$ is the unique function from $F$ to itself which satisfies $(f + g)(x) = f(x) + g(x)$ for every $x \in F$. Thus, $\epsilon(f + g) = (f + g)(\beta) = f(\beta) + g(\beta) = \epsilon(f) + \epsilon(g)$. This is equally true for multiplication. The constant polynomial 1 is mapped to 1 evaluated at $\beta$, which is still 1. Thus $\epsilon$ is a ring homomorphism.

We have previously seen that $F[\beta] = \{g(\beta) \mid g \in F[x]\}$, which is clearly the image of $\epsilon$. □

**Definition 14.** Let $\phi : R \to S$ be a ring homomorphism.

We say that $\phi$ is a *monomorphism* if $\phi$ is injective.

We say that $\phi$ is an *epimorphism* if $\phi$ is surjective.

We say that $\phi$ is an *isomorphism* if $\phi$ is bijective.

We say that $\phi$ is an *endomorphism* if $S = R$.

We say that $\phi$ is an *automorphism* if $\phi$ is bijective and $S = R$.

**Proposition 23.** *The composition of monomorphisms, epimorphisms, isomorphisms, endomorphisms, or automorphisms is again a monomorphism, epimorphism, isomorphism, endomorphism, or automorphism, respectively.*

*Proof.* The composition of injective functions is injective, the composition of surjective functions is surjective, the composition of functions from a set into itself is again a function from the set into itself. Finally, the composition of homomorphisms is a homomorphism. □

**Proposition 24.** *Let $\phi : R \to S$ be a ring isomorphism. Then $\phi$ is invertible, and if $\psi : S \to R$ is its inverse, then $\psi$ is a ring isomorphism.*

*Proof.* Since $\phi$ bijective, it is invertible; let $\psi$ denote its inverse. The inverse of a bijective function is bijective, so $\psi$ is bijective. We wish to show that $\psi$ is a homomorphism.

Let $r, s \in S$. Since $\psi$ is bijective, it is surjective, so there exist $a, b \in R$ such that $\phi(a) = r$ and $\phi(b) = s$. Then $\psi(r + s) = \psi(\phi(a) + \phi(b)) = \psi(\phi(a + b)) = a + b = \psi(r) + \psi(s)$, and $\psi(rs) = \psi(\phi(a)\phi(b)) = \psi(\phi(ab)) = ab = \psi(r)\psi(s)$. □

## 10. Field Homomorphisms

**Proposition 25.** *Let $\phi : F \to S$ be a ring homomorphism. If $F$ is a field, then $\phi$ is injective.*

*Proof.* Let $x_1, x_2 \in F$, and suppose that $\phi(x_1) = \phi(x_2)$. Then $\phi(x_1 - x_2) = 0_S$, and since $0_S$ is not invertible, it must be the case that $x_1 - x_2$ is not invertible. The only noninvertible element in $F$ is $0_F$, so $x_1 - x_2 = 0_F$; thus $x_1 = x_2$. Thus $\phi$ is injective. □

**Definition 15.** Let $F$, $K$, and $L$ be fields such that $F \subset K \cap L$, and let $\phi : K \to L$ be a homomorphism. We say that $\phi$ *fixes* $F$ if $\phi(a) = a$ for every $a \in F$.

**Proposition 26.** *Let $K/F$ and $L/F$ be field extensions, and let $\phi : K \to L$ be a homomorphism which fixes $F$. Let $f \in F[x]$ and $\beta \in K$. Then $f(\beta) \in K$, $f(\phi(\beta)) \in L$, and*

$$f(\phi(\beta)) = \phi(f(\beta)).$$

*Proof.* Let $f(x) = \sum_{i=0}^{n} a_i x^i$. Then

$$f(\phi(\beta)) = \sum_{i=0}^{n} a_i (\phi(\beta))^i = \sum_{i=0}^{n} a_i \phi(\beta^i) = \sum_{i=0}^{n} \phi(a_i \beta^i) = \phi\Big( \sum_{i=0}^{n} a_i \beta^i \Big) = \phi(f(\beta)).$$

□

**Definition 16.** Let $E/F$ be a field extension and let $\alpha, \beta \in E$ be algebraic over $F$. We say that $\alpha$ and $\beta$ are *conjugate over* $F$ if $\alpha$ and $\beta$ have the same minimum polynomial over $F$.

**Proposition 27.** *Let $E/F$ be a field extension with $\alpha, \beta \in E$ conjugate over $F$. If $\alpha \in F[\beta]$, then $F[\alpha] = F[\beta]$.*

*Proof.* Clearly $F[\alpha] \subset F[\beta]$. But since $\alpha$ and $\beta$ have the same minimum polynomial, $[F[\alpha] : F] = [F[\beta] : F]$. Thus $[F[\beta] : F[\alpha]] = 1$, which says that $F[\alpha] = F[\beta]$. □

**Proposition 28.** *Let $E/F$ and $K/F$ be field extensions, and let $\beta \in E$ be algebraic. If $\phi : E \to K$ is a field homomorphism which fixes $F$, then $\beta$ and $\phi(\beta)$ are conjugate over $F$.*

*Proof.* Let $f$ be the minimum polynomial of $\beta$ over $F$. We have $f(\phi(\beta)) = \phi(f(\beta)) = \phi(0) = 0$; thus $f$ annihilates $\phi(\beta)$, and since $f$ is monic and irreducible, it is the minimum polynomial of $\phi(\beta)$. □

**Proposition 29.** *Let $E/F$ be a field extension and let $\alpha, \beta \in E$ be conjugates over $F$. Then there exists a unique isomorphism*

$$\phi : F[\alpha] \to F[\beta] \quad \text{such that} \quad \phi \text{ fixes } F \text{ and } \phi(\alpha) = \beta.$$

*Proof.* Every element of $F[\alpha]$ is of the form $g(\alpha)$ for some $g \in F[x]$. Define $\phi$ by $\phi(g(\alpha)) = g(\beta)$. Since there are many polynomials whose value at $\alpha$ are equal, we wish to show that this is *well-defined*; that is, for $\gamma \in F[\alpha]$, that the value of $\phi(\gamma)$ does not depend on the polynomial $g$ selected with $g(\beta) = \gamma$. It is here that we need $\alpha$ and $\beta$ to have the same minimum polynomial.

