Field and Galois Theory

Swayam Chube

November 19, 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. The main reference followed while making these notes is [Lan02]

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 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 algebraicaly 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 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 2.4. *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 $\sigma : k \to L$ 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 2.3.

Finally, if E is algebraically closed, so is σE, consequently, we are done due to the preceeding 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 $\tau : E \to E'$ 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.

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 $\gamma_1, \ldots, \gamma_m \in k[\alpha]$ 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

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

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

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

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

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

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

The proof of the next theorem requires some tools from later chapters.

Theorem 2.9. *Let K/k be an algebraic extension such that every non-constant polynomial in $k[x]$ has a root in K. Then, K is algebraically closed.*

Proof. Let $\alpha \in k^a$. We shall show that $\alpha \in K$ which would imply the desired conclusion. Let $f(x) \in k[x]$ be the minimal polynomial of α over k and $F \subseteq k^a$ be the splitting field of $f(x)$ over k, which is obviously a finite extension.

Due to Lemma 5.8, there are subfields F_0 and E of F such that $F = F_0E$, E/k is purely inseparable and F_0 is the separable closure of k in F. Since F_0/k is a finite separable extension, due to Theorem 4.18, there is some $\beta \in F_0$ such that $F_0 = k(\beta)$.

Let $g(x)$ be the minimal polynomial of β over k and $\beta' \in K$ be a root of $g(x)$. Since $g(x)$ is the minimal polynomial of β' and is separable since β is separable over k, we have that $\beta' \in F_0 = k(\beta)$ and thus

$$F_0 = \underbrace{k(\beta) = k(\beta')}_{\text{due to a dimension argument}} \subseteq K.$$

E/k is finite, it has a basis, say $\gamma_1, \ldots, \gamma_n$. The minimal polynomial of γ_i is of the form $(x - \gamma_i)^{p^{r_i}}$ and thus has a single root, whence, $\gamma_i \in K$. Thus $E \subseteq K$. As a result,

$$F = F_0E \subseteq K$$

and thus $\alpha \in K$ thereby completing the proof. ■

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 2.5, 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.
(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.
(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 $\sigma : K \to k^a$ 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.
(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 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_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 4.5. 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 2.3. ∎

Theorem 4.6. *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:

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

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* $\operatorname{char} k = p > 0$. *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 $\alpha \in E \backslash k$. 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 4.10. 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 4.12 (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 $k(\alpha_1, \ldots, \alpha_n)/k$ be a finitely generated sub-extension of E/k. From our proof of Proposition 4.11, we know that α_i is separable over $k(\alpha_1, \ldots, \alpha_{i-1})$, and therefore, $k(\alpha_1, \ldots, \alpha_n)$ 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 $k(\alpha_1, \ldots, \alpha_n)$ 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 4.11, 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 4.15. *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 $k(a_0, \ldots, a_n)$. 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 4.13. This completes the proof. ■

Definition 4.16 (Separable Closure). Let k be a field and k^a be an algebrai 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 $\sigma_1, \ldots, \sigma_n$ be distinct embeddings of $k(\alpha, \beta)$ into $\bar{k}$ over k

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

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 $1 \le i \le n$, and thus

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

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 $\beta \in E \backslash k(\alpha)$. 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

Proposition 5.1. *Let $\alpha \in k^a$ and $f(x) \in k[x]$ be the minimal polynomial of α over k. If $\operatorname{char} k = 0$, then all the roots of f have multiplicity 1. If $\operatorname{char} k = p > 0$, 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 $\operatorname{char} k = p > 0$. 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 $\operatorname{char} k = p > 0$ 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

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

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 $\operatorname{char} k = p > 0$. 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, 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 $\operatorname{char} k = 0$, then E/k is separable and $E_0 = E$ and the conclusion is obvious. On the other hand, if $\operatorname{char} k = p > 0$, 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 $\sigma : K_0 \to k^a$ 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, $G = \operatorname{Aut}(K/k)$ 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 $\sigma : k(\alpha) \to k^a$ be an embedding over k. This can be extended to an embedding $\widetilde{\sigma} : K \to k^a$. Since K is normal, this is an automorphism $\widetilde{\sigma} : K \to K$ 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 $\sigma_1, \ldots, \sigma_n \in G$ such that the elements $\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$ 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_0K^G is both separable and purely inseparable whence $K = K_0K^G$. 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 $\overline{F}_p$, 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, $G = \operatorname{Aut}(\mathbb{F}_q) = \operatorname{Aut}(\mathbb{F}_q/\mathbb{F}_p)$. Furthermore, $|\operatorname{Aut}(\mathbb{F}_q/\mathbb{F}_p)| = [\mathbb{F}_q : \mathbb{F}_p]_s \le [\mathbb{F}_q : \mathbb{F}_p] = n$.

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 $\text{Gal}(K/k)$.

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 $\sigma : k(\alpha) \to \overline{K}$ be an embedding over k. Due to Theorem 2.5, 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 3.6 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 $\beta \in E \backslash k(\alpha)$ 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 $G = \operatorname{Gal}(K/k)$. 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 $\lambda : F \to \overline{k}$ be an embedding. Then,*

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

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 $\sigma \in \operatorname{Gal}(K/F)$. It is not hard to see that $\lambda\sigma\lambda^{-1} \in \operatorname{Gal}(K/\lambda F)$ and conversely, for $\tau \in \operatorname{Gal}(K/\lambda F)$, $\lambda^{-1}\tau\lambda \in \operatorname{Gal}(K/F)$. This implies the desired conclusion. ∎

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

Proof. Suppose F/k is normal. To see that the map $\sigma \to \sigma|_F$ 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, $G/H \cong \operatorname{Gal}(F/k)$.

On the other hand, if F/k is not normal, then there is an embedding $\lambda : F \to \overline{k}$ such that $F \neq \lambda F$. Note that due to Theorem 2.5, $\lambda F \subseteq K$. Then, we have $\operatorname{Gal}(K/F) \neq \operatorname{Gal}(K/\lambda F) = \lambda \operatorname{Gal}(K/F)\lambda^{-1}$, and equivalently, $\operatorname{Gal}(K/F)$ 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 $G = \operatorname{Gal}(K/k)$. 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* $\mathrm{Gal}(E/k)$.

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 $H = \mathrm{Gal}(KF/F)$ and $G = \mathrm{Gal}(K/k)$. For all $\sigma \in H$, the restriction of σ to K is in G and the restriction map $\sigma \mapsto \sigma|_K$ gives an isomorphism of H on $\mathrm{Gal}(K/K \cap F)$. Finally, if F/k is Galois, then so are KF/k and $K \cap F/k$.*

Proof. That KF/F and $K/K \cap F$ are Galois follow from Theorem 3.6 and Theorem 4.15. 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 $\alpha \in K \cap F$. The conclusion follows from Theorem 7.9.

Now, suppose F/k is Galois. Then, due to Theorem 3.6, both KF and $K \cap F$ are normal over k whence are Galois. ■

7.1 Normal Basis Theorem

Definition 7.12 (Normal Element). Let K/k be a finite Galois extension with $\mathrm{Gal}(K/k) = \{\sigma_1, \ldots, \sigma_n\}$. An element $\alpha \in K$ is said to be a *normal element* if $\{\sigma_1(\alpha), \ldots, \sigma_n(\alpha)\}$ forms a k-basis of K.

Theorem 7.13 (Normal Basis Theorem). *If K/k is a finite Galois extension, then it has a normal element.*

Proof. Let $G = \mathrm{Gal}(K/k) = \{\sigma_1, \ldots, \sigma_n\}$. We shall divide the proof into two cases.

Case 1. G is cyclic.

