Algebra II

Boğaziçi - Math 522

Spring 2026

Ayhan Günaydın

March 22, 2026

Contents

Preface

This course has two (related) parts. The first half of the course will be devoted to the study of fields and Galois Theory. Then we shall concentrate on extension of commutative rings. Below are the topics we shall cover:

- Field Extensions
- Normal and Separable Extensions
- Fundamental Theorem of Galois Theory
- Cyclotomic Extensions
- Norm and Trace
- Hilbert's 90 and Abelian Kummer Theory
- Noetherian Rings
- Integral Extensions
- Localization
- Discrete Valuation Rings and Dedekind Domains

We use the following sources: *Abstract Algebra* by Dummit and Foote [1], Hungerford's *Algebra* [2], and Lang's *Algebra* [3].

We assume some familiarity with at least the following concepts: ring, field, vector space, K-algebra, group, polynomial, integral domain

Chapter 1

Field Theory

1.1 Some Basics

Let F be a field. Then we have a ring homomorphism

$$\phi : \mathbb{Z} \to F; \quad \phi(n) = n\,1 = 1 + \cdots + 1.$$

We have two cases.

- If $\ker \phi = \{0\}$, then we say that the *characteristic of* F is 0. In this case, we have a copy of $\mathbb{Z}$ in F, hence a copy of $\mathbb{Q}$ in F. That subfield is called the *prime field of* F. Most of the times, we disregard the isomorphism and denote the prime field as $\mathbb{Q}$.

- If $\ker \phi = n\mathbb{Z}$ for $n > 0$, then F contains a copy of $\mathbb{Z}/n\mathbb{Z}$. Since $\mathbb{Z}/n\mathbb{Z}$ needs to be an integral domain, we have that n is a prime; hence we rename it as p. In this case, we say that the *characteristic of* F is p, and there is a copy of the finite field $\mathbb{F}_p$ in F, which is called the *prime field of* F.

If the characteristic of F is not 0, we say that F is of *positive characteristic.*

If F is a subfield of E, then we say that E is an *extension* of F, and we denote this as $E|F$. If E is an extension of F, then it is a vector space over F, and its dimension as such is called the *degree of the extension* $E|F$ and it is denoted as $[E : F]$. In these notes, we do not distinguish between different infinite cardinalities; hence $[E : F]$ is either a positive integer or is the symbol ∞. [1] We say that the extension is *finite* if its degree is finite.

Example 1.1.1. For instance, let E be the subfield of $\mathbb{C}$ generated by $\sqrt{17}$; so $E = \mathbb{Q}(\sqrt{17})$. Then $1, \sqrt{17}$ is a basis of E as a vector space over $\mathbb{Q}$. So $[E : \mathbb{Q}] = 2$.

[1] We do not define $+$ and $\cdot$ on $\mathbb{N} \cup \{\infty\}$; just follow your instincts.

If we let F be the subfield of $\mathbb{C}$ generated by $\sqrt{17}$ and $\sqrt[3]{17}$, then it its easy to check that $[F : \mathbb{Q}] = 6$. This will follow also from the next theorem.

If we consider π in the place of $\sqrt{17}$, then $\mathbb{Q}(\pi)|\mathbb{Q}$ is not a finite extension.[2] △

Proposition 1.1.2. *Let $E|F$ and $F|k$ be field extensions. Then*

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

Proof. Let $\{\alpha_i : i \in I\}$ and $\{\beta_j : j \in J\}$ be bases of E over F and F over k. Now it is routine to check that $\{\alpha_i\beta_j : i \in I, j \in J\}$ is a basis of E over k. ■

Corollary 1.1.3. *Let $E|F$ and $F|k$ be field extensions. Then $E|k$ is finite if and only if both $E|F$ and $F|k$ are finite.*

We will be using the following fundamental fact repeatedly.

Proposition 1.1.4. *Let k be a field and let $G \leq k^\times$ be finite. Then G is cyclic.*

Proof. Let n be the exponent of G[3]. Then $n \leq |G|$. It also means that each element of G is a root of the polynomial $x^n - 1 \in k[x]$. This polynomial can have only n many roots. So $|G| = n$ and hence G is cyclic. ■

1.2 Algebraic Extensions

Let $E|F$ be an extension and let $\alpha \in E$. We have an F-algebra homomorphism

$$\mathrm{ev}_\alpha : F[x] \to E; \quad \mathrm{ev}_\alpha(f) = f(\alpha).$$

The image of this homomorphism is precisely the subring of E generated by $F \cup \{\alpha\}$. It is denoted as $F[\alpha]$ and we sometimes call it the subring of E generated over F by α. The elements of $F[\alpha]$ are simply "polynomials of α."

If $\ker\ \mathrm{ev}_\alpha = \{0\}$, then $F[\alpha] \simeq F[x]$. In this case, we say that α is *transcendental over F*.

Since $F[x]$ is a PID, if $\ker\ \mathrm{ev}_\alpha \neq \{0\}$, then $\ker\ \mathrm{ev}_\alpha = \langle f \rangle$ for some nonzero $f \in F[x]$. So we have a copy of $F[x]/\langle f \rangle$ in E and hence f needs to be irreducible; otherwise E would have zero-divisors. Note that this f is determined up to a scaler from F and we may assume that its leading term is 1; in other words f is monic. Such an f is unique and it is called the *minimal polynomial of α over F*. In this case, we say that α is *algebraic over F*.

Note that $f(\alpha) = 0$; indeed $g(\alpha) = 0$ for all $g \in \langle f \rangle$. So α being algebraic over F can be characterized as being a zero of a nonzero polynomial over F. In this terminology, the minimal polynomial is the monic such polynomial with the smallest degree.

---

[2] I assume that you are familiar with the transcendence of π and e.

[3] Recall that the exponent of G is the largest $m > 0$ such that $a^m = 1$ for every $a \in G$.

Definition. An extension $E|F$ is called *algebraic* if every element of E is algebraic over F. ◇

Proposition 1.2.1. *If an extension $E|F$ is finite, then it is algebraic.*

Proof. Let $[E : F] = n$ and let $\alpha \in E$. Then $1, \alpha, \alpha^2, \dots, \alpha^n$ are linearly dependent over F. Hence α is the root of a nonzero polynomial over F. ■

Let $E|F$ be an extension and let $\alpha \in E$. Then being a subring of E, the ring $F[\alpha]$ is an integral domain and hence we may talk about its field of fractions. It is precisely the subfield of E generated by $F \cup \{\alpha\}$ and it is denoted as $F(\alpha)$. Its elements are of the form $\frac{f(\alpha)}{g(\alpha)}$ where $f, g \in F[x]$ and $g(\alpha) \neq 0$.

Proposition 1.2.2. *Let $E|F$ be an extension and let $\alpha \in E$ be algebraic over F. Then $F[\alpha] = F(\alpha)$, and $[F(\alpha) : F]$ is the degree of the minimal polynomial of α over F.*

Proof. Let f be the minimal polynomial of α over F and let n be its degree.

If $g \in F[x]$ such that $g(\alpha) \neq 0$, then $f \not| g$ and hence $k\,f + l\,g = 1$ for some $k, l \in F[x]$. Then $l(\alpha)g(\alpha) = 1$, which means that the nonzero element $g(\alpha)$ of $F[\alpha]$ has an inverse in $F[\alpha]$, proving that $F[\alpha]$ is indeed a field. Since $F[\alpha] \subseteq F(\alpha)$, we get that $F[\alpha] = F(\alpha)$ by the minimality of $F(\alpha)$.

Since $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ are linearly independent over F, we have that $[F(\alpha) : F] \geq n$. To show the equality, let $g(\alpha) \in F(\alpha)$ and divide g by f to get $g = q\,f + r$, where $r \in F[x]$ has degree less than n. So $g(\alpha) = r(\alpha)$, and $g(\alpha)$ can be written as a linear combination of $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$. ■

Corollary 1.2.3. *Let F be a field and let α be in an extension of F. Then the following are equal:*

1. *α is algebraic over F.*
2. *$F(\alpha)|F$ is finite.*
3. *α is contained in a finite extension of F.*
4. *α is contained in an algebraic extension of F.*

Proof. (*1* $\Rightarrow$ *2*) If α is algebraic over F, then by the proposition above $F(\alpha)$ is finite over F.
(*2* $\Rightarrow$ *3*) Clear.
(*3* $\Rightarrow$ *4*) We proved above that finite extension are algebraic.
(*4* $\Rightarrow$ *1*) By definition, elements of an algebraic extensions of F are algebraic over F. ■

Definition. Let $E|K$ and $E|F$ be field extensions. We let $K \cdot F$ or KF denote the subfield of E generated by $K \cup F$. It is called the *compositum* of K and F. ◇

Note that the role of E in the definition of compositum is minimal; we just need K and F to be contained in a common field.

For and extension $E|F$ and $\alpha_1, \ldots, \alpha_n$, we define $F[\alpha_1, \ldots, \alpha_n]$ and $F(\alpha_1, \ldots, \alpha_n)$ by induction on n.

Definition. An extension $E|F$ is called *finitely generated* if $E = F(\alpha_1, \ldots, \alpha_n)$ for some $\alpha_1, \ldots, \alpha_n$. ⋄

Proposition 1.2.4. *An extension $E|F$ is finite if and only if it is finitely generated and algebraic.*

Proof. First let $E|F$ be finite. We have proven above that it is then algebraic. Let $\{\alpha_1, \ldots, \alpha_n\}$ be a basis of E over F. Then

$$E = F\alpha_1 + \cdots + F\alpha_n = F(\alpha_1, \ldots, \alpha_n).$$

So $E|F$ is finitely generated as well.

Conversely suppose $E|F$ is algebraic and let $E = F(\alpha_1, \ldots, \alpha_n)$. Then $\alpha_1, \ldots, \alpha_n$ are algebraic over F. Clearly $F(\alpha_1, \ldots, \alpha_k)|F(\alpha_1, \ldots, \alpha_{k-1})$ is finite for each $k \leq n$. Then using Corollary 1.1.3, we get that $E|F$ is finite. ■

Example 1.2.5. Let F be any field and let α be an element of an extension of F that is transcendental over F; for instance, $F = \mathbb{Q}$ and $\alpha = \pi$. Then $F(\alpha)$ is finitely generated over F, but it is not a finite extension of F.

For an algebraic extension, that is not finite, let F be a field and for each prime p, let α_p be an element in a fixed extension of F that is of degree p over F. [4] Then the field E generated over F by $\{\alpha_p : p \text{ prime}\}$ is an algebraic extension of F. If $E|F$ were finite, then $[E : F]$ would be divisible by for every prime. Hence $E|F$ is not finite. △

Proposition 1.2.6. *Let $E|F$, $F|k$, $L|F$ be field extensions.*

1. *$E|k$ is finite if and only if $E|F$ and $F|k$ are finite.*
2. *If $E|F$ is finite, then $EL|L$ is finite.*
3. *$E|k$ is algebraic if and only if $E|F$ and $F|k$ are algebraic.*
4. *If $E|F$ is algebraic, then $EL|L$ is algebraic.*

Proof.

1. This is just Corollary 1.1.3.
2. Suppose that $E = F(\alpha_1, \ldots, \alpha_n)$ where $\alpha_1, \ldots, \alpha_n$ are algebraic over F. Then $EL = L(\alpha_1, \ldots, \alpha_n)$, then $EL|L$ is also finite.

[4] Can you find a concrete example of this?

3. If $E|k$ is algebraic, then it is clear that both $E|F$ and $F|k$ are algebraic. Suppose conversely that $E|F$ and $F|k$ are algebraic. Let $\alpha \in E$. Then $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$ for some $a_0, \ldots, a_{n-1} \in F$. We also know that $k(a_0, \ldots, a_{n-1})|k$ is algebraic and finitely generated, hence α is algebraic over k.

4. Let $\alpha \in EL$. Then $\alpha \in L(\alpha_1, \ldots, \alpha_n)$ for some $\alpha_1, \ldots, \alpha_n \in E$. We know that $\alpha_1, \ldots, \alpha_n$ are algebraic over F, and hence over L. Then $L(\alpha_1, \ldots, \alpha_n)|L$ is algebraic and in particular α is algebraic over L.

■

Corollary 1.2.7. *Let $E|k$ and $F|k$ be finite/algebraic extensions and suppose that E, F are contained in a common field L. Then $EF|k$ is finite/algebraic.*

Proof. We only prove the 'finite' version since the 'algebraic' version is done in almost exactly the same way. Using the second part of the previous proposition, we see that both $EF|E$ is finite. Now using the first part of the proposition, we get that $EF|k$ is finite. ■

1.3 Field Embeddings and Their Extensions

Recall that nonzero field homomorphisms are injective; we call them (field) embeddings. Every embedding $\sigma : F \to L$ extends to a ring embedding $F[x] \to L[x]$, by sending x to itself; we still denote this ring embedding by σ and sometimes we write f^σ in the place of $\sigma(f)$.

Let $E|F$ be an extension and let $\sigma : F \to L$ be an embedding. An embedding $\tau : E \to L$ is said be an *extension* of σ if $\tau|_F = \sigma$. In the diagram below ι denotes the natural embedding of F into E.

$$\begin{array}{ccc} E & \xrightarrow{\tau} & L \\ \uparrow{\scriptstyle\iota} & & \uparrow{\scriptstyle\mathrm{id}} \\ F & \xrightarrow{\sigma} & L \end{array}$$

If F is a subfield of L and σ is the natural embedding of F into L, then we say that τ *is over* F.

Proposition 1.3.1. *Let $\tau : E \to L$ be an extension of $\sigma : F \to L$. Suppose that $f(x) \in F[x]$ and $\alpha \in E$ is a root of f. Then $\tau(\alpha)$ is a root of f^σ.*

Proof. Write $f = a_0 + a_1x + \cdots + a_nx^n$ and note that

$$\begin{aligned} f^\sigma(\tau(\alpha)) &= \sigma(a_0) + \sigma(a_1)\tau(\alpha) + \cdots + \sigma(a_n)\tau(\alpha)^n \\ &= \tau(a_0 + a_1\alpha + \cdots + a_n\alpha^n) \\ &= \tau(f(\alpha)) \\ &= \tau(0) = 0. \end{aligned}$$

■

Corollary 1.3.2. *Let F be a subfield of E and L and let $\tau : E \to L$ be an embedding over F. Suppose that $f \in F[x]$. Then τ sends roots of f to roots of f.*

Lemma 1.3.3. *Let $E|F$ be an algebraic extension and $\sigma : E \to E$ be an endomorphism over F. Then σ is an automorphism of E.*

Proof. As σ fixes F, it cannot be the zero endomorphism, hence it is injective and all we need to show is that σ is surjective. This is clear if the extension is finite by dimension reasons.

Let $\beta \in E$ and let f be its minimal polynomial over F. Let E' be the field generated over F by the roots of f in E. Since $E'|F$ is finite, $\sigma|_{E'}$ is an automorphism of E'. Hence there is $\alpha \in E'$ such that $\sigma(\alpha) = \beta$. ■

Lemma 1.3.4. *Let $E|E_1$ and $E|E_2$ be extensions and let $\sigma : E \to L$ be an embedding. Then $\sigma(E_1E_2) = \sigma(E_1)\sigma(E_2)$.*

Proof. It is clear that $\sigma(E_1)\sigma(E_2) \subseteq \sigma(E_1E_2)$. For the other inclusion just note that elements of E_1E_2 are quotients of elements of the form $\alpha_1\beta_1 + \cdots + \alpha_n\beta_n$ where $\alpha_1, \ldots, \alpha_n \in E_1$ and $\beta_1, \ldots, \beta_n \in E_2$. ■

Proposition 1.3.5 (Kronecker)**.** *Let $f \in k[x]$ be non-constant. Then k has an extension in which f has a root.*

Proof. It suffices to prove this for irreducible f, so we assume so. We embed k into a field that contains a root of f; making this field an actual set-theoretic extension is a simple matter.

Consider

$$k \xrightarrow{\iota} k[x] \xrightarrow{\pi} k[x]/\langle f \rangle$$

Note that $\sigma := \pi \circ \iota$ is an embedding of k into the field $K := k[x]/\langle f \rangle$. Consider the element $\zeta := \pi(x) \in K$. We have

$$f^\sigma(\zeta) = f^\pi(x^\pi) = \pi(f(x)) = 0.$$

■

Proposition 1.3.6. *Let k be a field and let α be in some algebraic extension of k. Then $k(\alpha)$ is isomorphic to $k[x]/\langle f \rangle$, where f is the minimal polynomial of k.*

Proof. Let $\phi : k[x] \to k[\alpha]$ be the ring homomorphism sending $g(x)$ to $g(\alpha)$. As $k(\alpha) = k[\alpha]$, this ϕ is surjective, and it is clear that the kernel of ϕ is $\langle f \rangle$. ■

Corollary 1.3.7. *Let k be a field and let α, β be in two algebraic extensions of k with the same minimal polynomial. Then $k(\alpha)$ and $k(\beta)$ are isomorphic over k via an isomorphism sending α to β.*

Definition. A field K is said to be *algebraically closed* if every non-constant polynomial with coefficients from K has a root in K. ◇

Clearly, if K is algebraically closed, then K actually contains all the roots of all the non-constant polynomials over K.

Theorem 1.3.8. *Any field k has an extension that is algebraically closed.*

Proof. Let $S = \{X_f : f \in k[x] \setminus k\}$; so S contains a variable for each non-constant polynomial over k. Let R be the ring $k[S]$ and

$$I := \langle f(X_f) : f \in k[x] \setminus k \rangle.$$

We claim that I is not the whole R. If it were, then

$$1 = g_1 f_1(X_{f_1}) + \cdots + g_m f_m(X_{f_m}),$$

for some $g_1, \ldots, g_m \in R$ and $f_1, \ldots, f_m \in k[x] \setminus k$. Suppose that $X_1, \ldots, X_N$ be all the variable in the equation above.

Using the previous proposition, take an extension $E|k$ that contains a root of each one of $f_1, \ldots, f_m$; say $\alpha_{f_1}, \ldots, \alpha_{f_m}$. If X_j is a variable among $X_1, \ldots, X_N$ that is not of the form X_{f_i}, then put $\alpha_j = 0$. So we get a tuple $\vec{\alpha} = (\alpha_1, \ldots, \alpha_N)$ from E and we have

$$1 = g_1(\vec{\alpha}) f_1(\vec{\alpha}) + \cdots + g_m(\vec{\alpha}) f_m(\vec{\alpha}) = g_1(\vec{\alpha}) f_1(\alpha_{f_1}) + \cdots + g_m(\vec{\alpha}) f_m(\alpha_{f_m}) = 0.$$

This is a contradiction, hence we have $I \neq R$.

