Department of Mathematics

Introduction to Field Theory

Author
Gabriel Gress

June 11, 2021

Chapter 1

Introduction to Field Extensions

Recall the definition of a field.

Definition 1.0.1

A **field** is a commutative ring F with multiplicative identity 1_F in which every nonzero element has a multiplicative inverse.

Furthermore, recall that the **characteristic** of a field F, denoted $\mathrm{char}(F)$, is the smallest positive integer n such that

$$1_F + 1_F + \dots_n + 1_F = 0_F$$

if such an $n \in \mathbb{N}$ exists. Otherwise, we say that $\mathrm{char}(F) = 0$.

Proposition 1.0.1

For a field F, we have that $\mathrm{char}(F) = 0$ or $\mathrm{char}(F) = p$ for a prime integer p. If $\mathrm{char}(F) = p$, then $p \cdot \alpha = \alpha + \dots_p + \alpha = 0_F$ for all $\alpha \in F$.

We often refer to fields with prime characteristics as **fields of positive characteristic**.

Some fields of characteristic zero include $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$. Any field of the form $\mathbb{Z}/p\mathbb{Z} := \mathbb{F}_p$ is a field of characteristic p.

1.1 Subfields

Definition 1.1.1

A **subfield** of a field F is a nonempty subset S containing 1_F that is a subring under the addition and multiplication of F, and so that S is closed under taking multiplicative inverse.

The **prime subfield** of a field F is the subfield generated by the multiplicative identity 1_F of F, that is, it is the smallest subfield of F containing 1_F.

Proposition 1.1.1

The prime subfield of a field F is either $\mathbb{Q}$ if $\mathrm{char}(F) = 0$, or $\mathbb{F}_p$ if $\mathrm{char}(F) = p$.

Definition 1.1.2

A **homomorphism** $\Phi : F_1 \to F_2$ **between fields** F_1 **and** F_2 is a unital ring homomorphism: $\forall x, y \in F_1$

$$\varphi(x + y) = \varphi(x) + \varphi(y)$$
$$\varphi(xy) = \varphi(x)\varphi(y), \quad \varphi(1_{F_1}) = 1_{F_2}$$

Notice that either $F \cong \mathrm{Im}(\varphi)$ or $0 \cong \mathrm{Im}(\varphi)$. This follows from the fact that the only ideals of F are 0 and F.

A lot of fields are better viewed via a ring homomorphism. We can quotient out a ring R by any maximal ideal I of R to get an object isomorphic to a field.

Example 1.1.1

Consider the principal ideal domain $\mathbb{Q}[x]$. For any irreducible polynomial $p(x)$, we have that

$$\mathbb{Q}[x]/(p(x))$$

is a field, where $(p(x))$ denotes the root of $p(x)$. We can in fact see that this space is equivalent to $\mathbb{Q}$ but including the roots of $x^2 - 2$, namely $\sqrt{2}$. One can construct a unital isomorphism so that

$$\mathbb{Q}[x]/(x^2 - 2) \cong \mathbb{Q}(\sqrt{2})$$

1.2 Extension of Fields

Definition 1.2.1

If K is a field containing a subfield F, then K is said to be an **extension of** F, denoted by K/F.

The field F is sometimes called the **base field** of the extension.

Note that if K is an extension of a field F, then K is a F-vector space via the typical F action.

Definition 1.2.2

The **degree** or **index** of a field extension K/F, denoted $[K : F]$, is defined to be $\dim_F K$, the dimension of K as an F-vector space.

For example, $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ and $[\mathbb{C} : \mathbb{R}] = 2$. One can see the latter example by observing that $\mathbb{C} \cong \mathbb{R}[x]/(x^2 + 1)$.

Theorem 1.2.1

Let F be a field and $p(x) \in F[x]$ be an irreducible polynomial. Then $\exists$ a field extension K of F in which $p(x)$ has a root.

This field is given by $K := F[x]/(p(x))$, but we will show this more formally later.

Theorem 1.2.2

Let $p(x) \in F[x]$ be an irreducible polynomial of degree over F, and let K be the field $F[x]/(p(x))$. Take $\theta := x + (p(x))$ (root of $p(x)$). Then

1. The elements $\left\{1_F, \theta, \theta^2, \ldots, \theta^{n-1}\right\}$ are an F-vector space basis of the F-vector space K.
2. $[K : F] = n$
3. $K = \left\{a_0 + a_1\theta + a_2\theta^2 + \ldots + a_{n-1}\theta^{n-1} \mid a_0, \ldots, a_{n-1} \in F\right\}$ as an F-vector space.

Another nice example to be familiar with is $K = \mathbb{F}_2[x]/(x^2 + x + 1)$. This is a field extension of $\mathbb{F}_2$ as $x^2 + x + 1$ is irreducible in $\mathbb{F}_2$. We can see that $[\mathbb{F}_2[x]/(x^2 + x + 1) : \mathbb{F}_2[x]] = 2$ simply because the degree of the polynomial is 2, but we can also directly count elements in the set and see that it has twice the elements of $\mathbb{F}_2[x]$.