Let $G = \langle\sigma\rangle$ for some $\sigma \in G$. Let $m_\sigma(x) \in k[x]$ denote the minimal polynomial of σ. Since σ is a root of $x^n - 1 \in k[x]$, we must have $m_\sigma(x) \mid x^n - 1$. If $\deg(m_\sigma) = m < n$, then there are $a_0, \ldots, a_m \in k$ such that

$$m_\sigma(x) = a_m x^m + \cdots + a_0.$$

In particular, $a_m\sigma^m + \cdots + a_0\mathbf{id} = 0$, but this is a contradiction to Dedekind's Lemma on the independence of characters. Therefore, $m_\sigma(x) = x^n - 1$, consequently, $m_\sigma(x)$ must also be the characteristic polynomial of σ due to a degree argument. Since the minimal polynomial and the characteristic polynomial are the same, there is a σ-cyclic vector for the extension K/k, which is the desired normal element.

Case 2. k is infinite. Note that the previous case subsumes the case with k finite.

Due to Theorem 4.18, $K = k(\alpha)$ for some $\alpha \in K$. Suppose without loss of generality that $\sigma_1 = \mathbf{id}$. Let $\alpha_i = \sigma_i(\alpha)$, which are all pairwise distinct, and define

$$g_i(x) = \frac{\prod_{j \neq i}(x - \alpha_j)}{\prod_{j \neq i}(\alpha_i - \alpha_j)}.$$

Denote g_1 by simply g, then, $g_i = \sigma_i(g)$.

The polynomial

$$g_1(x) + \cdots + g_n(x)$$

attains the value 1 for $\alpha_1, \ldots, \alpha_n$ but since it has degree at most $n-1$, it must be identically equal to 1. Further, for $i \neq j$, $f \mid g_i g_j$ and $g_i^2 - g_i$ vanishes at $\alpha_1, \ldots, \alpha_n$ whence $f \mid g_i^2 - g_i$.

Define the matrix

$$A(x) = \begin{bmatrix} \sigma_1\sigma_1(g) & \sigma_1\sigma_2(g) & \ldots & \sigma_1\sigma_n(g) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n\sigma_1(g) & \sigma_n\sigma_2(g) & \ldots & \sigma_n\sigma_n(g) \end{bmatrix}.$$

We contend that $\det A(x)$ is a nonzero polynomial. Suppose not. Consider $M(x) = A(x)^T A(x)$. The (i,j)-th entry is given by

$$\sum_{\sigma \in G} \sigma\sigma_i(g)\sigma\sigma_j(g) = \sum_{\sigma \in G} \sigma(g_i g_j).$$

If $i \neq j$, note that $f \mid \sigma(g_i g_j)$ for all $\sigma \in G$. Therefore, f divides all non-diagonal entries of $M(x)$ while the diagonal entries of $M(x)$ are given by

$$\sum_{\sigma \in G} \sigma(g_i)^2 \equiv \sum_{\sigma \in G} \sigma(g_i) \pmod{f} \equiv \sum_{i=1}^{n} g_i \pmod{f} \equiv 1 \pmod{f}.$$

Hence, $\det M(x) = 1$ in $K[x]/(f(x))$, in particular, it is nonzero in $K[x]$, therefore, $\det A(x) \neq 0$ in $K[x]$.

Since K is infinite, there is some $\theta \in K$ such that $\det A(\theta) \neq 0$. Let $\beta = g(\theta)$. We claim that β is the desired normal element. To do so, it suffices to show that $\{\sigma_1(\beta), \ldots, \sigma_n(\beta)\}$ is linearly independent over k.

Indeed, suppose there is a linear combination

$$c_1\sigma_1(\beta) + \cdots + c_n\sigma_n(\beta) = 0 \iff c_1\sigma_1(g(\theta)) + \cdots + c_n\sigma_n(g(\theta)) = 0.$$

Applying σ_i to the above equation for $1 \leq i \leq n$, we obtain a system of linear equations given by

$$A(\theta)\begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = 0,$$

whence $c_1 = \cdots = c_n = 0$, since $A(\theta)$ is invertible. This completes the proof. ■

Once we have a normal element, we can easily find the primitive (and sometimes normal) elements of all intermediate fields.

Theorem 7.14. *Let K/k be a finite Galois extension with $G = \mathrm{Gal}(K/k)$ and $\alpha \in K$ be a normal element.*

(a) If $H \leq G$, then $\beta_H := \mathrm{Tr}_{K^H}^{K}(\alpha)$ is a primitive element of K^H/k.

(b) If $H \trianglelefteq G$, then β_H is a normal element of K^H/k.

Proof. (a) Obviously, $\beta_H \in K^H$. We shall show that $\mathrm{Gal}(K/k(\beta_H)) \subseteq H$, which would imply $K^H \subseteq k(\beta_H)$ and the conclusion would follow.

Let $\tau \in G \backslash H$. Then,

$$\tau(\beta_H) = \sum_{\sigma \in \tau H} \sigma(\alpha).$$

Since τH is a coset distinct from H, they are disjoint and since the collection $\{\sigma(\alpha) \mid \sigma \in G\}$ is a linearly independent set, we cannot have $\tau(\beta_H) = \beta_H$, consequently, $\mathrm{Gal}(K/k(\beta_H)) \subseteq H$.

(b) Let $\tau_1, \ldots, \tau_m$ be elements of G whose images under the canonical projection $G \twoheadrightarrow G/H$ are all the elements of G/H. Note that this projection map is simply the restriction map from $\mathrm{Gal}(K/k)$ to $\mathrm{Gal}(k(\beta_H)/k)$. Suppose

$$c_1\tau_1(\beta_H) + \cdots + c_m\tau_m(\beta_H) = 0,$$

then,

$$0 = \sum_{i=1}^{m} c_i \left(\sum_{\sigma \in \tau_i H} \sigma(\alpha) \right).$$

By our choice of τ_i's, the cosets $\tau_i H$ and $\tau_j H$ are pairwise distinct, consequently, the sum written above is essentially of linearly independent elements, $\sigma(\alpha)$ where σ ranges over G. Therefore, $c_1 = \cdots = c_m = 0$. This completes the proof. ■

7.2 Galois Groups of Polynomials

Definition 7.15. Let $f(x) \in k[x]$ be a polynomial and k^a an algebraic closure containing k. Let f have roots $r_1, \ldots, r_n \in k^a$. Define the discriminant of f as

$$\mathrm{disc}(f) := \left(\prod_{i<j} (r_i - r_j) \right)^2.$$

The Galois group of f, denoted G_f is defined as $\mathrm{Gal}(k(r_1, \ldots, r_n)/k)$.

The group G_f permutes $\{r_1, \ldots, r_n\}$ whence it can be embedded in $\mathfrak{S}_n$. Henceforth, we shall identify G_f with its image under this embedding.

Proposition 7.16. $\mathrm{disc}(f) \in k$.

Proof. Since the Galois group permutes $\{r_i \mid 1 \le i \le n\}$, $\mathrm{disc}(f)$ is the fixed field of the action of the entire Galois group on $k(r_1, \ldots, r_n)$ which is k. ■

Theorem 7.17. *Let* $\mathrm{char}\, k \neq 2$ *and* $f(x) \in k[x]$ *a separable polynomial. Then,* $G_f \subseteq \mathfrak{A}_n$ *if and only if* $\mathrm{disc}(f)$ *is a perfect square in* k.

