MA-414
Galois Theory

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

Last updated: June 20, 2021

Contents

Chapter 0

Preliminaries

§0.1. Notations and Conventions

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, $\mathbb{F}^\times = \mathbb{F} \setminus \{0\}$.
9. Given a ring R, $R^\times$ denotes the group of units of R.
10. Whenever we write "$F \subseteq E$ are fields," we mean that $\mathbb{E}$ is a field and $\mathbb{F}$ is a subfield of $\mathbb{E}$.
11. $\zeta_n := \exp\left(\dfrac{2\pi\iota}{n}\right)$.
12. The degree of the zero polynomial is $-\infty$.
13. Given a group G and $g \in G$, we denote the order of g (in G) as $o(g)$.
14. For $n \geq 1$, we denote $\{1, \ldots, n\}$ as $[n]$.

§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 $\operatorname{char} \mathbb{F}$.

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

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

Proof. Let $n := \operatorname{char} \mathbb{F}$ 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, $n = \operatorname{char} \mathbb{F} \leq a$. But $a \mid n \implies a \leq n$.

Thus, $a = n$. $\square$

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 $\operatorname{Frac}(\mathbb{Z}/\langle \operatorname{char} \mathbb{F} \rangle)$.

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 $n = \operatorname{char} \mathbb{F}$. 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] $\square$

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

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 $\operatorname{Frac}(\mathbb{Z}/\langle \operatorname{char}\mathbb{F}\rangle)$.
2. Let $\varphi : \mathbb{F} \to \mathbb{E}$ be a field homomorphism. Then, $\operatorname{char}\mathbb{F} = \operatorname{char}\mathbb{E}$ and φ is injective.
3. Let $\mathbb{F} \subseteq \mathbb{E}$ 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 $\mathbb{F} \subseteq \mathbb{E}_1, \mathbb{E}_2$, an $\mathbb{F}$-homomorphism from $\mathbb{E}_1$ to $\mathbb{E}_2$ is a field homomorphism $\varphi : \mathbb{E}_1 \to \mathbb{E}_2$ fixing $\mathbb{F}$. If φ is also an isomorphism, then it is called an $\mathbb{F}$-isomorphism.

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

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

Similarly, given a set $A \subseteq R$ (or $A \subseteq \mathbb{F}$), we can talk about $R[A]$ (or $\mathbb{F}(A)$) to be the smallest subring (or subfield) generated by A over R (or $\mathbb{F}$).

Proposition 0.15. Let $\mathbb{F} \subseteq \mathbb{E}$ be fields and $A \subseteq \mathbb{E}$ a set.

If $A = \varnothing$, then $\mathbb{F}(A) = \mathbb{F}$. Assume $A \neq \varnothing$.

Let

$$M := \{a_1 a_2 \cdots a_n \mid n \in \mathbb{N},\ a_1, \ldots, a_n \in A\}$$

be the set of all finite products (monomials) of elements of A.

Let

$$S := \{b_0 + b_1 m_1 + \cdots + b_n m_n \mid n \in \mathbb{N}_0,\ m_1, \ldots, m_n \in M,\ b_0, b_1, \ldots, b_n \in \mathbb{F}\}$$

be the set of all finite sums of elements of M. (These are polynomials in A with coefficients in $\mathbb{F}$.)

Then,

$$\mathbb{F}(A) = \left\{ \frac{s_1}{s_2} \mid s_1, s_2 \in S \text{ and } s_2 \neq 0 \right\}. \tag{0.1}$$

Proof. The case $A = \varnothing$ is trivial. Assume $A \neq \varnothing$.

Let the set on the right in (0.1) be called Q.

Note that M is closed under products and S is closed under sums and products both. Moreover, S contains $\mathbb{F}$ as the constant polynomials. Using this, it is clear that Q is a subfield of $\mathbb{E}$. By taking denominator 1, we also see that $S \subseteq Q$. Since $\mathbb{F} \subseteq S$ and $A \subseteq M \subseteq S$, we see that Q is a subfield of $\mathbb{E}$ containing A and $\mathbb{F}$. Thus, $\mathbb{F}(A) \subseteq Q$.

On the other hand, note that $M \subseteq \mathbb{F}(A)$ since $A \subseteq \mathbb{F}(A)$. Since $\mathbb{F} \subseteq \mathbb{F}(A)$ as well, we get $S \subseteq \mathbb{F}(A)$. Thus, $Q \subseteq \mathbb{F}(A)$. (In all the assertions, we have used that $\mathbb{F}(A)$ is a subfield of $\mathbb{E}$ and thus, has the required closure properties.) □

Corollary 0.16. Let $\mathbb{F} \subseteq \mathbb{E}$ be fields and $A \subseteq \mathbb{E}$ a set. If $a \in \mathbb{F}(A)$, then there exists a finite set $B \subseteq A$ such that $a \in \mathbb{F}(B)$.

Proof. Let $a \in F(A)$. Let M, S be as in Proposition 0.15. Then, $a = s_1/s_2$ for some $s_1, s_2 \in S$. Then, each s_i is a polynomial in some finitely many $a_i \in A$ with coefficients in $\mathbb{F}$. Let B be the set of those finitely many a_i. Then, $a \in \mathbb{F}(B)$. □

Proposition 0.17. If $\mathbb{F}$ is a finite field, then $\operatorname{char}(\mathbb{F}) =: p > 0$ and $|\mathbb{F}| = p^n$ for some $n \in \mathbb{N}$.

Proof. $\operatorname{char}(\mathbb{F}) = 0$ 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 $|\mathbb{F}| = |\mathbb{F}_p|^n = p^n$. $\square$

Theorem 0.18. 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 $ab = 0 \implies a = 0$ or $b = 0$, in a field. $\square$

Theorem 0.19. 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 $\operatorname{lcm}(m, n)$. (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

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

Thus, all n elements of $U \subseteq \mathbb{F}$ 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 $U = \langle a \rangle$. $\square$

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. $\square$

Proposition 0.20. Let $\mathbb{F} \subseteq \mathbb{K}$ be fields and $f(x), g(x) \in \mathbb{F}[x]$.
Then, $f(x) \mid g(x)$ in $\mathbb{F}[x]$ iff every root of $f(x) \mid g(x)$ in $\mathbb{K}[x]$.

In particular, if $f(x)$ factorises linearly into distinct factors in $\mathbb{K}[x]$, then it suffices to show that every root of $f(x)$ is also one of $g(x)$.

Proof. ($\Rightarrow$) This is obvious because a factorisation $g(x) = f(x)h(x)$ in $\mathbb{F}[x]$ also holds in $\mathbb{K}[x]$.

($\Leftarrow$) If $f(x) = 0$, then the result is true. Assume $f(x) \neq 0$.
By the division algorithm, we may write

$$g(x) = f(x)q(x) + r(x)$$

for unique $q(x), r(x) \in \mathbb{F}[x]$ with $\deg(r(x)) < \deg(q(x))$.

The above is also a division in $\mathbb{K}[x]$. But $f(x) \mid g(x)$ in $\mathbb{K}[x]$ and so, uniqueness forces $r(x) = 0$. $\square$

Chapter 1

Algebraic extensions

§1.1. Extensions and Degrees

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 $[\mathbb{K} : \mathbb{F}]$ 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 $\mathbb{F} \subseteq \mathbb{E} \subseteq \mathbb{K}$ be fields and $\alpha \in \mathbb{K}$.
If α is algebraic over $\mathbb{F}$, then α is algebraic 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 $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ 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 $\mathbb{F}[x] \to \mathbb{F}[\alpha] \subseteq \mathbb{K}$ 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 $\operatorname{irr}(\alpha, \mathbb{F})$.

The degree of $\operatorname{irr}(\alpha, \mathbb{F})$ is called the degree of α over $\mathbb{F}$ 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 $f(x) = \operatorname{irr}(\alpha, \mathbb{Q})$.

   However, $\operatorname{irr}(\alpha, \mathbb{Q}(\iota)) = x^2 - \iota$. 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 $\alpha, \beta \in \mathbb{K} \supseteq \mathbb{F}$ be algebraic over $\mathbb{F}$. Then, there exists an $\mathbb{F}$-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, $[\mathbb{F}(\alpha) : \mathbb{F}] = 2$. Thus, $\mathbb{F}(\alpha) = \mathbb{K}$.

That is, all quadratic extensions are simple.

Theorem 1.21 (Tower law). Let $\mathbb{F} \subseteq \mathbb{E} \subseteq \mathbb{K}$ 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 $\mathbb{F} \subseteq \mathbb{F}(\alpha) \subseteq \mathbb{K}$. $\square$

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 $\mathbb{F} \subseteq \mathbb{E}$ and $\mathbb{E} \subseteq \mathbb{K}$ be algebraic extensions. Then, $\mathbb{F} \subseteq \mathbb{K}$ 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. [↓]

§1.2. Compositum of fields

Definition 1.26. Let $\mathbb{E}_1, \mathbb{E}_2 \subseteq \mathbb{K}$ 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 $\mathbb{F} \subseteq \mathbb{E}_1, \mathbb{E}_2 \subseteq \mathbb{K}$ 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,

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

$\subseteq$ 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 $\mathbb{F} \subseteq \mathbb{E}_1, \mathbb{E}_2 \subseteq \mathbb{K}$ 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 $d := [\mathbb{E}_1 : \mathbb{F}][\mathbb{E}_2 : \mathbb{F}] < \infty$.
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

$$\begin{tikzcd}
& \mathbb{K} \arrow[d, dash] & \\
& \mathbb{E}_1\mathbb{E}_2 \arrow[dl, dash, "\leq m"'] \arrow[dr, dash, "\leq n"] & \\
\mathbb{E}_1 \arrow[dr, dash, "n"'] & & \mathbb{E}_2 \arrow[dl, dash, "m"] \\
& \mathbb{F} &
\end{tikzcd}$$

§1.3. Splitting Fields

Definition 1.31. Let $\mathbb{F}$ be a field and $f(x) \in \mathbb{F}[x]$ be a non-constant polynomial of degree n with leading coefficient $a \in \mathbb{F}^\times$. A field $\mathbb{K} \supseteq \mathbb{F}$ 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 $\mathbb{K} \supseteq \mathbb{F}$ 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

§2.1. Basic Definitions

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

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

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 $f \in R[u_1, \dots, u_n]$ is said to be a symmetric polynomial (in n variables) if

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

for all $\tau \in S_n$. In other words, $g_\tau(f) = f$ for all $\tau \in S_n$.

Definition 2.4. Let $S = R[u_1, \dots, u_n]$. 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

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

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

§2.2. Fundamental theorem of Symmetric Polynomials

Definition 2.6. Given an elementary symmetric polynomial $\sigma_i \in R[u_1, \ldots, u_n]$ in n variables (for $n \geq 2$), we define the elementary symmetric polynomial σ_i^0 in $(n-1)$ variables as
$$\sigma_i^0 := \sigma_1(u_1, \ldots, u_{n-1}, 0).$$

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 $S := R[u_1, \ldots, u_n]$ 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.) [↓]

§2.3. 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.

§2.4. 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

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

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

Moreover, by construction, $\operatorname{disc}_{\mathbb{K}}(f(x))$ has a square root in $\mathbb{K}$, namely

$$\prod_{1 \le i < j \le n} (r_i - r_j) \in \mathbb{K}.$$

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. (See the remark right after the definition, if you are confused.)

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,

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

Remark 2.15. In the above, σ_i are not the elementary symmetric polynomials, they are simply elements of $\mathbb{F}$. We are *defining* w_k recursively in terms of σ_i using the relations given in (2.1).

An alternate (but longer) definition could have been to start with $f(x) = x^n - a_1x^{n-1} + \cdots a_n \in \mathbb{F}[x]$ and define

$$w_k := \begin{cases} a_1w_{k-1} - a_2w_{k-2} + \cdots + (-1)^k a_{k-1}w_1 + (-1)^{k+1}a_k k & k \leq n, \\ a_1w_{k-1} - a_2w_{k-2} + \cdots + (-1)^{n+1}a_n w_{k-n} & k > n, \end{cases}$$

and then write the determinant.

Proposition 2.16 (Discriminant in terms of derivative)**.** Suppose $f(x) = \prod_{i=1}^{n}(x - r_i)$. Then, $\operatorname{disc}(f(x)) = (-1)^{\binom{n}{2}} \prod_{i=1}^{n} f'(r_i)$. [↓]

The derivative is formally defined later, it is Definition 4.1.

Example 2.17 (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 2.18 (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, $\mathrm{disc}(f(x)) = -4p^3 - 27q^2$.

§2.5. The Fundamental Theorem of Algebra

Recall the following facts.

Lemma 2.19.

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 all roots in $\mathbb{C}$. [↓]

Theorem 2.20 (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 an 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 of $\mathbb{F}$ 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 $\mathbb{F} \subseteq \mathbb{K}$ 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

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

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 $\mathbb{F}_i \subseteq \mathbb{F}_j$ (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 $\alpha \in \mathbb{K} \supseteq \mathbb{F}$ 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

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

[↓]

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 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 $\deg(p(x))$. 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 $\sigma(\mathbb{F})$, 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 theorem to the inclusion $i : \mathbb{F} \hookrightarrow \mathbb{E}_2$ to extend it to an $\mathbb{F}$-isomorphism $\tau : \mathbb{K}_1 \to \mathbb{K}_2$. □

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 $D_{\mathbb{F}} : \mathbb{F}[x] \to \mathbb{F}[x]$ by

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

Given $f(x) \in \mathbb{F}[x]$, we call $D_{\mathbb{F}}(f(x))$ the (formal) 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 $\mathbb{C}$, 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 $D_{\mathbb{F}}$ is indeed $\mathbb{F}$-linear.

Proposition 4.4. Let $\mathbb{F} \subseteq \mathbb{E}$ be a field extension. Then, $D_{\mathbb{E}}|_{\mathbb{F}} = D_{\mathbb{F}}$. 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 $r_1, \ldots, r_g$.
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 had seen to be independent of the splitting field. (Proposition 2.13.)
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. (Example 4.11.) Over fields of characteristic 0, however, it is true. We shall prove that as well. (Proposition 4.10.)

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 $r \in \mathbb{E} \supseteq \mathbb{F}$ 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 all roots simple 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.

The above can essentially be attributed to the fact that X has no p-th root in $\mathbb{F}_p(X)$. In fact, as we shall see, the existence of p-th roots will play an important role.

It should also be clear that we can replace $\mathbb{F}_p$ with any field of characteristic p in the above.

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. For this, 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 $\operatorname{char}(\mathbb{F}) = p > 0$. Then, $x^p - a \in \mathbb{F}[x]$ is either irreducible in $\mathbb{F}[x]$ or $a \in \mathbb{F}^p$. [↓]

In other words, either the above polynomial either has a root or is irreducible.

Proposition 4.15. Let $f(x) \in \mathbb{F}[x]$ be an irreducible polynomial and let $p := \operatorname{char}(\mathbb{F}) > 0$. 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 $\mathbb{F} \subseteq \mathbb{K}$ be a field extension.

An algebraic element $\alpha \in \mathbb{K}$ over $\mathbb{F}$ is called a separable element over $\mathbb{F}$ if $\operatorname{irr}(\alpha, \mathbb{F})$ 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 (in Example 4.11) that $\mathbb{F}_p(X)$ is not perfect for any prime p. (Or more generally, $\mathbb{F}(X)$ is not perfect if $\operatorname{char}(\mathbb{F}) \neq 0$.)
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 $\operatorname{char}(\mathbb{F}) = 0$, then all roots are simple.
If $\operatorname{char}(\mathbb{F}) =: p > 0$, 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 $\tau \circ \sigma^{-1} : \sigma(\mathbb{F}) \to \tau(\mathbb{F})$ (cf. Theorem 3.10).

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

$$
\begin{tikzcd}
\mathbb{L}' \arrow[d, dash] & & \mathbb{L} \arrow[ll, "\lambda"'] \arrow[d, dash] \\
\widetilde{\tau}(\mathbb{E}) \arrow[d, dash] & \mathbb{E} \arrow[l, "\widetilde{\tau} \in S_\tau"'] \arrow[r, "\widetilde{\sigma} \in S_\sigma"] & \widetilde{\sigma}(\mathbb{E}) \arrow[d, dash] \\
\tau(\mathbb{F}) & \mathbb{F} \arrow[l, "\tau"'] \arrow[r, "\sigma"] & \sigma(\mathbb{F})
\end{tikzcd}
$$

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 $\mathbb{L} \supseteq \mathbb{F}$ to be an algebraic closure of $\mathbb{F}$ 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 $\alpha \in \mathbb{E} \supseteq \mathbb{F}$ be algebraic over $\mathbb{F}$ and $n := \deg(\operatorname{irr}(\alpha, \mathbb{F}))$. 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 $p(x) := \operatorname{irr}(\alpha, \mathbb{F})$ 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 $\mathbb{F} \subseteq \mathbb{E} \subseteq \mathbb{K}$ 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 $\mathbb{F} \subseteq \mathbb{E} \subseteq \mathbb{K}$ 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 $\alpha \in \mathbb{E} \supseteq \mathbb{F}$ 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. $\square$

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

Corollary 4.31. Let $f(x) \in \mathbb{F}[x]$ be a separable polynomial and $\mathbb{E} \supseteq \mathbb{F}$ be a splitting field of $f(x)$ over $\mathbb{F}$. Then, $\mathbb{E}/\mathbb{F}$ is separable.

Proof. Write $\mathbb{E} = \mathbb{F}(r_1, \ldots, r_n)$ where $f(x) = a(x - r_1) \cdots (x - r_n)$ and use the previous corollary and proposition repeatedly. $\square$

Proposition 4.32. Let $\mathbb{E}/\mathbb{F}$ be a finite extension. Then, $[\mathbb{E} : \mathbb{F}]_s$ divides $[\mathbb{E} : \mathbb{F}]$. If $\operatorname{char}(\mathbb{F}) =: p > 0$, then quotient $\dfrac{[\mathbb{E} : \mathbb{F}]}{[\mathbb{E} : \mathbb{F}]_s}$ is a power of p. [↓]

Chapter 5

Finite fields

§5.1. Existence and Uniqueness

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

Theorem 5.1 (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 5.2. We shall denote *the* finite field with p^n elements by $\mathbb{F}_{p^n}$.

Remark 5.3. We have not yet shown that $\mathbb{F}_{p^n}$ exists for every prime p and $n \in \mathbb{N}$. Have only shown uniqueness up to isomorphism.

Theorem 5.4 (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

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

[↓]

Here's an interesting application to finite fields.

Proposition 5.5. The polynomial $f(x) := x^4 + 1$ is irreducible in $\mathbb{Z}[x]$ but it is reducible in $\mathbb{F}_p$ for every prime p. [↓]

§5.2. Gauss' Necklace Formula

Recall the Möbius inversion formula.

Definition 5.6. The Möbius function $\mu : \mathbb{N} \to \mathbb{N}$ is defined as

$$\mu(n) := \begin{cases} 1 & n = 1, \\ (-1)^r & n \text{ is a product of } r \text{ distinct primes}, \\ 0 & p^2 \mid n \text{ for some prime } p. \end{cases}$$

Theorem 5.7 (Möbius inversion formula)**.** Let $f, g : \mathbb{N} \to \mathbb{N}$ be functions satisfying

$$f(n) = \sum_{d \mid n} g(d).$$

Then, they also satisfy

$$g(n) = \sum_{d \mid n} f\left(\frac{n}{d}\right) \mu(d).$$

Notation: For the remaining of this section, p is an odd prime and q is a positive integral power of p.

Lemma 5.8. If $m \mid n$, then $x^{q^m} - x \mid x^{q^n} - x$ in $\mathbb{F}_q[x]$. [↓]

Lemma 5.9. Let $f(x) \in \mathbb{F}_q[x]$ be a monic irreducible polynomial.
Then, $f(x) \mid x^{q^n} - x$ iff $\deg(f(x)) \mid n$. [↓]

Remark 5.10. This shows that the monic factorisation of $x^{q^n} - x$ in $\mathbb{F}_q[x]$ consists of every (monic) irreducible polynomial of degree d as a factor, where d runs over all divisors of n. (No factor can be repeated twice since the polynomial is separable.)

Theorem 5.11 (Gauss)**.** The number of irreducible polynomials of degree n over $\mathbb{F}_q$ is given by

$$N_q(n) = \frac{1}{n}\sum_{d|n} \mu(d)q^{n/d}.$$

[↓]

§5.3. Primitive Element Theorem

Definition 5.12. Let $\mathbb{E}/\mathbb{F}$ be a field extension. An element $\alpha \in \mathbb{E}$ is called a primitive element for $\mathbb{E}$ over $\mathbb{F}$ if $\mathbb{E} = \mathbb{F}(\alpha)$.

We say that $\mathbb{E}$ is primitive over $\mathbb{F}$ if there exists a primitive element for $\mathbb{E}$ over $\mathbb{F}$.

Theorem 5.13 (Primitive Element Theorem)**.** Let $\mathbb{K}/\mathbb{F}$ be a finite extension.

1. There is a primitive element for $\mathbb{K}/\mathbb{F}$ iff the number of intermediate subfields $\mathbb{E}$ such that $\mathbb{F} \subseteq \mathbb{E} \subseteq \mathbb{K}$ is finite.

2. If $\mathbb{K}/\mathbb{F}$ is a separable extension, then it has a primitive element. [↓]

Chapter 6

Normal extensions

Definition 6.1. An algebraic extension $\mathbb{E}/\mathbb{F}$ is called a normal extension if whenever $f(x) \in \mathbb{F}[x]$ is irreducible and has a root in $\mathbb{E}$, then $f(x)$ splits into linear factors in $\mathbb{E}[x]$.

Definition 6.2. Let $\mathbb{E}/\mathbb{F}$ be an extension and $\mathcal{F} = \{f_i(x)\}_{i \in I}$ be a (possibly infinite) family of non-constant polynomials in $\mathbb{F}[x]$. Then, $\mathbb{E}$ is said to be a splitting field for the family $\mathcal{F}$ over $\mathbb{F}$ if each $f_i(x)$ splits as a product of linear factors in $\mathbb{E}[x]$ and is generated by the roots of the polynomials.

Remark 6.3. Note that a splitting field of any family always exists, since an algebraic closure always exists. So, we consider $A \subseteq \overline{\mathbb{F}}$ to be the set of roots of all the polynomials of the family $\mathcal{F}$ and then put $\mathbb{E} := \mathbb{F}(A) \subseteq \overline{\mathbb{F}}$.

Proposition 6.4. Let $\mathbb{F}$ be a field, and $\mathcal{F} \subseteq \mathbb{F}[x]$ be a family of separable polynomials. Let $\mathbb{E} \subseteq \overline{\mathbb{F}}$ be the splitting field of $\mathcal{F}$ over $\mathbb{F}$. Then, $\mathbb{E}/\mathbb{F}$ is a separable extension. [↓]

Lemma 6.5. Let $\mathbb{E}/\mathbb{F}$ be an algebraic extension. Let $\sigma : \mathbb{E} \to \mathbb{E}$ be an $\mathbb{F}$-embedding. Then, σ is an automorphism of $\mathbb{E}$. [↓]

Theorem 6.6. Let $\mathbb{F}$ be a field and fix an algebraic closure $\overline{\mathbb{F}}$ of $\mathbb{F}$. Let $\mathbb{F} \subseteq \mathbb{E} \subseteq \overline{\mathbb{F}}$ be fields. Then, the following are equivalent:

1. Every $\mathbb{F}$-embedding $\sigma : \mathbb{E} \to \overline{\mathbb{F}}$ is an automorphism of $\mathbb{E}$.
2. $\mathbb{E}$ is a splitting field of a family of polynomials in $\mathbb{F}[x]$.
3. $\mathbb{E}/\mathbb{F}$ is a normal extension. [↓]

Proposition 6.7. Let $\mathbb{F} \subseteq \mathbb{E}_1, \mathbb{E}_2 \subseteq \mathbb{K}$ be fields. Suppose that $\mathbb{E}_i/\mathbb{F}$ are normal. Then, so are $\mathbb{E}_1\mathbb{E}_2/\mathbb{F}$ and $(\mathbb{E}_1 \cap \mathbb{E}_2)/\mathbb{F}$. [↓]

Example 6.8. Quadratic extensions are always normal. Indeed, pick $\alpha \in \mathbb{E} \setminus \mathbb{F}$. Then, $\mathbb{E} = \mathbb{F}(\alpha)$ is a splitting field of $\operatorname{irr}(\alpha, \mathbb{F})$ over $\mathbb{F}$.

Remark 6.9. Unlike the "tower laws" for algebraic and separable extensions, the "composition" of normal extensions need not be normal. For example, consider the chain

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[4]{2}).$$

Each successive extension is quadratic and hence, normal. However, $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is not normal since the irreducible (via Eisenstein) polynomial $x^4 - 2 \in \mathbb{Q}[x]$ has a root in $\mathbb{Q}(\sqrt[4]{2})$ but does not factor completely.

On the other hand, consider

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{Q}(\sqrt[4]{2}, \iota).$$

Then, $\mathbb{Q}(\sqrt[4]{2}, \iota)/\mathbb{Q}$ is normal since $(\sqrt[4]{2}, \iota)$ is the splitting field for $x^4 - 2$ over $\mathbb{Q}$ but $(\sqrt[4]{2})/\mathbb{Q}$ is not.

However, one part of the "tower property" *does* hold, as can be easily verified, either directly from the definition or using one of the equivalences proven above.

Proposition 6.10. Let $\mathbb{F} \subseteq \mathbb{E} \subseteq \mathbb{K}$ be fields such that $\mathbb{K}/\mathbb{F}$ is normal. Then, $\mathbb{K}/\mathbb{E}$ is normal.

Remark 6.11. The above phenomenon is related (at least in the case of finite extensions) to the phenomenon that “is a normal subgroup” is not transitive either. Given groups $H \leq K \leq G$, it is possible that H is normal in K and K in G but H is not normal in G.

Similarly, if we know that H is normal in G, then we can conclude that H is normal in K but K need not be normal in G.

