# FIELD EXTENSIONS

PAUL L. BAILEY

## 1. Evaluation

Let $R$ be a commutative ring. The additive identity of $R$ is denoted by $0_R$ or simply 0 and the multiplicative identity is denoted by $1_R$ or simply 1. The group of invertible elements of $R$ is denoted $R^*$.

If $I$ is an ideal of $R$, we write $I \lhd R$. If $A$ is a subset of $R$, the ideal generated by $A$ is denoted $\langle A \rangle$ or $AR$. If $A = \{a\}$ is a singleton, we may write $\langle a \rangle$ instead of $\langle \{a\} \rangle$. Similarly, if $A = \{a_1, \ldots, a_n\}$, we may write $\langle a_1, \ldots, a_n \rangle$ for the ideal generated by $A$.

We require that ring homomorphisms send the multiplicative identity of the domain to that of the image. Since $\mathbb{Z}$ is generated (as a ring) by a single element, there exists a unique homomorphism $\phi : \mathbb{Z} \to R$. Since $\mathbb{Z}$ is a pid, the kernel of this homomorphism is a principal ideal. The *characteristic* of $R$ is the unique nonnegative element which generates $\ker(\phi)$. The image of $\phi$ is called the *characteristic subring* of $R$. The characteristic of a finite domain is necessarily a prime integer.

We require that subrings of $R$ contain the same multiplicative identity. If $S$ is a subring of $R$, we write $S \leq R$. If $A$ is a subset of $R$, let $S[A]$ be the subring of $R$ generated by $S$ and $A$, which is smallest subring of $R$ containing $S$ and all of the elements of $A$. This is necessarily the intersection of all subrings of $R$ which contains $S$ and $A$. If $S = \{a\}$ contains a single element, we may write this as $F[a]$, or if $S = \{a_1, \ldots, a_n\}$ is finite, we may write this as $S[a_1, \ldots, a_n]$. We should point out that $S[a_1, a_2] = S[a_1][a_2]$, and so forth.

The ring of polynomials in one variable over $R$ is denoted $R[X]$. This concurs with the above notation. The Universal Property of Polynomial Rings states that given a ring homomorphism $\psi : R \to S$ and $a \in S$, there exists to a unique homomorphism $\psi_\alpha : R[X] \to S$ which sends $X$ to $\alpha$. This homomorphism is given by $\psi_\alpha(f(X)) = f(\alpha)$, and is called the *evaluation homomorphism*. If $\psi$ is inclusion, denote the image $\psi_\alpha(R[X])$ by $R[\alpha]$. Let $I$ be the set of all polynomials in $R[X]$ which vanish at $a$; then $I = \ker(\psi_\alpha)$. Let $\overline{\psi}_\alpha : R[X]/I \to R[\alpha]$ denote the isomorphism induced by $\psi_\alpha$ as dictated by the isomorphism theorem for rings.

On the other hand, suppose that $f \in R[X]$ and we wish to create a ring which contains $R$ and a root of $f$. Set $S = R[X]/\langle f \rangle$ and let $\psi : R[X] \to S$ be the canonical homomorphism. Then $\psi$ is injective on $R$, and we may identify $R$ with its image under $\psi$. The image of $X$ under $\psi$ is an element of $S$ which is a root of $R$.

---

*Date*: May 18, 2001.

## 2. Fields

**Definition 1.** A *field* is a commutative ring in which every nonzero element is invertible. A *subfield* of a ring is a subring which is a field.

**Proposition 1.** *Let $F$ be a field and let $I \triangleleft F$. The $I = F$ or $I = \langle 0 \rangle$.*

*Proof.* Suppose $I$ is not the zero ideal. Let $I$ contains a nonzero element $a$ which is invertible in $F$. Since $a^{-1} \in F$, $a^{-1}a = 1 \in I$, so $I = R$. □

**Proposition 2.** *Let $F$ be a field and let $R$ be a nonzero ring. Let $\phi : F \to R$ be a ring homomorphism. Then $\phi$ is injective.*

*Proof.* Since $R$ is nonzero, it contains an element $1_R$ which is different from $0_R$, and $\phi(1_F) = 1_R$. Then $1_F \notin \ker(\phi)$, so $\ker(\phi) \neq R$, and $\ker(\phi) = \langle 0 \rangle$. Thus $\phi$ is injective. □

**Proposition 3.** *Let $R$ be a ring and let $\mathcal{F}$ be a collection of subfields of $R$. Then $\cap\mathcal{F}$ is a subfield of $R$.*

**Proposition 4** (Division Algorithm)**.** *Let $F$ be a field and let $f, g \in F[X]$. Then there exist polynomials $q, r \in F[X]$, with $\deg(r) < \deg(f)$, such that $g = fq + r$.*

**Proposition 5** (Euclidean Algorithm)**.** *Let $F$ be a field and let $f, g \in F[X]$. Let $d \in F[X]$ be a greatest common divisor for $f$ and $g$. Then there exist polynomials $a, b \in F[X]$ such that $af + bg = d$.*

**Proposition 6.** *Let $F$ be a field. Then $F[X]$ is a principal ideal domain (pid), and every ideal in $F[X]$ is generated by a unique monic polynomial.*

*Proof.* Let $I \triangleleft F[X]$ and let $f \in I$ be a polynomial of minimal degree among nonzero elements of $I$. If $g \in I$, then $g = fq + r$ for some $q, r \in F[X]$ with $\deg(r) < \deg(f)$. But $fq \in I$ since $I$ is an ideal so $r = g - fq \in I$. By the minimality of $f$, we must have $r = 0$, so $g$ is a multiple of $f$. Thus $f$ generates $I$. The other generators of $I$ are given by multiplying a given generator by an invertible element. The invertible elements of $F[X]$ are exactly the nonzero elements of $F$. Thus there is a unique monic polynomial which generates $I$. □

**Proposition 7.** *Let $R$ be a pid and let $I \triangleleft R$ be prime. Then $I$ is maximal.*

*Proof.* Since $R$ is a pid, $I = \langle a \rangle$ for some $a \in R$. Let $J$ be an ideal which properly contains $I$. Then $J = \langle b \rangle$ for some $b \in R$. Since $a \in J$, $a = cb$ for some $c \in R$, and since $I$ is prime, either $c \in I$ or $b \in I$. If $b \in I$, then $J \subset I$, which assumed is not the case. So $c \in I$, and $c = da$ for some $d \in R$. Then $a = dab$, so $bd = 1$ and $b$ is invertible, so $J = R$. Thus $I$ is maximal. □

**Proposition 8** (Preservation of Roots)**.** *Let $F$ be a subfield of a field $E$ and let $\sigma : E \to K$ be a homomorphism. For $f(X) = \sum_{i=0}^{n} a_i X^i \in F[X]$, set $f^\sigma(X) = \sum_{i=0}^{n} \sigma(a_i) X^i$. Then $\sigma$ induces a homomorphism $F[X] \to K[X]$ given by $f \mapsto f^\sigma$. Moreover, $\alpha \in E$ is a root of $f \in F[X]$ if and only if $\sigma(\alpha)$ is a root of $f^\sigma$.*

*Proof.* Note that for $\alpha \in E$, we have $\sigma(f(\alpha)) = f^\sigma(\sigma(\alpha))$. Since $\sigma$ is injective, this equals zero if and only if $f(\alpha) = 0$. □

## 3. Field Extensions

**Definition 2.** A *field extension* $E/F$ is a pairs of fields $E$ and $F$ such that $F \leq E$. We may view $E$ as a vector space over $F$, with scalar multiplication given by multiplication within $E$. The dimension of this vector space is called the *degree* of the extension, and is denoted by $[E : F]$.

Let $E/F$ be a field extension. We say that $E/F$ is *finite* if $[E : F] < \infty$.

**Theorem 1** (Product of Degrees Formula)**.** *Let $F \leq E \leq K$ be fields. Then $K/F$ is finite if and only if $E/F$ is finite and $K/E$ is finite. In this case, $[K : F] = [E : F][K : E]$.*

*Proof.* Suppose that $K/F$ is finite of dimension $n$. Then we have a basis $\{v_1, \ldots, v_n\}$. Since $E/F$ is a subspace, it is finite. Now a vector in $K/E$ is a linear combination of the $v_i$'s with coefficients in $F$ and thus in $E$, so the $v_i$'s span $K/E$ and it is finite.