Proof. Let

$$\delta = \prod_{i<j} (r_i - r_j).$$

Then, for each $\sigma \in G_f$, $\sigma(\delta) = \mathrm{sgn}(\sigma)\delta$. Thus,

$$G_f \subseteq \mathfrak{A}_n \iff \sigma(\delta) = \delta \quad \forall \sigma \in G_f \iff \delta \in k.$$

This completes the proof. ■

Chapter 8

Cyclotomic Extensions

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

Consider the polynomial $x^n - 1$ with $\gcd(\operatorname{char} k, n) = 1$. In this case, the polynomial is separable over k and thus has distinct roots. Let $Z_n = \{z_1, \ldots, z_n\}$ denote the distinct roots. It is not hard to see that $Z_n \subseteq k^\times$ forms a multiplicative group. Since every finite multiplicative subgroup of a field is cyclic, so is Z_n. A generator for the group Z_n is called a **primitive n-th root of unity**. Obviously, there are $\varphi(n)$ such primitive n-th roots of unity.

Consider now the case $\gcd(\operatorname{char} k, n) \neq 1$. Let $\operatorname{char} k = p > 0$. Then, there is a positive integer r such that $n = p^r m$ with $p \nmid m$. Then,

$$x^n - 1 = \left(x^m - 1\right)^{p^r}$$

and thus every n-th root of unity is an m-th root of unity, whence it suffices to study polynomials of the form $(x^n - 1)$ with $\gcd(\operatorname{char} k, n) = 1$.

Proposition 8.2. *Every root of unity is a primitive n-th root of unity for some positive integer n.*

Proof. Let ζ be a root of unity and let n be the smallest positive integer such that $\zeta^n = 1$. Consider the subgroup $\langle \zeta \rangle \leq Z_n$. If the order of this subgroup is m, then $\zeta^m = 1$ whence $m \geq n$ and thus $m = n$ and the conclusion follows. ■

As a result, need only concern ourselves with primitive n-th roots of unity with $\gcd(\operatorname{char} k, n) = 1$.

Proposition 8.3. *Let k be a field and $\zeta_n \in k^a$ a primitive n-th root of unity such that* $\gcd(n, \operatorname{char} k) = 1$. *Then, $k(\zeta_n)/k$ is a Galois extension.*

Proof. Since ζ_n is a generator for Z_n, $k(\zeta_n)$ is the splitting field of $x^n - 1$ over k and thus a normal extension of k. Further, since $x^n - 1$ is a separable polynomial over k, so is the extension $k(\zeta_n)/k$ whence it is Galois. ■

Proposition 8.4. *Let* $\gcd(\operatorname{char} k, n) = 1$. *If ζ is a primitive n-th root of unity, then $k(\zeta)/k$ is an abelian extension.*

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

Note that although we have shown $\mathrm{Gal}(k(\zeta)/k)$ 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 $\mathrm{Gal}(k(\zeta)/k) \cong \{\pm 1\}$.

Proposition 8.5. *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 $\psi : \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times$ is an isomorphism.

Proof. ■

Chapter 9

Norm and Trace

Rewrite this chapter following what JKV taught

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

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

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

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

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

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

is the minimal polynomial of α over k, then

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

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

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

whence the conclusion follows. ■

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

$$N_k^E = N_k^F \circ N_F^E \qquad \mathrm{Tr}_k^E = \mathrm{Tr}_k^F \circ \mathrm{Tr}_F^E$$

Proof. First, we must show that N_k^E is a map $E^\times \to k^\times$ and Tr_k^E is a map $E \to k$. 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 $\sigma : k^a \to k^a$ 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 $k^a \to k^a$.

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 $\sigma : E \to k^a$ 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

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

$$[E : F]_i[F : k]_i \sum_{i,j} \tau_j \circ \sigma_i(\alpha) = [F : k]_i \sum_j \tau_j \left([E : F]_i \sum_i \sigma_i(\alpha)\right)$$

and the conclusion follows. ∎

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

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

Note that we may unambiguously write $\det(m_\alpha)$ and $\mathrm{tr}(m_\alpha)$ 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

10.1 Hilbert's Theorems

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

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

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

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

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

$$\sigma_1 + \cdots + \sigma_n = 0$$

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 $\{\mathbf{id}, \sigma, \dots, \sigma^{n-1}\}$ from $K^\times \to K^\times$. Then, due to Theorem 10.2, the set map

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

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

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

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

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

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

$\impliedby$ 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. ∎

Lemma 10.6. *Let K/k be a cyclic extension of degree n with $\mathrm{Gal}(K/k) = \langle\sigma\rangle$ and suppose k contains a primitive n-th root of unity, ζ. Then, ζ is an eigenvalue of σ.*

Proof. Note that $N_k^K(\zeta^{-1}) = 1$. Due to Theorem 10.4 there is $\alpha \in K$ such that $\alpha/\sigma(\alpha) = \zeta^{-1}$ and the conclusion follows. ∎

Theorem 10.7 (Structure of Cyclic Extensions). *Let K/k be a cyclic extension of degree n and suppose k contains a primitive n-th root of unity. Then, $K = k(\alpha)$ for some $\alpha \in K$ such that $\alpha^n \in k$.*

Proof. Let $\mathrm{Gal}(K/k) = \langle\sigma\rangle$. Due to Lemma 10.6, there is $\alpha \in K$ such that $\sigma(\alpha) = \zeta\alpha$. Then, α has n-distinct conjugates in K whence $K = k(\alpha)$. Now,

$$\sigma(\alpha^n) = \sigma(\alpha)^n = \alpha^n.$$

Thus, α^n is fixed under the action of $\mathrm{Gal}(K/k)$, that is, $\alpha^n \in k$. This completes the proof. ∎

Theorem 10.8 (Additive Hilbert's Theorem 90). *Let K/k be a cyclic Galois extension with $\mathrm{Gal}(K/k) = \langle\sigma\rangle$ and $\beta \in K$. Then $\mathrm{Tr}_k^K(\beta) = 0$ 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 $\mathrm{Tr}_k^K(\theta) \neq 0$. Consider $\alpha \in K$ given by

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

We have

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

The converse is trivial. ∎

Theorem 10.9 (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) *Conversely, if $a \neq b^p - b$ for some $b \in k$, and K is the splitting field of $f(x) = x^p - x - a \in k[x]$, then $f(x)$ is irreducible and K/k is cyclic of degree p.*

Proof. (a) Let $\operatorname{Gal}(K/k) = \langle \sigma \rangle$, since it is a group of prime order. We have $\operatorname{Tr}_k^K(-1) = p \cdot (-1) = 0$ 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, $a \in K^{\operatorname{Gal}(K/k)} = k$.

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) Let $\alpha \in K$ be a root of $f(x)$. Then, so is $\alpha + 1$. Hence, all the roots of $f(x)$ in K are given by

$$\{\alpha, \alpha + 1, \ldots, \alpha + p - 1\},$$

whence $K = k(\alpha)$. Suppose $f(x) = g_1(x) \cdots g_r(x)$ where $g_1, \ldots, g_r \in k[x]$ are irreducible polynomials. If r is a root of some g_i, then r is a root of f and thus $K = k(r)$. In particular, $\deg g_i = [K : k]$. This gives us $r \deg g_1 = p$ and since $f(x)$ does not have a root in k, we must have $r = 1$ and $\deg g_1 = p$. That is, $f(x)$ is irreducible.

Finally, $\operatorname{Gal}(K/k) = \langle \sigma \rangle$ where $\sigma(\alpha) = \alpha + 1$. This completes the proof. ■

10.1.1 Lagrange Resolvents

Let $p > 0$ be a prime number and k a field such that $\operatorname{char} k = 0$ or $\gcd(\operatorname{char} k, p) = 1$. Suppose further, that $\mu_p \subseteq k$, that is, k contains a primitive p-th root of unity. Now let K/k be a cyclic extension of order p. Using Theorem 10.7, there is some $a \in k$ such that $K = k(\sqrt[p]{a})$. We shall explicitly find such an $a \in k$.

