MA-414
Galois Theory

Aryaman Maithani
https://aryamanmaithani.github.io/

Last updated: May 8, 2021

Contents

Chapter 0

Preliminaries

§0.1. Notations

1. $\mathbb{N}$ will denote the set of **positive** integers. That is, $\mathbb{N} = \{1, 2, \ldots\}$.
2. $\mathbb{Z}$ will denote the set of integers.
3. $\mathbb{N}_0$ will denote the set of all **non-negative** integers.
   That is, $\mathbb{N}_0 = \{0, 1, 2, \ldots\} = \mathbb{N} \cup \{0\}$.
4. $\mathbb{Q}$ will denote the set of rationals.
5. $\mathbb{R}$ will denote the set of real numbers.
6. $\mathbb{C}$ will denote the set of complex numbers.
7. Blackboard letters like $\mathbb{F}, \mathbb{E}, \mathbb{K}, \mathbb{L}$ will denote an arbitrary field.
8. Given any field $\mathbb{F}$, $\mathbb{F}^\times$ denotes the group of units of $\mathbb{F}$. That is, $\mathbb{F} = \mathbb{F} \setminus \{0\}$.
9. Whenever we write "$F \subset E$ are fields," we mean that $\mathbb{E}$ is a field and $\mathbb{F}$ is a subfield of $\mathbb{E}$.
10. $\zeta_n := \exp\left(\frac{2\pi\iota}{n}\right)$.

§0.2. Field Theory

We shall assume that the reader is familiar with the definitions and basic properties of groups and rings. All rings in this document will be assumed to be commutative with identity.

We list some basic definition and properties. The proofs might be a bit terse and you should not have much problem filling in the details. (This won't be the case in the later chapters!)

Definition 0.1. An integral domain is a ring with $0 \neq 1$ such $ab = 0 \implies a = 0$ or $b = 0$.

Definition 0.2. A field $(\mathbb{F}, +, \cdot)$ is a ring with $0 \neq 1$ such that every non-zero element has a multiplicative inverse.

Example 0.3. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all fields.

Definition 0.4. Given an integral domain R, the field of fractions of R is denoted by $\mathrm{Frac}(R)$.

Definition 0.5. A ring homomorphism is a map $\varphi : R \to S$ between rings such that

1. $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in R$,
2. $\varphi(a + b) = \varphi(a) + \varphi(b)$ for all $a, b \in R$,
3. $\varphi(1_R) = 1_S$.

A field homomorphism is a ring homomorphism between fields.

Definition 0.6. Given a prime $p \in \mathbb{N}$, $\mathbb{Z}/p\mathbb{Z}$ is a field, which we denote as $\mathbb{F}_p$.

Definition 0.7. Let $\mathbb{F}$ be a field. The characteristic of $\mathbb{F}$ is defined to be the smallest positive integer n such that

$$\underbrace{1_{\mathbb{F}} + \cdots + 1_{\mathbb{F}}}_{n} = 0_{\mathbb{F}}.$$

If no such n exists, then the characteristic is defined to be 0.

This is denoted by $\mathrm{char}\,\mathbb{F}$.

From now on, we shall omit the subscript $\mathbb{F}$ when it is clear what the 0 and 1 are.

Proposition 0.8. If $\mathrm{char}\,\mathbb{F} > 0$, then $\mathrm{char}\,\mathbb{F}$ is prime.

Proof. Let $n := \mathrm{char}\,\mathbb{F}$ and let $n = ab$ for some $a, b \in \mathbb{F}$. By distributivity and definition of n, we have

$$\underbrace{(1 + \cdots + 1)}_{a}\underbrace{(1 + \cdots + 1)}_{b} = 0.$$

Since $\mathbb{F}$ is a field, one of the above two terms is 0. Without loss of generality, the first term is 0. By definition, $n = \mathrm{char}\,\mathbb{F} \leq a$. But $a \mid n \implies a \leq n$.

Thus, $a = n$. □

Proposition 0.9. Every field contains an isomorphic copy of either $\mathbb{Q}$ or $\mathbb{F}_p$ for some prime p. In fact, this copy is precisely $\mathrm{Frac}(\mathbb{Z}/\langle \mathrm{char}\,\mathbb{F}\rangle)$.

Proof. Given a field $\mathbb{F}$, consider the ring homomorphism $\varphi : \mathbb{Z} \to \mathbb{F}$ given by $1 \mapsto 1$. Then, $\mathbb{F}$ contains an isomorphic copy of $\mathbb{Z}/\ker\varphi$. Note that $\varphi = \langle n\rangle$, where $n = \mathrm{char}\,\mathbb{F}$. If $n > 0$, then n is prime and we are done.

If $n = 0$, then $\mathbb{F}$ contains an isomorphic copy of $\mathbb{Z}$. Thus, it must contain $\mathbb{Q}$.[1] □

Definition 0.10. Given a field $\mathbb{F}$, the prime subfield of $\mathbb{F}$ is defined as the smallest subfield of $\mathbb{F}$. It is the intersection of all subfields of $\mathbb{F}$.

Proposition 0.11.

1. The prime subfield of $\mathbb{F}$ is isomorphic to $\mathrm{Frac}(\mathbb{Z}/\langle \mathrm{char}\,\mathbb{F}\rangle)$.
2. Let $\varphi : \mathbb{F} \to \mathbb{E}$ be a field homomorphism. Then, $\mathrm{char}\,\mathbb{F} = \mathrm{char}\,\mathbb{E}$ and φ is injective.
3. Let $\mathbb{F} \subset \mathbb{E}$ be fields. $\mathbb{F}$ and $\mathbb{E}$ have the same prime subfield. Any field homomorphism $\varphi : \mathbb{F} \to \mathbb{E}$ fixes this prime subfield.

Definition 0.12. Since any field homomorphism is injective, we also call them embeddings.

Definition 0.13. Given fields $\mathbb{F} \subset \mathbb{E}_1, \mathbb{E}_2$, and $\mathbb{F}$-isomorphism from $\mathbb{E}_1$ to $\mathbb{E}_2$ is a field homomorphism $\varphi : \mathbb{E}_1 \to \mathbb{E}_2$ fixing $\mathbb{F}$.

Definition 0.14. Given rings $R \subset S$, and $\alpha \in S$, we define $R[\alpha]$ to be the smallest subfield of S containing α and R.

Given fields $\mathbb{F} \subset \mathbb{K}$, and $\alpha \in \mathbb{K}$, we define $\mathbb{F}(\alpha)$ to be the smallest subfield of $\mathbb{K}$ containing α and $\mathbb{F}$.

Proposition 0.15. If $\mathbb{F}$ is a finite field, then $\mathrm{char}(\mathbb{F}) =: p > 0$ and $|\mathbb{F}| = p^n$ for some $n \in \mathbb{N}$.

Proof. $\mathrm{char}(\mathbb{F}) = 0$ is not possible since $\mathbb{Z}$ is infinite and so, the homomorphism $\varphi : \mathbb{Z} \to \mathbb{F}$ given by $1 \mapsto 1$ cannot be injective.

Now, $\mathbb{F}$ contains $\mathbb{F}_p$ as a subfield and hence, is a vector space over $\mathbb{F}$. Since $|\mathbb{F}| < \infty$, we have $\dim_{\mathbb{F}_p}(\mathbb{F}) =: n < \infty$.

It is clear now that $|\mathbb{F}| = |\mathbb{F}_p|^n = p^n$. □

[1] Either argue by explicitly constructing an isomorphism or use the universal property of fraction fields.

Theorem 0.16. Let $f(x) \in \mathbb{F}[x]$ have a degree $n \geq 1$. Then, $f(x)$ has at most n roots in $\mathbb{F}$.

Proof. Induct on n and use the fact that if $ab = 0 \implies a = 0$ or $b = 0$, in a field. □

Theorem 0.17. Let $\mathbb{F}$ be a field. Let U be a finite subgroup of $\mathbb{F}^\times$. Then, U is cyclic.

We give two proofs.

Proof. This proof uses the following fact: Let G be an abelian group and $a, b \in G$ have orders m and n. Then, there exist $c \in G$ with order $\mathrm{lcm}(m, n)$. (This needs a little argument. $c = ab$ works if $\gcd(m, n) = 1$. The general case has to be reduced to that.)

Let $n := |U|$. Let $a \in U$ be an element with maximal order, say d. Then, we have

$$d = \mathrm{lcm}\{\mathrm{order}(u) \mid u \in U\}.$$

Thus, all n elements of $U \subset \mathbb{F}$ satisfy the polynomial $x^d - 1 \in \mathbb{F}[x]$. Since $\mathbb{F}$ is a field, we have $n \leq d$. Thus, $d = n$ and $U = \langle a \rangle$. □

Proof. This prove uses the structure theorem of abelian groups. Let $n := |U|$.

Write $U \cong \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z}$ where $1 < d_1 \mid d_2 \mid \cdots \mid d_r$ and $n = d_1 \cdots d_r$. Now, every element of U satisfies $x^{d_r} - 1$. Thus, as earlier, we have $d_r = n$ and hence, $n = 1$. This means $U \cong \mathbb{Z}/n\mathbb{Z}$ is cyclic. □

Chapter 1

Algebraic extensions

Definition 1.1. Let $\mathbb{F}$ be a subfield of $\mathbb{K}$. We say that $\mathbb{K}$ is an extension field of $\mathbb{F}$ and $\mathbb{F}$ is called the base field. We also denote this by $\mathbb{K}/\mathbb{F}$.

Remark 1.2. The above is not to be confused with any sort of quotient. In fact, since the only ideals of a field $\mathbb{K}$ are 0 and $\mathbb{K}$, there is no discussion about quotienting.

Definition 1.3. Let $\mathbb{K}/\mathbb{F}$ be a field extension. Then, we may regard $\mathbb{K}$ as a vector space over $\mathbb{F}$. We denote $\dim_{\mathbb{F}} \mathbb{K}$ by $[K : F]$ and call it the degree of the field extension $\mathbb{K}/\mathbb{F}$.

Definition 1.4. The field extension $\mathbb{K}/\mathbb{F}$ is said to be a finite extension if $[\mathbb{K} : \mathbb{F}]$ is finite.

Definition 1.5. The field extension $\mathbb{K}/\mathbb{F}$ is said to be a simple extension if there exists $\alpha \in \mathbb{K}$ such that $\mathbb{K} = \mathbb{F}(\alpha)$.

Definition 1.6. Let $\mathbb{K}/\mathbb{F}$ be a field extension and let $\alpha \in \mathbb{K}$. α is said to be algebraic over $\mathbb{F}$ if there exists a non-zero polynomial $f(x) \in \mathbb{F}[x]$ such that $f(\alpha) = 0$.

α is said to be transcendental over $\mathbb{F}$ if it is not algebraic over $\mathbb{F}$.

If every element of $\mathbb{K}$ is algebraic over $\mathbb{F}$, then $\mathbb{K}/\mathbb{F}$ is called an algebraic extension.

Example 1.7. Note that every element of $\mathbb{F}$ is algebraic over $\mathbb{F}$.

Here's a simple proposition that we leave as an easy exercise.

Proposition 1.8. Let $\mathbb{F} \subset \mathbb{E} \subset \mathbb{K}$ be fields and $\alpha \in \mathbb{K}$.
If α is algebraic over $\mathbb{F}$, then α is algebra over $\mathbb{E}$.
If $\mathbb{K}/\mathbb{F}$ is algebraic, then so are $\mathbb{K}/\mathbb{E}$ and $\mathbb{E}/\mathbb{F}$.

Proposition 1.9. Every finite extension is an algebraic extension. [↓]

Example 1.10. Consider the extensions $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ and $\pi\iota \in \mathbb{C}$.

It is known that $\pi \in \mathbb{R}$ is transcendental over $\mathbb{Q}$. An easy consequence of this is that $\pi\iota \in \mathbb{C}$ is also transcendental over $\mathbb{Q}$. However, $\pi\iota$ is algebraic over $\mathbb{R}$ since it satisfies $x^2 + \pi^2 \in \mathbb{R}[x] \setminus \{0\}$.

Thus, the property of being algebraic/transcendental depends on the base field. In particular, $\mathbb{C}/\mathbb{Q}$ is not an algebraic extension. However, in view of the earlier proposition, $\mathbb{C}/\mathbb{R}$ is.

Example 1.11. Let $\mathbb{K}$ be a finite field and $\mathbb{F}$ be its prime subfield. Then, $\mathbb{K}$ is a finite dimensional $\mathbb{F}$-vector space and thus, $\mathbb{K}/\mathbb{F}$ is an algebraic extension.

Remark 1.12. The converse of the proposition is not true. We shall see later that

$$\mathbb{A} := \{\alpha \in \mathbb{C} : \alpha \text{ is algebraic over } \mathbb{Q}\}$$

is a subfield of $\mathbb{C}$ such that $\dim_{\mathbb{Q}}(\mathbb{A}) = \infty$. However, $\mathbb{A}/\mathbb{Q}$ is clearly algebraic, by construction.

Proposition 1.13. Let $\mathbb{K}/\mathbb{F}$ be a field extension and $\alpha \in \mathbb{K}$ be algebraic over $\mathbb{F}$. Then, the following are true.

1. There exists a unique monic irreducible polynomial $f(x) \in \mathbb{F}[x]$ such that $f(\alpha) = 0$.
2. $f(x)$ generates the kernel of the map $\mathbb{F}[x] \to \mathbb{F}[\alpha] \subset \mathbb{K}$ given by $p(x) \mapsto p(\alpha)$.
3. If $g(x) \in \mathbb{F}[x]$ is such that $g(\alpha) = 0$, then $f(x) \mid g(x)$.
4. In particular, $f(x)$ has the least positive degree among all polynomials in $\mathbb{F}[x]$ satisfied by α. [↓]

Of course, "irreducible" above means "irreducible in $\mathbb{F}[x]$."

Definition 1.14. Given a field extension $\mathbb{K}/\mathbb{F}$ and $\alpha \in \mathbb{K}$ with is algebraic over $\mathbb{F}$, the irreducible monic polynomial $f(x) \in \mathbb{F}[x]$ having α as a root is called the irreducible monic polynomial of α over $\mathbb{F}$. It is denoted by $\mathrm{irr}(\alpha, \mathbb{F})$.

The degree of $\mathrm{irr}(\alpha, \mathbb{F})$ is called the degree of α and is denoted by $\deg_{\mathbb{F}} \alpha$.

Example 1.15.

1. Let $\alpha \in \mathbb{C}$ be a square root of ι. Then, α satisfies $f(x) := x^4 + 1$. Show that $f(x) = \mathrm{irr}(\alpha, \mathbb{Q})$.

   However, $\mathrm{irr}(\alpha, \mathbb{Q}(i)) = x^2 - \iota$. Thus, degree also depends on the base field.