Let $f \in F[x]$ be the minimum polynomial of $\alpha$ and $\beta$, and let $g, h \in F[x]$ such that $g(\beta) = h(\beta)$. We wish to show that $g(\beta) = h(\beta)$. We have $g(\alpha) - h(\alpha) = 0$, so $(g - h)(\alpha) = 0$, so $g - h$ annihilates $\alpha$. Thus $f$ divides $g - h$, so $g - h = fr$ for some polynomial $r \in F[x]$ with $\deg(r) < \deg(f)$. Thus $g = h + fr$, so $g(\beta) = h(\beta) + f(\beta)r(\beta) = h(\beta)$. This completes the proof that $\phi$ is well-defined.

The elements of $F$ are contained in $F[\alpha]$ and $F[\beta]$ as the constant polynomials evaluated at $\alpha$ and $\beta$, respectively. But evaluating a constant polynomial gives the constant, whether we plug in $\alpha$ or $\beta$; thus if $a \in F$, then $g(x) = a$ is a constant polynomial, so $g(\alpha) = a$, and $\phi(a) = g(\beta) = a$.

Let $g(\alpha)$ and $h(\alpha)$ be arbitrary members of $F[\alpha]$. Now it is obvious that $\phi$ is a homomorphism, since

**(H0)** $\phi(1) = 1$;

**(H1)** $\phi(g(\alpha) + h(\alpha)) = \phi((g + h)(\alpha)) = (g + h)(\beta) = g(\beta) + h(\beta)$
$= \phi(g(\alpha)) + \phi(h(\alpha))$;

**(H2)** $\phi(g(\alpha)h(\alpha)) = \phi((gh)(\alpha)) = (gh)(\beta) = g(\beta)h(\beta) = \phi(g(\alpha))\phi(h(\alpha))$.

Finally, if $\phi$ fixes $F$ and $\phi(\alpha) = \beta$, then necessarily $\phi(g(\alpha)) = g(\phi(\alpha)) = g(\beta)$; thus the homomorphism constructed above is the only possible one with the desired properties, and is therefore unique. □

**Proposition 30.** *Let $E/F$ be an algebraic extension, and let $\phi : E \to E$ be a homomorphism which fixes $F$. Then $\phi$ is an automorphism.*

*Proof.* By hypothesis, $\phi$ is an endomorphism, and since $E$ is a field, $\phi$ is injective. Thus we show that $E$ is surjective.

Let $\beta \in E$; it suffices to show that $\beta = \phi(\alpha)$ for some $\alpha \in E$. Since $E/F$ is algebraic, $\beta$ is algebraic over $F$. Let $A$ denote the set of conjugates of $\beta$ in $E$. Since $\phi$ sends conjugates to conjugates, $\phi(A) = A$. Since $\phi$ is injective, the restriction of $\phi$ to $A$ is injective. An injective function from a finite set to itself is necessarily surjective, so $\phi$ restricted to $A$ is surjective. Since $\beta \in A$, $\beta = \phi(\alpha)$ for some $\alpha \in A \subset E$. Therefore, $\phi$ is surjective on $E$. □

## 11. Field Automorphisms

**Definition 17.** Let $E/F$ be a field extension. An *automorphism of $E/F$*, or an *automorphism of $E$ over $F$*, is an automorphism of $E$ which fixes $F$.

The set of all automorphisms of $E$ is denoted $\mathrm{Aut}(E)$. The set of all automorphisms of $E/F$ is denoted $\mathrm{Aut}(E/F)$.

Since the composition of automorphisms is an automorphism, the set $\mathrm{Aut}(E)$ is closed under composition of functions. Clearly $\mathrm{Aut}(E/F) \subset \mathrm{Aut}(E)$; moreover, since the composition of functions fixing $F$ also fixes $F$, we see that $\mathrm{Aut}(E/F)$ is also closed under composition of functions.

Suppose that $E/F$ is an algebraic extension; then every element of $E$ is algebraic over $F$. If $\phi \in \mathrm{Aut}(E/F)$ and $\alpha, \beta \in E$ with $\phi(\alpha) = \beta$, then $\alpha$ and $\beta$ have the same minimum polynomial; we have seen this. This greatly limits what can and cannot be an automorphism of an algebraic field extension, and puts a specific bound on the size of $\mathrm{Aut}(E/F)$.

**Proposition 31.** *Let $E = F[\beta]$, and let $m$ be the number of conjugates of $\beta$ in $E$. Then $|\mathrm{Aut}(E/F)| = m$. Hence $|\mathrm{Aut}(E/F)| \leq [E : F]$.*

*Proof.* For each conjugate of $\beta$ in $E$, there exists a unique automorphism of $E$ which fixes $F$ and sends $\beta$ to this conjugate. Since every automorphism sends $\beta$ to a conjugate, the number of automorphisms is equal to the number of conjugates $m$ of $\beta$ in $E$.