Let $\alpha \in K$ be primitive for the extension K/k and $\operatorname{Gal}(K/k) = \langle \sigma \rangle$. If $m_\alpha(x)$ is the minimum polynomial of α over k, then the roots of m_α are given by $\{\alpha, \sigma(\alpha), \ldots, \sigma^{p-1}(\alpha)\}$ and of course, are distinct. Let $\mu_p = \{z_1, \ldots, z_p\} \subseteq k$. Define

$$(z_i, \alpha) := \sum_{j=0}^{p-1} \sigma^j(\alpha) z_i^j.$$

These are called the *Lagrange Resolvents*.

Then,

$$\begin{bmatrix} (z_1, \alpha) \\ \vdots \\ (z_p, \alpha) \end{bmatrix} = \underbrace{\begin{bmatrix} 1 & z_1 & \ldots & z_1^{p-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & z_p & \ldots & z_p^{p-1} \end{bmatrix}}_{V(z_1, \ldots, z_p)} \begin{bmatrix} \alpha \\ \vdots \\ \sigma^{p-1}(\alpha) \end{bmatrix}.$$

The Vandermonde determinant, $\det V(z_1, \ldots, z_p)$ is nonzero and hence, the matrix is invertible. Note that

$$\sigma((z_i, \alpha)) = z_i^{-1}(z_i, \alpha),$$

whence (z_i, α) is an eigenvector corresponding to the eigenvalue z_i^{-1}. In particular, $(z_i, \alpha)^p$ is invariant under σ and thus lies in the base field k. This shows that $K = k((z_i, \alpha))$.

10.2 Solvability by Radicals

Definition 10.10. An extension K/k is said to be *radical* if there is a tower

$$k = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n = K$$

where F_{i+1}/F_i is obtained by adjoining an n_i-th root of an element in F_i. Each F_{i+1}/F_i is called a *simple radical extension*.

Definition 10.11. A polynomial $f(x) \in k[x]$ is said to be *solvable by radicals* if any splitting field K of f over k is contained in a radical extension of k.

Lemma 10.12. *Let E/k be a finite separable radical extension. Then, the normal closure, K of E is a radical Galois extension.*

Proof. Fix some algebraically closed field k^a containing k and let

$$k = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_m = E$$

be a tower of simple radical extensions. Let $\{\mathbf{id} = \sigma_1, \ldots, \sigma_n\}$ be the distinct k-embeddings of E/k into k^a. Then, note that $\sigma_j(F_{i+1})/\sigma_j(F_i)$ is also a simple radical extension. Thus, we have a tower of successive simple radical extensions

$$k = \sigma_1(F_0) \subseteq \cdots \subseteq \sigma_1(F_m) \subseteq \sigma_1(F_m)\sigma_1(F_0) \subseteq \cdots \subseteq \sigma_1(F_m)\ldots\sigma_n(F_m) = K.$$

This completes the proof. ■

Theorem 10.13 (Galois). *Let $\operatorname{char} k = 0$ and $f(x) \in k[x]$. Then, $f(x)$ is solvable by radicals over k if and only if G_f is a solvable group.*

Proof. $\implies$ Let K be the splitting field of f over k, which is contained in a radical extension E. Due to Lemma 10.12, we may suppose that E/k is Galois. There is a tower of extensions

$$k = F_0 \subseteq \cdots \subseteq F_r = E.$$

with $F_{i+1} = F_i\left(\sqrt[n_{i+1}]{a_{i+1}}\right)$. Let $n = n_1 \cdots n_r$ and ζ a primitive n-th root of unity. Note that $E(\zeta) = E \cdot k(\zeta)$, a compositium of two Galois extensions over k whence is a Galois extension of k. Denote by $M_i = F_i(\zeta)$. Then, we have

$$k \subseteq M_0 \subseteq \cdots \subseteq M_r = E(\zeta).$$

Note that M_i contains a primitive n_{i+1}-th root of unity (which is a suitable power of ζ) whence $\operatorname{Gal}(M_{i+1}/M_i)$ is cyclic. Consider the chain of subgroups

$$\operatorname{Gal}(M_r/k) \supseteq \operatorname{Gal}(M_r/M_0) \supseteq \cdots \supseteq \operatorname{Gal}(M_r/M_{r-1}) \supseteq \{1\}.$$

Each successive quotient is

$$\operatorname{Gal}(M_r/M_i)/\operatorname{Gal}(M_r/M_{i+1}) \cong \operatorname{Gal}(M_{i+1}/M_i) \quad \text{and} \quad \operatorname{Gal}(M_r/k)/\operatorname{Gal}(M_r/M_0) \cong \operatorname{Gal}(M_0/k),$$

all of which are abelian. Thus, $\operatorname{Gal}(M_r/k)$ is solvable, consequently,

$$G_f = \operatorname{Gal}(K/k) \cong \operatorname{Gal}(M_r/k)/\operatorname{Gal}(M_r/K),$$

is solvable.

$\Longleftarrow$ Let $|G_f| = n$ and ζ a primitive n-th root of unity in k^a. Let $L = K(\zeta)$ and $E = k(\zeta)$. Then, L/E is a Galois extension with Galois group isomorphic to a subgroup of $\mathrm{Gal}(K/k)$, in particular, $\mathrm{Gal}(L/E)$ is solvable. Thus, there is a series

$$\mathrm{Gal}(L/E) = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_m = \{1\}$$

with H_i/H_{i+1} abelian. Let $F_i = L^{H_i}$. This gives a filtration

$$E = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_m = L$$

wherein each extension F_{i+1}/F_i is abelian with degree n_i dividing n. Let $\mathrm{Gal}(F_{i+1}/F_i) = P$, an abelian group whence, due to the structure theorem, admits a filtration

$$P = Q_0 \supseteq Q_1 \supseteq \cdots \supseteq Q_r = \{1\}.$$

such that Q_i/Q_{i+1} is cyclic. Let $S_i = P^{Q_i}$. Then, we have a filtration

$$F_i = S_0 \subseteq S_1 \subseteq \cdots \subseteq S_r = F_{i+1}$$

where each extension S_{j+1}/S_j is cyclic with order dividing n. But since S_j contains a primitive n-th root of unity, the extension S_{j+1}/S_j must be a simple radical extension. In particular, F_{i+1}/F_i is a radical extension. Consequently, L/E is a radical extension. Finally, E/k itself is a simple radical extension and hence, L/k is a radical extension containing K/k. This completes the proof. ■

10.3 Kummer Extensions

Definition 10.14. A finite algebraic extension K/k is said to be a *Kummer extension* if $\mu_n \subseteq F$, there is $n \in \mathbb{N}$ and $a_i \in k$ for $1 \leq i \leq m$ such that $K = k(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_m})$. A Kummer extension is said to be a *simle Kummer extension* if $m = 1$.

