

Field and Galois Theory

Swayam Chube

June 27, 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

1	Algebraic Extensions	2
2	Algebraic Closure	3
3	Normal Extensions	5
4	Separable Extensions	7
5	Inseparable Extensions	12
6	Finite Fields	14
7	Galois Extensions	16
8	Cyclotomic Extensions	19
9	Norm and Trace	20
10	Cyclic Extensions	22
11	Infinite Galois Theory	24
11.1	Galois Groups as Inverse Limits	25

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 \mathcal{C} be a class of extension fields $F \subseteq E$. We say that \mathcal{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 \mathcal{C} if and only if $k \subseteq F$ is in \mathcal{C} and $F \subseteq E$ is in \mathcal{C} .
2. If $k \subseteq E$ is in \mathcal{C} , if F is any extension of k , and E, F are both contained in some field, then $F \subseteq EF$ is in \mathcal{C} .
3. If $k \subseteq F$ and $k \subseteq E$ are in \mathcal{C} and F, E are subfields of a common field, then $k \subseteq FE$ is in \mathcal{C} .

Lemma 1.4. Let E/k be algebraic and let $\sigma : E \rightarrow E$ 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 must have 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 algebraically closed field containing k .*

Proof due to Artin. ■

Corollary 2.2. *Let k be a field. Then there exists an extension k^a which is algebraic over k and algebraically closed.*

Proof. ■

Lemma 2.3. *Let k be a field and L an algebraically closed field with $\sigma : k \rightarrow L$ an embedding. Let α be algebraic over k in some extension of k . Then, the number of extensions of σ to an embedding $k(\alpha) \rightarrow L$ is precisely equal to the number of distinct roots of the minimal polynomial of α over k .*

Lemma 2.4. *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 2.5 (Extension Theorem). *Let E/k be algebraic, L an algebraically closed field and $\sigma : k \rightarrow L$ 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 \mathcal{S} be the set of all pairs (F, τ) where $F \subseteq E$ and F/k is algebraic and $\tau : F \rightarrow L$ is an extension of σ . Define a partial order \leq on \mathcal{S} by $(F_1, \tau_1) \leq (F_2, \tau_2)$ if and only if $F_1 \subseteq F_2$ and $\tau_2|_{F_1} \equiv \tau_1$. Note that \mathcal{S} is nonempty since it contains (k, σ) . Let $\mathcal{C} = \{(F_\alpha, \tau_\alpha)\}$ be a chain in \mathcal{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 2.3.

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

Corollary 2.6. 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 $\tau : E \rightarrow E'$ inducing the identity on k .

Proof. Consider the extension of $\sigma : k \rightarrow E'$ where $\sigma|_k = \text{id}_k$ 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 .

Definition 2.7 (Conjugates). Let E/k be an algebraic extension contained in an algebraic closure k^a . Then, the distinct roots of the minimal polynomial of α over k are called the *conjugates* of α . In particular, two roots of the same minimal polynomial over k are said to be *conjugate* to one another.

Here's a nice exercise from [DF04].

Example 2.8. A field is said to be *formally real* if -1 cannot be expressed as a sum of squares in it. Let k be a formally real field with k^a its algebraic closure. If $\alpha \in k^a$ with odd degree over k , then $k[\alpha]$ is also formally real.

Proof. Suppose not. Let $\alpha \in k^a$ be such that $k[\alpha]$ is not formally real and $[k[\alpha] : k]$ is minimum, greater than 1. Then, there are elements $\gamma_1, \dots, \gamma_m \in k[\alpha]$ such that $\sum_{i=1}^m \gamma_i^2 = -1$. We may choose polynomials $p_i(x) \in k[x]$ such that $p_i(\alpha) = \gamma_i$ with $\deg p_i(\alpha) < [k[\alpha] : k]$.

Let $f(x) \in k[x]$ be the irreducible polynomial of α over k . We have

$$p_1(\alpha)^2 + \dots + p_m(\alpha)^2 = -1$$

and thus, α is a root of the polynomial $p_1(x)^2 + \dots + p_m(x)^2 + 1$. Thus, there is a polynomial $g(x) \in k[x]$ such that

$$p_1(x)^2 + \dots + p_m(x)^2 + 1 = f(x)g(x).$$

Notice that the degree of the left hand side is even and less than $2 \deg f$ whence $\deg g < \deg f$ and is odd.

Further, note that $g(x)$ may not have a root in k lest -1 be written as a sum of squares in k . Consider now the factorization of $g(x)$ as a product of irreducibles:

$$g(x) = h_1(x) \cdots h_n(x).$$

Equating degrees, we see that there is an index j such that $\deg h_j$ is odd. Let β be a root of h_j in k^a . Then, $[k[\beta] : k] = \deg h_j \leq \deg g < \deg f$ and

$$p_1(\beta)^2 + \dots + p_m(\beta)^2 + 1 = f(\beta)g(\beta) = 0$$

whence $k[\beta]$ is not formally real and contradicts the choice of α . ■

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 \bar{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 $\sigma : E \rightarrow K$ inducing the identity on k . If $k \subseteq K \subseteq \bar{k}$, where \bar{k} is an algebraic closure of k , then any embedding of E in \bar{k} inducing the identity on k must be an isomorphism of E on K .

Proof. We prove both assertions together. Due to Theorem 2.5, there is an embedding $\sigma : E \rightarrow \bar{k}$ such that $\sigma|_k = \text{id}_k$. Therefore, it suffices to prove the second half of the theorem.