Now let's define fields formed by adjoining roots more formally.

Definition 1.2.3

Let K/F be a field extension, and let $\alpha_1, \alpha_2, \ldots \in K$ be elements. The smallest subfield of K containing both F and the elements $\alpha_1, \alpha_2, \ldots$, denoted $F(\alpha_1, \alpha_2, \ldots)$ is called the **field generated by** $\alpha_1, \alpha_2, \ldots$ **over** F.

Definition 1.2.4

The field $F(\alpha)$ generated by a single element α over F is called a **simple extension of** F, and the element α in this case is called **primitive**.

Theorem 1.2.3

Let F be a field and let $p(x) \in F[x]$ be an irreducible polynomial. Suppose K is an extension of F containing a root α of $p(x)$. Then $F[x]/(p(x)) \cong F(\alpha)$.

It is natural to view field extensions as the base field appended with roots, and as a result a few definitions arise.

Definition 1.2.5: Algebraic and Transcendental Elements

An element $\alpha \in K$ is called **algebraic over** F if α is a root of some nonzero polynomial $f(x) \in F[x]$.

If $\alpha \in K$ is not algebraic over F, then we say that α is **transcendental over** F.

The extension K/F is **algebraic over** F if all elements of K are algebraic over F.

Example 1.2.1: Examples of Algebraic and Transcendental Elements

- $\sqrt{2}$ is an algebraic element over $\mathbb{Q}$ via the polynomial $x^2 - 2$. This actually holds for all $\sqrt[n]{2}$ with $x^n - 2$.
- i is algebraic over $\mathbb{R}$ and $\mathbb{Q}$ via the polynomial $x^2 + 1$
- Transcendental elements are much rarer– examples include π and e, but it is non-trivial to show an element is transcendental.

1.3 Minimal Polynomials

Proposition 1.3.1

Let α be an algebraic element over F.

(a). Then there exists a monic irreducible polynomial of minimal degree $m_{\alpha,F}(x) \in F[x]$ which has α as a root.

(b). A polynomial $f(x) \in F[x]$ has α as a root if and only if $m_{\alpha,F}(x) \mid f(x)$ in $F[x]$.

(c). The polynomial $m_{\alpha,F}(x)$ with the property in (a) is unique.

We can see the minimal polynomial must be irreducible, because otherwise one of its factors would have α as a root and hence has degree smaller than $m_{\alpha,F}(x)$, contradicting our hypothesis. The divisibility $m_{\alpha,F}(x) \mid f(x)$ follows from the division algorithm in $F[x]$. The divisibility and minimality conditions together give uniqueness.

Corollary 1.3.1

If K/F is a field extension, and α is algebraic over both F and K, then $m_{\alpha,K}(x)$ divides $m_{\alpha,F}(x)$ in $K[x]$.

This directly follows as $m_{\alpha,F}(x)$ has a root α in K and hence (b) gives us divisibility.

Definition 1.3.1

The polynomial $m_{\alpha,F}(x)$ is called the **minimal polynomial of** α **over** F. The degree of $m_\alpha(x)$ is called the **degree of** α.

In other words, the minimal polynomial of α over F is a monic irreducible polynomial over F that has α as a root. Alternatively, it is a monic polynomial over F of minimal degree with α as a root– both imply the other.

Proposition 1.3.2

Let α be algebraic over F. Then

$$F(\alpha) \cong F[x]/(m_\alpha(x))$$

So that $[F(\alpha) : F] = \deg m_\alpha(x) \equiv \deg \alpha$.

Proposition 1.3.3

An element $\alpha \in F$ is algebraic over F if and only if the simple extension $F(\alpha)/F$ is finite.

If $\alpha \in K$ with $[K : F] = n$, then $\deg(\alpha) \leq n$.

This follows by applying linear dependence to powers α^i with $i = 0, 1, \ldots, n$.

Corollary 1.3.2

If K/F is finite, then K/F is algebraic.

Example 1.3.1

Take F to be a field with $\mathrm{char}(F) \neq 2$. Consider K/F of degree 2, which is hence algebraic. Let $\alpha \in K/F$ so that α is a root of a polynomial over F of degree 1 or 2. Because $\alpha \notin F$, the polynomial must has degree 2.

This implies that $m_{\alpha,F}(x) = x^2 + bx + c$ for $b, c \in F$. This implies that $F(\alpha)$ has the same dimension of K and hence $K = F(\alpha)$ (as K is a field extension of $F(\alpha)$. This implies that $K = F(\sqrt{b^2 - 4ac})$ and so any degree 2 extension of a field F with characteristic not equal to 2 is of the form $F(\sqrt{D})$ for D a non-square element of F.