Theorem 10.15. *Let $\mu_n \subseteq k$ and $a \in k^\times$. Let $b \in k^a$ such that $b^n = a$. Then, $\mathrm{Gal}(k(b)/k)$ is cyclic of order $|\overline{a}|$ where $\overline{a}$ is the coset of a in $k^\times/(k^\times)^n$.*

Proof. ■

Remark 10.3.1. *Due to Theorem 10.7, every simple Kummer extension K/k with $[K : k] = m$ can be obtained by adjoining th m-th root of some element in k. This makes our analysis a lot easier.*

Lemma 10.16. *Let $\mu_n \subseteq k$ and $a, b \in k^\times$ such that $[k(\sqrt[n]{a}) : k] = [k(\sqrt[n]{b}) : k] = n$. Then, these extensions are k-isomorphic if and only if $\langle \overline{a} \rangle = \langle \overline{b} \rangle$ in $k^\times/(k^\times)^n$.*

Proof. ■

Theorem 10.17. *Let K/k be a finite abelian extension and suppose that $\mu_n \subseteq k$. Then, $\mathrm{Gal}(K/k)$ has exponent n if and only if there are $b_1, \ldots, b_m \in k^\times$ such that $K = k(\sqrt[n]{b_1}, \ldots, \sqrt[n]{b_m})$.*

Proof. $\Longrightarrow$ Due to the structure thoerem, $\text{Gal}(K/k) \cong \mathbb{Z}/n_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_r\mathbb{Z}$ where $n_i \mid n$. Let H_i denote the subgroup corresponding to

$$\mathbb{Z}/n_1\mathbb{Z} \oplus \cdots \oplus \widehat{\mathbb{Z}/n_i\mathbb{Z}} \oplus \cdots \oplus \mathbb{Z}/n_r\mathbb{Z}$$

and $F_i = K^{H_i}$. Then, $\bigcap_{i=1}^r H_i = \{1\}$ and $\text{Gal}(F_i/k) \cong \mathbb{Z}/n_i\mathbb{Z}$. Due to Theorem 10.7, there is some $b_i \in k^\times$ such that $F_i = k(\sqrt[n]{b_i})$. Finally, since $K = F_1 \cdots F_r$, the conclusion follows.

$\Longleftarrow$ Let $F_i = k(\sqrt[n]{b_i})$. Then, $\text{Gal}(F_i/k)$ is cyclic of exponent n. Let $\rho_i : \text{Gal}(K/k) \twoheadrightarrow \text{Gal}(F_i/k)$ denote the restriction map. It is not hard to see that the map $\Phi : \text{Gal}(K/k) \to \prod_{i=1}^m \text{Gal}(F_i/k)$ given by $\Phi = \rho_1 \times \cdots \times \rho_m$ is an injection and thus $\text{Gal}(K/k)$ is abelian of exponent n. This completes the proof. ■

Chapter 11

Infinite Galois Theory

11.1 Galois Groups as Inverse Limits

11.1.1 Inverse Limit of Topological Groups

Lemma 11.1. *Let G be a compact topological group. Then, $H \leq G$ is open if and only if it is closed with finite index.*

Proof. Since G is compact, the number of cosets of H in G must be finite else we would have an infinite open cover of G with no finite subcover. Further, H is the complement of a disjoint union of cosets of H and hence, is closed, since every coset of H in G is open.

Conversely, if $H, \sigma_1 H, \ldots, \sigma_n H$ are the distinct cosets of H in G, then $H = G \backslash (\sigma_1 H \cup \cdots \cup \sigma_n H)$, and thus, is open. ■

11.1.2 Profinite Groups

Definition 11.2 (Profinite Group). A profinite group is a topological group that is isomorphic to an inverse limit of finite topological groups with the discrete topology.

The *profinite completion* of a topological group G is defined as $\widehat{G} = \varprojlim G/N$ where N ranges over the set of all open normal subgroups of finite index in G. If no topology is specified on the group, then $\widehat{G}$ refers to the profinite completion of G with the discrete topology.

Remark 11.1.1. *Note that if N is an open normal subgroup of a topological group G, then G/N has the discrete topology even if G is not Hausdorff.*

Theorem 11.3. *A profinite group is a compact Hausdorff topological group.*

Proof. ■

Theorem 11.4. *Let G be a topological group. Let $\phi : G \to \widehat{G}$ denote the natural map. Then, the image of ϕ is dense in $\widehat{G}$. If G is a profinite group, then ϕ is an isomorphism of topological groups.*

Proof. Let $X = \prod G/N$, which is a compact topological group containing $\widehat{G}$. Let U be a basic open set in X. ■

11.1.3 The Galois Group

We shall now show that every profinite group occurs as a Galois group. In order to do so, we shall require the following analogue of Artin's Theorem for profinite groups.

Theorem 11.5. *Let G be a profinite group acting faithfully by automorphisms on a field K such that for each $x \in K$, $\operatorname{stab}_G(x)$ is an open subgroup of G. Then, K/K^G is Galois with group G.*

Proof. ■

Theorem 11.6 (Waterhouse). *Let G be a profinite group. Then, it is the Galois group of some field extension.*

Proof. Let $\mathcal{H}$ denote the set of all open subgroups of G. Define

$$X = \bigsqcup_{H \in \mathcal{H}} G/H$$

and let G act on X through left multiplication on cosets. This action is faithful and every element of X has an open stabilizer in G. Let $K = \mathbb{Q}(X)$ and extend the action of G on X to an action by field automorphisms on K. Due to Theorem 11.5, $G \cong \operatorname{Gal}(K/K^G)$. ■

11.2 The Krull Topology

Definition 11.7. 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 Galois** extension.

Proposition 11.8. *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 Galois, 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 the basic open set $\sigma \operatorname{Gal}(K/F_1F_2)$ 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 11.9. *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 Galois extension F/k. 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. 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 11.10. $\text{Gal}(K/k)$ *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 be the normal closure of $k(\alpha)$ in K, which is a finite Galois extension, and note that $\sigma \text{Gal}(K/F) \neq \tau \text{Gal}(K/F)$ and thus must be disjoint (since they are cosets). ■

Proposition 11.11. *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 11.12. *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. ■

Theorem 11.13 (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 an closed subgroups of $\text{Gal}(K/k)$.

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

Proof. (a) and (b) follow from the previous two propositions. From this, the Galois correspondence is immediate. Finally to see (d), suppose $H \leq G$. Then, $\text{Gal}(K/K^H) = \overline{H}$, whence

$$K^H = K^{\text{Gal}(K/K^H)} = K^{\overline{H}}.$$

This completes the proof. ■

Theorem 11.14. $\text{Gal}(K/k)$ *in the Krull Topology is isomorphic, as topological groups to the inverse limit* $G = \varprojlim \text{Gal}(E/k)$ *as a subspace of* $X = \prod \text{Gal}(E/k)$*, each of which is given the discrete topology.*

In particular, $\text{Gal}(K/k)$ *in the Krull Topology is a profinite group.*

Proof. Define the map $\Phi : \mathrm{Gal}(K/k) \to X$ by $\Phi(\sigma) = (\sigma|_E)_E$. This is obviously an injective map whose image is G. To see that this is a continuous map, it suffices to check that each component of this map is continuous. Let E/k be a finite Galois extension. The component of Φ along E is given by $\Phi_E : \mathrm{Gal}(K/k) \to \mathrm{Gal}(E/k)$, which is the restriction map. A basic open set in $\mathrm{Gal}(E/k)$ is simply a point, say $\sigma \in \mathrm{Gal}(E/k)$. Then, $\Phi_E^{-1}(\sigma) = \tau\,\mathrm{Gal}(K/E)$ where τ is a k-automorphism of K whose restriction to E is σ. This is obviously an open set in $\mathrm{Gal}(K/k)$ whence Φ is continuous.

Lastly, we must show that Φ is an open map with respect to G, for which, it suffices to show that the image of a basic open set in $\mathrm{Gal}(K/k)$ is open in G. Consider the basic open set $\sigma\,\mathrm{Gal}(K/E)$ where E/k is a finite Galois extension. Then,

$$\Phi\left(\sigma\,\mathrm{Gal}(K/E)\right) = \left(\{\sigma_E\} \times \prod_{\substack{F \neq E \\ F/k \text{ is finite Galois}}} \mathrm{Gal}(F/k)\right) \cap G,$$

which is open in G. This completes the proof. ■

Corollary 11.15. $\mathrm{Gal}(K/k)$ is compact in the Krull topology.