Conversely suppose that $K/E$ and $E/F$ are finite. Let $\{u_1, \ldots, u_m\}$ be a basis for $E/F$ and let $\{v_1, \ldots, v_n\}$ be a basis for $K/E$. Let $B = \{u_i v_j \mid i = 1, \ldots, m \text{ and } j = 1, \ldots, n\}$.

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 thus by the linear independence of the $u_i$'s, each $b_{i,j} = 0$. Thus $B$ is linearly independent and is therefore a basis. Thus $K/F$ has dimension $ij$. □

## 4. Primitive Extensions

**Definition 3.** Let $E/F$ be a finite field extension. We say that $E/F$ is *primitive* if there exists $\alpha \in E$ such that $F[\alpha] = E$. In this case we call $\alpha$ a *primitive element* for the extension.

**Definition 4.** Let $E/F$ be a field extension and let $\alpha \in E$. We say that $\alpha$ is *algebraic* over $F$ if there exists a polynomial $f \in F[X]$ such that $f(a) = 0$. Otherwise, we say that $\alpha$ is *transcendental* over $F$.

If $E/F$ is a field extension, denote the smallest subfield of $E$ containing $F$ and $\alpha$ by $F(\alpha)$.

**Proposition 9.** *Let $E/F$ be a field extension and let $\alpha \in E$. Let $I = \ker(\psi_\alpha)$ be the kernel of evaluation. Then*

- **(a)** *$I$ is a prime ideal;*
- **(b)** *if $\alpha$ is transcendental over $F$, then $I = \langle 0 \rangle$, and $F[\alpha] \cong F[X]$;*
- **(c)** *if $\alpha$ is algebraic over $F$, then $I = \langle f \rangle$ where $f$ is a unique monic irreducible polynomial, and $F[\alpha]$ is a field.*

*Proof.* Since $F$ is a field, it contains no zero divisors, so the subring $\psi_\alpha(F[X]) = F[\alpha] \cong F[X]/I$ is an integral domain. Thus $I$ is a prime ideal.

The ideal $I$ is the set of polynomials in $F[X]$ that vanish at $\alpha$.

If $\alpha$ is transcendental over $F$, then $I$ is the zero ideal, and the map $F[X] \to R$ is injective. In this case, $F[\alpha]$ is isomorphic to $F[X]$, and $F(\alpha)$ is isomorphic to $F(X)$, the quotient field of $F[X]$.

If $\alpha$ is algebraic over $F$, then $I$ is a nonzero prime ideal. In a pid, nonzero prime ideals are maximal, so $I$ is a maximal ideal. In this case, $F[\alpha]$ is a field, and $F(\alpha) = F[\alpha]$. Generators of principal prime ideals are prime elements and prime elements are always irreducible, so a generator of $I$ is irreducible. □

**Definition 5.** Let $E/F$ be a field extension and let $\alpha \in E$ be algebraic over $F$. The unique monic irreducible polynomial which generates $I$ is called the *minimum polynomial* of $\alpha$ over $F$, and is denoted $\min(\alpha/F)$.

**Example 1.** Find $\min(\sqrt{\sqrt{2}+\sqrt{3}}, \mathbb{Q})$.

*Solution.* Let $\alpha = \sqrt{\sqrt{2}+\sqrt{3}}$. Then $\alpha^4 = 5 + 2\sqrt{2}\sqrt{3}$, and $(\alpha^4 - 5)^2 = 24$. Thus $\min(\alpha, \mathbb{Q}) = X^8 - 10X^4 + 1$. □

**Proposition 10.** *Let $E_1/F$ and $E_2/F$ be a field extensions and let $\alpha \in E_1$, $\beta \in E_2$ such that $\min(\alpha/F) = \min(\beta/F)$. Define $\psi_{\beta\alpha} : F[\alpha] \to F[\beta]$ by $\psi_{\beta\alpha} = \overline{\psi}_\beta^{-1} \circ \overline{\psi}_\alpha$. Then $\psi_{\beta\alpha}$ is an isomorphism.*

*Proof.* We defined $\psi_{\beta\alpha}$ as the composition of isomorphisms. □

**Example 2.** It is not necessary that $F[\alpha] = F[\beta]$. As an example, take $F = \mathbb{Q}$, $\alpha = \sqrt[3]{2}$, $\zeta = e^{2\pi i/3}$, and $\beta = \alpha\zeta$. Then $F[\alpha]$ is a subfield of $\mathbb{R}$, but $F[\beta]$ is not.

**Proposition 11.** *Let $E/F$ be a field extension and let $\alpha \in E$ be algebraic over $F$. Let $f = \min(\alpha/F)$ and set $n = \deg(f)$. Then a basis for the vector space $F(\alpha)/F$ is $\{1, \alpha, \ldots, \alpha^{n-1}\}$. In particular, $[F(\alpha) : F] = n$.*

*Proof.* Let $B = \{1, \alpha, \ldots, \alpha^{n-1}\}$.

Let $g(X) \in F[X]$. Then there exist polynomials $q(X)$ and $r(X)$ with $0 \leq \deg(r) < \deg(f)$ such that $g(X) = f(X)q(X) + r(X)$. Then $g(\alpha) = f(\alpha)q(\alpha) + r(\alpha) = r(\alpha)$. Since the evaluation map $F[X] \to F[\alpha]$ is surjective, each element of $F[\alpha] = F(\alpha)$ is of the form $r(\alpha)$ where $\deg(r) < n$. Thus $B$ spans $F(\alpha)/F$.

Now suppose that $\sum_{i=0}^{n-1} a_i\alpha^i = 0$, where $a_i \in F$. Then $\alpha$ is a root of the polynomial $g(X) = \sum_{i=0}^{n-1} a_i X^i$. Since the degree of this polynomial is less than the degree of the minimal polynomial, we must have that $g(X)$ is the zero polynomial So all of the $a_i$ are zero, and $B$ is a linearly independent set. □

**Proposition 12.** *Let $E/F$ be a field extension and let $\alpha_1, \ldots, \alpha_n \in E$ be algebraic over $F$. Let $L = F[\alpha_1, \ldots, \alpha_n]$. Then $L/F$ is finite, and $[L : F] \leq \prod_{i=1}^n [F[\alpha_i] : F]$.*

*Proof.* Let $K = F[\alpha_1, \ldots, \alpha_{n-1}]$; by induction, we assume that $[K : F] \leq \prod_{i=1}^{n-1} [F[\alpha_i] : F]$. Let $f$ be the minimum polynomial of $\alpha_n$ over $F$. Then the coefficients of $\alpha_n$ are in $K$, so view $f \in K[X]$. Since $f(\alpha_n) = 0$, $\alpha_n$ is algebraic over $K$, and the minimum polynomial of $\alpha_n$ over $K$ is a factors of $f$. In particular, the degree of this minimum polynomial is less than or equal to $\deg(f) = [F[\alpha_n] : F]$. Thus

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

□

## 5. Splitting Extensions

**Definition 6.** Let $E/F$ be a field extension and let $f \in F[X]$. We say that $f$ *splits* is $E$ if $f$ is the product of linear factors in $E[X]$. We say that $E$ is a *splitting field* of $f$ over $F$ if $f$ splits in $E$ and $E$ is generated over $F$ by the roots of $f$. In this case we call $E/F$ a *splitting extension* for $f$.

**Proposition 13.** *Let $F$ be a field and let $f(X) \in F[X]$ be a monic polynomial of positive degree. Then there exists an extension field $E$ containing $F$ such that $E$ is a splitting field of $f(X)$ over $F$.*

*Proof.* Proceed by induction on the degree of the polynomial.

If $\deg(f) = 1$, then the unique root of $f$ is already in $F$ and $F$ is a splitting field for $f$ over $F$. By strong induction on $\deg(f)$, we may assume that any polynomial of degree less than $f$ over any field has a splitting extension over that field.