Chapter 7

Galois Extensions

§7.1. Definitions

Definition 7.1. A field extension $\mathbb{E}/\mathbb{F}$ is called a Galois extension if it is normal and separable. The Galois group of a Galois extension $\mathbb{E}/\mathbb{F}$ is the group of all $\mathbb{F}$-automorphisms of $\mathbb{E}$ under the operation of composition of maps. It is denoted $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$.

If $f(x) \in \mathbb{F}[x]$ is a separable polynomial and $\mathbb{E}$ is a splitting field of $f(x)$ over $\mathbb{F}$, then $\mathbb{E}/\mathbb{F}$ is a Galois extension and the Galois group of $f(x)$ over $\mathbb{F}$ is defined to be $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$ and denoted as $\mathrm{Gal}(f(x), \mathbb{F})$ or simply G_f if $\mathbb{F}$ is clear.

Remark 7.2. Note that the definition of the $\mathrm{Gal}(f(x), \mathbb{F})$ does not depend on the splitting field chosen, up to isomorphism. Indeed, let $\mathbb{E}$ and $\mathbb{E}'$ be two splitting fields of $f(x)$ over $\mathbb{F}$. By Theorem 3.13, there is an $\mathbb{F}$-isomorphism $\tau : \mathbb{E} \to \mathbb{E}'$. Then, $\sigma \mapsto \tau \circ \sigma \circ \tau^{-1}$ is an isomorphism from $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$ to $\mathrm{Gal}(\mathbb{E}'/\mathbb{F})$.

Example 7.3. Here are some examples and non-examples.

1. Let $\mathbb{E}/\mathbb{F}$ be an extension of finite fields. Then, $|\mathbb{F}| = q$ and $|\mathbb{E}| = q^n$ for some prime power q and $n \in \mathbb{N}$. Then, $\mathbb{E}$ is a splitting field for $x^{q^n} - x \in \mathbb{F}[x]$ over $\mathbb{F}$. Thus, the extension is normal.
   Since the fields are finite, it is also separable.

2. The extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is **not** Galois. Since $\mathrm{char}(\mathbb{Q}) = 0$, it is separable.

However, it is not normal. Indeed, the irreducible (by Eisenstein) polynomial $x^3 - 2 \in \mathbb{Q}[x]$ has a root in $\mathbb{Q}(\sqrt[3]{2})$ but it does not split as a product of linear factors.

3. The extension $\mathbb{F}_p(X)(X^{1/p})/\mathbb{F}_p(X)$ is not separable and hence, **not** Galois. It *is* normal since the bigger field is the splitting field of $T^p - X \in \mathbb{F}_p(X)[T]$.

Proposition 7.4. Let $\mathbb{E}/\mathbb{F}$ be a finite Galois extension. Then, $|\mathrm{Gal}(\mathbb{E}/\mathbb{F})| = [\mathbb{E} : \mathbb{F}]_s = [\mathbb{E} : \mathbb{F}]$. [↓]

Note that the last equality is simply by definition of a Galois extension (and Theorem 4.28).

Remark 7.5. The above proposition shows why normality and separability are both needed. If the extension is normal but not separable, then the order of the group would be the separable degree.

On the other hand, if the extension is separable but not normal, then there would be an extension $\sigma : \mathbb{E} \to \overline{\mathbb{F}}$ would map $\mathbb{E}$ outside $\mathbb{E}$ and so, not all extensions will belong to the Galois group.

As an example, consider $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. Since there is only one root of $x^3 - 2$ in $\mathbb{Q}(\sqrt[3]{2})$, there is only one $\mathbb{Q}$-automorphism of $\mathbb{Q}(\sqrt[3]{2})$.

Proposition 7.6. Let q be a prime power.

The Galois group of the Galois extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ is a cyclic group of order n generated by the Frobenius automorphism $\varphi : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ defined as $a \mapsto a^q$. [↓]

Example 7.7. A field extension $\mathbb{K}/\mathbb{F}$ is called biquadratic if $[\mathbb{K} : \mathbb{F}] = 4$ and $\mathbb{K}$ is generated over $\mathbb{F}$ by roots of two irreducible quadratic separable polynomials.

In particular, $\mathbb{K}/\mathbb{F}$ is a Galois extension. Write $\mathbb{K} = \mathbb{F}(\alpha, \beta)$ and let $p(x) := \mathrm{irr}(\alpha, \mathbb{F})$ and $q(x) := \mathrm{irr}(\beta, \mathbb{F})$. Let $\overline{\alpha}, \overline{\beta} \in \mathbb{K}$ denote the other root of $p(x)$ and $q(x)$. By assumption of separability, $\overline{\alpha} \neq /\alpha$ and $\overline{\beta} \neq \beta$.

Since $[\mathbb{F}(\alpha, \beta) : \mathbb{F}] = 4$, the quadratic $p(x)$ is irreducible over $\mathbb{F}(\beta)$ and similarly for $q(x)$ over $\mathbb{F}(\alpha)$. Thus, the four automorphisms are determined by sending α to α or $\overline{\alpha}$ and β to β or $\overline{\beta}$.

Define the automorphisms $\tau, \sigma : \mathbb{K} \to \mathbb{K}$ by

$$\tau(\alpha) = \overline{\alpha}, \ \tau(\beta) = \beta,$$
$$\sigma(\alpha) = \alpha, \ \sigma(\beta) = \overline{\beta}.$$

Then, $\tau^2 = \sigma^2 = \mathrm{id}_{\mathbb{K}}$. Thus, $\mathrm{Gal}(\mathbb{K}/\mathbb{F}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, the Klein-4 group.

Example 7.8 (Galois group of a separable cubic)**.** We show the role of the discriminant in determining the Galois group of a cubic.

Let $\mathbb{F}$ be a field with $\mathrm{char}(\mathbb{F}) \neq 2, 3$. Let $f(x) = x^3 + px + q \in \mathbb{F}[x]$ be an irreducible cubic. In particular, $f(x)$ has no roots in $\mathbb{F}$. We wish to show that $f(x)$ is separable. Note that

$$f'(x) = 3x^2 + p \neq 0,$$

since $\mathrm{char}(\mathbb{F}) \neq 3$. Thus, $f(x)$ is separable, by Proposition 4.10.

Thus, a splitting field $\mathbb{E}$ of $f(x)$ over $\mathbb{F}$ has degree either 3 or 6. By Proposition 7.4, we know that $|\mathrm{Gal}(\mathbb{E}/\mathbb{F})| = 3$ or 6. We see now how the discriminant determines this.

Let $\mathbb{E} = \mathbb{F}(\alpha_1, \alpha_2, \alpha_3)$, where $f(x) = \prod_{i=1}^{3}(x - \alpha_i)$. Any $\sigma \in \mathrm{Gal}(\mathbb{E}/\mathbb{F})$ permutes these roots. Let $p_\sigma \in S_3$ denote the corresponding permutation. It is easy to see that $\sigma \mapsto p_\sigma$ is injective. (Action of σ on σ_i completely determines the automorphism.) Under this, we identify $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$ with a subgroup of S_3.

Thus, $\mathrm{Gal}(\mathbb{E}/\mathbb{F}) = A_3$ or S_3. Let

$$\delta = (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1).$$

Then, $\delta^2 = \mathrm{disc}(f(x)) = -(4p^3 + 27q^2) \in \mathbb{F}$. (Recall we had calculated this discriminant in Example 2.18.)

Thus, $[\mathbb{F}(\delta) : \mathbb{F}] \leq 2$. Now, if $\delta \in \mathbb{F}$, then $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$ cannot have any odd permutations since they do not fix δ and hence, $\mathrm{Gal}(\mathbb{E}/\mathbb{F}) = A_3$.

On the other hand, if $\delta \notin \mathbb{F}$, then $2 = [\mathbb{F}(\delta) : \mathbb{F}] \mid [\mathbb{E} : \mathbb{F}]$ and so, $\mathrm{Gal}(\mathbb{E}/\mathbb{F}) = S_3$.

Note that $\delta \in \mathbb{F} \iff \mathrm{disc}(f(x))$ is a perfect square in $\mathbb{F}$. Thus, the above is characterised entirely by $\mathrm{disc}(f(x))$ being a perfect square.

For example, if $f(x) = x^3 + x + 1 \in \mathbb{Q}[x]$, then $\operatorname{disc}(f(x)) = -31$ and so, $\operatorname{Gal}(\mathbb{E}/\mathbb{Q}) \cong S_3$. On the other hand, if $f(x) = x^3 - 3x + 1$, then $\operatorname{disc}(f(x)) = 81 = 9^2$ and thus, $\operatorname{Gal}(\mathbb{E}/\mathbb{Q}) \cong A_3$.

§7.2. The Fundamental Theorem of Galois Theory

Definition 7.9. Let $\mathbb{E}$ be a field and G be a group of automorphisms of $\mathbb{E}$. Then,

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

is called the fixed field of G acting on E.

Remark 7.10. As one can easily show, the above is indeed a field.

Note that G is not necessarily the group of *all* automorphisms of $\mathbb{E}$.

Theorem 7.11 (Fundamental Theorem of Galois Theory (FTGT))**.** Let $\mathbb{K}/\mathbb{F}$ be a finite Galois extension. Consider the sets

$$\mathcal{I} = \{\mathbb{E} \mid \mathbb{E} \text{ is an intermediate field of } \mathbb{K}/\mathbb{F}\} \quad \text{and} \quad \mathcal{G} = \{H \mid H \leq \operatorname{Gal}(\mathbb{K}/\mathbb{F})\}.$$

1. The maps
$$E \mapsto \operatorname{Gal}(\mathbb{K}/\mathbb{E}) \quad \text{and} \quad H \mapsto \mathbb{K}^H$$
give a one-to-one correspondence between $\mathcal{I}$ and $\mathcal{G}$, called the Galois correspondence. Moreover, these are inclusion reversing.
2. $\mathbb{E}/\mathbb{F}$ is Galois iff $\operatorname{Gal}(\mathbb{K}/\mathbb{E}) \trianglelefteq \operatorname{Gal}(\mathbb{K}/\mathbb{F})$ and in this case,
$$\operatorname{Gal}(\mathbb{E}/\mathbb{F}) \cong \frac{\operatorname{Gal}(\mathbb{K}/\mathbb{F})}{\operatorname{Gal}(\mathbb{K}/\mathbb{E})}.$$
3. $\mathbb{K}/\mathbb{E}$ is always Galois and $|\operatorname{Gal}(\mathbb{K}/\mathbb{E})| = [\mathbb{K} : \mathbb{E}] = \dfrac{[\mathbb{K} : \mathbb{F}]}{[\mathbb{E} : \mathbb{F}]}$.
4. If $\mathbb{E}_1, \mathbb{E}_2 \in \mathcal{I}$ correspond to H_1 and H_2, then $\mathbb{E}_1 \cap \mathbb{E}_2$ corresponds to $\langle H_1, H_2 \rangle$ and $\mathbb{E}_1\mathbb{E}_2$ to $H_1 \cap H_2$.

[↓]

The proof of the above will be given in many steps. Parts of it will be proven for infinite Galois extensions as well. Note that 3 follows from Proposition 7.4.

For the rest of the section, $\mathbb{K}/\mathbb{F}$ will denote a (possibly infinite) Galois extension and $\mathcal{I}$ and $\mathcal{G}$ will be as in Theorem 7.11.

Theorem 7.12. Let $\mathbb{K}/\mathbb{F}$ be a (possibly infinite) Galois extension and put $G = \text{Gal}(\mathbb{K}/\mathbb{F})$. Then,

1. $\mathbb{F} = \mathbb{K}^G$.
2. Let $\mathbb{E} \in \mathcal{I}$. Then, $\mathbb{K}/\mathbb{E}$ is Galois and the map $E \mapsto \text{Gal}(\mathbb{K}/\mathbb{E})$ is an injective map from $\mathcal{I}$ to $\mathcal{G}$. [↓]

Remark 7.13. The above again shows the need for Galois extension. For example, consider the non-Galois extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. If we consider G to be the "Galois group," that is, G to be the group of automorphisms of $\mathbb{Q}(\sqrt[3]{2})$ which fix $\mathbb{Q}$, we see that G is trivial. Thus, $\mathbb{Q}(\sqrt[3]{2})^G = \mathbb{Q}(\sqrt[3]{2})$.

However, for Galois extensions, the above says that the only field which is fixed by all the Galois automorphisms is precisely the base field.

Lemma 7.14. Let $\mathbb{E}/\mathbb{F}$ be a separable extension and $n \in \mathbb{N}$. Suppose that for all $\alpha \in \mathbb{E}$, $[\mathbb{F}(\alpha) : \mathbb{F}] \leq n$. Then, $[\mathbb{E} : \mathbb{F}] \leq n$. [↓]

Remark 7.15. Note that the above did not assume a priori that $\mathbb{E}/\mathbb{F}$ is finite. If that were the case, then the Primitive Element Theorem would yield the answer.

The above is not true without the assumption of separability. For example, consider $\mathbb{F} = \mathbb{F}_p(X, Y)$ where p is a prime. Consider $\mathbb{E} = \mathbb{F}(X^{1/p}, Y^{1/p})$.

Then, $\alpha^p \in \mathbb{F}$ for all $\alpha \in \mathbb{E}$ (exercise) and thus, $[\mathbb{E}(\alpha) : \mathbb{F}] \leq p$ for all $\alpha \in \mathbb{E}$. However, $[\mathbb{E} : \mathbb{F}] = p^2 > p$.

Theorem 7.16 (Artin's Theorem)**.** Let $\mathbb{E}$ be a field and G a <u>finite</u> group of automorphisms of $\mathbb{E}$. Then,

1. $\mathbb{E}/\mathbb{E}^G$ is a *finite* Galois extension.

2. $\mathrm{Gal}(\mathbb{E}/\mathbb{E}^G) = G$.
3. $[\mathbb{E} : \mathbb{E}^G] = |G|$. [↓]

Theorem 7.17. Let $\mathbb{K}/\mathbb{F}$ be a (possibly infinite) Galois extension with Galois group G. Let $\mathbb{E}_1$ and $\mathbb{E}_2$ be intermediate subfields of $\mathbb{K}/\mathbb{F}$. Let $H_i := \mathrm{Gal}(\mathbb{K}/\mathbb{E}_i)$ for $i = 1, 2$.Then

$$\mathbb{E}_1\mathbb{E}_2 = \mathbb{K}^{H_1 \cap H_2}, \ \mathbb{E}_1 \cap \mathbb{E}_2 = \mathbb{K}^{\langle H_1, H_2 \rangle}, \text{ and } \mathbb{E}_1 \subseteq \mathbb{E}_2 \iff H_1 \supseteq H_2.$$

[↓]

Remark 7.18. Essentially the thing to keep in mind is that smaller subfields corresponding to larger subgroups. Now, given two subfields/subgroups, we have the corresponding smallest (or largest) subfield/subgroup containing them (or being contained in them). The above shows that the Galois correspondence (in one direction) preserves them.

(The smallest field containing the subfields is the fixed field of the action of the largest subgroup contained in the Galois groups.
The largest field containing the subfields is the fixed field of the action of the smallest subgroup containing the Galois groups.)

Proposition 7.19. Let $\mathbb{K}/\mathbb{F}$ be a (possibly infinite) Galois extension. Let $\lambda : \mathbb{K} \to \lambda(\mathbb{K})$ be an isomorphism of fields. Then,

1. $\lambda(\mathbb{K})/\lambda(\mathbb{F})$ is a Galois extension.
2. $\mathrm{Gal}(\lambda(\mathbb{K})/\lambda(\mathbb{F})) = \lambda \, \mathrm{Gal}(\mathbb{K}/\mathbb{F})\lambda^{-1} \cong \mathrm{Gal}(\mathbb{K}/\mathbb{F})$. [↓]

Theorem 7.20. Let $\mathbb{K}/\mathbb{F}$ be a (possibly infinite) Galois extension. Let $\mathbb{E}$ be an intermediate subfield of $\mathbb{K}/\mathbb{F}$. Then,

1. $\mathbb{E}/\mathbb{F}$ is Galois iff $\mathrm{Gal}(\mathbb{K}/\mathbb{E}) \trianglelefteq \mathrm{Gal}(\mathbb{K}/\mathbb{F})$.
2. If $\mathbb{E}/\mathbb{F}$ is Galois, then
$$\mathrm{Gal}(\mathbb{E}/\mathbb{F}) \cong \frac{\mathrm{Gal}(\mathbb{K}/\mathbb{F})}{\mathrm{Gal}(\mathbb{K}/\mathbb{E})}.$$

[↓]

With this, we can now prove the Fundamental Theorem of Galois Theory (FTGT). [↓]

§7.3. Applications of FTGT

We give another proof of the Fundamental Theorem of Algebra.

Theorem 7.21 (Fundamental Theorem of Algebra)**.** The field of complex numbers is algebraically closed. [↓]

Example 7.22 (Symmetric rational functions)**.** Let $\mathbb{E} = \mathbb{F}(x_1, \ldots, x_n)$ be the fraction field of $R = \mathbb{F}[x_1, \ldots, x_n]$, where x_i are indeterminates over the field $\mathbb{F}$.

We had seen that the symmetric polynomials in R are the polynomials in the symmetric polynomials. We now prove an analogous result for symmetric rational functions.

Note that S_n acts on $\mathbb{E}$ in the natural way. More precisely, if $\sigma \in S_n$, then we have the $\mathbb{F}$-automorphism $\varphi_\sigma : \mathbb{E} \to \mathbb{E}$ determined by $\varphi_\sigma(x_i) = x_{\sigma(i)}$. Note that $\varphi_{\sigma_1\sigma_2} = \varphi_{\sigma_1} \circ \varphi_{\sigma_2}$ and thus, $G = \{\varphi_\sigma : \sigma \in S_n\}$ is a group of automorphisms of $\mathbb{E}$ and is isomorphic to S_n.

Let $\sigma_1, \ldots, \sigma_n \in \mathbb{E}$ be the elementary symmetric polynomials in $x_1, \ldots, x_n$. Let X be an indeterminate over $\mathbb{E}$ and consider the polynomial ring $\mathbb{E}[X]$.
Each the automorphisms φ_σ to automorphisms of $\mathbb{E}[X]$ by fixing X. We denote the extension again by φ_σ.

Consider

$$\begin{aligned} g(X) &:= (X - x_1) \cdots (X - x_n) \\ &= X^n - \sigma_1 X^{n-1} + \cdots + (-1)^n \sigma_n. \end{aligned}$$

Let $\sigma \in S_n$ be arbitrary. Applying φ_σ to the first line above yields

$$\varphi_\sigma(g(X)) = (X - x_{\sigma(1)}) \cdots (X - x_{\sigma(n)}) = g(X).$$

Thus, each φ_σ fixes $g(X)$ and in turn, it fixes the coefficients $\sigma_1, \ldots, \sigma_n$. Thus,

$$\mathbb{F}(\sigma_1, \ldots, \sigma_n) \subseteq \mathbb{E}^G.$$

Note that

$$\mathbb{E} = \mathbb{F}(\sigma_1, \ldots, \sigma_n, x_1, \ldots, x_n)$$

and so, $\mathbb{E}$ is a splitting field of $g(X)$ over $\mathbb{F}(\sigma_1, \ldots, \sigma_n)$. Since $g(X)$ is separable, we see that $\mathbb{E}/\mathbb{F}(\sigma_1, \ldots, \sigma_n)$ is a Galois extension.

Now, if $\pi \in \mathrm{Gal}(\mathbb{E}/\mathbb{F}(\sigma_1, \ldots, \sigma_n))$, then π permutes the roots of $g(X)$ and fixes $\mathbb{F}$. Thus, $\pi = \varphi_\sigma$ for some $\sigma \in S_n$. Thus, $G = \mathrm{Gal}(\mathbb{E}/\mathbb{F}(\sigma_1, \ldots, \sigma_n))$.

Thus, we see that

$$\mathbb{F}(\sigma_1, \ldots, \sigma_n) = \mathbb{E}^G.$$

The left is the field of all rational functions in the symmetric polynomials. The right is the field of all rational functions fixed by S_n, that is, the symmetric rational functions.

Chapter 8

Cyclotomic Extensions

§8.1. Roots of unity

Definition 8.1. Let $\mathbb{F}$ be a field. A root $\zeta \in \mathbb{F}$ of $x^n - 1 \in \mathbb{F}[x]$ is called an n-th root of unity in $\mathbb{F}$.

Remark 8.2. Suppose that $\operatorname{char}(\mathbb{F}) = p > 0$ and $n = p^e m$ with $p \nmid m$. Then, $x^n = (x^m - 1)^{p^e}$. By the derivative criterion, $x^m - 1$ is separable. Thus, the splitting field of $x^n - 1$ is the same as that of $x^m - 1$ and the roots are the same too (ignoring multiplicity). Thus, we either consider fields of characteristic 0 or assume that $(\operatorname{char}(\mathbb{F}), n) = 1$.

Definition 8.3. Let $\mathbb{F}$ be a field and $n \in \mathbb{K}$.
Suppose that $\operatorname{char}(\mathbb{F}) = 0$ or $\gcd(\operatorname{char}(\mathbb{F}), n) = 1$. Then, $Z = \{z_1, \ldots, z_n\} \subseteq \overline{\mathbb{F}}^{\times}$ is a cyclic subgroup (Theorem 0.19). Any of the $\varphi(n)$ generators of Z is called a primitive n-th root of unity.

A primitive root of unity over $\mathbb{Q}$ is denoted by ζ_n and we define $\Phi_n(x) := \operatorname{irr}(\zeta_n, \mathbb{Q})$.

Remark 8.4. We shall soon show that $\operatorname{irr}(\zeta_n, \mathbb{Q})$ is independent of the primitive root chosen (and so, Φ_n is indeed well-defined). This is **not** the case in general (see Example 8.7).

Definition 8.5. A splitting field of $x^n - 1$ over $\mathbb{F}$ is called a cyclotomic extension of order n over $\mathbb{F}$.

Proposition 8.6. Let $\operatorname{char}(\mathbb{F}) = 0$ or $\gcd(\operatorname{char}(\mathbb{F}), n) = 1$ and $f(x) = x^n - 1 \in \mathbb{F}[x]$. Then, G_f is isomorphic to a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$. In particular, G_f is an abelian group and $|G_f| \mid \varphi(n)$. [↓]

Example 8.7. Let us consider $\mathbb{F} = \mathbb{F}_2$. We shall consider the n-th roots of unity for odd n so that $\gcd(n, 2) = 1$. In this example, we will consider $n = 3$ and 7. Since these are prime, we know that there are 2 and 6 primitive roots in the respective cases. In particular, any (third or seventh) root of unity which is not 1 must be a primitive root.

First, consider $x^3 - 1 = (x-1)(x^2+x+1)$. The quadratic factor is irreducible since it has no root. Any root of the quadratic is a primitive cube root of unity.

Now, consider $n = 7$. Then, we have

$$x^7 - 1 = (x-1)(x^3+x^2+1)(x^3+x+1).$$

Note that both the cubics are irreducible since they have no roots in $\mathbb{F}$. Since any root apart from 1 is a primitive root, we see that any of the roots of the two cubics is a primitive root.

In particular, note that are 6 primitive 7-th roots of unity over $\mathbb{F}$ with two minimal polynomials. However, we will see that this does not happen over $\mathbb{Q}$.

Proposition 8.8. Let $x^n - a = f(x) \in \mathbb{F}[x]$ and suppose $\mathbb{F}$ has n distinct roots of $x^n - 1$. Then, G_f is a cyclic group and $|G_f|$ divides n. [↓]

Theorem 8.9. Let $n \in \mathbb{N}$ fix a primitive root n-th root of unity $\zeta_n \in \overline{\mathbb{Q}}$ and let $\Phi_n(x) := \operatorname{irr}(\zeta_n, \mathbb{Q})$. Then,

1. $\Phi_n(x) \in \mathbb{Z}[x]$,

2. every primitive n-th root of unity is a root of $\Phi_n(x)$,
3. $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$, and
4. $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$. [↓]

§8.2. Computation of Cyclotomic Polynomials

As earlier, $\Phi_n(x)$ defines the irreducible polynomial of any primitive n-th root of unity.

Theorem 8.10. We have $\Phi_1(x) = x - 1$ and

$$\Phi_n(x) = \frac{x^n - 1}{\prod\limits_{\substack{d \mid n \\ d < n}} \Phi_d(x)}$$

for $n > 1$. [↓]

Example 8.11 (First few cyclotomic polynomials)**.**

$$\begin{aligned}
\Phi_1(x) &= x - 1, \\
\Phi_2(x) &= \frac{x^2 - 1}{x - 1} = x + 1, \\
\Phi_3(x) &= \frac{x^3 - 1}{x - 1} = x^2 + x + 1, \\
\Phi_4(x) &= \frac{x^4 - 1}{(x-1)(x+1)} = x^2 + 1, \\
\Phi_5(x) &= \frac{x^5 - 1}{x - 1} = x^4 + x^3 + x^2 + x + 1, \\
\Phi_6(x) &= \frac{x^6 - 1}{(x-1)(x^2-1)(x^3-1)} = x^2 - x + 1, \\
\Phi_7(x) &= \frac{x^7 - 1}{x - 1} = x^6 + x^5 + \cdots + x + 1.
\end{aligned}$$

Note that the above may indicate that the coefficients are always $0, \pm 1$. However, that is **not** the case.

However, the first example of that is $\Phi_{105}(x)$. The coefficients of x^7 and x^{41} is -2. (Every other coefficient is $0, \pm 1$.)