Let $\mathfrak{m}$ be a maximal ideal of R containing I. So $E_1 := R/\mathfrak{m}$ is a field containing an isomorphic copy of k. Moreover, E_1 contains a root of each polynomial over k; namely $f(\overline{X}_f) = 0$, where $\overline{X}_f$ is the image of X_f in E_1.

Applying the same procedure to E_1 in the place of k, we get E_2 that contains a copy of E_1 and a root of each polynomial over E_1. Continuing this way, we get $E_1 \subseteq E_2 \subseteq E_3 \subseteq \ldots$. Now it is easy to check that $E = \bigcup_{i>0} E_i$ is an algebraically closed field containing k.[5] ■

Corollary 1.3.9. *Any field k has an algebraic extension K that is algebraically closed.*

Proof. Let E be an algebraically closed field containing k and let K be the union of all finite extensions of k that are included in E. It is clear that K is indeed a field extending k and that $K|k$ is algebraic. In order to show that K is algebraically closed, let $f \in K[x] \setminus K$. Then E contains a root α of f. Then α is algebraic over K, hence over k. Therefore $k(\alpha) \subseteq K$ and $\alpha \in K$. ■

[5] As in the previous proposition, E does not actually contain k, just an isomorphic copy of it, but again it is not a problem to carry the field structure on E to a field containing k.

An extension of a given field k as in this corollary is called *an algebraic closure of* k; in a bit we shall see that two algebraic closures are isomorphic over k, and thus we will talk about *the* algebraic closure of k. If we fix an algebraically closed field L containing k, then it follows from the proof of the previous corallary that there is indeed a unique algebraic closure of k contained in L. For instance, $\mathbb{C}$ is an algebraically closed field containing $\mathbb{Q}$; below when we refer to $\overline{\mathbb{Q}}$ we always refer to the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$; it is called the *field of algebraic numbers*, and an element of $\overline{\mathbb{Q}}$ is called an *algebraic number*.

Proposition 1.3.10. *Let $\sigma : k \to L$ be an embedding of a field k in an algebraically closed field L. Also α be in an algebraic extension of k with minimal polynomial f. Then there are as many extensions of σ to $k(\alpha)$ as the number of distinct roots of f^σ in L .*

Proof. Let $f \in k[x]$ be the minimal polynomial of α over k. Take a root $\beta \in L$ of f^σ. Then as in the proof of Proposition 1.3.6, σ extends to $k(\alpha)$, by sending α to β. Clearly, different $\beta \in L$ give different embeddings. Therefore the number of embeddings is at least the number of distinct roots of f^σ in L. If τ is an embedding of $k(\alpha)$ in L extending σ, then $\tau(\alpha)$ is a root of f^σ. Thus the embedding above are all the embeddings. ■

Using Proposition 1.3.1, we get the following consequence.

Corollary 1.3.11. *Let $\sigma : k \to L$ be an embedding of a field k in an algebraically closed field L. Also let K be an algebraically closed field containing k, and let α be in an algebraic extension of k with minimal polynomial f. Then the number of extensions of σ to $k(\alpha)$ is the same as the number of roots of f in K.*

Using the proposition above, we may count the number of extensions to σ to a finite extension, which we do below in detail.

Theorem 1.3.12. *Let $E|k$ be an algebraic extension and let $\sigma : k \to L$ be an embedding of k into an algebraically closed field L. Then σ extends to an embedding of E into L. Moreover, if E is algebraically closed and $L|\sigma(k)$ is algebraic, then E is isomorphic to L.*

Proof. Let

$$S := \{\tau : F \to L : k \subseteq F \subseteq E, \tau|_k = \sigma\}.$$

Then S is nonempty and it is ordered by inclusion of functions. One may easily see that S is closed under chains, hence S has a maximal element; say $\tau : F \to L$. We claim that $F = E$. Suppose not and let $\alpha \in E \setminus F$. Then α is algebraic over k and hence over F. Therefore by Proposition 1.3.10, τ extends to an embedding of $F(\alpha)$ into L. This contradicts the maximality of τ and $F = E$.

For the second part note that, under the assumptions there, $L|\tau(E)$ is also an algebraic extension. So if $\alpha \in L$, then α is algebraic over $\tau(E)$. Since $\tau(E)$ is algebraically closed, we get that $\alpha \in \tau(E)$ and that τ is surjective. ■

Corollary 1.3.13. *Let K and L be two algebraic closures of k. Then K and L are isomorphic over k.*

Proof. Take σ in the previous theorem to be the inclusion of k into L. Then it extends to the whole of K and by the second part of the theorem that extension is an isomorphism. ∎

Using this, we generally fix one algebraic closure of k and denote it as $\overline{k}$. Note that we are very flexible in the choice of this algebraic closure. For instance, we may take the one that is contained in some fixed algebraically closed field containing k; as in the case of algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$. As mentioned before, in that case the algebraic closure is really unique.

Fix an algebraic closure $\overline{k}$ of k. Two elements α, β of $\overline{k}$ are said to be *conjugate over* k if they have the same minimal polynomials over k. This also means that there is an automorphism of $\overline{k}$ over k that sends α to β.

Let α be algebraic over k with minimal polynomial f. The *multiplicity of* α is the largest $m > 0$ such that $(x - \alpha)^m$ divides f. In other words, if m is the multiplicity of α, then $f(x) = (x - \alpha)^m h(x)$, where $h(x) \in k[x]$ with $h(\alpha) \neq 0$. If β is a conjugate of α, then there is an isomorphism $\sigma : k(\alpha) \simeq k(\beta)$ over k. Hence $f^\sigma = f$ and the multiplicity of β is also m.

1.4 Normal Extensions

Let k be a field and let $f \in k[x]$ be non-constant. An extension K of k is called *a splitting field of* f if $K = k(\alpha_1, \ldots, \alpha_n)$ where $\alpha_1, \ldots, \alpha_n$ are roots of f with the property that $f = c(x - \alpha_1) \cdots (x - \alpha_n)$ for some constant $c \in k$. In vague terms, a splitting field of f over k is a field generated over k by *all* the roots of f. We are allowed to say this since we know by the work done in the previous section that there is an extension of k that contains all the roots of f; at least we may take the roots in the algebraic closure of k. In particular, splitting fields always exist and the next result says that they are unique up to isomorphisms.

Proposition 1.4.1. *Let $f \in k[x]$ be non-constant and let K and L be splitting fields of f. Then K and L are isomorphic over k,*

Proof. Embed K into $\overline{L}$ over k; say via σ. We claim that σ is an isomorphism of K and L.

Let $K = k(\alpha_1, \ldots, \alpha_n)$ and $L = k(\beta_1, \ldots, \beta_n)$, where

$$f = c(x - \alpha_1) \cdots (x - \alpha_n) = c(x - \beta) \cdots (x - \beta_n).$$

Clearly, $f^\sigma = f$ and hence

$$f = c(x - \sigma(\alpha_1)) \cdots (x - \sigma(\alpha_n)) = c(x - \beta) \cdots (x - \beta_n).$$

By unique factorization, we see that

$$\{\beta_1, \dots, \beta_n\} = \{\sigma(\alpha_1), \dots, \sigma(\alpha_n)\},$$

and hence $L = \sigma(K)$ and σ is an isomorphism of K and L. ■

We may define the splitting field of a family $\{f_i : i \in I\}$ of a family of non-constant polynomials in $k[x]$ over k. Also the existence and uniqueness of such splitting fields can be proven similarly.

Theorem 1.4.2. *Let $K|k$ be algebraic and fix an algebraic closure $\overline{k}$ of k containing K. Then the following are equivalent.*

1. *K is the splitting field of a family of non-constant polynomials in $k[x]$.*
2. *Every embedding of K into $\overline{k}$ over k is an automorphism (of K).*
3. *If $f \in k[x]$ is irreducible and has a root in K, then K contains all the roots of f (in $\overline{k}$).*

Proof. (*1* ⇒ *2*) Let K be the splitting field of $\{f_i \in k[x] : i \in I\}$. An embedding of K over k into $\overline{k}$ is determined by where the roots of f_i are sent to. By assumption, all roots of each f_i are in K. Therefore any embedding sends K into itself and hence by Lemma 1.3.3, it is indeed an automorphism of K.

(*2* ⇒ *3*) Let $f \in k[x]$ be irreducible and let let $\alpha \in K$ be a root of f. Let $\beta \in \overline{k}$ be another root of f. Then there is an embedding of K into $\overline{k}$ that sends α to β. By assumption, such an embedding sends K into itself, hence $\beta \in K$.

(*3* ⇒ *1*) We claim that K is the splitting field of

$$\{f \in k[x] : f \text{ is irreducible and has a root in } K\}.$$

By the assumption, K contains all the roots of all the polynomials in this collection. If $\alpha \in K$, then α is algebraic over k and hence its minimal polynomial is contained in the collection above. ■

Definition. An algebraic extension $K|k$ is called *normal* if it satisfies one of the conditions in Theorem 1.4.2. ◇

Example 1.4.3. Let $k = \mathbb{Q}$ and let $f(x) = x^3 - 2$. Then f is irreducible in $\mathbb{Q}[x]$. The roots of f in $\overline{\mathbb{Q}}$ are $\alpha = \sqrt[3]{2}, \alpha\zeta_3, \alpha\zeta_3^2$, where $\zeta_3 = e^{\frac{2\pi i}{3}}$ is a primitive third root of unity. So the splitting field of f (in $\overline{\mathbb{Q}}$) is $K = \mathbb{Q}(\alpha, \alpha\zeta_3, \alpha\zeta_3^2)$; note that it is indeed $\mathbb{Q}(\alpha, \zeta_3)$. Note that $K|\mathbb{Q}(\alpha)$, $K|\mathbb{Q}(\zeta_3)$, and $\mathbb{Q}(\zeta_3)|\mathbb{Q}$ are normal, but $\mathbb{Q}(\alpha)|\mathbb{Q}$ is not. △

Proposition 1.4.4.

1. *Let $E|k$ be a normal extension and $k \subseteq F \subseteq E$. Then $E|F$ is normal.*
2. *Let $E|k$ be a normal extension and let $F|k$ be any extension. Suppose that E, F are contained in a common extension. Then $EF|F$ is normal.*

3. *Let $E_1|k$ and $E_2|k$ be normal extensions and suppose that E_1 and E_2 are contained in a common extension. Then $E_1E_2|k$ and $E_1 \cap E_2|k$ are normal.*

Proof. (*1*) This is clear since any embedding of K over F is also an embedding over k.

(*2*) We may assume that $\overline{k} \subseteq \overline{F}$. Let σ be an embedding of EF over F. Then $\sigma|_E$ is an embedding of E over k. By assumption, $\sigma(E) = E$ and therefore $\sigma(EF) = \sigma(E)\sigma(F) = EF$.

(*3*) Let σ be an embedding of E_1E_2 into $\overline{k}$ over k. Then $\sigma(E_1) = E_1$ and $\sigma(E_2) = E_2$. Therefore $\sigma(E_1E_2) = \sigma(E_1)\sigma(E_2) = E_1E_2$; proving that $E_1E_2|k$ is normal. Note that $\sigma(E_1 \cap E_2) = \sigma(E_1) \cap \sigma(E_1) = E_1 \cap E_2$, hence $E_1 \cap E_2|k$ is normal. ∎

Let $E|k$ be algebraic and fix an algebraic closure $\overline{k}$ of k containing E. Consider the intersection K of all $K' \subseteq \overline{k}$ such that $E \subseteq K'$ and $K'|k$ is normal. Then K is the smallest extension of E that is normal over k; we call it as the *normal closure of* $E|k$.

When $E|k$ is finite, say $\sigma_1, \dots, \sigma_n$ are all the embeddings of E into $\overline{k}$ over k, we may characterize the normal closure of $E|k$ as the compositum of the fields $\sigma_1(E), \dots, \sigma_n(E)$. Another way to express E is as the splitting field of minimal polynomials of $\alpha_1, \dots, \alpha_m$, where $E = k(\alpha_1, \dots, \alpha_m)$.

Example 1.4.5. Let $k = \mathbb{Q}$ and $E = \mathbb{Q}(\sqrt[3]{2})$. As investigated above $E|k$ is not normal and its normal closure is $K = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$. △

1.5 Separable Extensions

Let $E|k$ be an algebraic extension and L be an algebraically closed field. For an embedding $\sigma : k \to L$, we define $S_L(\sigma, E)$ to be the set of extensions of σ to E; so it is the set of embeddings $\tilde{\sigma} : E \to L$ with $\tilde{\sigma}|_k = \sigma$. Note that $S_L(\sigma, E) = S_{\overline{\sigma(k)}}(\sigma, E)$; so for many purposes, we may assume that $L = \overline{\sigma(k)}$.

Proposition 1.5.1. *Let $E|k$ be an algebraic extension and let $\sigma : k \to L$ and $\tau : k \to L'$ be embeddings of k into algebraically closed fields L, L'. Then*

$$|S_L(\sigma, E)| = |S_{L'}(\tau, E)|.$$

Proof. Assume that L and L' are algebraic closures of $\sigma(k)$ and $\tau(k)$, and fix an isomorphism $\lambda : L \to L'$ extending the isomorphism $\tau \circ \sigma^{-1}$ between $\sigma(k)$ and $\tau(k)$. Now it is easy to see that the map

$$f : S_L(\sigma, E) \to S_{L'}(\tau, E); \quad f(\tilde{\sigma}) = \lambda \circ \tilde{\sigma}$$

is indeed a bijection. ∎

As a result of this proposition, we may define the *separable degree* of E over k as

$$[E : k]_s := |S_L(\sigma, E)|$$

for some embedding σ of k into an algebraically closed field. We may even take the inclusion of k into an algebraic closure of k containing E.

Proposition 1.5.2. *Let $E|F$ and $F|k$ be algebraic extensions.*

1. $[E : k]_s = [E : F]_s[F : k]_s$.
2. *If $E|k$ is finite, then $[E : k]_s \leq [E : k]$.*
3. *Suppose that both $E|F$ and $F|k$ are finite. Then $[E : k]_s = [E : k]$ if and only if $[E : F]_s = [E : F]$ and $[F : k]_s = [F : k]$.*

Proof. (*1*) We may assume $L = \overline{k} = \overline{F} = \overline{E}$. Let $\sigma : k \to L$ be an embedding and consider $\tilde{\sigma} \in S_L(\sigma, E)$. Then $\tilde{\sigma} \restriction_F \in S_L(\sigma, F)$ and it can be extended to E in $[E : F]_s$ many ways. Since every element of $S_L(\sigma, F)$ extends to an element of $S_L(\sigma, E)$, we get the desired equality.

(*2*) Let $E = k(\alpha_1, \ldots, \alpha_n)$. Put $E_0 = k$, and $E_i = E_{i-1}(\alpha_i)$ for $i = 1, \ldots, n$. Then by Proposition 1.3.10, we have $[E_i : E_{i-1}]_s$ is the number of roots of the minimal polynomial of α_i over E_{i-1}. Since that number is less than the degree of the minimal polynomial, we get $[E_i : E_{i-1}]_s \leq [E_i : E_{i-1}]$. Since both degrees are multiplicative, we get $[E : k]_s \leq [E : k]$.

(*3*) Clear from the previous parts. ■

Definition.

1. A finite extension $E|k$ is *separable* if $[E : k]_s = [E : k]$.
2. An element α that is algebraic over k is called *separable over* k if $k(\alpha)|k$ is separable.
3. A polynomial $f \in k[x]$ is called *separable* if it has no multiple roots in an algebraic closure of k.

◇

Note that α is separable over k if and only if its minimal polynomial over k is separable.

The third part of Proposition 1.5.2 states that for $k \subseteq L \subseteq E$, we have $E|F$ and $F|k$ are (finite) separable extensions if and only if $E|k$ is separable.

Proposition 1.5.3. *Let $E|k$ be finite. Then $E|k$ is separable if each $\alpha \in E$ is separable over k.*

Proof. Suppose that $E|k$ is separable and let $\alpha \in E$. Then $E|k(\alpha)$ and $k(\alpha)|k$ are separable and hence α is separable over k.

Conversely, suppose that every element of E is separable over k. Write $E = k(\alpha_1, \ldots, \alpha_n)$. Let $E_0 = k$ and for $i > 0$, let $E_i = E_{i-1}(\alpha_i)$. Then $E|k$ is separable if and only if for each $i > 0$, we have $E_i|E_{i-1}$ is separable. It is clear that each $E_i|E_{i-1}$ is separable since each α_i is separable over k. ■

In the light of this proposition, we define an algebraic extension $E|k$ to be *separable* if each $\alpha \in E$ is separable over k. It means that each finite extension $F|k$ with $F \subseteq E$ is separable.

Proposition 1.5.4. *1. Let $k \subseteq F \subseteq E$ be fields such that $E|k$ is algebraic. Then $E|k$ is separable if and only if $E|F$ and $F|k$ are separable.*

2. Let $E|k$ be a separable extension and let $F|k$ be an arbitrary extension. Then $EF|F$ is separable.

3. Let $E|k$ and $F|k$ be separable. Then $EF|k$ is separable.

Proof. 1. Suppose $E|k$ is separable and let $\alpha \in E$. Then the minimal polynomial of α over F divides the minimal polynomial of it over k. Hence α is separable over F and $E|F$ is separable. Next let $\alpha \in F$. Then the minimal polynomial of α over k is separable since $\alpha \in E$. Hence $F|k$ is separable.
Conversely, suppose that $E|F$ and $F|k$ are separable, and let $\alpha \in E$. Let $K|k$ be separable such that the minimal polynomial of α over F is in $K[x]$. Then $K|k$ is separable since $F|k$ is and $K(\alpha)|K$ is separable since $E|F$ is separable. So $K(\alpha)|k$ is separable and hence α is separable over k.

2. Note that $EF = F(\alpha : \alpha \in E)$ and by assumption each $\alpha \in E$ is separable over k, hence over F. So $EF|F$ is separable.

3. Clear from the previous parts. ■

Suppose that $E|k$ is separable, then it follows from the last part of this proposition that the normal closure of $E|k$ is separable over k.

Definition. Let k be a field and fix an algebraic closure $\overline{k}$ of it. The *separable closure* (in $\overline{k}$) of k is

$$k^{\text{sep}} := \{\alpha \in \overline{k} : \alpha \text{ is separable over } k\}.$$

◇

Note that k^{sep} can be characterized as the compositum of all (finite) separable extensions of k inside $\overline{k}$. Hence $k^{\text{sep}}|k$ is indeed separable.