Let $h$ be an irreducible factor of $f$, and let $K = F[X]/\langle h \rangle$. Denote the image of $X$ in $K$ by $\alpha_1$. Divide $f(X)$ by $(X - \alpha_1)$ in $K$ to obtain $f(X) = (X - \alpha_1)g(X)$ for some $g(X) \in K[X]$. Then there exists a splitting extension $E/K$ for $g$. That is, $E = K[\alpha_2, \ldots, \alpha_n]$, where $\alpha_2, \ldots, \alpha_n$ are the roots of $g$. Now $E = F[\alpha_1, \alpha_2, \ldots, \alpha_n]$ is a splitting field for $f$ over $F$. □

**Proposition 14.** *Let $F$ be a field and $f \in F[X]$. Let $E_1$ and $E_2$ be splitting fields of $f(X)$ over $F$. Then there exists an isomorphism $\phi : E_1 \to E_2$ which is the identity on $F$.*

*Hedge.* We will show this later, when we have more tools. □

**Proposition 15.** *Let $F$ be a field and $f(X) \in F[X]$ with $\deg(f) = n$. Let $E$ be a splitting field of $f(X)$ over $F$. Then $[E : F] | n!$.*

*Proof.* Proceed by induction on the degree of the polynomial.

Let $E$ be a splitting field of $F$. Let $\alpha$ be a root of $f(X)$ in $E$. Then $f(X) = (X - \alpha)g(X)$ in $F[\alpha] \leq E$, and $\deg(g) = n - 1$. Now $g(X)$ splits in $E$, and if $g(X)$ splits in a proper subfield of $E$, then so does $f(X)$; thus $E$ is a splitting field for $g(X)$ over $K$. By induction, $[E : K] | (n-1)!$. Now $[E : F] = [E : K][K : F] = [E : K]n$; thus $[E : F] | n!$. □

**Example 3.** Let $E/\mathbb{Q}$ be a splitting extension for $f \in \mathbb{Q}[X]$ in each of the following cases, and find $[E : \mathbb{Q}]$.

- **(a)** $f(X) = X^3 - 2$;
- **(b)** $f(X) = X^4 - 2$;
- **(c)** $f(X) = X^8 - 10X^4 + 1$;
- **(d)** $f(X) = X^5 - 2$;
- **(e)** $f(X) = X^5 - 4X + 2$.

## 6. Algebraic Extensions

**Definition 7.** Let $E/F$ be a field extension. We say that $E/F$ is *algebraic* if every element in $E$ is algebraic over $F$.

**Proposition 16.** *Let $E/F$ be a finite field extension. Then $E/F$ is algebraic.*

*Proof.* Let $[E : F] = n$ and let $\alpha \in E$. Then $\{1, \alpha, \ldots, \alpha^n\}$ is a linearly dependent set over $F$, so there exist $a_0, \ldots, a_n \in F$ such that $a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$. Then $\alpha$ is a root of $a_0 + a_1X + \cdots + a_nX^n$, so $\alpha$ is algebraic over $F$. □

**Proposition 17.** *Let $E/F$ be a field extension and let $\alpha_1, \ldots, \alpha_n \in E$ be algebraic over $F$. Then $F[\alpha_1, \ldots, \alpha_n]/F$ is algebraic.*

*Proof.* By a previous proposition, this is a finite extension, so it is algebraic. □

**Proposition 18.** *Let $K/E$ and $E/F$ be algebraic extensions. Then $K/F$ is algebraic.*

*Proof.* Let $\alpha \in K$ and let $f \in E[X]$ be the minimum polynomial of $\alpha$ over $E$. The coefficients of $f$ are in $E$, so they are algebraic over $F$. Let $A$ be the set of these coefficients. Then $F[A]/F$ is a finite extension. Now $f \in F[A][X]$, and $[F[A][\alpha] : F[A]] = \deg(f)$, so $F[A][\alpha]/F[A]$ is a finite extension. Thus $F[A][\alpha]/F$ is an algebraic extension, and $\alpha$ is algebraic over $F$. □

**Proposition 19.** *Let $E/F$ be an algebraic extension and let $R$ be a subring of $E$ which contains $F$. Then $R$ is a field.*

*Proof.* It is clear that $R$ is commutative, because $E$ is. Let $\alpha \in R \setminus 0$. Then $\alpha$ is algebraic over $F$, so $F[\alpha]$ is a field. Clearly $F[\alpha]$ is contained in $R$, so $\alpha^{-1} \in R$. Thus $R$ is a field. □

**Proposition 20.** *Let $E/F$ be a field extension and set*

$$K = \{\alpha \in E \mid \alpha \text{ is algebraic over } F\}.$$

*Then $K$ is a subfield of $E$ containing $F$.*

*Proof.* Let $\alpha, \beta \in K$. Since $\beta$ is algebraic over $F$, it is also algebraic over $F[\alpha]$. We have $[F[\alpha, \beta] : F] \leq [F[\alpha] : F][F[\beta] : F]$. So $F[\alpha, \beta]$ is an algebraic extension of $F$, which implies that $\alpha + \beta$ and $\alpha\beta$ are algebraic over $F$ and thus in $K$, so $K$ is a subring of $E$. Then $K$ is a subfield by the previous proposition. □

**Proposition 21.** *Let $E/F$ be an algebraic field extension and let $\phi : E \to E$ be a field monomorphism which fixes $F$ pointwise. Then $\phi$ is an automorphism.*

*Proof.* Let $\alpha \in E \setminus F$. Let $f(X)$ be the minimum polynomial of $\alpha$ over $F$. Let $A$ be the set of roots of this polynomial in $E$. Note that $A$ is nonempty and finite. Since $\phi$ sends roots of $f$ to other roots of $f$, the restriction $\phi \restriction_A : A \to A$ is an injective function from a finite set into itself. Therefore $\phi \restriction_A$ is surjective. Thus $\phi$ sends some element to $\alpha$, and $\phi$ is surjective on $E$. Thus $\phi$ is an isomorphism. □

## 7. Algebraic Closure

**Definition 8.** A field $E$ is called *algebraically closed* if every polynomial in $E[X]$ has a root in $E$. It follows immediately that if $E$ is algebraically closed, then every polynomial in $E[X]$ is the product of linear factors in $E[X]$.

Let $E/F$ be a field extension. The set of all elements in $E$ which are algebraic over $F$ is called the *algebraic closure* of $F$ in $E$. We say that $E$ is an *algebraic closure* of $F$ if $E$ is algebraically closed and $E/F$ is an algebraic extension.

We wish to prove that every field has an algebraic closure, and that any two algebraic closures are isomorphic via an isomophism which is the identity on $F$. Showing that there exists an algebraically closed field containing $F$ requires one of the forms of the Axiom of Choice. We use Zorn's Lemma.

**Fact 1** (Zorn's Lemma)**.** Let $A$ be a partially ordered set. A *chain* in $A$ is a subset of $A$ which is linearly ordered. If every chain in $A$ has an upper bound, then every element of $A$ is bounded above by a maximal element.

**Theorem 2** (Algebraic Closure Theorem)**.** *Let $F$ be a field. Then there exists an algebraically closed field $K$ which contains $F$.*

*Proof.* Let $\mathbb{N}$ denote the set of nonnegative integers. Let $S = F[X] \times \mathbb{N}$. The map $\phi : F \to S$ given by $a \mapsto ((X - a), 0)$ is injective, and induces the structure of a field on the image. Identify $\phi(F)$ with $F$.

Let $\mathcal{F}$ be the collection of all fields $E$ such that

- **(a)** the underlying set of $E$ is a subset of $S$;
- **(b)** $E$ contains $F$;
- **(c)** if $\alpha = (f, n) \in E$ then $f(\alpha) = 0$.

The set $\mathcal{F}$ is partially ordered by inclusions which preserve the field structure. Given a chain in $\mathcal{F}$, its union is also a field which is an upper bound for the chain. By Zorn's lemma, there exists a maximal field $K \in \mathcal{F}$.

It follows from **(c)** that $K$ is algebraic over $F$; it remains to show that $K$ is algebraically closed. Suppose it is not; then there exists a a proper algebraic extension of $K$, say $L$.