Exercise 8.12. Show that the cyclotomic polynomials are symmetric, i.e.,

$$\Phi_n(x) = x^{\varphi(n)}\Phi_n\left(\frac{1}{x}\right).$$

§8.3. Subfields of $\mathbb{Q}(\zeta_n)$

Proposition 8.13. Let p be a prime. Then, $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ is cyclic of order $p-1$. Consequently, given any divisor $d \mid p-1$, there is a unique intermediate subfield $\mathbb{E}$ of $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ such that $[\mathbb{E} : \mathbb{Q}] = d$. Equivalently, there is a unique intermediate $\mathbb{E}$ such that $[\mathbb{Q}(\zeta_p) : \mathbb{E}] = \frac{p-1}{d}$. [↓]

Lemma 8.14. Let p be an odd prime. Then $\mathrm{disc}(\Phi_p(x)) = (-1)^{\binom{p}{2}}p^{p-2}$. [↓]

Proposition 8.15. Let p be an odd prime. The field $\mathbb{Q}(\zeta_p)$ contains a unique quadratic extension of $\mathbb{Q}$, namely

$$\mathbb{Q}\left(\sqrt{\mathrm{disc}(\Phi_p(x))}\right) = \mathbb{Q}\left(\sqrt{(-1)^{\binom{p}{2}}p}\right),$$

which is real if $p \equiv 1 \pmod 4$ and (non-real) complex if $p \equiv 3 \pmod 4$. [↓]

Corollary 8.16. Every quadratic extension of $\mathbb{Q}$ is contained in a cyclotomic extension. [↓]

Proposition 8.17. Let p be an odd prime and $\mathbb{F} \subseteq \mathbb{Q}(\zeta_p)$ be a subfield such that

$[\mathbb{Q}(\zeta_p) : \mathbb{F}] = 2$. Then,

$$\mathbb{F} = \mathbb{Q}(\zeta_p + \zeta_p^{-1}).$$

[↓]

Proposition 8.18. Let $p > 2$ be a prime number. Let H be a subgroup of $G := \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. Define

$$\beta := \sum_{\sigma \in H} \sigma(\zeta_p).$$

Then,

$$\mathbb{Q}(\zeta_p)^H = \mathbb{Q}(\beta_H).$$

[↓]

Example 8.19. Let $p = 7$ and $\omega = \zeta_7$. Then, $[\mathbb{Q}(\omega + \omega^{-1}) : \mathbb{Q}] = 3$. Let us find the irreducible polynomial of $\omega + \omega^{-1}$.

Note that the degree of this is 3. Since this is also the separable degree, we see that $\omega + \omega^{-1}$ has an orbit of size 3 under $G := \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$.

If $\{\beta_1, \beta_2, \beta_3\}$ is the orbit of ω under G, then note that the polynomial

$$f(x) = (x - \beta_1)(x - \beta_2)(x - \beta_3)$$

is fixed by G and hence, must be in $\mathbb{Q}[x]$. Since it is of the correct degree, it is the irreducible polynomial of $\omega + \omega^{-1}$.

Thus, we now find the orbit. Note that $G \cong (\mathbb{Z}/7\mathbb{Z})^\times$. The latter is generated by $\bar{3}$. Thus, consider the automorphism $\sigma \in G$ determined by $\sigma(\omega) = \omega^3$. Then, $G = \langle \sigma \rangle$.

Now, we have

$$\begin{aligned}
\sigma(\omega + \omega^{-1}) &= \omega^3 + \omega^{-3} = \omega^3 + \omega^4 =: \beta_2 \\
\sigma^2(\omega + \omega^{-1}) &= \omega^9 + \omega^{-9} = \omega^2 + \omega^5 =: \beta_3.
\end{aligned}$$

Since the above elements are distinct from $\omega + \omega^{-1} =: \beta_1$, we have the orbit as

$$\{\beta_1, \beta_2, \beta_3\}.$$

Thus, we have

$$\operatorname{irr}(\alpha, \mathbb{Q}) = \prod_{i=1}^{3}(x - \beta_i) = x^3 + x^2 - 2x - 1.$$

Chapter 9

Abelian and Cyclic extensions

§9.1. Inverse Galois Problem

The inverse Galois problem asks whether every finite group appears as the Galois group of some Galois extension of $\mathbb{Q}$. This is currently unsolved. We prove this for finite abelian groups.

Definition 9.1. A Galois extension $\mathbb{E}/\mathbb{F}$ is called abelian (resp., cyclic) if $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$ is abelian (resp., cyclic).

Lemma 9.2. Let p be a prime number and n be relatively prime to p. Suppose $\bar{\Phi}_n(x)$ has a root in $\mathbb{F}_p$. Then, $p \equiv 1 \pmod{n}$. [↓]

Theorem 9.3. Let $n \in \mathbb{N}$. Then, there are infinitely many primes p such that $p \equiv 1 \pmod{n}$. [↓]

Theorem 9.4. Let G be a finite abelian group. Then, there exists an extension $\mathbb{K}/\mathbb{Q}$ such that $G \cong \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$. [↓]

In fact, there is a stronger version of the above theorem, which we do not prove.

Theorem 9.5 (Kronecker–Weber). Let G be a finite abelian group. Then, there exists $n \in \mathbb{N}$ and a tower of fields

$$\mathbb{Q} \subseteq \mathbb{K} \subseteq \mathbb{Q}(\zeta_n)$$

such that $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) = G$.

In other words, every finite abelian Galois extension of $\mathbb{Q}$ is contained in a cyclotomic extension.

§9.2. Cyclic Galois Extensions

Definition 9.6. Let G be a group and $\mathbb{K}$ a field. A character of G in $\mathbb{K}$ is a homomorphism $\chi : G \to \mathbb{K}^\times$.

Remark 9.7. Note that the set of all functions from G to $\mathbb{K}$ is a vector space over $\mathbb{K}$ with point-wise operations. Thus, we can talk about linear independence of characters.

Theorem 9.8 (Dedekind). Let $\chi_1, \ldots, \chi_n : G \to \mathbb{K}^\times$ be distinct characters. Then, $\chi_1, \ldots, \chi_n$ are linearly independent. [↓]

Lemma 9.9. Let $n \in \mathbb{N}$ and $\mathbb{F}$ be a field containing a primitive n-th root of unity ζ. Suppose that $\mathbb{E}/\mathbb{F}$ is a cyclic Galois extension of degree n with $G := \mathrm{Gal}(\mathbb{E}/\mathbb{F}) = \langle \sigma \rangle$. Then, ζ is an eigenvalue of the $\mathbb{F}$-linear map σ. [↓]

Theorem 9.10. Let $\mathbb{E}/\mathbb{F}$ be a cyclic Galois extension of degree n. Then, there exists $a \in \mathbb{E}$ such that $\mathbb{E} = \mathbb{F}(a)$ and $a^n \in \mathbb{F}$. [↓]

Proposition 9.11. Let $\mathbb{E}/\mathbb{F}$ be a cyclic Galois extension of degree n where $\mathbb{F}$ has a primitive n-th root of unity. Let $\mathbb{E} = \mathbb{F}(a)$, where $a \in \mathbb{E}$ is such that $a^n \in \mathbb{F}$, in view of Theorem 9.10.

Then, the intermediate subfields of $\mathbb{E}/\mathbb{F}$ are $\mathbb{F}(a^d)$ where d is a divisor of n. [↓]

Theorem 9.12 (Artin-Schreier)**.** Let $\mathbb{F}$ be a field of prime characteristic p.

1. Let $\mathbb{E}/\mathbb{F}$ be a finite Galois extension of degree p. Then, $\mathbb{E} = \mathbb{F}(a)$ for some $a \in \mathbb{E}$ such that $a^p - a \in \mathbb{F}$.
2. Let $b \in \mathbb{F}$ be such that $f(x) := x^p - x - b \in \mathbb{F}[x]$ has no root in $\mathbb{F}$. Then, $f(x)$ is irreducible over $\mathbb{F}$ and a splitting field of $f(x)$ over $\mathbb{F}$ is cyclic of degree p. [↓]

Chapter 10

Some Group Theory

Although already mentioned in Chapter 0, we repeat: $[n] := \{1, \ldots, n\}$ for $n \in \mathbb{N}$.

§10.1. Solvable groups

Definition 10.1. Let G be a group. A sequence of subgroups

$$1 = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_s = G$$

is called a normal series for G if G_i is a normal subgroup of G_{i-1} for $i = 1, \ldots, s$. The length of this series is s. The normal series is called abelian (resp., cyclic) if the quotients G_i/G_{i-1} are abelian (resp., cyclic) for $i = 1, \ldots, s$.

A group having an abelian series is called a solvable group.

Remark 10.2. Note that the length is the number of inclusions, whereas there are $s + 1$ subgroups in the above series (including 1 and G).

Example 10.3 (Solvable groups)**.**

1. Any abelian group G is solvable with

$$1 \trianglelefteq G$$

being an abelian series. In particular, so are S_1 and S_2.

2. S_3 is solvable since
$$1 \trianglelefteq A_3 \trianglelefteq S_3$$
is an abelian series. Indeed, A_3 is normal in S_3 since it has index 2 and the quotient has order 2 and hence, is abelian. Since A_3 has order 3, it is abelian; thus, $1 \trianglelefteq A_3$ and $A_3/1$ is abelian.

3. S_4 is solvable as well with
$$1 \trianglelefteq V_4 \trianglelefteq A_4 \trianglelefteq S_4$$
being an abelian series. Here, $V_4 = \{1, (12)(34), (13)(24), (14)(23)\}$.

   We only need to verify that $V_4 \trianglelefteq A_4$. (The quotient will be abelian since it has order 3.) That $V_4 \leq A_4$ is clear since all the permutations are indeed even. Now, from the cycle type, we see that V_4 is actually normal in S_4 itself.

4. As we shall see later, S_n is not solvable for $n \geq 5$.

Proposition 10.4. Any group with order p^n is solvable, where p is a prime and $n \in \mathbb{N}_0$. [↓]

Definition 10.5. Let G be a group. The commutator of $g, h \in G$ is defined as
$$[g, h] := g^{-1}h^{-1}gh.$$
The derived subgroup of G denoted by G' or $G^{(1)}$ or $[G, G]$ is the subgroup generated by all the commutators in G. The k-th derived subgroup of G is defined inductively as $G^{(k)} = \left(G^{(k-1)}\right)'$ for $k \geq 2$.

Remark 10.6.

1. $[g, h] = 1$ iff g and h commute.
2. As a result, $G' = 1$ iff G is abelian.
3. If $H \leq G$, then $H' \leq G'$.

4. In general, the derived subgroup is *generated* by commutators and is not equal to the set of commutators itself. (The smallest example is a certain group of order 96.)

Definition 10.7. Let G be a group and $a \in G$. Then, the inner automorphism i_a is the automorphism $i_a \in \mathrm{Aut}(G)$ defined as

$$i_a(g) := a^{-1}ga.$$

Clearly, i_a is a homomorphism. To see that it an isomorphism, note that $i_{a^{-1}}$ is an inverse.

Proposition 10.8. Let $f : G \to H$ be a homomorphism of groups and $s \in \mathbb{N}$.

1. $f(G^{(s)}) \leq H^{(s)}$. If f is onto, then $f(G^{(s)}) = H^{(s)}$.
2. If $K \trianglelefteq G$, then $K' \trianglelefteq G$. In particular, $G' \trianglelefteq G$.
3. If $K \trianglelefteq G$, then G/K is abelian iff $G' \leq K$. [↓]

Remark 10.9. The last point essentially says that the derived subgroup is the smallest subgroup one must quotient by, to get an abelian group.

Proposition 10.10. A group G is solvable iff $G^{(s)} = 1$ for some $s \in \mathbb{N}$. [↓]

Proposition 10.11. Let $K \trianglelefteq G$ be groups. Then,

$$\left(\frac{G}{K}\right)^{(s)} = \frac{\langle G^{(s)}, K\rangle}{K}.$$

[↓]

Proposition 10.12. Let G and H be groups.

1. If G is solvable and there is an injection $i : H \to G$, then H is solvable. In particular, subgroups of solvable groups are solvable.
2. If G is solvable and there is a surjection $f : G \to H$, then H is solvable. In particular, quotients of solvable groups are solvable.
3. If $K \trianglelefteq G$ is such that K and G/K are solvable, then G is solvable. [↓]

Proposition 10.13. Let G be a finite solvable group. Then, there exists a normal series

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_s = G$$

such that G_i/G_{i-1} is cyclic of prime order for all $i = 1, \ldots, s$. [↓]

§10.2. Some results about Symmetric Groups

Lemma 10.14. For $n \geq 3$, A_n is generated by 3-cycles. If $n \geq 5$, then all the 3-cycles are conjugates in A_n. [↓]

Theorem 10.15. The groups S_n and A_n are not solvable for $n \geq 5$. [↓]

Theorem 10.16. The alternating group A_n is simple for $n \geq 5$. [↓]

§§10.2.1. Generators of Symmetric Groups

Of course, everyone knows the first one.

Theorem 10.17. For $n \geq 2$, S_n is generated by its transpositions.

Theorem 10.18. For $n \geq 2$, S_n is generated by the $n - 1$ transpositions

$$(12), (13), \ldots, (1n).$$

[↓]

Theorem 10.19. For $n \geq 2$, S_n is generated by the $n-1$ transpositions

$$(1\ 2), (2\ 3), \ldots, (n-1\ n).$$

[↓]

Theorem 10.20. For $n \geq 2$, S_n is generated by the transposition (12) and the n-cycle $(12\ldots n)$. [↓]

Corollary 10.21. Let $p \geq 3$ be a prime. Then, S_p is generated by any pair of transposition and p-cycle. [↓]

Remark 10.22. In general, it is not true that any transposition and n-cycle generates S_n. For example, (12) and (1234) do not generate S_4. To see this, consider the dihedral group D_8 of order 8 as a subgroup of S_4 by numbering the vertices of a square as $1, 2, 3, 4$. Then, $(12), (1234) \in D_8 \subsetneq S_4$ and thus, $\langle (12), (1234) \rangle \subseteq D_8 \subsetneq S_4$.

Chapter 11

Galois Groups of Composite Extensions

In this section, $\mathbb{F}$ be a field and $\overline{\mathbb{F}}$ some fixed algebraic closure of $\mathbb{F}$. Whenever we talk about extensions $\mathbb{E}/\mathbb{F}$ and $\mathbb{K}/\mathbb{F}$, it will be understood that $\mathbb{E}, \mathbb{K} \subseteq \overline{\mathbb{F}}$. In particular, it makes sense to talk about $\mathbb{E}\mathbb{K}$ and $\mathbb{E} \cap \mathbb{K}$.

Proposition 11.1. If $\mathbb{E}/\mathbb{F}$ is a Galois extension and $\mathbb{K}/\mathbb{F}$ is a field extension, then $\mathbb{E}\mathbb{K}/\mathbb{K}$ is Galois. Moreover, if $\mathbb{K}/\mathbb{F}$ is also Galois, then $\mathbb{E}\mathbb{K}/\mathbb{F}$ and $(\mathbb{E} \cap \mathbb{K})/\mathbb{F}$ are Galois. [↓]

$$\begin{tikzcd}
& \overline{\mathbb{F}} \arrow[d, no head] & \\
& \mathbb{E}\mathbb{K} \arrow[dl, no head] \arrow[dr, no head] & \\
\mathbb{E} \arrow[dr, no head] \arrow[ddr, dashed, no head, bend right, "\text{Galois}"'] & & \mathbb{K} \arrow[dl, no head] \\
& \mathbb{E} \cap \mathbb{K} \arrow[d, no head] & \\
& \mathbb{F} &
\end{tikzcd}$$

Proposition 11.2. Let $\mathbb{E}/\mathbb{F}$ be a finite Galois extension and $\mathbb{K}/\mathbb{F}$ be a field extension (with $\mathbb{E}, \mathbb{K} \subseteq \overline{\mathbb{F}}$). Then, the map

$$\psi : \mathrm{Gal}(\mathbb{E}\mathbb{K}/\mathbb{K}) \to \mathrm{Gal}(\mathbb{E}/\mathbb{F})$$

defined by $\psi(\sigma) = \sigma|_{\mathbb{E}}$ is injective and induces an isomorphism

$$\mathrm{Gal}(\mathbb{E}\mathbb{K}/\mathbb{K}) \cong \mathrm{Gal}(\mathbb{E}/\mathbb{E} \cap \mathbb{K}).$$

[↓]

$$\begin{tikzcd}[arrows=dash]
 & \mathbb{E}\mathbb{K} \arrow[dl] \arrow[dr] & \\
\mathbb{E} \arrow[dr] & & \mathbb{K} \arrow[dl] \\
 & \mathbb{E} \cap \mathbb{K} &
\end{tikzcd}$$

Corollary 11.3. Let $\mathbb{E}/\mathbb{F}$ be a finite Galois extension and $\mathbb{K}/\mathbb{F}$ any field extension. Then,

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

In particular, $[\mathbb{E}\mathbb{K} : \mathbb{F}] = [\mathbb{E} : \mathbb{F}][\mathbb{K} : \mathbb{F}]$ iff $\mathbb{E} \cap \mathbb{K} = \mathbb{F}$. [↓]

Theorem 11.4. Let $\mathbb{E}/\mathbb{F}$ and $\mathbb{K}/\mathbb{F}$ be finite Galois extensions with $\mathbb{E}, \mathbb{K} \subseteq \overline{\mathbb{F}}$. Then, the homomorphism

$$\psi : \mathrm{Gal}(\mathbb{E}\mathbb{K}/\mathbb{F}) \to \mathrm{Gal}(\mathbb{E}/\mathbb{F}) \times \mathrm{Gal}(\mathbb{K}/\mathbb{F}), \quad \psi(\sigma) = (\sigma|_{\mathbb{E}}, \sigma|_{\mathbb{K}})$$

is injective. If $\mathbb{E} \cap \mathbb{K} = \mathbb{F}$, then ψ is an isomorphism. [↓]

Chapter 12

Normal Closure of an Algebraic Extension

Definition 12.1. Let $\mathbb{E}/\mathbb{F}$ be an algebraic extension and $\mathbb{E} \subseteq \overline{\mathbb{F}}$. The normal closure of $\mathbb{E}/\mathbb{F}$ in $\overline{\mathbb{F}}$ is the splitting field $\mathbb{K}$ over $\mathbb{F}$ of the polynomials $\{\operatorname{irr}(\alpha, \mathbb{F}) \mid \alpha \in \mathbb{E}\}$.

Proposition 12.2. Let the notations be as in Definition 12.1. The following are true.

1. $\mathbb{K}$ is a normal extension of $\mathbb{F}$ containing $\mathbb{E}$.
2. Any such normal extension $\mathbb{K}' \subseteq \overline{\mathbb{F}}$ as above contains $\mathbb{K}$.
3. If $\mathbb{E}/\mathbb{F}$ is a finite extension, then so is $\mathbb{K}/\mathbb{F}$.
4. If $\mathbb{E}/\mathbb{F}$ is separable, then $\mathbb{K}/\mathbb{F}$ is Galois.
5. Suppose $\mathbb{E}/\mathbb{F}$ is separable and not normal. Suppose $H \leq \operatorname{Gal}(\mathbb{K}/\mathbb{E}) \leq \operatorname{Gal}(\mathbb{K}/\mathbb{F}) =: G$ is normal in G. Then, $H = 1$. [↓]

Chapter 13

Solvability by Radicals

§13.1. Radical extensions

Definition 13.1. A field extension $\mathbb{K}/\mathbb{F}$ is called a simple radical extension if $\mathbb{K} = \mathbb{F}(a)$ and $a^n \in \mathbb{F}$ for some $a \in \mathbb{K}$ and some $n \in \mathbb{N}$.

We say that $\mathbb{K}/\mathbb{F}$ is a radical extension if there is a sequence of field extensions

$$\mathbb{F} = \mathbb{F}_0 \subseteq \mathbb{F}_1 \subseteq \cdots \subseteq \mathbb{F}_n = \mathbb{K}$$

such that $\mathbb{F}_i/\mathbb{F}_{i-1}$ is a simple radical extension for $i = 1, \ldots, n$.

A polynomial $f(x) \in \mathbb{F}[x]$ is called solvable by radicals over $\mathbb{F}$ if a splitting field of $f(x)$ over $\mathbb{F}$ is contained in a radical extension of $\mathbb{F}$.

Remark 13.2. Note that radical extensions are finite extensions.

Proposition 13.3. Let $\mathbb{F}, \mathbb{E}, \mathbb{K} \subseteq \overline{\mathbb{F}}$ be fields.

1. Suppose $\mathbb{F} \subseteq \mathbb{E} \subseteq \mathbb{K}$. If $\mathbb{K}/\mathbb{E}$ and $\mathbb{E}/\mathbb{F}$ are radical extensions, then so is $\mathbb{K}/\mathbb{F}$.

2. Suppose $\mathbb{F} \subseteq \mathbb{E}, \mathbb{K}$ are such that $\mathbb{E}/\mathbb{F}$ is a radical extension. Then, $\mathbb{E}\mathbb{K}/\mathbb{K}$ is a radical extension. If $\mathbb{K}/\mathbb{F}$ is also a radical extension, then so is $\mathbb{E}\mathbb{K}/\mathbb{F}$.

$$\begin{tikzcd}
 & \mathbb{EK} \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{E} \arrow[dr, dash] & & \mathbb{K} \arrow[dl, dash] \\
 & \mathbb{F} &
\end{tikzcd}$$

[↓]

Proposition 13.4. Let $\mathbb{E}/\mathbb{F}$ be a separable radical extension. Let $\mathbb{K} \subseteq \overline{\mathbb{F}}$ be the smallest Galois extension of $\mathbb{F}$ containing $\mathbb{E}$. Then, $\mathbb{K}$ is a radical extension of $\mathbb{F}$. [↓]

Note that the $\mathbb{K}$ above is simply the normal closure. In particular, such a $\mathbb{K}$ does exist.

§13.2. Solvability Criterion

Theorem 13.5. Let $\mathbb{F}$ be a field with $\operatorname{char}(\mathbb{F}) = 0$. If $f(x) \in \mathbb{F}[x]$ is solvable by radicals, then G_f is a solvable group. [↓]

Example 13.6 (Quintic not solvable by radicals)**.** Suppose $f(x) \in \mathbb{Q}[x]$ is an irreducible quintic (degree five) polynomial which has exactly 3 roots. Let $\mathbb{E} = \mathbb{Q}(\alpha) \subseteq \mathbb{C}$ be a splitting field of $f(x)$ over $\mathbb{Q}$. Any $\sigma \in G_f$ will permute the roots of $f(x)$ and thus, we can identify G_f with a subgroup of S_5.

Then, $G_f \cong \operatorname{Gal}(\mathbb{E}/\mathbb{Q})$ has order divisible by 5. Thus, G_f contains an element of order 5 and thus, a 5-cycle.

On the other hand, the automorphism is a non-trivial automorphism of order 2. Thus, G_f contains a 5-cycle and a transposition. By Corollary 10.21, we have $G_f = S_5$.

By Theorem 10.15, we see that G_f is not solvable and thus, $f(x)$ is not solvable by radicals over $\mathbb{Q}$.

Such an $f(x)$ does indeed exist. For example, consider

$$f(x) := x^5 - 16x + 2.$$

$f(x)$ is irreducible by Eisenstein at 2. Elementary calculus techniques show that $f(x)$ has exactly 3 real roots.

Theorem 13.7. Let $\mathbb{F}$ be a field with $\mathrm{char}(\mathbb{F}) = 0$ and $f(x) \in \mathbb{F}[x]$. If G_f is a solvable group, then $f(x)$ is solvable by radicals. [↓]

Putting Theorem 13.5 and Theorem 13.7 together, we get the following.

Theorem 13.8 (Solvability via radicals)**.** Let $\mathbb{F}$ be a field with $\mathrm{char}(\mathbb{F}) = 0$ and $f(x) \in \mathbb{F}[x]$. $f(x)$ is solvable by radicals if and only if G_f is a solvable group.

Example 13.9. Note that "solvable by radicals" does not necessarily mean that the splitting field is a radical extension.

Consider the polynomial $f(x) = x^3 - 3x + 1 \in \mathbb{Z}[x]$. Reducing modulo 2, we see that polynomial is irreducible since it has no root in $\mathbb{F}_2$. Thus, $f(x)$ is irreducible in $\mathbb{Z}[x]$ and in turn, over $\mathbb{Q}[x]$.

Let $\mathbb{E}$ be a splitting field of $f(x)$ over $\mathbb{Q}$. We show that $\mathbb{E}$ is not a radical extension of $\mathbb{Q}$. Note that $\mathrm{disc}(f(x)) = 81$ and thus, $G_f \cong A_3$, by Example 7.8. Thus, $[\mathbb{E} : \mathbb{Q}] = 3$. Let r be a real root of $f(x)$. Then, we may assume that $\mathbb{E} = \mathbb{Q}(r)$, by consideration of degree. In particular, $\mathbb{E} \subseteq \mathbb{R}$.

Now, for the sake of contradiction, suppose that $\mathbb{E}/\mathbb{Q}$ is a radical extension. Since 3 is prime, there is no proper intermediate subfield of $\mathbb{E}/\mathbb{Q}$. This means that $\mathbb{E}$ itself is a simple radical extension over $\mathbb{Q}$.

Let $\mathbb{E} = \mathbb{Q}(a)$ where $a^n \in \mathbb{Q}$ for some $n \in \mathbb{N}$. Let $g(x) := \mathrm{irr}(a, \mathbb{Q})$. Then, $\mathbb{E}$ is a splitting field of $g(x)$ over $\mathbb{Q}$. Moreover, $g(x) \mid (x^n - a^n) \in \mathbb{Q}[x]$. Thus, every root $b \in \mathbb{E}$ of $g(x)$ satisfies $b^n = a^n$ or $(b/a)^n = 1$. Note that $b, a \in \mathbb{E} \subseteq \mathbb{R}$. But there are at most 2 roots of unity in $\mathbb{R}$ and hence, $g(x)$ has at most 2 roots in $\mathbb{E}$. This is a contradiction since $g(x)$ is a separable cubic and $\mathbb{E}$ is its splitting field.

Chapter 14

Solutions of Cubic and Quartic equations

In this chapter, we assume that $\mathbb{F}$ is a field of characteristic different from 2 or 3. We shall describe algorithms for solving an arbitrary cubic and quartic polynomials over $\mathbb{F}$ in terms of radicals.

§14.1. Cubics

Consider a cubic of the form $f(x) := x^3 + px + q \in \mathbb{F}[x]$. (Note that we can assume any cubic to be of this form since we can always kill the square term by "completing the cube" and then scale to make the leading coefficient unity.)