We have two factorizations

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

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 $(\sigma\beta_1, \dots, \sigma\beta_n)$ differs from $(\alpha_1, \dots, \alpha_n)$ by a permutation. Since $\sigma E = k(\sigma\beta_1, \dots, \sigma\beta_n)$, we immediately have the desired conclusion. ■

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

1. Every embedding σ of K in \bar{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.

(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 \bar{k} . Then, there is an isomorphism $\sigma : k(\alpha) \rightarrow k(\beta)$. One may extend this to an embedding $\sigma : K \rightarrow \bar{k}$, which by our hypothesis, is an automorphism of K , implying that $\beta \in K$ and giving us the desired conclusion.

(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 $\sigma : K \rightarrow k^a$ be an embedding of fields. Since f_i remains invariant under σ , it must map a root of f_i to another root 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.

(3) \implies (1): Let $\sigma : K \rightarrow \bar{k}$ 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 \bar{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 3.5. The splitting field of a polynomial is a normal extension.

Theorem 3.6. 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 $K_1 K_2$ 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 \bar{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 \bar{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 $K_1 K_2$ over k , then its restriction to K_1 and K_2 respectively are also embeddings over k and consequently are automorphisms. This gives us

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

Finally, since any embedding of $K_1 \cap K_2$ can be extended to that of $K_1 K_2$, 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 $\sigma : k \rightarrow L$. Define S_σ to be the set of extensions of σ to $\sigma^* : E \rightarrow L$.

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 $\tau : k \rightarrow L'$ 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 $\sigma : k \rightarrow L$ be an embedding. Let $\{\sigma_i\}_{i \in I}$ be the extensions of σ to an embedding $F \rightarrow L$ and $\{\tau_{ij}\}$ be the extensions of σ_i to an embedding $E \rightarrow L$. We have indexed τ in such a way that the restriction $\tau_i|_F = \sigma_i$. 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 4.5. Let E/k be finite. Then, $[E : k]_s \leq [E : k]$.

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

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

We may now finish using Lemma 2.3. ■

Theorem 4.6. Let E/k be finite and $\text{char } k = 0$. Then E/k is separable.

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

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

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 2.3, we must have $k(\alpha)/k$ is separable.

This immediately implies the desired conclusion, since

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

■

Theorem 4.7. Let E/k be finite and $\text{char } k = p > 0$. Then, there is $m \in \mathbb{N}_0$ such that

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

Proof.

■

Remark 4.0.1. From the above proof we obtain that if $\alpha \in E$, then $\alpha^{[E:k]_i}$ is separable over k .

Corollary 4.8. Let E/k be a finite extension. Then, $[E : k]_s$ divides $[E : k]$.

Proof. Follows from Theorem 4.6 and Theorem 4.7.

■

Definition 4.9 (Inseparable Degree). Let E/k be finite. Then, we denote

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

as the *inseparable degree*.

Lemma 4.10. 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 4.11. 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 $\alpha \in E \setminus k$. Then, there is a tower of extensions

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

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 $k(\alpha_1, \dots, \alpha_{i-1})$ due to Lemma 4.10. Consequently, for each step in the tower,

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

implying the desired conclusion. ■

Definition 4.12 (Infinite Separable Extensions). An algebraic extension E/k is said to be *separable* if each finitely generated sub-extension is separable.

Theorem 4.13. 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 $k(\alpha_1, \dots, \alpha_n)/k$ be a finitely generated sub-extension of E/k . From our proof of Proposition 4.11, we know that α_i is separable over $k(\alpha_1, \dots, \alpha_{i-1})$, and therefore, $k(\alpha_1, \dots, \alpha_n)$ is separable over k and we have the desired conclusion. ■

Theorem 4.14. 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 $k(\alpha_1, \dots, \alpha_n)$ be a finitely generated sub-extension of E . Then, we have the following tower

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

From our proof of Proposition 4.11, we know that α_i is separable over $k(\alpha_1, \dots, \alpha_{i-1})$, this immediately implies that $k(\alpha_1, \dots, \alpha_n)/k$ is separable. ■

Theorem 4.15. 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 4.14. 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 $k(a_0, \dots, a_n)$. Since α is separable over F , $p(x)$ has no repeated roots and therefore α is also separable over $k(a_0, \dots, a_n)$. We now have a finite tower

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

Furthermore, since each a_i is separable over k for $0 \leq i \leq n$, it must be the case that $k(a_0, \dots, a_n)$ 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 4.13. This completes the proof. ■

Definition 4.16 (Separable Closure). Let k be a field and k^a be an algebraic closure. We define the separable closure k^{sep} as

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

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 4.17 (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 4.18 (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 $\bar{k}[x]$, $g_F \mid f$ 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 $\sigma_1, \dots, \sigma_n$ be distinct embeddings of $k(\alpha, \beta)$ into \bar{k} over k

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

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 4.19. *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 $\beta \in E \setminus k(\alpha)$. Now, since $k(\alpha, \beta)$ is a separable extension and is finite, it must be primitive. 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

Proposition 5.1. Let $\alpha \in k^a$ and $f(x) \in k[x]$ be the minimal polynomial of α over k . If $\text{char } k = 0$, then all the roots of f have multiplicity 1. If $\text{char } k = p > 0$, then there is a non-negative integer m such that every root of f has multiplicity p^m . Consequently, we have

$$[k(\alpha) : k] = p^m [k(\alpha) : k]_s$$

and α^{p^m} is separable over k .

