Field and Galois Theory

Swayam Chube

March 13, 2023

Abstract

This is meant to be a rapid introduction to Galois Theory. We shall not provide intuition or comment far too much on any specific result.

Contents

Chapter 1

Algebraic Extensions

Definition 1.1 (Extension, Degree). Let F be a field. If F is a subfield of another field E, then E is said to be an *extension* field of F. The dimension of E when viewed as a vector space over F is said to be the *degree of the extension* E/F and is denoted by $[E : F]$.

Definition 1.2 (Algebraic Element).

Definition 1.3 (Distinguished Class). Let $\mathscr{C}$ be a class of extension fields $F \subseteq E$. We say that $\mathscr{C}$ is distinguished if it satisfies the following conditions:

1. Let $k \subseteq F \subseteq E$ be a tower of fields. The extension $K \subseteq E$ is in $\mathscr{C}$ if and only if $k \subseteq F$ is in $\mathscr{C}$ and $F \subseteq E$ is in $\mathscr{C}$.
2. If $k \subseteq E$ is in $\mathscr{C}$, if F is any extension of k, and E, F are both contained in some field, then $F \subseteq EF$ is in $\mathscr{C}$.
3. If $k \subseteq F$ and $k \subseteq E$ are in $\mathscr{C}$ and F, E are subfields of a common field, then $k \subseteq FE$ is in $\mathscr{C}$.

Lemma 1.4. *Let E/k be algebraic and let $\sigma : E \to E$ be an embedding of E over k. Then σ is an automorphism.*

Proof. Since σ is known to be injective, it suffices to show that it is surjective. Pick some $\alpha \in E$ and let $p(x) \in k[x]$ be its minimal polynomial over k. Let K be the subfield of E generated by all the roots of p in E. Obviously, $[K : k]$ is finite. Since p remains unchanged under σ, it is not hard to see that σ maps a root of p in E to another root of p in E. Therefore, $\sigma(K) \subseteq K$. But since $[\sigma(K) : k] = [K : k]$ due to obvious reasons, we musth ave that $\sigma(K) = K$, consequently, $\alpha \in K = \sigma(K)$. This shows surjectivity. ■

Chapter 2

Algebraic Closure

Theorem 2.1. *Let k be a field. Then there is an algebraicaly closed field containing k.*

Proof due to Artin. ■

Corollary. Let k be a field. Then there exists an extension k which is algebraic over k and algebraically closed.

Proof. ■

Lemma 2.2. *Let k be a field and L and algebraically closed field with $\sigma : k \to L$ an embedding. Let α be algebraic over k in some extension of k. Then, the number of extensions of σ to an embedding $k(\alpha) \to L$ is precisely equal to the number of distinct roots of the minimal polynomial of α over k.*

Lemma 2.3. *Suppose E and L are algebraically closed fields with $E \subseteq L$. If L/E is algebraic, then $E = L$.*

Proof. Let $\alpha \in L$. Let $p(x) \in E[x]$ be the minimal polynomial of α over E. Since E is algebraically closed, p splits into linear factors over E, one of them being $(x - \alpha)$, implying that $\alpha \in E$. This completes the proof. ■

Theorem 2.4 (Extension Theorem). *Let E/k be algebraic, L an algebraically closed field and $\sigma : k \to L$ be an embedding of k. Then there exists an extension of σ to an embedding of E in L. If E is algebraically closed and L is algebraic over σk, then any such extension of σ is an isomorphism of E onto L.*

Proof. Let $\mathscr{S}$ be the set of all pairs (F, τ) where $F \subseteq E$ and F/k is algebraic and $\tau : F \to L$ is an extension of σ. Define a partial order $\leqq$ on $\mathscr{S}$ by $(F_1, \tau_1) \leqq (F_2, \tau_2)$ if and only if $F_1 \subseteq F_2$ and $\tau_2 |_{F_1} \equiv \tau_1$. Note that $\mathscr{S}$ is nonempty since it contains (k, σ). Let $\mathscr{C} = \{(F_\alpha, \tau_\alpha)\}$ be a chain in $\mathscr{S}$.

Define $F = \bigcup_\alpha F_\alpha$. Now, for any $t \in F$, there is β such that $t \in F_\beta$; using this, define $\tau(t) = \tau_\beta(t)$. It is not hard to see that this is a valid embedding.

Now, invoking Zorn's Lemma, there is a maximal element, say (K, τ). We claim that $K = E$, for if not, then we may choose some $\alpha \in E$ and invoke Lemma 2.2.

Finally, if E is algebraically closed, so is σE, consequently, we are done due to the preceeding lemma. ■

Corollary. Let k be a field and E, E' be algebraic extensions of k. Assume that E, E' are algebraically closed. Then there exists an isomorphism $\tau : E \to E'$ inducing the identity on k.

Proof. Consider the extension of $\sigma : k \to E'$ where $\sigma\ |_k = \mathbf{id}_k$ whence the conclusion immediately follows. ■

Since an algebraically closed and algebraic extension of k is determined upto an isomorphism, we call such an extension an *algebraic closure* of k and is denoted by k^a.

Chapter 3

Normal Extensions

Definition 3.1 (Splitting Field). Let k be a field and $\{f_i\}_{i\in I}$ be a family of polynomials in $k[x]$. By a *splitting field* for this family, we shall mean an extension K of k such that every f_i splits in linear factors in $K[x]$ and K is generated by all the roots of all the polynomials f_i for $i \in I$ in some algebraic closure $\overline{k}$.

In particular, if $f \in k[x]$ is a polynomial, then the splitting field of f over k is an extension K/k such that f splits into linear factors in K and K is generated by all the roots of f.