For a polynomial $f(x) = a_n x^n + \cdots + a_0 \in k[x]$, we define the *formal derivative* of f as

$$f'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + 2a_2 x + a_1.$$

Clearly, $f' \in k[x]$.

It is easy to see that the formal derivative operator is k-linear and satisfies the *Leibniz rule*: $(fg)' = f'g + fg'$. It follows that f has a double root if and only if f and f' have a common root. So if f is irreducible, then f is not separable if and only if f' is identically 0, because f is the minimal polynomial of any root of it (in $\overline{k}$).

If k is of characteristic 0, then f' is not identically zero since $na_n \neq 0$. Therefore any algebraic extension in characteristic 0 is separable. We shall investigate the positive characteristic case later.

Definition. A field k is called *perfect* if all of its algebraic extensions are separable. $\diamond$

So fields of characteristic 0 are always perfect. We'll see a characterization of perfect fields of positive characteristic later.

Theorem 1.5.5 (Primitive Element Theorem). *Let $E|k$ be a finite separable extension. Then $E = k(\alpha)$ for some $\alpha \in E$.*

Proof. If k is finite, then so is E and hence $E^\times$ is cyclic, say generated by α. Hence $E = k(\alpha)$ in this case. So assume that k is infinite.

Using an inductive argument, we may assume that $E = k(\alpha, \beta)$ for some α, β. Let $[E : k] = n$ and let $\sigma_1, \dots, \sigma_n$ be the embeddings of E over k into $\overline{k}$. Consider the polynomial

$$P(x) = \prod_{i \neq j} \big((\sigma_i\alpha - \sigma_j\alpha) + (\sigma_i\beta - \sigma_j\beta)x\big).$$

Note that P is not the zero polynomial since $\sigma_i \neq \sigma_j$ for all $i \neq j$. Then, as k is infinite, there is $c \in k$ such that $P(c) \neq 0$. This means that $\sigma_i(\alpha + c\beta) \neq \sigma_j(\alpha + c\beta)$ for every distinct i, j. This means that the field $k(\alpha + c\beta)$ has n many embeddings over k into $\overline{k}$. This means that

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

Hence $[k(\alpha + c\beta) : k] = n$ and $E = k(\alpha + c\beta)$. ∎

The generator as in this theorem is called a *primitive element* of the extension. We observed above that every algebraic extension in characteristic zero is separable. Hence every finite extension in characteristic zero has a primitive element.

Using a proof similar to the proof of the Primitive Element Theorem above, we may prove the following equivalence for a finite extension $E|k$:

$$E = k(\alpha) \text{ for some } \alpha \iff \text{there are only finitely many intermediate fields between } k \text{ and } E.$$

The following consequence of the primitive element will be used later.

Lemma 1.5.6. *Let $E|k$ be a separable extension. Suppose that there is $n > 0$ such that each $\alpha \in E$ has degree at most n over k. Then $E|k$ is finite of degree at most n.*

Proof. Let $\alpha \in E$ be of largest degree m; so $m \leq n$. We claim that $E = k(\alpha)$. Let $\beta \in E \setminus k(\alpha)$ and consider $k(\alpha, \beta)$. Since the extension is separable, using the Primitive Element Theorem, there is γ such that $k(\gamma) = k(\alpha, \beta)$. Then $[k(\gamma) : k] = [k(\alpha, \beta) : k] \geq [k(\alpha) : k]$. So $k(\alpha, \beta) = k(\alpha)$ by the maximality of m, and hence $E = k(\alpha)$. It is clear that $[E : k] = m \leq n$. ∎

1.6 Finite Fields

Note that a finite field needs to be of positive characteristic, as others contain the rationals. So let F be a finite field of characteristic p. One finite field we know is the prime field $\mathbb{F}_p$; fix an algebraic closure $\overline{\mathbb{F}}_p$ of it. Suppose that $[F:\mathbb{F}_p]=n$. Then F has p^n many members. Can we find for any $n>0$, a field with p^n many elements? Yes! Consider the polynomial $x^{p^n}-x$. One root of it is 0 and the formal derivative of the polynomial $x^{p^n-1}-1$ is $(p^n-1)x^{p^n-2}$. Hence $x^{p^n}-x$ is separable and has exactly p^n many roots in $\overline{\mathbb{F}}_p$. It is easy to see that those roots form a field. So we have field with p^n many elements; we denote it as $\mathbb{F}_{p^n}$. Actually, if F were included in $\overline{\mathbb{F}}_p$, then $F=\mathbb{F}_{p^n}$, because $F^\times$ is cyclic and a generator is a root of $x^{p^n-1}-1$.

Note that $\mathbb{F}_{p^n}|\mathbb{F}_p$ is normal and separable, because it is the splitting field of the separable polynomial $x^{p^n-1}-1$. Also it is easy to see that $\mathbb{F}_{p^m}\subseteq\mathbb{F}_{p^n}$ if and only if $m|n$.

Consider the map $\phi:\overline{\mathbb{F}}_p\to\overline{\mathbb{F}}_p$ defined as $\phi(x)=x^p$. This is an automorphism of $\overline{\mathbb{F}}_p$. It is called the *Frobenius automorphism*. For $n>0$ consider $\phi_n=\phi|_{\mathbb{F}_{p^n}}$; it is an automorphism of $\mathbb{F}_{p^n}$. Clearly, $\phi_n^n=id_{\mathbb{F}_{p^n}}$ and it is not hard to see that the order of ϕ_n is actually n and moreover $\mathrm{Aut}(\mathbb{F}_{p^n})$ is generated by ϕ_n. Hence $\mathrm{Aut}(\mathbb{F}_{p^n})\simeq\mathbb{Z}/n\mathbb{Z}$.

1.7 Inseparable Extensions

Let k be a field of characteristic p. Take an element $\alpha\in\overline{k}$ whose its minimal polynomial f over k is not separable.

We know that f' is the zero polynomial and considering the coefficients we see that $f(x)=g(x^p)$ for some $g(x)\in k[x]$. Note that g is indeed the minimal polynomial of α^p over k; otherwise we could construct a polynomial whose degree is less than the degree of f and gives zero when evaluated at α. Then

$$[k(\alpha^p):k]=\deg g=\frac{\deg f}{p}=\frac{[k(\alpha):k]}{p}.$$

It follows that the minimal polynomial of α over $k(\alpha^p)$ is $x^p-\alpha^p$. The only zero of this polynomial is α. Hence $[k(\alpha):k(\alpha^p)]_s=1$ and $[k(\alpha):k]_s=[k(\alpha^p):k]_s$.

If g were separable, then we would get

$$[k(\alpha):k]_s=[k(\alpha^p):k]_s=[k(\alpha^p):k]=\frac{[k(\alpha):k]}{p}.$$

Hence we get $[k(\alpha^p):k]=p[k(\alpha^p):k]_s$ in that case. If g is not separable, then we could do the same calculations with g in the place of f. Continuing this way, we get that

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

for some $\mu \geq 0$. The number p^μ is called the *degree of inseparability of α over k*. Note that this is exactly the multiplicity of α over k.

Let $E|k$ be finite. Then iterating the arguments above, we get

$$[E:k] = p^\mu [E:k]_s$$

for some $\mu \geq 0$. Again, the number p^μ is *degree of inseparability* of the extension $E|k$ and it is denoted as $[E:k]_i$.

Clearly, the extension $E|k$ is separable if and only if $[E:k]_i = 1$. The other extreme is $[E:k]_i = [E:k]$; in this case the extension is said to be *purely inseparable.* If $k(\alpha)|k$ is purely inseparable, then we say that α is *purely inseparable over k*. Note that α is purely is separable if and only if the minimal polynomial of α over k is of the form $x^{p^\mu} - a$ for some $a \in k$; this polynomial can be written as $x^{p^\mu} - \alpha^{p^\mu}$. It follows that a field k of characteristic p is perfect if it is closed under taking p^{th} roots; more precisely, the subfield

$$k^p := \{\alpha^p : \alpha \in k\}$$

is indeed the whole k. Another way to express is that the *Frobenius map* $\phi : k \to k$ sending x to x^p is surjective; hence is an automorphism.

Proposition 1.7.1.

1. *Let $k \subseteq F \subseteq E$ be fields such that $E|k$ is algebraic. Then $E|k$ is purely inseparable if and only if $E|F$ and $F|k$ are purely inseparable.*
2. *If $E|k$ is a purely inseparable (algebraic) extension and $F|k$ any extension, then $EF|F$ is purely inseparable.*

Proof. Exercise. ■

Chapter 2

Galois Theory

2.1 Galois Correspondence

An algebraic extension $E|k$ is called *Galois* if it is both normal and separable. For such an extension $E|k$, we define the *Galois group* of $E|k$ as

$$\mathrm{Gal}(E/k) := \{\sigma : E \to E : \sigma \text{ is an automorphism of } E \text{ over } k\}$$

Assuming $\overline{k} = \overline{E}$, elements of $\mathrm{Gal}(E/k)$ exactly the embeddings of E over k into $\overline{k}$. If $E|k$ is finite, then $|\mathrm{Gal}(E/k)| = [E : k]$.

An *intermediate field* of $E|k$ is simply a subfield F of E containing k. Note that when F is an intermediate field, the extension $E|F$ is still Galois and $\mathrm{Gal}(E/F) \leq \mathrm{Gal}(E/k)$. Our eventual aim is to show obtain a correspondence between intermediate fields and subgroups of $\mathrm{Gal}(E/k)$ when the extension $E|k$ is finite.

For that correspondence, let $G \leq \mathrm{Aut}(E)$ for some field k. Then we let the *fixed field* of G to be

$$E^G := \{\alpha \in E : \sigma(\alpha) = \alpha \text{ for all } \sigma \in G\}.$$

When $E|k$ is a Galois extension and $H \leq \mathrm{Gal}(E/k)$, the fixed field E^H is indeed an intermediate field.

Proposition 2.1.1. *Let $E|k$ be a Galois extension and let $G = \mathrm{Gal}(E/k)$. Then $E^G = k$*

Proof. It is clear by definition that $k \subseteq E^G$. For the other inclusion, let $\alpha \in E^G$. Let F be the splitting field of the minimal polynomial of α over k. Then $F|k$ is also Galois any element of $\mathrm{Gal}(F/k)$ extends to an element of G. The orbit of α under the action of $\mathrm{Gal}(F/k)$ consists of the conjugates of it over k. However, by the assumption this orbit consists of α and by separability the only way this can happen is that $\alpha \in k$. ■

It follows from this proposition that when $E|k$ is a Galois extension and F is an intermediate field, we have $E^{\mathrm{Gal}(E|F)} = F$. This proves that the map sending an intermediate field F to to the subgroup $\mathrm{Gal}(E|F)$ of $\mathrm{Gal}(E|k)$ is injective: If $\mathrm{Gal}(E|F) = \mathrm{Gal}(E|F')$, then $F = E^{\mathrm{Gal}(E|F)} = E^{\mathrm{Gal}(E|F')} = F'$. Note that for this result, we haven't assumed that the extension $E|k$ is finite.

The surjectivity of the correspondence for finite extensions follows from the following result.

Theorem 2.1.2 (Artin's Theorem)**.** *Let K be a field and let G be a finite subgroup of $\mathrm{Aut}(K)$. Then the extension $E|E^G$ is finite Galois with Galois group $|G|$. (In particular $[E : E^G] = |G|$.)*

Proof. Let $n = |G|$ and take $\alpha \in E$. We first show that α is separable over E^G and that its degree over E^G is at most n.

Let $\sigma_1, \ldots, \sigma_m \in G$ be maximal set such that $\{\sigma_1\alpha, \ldots, \sigma_m\alpha\}$ has m members. Note that if $\tau \in G$, then $\{\sigma_1\alpha, \ldots, \sigma_m\alpha\} = \{\tau\sigma_1\alpha, \ldots, \tau\sigma_m\alpha\}$. In particular, $\sigma_i\alpha = \alpha$ for some i. So α is a root of

$$f(x) = \prod_i^m (x - \sigma_i\alpha).$$

Then for any $\tau \in G$, we have $f^\tau = f$. Therefore $f(x) \in E^G[x]$ and hence the degree of α over E^G is at most n . Clearly, f is separable over k; so α is separable over E^G. By Lemma 1.5.6, we have that $[E : E^G] \leq n$. Also since f splits into linear factors in E, then $E|E^G$ is also normal.

Note that $\mathrm{Gal}(E/E^G)$ contains G, hence $[E : E^G] \geq |G| = n$. So $[E : E^G] = n$ and $\mathrm{Gal}(E/E^G) = G$. ∎

Corollary 2.1.3. *Let $E|k$ be finite Galois extension with $G = \mathrm{Gal}(E/k)$. Then for any subgroup H of G, there is an intermediate field F such that $H = \mathrm{Gal}(E/F)$.*

Proof. Just take $F = E^H$ and use Artin's Theorem. ∎

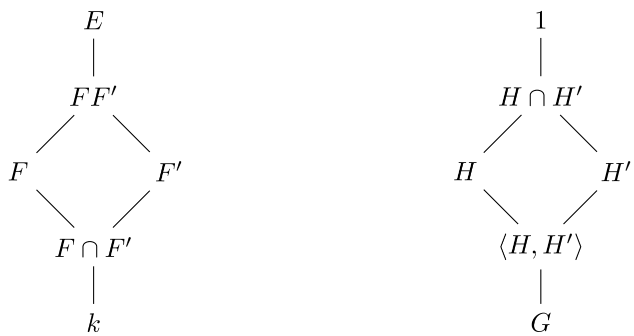
This finishes the desired correspondence between intermediate fields and subgroups of the Galois group for a finite Galois extension. We have some consequences of this.

Proposition 2.1.4. *Let $E|k$ be a finite Galois extension with Galois group G. Also let F, F' be intermediate fields, say $H = \mathrm{Gal}(E/F)$ and $H' = \mathrm{Gal}(E/F')$.*

1. *$F \subseteq F'$ if and only if $H \supseteq H'$.*
2. *$\mathrm{Gal}(E/FF') = H \cap H'$.*
3. *$\mathrm{Gal}(E/F \cap F')$ is the subgroup of G generated by H and H'.*

4. *$F|k$ is normal if and only if $H \triangleleft G$. Moreover, when that happens we have* $\mathrm{Gal}(F/k) \simeq G/H$*.*

Proof. The diagrams of the field extensions under consideration and the corresponding groups is as follows:



Part (*1*) is clear from the correspondence.

For part (*2*), note that $FF' = E^H E^{H'} \subseteq E^{H \cap H'}$. Using part (*1*), we get $H \cap H' \subseteq \mathrm{Gal}(E/FF')$. If σ is an automorphism of E fixing FF', then σ fixes F and F', and hence $\sigma \in H \cap H'$. Then $H \cap H' = \mathrm{Gal}(E/FF')$.

Using part (*1*) again, it is clear that $\langle H, H' \rangle \subseteq \mathrm{Gal}(E/F \cap F')$. Similarly, $E^{\langle H,H' \rangle} \subseteq F \cap F'$ and hence $\mathrm{Gal}(E/F \cap F') = \langle H, H' \rangle$.

Now for the first part of (*4*), suppose $F|k$ is normal. So, it is Galois, with $G' = \mathrm{Gal}(F/k)$. Then, $\varphi : G \to G'$ defined as $\phi(\sigma) = \sigma|_F$ is a group homomorphism with kernel H. So $H \triangleleft G$. Conversely, suppose that $F|k$ is not normal. Then, there is $\sigma : F \hookrightarrow E$ over k such that $\sigma F \neq F$. We may extend σ to E, an element of G. Now $\mathrm{Gal}(E/\sigma F) = \sigma \,\mathrm{Gal}(E/F)\sigma^{-1} = H^\sigma$, but $H^\sigma \neq H$. So H is not normal in G. For the second part, all we need is the surjectivity of φ. Let $\tau \in G'$. Then, τ extends to E. Then τ is the image of that extension under φ. ■

Proposition 2.1.5. *Let K/k be (finite) Galois extension with $G = \mathrm{Gal}(K/k)$, and let F/k be any field extension such that KF exists.*

1. *The extensions KF/F and $K/(F \cap K)$ are Galois. We let $H = \mathrm{Gal}(KF/F)$ and $H' = \mathrm{Gal}(K/F \cap K)$.*

2. *Define $\varphi : H \to G$ by $\varphi(\sigma) = \sigma|_K$. Then φ is an injective group homomorphism with $\mathrm{Im}(\varphi) = H'$. Moreover, $H \simeq H'$.*

3. $[KF : F] \mid [K : k]$.

Proof. We shall assume that $K|k$ is finite; the infinite case is correct, but its proof requires some less elementary tools.
(*1*) Done earlier.
(*2*) It is clear that φ is a homomorphism. If $\sigma \in \mathrm{Ker}(\varphi)$, then $\sigma|_K = \mathrm{Id}_K$. So σ is identity on KF and φ is injective. If $\sigma \in \mathrm{Im}(\varphi)$, then σ fixes $K \cap F$, and

$K \cap F \subseteq K^{\mathrm{Im}(\varphi)}$. Suppose $\alpha \in K^{\mathrm{Im}(\varphi)}$; so $\sigma(\alpha) = \alpha$ for every $\sigma \in \mathrm{Im}(\varphi)$. Such σ are of the form $\tau|_K$ for some $\tau \in H$. So elements of H also fix α and $\alpha \in (KF)^H = F$. This shows $\alpha \in K^{\mathrm{Im}(\varphi)} \subseteq K \cap F$ and $\alpha \in K^{\mathrm{Im}(\varphi)} = K \cap F = K^{H'}$. So $\mathrm{Im}(\varphi) = H'$. (Note that last step uses finiteness.)
(3) $[KF : F] = |H| = |H'| \mid |G| = [K : k]$.