Proof. ■

Definition 5.2. Let $\text{char } k = p > 0$. An element $\alpha \in k^a$ is said to be *purely inseparable* over k if there is a non-negative integer $n \geq 0$ such that $\alpha^{p^n} \in k$.

Theorem 5.3. Let $\text{char } k = p > 0$ and E/k be an algebraic extension. Then the following are equivalent:

- (a) $[E : k]_s = 1$.
- (b) Every element $\alpha \in E$ is purely inseparable over k .
- (c) For every $\alpha \in E$, the irreducible equation of α over k is of type $X^{p^n} - a = 0$ for some $n \geq 0$ and $a \in k$.
- (d) There is a set of generators $\{\alpha_i\}_{i \in I}$ of E over k such that each α_i is purely inseparable over k .

Proof. (a) \implies (b). Let $\alpha \in E$. From the multiplicativity of the separable degree, we must have $[k(\alpha) : k]_s = 1$. Let $f(x) \in k[x]$ be the minimal polynomial of α over k . Since $[k(\alpha) : k]_s$ is equal to the number of distinct roots of f , we see that $f(x) = (x - \alpha)^m$ for some positive integer m . Let $m = p^n r$ such that $p \nmid r$. Then, we have

$$f(x) = (x - \alpha)^{p^n r} = \left(x^{p^n} - \alpha^{p^n} \right)^r = x^{p^n r} - r \alpha^{p^n} x^{p^n(r-1)} + \dots$$

Since the coefficients of f lie in k , we have $r \alpha^{p^n} \in k$ whence $\alpha^{p^n} \in k$.

(b) \implies (c). There is a minimal non-negative integer n such that $\alpha^{p^n} \in k$. Consider the polynomial $g(x) = x^{p^n} - \alpha^{p^n} \in k[x]$. Note that $g(x) = (x - \alpha)^{p^n}$, whence the minimal polynomial for α over k divides g and is thus of the form $(x - \alpha)^m$ for some positive integer $m \leq p^n$. Using a similar argument as in the previous paragraph, we see that there is a non-negative integer r such that $\alpha^{p^r} \in k$. Due to the minimality of n , we must have $m = p^n$ and g the minimal polynomial of α over k .

(c) \implies (d). Trivial.
(d) \implies (a). Any embedding of E in k^a must be the identity on the α_i 's whence the embedding must be the identity on all of E which completes the proof. ■

Definition 5.4. An algebraic extension E/k is said to be *purely inseparable* if it satisfies the equivalent conditions of Theorem 5.3.

Proposition 5.5. *Purely inseparable extensions form a distinguished class of extensions.*

Proof. Let $\text{char } k = p > 0$. The assertion about the tower of fields follows from the multiplicativity of separable degree. Now, let E/k be purely inseparable. Then there is a set of generators $\{\alpha_i\}_{i \in I}$ generating E over k . Then, $\{\alpha_i\}_{i \in I}$ generates EF over F . Since the minimal polynomial of α_i over F must divide the minimal polynomial of α_i over k , which is of the form $(x - \alpha_i)^{p^{n_i}}$ for some non-negative integer n_i , we see that α_i is purely inseparable over F whence EF is purely inseparable over F .

Finally, let E/k and F/k be purely inseparable extensions. If $\{\alpha_i\}_{i \in I}$ and $\{\beta_j\}_{j \in J}$ generate E and F over k respectively such that each α_i and β_j is purely inseparable over k , then EF is generated by $\{\alpha_i\}_{i \in I} \cup \{\beta_j\}_{j \in J}$ over k whence is purely inseparable over k . ■

Proposition 5.6. *Let E/k be an algebraic extension and E_0 the separable closure of k in E . Then, E/E_0 is purely inseparable.*

Proof. If $\text{char } k = 0$, then E/k is separable and $E_0 = E$ and the conclusion is obvious. On the other hand, if $\text{char } k = p > 0$, then for every $\alpha \in E$, there is a non-negative integer m such that α^{p^m} is separable over k whence an element of E_0 . Thus, E/E_0 is purely inseparable. ■

Proposition 5.7. *Let K/k be normal and K_0 the separable closure of k in K . Then K_0/k is normal.*

Proof. Let $\sigma : K_0 \rightarrow k^a$ be an embedding of fields. This extends to an embedding of K and is thus an automorphism of K . Note that $\sigma(K_0)$ is separable over k and is thus contained in k_0 whence $\sigma(K_0) = K_0$ and σ is an automorphism. This completes the proof. ■

Lemma 5.8. *Let K/k be normal, $G = \text{Aut}(K/k)$ and K^G the fixed field of G . Then K^G/k is purely inseparable and K/K^G is separable. If K_0 is the separable closure of k in K , then $K = K^G K_0$ and $K^G \cap K_0 = 0$.*

Proof. Let $\alpha \in K^G$ and $\sigma : k(\alpha) \rightarrow k^a$ be an embedding over k . This can be extended to an embedding $\tilde{\sigma} : K \rightarrow k^a$. Since K is normal, this is an automorphism $\tilde{\sigma} : K \rightarrow K$ and thus an element of G . This must leave α fixed whence σ is the identity map, consequently, α is purely inseparable over k and the conclusion follows.