Now, we introduce two new variables u and v. We will get our roots to be of the form $u + v$.
We expand the equation $f(u + v) = 0$ to get

$$u^3 + v^3 + q + (3uv + p)(u + v) = 0.$$

We now set

$$u^3 + v^3 + q = 0 \tag{14.1}$$

and

$$3uv + p = 0. \tag{14.2}$$

From (14.2), we have $uv = -p/3$. Multiplying (14.1) with u^3 and using $uv = -p/3$ gives

$$u^6 + qu^3 - p^3/27 = 0.$$

The above is a quadratic in u^3. Put $D = -(4p^3 + 27q^2)$. (Recall that this is the discriminant! Example 2.18.) Bu the quadratic formula, we get

$$u^3 = \frac{-q \pm \sqrt{q^2 + (4p^3/27)}}{2} = -\frac{q}{2} \pm \sqrt{-\frac{D}{108}}.$$

By symmetry, in u and v, we set

$$A := -\frac{q}{2} + \sqrt{-\frac{D}{108}} = u^3 \quad \text{and} \quad B := -\frac{q}{2} - \sqrt{-\frac{D}{108}} = v^3.$$

Let ω be a primitive cube root of unity. Thus, we see that the possible values of u and v are given as

$$u = \sqrt[3]{A}, \omega\sqrt[3]{A}, \omega^2\sqrt[3]{A}, \quad \text{and} \quad v = \sqrt[3]{B}, \omega\sqrt[3]{B}, \omega^2\sqrt[3]{B}.$$

However, we cannot choose u and v independently. We need to ensure that $uv = -p/3$.

First, choose cube roots $\sqrt[3]{A}$ and $\sqrt[3]{B}$ such that $\sqrt[3]{A}\sqrt[3]{B} = -p/3$. (The reason we can do this is because $AB = -p^3/27$.)

Then, the three roots of $f(x)$ are seen to be

$$\sqrt[3]{A} + \sqrt[3]{B}, \omega\sqrt[3]{A} + \omega^2\sqrt[3]{B}, \omega^2\sqrt[3]{A} + \omega\sqrt[3]{B}.$$

Example 14.1 (Negative discriminant)**.** Suppose $f(x) = x^3 + px + q \in \mathbb{R}[x]$ with $\operatorname{disc}(f(x)) < 0$. In this case, A and B are real. Moreover, we can choose the cube roots of A and B to be real. We get the roots as

$$\begin{aligned} r_1 &= \sqrt[3]{A} + \sqrt[3]{B} \in \mathbb{R}, \\ r_2 &= -\frac{\sqrt[3]{A} + \sqrt[3]{B}}{2} + \iota\sqrt{3}\left(\frac{\sqrt[3]{A} - \sqrt[3]{B}}{2}\right), \\ r_3 &= \overline{r_2}. \end{aligned}$$

Note that the roots are distinct. This can be seen by either observing that $A \neq B$ or that $\operatorname{disc}(f(x)) \neq 0$.

Example 14.2 (Positive discriminant)**.** Suppose $f(x) = x^3 + px + q \in \mathbb{R}[x]$ with $\operatorname{disc}(f(x)) > 0$. Then, we have

$$A = -\frac{q}{2} + \iota\sqrt{\frac{D}{108}} \quad \text{and} \quad B = \overline{A}.$$

Let $a + \iota b$ be a cube root of $\sqrt[3]{A}$. Then, since $B = \overline{A}$, we know the cube roots of B. Since we wish the product to be $-p/3 \in \mathbb{R}$, we pick $\sqrt[3]{B} = a - \iota b$. Thus, the roots are

$$\begin{aligned} r_1 &= 2a, \\ r_2 &= -a - b\sqrt{3}, \\ r_3 &= -a + b\sqrt{3}. \end{aligned}$$

In particular, all the roots are real and distinct.

§14.2. Quartics

As before, it suffices to consider a polynomial of the form

$$g(y) = y^4 + py^2 + qy + r \in \mathbb{F}[y].$$

Let $r_1, \ldots, r_4$ be the roots of $g(y)$. Consider the following quantities

$$\theta_1 := (r_1 + r_2)(r_3 + r_4),\ \theta_2 := (r_1 + r_3)(r_2 + r_4),\ \theta_3 := (r_1 + r_4)(r_2 + r_3).$$

Now, note that we compute the elementary symmetric polynomials in θ_i since these will be elementary symmetric polynomials in r_j and we already know those in terms of p, q, r. In particular, we may compute the monic cubic polynomial having $\theta_1, \theta_2, \theta_3$ as roots. This is called the resolvent cubic of $g(y)$. This turns out to be

$$h(x) := x^3 - 2px^2 + (p^2 - 4r)x + q^2.$$

Using the relation $r_1 + r_2 + r_3 + r_4 = 0$, we get

$$(r_1 + r_2)^2 = (r_3 + r_4)^2 = -\theta_1$$

and so on. Fixing a square root for each $-\theta_i$, we get.

$$\begin{aligned} r_1 + r_2 &= \sqrt{-\theta_1}, & r_3 + r_4 &= -\sqrt{-\theta_1}, \\ r_1 + r_3 &= \sqrt{-\theta_2}, & r_2 + r_4 &= -\sqrt{-\theta_2}, \\ r_1 + r_4 &= \sqrt{-\theta_3}, & r_2 + r_3 &= -\sqrt{-\theta_3}. \end{aligned}$$

One can show that the product of the elements on the left is $-q$, i.e., the choice of square roots must satisfy

$$\sqrt{-\theta_1}\sqrt{-\theta_2}\sqrt{-\theta_3} = -q.$$

Thus, two of the square roots determine the third. Now, using the relation $r_2 + r_3 + r_4 = -r_1$, adding the four equations on the left lead to the following solutions.

$$\begin{aligned} 2r_1 &= \sqrt{-\theta_1} + \sqrt{-\theta_2} + \sqrt{-\theta_3}, \\ 2r_2 &= \sqrt{-\theta_1} - \sqrt{-\theta_2} - \sqrt{-\theta_3}, \\ 2r_3 &= -\sqrt{-\theta_1} + \sqrt{-\theta_2} - \sqrt{-\theta_3}, \\ 2r_4 &= -\sqrt{-\theta_1} - \sqrt{-\theta_2} + \sqrt{-\theta_3}. \end{aligned}$$

Thus, the roots of the resolvent cubic determine the roots of the quartic.

Proposition 14.3. The discriminants of the quartic $g(y)$ and its resolvent $h(x)$ are equal.

Proof. The differences of roots are

$$\theta_1 - \theta_2 = (r_2 - r_3)(r_4 - r_1),\ \theta_1 - \theta_3 = (r_2 - r_4)(r_3 - r_1),\ \theta_2 - \theta_3 = (r_3 - r_4)(r_2 - r_1).$$

It is now clear that the discriminants are equal. □

Chapter 15

Proofs

§15.1. Algebraic extensions

Proposition 15.1. 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 15.2. 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 $\mathbb{F}[x] \to \mathbb{F}[\alpha] \subseteq \mathbb{K}$ 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 15.3. 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 15.4. Let $\alpha, \beta \in \mathbb{K} \supseteq \mathbb{F}$ be algebraic over $\mathbb{F}$. Then, there exists an $\mathbb{F}$-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 $f(x) := \operatorname{irr}(\alpha, \mathbb{F})$ and $g(x) := \operatorname{irr}(\beta, \mathbb{F})$. Then,

$$\begin{aligned} 0 &= \psi(0) \\ &= \psi(f(\alpha)) \\ &= f(\psi(\alpha)) \quad \psi \textit{ is an } \mathbb{F}\textit{-isomorphism} \\ &= f(\beta). \end{aligned}$$

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

($\impliedby$) Let $f(x) := \operatorname{irr}(\alpha, \mathbb{F}) = \operatorname{irr}(\beta, \mathbb{F})$.
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 15.5 (Tower law)**.** Let $\mathbb{F} \subseteq \mathbb{E} \subseteq \mathbb{K}$ 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 $\{\alpha_i\}_{i=1}^n \subseteq \mathbb{K}$ be an $\mathbb{E}$-basis and $\{\beta_j\}_{j=1}^m \subseteq \mathbb{E}$ be an $\mathbb{F}$-basis.

Put $B := \{\alpha_i\beta_j : 1 \le i \le n,\ 1 \le j \le m\} \subseteq \mathbb{K}$. 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 $b_{ij} \in \mathbb{F}$. 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 $\{b_{ij} : 1 \le i \le n,\ 1 \le j \le m\} \subseteq \mathbb{F}$ be such that

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

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 15.6. 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

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

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 15.7. Let $\mathbb{F} \subseteq \mathbb{E}$ and $\mathbb{E} \subseteq \mathbb{K}$ be algebraic extensions. Then, $\mathbb{F} \subseteq \mathbb{K}$ 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 $a_i \in \mathbb{E}$ 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.) $\square$

Corollary 15.8. 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. $\mathbb{F} \subseteq \mathbb{A}$ 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 $\alpha\beta^{-1}$. $\square$

Proposition 15.9. 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 over $\mathbb{F}$. 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 the element

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

is a multiplicative inverse of a. $\square$

Proposition 15.10. Let $\mathbb{F} \subseteq \mathbb{E}_1, \mathbb{E}_2 \subseteq \mathbb{K}$ 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 $d := [\mathbb{E}_1 : \mathbb{F}][\mathbb{E}_2 : \mathbb{F}] < \infty$.
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, $\dim_{\mathbb{F}}(\mathbb{L}) \leq mn = d$.

Note that $\mathbb{L}$ is clearly the smallest subring of $\mathbb{K}$ containing $\mathbb{E}_1$ and E_2. 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. Thus, $\mathbb{L} = \mathbb{E}_1\mathbb{E}_2$.

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. $\square$

Theorem 15.11. Let $\mathbb{F}$ be a field and $f(x) \in \mathbb{F}[x]$ be non-constant. Then, there exists a field $\mathbb{K} \supseteq \mathbb{F}$ 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 15.12 (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 Theorem 1.34, there exists a field $\mathbb{F}_1 \supseteq \mathbb{F}$ 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

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

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

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

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

§15.2. Symmetric Polynomials

Theorem 15.13 (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

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

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 $n > 1$ 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

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

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

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. $\square$

Theorem 15.14 (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

$$(1 - u_1 z) \cdots (1 - u_n z) = 1 - \sigma_1 z + \cdots + (-1)^n \sigma_n z^n =: \sigma(z). \tag{15.1}$$

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 (15.1) 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 z^k on both sides gives the result. □

Proposition 15.15. 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 $f(x) = (x - r_1) \cdots (x - r_n)$.

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, $\operatorname{disc}_{\mathbb{K}}(f(x)) = (\det(M))^2 = \det(MM^T)$. As before, let $\sigma_1, \ldots, \sigma_n \in \mathbb{F}[u_1, \ldots, u_n]$ 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

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

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

Note that v_k can be calculated directly in terms of s_i, the coefficients of $f(x)$. Thus, the discriminant does not depend on the choice of the splitting field. □

Proposition 15.16 (Discriminant in terms of derivative)**.** Suppose $f(x) = \prod_{i=1}^n (x - r_i)$. Then, $\mathrm{disc}(f(x)) = (-1)^{\binom{n}{2}} \prod_{i=1}^n f'(r_i)$. [↓]

[↑]

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 15.17.

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 all roots 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, $(c + d\iota)^2 = a + b\iota$. ☐

Theorem 15.18 (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

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

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 $z_r \in \mathbb{C} \subseteq \mathbb{K}$. Thus, $z_r = y_{i(r)j(r)}(r)$ for some pair $(i(r), j(r))$ with $1 \le i(r) \le j(r) \le d$.

Let $P = \{(i, j) : 1 \le i \le j \le d\}$ 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 $c \ne d \in \mathbb{R}$ with

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

Thus,

$$z_c = \alpha_a + \alpha_b + c\alpha_a\alpha_b \quad \text{and} \quad z_d = \alpha_a + \alpha_b + d\alpha_a\alpha_b.$$

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. □

§15.3. Algebraic Closure of a Field

Proposition 15.19. Let $\mathbb{F} \subseteq \mathbb{K}$ 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 15.20. Let $\{\mathbb{F}_i\}_{i\geq 1}$ be a sequence of fields as

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

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 15.21 (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 $\mathbb{F}_1 \supseteq \mathbb{F}$ 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 $\mathbb{E} \supseteq \mathbb{F}$ 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 $\mathfrak{m} \subseteq \mathbb{F}[S]$. 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

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

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 $\mathbb{F}_{n+1} \subseteq \mathbb{K}$, as desired. □

Corollary 15.22 (Existence of Algebraic Closure)**.** Every field $\mathbb{F}$ has an algebraic closure. [↓]

[↑]

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

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

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

Proposition 15.23. Let $\sigma : \mathbb{F} \to \mathbb{L}$ be an embedding of fields where $\mathbb{L}$ is algebraically closed. Let $\alpha \in \mathbb{K} \supseteq \mathbb{F}$ 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

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

[↓]

[↑]

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 $\tau \mapsto \tau(\alpha)$. $\square$

Theorem 15.24. 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 $\sigma(\mathbb{F})$, then τ is an isomorphism extending σ. [↓]

[↑]

Proof. Consider the set

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

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

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

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 $\mathbb{E} := \bigcup_{\alpha \in I} \mathbb{E}_\alpha$ is a subfield of $\mathbb{K}$ 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

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

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

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

Theorem 15.25 (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. [↓]

[↑]

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,

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

(Note that $a \in \mathbb{F}^\times$.) 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. $\square$

§15.4. Separable extensions

Proposition 15.26. 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. $\square$

Proposition 15.27. Let $f(x) \in \mathbb{F}[x]$ be a monic and let $r \in \mathbb{E} \supseteq \mathbb{F}$ 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, $(x-r)^2 \mid f(x)$. $\square$

Theorem 15.28 (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 all roots simple 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. $\square$

Proposition 15.29. 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. [↓]

[↑]

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 Theorem 4.9.

   ($\Leftarrow$) 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 $f(x)$ 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 15.30. Let $\mathbb{F}$ be a field with $\operatorname{char}(\mathbb{F}) = p > 0$. 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 15.31. Let $f(x) \in \mathbb{F}[x]$ be an irreducible polynomial and let $p := \operatorname{char}(\mathbb{F}) > 0$. 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 15.32. 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 15.33. 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 15.34. 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 $\operatorname{char}(\mathbb{F}) = 0$, then all roots are simple.
If $\operatorname{char}(\mathbb{F}) =: p > 0$, then all roots have multiplicity p^n for some $n \in \mathbb{N}_0$. [↓]

[↑]

Proof. Let $\overline{\mathbb{F}} \supseteq \mathbb{F}$ be an algebraic closure of $\mathbb{F}$. Let $\alpha, \beta \in \overline{\mathbb{F}}$ be roots of f. We have an $\mathbb{F}$-isomorphism $\sigma : \mathbb{F}(\alpha) \longrightarrow \mathbb{F}(\beta)$ 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 $\operatorname{char}(\mathbb{F}) = 0$, then $f(x)$ is separable (Proposition 4.10) and thus, all roots are simple.

Now, assume that $\operatorname{char}(\mathbb{F}) =: p > 0$. 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 4.15. Then, $f(x) = h(x^{p^{n+1}})$ 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 15.35. 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 $\tau \circ \sigma^{-1} : \sigma(\mathbb{F}) \to \tau(\mathbb{F})$ (cf. Theorem 3.10).

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

$$\begin{tikzcd}
\mathbb{L}' & & \mathbb{L} \arrow[ll, "\lambda"'] \\
\widetilde{\tau}(\mathbb{E}) \arrow[u, dash] & \mathbb{E} \arrow[l, "\widetilde{\tau} \in S_\tau"'] \arrow[r, "\widetilde{\sigma} \in S_\sigma"] & \widetilde{\sigma}(\mathbb{E}) \arrow[u, dash] \\
\tau(\mathbb{F}) \arrow[u, dash] & \mathbb{F} \arrow[l, "\tau"'] \arrow[r, "\sigma"] & \sigma(\mathbb{F}) \arrow[u, dash]
\end{tikzcd}$$

[↑]

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 15.36 (Tower Law for separable degree)**.** Let $\mathbb{F} \subseteq \mathbb{E} \subseteq \mathbb{K}$ 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 σ. Then, each σ_i has extensions $\sigma_i^{(1)}, \ldots, \sigma_i^{(n)} : \mathbb{K} \to \mathbb{L}$. Note that $\{\sigma_i^{(j)} : 1 \le i \le m,\ 1 \le j \le n\}$ has cardinality mn. (All the extensions obtained are distinct.)

Clearly, any embedding $\tau : \mathbb{K} \to \mathbb{L}$ extending σ 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

$$\mathbb{F} \subseteq \mathbb{F}(\alpha_1) \subseteq \mathbb{F}(\alpha_1, \alpha_2) \subseteq \cdots \subseteq \mathbb{F}(\alpha_1, \ldots, \alpha_g).$$

Note that by Proposition 4.25, we know that

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

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

Theorem 15.37. 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 $\mathbb{F}_i$ for $i = 1, \ldots, n$. (Note that $\operatorname{irr}(\alpha_i, \mathbb{F}_i) \mid \operatorname{irr}(\alpha_i, \mathbb{F})$.) 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

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

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 15.38. Let $\mathbb{F} \subseteq \mathbb{E} \subseteq \mathbb{K}$ 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, $\operatorname{irr}(\alpha, \mathbb{E}) \mid \operatorname{irr}(\alpha, \mathbb{F})$. (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 $\operatorname{irr}(\alpha, \mathbb{F})$ has no repeated roots, neither does its factor $\operatorname{irr}(\alpha, \mathbb{E})$. Thus, $\mathbb{K}/\mathbb{E}$ is separable.
Now, let $\beta \in \mathbb{E}$ be arbitrary. Then, $\beta \in \mathbb{K}$ and thus, $\operatorname{irr}(\alpha, \mathbb{F})$ 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 $\operatorname{irr}(\alpha, \mathbb{E}) = a_1 + \cdots + a_n x^{n-1} + x^n \in \mathbb{E}[x]$.

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,

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

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 $\operatorname{irr}(\alpha, \mathbb{F}_n) = \operatorname{irr}(\alpha, \mathbb{E})$, 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 15.39. Let $\mathbb{E}/\mathbb{F}$ be a finite extension. Then, $[\mathbb{E}:\mathbb{F}]_s$ divides $[\mathbb{E}:\mathbb{F}]$. If $\operatorname{char}(\mathbb{F}) =: p > 0$, then quotient $\dfrac{[\mathbb{E}:\mathbb{F}]}{[\mathbb{E}:\mathbb{F}]_s}$ is a power of p. [↓]

[↑]

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

First, suppose that $\mathbb{E} = \mathbb{F}(\alpha)$ for some $\alpha \in \mathbb{E}$. Let $p(x) := \operatorname{irr}(\alpha, \mathbb{F})$ 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. □

§15.5. Finite fields

Theorem 15.40 (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 $p := \operatorname{char}(\mathbb{K})$. 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 15.41 (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, $[\mathbb{F}(\alpha) : \mathbb{F}_p] = d$ and hence, $\alpha \in \mathbb{F}(\alpha) = \mathbb{F}_{p^d}$. □

Proposition 15.42. The polynomial $f(x) := x^4 + 1$ is irreducible in $\mathbb{Z}[x]$ but it is reducible in $\mathbb{F}_p$ for every prime p. [↓]

[↑]

Proof. For irreducibility over $\mathbb{Z}[x]$, note that

$$f(x+1) = x^4 + 4x^3 + 6x^2 + 4x + 2$$

is Eisenstein at the prime 2.

Now, let p be a prime. If $p = 2$, the we have $x^4 + 1 = (x+1)^4$. Let $p > 2$ be an odd prime. Then, $p^2 \equiv 1 \pmod 8$. Hence, we have

$$x^4 + 1 \mid x^8 - 1 \mid x^{p^2-1} - 1 \mid x^{p^2} - x.$$

For the sake of contradiction, assume that $x^4 + 1$ is irreducible and let $\alpha \in \overline{\mathbb{F}}_p$ be a root. Then, $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = \deg(x^4 + 1) = 4$.

But α is clearly contained in the splitting of $x^{p^2} - x$ over $\mathbb{F}_p$, which is $\mathbb{F}_{p^2} \subseteq \overline{\mathbb{F}}_p$ and so, α is contained in a degree 2 extension. This is a contradiction. □

Lemma 15.43. If $m \mid n$, then $x^{q^m} - x \mid x^{q^n} - x$ in $\mathbb{F}_q[x]$. [↓]

[↑]

Proof. Fix an algebraic closure $\overline{\mathbb{F}}_q$. Since $f(x) := x^{q^m} - x$ is separable, it suffices to show that every root of $f(x)$ is also a root of $x^{q^n} - x =: g(x)$. (Recall Proposition 0.20.)

To this end, let α be a root of $f(x)$. We have

$$\alpha^{q^m} = \alpha.$$

Now raise both sides to the power q^m to obtain

$$\alpha^{q^{2m}} = \alpha^{q^m} = \alpha.$$

Continue repeatedly to get

$$\alpha^{q^{km}} = \alpha$$

for all $k \in \mathbb{N}$. In particular, for $k = n/m$, the above is true. This gives us that $g(\alpha) = 0$, as desired. $\square$

Lemma 15.44. Let $f(x) \in \mathbb{F}_q[x]$ be a monic irreducible polynomial.
Then, $f(x) \mid x^{q^n} - x$ iff $\deg(f(x)) \mid n$. [↓]

[↑]

Proof. ($\Rightarrow$) Suppose $f(x) \mid x^{q^n} - x$. Then, $\mathbb{F}_{q^n}$ contains all the roots of $f(x)$. Let $\alpha \in \overline{\mathbb{F}}_q$ be a root of $f(x)$. Thus, $\alpha \in \mathbb{F}_{q^n}$. Considering the tower $\mathbb{F}_q \subseteq \mathbb{F}_q(\alpha) \subseteq \mathbb{F}_{q^n}$ shows that $\deg(f(x)) = [\mathbb{F}_q(\alpha) : \mathbb{F}_q]$ divides $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$.

($\Leftarrow$) Let $d := \deg(f(x)) \mid n$. Fix an algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$. We show that every root of $f(x)$ in $\overline{\mathbb{F}}_q$ satisfies $x^{q^d} - x$. Since this divides $x^{q^n} - x$, we would be done.

Let $\alpha \in \overline{\mathbb{F}}_q$ be a root of $f(x)$. Then, $[\mathbb{F}(\alpha) : \mathbb{F}] = d$ and thus, by Theorem 5.4, we have that

$$\mathbb{F}(\alpha) = \mathbb{F}_{q^d} = \{\beta^{q^d} - \beta = 0 \mid \beta \in \overline{\mathbb{F}}_q\}.$$

(Note that any algebraic closure $\overline{\mathbb{F}}_q$ is also an algebraic closure of $\mathbb{F}_p \subseteq \mathbb{F}_q$.)

Thus, α satisfies $x^{q^d} - x$, as desired. $\square$

Theorem 15.45 (Gauss)**.** The number of irreducible polynomials of degree n over $\mathbb{F}_q$ is given by

$$N_q(n) = \frac{1}{n}\sum_{d|n} \mu(d) q^{n/d}.$$

[↓]

[↑]

Proof. Note that $x^{q^n} - x$ is a separable polynomial. By Lemma 5.9, we see that

$$x^{q^n} - x = \prod_{d|n} f_1^{(d)}(x) \cdots f_{N_q(d)}^{(d)}(x),$$

where $f_1^{(d)}(x), \ldots, f_{N_q(d)}^{(d)}(x)$ are all the irreducible monic polynomials of degree d.

Equating the degrees of both sides gives

$$q^n = \sum_{d|n} d N_q(d).$$

Thus, defining $f(n) := q^n$ and $g(n) := nN_q(n)$, we use Möbius inversion formula to conclude that

$$nN_q(n) = \sum_{d|n} \mu(d) q^{n/d}.$$

□

Theorem 15.46 (Primitive Element Theorem)**.** Let $\mathbb{K}/\mathbb{F}$ be a finite extension.

1. There is a primitive element for $\mathbb{K}/\mathbb{F}$ iff the number of intermediate subfields $\mathbb{E}$ such that $\mathbb{F} \subseteq \mathbb{E} \subseteq \mathbb{K}$ is finite.

2. If $\mathbb{K}/\mathbb{F}$ is a separable extension, then it has a primitive element. [↓]

[↑]

Proof. If $\mathbb{F}$ is a finite, then $\mathbb{K}$ is also finite and hence, $\mathbb{K}^\times$ is cyclic by Theorem 0.19. A generator of $\mathbb{K}^\times$ is clearly a primitive element of $\mathbb{K}$ over $\mathbb{F}$. Clearly, there are only finitely many intermediate subfields as well.

Thus, we may assume that $\mathbb{F}$ is infinite.

1. ($\Rightarrow$) Let $\mathbb{K} = \mathbb{F}(\alpha)$ for some $\alpha \in \mathbb{K}$ and let $f(x) := \operatorname{irr}(\alpha, \mathbb{F})$. Let $\mathbb{E}$ be an intermediate subfield.

   Let $h_{\mathbb{E}}(x) := \operatorname{irr}(\alpha, \mathbb{E})$. Then, $h_{\mathbb{E}}(x) \mid f(x)$ for all intermediate subfields $\mathbb{E}$.

   Now, let $\mathbb{E}_0 \subseteq \mathbb{E}$ be the field obtained by adjoining the coefficients of $h(x)$ to $\mathbb{F}$. Then, $\operatorname{irr}(\alpha, \mathbb{E}) = \operatorname{irr}(\alpha, \mathbb{E}_0)$. Note that we also have $\mathbb{K} = \mathbb{E}(\alpha) = \mathbb{E}_0(\alpha)$. Thus, we get that

   $$[\mathbb{K} : \mathbb{E}] = \deg(\operatorname{irr}(\alpha, \mathbb{E})) = \deg(\operatorname{irr}(\alpha, \mathbb{E}_0)) = [\mathbb{K} : \mathbb{E}_0]$$

   and hence, $\mathbb{E} = \mathbb{E}_0$.