Let $f$ be the minimum polynomial of $\beta$ over $F$. The conjugates of $\beta$ are zeros of this polynomial, which must be less than or equal to its degree; since $[E : F] = \deg(f)$, we have $|\mathrm{Aut}(E/F)| = m \leq \deg(f) = [E : F]$. □

**Proposition 32.** *Let $E/F$ be a finite separable extension.*
*Then $\mathrm{Aut}(E/F) \leq [E : F]$.*

*Proof.* Since $E/F$ is finite and separable, the primitive element theorem dictates that $E/F$ has a primitive element. Thus $E = F[\beta]$ for some $\beta \in E$. The result follows. □

**Proposition 33.** *Let $K/F$ be an field extension, and let $E$ be a subfield of $K$ containing $F$ such that $E/F$ is a splitting extension. If $\phi$ is an automorphism of $K$ which fixes $F$, then $\phi(E) = E$.*

*Proof.* Let $f \in F[x]$ such that $E$ is a splitting field of $f$ over $F$, and let $\alpha_1, \ldots, \alpha_n$ be the roots of $f$ in $E$. Every element of $E$ is a linear combination over $F$ of powers of the roots of $f$.

Let $\beta \in E$; then $\beta = \sum_{i=1}^{m} a_i \alpha_{j_i}^{k_i}$ for some $a_i \in F$, $j_i$ between 1 and $n$, and $k_i \in \mathbb{Z}$. Since $\phi$ is an automorphism which fixes $F$, we have $\phi(\beta) = \sum_{i=1}^{m} a_i \phi(\alpha_{j_i})^{k_i}$, and since $\alpha_j \in E$ for all $j$, so is $\phi(\beta)$.

In other words, $\phi$ fixes $F$ and permutes the roots of $f$; moreover, $E$ is generated by these roots, so

$$\phi(E) = \phi(F[\alpha_1, \ldots, \alpha_n]) = F[\phi(\alpha_1), \ldots, \phi(\alpha_n)] = F[\alpha_1, \ldots, \alpha_n] = E.$$

□

## 12. Normal Extensions

**Definition 18.** Let $E/F$ be a field extension.

We say that $E/F$ is *normal* if every polynomial over $F$ which has a root in $E$ splits over $E$.

**Proposition 34.** *Let $K/F$ be an field extension, and let $E$ be a subfield of $K$ containing $F$ such that $E/F$ is normal and algebraic. If $\phi \in \mathrm{Aut}(K/F)$, then $\phi(E) = E$.*

*Proof.* Let $\alpha \in E$. Then $\alpha$ is algebraic over $F$, so $\alpha$ is the root of a polynomial $f \in F[x]$. Since $E/F$ is normal, $f$ splits in $E$ so all of the conjugates of $\alpha$ are in $E$. But $\phi(\alpha)$ must be a conjugate of $\alpha$, so $\phi(a) \in E$. This shows that $\phi(E) \subset E$.

Let $\beta \in \phi(E)$. Then $\beta = \phi(\alpha)$ for some $\alpha \in E$. Then $\alpha$ is a conjugate of $\beta$, and $\alpha \in E$, so $\beta \in E$. This shows that $\phi(E) \subset E$. □

**Proposition 35.** *Let $E/F$ be a finite, normal, and separable extension. Then $E$ is the splitting field for an irreducible polynomial over $F$ of degree $[E : F]$.*

*Proof.* Since $E/F$ is finite and separable, there exists $\beta \in E$ such that $E = F[\beta]$. Let $f$ be the minimum polynomial of $\beta$ over $F$; then $[E : F] = \deg(f)$. Since $E/F$ is normal, $f$ splits over $E$, so all of the roots of $f$ are in $E$. Since $E$ is generated over $F$ one of these roots, it is certainly generated over $F$ by all of the roots; thus $E$ is a splitting field for $f$ over $F$. □

**Proposition 36.** *Let $E/F$ be a finite, separable extension. The following conditions are equivalent:*

- **(i)** *$E$ is a splitting field of an irreducible polynomial over $F$ of degree $[E : F]$;*
- **(ii)** $|\mathrm{Aut}(E/F)| = [E : F]$.

*Proof.* **(i)** ⇒ **(ii)** Suppose that $E$ is a splitting field of an irreducible polynomial $f$ over $F$ of degree $[E : F]$. If $\beta$ is a root of $f$ in $E$, then $F[\beta] \subset E$, but also $[F[\beta] : F] = \deg(f) = [E : F]$. Therefore $E = F[\beta]$.

Now $f$ splits over $E$, so all of the roots of $f$ are in $E$. Since $E/F$ is separable, $f$ has distinct roots, so there are $\deg(f) = [E : F]$ roots of $f$ in $E$.

Given two roots $\beta_1, \beta_2 \in E$, there is a unique isomorphism which maps $F[\beta_1]$ onto $F[\beta_2]$ by fixing $F$ and sending $\beta_1$ to $\beta_2$. Since $F[\beta_1] = F[\beta_2] = E$, each of these isomorphisms is an automorphism of $E$; moreover, these are the only possible automorphisms of $E$. Thus $|\mathrm{Aut}(E/F)| = [E : F]$.

**(ii)** ⇒ **(i)** Suppose $|\mathrm{Aut}(E/F)| = [E : F]$. Since $E/F$ is finite and separable, there exists $\beta \in E$ such that $E = F[\beta]$.