We shall now show that K/K^G is separable. Pick some $\alpha \in K$ and let $\sigma_1, \dots, \sigma_n \in G$ such that the elements $\sigma_1(\alpha), \dots, \sigma_n(\alpha)$ form a maximal set of pairwise distinct elements. Consider the polynomial $f(x)$ in $K[x]$ given by

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

It is not hard to see that for any $\sigma \in G$, $\sigma(f) = f$, whence $f \in K^G[x]$ and α is separable over K^G .

Note that any element of $K^G \cap K_0$ is both separable and purely inseparable over k whence an element of k . Thus $K^G \cap K_0 = k$.

Finally, since both purely inseparable and separable extensions form a distinguished class, we have $K/K_0 K^G$ is both separable and purely inseparable whence $K = K_0 K^G$. This completes the proof. ■

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 $\overline{\mathbb{F}_p}$, 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 $\overline{\mathbb{F}_p}$ 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, $\varphi : \mathbb{F}_q \rightarrow \mathbb{F}_q$ 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, $G = \text{Aut}(\mathbb{F}_q) = \text{Aut}(\mathbb{F}_q/\mathbb{F}_p)$. Furthermore, $|\text{Aut}(\mathbb{F}_q/\mathbb{F}_p)| = [\mathbb{F}_q : \mathbb{F}_p]_s \leq [\mathbb{F}_q : \mathbb{F}_p] = n$.

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 $p^d \geq q$ and $d \geq n$ 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 $\text{Gal}(K/k)$.

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

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

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

Proof. Let $\alpha \in K^G$ and $\sigma : k(\alpha) \rightarrow \bar{K}$ be an embedding over k . Due to Theorem 2.5, σ may be extended to an embedding of K over k in \bar{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 3.6 and Theorem 4.15, 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 $\beta \in E \setminus k(\alpha)$ and thus, we have a tower $k \subseteq k(\alpha) \subsetneq k(\alpha, \beta)$. Due to Theorem 4.18, 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 $[k(\alpha) : k] \leq \deg f \leq n$ whence due to Lemma 7.4, $[K : k] \leq n$. Now, recall that $n = |G| \leq [K : k]_s \leq [K : k]$ and we have the desired conclusion. ■

Corollary 7.6. Let K/k be a finite Galois extension and $G = \text{Gal}(K/k)$. Then, every subgroup of G belongs to some subfield F such that $k \subseteq F \subseteq K$.

Lemma 7.7. Let K/k be Galois and F an intermediate field, $k \subseteq F \subseteq K$, and let $\lambda : F \rightarrow \bar{k}$ be an embedding. Then,

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

Proof. The embedding λ can be extended to an embedding of K due to Theorem 2.5 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 $\sigma \in \text{Gal}(K/F)$. It is not hard to see that $\lambda\sigma\lambda^{-1} \in \text{Gal}(K/\lambda F)$ and conversely, for $\tau \in \text{Gal}(K/\lambda F)$, $\lambda^{-1}\tau\lambda \in \text{Gal}(K/F)$. This implies the desired conclusion. ■

Theorem 7.8. Let K/k be Galois with $G = \text{Gal}(K/k)$. Let F be an intermediate field, $k \subseteq F \subseteq K$, and let $H = \text{Gal}(K/F)$. 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 $\text{Gal}(F/k)$ whose kernel is H . This gives us $\text{Gal}(F/k) \cong G/H$.

Proof. Suppose F/k is normal. To see that the map $\sigma \rightarrow \sigma|_F$ is surjective, simply recall Theorem 2.5. The kernel of said mapping is obviously H and we have that $H \trianglelefteq G$ and due to the First Isomorphism Theorem, $G/H \cong \text{Gal}(F/k)$.

On the other hand, if F/k is not normal, then there is an embedding $\lambda : F \rightarrow \bar{k}$ such that $F \neq \lambda F$. Note that due to Theorem 2.5, $\lambda F \subseteq K$. Then, we have $\text{Gal}(K/F) \neq \text{Gal}(K/\lambda F) = \lambda \text{Gal}(K/F) \lambda^{-1}$, and equivalently, $\text{Gal}(K/F)$ 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 7.9 (Fundamental Theorem of Galois Theory). Let K/k be a finite Galois extension with $G = \text{Gal}(K/k)$. 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 $\sigma \mapsto \sigma|_E$ induces an isomorphism of G/H onto $\text{Gal}(E/k)$.

Definition 7.10. A Galois extension K/k is said to be *abelian* (resp. *cyclic*) if its Galois group is *abelian* (resp. *cyclic*).

Theorem 7.11. 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 $H = \text{Gal}(KF/F)$ and $G = \text{Gal}(K/k)$. For all $\sigma \in H$, the restriction of σ to K is in G and the restriction map $\sigma \mapsto \sigma|_K$ gives an isomorphism of H on $\text{Gal}(K/K \cap F)$.

Proof. That KF/F and $K/K \cap F$ are Galois follow from Theorem 3.6 and Theorem 4.15. Let $\chi : H \rightarrow G$ 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 7.9. ■

Chapter 8

Cyclotomic Extensions

Definition 8.1. Let k be a field. A *root of unity* in k is an element $\zeta \in k$ such that $\zeta^n = 1$ for some $n \in \mathbb{N}$.

Now, if $n > 1$ is an integer not divisible by $\text{char } k$, then the polynomial $x^n - 1$ is separable, and hence, in k^a , has n distinct roots. It is not hard to see that these form a group under multiplication. Since this is a finite multiplicative subgroup of a field, it must be cyclic. A generator for this group is called a *primitive n -th root of unity*. We use μ_n to denote the group of n -th roots of unity in k^a .