Define a map $\phi : L \to S$ as follows. If $\alpha \in K$, then $\phi(\alpha) = \alpha$. Otherwise $\alpha$ is algebraic over $F$ and is a root of a minimum polynomial $f \in F[X]$. Let $a_1, \ldots, a_r$ be roots of $f$ which are in $K$ and let $b_1, \ldots, b_s$ be roots of $f$ which are in $L \setminus K$. Let $n_1, \ldots, n_s$ be positive integers such that $(f, n_i) \notin K$. Set $\phi(b_i) = (f, n_i)$ for $i = 1, \ldots, s$. With such choices, $\phi$ is defined on all of $L$ and is clearly injective and maps $L$ onto a subset of $S$ which contains $F$. Also $\phi$ maps $M$ onto itself. The map $\phi$ induces a field structure on its image, and this field contains $M$ as a subfield, contradicting the maximality of $K$. This proves that $K$ is algebraically closed. □

**Proposition 22.** *Let $F$ be a field and let $K$ be an algebraically closed field containing $F$. Let $E$ be the algebraic closure of $F$ in $K$. Then $E$ is an algebraic closure of $F$.*

*Proof.* By construction, $E/F$ is algebraic. To see that $E$ is algebraically closed, let $f \in E[X]$ and let $\alpha \in K$ be a root of $f$. Then $E[\alpha]/E$ is algebraic, so $E[\alpha]/F$ is algebraic, and $\alpha$ is algebraic over $F$. Thus $\alpha \in E$, and $E$ is algebraically closed. □

**Theorem 3** (Algebraic Embedding Theorm)**.** *Let $L$ be an algebraically closed field and let $E/F$ be an algebraic field extension. Let $\phi : F \to L$ be a field embedding. Then $\phi$ extends to an embedding $\psi : E \to L$.*

*Proof.* Define $\mathcal{E} = \{(K, \tau) \mid F \leq K \leq E \text{ and } \tau : K \to L \text{ extends } \phi\}$. This set is partially ordered by declaring $(K_1, \tau_1) \leq (K_2, \tau_2)$ if $K_1 \leq K_2$ and $\tau_2$ extends $\tau_1$. Then $\mathcal{E}$ contains a minimal element $(F, \phi)$, and all of the elements of the form $(F[\alpha], \epsilon)$, where $\alpha$ is a root in $E$ of a polynomial over $F$, and $\epsilon$ maps this root to a root of the polynomial in $L$.

This set admits an partial order relation given by

$$(K_1, \tau_1) \leq (K_2, \tau_2) \Leftrightarrow K_1 \leq K_2 \text{ and } \tau_2 \text{ extends } \tau_1.$$

Every chain in $\mathcal{E}$ admits an upper bound given by taking the union of the fields in the chain and defining an embedding on this union which agrees with every embedding in the chain.

By Zorn's Lemma, $\mathcal{E}$ contains maximal elements. Let $(K, \psi)$ be a maximal element. Now we claim that $K = E$. Suppose not, and let $\alpha \in E/K$. Since $E/F$ is algebraic, so is $E/K$. Let $f(X)$ be the minimum polynomial of $\alpha$ over $K$. Then $\psi(f)$ is a polynomial over $L$, and thus has a root in $L$, say $\beta$. Then we obtain an embedding $K[\alpha] \hookrightarrow L$ which extends $K$ by sending $\alpha$ to $\beta$. This contradicts the maximality of $(K, \psi)$, and completes the proof. □

**Proposition 23.** *Let $F$ be a field and let $K_1$ and $K_2$ be algebraic closures of $F$. Then there exists an isomorphism $\phi : K_1 \to K_2$ which is the identity on $F$.*

*Proof.* By the previous proposition, the inclusion of $F$ into $K_2$ extends to an embedding $\phi_1 : K_1 \to K_2$. Similarly, there is an embedding $\phi_2 : K_2 \to K_1$ which is the identity on $F$. Then the composition $\phi_1 \circ \phi_2$ is an embedding of $K_2$ into itself over $F$, and since $K_2/F$ is algebraic, this is an automorphism. In particular, it is surjective, so $\phi_1$ is surjective, and thus an isomorphism. □

**Proposition 24.** *Let $E/F$ be an algebraic extension. Let $L$ be an algebraically closed field which is algebraic over either $F$ or $E$. Then $L$ is an algebraic closure for both $E$ and $F$.*

*Proof.* If $L$ is algebraic over $E$, then since the composition of algebraic extensions is algebraic, $L$ is algebraic over $F$. If $L$ is algebraic over $F$, then $L/E$ is a subextension, which is necessary algebraic. By definition, $L$ is an algebraic closure for $F$ and for $E$. □

## 8. Finite Fields

**Definition 9.** Let $R$ be a ring. Then there exists a unique homomorphism $\eta : \mathbb{Z} \to R$. The *characteristic* of $R$ is the unique nonnegative generator for the kernel of $\eta$. If positive, this is the smallest positive integer that annihilates $R$. The image of $\eta$ is the *characteristic subring*

**Proposition 25.** *Let $R$ be an integral domain. Then the charactertistic of $R$ is either $0$ or $p$ for some prime $p$.*

*Proof.* Otherwise, the characteristic subring of $R$ has zero divisors. □

**Proposition 26.** *Let $R$ be a finite integral domain. Then $R$ is a field.*

*Proof.* Let $a \in R \setminus \{0\}$ and define $\xi_a : R \to R$ by $\xi_a(x) = ax$. Since $R$ is an integral domain, the cancellation law holds, and $ax = ay \Rightarrow x = y$. Thus $\xi_a$ is injective. Since $R$ is finite, $\xi_a$ is also surjective and admits an inverse. Then the inverse of $a$ in $R$ is $\xi_a^{-1}(1)$. □

**Proposition 27.** *Let $F$ be a field and let $G$ be a finite subgroup of $F^*$. Then $G$ is cyclic.*

*Proof.* Let $\exp(G)$ denote the exponent of $G$; this is the smallest positive integer $n$ such that $g^n = 1$ for every $g \in G$. Clearly $\exp(G) \leq |G|$ and by a group theory lemma, an abelian group is cyclic if and only if $|G| = \exp(G)$.

Consider the polynomial $f(X) = X^{\exp(G)} - 1 \in F[X]$. Then every element of $G$ is a root of $f$, so $f$ has at least $|G|$ roots. But since $\deg(f) = \exp(G)$, $f$ has at most $\exp(G)$ roots, so $|G| \leq \exp(G)$, implying that $|G| = \exp(G)$ and $G$ is cyclic. □

**Proposition 28.** *Let $E$ be a field and let $F_1$ and $F_2$ be finite subfields of $E$ of the same cardinality. Then $F_1 = F_2$.*

*Proof.* Let $n$ be the common cardinality of $F_1$ and $F_2$, and consider the polynomial $f(X) = X^n - X$. Then every element of $F_1$ is a root of $f$, and there are $n = \deg(f)$ such elements, so these are all the roots. Similarly, $F_2$ equals the set of roots of $f$, so $F_1 = F_2$. □

Let $p$ be prime. Denote the field $\mathbb{Z}/p\mathbb{Z}$ by $\mathbb{F}_p$.

**Proposition 29.** *Let $E/F$ be an algebraic field extension, where $F \cong \mathbb{F}_p$. Let $r$ be a positive integer and set $q = p^r$. Define $\phi : E \to E$ by $\phi(a) = a^q$. Then $\phi$ is an automorphism which fixes $F$ pointwise.*

*Proof.* Clearly $\phi(1) = 1$ and $\phi(ab) = \phi(a)\phi(b)$. Also $\phi(a + b) = (a + b)^q = \sum_{i=0}^{q} \binom{q}{i} a^i b^{q-i}$. For $i \neq 0, q$, $\binom{q}{i}$ is divisible by $q$ and thus by $p$, and is zero modulo $p$. This gives $\phi(a + b) = \phi(a) + \phi(b)$. Since $E$ is a field, it contains no zero divisors, so $\phi$ is injective. Now $F^*$ is cyclic of order $p - 1$, and $p - 1$ divides $q - 1$, so $\phi(a) = a^{q-1}a = a$ for $a \in F$. That is, $\phi$ is fixed on $F$, and since $E/F$ is algebraic, $\phi$ must be an automorphism. □

**Proposition 30.** *Let $E$ be a finite field of characteristic $p$. Then $|E| = p^r$ for some positive integer $r$.*

*Proof.* The characteristic subring of $E$ is isomorphic to the field $\mathbb{F}_p$, and $E$ is a finite dimensional vector space over this, say of dimension $r$. Thus $E \cong \mathbb{F}_p^r$ as a vector space, and $|E| = p^r$. □

**Proposition 31.** *Let $p$ be prime and let $r$ be a positive integer. Set $q = p^r$. Then there exists a field of cardinality $q$ which is unique up to isomorphism. Denote such a field by $\mathbb{F}_q$.*

*Proof.* Any field of prime cardinality must equal its characteristic subring, so it is isomorphic to $\mathbb{F}_p$.