   This shows that if $\mathbb{E}$ and $\mathbb{E}'$ are intermediate fields with $h_{\mathbb{E}} = h_{\mathbb{E}'}$, then $\mathbb{E} = \mathbb{E}'$. Since $f(x)$ only has finitely many monic divisors, there are only finitely many intermediate subfields.

   ($\Leftarrow$) Suppose $\mathbb{K}/\mathbb{F}$ has finitely many intermediate subfields. Write $\mathbb{K} = \mathbb{F}(\alpha_1, \ldots, \alpha_n)$.

   Assume that $n = 2$. We show that $\mathbb{K}/\mathbb{F}$ has a primitive element. The general case then follows inductively.
   Thus, we have $\mathbb{K} = \mathbb{F}(\alpha_1, \alpha_2)$.

   For each $c \in \mathbb{F}$, we have the subfield $\mathbb{F}(\alpha_1 + c\alpha_2)$. Since $\mathbb{F}$ is finite and there are only finitely many intermediate subfields, there exist $c \neq d \in \mathbb{F}$ such that

   $$\mathbb{F}(\alpha_1 + c\alpha_2) = \mathbb{F}(\alpha_1 + d\alpha_2) =: \mathbb{L}.$$

   We show that $\mathbb{L} = \mathbb{K}$. (Note that $\mathbb{L}$ is primitive over $\mathbb{F}$.)

   By the above, we see that $(c - d)\alpha_2 \in \mathbb{L}$ and hence, $\alpha_2 \in \mathbb{L}$. In turn, $\alpha_1 \in \mathbb{L}$. Thus,

   $$\mathbb{L} \subseteq \mathbb{K} = \mathbb{F}(\alpha_1, \alpha_2) \subseteq \mathbb{L}$$

   and hence, we have equality.

2. Now, assume that $\mathbb{K}/\mathbb{F}$ is a finite separable extension. By the same inductive argument as earlier, it is sufficient to prove the existence of a primitive element when $\mathbb{K} = \mathbb{F}(\alpha, \beta)$ for some $\alpha, \beta \in \mathbb{K}$. Fix an algebraic closure $\overline{\mathbb{F}}$ of $\mathbb{F}$.

   As earlier, we show that there exists $c \in \mathbb{F}$ such that

   $$\mathbb{K} = \mathbb{F}(\alpha + c\beta). \tag{$*$}$$

   We now seek a condition on c that implies ($*$). Let $n := [\mathbb{K} : \mathbb{F}] = [\mathbb{K} : \mathbb{F}]_s$. (Equality by Theorem 4.28.)

Then, by definition of separable degree, there exist n embeddings $\sigma_1, \ldots, \sigma_n : \mathbb{K} \to \overline{\mathbb{F}}$ extending the natural inclusion.

Now, if $c \in \mathbb{F}$ is such that the conjugates $\sigma_i(\alpha + c\beta)$ are distinct for $i = 1, \ldots, n$, then this means that

$$n = [\mathbb{K} : \mathbb{F}]_s \geq [\mathbb{F}(\alpha + c\beta) : \mathbb{F}]_s \geq n = [\mathbb{K} : \mathbb{F}]$$

and thus, ($*$) holds. Our job now is to find such a $c \in \mathbb{F}$ for which the conjugates are distinct.

Let $c \in \mathbb{F}$ be arbitrary. Then, $\sigma_i(\alpha + c\beta) = \sigma_i(\alpha) + c\sigma_i(\beta)$. Consider the polynomial

$$f(x) := \prod_{1 \leq i < j \leq n} \left[(\sigma_i(\alpha) - \sigma_j(\alpha)) + x(\sigma_i(\beta) - \sigma_j(\beta))\right] \in \mathbb{K}[x].$$

Thus, the conjugates of c are distinct iff $f(c) \neq 0$. Note that if σ_i and σ_j agree on α and β, then $\sigma_i = \sigma_j$ since $\mathbb{K} = \mathbb{F}(\alpha, \beta)$. Thus, $f(x)$ above is not the zero polynomial. But since $\mathbb{F}$ is infinite, there exists $c \in \mathbb{F}$ such that $f(c) \neq 0$ and thus, we are done. □

§15.6. Normal extensions

Proposition 15.47. Let $\mathbb{F}$ be a field, and $\mathcal{F} \subseteq \mathbb{F}[x]$ be a family of separable polynomials. Let $\mathbb{E} \subseteq \overline{\mathbb{F}}$ be the splitting field of $\mathcal{F}$ over $\mathbb{F}$. Then, $\mathbb{E}/\mathbb{F}$ is a separable extension. [↓]

[↑]

Proof. Let $a \in \mathbb{E} = \mathbb{F}(A)$ where A is as in Remark 6.3. By Corollary 0.16, there is a finite set $\{a_1, \ldots, a_n\} \subseteq A$ such that $a \in \mathbb{F}(a_1, \ldots, a_n)$. Since each a_i is a root of a separable, it is separable. By applying Corollary 4.29 (repeatedly), we see that $\mathbb{F}(a_1, \ldots, a_n)/\mathbb{F}$ is a separable extension and thus, a is separable over $\mathbb{F}$. □

Lemma 15.48. Let $\mathbb{E}/\mathbb{F}$ be an algebraic extension. Let $\sigma : \mathbb{E} \to \mathbb{E}$ be an $\mathbb{F}$-embedding. Then, σ is an automorphism of $\mathbb{E}$. [↓]

[↑]

Proof. We only need to prove that σ is onto. Let $\alpha \in \mathbb{E}$ be arbitrary. Put $p(x) := \operatorname{irr}(\alpha, \mathbb{F})$. Let $\mathbb{K} \subseteq \mathbb{E}$ be the subfield generated by the roots of $p(x)$ in $\mathbb{E}$. Then, $\mathbb{K}$ is a finite dimensional vector space over $\mathbb{F}$ and $\alpha \in \mathbb{K}$. Since σ is an $\mathbb{F}$-embedding, it maps roots of $p(x)$ to roots of $p(x)$. Thus, $\sigma(\mathbb{K}) \subseteq \mathbb{K}$.

But σ is an $\mathbb{F}$-linear map and $\mathbb{K}$ is a finite dimensional $\mathbb{F}$-vector space. Thus, $\sigma|_{\mathbb{K}}$ is onto and contains α in its image. □

Theorem 15.49. Let $\mathbb{F}$ be a field and fix an algebraic closure $\overline{\mathbb{F}}$ of $\mathbb{F}$. Let $\mathbb{F} \subseteq \mathbb{E} \subseteq \overline{\mathbb{F}}$ be fields. Then, the following are equivalent:

1. Every $\mathbb{F}$-embedding $\sigma : \mathbb{E} \to \overline{\mathbb{F}}$ is an automorphism of $\mathbb{E}$.
2. $\mathbb{E}$ is a splitting field of a family of polynomials in $\mathbb{F}[x]$.
3. $\mathbb{E}/\mathbb{F}$ is a normal extension. [↓]

[↑]

Proof. 1 $\Rightarrow$ 2: Let $a \in E$ and $p_a(x) = \operatorname{irr}(a, \mathbb{F})$. If $b \in \overline{\mathbb{F}}$ is a root of $p_a(x)$, then there exists an $\mathbb{F}$-isomorphism $\mathbb{F}(a) \to \overline{\mathbb{F}}$ with $a \mapsto b$. Extend this to a map $\sigma : \mathbb{E} \to \overline{\mathbb{F}}$. By hypothesis, we have $\mathbb{E} = \sigma(\mathbb{E}) \ni b$. Thus, $\mathbb{E}$ is a splitting field of the family $\{p_a(x)\}_{a \in E}$.

2 $\Rightarrow$ 3: Let $\mathbb{E}$ be a spitting field of $\{p_i(x)\}_{i \in I} \subseteq \mathbb{F}[x]$ over $\mathbb{F}$. Let $f(x) \in \mathbb{F}[x]$ be an irreducible polynomial having a root $a \in \mathbb{E}$. Let $b \in \overline{\mathbb{F}}$ be any root of $f(x)$. There exists an $\mathbb{F}$-embedding $\mathbb{F}(a) \to \overline{\mathbb{F}}$ with $a \mapsto b$. Extend this to an $\mathbb{F}$-embedding $\sigma : \mathbb{E} \to \overline{\mathbb{F}}$. Since σ fixes $\mathbb{F}$, it maps roots of $p_i(x)$ to its roots for all $i \in I$. Since $\mathbb{E}$ is generated by these roots, we see that $\sigma(\mathbb{E}) \subseteq \mathbb{E}$ and hence, $b \in \mathbb{E}$.

3 $\Rightarrow$ 1: Let $\sigma : \mathbb{E} \to \overline{\mathbb{F}}$ be an $\mathbb{F}$-embedding. Let $a \in \mathbb{E}$. Then, $p(x) := \operatorname{irr}(\alpha, \mathbb{F})$ splits into linear factors in $\mathbb{E}$. Since $\sigma(a)$ is a root of $p(x)$, we have $\sigma(a) \in \mathbb{E}$. Thus, $\sigma(E) \subseteq E$. By Lemma 6.5, we have that σ is an automorphism. (Note that $\mathbb{E}/\mathbb{F}$ is indeed algebraic since $\mathbb{E} \subseteq \overline{\mathbb{F}}$.) □

Proposition 15.50. Let $\mathbb{F} \subseteq \mathbb{E}_1, \mathbb{E}_2 \subseteq \mathbb{K}$ be fields. Suppose that $\mathbb{E}_i/\mathbb{F}$ are normal. Then, so are $\mathbb{E}_1\mathbb{E}_2/\mathbb{F}$ and $(\mathbb{E}_1 \cap \mathbb{E}_2)/\mathbb{F}$. [↓]

[↑]

Proof. Fix an algebraic closure $\overline{\mathbb{F}} \supseteq \mathbb{K}$.

Let $\sigma : \mathbb{E}_1\mathbb{E}_2 \to \overline{\mathbb{F}}$ be an $\mathbb{F}$-embedding. Then, $\sigma(\mathbb{E}_1\mathbb{E}_2) = \sigma(\mathbb{E}_1)\sigma(\mathbb{E}_2) = \mathbb{E}_1\mathbb{E}_2$. Since this is true for all $\mathbb{F}$-embeddings, $\mathbb{E}_1\mathbb{E}_2/\mathbb{F}$ is normal, by Theorem 6.6.

Similar calculation shows the same for intersection as well. □

§15.7. Galois Extensions

Proposition 15.51. Let $\mathbb{E}/\mathbb{F}$ be a finite Galois extension. Then, $|\mathrm{Gal}(\mathbb{E}/\mathbb{F})| = [\mathbb{E} : \mathbb{F}]_s = [\mathbb{E} : \mathbb{F}]$. [↓]

[↑]

Proof. Fix an algebraic closure $\overline{\mathbb{F}} \supseteq \mathbb{E}$.

Let $n := [\mathbb{E} : \mathbb{F}]_s$. Let $\sigma_1, \ldots, \sigma_n : \mathbb{E} \to \overline{\mathbb{F}}$ be $\mathbb{F}$-embeddings. Then, normality of $\mathbb{E}/\mathbb{F}$ implies that $\sigma_i \in \mathrm{Gal}(\mathbb{E}/\mathbb{F})$. Thus, $|\mathrm{Gal}(\mathbb{E}/\mathbb{F})| \geq n$.

On the other hand, if $\sigma \in \mathrm{Gal}(\mathbb{E}/\mathbb{F})$, then σ is an $\mathbb{F}$-embedding of $\mathbb{E}$ into $\overline{\mathbb{F}}$ upon composition by the inclusion. Thus, $\mathrm{Gal}(\mathbb{E}/\mathbb{F}) = \{\sigma_1, \ldots, \sigma_n\}$. □

Proposition 15.52. Let q be a prime power.

The Galois group of the Galois extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ is a cyclic group of order n generated by the Frobenius automorphism $\varphi : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ defined as $a \mapsto a^q$. [↓]

[↑]

Proof. Note that φ does indeed fix $\mathbb{F}_q$ since any $a \in \mathbb{F}_q$ satisfies $x^q - x$ and thus, $\varphi \in \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$.

By Proposition 7.4, we know that $|\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)| = n$. Thus, it suffices to show that φ has order no less than n. Let order of φ be $d \leq n$. Note that

$$\varphi^d(a) = a^{q^d}.$$

Thus, if $\varphi^d = \mathrm{id}_{\mathbb{F}_{q^n}}$, then every element of $\mathbb{F}_{q^n}$ satisfies $x^{q^d} - x$. Thus, the degree is at least q^n. Thus, $q^d \geq q^n$ or $d \geq n$. □

Theorem 15.53. Let $\mathbb{K}/\mathbb{F}$ be a (possibly infinite) Galois extension and put $G = \mathrm{Gal}(\mathbb{K}/\mathbb{F})$. Then,

1. $\mathbb{F} = \mathbb{K}^G$.
2. Let $\mathbb{E} \in \mathcal{I}$. Then, $\mathbb{K}/\mathbb{E}$ is Galois and the map $E \mapsto \mathrm{Gal}(\mathbb{K}/\mathbb{E})$ is an injective map from $\mathcal{I}$ to $\mathcal{G}$. [↓]

[↑]

Proof.

1. Clearly, $\mathbb{F} \subseteq \mathbb{K}^G$, by definition of the Galois group. Only the reverse inclusion needs to be shown.

   Let $a \in \mathbb{K}^G$. Then, a is separable over $\mathbb{F}$ and hence, $[\mathbb{F}(a) : \mathbb{F}]_s = [\mathbb{F}(a) : \mathbb{F}]$, by Corollary 4.29 and Theorem 4.28.

   Thus, if $a \notin \mathbb{F}$, then $[\mathbb{F}(a) : \mathbb{F}] > 1$ and so, there is one non-identity embedding $\mathbb{F}(a) \to \mathbb{K}$, which would necessarily move a. Thus, we must have $a \in \mathbb{F}$.

2. The fact that $\mathbb{K}/\mathbb{E}$ is separable follows from Proposition 4.30 and that it is normal follows from Proposition 6.10. Thus, $\mathbb{K}/\mathbb{E}$ is Galois.

   Now, if $\mathbb{E}, \mathbb{E}' \in \mathcal{I}$ are such that

   $$H := \mathrm{Gal}(\mathbb{K}/\mathbb{E}) = \mathrm{Gal}(\mathbb{K}/\mathbb{E}') =: H',$$

   then the first part gives

   $$\mathbb{E} = \mathbb{K}^H = \mathbb{K}^{H'} = \mathbb{E}'$$

   and thus, the map is an injection. □

Lemma 15.54. Let $\mathbb{E}/\mathbb{F}$ be a separable extension and $n \in \mathbb{N}$. Suppose that for all $\alpha \in \mathbb{E}$, $[\mathbb{F}(\alpha) : \mathbb{F}] \leq n$. Then, $[\mathbb{E} : \mathbb{F}] \leq n$. [↓]

[↑]

Proof. Let $\beta \in \mathbb{E}$ be such that $[\mathbb{F}(\beta) : \mathbb{F}]$ is maximal. Note that $[\mathbb{F}(\beta) : \mathbb{F}] \leq n$, by hypothesis. It suffices to show that $\mathbb{E} = \mathbb{F}(\beta)$.

Suppose that $\mathbb{E} \neq \mathbb{F}(\beta)$. Then, pick $\alpha \in \mathbb{E} \setminus \mathbb{F}(\beta)$. Then, $\mathbb{F}(\alpha, \beta)$ is a separable extension and thus, there exists $\eta \in \mathbb{F}(\alpha, \beta) \subseteq \mathbb{E}$ such that $\mathbb{F}(\alpha, \beta) = \mathbb{F}(\eta)$, by the Primitive Element Theorem.

But this is a contradiction since $\mathbb{F}(\beta) \subsetneq \mathbb{F}(\alpha, \beta) = \mathbb{F}(\eta)$ implies that $[\mathbb{F}(\eta) : \mathbb{F}] > [\mathbb{F}(\beta) : \mathbb{F}]$, contradicting the maximality of β. □

Theorem 15.55 (Artin's Theorem)**.** Let $\mathbb{E}$ be a field and G a finite group of automorphisms of $\mathbb{E}$. Then,

1. $\mathbb{E}/\mathbb{E}^G$ is a *finite* Galois extension.
2. $\mathrm{Gal}(\mathbb{E}/\mathbb{E}^G) = G$.
3. $[\mathbb{E} : \mathbb{E}^G] = |G|$. [↓]

[↑]

Proof. Let $G = \{\sigma_1, \ldots, \sigma_n\}$ and $|G| = n$.

1. Let $\alpha \in \mathbb{E}$. Consider $S = \{\sigma_1(\alpha), \ldots, \sigma_n(\alpha)\}$. Note that the elements written need not all be distinct. Let $r := |S|$. Without loss of generality, assume that $S = \{\sigma_1(\alpha), \ldots, \sigma_r(\alpha)\}$.

   Let $\tau \in G$. Then, $\tau(S) = S$.[3] Thus, $\tau|_S$ is a permutation of S. Consider the polynomial
   $$f(x) := (x - \sigma_1(\alpha)) \cdots (x - \sigma_r(\alpha)).$$

   The coefficients of $f(x)$ are symmetric functions of $\sigma_1(\alpha), \ldots, \sigma_r(\alpha)$ and thus, are fixed by every $\tau \in G$, by the previous observation. Thus, $f(x) \in \mathbb{E}^G[x]$.

   Note that $f(\alpha) = 0$ since one of the σ_i is the identity map. Thus, $\mathrm{irr}(\alpha, \mathbb{E}^G) \mid f(x)$. Note that $f(x)$ has distinct roots, by construction. In particular, α is separable over $\mathbb{E}^G$. Since $\alpha \in \mathbb{E}$ was arbitrary, this tells us that $\mathbb{E}/\mathbb{E}^G$ is separable.

   Moreover, $f(x)$ splits completely in $\mathbb{E}[x]$ and thus, so does $\mathrm{irr}(\alpha, \mathbb{E}^G)$. Thus, $\mathbb{E}/\mathbb{E}^G$ is normal as well and hence, Galois.

   To see that it is finite, note that $[\mathbb{E}^G(\alpha) : \mathbb{E}^G] = r \leq n$ and thus, $[\mathbb{E} : \mathbb{E}^G]$, by Theorem 7.16.

2. Note that $G \subseteq \mathrm{Gal}(\mathbb{E}/\mathbb{E}^G)$. As we noted earlier, $[\mathbb{E} : \mathbb{E}^G] \leq n = |G|$.

[3] Each $\tau\sigma_i$ is an element of G and $\tau\sigma_i(\alpha)$ are distinct for $i = 1, \ldots, r$.

By Proposition 7.4, we have $\mathrm{Gal}(\mathbb{E}/\mathbb{E}^G) = [\mathbb{E} : \mathbb{E}^G]$. Thus, comparing cardinalities gives $G = \mathrm{Gal}(\mathbb{E}/\mathbb{E}^G)$.

3. Follows from the second part. □

Theorem 15.56. Let $\mathbb{K}/\mathbb{F}$ be a (possibly infinite) Galois extension with Galois group G. Let $\mathbb{E}_1$ and $\mathbb{E}_2$ be intermediate subfields of $\mathbb{K}/\mathbb{F}$. Let $H_i := \mathrm{Gal}(\mathbb{K}/\mathbb{E}_i)$ for $i = 1, 2$.Then

$$\mathbb{E}_1\mathbb{E}_2 = \mathbb{K}^{H_1 \cap H_2},\ \mathbb{E}_1 \cap \mathbb{E}_2 = \mathbb{K}^{\langle H_1, H_2\rangle},\ \text{and } \mathbb{E}_1 \subseteq \mathbb{E}_2 \iff H_1 \supseteq H_2.$$

[↓]

[↑]

Proof. The third assertion about the inclusion is obvious since $H_1 \supseteq H_2$ implies that every element fixed by H_2 is also fixed by H_1. Since the extensions are Galois, the fields fields are precisely the $\mathbb{E}_i$, by Theorem 7.12.

Note that $\mathbb{K}/\mathbb{E}_i$ is Galois and thus, $\mathbb{E}_i = \mathbb{K}^{H_i} \subseteq \mathbb{K}^{H_1 \cap H_2}$ for $i = 1, 2$. Thus, $\mathbb{E}_1\mathbb{E}_2 \subseteq \mathbb{K}^{H_1 \cap H_2}$.

On the other hand, if $\sigma \in G$ fixes $\mathbb{E}_1\mathbb{E}_2$, then it fixes both $\mathbb{E}_1$ and $\mathbb{E}_2$. Thus, $\mathrm{Gal}(\mathbb{K}/\mathbb{E}_1\mathbb{E}_2) \subseteq H_1 \cap H_2$ and so, $\mathbb{E}_1\mathbb{E}_2 \supseteq \mathbb{K}^{H_1 \cap H_2}$.

Let $H := \mathrm{Gal}(\mathbb{K}/(\mathbb{E}_1 \cap \mathbb{E}_2))$. Note that $H_1, H_2 \subseteq H$ since every $\sigma \in H_i$ fixes $\mathbb{E}_i$ and thus, fixes the intersection. Thus, $\langle H_1, H_2\rangle \subseteq H$ or $\mathbb{E}_1 \cap \mathbb{E}_2 \subseteq \mathbb{K}^{\langle H_1, H_2\rangle}$.

On the other hand,

$$\mathbb{K}^{\langle H_1, H_2\rangle} \subseteq \mathbb{K}^{H_i} = \mathbb{E}_i$$

and thus,

$$\mathbb{K}^{\langle H_1, H_2\rangle} \subseteq \mathbb{E}_1 \cap \mathbb{E}_2.$$

□

Proposition 15.57. Let $\mathbb{K}/\mathbb{F}$ be a (possibly infinite) Galois extension. Let $\lambda : \mathbb{K} \to \lambda(\mathbb{K})$ be an isomorphism of fields. Then,

1. $\lambda(\mathbb{K})/\lambda(\mathbb{F})$ is a Galois extension.
2. $\mathrm{Gal}(\lambda(\mathbb{K})/\lambda(\mathbb{F})) = \lambda\,\mathrm{Gal}(\mathbb{K}/\mathbb{F})\lambda^{-1} \cong \mathrm{Gal}(\mathbb{K}/\mathbb{F})$. [↓]

[↑]

Proof.

1. We use Theorem 6.6. Since $\mathbb{K}/\mathbb{F}$ is Galois, $\mathbb{K}$ is the splitting field of a family of separable polynomials $\{f_i(x) : i \in I\}$ over $\mathbb{F}$. Then, $\lambda(\mathbb{K})$ is the splitting field of the separable polynomials $\{f_i^\lambda(x) : i \in I\}$ over $\lambda(\mathbb{F})$.
2. Define $\psi : \text{Gal}(\mathbb{K}/\mathbb{F}) \to \text{Gal}(\lambda(\mathbb{K})/\lambda(\mathbb{F}))$ be $\sigma \mapsto \lambda\sigma\lambda^{-1}$. Clearly, ψ is a well-defined homomorphism. It is easy to see that $\tau \mapsto \lambda^{-1}\tau\lambda$ acts as an inverse. $\square$

Theorem 15.58. Let $\mathbb{K}/\mathbb{F}$ be a (possibly infinite) Galois extension. Let $\mathbb{E}$ be an intermediate subfield of $\mathbb{K}/\mathbb{F}$. Then,

1. $\mathbb{E}/\mathbb{F}$ is Galois iff $\text{Gal}(\mathbb{K}/\mathbb{E}) \trianglelefteq \text{Gal}(\mathbb{K}/\mathbb{F})$.
2. If $\mathbb{E}/\mathbb{F}$ is Galois, then

$$\text{Gal}(\mathbb{E}/\mathbb{F}) \cong \frac{\text{Gal}(\mathbb{K}/\mathbb{F})}{\text{Gal}(\mathbb{K}/\mathbb{E})}.$$

[↓]

[↑]

Proof. Let $\mathbb{E}/\mathbb{F}$ be Galois. Define

$$\psi : \text{Gal}(\mathbb{K}/\mathbb{F}) \to \text{Gal}(\mathbb{E}/\mathbb{F})$$
$$\psi(\sigma) = \sigma|_{\mathbb{E}}.$$

Note that the above is well-defined since $\mathbb{E}$ is normal and so, $\sigma|_{\mathbb{E}}$ is indeed an automorphism of $\mathbb{F}$. (That it fixes $\mathbb{F}$ is obvious since σ did so.) Clearly, ψ is a homomorphism. However, now note that

$$\ker(\psi) = \{\sigma \in \text{Gal}(\mathbb{K}/\mathbb{F}) \mid \sigma|_{\mathbb{E}} = \text{id}_{\mathbb{E}}\} = \text{Gal}(\mathbb{K}/\mathbb{E}).$$

Thus, $\text{Gal}(\mathbb{K}/\mathbb{E})$ is a normal subgroup of $\text{Gal}(\mathbb{K}/\mathbb{F})$.

Moreover, since $\mathbb{K}/\mathbb{E}$ is an algebraic and normal extension, every automorphism of $\mathbb{E}$ can indeed be extended to an automorphism of $\mathbb{K}$.[4] Thus, ψ is a surjective map and thus,

$$\text{Gal}(\mathbb{E}/\mathbb{F}) \cong \frac{\text{Gal}(\mathbb{K}/\mathbb{F})}{\text{Gal}(\mathbb{K}/\mathbb{E})}.$$

[4] First extend it to a map $\mathbb{K} \to \overline{\mathbb{E}} \supseteq \mathbb{K}$. Normality then forces the map to be an automorphism of $\mathbb{K}$.

This proves one direction of the first part as well as the second part.

Conversely, suppose that $\mathrm{Gal}(\mathbb{K}/\mathbb{E}) \trianglelefteq \mathrm{Gal}(\mathbb{K}/\mathbb{F})$. Let $\lambda : \mathbb{K} \to \mathbb{K}$ be any $\mathbb{F}$-isomorphism. We first show that $\lambda(\mathbb{E}) = \mathbb{E}$. By Proposition 7.19, we have

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

Thus, $\mathrm{Gal}(\mathbb{K}/\mathbb{E}) = \mathrm{Gal}(\mathbb{K}/\lambda(\mathbb{E}))$. By Theorem 7.12, we get $\mathbb{E} = \lambda(\mathbb{E})$.