Chapter 12

Transcendental Extensions

Definition 12.1 (Algebraically Independent). Let K/k be any extension. Elements $a_1, \ldots, a_n \in K$ are said to be *algebraically independent over k* if there is no non-zero polynomial $f(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]$ such that $f(a_1, \ldots, a_n) = 0$. A set $A \subseteq K$ is said to be algebraically independent over k if every finite subset of A is algebraically independent over k.

Lemma 12.2. *Let K/k be any extension $a \in K$ and $A \subseteq K$. The following are equivalent:*

(a) $a \in K$ *is algebraic over* $k(A)$.

(b) *There are* $\beta_0, \ldots, \beta_{n-1} \in K(A)$ *such that* $a^n + \beta_{n-1}a^{n-1} + \cdots + \beta_0 = 0$.

(c) *There are* $\beta_0, \ldots, \beta_n \in k[A]$ *such that* $\beta_n a^n + \cdots + \beta_0 = 0$.

(d) *There is a non-zero polynomial* $f(x_1, \ldots, x_m, y) \in k[x_1, \ldots, x_m, y]$ *such that there are* $b_1, \ldots, b_m \in A$ *with* $f(b_1, \ldots, b_m, y) \neq 0$ *in* $K[y]$ *but* $f(b_1, \ldots, b_m, a) = 0$.

Proof. Trivial. ■

Lemma 12.3 (Exchange Lemma). *Let K/k be any extension and $b \in K$ be algebraically dependent on $\{a_1, \ldots, a_m\} \subseteq K$ but not on $\{a_1, \ldots, a_{m-1}\}$. Then, a_m is algebraically dependent on $\{a_1, \ldots, a_{m-1}, b\}$.*

Proof. Since b is algebraically dependent on $\{a_1, \ldots, a_m\}$, there is a non-zero polynomial $f(x_1, \ldots, x_m, y) \in k[x]$ such that $f(a_1, \ldots, a_m, b) = 0$. Then, we may write

$$f(x_1, \ldots, x_m, y) = \sum_i f_i(x_1, \ldots, x_{m-1}, y)x_m^i.$$

Since b is not algebraically dependent on $\{a_1, \ldots, a_{m-1}\}$, one of the f_i's must be non-zero, say f_j. Thus, a_m is algebraically dependent over $\{a_1, \ldots, a_{m-1}, b\}$. ■

Definition 12.4. Let K/k be any extension. An algebraically independent subset $A \subseteq K$ is said to be a *transcendence basis* if $K/k(A)$ is algebraic.

Theorem 12.5. *Let K/k be any field extension and $A, B \subseteq K$ be two transcendence bases. Then, $|A| = |B|$.*

Proof. First, suppose A is finite. Let $A = \{a_1, \ldots, a_n\}$. Then, for every $a_i \in A$, there is a finite subset B_i of B such that a_i is algebraically dependent on $k(B_i)$. Therefore, K is algebraic over $k(B_1 \cup \cdots \cup B_n)$. Hence, B must be finite. Say $B = \{b_1, \ldots, b_m\}$.

Let $l = |A \cap B|$ and without loss of generality, say $A \cap B = \{a_1, \ldots, a_l\}$, thus, $B = \{a_1, \ldots, a_l, b_{l+1}, \ldots, b_n\}$. If $l = n$, then $A \subseteq B$ and we have $n \leq m$. Suppose not, that is, $l < n$.

Now, a_{l+1} is algebraic over B but algebraic independent over $\{a_1, \ldots, a_l\}$. Let j be the smallest index such that a_{l+1} is algebraically dependent over $\{a_1, \ldots, a_l, b_{l+1}, \ldots, b_j\}$. Due to Lemma 12.3, we see that b_j is algebraically dependent over

$$B_1 = \{a_1, \ldots, a_l, a_{l+1}, b_{l+1}, \ldots, b_{j-1}, b_{j+1}, \ldots, b_m\}.$$

Note that B_1 is algebraically independent, for if not, then we must have a_{l+1} algebraically dependent over $B_1 \backslash \{a_{l+1}\}$. But this would mean that $B_1 \backslash \{a_{l+1}\}$ is a transcendence basis of K/k, which is absurd. Hence, B_1 is algebraically independent and thus, a transcendence basis of K/k. Now, $|A \cap B_1| = l + 1$.

We may continue this process and at each step increase the size of the intersection $|A \cap B_i|$. The process terminates when $A \backslash B_i = \varnothing$, in other words, $A \subseteq B_i$ whence $n = |A| \leq |B_i| = m$. Arguing in the other direction, one can show that $m \leq n$, whence $m = n$. This proves the theorem in the finite case.

Now, suppose both A and B are infinite. Then, for each $a \in A$, there is a corresponding finite subset $B_a \subseteq B$ such that a is algebraically dependent on B_a. Therefore, every element of A is algebraically dependent over $C = \bigcup_{a \in A} B_a \subseteq B$. This means that K is algebraic over $k(C)$ and hence, $C = B$. Consequently,

$$|B| = |C| = \left| \bigcup_{a \in A} B_a \right| \leq |A \times \mathbb{N}| = |A|.$$

A similar argument in the other direction would give $|A| \leq |B|$. This completes the proof. ■

Definition 12.6 (Transcendence Degree). Let K/k be any extension. The *transcendence degree* of K/k, denoted $\operatorname{trdeg}(K/k)$ is the cardinality of a transcendence basis of K/k.

Remark 12.0.1. *Let K/k be any extension and $A \subseteq K$ be an algebraically independent subset of K. Let Σ be the poset of all algebraically independent subsets of K that contain A. Using a standard Zorn argument, one can show that Σ contains a maximal element, which obviously must be a transcendence basis.*

Theorem 12.7 (Additivity of trdeg). *Let $k \subseteq E \subseteq K$ be a tower of field extensions with $\operatorname{trdeg}(K/E)$ and $\operatorname{trdeg}(E/k)$ finite. Then, $\operatorname{trdeg}(K/k) = \operatorname{trdeg}(K/E) + \operatorname{trdeg}(E/k)$.*

Proof. ■

12.1 Lüroth's Theorem

Lemma 12.8. *Let x be an indeterminate over a field k and $r(x) \in k(x)$. Then, $[k(x) : k(r(x))] = \deg(r(x))$.*

Proof. ■

Theorem 12.9. $\text{Aut}(k(x)/k) \cong \text{PGL}_2(k)$.

Proof. If $\theta : k(x) \to k(x)$ is a k-automorphism, then $\deg(\theta(x)) = 1$ and hence, must be of the form $\frac{ax+b}{cx+d}$ where $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}_2(k)$. The conclusion now follows from an application of the First Isomorphism Theorem. ■

Theorem 12.10 (Lüroth's Theorem). *Let $k(t)/k$ be a purely transcendental extension. Then, any intermediate field strictly containing k is of the form $k(r(t))$ where $r(t) \in k(t)$ is a rational function. Further, $[k(t) : k(r(t))] = \deg(r(t))$.*

Proof. ■

12.2 Linear Disjointness

Definition 12.11 (Linearly Disjoint). Let K and L be two field extensions of k contained in a larger field Ω. Then, K and L are said to be *linearly disjoint* if every k-linearly independent subset of K is L-linearly independent as elements of Ω.