Let $E$ be the splitting field of the polynomial $f(X) = X^q - X$ over $\mathbb{F}_p$, and let $\phi$ be the $q^{\text{th}}$ power map on $E$. Then $\phi$ is an automorphism. The fixed field of $\phi$ consists exactly of the roots of $f(X)$. These roots are distinct, since the derivative of $f$ equals $-1$ modulo $p$, and has no roots. Then clearly $E = \text{Fix}(\phi)$ and $|E| = q$.

Given two fields of cardinality $q$, each is of characteristic $p$ and may be embedded in an algebraic closure of $\mathbb{F}_p$. There images there must be equal, so they must be isomorphic. □

**Proposition 32.** *Let $r$ and $s$ be positive integers. Then $\mathbb{F}_{p^r} \leq F_{p^s}$ if and only if $r \mid s$.*

*Proof.* Suppose $\mathbb{F}_{p^r} \leq \mathbb{F}_{p^s}$. Then $\mathbb{F}_{p^s}$ is a vector space over $\mathbb{F}_{p^r}$, say of dimension $n$, so $p^s = |\mathbb{F}_{p^s}| = (p^r)^n = p^r n$. Thus $r$ divides $s$.

On the other hand, suppose $r$ divides $s$. Let $\widetilde{\mathbb{F}}_p$ be an algebraic closure of $\mathbb{F}_p$, and view $\mathbb{F}_{p^r}$ and $\mathbb{F}_{p^s}$ as subfields of $\widetilde{\mathbb{F}}_p$. Then $\mathbb{F}_{p^s}$ is exactly the set of roots of the polynomial $f_s(X) = X^{p^s} - X$, and $\mathbb{F}_{p^r}$ is the set of roots of $f_r(X) = X^{p^r} - X$. Now $f_r$ divides $f_s$, so the roots of $f_r$ are in $\mathbb{F}_{p^s}$. □

## 9. Splitting Extensions of Collections

**Definition 10.** Let $E/F$ be a field extension and let $\Gamma = \{f_i(X) \mid i \in I\} \subset F[X]$ be a collection of polynomials over $F$, where $I$ is any indexing set. We say that $\Gamma$ *splits* in $E$ if each of the $f_i \in \Gamma$ splits in $E$. We say that $E$ is a *splitting field* for $\Gamma$ if $\Gamma$ splits in $E$ and $E$ is generated by $F$ and all the roots of all the polynomials in $\Gamma$.

**Proposition 33.** *Let $F$ be a field and let $\Gamma = \{f_i \mid i \in I\} \subset F[X]$ be a collection of polynomials over $F$, where $I$ is any indexing set. Then there exists a field $E$ containing $F$ which is a splitting field for $\Gamma$.*

*Proof.* Let $K$ be an algebraic closure of $F$. Then $\Gamma$ splits in $K$; the subfield of $K$ generated by $F$ and all the roots of the polynomials in $\Gamma$ is a splitting field. □

**Proposition 34.** *Let $F$ be a field and let $\Gamma = \{f_i \mid i \in I\} \subset F[X]$ be a collection of polynomials over $F$, where $I$ is any indexing set. Let $E_1$ and $E_2$ be splitting fields for $\Gamma$ over $F$. Then there exists an isomorphism $\phi : E_1 \to E_2$ which is the identity on $F$.*

*Proof.* Let $K$ be an algebraic closure of $F$. Since $E_1/F$ and $E_2/F$ are algebraic extensions, there exist embeddings $\phi_1 : E_1 \to K$ and $\phi_2 : E_2 \to K$. The images of both maps are generated by $F$ and the roots of the polynomials in $\Gamma$, so the images are identical, and $\phi_2^{-1} \circ \phi_1 : E_1 \to E_2$ is an isomorphism. □

## 10. Normal Extensions

**Definition 11.** Let $E/F$ be an algebraic field extension. We say that $E/F$ is *normal* if every polynomial $f(X) \in F[X]$ which has a root in $E$ splits in $E$.

**Proposition 35.** *Let $F \leq E \leq K$ be fields with $K/F$ algebraic. If $K/F$ is normal, then so is $K/E$.*

*Proof.* Let $f \in E[X]$ be a polynomial with a root $\alpha \in K$. Since $K/F$ is normal, all of the roots $f = \min(\alpha/F)$ are in $K$. Since $f$ may be viewed as a polynomial over $E$, $g = \min(\alpha/E)$ is a factor of $f$, so all the roots of $g$ are in $K$. Thus $K/E$ is normal. □

**Proposition 36.** *Let $E/F$ be a finite normal extension. Then $E$ is the splitting field over $F$ of a polynomial over $F$.*

*Proof.* Suppose $E/F$ is a normal extension. Since it is a finite extension, $E = F(\alpha_1, \ldots, \alpha_n)$ for some $\alpha_i \in E$. Let $f_i(X) \in F[X]$ be the minimum polynomial of $\alpha_i$. Let $f(X) = \prod_{i=1}^{n} f_i(X)$. Then since $E/F$ is normal, $f(X)$ splits in $E$, and since $E$ is generated by some of the roots of $f$ and contains them all, $E$ is generated by all the roots of $f$. Thus $E$ is a splitting field of $f$. □

Thus finite normal extensions are splitting fields; later we will see when they are splitting fields of an irreducible polynomial.

**Theorem 4** (Normality Characterization Theorem)**.** *Let $E/F$ be an algebraic extension, and let $K$ be an algebraic closure of $E$. Then the following conditions are equivalent:*

- **(a)** *$E/F$ is a normal extension;*
- **(b)** *$E$ is the splitting field over $F$ of a collection of polynomials over $F$;*
- **(c)** *every automorphism of $K$ which fixes $F$ pointwise fixes $E$ setwise.*

*Proof.*

**(a) ⇒ (b)** Suppose $E/F$ is a normal extension. Let $\Gamma = \{f \in F[X] \mid f(\alpha) = 0 \text{ for some } \alpha \in E\}$. For $f \in \Gamma$, $f$ splits in $E$ because $E/F$ is normal. Clearly $E$ is generated by $F$ and the roots of the polynomials in $\Gamma$. It follows that $E$ is the splitting field over $F$ of $\Gamma$.

**(b) ⇒ (c)** Suppose $E$ is the splitting field over $F$ of $\Gamma \subset F[X]$. Let $A = \{\alpha \in E \mid f(\alpha) = 0 \text{ for some } f \in \Gamma\}$. Then $E = F[A]$.

Let $\phi$ be an automorphism of $K$ which fixes $F$ pointwise. We wish to show that $\phi(E) = E$. Let $\alpha \in A$ so that $\alpha$ is a root of some $f \in \Gamma$. Then $\phi(f(\alpha)) = f(\phi(\alpha))$ because $\phi$ fixes the coefficients of $f$, so $f(\phi(\alpha)) = 0$, and $\phi(\alpha)$ is also a root of $f$, and $\phi(\alpha) \in A$, so $\phi(A) \subset A$. Similarly $\phi^{-1}(\alpha) \in A$, which shows that $\phi(A) = A$. Thus $\phi(E) = \phi(F[A]) = \phi(F)[\phi(A)] = F[A] = E$.

**(c) ⇒ (a)** Suppose that $E/F$ is not normal. Then there exists a polynomial $f \in F[X]$ with roots $\alpha, \beta \in K$ such that $\alpha \in E$ and $\beta \notin E$. The embedding $F[\alpha] \to K$ fixed pointwise on $F$ and otherwise given by $\alpha \mapsto \beta$ extends to an embedding $K \to K$ which is an automorphism of $K$. This automorphism does not fix $E$ setwise. □

**Definition 12.** Let $E/F$ be an algebraic extension and let $\widetilde{F}$ be an algebraic closure of $F$. The *normal closure* of $E/F$ in $\widetilde{F}$ is the intersection of all normal extensions of $F$ in $\widetilde{F}$ containing the image of an embedding of $E/F$ in $\widetilde{F}$.

## 11. Separable Extensions

**Definition 13.** Let $E/F$ be a field extension. We say that $E/F$ is *separable* if every polynomial $f$ over $F$ with a root in $E$ has $\deg(f)$ distinct roots in a splitting field of $f$ over $F$.