2. Let p be a prime and $\zeta_p := \exp\left(\frac{2\pi\iota}{p}\right) \in \mathbb{C}$. Then, $\zeta_p^p = 1$. Note that $x^p - 1 = (x-1)\Phi_p(x)$ where
$$\Phi_p(x) := x^{p-1} + \cdots + 1.$$
Then, $\Phi_p(\zeta_p) = 0$. Use Eisenstein's criterion on $\Phi_p(x+1)$ to conclude that $\Phi_p(x)$ is irreducible in $\mathbb{Q}[x]$ and hence, $\Phi_p(x) = \operatorname{irr}(\zeta_p, \mathbb{Q})$.

Proposition 1.16. Let $\mathbb{K}/\mathbb{F}$ be a field extension and $\alpha \in \mathbb{K}$ be algebraic over $\mathbb{F}$. Let $f(x) := \operatorname{irr}(\alpha, \mathbb{F})$ and $n := \deg f(x)$. Then,

1. $\mathbb{F}[\alpha] = \mathbb{F}(\alpha) \cong \mathbb{F}[x]/\langle f(x)\rangle$.
2. $\dim_{\mathbb{F}}(\mathbb{F}(\alpha)) = n$ and $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is an $\mathbb{F}$-basis of $\mathbb{F}(\alpha)$. [↓]

Corollary 1.17. Let $\mathbb{K}/\mathbb{F}$ be a field extension and $\alpha \in \mathbb{K}$ be algebraic over $\mathbb{F}$. Then, $\mathbb{F}(\alpha)/\mathbb{F}$ is a finite and hence, algebraic extension, by Proposition 1.9.

Proposition 1.18. Let $\alpha, \beta \in \mathbb{K} \supset \mathbb{F}$ be algebraic over $\mathbb{F}$. Then, there exists and $\mathbb{F}$-isomorphism $\psi : \mathbb{F}(\alpha) \to \mathbb{F}(\beta)$ such that $\psi(\alpha) = \beta$ iff $\operatorname{irr}(\alpha, \mathbb{F}) = \operatorname{irr}(\beta, \mathbb{F})$. [↓]

Definition 1.19. The extension $\mathbb{K}/\mathbb{F}$ is said to be a quadratic extension if $[\mathbb{K} : \mathbb{F}] = 2$.

Remark 1.20. Note that if $\mathbb{K}/\mathbb{F}$ is a quadratic extension and $\alpha \in \mathbb{K} \setminus \mathbb{F}$, then $[\mathbb{F}(\alpha) : \mathbb{F}] > 1$ and hence, $\mathbb{F}(\alpha) = 2$. Thus, $\mathbb{F}(\alpha) = \mathbb{K}$.

That is, all quadratic extensions are simple.

Theorem 1.21 (Tower law)**.** Let $\mathbb{F} \subset \mathbb{E} \subset \mathbb{K}$ be a tower of fields. Then,
$$[\mathbb{K} : \mathbb{F}] = [\mathbb{K} : \mathbb{E}][\mathbb{E} : \mathbb{F}].$$
In particular, the left side is ∞ iff the right side is. [↓]

Corollary 1.22. Let $\mathbb{K}/\mathbb{F}$ be a finite extension and $\alpha \in \mathbb{K}$. Then, $\deg_{\mathbb{F}} \alpha \mid [\mathbb{K} : \mathbb{F}]$.

Proof. Consider the tower $\mathbb{F} \subset \mathbb{F}(\alpha) \subset \mathbb{K}$. □

Proposition 1.23. Let $\mathbb{K}/\mathbb{F}$ be a field extension and let $\alpha_1, \ldots, \alpha_n \in \mathbb{K}$ be algebraic over $\mathbb{F}$. Then, $\mathbb{F}(\alpha_1, \ldots, \alpha_n)$ is a finite (and hence, algebraic) extension of $\mathbb{F}$. [↓]

Corollary 1.24. Let $\mathbb{F} \subset \mathbb{E}$ and $\mathbb{E} \subset \mathbb{K}$ be algebraic extensions. Then, $\mathbb{F} \subset \mathbb{K}$ is an algebraic extension. [↓]

Corollary 1.25. Let $\mathbb{K}/\mathbb{F}$ be a field extension. Then,
$$\mathbb{A} := \{\alpha \in \mathbb{K} : \alpha \text{ is algebraic over } \mathbb{F}\}$$
is a subfield of $\mathbb{K}$ containing $\mathbb{F}$.
Moreover, $\mathbb{A}/\mathbb{F}$ is an algebraic extension. [↓]

§1.1. Compositum of fields

Definition 1.26. Let $\mathbb{E}_1, \mathbb{E}_2 \subset \mathbb{K}$ be fields. The compositum of $\mathbb{E}_1$ and $\mathbb{E}_2$ is the smallest subfield of $\mathbb{K}$ containing $\mathbb{E}_1$ and $\mathbb{E}_2$. It is denoted by $\mathbb{E}_1\mathbb{E}_2$.

Example 1.27. Suppose $\mathbb{F} \subset \mathbb{E}_1, \mathbb{E}_2 \subset \mathbb{K}$ and $\mathbb{E}_1 = \mathbb{F}(\alpha_1, \ldots, \alpha_n)$. Then,

$$\mathbb{E}_1\mathbb{E}_2 = \mathbb{E}_2(\alpha_1, \ldots, \alpha_n).$$

Example 1.28. Let m and n be coprime positive integers. Consider the subfields $\mathbb{F} := \mathbb{Q}(\zeta_m)$ and $\mathbb{E} := \mathbb{Q}(\zeta_n)$ of $\mathbb{C}$. Then,

$$\mathbb{E}\mathbb{F} = \mathbb{Q}(\zeta_{mn}).$$

$\subset$ is clear since $\zeta_n = \zeta_{mn}^m$ and similarly, $\zeta_m = \zeta_{mn}^n$.

On the other hand, since $\gcd(m, n) = 1$, there exist integers $a, b \in \mathbb{Z}$ such that $am + bn = 1$. Thus,

$$\frac{a}{n} + \frac{b}{m} = \frac{1}{mn}$$

and hence

$$\zeta_{mn} = \zeta_n^a \zeta_m^b.$$

Proposition 1.29. Let $\mathbb{F}$ be a field which is a subring of an integral domain R. Suppose R is finite dimensional as an $\mathbb{F}$ vector space. Then, R is a field. [↓]

Proposition 1.30. Let $\mathbb{F} \subset \mathbb{E}_1, \mathbb{E}_2 \subset \mathbb{K}$ be fields. Consider

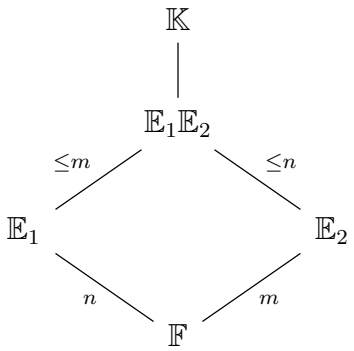
$$\mathbb{L} = \left\{ \sum_{i=1}^{n} \alpha_i \beta_i : n \in \mathbb{N}, \alpha_i \in \mathbb{E}_1, \beta_i \in \mathbb{E}_2 \right\}.$$

That is, let $\mathbb{L}$ be the set of all finite sums of products of elements of $\mathbb{E}_1$ and $\mathbb{E}_2$.

Suppose $d := [\mathbb{E}_1 : \mathbb{K}][\mathbb{E}_2 : \mathbb{K}] < \infty$.
Then $\mathbb{L} = \mathbb{E}_1\mathbb{E}_2$ and $[\mathbb{L} : \mathbb{F}] \leq d$.

If $[\mathbb{E}_1 : \mathbb{F}]$ and $[\mathbb{E}_2 : \mathbb{F}]$ are coprime, then equality holds. [↓]

Diagrammatically, this can be depicted as



§1.2. Splitting Fields

Definition 1.31. Let $\mathbb{F}$ be a field and $f(x) \in \mathbb{F}[x]$ be a non-constant monic polynomial of degree n with leading coefficient $a \in \mathbb{F}^\times$. A field $\mathbb{K} \supset \mathbb{F}$ is called a splitting field of $f(x)$ over $\mathbb{F}$ if there exist $r_1, \ldots, r_n \in \mathbb{K}$ so that $f(x) = a(x - r_1) \cdots (x - r_n)$ and $\mathbb{K} = \mathbb{F}(r_1, \ldots, r_n)$.

Note that $r_1, \ldots, r_n$ above need not be distinct.

Example 1.32. Consider $\mathbb{F} = \mathbb{Q}$, $f(x) = x^2 + 1 \in \mathbb{Q}[x]$ and $\mathbb{K} = \mathbb{C}$. While $f(x)$ does factor linearly over $\mathbb{C}$, $\mathbb{C}$ is **not** a splitting field of $f(x)$ over $\mathbb{Q}$ since $\mathbb{C} \neq \mathbb{Q}(\iota, -\iota)$.

On the other hand, $\mathbb{C}$ *is* a splitting field of $f(x) \in \mathbb{R}[x]$ over $\mathbb{R}$.

Corollary 1.33. Let $f(x) \in \mathbb{F}[x]$ be non-constant and $\mathbb{K}$ be a splitting field of $f(x)$ over $\mathbb{F}$. Then, $\mathbb{K}/\mathbb{F}$ is an algebraic extension.

Proof. Follows from Proposition 1.23. □

Theorem 1.34. Let $\mathbb{F}$ be a field and $f(x) \in \mathbb{F}[x]$ be non-constant. Then, there exists a field $\mathbb{K} \supset \mathbb{F}$ such that $f(x)$ has a root in $\mathbb{K}$. [↓]

Theorem 1.35 (Existence of Splitting Field)**.** Let $\mathbb{F}$ be a field. Any polynomial $f(x) \in \mathbb{F}[x]$ of positive degree has a splitting field. [↓]

Chapter 2

Symmetric Polynomials

Definition 2.1. Given a ring R, consider the polynomial ring $S = R[u_1, \ldots, u_n]$. Let S_n denote the symmetric group. Then, any $\tau \in S_n$ induces an automorphism $g_\tau : S \to S$ by

$$g_\tau(f(u_1, \ldots, u_n)) = f(u_{\tau(1)}, \ldots, u_{\tau(n)}).$$

Example 2.2. Consider $R = \mathbb{Z}$ and $n = 3$. Suppose $\tau = (12)$. Consider the polynomial $f = u_1 + u_2^2 + u_3^3$. Then, $g_\tau(f) = u_2 + u_1^2 + u_3^3$.

Definition 2.3. A polynomial $f \in R[u_1, \ldots, u_n]$ is said to be a symmetric polynomial (in n variables) if

$$f(u_1, \ldots, u_n) = f(u_{\tau(1)}, \ldots, u_{\tau(n)})$$

for all $\tau \in S_n$.

Definition 2.4. Let $S = R[u_1, \ldots, u_n]$. Consider $f(T) \in S[T]$ given by

$$f(T) = (T - u_1) \cdots (T - u_n).$$

Write $f(T)$ as

$$f(T) = T^n - \sigma_1 T^{n-1} + \cdots + (-1)^n \sigma_n,$$

for $\sigma_1, \ldots, \sigma_n \in S$.

Then, $\sigma_1, \ldots, \sigma_n$ are symmetric polynomials, which are called the elementary symmetric polynomials (in n variables).

Remark 2.5. Note that one can explicitly write down the elementary symmetric polynomials. We have

$$\begin{aligned}\sigma_1 &= \sum_{i=1}^{n} u_i,\\ \sigma_2 &= \sum_{1\le i_1<i_1\le n} u_{i_1}u_{i_2},\\ &\vdots\\ \sigma_n &= u_1\cdots u_n.\end{aligned}$$

It is now easy to verify that these are all indeed symmetric polynomials.

§2.1. Fundamental theorem of Symmetric Polynomials

Definition 2.6. Given an elementary symmetric polynomial $\sigma_i \in R[u_1,\dots,u_n]$ in n variables (for $n \ge 1$), we define the elementary symmetric polynomial σ_i^0 in $(n-1)$ variables as

$$\sigma_i^0 := \sigma_1(u_1,\dots,u_{n-1},0).$$

Example 2.7. Consider $n = 3$. Then, $\sigma_2 = u_1u_2 + u_1u_3 + u_2u_3$. Then, $\sigma_2^0 = u_1u_2$. This is the second symmetric polynomial in two variables.

In fact, any elementary symmetric polynomial in $n-1$ variables is of the form σ_i^0 for the corresponding elementary symmetric polynomial σ_i in n variables.

Theorem 2.8 (Fundamental Theorem of Symmetric Polynomials)**.** Let R be a commutative ring. Then, every symmetric polynomial in $S := R[u_1,\dots,u_n]$ is a polynomial in the elementary symmetric polynomials in a unique way.

More precisely, if $f(u_1,\dots,u_n)$ is symmetric, then there exists a unique $g \in R[x_1,\dots,x_n]$ such that

$$g(\sigma_1,\dots,\sigma_n) = f(u_1,\dots,u_n).$$

(The above is equality in S.) [↓]

§2.2. Newton's identities for power sum symmetric polynomials

Definition 2.9. Let $S = R[u_1, \ldots, u_n]$. For $k \geq 1$, define

$$w_k = u_1^k + \cdots + u_n^k.$$

Theorem 2.10 (Newton's Identities)**.** We have

$$w_k = \begin{cases} \sigma_1 w_{k-1} - \sigma_2 w_{k-2} + \cdots + (-1)^k \sigma_{k-1} w_1 + (-1)^{k+1} \sigma_k k & k \leq n, \\ \sigma_1 w_{k-1} - \sigma_2 w_{k-2} + \cdots + (-1)^{n+1} \sigma_n w_{k-n} & k > n. \end{cases} \tag{2.1}$$

[↓]

Note that the last term is $(-1)^{k+1}\sigma_k k$. One might have expected that it would be an 'n' instead but that is not the case.

§2.3. Discriminant of a polynomial

Definition 2.11. Let $f(x) \in \mathbb{F}[x]$ be a non-constant monic polynomial and $\mathbb{K}$ be a splitting field of $f(x)$ over $\mathbb{F}$. Write

$$f(x) = (x - r_1) \cdots (x - r_n)$$

for $r_1, \ldots, r_n \in \mathbb{K}$. Then, the discriminant of $f(x)$ is defined as

$$\operatorname{disc}_{\mathbb{K}}(f(x)) := \prod_{1 \leq i < j \leq n} (r_i - r_j)^2.$$

Remark 2.12. Note that $\operatorname{disc}_{\mathbb{K}}(f(x)) = 0 \iff f(x)$ has repeated roots in $\mathbb{K}$.

Proposition 2.13. Let $f(x) \in \mathbb{F}[x]$ be non-constant and monic. Suppose $\mathbb{K}$ and $\mathbb{K}'$ are two splitting fields of $f(x)$ over $\mathbb{F}$. Then,

$$\operatorname{disc}_{\mathbb{K}}(f(x)) = \operatorname{disc}_{\mathbb{K}'}(f(x)) \in \mathbb{F}.$$

In other words, the discriminant takes values in $\mathbb{F}$ and is independent of the splitting field chosen. [↓]

In view of the (proof of the) above proposition, we have the following alternate definition of discriminant.