From the previous paragraph, we see that if $\gcd(\text{char } k, n) = 1$, then $k(\zeta)$ is a splitting field for $x^n - 1$ and ζ is separable over k , therefore, $k(\zeta)/k$ is Galois.

Proposition 8.2. Let $\gcd(\text{char } k, n) = 1$. If ζ is a primitive n -th root of unity, then $k(\zeta)/k$ is an abelian extension.

Proof. Define the map $\psi : \text{Gal}(k(\zeta)/k) \rightarrow \text{Aut}(\mu_n)$ by $\sigma \mapsto \sigma|_{\mu_n}$. Note that $\text{Aut}(\mu_n) \cong (\mathbb{Z}/n\mathbb{Z})^\times$, further, it is not hard to see that ψ is injective and the conclusion follows. ■

Note that although we have shown $\text{Gal}(k(\zeta)/k)$ to be embeddable into $(\mathbb{Z}/n\mathbb{Z})^\times$, the map may not be a surjection take for example $k = \mathbb{R}$ and $\zeta = \exp(2\pi i/5)$. Then, $k(\zeta) = \mathbb{C}$, and $\text{Gal}(k(\zeta)/k) \cong \{\pm 1\}$.

Proposition 8.3. Let ζ be a primitive n -th root of unity over \mathbb{Q} . Then,

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$$

and consequently, the map $\psi : \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \rightarrow (\mathbb{Z}/n\mathbb{Z})^\times$ is an isomorphism.

Proof. **TODO: Add in later** ■

Chapter 9

Norm and Trace

Definition 9.1. Let E/k be a finite extension and $[E : k]_s = r$ and let $\sigma_1, \dots, \sigma_r$ be distinct embeddings of E in an algebraic closure k^a of k . We define the *norm* and *trace* of $\alpha \in E$ as

$$N_{E/k}(\alpha) = N_k^E(\alpha) = \left(\prod_{j=1}^r \sigma_j \alpha \right)^{[E:k]_i}$$

$$\text{Tr}_{E/k}(\alpha) = \text{Tr}_k^E(\alpha) = [E : k]_i \sum_{j=1}^r \sigma_j \alpha$$

Notice that if E/k were not separable, then $\text{char } k > 0$ and would be a prime, say p . Further, $[E : k]_i = p^\nu$ for some $\nu \geq 1$, consequently, $\text{Tr}_k^E(\alpha) = 0$ (since $\text{char } E = \text{char } k = p$).

Proposition 9.2. Let E/k be a finite extension such that $E = k(\alpha)$ for some $\alpha \in E$. If

$$p(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0$$

is the minimal polynomial of α over k , then

$$N_k^E(\alpha) = (-1)^n a_0 \quad \text{Tr}_k^E(\alpha) = -a_{n-1}$$

Proof. This follows from the fact that the minimal polynomial splits as

$$p(x) = ((x - \alpha_1) \cdots (x - \alpha_r))^{[E:k]_i}$$

whence the conclusion follows. ■

Proposition 9.3. Let E/k be a finite extension. Then the norm $N_k^E : E^\times \rightarrow k^\times$ is a multiplicative homomorphism and the trace $\text{Tr}_k^E : E \rightarrow k$ is an additive homomorphism. Further, if we have a tower of finite extensions $k \subseteq F \subseteq E$, then

$$N_k^E = N_k^F \circ N_F^E \quad \text{Tr}_k^E = \text{Tr}_k^F \circ \text{Tr}_F^E$$

Proof. First, we must show that N_k^E is a map $E^\times \rightarrow k^\times$ and Tr_k^E is a map $E \rightarrow k$. Recall that for $\alpha \in E$, $\beta = \alpha^{[E:k]_i}$ is separable over k and thus N_k^E , which is the product of all the conjugates of β is also separable since all conjugates lie in k^{sep} . Now, let $\sigma : k^a \rightarrow k^a$ be a homomorphism fixing k . Then, it is not hard to see that $\sigma(\beta) = \beta$ and thus $[k(\beta) : k]_s = 1$ but since β is separable, we have $[k(\beta) : k] = 1$ and $\beta \in k$. A similar argument can be applied to the trace.

Let $\{\sigma_i\}$ be the set of distinct embeddings of E into k^a fixing F and $\{\tau_j\}$ be the set of distinct embeddings of F into k^a fixing k . Extend each τ_j to a homomorphism $k^a \rightarrow k^a$.

We contend that the set of all distinct embeddings of E into k^a fixing k is precisely $\{\tau_j \circ \sigma_i\}$. Obviously, every element of the aforementioned family is distinct and is an embedding of E into k^a fixing k . Now, let $\sigma : E \rightarrow k^a$ be an embedding of E into k^a . Then, the restriction $\sigma|_F$ is equal to (the restriction of) some τ_j , whereby $\tau_j^{-1}\sigma$ fixes F whereby it is equal to some σ_i . Thus every embedding of E into k^a over k is of the form $\tau_j \circ \sigma_i$.