**Proposition 37** (Primitive Element Theorem)**.** *Let $E/F$ be a finite separable extension. Then $E/F$ is primitive.*

*Proof.* First assume that $F$ is finite. Then $E$ is also finite, and $E^*$ is a cyclic group, and a generator for this group will be a primitive element for $E/F$. Thus we may assume that $F$ is infinite.

Since $E/F$ is finite, we have $E = F[\alpha_1, \ldots, \alpha_n]$ for some elements $\alpha_i \in E$ which are algebraic over $F$. By induction on the number of generators, we may assume that $F[\alpha_1, \ldots, \alpha_{n-1}]$ has a primitive element $\alpha \in E$. Set $\beta = \alpha_n$ so that $E = F[\alpha, \beta]$. Let $f = \min(\alpha/F)$ and $g = \min(\beta/F)$, and let $K$ be a splitting field of $fg$ over $F$. Let $A = \{-\frac{a-\alpha}{b-\beta} \in K \mid a, b \in K \setminus \{\alpha, \beta\},\ f(a) = 0,\ g(b) = 0\}$. This is a finite set. Since $F$ is infinite, we may select $c \in F \setminus A$. Set $\gamma = \alpha + c\beta$ and $L = F[\gamma]$. We claim that $E = L$.

Let $h(X) = f(\gamma - cX)$. Then $h \in L[X]$ and $h(\beta) = 0$. Let $b \in K \setminus \{\beta\}$ be a root of $g$ and suppose $h(b) = 0$. Then $f(\alpha + c\beta - cb) = 0$ so $\alpha + c\beta - cb = a$ for some root $a$ of $f$. Solving for $c$ gives $c = -\frac{a-\alpha}{b-\beta}$; but we selected $c$ away from this set. Thus the only common root between $g$ and $h$ is $\beta$, so $\gcd(g, h) = (X - \beta)^k$ for some $k$. Since $E/F$ is separable, $k = 1$. Thus $\beta \in L$, which implies that $\alpha \in L$, and $L = E$. □

**Theorem 5** (Primitive Characterization Theorem)**.** *Let $E/F$ be a finite extension. Then $E/F$ is a primitive extension if and only if there are only finitely many distinct intermediate fields between $E$ and $F$.*

*Proof.*

($\Rightarrow$) Suppose that $E/F$ is a primitive extension and let $\alpha$ be a primitive element. Let $f(X)$ be the minimum polynomial of $\alpha$ over $F$. Let $K$ be an intermediate field and let $g_K$ be the irreducible polynomial of $\alpha$ over $K$. Then $g_K$ divides $f$. We obtain a map $K \mapsto g_K$ defined on the collection of intemediate fields into a finite set of polynomials.

Now let $K_1$ and $K_2$ be intermediate fields and suppose that $g_{K_1} = g_{K_2} = g$. Let $K_0$ be the subfield of $K_1$ (and $K_2$) generated over $F$ by the roots of $g$. Since $g$ is irreducible over $K_1$ (and $K_2$), it is irreducible over $K_0$. Thus $[E : K_0] = [E : K_1]$, so $K_0 = K_1$; similarly $K_0 = K_2$, so the maps $K \mapsto g_K$ is injective. This proves that there are only finitely many intermediate fields between $E$ and $F$.

($\Leftarrow$) Assume that $F$ is infinite. For every element $\alpha \in E$, we have $[F(\alpha) : F] \leq [E : F] < \infty$; we may select $\alpha$ such that $[F(\alpha) : F]$ is maximal among all of the primitive subextensions. Suppose that $F(\alpha) \neq E$. Let $\beta \in E \setminus F(\alpha)$. There are only finitely many fields of the form $F(\alpha + c\beta)$ as $c$ ranges throughout the infinite field $F$; thus for some $c_1 \neq c_2$, we have $F(\alpha + c_1\beta) = F(\alpha + c_2\beta)$. Call this field $K$. Then $\alpha + c_1\beta$ and $\alpha + c_2\beta$ are both in $K$, and so there difference $(c_2 - c_1)\beta$. Since $c_2 - c_1 \in K$, so is $\beta$; thus $\alpha$ is also in $K$. Thus $K = F(\alpha + c_1\beta)$ is a primitive field extension of $F$ containing $F(\alpha)$, contradicting our choice of $\alpha$. □

## 12. Automorphisms and Fixed Fields

**Definition 14.** Let $E$ be a field. The *automorphism group* of $E$ is

$$\mathrm{Aut}(E) = \{\phi : E \to E \mid \phi \text{ is a bijective homomorphism }\},$$

and $\mathrm{Aut}(E) \leq \mathrm{Sym}(E)$.

Let $E/F$ be a field extension. The *automorphism group* of $E/F$ is

$$\mathrm{Aut}(E/F) = \{\phi \in \mathrm{Aut}(E) \mid \phi(a) = a \text{ for every } a \in F\},$$

and $\mathrm{Aut}(E/F) \leq \mathrm{Aut}(E)$.

**Proposition 38.** *Let $E/F$ be a finite separable extension. Then $|\mathrm{Aut}(E/F)| \leq [E : F]$.*

*Proof.* Let $\alpha$ be a primitive element for $E/F$ so that $E = F[\alpha]$. Let $f = \min(\alpha/F)$. Then $\deg(f) = [E : F]$. Now any automorphism $\phi$ of $E$ which fixes $F$ also fixes $f$, so it sends $\alpha$ to another root of $f$. The automorphism is completely determined by the destination of $\alpha$, and there are at most $\deg(f)$ roots of $f$ in $E$. Thus $|\mathrm{Aut}(E/F)| \leq [E : F]$. □

**Remark 1.** This remains true without the hypothesis of separable.

**Definition 15.** Let $\phi \in \mathrm{Aut}(E)$. The *fixed field* of $\phi$ is

$$\mathrm{Fix}(\phi) = \{x \in E \mid \phi(x) = x\},$$

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

Let $G \leq \mathrm{Aut}(E)$. The *fixed field* of $G$ is

$$\mathrm{Fix}(G) = \{x \in E \mid \phi(x) = x \text{ for every } \phi \in G\},$$

and $\mathrm{Fix}(G) = \cap_{\phi \in G} \mathrm{Fix}(\phi)$ is a subfield of $E$.

**Proposition 39.** *Let $E$ be a field with subfields $F$ and $K$. Let $H, G \leq \mathrm{Aut}(E)$. 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)** $\mathrm{Fix}(\mathrm{Aut}(E/F)) \supset F$.

## 13. Galois Extensions

**Definition 16.** Let $E/F$ be a field extension. We say that $E/F$ is *Galois* if it is finite, normal, and separable.

**Proposition 40.** *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 41** (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, so it must be the minimum polynomial. 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 fix $F$, 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 6** (Galois Characterization Theorem)**.** *Let $E/F$ be a finite extension. Then the following conditions are equivalent:*

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

*Proof.*

**(a)** $\Rightarrow$ **(b)** 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 $E$.

**(b)** $\Rightarrow$ **(c)** 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 $F = K$.

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

**Proposition 42.** *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. □

## 14. Galois Correspondence

**Definition 17.** If $E/F$ is a Galois extension, the set of all automorphisms of $E$ which fix $F$ is denoted $\mathrm{Gal}(E/F)$.

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.

**Theorem 7** (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. □

## 15. Fundamental Theorem of Algebra

**Theorem 8** (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 $\mathbb{C}$. □

## 16. Galois Solvability Criterion

**Definition 18.** 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 19.** 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 abelian.

**Theorem 9.** *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.*

Additional Material

## 17. Multiplicity of Roots

**Definition 20.** Let $F$ be a field and let $K$ be an algebraic closure of $F$. Let $f \in F[X]$ and let $\alpha \in K$. The *multiplicity* of $\alpha$ in $f$, denoted by $\mathrm{mul}(f, \alpha)$, is the largest nonnegative integer $n$ such that $f(X) = (X - \alpha)^n g(X)$ for some $g \in E[X]$, where $E$ is a splitting field of $f$.

If $\mathrm{mul}(f, \alpha) = 0$, then $\alpha$ is not a root of $f$. If $\mathrm{mul}(f, \alpha) = 1$, we call $\alpha$ a *simple root* of $f$. If $\mathrm{mul}(f, \alpha) > 1$, we call $\alpha$ a *multiple root* of $f$.