Conversely, for such a field, $[F(\sqrt{D}) : F] = 2$ and hence extensions of the form $F(\sqrt{D})/F$ are called **quadratic extensions of** F.

Chapter 2

Types of Field Extensions

2.1 Algebraic Extensions

Theorem 2.1.1: Tower Theorem

Let $F \hookrightarrow E \hookrightarrow K$ be a composition of field extensions. Then $[K : F] = [K : E][E : F]$.

One can show this via vector space arguments (look at the bases of the spaces).

Corollary 2.1.1

If K/F is a finite extension, and E is a subfield of K containing F, then $[E : F] \mid [K : F]$.

Example 2.1.1

Let

$$
\begin{aligned}
K &= \mathbb{Q}(\sqrt[6]{2}) \\
E &= \mathbb{Q}(\sqrt{2}) \\
F &= \mathbb{Q}
\end{aligned}
$$

It follow directly from previous work that $[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}] = 6$ and $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. As for K/E, the minimal polynomial is $x^3 - \sqrt{2}$, which gives $[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}(\sqrt{2})] = 3$, which corresponds to what the tower theorem gives us.

Definition 2.1.1

An extension K/F is called **finitely generated** if there exist elements $\alpha_1, \alpha_2, \ldots, \alpha_n$ such that

$$
K = F(\alpha_1, \alpha_2, \ldots, \alpha_n) \quad \text{for } n < \infty
$$

Such an extension can be obtained recursively via simple extensions.

We have that $F(\alpha, \beta) = (F(\alpha))(\beta)$, hence the definition above is consistent.

Example 2.1.2

- $\mathbb{Q}(\sqrt[6]{2}, \sqrt{2}) = \left(\mathbb{Q}(\sqrt[6]{2})\right)(\sqrt{2}) = \mathbb{Q}(\sqrt[6]{2})$ because $\sqrt{2} = (\sqrt[6]{2})^3$.
- One can check that $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is a proper field extension for both $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$.

Theorem 2.1.2

K/F is finite if and only if K is generated by a finite number of algebraic elements over F.

We denote by $\overline{\mathbb{Q}}$ the subfield of $\mathbb{C}$ generated by all algebraic elements of $\mathbb{C}$ over $\mathbb{Q}$. $\overline{\mathbb{Q}}$ is an infinite algebraic extension of $\mathbb{Q}$, and referred to as the **field of algebraic numbers**.

Theorem 2.1.3

If E/F and K/E are algebraic, then K/F is algebraic.

2.2 Composite Field Extensions

Definition 2.2.1: Composite Field

Let K_1 and K_2 be two subfields of a field K. Then the **composite field of** K_1 **and** K_2, denoted by K_1K_2 is the smallest subfield of K containing both K_1 and K_2.

The composite of any collection of subfields $\{K_i\}$ is defined similarly.

Proposition 2.2.1

Let K_1 and K_2 be two finite extensions of F contained in K. Then

$$[K_1K_2 : F] \leq [K_1 : F][K_2 : F]$$

with equality if and only if an F-vector space basis for K_1 is linearly independent over K_2 (or vice versa).

If the F-vector space basis of K_1 is $\alpha_1, \ldots, \alpha_n$ and the F-vector space basis of K_2 is $\beta_1, \ldots, \beta_m$, then $\{\alpha_i\beta_j\}_{i,j=1}^{n,m}$ is a F-vector span of K_1K_2.

Corollary 2.2.1

If, furthermore, $[K_1 : F] = n$ and $[K_2 : F] = m$ with $\gcd(n, m) = 1$, then $[K_1K_2 : F] = [K_1 : F][K_2 : F] = nm$.

Example 2.2.1

- Consider $K = \mathbb{Q}(\sqrt{2})\mathbb{Q}(\sqrt[3]{2})$. We have

$$\begin{aligned}
&\mathbb{Q} \hookrightarrow^2 \mathbb{Q}(\sqrt{2}) \hookrightarrow^3 \mathbb{Q}(\sqrt{2})\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}(\sqrt[6]{2})\\
&\mathbb{Q} \hookrightarrow^3 \mathbb{Q}(\sqrt[3]{2}) \hookrightarrow^2 \mathbb{Q}(\sqrt[6]{2})\\
&\mathbb{Q} \hookrightarrow^6 \mathbb{Q}(\sqrt[6]{2})
\end{aligned}$$

  where $\hookrightarrow^k$ represents a degree k extension.

2.3 Splitting Fields

Recall that for any field F and any polynomial $f(x) \in F[x]$, there exists a field extension K over F that contains a root, say $\alpha \in K$, of $f(x)$. In this case, $f(x) = (x - \alpha)g(x)$ in $K[x]$ as $K[x]$ is a Euclidean domain.

Now we want a field extension K/F so that $f(x) \in F[x]$ splits completely into linear factors in $K[x]$.