Finally, we have

$$\begin{aligned} \left(\prod_{i,j} (\tau_j \circ \sigma_i)(\alpha) \right)^{[E:F]_i [F:k]_i} &= \left(\prod_j \tau_j \left(\prod_i \sigma_i(\alpha) \right) \right)^{[E:F]_i} \left(\prod_i \sigma_i(\alpha) \right)^{[F:k]_i} = N_k^F \circ N_F^E(\alpha) \\ [E:F]_i [F:k]_i \sum_{i,j} \tau_j \circ \sigma_i(\alpha) &= [F:k]_i \sum_j \tau_j \left([E:F]_i \sum_i \sigma_i(\alpha) \right) \end{aligned}$$

and the conclusion follows. ■

Theorem 9.4. *Let E/k be a finite extension and $\alpha \in E$. Let $m_\alpha : E \rightarrow E$ be the linear transformation given by $m_\alpha(x) = \alpha x$. Then,*

$$N_k^E(\alpha) = \det(m_\alpha) \quad \text{Tr}_k^E(\alpha) = \text{tr}(m_\alpha)$$

Note that we may unambiguously write $\det(m_\alpha)$ and $\text{tr}(m_\alpha)$ since both these quantities do not depend on the choice of a basis, since similar matrices have the same determinant and trace.

Proof. ■

Chapter 10

Cyclic Extensions

Definition 10.1. A Galois extension K/k is said to be *cyclic* if $\text{Gal}(K/k)$ is a cyclic group. Similarly, it is said to be *abelian* if $\text{Gal}(K/k)$ is abelian.

Theorem 10.2 (Linear Independence of Characters). Let G be a group (monoid) and K a field. If $\sigma_1, \dots, \sigma_n : G \rightarrow K^\times$ are distinct group homomorphisms. Then,

$$c_1\sigma_1 + \dots + c_n\sigma_n = 0 \iff c_1 = \dots = c_n = 0$$

Corollary 10.3. Let K/k be a Galois extension. Then, there is $\alpha \in K$ such that $\text{Tr}_k^K(\alpha) \neq 0$.

Proof. Suppose not. If $\text{Gal}(K/k) = \{\sigma_1, \dots, \sigma_n\}$, then

$$\sigma_1 + \dots + \sigma_n = 0$$

on K , a contradiction to Theorem 10.2. ■

Theorem 10.4 (Hilbert's Theorem 90). Let K/k be a cyclic degree n extension with galois group G . Let $\sigma \in G$ be a generator and $\beta \in K$. The norm $N_k^K(\beta) = 1$ if and only if there is $\alpha \in K^\times$ such that $\beta = \alpha / \sigma(\alpha)$

Proof. \implies Suppose $N_k^K(\beta) = 1$. We have a set of distinct characters $\{\text{id}, \sigma, \dots, \sigma^{n-1}\}$ from $K^\times \rightarrow K^\times$. Then, due to Theorem 10.2, the set map

$$\tau = \text{id} + \beta\sigma + (\beta\sigma(\beta))\sigma^2 + \dots + (\beta\sigma(\beta) \dots \sigma^{n-2}(\beta))\sigma^{n-1}$$

is nonzero, whereby, there is $\theta \in K^\times$ such that $\alpha = \tau(\theta) \neq 0$. Notice that

$$\sigma(\alpha) = \sigma(\theta) + (\sigma(\beta))\sigma^2(\theta) + \dots + (\sigma(\beta)\sigma^2(\beta) \dots \sigma^{n-1}(\beta))\sigma^n(\theta)$$

Since $N_k^K(\beta) = 1$, we have

$$\beta\sigma(\beta) \dots \sigma^{n-1}(\beta) = 1$$

whence, we have $\sigma(\alpha) = \alpha / \beta$ and the conclusion follows.

\longleftarrow This is trivial enough. ■

Example 10.5. Find all rational points on the curve $x^2 + y^2 = 1$.

Proof. This reduces to finding all elements $\alpha \in \mathbb{Q}[i]$ with $N_{\mathbb{Q}}^{\mathbb{Q}[i]}(\alpha) = 1$. Any element α of $\mathbb{Q}[i]$ may be written as $(a + bi)/c$. Due to Theorem 10.4, there is an element $\alpha \in \mathbb{Q}[i]$, such that $N_{\mathbb{Q}}^{\mathbb{Q}[i]}(\alpha) = 1$. Using the general form of elements in $\mathbb{Q}[i]$, we have

$$\alpha = \frac{a + bi}{a - bi} = \frac{(a^2 - b^2) + 2abi}{a^2 + b^2}$$

this completes the proof. ■

Theorem 10.6 (Additive Hilbert's Theorem 90). Let K/k be a cyclic Galois extension with $\text{Gal}(K/k) = \langle \sigma \rangle$ and $\beta \in K$. Then $\text{Tr}_k^K(\beta) = 0$ iff there is $\alpha \in K$ such that $\beta = \alpha - \sigma(\alpha)$.

Proof. Due to Corollary 10.3, there is some $\theta \in K$ with $\text{Tr}_k^K(\theta) \neq 0$. Consider $\alpha \in K$ given by

$$\alpha = \frac{1}{\text{Tr}_k^K(\theta)} \left(\beta\sigma(\theta) + (\beta + \sigma(\beta))\sigma^2(\theta) + \cdots + (\beta + \cdots + \sigma^{n-2}(\beta))\sigma^{n-1}(\theta) \right).$$

We have

$$\begin{aligned} \sigma(\alpha) &= \frac{1}{\text{Tr}_k^K(\theta)} \left(\sigma(\beta)\sigma^2(\theta) + (\sigma(\beta) + \sigma^2(\beta))\sigma^3(\theta) + \cdots + (\sigma(\beta) + \cdots + \sigma^{n-1}(\beta))\sigma^n(\theta) \right) \\ &= \alpha - \beta \frac{1}{\text{Tr}_k^K(\theta)} (\sigma(\theta) + \cdots + \sigma^n(\theta)) \\ &= \alpha - \beta \end{aligned}$$

The converse is trivial. ■

Theorem 10.7 (Artin-Schreier). Let k be a field of characteristic $p > 0$.