Now, to show that $\mathbb{E}/\mathbb{F}$ is normal, let $\sigma : \mathbb{E} \to \overline{\mathbb{F}} \supseteq \mathbb{E}$ be an $\mathbb{F}$-embedding. Then, σ can be extended to an $\mathbb{F}$-embedding $\lambda : \mathbb{K} \to \overline{\mathbb{F}}$. Since $\mathbb{K}/\mathbb{F}$ is normal, we have $\lambda(\mathbb{K}) = \mathbb{K}$. By the above, we have $\sigma(\mathbb{E}) = \lambda(\mathbb{E}) = \mathbb{E}$. □

Theorem 15.59 (Fundamental Theorem of Galois Theory (FTGT))**.** Let $\mathbb{K}/\mathbb{F}$ be a <u>finite</u> Galois extension. Consider the sets

$$\mathcal{I} = \{\mathbb{E} \mid \mathbb{E} \text{ is an intermediate field of } \mathbb{K}/\mathbb{F}\} \quad \text{and} \quad \mathcal{G} = \{H \mid H \leq \mathrm{Gal}(\mathbb{K}/\mathbb{F})\}.$$

1. The maps
$$E \mapsto \mathrm{Gal}(\mathbb{K}/\mathbb{E}) \quad \text{and} \quad H \mapsto \mathbb{K}^H$$
give a one-to-one correspondence between $\mathcal{I}$ and $\mathcal{G}$, called the Galois correspondence. Moreover, these are inclusion reversing.
2. $\mathbb{E}/\mathbb{F}$ is Galois iff $\mathrm{Gal}(\mathbb{K}/\mathbb{E}) \trianglelefteq \mathrm{Gal}(\mathbb{K}/\mathbb{F})$ and in this case,
$$\mathrm{Gal}(\mathbb{E}/\mathbb{F}) \cong \frac{\mathrm{Gal}(\mathbb{K}/\mathbb{F})}{\mathrm{Gal}(\mathbb{K}/\mathbb{E})}.$$
3. $\mathbb{K}/\mathbb{E}$ is always Galois and $|\mathrm{Gal}(\mathbb{K}/\mathbb{E})| = [\mathbb{K} : \mathbb{E}] = \dfrac{[\mathbb{K} : \mathbb{F}]}{[\mathbb{E} : \mathbb{F}]}$.
4. If $\mathbb{E}_1, \mathbb{E}_2 \in \mathcal{I}$ correspond to H_1 and H_2, then $\mathbb{E}_1 \cap \mathbb{E}_2$ corresponds to $\langle H_1, H_2 \rangle$ and $\mathbb{E}_1\mathbb{E}_2$ to $H_1 \cap H_2$.

[↓]

[↑]

Proof. Note that only the first part needs to be proven. We have proven the others (Theorem 7.20, Proposition 7.4, Theorem 7.17).

Let $\Psi : \mathcal{I} \to \mathcal{G}$ be the map $\mathbb{E} \mapsto \mathrm{Gal}(\mathbb{K}/\mathbb{E})$. Let $\Phi : \mathcal{G} \to \mathcal{I}$ denote the map $H \mapsto \mathbb{K}^H$. The fact that these maps reverse inclusion is obvious.

By Theorem 7.12, we know that Ψ is an injection.

Let $H \in \mathcal{G}$. Then, H is finite and is the Galois group of $\mathbb{K}/\mathbb{K}^H$, by Theorem 7.16. Thus, Ψ is onto.

Hence, Ψ is bijective. Therefore, to show that $\Phi = \Psi^{-1}$, it suffices to show only that $\Phi \circ \Psi = \mathrm{id}_{\mathcal{I}}$.

To this end, let $\mathbb{E} \in \mathcal{I}$ be arbitrary. Then, $H := \Psi(\mathbb{K}/\mathbb{E})$ is the Galois group of $\mathbb{K}/\mathbb{E}$. Thus, $\mathbb{E} = \mathbb{K}^H$, by Theorem 7.12. In other words

$$\mathbb{E} = \Phi(\Psi(\mathbb{E})).$$ □

Theorem 15.60 (Fundamental Theorem of Algebra)**.** The field of complex numbers is algebraically closed. [↓]

[↑]

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 $f(x)$ has a root in $\mathbb{C}$.

Let $\mathbb{E}$ denote a splitting field of $f(x)$ over $\mathbb{C}$. Then, it is a splitting of $(x^2+1)f(x)$ over $\mathbb{R}$. It suffices to show that $\mathbb{E} = \mathbb{C}$.

Since $\mathbb{R}$ has no proper odd degree extensions,[5] we see that $2 \mid [\mathbb{E} : \mathbb{R}]$. Thus, $G = \mathrm{Gal}(\mathbb{E}/\mathbb{R})$ has a Sylow-2 subgroup, say S.

Now, if $S \neq G$, then $\mathbb{E} \supseteq \mathbb{E}^S \supsetneq \mathbb{R}$. However, note that

$$[\mathbb{E}^S : \mathbb{R}] = \frac{[\mathbb{E} : \mathbb{R}]}{[\mathbb{E} : \mathbb{E}^S]} = \frac{|G|}{|S|}$$

is odd. But $\mathbb{R}$ has no proper odd degree extension and thus, $S = G$.

Thus, G is a 2-group. (That is, $|G| = 2^n$ for some $n \in \mathbb{N}$.) If $|G| = 2$, then $\mathbb{C} = \mathbb{E}$ are we are done.

Thus, $|G| \geq 4$. Then, $|\mathrm{Gal}(\mathbb{E}/\mathbb{C})| \geq 2$. Let $H \leq \mathrm{Gal}(\mathbb{E}/\mathbb{C})$ be a subgroup of index 2. Then, $[\mathbb{E}^H : \mathbb{C}] = 2$, which is a contradiction, since $\mathbb{C}$ has no quadratic extensions. Thus, $\mathbb{C} = \mathbb{E}$. □

[5] Every odd degree real polynomial has a root in $\mathbb{R}$.

§15.8. Cyclotomic Extensions

Proposition 15.61. Let $\text{char}(\mathbb{F}) = 0$ or $\gcd(\text{char}(\mathbb{F}), n) = 1$ and $f(x) = x^n - 1 \in \mathbb{F}[x]$. Then, G_f is isomorphic to a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$. In particular, G_f is an abelian group and $|G_f| \mid \varphi(n)$. [↓]

[↑]

Proof. As $f(x)$ is separable, it has n distinct roots in $\overline{\mathbb{F}}$. Let $Z = \{z_1, \ldots, z_n\}$ be the set of roots and $\mathbb{E} = \mathbb{F}(z_1, \ldots, z_n)$. By Theorem 0.19, we know that Z is cyclic. The map $\psi : \text{Gal}(\mathbb{E}/\mathbb{F}) \to \text{Aut}(Z)$ given as $\sigma \mapsto \sigma|_Z$ is an injective group homomorphism. Note that $\text{Aut}(Z) \cong (\mathbb{Z}/n\mathbb{Z})^\times$, which proves the result. □

Proposition 15.62. Let $x^n - a = f(x) \in \mathbb{F}[x]$ and suppose $\mathbb{F}$ has n distinct roots of $x^n - 1$. Then, G_f is a cyclic group and $|G_f|$ divides n. [↓]

[↑]

Proof. Let $Z = \{z_1, \ldots, z_n\} \subseteq \mathbb{F}^\times$ be the set of roots of $x^n - 1$. Let r be a root of $f(x)$ in a splitting field $\mathbb{E}$ of $f(x)$. Then, $rz_1, \ldots, rz_n$ are n distinct roots of $f(x)$ and hence, all the roots. Thus, $\mathbb{E} = \mathbb{F}(r)$.

Let $\sigma, \tau \in \text{Gal}(\mathbb{E}/\mathbb{F})$. Then, $\sigma(r) = z_\sigma r$ and $\tau(r) = z_\tau r$ for some $z_\sigma, z_\tau \in Z$. In turn, we see $\sigma\tau(r) = z_\sigma z_\tau r$. Thus, the map

$$\psi : \text{Gal}(\mathbb{E}/\mathbb{F}) \to Z$$

defined by $\psi(\sigma) = z_\sigma$ is a group homomorphism. Moreover it is injective since every $\mathbb{F}$-automorphism of $\mathbb{E} = \mathbb{F}(r)$ is uniquely determined by its action on r. Thus, G_f is isomorphic to a subgroup of Z and we are done. □

Theorem 15.63. Let $n \in \mathbb{N}$ fix a primitive root n-th root of unity $\zeta_n \in \overline{\mathbb{Q}}$ and let $\Phi_n(x) := \text{irr}(\zeta_n, \mathbb{Q})$. Then,

1. $\Phi_n(x) \in \mathbb{Z}[x]$,
2. every primitive n-th root of unity is a root of $\Phi_n(x)$,
3. $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$, and

4. $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$. [↓]

[↑]

Proof. We have $x^n - 1 = \Phi_n(x)h(x)$, where $h(x) \in \mathbb{Q}[x]$ is monic. Thus, by Gauss' Lemma, we have $\Phi_n(x) \in \mathbb{Z}[x]$.

Now, suppose that p is prime not dividing n. We contend that $\Phi(\zeta_n^p) = 0$. Indeed, suppose not. Then, $h(\zeta_n^p) = 0$. Alternately, ζ_n is a root of $h(x^p) \in \mathbb{Q}[x]$. But note that $\Phi_n(x)$ is the minimal polynomial of ζ_n over $\mathbb{Q}$. Thus, we can write

$$h(x^p) = \Phi_n(x)g(x)$$

for monic $g(x) \in \mathbb{Z}[x]$. (Again, by Gauss' Lemma.) Reduce the above equation mod p to get

$$(\bar{h}(x))^p = \bar{\Phi}_n(x)\bar{g}(x).$$

(Note that every element $a \in \mathbb{Z}/p\mathbb{Z}$ satisfies $a^p = a$ and so, $\bar{h}(x^p) = \bar{h}(x))^p$.)

From the above, we see that $\bar{\Phi}_n(x)$ and $\bar{h}(x)$ have a common factor of $\mathbb{F}_p[x]$. ($\mathbb{F}_p[x]$ is a UFD. Factorise both sides of the above equation into primes.)

But this, in turn, implies that

$$x^n - 1 = \bar{\Phi}_n(x)\bar{h}(x)$$

in $\mathbb{F}_p[x]$. In particular, $x^n - 1 \in \mathbb{F}_p[x]$ has repeated roots in $\overline{\mathbb{F}}_p$. This is a contradiction since $x^n - 1$ is separable because $\gcd(n, p) = 1$.

Thus, $\Phi_n(\zeta_n^p) = 0$. Now, if $a \in \mathbb{N}$ is any integer such that $\gcd(a, n) = 1$, we factorise $a = p_1 \cdots p_r$ where $p_1, \ldots, p_r$ are (not necessarily distinct) primes not dividing n. Now, note that $\zeta_n^{p_1}$ is again a primitive root of unity satisfying $\Phi_n(x)$. Thus, the above argument applies and we get $\Phi_n\left((\zeta_n^{p_1})^{p_2}\right) = 0$. Again, since $\gcd(n, p_1p_2) = 1$, we see that $\zeta_n^{p_1p_2}$ is a primitive root and so on. Thus,

$$\Phi_n(\zeta_n^a) = 0$$

for every $a \in \mathbb{N}$ with $\gcd(a, n) = 1$. As a varies over all such integers, we see that every primitive root of unity is a root of $\Phi_n(x)$.

In particular, $\Phi_n(x)$ has $\varphi(n)$ many distinct roots, each with multiplicity 1. Thus, $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$.

By Proposition 8.6, we already know that $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is isomorphic to a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$. By comparing cardinalities, we see that the groups are isomorphic. □

Theorem 15.64. We have $\Phi_1(x) = x - 1$ and

$$\Phi_n(x) = \frac{x^n - 1}{\prod\limits_{\substack{d|n \\ d<n}} \Phi_d(x)}$$

for $n > 1$. [↓]

[↑]

Proof. Clearly, $\Phi_1(x) = x - 1$. Let ζ_n be a primitive n-th root of unity. By Theorem 8.9, we know that the other roots of $\Phi_n(x)$ are ζ_n^i for $i \in \{1, \ldots, n\}$ with $\gcd(i, n) = 1$. Thus,

$$\Phi_n(x) = \prod_{\substack{1 \le i \le n \\ \gcd(n,i)=1}} (x - \zeta_n^i).$$

In turn, we have

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

(Factor the above in $\overline{\mathbb{Q}}$ and note that every root of the left side is a primitive d-th root of unity for some unique d. Since the n-th roots form a group of order n, we must have $d \mid n$. Conversely, every such d-th root is indeed a root of $x^n - 1$ and no two different cyclotomic polynomials have a common root.)

Thus,

$$\Phi_n(x) = \frac{x^n - 1}{\prod\limits_{\substack{d|n \\ d<n}} \Phi_d(x)}. \qquad \square$$

Proposition 15.65. Let p be a prime. Then, $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ is cyclic of order $p - 1$. Consequently, given any divisor $d \mid p - 1$, there is a unique intermediate subfield $\mathbb{E}$ of $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ such that $[\mathbb{E} : \mathbb{Q}] = d$. Equivalently, there is a unique intermediate $\mathbb{E}$ such that $[\mathbb{Q}(\zeta_p) : \mathbb{E}] = \frac{p-1}{d}$. [↓]

[↑]

Proof. Note that $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$, by Theorem 8.9. Since $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ is a finite field, Theorem 0.19 tells us that $\mathbb{F}_p^\times$ is cyclic.

Recall the general fact about finite cyclic groups: given a cyclic group G of order n, there is a unique subgroup of *index* d for every $d \mid n$.

Using this with the Galois correspondence gives the last statement. □

Lemma 15.66. Let p be an odd prime. Then $\mathrm{disc}(\Phi_p(x)) = (-1)^{\binom{p}{2}} p^{p-2}$. [↓]

[↑]

Proof. We shall use Discriminant in terms of derivative. First, we note that we have

$$x^p - 1 = \Phi_p(x)(x-1)$$

and thus,

$$px^{p-1} = \Phi_p'(x)(x-1) + \Phi_p(x).$$

Substituting ζ_n^i above for $i = 1, \ldots, p-1$ gives

$$\frac{p}{\zeta_p^i} = \Phi_p'(\zeta_p^i)(\zeta_p^i - 1).$$

(We have used $\zeta_p^{p-1} = \zeta_p^{-1}$ to simplify the left hand side.)

Thus, we have

$$\prod_{i=1}^{p-1} \Phi_p'(\zeta_p^i) = \prod_{i=1}^{p-1} \frac{p}{\zeta_p^i(\zeta_p^i - 1)}. \tag{$\prod$}$$

Note that we have the following expressions for $\Phi_p(x)$.

$$\begin{aligned}\Phi_p(x) &= (x-\zeta_p)(x-\zeta_p^2)\cdots(x-\zeta_p^{p-1}) \\ &= x^{p-1} + \cdots + x + 1.\end{aligned}$$

Thus,

$$\prod_{i=1}^{p-1} \zeta_p^i = (-1)^{p-1} \quad \text{and} \quad \prod_{i=1}^{p-1}(\zeta_p^i - 1) = (-1)^{p-1}\Phi_p(1).$$

Since p is odd, we have $(-1)^{p-1} = 1$ and putting it back in ($\prod$) gives

$$\prod_{i=1}^{p-1} \Phi_p'(\zeta_p^i) = \frac{p^{p-1}}{1 \cdot \Phi_p(1)} = p^{p-2}.$$

Now using the formula of discriminant in terms of derivatives, we get

$$\operatorname{disc}(\Phi_p(x)) = (-1)^{\binom{p-1}{2}} p^{p-2} = (-1)^{\binom{p}{2}} p^{p-2}. \qquad \square$$

Proposition 15.67. Let p be an odd prime. The field $\mathbb{Q}(\zeta_p)$ contains a unique quadratic extension of $\mathbb{Q}$, namely

$$\mathbb{Q}\left(\sqrt{\operatorname{disc}(\Phi_p(x))}\right) = \mathbb{Q}\left(\sqrt{(-1)^{\binom{p}{2}} p}\right),$$

which is real if $p \equiv 1 \pmod 4$ and (non-real) complex if $p \equiv 3 \pmod 4$. [↓]

[↑]

Proof. The existence and uniqueness of quadratic subfield is given by Proposition 8.13, since $2 \mid p-1$.

Note that $\operatorname{disc}(\Phi_p(x))$ is not a perfect square in $\mathbb{Q}$. On the other hand, by definition of $\operatorname{disc}(\Phi_p(x))$, it is clear that $\operatorname{disc}(\Phi_p(x))$ has a square root in any splitting field of $\Phi_p(x)$. (Recall Remark 2.12.) Thus, $\sqrt{\operatorname{disc}(\Phi_p(x))} \in \mathbb{Q}(\zeta_p) \setminus \mathbb{Q}$.

Hence, this generates the unique quadratic extension. Moreover note that

$$(-1)^{\binom{p}{2}} = (-1)^{\frac{p-1}{2}}.$$

Thus, the square root is real iff $p \equiv 1 \pmod 4$. $\square$

Corollary 15.68. Every quadratic extension of $\mathbb{Q}$ is contained in a cyclotomic extension. [↓]

[↑]

Proof. Any quadratic extension of $\mathbb{Q}$ is of the form $\mathbb{Q}(\sqrt{d})$ for some square free integer d. (Negative or positive.)

Let $\zeta_n := \exp\left(\dfrac{2\pi\iota}{n}\right)$. Note that ζ_n is indeed a primitive n-th root of unity.

Let p be an odd prime and note that $\mathbb{Q}(\sqrt{-p}) \subseteq \mathbb{Q}(\zeta_p)$ if $p \equiv 3 \pmod 4$ and $\mathbb{Q}(\sqrt{p}) \subseteq \mathbb{Q}(\zeta_p)$ if $p \equiv 1 \pmod 4$. Also, $\sqrt{2} \in \mathbb{Q}(\zeta_8)$.[6] Lastly, $\iota \in \mathbb{Q}(\zeta_4)$ and $\mathbb{Q}(\zeta_4) \subseteq \mathbb{Q}(\zeta_8)$.

[6]Note that $(\zeta_8 + \zeta_8^{-1})^2 = 2$.

Armed with these facts, we note that if $d = \pm p_1 \cdots p_r$ where p_i are distinct odd primes, then,

$$\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{Q}(\zeta_{p_1}, \ldots, \zeta_{p_r}, \zeta_4) = \mathbb{Q}(\zeta_{4p_1 \cdots p_r}).$$

On the other hand, if $d = \pm 2p_1 \cdots p_r$ where p_i are distinct odd primes, then,

$$\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{Q}(\zeta_{p_1}, \ldots, \zeta_{p_r}, \zeta_8) = \mathbb{Q}(\zeta_{8p_1 \cdots p_r}).$$

In both the above equations, the last equality follows from Example 1.28. □

Proposition 15.69. Let p be an odd prime and $\mathbb{F} \subseteq \mathbb{Q}(\zeta_p)$ be a subfield such that $[\mathbb{Q}(\zeta_p) : \mathbb{F}] = 2$. Then,

$$\mathbb{F} = \mathbb{Q}(\zeta_p + \zeta_p^{-1}).$$

[↓]

[↑]

Proof. Note that ζ_p is a root of the quadratic

$$x^2 - (\zeta_p + \zeta_p^{-1})x + 1 \in \mathbb{Q}(\zeta_p + \zeta_p^{-1}).$$

Thus, $[\mathbb{Q}(\zeta_p) : \mathbb{Q}(\zeta_p + \zeta_p^{-1})] \leq 2$. The degree will be 1 iff $\mathbb{Q}(\zeta_p) = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$. However, note that the latter is contained in $\mathbb{R}$ whereas the former is not. Thus, $[\mathbb{Q}(\zeta_p) : \mathbb{Q}(\zeta_p + \zeta_p^{-1})] = 2$.

Now, by Proposition 8.13, there is a unique intermediate subfield $\mathbb{E}$ of $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ satisfying $[\mathbb{Q}(\zeta_p) : \mathbb{E}] = 2$. Thus, $\mathbb{E} = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$. □

Proposition 15.70. Let $p > 2$ be a prime number. Let H be a subgroup of $G := \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. Define

$$\beta := \sum_{\sigma \in H} \sigma(\zeta_p).$$

Then,

$$\mathbb{Q}(\zeta_p)^H = \mathbb{Q}(\beta_H).$$

[↓]

[↑]

Proof. Fix p and let $\zeta := \zeta_p$.

Clearly, $\beta_H \in \mathbb{Q}(\zeta)^H$ since given any $\tau \in H$, we have

$$\tau(\beta_H) = \tau\left(\sum_{\sigma\in H} \sigma(\zeta)\right) = \sum_{\sigma\in H} \tau\sigma(\zeta) = \beta_H,$$

since the map $\sigma \mapsto \tau\sigma$ is a bijection from H to itself.

Thus, $\mathbb{Q}(\beta_H) \subseteq \mathbb{Q}(\zeta)^H$. By the Galois correspondence, we know that there exists a subgroup K with $H \leq K \leq G$ such that

$$\mathbb{Q}(\beta_H) = \mathbb{Q}(\zeta)^K.$$

(In fact, we know exactly what this subgroup is, namely $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}(\beta_h))$.)

It suffices to prove that $H = K$. Suppose not. Then, $H \subsetneq K$ and β is fixed by every element of K. Pick $\tau \in K \setminus H$. We show that $\tau(\beta_H) \neq \beta_H$ and reach a contradiction.

Note that the set

$$B = \{\zeta, \zeta^2, \ldots, \zeta^{p-1}\}$$

is a $\mathbb{Q}$-basis for $\mathbb{Q}(\zeta)$. Moreover, the above is the set of all roots of $\mathrm{irr}(\zeta, \mathbb{Q})$. Thus, any $\sigma \in G$ permutes B. Since any $\sigma \in G$ is determined by its action on ζ, we see that the elements $\sigma(\zeta)$ are distinct for distinct $\sigma \in G$ and hence, linearly independent.

Thus, if $\tau(\beta_H) = \beta_H$, then there is some $\sigma \in H$ such that $\tau\sigma = \mathrm{id}_{\mathbb{Q}(\zeta)}$ but then $\tau = \sigma^{-1} \in H$, a contradiction. Thus, $\tau(\beta_H) \neq \beta_H$ but that contradicts the fact that K fixes $\mathbb{Q}(\beta_H)$. Thus, $\mathbb{Q}(\beta_H) = \mathbb{Q}(\zeta)^H$. □

§15.9. Abelian and Cyclic extensions

Lemma 15.71. Let p be a prime number and n be relatively prime to p. Suppose $\bar{\Phi}_n(x)$ has a root in $\mathbb{F}_p$. Then, $p \equiv 1 \pmod{n}$. [↓]

[↑]

Proof. Let $k \in \mathbb{Z}$ be such that $\bar{k} \in \mathbb{F}_p$ is a root of $\bar{\Phi}_n(x)$. Then, $p \mid \Phi_n(k)$ in $\mathbb{Z}$. In turn, $p \mid k^n - 1$ or $k^n \equiv 1 \pmod{p}$.

We contend that $o(\bar{k}) = n$ in $(\mathbb{F}_p)^\times$. Suppose not. Then, $m := o(\bar{k}) < n$. Then, $m \mid n$ and so, we have

$$\begin{aligned} x^n - 1 &= \prod_{d \mid n} \Phi_d(x) \\ &= \Phi_n(x) \prod_{\substack{d \mid n \\ d \neq n}} \Phi_d(x) \\ &= \Phi_n(x) \cdot \prod_{d \mid m} \Phi_d(x) \cdot \prod_{\substack{d \nmid m \\ d \neq n}} \Phi_d(x) \\ &= \Phi_n(x)(x^m - 1)h(x) \end{aligned}$$

for some $h(x) \in \mathbb{Z}[x]$. We have used Theorem 8.10 in the above.

Going $\mod p$ gives

$$x^n - 1 = \bar{\Phi}_n(x)(x^m - 1)\bar{h}(x).$$

However, note that $\bar{k}$ is a root of both $\bar{\Phi}_n(x)$ and $x^m - 1$ and so, $x^n - 1$ has repeated roots in $\mathbb{F}_p$. This is a contradiction since $p \nmid n$.

Thus, $o(\bar{k}) = n$ and in particular, $n \mid (p - 1)$, as desired. □

Theorem 15.72. Let $n \in \mathbb{N}$. Then, there are infinitely many primes p such that $p \equiv 1 \pmod{n}$. [↓]

[↑]

Proof. Suppose to the contrary that $p_1, \ldots, p_r$ are all such primes. Let $m = np_1 \cdots p_r$. Consider the cyclotomic polynomial $\Phi_m(x)$. Since it is monic (and non-constant), we have

$$\lim_{x \to \infty} \Phi_m(mx) = \infty.$$

In particular, there exists $k \in \mathbb{N}$ such that $\Phi_m(mk) \geq 2$. Thus, it has a prime factor p. Then,

$$p \mid (mk)^m - 1$$

and thus, $p \nmid (mk)$. Hence, $\gcd(p, n) = 1$. Consequently, $p \neq p_1, \ldots, p_r$. But $\bar{\Phi}_m(\overline{mk}) = 0$ and so, $p \equiv 1 \pmod{mk}$. In turn, we have

$$p \equiv 1 \pmod{n},$$

a contradiction. □

Theorem 15.73. Let G be a finite abelian group. Then, there exists an extension $\mathbb{K}/\mathbb{Q}$ such that $G \cong \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$. [↓]

[↑]

Proof. We may assume that $|G| =: n \geq 2$. For $m \in \mathbb{N}$, define $C_m := \mathbb{Z}/m\mathbb{Z}$ and $U(m) := (\mathbb{Z}/m\mathbb{Z})^\times$. We have

$$G \cong C_{n_1} \times \cdots \times C_{n_k}$$

for some integers $n_1, \ldots, n_k \geq 2$ with

$$n = n_1 \cdots n_k.$$

Let $p_1, \ldots, p_k$ be distinct primes such that $p_i \equiv 1 \pmod{n_i}$ for all $i = 1, \ldots, k$. (Existence is given by Theorem 9.3.)