**Definition 21.** Let $F$ be a field and let $f \in F[X]$, and write $f(X) = \sum_{i=0}^{n} a_i X^i$, where $a_i \in F$. Define the *derivative* of $f$, denoted $f'$, to be the polynomial

$$f'(X) = a_1 + 2a_2 X + \cdots + n a_n X^{n-1}.$$

**Proposition 43.** *Let $F$ be a field and let $f \in F[X]$. Let $h$ be another indeterminate and view $f$ and $f'$ as polynomials in $F[X, h]$. Then $f(X+h) \in F[X, h]$ and $h$ divides $f(X + h) - f(X)$. Define $g(X) = \frac{f(X+h)-f(X)}{h}$. Then $f'(X) = g(X, 0)$.*

*Proof.* Apply the binonmial theorem to terms $(X+h)^k$ in $f(X+h)$, cancel duplicate terms in the numerator, then cancel the $h$. □

**Proposition 44.** *Let $F$ be a field, $f(X) \in F[X]$, $E$ a splitting field of $f$, and $\alpha \in E$ a root of $f$. Then*

- **(a)** $\mathrm{mul}(f, \alpha) = \mathrm{mul}(f', \alpha) + 1$*;*
- **(b)** *$\alpha$ is a multiple root if and only if $\alpha$ is a root of $f'$.*

*Proof.* Compute. □

**Definition 22.** Let $F$ be a field and let $f \in F[X]$. We say that $f$ is *separable* if its irreducible factors have only simple roots. Otherwise $f$ is *inseparable*. Let $E/F$ be a field extension and let $\alpha \in E$ be algebraic over $F$. We say that $\alpha$ is separable over $F$ if $\min(\alpha/F)$ is separable.

**Example 4.** We give an example of an inseparable polynomial. Let $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ be the field of cardinality $p$. Let $t$ be transcendental over $\mathbb{F}_p$. Let $K = \mathbb{F}_p(t)$. Consider $f \in K[X]$ given by $f(X) = X^p - t$. Let $r$ be a $p^{\text{th}}$ root of $t$. Then $f(X) = (X - r)^p = X^p - r^p$, so $r$ is a root of multiplicity $p$.

**Definition 23.** Let $F$ be a field. We say that $F$ is *perfect* if every nonzero polynomial over $F$ is separable.

**Proposition 45.** *Let $F$ be a field of characteristic zero. Then $F$ is perfect.*

*Proof.* Let $f \in F[X]$ be a nonzero polynomial which we may assume is irreducible. Let $E$ be a splitting field of $f$ over $F$. Let $\alpha \in E$ be a root of $f$. Then $\deg(f') < \deg(f)$, and $f'$ is not the zero polynomial. Since $f$ is a nonzero polynomial of minimal degree of which $\alpha$ is a root, $\alpha$ is not a root of $f'$. Thus $f$ is separable. □

**Proposition 46.** *Let $F$ be a field of characteristic $p > 0$. Then $F$ is perfect if and only if the map $F \to F$ given by $a \mapsto a^p$ is surjective.*

*Wait.* We will see this later. As a consequence, every finite field is perfect. □

## 18. Embeddings

**Definition 24.** Let $E/F$ and $L/F$ be field extensions. The *embedding set* of $E/F$ with respect to $L$ is

$$\mathrm{Emb}_L(E/F) = \{\phi : E \to L \mid \phi(a) = a \text{ for every } a \in F\}.$$

**Proposition 47.** *Let $E/F$ be an algebraic field extension and let $L$ be a field containing $F$. Then $\mathrm{Aut}(E/F)$ acts freely on the right of $\mathrm{Emb}_{\widetilde{F}}(E/F)$ via composition. Thus $|\mathrm{Aut}(E/F)| \leq |\mathrm{Emb}_{\widetilde{F}}(E/F)|$.*

*Proof.* The action is given by, for $\psi \in \mathrm{Aut}(E/F)$ and $\sigma \in \mathrm{Emb}_L(E/F)$, $\sigma\psi = \sigma \circ \psi$. This clearly a group action. To see that it is free, select $\psi_1, \psi_2 \in \mathrm{Aut}(E/F)$ and $\sigma \in \mathrm{Emb}_L(E/F)$ such that $\sigma\psi_1 = \sigma\psi_2$. View $\sigma$ as an isomorphism onto $\sigma(E)$. As such, it is invertible, and multiplying on the left yields $\psi_1 = \psi_2$. This shows that the action is free. □

**Proposition 48.** *Let $E/F$ be an algebraic field extension and let $\widetilde{F}$ be an algebraic closure of $F$. Then $\mathrm{Aut}(\widetilde{F}/F)$ acts transitively on the left of $\mathrm{Emb}_{\widetilde{F}}(E/F)$ via composition.*

*Proof.* The action is given by, for $\phi \in \mathrm{Aut}(E/F)$ and $\sigma \in \mathrm{Emb}_{\widetilde{F}}(E/F)$, $\phi\sigma = \phi \circ \sigma$. This clearly a group action. To see that it is transitive, let $\sigma_1, \sigma_2 \in \mathrm{Emb}_{\widetilde{F}}(E/F)$. Let $\widetilde{E}$ be an algebraic closure of $E$. Then $\sigma_i$ extends to an embedding $\widetilde{\sigma}_i : \widetilde{E} \to \widetilde{F}$ for $i = 1, 2$, which are isomorphisms by a previous argument. Then $\phi = \widetilde{\sigma}_2 \circ \widetilde{\sigma}_1^{-1}$ is an automorphism of $\mathrm{Aut}(\widetilde{F}/F)$. Moreover, $\phi\sigma_1 = \sigma_2$. This shows that the action is transitive. □

**Definition 25.** Let $E/F$, $K/E$, and $L/F$ be field extensions and let $\sigma \in \mathrm{Emb}_L(E/F)$. The *lifting set* of $\sigma$ to $K$ is

$$\mathrm{Lif}_L(K/F, \sigma) = \{\tau \in \mathrm{Emb}_L(K/F) \mid \tau \restriction_E = \sigma\}.$$

**Proposition 49.** *Let $E/F$ and $K/E$ be finite extensions and let $\widetilde{F}$ be an algebraic closure of $F$. Let $\sigma_1, \sigma_2 \in \mathrm{Emb}_{\widetilde{F}}(E/F)$. Then*

$$|\mathrm{Lif}_{\widetilde{F}}(K/F, \sigma_1)| = |\mathrm{Lif}_{\widetilde{F}}(K/F, \sigma_2)|.$$

*Proof.* The group $\mathrm{Aut}(\widetilde{F}/F)$ acts transitively on $\mathrm{Emb}_{\widetilde{F}}(E/F)$; let $\phi \in \mathrm{Aut}(\widetilde{F}/F)$ such that $\phi\sigma_1 = \sigma_2$. Define a function $\mathrm{Lif}_{\widetilde{F}}(K/F, \sigma_1) \to \mathrm{Lif}_{\widetilde{F}}(K/F, \sigma_2)$ by $\tau \mapsto \phi \circ \tau$. The function $\tau \mapsto \phi^{-1} \circ \tau$ is clearly an inverse, so this function is bijective. □

**Proposition 50.** *Let $E/F$ and $K/E$ be finite field extensions, and let $\widetilde{F}$ be an algebraic closure of $F$ which contains $E$. Then*

$$|\mathrm{Emb}_{\widetilde{F}}(K/F)| = |\mathrm{Emb}_{\widetilde{F}}(K/E)||\mathrm{Emb}_{\widetilde{F}}(E/F)|.$$

*Proof.* Each embedding of $K/F$ into $\widetilde{F}$ produces an embedding of $E/F$ and a lift of this embedding to $K/E$. Each embedding has the same number of lifts, and that number is $|\mathrm{Emb}_{\widetilde{F}}(K/E)|$, since these are lifts of the identity embedding. The result follows. □

**Definition 26.** Let $E/F$ be a field extension and let $\widetilde{F}$ be an algebraic closure of $F$.

Let $\Psi : \mathrm{Aut}(E/F) \to \mathrm{Sym}(\mathrm{Emb}_{\widetilde{F}}(E/F))$ be the homomorphism given by the free right action of $\mathrm{Aut}(E/F)$.

Let $\Phi : \mathrm{Aut}(\widetilde{F}/F) \to \mathrm{Sym}(\mathrm{Emb}_{\widetilde{F}}(E/F))$ be the homomorphism given by the transitive left action of $\mathrm{Aut}(E/F)$.