■

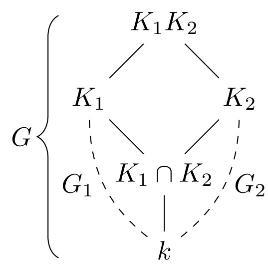
Proposition 2.1.6. *Let $K_1|k$ and $K_2|k$ be Galois with $G_1 = \mathrm{Gal}(K_1/k)$ and $G_2 = \mathrm{Gal}(K_2/k)$. Suppose K_1K_2 exists.*

1. *$K_1K_2|k$ is Galois. Let $G = \mathrm{Gal}(K_1K_2/k)$.*

2. *The map $\varphi : G \to G_1 \times G_2$ defined as $\varphi(\sigma) = (\sigma|_{K_1}, \sigma|_{K_2})$ is an injective group homomorphism.*

3. *If $K_1 \cap K_2 = k$, then φ is surjective.*

We have the following diagram,



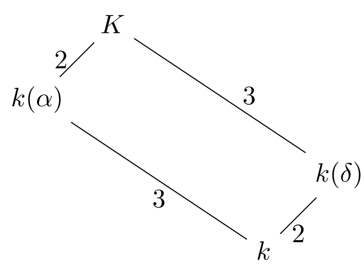
Proof. *(1)* is done before
(2) If σ is an automorphism of K_1K_2, then $\sigma|_{K_1}$ and $\sigma|_{K_2}$ determine σ. So, φ is injective.
(3) Kernel of φ is automorphisms of σ of K_1K_2 fixing K_1 and K_2. So if $K_1 \cap K_2 = k$, then $G_1 \simeq \mathrm{Gal}(K_1K_2/K_1)$ and $G_2 \simeq \mathrm{Gal}(K_1K_2/K_2)$ and φ is surjective. ■

2.2 Some Examples

Example 2.2.1 (Quadratic Extensions)**.** Let $[K : k] = 2$. Say $K = k + k\alpha$. Then, $K = k(\alpha)$ where α is the root of a degree two polynomial; say $f(X) = X^2 + aX + b$. Suppose $\mathrm{char}(k) \neq 2$. Then, $f(X) = \left(X + \frac{a}{2}\right)^2 - \left(\frac{a^2}{4} - b\right)$. Let $\beta = \alpha + \frac{a}{2}$. Then $\beta^2 = \frac{a^2}{4} - b \in k$ and $K = k(\alpha) = k(\beta)$. So K is generated over k by a square root of an element of k. Thus, at least in characteristic not equal to 2 case, quadratic extensions are of the form $K = k(\sqrt{A})$ where A is a non-square in k.[1] △

[1]What happens in characteristic 2?

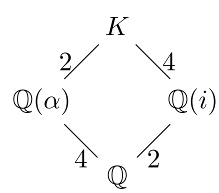
Example 2.2.2 (Cubic Extensions)**.** Assume $\mathrm{char}(k)$ is neither 2 nor 3, and let $f(X) = X^3 + aX + b$ be a polynomial in $k[X]$, that has no roots in k.[2] Let α be a root of f in $\overline{k}$ and let K be the splitting field of f. Then, $K|k$ is Galois, because f can't have multiple roots. Note that $[k(\alpha) : k] = 3$ and $k(\alpha) \subseteq K$. So, $3 \mid [K : k]$ and $[K : k] \mid 3! = 6$.[3] Therefore, $[K : k] = 3$ or $[K : k] = 6$. In the first case, $K = k(\alpha)$. Let $\alpha_1, \alpha_2, \alpha_3$ be the roots of f and let $\delta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)$ and $\Delta = \delta^2$. Put $G = \mathrm{Gal}(K/k)$. For any $\sigma \in G$ we have $\sigma(\delta) = \pm\delta$; so $\sigma(\Delta) = \Delta$. As a result $\Delta \in K^G = k$. Indeed, we may calculate it as $\Delta = -4a^3 - 27b^2$. If $\delta \notin k$, then $[k(\delta) : k] = 2$; and $\delta \in K$. So $[K : k] = 6$ and $G \simeq S_3$. So $K = k(\alpha, \delta)$ in this case and we have the following diagram



If $\delta \in k$, then $K = k(\alpha)$ ($\delta \in K^G$, hence $\sigma(\delta) = \delta$ for all $\sigma \in G$). So in that case $[K : k] = 3$ and $G \simeq A_3 \simeq C_3$.

△

Example 2.2.3 (A Degree 4 Polynomial)**.** Let $f(X) = X^4 - 2 \in \mathbb{Q}[x]$. Either by using Eisenstein Criterion or by writing down the roots, we see that f is irreducible over $\mathbb{Q}$. If $\alpha \in \mathbb{R}$ is a real root, then other roots are $-\alpha, i\alpha, -i\alpha$. So $K = \mathbb{Q}(\alpha, i)$ is the splitting field.



So $G = \mathrm{Gal}(f) := \mathrm{Gal}(K/k)$ has 8 elements.

Consider the following elements of G:

$$\tau(i) = -i \text{ and } \tau(\alpha) = \alpha$$

$$\sigma(i) = i \text{ and } \sigma(\alpha) = i\alpha$$

So, we see that

$$\tau\sigma(i) = -1 \text{ and } \tau\sigma(\alpha) = \tau(i\alpha) = -i\alpha$$

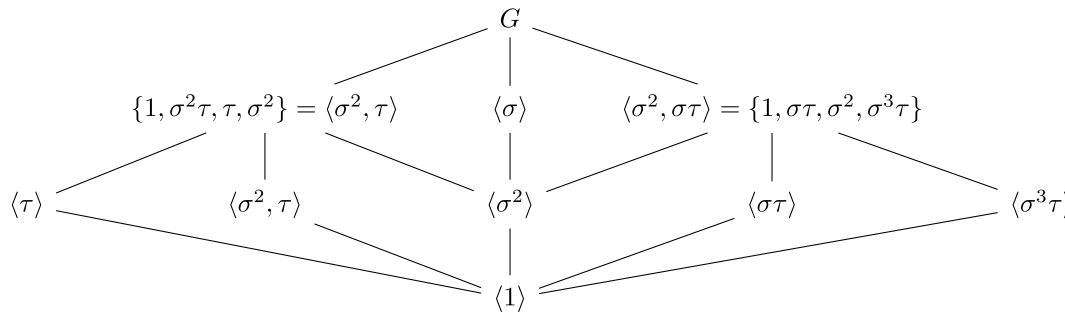
[2] What happened to X^2?

[3] Why?

$$\sigma^3\tau(i) = \sigma^3(-i) = -i \text{ and } \sigma^3\tau(\alpha) = \sigma^3(\alpha) = \sigma^2(i\alpha) = i\sigma^2(\alpha) = -i\alpha.$$

$\triangle$

Therefore, $\tau\sigma = \sigma^3\tau$, and $G \simeq D_4$. So we have the following diagram,



Now, we can find the corresponding intermediate fields. Clearly, G corresponds to $\mathbb{Q}$ and 1 corresponds to K. $\langle\sigma\rangle$ corresponds to $\mathbb{Q}(i)$ since σ fixes i and has order 4. $\langle\sigma^2, \tau\rangle$ corresponds to $\mathbb{Q}(\alpha^2)$ since all elements of $\langle\sigma^2, \tau\rangle$ fixes α and $[\mathbb{Q}(\alpha) : \mathbb{Q}(\alpha^2] = 2$. For similar reasons we see that $\langle\tau\rangle$ corresponds to $\mathbb{Q}(\alpha)$, $\langle\sigma^2, \sigma\tau\rangle$ corresponds to $\mathbb{Q}(i\alpha^2)$, $\langle\alpha^2\rangle$ corresponds to $\mathbb{Q}(i, \alpha^2)$ and $\langle\sigma^2\tau\rangle$ corresponds to $\mathbb{Q}(i\alpha)$. What about $\langle\sigma\tau\rangle$ and $\langle\sigma^3\tau\rangle$?

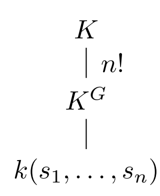
An example with $G \simeq S_n$:
Let $K = k(T_1, \ldots, T_n)$ where k is a field and $A = \{T_1, \ldots, T_n\}$ is a set of indeterminates that are algebraically independent over k. Let $G = S_n = S(A)$. Each element of G gives an automorphism of K; so we think it as a subgroup of $\mathrm{Aut}(K)$. Applying Artin's theorem, we get that $K|K^G$ is Galois with Galois group G. So we found an extension with Galois group S_n, but can we describe K^G? Yes, we can and we will!
Let

$$f(X) = \prod_{i=1}^{n}(X - T_i)$$

Note that K is the splitting field over K^G of $f(X)$, which is separable. Then,

$$f(X) = X^n \pm s_1(\overrightarrow{T})X^{n-1} \pm \cdots \pm s_i(\overrightarrow{T})X^{n-1} \pm \cdots \pm s_{n-1}(\overrightarrow{T})X \pm s_n(\overrightarrow{T})$$

where $s_1, \cdots, s_n$ are elementary symmetric polynomials in $\overrightarrow{T} = (T_1, \ldots, T_n)$, for instance, $s_1(\overrightarrow{T}) = \sum_{i=1}^{n} T_i$ and $s_n(\overrightarrow{T}) = T_1 \cdots T_n$. Now, we have,



Clearly, every element of G fixes each s_i (This is more or less the definition of s_i's). Thus $k(s_1, \ldots, s_n) \subseteq K^G$. Also $K|k(s_1, \ldots, s_n)$ is normal: it's the splitting field of f and it's degree is less than $n!$. So $K^G = k(s_1, \ldots, s_n)$.

Example 2.2.4 (A Degree 5 Example)**.** Let $f(X) = X^5 - 4X + 2 \in \mathbb{Q}[x]$; we see that it is irreducible, using Eisenstein Criterion. Let K be its splitting field. $f'(x) = 5X^4 - 4$. So, for $\alpha \in \mathbb{R}$, $f'(\alpha) = 0$ if and only if $\alpha = \sqrt[4]{\frac{4}{5}}$ or $\alpha = -\sqrt[4]{\frac{4}{5}}$. The other roots of $f'(X)$ are complex. Then, $f(X)$ has at most 3 real roots. Using Newton approximation, one may show that it has exactly 3 roots. Say the roots are $\alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_2$ where β_1 and β_2 are complex numbers that are not real numbers. Then $G = \mathrm{Gal}(K/\mathbb{Q})$ has an element switching β_1 and β_2, and fixing $\alpha_1, \alpha_2, \alpha_3$. In other words, the restriction of complex conjugation to K is in G. So it has a transposition. As $5 \mid |G|$[4], G has an element of order 5. So it's a cycle. It's easy to show that a 5-cycle and a transposition generates the whole S_5. So $G \simeq S_5$.

△

Example 2.2.5 (Cyclotomic Extensions)**.** Let k be a field of characteristic p, possibly $p = 0$. A *root of unity* in k is a root of the polynomial $X^n - 1$ in k for some $n > 0$; these roots are called *n^{th} roots of unity.* Put

$$\mu_n(k) = \{\alpha \in k : \ \alpha \text{ is an } n^{\text{th}} \text{ root of unity}\}.$$

Note that $|\mu_n(\overline{k})| = n$ if $p \nmid n$, because $X^n - 1$ is separable in that case. Also, $\mu_{p^n}(\overline{k}) = \{1\}$.

Clearly, $\mu_n(\overline{k})$ is a multiplicative group; hence it is cyclic. A generator is called a *primitive n^{th} root of unity*.

If $p \nmid m$, $p \nmid n$, and $\gcd(m, n) = 1$, then

$$\mu_{mn}(\overline{k}) \simeq \mu_m(\overline{k}) \times \mu_n(\overline{k}).$$

Let $\zeta \in \overline{k}$ be a primitive n^{th} root of unity, and consider $k(\zeta)$. Any conjugate of ζ under any embedding is again an n^{th} root of unity, and hence $k(\zeta)|k$ is normal and separable. Let $G = \mathrm{Gal}(k(\zeta)/k)$. Let $\sigma \in G$, then $\sigma(\zeta) = \zeta^i$ for some i. We need the order of ζ^i to be n as well; so it follows that $\gcd(i, n) = 1$. Also this i is determined up to a multiple of n. Then we have a group homomorphism:

$$\varphi : G \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$$
$$\sigma \longmapsto i(\sigma)$$

where $\sigma(\zeta) = \zeta^{i(\sigma)}$. This map is injective, so G is cyclic and $|G| \mid |(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n)$. Thus, $[k(\zeta) : k] \mid \varphi(n)$. In general, we don't have equality; for instance, $[\mathbb{R}(\zeta) : \mathbb{R}] = 2$ for any primitive n^{th} of unity ζ. One important case of the equality is as follows.

[4] Why?

Theorem 2.2.6. *Let $\zeta \in \mathbb{C}$ be a primitive n^{th} root of unity. Then $[\mathbb{Q}(\zeta) : \mathbb{Q}]$ is $\varphi(n)$.*

Proof. Let $f \in \mathbb{Q}[X]$ be the minimal polynomial of ζ over $\mathbb{Q}$. Then $X^n - 1 = f(X)h(X)$ for some $h \in \mathbb{Q}[X]$. By Gauss' lemma, $f, h \in \mathbb{Z}[X]$. It suffices to show that ζ^p is a root of f, where $p \nmid n$ is a prime, because that would mean that all the n^{th} primitive roots of unity are roots of f; then $\deg(f) \geq \varphi(n)$.
Suppose that ζ^p is not a root of f. Then it's a root of $h(x)$, and hence ζ is a root of $h(x^p)$. Then $f(X) \mid h(X^p)$. Say $h(X^p) = f(X)g(X)$ with $g \in \mathbb{Z}[X]$. Consider this equality modulo p:

$$\overline{h(X^p)} = \overline{f(X)} \cdot \overline{g(X)} \pmod{p}.$$

Then,

$$\overline{h(x^p)} = \overline{h(x)}^p = \overline{f(x)} \cdot \overline{g(x)} \pmod{p}.$$

Then $\overline{h(X)}$ and $\overline{f(X)}$ have a common root in $\overline{\mathbb{F}}_p$. This means that $X^n - 1$ has a double root in $\overline{\mathbb{F}}_p$; however this is not possible as $p \nmid n$. Hence ζ^p is a root of f. ■

△

2.3 Norm and Trace

Let $E|k$ be finite, $r = [E : k]_s$, $p^m = [E : k]_i$ and let $\{\sigma_1, \ldots, \sigma_r\}$ be the set of embeddings of E into $\overline{k}$, over k. For $\alpha \in E$, define

$$\mathrm{N}_{E/k}(\alpha) = \prod_{i=1}^{r} \sigma_i(\alpha)^{p^m} \text{ and } \mathrm{Tr}_{E/k}(\alpha) = [E : k]_i \sum_{i=1}^{r} \sigma_i(\alpha).$$

Note that $\mathrm{Tr}_{E/k}(\alpha) = 0$ if E is not a separable extension of k.

Proposition 2.3.1. *$\mathrm{N}_{E/k}$ is a multiplicative group homomorphism from $E^\times$ to $k^\times$.*

Proof. Let α, $\beta \in E^\times$. Then

$$\begin{aligned}\mathrm{N}_{E/k}(\alpha\beta) = \left(\prod_{i=1}^{r} \sigma_i(\alpha\beta)\right)^{p^m} &= \left(\prod_{i=1}^{r} \sigma_i(\alpha)\sigma_i(\beta)\right)^{p^m} \\ &= \left(\prod_{i=1}^{r} \sigma_i(\alpha)\right)^{p^m} \cdot \left(\prod_{i=1}^{r} \sigma_i(\beta)\right)^{p^m} \\ &= \mathrm{N}_{E/k}(\alpha) \cdot \mathrm{N}_{E/k}(\beta).\end{aligned}$$

Therefore $\mathrm{N}_{E/k}$ is multiplicative.

In order to show that $\mathrm{N}_{E/k}(\alpha)$ is in $k^\times$, note that α^{p^m} is separable over k and hence the normal closure of the extension $k(\alpha^{p^m})|k$ is also separable. So it is enough to show that $\mathrm{N}_{E/k}(\alpha)$ is fixed by each σ_i, but this is clear from the definition. ■

Proposition 2.3.2. $\mathrm{Tr}_{E/k}$ *is an additive group homomorphism from E into k.*

Proof. Similar to the proof above. ■

Let $E \supseteq F \supseteq k$ be a tower of fields. Then we have the norms $\mathrm{N}_{E/k}, \mathrm{N}_{E/F}, \mathrm{N}_{F/k}$. We claim that $\mathrm{N}_{E/k} = \mathrm{N}_{F/k} \circ \mathrm{N}_{E/F}$. Let $\sigma_1, \ldots, \sigma_r$ be the embeddings of E into $\overline{F}$ over F and $\tau_1, \ldots, \tau_s$ be the embeddings of F into $\overline{k}$ over k. Then,

$$\begin{aligned}
\mathrm{N}_{E/k}(\alpha) = \left(\prod_{j=1}^{s}\prod_{i=1}^{r}\tau_j\sigma_i\alpha\right)^{[E:k]_i} &= \left(\prod_{j=1}^{s}\tau_j\left(\prod_{i=1}^{r}\sigma_i\alpha\right)^{[E:F]_i}\right)^{[F:k]_i} \\
&= \left(\prod_{j=1}^{s}\tau_j\,\mathrm{N}_{E/F}(\alpha)\right)^{[F:k]_i} \\
&= \mathrm{N}_{F/k}(\mathrm{N}_{E/F}(\alpha)).
\end{aligned}$$

Similarly, $\mathrm{Tr}_{E/k} = \mathrm{Tr}_{F/k} \circ \mathrm{Tr}_{E/F}$.

Let $E = k(\alpha)$ and let $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in k[X]$ be the minimal polynomial of α over k. Also let $\alpha_1, \ldots, \alpha_r$ be the distinct roots of f in $\overline{k}$. Then

$$f(x) = \left(\prod_{i=1}^{r}(X - \alpha_i)\right)^{[E:k]_i}.$$

Then

$$\mathrm{N}_{E/k}(\alpha) = (\alpha_1 \cdots \alpha_r)^{[E:k]_i} = (-1)^n a_0 \text{ and } \mathrm{Tr}_{E/k}(\alpha) = -a_{n-1}.$$

Therefore, we have:

1. $\mathrm{N}_{E/k}(\alpha) = \alpha^{[E:k]}$.
2.
$$\begin{aligned}
\mathrm{N}_{E/k}(\alpha) &= \mathrm{N}_{k(\alpha)/k}(\mathrm{N}_{E/k(\alpha)}(\alpha)) \\
&= \mathrm{N}_{k(\alpha)/k}(\alpha^{[E:k(\alpha)]}) \\
&= \left((-1)^{[k(\alpha):k]}a_0\right)^{[E:k(\alpha)]} \\
&= (-1)^{[E:k]}\, a_0^{[E:k]/[k(\alpha):k]}.
\end{aligned}$$

   (Note that $[k(\alpha) : k]$ is the degree of the minimal polynomial.)

3. $\mathrm{Tr}_{E/k}(\alpha) = n\alpha$ if $\alpha \in k$.
4. $\mathrm{Tr}_{E/k}(\alpha) = -[E : k(\alpha)]a_{n-1}$.
5. $\mathrm{Tr}_{E/k}$ is k-linear.