Definition 2.14. Let $f(x) = x^n - \sigma_1 x^{n-1} + \cdots + (-1)^n \sigma_n \in \mathbb{F}[x]$ be a monic polynomial. Define w_k for $k = 1, \ldots, 2n-2$ as in (2.1). Then,

$$\operatorname{disc}(f(x)) := \det \begin{bmatrix} n & w_1 & \cdots & w_{n-1} \\ w_1 & w_2 & \cdots & w_n \\ w_2 & w_3 & \cdots & w_{n+1} \\ \vdots & \vdots & \ddots & \vdots \\ w_{n-1} & w_n & \cdots & w_{2n-2} \end{bmatrix}.$$

Proposition 2.15 (Discriminant in terms of derivative)**.** Suppose $f(x) = \prod_{i=1}^n (x - r_i)$. Then, $\operatorname{disc}(f(x)) = (-1)^{\binom{n}{2}} \prod_{i=1}^n f'(r_i)$. [↓]

Example 2.16 (Discriminant of a quadratic)**.** Let $x^2 + bx + c \in \mathbb{F}[x]$ be a quadratic. We have $\sigma_1 = -b$, $\sigma_2 = c$. Thus, we have

$$\begin{aligned} w_1 &= -b, \\ w_2 &= b^2 - 2c. \end{aligned}$$

Thus,

$$\operatorname{disc}(f(x)) = \det \begin{bmatrix} 2 & -b \\ -b & b^2 - 2c \end{bmatrix} = b^2 - 4c.$$

This is the usual discriminant of a quadratic.

Example 2.17 (Discriminant of a special cubic)**.** Let $x^3 + px + q \in \mathbb{F}[x]$ be a cubic. Here, $\sigma_1 = 0$, $\sigma_2 = p$, and $\sigma_3 = -q$. Then, Newton's identities become

$$\begin{aligned} w_1 &= 0, \\ w_2 &= -2p, \\ w_3 &= -3q, \\ w_4 &= 2p^2. \end{aligned}$$

Thus, $\operatorname{disc}(f(x)) = -4p^3 - 27q^2$.

§2.4. The Fundamental Theorem of Algebra

Recall the following facts.

Lemma 2.18.

1. Every real polynomial of odd degree has a real root.

2. Every complex number has a square root. Thus, every complex quadratic polynomial has a root in $\mathbb{C}$. [↓]

Theorem 2.19 (Fundamental Theorem of Algebra)**.** Every non-constant complex polynomial has a root in $\mathbb{C}$. [↓]

Chapter 3

Algebraic Closure of a Field

§3.1. Existence

Definition 3.1. A field $\mathbb{K}$ is called a algebraically closed field if every non-constant polynomial $f(x) \in \mathbb{K}[x]$ has a root in $\mathbb{K}$.

Definition 3.2. Let $\mathbb{K}/\mathbb{F}$ be a field extension. We say that $\mathbb{K}$ is an algebraic closure if $\mathbb{K}$ is algebraically closed and $\mathbb{K}/\mathbb{F}$ is an algebraic extension.

We have the following simple proposition.

Proposition 3.3.

1. $\mathbb{K}$ is algebraically closed iff every non-constant polynomials factors as a product of linear factors.
2. $\mathbb{C}$ is algebraically closed.
3. If $\mathbb{K}$ is algebraically closed and $\mathbb{L}/\mathbb{K}$ is an algebraic extension, then $\mathbb{L} = \mathbb{K}$.

Proposition 3.4. Let $\mathbb{F} \subset \mathbb{K}$ be an extension where $\mathbb{K}$ is algebraically closed. Define,

$$\mathbb{A} := \{\alpha \in \mathbb{K} : \alpha \text{ is algebraic over } \mathbb{F}\}.$$

Then, $\mathbb{A}$ is an algebraic closure of $\mathbb{F}$. [↓]

Lemma 3.5. Let $\{\mathbb{F}_i\}_{i\geq 1}$ be a sequence of fields as

$$\mathbb{F}_1 \subset \mathbb{F}_2 \subset \cdots .$$

Then, $\mathbb{F} := \bigcup_{i\geq 1} \mathbb{F}_i$ is a field with the following operations: Given $a, b \in \mathbb{F}$, there exist smallest $i, j \in \mathbb{N}$ with $a \in \mathbb{F}_i$ and $b \in \mathbb{F}_j$. Then, $a, b \in \mathbb{F}_{i+j}$. Define $a + b$ and ab to be the corresponding elements from $\mathbb{F}_{i+j}$.

Moreover, each $\mathbb{F}_i$ is a subfield of $\mathbb{F}$. [↓]

Note that the "smallest" above is just to ensure that the operations are well-defined. Since $\mathbb{F}_i \subset \mathbb{F}_j$ (note that we always use this to mean "is a subfield of") for $i \leq j$, we can actually pick any i and j.

Theorem 3.6 (Existence of Algebraic Closed Extension)**.** Let $\mathbb{F}$ be a field. Then, there exists an algebraically closed field containing $\mathbb{F}$. [↓]

The proof we have given is due to Artin.

Corollary 3.7 (Existence of Algebraic Closure)**.** Every field $\mathbb{F}$ has an algebraic closure. [↓]

§3.2. Uniqueness

Proposition 3.8. Let $\sigma : \mathbb{F} \to \mathbb{L}$ be an embedding of fields where $\mathbb{L}$ is algebraically closed. Let $\alpha \in \mathbb{K} \supset \mathbb{F}$ be algebraic over $\mathbb{F}$ and $p(x) = \operatorname{irr}(\alpha, \mathbb{F})$.
Write $p(x) = \sum a_i x^i$ and define $p^\sigma(x) := \sum \sigma(a_i) x^i$. Then, $\tau \mapsto \tau(\alpha)$ is a bijection between the sets

$$\{\tau : \mathbb{F}(\alpha) \to \mathbb{L} \mid \tau \text{ is an embedding and } \tau|_{\mathbb{F}} = \sigma\} \leftrightarrow \{\beta \in L \mid p^\sigma(\beta) = 0\}.$$

[↓]

Remark 3.9. The above proposition says that the number of ways to extend from $\mathbb{F}$ to $\mathbb{F}(\alpha)$ is precisely the number of roots of that $p(x)$ has in $\mathbb{L}$. (Not exactly, we need to apply σ to the coefficients. This is essentially saying that we consider $\mathbb{F}$ as a subfield under $\mathbb{L}$.) In particular, this set is non-empty since $\mathbb{L}$ is algebraically closed.
Note that this number need not be $\deg(f(x))$. We shall see in the next chapter that a polynomial may be irreducible but still have repeated roots in its splitting field.

Theorem 3.10. Let $\sigma : \mathbb{F} \to \mathbb{L}$ be an embedding where $\mathbb{L}$ is algebraically closed. Let $\mathbb{K}/\mathbb{F}$ be an algebraic extension. Then, there exists an embedding $\tau : \mathbb{K} \to \mathbb{L}$ extending σ.
Moreover, if $\mathbb{K}$ is an algebraic closure of $\mathbb{F}$ and $\mathbb{L}$ of $\sigma(\mathbb{K})$, then τ is an isomorphism extending σ. [↓]

Corollary 3.11 (Isomorphism of algebraic closures)**.** If $\mathbb{K}_1$ and $\mathbb{K}_2$ are two algebraic closures of $\mathbb{F}$, then they are $\mathbb{F}$-isomorphic.

Proof. Apply previous proposition to the inclusion $i : \mathbb{F} \hookrightarrow \mathbb{E}_2$ to extend it to an $\mathbb{F}$-isomorphism $\tau : \mathbb{E}_1 \to \mathbb{E}_2$. □

Definition 3.12. Given a field $\mathbb{F}$, we use $\overline{\mathbb{F}}$ to denote an algebraic closure of $\mathbb{F}$.

Theorem 3.13 (Isomorphism of splitting fields)**.** Let $\mathbb{E}$ and $\mathbb{E}'$ be two splitting fields of a non-constant polynomial $f(x) \in \mathbb{F}[x]$ over $\mathbb{F}$. Then, they are $\mathbb{F}$-isomorphic. [↓]

Chapter 4

Separable extensions

§4.1. Derivatives

Definition 4.1. Let $\mathbb{F}$ be a field. Define the $\mathbb{F}$-linear map $\mathrm{D}_{\mathbb{F}} : \mathbb{F}[x] \to \mathbb{F}[x]$ by

$$\mathrm{D}_{\mathbb{F}}\left(\sum_{i=0}^{n} a_i x^i\right) = \sum_{i=1}^{n} i a_i x^{i-1}.$$

Given $f(x) \in \mathbb{F}[x]$, we call $\mathrm{D}_{\mathbb{F}}(f(x))$ the derivative of $f(x)$ and also denote it by $f'(x)$.

Remark 4.2. Note that the above definition requires no notion of limits. For the case of $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$, then it coincides with the usual definition if we identify a polynomial with the function it represents. We shall not require this, however.

We have the follow easy-to-check proposition.

Proposition 4.3. Let $f(x), g(x) \in \mathbb{F}[x]$ and $a \in \mathbb{F}$ be arbitrary. Then,

1. $(f \pm ag)'(x) = f'(x) \pm ag'(x)$,
2. $(fg)'(x) = f'(x)g(x) + f(x)g'(x)$.

The first point is just verifying that $\mathrm{D}_{\mathbb{F}}$ is indeed $\mathbb{F}$-linear.

Proposition 4.4. Let $\mathbb{F} \subset \mathbb{E}$ be a field extension. Then, $\mathrm{D}_{\mathbb{E}}|_{\mathbb{F}} = \mathrm{D}_{\mathbb{F}}$. Thus, the notation $f'(x)$ is unambiguous.

Definition 4.5. Let $f(x) \in \mathbb{F}[x]$ be a non-constant monic polynomial. Let $\mathbb{E}$ be a splitting field of $f(x)$ over $\mathbb{F}$. In $\mathbb{E}[x]$, factorise $f(x)$ uniquely as

$$f(x) = (x - r_1)^{e_1} \cdots (x - r_g)^{e_g},$$

where $r_1, \ldots, r_g \in \mathbb{E}$ are distinct and each $e_i \in \mathbb{N}$.

The numbers $e_1, \ldots, e_g$ are called the multiplicities of the roots $r_1, \ldots, r_n$.
If $e_i = 1$ for some i, then r_i is called a simple root and a repeated root otherwise.

If each $e_i = 1$, then $f(x)$ is said to be a separable polynomial.

If f is not monic, we have the same definitions upon division by the leading coefficient.

Remark 4.6. Note that the definition of "separable polynomial" is ad hoc since the separability presumably depends on the splitting field. However, in view of Remark 2.12, we see that separability depends only on $\operatorname{disc}(f(x))$, which we have seen to be independent of the splitting field.
The next proposition shows something even stronger.

Also, note that one might think that an irreducible polynomial is always separable. We will see an example of how that is not true, in general. Over fields of characteristic 0, however, it is true. We shall prove that as well.

Proposition 4.7. The number of roots and their multiplicities are independent of the splitting field chosen for $f(x)$ over $\mathbb{F}$. [↓]

Proposition 4.8. Let $f(x) \in \mathbb{F}[x]$ be a monic and let $r \in \mathbb{E} \supset \mathbb{F}$ be a root of $f(x)$. Then, r is a repeated root iff $f'(r) = 0$. [↓]

Theorem 4.9 (The Derivative Criterion for Separability)**.** Let $f(x) \in \mathbb{F}[x]$ be a monic polynomial.

1. If $f'(x) = 0$, then every root of $f(x)$ is a multiple root.
2. If $f'(x) \neq 0$, then $f(x)$ has simple roots iff $\gcd(f(x), f'(x)) = 1$. [↓]

Proposition 4.10. Let $f(x) \in \mathbb{F}[x]$ be irreducible and non-constant.

1. $f(x)$ is separable iff $f'(x) \neq 0$.
2. If $\operatorname{char}(\mathbb{F}) = 0$, then $f(x)$ is separable.

In other words, irreducible polynomials over fields of characteristic 0 are separable. [↓]

Example 4.11. Let $p \in \mathbb{N}$ be a prime. Consider the field $\mathbb{F}_p(X)$ and the polynomial $f(T) = T^p - X \in \mathbb{F}_p(X)[T]$.
Then, $f(T)$ is irreducible, by applying Eisenstein at the prime X. However, $f'(T) = 0$ and hence, not separable.

In fact, as we shall see, the existence of p-th roots will play an important role.

Definition 4.12. Let $\mathbb{F}$ be a field of prime characteristic p. Define

$$\mathbb{F}^p := \{\alpha^p \in \mathbb{F} : \alpha \in \mathbb{F}\}.$$

That is, $\mathbb{F}^p$ is the set of all p-th powers of elements of $\mathbb{F}$.

Proposition 4.13. $\mathbb{F}^p$ is a subfield of $\mathbb{F}$.

Proof. Only closure under addition is not so obvious. Note that $(x+y)^p = x^p + y^p$ for all $x, y \in \mathbb{F}$. □

Proposition 4.14. Let $\mathbb{F}$ be a field with $\mathrm{char}(\mathbb{F}) = p > 0$. Then, $x^p - a \in \mathbb{F}[x]$ is either irreducible in $\mathbb{F}[x]$ or $a \in \mathbb{F}^p$. [↓]

Proposition 4.15. Let $f(x) \in \mathbb{F}[x]$ be an irreducible polynomial and let $p := \mathrm{char}(\mathbb{F}) > 0$. If $f(x)$ is not separable, then there exists $g(x) \in \mathbb{F}[x]$ such that $f(x) = g(x^p)$. [↓]

§4.2. Perfect fields

Definition 4.16. Let $\mathbb{F} \subset \mathbb{K}$ be a field extension.

An algebraic element $\alpha \in \mathbb{K}$ over $\mathbb{F}$ is called a separable element over $\mathbb{F}$ if $\mathrm{irr}(\alpha, \mathbb{F})$ is separable over $\mathbb{F}$.

We say that $\mathbb{K}/\mathbb{F}$ is a separable field extension if every $\alpha \in \mathbb{K}$ is separable (and in particular, algebraic).

We say that $\mathbb{F}$ is a perfect field if every algebraic extension of $\mathbb{F}$ is separable. Equivalently, every irreducible polynomial in $\mathbb{F}[x]$ is separable.

Example 4.17.

1. We had seen that $\mathbb{F}_p(X)$ is not perfect for any prime p.
2. By Proposition 4.10, we have that every field of characteristic 0 is perfect.