Definition 3.2 (Normal Extension). An algebraic extension K/k is said to be *normal* if whenever an irreducible polynomial $f(x) \in k[x]$ has a root in K, it splits into linear factors over K.

Theorem 3.3 (Uniqueness of Splitting Fields). *Let K be a splitting field of the polynomial $f(x) \in k[x]$. If E is another splitting field of f, then there exists an isomorphism $\sigma : E \to K$ inducing the identity on k. If $k \subseteq K \subseteq \overline{k}$, where $\overline{k}$ is an algebraic closure of k, then any embedding of E in $\overline{k}$ inducing the identity on k must be an isomorphism of E on K.*

Proof. We prove both assertions together. Due to Theorem 2.4, there is an embedding $\sigma : E \to \overline{k}$ such that $\sigma\,|_k = \mathbf{id}_k$. Therefore, it suffices to prove the second half of the theorem.

We have two factorizations

$$\begin{aligned} f(x) &= c(x-\alpha_1)\cdots(x-\alpha_n) \qquad \text{over } E \\ &= c(x-\beta_1)\cdots(x-\beta_n) \qquad \text{over } K \end{aligned}$$

Since σ induces the identity map on k, f must remain invariant under σ. Further, we have

$$\sigma f(x) = c(x-\sigma\beta_1)\cdots(x-\sigma\beta_n)$$

Due to unique factorization, we must have that $(\sigma\beta_1,\ldots,\sigma\beta_n)$ differs from $(\alpha_1,\ldots,\alpha_n)$ by a permutation. Since $\sigma E = k(\sigma\beta_1,\ldots,\sigma\beta_n)$, we immediately have the desired conclusion. ■

Theorem 3.4. *Let K/k be algebraic in some algebraic closure $\overline{k}$ of k. Then, the following are equivalent:*

1. *Every embedding σ of K in $\overline{k}$ over k is an automorphism of K*
2. *K is the splitting field of a family of polynomials in $k[x]$*
3. *K/k is normal*

Proof.
$\underline{(1) \implies (2) \wedge (3)}$: For each $\alpha \in K$, let $m_\alpha(x)$ denote the minimal polynomial for α over k. We shall show that K is the splitting field for $\{m_\alpha\}_{\alpha \in K}$. Obviously, K is generated by $\{\alpha\}_{\alpha \in K}$, hence, it suffices to show that m_α splits into linear factors over K. Let β be a root of m_α in $\overline{k}$. Then, there is an isomorphism $\sigma : k(\alpha) \to k(\beta)$. One may extend this to an embedding $\sigma : K \to \overline{k}$, which by our hypothesis, is an automorphism of K, implying that $\beta \in K$ and giving us the desired conclusion.
$\underline{(2) \implies (1)}$: Let K be the splitting field for the family of polynomials $\{f_i\}_{i \in I}$. Let $\alpha \in K$ and α be the root of some polynomial f_i and $\sigma : K \to \overline{k}$ be an embedding of fields. Since f_i remains invariant under σ, it must map a root of f_i to another toot of f_i, that is, $\sigma\alpha$ is a root of f_i. Consequently, σ maps K into K. Now, due to Lemma 1.4, σ is an automorphism and K/k is normal.
$\underline{(3) \implies (1)}$: Let $\sigma : K \to \overline{k}$ be an embedding of fields. Let $\alpha \in K$ and $p(x) \in k[x]$ be its irreducible polynomial over k. Since p remains invariant under σ, it must map α to a root β of p in $\overline{k}$. But since p splits into linear factors over K, $\beta \in K$ and thus $\sigma(K) \subseteq K$, consequently, $\sigma(K) = K$ due to Lemma 1.4, therefore completing the proof. ■

Corollary. The splitting field of a polynomial is a normal extension.

Theorem 3.5. *Normal extensions remain normal under lifting. If $k \subseteq E \subseteq K$, and K is normal over k, then K is normal over E. If K_1, K_2 are normal over k and are contained in some field L, then K_1K_2 is normal over k and so is $K_1 \cap K_2$.*

Proof. Let K/k be normal and F/k be any extension with K and F contained in some larger extension. Let σ be an embedding of KF over F in $\overline{F}$. The restriction of σ to K is an embedding of K over k and therefore, is an automorphism of K. As a result, $\sigma(KF) = (\sigma K)(\sigma F) = KF$ and thus KF/F is normal.

Now, suppose $k \subseteq E \subseteq K$ with K/k normal. Let σ be an embedding of K in $\overline{k}$ over E. Then, σ induces the identity on k and is therefore an automorphism of K. This shows that K/E is normal.

Next, if K_1 and K_2 are normal over k and σ is an embedding of K_1K_2 over k, then its restriction to K_1 and K_2 respectively are also embeddings over k and consequently are automorphisms. This gives us

$$\sigma(K_1K_2) = (\sigma K_1)(\sigma K_2) = K_1K_2$$

Finally, since any embedding of $K_1 \cap K_2$ can be extended to that of K_1K_2, we have, due to a similar argument, that $K_1 \cap K_2$ is normal over k. ■

Chapter 4

Separable Extensions

Let E/k be a finite extension, and therefore, algebraic. Let L be an algebraically closed field along with an embedding $\sigma : k \to L$. Define S_σ to be the set of extensions of σ to $\sigma^* : E \to L$.

Definition 4.1 (Separable Degree). Given the above setup, the *separable degree* of the finite extension E/k, denoted by $[E : k]_s$ is defined to be the cardinality of S_σ.