The *Galois group* of $E/F$ is the image of $\Phi$, and is denoted $\mathrm{Gal}(E/F)$.

**Proposition 51.** *Let $E/F$ be a field extension and let $\widetilde{F}$ be an algebraic closure of $F$. Let $S = \mathrm{Sym}(\mathrm{Emb}_{\widetilde{F}}(E/F))$, $G = \mathrm{Gal}(E/F)$, and $A = \Psi(\mathrm{Aut}(E/F))$. Then*

**(a)** *$C_S(G) = A$;*
**(b)** *$N_G(T)/T \cong A$.*

**Definition 27.** Let $f \in F[X]$. The *distinct root set* of $f$ with respect to $L$ is

$$\mathrm{Zer}_L(f) = \{\beta \in L \mid f(\beta) = 0\}.$$

**Proposition 52.** *Let $E/F$ and $L/F$ be fields extensions and let $\alpha \in E$ be algebraic over $F$ with $f = \min(\alpha/F)$. Define $\epsilon_\alpha : \mathrm{Zer}_L(f) \to \mathrm{Emb}_L(F[\alpha]/F)$ by $\beta \mapsto \psi_{\beta\alpha}$. Then $\epsilon_\alpha$ is bijective.*

*Proof.* We have already noted by $\psi_{\beta\alpha}$ is an isomorphism of $F[\alpha]$ onto $F[\beta]$, and thus into $L/F$ when $\beta \in K$. Clearly, sending $\alpha$ to different destinations in $K$ produces different embeddings, so $\epsilon_\alpha$ is injective. Moreover, any embedding sends $\alpha$ to a root of $f$, so $\epsilon_\alpha$ is surjective. □

## 19. Separable Extensions

**Definition 28.** Let $E/F$ be an algebraic extension. We say that $E/F$ is *separable* if every nonzero element of $E$ is separable over $F$.

**Proposition 53.** *Let $F \leq E \leq K$ be fields with $K/F$ algebraic. If $K/F$ is separable, then so is $K/E$.*

*Proof.* Let $\alpha \in K$, $f = \min(\alpha/F)$, and $g = \min(\alpha/E)$. Since $K/F$ is separable, $f$ has no multiple roots. Since $g$ is a factor of $f$, $g$ has no multiple roots. Thus $K/E$ is separable. □

**Proposition 54.** *Let $E/F$ be a finite extension and let $\widetilde{F}$ be an algebraic closure of $F$. Then*

**(a)** *$|\mathrm{Emb}_{\widetilde{F}}(E/F)| \leq [E : F]$;*
**(b)** *$|\mathrm{Emb}_{\widetilde{F}}(E/F)| = [E : F]$ if $E/F$ is separable.*

*Proof.* Since $E/F$ is finite, we may find a a proper subfield $K \leq E$ containing $F$ such that $K/F$ is finite and $E/K$ is primitive, say $E = K[\alpha]$ with $\alpha$ algebraic over $K$. By induction on the degree of the extension, we may assume that $|\mathrm{Emb}_{\widetilde{F}}(K/F)| \leq [K : F]$ and that $|\mathrm{Emb}_{\widetilde{F}}(K/F)| = [K : F]$ if $K/F$ is separable. □

**Theorem 10** (Primitive Element Theorem)**.** *Let $E/F$ be a finite separable extension. Then $E/F$ is a primitive extension.*

*Proof.* If $F$ is a finite field, then so is $E$, so $E^*$ is a cyclic group. A generator for $E^*$ is a primitive element for $E/F$. Thus assume that $F$ is infinite.

Since $E/F$ is a finite extension, it is generated by a finite number of elements: $E = F(\alpha_1, \ldots, \alpha_n, \beta)$. By induction, any proper subextension has a primitive element, so let $F(\alpha_1, \ldots, \alpha_n) = F(\alpha)$ for some $\alpha \in E$. Now $E = F(\alpha, \beta)$.

Let $\widetilde{F}$ be an algebraic closure of $F$. Since $E/F$ is separable, there exist $n = [E : F]$ distinct embeddings of $E$ into $\widetilde{F}$; label them $\sigma_1, \ldots, \sigma_n$. Consider the polynomial

$$f(X) = \prod_{i \neq j} (\sigma_i \alpha + \sigma_i \beta X - \sigma_j \alpha - \sigma_j \beta X).$$

This is not the zero polynomial, so it has a finite number of roots in $\widetilde{F}$, but $F$ is infinite. Thus $f(c) \neq 0$ for some $c \in F$. Thus the elements $\sigma_i \alpha + c\sigma_i \beta$ are distinct as $i$ ranges from 1 to $n$.

This shows that the $\sigma_i$ are distinct embeddings of $K = F(\alpha + c\beta)$ into $\widetilde{F}$, so that $[K : F] \geq [K : F]_s \geq n$. But $K \leq E$, so $[K : F] \leq [E : F] = n$. Then $[K : F] = [E : F]$, and $K = E$. Thus $E/F$ is a primitive extension, generated by $\alpha + c\beta$. $\square$

## 20. Field Exercises

**Problem 1.** Let $D$ be pid.
For $f(X) = a_0 + a_1X + \cdots + a_nX^n \in D[X]$, define

$$\sigma(f) = \sum_{i=0}^{n} a_i; \qquad I = \{f(X) \in D[X] \mid \sigma(f) = 0\}.$$

Show that $I$ is a prime ideal of $D[X]$ and that $D[X]/I \cong D$.

**Problem 2.** Let $D$ be pid and let $a \in D$ be prime.
For $f(X) = a_0 + a_1X + \cdots + a_nX^n \in D[X]$, define

$$\sigma(f) = a_0; \qquad I = \{f(X) \in D[X] \mid a \text{ divides } \sigma(f)\}.$$

Show that $I$ is a maximal ideal of $D[X]$ and that $D[X]/I \cong D/aD$.

**Problem 3.** Let $F$ be a finite field of cardinality 1331.
Show that the polynomial $f(X) = X^2 + X + 1$ is irreducible over $F$.
(Hint: Note that $X^3 - 1 = (X - 1)(X^2 + X + 1)$ and that $F^*$ is a group under multiplication; what are the possible orders of its elements?)

**Problem 4.** Let $F$ be a finite field of cardinality 343.
Show that the polynomial $f(X) = X^5 + X^4 + X^3 + X^2 + X + 1$ splits in $F[X]$.

**Problem 5.** Let $F$ be a finite field of cardinality 101.
Find all square roots of $-1$ in $F$.

**Problem 6.** Let $F$ be a finite field of cardinality 243.
Show that $\sqrt{-1}$ does not exist in $F$.

**Problem 7.** Let $F$ be a finite field of cardinality $q$, and suppose that $q \equiv 3 \mod 4$.
Show that the polynomial $f(X) = X^2 + 1$ is irreducible over $F$.

**Problem 8.** Show that $\mathbb{F}_{51}[X]/\langle X^2 - 15X - 1\rangle$ is not a field.

**Problem 9.** Let $R = \mathbb{F}_3[X]$ be the ring of polynomials over $\mathbb{F}_3$.
Find an ideal $A \triangleleft R$ such that $R/A$ is a nondomain with six elements.

**Proposition 55.** *Determine the Galois correspondence for each of the following polynomials over* $\mathbb{Q}$*:*

- **(a)** $f(X) = X^3 - 2$*;*
- **(b)** $f(X) = X^4 - 2$*;*
- **(c)** $f(X) = X^8 - 10X^4 + 19$*;*
- **(d)** $f(X) = X^5 - 2$*;*
- **(e)** $f(X) = X^5 - 4X + 2$.

## References


[Ar44] Artin, Emil, *Galois Theory* 2nd edition, University of Notre Dame (1944)
[Ar91] Artin, Michael, *Algebra*, Prentice-Hall, Inc. (1991)
[Ja85] Jacobson, Nathan, *Basic Algebra I* 2nd edition, W. H. Freeman and Company (1985)
[La93] Lang, Serge, *Algebra* 3th edition, Addison-Wesley Publishing Company (1993)
[Mc76] McCarthy, Paul J., *Algebraic Extensions of Fields*, Dover Publications, Inc. (1976)



Department of Mathematics, University of California, Irvine
*Email address*: pbailey@math.uci.edu