The number of automorphisms of $E/F$ equals the number of roots of $f$ in $E$, which is $[E : F] = \deg(f)$. Thus all of the roots of $f$ are in $E$, so $E$ contains a splitting field for $f$ over $F$. Since $E$ is generated by one of the roots of $f$, we see that $E$ is a splitting field for $f$ over $F$. □

## 13. Extending Isomorphisms

We wish to show that splitting extensions are normal; we do this by showing that the unique isomorphism between primitive extensions of conjugates extends to an automorphism of the splitting extension. We begin with a technical lemma which serves as the induction step of the main argument.

**Proposition 37.** *Let $F$ be a field and let $\phi : F \to \widehat{F}$ be an isomorphism. For $g \in F[x]$ given by $g(x) = \sum_{i=0}^{m} b_i x^i$, define $\widehat{g} \in \widehat{F}[x]$ by $\widehat{g}(x) = \sum_{i=0}^{m} \phi(b_i) x^i$.*

*Let $E/F$ be an field extension and let $\beta \in E$ be algebraic over $F$ with minimum polynomial*

$$f(x) = \sum_{i=0}^{n} a_i x^i,$$

*where $a_i \in F$ so that $f \in F[x]$.*

*Let $\widehat{E}$ be a field containing $\widehat{F}$ such that there exists $\widehat{\beta} \in \widehat{E}$ with $\widehat{f}(\widehat{\beta}) = 0$.*

*Then there exists a unique isomorphism $\widehat{\phi} : F[\beta] \to \widehat{F}[\widehat{\beta}]$ such that $\widehat{\phi}(a) = \phi(a)$ for $a \in F$, and $\widehat{\phi}(\beta) = \widehat{\beta}$.*

*Proof.* The argument is analogous to that of Proposition 29; we give an outline.

It is clear that for $g, h \in F[x]$, $\widehat{gh} = \widehat{g}\widehat{h}$, and since $f$ is irreducible, $\widehat{f}$ is irreducible. Moreover, $\widehat{f}(\widehat{\beta}) = 0$. Thus $\widehat{f}$ is the minimum polynomial of $\widehat{\beta}$ over $\widehat{F}$.

Each element of $F[\beta]$ is of the form $g(\beta)$ for some polynomial $g \in F[x]$. Define $\widehat{\phi} : F[\beta] \to \widehat{F}[\widehat{\beta}]$ by $g(\beta) \mapsto \widehat{g}(\widehat{\beta})$. This is well-defined, because $g(\beta) = h(\beta)$ implies the $g - h$ is divisible by $f$, so $\widehat{g - h}$ is divisible by $\widehat{f}$, so $\widehat{g}(\widehat{\beta}) = \widehat{h}(\widehat{\beta})$. Moreover, this is an isomorphism of fields. □

**Proposition 38.** *Let $E/F$ be a separable splitting extension. Let $E_1, E_2$ be subfields of $E$ which contain $F$, and let $\phi : E_1 \to E_2$ be an isomorphism which fixes $F$. Then there exists a $\widehat{\phi} \in \mathrm{Aut}(E/F)$ such that $\widehat{\phi}(\alpha) = \phi(\alpha)$ for every $\beta \in E_1$.*

*Proof.* Let $g \in F[x]$ such that $f$ splits in $E$ and $E$ is generated over $F$ by the roots over $g$. If all of the roots of $g$ are in $E_1$, then $E_1 = E$, and $\phi$ maps $E$ into $E$. Since $\phi$ is injective, it is surjective on the finitely many roots of $g$, and thus $\phi(E) = E$; that is, $\phi$ is already an automorphism.

Otherwise, select a root $\beta$ of $g$ such that $\beta \notin E_1$. Let $f$ be the minimum polynomial of $\beta$ over $E_1$. Let $\widehat{f}$ be the polynomial obtained from $f$ by applying $\phi$ is the coefficients of $f$, as in the previous proposition. The roots of $\widehat{f}$ are also roots of $g$ (why?), and $g$ splits over $E$, so there is a root $\widehat{\beta}$ of $\widehat{f}$ in $E$. Thus there exists an isomorphism which sends $E_1[\beta]$ to $E_2[\widehat{\beta}]$.

Continue in this way until all of the roots of $g$ are being mapped; one arrives at an automorphism $\widehat{\phi}$ which extends $\phi$. □

**Proposition 39.** *Let $E/F$ be a separable splitting extension of a polynomial $f \in F[x]$. Let $\beta, \widehat{\beta} \in E$ be conjugate over $F$. Then there exists $\widehat{\phi} \in \mathrm{Aut}(E/F)$ such that $\widehat{\phi}(\beta) = \widehat{\beta}$.*

*Proof.* Apply Proposition with $E_1 = F[\beta]$, $E_2 = F[\widehat{\beta}]$, and $\widehat{\beta} : E_1 \to E_2$ the unique isomorphism which fixes $F$ and maps $\beta$ to $\widehat{\beta}$. □

**Proposition 40.** *Let $K/F$ be a normal extension and let $E \subset K$ be a splitting field of an irreducible polynomial over $F$. Then $E/F$ is normal.*

*Proof.* Since $E/F$ is a splitting extension, Proposition 33 tells us that every automorphism of $K$ restricts to an automorphism of $E$

Let $f \in F[x]$ be a polynomial with a root, say $\beta$, in $E$. Now $f$ splits in $K$; let $\widehat{\beta}$ be a root of $f$ in $K$. There exists $\phi \in \mathrm{Aut}(E/F)$ such that $\phi(\beta) = \widehat{\beta}$. But $\phi(E) = E$, so $\widehat{\beta} \in E$. Thus $f$ splits in $E$, so $E/F$ is normal. □

**Proposition 41.** *Let $E/F$ be a finite separable extension. The following conditions are equivalent:*

- **(i)** *$E/F$ is normal*
- **(ii)** *$E$ is a splitting field of a polynomial over $F$*
- **(iii)** $|\mathrm{Aut}(E/F)| = [E : F]$.