Proposition 4.2. *The separable degree is well defined. That is, if L' is an algebraically closed field and $\tau : k \to L'$ be an embedding, then the cardinality of S_τ is equal to that of S_σ*

Definition 4.3 (Separable Extension). Let E/k be a finite extension. Then it is said to be *separable* if $[E : k]_s = [E : k]$. Similarly, let $\alpha \in \bar{k}$. Then α is said to be separable over k if $k(\alpha)/k$ is separable.

Proposition 4.4. *Let E/F and F/k be finite extensions. Then*

$$[E : k]_s = [E : F]_s[F : k]_s$$

Proof. Let L be an algebraically closed field and $\sigma : k \to L$ be an embedding. Let $\{\sigma_i\}_{i\in I}$ be the extensions of σ to an embedding $F \to L$ and $\{\tau_{ij}\}$ be the extensions of σ to an embedding $E \to L$. We have indexed τ in such a way that the restriction $\tau_i \mid_E = \sigma_i$. Using the definition of the separable degree, we have that for each i there are precisely $[E : F]_s$ j's such that τ_{ij} is a valid extension. This immediately implies the desired conclusion. ∎

Corollary. Let E/k be finite. Then, $[E : k]_s \leq [E : k]$.

Proof. Due to finitness, we have a tower of extensions

$$k \subsetneq k(\alpha_1) \subsetneq \cdots \subsetneq k(\alpha_1, \ldots, \alpha_n)$$

We may now finish using Lemma 2.2. ∎

Theorem 4.5. *Let E/k be finite and* $\operatorname{char} k = 0$. *Then E/k is separable.*

Proof. Since E/k is finite, there is a tower of extensions as follows:

$$k \subsetneq k(\alpha_1) \subsetneq \cdots \subsetneq k(\alpha_1, \ldots, \alpha_n)$$

We shall show that the extension $k(\alpha)/k$ is separable for some $\alpha \in \bar{k}$. Let $p(x) = m_\alpha(x)$ be the minimal polynomial over $k[x]$. We contend that $p(x)$ does not have any multiple roots. Suppose not, then $p(x)$ and $p'(x)$ share a root, say β. But since $p(x)$ is the minimal polynomial for β over k, it must divide $p'(x)$ which is impossible over a field of characteristic 0. Finally, due to Lemma 2.2, we must have $k(\alpha)/k$ is separable.

This immediately implies the desired conclusion, since

$$[E : k]_s = [k(\alpha_1, \ldots, \alpha_n) : k(\alpha_1, \ldots, \alpha_{n-1}] \cdots [k(\alpha_1) : k] = [E : k]$$

■

Theorem 4.6. *Let E/k be finite and* $\operatorname{char} k = p > 0$. *Then, there is $m \in \mathbb{N}_0$ such that*

$$[E : k] = p^m [E : k]_s$$

Proof. ■

Corollary. Let E/k be a finite extension. Then, $[E : k]_s$ divides $[E : k]$.

Proof. Follows from Theorem 4.5 and Theorem 4.6. ■

Definition 4.7 (Inseparable Degree). Let E/k be finite. Then, we denote

$$[E : k]_i = \frac{[E : k]}{[E : k]_s}$$

as the *inseparable degree*.

Lemma 4.8. *Let K/k be algebraic and $\alpha \in K$ is separable over k. Let $k \subseteq F \subseteq K$. Then, α is separable over F.*

Proof. Let $p(x) \in k[x]$ and $f(x) \in F[x]$ be the minimal polynomial of α over k and F respectively. By definition, $f(x) \mid p(x)$ and therefore has distinct roots in the algebraic closure of k. Consequently, α is separable over F. ■

Proposition 4.9. *Let E/k be finite. Then, it is separable if and only if each element of E is separable over k.*

Proof. Suppose E/k is separable and $\alpha \in E \backslash k$. Then, there is a tower of extensions

$$k \subsetneq k(\alpha_1) \subsetneq \cdots \subsetneq k(\alpha_1, \ldots, \alpha_n) = E$$

with $\alpha_1 = \alpha$. Recall that $[E : k]_s \leq [E : k]$ with equality if and only if there is an equality at each step in the tower. This implies the desired conclusion.

Conversely, suppose each element of E is separable over k. Then, each α_i is separable over $k(\alpha_1, \ldots, \alpha_{i-1})$ due to Lemma 4.8. Consequently, for each step in the tower,

$$[k(\alpha_1, \ldots, \alpha_i) : k(\alpha_1, \ldots, \alpha_{i-1})]_s = [k(\alpha_1, \ldots, \alpha_i) : k(\alpha_1, \ldots, \alpha_{i-1})]$$

implying the desired conclusion. ■

Definition 4.10 (Infinite Separable Extensions). An algebraic extension E/k is said to be *separable* if each finitely generated sub-extension is separable.

Theorem 4.11. *Let E/k be algebraic and generated by a family $\{\alpha_i\}_{i \in I}$. If each α_i is separable over k, then E is separable over k.*

Proof. Let $k(\alpha_1, \ldots, \alpha_n)/k$ be a finitely generated sub-extension of E/k. From our proof of Proposition 4.9, we know that α_i is separable over $k(\alpha_1, \ldots, \alpha_{i-1})$, and therefore, $k(\alpha_1, \ldots, \alpha_n)$ is separable over k and we have the desired conclusion. ■

Theorem 4.12. *Let E/k be algebraic. Then, E/k is separable if and only if each element of E is separable over k.*

Proof. Suppose E/k is separable, then for each $\alpha \in E$, $k(\alpha)$ is a finitely generated sub-extension of E, which is separable by definition. This implies that α is separable over k, again by definition.