Note that each $U(p_i)$ is cyclic with order $p_i - 1$, a multiple of n_i. Thus, there exists a subgroup $H_i \leq U(p_i)$ with

$$\frac{U(p_i)}{H_i} \cong C_{n_i},$$

for each $i = 1, \ldots, k$.

Thus, we have

$$\frac{U(p_1) \times \cdots \times U(p_k)}{H_1 \times \cdots \times H_k} \cong C_{n_1} \times \cdots \times C_{n_k} \cong G.$$

By the Chinese Remainder Theorem, we have

$$U(p_1) \times \cdots \times U(p_k) \cong U(m) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}),$$

where $m = p_1 \cdots p_k$. Let H be the subgroup of $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ corresponding to $H_1 \times \cdots \times H_k$, under this isomorphism.

Thus, we have

$$\frac{\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})}{H} \cong G.$$

By the Galois correspondence, we see that $G \cong \mathrm{Gal}(\mathbb{Q}(\zeta_m)^H/\mathbb{Q})$. $\square$

Theorem 15.74 (Dedekind)**.** Let $\chi_1, \ldots, \chi_n : G \to \mathbb{K}^\times$ be distinct characters. Then, $\chi_1, \ldots, \chi_n$ are linearly independent. [↓]

[↑]

Proof. If $n = 1$, then the statement is clearly true since χ_1 does not take the value 0.

Suppose that $n \geq 2$. Suppose that $\chi_1, \ldots, \chi_n$ are linearly dependent. Among all relations of linear dependence, choose $m \geq 2$ to be the one with the least number of non-zero coefficients. (We have $m \geq 2$ by the first line.) By renumbering, we may assume that we have

$$a_1\chi_1 + \cdots + a_m\chi_m = 0$$

with $a_1, \ldots, a_m \in \mathbb{K} \setminus \{0\}$. Thus, for any $g \in G$, we have

$$a_1\chi_1(g) + \cdots + a_m\chi_m(g) = 0. \tag{15.2}$$

Now, fix $g_0 \in G$ such that $\chi_1(g_0) \neq \chi_m(g_0)$. (Exists since $m \geq 1$ and $\chi_1 \neq \chi_m$.) Then, (15.2) gives

$$a_1\chi_1(g_0g) + \cdots + a_m\chi_m(g_0g) = 0$$

for all $g \in G$. Since each χ_i is a homomorphism, we have

$$a_1\chi_1(g_0)\chi_1(g) + \cdots + a_m\chi_m(g_0)\chi_m(g) = 0. \tag{15.3}$$

Multiplying (15.2) with $\chi_m(g_0)$ and subtracting from (15.3) gives

$$a_1(\chi_1(g_0) - \chi_m(g_0))\chi_1(g) + \cdots + a_{m-1}(\chi_{m-1}(g_0) - \chi_m(g_0))\chi_{m-1}(g) = 0.$$

The above holds for all $g \in G$. But the first coefficient is non-zero. This is an equation of linear dependence with $\leq m - 1$ non-zero coefficients. This is a contradiction. $\square$

Lemma 15.75. Let $n \in \mathbb{N}$ and $\mathbb{F}$ be a field containing a primitive n-th root of unity ζ. Suppose that $\mathbb{E}/\mathbb{F}$ is a cyclic Galois extension of degree n with $G := \mathrm{Gal}(\mathbb{E}/\mathbb{F}) = \langle\sigma\rangle$. Then, ζ is an eigenvalue of the $\mathbb{F}$-linear map σ. [↓]

[↑]

Proof. The order of σ is n and hence, it satisfies $T^n - 1 = 0$. (As an operator.)

We contend that $T^n - 1 \in \mathbb{F}[T]$ is the minimal polynomial of σ. Indeed, if σ satisfies a polynomial of degree $m < n$, then the distinct operators $\sigma, \ldots, \sigma^m$ are linearly dependent. This contradicts Theorem 9.8, since we can view $\sigma, \ldots, \sigma^m$ as distinct characters of $\mathbb{E}^\times$ in $\mathbb{E}$.

Hence, $T^n - 1$ is the minimal polynomial of σ. Since $\zeta \in \mathbb{F}$ is a root of $T^n - 1$, it is an eigenvalue of σ. □

(In case you're not aware of minimal polynomials: We have shown that $T^n - 1$ is the least degree polynomial that is satisfied by σ. Use this to conclude that $T^n - 1$ divides every polynomial $p(T) \in \mathbb{F}[T]$ such that $p(\sigma) = 0$. In particular, it must divide the characteristic polynomial (here we use Cayley Hamilton) and thus, ζ is an eigenvalue.)

Theorem 15.76. Let $\mathbb{E}/\mathbb{F}$ be a cyclic Galois extension of degree n. Then, there exists $a \in \mathbb{E}$ such that $\mathbb{E} = \mathbb{F}(a)$ and $a^n \in \mathbb{F}$. [↓]

[↑]

Proof. Let $G := \mathrm{Gal}(\mathbb{E}/\mathbb{F}) = \langle\sigma\rangle$ and $\zeta \in \mathbb{F}$ be a primitive n-th root of unity. By Lemma 9.9, we see that ζ is an eigenvalue of σ. Thus, there exists an eigenvector $a \in \mathbb{E}^\times$ such that $\sigma(a) = \zeta a$ and hence, $\sigma^i(a) = \zeta^i a$.

Since ζ is a primitive n-th root, we see that $a, \zeta a, \ldots, \zeta^{n-1}a$ are all distinct and hence, a has at least n Galois conjugates and so,

$$[\mathbb{F}(a) : \mathbb{F}] \geq [\mathbb{F}(a) : \mathbb{F}]_s \geq n.$$

Since $[\mathbb{E} : \mathbb{F}] = n$, we see that $\mathbb{F}(a) = \mathbb{E}$.

Now, note that $\sigma(a^n) = (\sigma(a))^n = \zeta^n a^n = a^n$ and thus, $a^n \in \mathbb{E}^G = \mathbb{F}$. □

Proposition 15.77. Let $\mathbb{E}/\mathbb{F}$ be a cyclic Galois extension of degree n where $\mathbb{F}$ has a primitive n-th root of unity. Let $\mathbb{E} = \mathbb{F}(a)$, where $a \in \mathbb{E}$ is such that $a^n \in \mathbb{F}$, in view of Theorem 9.10.

Then, the intermediate subfields of $\mathbb{E}/\mathbb{F}$ are $\mathbb{F}(a^d)$ where d is a divisor of n. [↓]

[↑]

Proof. Clearly, each $\mathbb{F}(a^d)$ is indeed an intermediate subfield of $\mathbb{E}/\mathbb{F}$. We show that these are the only ones.

Note that since G is cyclic of order n, it has exactly one subgroup of order d, for every divisor d of n. In turn, $\mathbb{E}/\mathbb{F}$ has exactly one intermediate subfield of degree n/d over $\mathbb{F}$. We show that $\mathbb{F}(a^d)$ has this property and thus, we have covered all intermediate subfields.

To this end, first note that $(a^d)^{n/d} \in \mathbb{F}$ and thus,

$$[\mathbb{F}(a^d) : \mathbb{F}] \leq n/d.$$

On the other hand, a satisfies $x^d - a^d \in \mathbb{F}(a^d)[x]$ and so,

$$[\mathbb{E} : \mathbb{F}(a^d)] \leq d.$$

Since $[\mathbb{E} : \mathbb{F}] = n$, the Tower law forces both of the above inequalities to be equalities. $\square$

Theorem 15.78 (Artin-Schreier)**.** Let $\mathbb{F}$ be a field of prime characteristic p.

1. Let $\mathbb{E}/\mathbb{F}$ be a finite Galois extension of degree p. Then, $\mathbb{E} = \mathbb{F}(a)$ for some $a \in \mathbb{E}$ such that $a^p - a \in \mathbb{F}$.
2. Let $b \in \mathbb{F}$ be such that $f(x) := x^p - x - b \in \mathbb{F}[x]$ has no root in $\mathbb{F}$. Then, $f(x)$ is irreducible over $\mathbb{F}$ and a splitting field of $f(x)$ over $\mathbb{F}$ is cyclic of degree p. [↓]

[↑]

Proof.

1. Let $G := \mathrm{Gal}(\mathbb{E}/\mathbb{F}) = \langle\sigma\rangle$. Define the $\mathbb{F}$-linear map $T : \mathbb{E} \to \mathbb{E}$ as

$$T := \sigma - \mathrm{id}_{\mathbb{E}}.$$

Note that

$$\ker(T) = \{a \in \mathbb{E} : \sigma(a) = a\} = \mathbb{E}^G = \mathbb{F}.$$

Also, we have

$$T^p = (\sigma - \mathrm{id}_{\mathbb{E}})^p = \sigma^p - \mathrm{id}_{\mathbb{E}} = 0$$

and so, $\mathrm{im}(T^{p-1}) \subseteq \ker(T) = \mathbb{F}$. However, note that $T^{p-1} \neq 0$ since that would give a non-trivial relation between the distinct $\mathbb{E}^\times$ characters $1, \sigma, \ldots, \sigma^{p-1}$, contradicting Dedekind.

Thus, $\operatorname{im}(T^{p-1})$ is at least one dimensional over $\mathbb{F}$. Since it is contained in $\mathbb{F}$, we have $\operatorname{im}(T^{p-1}) = \mathbb{F}$.

Let $b \in \mathbb{E}$ be such that $T^{p-1}(b) = 1$ and put $a = T^{p-2}(b) \in \mathbb{E}$. Note that

$$\sigma(a) = T(a) + a = 1 + a.$$

Thus, $\sigma^i(a) = i + a$ for $i = 0, \ldots, p-1$. All of these are distinct. Thus, $\mathbb{E} = \mathbb{F}(a)$. (Compare the separability degree.)

Now, note that

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

and thus, $a^p - a \in \mathbb{E}^G = \mathbb{F}$.

2. Suppose $b \in \mathbb{F}$ is such that $f(x) := x^p - x - b$ has no root in $\mathbb{F}$. Let $\mathbb{E}$ be a splitting field of $f(x)$ over $\mathbb{F}$ and let $\alpha \in \mathbb{E}$ be a root. Then, $\alpha + 1, \ldots, \alpha + (p - 1)$ are also roots. Thus,

$$\mathbb{E} = \mathbb{F}(\alpha, \ldots, \alpha + p - 1) = \mathbb{F}(\alpha).$$

Now, write $f(x) = g_1(x) \cdots g_r(x)$ for irreducible $g_i(x) \in \mathbb{F}[x]$. Now, if $\beta \in \mathbb{E}$ is a root of some $g_i(x)$, then $\mathbb{E} = \mathbb{F}(\beta)$, by the same argument as above and hence, each g_i has degree $d := [\mathbb{F}(\beta) : \mathbb{F}] > 1$.[7] Thus, we have

$$p = \deg(f(x)) = rd.$$

Since p is prime and $d > 1$, we have $d = p$ and $r = 1$.

Thus, $[\mathbb{E} : \mathbb{F}] = d = p$ and G is generated by the automorphism σ determined by $\sigma(\alpha) = \alpha + 1$. □

§15.10. Some Group Theory

Proposition 15.79. Any group with order p^n is solvable, where p is a prime and $n \in \mathbb{N}_0$. [↓]

[↑]

[7] Strictly greater since $\beta \notin \mathbb{F}$.

Proof. We prove this by induction on n. If $n = 0, 1$, then G is abelian and hence, solvable. Suppose $n > 1$ and groups of order p^k for $0 \le k < n$ are solvable.

Let $Z(G) \trianglelefteq G$ denote the center of G. We have $|Z(G)| > 1$ and thus, $\overline{G} = G/Z(G)$ is a group of order p^k for some $k < n$. By induction hypothesis, $\overline{G}$ has a series

$$\overline{G} = \overline{G_0} \supseteq \overline{G_1} \supseteq \cdots \supseteq \overline{G_s} = 1.$$

By the correspondence theorem, the above lifts to a series

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_s = Z(G) \supseteq G_{s+1} := 1.$$

Since the quotients G_i/G_{i-1} are isomorphic to $\overline{G_i}/\overline{G_{i-1}}$ for $i = 1, \ldots, s$, we see that the above is an abelian series except possibly at the right-most stage. However, $Z(G)$ is abelian and so, the right-most stage is verified as well. □

Proposition 15.80. Let $f : G \to H$ be a homomorphism of groups and $s \in \mathbb{N}$.

1. $f(G^{(s)}) \le H^{(s)}$. If f is onto, then $f(G^{(s)}) = H^{(s)}$.
2. If $K \trianglelefteq G$, then $K' \trianglelefteq G$. In particular, $G' \trianglelefteq G$.
3. If $K \trianglelefteq G$, then G/K is abelian iff $G' \le K$. [↓]

[↑]

Proof.

1. Let $g, h \in G$. Then,

   $$f([g,h]) = f(g^{-1}h^{-1}gh) = f(g)^{-1}f(h)^{-1}f(g)f(h) = [f(g), f(h)].$$

   Thus, $f(G') \subseteq H'$ and we may consider the homomorphism $f'|_{G'} : G' \to H'$. Applying the result again gives

   $$f(G^{(2)}) = f((G')') \subseteq (H')' = H^{(2)}.$$

   Inductively, we get the result for all $s \ge 1$.

   If f is onto, then every commutator is in the image $f(G')$ and thus, $H' = f(G')$.

   Thus, we may consider f as an onto homomorphism $f : G' \to H'$. As before, induction gives the result for all $s \ge 1$.

2. Let $a \in G$. The inner automorphism $i_a : G \to G$ restricts to one of K since $K \trianglelefteq G$. By the previous part, $i_a(K') = K'$ and thus, K is normal. $G' \trianglelefteq G$ follows since $G \trianglelefteq G$.

3. G/K is abelian $\iff$ $ghK = hgK$ for all $h, g \in G$ $\iff$ $g^{-1}h^{-1}gh \in K$ for all $g, h \in K$ $\iff$ $G' \leq K$. $\square$

Proposition 15.81. A group G is solvable iff $G^{(s)} = 1$ for some $s \in \mathbb{N}$. [↓]

[↑]

Proof. ($\Rightarrow$) Suppose G is solvable. Then, there is an abelian series

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_s = G \tag{15.4}$$

for G. We show by induction on s that $G^{(s)} = 1$.

If $s = 1$, then G is abelian and $G^{(1)} = 1$. Now, let $s > 1$ and assume that $G^{(s-1)} = 1$ whenever G has an abelian series of length $s - 1$. Let G be a group with an abelian series of length s as in (15.4). Then,

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_{s-1}$$

is an abelian series for G_{s-1}. By induction hypothesis, we have $G_{s-1}^{(s-1)} = 1$. Since G/G_{s-1} is abelian, we have $G' \subseteq G_{s-1}$, by Proposition 10.8. Thus,

$$G^{(s)} = (G')^{(s-1)} \subseteq (G_{s-1})^{(s-1)} = 1.$$

($\Leftarrow$) Suppose that $G^{(s)} = 1$ for some s. Then,

$$1 = G^{(s)} \trianglelefteq G^{(s-1)} \trianglelefteq \cdots \trianglelefteq G^{(1)} \trianglelefteq G$$

is an abelian series. $\square$

Proposition 15.82. Let $K \trianglelefteq G$ be groups. Then,

$$\left(\frac{G}{K}\right)^{(s)} = \frac{\langle G^{(s)}, K\rangle}{K}.$$

[↓]

[↑]

Proof. Let $\pi : G \to G/K$ be the natural onto map. Then, $\pi(G^{(s)}) = (G/K)^{(s)}$, by Proposition 10.8. By the correspondence theorem, we see that $\langle G^{(s)}, K\rangle/K = (G/K)^{s}$. □

Proposition 15.83. Let G and H be groups.

1. If G is solvable and there is an injection $i : H \to G$, then H is solvable. In particular, subgroups of solvable groups are solvable.
2. If G is solvable and there is a surjection $f : G \to H$, then H is solvable. In particular, quotients of solvable groups are solvable.
3. If $K \trianglelefteq G$ is such that K and G/K are solvable, then G is solvable. [↓]

[↑]

Proof. For the first two parts, let s be such that $G^{(s)} = 1$. (Exists by Proposition 10.10.) Using the same result, it suffices to show that $H^{(s)} = 1$ for the first two parts.

1. $H^{(s)} \cong i(H^{(s)}) \subseteq G^{(s)} = 1$.
2. Since f is onto, we have $H^{(s)} = f(G^{(s)}) = 1$.
3. There exist s and t such that $K^{(s)} = 1$ and $(G/K)^{(t)} = 1$.
   By Proposition 10.11, we have $(G/K)^{(t)} = \langle G^{(t)}, K\rangle/K$. Since this is trivial, we have $G^{(t)} \subseteq K$ and so, $G^{(s+t)} \subseteq K^{(s)} = 1$. □

Proposition 15.84. Let G be a finite solvable group. Then, there exists a normal series

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_s = G$$

such that G_i/G_{i-1} is cyclic of prime order for all $i = 1, \ldots, s$. [↓]

[↑]

Proof. Since G is solvable, there exists an abelian series

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_s = G.$$

We show that between G_i and G_{i+1}, we can insert groups $H_1^{(i)}, \ldots, H_{r_i}^{(i)}$ such that

$$G_i \trianglelefteq H_1^{(i)} \trianglelefteq \cdots \trianglelefteq H_{r_i}^{(i)} \trianglelefteq G_{i+1}$$

and each quotient above is cyclic of prime order.

Note that by the correspondence theorem of subgroups of the original group and a quotient group, it suffices to prove that for $s = 1$.

That is, assume that G is an abelian group. We show that there exists a chain

$$1 = G_0 \trianglelefteq \cdots \trianglelefteq G_s = G$$

such that the quotients are cyclic of prime order.

Let $|G| = p_1 \cdots p_n$, where p_i are (not necessarily distinct) primes. We prove the statement by induction on n. If $n = 0$ or 1, the result is obvious. Assume $n \geq 2$ and that the result is true for $n - 1$. Then, since $p_n \mid G$, there exists an element $g \in G$ order p_n. Let $G_1 := \langle g \rangle$. Then, $G_1 \trianglelefteq G$ since G is abelian. By induction, G/G_1 has a normal series where the quotients are cyclic of prime order. Lift that chain to complete the proof. $\square$

Lemma 15.85. For $n \geq 3$, A_n is generated by 3-cycles. If $n \geq 5$, then all the 3-cycles are conjugates in A_n. [↓]

[↑]

Proof. Clearly, every three cycle $(abc) = (ac)(ab)$ is indeed in A_n. Let $H \leq A_4$ be the subgroup generated by the 3-cycles.

Let $\tau_1 = (ij)$ and $\tau_2 = (rs)$ be distinct transpositions. Then, we have

$$\tau_1\tau_2 = \begin{cases} (ijr)(rsj) & \tau_1 \text{ and } \tau_2 \text{ are disjoint,} \\ (irs) & \text{otherwise.} \end{cases}$$

Thus, H contains all products of distinct pairs of transpositions. Since these generate A_n (by definition), we have $H = A_n$.

Now, assume that $n \geq 3$. Recall that if $\sigma \in S_n$ is any permutation and $(j_1, \ldots, j_k)$ is a k-cycle, then

$$\sigma(j_1, \ldots, j_k)\sigma^{-1} = (\sigma(j_1), \ldots, \sigma(j_k)).$$

Now, let (ijk) and (rst) be any two 3-cycles. Define $\gamma \in S_n$ by

$$\gamma(u) := \begin{cases} r & u = i, \\ s & u = j, \\ t & u = k, \\ u & \text{otherwise.} \end{cases}$$

Clearly, the above is indeed a bijection from $[n]$ to itself. Then, we have

$$\gamma \cdot (ijk) \cdot \gamma^{-1} = (rst).$$

Thus, if γ is even, then the above shows that the 3-cycles are conjugate in A_n. Otherwise, pick distinct $u, v \in [n] \setminus \{r, s, t\}$ (exist since $n \geq 5$) and define $\sigma := (ij) \cdot \gamma$. Then,

$$\sigma \cdot (ijk) \cdot \sigma^{-1} = (uv)(rst)(uv)^{-1} = (rst)$$

and $\sigma \in A_n$. □

Theorem 15.86. The groups S_n and A_n are not solvable for $n \geq 5$. [↓]

[↑]

Proof. In view of Proposition 10.12, it suffices to show that A_n is not solvable. We now show that $A_n' = A_n$ and hence, $A_n^{(s)} = A_n \neq 1$ for all $s \geq 1$.

We actually show that every 3-cycle $(ijk) \in A_n$ is a commutator. Then, by Lemma 10.14, it follows that $A_n' = A_n$. Since $n \geq 5$, we can distinct $r, v \in [n] \setminus \{i, j, k\}$. Then, we have

$$[(jkv), (ikr)] = (vkj)(rki)(jkv)(ikr) = (vkj)(ivj) = (ikj).$$ □

Theorem 15.87. The alternating group A_n is simple for $n \geq 5$. [↓]

[↑]

Proof. Suppose $1 \neq N \trianglelefteq A_n$. We show that $N = A_n$. If N contains a 3-cycle, then N contains all 3-cycles since N is normal in A_4 and all 3-cycles in A_n are conjugates, by Lemma 10.14. But that lemma also tells us that A_n is generated by 3-cycles. Thus, we get $N = A_4$. So, it suffices to show that N contains a 3-cycle.

For $\sigma \in S_n$ and $j \in [n]$, we say that j is a fixed point of σ if $\sigma(j) = j$. Pick $\sigma \in N \setminus \{1\}$ with maximum number of fixed points in $N \setminus \{1\}$. We will show that σ is a 3-cycle.

Write $\sigma = \tau_1 \cdots \tau_g$ where $\tau_1, \ldots, \tau_g$ are disjoint cycles of length at least 2 and $g \geq 1$. This is possible since $\sigma \neq 1$.

Case 1. Each τ_i has length exactly 2. Then, since σ is even, we have $g \geq 2$. Let $\tau_1 = (ij)$ and $\tau_2 = (rs)$. Since $n \geq 5$, we can fix $k \in [n] \setminus \{i, j, r, s\}$ and set $\tau = (rsk) \in A_n$. Consider the commutator

$$\sigma' = [\sigma, \tau] = \sigma^{-1} \underbrace{(\tau^{-1}\sigma\tau)}_{\in N} \in N$$

Let $\gamma = \tau_3 \cdots \tau_g$ so that

$$\sigma = (ij)(rs)\gamma$$

with γ fixing i, j, r, s. (Since the τs were disjoint.)

Note that $\tau\sigma(k) = \tau\gamma(k) = \gamma(k)$, since γ restricts to a permutation on $[n] \setminus \{i, j, r, s\}$. On the other hand, we have $\sigma\tau(k) = \sigma(r) = s \neq k$. Thus, $\tau\sigma \neq \sigma\tau$ and hence, $\sigma' \neq 1$.

But note that σ' fixes all fixed points of σ, with possible exception of k.[8] However, σ' also fixes i and j. Thus, $\sigma' \in N \setminus \{1\}$ has more fixed points than σ. A contradiction.

Case 2. There is some τ_i with length at least 3. Since all the τs commute, we may assume $\tau_1 = (ijk\ldots)$ has length at least 3. If $\sigma = (ijk)$, then we are done.

Otherwise, there are at least two other elements r, s apart from i, j, k that σ does not fix.[9] Let $\tau = (rsk) \in A_n$ and consider $\sigma' = [\sigma, \tau]$. Note that $\sigma'(j) \neq j$ and thus, $\sigma' \neq 1$. Thus, $\sigma' \in N \setminus \{1\}$.

However, note that $\sigma'(i) = i$ and σ' fixes every fixed element of σ. (Since τ only moves those elements already moved by σ.) Thus, σ' fixes more elements than σ, a contradiction.

Thus, σ is a 3-cycle and we are done. □

Theorem 15.88. For $n \geq 2$, S_n is generated by the $n - 1$ transpositions

$$(12), (13), \ldots, (1n).$$

[↓]

[↑]

[8] By this, we mean that it was possible that σ fixed k.

[9] If $g = 1$, then τ_1 is a cycle with odd number of elements since $\sigma \in A_n$. If $g \geq 2$, then τ_2 has at least two elements which it moves.

Proof. For $n = 2$, the theorem is clear. Assume $n \geq 3$. Then, by Theorem 10.17, it suffices to show that every transposition is generated by the above list. Let $(ij) \in S_n$ be a transposition. If $i = 1$ or $j = 1$, then it is in the above list. Assume $i \neq 1 \neq j$. Then, we have
$$(ij) = (1i)(1j)(1i).$$
□

Theorem 15.89. For $n \geq 2$, S_n is generated by the $n-1$ transpositions
$$(1\ 2), (2\ 3), \ldots, (n-1\ n).$$
[↓]

[↑]

Proof. Again, by Theorem 10.17, it suffices to show that every transposition is generated by the above list.

Let $(a\ b) \in S_n$ be a transposition. Without loss of generality, we assume that $a < b$.[10] We show that $(a\ b)$ is a product of elements of the given list by induction on $b - a$.

If $b - a = 1$, then $(a\ b)$ is in the list itself. Assume $b - a = k > 1$ and the theorem is true for $k - 1$. Note that we have
$$(a\ b) = (a\ a+1)(a+1\ b)(a\ a+1).$$
Since $(a+1) - a = 1$ and $b - (a+1) = k - 1$, we are done. □

Theorem 15.90. For $n \geq 2$, S_n is generated by the transposition (12) and the n-cycle $(12\ldots n)$. [↓]

[↑]

Proof. The theorem is clearly true for $n = 2$. Assume $n \geq 3$.

By Theorem 10.19, it suffices to show the two elements above generate all transpositions of the form $(i\ i+1)$ for $1 \leq i < n$.