Theorem 4.18. Let $\mathbb{F}$ be a field with characteristic $p > 0$. Then, $\mathbb{F}$ is perfect iff $\mathbb{F} = \mathbb{F}^p$. [↓]

Corollary 4.19. Every finite field is perfect. [↓]

§4.3. Extensions of embeddings

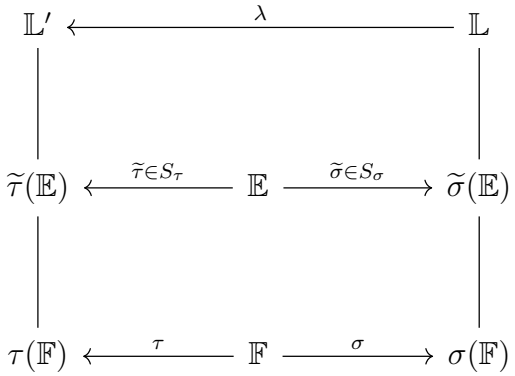
Proposition 4.20. Let $f(x) \in \mathbb{F}[x]$ be an irreducible monic polynomial. Then, all roots of $f(x)$ have equal multiplicity (in any splitting field).
If $\mathrm{char}(\mathbb{F}) = 0$, then all roots are simple.
If $\mathrm{char}(\mathbb{F}) =: p > 0$, then all roots have multiplicity p^n for some $n \in \mathbb{N}_0$. [↓]

Note that by Proposition 4.7, the n also does not depend on choice of splitting field.

Theorem 4.21. Let $\sigma : \mathbb{F} \to \mathbb{L}$ be an embedding of fields where $\mathbb{L}$ is an algebraic closure of $\sigma(\mathbb{F})$. Similarly, let $\tau : \mathbb{F} \to \mathbb{L}'$ be an embedding of fields where $\mathbb{L}'$ is an algebraic closure of $\tau(\mathbb{F})$. Let $\mathbb{E}$ be an algebraic extension of $\mathbb{F}$.

Let S_σ (resp. S_τ) denote the set of extensions of σ (resp. τ) to embeddings of $\mathbb{E}$ into $\mathbb{L}$ (resp. $\mathbb{L}'$). Let $\lambda : \mathbb{L} \to \mathbb{L}'$ be an isomorphism extending $\tau \circ \sigma^{-1} : \sigma(\mathbb{F}) \to \tau(\mathbb{F})$.

The map $\psi : S_\sigma \to S_\tau$ given by $\psi(\widetilde{\sigma}) = \lambda \circ \widetilde{\sigma}$ is a bijection. [↓]



Remark 4.22. What the above proposition is really saying is that the "number" (cardinality) of extensions does not depend on $\mathbb{L}$ **or** on the embedding σ. Note that since $\mathbb{E}$ is an arbitrary algebraic extension, the set S_σ need not be finite.

Thus, we may assume $\mathbb{L} \supset \mathbb{F}$ to be an algebraic closure and σ to be the natural inclusion.

Definition 4.23. If $\mathbb{E}/\mathbb{F}$ is an algebraic extension, then the cardinality of S_σ (as in Theorem 4.21) is called the separable degree of $\mathbb{E}/\mathbb{F}$ and is denoted $[\mathbb{E} : \mathbb{F}]_s$.

Remark 4.24. Note that if $\sigma : \mathbb{F} \to \mathbb{L}$ is an embedding into an algebraically closed field $\mathbb{L}$, and $\widetilde{\sigma} : \mathbb{E} \to \mathbb{L}$ is an extension of σ, where $\mathbb{E}/\mathbb{F}$ is algebraic, then $\widetilde{\sigma}(\mathbb{E})$ is actually contained in the algebraic closure of $\sigma(\mathbb{F})$ within $\mathbb{L}$. Thus, it is fine even if $\mathbb{L}$ is not an algebraic closure of $\sigma(\mathbb{F})$.

Proposition 4.25. Let $\alpha \in \mathbb{E} \supset \mathbb{F}$ be algebraic over $\mathbb{F}$ and $n := \deg(\mathrm{irr}(\alpha, \mathbb{F}))$. Then, $[\mathbb{F}(\alpha) : \mathbb{F}]_s \leq n = [\mathbb{F}(a) : \mathbb{F}]$ with equality iff α is separable over $\mathbb{F}$.

Proof. By Proposition 3.8, we know that $[\mathbb{F}(\alpha) : \mathbb{F}]_s$ is exactly the number of roots of $p(x) = \mathrm{irr}(\alpha, \mathbb{F})$ in $\overline{\mathbb{F}}$. This is at most $n = \deg(p(x))$. Moreover, equality implies that all roots are distinct and hence, α is separable. □

Theorem 4.26 (Tower Law for separable degree)**.** Let $\mathbb{F} \subset \mathbb{E} \subset \mathbb{K}$ be a tower of finite algebraic extensions. Then, $[\mathbb{E} : \mathbb{F}]_s \leq [\mathbb{E} : \mathbb{F}]$ and

$$[\mathbb{K} : \mathbb{F}]_s = [\mathbb{K} : \mathbb{E}]_s [\mathbb{E} : \mathbb{F}]_s.$$

[↓]

Corollary 4.27. Let $\mathbb{F} \subset \mathbb{E} \subset \mathbb{K}$ be a tower of finite algebraic extensions. Then, $[\mathbb{K} : \mathbb{F}] = [\mathbb{K} : \mathbb{F}]_s$ iff equality holds at each stage.

Theorem 4.28. Let $\mathbb{E}/\mathbb{F}$ be a finite extension. Then, $\mathbb{E}/\mathbb{F}$ is separable iff $[\mathbb{E} : \mathbb{F}]_s = [\mathbb{E} : \mathbb{F}]$. [↓]

Corollary 4.29. Let $\alpha \in \mathbb{E} \supset \mathbb{F}$ be separable over $\mathbb{F}$. Then, $\mathbb{F}(\alpha)/\mathbb{F}$ is a separable extension.

Proof. By Proposition 4.25, we have $[\mathbb{F}(\alpha) : \mathbb{F}]_s = [\mathbb{F}(\alpha) : \mathbb{F}]$. By Theorem 4.28, this means that $\mathbb{F}(\alpha)/\mathbb{F}$ is separable. □

Proposition 4.30. Let $\mathbb{F} \subset \mathbb{E} \subset \mathbb{K}$ be a tower of fields. Then, $\mathbb{K}/\mathbb{F}$ is separable iff $\mathbb{K}/\mathbb{E}$ and $\mathbb{E}/\mathbb{F}$ are separable. [↓]

Proposition 4.31. Let $\mathbb{E}/\mathbb{F}$ be a finite extension. Then, $[\mathbb{E} : \mathbb{F}]_s$ divides $[\mathbb{E} : \mathbb{F}]$. If $\mathrm{char}(\mathbb{F}) =: p > 0$, then quotient $\dfrac{[\mathbb{E} : \mathbb{F}]}{[\mathbb{E} : \mathbb{F}]_s}$ is a power of p. [↓]

§4.4. Finite fields

§4.5. Existence and Uniqueness

In this section, p will denote an arbitrary prime number.

Theorem 4.32 (Uniqueness of finite fields)**.** Let $\mathbb{K}$ and $\mathbb{L}$ be finite fields with same cardinality. Then, $\mathbb{K}$ and $\mathbb{L}$ are isomorphic. [↓]

Definition 4.33. We shall denote the finite with p^n elements by $\mathbb{F}_{p^n}$.

Remark 4.34. We have not yet shown that $\mathbb{F}_{p^n}$ for every prime p and $n \in \mathbb{N}$. Have only shown uniqueness up to isomorphism.

Theorem 4.35 (Existence of finite fields)**.** Fix a prime p and an algebraic closure $\overline{\mathbb{F}}_p$. For every $n \in \mathbb{N}$, there exists a unique subfield of $\overline{\mathbb{F}}_p$ of size p^n, denoted $\mathbb{F}_{p^n}$. Moreover

$$\overline{\mathbb{F}}_p = \bigcup_{n \in \mathbb{N}} \mathbb{F}_{p^n}.$$

[↓]

§4.6. Gauss' Necklace Formula

Recall the Möbius inversion formula.

Theorem 4.36 (Möbius inversion formula)**.**

Chapter 5

Proofs

Proposition 1.9. Every finite extension is an algebraic extension. [↓]

[↑]

Proof. Let $\mathbb{K}/\mathbb{F}$ be a finite extension with $n := \dim_{\mathbb{F}}(\mathbb{K})$. Let $b \in \mathbb{K}$ be arbitrary. Consider the multiset $\{1, b, \ldots, b^n\}$. It has $n+1$ elements and thus, is linearly dependent. Thus, there exist $a_0, \ldots, a_n \in \mathbb{F}$ not all 0 such that

$$a_0 + a_1 b + \cdots + a_n b^n = 0.$$

Then, $f(x) := a_0 + a_1 b + \cdots + a_n x^n \in \mathbb{F}[x]$ is a non-zero polynomial such that $f(b) = 0$. □

Proposition 1.13. Let $\mathbb{K}/\mathbb{F}$ be a field extension and $\alpha \in \mathbb{K}$ be algebraic over $\mathbb{F}$. Then, the following are true.

1. There exists a unique monic irreducible polynomial $f(x) \in \mathbb{F}[x]$ such that $f(\alpha) = 0$.
2. $f(x)$ generates the kernel of the map $\mathbb{F}[x] \to \mathbb{F}[\alpha] \subset \mathbb{K}$ given by $p(x) \mapsto p(\alpha)$.
3. If $g(x) \in \mathbb{F}[x]$ is such that $g(\alpha) = 0$, then $f(x) \mid g(x)$.
4. In particular, $f(x)$ has the least positive degree among all polynomials in $\mathbb{F}[x]$ satisfied by α. [↓]

[↑]

Proof. Define $\psi : \mathbb{F}[x] \to \mathbb{K}$ by $p(x) \mapsto p(\alpha)$. Since α is algebraic, $I := \ker(\psi)$ is non-zero.

Since $\mathbb{F}[x]$ is a PID, we have $I = \langle f(x) \rangle$ for some $0 \neq f(x) \in \mathbb{F}[x]$. Since $\mathbb{F}[x]/I$ is isomorphic to a subring of $\mathbb{K}$, it is an integral domain and hence, $f(x)$ is irreducible. By scaling, we may assume that $f(x)$ is monic. Clearly, any other $g(x)$ as in the proposition is in the kernel and hence, $f(x) \mid g(x)$.

In particular, if $g(x)$ is irreducible and monic, then $f(x) \mid g(x) \implies g(x) = af(x)$ for some $a \in \mathbb{F}^\times$. Since $g(x)$ is also monic, we have $a = 1$. □

Proposition 1.16. Let $\mathbb{K}/\mathbb{F}$ be a field extension and $\alpha \in \mathbb{K}$ be algebraic over $\mathbb{F}$. Let $f(x) := \operatorname{irr}(\alpha, \mathbb{F})$ and $n := \deg f(x)$. Then,

1. $\mathbb{F}[\alpha] = \mathbb{F}(\alpha) \cong \mathbb{F}[x]/\langle f(x) \rangle$.
2. $\dim_{\mathbb{F}}(\mathbb{F}(\alpha)) = n$ and $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is an $\mathbb{F}$-basis of $\mathbb{F}(\alpha)$. [↓]

[↑]

Proof. Consider the substitution homomorphism $\psi : \mathbb{F}[x] \to \mathbb{F}[\alpha]$ given by $p(x) \mapsto p(\alpha)$.

By Proposition 1.13, we know that $\ker(\psi) = \langle f(x) \rangle$. Since $f(x) \neq 0$, the ideal $\langle f(x) \rangle$ is maximal.

Since ψ is onto and $\ker(\psi)$ maximal, we see that $\mathbb{F}[\alpha]$ is in fact a field and hence, $\mathbb{F}[\alpha] = \mathbb{F}(\alpha)$.

Consider $B = \{1, \alpha, \ldots, \alpha^{n-1}\}$.
Using $f(x)$, we may recursively write all higher powers of α as an $\mathbb{F}$-linear combination of elements of B. Thus, B spans $\mathbb{F}[\alpha]$.
For linear independence, suppose that $a_0, \ldots, a_{n-1} \in \mathbb{F}$satisfy

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = 0.$$

Then, we get a polynomial $g(x) = a_0 + a_1 x + \cdots a_{n-1}x^{n-1} \in \mathbb{F}[x]$ satisfied by α. Since $\deg(g(x)) < \deg(f(x))$, we see that $g(x) = 0$, again by Proposition 1.13. □

Proposition 1.18. Let $\alpha, \beta \in \mathbb{K} \supset \mathbb{F}$ be algebraic over $\mathbb{F}$. Then, there exists and $\mathbb{F}$-isomorphism $\psi : \mathbb{F}(\alpha) \to \mathbb{F}(\beta)$ such that $\psi(\alpha) = \beta$ iff $\operatorname{irr}(\alpha, \mathbb{F}) = \operatorname{irr}(\beta, \mathbb{F})$. [↓]

[↑]

Proof. ($\implies$) Let $\psi : \mathbb{F}(\alpha) \to \mathbb{F}(\beta)$ be as mentioned.

Put $f(x) := \mathrm{irr}(\alpha, \mathbb{F})$ and $g(x) := \mathrm{irr}(\beta, \mathbb{F})$. Then,

$$\begin{aligned} 0 &= \psi(0) \\ &= \psi(f(\alpha)) \\ &= f(\psi(\alpha)) \\ &= f(\beta). \end{aligned}$$

ψ *is an* $\mathbb{F}$*-isomorphism*

Thus, $g(x) \mid f(x)$. Since both are irreducible and monic, $g(x) = f(x)$.

($\Longleftarrow$) Let $f(x) := \mathrm{irr}(\alpha, \mathbb{F}) = \mathrm{irr}(\beta, \mathbb{F})$.
The isomorphisms $\mathbb{F}(\alpha) \cong \mathbb{F}[x]/\langle f(x)\rangle \cong \mathbb{F}(\beta)$ are $\mathbb{F}$-isomorphisms and so is their composition. □

Theorem 1.21 (Tower law)**.** Let $\mathbb{F} \subset \mathbb{E} \subset \mathbb{K}$ be a tower of fields. Then,

$$[\mathbb{K} : \mathbb{F}] = [\mathbb{K} : \mathbb{E}][\mathbb{E} : \mathbb{F}].$$

In particular, the left side is ∞ iff the right side is. [↓]

[↑]

Proof. If $\mathbb{K}/\mathbb{F}$ is a finite extension, then so are $\mathbb{K}/\mathbb{E}$ (pick a finite basis of $\mathbb{K}/\mathbb{F}$, it is a spanning set for $\mathbb{K}/\mathbb{E}$) and $\mathbb{E}/\mathbb{F}$ ($\mathbb{E}$ is an $\mathbb{F}$-subspace of $\mathbb{K}$.)

Thus, if either of $\mathbb{K}/\mathbb{E}$ or $\mathbb{E}/\mathbb{F}$ is not a finite extension, then neither is $\mathbb{K}/\mathbb{F}$.

Now, assume that both $n := [\mathbb{K} : \mathbb{E}]$ and $m := [\mathbb{E} : \mathbb{F}]$ are finite. Let $\{\alpha_i\}_{i=1}^n \subset \mathbb{K}$ be an $\mathbb{E}$-basis and $\{\beta_j\}_{j=1}^m \subset \mathbb{E}$ be an $\mathbb{F}$-basis.