Conversely, suppose each element is separable over k. Let $k(\alpha_1, \ldots, \alpha_n)$ be a finitely generated sub-extension of E. Then, we have the following tower

$$k \subsetneq k(\alpha_1) \subsetneq \cdots \subsetneq k(\alpha_1, \ldots, \alpha_n)$$

From our proof of Proposition 4.9, we know that α_i is separable over $k(\alpha_1, \ldots, \alpha_{i-1})$, this immediately implies that $k(\alpha_1, \ldots, \alpha_n)/k$ is separable. ■

Theorem 4.13. *Separable extensions (not necessarily finite) form a distinguished class of extensions.*

Proof. Suppose E/k is separable and F is an intermediate field. Since each element of F is an element of E, we have that F must be separable over K, due to Theorem 4.12. Conversely, suppose both E/F and F/k are separable. Now, if E/k is finite, so is F/k and we are done due to Proposition 4.4.

Now, suppose E/k is not finite. It suffices to show that for all $\alpha \in E$, α is separable over k. Let $p(x) = a_n x^n + \cdots + a_0$ be the unique monic irreducible polynomial of α over F. Then, $p(x)$ is also the monic irreducible polynomial of α over $k(a_0, \ldots, a_n)$. Since α is separable over F, $p(x)$ has no repeated roots and therefore α is also separable over $k(a_0, \ldots, a_n)$. We now have a finite tower

$$k \subsetneq k(a_0, \ldots, a_n) \subsetneq k(a_0, \ldots, a_n)(\alpha)$$

Furthermore, since each a_i is separable over k for $0 \leq i \leq n$, it must be the case that $k(a_0, \ldots, a_n)$ is separable over k and finally so must α.

Next, suppose E/k is separable and F/k is an extension, where both E and F are contained in some algebraically closed field L. Since every element of E is separable over k, it must be separable over F, through a similar argument involving the minimal polynomial as carried out above. Since EF is generated by all the elements of E, we may finish using Theorem 4.11. This completes the proof. ■

Definition 4.14 (Separable Closure). Let k be a field and $\bar{k}$ be an algebrai closure. We define the separable closure k^{sep} as

$$k^{\text{sep}} = \{a \in \bar{k} \mid a \text{ is separable over } k\}$$

If $\alpha, \beta \in k^{\text{sep}}$, then $\alpha, \beta \in k(\alpha, \beta)$, which by choice of α, β is separable over k. Therefore, $\alpha\beta, \alpha/\beta, \alpha + \beta, \alpha - \beta \in k(\alpha, \beta)$ are separable over k, and lie in k^{sep}, from which it follows that k^{sep} is a field extension of k.

Primitive Element Theorem

Definition 4.15 (Primitive Element). Let E/k be a finite extension. Then $\alpha \in E$ is said to be *primitive* if $E = k(\alpha)$. In this case, the extension E/k is said to be simple.

Theorem 4.16 (Steinitz, 1910). *Let E/k be a finite extension. Then, there exists a primitive element $\alpha \in E$ if and only if there exist only a finite number of fields F such that $k \subseteq F \subseteq E$. If E/k is separable, then there exists a primitive element.*

Proof. If k is finite, then so is E and it is known that the multiplicative group of finite fields are cyclic, therefore generated by a single element, immediately implying the desired conclusion. Henceforth, we shall suppose that k is infinite.

Suppose there are only a finite number of fields intermediate between k and E. Let $\alpha, \beta \in E$. We shall show that $k(\alpha, \beta)/k$ has a primitive element. Indeed, consider the intermediate fields $k(\alpha + c\beta)$ for $c \in k$, which are infinite in number. Therefore, there are distinct elements $c_1, c_2 \in k$

such that $k(\alpha + c_1\beta) = k(\alpha + c_2\beta)$. Consequently, $(c_1 - c_2)\beta \in k(\alpha + c_1\beta)$, therefore, $\beta \in k(\alpha + c_1\beta)$ and thus $\alpha \in k(\alpha + c_1\beta)$. This implies that $\alpha + c_1\beta$ is a primitive element for $k(\alpha, \beta)/k$. Now, since E/k is finite, it must be finitely generated. We may now use induction to finish.

Conversely, suppose E/k has a primitive element, say $\alpha \in E$. Let $f(x)$ be the monic irreducible polynomial for α over k. Now, for each intermediate field $k \subseteq F \subseteq E$, let g_F denote the monic irreducible polynomial for α over F. Using the unique factorization over $\overline{k}[x]$, $g_F \mid f$ for each intermediate field F, therefore, there may be only finitely many such g_F and thus, only finitely many intermediate fields F.

Finally, suppose E/k is separable and therefore, finitely generated. Hence, it suffices to prove the statement for $k(\alpha, \beta)/k$. Say $n = [k(\alpha, \beta) : k]$ and let $\sigma_1, \ldots, \sigma_n$ be distinct embeddings of $k(\alpha, \beta)$ into $\overline{k}$ over k

$$f(x) = \prod_{1 \leq i \neq j \leq n} \big(x(\sigma_i\beta - \sigma_j\beta) + (\sigma_i\alpha - \sigma_j\beta) \big)$$

Since f is not identically zero, there is $c \in k$ (due to the infiniteness of k), such that $f(c) \neq 0$ and thus, the elements $\sigma_i(\alpha + c\beta)$ are distinct for $1 \leq i \leq n$, and thus

$$n \leq [k(\alpha + c\beta) : k]_s \leq [k(\alpha + c\beta) : k] \leq [k(\alpha, \beta) : k] = n$$