Let $\sigma := (12\ldots n)$. Then, for $k = 1, \ldots, n-2$, we have
$$\sigma^k(1\ 2)\sigma^{-k} = (\sigma^k(1)\ \sigma^k(2)) = (k+1\ k+2).$$
□

[10]Note that $(a\ b) = (b\ a)$.

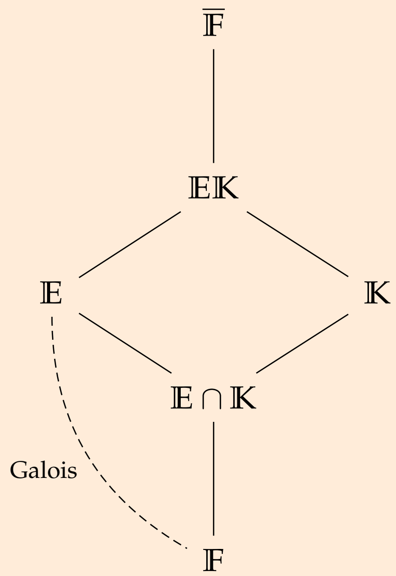
Corollary 15.91. Let $p \geq 3$ be a prime. Then, S_p is generated by any pair of transposition and p-cycle. [↓]

[↑]

Proof. Let renumbering, we may assume that the transposition is (12). The p-cycle is of the form $(1a_1 \dots a_{p-2}) =: \sigma$. Since p is a prime, there exists k such that σ^k is of the form $(12b_3 \dots b_{p-3})$. By renumbering again, we may assume that $b_i = i$ for $i = 3, \dots, n$. By Theorem 10.20, we are done. □

§15.11. Galois Groups of Composite Extensions

Proposition 15.92. If $\mathbb{E}/\mathbb{F}$ is a Galois extension and $\mathbb{K}/\mathbb{F}$ is a field extension, then $\mathbb{E}\mathbb{K}/\mathbb{K}$ is Galois. Moreover, if $\mathbb{K}/\mathbb{F}$ is also Galois, then $\mathbb{E}\mathbb{K}/\mathbb{F}$ and $(\mathbb{E} \cap \mathbb{K})/\mathbb{F}$ are Galois. [↓]



[↑]

Proof. As $\mathbb{E}/\mathbb{F}$ is Galois, $\mathbb{E}$ is a splitting field of a family of separable polynomials $\{f_i(x)\}_{i \in I} \subseteq \mathbb{F}[x]$ over $\mathbb{F}$. Then, $\mathbb{E}\mathbb{K}$ is splitting of the same family over $\mathbb{K}$ and thus, is Galois over $\mathbb{K}$.

Now, assume that $\mathbb{K}/\mathbb{F}$ is also Galois. Then, $\mathbb{K}$ is a splitting field of a family of separable polynomials $\{g_j(x)\}_{j\in J} \subseteq \mathbb{F}[x]$ over $\mathbb{F}$. Then, $\mathbb{E}\mathbb{F}$ is a splitting field the the family $\{f_i(x)\}_{i\in I} \cup \{g_j(x)\}_{j\in J} \subseteq \mathbb{F}[x]$ over $\mathbb{F}$ and thus, Galois.

Now we show the same for the intersection. Let $\sigma : (\mathbb{E} \cap \mathbb{K}) \to \overline{\mathbb{F}}$ be an $\mathbb{F}$-embedding. Extend it to an $\mathbb{F}$-embedding $\tau : \mathbb{E}\mathbb{K} \to \overline{\mathbb{F}}$.
Since $\mathbb{E}/\mathbb{F}$ and $\mathbb{K}/\mathbb{F}$ are normal, we get $\tau(\mathbb{E}) = \mathbb{E}$ and $\tau(\mathbb{K}) = \mathbb{K}$. Therefore, $\tau(\mathbb{E} \cap \mathbb{K}) \subseteq \mathbb{E} \cap \mathbb{K}$. But since $(\mathbb{E} \cap \mathbb{K})/\mathbb{F}$ is algebraic, we have $\tau(\mathbb{E} \cap \mathbb{K}) = \mathbb{E} \cap \mathbb{K}$, by Lemma 6.5. Thus, $\sigma(\mathbb{E} \cap \mathbb{K}) = \mathbb{E} \cap \mathbb{K}$, as desired and so, $\mathbb{E} \cap \mathbb{K}$ is Galois over $\mathbb{F}$. (We have used Theorem 6.6.) $\square$

Proposition 15.93. Let $\mathbb{E}/\mathbb{F}$ be a finite Galois extension and $\mathbb{K}/\mathbb{F}$ be a field extension (with $\mathbb{E}, \mathbb{K} \subseteq \overline{\mathbb{F}}$). Then, the map

$$\psi : \operatorname{Gal}(\mathbb{E}\mathbb{K}/\mathbb{K}) \to \operatorname{Gal}(\mathbb{E}/\mathbb{F})$$

defined by $\psi(\sigma) = \sigma|_{\mathbb{E}}$ is injective and induces an isomorphism

$$\operatorname{Gal}(\mathbb{E}\mathbb{K}/\mathbb{K}) \cong \operatorname{Gal}(\mathbb{E}/\mathbb{E} \cap \mathbb{K}).$$

[↓]

$$\begin{tikzcd}[arrows=dash]
 & \mathbb{E}\mathbb{K} \arrow[dl] \arrow[dr] & \\
\mathbb{E} \arrow[dr] & & \mathbb{K} \arrow[dl] \\
 & \mathbb{E} \cap \mathbb{K} &
\end{tikzcd}$$

[↑]

Proof. First note that σ is actually well-defined. Indeed, if $\sigma \in \operatorname{Gal}(\mathbb{E}\mathbb{K}/\mathbb{K})$, then σ fixes $\mathbb{K}$ and in particular, $\mathbb{F}$. Thus, so does $\sigma|_{\mathbb{E}}$. That it is a homomorphism is clear.

Now, suppose that $\sigma \in \operatorname{Gal}(\mathbb{E}\mathbb{K}/\mathbb{K})$ is such that $\sigma|_{\mathbb{E}} = \mathrm{id}_{\mathbb{E}}$. By definition of the Galois group, we have $\sigma|_{\mathbb{K}} = \mathrm{id}_{\mathbb{K}}$. Thus, σ fixes both $\mathbb{E}$ and $\mathbb{K}$ and in turn, $\mathbb{E}\mathbb{K}$. Hence, ψ is injective.

Let $H := \operatorname{im}(\psi) \leq G := \operatorname{Gal}(\mathbb{E}/\mathbb{F})$. Note that $\mathbb{E} \cap \mathbb{K} \subseteq \mathbb{E}^H$. Indeed, if $a \in \mathbb{E} \cap \mathbb{K}$ and $\tau = \psi(\sigma) \in H$ for some $\sigma \in \operatorname{Gal}(\mathbb{E}\mathbb{K}/\mathbb{K})$, then $\tau(a) = \sigma(a) = a$, since σ

fixes $\mathbb{K}$.

On the other hand, if $a \in \mathbb{E} \setminus (\mathbb{E} \cap \mathbb{K})$, then $a \in \mathbb{E}\mathbb{K} \setminus \mathbb{K}$ and hence, there exists $\sigma \in \mathrm{Gal}(\mathbb{E}\mathbb{K}/\mathbb{K})$ such that $\sigma(a) \neq a$. (See Theorem 7.12 and Remark 7.13.) Thus, $a \notin \mathbb{E}^H$. Hence, $\mathbb{E}^H = \mathbb{E} \cap \mathbb{K}$.

Now, note H is finite since G is so. By Artin's Theorem, we have

$$\mathrm{Gal}(\mathbb{E}\mathbb{K}/\mathbb{K}) \cong H = \mathrm{Gal}(\mathbb{E}/\mathbb{E}^H) = \mathrm{Gal}(\mathbb{E}/(\mathbb{E} \cap \mathbb{K})).$$ □

Corollary 15.94. Let $\mathbb{E}/\mathbb{F}$ be a finite Galois extension and $\mathbb{K}/\mathbb{F}$ any field extension. Then,

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

In particular, $[\mathbb{E}\mathbb{K} : \mathbb{F}] = [\mathbb{E} : \mathbb{F}][\mathbb{K} : \mathbb{F}]$ iff $\mathbb{E} \cap \mathbb{K} = \mathbb{F}$. [↓]

[↑]

Proof. The first equation about the degrees follows from Proposition 7.4.

Thus,

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

The last statement now follows. □

Theorem 15.95. Let $\mathbb{E}/\mathbb{F}$ and $\mathbb{K}/\mathbb{F}$ be finite Galois extensions with $\mathbb{E}, \mathbb{K} \subseteq \overline{\mathbb{F}}$. Then, the homomorphism

$$\psi : \mathrm{Gal}(\mathbb{E}\mathbb{K}/\mathbb{F}) \to \mathrm{Gal}(\mathbb{E}/\mathbb{F}) \times \mathrm{Gal}(\mathbb{K}/\mathbb{F}), \quad \psi(\sigma) = (\sigma|_{\mathbb{E}}, \sigma|_{\mathbb{K}})$$

is injective. If $\mathbb{E} \cap \mathbb{K} = \mathbb{F}$, then ψ is an isomorphism. [↓]

[↑]

Proof. That ψ is a well-defined homomorphism is clear. (Same proof as Proposition 11.2.) Suppose $\sigma \in \ker(\psi)$. Then, $\sigma(a) = a$ for all $a \in \mathbb{E}$ and for all $a \in \mathbb{K}$. Thus, $\sigma = \mathrm{id}_{\mathbb{E}\mathbb{K}}$ and hence, ψ is injective.

Suppose that $\mathbb{E} \cap \mathbb{K} = \mathbb{F}$, then by Corollary 11.3, we have

$$|\mathrm{Gal}(\mathbb{E}\mathbb{K}/\mathbb{F})| = [\mathbb{E}\mathbb{K} : \mathbb{F}] = [\mathbb{E} : \mathbb{F}][\mathbb{K} : \mathbb{F}] = |\mathrm{Gal}(\mathbb{E}/\mathbb{F}) \times \mathrm{Gal}(\mathbb{K}/\mathbb{F})|$$

and thus, comparing cardinalities gives that ψ is onto as well. □

§15.12. Normal Closure of an Algebraic Extension

Proposition 15.96. Let the notations be as in Definition 12.1. The following are true.

1. $\mathbb{K}$ is a normal extension of $\mathbb{F}$ containing $\mathbb{E}$.
2. Any such normal extension $\mathbb{K}' \subseteq \overline{\mathbb{F}}$ as above contains $\mathbb{K}$.
3. If $\mathbb{E}/\mathbb{F}$ is a finite extension, then so is $\mathbb{K}/\mathbb{F}$.
4. If $\mathbb{E}/\mathbb{F}$ is separable, then $\mathbb{K}/\mathbb{F}$ is Galois.
5. Suppose $\mathbb{E}/\mathbb{F}$ is separable and not normal. Suppose $H \leq \mathrm{Gal}(\mathbb{K}/\mathbb{E}) \leq \mathrm{Gal}(\mathbb{K}/\mathbb{F}) =: G$ is normal in G. Then, $H = 1$. [↓]

[↑]

Proof.

1. $\mathbb{K}$ is normal by Theorem 6.6. That it contains $\mathbb{E}$ is trivial.
2. Since $\mathbb{K}' \supseteq \mathbb{E}$, given any $a \in \mathbb{E}$, the polynomial $\mathrm{irr}(a, \mathbb{F})$ must factor completely in $\mathbb{K}'$, by definition of normality. Thus, it contains the splitting field of $\mathrm{irr}(a, \mathbb{F})$ over $\mathbb{F}$. Since this is true for all $a \in \mathbb{E}$, $\mathbb{K}' \supseteq \mathbb{K}$.
3. Write $\mathbb{E} = \mathbb{F}(a_1, \ldots, a_n)$. Then, consider the splitting field $\mathbb{K}$ of $\{\mathrm{irr}(a_i, \mathbb{F}) \mid 1 \leq i \leq n\}$ over $\mathbb{F}$. Then, $\mathbb{K}$ is normal over $\mathbb{F}$ and any normal extension of $\mathbb{F}$ must contain $\mathbb{K}$. Thus, $\mathbb{K}$ is the normal closure. $\mathbb{K}/\mathbb{F}$ is clearly a finite extension.
4. Since $\mathrm{irr}(a, \mathbb{F})$ is separable over $\mathbb{F}$ for each $a \in \mathbb{E}$, we see that $\mathbb{K}/\mathbb{F}$ is normal, in view of Proposition 6.4.
5. Let $K := \mathrm{Gal}(\mathbb{K}/\mathbb{E})$. Note that K is not normal in G since $\mathbb{E}/\mathbb{F}$ is not normal. (Recall Theorem 7.20, which was for infinite extensions as well.)

   Thus, we see that $\mathbb{K}^H \supsetneq \mathbb{K}^K = \mathbb{E}$. By Theorem 7.20 again, we see that $\mathbb{K}^H/\mathbb{F}$ is normal. Thus, $\mathbb{K}^H$ is a normal extension of $\mathbb{F}$ containing $\mathbb{E}$ which is contained in $\mathbb{K}$. By minimality of $\mathbb{K}$, we have $\mathbb{K}^H = \mathbb{K}$ and thus, $H = 1$. $\square$

§15.13. Solvability by Radicals

Proposition 15.97. Let $\mathbb{F}, \mathbb{E}, \mathbb{K} \subseteq \overline{\mathbb{F}}$ be fields.

1. Suppose $\mathbb{F} \subseteq \mathbb{E} \subseteq \mathbb{K}$. If $\mathbb{K}/\mathbb{E}$ and $\mathbb{E}/\mathbb{F}$ are radical extensions, then so is $\mathbb{K}/\mathbb{F}$.
2. Suppose $\mathbb{F} \subseteq \mathbb{E}, \mathbb{K}$ are such that $\mathbb{E}/\mathbb{F}$ is a radical extension. Then, $\mathbb{E}\mathbb{K}/\mathbb{K}$ is a radical extension. If $\mathbb{K}/\mathbb{F}$ is also a radical extension, then so is $\mathbb{E}\mathbb{K}/\mathbb{F}$.

$$\begin{tikzcd}[column sep=small] & \mathbb{E}\mathbb{K} \arrow[dl, dash] \arrow[dr, dash] & \\ \mathbb{E} & & \mathbb{K} \\ & \mathbb{F} \arrow[ul, dash] \arrow[ur, dash] & \end{tikzcd}$$

[↓]

[↑]

Proof.

1. Let
$$\mathbb{F} = \mathbb{F}_0 \subseteq \mathbb{F}_1 \subseteq \cdots \subseteq \mathbb{F}_n = \mathbb{E}$$
and
$$\mathbb{E} = \mathbb{E}_0 \subseteq \mathbb{E}_1 \subseteq \cdots \subseteq \mathbb{E}_m = \mathbb{K}$$
be towers of simple radical extensions. Append the two together to see that $\mathbb{K}/\mathbb{F}$ is a radical extension.

2. Let
$$\mathbb{F} = \mathbb{F}_0 \subseteq \mathbb{F}_1 \subseteq \cdots \subseteq \mathbb{F}_n = \mathbb{E}$$
be a tower of simple radical extensions. Then, there exist $a_i \in \mathbb{F}_i$ such that
$$\mathbb{F}_i = \mathbb{F}_{i-1}(a_i)$$
for $i = 1, \ldots, n$, such that a power of a_i is in $\mathbb{F}_{i-1}$.

   Consider the tower
$$\mathbb{K} \subseteq \mathbb{K}(a_1) \subseteq \cdots \subseteq \mathbb{K}(a_1, \ldots, a_m) = \mathbb{E}\mathbb{K}.$$

Clearly, each extension above is a simple radical extension. Thus, $\mathbb{E}\mathbb{K}/\mathbb{K}$ is a radical extension. If $\mathbb{K}/\mathbb{F}$ is also radical, then the previous part gives us that $\mathbb{E}\mathbb{K}/\mathbb{F}$ is also radical. □

Proposition 15.98. Let $\mathbb{E}/\mathbb{F}$ be a separable radical extension. Let $\mathbb{K} \subseteq \overline{\mathbb{F}}$ be the smallest Galois extension of $\mathbb{F}$ containing $\mathbb{E}$. Then, $\mathbb{K}$ is a radical extension of $\mathbb{F}$. [↓]

[↑]

Proof. Let $n := [\mathbb{E} : \mathbb{F}]$. (Note that $n < \infty$ since $\mathbb{E}/\mathbb{F}$ is a radical extension.) Since $\mathbb{E}/\mathbb{F}$ is separable, there are n distinct $\mathbb{F}$-embeddings

$$\sigma_1, \ldots, \sigma_n : \mathbb{E} \to \overline{\mathbb{F}}.$$

We show that compositum $\mathbb{K} = \sigma_1(\mathbb{E}) \cdots \sigma_n(\mathbb{E})$ is the smallest Galois extension of $\mathbb{F}$ containing $\mathbb{E}$.

By the Primitive Element Theorem, we know that $\mathbb{E} = \mathbb{F}(a)$ for some $a \in \mathbb{E}$. Then, the roots of $p(x) := \operatorname{irr}(a, \mathbb{F})$ in $\overline{\mathbb{F}}$ are precisely $\sigma_1(a), \ldots, \sigma_n(a)$. Let $\mathbb{K} := \mathbb{F}(\sigma_1(a), \ldots, \sigma_n(a))$. Then, $\mathbb{K}$ is a splitting field of a separable polynomial and hence, Galois over $\mathbb{K}$. Moreover, it contains $\mathbb{E}$. It is clear any such another field must contain $\mathbb{K}$. Thus, $\mathbb{K}$ satisfies the hypothesis of the theorem.

Note that we have $\mathbb{K} = \sigma_1(\mathbb{E}) \cdots \sigma_n(\mathbb{E})$. Since $\sigma(\mathbb{E}_i) \cong \mathbb{E}_i$, we see that each $\sigma(\mathbb{E}_i)/\mathbb{F}$ is a radical extension and thus, so is $\mathbb{K}/\mathbb{F}$, by Proposition 13.3. □

Theorem 15.99. Let $\mathbb{F}$ be a field with $\operatorname{char}(\mathbb{F}) = 0$. If $f(x) \in \mathbb{F}[x]$ is solvable by radicals, then G_f is a solvable group. [↓]

[↑]

Proof. Let

$$\mathbb{F} = \mathbb{F}_0 \subsetneq \mathbb{F}_1 \subsetneq \cdots \subsetneq \mathbb{F}_r = \mathbb{K}$$

be a sequence of simple radical extensions with $\mathbb{F}_i = \mathbb{F}_{i-1}(a_i)$ such that $a_i^{n_i} \in \mathbb{F}_{i-1}$ for $i = 1, \ldots, r$ and $\mathbb{K}$ contains a splitting field $\mathbb{E}$ of $f(x)$ over $\mathbb{F}$.

Since $\operatorname{char}(\mathbb{F}) = 0$, we know that $\mathbb{K}/\mathbb{F}$ is separable. Thus, by Proposition 13.4, we may assume that $\mathbb{K}/\mathbb{F}$ is Galois. Let $n := n_1 \cdots n_r$ and $\mathbb{L}$ be the splitting field of $x^n - 1$ over $\mathbb{K}$.

Then, $\mathbb{L} = \mathbb{K}(\omega)$ where ω is any primitive n-th root of unity. Consider the fields $\mathbb{L}_0, \ldots, \mathbb{L}_r = \mathbb{L}$ defined as $\mathbb{L}_i := \mathbb{F}_i(\omega)$.

Since $\mathbb{K}/\mathbb{F}$ is Galois, $\mathbb{K}$ is the splitting of some $g(x) \in \mathbb{F}[x]$ over $\mathbb{F}$. Then, $\mathbb{L}$ is a splitting field of $(x^n - 1)g(x) \in \mathbb{F}[x]$ over $\mathbb{F}$. Thus, $\mathbb{L}$ is Galois over $\mathbb{F}$ and in turn, over all $\mathbb{L}_i$.

Let $H_i := \mathrm{Gal}(\mathbb{L}/\mathbb{L}_i)$ for $i = 0, \ldots, r$. See the diagram (at the end of this proof) for a picture. By FTGT, we have

$$G_f \cong \mathrm{Gal}(\mathbb{E}/\mathbb{F}) \cong \frac{\mathrm{Gal}(\mathbb{L}/\mathbb{F})}{\mathrm{Gal}(\mathbb{L}/\mathbb{E})}.$$

(Note that $\mathbb{L}/\mathbb{E}$ is normal since $\mathbb{L}$ is a splitting field over $\mathbb{E}$.)

Thus, to prove that G_f is solvable, it is enough to prove that $\mathrm{Gal}(\mathbb{L}/\mathbb{F})$ is solvable, by Proposition 10.12.

Note that $\mathbb{L}_i = \mathbb{L}_{i-1}(a_i)$ and that $\mathbb{L}_{i-1} \ni \omega$ and so, $\mathbb{L}_{i-1}$ contains a primitive n_i-th root of unity. Thus, $\mathbb{L}_i$ is a splitting field of $x^{n_i} - a_i^{n_i} \in \mathbb{L}_{i-1}$ over $\mathbb{L}_{i-1}$. Hence, $\mathbb{L}_i/\mathbb{L}_{i-1}$ is Galois. Thus, $H_{i-1} \trianglelefteq H_i$ for all $i = 1, \ldots, r$.

Moreover, by Proposition 8.8, we see that $\mathrm{Gal}(\mathbb{L}_i/\mathbb{L}_{i-1})$ is cyclic. Since $H_i/H_{i-1} \cong \mathrm{Gal}(\mathbb{L}_i/\mathbb{L}_{i-1})$, we see that

$$1 = H_r \trianglelefteq H_{r-1} \trianglelefteq \cdots \trianglelefteq H_0 = \mathrm{Gal}(\mathbb{L}/\mathbb{L}_0)$$

is an abelian series for $\mathrm{Gal}(\mathbb{L}/\mathbb{L}_0)$ and hence, it is solvable.

On the other hand, we know that $\mathrm{Gal}(\mathbb{L}_0/\mathbb{F})$ is abelian, by Proposition 8.6. Again, by Proposition 10.12, we see that $\mathrm{Gal}(\mathbb{L}/\mathbb{F})$ is solvable, as desired.

$$
\begin{tikzcd}
 & & \mathbb{K}(\omega)=\mathbb{L}_r=\mathbb{L} \arrow[r, dash] \arrow[dd, dash] & \mathrm{Gal}(\mathbb{L}/\mathbb{L})=1 \arrow[dd, dash] \\
 & \mathbb{K}=\mathbb{F}_r \arrow[ur, dash] \arrow[dd, dash] & & \\
 & & \mathbb{F}_{r-1}(\omega)=\mathbb{L}_{r-1} \arrow[r, dash] \arrow[dd, dash, dashed] & \mathrm{Gal}(\mathbb{L}/\mathbb{L}_{r-1})=H_{r-1} \arrow[dd, dash, dashed] \\
 & \mathbb{F}_{r-1} \arrow[ur, dash] \arrow[dd, dash, dashed] & & \\
\mathbb{E} \arrow[uuur, dash] \arrow[dddr, dash] & & \mathbb{F}_1(\omega)=\mathbb{L}_1 \arrow[r, dash] \arrow[dd, dash] & \mathrm{Gal}(\mathbb{L}/\mathbb{L}_1)=H_1 \arrow[dd, dash] \\
 & \mathbb{F}_1 \arrow[ur, dash] \arrow[dd, dash] & & \\
 & & \mathbb{F}_0(\omega)=\mathbb{L}_0 \arrow[r, dash] & \mathrm{Gal}(\mathbb{L}/\mathbb{L}_0)=H_0 \\
 & \mathbb{F}=\mathbb{F}_0 \arrow[ur, dash] & &
\end{tikzcd}
$$

□

Theorem 15.100. Let $\mathbb{F}$ be a field with $\mathrm{char}(\mathbb{F})=0$ and $f(x)\in\mathbb{F}[x]$. If G_f is a solvable group, then $f(x)$ is solvable by radicals. [↓]

[↑]

Proof. Let $\mathbb{K}$ be a splitting field of $f(x)$ over $\mathbb{F}$ and $[\mathbb{K}:\mathbb{F}]=n$. Let $\mathbb{L}$ be a splitting field of x^n-1 over $\mathbb{K}$ and $\omega\in\mathbb{L}$ be a primitive n-th root of unity. We have $\mathbb{L}=\mathbb{K}(\omega)$. Put $\mathbb{E}=\mathbb{F}(\omega)$. Then, $\mathbb{L}$ is a splitting of $f(x)$ over $\mathbb{E}$.[11] Since $H=\mathrm{Gal}(\mathbb{L}/\mathbb{E})$ embeds into $\mathrm{Gal}(\mathbb{K}/\mathbb{F})\cong G_f$, H is also a solvable group, by Section 15.10. Note that $\mathbb{E}/\mathbb{F}$ is a simple radical extension. Thus, if we show that $\mathbb{L}/\mathbb{E}$ is a radical extension, then we are done. (Proposition 13.3.)

Since H is finite, by Proposition 10.13, we have an abelian series

$$1=H_k\trianglelefteq H_{k-1}\trianglelefteq\cdots\trianglelefteq H_0=H$$

[11]The embedding is given as $\sigma\mapsto\sigma_{\mathbb{K}}$. It is injective because σ fixes ω to begin with.

such that H_i/H_{i+1} is cyclic of prime order p_{i+1} for $i = 0, \ldots, k-1$. Note that $n = p_1 \cdots p_k$.

Let $\mathbb{E}_i := \mathbb{L}^{H_i}$ for $i = 1, \ldots, k$. Then, $[\mathbb{E}_i : \mathbb{E}_{i-1}] = |H_{i-1}/H_i| = p_i$. Since $\mathbb{E}_{i-1}$ contains ω, it has a primitive p_i-th root of unity. Thus, $\mathbb{E}_i/\mathbb{E}_{i-1}$ is a simple radical extension, by Theorem 9.10. Thus, $\mathbb{L}/\mathbb{E}$ is a radical extension. $\square$