Put $B := \{\alpha_i\beta_j : 1 \le i \le n,\ 1 \le j \le m\} \subset \mathbb{K}$. We show that B is an $\mathbb{F}$-basis of $\mathbb{K}$.

Spanning. Let $a \in \mathbb{K}$ be arbitrary. Write

$$a = \sum_{i=1}^{n} a_i \alpha_i$$

for $a_i \in \mathbb{E}$. For each $i = 1, \ldots, n$, write

$$a_i = \sum_{j=1}^{m} b_{ij} \beta_j$$

for $j \in \mathbb{F}$. Then,

$$a = \sum_{i=1}^{n} \sum_{j=1}^{m} b_{ij} (\alpha_i \beta_j)$$

is an $\mathbb{F}$-linear combination of elements of B.

Linear independence. Let $\{b_{ij} : 1 \leq i \leq n,\ 1 \leq j \leq m\} \subset \mathbb{F}$ be such that

$$\sum_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} b_{ij}\alpha_i\beta_j = 0.$$

Group the above to get

$$\sum_{i=1}^{n} \left[\sum_{j=1}^{m} b_{ij}\alpha_i \right] \beta_j = 0.$$

Linear independence of $\{\beta_j\}$ forces $\sum_{j=1}^{m} b_{ij}\alpha_i = 0$ for all i. In turn, linear independence of $\{\alpha_i\}$ that forces each b_{ij} to be 0.

Note that B actually has cardinality mn. (Why?) This finishes the proof. □

Proposition 1.23. Let $\mathbb{K}/\mathbb{F}$ be a field extension and let $\alpha_1, \ldots, \alpha_n \in \mathbb{K}$ be algebraic over $\mathbb{F}$. Then, $\mathbb{F}(\alpha_1, \ldots, \alpha_n)$ is a finite (and hence, algebraic) extension of $\mathbb{F}$. [↓]

[↑]

Proof. Consider the tower

$$\mathbb{F} \subset \mathbb{F}(\alpha_1) \subset \mathbb{F}(\alpha_1, \alpha_2) \subset \cdots \subset \mathbb{F}(\alpha_1, \ldots, \alpha_n).$$

At each stage, an element being adjoined is algebraic over the previous field. (Proposition 1.8.)

Thus, each consecutive degree above is finite. (Corollary 1.17.)

By the Tower law, so is the overall degree. □

Corollary 1.24. Let $\mathbb{F} \subset \mathbb{E}$ and $\mathbb{E} \subset \mathbb{K}$ be algebraic extensions. Then, $\mathbb{F} \subset \mathbb{K}$ is an algebraic extension. [↓]

[↑]

Proof. Let $\alpha \in \mathbb{K}$. Let $\operatorname{irr}(\alpha, \mathbb{E}) =: f(x) = a_0 + \cdots + a_{n-1}x^{n-1} + x^n$.

Let $\mathbb{L} := \mathbb{F}(a_0, \ldots, a_{n-1})$.

Then, $\mathbb{L}$ is finite over $\mathbb{F}$ since each $a_i \in \mathbb{R}$ is algebraic over $\mathbb{F}$. Moreover, $0 \neq f(x) \in \mathbb{L}[x]$. Thus, α is algebraic over $\mathbb{L}$ and hence, $\mathbb{L}(\alpha)$ is finite over $\mathbb{L}$.

By the Tower law, $\mathbb{L}/\mathbb{F}$ is finite and thus, α is algebraic over $\mathbb{F}$. (Proposition 1.9.) □

Corollary 1.25. Let $\mathbb{K}/\mathbb{F}$ be a field extension. Then,

$$\mathbb{A} := \{\alpha \in \mathbb{K} : \alpha \text{ is algebraic over } \mathbb{F}\}$$

is a subfield of $\mathbb{K}$ containing $\mathbb{F}$.
Moreover, $\mathbb{A}/\mathbb{F}$ is an algebraic extension. [↓]

[↑]

Proof. $\mathbb{F} \subset \mathbb{A}$ is clear. We show that $\mathbb{A}$ is a subfield. Let $\alpha, \beta \in \mathbb{A}$ with $\beta \neq 0$. Then, $\mathbb{L} := \mathbb{F}(\alpha, \beta)$ is a finite extension over $\mathbb{F}$.
Thus, all elements of $\mathbb{L}$ are algebraic over $\mathbb{F}$. In particular, so are $\alpha \pm \beta$, $\alpha\beta$ and $\alpha\beta^{-1}$. □

Proposition 1.29. Let $\mathbb{F}$ be a field which is a subring of an integral domain R. Suppose R is finite dimensional as an $\mathbb{F}$ vector space. Then, R is a field. [↓]

[↑]

Proof. We only need to show that every non-zero element of R has a multiplicative inverse (in R). Let $0 \neq a \in R$ be arbitrary. Since $\dim_{\mathbb{F}}(R) < \infty$, there is a smallest $n \geq 1$ such that the set $\{1, a, \ldots, a^n\}$ is linearly dependent. Then, let $b_0, \ldots, b_n \in \mathbb{F}$ be not all zero such that

$$b_0 + b_1 a + \cdots b_n a^n = 0.$$

If $b_n = 0$, then the minimality of n is contradicted. If $b_0 = 0$, then we may cancel a (R is an integral domain and $a \neq 0$) and again contradict the minimality of n. Thus, we get

$$a(b_1 + \cdots + b_n a^{n-1}) = -b_0.$$

This shows that

$$-\frac{1}{b_0}(b_1 + \cdots + b_n a^{n-1}) \in R$$

is a multiplicative inverse of a. □

Proposition 1.30. Let $\mathbb{F} \subset \mathbb{E}_1, \mathbb{E}_2 \subset \mathbb{K}$ be fields. Consider

$$\mathbb{L} = \left\{ \sum_{i=1}^{n} \alpha_i \beta_i : n \in \mathbb{N}, \alpha_i \in \mathbb{E}_1, \beta_i \in \mathbb{E}_2 \right\}.$$

That is, let $\mathbb{L}$ be the set of all finite sums of products of elements of $\mathbb{E}_1$ and $\mathbb{E}_2$.

Suppose $d := [\mathbb{E}_1 : \mathbb{K}][\mathbb{E}_2 : \mathbb{K}] < \infty$.
Then $\mathbb{L} = \mathbb{E}_1\mathbb{E}_2$ and $[\mathbb{L} : \mathbb{F}] \leq d$.

If $[\mathbb{E}_1 : \mathbb{F}]$ and $[\mathbb{E}_2 : \mathbb{F}]$ are coprime, then equality holds. [↓]

[↑]

Proof. Simple computations show that $\mathbb{L}$ is indeed a subring of $\mathbb{K}$. If $\{\alpha_1, \ldots, \alpha_n\}$ and $\{\beta_1, \ldots, \beta_m\}$ are $\mathbb{F}$-bases for $\mathbb{E}_1$ and $\mathbb{E}_2$, then clearly $\{\alpha_i\beta_j : 1 \leq i \leq n,\ 1 \leq j \leq m\}$ spans $\mathbb{L}$ over $\mathbb{F}$. Thus, $\dim_{\mathbb{F}}(\mathbb{L}) \leq mn = d$.

Since $\mathbb{L}$ is a subring of $\mathbb{K}$, it is an integral domain and hence, $\mathbb{L}$ is a field, by Proposition 1.29.

Lastly, note that $[\mathbb{E}_i : \mathbb{F}]$ divides $[\mathbb{L} : \mathbb{F}]$, in view of the Tower law. In particular, if $\gcd(m, n) = 1$, then $mn \mid [\mathbb{L} : \mathbb{F}]$. Since $[\mathbb{L} : \mathbb{F}] \leq mn$, we are done. □

Theorem 1.34. Let $\mathbb{F}$ be a field and $f(x) \in \mathbb{F}[x]$ be non-constant. Then, there exists a field $\mathbb{K} \supset \mathbb{F}$ such that $f(x)$ has a root in $\mathbb{K}$. [↓]

[↑]

Proof. Let $g(x)$ be an irreducible factor of $f(x)$.

Put $\mathbb{K} = \mathbb{F}[x]/\langle g(x)\rangle$. Since $g(x)$ is irreducible and non-zero, the quotient is indeed a field. Clearly, $\mathbb{F}$ is a subfield under the identification $a \mapsto \bar{a}$. Moreover, $\bar{x}$ is a root of $g(x)$. □

Theorem 1.35 (Existence of Splitting Field)**.** Let $\mathbb{F}$ be a field. Any polynomial $f(x) \in \mathbb{F}[x]$ of positive degree has a splitting field. [↓]

[↑]

Proof. Let $n := \deg(f)$. By Chapter 5, there exists a field $\mathbb{F}_1 \supset \mathbb{F}$ such that $f(x)$ has a root in $\mathbb{F}_1$. Calling this root a_1, we see that

$$f(x) = (x - a_1)f_1(x)$$

with $\deg(f_1) = n - 1$. Continuing inductively, we get fields

$$\mathbb{F}_n \supset \cdots \supset \mathbb{F}_1 \supset \mathbb{F}$$

with $a_i \in \mathbb{F}_i$, such that

$$f(x) = a(x - a_1) \cdots (x - a_n).$$

Then, $\mathbb{K} = \mathbb{F}(a_1, \ldots, a_n) \subset \mathbb{F}_n$ is a splitting field. □

Theorem 2.8 (Fundamental Theorem of Symmetric Polynomials)**.** Let R be a commutative ring. Then, every symmetric polynomial in $S := R[u_1, \ldots, u_n]$ is a polynomial in the elementary symmetric polynomials in a unique way.

More precisely, if $f(u_1, \ldots, u_n)$ is symmetric, then there exists a unique $g \in R[x_1, \ldots, x_n]$ such that

$$g(\sigma_1, \ldots, \sigma_n) = f(u_1, \ldots, u_n).$$

(The above is equality in S.) [↓]

[↑]

Proof. **Existence.** We apply induction on n. The case $n = 1$ is clear since every polynomial is symmetric and $\sigma_1 = u_1$. So, $g = f$ itself works[1].

Suppose the theorem is true for $n-1$. Now, to prove the theorem for n, apply induction on $\deg(f)$. If f is constant, then again $g = f$ works. Suppose $\deg(f) \geq 1$. Define

$$f^0 := f(u_1, \ldots, u_{n-1}, 0) \in R[u_1, \ldots, u_{n-1}].$$

Then, f^0 is a symmetric polynomial in $n-1$ variables. By induction hypothesis (on variables), there exists $g \in R[x_1, \ldots, x_{n-1}]$ such that

$$f^0(u_1, \ldots, u_{n-1}) = g(\sigma_1^0, \ldots, \sigma_{n-1}^0).$$

Define $f_1 \in R[u_1, \ldots, u_n]$ by

$$f_1(u_1, \ldots, u_n) = f(u_1, \ldots, u_n) - g(\sigma_1, \ldots, \sigma_{n-1}).$$

Then, $f_1(u_1, \ldots, u_{n-1}, 0) = 0$. Thus, $u_n \mid f_1$. However, note that f_1 is symmetric and thus, $\sigma_n \mid f_1$. Thus, we can write

$$f_1(u_1, \ldots, u_n) = \sigma_n h(u_1, \ldots, u_n)$$

for some $h \in R[u_1, \ldots, u_n]$. Since σ_n is not a zero-divisor in $R[u_1, \ldots, u_n]$, we see that h is also symmetric with $\deg(h) < \deg(f)$. Thus, by inductive hypothesis, h is a polynomial in $\sigma_1, \ldots, \sigma_n$ and hence, f is so.

Uniqueness. It suffices to show that the elementary symmetric polynomials are algebraically independent. That is, to show that the map

$$\varphi : R[z_1, \ldots, z_n] \to R[u_1, \ldots, u_n]$$

[1] Being slightly sloppy since the indeterminates are different. We mean that you must take the same coefficients

defined by

$$z_i \mapsto \sigma_i \quad \text{and} \quad \varphi|_R = \mathrm{id}_R$$

is an injection.

We prove this by induction on n. For $n = 1$, it is clear since $\sigma_1 = u_1$, an indeterminate. Assume that $n \geq 1$ and that the result is true for $n - 1$. If φ is not an injection, then we pick a nonzero polynomial $f(z_1, \ldots, z_n) \in \ker(\varphi)$ of least degree. Write f as a polynomial in z_n as

$$f(z_1, \ldots, z_n) = f_0(z_1, \ldots, z_{n-1}) + \cdots + f_d(z_1, \ldots, z_{n-1}) z_n^d$$

with $f_d \neq 0$. Minimality of d (and the fact that σ_n is not a zero-divisor) forces that $f_0 \neq 0$. Since $f \in \ker(\varphi)$, we have

$$f_0(\sigma_1, \ldots, \sigma_{n-1}) + \cdots + f_d(\sigma_1, \ldots, \sigma_{n-1}) \sigma_n^d = 0.$$

The above is an equality in $R[u_1, \ldots, u_n]$. Put $u_n = 0$ to get

$$f_0(\sigma_1^0, \ldots, \sigma_{n-1}^0) = 0.$$

But the above shows that the corresponding φ for $n - 1$ variables is not injective. A contradiction. □

Theorem 2.10 (Newton's Identities)**.** We have

$$w_k = \begin{cases} \sigma_1 w_{k-1} - \sigma_2 w_{k-2} + \cdots + (-1)^k \sigma_{k-1} w_1 + (-1)^{k+1} \sigma_k k & k \leq n, \\ \sigma_1 w_{k-1} - \sigma_2 w_{k-2} + \cdots + (-1)^{n+1} \sigma_n w_{k-n} & k > n. \end{cases} \tag{2.1}$$

[↓]

[↑]

Proof. Let z be an indeterminate over $S := R[u_1, \ldots, u_n]$. Note that

$$(1 - u_1 z) \cdots (1 - u_n z) = 1 - \sigma_1 z + \cdots + (-1)^n \sigma_n z^n =: \sigma(z). \tag{5.1}$$

Define $w(z) \in S[\![z]\!]$ as

$$\begin{aligned} w(z) &= \sum_{k=1}^{\infty} w_k z^k \\ &= \sum_{k=1}^{\infty} \left(\sum_{i=1}^{n} u_i^k \right) z^k \\ &= \sum_{i=1}^{n} \left(\sum_{k=1}^{\infty} (u_i z)^k \right) \\ &= \sum_{i=1}^{n} \frac{u_i z}{1 - u_i z}. \end{aligned}$$

Now, since $\sigma(z) = (1 - u_1 z) \cdots (1 - u_n z)$, we get

$$\sigma'(z) = -\sum_{i=1}^{n} \frac{u_i \sigma(z)}{1 - u_i z},$$

where we have taken the formal derivative in $S[\![z]\!]$. Rearranging the above gives

$$-\frac{z\sigma'(z)}{\sigma(z)} = \sum_{i=1}^{n} \frac{u_i z}{1 - u_i z} = w(z)$$

and hence,

$$w(z)\sigma(z) = -z\sigma'(z).$$

Computing $\sigma'(z)$ from (5.1) gives

$$w(z)\sigma(z) = \sigma_1 z - 2\sigma_2 z^2 + \cdots + (-1)^{n+1} n \sigma_n z^n.$$

Comparing the coefficients of x^k on both sides gives the result. □

Proposition 2.13. Let $f(x) \in \mathbb{F}[x]$ be non-constant and monic. Suppose $\mathbb{K}$ and $\mathbb{K}'$ are two splitting fields of $f(x)$ over $\mathbb{F}$. Then,

$$\operatorname{disc}_{\mathbb{K}}(f(x)) = \operatorname{disc}_{\mathbb{K}'}(f(x)) \in \mathbb{F}.$$

In other words, the discriminant takes values in $\mathbb{F}$ and is independent of the splitting field chosen. [↓]

[↑]

Proof. Let $r_1, \ldots, r_n \in \mathbb{K}$ be such that $f(x) = (x - r_1) \cdot (x - r_n)$.