Proposition 2.3.3. *Let $E|k$ be finite separable. Then $(x, y) \mapsto \mathrm{Tr}_{E/k}(xy)$ is a bilinear map from $E \times E$ to k.*

Proof. Clear. ∎

As a result, if $E|k$ is finite, then

$$\begin{aligned} \mathrm{Tr} : E &\longrightarrow E^* \\ x &\longmapsto \mathrm{Tr}_x \end{aligned}$$

is a k-linear map, where Tr_x is a map from E to k defined as $y \mapsto \mathrm{Tr}_{E/k}(xy)$. Suppose that $E|k$ is also separable and let $x \in \mathrm{Ker}(\mathrm{Tr})$; so $\mathrm{Tr}_{E/k}(xE) = 0$. If $x \neq 0$, then $xE = E$, and hence $\mathrm{Tr}_{E/k}(xE) = \mathrm{Tr}_{E/k}(E) \neq 0$. So Tr is injective and it is an isomorphism of k-linear spaces because of dimension reasons. Hence E is identified with E^* via Tr.[5]

2.4 Characters

Let G be a monoid and let K be a field. A *character of G in K* is a group homomorphism

$$\chi : G \longrightarrow K^\times.$$

Character that maps every element of G to 1 is called the *trivial character.*

Theorem 2.4.1. *Let $\chi_1, \ldots, \chi_n$ be distinct characters of G in K. Then they are linearly independent over K; that is if there are $a_1, \ldots, a_n \in K$ such that $a_1\chi_1 + \cdots + a_n\chi_n$ is identically 0, then $a_i = 0$ for all i.*

Proof. Assume that a non-zero K-linear combination of distinct characters of G is zero and let n be the smallest positive integer such that there are distinct $\chi_1, \ldots, \chi_n$ and $a_1, \ldots, a_n \in K^\times$ such that $a_1\chi_1 + \cdots + a_n\chi_n$ is identically 0. Let $g \in G$ such that $\chi_1(g) \neq \chi_2(g)$. Then

$$a_1\chi_1(gx) + a_2\chi_2(gx) + \cdots + a_n\chi_n(gx) = 0$$

for all $x \in G$. So after dividing by $\chi_1(g)$:

$$a_1\frac{\chi_1(g)}{\chi_1(g)}\chi_1(x) + a_2\frac{\chi_2(g)}{\chi_1(g)}\chi_2(x) + \cdots + a_n\frac{\chi_n(g)}{\chi_1(g)}\chi_n(x) = 0$$

for every $x \in G$. We also have

$$a_1\chi_1(x) + a_2\chi_2(x) + \cdots + a_n\chi_n(x) = 0.$$

[5] E^* is the dual space of E.

Hence, we get

$$a_2\left(\frac{\chi_2(g)}{\chi_1(g)}-1\right)\chi_2(x)+\cdots+a_n\left(\frac{\chi_n(g)}{\chi_1(g)}-1\right)\chi_n(x)=0$$

which contradicts the minimality of n since $a_2\left(\frac{\chi_2(g)}{\chi_1(g)}-1\right)\neq 0$. ■

An application of the linear independence of characters is as follows.

Proposition 2.4.2. *Let $E|k$ be a finite separable extension and $\sigma_1,\ldots,\sigma_n$ be distinct embeddings of E into $\overline{k}$ over k. If $\{w_1,\ldots,w_n\}$ is a basis of E over k, then $\xi_i=(\sigma_j w_i)_{i=1,\ldots,n}\in E^n$ are linearly independent over E for $j=1,\ldots,n$.*

Proof. Let $\alpha_1,\ldots,\alpha_n\in E$ be such that $\alpha_1\xi_1+\cdots+\alpha_n\xi_n=\overrightarrow{0}$. Then

$$(\alpha_1\sigma_1+\cdots+\alpha_n\sigma_n)(w_i)=0$$

for all i. Then $\alpha_1\sigma_1+\cdots+\alpha_n\sigma_n$ is identically zero. Since $\sigma_1|_{E^\times},\ldots,\sigma_n|_{E^\times}$ are characters, by the linear independence of characters we get $\alpha_i=0$ for all i. ■

Let $E|k$ be finite and let $\alpha\in E$. Consider the k-linear map:

$$\begin{aligned} m_\alpha : E &\longrightarrow E \\ x &\longmapsto \alpha\, x \end{aligned}\quad .$$

Let M_α be the matrix of m_α for a given basis. We claim that $\det(M_\alpha)=\mathrm{N}_{E/K}(\alpha)$.

First, let $E=k(\alpha)$ and let $X^d+a_{d-1}X^{d-1}+\cdots+a_1X+a_0$ be the minimal polynomial of α over k, Then the matrix M_α of m_α with respect to the basis $1,\alpha,\ldots,\alpha^{d-1}$ is

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0\\ 1 & 0 & \cdots & 0 & -a_1\\ 0 & 1 & \cdots & 0 & -a_2\\ \vdots & \vdots & \ddots & \vdots & \vdots\\ 0 & 0 & \cdots & 1 & -a_{d-1}\end{pmatrix}.$$

Hence, we see that $\det(M_\alpha)=(-1)^{d-1}(-a_0)=(-1)^d a_0=\mathrm{N}_{k(\alpha)/k}(\alpha)$.

In general: $\mathrm{N}_{E/k}(\alpha)=\left((-1)^d a_0\right)^{[E:k]/d}$. Let $w_1,\ldots,w_k$ be a basis of E over $k(\alpha)$. Then $\{\alpha^i w_j : i=0,1,\ldots,d-1, j=1,\ldots,k\}$ is a basis of E over k. Now

$m_\alpha(\alpha^i w_j) = \alpha^{i+1} w_j$ for $i = 1, \dots, d-1$. Then M_α with respect to this basis is:

$$\begin{pmatrix} \begin{matrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{d-1} \end{matrix} & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & \begin{matrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{d-1} \end{matrix} & \cdots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & \cdots \end{pmatrix}$$

Now we see that $\det(M_\alpha) = \left((-1)^d a_0\right)^{[E:k]/d} = \mathrm{N}_{E/k}(\alpha)$.

Using the same bases, one can easily show that $\mathrm{Tr}_{E/k}(\alpha) = \mathrm{Tr}(M_\alpha)$.

2.5 Cyclic Extensions

For an adjective A that is applicable to groups, we say that an extension is A if it is Galois and its Galois group is A.

Our aim is to determine finite cyclic extensions. Our main tool is the following.

Theorem 2.5.1 (Hilbert's 90). *Let $K|k$ be cyclic of order n; say* $\mathrm{Gal}(K/k) = \langle\sigma\rangle$. *Let $\alpha \in K$. Then $\mathrm{N}_{K/k}(\alpha) = 1$ if and only if $\alpha = \frac{\beta}{\sigma\beta}$ for some $\beta \in K^\times$.*

Proof. Sufficiency is clear. For the necessity, we first observe that the automorphisms $\mathrm{Id}_K, \sigma, \sigma^2, \dots, \sigma^{n-1}$ are linearly independent over K. Let $a_1 = 1, a_2 = \alpha, a_3 = \alpha\sigma(\alpha), \dots, a_n = \alpha\sigma(\alpha)\cdots\sigma^{n-2}(\alpha)$. These are all elements of $K^\times$. We know that the linear combination $a_1 \mathrm{Id}_K + a_2\sigma + \cdots + a_n\sigma^{n-1}$ is not identically 0. So take $\theta \in K$ such that

$$\beta := \theta + \alpha\sigma(\theta) + \alpha\sigma(\alpha)\sigma^2(\theta) + \cdots + \alpha\sigma(\alpha)\cdots\sigma^{n-2}(\alpha)\sigma^{n-1}(\theta) \neq 0.$$

We claim that $\alpha = \frac{\beta}{\sigma\beta}$. Since $\mathrm{N}_{K/k}(\alpha) = \alpha\sigma(\alpha)\cdots\sigma^{n-1}(\alpha)$ and $\sigma^n(\theta) = \theta$, we have

$$\begin{aligned} \sigma\beta &= \sigma(\theta) + \sigma(\alpha)\sigma^2(\theta) + \cdots + \alpha\sigma(\alpha)\cdots\sigma^{n-1}(\alpha)\sigma^n(\theta) \\ &= \sigma(\theta) + \sigma(\alpha)\sigma^2(\theta) + \cdots + \alpha\sigma(\alpha)\cdots\sigma^{n-2}(\alpha)\sigma^{n-1}(\theta) + \mathrm{N}_{K/k}(\alpha)\theta. \end{aligned}$$

Then $\alpha = \frac{\beta}{\sigma\beta}$ as $\mathrm{N}_{K/k}(\alpha) = 1$. ■

A characterization of cyclic extensions in a certain special case is as follows.

Theorem 2.5.2. *Let k be a field and n be a natural number such that* $\mathrm{char}(k) \nmid n$. *Suppose that k contains a primitive n^{th} root of unity, say ζ.*

1. *If $K|k$ is cyclic of order n, then $K = k(\beta)$ for some $\beta \in K$ which is a root of $X^n - a$ for some $a \in k$.*

2. *If $\alpha \in \overline{k}$ is a root of $X^n - a$ for some $a \in k$, then $k(\alpha)|k$ is cyclic of order $d \mid n$. Moreover $\alpha^d \in k$.*

Proof. (*1*) Let $\mathrm{Gal}(K/k) = \langle\sigma\rangle$. Note that $\mathrm{N}_{K/k}(\zeta) = \zeta^n = 1$ and $\mathrm{N}_{K/k}(\zeta^{-1}) = 1$. So by Hilbert's 90, $\zeta^{-1} = \frac{\beta}{\sigma\beta}$ for some $\beta \in K^\times$, and $\sigma\beta = \zeta\beta$ and $\sigma^i(\beta) = \beta\zeta^i$ for $i = 1, \ldots, n$. So $\beta, \beta\zeta, \ldots, \beta\zeta^{n-1}$ are conjugate over k. Then $[k(\beta) : k] \geq n$ and $k(\beta) = K$. Note that $\sigma(\beta^n) = (\sigma\beta)^n = \beta^n\zeta^n = \beta^n$. Then $a = \beta^n \in k$ and β is a root of $X^n - a$.
(*2*) Let α be a root of $X^n - a$. Then $\zeta^i\alpha$ are also roots of $X^n - a$. Then $k(\alpha)|k$ is Galois; say $G = \mathrm{Gal}(k(\alpha)/k)$. Let $\sigma \in G$. Then $\sigma\alpha$ is a root of $X^n - a$, as well. Then $\sigma\alpha = \zeta_\sigma\alpha$ for some n^{th} root of unity ζ_σ. This gives an injective group homomorphism

$$G \longrightarrow \mu_n(k).$$

So G is cyclic. If $|G| = d$, then $d|n$. For a generator σ of G, we have that ζ_σ is a primitive d^{th}-root of unity, and $\sigma(\alpha)^d = (\sigma\alpha)^d = (\zeta_\sigma\alpha)^d = \alpha^d$. So $\alpha^d \in k$. ■

Theorem 2.5.3 (Hilbert's 90 – Additive Form)**.** *Let $K|k$ be cyclic of order n and let σ be a generator of* $\mathrm{Gal}(K/k) = \langle\sigma\rangle$. *Let $\beta \in K$. Then* $\mathrm{Tr}_{K/k}(\beta) = 0$ *if and only if $\beta = \alpha - \sigma\alpha$ for some $\alpha \in K$.*

Proof. Sufficiency is clear, we prove the necessity. Take some $\theta \in K$ with $\mathrm{Tr}_{K/k}(\theta) \neq 0$. We can take a such θ since Tr is not identically 0. Let

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

Then

$$\sigma\alpha = \frac{\sigma(\beta)\sigma^2(\theta) + (\sigma(\beta) + \sigma^2(\beta))\sigma^3(\theta) + \cdots + (\sigma(\beta) + \sigma^2(\beta) + \cdots + \sigma^{n-1}(\beta))\sigma^n(\theta)}{\mathrm{Tr}(\theta)}.$$

Now we see that $\sigma(\beta) + \sigma^2(\beta) + \cdots + \sigma^{n-1}(\beta) = -\beta$. So, we have

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

■

Theorem 2.5.4 (Artin-Schreier)**.** *Let k be a field of characteristic p.*

1. *Let $K|k$ be cyclic of degree p. Then there is $\alpha \in K$ such that $K = k(\alpha)$ and α is a root of $X^p - X - a$ for some $a \in k$.*

2. *If $\alpha \in \overline{k}$ is a root of an irreducible polynomial of the form $X^p - X - a$ for some $a \in k$, then $k(\alpha)|k$ is cyclic of order p.*

Proof. (*1*) Let $G = \mathrm{Gal}(K/k) = \langle \sigma \rangle$. $\mathrm{Tr}_{K/k}(-1) = p(-1) = 0$. So $1 = \sigma\alpha - \alpha$ for some $\alpha \in K$. So $\sigma\alpha = \alpha + 1$ and $\sigma^i(\alpha) = \alpha + i$ for each $i \in \{0, 1, \ldots, p-1\}$. These are all distinct conjugates of α. So $[k(\alpha) : k] \geq p$ and $k(\alpha) = K$.

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

So $a = \alpha^p - \alpha \in k$ and hence α is a root of $X^p - X - a$.
(*2*) If $\alpha \in \overline{k}$ is a root of $X^p - X - a$, then each $\alpha + i$ is a root of $X^p - X - a$ for $i = 0, \ldots, p-1$. So these are exactly the roots. As $X^p - X - a$ is assumed to be irreducible in $k[X]$, we get that $k(\alpha)|k$ is Galois of degree p; so it's cyclic. ∎

In the second part of this result the polynomial $X^p - X - a$ is assumed to be irreducible. We claim that if no root of $f(X) = X^p - X - a$ is in k, then it is irreducible. Suppose $f(X) = g(X)h(X)$, where $\deg(g), \deg(h) < p$; Let $d = \deg(g)$. So $g(X)$ is a product of $X - \alpha - i$ for d many i's. The coefficient of X^{d-1} is $-d\alpha + j$ for some j. But this element is not in k unless $d = 0$. So $X^p - X - a$ is irreducible over k.

2.6 Solvability By Radicals

Let $F|k$ be a finite separable extension of fields of characteristic $p \geq 0$. We say $F|k$ is *solvable by radicals* if there is a finite extension $E|k$ with $F \subseteq E$ and there is a tower $k = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_{n-1} \subseteq E_n = E$ of intermediate fields such that E_{i+1} is obtained from E_i by one of the following:

(i) Adjoining a root of unity.

(ii) Adjoining a root of $X^n - a$ where $a \in E_i$ and $p \nmid n$.

(iii) Adjoining a root of $X^p - X - a$ with $a \in E_i$.

Observe that (i) is a part of (ii), but we still want to isolate the case of adding a root of unity. Note that (iii) appears only when $p > 0$.

Recall that a group G is *solvable* if there is a tower

$$1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_{m-1} \triangleleft G_m = G$$

such that G_{i+1}/G_i is abelian for $i = 0, \ldots, m-1$.

Recall also the following facts about solvable groups:

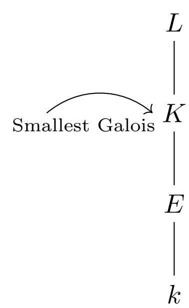
1. If G is finite solvable, then we can refine the tower in a way that G_i/G_{i+1} are cyclic.

2. Let G be a group with $H \triangleleft G$. Then G is solvable if and only if H and G/H are solvable.

3. S_n is not solvable for $n \geq 5$.

Definition. Let $E|k$ be a finite extension. $E|k$ is *solvable* if the smallest Galois extension $K|k$ with $E \subseteq K$ is solvable. $\diamond$

Note that "smallest" is not necessary; i.e. if there is a solvable Galois extension $K|k$ with $E \subseteq K$, then $E|k$ is solvable. If we have tower as the following,



we have $\mathrm{Gal}(L/k) \subseteq \mathrm{Gal}(L/K) \simeq \mathrm{Gal}(L/k)/\,\mathrm{Gal}(K/k)$.

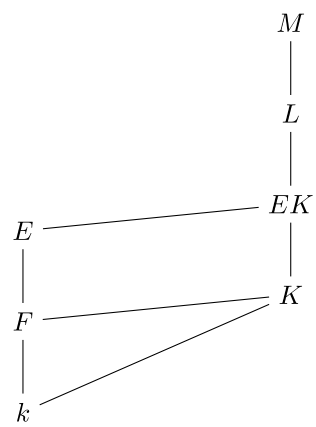
Proposition 2.6.1.

1. *Let $k \subseteq F \subseteq E$ be fields. $E|k$ is solvable if and only if $E|F$ and $F|k$ are solvable.*

2. *Let $E|k$ be solvable and $F|k$ be arbitrary. Then $EF|F$ is solvable.*

Proof. (*2*) Let $K|k$ be solvable with $E \subseteq K$. Then $KF|F$ is Galois and $\mathrm{Gal}(KF/F)$ embeds into $\mathrm{Gal}(K/k)$. So $\mathrm{Gal}(KF/F)$ is solvable and since $EF \subseteq KF$, we have $EF|F$ is solvable.

(*1*) It is clear that $E|F$ and $F|k$ are solvable if $E|k$ is. For the other implication, let $E|F$ and $F|k$ be solvable. Let $K \supseteq F$ be such that $K|k$ is Galois and solvable. Also by (*2*), $EK|K$ is solvable. Let $L \supseteq EK$ be such that $L|K$ is Galois and $\mathrm{Gal}(L/K)$ is solvable. Let $\sigma : L \to \overline{k}$ over k. Then $\sigma K = K$ as K/k is Galois. So $\sigma L|K$ is solvable. Let M be the composition of the fields σL. Then $M|k$ is Galois; hence $M|K$ is Galois and $\mathrm{Gal}(M/K) \subseteq \prod_\sigma \mathrm{Gal}(\sigma L/K)$ is solvable. Consider $\mathrm{Gal}(M/k) \to \mathrm{Gal}(K/k)$ given as restriction. It is a surjective group homomorphism and it's kernel is normal in $\mathrm{Gal}(M/k)$ and it's isomorphic to $\mathrm{Gal}(M/k)$. So $\mathrm{Gal}(M/k)/\ker \simeq \mathrm{Gal}(K/k)$. Then by the fact (*2*) above, $\mathrm{Gal}(M/k)$ is solvable, finishing the proof.