Thus, $\alpha + c\beta$ is primitive for $k(\alpha, \beta)/k$ which completes the proof. ■

Note that there are finite extension with infinitely many subfields. For example, consider the extension $\mathbb{F}_p(x, y)/\mathbb{F}_p(x^p, y^p)$ which has degree p^2. Let $z \in k = \mathbb{F}_p(x^p, y^p)$ and $w = x + zy \in \mathbb{F}_p(x, y)$. We have $w^p = x^p + z^p y^p \in \mathbb{F}_p(x^p, y^p)$ and thus, $k(w)/k$ has degree p. Furthermore, for $z \neq z'$ and $w' = x + z'y$, it is not hard to see that $k(w, w')$ contains both x and y, and is equal to $\mathbb{F}_p(x, y)$, from which it follows that $w \neq w'$. Since we have infinitely many choices of z, there are infinitely many subfields of the extension $\mathbb{F}_p(x, y)/\mathbb{F}_p(x^p, y^p)$.

Lemma 4.17. *Let E/k be an algebraic separable extension. Further, suppose that there is an integer $n \geq 1$ such that for every element $\alpha \in E$, $[k(\alpha) : k] \leq n$. Then E/k is finite and $[E : k] \leq n$.*

Proof. Let $\alpha \in E$ such that $[k(\alpha) : k]$ is maximal. We claim that $E = k(\alpha)$, for if not, there would be $\beta \in E \backslash k(\alpha)$. Now, since $k(\alpha, \beta)$ is a separable extension and is finite, it must be primitve. Thus, there is $\gamma \in E$ such that $k(\alpha, \beta) = k(\gamma)$ and $[k(\gamma) : k] = [k(\alpha, \beta) : k] > [k(\alpha) : k]$, contradicting the assumed maximality. This completes the proof. ■

Chapter 5

Inseparable Extensions

Chapter 6

Finite Fields

It is well known that every finite field must have prime characteristic. In fact, any integral domain with nonzero characteristic must have prime characteristic.

Theorem 6.1. *Let F be a finite field with characteristic $p > 0$. Then there is a positive integer n such that F has cardinality p^n. Further, there is a unique field upto isomorphism of cardinality p^n.*

Proof. The prime subfield of F is the subfield generated by 1 and is isomorphic to $\mathbb{F}_p$. Then $[F : \mathbb{F}_p] = n$, whence the conclusion follows. Now, we show that there is a field with cardinality p^n. Consider the polynomial $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$. First, note that $Df(x) = -1$, and thus $f(x)$ has distinct roots in $\overline{\mathbb{F}}_p$. It is not hard to see that if α, β are roots of $f(x)$ in $\overline{F}_p$, then $\alpha - \beta$ and $\alpha\beta$ are roots of $f(x)$ in $\overline{\mathbb{F}}_p$. Therefore, the collection of roots of $f(x)$ in $\overline{F}_p$ form a field. The cardinality of this field is the number of distinct roots of $f(x)$ in $\overline{\mathbb{F}}_p$, which is precisely p^n.

As for uniqueness, note that if F is a field of cardinality p^n, then every element of F is a root of $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$ (this is because F contains a copy of $\mathbb{F}_p$ in it). Therefore, F is the splitting field for $f(x)$ over $\mathbb{F}_p[x]$ in some algebraic closure. But since all splitting fields are isomorphic, we have the desired conclusion. ■

Theorem 6.2 (Frobenius). *The group of automorphisms of $\mathbb{F}_q$ where $q = p^n$ is cyclic of degree n, generated by the Frobenius mapping, $\varphi : \mathbb{F}_q \to \mathbb{F}_q$ given by $\varphi(x) = x^p$.*

Proof. We first verify that φ is an automorphism. That φ is a ring homomorphism is easy to show, from which it would follow that φ is injective. Surjectivity follows from here since $\mathbb{F}_q$ is finite. Next, note that φ leaves $\mathbb{F}_p$ fixed, thus, $G = \mathrm{Aut}(\mathbb{F}_q) = \mathrm{Aut}(\mathbb{F}_q/\mathbb{F}_p)$. Furthermore, $|\mathrm{Aut}(\mathbb{F}_q/\mathbb{F}_p)| = [\mathbb{F}_q : \mathbb{F}_p]_s \le [\mathbb{F}_q : \mathbb{F}_p] = n$.

We now show that the order of φ in G is precisely n, for if d were the order of φ, then $\varphi^d(x) = x$ for all $x \in \mathbb{F}_q$ and thus, $x^{p^d} - x = 0$ for all $x \in \mathbb{F}_q$, from which it follows that $p^d \ge q$ and $d \ge n$ and the conclusion follows. ■

Theorem 6.3. *Let $m, n \in \mathbb{N}$. Then in an algebraic closure $\overline{\mathbb{F}_p}$ of $\mathbb{F}_p$, the subfield $\mathbb{F}_{p^n}$ is contained in*

$\mathbb{F}_{p^m}$ *if and only if* $n \mid m$.