*Proof.* Since $E/F$ is finite and separable, there exists $\beta \in E$ such that $E = F[\beta]$. Let $f \in F[x]$ be the minimum polynomial of $\beta$ over $F$. Then $[E : F] = \deg(f)$. We prove **(ii)** ⇒ **(i)** ⇒ **(iii)**.

**(ii)** ⇒ **(i)** Suppose that $E$ is a splitting field of a polynomial over $F$. Let $g \in F[x]$ be a polynomial with a root in $E$. By Proposition 40, $E$ contains a splitting field for $g$ over $F$. Thus all of the roots of $g$ are in $E$, so $E/F$ is normal.

**(i)** ⇒ **(iii)** Suppose that $E/F$ is normal. Then $f$ splits over $E$, so all of the roots of $f$ are in $E$. Since $E/F$ is separable, $f$ has distinct roots, so there are $\deg(f) = [E : F]$ roots of $f$ in $E$. For each of these roots $\beta'$, there is a unique isomorphism which sends $F[\beta]$ to $F[\beta']$. Since $F[\beta'] = E$, this isomorphism is an automorphism of $E$, giving $[E : F]$ distinct automorphisms of $E/F$. Thus $|\mathrm{Aut}(E/F)| = [E : F]$.

**(iii)** ⇒ **(ii)** Suppose $|\mathrm{Aut}(E/F)| = [E : F]$. The number of automorphisms of $E/F$ equals the number of roots of $f$ in $E$, which is $[E : F] = \deg(f)$. Thus all of the roots of $f$ are in $E$, so $E$ contains a splitting field for $f$ over $F$. Since $E$ is generated by one of the roots of $f$, we see that $E$ is a splitting field for $f$ over $F$. □

## 14. Groups of Automorphisms

Let $E$ be a field, and let $\epsilon : E \to E$ denote the identity function from $E$ to itself. This is an automorphism of $E$. If $\phi, \psi \in \mathrm{Aut}(E)$, let $\phi\psi$ denote the composition of $\phi$ and $\psi$, and let $\phi^{-1}$ denote the inverse function. For example, $\phi^{-1}\phi = \epsilon$.

If $n$ is a positive integer, then $\phi^n$ means $\phi$ composed with itself $n$ times. Also $\phi^0 = \epsilon$ and $\phi^{-n} = (\phi^{-1})^n$.

**Definition 19.** Let $E$ be a field and let $G \subset \mathrm{Aut}(E)$. We say that $G$ is a *group of automorphisms* of $E$, if

- **(a)** $\epsilon \in G$;
- **(b)** $\phi, \psi \in G$ implies $\phi\psi \in G$;
- **(c)** $\phi \in G$ implies $\phi^{-1} \in G$.

If $G$ is nonempty and finite, the first and third conditions are superfluous. To see this, let $\phi \in G$. Note that since $G$ is finite, if we keep taking powers of $\phi$, we will eventually repeat; $\phi^n = \phi^m$ for some $m < n$. Then $\phi^{n-m} = \phi^n\phi^{-m} = \epsilon$, so $\epsilon \in G$, and condition **(a)** is extraneous. If $k$ is the smallest positive integer such that $\phi^k = \epsilon$, then $\phi^{k-1} = \phi^{-1}$, so condition **(c)** is extraneous.

**Definition 20.** Let $E$ be a field and let $G$ be a group of automorphisms of $E$. A *subgroup* of $G$ is a subset $H \subset G$ which is itself a group of automorphisms.

Note that $\mathrm{Aut}(E)$ is itself a group of automorphisms of $E$, and all other groups of automorphisms of $E$ are subgroups of $\mathrm{Aut}(E)$.

If $H$ is nonempty and finite, to see that $H$ is a subgroup of $G$, it suffices to check that $H$ is closed under composition.

**Definition 21.** Let $E$ be a field, and let $\phi \in \mathrm{Aut}(E)$. The *fixed field* of $\phi$ is

$$\mathrm{Fix}(\phi) = \{a \in E \mid \phi(a) = a\}.$$

**Proposition 42.** *Let $E$ be a field, and let $\phi \in \mathrm{Aut}(E)$. Then $\mathrm{Fix}(\phi)$ is a subfield of $E$.*

*Proof.* Since $\mathrm{Fix}(\phi)$ is a subset of $E$ by definition, it suffices to check that $\mathrm{Fix}(\phi)$ is closed under addition, multiplication, additive inverses, and multiplicative inverses. If $a, b \in \mathrm{Fix}(\phi)$, then $\phi(a + b) = \phi(a) + \phi(b) = a + b$, so $a + b$ is fixed, and $a + b \in \mathrm{Fix}(\phi)$; similarly, $ab$ is fixed. Also $\phi(-a) = -\phi(a) = -a$, so $-a \in \mathrm{Fix}(\phi)$; similarly, $a^{-1}$ is fixed when $a \neq 0$. Thus $\mathrm{Fix}(\phi)$ is a field. □