∎

Theorem 2.6.2. *Let $K|k$ be a finite extension of characteristic $p \geq 0$. Then $K|k$ is solvable if and only if it is solvable by radicals.*

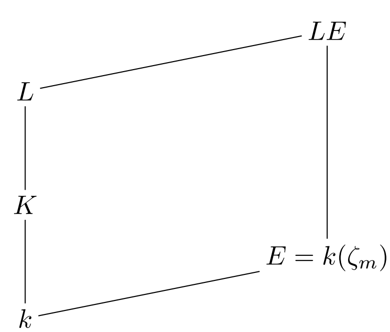
Proof. First suppose that $K|k$ is solvable and let $L|k$ be Galois with solvable Galois group and $L \supseteq K$. Let m be the product of all primes dividing $[L : k]$ and not equal to p. Let ζ_m be the primitive m^{th} root of unity, and put $E = k(\zeta_m)$. Then $LE|E$ is Galois and solvable; say $G = \mathrm{Gal}(LE/E)$. Then there is a tower

$$\{1\} = G_n \lhd G_{n-1} \lhd \cdots \lhd G_1 \lhd G_0 = G$$

such that G_i/G_{i+1} is cyclic. By the correspondence, we get intermediate fields

$$E = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_{n-1} \subseteq E_n = LE$$

such that $\mathrm{Gal}(E_{i+1}/E_i) \simeq G_i/G_{i+1}$, hence cyclic. Therefore using earlier results on cyclic extensions, we see that E_{i+1} is obtained from E_i by adjoining a root of a polynomial either of the form $X^n - a$ or of the form $X^p - X - a$, where $a \in E_i$. Since $E|k$ is clearly solvable by radicals, we see that $K|k$ is solvable by radicals.



Now let $K|k$ be solvable by radicals, then the normal closure, say L, of $K|k$ is also solvable by radicals. Again, let m be the product of all primes dividing $[L : k]$ and not equal to p and let ζ_m be the primitive m^{th} root of unity. Put $F = k(\zeta_m)$. It suffices to prove that $LF|F$ is solvable[6]. Tthis again follows from previous theorems on cyclic extensions. ■

Theorem 2.6.3. *Let k be any field, $n > 1$, $a \in k^\times$. Suppose that $a \notin k^p$ for any prime $p \mid n$, and $a \notin -4k^4$ if $4 \mid n$. Then $X^n - a$ is irreducible in $k[X]$.*

Proof. We proceed by induction on n. The case $n = 2$ is clear.

Step 1: (Reduction to the case that n is a prime power)

Let $n = p^r \cdot m$, $p \nmid m$, $p \neq 2$. Suppose that $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_m$ are the roots of $X^m - a$ with possible repetitions. By induction $X^m - a$ is irreducible. Write

$$X^n - a = \left(X^{p^r}\right)^m - a = \prod_{i=1}^{m} \left(X^{p^r} - \alpha_i\right).$$

If $\alpha = \beta^p$ in $k(\alpha)$, then

$$\begin{aligned} -a = (-1)^m \operatorname{N}_{k(\alpha)/k}(\alpha) &= (-1)^m \operatorname{N}_{k(\alpha)/k}(\beta^p) \\ &= (-1)^m \operatorname{N}_{k(\alpha)/k}(\beta)^p \end{aligned}$$

If m is odd, then $a \in k^p$, and if m is even, then $a = -\operatorname{N}_{k(\alpha)/k}(\beta)^p \in k^p$. So $\alpha \notin k/\alpha)^p$.

As a result, if we know that $X^{p^r} - a$ is irreducible in $k(\alpha)[X]$, then we would have concluded that

$$\begin{aligned} [k(\beta) : k] &= [k(\beta) : k(\alpha)] \cdot [k(\alpha) : k] \\ &= p^r \cdot m = n \end{aligned}$$

where β is a root of $X^{p^r} - \alpha$. Then $X^n - a$ would be the minimal polynomial of β over k, and hence $X^n - a$ would be irreducible in $k[X]$.

Step 2: ($X^{p^r} - a$ is irreducible in $k[X]$)

Case 1: ($p = \operatorname{char}(k)$)

$$X^{p^r} - a = \left(X^{p^{r-1}} - \alpha\right)^p$$

where $\alpha^p = a$. By induction $\left(X^{p^{r-1}} - \alpha\right)^p$ is irreducible in $k(\alpha)[X]$, hence $X^p - a$ is irreducible in $k[X]$.

Case 2: ($p \nmid \operatorname{char}(k)$)
Let α be a root of $x^p - a$. If $x^p - a$ is not irreducible in $k[x]$ then $[k(\alpha) : k] = d < p$. Then, $d = \operatorname{N}_{k(\alpha)/k}(\alpha^p) = \operatorname{N}_{k(\alpha)/k}(\alpha)^p \in k^p$ and hence $a \in k^p$. Therefore $X^p - a$ is irreducible.

[6] Why?

We proceed by induction on r with $r = 1$ case being the previous paragraph. Let $\alpha_1, \dots, \alpha_p \in \overline{k}$ be the roots of $X^p - a$. Then,

$$X^p - a = \prod_{i=1}^{p} \left(X^{p^{r-1}} - \alpha_i \right)$$

Case a: $(\alpha \notin k(\alpha)^p)$
Let β be a root of $X^{p^{r-1}} - \alpha$. If $p \neq 2$, then

$$[k(\beta) : k(\alpha)] = p^{r-1}$$

and

$$[k(\beta) : k] = p^{r-1} \cdot p = p^r$$

This shows that $x^{p^r} - a$ is irreducible in $k[x]$.
If $p = 2$ and let $\beta \in k(\alpha)$ be such that $\alpha = -4\beta^4$. Then

$$-a = \mathrm{N}_{k(\alpha)/k}(\alpha) = 16\,\mathrm{N}_{k(\alpha)/k}(\beta)^4$$

is a square in k and $\sqrt{-1} \in k(\alpha)$. Then $\alpha = \left(\sqrt{-1}2\beta^2\right)^2$ is a contradiction.

Case b: $(\alpha \in k(\alpha)^p)$
Say $\alpha = \beta^p$ with $\beta \in k(\alpha)$. Now

$$-a = (-1)^p\,\mathrm{N}_{k(\alpha)/k}(\alpha) = (-1)^p\,\mathrm{N}(\beta)^p$$

If $p \neq 2$, then $a \in k^p$ and we get a contradiction once again. Let $p = 2$. Then, $-a = \mathrm{N}(\beta)^2$, put $b = \mathrm{N}(\beta) \in k$. So $-1 \notin k^2$, let $i \in \overline{k}$ be with $i^2 = -1$. Then

$$\begin{aligned} X^{2^r} - a &= X^{2^r} + b^2 \\ &= \left(X^{2^{r-1}} + ib\right)\left(X^{2^{r-1}} - ib\right) \end{aligned}$$

in $k(i)[X]$. By induction, if $X^{2^{r-1}} + ib$ or $X^{2^{r-1}} - ib$ is not irreducible in $k(i)[X]$, then either $\pm ib \in k(i)^2$ or $\pm ib \in -4k(i)^4$. So in that case $\pm ib$ is a square in $k(i)$; say $\pm ib = (c + di)^2 = c^2 - d^2 + 2cdi$ with $c, d \in k$. Then $c^2 = d^2$ and hence $d = \pm c$ and $\pm ib = 2cdi = \pm 2c^2 i$. But then $a = -b^2 = -4c^4 \in -4k^4$. So $x^{2^{r-1}} \pm ib$ are irreducible in $k(i)[X]$. Therefore $X^{2^r} - a$ is irreducible in $k[X]$. ■

As an example, note that $X^4 + 4b^4 = \left(X^2 + 2bX + 2b^2\right)\left(X^2 - 2bX + 2b^2\right)$. So $X^{4m} - a$ is irreducible in $k[X]$ if we choose $a \in -4k^4$. Therefore the assumptions of the theorem are tight.

A particular case of the theorem is when $a \notin k^p$ for some odd prime p. In that case, $x^{p^r} - a$ is irreducible in $k[x]$ for all $r \geq 1$.

Corollary 2.6.4. *Let k be a field of characteristic 0 such that $[\overline{k} : k]$ is finite. Then either k is algebraically closed or $\overline{k} = k(i)$ with $i^2 = -1$. In other words, if $[\overline{k} : k]$ is finite, then it's either 1 or 2.*

Proof. Clearly $\overline{k}|k$ is a Galois extension. Put $k_1 = k(i)$ with $i^2 = -1$. Let $G = \mathrm{Gal}(\overline{k}/k_1)$; say $|G| = n$. Suppose that $n \neq 1$ and take p, a prime dividing n. Let $H \leqslant G$ with $|H| = p$ and let $F = \overline{k}^H$. Since $[\overline{k} : F] = p$, we have that $\mu_p(\overline{k}) \subseteq F$; otherwise there is an intermediate field, namely $F(\zeta_p)$, which is of degree $p-1$. Then by the earlier theorem about cyclic extensions we have that $\overline{k}$ is the splitting field of $x^p - a$ over F for some $a \in F$. Then $x^{p^2} - a$ is reducible in $F[x]$. Then $p = 2$ and $a \in -4F^4$. This forces i not to be in F. This is a contradiction; so $n = 1$ and hence $\overline{k} = k(i)$. If $i \in k$, then $\overline{k} = k$; otherwise $[\overline{k} : k] = 2$. ■

As a matter of fact, we do not have to assume that characteristic is 0. It follows from the assumption that $[\overline{k} : k]$ is finite and not 1. See page 299 of [3] for details.

Theorem 2.6.5 (Normal Basis Theorem)**.** *Let $K|k$ be a finite Galois extension with $G = \mathrm{Gal}(K/k) = \{\sigma_1, \dots, \sigma_n\}$. Suppose that k is infinite. Then there is $w \in K$ such that $\sigma_1(w), \dots, \sigma_n(w)$ is a linear basis of K over k.*

Proof. Let $K = k(\alpha)$ and let $f(X) \in k[X]$ be the minimal polynomial of α. Without loss of generality assume that σ_1 is the identity. Define

$$g(X) = \frac{f(X)}{(X-\alpha)f'(\alpha)}$$

a polynomial in $K[X]$. Note that for $i = 1, \dots, n$

$$\sigma_i g(X) = \frac{f(X)}{(X-\alpha_i)f'(\alpha_i)}$$

where $\alpha_i = \sigma_i(\alpha)$. In addition, $g(\alpha) = 1$ and $\sigma_i g(\alpha) = 0$ for $i \neq 1$.[7] Now let $D(X) = \det\left(\sigma_i\sigma_j g(X)\right)_{i,j\in\{1,\dots,n\}}$. Note that $D(X)$ is a polynomial, and $D(\alpha) = \pm 1 \neq 0$. So $D(X) \not\equiv 0$, and hence we may take $a \in k$ such that $D(a) \neq 0$. Put $w = g(a)$. We'd like to show that $w, \sigma_2(w), \dots, \sigma_n(w)$ are linearly independent over k.

Suppose that $b_1 w + b_2\sigma_2(w) + \cdots + b_n\sigma_n(w) = 0$. For $i = 1, \dots, n$, applying σ_i to this equality we get

$$b_1\sigma_i(w) + b_2\sigma_i\sigma_2(w) + \cdots + b_n\sigma_i\sigma_n(w) = 0$$

Then,

$$\left(\sigma_i\sigma_j g(x)\right)_{i,j\in\{1,\dots,n\}} \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Since $\left(\sigma_i\sigma_j g(X)\right)_{i,j\in\{1,\dots,n\}}$ is invertible, we get that $b_i = 0$ for $i = 1, \dots, n$. So $w, \sigma_2(w), \dots, \sigma_n(w)$ are linearly independent over k. ■

[7] Note that $\sigma_i g(\alpha) \neq \sigma_i(g(\alpha))$

A basis of K as a vector space over k of the form $\sigma_1(w), \ldots, \sigma_n(w)$ is called a *normal basis*. As an example, Let's consider the case of a quadratic extension $K = k(\sqrt{d})$ for some $d \in k \setminus k^2$. Then $\mathrm{Gal}(K/k) = \{\mathrm{id}, \sigma\}$ where $\sigma(\sqrt{d}) = -\sqrt{d}$. We'd like to find $w = a + b\sqrt{d}$ such that w and $\sigma(w) = a - b\sqrt{d}$ are linearly independent over k. Note that we can't take $a = 0$ or $b = 0$. So suppose $a \neq 0$ and $b \neq 0$ and let $c(a + b\sqrt{d}) + d(a - b\sqrt{d}) = 0$ with $c, d \in k$. Then $a(c + d) = 0$ and $b(c - d) = 0$. So $c + d = c - d = 0$ and hence $c = d = 0$. Therefore, in this case, any $w = a + b\sqrt{d}$ with $a \neq 0$, $b \neq 0$ gives a normal basis.

2.7 Generic Resolvent

Let $\vec{X} = (X_1, \ldots, X_n)$ be a tuple of independent variables, and let k be a field. Most of the time, we'll assume that $\mathrm{char}(k) = 0$ to avoid separability issues.

Put $L = k(\vec{X})$ and $K = k(s_1, \ldots, s_n)$, where $s_i(\vec{X})$ is the elementary symmetric polynomial of degree i. Recall that $L|K$ is Galois and $\mathrm{Gal}(L/K) \simeq S_n$. From now on, we identify these groups. So S_n acts on L by permuting X_i's. Now put

$$\theta(T) = (T - X_1) \cdots (T - X_n) = \sum_{i=0}^{n} (-1)^n s_i T^{n-i} \in K[T].$$

So L is the splitting field of $\theta(T)$ over K. Let $H \leqslant S_n$ and put $F = L^H$. Hence $L|F$ is Galois with $\mathrm{Gal}(L/F) = H$. Write $F = K(\alpha)$ for some $\alpha \in F$. This α is called a *generic resolvent* for H.

Example 2.7.1. Let $H = A_n$. In this case, $A_n \triangleleft S_n$; so $F|K$ is Galois with $\mathrm{Gal}(F/K) \simeq S_n/A_n \simeq C_2$. So α must have degree 2 over K. We may determine it to be $\Delta = \prod_{i<j} X_i - X_j$. Clearly, Δ is fixed exactly by elements of A_n and then $\Delta^2 \in K$ and $F = K(\Delta)$. △

Example 2.7.2. Let $H = \langle (12) \rangle \leq S_3$. It is easy to see that $\alpha = X_1 + X_2 + X_3^2$ generates L^H over K. Also $\beta = X_1^2 + X_2^2 + X_3$ generates L^H over K. Note that $\alpha + \beta \in K$. △

Let's go to the opposite direction. Let $\alpha \in L$; actually there is no harm to assume $\alpha \in k[\vec{X}]$. Define $H(\alpha)$ to be the stabilizer of α under the action of S_n; that is

$$H(\alpha) = \{\sigma \in S_n : \sigma(\alpha) = \alpha\}.$$

Then $L|L^{H(\alpha)}$ is Galois with $\mathrm{Gal}(L/L^{H(\alpha)}) = H(\alpha)$. Clearly, $K(\alpha) \subseteq L^{H(\alpha)}$. Actually, they are equal (take this as an exercise). Therefore, α is a generic resolvent for $H(\alpha)$. More importantly, we have

$$H(\alpha) = H(\beta) \Longleftrightarrow K(\alpha) = K(\beta)$$

for all $\alpha, \beta \in L$. This was already observed in Example 2.7.2.

Let $\sigma_1 = \mathrm{id}, \sigma_2, \ldots, \sigma_m \in S_n$ be a complete set of coset representatives for $H(\alpha)$. Then $\alpha_i := \sigma_i(\alpha)$ are distinct and they are the conjugates of α over K. Hence

$$m_\alpha(T) := \prod_{i=1}^{m}(T - \alpha_i)$$

is the minimal polynomial of α over K. Write

$$m_\alpha(T) = T^m + c_{m-1}(\vec{s})T^{m-1} + \cdots + c_1(\vec{s})T + c_0(\vec{s})$$

where $c_0, c_1, \ldots, c_m \in k[Y_1, \ldots, Y_n]$ and $\vec{s} = (s_1, \ldots, s_n)$. For instance in the case of Example 2.7.2, the coefficients of the minimal polynomial $m_\alpha(T)$ of α over K are as follows[8]:

$$\begin{aligned}
c_2 =& -2s_1^2 + 4s_2 - s_1,\\
c_1 =& s_1^4 - s_1^3 - 4s_1^2 s_2 + 2s_1 s_2 + 2s_2^2 + 3s_1 s_3 - 6s_3,\\
c_0 =& s_1^6 - 3s_1^5 + (3 - 6s_2)s_1^4 + (12s_2 - 1)s_1^3 + (3s_2^2 - 6s_2 - 9s_3)s_1^2 +\\
& (6s_2^2 + 9s_3 - 6s_2)s_1 + s_2^3 + 3s_2 s_3 - s_3 + s_3^2.
\end{aligned}$$

Now let $f(X) \in k[X]$ be irreducible and separable with roots $a_1, \ldots, a_n$ in $\overline{k}$. Put $b_i := s_i(a_1, \ldots, a_n)$ and let $\vec{b} = (b_1, \ldots, b_n) \in \overline{k}^n$. Then

$$f(X) = X^n - b_1 X^{n-1} + \cdots + (-1)^n b_n.$$

Define $m_{\alpha,f} = T^m + c_{m-1}(\vec{b})T^{m-1} + \cdots + c_1(\vec{b})T + c_0(\vec{b})$. So if we think of m_α as a function of $X_1, \ldots, X_n$, then $m_{\alpha,f}$ is that function evaluated at $(a_1, \ldots, a_n)$. However, we do not need to know what the roots $a_1, \ldots, a_n$ are, we only need to know the coefficients of f.

Here is the main result, which we present without a proof.[9]

Theorem 2.7.3. *Given k and $f \in k[X]$, the Galois group of the splitting field of f over k is contained in a conjugate of $H(\alpha)$ (in S_n) if and only if $m_{\alpha,f}$ has a root in k.*

2.8 Galois Groups over $\mathbb{Q}$

Let $f \in \mathbb{Z}[X]$ be irreducible, and let K be the splitting field of f over K. We would like to understand $\mathrm{Gal}(K/\mathbb{Q})$.

Let $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}}$ be roots of f and put $\Delta := \prod_{1 \le i < j \le n}(\alpha_i - \alpha_j)^2$.

Fact 1: Let p be a prime and let $\overline{f} \in \mathbb{F}_p[X]$ be the reduction of f modulo p. Then $\overline{f}$ is separable if and only if $p \nmid \Delta$.