Proposition 12.12. *K and L are linearly disjoint over k if and only if L and K are linearly disjoint over k.*

Proof. Suppose K and L are linearly disjoint but not L and K. Then, there is a k-linearly independent subset $\{y_1, \ldots, y_n\}$ of L that is not K-linearly independent. Hence, there are $x_i \in K$, not all zero, such that $\sum_{i=1}^n x_i y_i = 0$. The vector space generated by the x_i's is a finite dimensional one over k and admits a finite basis, $u_1, \ldots, u_m$. We may write

$$x_i = \sum_{j=1}^m a_{ij} u_j$$

with $a_{ij} \in k$ and hence,

$$0 = \sum_{i=1}^n x_i y_i = \sum_{i=1}^n \sum_{j=1}^m a_{ij} y_i u_j = \sum_{j=1}^m \left(\sum_{i=1}^n a_{ij} y_i \right) u_j.$$

Using the linear disjointness of K and L, we must have $\sum_{i=1}^n a_{ij} y_i = 0$ for all j. But since the y_i's are linearly independent over k, we must have $a_{ij} = 0$ for all i, j. A contradiction. ■

Henceforth, we shall tacitly assume that all pairs of field extensions are contained in a larger field extension Ω/k.

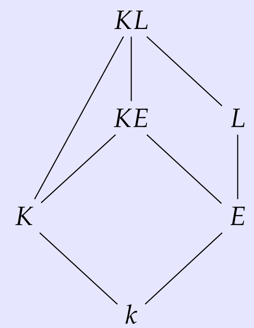
Proposition 12.13. *Let $k \subseteq R$ be a domain with $K = Q(R)$ and $\{u_\alpha\} \subseteq R$ be a k-basis of R. If $\{u_\alpha\}$ is L-linearly independent, then K and L are linearly disjoint.*

Proof. Suppose not, then there are $x_1, \ldots, x_n \in K$ that are k-linearly independent but not L-linearly independent. Hence, there is a linear combination $\sum_{i=1}^n z_i x_i = 0$ where $z_i \in L$. There is an $r \in R$ such that $r x_i \in R$ for each $1 \le i \le n$. Note that the $r x_i$'s still remain k-linearly independent. Thus, we may suppose that every $x_i \in R$.

The k-vector subspace of R generated by the x_i's is contained in a k-vector space V generated by finitely many $\{u_j\}_{j=1}^m \subseteq \{u_\alpha\}$. Obviously, $n < m$. Hence, the set $\{x_i\}_{i=1}^n$ can be completed to a basis of V, $\{x_1, \dots, x_n, x_{n+1}, \dots, x_m\}$.

Let W denote the L-vector space generated by $\{u_i\}_{i=1}^m$. We have $\dim W = m$ and that $\{x_1, \dots, x_m\}$ is a generating set for W and hence, forms a basis. Consequently, $x_1, \dots, x_n$ is linearly independent over L. This completes the proof. ■

Theorem 12.14 (Transitivity of Linear Disjointness). *Consider the following lattice of fields.*



Then, K, L are linearly disjoint over k if and only if K, E are linearly disjoint over k and KE, L are linearly disjoint over E.

Proof. ■

Proposition 12.15. *Suppose K/k is separable and L/k is purely inseparable with* $\operatorname{char} k = p > 0$. *Then, K and L are linearly disjoint over k.*

Proof. Suppose not, then there is a finite k-linearly independent subset X of K that is not L-linearly independent. We may now replace K by $K(X)$ and suppose that K/k is a finite separable extension and hence, admits a primitive element, $K = k(\alpha)$. A basis for K/k is then given by $\{1, \alpha, \dots, \alpha^{n-1}\}$. Let $f(x)$ be the irreducible polynomial of α over k. We contend that $f(x)$ is the irreducible polynomial of α over L.

Let $g(x) \in L[x]$ be the irreduible polynomial of k. Then, there is a non-negative integer m such that $g(x)^{p^m} \in k[x]$. Since α is a root of $g(x)$ and $f(x)$, there is a positive integer r such that $f(x) = g(x)^r h(x)$ for some $h(x) \in L[x]$ such that $\gcd(g, h) = 1$. But since f is separable, we must have $r = 1$ and $f(x) = g(x)h(x)$. Further, $g(x)^{p^m} = f(x)q(x)$ for some $q(x) \in k[x]$ and hence, $g(x)^{p^m - 1} = h(x)q(x)$. Since $\gcd(g, h) = 1$, we must have $h(x) = 1$, consequently, $g(x) = f(x)$.

This shows that $\{1, \alpha, \dots, \alpha^{n-1}\}$ is linearly independent over L and hence, K and L are linearly disjoint. ■

Proposition 12.16. *Let K/k be purely transcendental and L/k purely inseparable with* $\operatorname{char} k = p > 0$. *Then, K and L are linearly disjoint.*

Proof. Let $K = k(X)$ where X is a set of k-algebraically independent elements. Let $R = k[X]$ and note that the monomials formed from X form a k-basis for R and it suffices to show that these are linearly independent over L. Suppose there were a relation $\sum_i a_i X^{\alpha_i} = 0$ where $a_i \in L$. Since this is a finite sum, there is a positive integer m such that $a_i^{p^m} \in k$ for all i.

Raising the aforementioned relation to the power p^m, we have

$$\sum_i a_i^{p^m} X^{p^m \cdot \alpha_i} = 0.$$

Thus, $a_i^{p^m} = 0$ for all i. And the conclusion follows. ■

Definition 12.17 (Separably Generated). An extension K/k is said to be *separably generated* if it has a transcendence bais $S \subseteq K$ such that $K/k(S)$ is separable. Such a transcendence basis is called a *separating transcendence basis*.

Remark 12.2.1. *If K/k is separably generated, it is not necessary that every transcendence basis is a separating transcendence basis. For example, consider the extension $\mathbb{F}_p(x)/\mathbb{F}_p$. This has a separating transcendence basis $\{x\}$. Also, $\{x^p\}$ is a transcendence basis but $\mathbb{F}_p(x)/\mathbb{F}_p(x^p)$ is purely inseparable.*

Theorem 12.18 (McLane). *Let* $\operatorname{char} k = p > 0$ *and K/k any extension. Then, the following are equivalent:*

(a) K is linearly disjoint from $k^{p^{-\infty}}$.

(b) K is linearly disjoint from $k^{p^{-n}}$ for some positive integer n.

(c) K is linearly disjoint from $k^{p^{-1}}$.

(d) Any finitely generated subfield of K/k is separably generated.

Proof. $(a) \implies (b) \implies (c)$ is clear.

$(c) \implies (d)$ Let $A = \{a_1, \ldots, a_n\} \subseteq K$ and $E = k(A) \subseteq K$. If A is algebraically independent over k, then we are done by taking A to be a transcendence basis.

Suppose A is not algebraically independent and choose $0 \neq f \in k[x_1, \ldots, x_n]$ to be of smallest degree such that $f(a_1, \ldots, a_n) = 0$. Suppose that every monomial in f is a power of p. Then, there are monomials $m_\alpha(x) \in k[x_1, \ldots, x_n]$ such that

$$f(X) = \sum_\alpha a_\alpha m_\alpha(X)^p,$$

where not all a_α's are zero. Hence, there is a $g(X) \in k^{p^{-1}}[x_1, \ldots, x_n]$ such that $f(X) = g(X)^p$. Denote

$$g(X) = \sum_\alpha a_\alpha^{1/p} m_\alpha(\vec{a}).$$

The elements $m_\alpha(\vec{a})$ are linearly dependent over $k^{p^{-1}}$ and hence, are linearly dependent over k. Consequently, there exist $b_\alpha \in k$ such that

$$\sum_\alpha b_\alpha m_\alpha(\vec{a}) = 0.$$

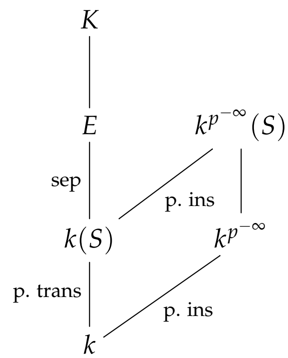
Set $h(X) = \sum_\alpha b_\alpha m_\alpha(X) \in k[X]$. Then, $h(\vec{a}) = 0$, which contradicts the minimality of the degree of f.