**Definition 22.** Let $E$ be a field, and let $G$ be a group of automorphisms of $E$. The *fixed field* of $G$ is

$$\mathrm{Fix}(G) = \{a \in E \mid \phi(a) = a \text{ for all } \phi \in G\}.$$

**Proposition 43.** *Let $E$ be a field, and let $G$ be a group of automorphisms of $E$. Then*

$$\mathrm{Fix}(G) = \cap_{\phi \in G} \mathrm{Fix}(\phi),$$

*and $\mathrm{Fix}(G)$ is a subfield of $E$.*

*Proof.* Clearly, $\mathrm{Fix}(G) = \cap_{\phi \in G} \mathrm{Fix}(\phi)$. Since the intersection of fields is a field, $\mathrm{Fix}(G)$ is a field. □

**Proposition 44.** *Let $E$ be a field with subfields $F$ and $K$. Let $H, G$ be subgroups of $\mathrm{Aut}(E)$. Then*

**(a)** $F \subset K \Rightarrow \mathrm{Aut}(E/F) \supset \mathrm{Aut}(E/K)$*;*
**(b)** $H \subset G \Rightarrow \mathrm{Fix}(H) \supset \mathrm{Fix}(G)$*;*
**(c)** $\mathrm{Aut}(E/\mathrm{Fix}(G)) \supset G$*;*
**(d)** $\mathrm{Fix}(\mathrm{Aut}(E/F)) \supset F$.

*Proof.* Each of these is easy.

**(a)** Suppose $F \subset K$ and let $\phi \in \mathrm{Aut}(E/K)$. Then $\phi$ fixes $K$, so $\phi$ fixes $F$, so $\phi \in \mathrm{Aut}(E/F)$.

**(b)** Suppose $H \subset G$, and let $a \in \mathrm{Fix}(G)$. If $\phi \in H$, then $\phi \in G$, so $\phi(a) = a$; thus $H$ fixes $a$, so $a \in \mathrm{Fix}(H)$.

**(c)** Let $\phi \in G$; then $\phi$ is an automorphism of $E$ which fixes $\mathrm{Fix}(G)$. Thus $\phi \in \mathrm{Aut}(E/\mathrm{Fix}(G))$.

**(d)** Let $a \in F$ and let $\phi \in \mathrm{Aut}(E/F)$. Then $\phi$ fixes $F$, so $\phi(a) = a$. Thus $a \in \mathrm{Fix}(\mathrm{Aut}(E/F))$. □

## 15. Galois Extensions

**Definition 23.** Let $E/F$ be a field extension. We say that $E/F$ is *Galois* if it is finite, normal, and separable.

**Proposition 45.** *Let $F \leq E \leq K$ be fields, with $K/F$ algebraic. If $K/F$ is Galois, then so is $K/E$.*

*Proof.* Since $K/F$ is finite, normal, and separable, so is $K/E$. □

**Proposition 46** (Artin's Lemma)**.** *Let $E$ be a field and let $G \leq \mathrm{Aut}(E)$ be a finite group of automorphisms of $E$. Let $F = \mathrm{Fix}(G)$. Then*

**(a)** *$E/F$ is a Galois extension;*
**(b)** $|G| = [E : F]$*;*
**(c)** $\mathrm{Aut}(E/F) = G$.

*Proof.* Let $\alpha \in E \setminus F$ and let $A = \{\phi(\alpha) \mid \phi \in G\}$. Since $G$ is finite, so is $A$. Let $f(X) = \prod_{a \in A}(X - a) \in E[X]$. Then $f$ is a monic polynomial with $\deg(f) = |A|$. Moreover, the coefficients of $f$ are fixed by the action of $G$ on $E$, and so they are in $F$. Thus $E/F$ is an algebraic extension. Furthermore, $\deg(f) = [F[\alpha] : F] \leq |G|$.

The elements of $A$ are distinct roots of the minimum polynomial of $\alpha$ over $F$, so the degree of this minimum polynomial must be greater than or equal to $|A| = \deg(f)$. But $f$ is a monic polynomial over $F$ of which $\alpha$ is a root; moreover, all of its roots are conjugate, so it must be irreducible. Thus $f$ must be the minimum polynomial of $\alpha$ over $F$. Since $\alpha$ was chosen arbitrarily, $f$ is an arbitrary irreducible monic polynomial over $F$ with a root in $E$, and all of the roots of $f$ are in $E$. Thus $E/F$ is normal. Moreover, $f$ has distinct roots, so $E/F$ is separable.

Suppose that $\alpha$ is an element of $E$ such that $[F(\alpha) : F]$ is a maximum, and suppose that $[E : F] > |G|$. Then since $[F(\alpha) : F] \leq |G|$, there exists an element $\beta \in E$ such that $\beta \notin F(\alpha)$. Then $F(\alpha, \beta)/F$ is a separable finite extension, and so has a primitive element $\gamma$. Then $[F(\gamma) : F] > [F(\alpha) : F]$, contradicting our choice of $\alpha$. Thus $[E : F] \leq |G|$, so $E/F$ is finite and therefore Galois.

Finally, $G$ is a group of automorphisms of $E$ which fixes $F$, so $G \leq \mathrm{Aut}(E/F)$, and $|G| \leq |\mathrm{Aut}(E/F)| \leq [E : F]$. This proves $|G| = [E : F]$, and moreover, $|G| = |\mathrm{Aut}(E/F)|$ so $G = \mathrm{Aut}(E/F)$. □

**Theorem 2** (Galois Characterization Theorem)**.** *Let $E/F$ be a finite extension. Then the following conditions are equivalent:*

**(i)** *$E/F$ is a Galois extension;*
**(ii)** $|\mathrm{Aut}(E/F)| = [E : F]$*;*
**(iii)** $\mathrm{Fix}(\mathrm{Aut}(E/F)) = F$*.*

*Proof.* We show **(i)** $\Rightarrow$ **(ii)** $\Rightarrow$ **(iii)** $\Rightarrow$ **(i)**.