[8] I would like to thank ChatGPT for this, however I haven't checked it's correctness.

[9] You may try to prove this as a slightly challenging exercise.

Hence $\overline{f} \in \mathbb{F}_p[X]$ is separable expect for finitely many values of p.

Let $p \nmid \Delta$ and write $\overline{f} = \overline{f_1} \cdots \overline{f_k}$ in $\mathbb{F}_p[X]$; $\overline{f_i}$'s are irreducible in $\mathbb{F}_p[X]$.

Fact 2: $\mathrm{Gal}(\overline{f}/\mathbb{F}_p) \leqslant \mathrm{Gal}(f/\mathbb{Q})$.

This means that there are orderings of roots of f and $\overline{f}$ so that each action of $\mathrm{Gal}(\overline{f}/\mathbb{F}_p)$ on the roots of f gives an action of $\mathrm{Gal}(f/\mathbb{Q})$ on the roots of f. Also $\mathrm{Gal}(\overline{f}/\mathbb{F}_p)$ is cyclic, say generated by σ. Since $\mathrm{Gal}(\overline{f}/\mathbb{F}_p)$ permutes roots of $\overline{f_i}$ among themselves in a transitive way, we see that σ is a product of disjoint cycles; moreover, the lengths of the cycles are the same as the degrees of $\overline{f_i}$; say $n_i = \deg \overline{f_i}$. As a result, $\mathrm{Gal}(f/\mathbb{Q})$ has an element with the cycle structure $(n_1, \ldots, n_k)$.

Example 2.8.1. Let $f(X) = X^5 - X - 1 \in \mathbb{Z}[X]$. One may calculate the discriminant to be $\Delta = 2869 = 19 \cdot 151$. First let $p = 2$. Then

$$\overline{f} = \left(X^2 + X + 1\right)\left(X^3 + X + 1\right).$$

Therefore, $G = \mathrm{Gal}(f/\mathbb{Q})$ contains a $(2,3)-$cycle, hence a transposition.

Now let $p = 3$. Then, $\overline{f}$ is irreducible and hence G contains a $5-$cycle. Therefore $G \simeq S_5$. △

Exercise. Show that for any $n > 1$, there are infinitely many polynomials in $\mathbb{Q}[X]$ whose Galois groups over $\mathbb{Q}$ are isomorphic to S_n.

2.9 Infinite Galois Extensions

Most of the results we talked were about finite extensions. Now we would like to give an idea about how infinite extensions can be handled.

Let $K|k$ be an infinite Galois extension with Galois group $G := \mathrm{Gal}(K/k)$. For any intermediate field F with $F|k$ finite Galois, the group $\mathrm{Gal}(K/F)$ is a normal subgroup of G of finite index. Also we have the natural projection

$$\pi : G \longrightarrow \mathrm{Gal}(K/k)/\mathrm{Gal}(K/F) \simeq \mathrm{Gal}(F/k).$$

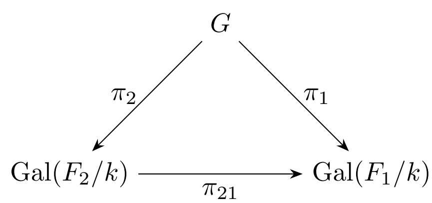
If $k \subseteq F_1 \subseteq F_2 \subseteq K$ are such that $F_2|k$ and $F_1|k$ are finite Galois, then we also have $H_2 := \mathrm{Gal}(K/F_2) \subseteq H_1 := \mathrm{Gal}(K/F_1)$, and hence we have

$$\pi_{F_2 F_1} : G/H_2 \longrightarrow G/H_1,$$

and $G/H_2 \simeq \mathrm{Gal}(F_2/k)$ and $G/H_1 \simeq \mathrm{Gal}(F_1/k)$. So we have an "inverse system"

$$\begin{aligned}\tau &= \{\pi_{F_2 F_1} : \mathrm{Gal}(F_2/k) \longrightarrow \mathrm{Gal}(F_1/k) | F_1 \subseteq F_2\} \\ &= \{\pi_{F_2 F_1} : G/H_2 \longrightarrow G/H_1 | H_2 \subseteq H_1\}\end{aligned}$$

and



We have $\pi_1 = \pi_{21} \circ \pi_2$. So indeed $G = \varprojlim_{H \in \tau} G/H$.

An element σ of G is determined by $\sigma|_F$ where F varies over intermediate fields such that $F|k$ is finite Galois. The important thing with inverse limit is that we may equip G with topology. We are not going to get into this, but we'll just say that Galois correspondence holds with closed subgroups of G.

Example 2.9.1. For a fixed prime p, let K be the splitting field of the collection $\{X^{p^n} - 1 : n > 0\}$ over $\mathbb{Q}$. So $K = \mathbb{Q}(\zeta_p, \zeta_{p^2}, \dots)$ where $\zeta_{p^n} = e^{2\pi i/p^n}$.
Let $K_n = \mathbb{Q}(\zeta_{p^n})$. Then $[K_n : \mathbb{Q}] = \phi(p^n)$ and $G_n := \mathrm{Gal}(K_n/\mathbb{Q}) \simeq (\mathbb{Z}/p^n\mathbb{Z})^\times$. Also $K_n \subseteq K_{n+1}$ since $\zeta_{p^{n+1}}^p = \zeta_{p^n}$; and we have

$$\pi_{n+1} : G_{n+1} \longrightarrow G_n$$

given by $\pi_{n+1}(\overline{a}) = \overline{a}$; or $\pi_{n+1}(a + p^{n+1}\mathbb{Z}) = a + p^n\mathbb{Z}$. Clearly, π_{n+1} is injective. Now $G := \mathrm{Gal}(K/\mathbb{Q}) \simeq \varprojlim_n (\mathbb{Z}/p^n\mathbb{Z})^\times$. This means that $\sigma \in G$ is determined by

$$\sigma_n = \sigma|_{K_n} : \mathbb{Q}(\zeta_{p^n}) \longrightarrow: \mathbb{Q}(\zeta_{p^{n+1}})$$

We know that σ_n is determined by $\sigma(\zeta_{p^n}) = \zeta_{p^n}^{a_n}$ where $p^n \nmid a_n$. However, a_{n+1} and a_n have a relation. We have

$$\begin{aligned} \sigma(\zeta_{p^n}) = \zeta_{p^n}^{a_n} &= \sigma(\zeta_{p^{n+1}}^p) \\ &= (\zeta_{p^{n+1}}^{a_{n+1}})^p \\ &= \zeta_{p^n}^{a_{n+1}} \end{aligned}$$

This means that $a_n \equiv a_{n+1} \pmod{p^n}$; this is exactly $\pi_{n+1}(a_{n+1}) = a_n$. △

Example 2.9.2. Let $K = \overline{\mathbb{F}}_p$. Then $\overline{\mathbb{F}}_p = \bigcup_{n>0} \mathbb{F}_{p^n}$. We know that the Galois group $G_n := \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is cyclic of order n. We have $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ if and only if $m \mid n$. This time

$$G := \mathrm{Gal}(K/\mathbb{F}_p) \simeq \varprojlim_n \mathbb{Z}/n\mathbb{Z}.$$

This is called the *profinite completion* of $\mathbb{Z}$, and is denoted as $\hat{\mathbb{Z}}$. Note that here we ordered $\mathbb{N}^{>0}$ by dividing rather than usual ordering. △

Chapter 3

Transcendental Extensions

Definition. Let $K|k$ be any field extension. A subset $\{a_1, \ldots, a_n\}$ of K is said to be *algebraically independent over* k if there is no $f \in k[X_1, \ldots, X_n] \setminus \{0\}$ such that $f(a_1, \ldots, a_n) = 0$.
An arbitrary subset $S \subseteq K$ is called *algebraically independent over* k if each finite subset of S is algebraically independent over k. $\diamond$

A singleton $\{a\}$ is algebraically independent over k if and only if a is transcendental over k.

Theorem 3.0.1. *Let $K|k$ be a field extension. Then there is a maximally independent (over k) subset S of K; that is S is algebraically independent over k and if $T \supseteq S$ is also algebraically independent over k, then $T = S$. Moreover if S and T are maximally independent (over k) subsets of K, then $|S| = |T|$.*

Proof. Standard: Zorn's lemma and Exchange Lemma. ■

Definition. Given $K|k$, a maximally independent (over k) subset of K is called a *transcendence basis* and its cardinality is called the *transcendence degree*; denoted as $\operatorname{trdeg}(K/k)$. $\diamond$

Note that if S is a transcendence basis of K over k, then it might not be the case that $k(S) = K$. All we know is that $K|k(S)$ is algebraic. For instance, let $K = k(T)$, where T is an indeterminate. Then a natural choice for transcendence basis is $\{T\}$. However, $\{T^2\}$ is also a transcendence basis. As a matter of fact, any non-constant element of K gives a transcendence basis.

Example 3.0.2. Let $K|k$ be such that $\operatorname{trdeg}(K/k) = 1$ and let $\{t\}$ be a transcendence basis. Then $K|k(t)$ is algebraic. Assuming that $\operatorname{char}(k) = 0$, we have $K = k(t)(s)$ for some $s \in K$ algebraic over $k(t)$. Say $f \in k(t)[X] \setminus \{0\}$ such that $f(s) = 0$. Write,

$$f(X) = \sum_{i=0}^{d} f_i(t) X^i$$

where $f_i \in k[Y]$. So there is

$$g(x,y) := \sum_{i=0}^{d} f_i(Y)X^i \in k[X,Y]$$

such that $g(s,t) = 0$. So (s,t) is on a curve in the plane. In this case we say that K is a *function field over k*. If $k = \mathbb{C}$, then elements of K could be thought as meromorphic functions on that curve. △

Theorem 3.0.3. *Let $K|k$ and $S \subseteq K$ be algebraically independent over k with $|S| = n$. Then $k(S) \simeq k(X_1, \ldots, X_n)$.*

Proof. Define,

$$\begin{aligned} \varphi : k[X_1, \ldots, X_n] &\longrightarrow k[a_1, \ldots, a_n] \\ X_i &\longmapsto a_i \end{aligned}$$

where $S = \{a_1, \ldots, a_n\}$. This is clearly a surjective ring homomorphism and it's injective since S is algebraically independent over k. Hence it extends to the function fields. ■

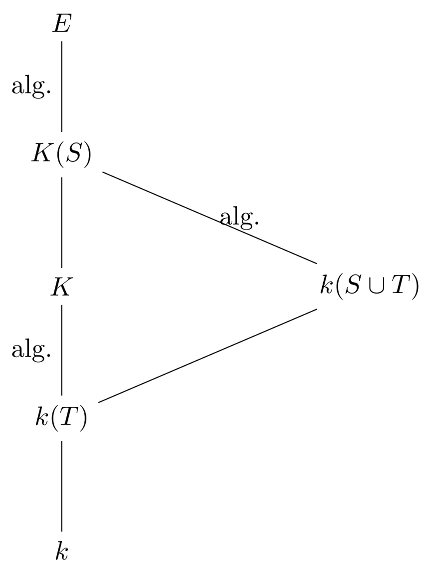
Corollary 3.0.4. *Let $K_1|k_1$, $K_2|k_2$ be extensions and let $S_1 \subseteq K_1$ and $S_2 \subseteq K_2$ be algebraically independent over k_1 and k_2. Suppose that we have an injective function $\varphi : S_1 \to S_2$ and $\sigma : k_1 \to k_2$ embedding of fields. Then σ extends to a field embedding $k_1(S_1) \to k_2(S_2)$. If φ is a bijection and σ is an isomorphism, then $k_1(S_1) \simeq k_2(S_2)$.*

An extension of the form $k(S)$, where S is algebraically independent over k is said to be *purely transcendental*.

Theorem 3.0.5. *Let $E|K$ and $K|k$ be field extensions. Then* $\operatorname{trdeg}(E/k) = \operatorname{trdeg}(E/K) + \operatorname{trdeg}(K/k)$.

Proof. Let S and T be transcendence bases of $E|K$ and $K|k$ respectively. Note that $S \cap T = \varnothing$. So it is enough to show that $S \cup T$ is a transcendence basis of E over k.

We first show that $E|k(S \cup T)$ is algebraic. We have



Since $K|k(T)$ is algebraic, $K \cdot k(S \cup T)|k(S \cup T)$ is algebraic and $K \cdot k(S \cup T) = K(S)$. Now it remains to show that $S \cup T$ is algebraically independent over k. Let $f(X_1, \ldots, X_m, Y_1, \ldots, Y_n) \in k[\vec{X}, \vec{Y}]$, and $s_1, \ldots, s_m \in S$, $t_1, \ldots, t_n \in T$ with $f(s_1, \ldots, s_m, t_1, \ldots, t_n) = 0$. Let

$$g(\vec{X}) := f(\vec{X}, t_1, \ldots, t_n) \in k(\vec{t})[\vec{X}].$$

Since $s_1, \ldots, s_m$ are algebraically independent over K, we see that $g \equiv 0$. Write

$$g(\vec{X}) = \sum_{i \in I} h_i(\vec{X}) l_i(\vec{Y})$$

where $h_i \in k[\vec{X}]$, $l_i \in k[\vec{Y}]$, and I is a finite set. Then $l_i(\vec{t}) = 0$ for all i; hence $l_i \equiv 0$ for all i. But then $f(\vec{X}, \vec{Y}) = 0$. ■

Theorem 3.0.6. *Let $K_1|k_1$, $K_2|k_2$ be field extensions where K_1, K_2 are algebraically closed with* $\operatorname{trdeg}(K_1/k_1) = \operatorname{trdeg}(K_2/k_2)$. *Then every isomorphism of k_1 and k_2 extends to an isomorphism of K_1 and K_2.*

Proof. Let $\sigma : k_1 \to k_2$ be an isomorphism. Using the corollary from the previous page, σ extends to an isomorphism $\sigma : k_1(S_1) \to k_2(S_2)$. By an earlier result, this extends to an isomorphism $\sigma : \overline{k_1(S_1)} \to \overline{k_2(S_2)}$. However, it is clear that $\overline{k_1(S_1)} = K_1$ and $\overline{k_2(S_2)} = K_2$. ■

Let's look at the case $\operatorname{trdeg}(K/k) = 1$ in a little bit more detail. In that case, there is $T \in K$ such that $K|k(T)$ is algebraic. We also know that $k(T) \simeq k(X)$. What are between k and $k(T)$? The next theorem answers that.

Theorem 3.0.7 (Lüroth)**.** *Let $k \subsetneq F \subsetneq k(T)$. Then $F = k(Y)$ for some $Y \in k[T]$ So they are all purely transcendental over k.*

Consider an automorphism $\sigma : k(T) \to k(T)$ over k. This σ is determined by $\sigma(T)$; say $\sigma(T) = \frac{f(T)}{g(T)}$ where $f, g \in k[T]$, $g \neq 0$. First thing to note that not both f, g are constant.

Exercise. Let $f, g \in k[T]$ be relatively prime and that they are not both constant and $g \neq 0$. Then,

$$\left[k(T) : k\left(\frac{f}{g}\right)\right] = \max\{\deg(f), \deg(g)\}.$$

Assuming this exercise, we see that if σ is an automorphism, then $\deg(f), \deg(g) \leq 1$; and not both 0. Say

$$\frac{f}{g} = \frac{aT + b}{cT + d}$$

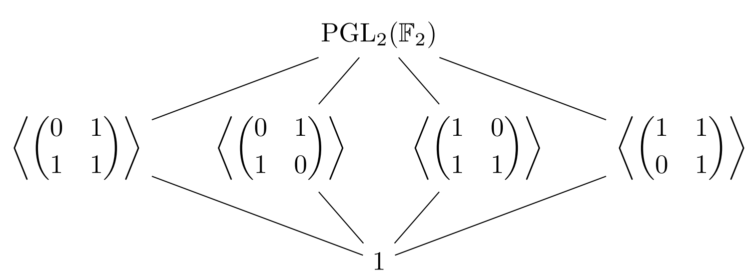
with $a, b, c, d \in k$. Note that $\frac{f}{g} \in k$ if $ad - bc = 0$. So $ad - bc \neq 0$. Therefore the group homomorphism

$$\psi : \mathrm{GL}_2(k) \longrightarrow \mathrm{Aut}(k(T)/k)$$

given by $\psi \begin{pmatrix} a & b \\ c & d \end{pmatrix} (T) = \frac{aT+b}{cT+d}$ is surjective. Note that $\psi \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \mathrm{id}_{k(T)}$ if and only if $a = d$ and $b = c = 0$. So,

$$\ker \psi = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : a \neq 0 \right\} \simeq k^{\times}.$$

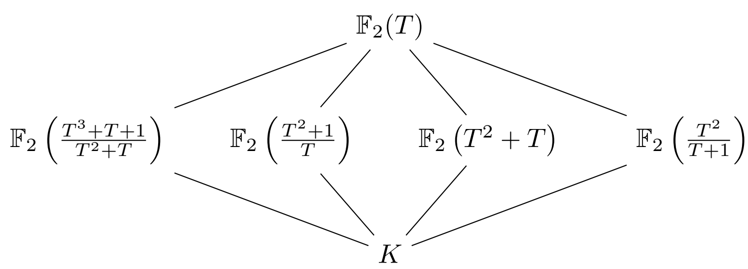
Hence $\mathrm{Aut}(k(T)/k) \simeq \mathrm{PGL}_2(k)$. Let $k = \mathbb{F}_q$ ($q = p^m$). Note that $|\mathrm{PGL}_2(\mathbb{F}_q)| = q \cdot (q-1) \cdot (q+1)$(why?). Consider $q = 2$ case. Then $\mathrm{PGL}_2(\mathbb{F}_2)$ is a non-abelian group of order 6. So $\mathrm{PGL}_2(\mathbb{F}_2) \simeq S_3$, and its subgroups look like as follows:



Let $K = \mathbb{F}_2(T)^{\mathrm{PGL}_2(\mathbb{F}_2)}$. then $\mathbb{F}_2(T)|K$ is Galois with Galois group isomorphic to $\mathrm{PGL}_2(\mathbb{F}_2)$. One may calculate K to be

$$K = \mathbb{F}_2\left(\frac{(T^3 + T + 1)(T^3 + T^2 + 1)}{(T^2 + T)^2}\right)$$

The other intermediate fields are as follows:



3.1 Linear Disjointness

Definition. Let k be a field and K, L its extensions. We say that K is linearly disjoint from L over k if the following is satisfied for all $a_1, \dots, a_n \in K$:

$a_1, \dots, a_n$ are linearly independent over $k \implies a_1, \dots, a_n$ are linearly independent over L.