Proof. If $\mathbb{F}_{p^n}$ is contained in $\mathbb{F}_{p^m}$, then $p^m = (p^n)^d$ where $d = [\mathbb{F}_{p^m} : \mathbb{F}_{p^n}]$. The converse follows from noting that $x^{p^n} - x \mid x^{p^m} - x$. ■

Theorem 6.4. *Let* $m, n \in \mathbb{N}$ *such that* $n \mid m$. *Then the extension* $\mathbb{F}_{p^m}/\mathbb{F}_{p^n}$ *is finite Galois.*

Proof. We have $[\mathbb{F}_{p^m} : \mathbb{F}_p] = m$ and $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$, consequently, $[\mathbb{F}_{p^m} : \mathbb{F}_{p^n}]_s = m/n = [\mathbb{F}_{p^m} : \mathbb{F}_{p^n}]$ and thus the extension is separable. To show that the extension $\mathbb{F}_{p^m}/\mathbb{F}_{p^n}$ is normal, it suffices to show that the extension $\mathbb{F}_{p^m}/\mathbb{F}_p$ is normal but this trivially follows from the fact that $\mathbb{F}_{p^m}$ is the splitting field of $x^{p^m} - x \in \mathbb{F}_p[x]$. This completes the proof. ■

Chapter 7

Galois Extensions

Definition 7.1 (Fixed Field). Let K be a field and G be a group of automorphisms of K. The *fixed field* of K under G, denoted by K^G is the set of all elements $x \in K$ such that $\sigma x = x$ for all $\sigma \in G$.

That the aforementioned set forms a field is trivial.

Definition 7.2 (Galois Extension, Group). An extension K/k is said to be *Galois* if it is normal and separable. The group of automorphisms of K over k is known as the *Galois Group* of K/k and is denoted by $\mathrm{Gal}(K/k)$.

Theorem 7.3. *Let K be a Galois extension of k and $G = \mathrm{Gal}(K/k)$. Then $k = K^G$. If F is an intermediate field, $k \subseteq F \subseteq K$, then K is Galois over F and the map*

$$F \mapsto \mathrm{Gal}(K/F)$$

from the intermediate fields to subgroups of G is injective. Finiteness is not required in this case.

Proof. Let $\alpha \in K^G$ and $\sigma : k(\alpha) \to \overline{K}$ be an embedding over k. Due to Theorem 2.4, σ may be extended to an embedding of K over k in $\overline{K}$. Since K/k is normal, this is an automorphism and therefore, an element of G. As a result, σ sends α to itself, therefore, any embedding of $k(\alpha)$ over k is the identity map, implying that $[k(\alpha) : k]_s = 1$, or equivalently, $k(\alpha) = k$ whence $\alpha \in k$.

Let F be an intermediate field. Due to Theorem 3.5 and Theorem 4.13, we have that K/F is normal and separable, therefore Galois.

Finally, if F and F' map to the same subgroup H of G, then due to the first part, of this theorem, we must have $F = K^H = F'$, establishing injectivity. ■

Lemma 7.4. *Let E/k be algebraic and separable, further suppose that there is an integer $n \geq 1$ such that every element $\alpha \in E$ is of degree at most n over k. Then $[E : k] \leq n$.*

Proof. Let $\alpha \in E$ such that $[k(\alpha) : k]$ is maximized. We shall show that $k(\alpha) = E$. Suppose not, then there is $\beta \in E \backslash k(\alpha)$ and thus, we have a tower $k \subseteq k(\alpha) \subsetneq k(\alpha, \beta)$. Due to Theorem 4.16, there is $\gamma \in E$ such that $k(\alpha, \beta) = k(\gamma)$. But then,

$$[k(\gamma) : k] = [k(\alpha, \beta) : k] > [k(\alpha) : k]$$

a contradiction to the maximality of α. Therefore, $E = k(\alpha)$ and we have the desired conclusion. ■

Theorem 7.5 (Artin). *Let K be a field and let G be a finite group of automorphisms of K, of order n. Let $k = K^G$. Then K is a finite Galois extension of k, and its Galois group is G. Further, $[K : k] = n$.*

Proof. Let $\alpha \in K$. We shall show that K is the splitting field of the family $\{m_\alpha(x)\}_{\alpha \in K}$ and that α is separable over k.

Let $\{\sigma_1\alpha, \dots, \sigma_m\alpha\}$ be a maximal set of images of α under the elements of G. Define the polynomial:

$$f(x) = \prod_{i=1}^{m}(x - \sigma_i\alpha)$$

For any $\tau \in G$, we note that $\{\tau\sigma_1\alpha, \dots, \tau\sigma_m\alpha\}$ must be a permutation of $\{\sigma_1\alpha, \dots, \sigma_m\alpha\}$, lest we contradict maximality. As a result, α is a root of f^τ for all $\tau \in G$ and therefore, the coefficients of f lie in $K^G = k$, i.e. $f(x) \in k[x]$.

Since the $\sigma_i\alpha$'s are distinct, the minimal polynomial of α over k must be separable, and thus K/k is separable. Next, we see that the minimal polynomial for α also splits in K and thus, K is the splitting field for the family $\{m_\alpha(x)\}_{\alpha \in K}$. Consequently, K/k is normal and hence, Galois.

Finally, since the minimal polynomial for α divides f, we must have $[k(\alpha) : k] \le \deg f \le n$ whence due to Lemma 7.4, $[K : k] \le n$. Now, recall that $n = |G| \le [K : k]_s \le [K : k]$ and we have the desired conclusion. ■

Corollary. Let K/k be a finite Galois extension and $G = \mathrm{Gal}(K/k)$. Then, every subgroup of G belongs to some subfield F such that $k \subseteq F \subseteq K$.