**(i)** $\Rightarrow$ **(ii)** Suppose $E/F$ is Galois. Then $E/F$ is separable and admits a primitive element $\alpha$. Each root of the minimum polynomial of $\alpha$ which is and elements of $E$ gives an automorphism of $E/F$ by sending $\alpha$ to it, and these are the only automorphisms. Since $E/F$ is separable, there are $[E : F]$ such roots, and since $E/F$ is normal, all of them are in $E$.

**(ii)** $\Rightarrow$ **(iii)** Suppose that $|\mathrm{Aut}(E/F)| = [E : F]$. Let $K = \mathrm{Fix}(\mathrm{Aut}(E/F))$; we have $F \leq K$. Then $\mathrm{Aut}(E/K)$ is a group of automorphisms of $E$ which fix $K$ and therefore fix $F$, so $\mathrm{Aut}(E/K) \leq \mathrm{Aut}(E/F)$. On the other hand, $\mathrm{Aut}(E/F)$ is a group of automorphisms of $E$ which fix $K$ by definition of $K$, we have $\mathrm{Aut}(E/F) \leq \mathrm{Aut}(E/K)$. Thus $\mathrm{Aut}(E/K) = \mathrm{Aut}(E/F)$. Now

$$[E : F] = |\mathrm{Aut}(E/F)| = |\mathrm{Aut}(E/K)| \leq [E : K],$$

so $F \leq K$ implies that $F = K$.

**(iii)** $\Rightarrow$ **(i)** Suppose that $\mathrm{Fix}(\mathrm{Aut}(E/F)) = F$. Apply Artin's Lemma with $G = \mathrm{Aut}(E/F)$. □

**Proposition 47.** *Let $E/F$ be a Galois extension.*

**(a)** $H \leq \mathrm{Aut}(E/F) \Rightarrow \mathrm{Aut}(E/\mathrm{Fix}(H)) = H$*;*
**(b)** $K \leq E/F \Rightarrow \mathrm{Fix}(\mathrm{Aut}(E/K)) = K$*;*

*Proof.* Part **(a)** is from Artin's Lemma. The notation $K \leq E/F$ means that $F \leq K \leq E$. Since $E/F$ is Galois, so is $E/K$. Now **(b)** follows from the Galois Characterization Theorem. □

## 16. Galois Correspondence

**Definition 24.** If $E/F$ is a Galois extension, the set of all automorphisms of $E$ which fix $F$ is denoted $\mathrm{Gal}(E/F)$, and is known as the *Galois group* of $E/F$.

This is simply a mnemonic device. If one sees $\mathrm{Gal}(E/F)$, one recalls its fixed field is $F$. If one sees $\mathrm{Aut}(E/F)$, one knows that $F$ is a subfield of its fixed field, but there is a question about whether $F$ is the entire fixed field.

If $f \in F[x]$, the Galois group of $f$ over $F$ is $\mathrm{Gal}(E/F)$, where $E$ is a splitting field of $f$ over $F$.

The next theorem is essential, but uses some concepts of group theory. If $H$ is a subgroup of $G$, the cardianlity of $H$ divides the cardinality of $G$. The *index* of $H$ in $G$ is $[G : H] = |G|/|H|$. We say that $H$ is a *normal* subgroup if $g^{-1}hg \in H$ for all $h \in H$ and $g \in G$.

**Theorem 3** (Galois Correspondence Theorem)**.** *Let $E/F$ be a Galois extension with $G = \mathrm{Gal}(E/F)$. Let $\mathfrak{F}$ be the set of subfields of $E$ which contain $F$ and let $\mathfrak{G}$ be the set of subgroups of $G$. Then there exists a bijective correspondence*

$$\Phi : \mathfrak{F} \to \mathfrak{G} \text{ given by } K \mapsto \mathrm{Gal}(E/K),$$

*with inverse $H \mapsto \mathrm{Fix}(H)$. Additionally,*

- **(a)** $H_1 \subset H_2 \Leftrightarrow \mathrm{Fix}(H_1) \supset \mathrm{Fix}(H_2)$;
- **(b)** $|H| = [E : \mathrm{Fix}(H)]$;
- **(c)** $[G : H] = [\mathrm{Fix}(H) : F]$.

*Finally, if $H \leq G$ and $K = \mathrm{Fix}(H)$, then $H \triangleleft G$ if and only if $K/F$ is a normal extension, in which case* $\mathrm{Gal}(K/F) \cong G/H$.

*Proof.* Let $K_1, K_2 \leq E/F$ and suppose $\Phi(K_1) = \Phi(K_2)$. Then $\mathrm{Gal}(E/K_1) = \mathrm{Gal}(E/K_2)$. Then $K_1 = \mathrm{Fix}(\mathrm{Gal}(E/K_1)) = \mathrm{Fix}(\mathrm{Gal}(E/K_2)) = K_2$, so $\Phi$ in injective.

Let $H \leq G$. Then $\Phi(\mathrm{Fix}(H)) = \mathrm{Gal}(\mathrm{Fix}(H)) = H$, so $\Phi$ in surjective. Thus $\Phi$ is a bijection.