Definition 2.3.1

A field extension K of F is called a **splitting field for** $f(x) \in F[x]$ if $f(x) = \prod_i (x - \alpha_i)$ in $K[x]$ and $f(x)$ does NOT factor completely in $K'[x]$ for any proper subfield K' of K.

$f(x) \in K[x]$ splits completely if and only if K contains all roots of $f(x)$.

Example 2.3.1

- The splitting field of $x^2 - 2$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{2})$
- The splitting field of $(x^2 - 2)(x^2 - 3)$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{2}, \sqrt{3})$
- The splitting field of $x^3 - 2$ over $\mathbb{Q}$ is NOT $\mathbb{Q}(\sqrt[3]{2})$. The roots $\sqrt[3]{2}\omega$ and $\sqrt[3]{2}\omega^2$ are in fact imaginary and hence are not in $\mathbb{Q}(\sqrt[3]{2})$ (note that ω represents the principal root of unity).

Theorem 2.3.1

Splitting fields always exist. For any field F, if $f(x) \in F[x]$, then there exists a field extension K of F that is a splitting field for $f(x)$.

Proposition 2.3.1

Take $f(x) \in F[x]$ of degree n. Then for $K :=$ splitting field of $f(x)$, we get that $[K : F] \leq n!$.

Now we discuss the uniqueness of splitting fields.

Theorem 2.3.2

Let $\varphi : F \to F'$ be an isomorphism of fields. Let

$$f(x) = a_n x^n + \ldots + a_1 x + a_0 \in F[x]$$
$$f'(x) = \varphi(a_n) x^n + \ldots + \varphi(a_1) x + \varphi(a_0) \in F'[x].$$

Let E be the splitting field of $f(x)$ over F and E' be the splitting field of $f'(x)$ over F'. Then the isomorphism φ extens to an isomorphism $\sigma : E \to E'$, so that $\sigma\,|_F = \varphi$.

This can be proven by induction on the degree of $f(x)$.

Corollary 2.3.1

Any two splitting fields for a polynomial $f(x) \in F[x]$ over a field F are isomorphic.

Thus we can safely refer to -the- splitting field of a polynomial over a field.

Definition 2.3.2

If K is an algebraic extension of F, which is the splitting field over F for a collection of polynomials $\{f_i(x)\} \in F[x]$, then K is called a **normal** extension of F.

In other words, a normal extension is simply an algebraic extension that is also a splitting field.

Exercise 2.3.1

Determine the splitting field of $x^6 - 4$ over $\mathbb{Q}$ and its degree over $\mathbb{Q}$.

We now focus on the splitting field of $x^n - 1$ in $\mathbb{Q}[x]$. Roots of $x^n - 1$ are of the form $\left\{e^{2\pi i k/n} \mid k = 0, 1, \dots, n-1\right\}$. Some useful notation:

1. $\zeta_n := e^{2\pi i/n}$, the primitive n-th root of 1
2. $\mu_n := \langle \zeta_n \rangle$, the cyclic group of order n under multiplication with identity 1
3. $\varphi(n)$ is the number of integers between $1, \dots, n$ that are coprime– the Euler-Phi function.

Definition 2.3.3: Cyclotomic Field

The **cyclotomic field of n-th roots of unity** or the **n-th cyclotomic field** is $\mathbb{Q}(\zeta_n)$.

The **n-th cyclometric polynomial** is

$$\Phi_n(x) = \prod_{\zeta \text{primitive} \in \mu_n} (x - \zeta).$$

Recall that an n-th root of 1 (that is, $e^{2\pi i k/n}$) is primitive if and only if $(k, n) = 1$. We conventionally choose 1 to be a primitive.

Theorem 2.3.3

(a). $\Phi_n(x)$ is a monic polynomial in $\mathbb{Z}[x]$ of degree $\varphi(n)$

(b). $\Phi_n(x) \in \mathbb{Z}[x]$ is irreducible

(c). The minimal polynomial of a primitive n-th root of unity over $\mathbb{Q}$ is $\Phi_n(x)$

(d). $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$

These will be proved in various ways by later constructions.

Corollary 2.3.2

$$\Phi_n(x) = (x^n - 1) / \prod_{d|n, d<n} \Phi_d(x)$$

We can compute $\Phi_n(x)$ inductively.

As an example, for a prime p:

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x^2 + x + 1$$

2.4 Algebraic Closure

Before, we were looking at extensions of some polynomial in $F[x]$ that contains all the roots of the polynomial. Now we consider field extensions that contain *all* the roots of all $f(x) \in F[x]$.

Definition 2.4.1: Algebraic Closure

Given a field F, a field $\overline{F}$ is the **algebraic closure** of F if

(a). $\overline{F}$ is algebraic over F,

(b). Every polynomial $f(x) \in F[x]$ splits completely over $\overline{F}$

Recall that splitting completely implies that $f(x)$ factors into a product of degree 1 polynomials.