Hence, in f, there is a monomial that is not a power of p. Without loss of generality, suppose that monomial contains x_1 whose exponent is not a power of p. Then, consider the polynomial $f_0(x_1) \in k[a_2, \ldots, a_n][x_1]$ given by

$$f_0(x_1) = f(x_1, a_2, \ldots, a_n).$$

Note that $f_0(a_1) = 0$ and $f_0'(x_1)$ is a non-zero polynomial which cannot have a_1 as a root, lest we contradict the minimality of the degree of f. Hence, a_1 is separable over $k[a_2, \ldots, a_n]$. Now, induct downwards.

$(d) \implies (a)$ Let $a_1, \ldots, a_n \in K$ be k-linearly independent and set $E = k(a_1, \ldots, a_n)$. This is a finitely generated subfield of K/k and hence, has a separating transcendence basis $S \subseteq k(a_1, \ldots, a_n)$. Since $k(S)$ is purely transcendental and $k^{p^{-\infty}}$ is purely inseparable, they are linearly disjoint over k.



Next, since $k^{p^{-\infty}}(S)/k(S)$ is purely inseparable and $E/k(S)$ is separable, they are linearly disjoint over $k(S)$. Thus, due to Theorem 12.14, E and $k^{p^{-\infty}}$ are linearly disjoint over k.

Since every finitely generated subfield of K is linearly disjoint from $k^{p^{-\infty}}$ over k, we must have that K is linearly disjoint from $k^{p^{-\infty}}$ over k. This completes the proof. ■

Definition 12.19 (Separable). An extension K/k that satisfies the equivalent statements of Theorem 12.18 is said to be *separable*.

Theorem 12.20. *Let* $\operatorname{char} k = p$ *and* $k \subseteq E \subseteq K$ *be a tower of fields.*

(a) If K/k is separable, then E/k is separable.

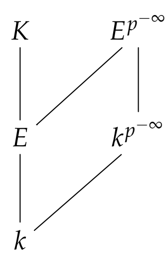
(b) If K/E and E/k are separable, then K/k is separable.

(c) If k is perfect, then any extension of k is separable.

(d) If K/k is separable and E/k is algebraic, then K/E is separable.

Proof. (a) follows from the fact that any finitely generated subextension of E is a finitely generated subextension of K.

(b) We have the following lattice of fields.



According to the hypothesis, K and $E^{p^{-\infty}}$ are linearly disjoint over E and E and $k^{p^{-\infty}}$ are linearly disjoint over k. Note that the compositum $Ek^{p^{-\infty}}$ is contained in $E^{p^{-\infty}}$ whence K and $Ek^{p^{-\infty}}$ are linearly disjoint over k. From Theorem 12.14, we have that K and $k^{p^{-\infty}}$ are linearly disjoint over k.

(c) Clear.

(d) Let $F = E(a_1, \ldots, a_n) \subseteq K$ be a finitely generated subextension of K/E and set $L = k(a_1, \ldots, a_n)$. This has a separating transcendence basis $S \subseteq L$. Then, $F/E(S)$ is separable. Hence, it suffices to show that S is algebraically independent over E.

Since $F/E(S)$ is algebraic and $E(S)/k(S)$ is algebraic, we have $\operatorname{trdeg}(F/k) = |S|$. Hence, $\operatorname{trdeg}(F/E) = \operatorname{trdeg}(F/k) - \operatorname{trdeg}(E/k) = |S|$. Hence, S must be a transcendence basis of F/E. This completes the proof. ∎

Definition 12.21 (Free). The pair of extensions $(K/k, L/k)$ is said to be *free* if every k-algebraically independent subset of K is L-algebraically independent.

Proposition 12.22. *If $(K/k, L/k)$ is free, then so is $(L/k, K/k)$.*

Proof. ∎

12.3 A Brief Treatment of Varieties

Throughout this section, k is an arbitrary field and K, an algebraic closure of k.

12.3.1 Parametrization

Definition 12.23. An irreducible k-variety V is called *rational* if the function field $k(V)$ is a purely transcendental extension of k.

Definition 12.24. A *curve* is an irreducible k-variety that has dimension 1. Equivalently, $\dim k[V] = 1$. We say that V can be *parametrized* by rational functions in $k(t)$ if there are rational functions $f_1, \ldots, f_n \in k(t)$ such that

$$\{(f_1(t), \ldots, f_n(t)) \mid t \in K\},$$

wherever defined, is a dense subset of V in the k-Zariski topology.

Theorem 12.25. *Let V be an irreducible curve defined over a field k. Then, V can be parametrized by rational functions in $k(t)$ if and only if there is an k-isomorphism $k(V) \cong k(t)$.*

Proof. ($\Longrightarrow$) Suppose we have a parametrization given by $(f_1(t), \ldots, f_n(t))$ where $f_i(t) \in k(t)$. Let

$$U = \{(f_1(a), \ldots, f_n(a)) \mid a \in K\}.$$

Then, $\overline{U} = V$ in the k-Zariski topology. Consier the ring homomorphism $\varphi : k[X] \to k(t)$ given by $\varphi(X_i) = f_i(t)$. Note that

$$\ker \varphi = \{h \in k[X] \mid h(f_1(t), \ldots, f_n(t)) = 0\}.$$

If $h \in \ker \varphi$, then $h(f_1(a), \ldots, f_n(a)) = 0$ for all $a \in K$. Hence, $U \subseteq Z(h)$, consequently, $V = \overline{U} \subseteq Z(h)$. In particular, $h \in \mathscr{I}(V)$. Conversely, if $g \in \mathscr{I}(V)$, then for all but finitely many elements of K, $g(f_1(a), \ldots, f_n(a)) = 0$. Hence, $g(f_1(t), \ldots, f_n(t)) = 0$, that is, $g \in \ker \varphi$ and this gives, $\ker \varphi = \mathscr{I}(V)$. And hence, φ induces a map $\varphi' : k[V] \to k(t)$, which in turn induces $\psi : k(V) \to k(t)$. Finally, from Lüroth's Theorem, $k(V) \cong k(t)$.

($\Longleftarrow$) Let $\varphi : k(V) \to k(t)$ be a k-automorphism. Let x_i denote the image of X_i in $k[V] \subseteq k(V)$ and let $f_i(t) = \varphi(x_i)$ and $\varphi^{-1}(t) = g(x_1, \ldots, x_n)/h(x_1, \ldots, x_n)$. Note that $x_i = \varphi^{-1}(\varphi(x_i)) = \varphi^{-1}(f_i(t)) = f_i(g/h)$.

Now, given any $p \in V$ such that $h(p) \neq 0$, with $p = (p_1, \ldots, p_n)$, then $p_i = f_i(g(p)/h(p))$ and hence, $p = (f_1(a), \ldots, f_n(a))$ where $a = g(p)/h(p)$. Hence, all but finitely many points in V can be expressed as

$(f_1(a), \ldots, f_n(a))$ for some $a \in K$. On the other hand, if $a \in K$ such that each $f_i(a)$ is defined, then setting $p = (f_1(a), \ldots, f_n(a))$, we have $u(p) = 0$ for every $u \in \mathscr{I}(V)$. This means, $p \in Z(\mathscr{I}(V)) = V$.

In conclusion, we have that the set $\{(f_1(a), \ldots, f_n(a)) \mid a \in K\}$ misses finitely many points of V and hence, is dense in V. ■

Bibliography

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

[Lan02] Serge Lang. *Algebra*. Springer Science & Business Media, 2002.