We always have $H_1 \subset H_2 \Rightarrow \mathrm{Fix}(H_1) \supset \mathrm{Fix}(H_2)$, and that $K_1 \subset K_2 \Rightarrow \mathrm{Aut}(E/K_1) \supset \mathrm{Aut}(E/K_2)$. Now suppose that $\mathrm{Fix}(H_1) \supset \mathrm{Fix}(H_2)$, and apply $\mathrm{Gal}(E/*)$, which in this case is the same as $\mathrm{Aut}(E/*)$, to both sides to obtain $H_1 = \mathrm{Gal}(\mathrm{Fix}(H_1)) \subset \mathrm{Gal}(\mathrm{Fix}(H_2)) = H_2$. This proves **(a)**.

Since $E/\mathrm{Fix}(H)$ is a Galois extension and $H = \mathrm{Aut}(E/\mathrm{Fix}(H))$, we have **(b)**.

By Lagrange's Theorem, we know that $|G| = |H|[G : H]$. By the dimension formula, $[E : F] = [E : \mathrm{Fix}(H)][\mathrm{Fix}(H) : F]$. Since $E/F$ and $E/\mathrm{Fix}(H)$ are Galois extensions, $[E : F] = |G|$ and $[E : \mathrm{Fix}(H)] = |H|$. Thus $[G : H] = [\mathrm{Fix}(H) : F]$, proving **(c)**.

As for the a last part, suppose that $K/F$ is a normal extension. Then every automorphism of $E$ stabilizes $K$ setwise. If $\phi \in G$, then $\phi \restriction_K : K \to K$ is an automorphism of $K$, which necessarily fixes $F$ and thus is in $\mathrm{Gal}(K/F)$. The map $\phi \mapsto \phi \restriction_K$ is a homomorphism $\mathrm{Gal}(E/F) \to \mathrm{Gal}(K/F)$. The kernel of this homomorphism is $\mathrm{Gal}(E/K)$. Thus $\mathrm{Gal}(E/K)$ is normal, and $\mathrm{Gal}(K/F) \cong G/H$ by the isomorphism theorem.

Suppose that $K/F$ is not a normal extension. Then there exists an automorphism $\phi \in \mathrm{Gal}(E/F)$ which does not stabilize $K$ setwise; thus $\phi(K) \neq K$. Then $\mathrm{Gal}(E/\phi(K)) = \phi H \phi^{-1}$, so $\phi H \phi^{-1} \neq H$, and $H$ is not normal. □

## 17. Fundamental Theorem of Algebra

A *p-group* is a group whose cardinality is a power of $p$. A *Sylow p-subgroup* of a group $G$ is a maximal subgroup whose cardinality is a power of $p$. The proof below uses Sylow 2-subgroups.

**Theorem 4** (Fundamental Theorem of Algebra)**.** *The field $\mathbb{C}$ is algebraically closed.*

*Proof.* Let $f(X) = X^2 + 1 \in \mathbb{R}[X]$. Let $i$ be a root of $f$ and note that

$$\mathbb{C} = \mathbb{R}(i) = \{a + ib \mid a, b \in \mathbb{R}\}.$$

Let $g(X) \in \mathbb{C}[X]$ and let $E$ be the splitting field of $g(X)$ over $\mathbb{C}$. It suffices to show that $E = \mathbb{C}$.

Since $E$ is a splitting field, it is a Galois extension of $\mathbb{C}$. Thus it is Galois over $\mathbb{R}$. Let $G = \mathrm{Gal}(E/\mathbb{R})$. Let $H$ be a Sylow 2-subgroup of $G$. Let $F = \mathrm{Inv}(H)$. By comparing degrees, $[F : \mathbb{R}]$ has odd degree. By the primitive element theorem, $F = \mathbb{R}(\alpha)$, such that $\alpha$ is the root of an irreducible polynomial over $\mathbb{R}$ of odd degree. But every polynomial of odd degree over $\mathbb{R}$ has a root in $\mathbb{R}$, so the only irreducible polynomials over $\mathbb{R}$ are the linear ones. Thus $\alpha \in \mathbb{R}$, and $F = \mathbb{R}$. Therefore $H = G$ is a 2-group, which demands that $\mathrm{Gal}(E/\mathbb{C})$ is a 2-group.

If $\mathrm{Gal}(E/\mathbb{C})$ is nontrivial, it has a subgroup of index 2, necessary normal, which corresponds to a Galois subextension $K/\mathbb{C}$ of degree 2. This extension has a primitive element $\beta$, which is the root of an irreducible quadratic equation over $\mathbb{C}$. But by the quadratic formula, there are no irreducible quadratic polynomials over $\mathbb{C}$. □

## 18. Galois Solvability Criterion

A group is *cyclic* if every element in it is a power of some one element in it.

**Definition 25.** Let $F$ be a field and let $f \in F[X]$. Let $E$ be a splitting field of $f$ over $F$. We say that $f$ is *solvable by radicals* if there exists a sequence of subfields of $E$

$$F = F_0 \leq F_1 \leq \cdots \leq F_r = E$$

such that $F_{i+1} = F_i[\alpha_i]$ for $i = 1, \ldots, r$, where $\alpha_i$ is a root of $X^{n_i} - b_i$ for some $b_i \in F_i$.

**Definition 26.** Let $G$ be a group. We say that $G$ is *solvable* if there exists a sequence of subgroups of $G$

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

such that $G_i \triangleleft G$ and $G_{i+1}/G_i$ is cyclic.

**Theorem 5.** *Let $F$ be a field and let $f \in F[X]$. Let $E$ be a splitting field of $f$ over $F$. Then $f$ is solvable by radicals if and only if* $\mathrm{Gal}(E/F)$ *is a solvable group.*

Department of Mathematics and CSci, Southern Arkansas University
*E-mail address*: plbailey@saumag.edu