Consider the Vandermonde matrix

$$M = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ r_1 & r_2 & \cdots & r_n \\ r_1^2 & r_2^2 & \cdots & r_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ r_1^{n-1} & r_2^{n-1} & \cdots & r_n^{n-1} \end{bmatrix}.$$

Then, $\operatorname{disc}_{\mathbb{K}}(f(x)) = (\det(M))^2 = \det(MM^{\mathsf{T}})$. As before, let $\sigma_1, \ldots, \sigma_n \in R[u_1, \ldots, u_n]$ be the elementary symmetric polynomials. Put

$$s_i := \sigma_i(r_1, \ldots, r_n).$$

Then, note that

$$f(x) = x^n - s_1 x^{n-1} + \cdots + (-1)^n s_n$$

and hence, $s_i \in \mathbb{F}$ for all $i = 1, \ldots, n$. Also, define

$$v_k := r_1^k + \cdots + r_n^k$$

for all $k \geq 1$. In view of Newton's Identities, we see that each $v_k \in \mathbb{F}$ as well. Moreover, note that

$$MM^{\mathsf{T}} = \begin{bmatrix} n & v_1 & \cdots & v_{n-1} \\ v_1 & v_2 & \cdots & v_n \\ v_2 & v_3 & \cdots & v_{n+1} \\ \vdots & \vdots & \ddots & \vdots \\ v_{n-1} & v_n & \cdots & v_{2n-2} \end{bmatrix}.$$

Thus, $\operatorname{disc}_{\mathbb{K}}(f(x)) = \det(MM^{\mathsf{T}}) \in \mathbb{F}$.

Note that since v_k can be calculated directly in terms of s_i, which are coefficients of $\mathbb{F}$. Thus, the discriminant does not depend on the choice of the splitting field. □

Proposition 2.15 (Discriminant in terms of derivative)**.** Suppose $f(x) = \prod_{i=1}^n (x - r_i)$. Then, $\operatorname{disc}(f(x)) = (-1)^{\binom{n}{2}} \prod_{i=1}^n f'(r_i)$. [↓]

[↑]

Proof. Note that

$$f'(x) = \sum_{i=1}^n \frac{f(x)}{x - r_i} = \sum_{i=1}^n \prod_{\substack{j=1 \\ j \neq i}}^n (x - r_j)$$

and thus,

$$f'(r_i) = \prod_{\substack{j=1 \\ j\neq i}}^{n} (r_i - r_j).$$

The result now follows. □

Lemma 2.18.

1. Every real polynomial of odd degree has a real root.
2. Every complex number has a square root. Thus, every complex quadratic polynomial has a root in $\mathbb{C}$. [↓]

[↑]

Proof. The first follows from intermediate value property. For the second, given $a + b\iota \in \mathbb{C}$ with $a, b \in \mathbb{R}$, define $c, d \in \mathbb{R}$ by

$$c := \sqrt{\frac{1}{2}[a + \sqrt{a^2 + b^2}]} \quad \text{and} \quad d := \sqrt{\frac{1}{2}[-a + \sqrt{a^2 + b^2}]}.$$

Then, $(c + d\iota)^2 = z$. □

Theorem 2.19 (Fundamental Theorem of Algebra)**.** Every non-constant complex polynomial has a root in $\mathbb{C}$. [↓]

[↑]

Proof. Let $g(x) \in \mathbb{C}[x]$ be a non-constant polynomial. Then, $f(x) = g(x)\bar{g}(x)$ is a non-constant polynomial with real coefficients. Here, $\bar{g}(x)$ denotes the polynomial whose coefficients are complex conjugates of those of $g(x)$. Note that if $f(z) = 0$ for some $z \in \mathbb{C}$, then $g(z) = 0$ or $\bar{g}(z) = 0$. If $\bar{g}(z) = 0$, then $g(\bar{z}) = 0$. In either case, g has a complex root.

Thus, it suffices to show that all non-constant real polynomials have a root in $\mathbb{C}$. Given any $f(x) \in \mathbb{R}[x]$, we can write $\deg(f) = 2^n q$ for unique $n \geq 0$ and odd $q \in \mathbb{N}$.

We prove the statement by induction on n. If $n = 0$, then f has odd degree and hence, has a real root.
Suppose $n \geq 1$ and the statement is true for $n - 1$. Let $d := \deg(f)$ and $\mathbb{K} = \mathbb{C}(\alpha_1, \ldots, \alpha_d)$ be a splitting field of $f(x)$ over $\mathbb{C}$, where the α_i are the roots of $f(x)$. For $r \in \mathbb{R}$, define

$$y_{ij}(r) = \alpha_i + \alpha_j + r\alpha_i\alpha_j$$

for $1 \leq i \leq j \leq d$. There are $\binom{d+1}{2}$ such pairs (i, j). Hence, the polynomial

$$h_r(x) := \prod_{1 \leq i \leq j \leq d} (x - y_{ij}(r))$$

has degree

$$\deg(h(x)) = \binom{d+1}{2} = \frac{d}{2}(d+1) = 2^{n-1} \underbrace{q(d+1)}_{\text{odd}}.$$

Note that the coefficients of $h_r(x)$ are elementary symmetric polynomials in y_{ij}s. Thus, they are symmetric polynomials in $\alpha_i, \ldots, \alpha_d$. Hence, they are polynomials in the coefficients of $f(x)$. Thus, $h(x) \in \mathbb{R}[x]$. By inductive hypothesis (on n), we see that $h_r(x)$ has a root $z_r \in \mathbb{C} \subset \mathbb{K}$. Thus, $z_r = y_{i(r)j(r)}(r)$ for some pair $(i(r), j(r))$ with $1 \leq i(r) \leq j(r) \leq d$.

Let $P = \{(i, j) : 1 \leq i \leq j \leq d\}$ and define $\varphi : \mathbb{R} \to P$ by $r \mapsto (i(r), j(r))$. Since P is finite and $\mathbb{R}$ is not, φ is not one-one and thus, there exist $c \neq d \in \mathbb{R}$ with

$$(i(c), j(c)) = (i(d), j(d)) =: (a, b) \in P.$$

Thus,

$$z_c = \alpha_a + \alpha_b + c\alpha_a\alpha_b = z_d = \alpha_a + \alpha_b + d\alpha_a\alpha_b.$$

Note that a priori, we only know that $\alpha_a, \alpha_b \in \mathbb{K}$. But note that

$$\alpha_a\alpha_b = \frac{z_c - z_d}{d - c} \in \mathbb{C}$$

and consequently,

$$\alpha_a + \alpha_b = z_c - c\alpha_a\alpha_b \in \mathbb{C}.$$

Thus, $\alpha_a\alpha_b$ and $\alpha_a + \alpha_b \in \mathbb{C}$. However, these are roots of the quadratic

$$x^2 - (\alpha_a + \alpha_b)x + \alpha_a\alpha_b \in \mathbb{C}[x].$$

Thus, $\alpha_a \in \mathbb{C}$. But α_a was a root of $f(x)$, as desired. □

Proposition 3.4. Let $\mathbb{F} \subset \mathbb{K}$ be an extension where $\mathbb{K}$ is algebraically closed. Define,

$$\mathbb{A} := \{\alpha \in \mathbb{K} : \alpha \text{ is algebraic over } \mathbb{F}\}.$$

Then, $\mathbb{A}$ is an algebraic closure of $\mathbb{F}$. [↓]

[↑]

Proof. By Corollary 1.25, we already know that $\mathbb{A}/\mathbb{F}$ is actually an algebraic extension. We just need to show that $\mathbb{A}$ is algebraically closed. To this end, let $f(x) \in \mathbb{A}[x]$ be non-constant. Then, $f(x)$ has a root $\alpha \in \mathbb{K}$. But then, α is algebraic over $\mathbb{A}$ and hence, over $\mathbb{F}$. (Corollary 1.24.) Thus, $\alpha \in \mathbb{A}$. □

Lemma 3.5. Let $\{\mathbb{F}_i\}_{i\geq 1}$ be a sequence of fields as

$$\mathbb{F}_1 \subset \mathbb{F}_2 \subset \cdots .$$

Then, $\mathbb{F} := \bigcup_{i\geq 1} \mathbb{F}_i$ is a field with the following operations: Given $a, b \in \mathbb{F}$, there exist smallest $i, j \in \mathbb{N}$ with $a \in \mathbb{F}_i$ and $b \in \mathbb{F}_j$. Then, $a, b \in \mathbb{F}_{i+j}$. Define $a + b$ and ab to be the corresponding elements from $\mathbb{F}_{i+j}$.

Moreover, each $\mathbb{F}_i$ is a subfield of $\mathbb{F}$. [↓]

[↑]

Proof. The operations are clearly well-defined. It is easy to see that the desired commutative and associative laws hold since they hold in each $\mathbb{F}_i$. The 0 and 1 are those of each $\mathbb{F}_i$. The appropriate inverses of any $a \in \mathbb{F}$ also exist in any $\mathbb{F}_i$ containing a. The last sentence is also easy to check. □

Theorem 3.6 (Existence of Algebraic Closed Extension)**.** Let $\mathbb{F}$ be a field. Then, there exists an algebraically closed field containing $\mathbb{F}$. [↓]

[↑]

Proof. We first show that given any field $\mathbb{F}$, we can create a field $\mathbb{F}_1 \supset \mathbb{F}$ containing roots of any non-constant polynomial in $\mathbb{F}[x]$. Let S be a set of indeterminates which are in one-to-one correspondence with set of all polynomials in $\mathbb{F}[x]$ with degree ≥ 1. Let $x_f \in S$ denote the indeterminate corresponding to f.

Consider the (very large) polynomial ring $\mathbb{F}[S]$. Let

$$I = \langle f(x_f) : f \in \mathbb{F}[x],\ \deg(f) \geq 1 \rangle$$

be the ideal generated by the polynomials $f(x_f) \in \mathbb{F}[S]$. We contend that $1 \notin I$. Suppose the contrary. Then,

$$1 = g_1 f_1(x_{f_1}) + \cdots + g_n f_n(x_{f_n})$$

for some $g_1, \ldots, g_n \in \mathbb{F}[S]$. Note that these polynomials g_j only involve finitely many variables. Let $x_i := x_{f_i}$ for $i = 1, \ldots, n$ and let $x_{n+1}, \ldots, x_m$ be the remaining variables in $g_1, \ldots, g_n$. Then, we have

$$\sum_{i=1}^{n} g_i(x_1, \ldots, x_n, x_{n+1}, \ldots, x_m) f_i(x_i) = 1.$$

Now, let $\mathbb{E} \supset \mathbb{F}$ be an extension containing roots α_i of f_i. (Note that $\deg(f_i) \geq 1$ and thus, we may use Theorem 1.34.) Then, putting $x_i = \alpha_i$ for $i = 1, \ldots, n$ and putting $x_{n+1} = \cdots = x_m = 0$ in the above equation gives a contradiction.

Thus, $1 \notin I$ and hence, I is a proper ideal of $\mathbb{F}[S]$. Thus, it is contained in some maximal ideal $\mathfrak{m} \subset \mathbb{F}[S]$. Put $\mathbb{F}_1 := \mathbb{F}[S]/\mathfrak{m}$. Then, $\mathbb{F}_1$ is a field extension of $\mathbb{F}$.
Note that $\overline{x_f} = x_f + \mathfrak{m} \in \mathbb{F}_1$ is a root of $f(x) \in \mathbb{F}[x]$. Thus, we have constructed a field $\mathbb{F}_1$ in which every non-constant polynomial of $\mathbb{F}[x]$ has a root.

Repeating the procedure, we get fields

$$\mathbb{F} = \mathbb{F}_0 \subset \mathbb{F}_1 \subset \mathbb{F}_2 \subset \mathbb{F}_3 \subset \cdots$$

such that every non-constant polynomial in $\mathbb{F}_i$ has a root in $\mathbb{F}_{i+1}$.

Now, put $\mathbb{K} = \bigcup_{i \geq 0} \mathbb{F}_i$. This is a field as per Lemma 3.5, having each $\mathbb{F}_i$ as a subfield.

Now, if $f(x) \in \mathbb{K}[x]$, then $f(x) \in \mathbb{F}_n[x]$ for some n. This has a root in $\mathbb{F}_{n+1} \subset \mathbb{K}$, as desired. □

Corollary 3.7 (Existence of Algebraic Closure)**.** Every field $\mathbb{F}$ has an algebraic closure. [↓]

[↑]

Proof. Let $\mathbb{L} \supset \mathbb{F}$ be algebraically closed. (Existence given by Theorem 3.6.) Define

$$\mathbb{K} := \{\alpha \in \mathbb{L} : \alpha \text{ is algebraic over } \mathbb{K}\}.$$

By Proposition 3.4, $\mathbb{K}$ is an algebraic closure of $\mathbb{F}$. □

Proposition 3.8. Let $\sigma : \mathbb{F} \to \mathbb{L}$ be an embedding of fields where $\mathbb{L}$ is algebraically closed.
Let $\alpha \in \mathbb{K} \supset \mathbb{F}$ be algebraic over $\mathbb{F}$ and $p(x) = \operatorname{irr}(\alpha, \mathbb{F})$.
Write $p(x) = \sum a_i x^i$ and define $p^\sigma(x) := \sum \sigma(a_i) x^i$. Then, $\tau \mapsto \tau(\alpha)$ is a bijection between the sets

$$\{\tau : \mathbb{F}(\alpha) \to \mathbb{L} \mid \tau \text{ is an embedding and } \tau|_{\mathbb{F}} = \sigma\} \leftrightarrow \{\beta \in L \mid p^\sigma(\beta) = 0\}.$$

[↓]

[↑]

Proof. First, we note that the map is indeed well-defined. Let τ be an embedding extending σ. Then,

$$\tau(p(\alpha)) = p^\sigma(\tau(\alpha)) = 0$$

and thus, $\tau(\alpha)$ is indeed a root of p^σ.