(a) Let K/k be a cyclic extension of degree p . Then there is $\alpha \in K$ such that $K = k(\alpha)$ and α is a root of $f(x) = x^p - x - a$ for some $a \in k$. Further, K is the splitting field of $f(x)$ over k .

(b)

Proof. (a) Let $\text{Gal}(K/k) = \langle \sigma \rangle$, since it is a group of prime order. We have $\text{Tr}_k^K(-1) = p \cdot (-1) = 0$ whence there is $\alpha \in K$ such that $-1 = \alpha - \sigma(\alpha)$, equivalently, $\sigma(\alpha) = \alpha + 1$. Let $a = \alpha^p - \alpha$. Then,

$$\sigma(a) = \sigma(\alpha^p - \alpha) = \sigma(\alpha)^p - (\alpha + 1) = \alpha^p + 1 - (\alpha + 1) = a.$$

Thus, $\sigma^n(a) = a$ for $1 \leq n \leq p$, consequently, $a \in K^{\text{Gal}(K/k)} = k$.

Note that for $1 \leq m \neq n \leq p$, we have

$$\sigma^m(\alpha) = \alpha + m \neq \alpha + n = \sigma^n(\alpha).$$

Thus, $p \leq [k(\alpha) : k]_s \leq [k(\alpha) : k] \leq [K : k] = p$ whence $[k(\alpha) : k] = p$ and $K = k(\alpha)$.

(b) ■

Chapter 11

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

Proof. We shall prove the contrapositive. If $\text{Gal}(K/k)$ 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 11.2. Let K/k be a Galois extension. For $\sigma \in \text{Gal}(K/k)$, a *basic open set* around σ is a coset $\sigma \text{Gal}(K/F)$ where F/k is a **finite** extension.

Proposition 11.3. *The collection of basic open sets as defined above form a basis for a topology on $\text{Gal}(K/k)$.*

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

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

Theorem 11.4. *The Krull Topology on $\text{Gal}(K/k)$ makes it a topological group.*

Proof. We must show that the multiplication map and the inversion map are continuous. Let $G = \text{Gal}(K/k)$ and $\varphi : G \times G \rightarrow G$ 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 $\sigma \tau \text{Gal}(K/F)$ for some finite extension F/k . Since the larger F is, the smaller $\text{Gal}(K/F)$ gets, we may suppose that F/k is Galois. Consider the basic open set $\sigma \text{Gal}(K/F) \times \tau \text{Gal}(K/F)$ that contains (σ, τ) . I claim that the image of this basic open set lies inside $\sigma \tau \text{Gal}(K/F)$. 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 $\gamma \in \text{Gal}(K/F)$. Where we used the normality of $\text{Gal}(K/F)$ in G since the extension is normal. Thus φ is continuous.

Let $\psi : G \rightarrow G$ 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 $\sigma^{-1} \text{Gal}(K/F)$ that is contained in U . We may make F larger to make it a Galois extension of k . Thus, $\text{Gal}(K/F)$ is normal in G . As a result, under ψ , $\sigma \text{Gal}(K/F)$ maps to $\sigma^{-1} \text{Gal}(K/F)$. This completes the proof. ■

Proposition 11.5. *$\text{Gal}(K/k)$ under the Krull Topology is Hausdorff.*

Proof. Let $\sigma, \tau \in \text{Gal}(K/k)$ be distinct elements. Then, there is $\alpha \in K$ such that $\sigma(\alpha) \neq \tau(\alpha)$. Let $F = k(\alpha)$, and note that $\sigma \text{Gal}(K/F) \neq \tau \text{Gal}(K/F)$ and thus must be disjoint (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 11.6 (Krull). *Let K/k be Galois and equip $G = \text{Gal}(K/k)$ with the Krull topology. Then*

- (a) *For all intermediate fields E , $\text{Gal}(K/E)$ is a closed subgroup of G .*
- (b) *For all $H \leq G$, $\text{Gal}(K/K^H)$ is the closure of H in G .*
- (c) *(The Galois Correspondence) There is an inclusion reversing bijection between the intermediate fields of K/k and closed subgroups of $\text{Gal}(K/k)$.*
- (d) *For an arbitrary subgroup H of G , $K^H = K^{\overline{H}}$.*

Proposition 11.7. *Let K/k be a Galois extension and E an intermediate field. Then $\text{Gal}(K/E)$ is a closed subgroup of $\text{Gal}(K/k)$.*

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

Proposition 11.8. *Let $H \leq G = \text{Gal}(K/k)$. Then $\text{Gal}(K/K^H)$ is the closure of H in G .*

Proof. Obviously, $H \subseteq \text{Gal}(K/K^H)$. Further, since the latter is closed, $\overline{H} \subseteq \text{Gal}(K/K^H)$. We shall show the reverse inclusion. Let $\sigma \in G \setminus \overline{H}$. As we have seen earlier, there is a finite Galois extension F/k such that the basic open set $\sigma \text{Gal}(F/k)$ 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, $\sigma \text{Gal}(K/F) = h \text{Gal}(K/F)$, a contradiction.