Definition 2.4.2: Algebraically Closed

A field K is **algebraically closed** if every polynomial with coefficients in K has a root in K.

Proposition 2.4.1

If $\overline{F}$ is the algebraic closure of F, then $\overline{F}$ is algebraically closed.

Exercise 2.4.1

For a field K, the following are equivalent:

- K is algebraically closed
- Every $f(x) \in K[x]$ nonconstant splits completely over K
- Every irreducible $f(x) \in K[x]$ has degree 1
- There does not exist an algebraic extension of K other than K itself

Proposition 2.4.2

For every field F there exists an algebraically closed field K containing F.

Exercise 2.4.2

Let K be a finite extension of F. Prove that K is a splitting field over F if and only if every irreducible polynomial in $F[x]$ that has a root in K splits completely in $K[x]$.

2.5 Separability

Definition 2.5.1: Multiplicity

Take $f(x) \in F[x]$. Then over a splitting field over F, we get $f(x) = (x-\alpha_1)^{n_1}(x-\alpha_2)^{n_2}\dots(x-\alpha_k)^{n_k}$ where $\alpha_1, \dots, \alpha_k$ are distinct elements of the splitting field and $n_1 \geq 1$ for all i. The value n_i is called the **multiplicity** of α_i, and if $n_i > 1$, α_i is a **multiple root** of $f(x)$. If $n_i = 1$ instead, then we say that α_i is a **simple root**.

Definition 2.5.2: Separable polynomials

A polynomial $f(x) \in F[x]$ is called **separable** if it has no multiple roots over a splitting field for F. Else, $f(x)$ is called **inseparable**.

Definition 2.5.3: Polynomial derivative

If $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_2x^2 + a_1x + a_0 \in F[x]$, then its **derivative** is

$$D_x f(x) = na_n x^{n-1} + \ldots + 2a_2 x + a_1 \in F[x]$$

Proposition 2.5.1

Take $f(x) \in F[x]$ with root α. Then the multiplicity of α is greater than one if and only if $D_x f(\alpha) = 0$.

In other words, $f(x)$ is separable when $f(x)$ and $D_x f(x)$ share no roots.

Corollary 2.5.1

(a). Every irreducible polynomial over a field F of characteristic zero is separable

(b). A polynomial over a field of characteristic zero is separable if and only if it is the product of distinct irreducible factors

Now we discuss how separability relates to field extensions.

Definition 2.5.4: Separable

Let K/F be a field extension. An element $\alpha \in K$ is **separable over** F if α is algebraic over F and $m_{\alpha,F}(x)$ is separable.

The extension K/F is **separable** if every element of K is separable over F. If there is an $\alpha \in K$ that is not separable over F, then K/F is an **inseparable** extension.

Proposition 2.5.2

Every finitely generated algebraic extension of $\mathbb{Q}$ is separable.

2.6 Techniques in Characteristic p > 0

Proposition 2.6.1

Let F be a field of characteristic $p > 0$. Then for all $a, b \in F$, we get that

$$(a+b)^p = a^p + b^p$$
$$(ab)^p = a^p b^p$$

This is the "Freshman's Dream".

Definition 2.6.1: Frobenius Endomorphism

For a field F of characteristic $p > 0$, the function

$$\varphi : F \to F$$
$$a \mapsto a^p$$

is the **Frobenius endomorphism** of F.

Corollary 2.6.1

The Frobenius endomorphism of F is an injective field homomorphism. When F is finite, it is also surjective.

Now we will go back to some propositions about finite fields using these ideas.

Proposition 2.6.2

Every irreducible polynomial over a finite field F is separable. Moreover, $f(x) \in F[x]$ is separable if and only if it is the product of distinct irreducible polynomials in $F[x]$.

This follows by contradiction. One can express the irreducible polynomial as a polynomial of the form $g(x^p)$, but this polynomial can be shown to be reducible, and so cannot occur.

Definition 2.6.2: Perfect

A field K of characteristic $p > 0$ is called **perfect** if every element of K is a p-th power in $K-$ that is, $K = K^p$.

By convention any field of characteristic zero is also called perfect.

We have just shown that every irreducible polynomial over a perfect field is separable, and hence finite extensions of perfect fields are separable.

Exercise 2.6.1

Prove that there exists a non-perfect infinite field F, i.e. find $f(x) \in F[x]$ so that f is irreducible and not separable.

These concepts can be used to prove that the n-th cyclotomic polynomial $\Phi_n(x) \in \mathbb{Z}[x]$ is irreducible.

Theorem 2.6.1

Let $K/\mathbb{F}_p$ be a field extension of the prime subfield $\mathbb{F}_p$.

- If K is finite, then $|K| = p^n$ for some positive integer n.
- $|K| = p^n$ if and only if K is the splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$.

By the uniqueness of splitting fields, we can simply denote K by $\mathbb{F}_{p^n}$.