Lemma 7.6. *Let K/k be Galois and F an intermediate field, $k \subseteq F \subseteq K$, and let $\lambda : F \to \overline{k}$ be an embedding. Then,*

$$\mathrm{Gal}(K/\lambda F) = \lambda\,\mathrm{Gal}(K/F)\lambda^{-1}$$

Proof. The embedding λ can be extended to an embedding of K due to Theorem 2.4 and since K/k is normal, λ is an automorphism. As a result, $\lambda F \subseteq K$ and thus, $K/\lambda F$ is Galois. Let $\sigma \in \mathrm{Gal}(K/F)$. It is not hard to see that $\lambda\sigma\lambda^{-1} \in \mathrm{Gal}(K/\lambda F)$ and conversely, for $\tau \in \mathrm{Gal}(K/\lambda F)$, $\lambda^{-1}\tau\lambda \in \mathrm{Gal}(K/F)$. This implies the desired conclusion. ■

Theorem 7.7. *Let K/k be Galois with $G = \mathrm{Gal}(K/k)$. Let F be an intermediate field, $k \subseteq F \subseteq K$, and let $H = \mathrm{Gal}(K/F)$. Then F is normal over k if and only if H is normal in G. If F/k is normal, then the restriction map $\sigma \mapsto \sigma\,|_F$ is a homomorphism of G onto $\mathrm{Gal}(F/k)$ whose kernel is H. This* *gives us* $\mathrm{Gal}(F/k) \cong G/H$.

Proof. Suppose F/k is normal. To see that the map $\sigma \to \sigma\mid_F$ is surjective, simply recall Theorem 2.4. The kernel of said mapping is obviously H and we have that $H \trianglelefteq G$ and due to the First Isomorphism Theorem, $G/H \cong \mathrm{Gal}(F/k)$.

On the other hand, if F/k is not normal, then there is an embedding $\lambda : F \to \bar{k}$ such that $F \neq \lambda F$. Note that due to Theorem 2.4, $\lambda F \subseteq K$. Then, we have $\mathrm{Gal}(K/F) \neq \mathrm{Gal}(K/\lambda F) = \lambda\,\mathrm{Gal}(K/F)\lambda^{-1}$, and equivalently, $\mathrm{Gal}(K/F)$ is not normal in G. This completes the proof of the theorem. ■

Note that in the proof of the above theorem, while showing H is normal in G, we did not use that the Galois extension is finite. We can now put together all the above results into one all-powerful theorem.

Theorem 7.8 (Fundamental Theorem of Galois Theory). *Let K/k be a finite Galois extension with $G = \mathrm{Gal}(K/k)$. There is a bijection between the set of subfields E of K containing k and the set of subgroups H of G given by $E = K^H$. The field E is Galois over k if and only if H is normal in G, and if that is the case, then the restriction map $\sigma \mapsto \sigma\mid_E$ induces an isomorphism of G/H onto* $\mathrm{Gal}(E/k)$.

Definition 7.9. A Galois extension K/k is said to be *abelian (resp. cyclic)* if its Galois group is *abelian (resp. cyclic)*.

Theorem 7.10. *Let K/k be finite Galois and F/k an arbitrary extension. Suppose K, F are subfields of some larger field. Then KF is Galois over F, and K is Galois over $K \cap F$. Let $H = \mathrm{Gal}(KF/F)$ and $G = \mathrm{Gal}(K/k)$. For all $\sigma \in H$, the restriction of σ to K is in G and the restriction map $\sigma \mapsto \sigma\mid_K$ gives an isomorphism of H on* $\mathrm{Gal}(K/K \cap F)$.

Proof. That KF/F and $K/K \cap F$ are Galois follow from Theorem 3.5 and Theorem 4.13. Let $\chi : H \to G$ denote the restriction map. Note that $\ker\chi$ contains all $\sigma \in H$ such that σ fixes K. But since σ implicitly fixes F, it must also fix KF and is therefore the unique identity automorphism. As a result, $\ker\chi$ is trivial and χ is injective. Let $H' = \chi(H) \subseteq G$. We shall show that $K^{H'} = K \cap F$. Indeed, if $\alpha \in K^{H'}$, then α is also fixed by all elements of H, since χ is only the restriction map. As a result, $\alpha \in F$, consequently $\alpha \in K \cap F$. We are now done due to Theorem 7.8. ■

Chapter 8

Infinite Galois Theory

In the infinite case, a Galois extension is defined as usual, that is, an extension which is normal and separable. The Galois group is again defined to be the group of automorphisms that fix a base field. Since our definitions of normal and separable extensions do not assume finiteness, we are in the clear. As we have seen earlier, finite-degree Galois extensions have finite Galois groups. The following proposition establishes the converse.

Proposition 8.1. *If K/k is an infinite-degree Galois extension, then* $\operatorname{Gal}(K/k)$ *is an infinite group.*

Proof. We shall prove the contrapositive. If $\operatorname{Gal}(K/k)$ is a finite group with cardinality M, then for each $\alpha \in K$, $[k(\alpha) : k] \leq M$, and it follows from Lemma 7.4 that $[K : k] \leq M$. ∎

Definition 8.2. Let K/k be a Galois extension. For $\sigma \in \operatorname{Gal}(K/k)$, a *basic open set* around σ is a coset $\sigma \operatorname{Gal}(K/F)$ where F/k is a **finite** extension.

Proposition 8.3. *The collection of basic open sets as defined above form a basis for a topology on* $\operatorname{Gal}(K/k)$.

Proof. Since $\operatorname{Gal}(K/F)$ contains the identity element for each F/k finite, the union of all the basic open sets is equal to $\operatorname{Gal}(K/k)$. Consider two basic open sets $\sigma_1 \operatorname{Gal}(K/F_1)$ and $\sigma_2 \operatorname{Gal}(K/F_2)$ having a nonempty intersection. Let σ be an automorphism in that intersection. We shall show that $\sigma \operatorname{Gal}(K/F_1F_2)$ is contained in the intersection. Since $\sigma \in \sigma_1 \operatorname{Gal}(K/F_1)$, there is $\alpha \in \operatorname{Gal}(K/F_1)$ such that $\sigma = \sigma_1\alpha$. Let $\tau \in \sigma \operatorname{Gal}(K/F_1F_2)$, then there is $\beta \in \operatorname{Gal}(K/F_1F_2)$ such that $\tau = \sigma\beta$. Now, $\sigma_1^{-1}\tau = \alpha\beta \in \operatorname{Gal}(K/F_1)$, whence $\tau \in \sigma_1 \operatorname{Gal}(K/F_1)$. This completes the proof. ∎

The topology defined above is known as the **Krull Topology**.