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

11.1 Galois Groups as Inverse Limits

Let K/k be a Galois extension, not necessarily finite. Let

$$\Sigma = \{\text{Gal}(F/k) \mid F/k \text{ is finite Galois}\}$$

be a poset with restriction maps

$$\pi_F^E : \text{Gal}(E/k) \rightarrow \text{Gal}(F/k).$$

which are continuous maps between topological groups where $\text{Gal}(E/k)$ and $\text{Gal}(F/k)$ have the discrete topology.

This gives Σ the implicit structure of a categorical *diagram*. We contend that $\text{Gal}(K/k)$ is the inverse limit¹ over this diagram in the category of topological groups, **TopGrp**.

First, we shall show that there is a cone $(\text{Gal}(K/k), \varphi)$ on the diagram Σ . Indeed, for every finite Galois subextension, define

$$\varphi_F : \text{Gal}(K/k) \rightarrow \text{Gal}(F/k)$$

as the restriction map $\sigma \mapsto \sigma|_F$. Recall that $\text{Gal}(F/k)$ has the discrete topology, whereby the preimage of $\sigma \in \text{Gal}(F/k)$ is $\sigma \text{Gal}(K/F)$ which is a basic open set in $\text{Gal}(K/k)$ whence the restriction map is continuous and thus a morphism in **TopGrp**.

It is not hard to see that the diagram

$$\begin{array}{ccc} \text{Gal}(E/k) & \xrightarrow{\pi_F^E} & \text{Gal}(F/k) \\ & \nwarrow \varphi_E \quad \nearrow \varphi_F & \\ & \text{Gal}(K/k) & \end{array}$$

commutes.

Now let (G, ψ) be another cone on the diagram Σ where G is a topological group we shall show that there is a unique morphism of cones $\Phi : (G, \psi) \rightarrow (\text{Gal}(K/k), \varphi)$. That is, a unique continuous group homomorphism that makes

$$\begin{array}{ccc} \text{Gal}(E/k) & \xrightarrow{\pi_F^E} & \text{Gal}(F/k) \\ & \nwarrow \psi_E \quad \nearrow \psi_F & \\ & G & \\ & \swarrow \varphi_E \quad \searrow \varphi_F & \\ & \text{Gal}(K/k) & \end{array}$$

commute.

Pick some $g \in G$. Let $\alpha \in K$ and $L \subseteq K$ be the normal closure of $k(\alpha)$ in K . Then, L/k is finite Galois. Now, define

$$\sigma(\alpha) = \psi_L(g)(\alpha).$$

We shall show that σ is indeed an automorphism. Let $\alpha, \beta \in K$ and L be the normal closure of $k(\alpha, \beta)$ in K . This is a finite Galois extension of k that contains the normal closures of $k(\alpha)$, $k(\beta)$ and $k(\alpha\beta)$, say M, N, P respectively. Then,

$$\begin{aligned} \sigma(\alpha\beta) &= \psi_P(g)(\alpha\beta) \\ &= \psi_L(g)(\alpha\beta) \\ &= \psi_L(g)(\alpha)\psi_L(g)(\beta) \\ &= \psi_M(\alpha)\psi_N(\beta) \\ &= \sigma(\alpha)\sigma(\beta). \end{aligned}$$

and similarly, one may show that $\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta)$ thus $\sigma \in \text{Hom}(K, K)$ which fixes k .

Lastly, we must show that σ is surjective. Let $\beta \in K$ and N the normal closure of $k(\beta)$ in K . Then, there is some $\alpha \in N$ such that $\psi_N(g)(\alpha) = \beta$. Let M be the normal closure of $k(\alpha)$ in K . Then $M \subseteq N$, whence

$$\sigma(\alpha) = \psi_M(g)(\alpha) = \psi_N(g)(\alpha) = \beta.$$

¹This is the categorical limit

Thus, $\sigma \in \text{Gal}(K/k)$ and set $\Phi(g) = \sigma$.

Let $g, h \in G$, $\Phi(g) = \sigma$, $\Phi(h) = \tau$ and $\alpha \in K$. Let M be the normal closure of $k(\alpha)$ in K . Then

$$\Phi(gh)(\alpha) = \psi_M(gh)(\alpha) = \psi_M(g) \circ \psi_M(h)(\alpha) = \sigma \circ \tau(\alpha)$$

and thus $\Phi(gh) = \sigma \circ \tau$ and Φ is a group homomorphism.

Finally, we must show that Φ is continuous, for which it suffices to show that the preimage of a basic open set in $\text{Gal}(K/k)$ is open in G .

Let $\sigma \in \text{Gal}(K/k)$ and F/k an intermediate finite Galois extension of k . We have

$$\begin{aligned} \Phi^{-1}(\sigma \text{Gal}(K/F)) &= \{g \in G \mid \Phi(g) \in \sigma \text{Gal}(K/F)\} \\ &= \{g \in G \mid \Phi(g)|_F = \sigma|_F\} \\ &= \{g \in G \mid \psi_F(g) = \sigma|_F\} \\ &= \psi_F^{-1}(\sigma|_F) \end{aligned}$$

which is open in G since $\text{Gal}(F/k)$ has the discrete topology whence Φ is continuous.

This finishes the proof and shows that $\text{Gal}(K/k)$ is the inverse limit $\varprojlim \text{Gal}(F/k)$, and is a profinite group since every topological group in the inverse limit is a finite group with the discrete topology.

Corollary 11.9. $\text{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) = \hat{\mathbb{Z}}$.

Bibliography

[DF04] David S. Dummit and Richard M. Foote. *Abstract algebra*. Wiley, New York, 3rd ed edition, 2004.