This theorem gives us a complete characterization of finite fields. The first part is proven in Dummitt-Foote 13.2 #1.

Corollary 2.6.2

For all prime p, for all $n \in \mathbb{Z}_+$, there exists a field of cardinality p^n. Furthermore, any two finite fields of the same cardinality are isomorphic.

2.7 Simple Extensions

Theorem 2.7.1

If $|F| < \infty$, and K/F is a finite extension of F, then $K = F(\alpha)$ for some $\alpha \in K$.

This holds because $K^\times$ is a cyclic group, and so there must exist α so $\langle\alpha\rangle = K^\times$, and hence $K = F(\alpha)$.

Theorem 2.7.2

If F is an infinite field, and K/F is a finite separable extension, then $K = F(\alpha)$ for some $\alpha \in K$.

Every field extension can be written by appending a sequence of elements, and we can reduce the elements to one by the combination $\alpha = \beta + \gamma\delta$, where (β, γ) is the two additional elements, and $\delta \neq \frac{\beta_i - \beta}{\gamma - \gamma_j}$. Often we can simply choose $\delta = 1$ if we are lucky.

Chapter 3

Galois Theory

Galois theory studies the connection between finite field extensions via roots of polynomials and the structures of groups that permute those roots.

Let F, K be fields, and K/F a field extension.

Definition 3.0.1: Field Automorphism

We say that $\sigma : K \to K$ is a **field automorphism** if σ is a bijective unital ring homomorphism. We denote the collection of field automorphisms of K by $\mathrm{Aut}(K)$.

An automorphism $\sigma \in \mathrm{Aut}(K)$ **fixes an element** $\alpha \in K$ if $\sigma(\alpha) = \alpha$.

An automorphism $\sigma \in \mathrm{Aut}(K)$ **fixes a subset** E **of** K if $\sigma(\alpha) = \alpha$ for all $\alpha \in E$.

For $\sigma \in \mathrm{Aut}(K)$ and $E \subset K$, $\sigma(E)$ denotes the subset $\{\sigma(\alpha) \mid \alpha \in E\}$

Recall that the prime subfield of a field K is given by

$$K_{\text{prime}} = \begin{cases} \mathbb{Q} & K \text{ has characteristic } 0 \\ \mathbb{Z}_p & p \text{ prime} \end{cases}$$

because $\sigma \in \mathrm{Aut}(K)$ fixes 1_K, it must hold that σ fixes K_{prime} and hence prime subfields are fixed by any automorphism of a field.

3.1 Automorphisms fixing subfields

Definition 3.1.1

We define $\mathrm{Aut}(K/F)$ to be the collection of automorphisms of K that fix F.

Proposition 3.1.1

$\mathrm{Aut}(K)$ is a group under composition, and $\mathrm{Aut}(K/F)$ is a subgroup of $\mathrm{Aut}(K)$.

Proposition 3.1.2

Let $\alpha \in K$ be an algebraic element over F. Then for any $\alpha \in \mathrm{Aut}(K/F)$, we get that $m_{\alpha,F}(\sigma(\alpha)) = 0$.

In other words, automorphisms permute roots of minimal polynomials.

3.2 Subfields and Subgroups

Proposition 3.2.1

Let H be a subgroup of $\mathrm{Aut}(K)$. Then

$$\{\alpha \in K \mid \sigma(\alpha) = \alpha \quad \forall \sigma \in H\}$$

is a subfield of K. We call this subfield the **fixed field of** H denoted by K^H.

In fact, this structure induces a correspondence between field extensions and chains of subgroups.

Proposition 3.2.2

Let $F_1 \subset F_2 \subset K$ be a sequence of field extensions. Then $\mathrm{Aut}(K/K) = \mathrm{Id}_{\mathrm{Aut}(K)} \leq \mathrm{Aut}(K/F_2) \leq \mathrm{Aut}(K/F_1)$.

Conversely, let $H_1 \leq H_2 \leq \mathrm{Aut}(K)$ be a chain of subgroups. Then $K^{\mathrm{Aut}(K)} = K_{\mathrm{prime}} \subset K^{H_2} \subset K^{H_1}$

Proposition 3.2.3

Let E be the splitting field over F of a polynomial $f(x) \in F[x]$. Then

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

with equality if and only if $f(x)$ is separable over F.

The techniques used to prove this proposition also tell us that if K/F is finite, then $|\mathrm{Aut}(K/F)| \leq [K : F]$.

Definition 3.2.1

Let K/F be a finite extension.

- If $|\mathrm{Aut}(K/F)| = [K : F]$ then K is **Galois over** F and K/F is a **Galois extension**.
- If K/F is Galois, then the group $\mathrm{Aut}(K/F)$ is called the **Galois group** of K/F and is denoted $\mathrm{Gal}(K/F)$.

Example 3.2.1

Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Then one can see that $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, and $\mathbb{Q}(\sqrt{6})$ are all subfields for which K is a Galois extension. Furthermore, these fields are all Galois extensions of $\mathbb{Q}$.