Now, let $\beta \in L$ be such that $p^\sigma(\beta) = 0$. Define $\tau_\beta : \mathbb{F}(\alpha) \to \mathbb{L}$ by $\tau_\beta(f(\alpha)) = f^\sigma(\beta)$ for $f(x) \in \mathbb{F}[x]$.[2] We now show that τ_β is well-defined.

Suppose $f(\alpha) = g(\alpha)$. Then, $p(x) \mid f(x) - g(x)$ and hence, $p^\sigma(x) \mid f^\sigma(x) - g^\sigma(x)$. Thus, $f^\sigma(\beta) = g^\sigma(\beta)$. Thus, τ_β is well-defined. It is clearly a homomorphism (and hence, an embedding). Moreover, it extends σ.

It is now easily seen that $\beta \mapsto \tau_\beta$ is a two-sided inverse of the map $\tau \mapsto \tau(\alpha)$. □

Theorem 3.10. Let $\sigma : \mathbb{F} \to \mathbb{L}$ be an embedding where $\mathbb{L}$ is algebraically closed. Let $\mathbb{K}/\mathbb{F}$ be an algebraic extension. Then, there exists an embedding $\tau : \mathbb{K} \to \mathbb{L}$ extending σ.
Moreover, if $\mathbb{K}$ is an algebraic closure of $\mathbb{F}$ and $\mathbb{L}$ of $\sigma(\mathbb{K})$, then τ is an isomorphism extending σ. [↓]

[↑]

Proof. Consider the set

$$\Sigma := \{(\mathbb{E}, \tau) \mid \mathbb{F} \subset \mathbb{E} \subset \mathbb{K} \text{ are fields and } \tau : \mathbb{E} \to \mathbb{L} \text{ such that } \tau|_{\mathbb{F}} = \sigma\}.$$

Note that $\Sigma \neq \varnothing$ since $(\mathbb{F}, \sigma) \in \Sigma$. Define the relation $\leq$ on Σ by

$$(\mathbb{E}, \tau) \leq (\mathbb{E}', \tau') \iff \mathbb{E} \subset \mathbb{E}' \text{ and } \tau'|_{\mathbb{E}} = \tau.$$

Then, $(\Sigma, \leq)$ is a partially ordered set. Moreover, if $\Lambda = \{(\mathbb{E}_\alpha, \tau_\alpha)\}_{\alpha \in I}$ is a chain in Σ, then $\mathbb{E} := \bigcup_{\alpha \in I} \mathbb{F}_\alpha$ is a subfield of $\mathbb{E}$ and $\tau : \mathbb{E} \to \mathbb{L}$ defined as $\tau(x) := \tau_\alpha(x)$ for $x \in \mathbb{F}_\alpha$ is well-defined. (The proof is similar to that of Lemma 3.5.) Moreover, $(\mathbb{E}, \tau)$ is an upper bound of Λ.

Thus, by Zorn's lemma, there exists a maximal element $(\mathbb{E}, \tau) \in \Sigma$. We contend that $\mathbb{E} = \mathbb{K}$. If not, then pick $\alpha \in \mathbb{K} \setminus \mathbb{E}$. By Proposition 3.8, we can extend τ to an embedding $\tau' : \mathbb{E}(\alpha) \to \mathbb{L}$. But this contradicts maximality of $(\mathbb{E}, \tau)$.

Now, suppose that $\mathbb{K}$ is an algebraic closure of $\mathbb{F}$ and $\mathbb{L}$ of $\sigma(\mathbb{F})$. We have

$$\sigma(\mathbb{F}) \subset \tau(\mathbb{K}) \subset \mathbb{L}$$

and thus, $L/\tau(\mathbb{K})$ is also algebraic. But $\tau(\mathbb{K})$ is also algebraically closed and thus, $\mathbb{L} = \tau(\mathbb{K})$. □

Theorem 3.13 (Isomorphism of splitting fields)**.** Let $\mathbb{E}$ and $\mathbb{E}'$ be two splitting fields of a non-constant polynomial $f(x) \in \mathbb{F}[x]$ over $\mathbb{F}$. Then, they are $\mathbb{F}$-isomorphic. [↓]

[2] Note that elements of $\mathbb{F}(\alpha)$ are precisely polynomials in α.

[↑]

Proof. Let $\overline{\mathbb{E}}$ be an algebraic closure of $\mathbb{E}$. Then, it is also one of $\mathbb{F}$. Thus, there exists an embedding $\tau : \mathbb{E}' \to \overline{\mathbb{E}}$ extending the inclusion $i : \mathbb{F} \hookrightarrow \overline{\mathbb{E}}$.

Let $f(x) = a(x - \alpha_1) \cdots (x - \alpha_n)$ be a factorisation of $f(x)$ in $\mathbb{E}'[x]$. Then,

$$f^\tau(x) = (x - \tau(\alpha_1)) \cdots (x - \tau(\alpha_n)) \in \overline{\mathbb{E}}[x].$$

Note that we have $\mathbb{E}' = \mathbb{F}(\alpha_1, \ldots, \alpha_n)$ and so, $\tau(\mathbb{E}') = \mathbb{F}(\tau(\alpha_1), \ldots, \tau(\alpha_n))$. Thus, $\tau(\mathbb{E}')$ is a splitting field of f^τ. But $f^\tau = f$ since $f(x) \in \mathbb{F}[x]$ and τ extends the inclusion map. Thus, $\tau(\mathbb{E}') = \mathbb{E}$, since any algebraic closure contains a unique splitting field. □

Proposition 4.7. The number of roots and their multiplicities are independent of the splitting field chosen for $f(x)$ over $\mathbb{F}$. [↓]

[↑]

Proof. Let $\mathbb{E}$ and $\mathbb{K}$ be splitting fields for $f(x)$ over $\mathbb{F}$. By Theorem 3.13, there exists an $\mathbb{F}$-isomorphism $\tau : \mathbb{E} \to \mathbb{K}$. In turn, we get an isomorphism

$$\begin{aligned} \varphi_\tau : \mathbb{E}[x] &\to \mathbb{K}[x] \\ \sum a_i x^i &\mapsto \sum \tau(a_i) x^i. \end{aligned}$$

Now, let $f(x) = \prod_{i=1}^{g} (x - r_i)^{e_i}$ be the unique factorisation of $f(x)$ in $\mathbb{E}[x]$. The above isomorphism shows that

$$f(x) = \prod_{i=1}^{g} (x - \tau(r_i))^{e_i}$$

is the unique factorisation of $f(x)$ in $\mathbb{K}[x]$. The result follows. □

Proposition 4.8. Let $f(x) \in \mathbb{F}[x]$ be a monic and let $r \in \mathbb{E} \supset \mathbb{F}$ be a root of $f(x)$. Then, r is a repeated root iff $f'(r) = 0$. [↓]

[↑]

Proof. ($\Rightarrow$) If r is a repeated root, then write $f(x) = (x - r)^2 g(x)$ for $g \in \mathbb{E}[x]$. Then, taking the derivative gives

$$f'(x) = 2(x - r)g(x) + (x - r)^2 g'(x).$$

Thus, $f'(r) = 0$.

($\Leftarrow$) Write $f(x) = (x - r)g(x)$. Then,

$$0 = f'(r) = (r - r)g'(r) + g(r) = g(r).$$

Thus, $(x - r) \mid g(x)$ and hence, $(x - r)^2 \mid f(x)$. □

Theorem 4.9 (The Derivative Criterion for Separability)**.** Let $f(x) \in \mathbb{F}[x]$ be a monic polynomial.

1. If $f'(x) = 0$, then every root of $f(x)$ is a multiple root.
2. If $f'(x) \neq 0$, then $f(x)$ has simple roots iff $\gcd(f(x), f'(x)) = 1$. [↓]

[↑]

Proof. Let $\mathbb{E}$ be a splitting field of $f(x)$.

1. Let $r \in \mathbb{E}$ be a root of $f(x)$. Then, $f'(r) = 0$, by hypothesis and thus, r is a repeated root, by Proposition 4.8.
2. Suppose $f'(x) \neq 0$.
   ($\Rightarrow$) Suppose $f(x)$ has simple roots. We need to show that $f(x)$ and $f'(x)$ have no common root. Let r be a root of $f(x)$. Then $f'(r) \neq 0$, by Proposition 4.8.

   ($\Leftarrow$) Suppose $\gcd(f(x), f'(x)) = 1$ and $r \in \mathbb{E}$ is an arbitrary root of $f(x)$. Then, $f'(r) \neq 0$. Thus, r is a simple root. □

Proposition 4.10. Let $f(x) \in \mathbb{F}[x]$ be irreducible and non-constant.

1. $f(x)$ is separable iff $f'(x) \neq 0$.
2. If $\mathrm{char}(\mathbb{F}) = 0$, then $f(x)$ is separable.

In other words, irreducible polynomials over fields of characteristic 0 are separable. [↓]

[↑]

Proof. Let $\mathbb{E}$ be a splitting field of $f(x)$ over $\mathbb{F}$.

1. ($\Rightarrow$) $f(x)$ has no repeated roots and thus, $f'(x) \neq 0$, by Proposition 4.10.

   ($\Leftarrow$) Suppose $f'(x) \neq 0$ and $f(x)$ has a repeated root $r \in \mathbb{E}$. Then, by Proposition 4.8, $f'(r) = 0$. Thus, $g(x) := \gcd(f(x), f'(x)) \neq 1$. Irreducibility of $g(x)$ forces $f(x) = g(x)$. But then, $f(x) \mid f'(x)$, which is a contradiction since $\deg(f'(x)) < \deg(f(x))$.
2. If $f(x)$ is non-constant, then $f'(x) \neq 0$. The previous part applies.

□

Proposition 4.14. Let $\mathbb{F}$ be a field with $\mathrm{char}(\mathbb{F}) = p > 0$. Then, $x^p - a \in \mathbb{F}[x]$ is either irreducible in $\mathbb{F}[x]$ or $a \in \mathbb{F}^p$. [↓]

[↑]

Proof. Suppose $f(x)$ is not irreducible. Write $f(x) = g(x)h(x)$ with $1 \leq \deg(g(x)) =: m < p$. Let $b \in \mathbb{E}$ be a root in a splitting field $\mathbb{E}$ of $f(x)$ over $\mathbb{F}$. Then, $b^p = a$. Thus, $f(x)$ factorises in $\mathbb{E}[x]$ as

$$f(x) = x^p - b^p = (x - b)^p.$$

Since $\mathbb{E}[x]$ is a UFD, we see that $g(x) = (x - b)^m$. (We may assume that $g(x)$ is monic.) However, note that the coefficient of x^{m-1} is mb. By assumption, $mb \in \mathbb{F}$. Since $1 \leq m < p$, we see that $b \in \mathbb{F}$. Thus, $a = b^p \in \mathbb{F}^p$. □

Proposition 4.15. Let $f(x) \in \mathbb{F}[x]$ be an irreducible polynomial and let $p := \mathrm{char}(\mathbb{F}) > 0$. If $f(x)$ is not separable, then there exists $g(x) \in \mathbb{F}[x]$ such that $f(x) = g(x^p)$. [↓]

[↑]

Proof. Since $f(x)$ is irreducible and not separable, we must have $f'(x) = 0$. Write

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n$$

and note that

$$0 = f'(x) = a_1 + 2a_2 x + \cdots + n a_n x^{n-1}.$$

Thus, $k a_k = 0$ for all $k = 1, \ldots, n$. If $\gcd(k, p) = 1$, then we may cancel k to see that $a_k = 0$ whenever $p \nmid k$. Thus, $f(x)$ is of the form

$$f(x) = a_0 + a_p x^p + \cdots + a_{mp} x^{mp}$$

for some $m \in \mathbb{N}$. Thus, $g(x) = a_0 + a_p x + \cdots + a_{mp} x^m$ works. □

Theorem 4.18. Let $\mathbb{F}$ be a field with characteristic $p > 0$. Then, $\mathbb{F}$ is perfect iff $\mathbb{F} = \mathbb{F}^p$. [↓]

[↑]

Proof. ($\Rightarrow$) Suppose $\mathbb{F} \neq \mathbb{F}^p$. Pick $\alpha \in \mathbb{F} \setminus \mathbb{F}^p$. Then, $x^p - \alpha$ is irreducible (by Proposition 4.14) but not separable, by Proposition 4.10.

($\Leftarrow$) Suppose $\mathbb{F} = \mathbb{F}^p$ and $f(x) \in \mathbb{F}[x]$ is irreducible and not separable. By Proposition 4.15, we can write

$$f(x) = \sum_{i=0}^{m} a_i x^{ip}.$$

Let $b_i \in \mathbb{F}$ be such that $a_i = b_i^p$. Then,

$$f(x) = \sum_{i=0}^{m} a_i x^{ip} = \sum_{i=0}^{m} b_i^p x^{ip} = \left(\underbrace{\sum_{i=0}^{m} b_i x^i}_{\in \mathbb{F}[x]} \right)^p,$$

contradicting the irreducibility of $f(x)$ in $\mathbb{F}[x]$. □

Corollary 4.19. Every finite field is perfect. [↓] [↑]

Proof. Let $\mathbb{F}$ be a finite field of characteristic $p > 0$. We show that $\mathbb{F} = \mathbb{F}^p$.

Note that $|\mathbb{F}| = p^n$ for some $n \in \mathbb{N}$. Thus, by Lagrange's theorem from group theory, we see that $\alpha^{p^n - 1} = 1$ for all $\alpha \in \mathbb{F}^\times$. Thus, $\alpha^{p^n} = \alpha$ for all $\alpha \in \mathbb{F}$. (This holds for $\alpha = 0$ as well.)

Thus, given any arbitrary $\alpha \in \mathbb{F}$, put $\beta = \alpha^{p^{n-1}}$ to get $\alpha = \beta^p \in \mathbb{F}^p$. □

Proposition 4.20. Let $f(x) \in \mathbb{F}[x]$ be an irreducible monic polynomial. Then, all roots of $f(x)$ have equal multiplicity (in any splitting field).
If $\mathrm{char}(\mathbb{F}) = 0$, then all roots are simple.
If $\mathrm{char}(\mathbb{F}) =: p > 0$, then all roots have multiplicity p^n for some $n \in \mathbb{N}_0$. [↓] [↑]

Proof. Let $\overline{\mathbb{F}} \supset \mathbb{F}$ be an algebraic closure of $\mathbb{F}$. Let $\alpha, \beta \in \overline{\mathbb{F}}$ be roots of f. We have an $\mathbb{F}$-isomorphism $\sigma : \mathbb{F}(\alpha) \to \mathbb{F}(\beta)$ determined by $\alpha \mapsto \beta$.

Thus, σ can be extended to an automorphism τ of $\overline{\mathbb{F}}$. Then, write $f(x) = (x-\alpha)^m h(x)$ where m is the multiplicity of α and $h(x) \in \overline{\mathbb{F}}[x]$. Applying τ, we get

$$f(x) = f^\tau(x) = (x - \beta)^m h^\tau(x).$$

Thus, the multiplicity of β is at least m. By symmetry, we have equality.