When this is the case, we write $K \perp_k L$. ◇

Proposition 3.1.1. *For field extensions $K|k$ and $L|k$ we have*

$$K \perp_k L \iff L \perp_k K.$$

Proof. Suppose that $K \perp_k L$, and let $y_1, \dots, y_n \in L$ be linearly independent over k. Suppose for a contradiction that there exist $x_1, \dots, x_n \in K$ such that $x_1 y_1 + \dots + x_n y_n = 0$ and not all x_i are zero. Without loss of generality, $x_1, \dots, x_r$ are linearly independent over k and $x_{r+1}, \dots, x_n$ are in $\mathrm{Span}_k(x_1 \dots, x_r)$. Say

$$x_i = \sum_{j=1}^{r} a_{ij} x_j$$

for $i < j$ with $a_{ij} \in k$. Therefore,

$$x_1 y_1 + \dots + x_r y_r + \sum_{i=r+1}^{n} \sum_{j=1}^{r} a_{ij} x_j y_i = 0.$$

This gives

$$\sum_{j=1}^{r} \left(y_j + \sum_{i=r+1}^{n} a_{ij} y_i \right) x_j = 0,$$

and hence

$$y_j + \sum_{i=r+1}^{n} a_{ij} y_i = 0$$

for all $j = 1, \dots, r$, since $K \perp_k L$. However, this means that $y_1, \dots, y_n$ are not linearly independent over k, a contradiction. ■

Theorem 3.1.2. *Let k be a field with extensions K, L. Then the following are equivalent:*

1. *$K \perp_k L$.*

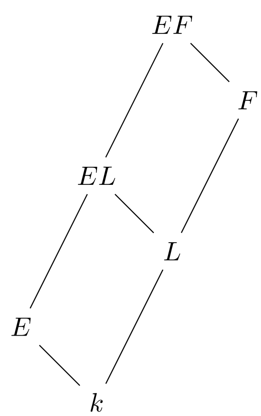
2. *If —R, S are rings with K, L as function fields of them, and if $a_1, \ldots, a_n \in R$ are linearly independent over k, then $a_1, \ldots, a_n$ are linearly independent over S.*

3. *Suppose that $R \subseteq K$ is a vector space over k with basis B such that the function field of R is K. Then B is linearly independent over L.*

Proof. Straightforward calculations. ■

Theorem 3.1.3. *Let $k \subseteq E$, $k \subseteq L \subseteq F$ be fields. Then $E \perp_k F$ if and only if $E \perp_k L$ and $EL \perp_L F$.*

Proof.



($\Leftarrow$) Let $X \subseteq E$ be linearly independent over k. Then X is linearly independent over L. Considered as a subgroup of EL, it is independent over F.
($\Rightarrow$) The condition $E \perp_k L$ is automatic. Let $EL = L[R]$ where $R = L[E]$. Note that a linear basis of E as a $k-$vector space is also a basis of R as an $L-$vector space. Such a basis remains linearly independent over F by the assumption that $E \perp_k F$. Then $EL \perp_L F$ by the previous theorem. ■

Definition. Let $K|k$ and $L|k$ be field extensions. We say that K is free from??? L over k if every algebraically independent (over k) subset $X \subseteq K$ remains algebraically independent over L. We denote this by $K \mathrel{\smile\!\!\!\!\!\!|}_k L$. ⋄

Proposition 3.1.4. *Let $K|k$ and $L|k$ be field extensions. Then $K \mathrel{\smile\!\!\!\!\!\!|}_k L$ if and only if $L \mathrel{\smile\!\!\!\!\!\!|}_k K$.*

Proof. Similar to the corresponding result for linear disjointness. ■

Theorem 3.1.5. *Let $K|k$ and $L|k$ be extensions such that $K \perp_k L$. Then $K \mathrel{\smile\!\!\!\!\!\!|}_k L$.*

Proof. Suppose that $x_1, \ldots, x_n \in K$ are algebraically dependent over L; say

$$\sum_{\vec{i} \in I} \beta_{\vec{i}} \vec{x}^{\vec{i}} = 0.$$

Where I a finite set of multi-indices and $\beta_{\vec{i}} \in L$ for each $\vec{i} \in I$, not all 0. But then the set $\{\vec{x}^{\vec{i}} : \vec{i} \in I\}$ is linearly dependent over L, hence over k. Therefore, $x_1, \ldots, x_n$ are algebraically dependent over k. ∎

Proposition 3.1.6. *Let $u_1, \ldots, u_n$ be elements of a field containing L such that they are algebraically independent over L. Then $k(u_1, \ldots, u_n) \perp_k L$.*

Proof. A linear basis of $k[u_1, \ldots, u_n]$ over k consists of monomials iof $\vec{u} = (u_1, \ldots, u_n)$. They remain linearly independent over L. Hence $k(u_1, \ldots, u_n) \perp_k L$. ∎

3.2 separable extension

Definition. Let $K|k$ be a finitely generated extension. A separating basis of $K|k$ is a transcendence basis S of $K|k$ such that $K|k(S)$ is separable. ◇

Definition. Let k be a field of characteristic $p > 0$, and let $m > 0$. We define

$$A_m := \{x \in \bar{k} : x^{p^m} \in k\} \text{ and } k^{1/p^m} := k(A_m).$$

We also define

$$k^{1/p^\infty} := \bigcup_{m>0} k^{1/p^m}.$$

Clearly $k^{1/p^m} \subseteq k^{1/p^{m+1}}$, hence k^{1/p^∞} is a field. ◇

Theorem 3.2.1. *Let $K|k$ be a field extension. The following are equivalent:*

1. *$K \perp_k k^{1/p^\infty}$.*
2. *$K \perp_k k^{1/p^m}$ for some $m > 0$.*
3. *Every subfield of K that is finitely generated over k has a separating basis over k.*

Proof. (1) ⇒ (2) is clear.
(2) ⇒ (3) Let L be finitely generated (over k) subfield of K, say $L = k(x_1, \ldots, x_n)$. If $\operatorname{trdeg}(L/k) = n$, then $x_1, \ldots, x_n$ are algebraically independent over k and hence form a separating basis of L over k. Assume $r := \operatorname{trdeg}(L/k) < n$; without loss of generality, $x_1, \ldots, x_r$ is a transcendence basis of L over k. Let $f \in k[x_1 \ldots, x_{r+1}]$ be a polynomial with lowest degree such that

$$f(x_1, \ldots, x_{r+1}) = 0.$$

Then f is irreducible. Suppose that each appearance of x_i in f is a p-th power. Then

$$f = \sum_{\vec{i} \in I} c_{\vec{i}} (\vec{x}^{\vec{i}})^p$$

Where I is a finite set of multi-indices and $c_{\vec{i}} \in k$. For each $\vec{i} \in I$, let $d_{\vec{i}} \in \bar{k}$ be such that $d_i^p = c_i$. Then $d_i \in k^{1/p}$, and

$$f(x_1, \ldots, x_{r+1}) = \sum_{i \in I} d_i^p (\vec{x}^i)^p = \left(\sum_{i \in I} d_i \vec{x}^i \right)^p.$$

Therefore $\{\vec{x}^i : i \in I\}$ is linearly dependent over $k^{1/p}$; hence by assumption they are linearly dependent over k. But this is against f being of lowest degree. Therefore, there is x_i that doesn't appear in f as a p-th power; without loss of generality, let $i = 1$. Consider

$$f(X_1, x_2, \ldots, x_{r+1}) \in k(x_2, \ldots, x_{r+1})[X_1]$$

This is the minimal polynomial of x_1 over $k(x_2, \ldots, x_{r+1})$ (after dividing by an element of k). Hence x_1 is separable over $k(x_2, \ldots, x_{r+1})$, and so over $k(x_2, \ldots, x_n)$. If $\operatorname{trdeg}(L/k) = n - 1$, then we are done. Otherwise we continue the same process with $x_2, \ldots, x_n$ to eventually get a separating basis for L over k.

(3) $\Rightarrow$ *(1)* It suffices to show that every finitely generated subfield of K that is finitely generated over k is linearly disjoint from k^{1/p^∞}.

So let $L \subseteq K$ be finitely generated over k with a separating basis $u_1, \ldots, u_n$. Note that $u_1, \ldots, u_n$ remain algebraically independent over k^{1/p^∞}. So $k(\vec{u}) \perp_k k^{1/p^\infty}$.

We know that $L = k(\vec{u})(\alpha)$ for some $\alpha \in L$; say α is of degree d over $k(\vec{u})$. Then $1, \alpha, \ldots, \alpha^{d-1}$ is a linear basis of L over $k(\vec{u})$. It's clear that $1, \alpha, \ldots, \alpha^{d-1}$ remains linearly independent over $k(\vec{u}) \cdot k^{1/p^\infty} = k^{1/p^\infty}(\vec{u})$ since $k^{1/p^\infty}(\vec{u}) | k(\vec{u})$ is purely inseparable. Therefore $L \perp_k k^{1/p^\infty}(\vec{u})$, and hence $L \perp_k k^{1/p^\infty}$. ■

An extension $K|k$ satisfying one of the three conditions of this theorem is called separable. It is easy to see that if $K|k$ is algebraic, then it's separable with the original definition if and only if it's separable with this definition. (It's easiest to use *(3) to see this.)*

Below we list some properties of separable extensions.

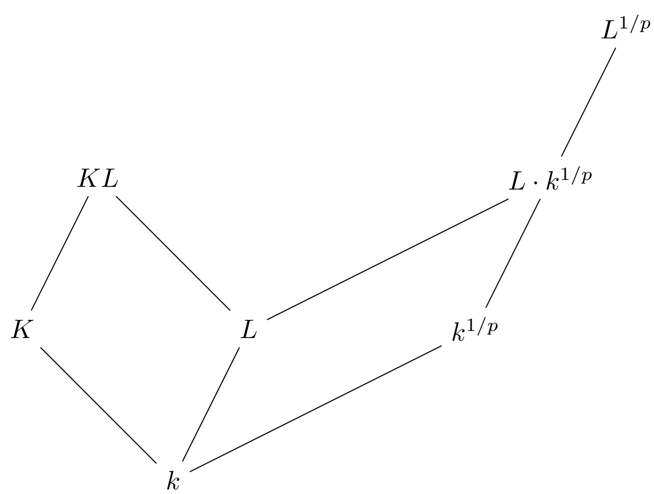
Proposition 3.2.2. *Let $K|k$, $E|k$, and $L|k$ be extensions with $E \subseteq K$.*

1. *If $K|k$ is separable, then $E|k$ is separable.*
2. *If $K|E$ and $E|k$ are separable, then $K|k$ is separable.*
3. *If k is perfect (i.e. $k^p = k$), then any extension of k is separable.*
4. *If $K|k$ is separable and $K \perp_k L$, then $KL|L$ is separable.*

5. *If $K|k$ and $L|k$ are separable and $K \mathrel{\smile\!\!\!\!\!\!|}_k L$, then $KL|k$ is separable.*
6. *Let $K \perp_k L$, then $K|k$ is separable if and only if $KL|L$ is separable.*

Proof.

1. Clear.
2. Note that $E \cdot k^{1/p^\infty} \subseteq E^{1/p^\infty}$. If $K \perp_E E^{1/p^\infty}$, then $K \perp_E E \cdot k^{1/p^\infty}$. Also if $E \perp_k k^{1/p^\infty}$, then $K \perp_k k^{1/p^\infty}$. This finishes the proof
3. If $k^p = k$, then $k^{1/p^\infty} = k$; and $K \perp_k k$ for any extension K.
4. A finitely generated (over L) subfield of KL is of the form FL where $F \subseteq K$ is finitely generated over k. So let $\{t_1, \dots, t_n\}$ be a separating basis of F over k. Since $K \mathrel{\smile\!\!\!\!\!\!|}_k L$, $\{t_1, \dots, t_n\}$ remains algebraically independent over L and hence it is a basis over L. It also follows that $FL|L(t_1, \dots, t_n)$ is separable. Hence $KL|L$ is separable.
5. Since $K|k$ is separable and $K \mathrel{\smile\!\!\!\!\!\!|}_k L$, we have $KL|L$ is separable. Hence $KL|k$ is separable by (*2*).
6. Since $K \perp_k L$ implies $K \mathrel{\smile\!\!\!\!\!\!|}_k L$, we get the first direction by (*4*). For the other direction suppose that $K \not\perp_k k^{1/p}$. Then $K \not\perp_k L \cdot k^{1/p^\infty}$ and hence $KL \not\perp_L L \cdot k^{1/p}$. If $KL|L$ is separable, then $KL \perp_L L^{1/p}$. Then $K \perp_k L^{1/p}$ and $K \perp_k L \cdot k^{1/p}$. but this contradicts $KL \perp_L L \cdot k^{1/p}$. (See picture below)



∎

Proposition 3.2.3. *Let $K|k$ be finitely generated. If $K^{p^m} \cdot k = K$ for some $m > 0$, then $K|k$ is separable algebraic. Conversely, if $K|k$ is separable algebraic, then $K^{p^m} \cdot k = K$ for some $m > 0$.*

Definition. An extension $K|k$ is called regular if it is separable and for every $\alpha \in K$ if α is algebraic over k, then $\alpha \in k$. $\diamond$

The second condition can simply be interpreted as "k is algebraically closed in K".

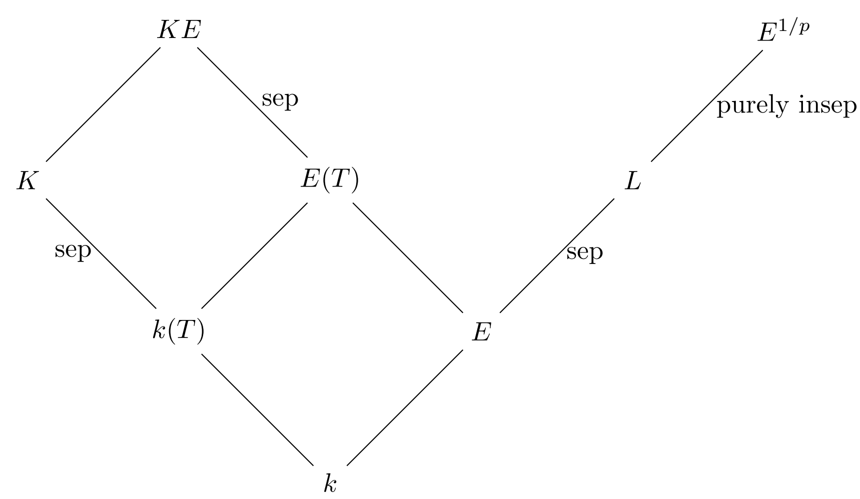
Theorem 3.2.4. *An extension $K|k$ is regular if and only if $K \perp_k \bar{k}$.*

Proof. ($\Leftarrow$) If $K \perp_k \bar{k}$, then in particular $K \perp_k k^{1/p}$. So $K|k$ is separable. Also $K \cup \bar{k} = k$, and hence k is algebraically closed in K.
($\Rightarrow$) First a lemma:

Lemma 3.2.5. *Let k be algebraically closed in K. Let α be an element in some extension of K that is algebraic over k. Then $k(\alpha) \perp_k K$ and $[k(\alpha) : k] = [K(\alpha) : K]$.*

Proof. The minimal polynomial of α over k is also the minimal polynomial over K. Hence $[k(\alpha) : k] = [K(\alpha) : K]$ and since $1, \alpha, \ldots, \alpha^d$ forms a basis of $k(\alpha)$ over k, it also forms a basis of $K(\alpha)$ over k. So $k(\alpha) \perp_k K$. ■

Let's assume that $K|k$ is regular, and let $L|k$ be finite extension. We'd like to show that $K \perp_k L$.
Let $E \subseteq L$ be the minimal separable extension of k (in L). Then $L|E$ is purely inseparable, and hence $L \subseteq E^{1/p^m}$ for some $m > 0$. We have the following picture:



Here T is a separating basis of K over k.. So $K|k(T)$ is separable. Since $E|k$ is separable, it's generated by one element over k and $K \perp_k E$ by the lemma. Also T remains a separating basis of KE over E. Hence $KE|E$ is separable, and $KE \perp_E E^{1/p^m}$. Then $KE \perp_E L$ and $K \perp_k L$. ■

Proposition 3.2.6. *Let $k \subseteq E \subseteq K$ be fields. If $K|k$ is regular, then $E|k$ is regular. If both $K|E$ and $E|k$ regular, then $K|k$ is regular.*

Proof. The first is clear. For the second statement, note that $E\bar{k} \subseteq \bar{E}$. So if $K \perp_E \bar{E}$, then $K \perp_E E\bar{k}$. Also if $E \perp_k \bar{k}$, then $K \perp_k \bar{k}$ and $K|k$ is regular. ■

Proposition 3.2.7. *If k is algebraically closed, then any extension of k is regular.*

Proof. Trivial. ■

Theorem 3.2.8. *Let $K|k$ be regular and $K \downfree_k L$. Then $K \perp_k L$.*

Proof. ... ■

Theorem 3.2.9. *Suppose that $K|k$ is regular and $K \downfree_k L$, then $KL|L$ is regular.*

Proof. If $K \downfree_k L$, then $K \downfree_k \bar{L}$ as a general fact when $K|k$ is regular, we get that $K \perp_k \bar{L}$. Then $KL \perp_L \bar{L}$, meaning $KL|L$ is regular ■

Corollary 3.2.10.

1. *Let $K|k$ and $L|k$ be regular and $K \downfree_k L$. Then $KL|k$ is regular.*
2. *Let $K = k(\alpha_1, \ldots, \alpha_n)$ be a finitely generated regular extension with $K \downfree_k L$. Then the natural $k-$algebra homomorphism*

$$L \otimes_k k[\vec{\alpha}] \to L[\vec{\alpha}]$$

   is an isomorphism.

Proof.

1. We have both $KL|L$ and $KL|K$ are regular by the previous theorem. Then $KL|k$ is regular by the proposition above.
2. This map is always surjective, and it's injective if and only if $L \perp_k K$. But if $K \downfree_k L$ and $K|k$ is regular, then $L \perp_k K$ by the theorem above.

■

Chapter 4

Commutative Algebra

Bibliography

[1] *David S. Dummit and Richard M. Foote.* Abstract algebra*. John Wiley & Sons, Inc., Hoboken, NJ, third edition, 2004.*

[2] *Thomas W. Hungerford.* Algebra*, volume 73 of* Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1980. Reprint of the 1974 original.*

[3] *S. Lang.* Algebra*. Addison-Wesley Publishing Co. Inc., Reading, Mass., 1997.*

Index