Example 3.2.2

Consider the quotient field $\mathbb{F}_2(t)$ of $\mathbb{F}_2[t]$ and consider $f(x) = x^2 - t \in \mathbb{F}_2(t)[x]$. One can show that $f(x)$ is irreducible but not separable over $\mathbb{F}_2(t)$, and hence if θ is a root of $f(x)$, $\mathbb{F}_2(t)(\theta)$ is NOT a Galois extension of $\mathbb{F}_2(t)$.

Example 3.2.3

Let K be the splitting field of $x^3 - 2$, i.e. $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$. K is Galois over $\mathbb{Q}$, but $\mathbb{Q}(\sqrt[3]{2})$ is NOT Galois over $\mathbb{Q}$.

In fact, $\mathrm{Gal}(K/\mathbb{Q})$ is a nonabelian group of order 6, and thus is isomorphic to S_3.

We can summarize our characterization thus far by a set of equivalences. The following are equivalent:

- A finite field extension K/F is Galois
- $|\mathrm{Aut}(K/F)| = [K : F]$
- K/F is the splitting field of a separable polynomial over F
- K/F is normal and separable
- $F = K^{\mathrm{Aut}(K/F)}$

3.3 Fundamental Theorem of Galois Theory

Theorem 3.3.1: Fundamental Theorem of Galois Theory

Let K/F be Galois and set $G := \mathrm{Gal}(K/F)$. Then there exists a bijection between the subfields $E \subset K$ with $F \subset E$ and the subgroups $H \leq G$ given by

$$E \mapsto \mathrm{Aut}(K/E)$$
$$H \mapsto K^H$$

and these maps are inverses of each other. Furthermore, this bijection has some additonal properties:

- If $E_1 \leftrightarrow H_1$ and $E_2 \leftrightarrow H_2$, then $E_1 \subset E_2 \iff H_2 \leq H_1$.
- If $E \leftrightarrow H$, then $[K : E] = |H|$ and $[E : F] = [G : H]$.
- K/E is always Galois for $F \subset E \subset K$.
- E/F is Galois if and only if $H \triangleleft G$. In this case, $\mathrm{Gal}(E/F) \cong G/H$.
- If $E_1 \leftrightarrow H_1$ and $E_2 \leftrightarrow H_2$, then $E_1 \cap E_2 \leftrightarrow \langle H_1, H_2 \rangle$ and $E_1 E_2 \leftrightarrow H_1 \cap H_2$.

Remember that $H \triangleleft G$ is equivalent to $\mathrm{Aut}(K/E) \triangleleft \mathrm{Aut}(K/F)$. Also recaall that $\langle H_1, H_2 \rangle$ is the smallest subgroup of G that contains H_1, H_2, and $E_1 E_2$ is the smallest subfield of K containing E_1, E_2. They are not necessarily equivalent!

Now we apply this theorem to finite fields. Consider $\mathbb{F}_{p^n}$, the splitting field of $x^{p^n} - x$. This is Galois over $\mathbb{F}_p$. Thus we have $|\mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p)| = [\mathbb{F}_{p^n} : \mathbb{F}_p] = n$. This gives us $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \mathbb{Z}/n\mathbb{Z}$ and the Galois group consists solely of the Frobenius endomorphism.

One can see then that all subfields $\mathbb{F}_p \subset E \subset \mathbb{F}_{p^n}$ have the form $E \cong \mathbb{F}_{p^d}$ for some $d \mid n$. Of course, this means that E/F is necessarily Galois as well!

3.4 Applications of Galois Theory

Proposition 3.4.1

The irreducible polynomial $x^4 + 1 \in \mathbb{Z}[x]$ is reducible over $\mathbb{F}_p$ for any prime p.

Proof. One can check this directly for $p = 2$. If $p > 2$, then observe that $p \cong 1, 3, 5$ or $7 \mod 8$, and hence $p^2 \cong 1 \mod 8$. Therefore we have that $x^8 - 1 \mid x^{p^2-1} - 1$ over $\mathbb{F}_p$.

Of course, $x^4 + 1 \mid x^8 - 1$ and so any root of $x^4 + 1$ is a root of $x^{p^2} - x$ and hence are elements of the field $\mathbb{F}_{p^2}$. Since $[\mathbb{F}_{p^2} : \mathbb{F}_p] = 2$, the degree of the extension is no more than 2. Of course, if $x^4 + 1$ were irreducible over $\mathbb{F}_p$, then it would necessarily be 4, and hence it must be reducible. ■

Proposition 3.4.2

$$x^{p^n} - x = \prod_{d|n} \{\text{irreducible polynomial in } \mathbb{F}_p[x] \text{ of degree } d\}$$

We can use this recursively as n increases.

Now we discuss composite field extensions.