If $\mathrm{char}(\mathbb{F}) = 0$, then $f(x)$ is separable (Theorem 4.9) and thus, all roots are simple.

Now, assume that $\mathrm{char}(\mathbb{F}) =: p > 0$. Let $n \in \mathbb{N}_0$ be the largest such that there exists a polynomial $g(x) \in \mathbb{F}[x]$ with $f(x) = g(x^{p^n})$. (Note that we can take $g = f$ and $n = 0$ if no positive n exists.)

Then, g is irreducible since f is so. Moreover, g must be separable. Indeed, if not, then we can write $g(x) = h(x^p)$ for some $h(x) \in \mathbb{F}[x]$, by Proposition 4.10. Then, $f(x) = g(x^{p^{n+1}})$ contradicting maximality of n.

Thus, $g(x)$ factors in $\overline{\mathbb{F}}$ as $g(x) = (x - r_1) \cdots (x - r_g)$ for distinct r_g. Since $\overline{\mathbb{F}}$ is algebraically closed, we can find $s_1, \ldots, s_g$ necessarily distinct such that $s_i^{p^n} = r_i$. Then, we have

$$f(x) = g(x^{p^n}) = (x - s_1)^{p^n} \cdots (x - s_g)^{p^n},$$

as desired. □

Theorem 4.21. Let $\sigma : \mathbb{F} \to \mathbb{L}$ be an embedding of fields where $\mathbb{L}$ is an algebraic closure of $\sigma(\mathbb{F})$. Similarly, let $\tau : \mathbb{F} \to \mathbb{L}'$ be an embedding of fields where $\mathbb{L}'$ is an algebraic closure of $\tau(\mathbb{F})$. Let $\mathbb{E}$ be an algebraic extension of $\mathbb{F}$.

Let S_σ (resp. S_τ) denote the set of extensions of σ (resp. τ) to embeddings of $\mathbb{E}$ into $\mathbb{L}$ (resp. $\mathbb{L}'$). Let $\lambda : \mathbb{L} \to \mathbb{L}'$ be an isomorphism extending $\tau \circ \sigma^{-1} : \sigma(\mathbb{F}) \to \tau(\mathbb{F})$.

The map $\psi : S_\sigma \to S_\tau$ given by $\psi(\widetilde{\sigma}) = \lambda \circ \widetilde{\sigma}$ is a bijection. [↓]

[↑]

Proof. If $\widetilde{\sigma} \in S_\sigma$, then for any $x \in \mathbb{F}$, we have

$$(\lambda \circ \widetilde{\sigma})(x) = \lambda(\sigma(x)) = (\tau \circ \sigma^{-1})(\sigma(x)) = \tau(x).$$

Thus, ψ actually maps into S_τ. Since λ is an isomorphism, ψ is easily seen to be a bijection. Explicitly, the inverse of ψ can be seen to be $\widetilde{\tau} \mapsto \lambda^{-1} \circ \tau$. □

Theorem 4.26 (Tower Law for separable degree)**.** Let $\mathbb{F} \subset \mathbb{E} \subset \mathbb{K}$ be a tower of finite algebraic extensions. Then, $[\mathbb{E} : \mathbb{F}]_s \leq [\mathbb{E} : \mathbb{F}]$ and

$$[\mathbb{K} : \mathbb{F}]_s = [\mathbb{K} : \mathbb{E}]_s [\mathbb{E} : \mathbb{F}]_s.$$

[↓]

[↑]

Proof. First, we show that the separable degree is multiplicative. Let $n := [\mathbb{K} : \mathbb{E}]_s$ and $m := [\mathbb{E} : \mathbb{F}]_s$ and $\sigma : \mathbb{F} \to \mathbb{L}$ be an embedding into an algebraically closed field $\mathbb{L}$.

Let $\sigma_1, \ldots, \sigma_m : \mathbb{E} \to \mathbb{L}$ be extensions of $\mathbb{F}$. Then, each σ_i has extensions $\sigma_i^{(1)}, \ldots, \sigma_i^{(n)} : \mathbb{K} \to \mathbb{L}$. Note that $\{\sigma_i^{(j)} : 1 \leq i \leq m,\ 1 \leq j \leq n\}$ has cardinality mn. (All the extensions obtained are distinct.)

Clearly, any embedding $\tau : \mathbb{K} \to \mathbb{L}$ extending τ is obtained this way. ($\tau|_{\mathbb{E}}$ is σ_i for some i and thus, $\tau = \sigma_i^{(j)}$ for some j.)

Thus, $[\mathbb{K} : \mathbb{F}]_s = mn$, as desired.

Now, since $\mathbb{E}/\mathbb{F}$ is finite, we can construct $\alpha_1, \ldots, \alpha_g$ such that $\mathbb{E} = \mathbb{F}(\alpha_1, \ldots, \alpha_g)$. We have the chain

$$\mathbb{F} \subset \mathbb{F}(\alpha_1) \subset \mathbb{F}(\alpha_1, \alpha_2) \subset \cdots \subset \mathbb{F}(\alpha_1, \ldots, \alpha_n).$$

Note that by Proposition 4.25, we know that

$$[\mathbb{F}(\alpha_1, \ldots, \alpha_{i+1}) : \mathbb{F}(\alpha_1, \ldots, \alpha_i)]_s \leq [\mathbb{F}(\alpha_1, \ldots, \alpha_{i+1}) : \mathbb{F}(\alpha_1, \ldots, \alpha_i)]$$

for all $i = 0, \ldots, n-1$. Since both degrees are multiplicative, we are done. □

Theorem 4.28. Let $\mathbb{E}/\mathbb{F}$ be a finite extension. Then, $\mathbb{E}/\mathbb{F}$ is separable iff $[\mathbb{E} : \mathbb{F}]_s = [\mathbb{E} : \mathbb{F}]$. [↓]

[↑]

Proof. Write $\mathbb{E} = \mathbb{F}(\alpha_1, \ldots, \alpha_n)$ for $\alpha_i \in \mathbb{E}$. (Note that $\mathbb{E}/\mathbb{F}$ is a finite extension.)

Put

$$\mathbb{F}_0 := \mathbb{F} \quad \text{and} \quad \mathbb{F}_i := \mathbb{F}(\alpha_1, \ldots, \alpha_i),$$

for $i = 1, \ldots, n$.

($\Rightarrow$) Assume $\mathbb{E}/\mathbb{F}$ is separable. Then, since each α_i is separable over $\mathbb{F}$, it follows that α_i is separable over $\mathbb{F}$ for $i = 1, \ldots, n$. (Note that $\operatorname{irr}(\alpha, \mathbb{F}_i) \mid \operatorname{irr}(\alpha, \mathbb{F})$.) Thus, we see that

$$[\mathbb{F}_i : \mathbb{F}_{i-1}]_s = [\mathbb{F}_i : \mathbb{F}_{i-1}]$$

for all $i = 1, \ldots, n$. Multiplying gives $[\mathbb{E} : \mathbb{F}]_s = [\mathbb{E} : \mathbb{F}]$.

($\Leftarrow$) Let $\alpha \in \mathbb{E}$ be arbitrary. Consider the tower

$$\mathbb{F} \subset \mathbb{F}(\alpha) \subset \mathbb{E}.$$

Since, we have the equality $[\mathbb{E} : \mathbb{F}]_s = [\mathbb{E} : \mathbb{F}]$, we also have the equality $[\mathbb{F}(\alpha) : \mathbb{F}]_s = [\mathbb{F}(\alpha) : \mathbb{F}]$, by the previous corollary. Thus, α is separable over $\mathbb{F}$, by Proposition 4.25. □

Proposition 4.30. Let $\mathbb{F} \subset \mathbb{E} \subset \mathbb{K}$ be a tower of fields. Then, $\mathbb{K}/\mathbb{F}$ is separable iff $\mathbb{K}/\mathbb{E}$ and $\mathbb{E}/\mathbb{F}$ are separable. [↓]

[↑]

Proof. For both parts, we first note that if $\alpha \in \mathbb{K}$ is algebraic over $\mathbb{F}$, then it is also algebraic over $\mathbb{E}$. Moreover, $\mathrm{irr}(\alpha, \mathbb{E}) \mid \mathrm{irr}(\alpha, \mathbb{F})$. (The divisibility is in $\mathbb{E}[x]$.)

($\Rightarrow$) Let $\alpha \in \mathbb{K}$ be arbitrary. Then, α is algebraic over $\mathbb{F}$ and hence, over $\mathbb{E}$. Since $\mathrm{irr}(\alpha, \mathbb{F})$ has no repeated roots, neither does its factor $\mathrm{irr}(\alpha, \mathbb{E})$. Thus, $\mathbb{K}/\mathbb{E}$ is separable.
Now, let $\beta \in \mathbb{E}$ be arbitrary. Then, $\beta \in \mathbb{K}$ and thus, $\mathrm{irr}(\alpha, \mathbb{F})$ is separable. Thus, $\mathbb{E}/\mathbb{F}$ is separable.

($\Leftarrow$) Let $\alpha \in \mathbb{K}$ be arbitrary. Note that α is algebraic over $\mathbb{E}$, since it is separable over $\mathbb{E}$. Let $\mathrm{irr}(\alpha, \mathbb{E}) = a_1 + \cdots + a_n x^{n-1} + x^n \in \mathbb{E}[x]$.

Put

$$\mathbb{F}_0 := \mathbb{F} \quad \text{and} \quad \mathbb{F}_i := \mathbb{F}(a_1, \ldots, a_i),$$

for $i = 1, \ldots, n$. By ($\Rightarrow$) , we see that a_i is separable over $\mathbb{F}_{i-1}$ and hence,

$$[\mathbb{F}_i : \mathbb{F}_{i-1}]_s = [\mathbb{F}_i : \mathbb{F}_{i-1}] \qquad (*)$$

for all $i = 1, \ldots, n$.

Finally, put $\mathbb{F}_{n+1} := \mathbb{F}_n(\alpha)$. Then, ($*$) holds for $i = n + 1$ as well, since α is separable over $\mathbb{F}_n$. (Note that $\mathrm{irr}(\alpha, \mathbb{F}_n) = \mathrm{irr}(\alpha, \mathbb{E})$, by our construction and the latter is separable by assumption.)

Thus, upon multiplying, we get $[\mathbb{F}_{n+1} : \mathbb{F}]_s = [\mathbb{F}_{n+1} : \mathbb{F}]$ and hence, $\mathbb{F}_{n+1}/\mathbb{F}$ is separable. Since $\alpha \in \mathbb{F}_{n+1}$, we see that α is separable over $\mathbb{F}$ and hence, $\mathbb{K}/\mathbb{F}$ is separable. □

Proposition 4.31. Let $\mathbb{E}/\mathbb{F}$ be a finite extension. Then, $[\mathbb{E} : \mathbb{F}]_s$ divides $[\mathbb{E} : \mathbb{F}]$. If $\mathrm{char}(\mathbb{F}) =: p > 0$, then quotient $\dfrac{[\mathbb{E} : \mathbb{F}]}{[\mathbb{E} : \mathbb{F}]_s}$ is a power of p. [↓]

[↑]

Proof. Clearly the statement is true if $\mathrm{char}(\mathbb{F}) = 0$ since we have equality of degrees. Suppose $\mathrm{char}(\mathbb{F}) =: p > 0$.

First, suppose that $\mathbb{E} = \mathbb{F}(\alpha)$ for some $\alpha \in \mathbb{E}$. Let $p(x) := \mathrm{irr}(\alpha, \mathbb{F})$ and $d := \deg(p(x))$. By Proposition 4.20, $p(x)$ factors in $\overline{\mathbb{F}}[x]$ as

$$p(x) = (x - \alpha)^{p^n}(x - \alpha_2)^{p^n} \cdots (x - \alpha_g)^{p^n},$$

where $\alpha_2, \ldots, \alpha_g \in \overline{\mathbb{F}} \setminus \{\alpha\}$ are distinct. Note that we have $gp^n = d$. By Proposition 3.8, we know that $[\mathbb{F}(\alpha) : \mathbb{F}]_s = g$. Thus, the statement is true.

For a general finite extension $\mathbb{E}/\mathbb{F}$, write $\mathbb{E} = \mathbb{F}(\beta_1, \ldots, \beta_k)$ and use the fact that degrees are multiplicative. □

Theorem 4.32 (Uniqueness of finite fields)**.** Let $\mathbb{K}$ and $\mathbb{L}$ be finite fields with same cardinality. Then, $\mathbb{K}$ and $\mathbb{L}$ are isomorphic. [↓]

[↑]

Proof. Let $q := |\mathbb{K}|$ and $p := \mathrm{char}(\mathbb{K})$. Then, $q = p^n$ for some $n \in \mathbb{N}$. Note that $\mathbb{K}^\times$ is a group of order $q - 1$. By Lagrange's theorem, we have $a^{q-1} = 1$ for all $a \in \mathbb{K}^\times$. In turn, we get $a^q - a = 0$ for *all* $a \in \mathbb{K}$.

Hence, $\mathbb{K}$ is a splitting field of $x^q - x$ over $\mathbb{F}_p$ and so is $\mathbb{L}$. By Theorem 3.13, $\mathbb{K}$ and $\mathbb{L}$ are isomorphic. □

Theorem 4.35 (Existence of finite fields)**.** Fix a prime p and an algebraic closure $\overline{\mathbb{F}}_p$. For every $n \in \mathbb{N}$, there exists a unique subfield of $\overline{\mathbb{F}}_p$ of size p^n, denoted $\mathbb{F}_{p^n}$. Moreover

$$\overline{\mathbb{F}}_p = \bigcup_{n \in \mathbb{N}} \mathbb{F}_{p^n}.$$

[↓]

[↑]

Proof. Fix $n \in \mathbb{N}$ and let $q = p^n$. $\overline{\mathbb{F}}_p$ contains a unique splitting field of $x^q - x =: f(x)$ over $\mathbb{F}_p$. We show that this splitting field has q elements. Consider

$$\mathbb{K} = \{\alpha \in \overline{\mathbb{F}}_p \mid f(\alpha) = 0\}.$$

Then, $|\mathbb{K}| = q$ since $f(x)$ is separable, by Theorem 4.9.

Thus, $\mathbb{K}$ is the desired splitting field. Conversely any other field with q elements would be the set of roots of $x^q - x$ and hence, we have uniqueness.

We now show that $\overline{\mathbb{F}}_p = \bigcup_{k \geq 1} \mathbb{F}_{p^k}$. Let $\alpha \in \overline{\mathbb{F}}_p$ and let $d := \deg_{\mathbb{F}}(\alpha)$. Then, $[\mathbb{F}(\alpha) : \mathbb{F}] = d$ and hence, $\alpha \in \mathbb{F}(\alpha) = \mathbb{F}_{p^d}$. □