Theorem 8.4. *The Krull Topology on* $\operatorname{Gal}(K/k)$ *makes it a topological group.*

Proof. We must show that the multiplication map and the inversion map are continuous. Let $G = \operatorname{Gal}(K/k)$ and $\varphi : G \times G \to G$ be given by $(x, y) \mapsto xy$. Let U be an open set in G and $(\sigma, \tau) \in \varphi^{-1}(U)$. Then there is a basic open set of the form $\sigma\tau \operatorname{Gal}(K/F)$ for some finite extension F/k. Since the larger F is, the smaller $\operatorname{Gal}(K/F)$ gets, we may suppose that F/k is Galois. Consider the basic open set $\sigma \operatorname{Gal}(K/F) \times \tau \operatorname{Gal}(K/F)$ that contains (σ, τ). I claim that the image of this basic open set lies inside $\sigma\tau \operatorname{Gal}(K/F)$. Indeed, for $(\sigma\alpha, \tau\beta)$ in the basic open set, its image is $\sigma\alpha\tau\beta = \sigma\tau\alpha'\beta = \sigma\tau\gamma$ for some $\gamma \in \operatorname{Gal}(K/F)$. Where we used the normality of $\operatorname{Gal}(K/F)$ in G since the extension is normal. Thus φ is continuous.

Let $\psi : G \to G$ be the inversion map, that is, $x \mapsto x^{-1}$. We use a similar strategy as above. Let U be an open set containing σ^{-1} for some $\sigma \in G$. Then, there is a basic open set $\sigma^{-1} \operatorname{Gal}(K/F)$ that is contained in U. We may make F larger to make it a Galois extension of k. Thus, $\operatorname{Gal}(K/F)$ is normal in G. As a result, under ψ, $\sigma \operatorname{Gal}(K/F)$ maps to $\sigma^{-1} \operatorname{Gal}(K/F)$. This completes the proof. ∎

Proposition 8.5. $\operatorname{Gal}(K/k)$ *under the Krull Topology is Hausdorff.*

Proof. Let $\sigma, \tau \in \operatorname{Gal}(K/k)$ be distinct elements. Then, there is $\alpha \in K$ such that $\sigma(\alpha) \neq \tau(\alpha)$. Let $F = k(\alpha)$, and note that $\sigma \operatorname{Gal}(K/F) \neq \tau \operatorname{Gal}(K/F)$ and thus must be disjiont (since they are cosets). ∎

We state the main theorem of this chapter below. We shall prove it in parts and not all at once. It would seem less daunting that way.

Theorem 8.6 (Krull). *Let K/k be Galois and equip $G = \operatorname{Gal}(K/k)$ with the Krull topology. Then*

(a) For all intermediate fields E, $\operatorname{Gal}(K/E)$ is a closed subgroup of G.

(b) For all $H \leq G$, $\operatorname{Gal}(K/K^H)$ is the closure of H in G.

(c) (The Galois Correspondence) There is an inclusion reversing bijection between the intermediate fields of K/k an closed subgroups of $\operatorname{Gal}(K/k)$.

(d) For an arbitrary subgroup H of G, $K^H = K^{\overline{H}}$.

Proposition 8.7. *Let K/k be a Galois extension and E an intermediate field. Then $\operatorname{Gal}(K/E)$ is a closed subgroup of $\operatorname{Gal}(K/k)$.*

Proof. Let $\sigma \in G \setminus \operatorname{Gal}(K/E)$. Then $\sigma \operatorname{Gal}(K/E)$ is a basic open set containing σ and disjiont from $\operatorname{Gal}(K/E)$ (since it is a coset). This implies the desired conclusion. ∎

Proposition 8.8. *Let $H \leq G = \operatorname{Gal}(K/k)$. Then $\operatorname{Gal}(K/K^H)$ is the closure of H in G.*

Proof. Obviously, $H \subseteq \mathrm{Gal}(K/K^H)$. Further, since the latter is closed, $\overline{H} \subseteq \mathrm{Gal}(K/K^H)$. We shall show the reverse inclusion. Let $\sigma \in G \backslash \overline{H}$. As we have seen earlier, there is a finite Galois extension F/k such that the basic open set $\sigma \,\mathrm{Gal}(F/k)$ is disjoint from $\overline{H}$. We claim that there is $\alpha \in F$ such that α is fixed under H but not under σ. Suppose there is no such α. Then, $\sigma|_F$ fixes $F^{H|_F}$ where $H|_F = \{h|_F : h \in H\}$. From finite Galois theory, we know that $\sigma|_F \in H|_F$. And thus, there is some $h \in H$ such that $\sigma|_F = h|_F$, consequently, $\sigma \,\mathrm{Gal}(K/F) = h \,\mathrm{Gal}(K/F)$, a contradiction.

Since there is some $\alpha \in F$ that is not fixed by σ but fixed under H, we must have that $\sigma \notin \mathrm{Gal}(K/K^H)$. This completes the proof. ■

Chapter 9

Inverse Galois Theory

9.1 $\mathfrak{S}_n$ and $\mathfrak{A}_n$