Proposition 3.4.3

If K/F is Galois, and F'/F is any field extension, then KF'/F' is Galois and $\mathrm{Gal}(KF'/F') \cong \mathrm{Gal}(K/K \cap F')$.

Example 3.4.1

Consider $K = \mathbb{Q}(\omega)$, $F' = \mathbb{Q}(\sqrt[3]{2})$, $F = \mathbb{Q}$. Then $KF' = \mathbb{Q}(\omega, \sqrt[3]{2})$ and by this theorem is Galois over $\mathbb{Q}(\sqrt[3]{2})$. Furthermore, the Galois group is isomorphic to $\mathbb{Q}(\omega) \cap \mathbb{Q}(\sqrt[3]{2})$.

Notice that $\mathbb{Q}(\sqrt[3]{2})$ is not Galois over $\mathbb{Q}$!

Corollary 3.4.1

If K/F is Galois and F'/F is any field extension, then

$$[KF' : F] = [KF' : F'][F' : F] \equiv [K : K \cap F'][F' : F] = \frac{[K : F][F' : F]}{[K \cap F' : F]}.$$

Proposition 3.4.4

If K_1/F and K_2/F are Galois, then K_1K_2/F and $K_1 \cap K_2/F$ are Galois. Furthermore,

$$\mathrm{Gal}(K_1K_2/F) \cong \{(\sigma, \tau) \mid \sigma|_{K_1 \cap K_2} = \tau|_{K_1 \cap K_2}\} \leq \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F).$$

Equality holds if and only if $K_1 \cap K_2 = F$.

Corollary 3.4.2

Let E/F be a finite separable extension. Then there exists K/F Galois extension with $F \subset E \subset K$, and the choice of K is minimal in the sense that, if $E \subset K'$ and $K' \subset \overline{K}$, then $K \subset K'$.

We call the Galois extension above the **Galois closure** of E/F.

3.5 Solvable Groups

Definition 3.5.1: Radical Extension

A field K is said to be a **radical extension** of a field F if there is a chain of fields

$$F = F_0 \subset F_1 \subset F_2 \subset \ldots \subset F_n = K$$

such that, for each $i = 1, \ldots, n$, $F_i = F_{i-1}(\alpha_i)$ and some power of α_i is in F_{i-1}.

Let $f \in F[x]$. The equation $f(x) = 0_F$ is **solvable by radicals** if there exists a radical extension of F that contains a splitting field of $f(x)$. This is equivalent to the notion of there existing a "formula" for the solutions.

Definition 3.5.2: Solvable

A group G is said to be **solvable** if it has a chain of subgroups

$$\langle e \rangle = G_n \lhd \ldots \lhd G_1 \lhd G_0 = G$$

such that each quotient group G_{i-1}/G_i is abelian.

Notice that all abelian groups are solvable.

Proposition 3.5.1

For $n \geq 5$ the group S_n is not solvable.

Theorem 3.5.1

Every homomorphic image of a solvable group G is solvable.

Our goal is to prove the Galois Criterion. That is, let $f \in F[x]$. $f(x) = 0_F$ is solvable by radicals if and only if the Galois group of $f(x)$ is a solvable group.

Lemma 3.5.1

Let F be a field and η a primitive n-th root of unity in F. Then F contains a primitive d-th root of unity for every positive $d \mid n$.

This combined with the next two theorems will allow us to prove the Galois Criterion.

Theorem 3.5.2

Let F be a field of characteristic zero and η a primitive n-th root of unity in some field extension of F. Then $K = F(\eta)$ is a normal extension of F and $\mathrm{Gal}_F(K)$ is abelian.

Theorem 3.5.3

Let F be a field of characteristic zero that contains a primitive n-th root of unity. If α is a root of $x^n - c \in F[x]$ in some extension field of F, then $K = F(\alpha)$ is a normal extension of F and $\mathrm{Gal}_F(K)$ is abelian.

Lemma 3.5.2

Let F, E, K be fields of characteristic zero with

$$F \subset E \subset K = E(\alpha) \quad \alpha^k \in E$$

If K is finite-dimensional over F and E is normal over F, then there exists a field extension L of K which is a radical extension of E and a normal extension of F.

Theorem 3.5.4: Galois Criterion

Let $f \in F[x]$. $f(x) = 0_F$ is solvable by radicals if and only if the Galois group of $f(x)$ is a solvable group.

We can use this to show that there is no formula for the solutions of all fifth-degree polynomials, as there are fifth-degree polynomials whose Galois group is S_5.

Theorem 3.5.5

Let F be a field of characteristic zero and $f(x) \in F[x]$. If $f(x) = 0_F$ is solvable by radicals, then there is a normal radical field extension of F that contains the splitting field of $f(x)$.

Theorem 3.5.6

Let K be a normal radical field extension of F and E an intermediate field, all of characteristic zero. If E is normal over F, then $\mathrm{Gal}_F(E)$ is a solvable group.