Galois Theory

IKHAN CHOI

Contents

1. Basic field theory 1
1.1. Field extensions 2
1.2. Polynomial rings 2
1.3. Characteristic 3
2. Algebraic extensions 3
2.1. Algebraic elements 3
2.2. Algebraic extensions 6
2.3. Algebraic closures 7
3. Separable extensions 10
3.1. Separable polynomials 10
3.2. Separable extensions 11
3.3. Separable closures 11
4. Normal extensions 12
4.1. Automorphism group 12
4.2. Normal extensions 12
5. Galois theory 12
5.1. Galois correspondence 12
5.2. Insolvability of quintics 12
5.3. Finite fields 12
5.4. Cyclotomic fields 13
6. Computational techniques 13
6.1. General strategies 13
6.2. Quartic 13

1. Basic field theory

Definition 1.1. A *field* is a commutative division ring.

Proposition 1.1. *A field homomorphism is either a zero morhpism or injective.*

Proof. The kernel is an ideal in a field so that it should be either entire or zero. □

A nontrivial field homomorphism is often called an *embedding* or an *isomorphism onto a subfield*. A field isomorphism is just a surjective field embedding.

First Written : November 19, 2019.
Last Updated : November 19, 2019.

1.1. **Field extensions.**

Definition 1.2. A *field extension* is a pair of fields (E, F) such that $E \geq F$, i.e. F belongs to E as a subset. We often denote it by E/F.

A field E is also called a *field extension* or a*superfield* of another field F if $E \geq F$. Our goal is to understand field extensions.

Proposition 1.2. *Let E/F be a field extension. Then, E is a vector space over F.*

Proof. Obvious. □

Definition 1.3. A *degree* of a field extension E/F is the dimension of the vector space E over F and denoted by $[E : F]$. A field extension is called *finite* if its degree is finite.

Theorem 1.3. *If K is an intermediate field in a field extension E/F, then*

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

Proof. Boring basis counting. □

Corollary 1.4. *Finite extension of finite extension is finite.*

Simple extension is a field extension by an element. It is very useful when we consider where specific element goes to through a given field homomorphism.

Definition 1.4. A field extension E/F is called *simple* if there is an element $\alpha \in E$ such that E is the smallest field containing both α and F. In this case, we write $E = F(\alpha)$.

Lemma 1.5. *Let E/F be a finite extension. There is a finite tower of finite simple extensions.*

Although it is hard to find a counterexample, there is a finite extension which is not simple. We will see in Section 3.

1.2. **Polynomial rings.**

1.2.1. *Review on integral domains.*

Proposition 1.6. *In PID R,*

(1) *every irreducible element is prime,* *(Euclid's lemma)*
(2) *every two elements has greatest common divisor,* *(existence of gcd)*
(3) *the gcd is given as a R-linear combination,* *(Bźout's identity)*
(4) *factorization into primes is unique up to permutation,* *(UFD)*
(5) *every prime ideal is maximal.* *(Krull dimension 1)*

Notice that, since $F[x]$ is a PID, there exists a one-to-one correspondence:

$$\begin{tikzcd}
\text{\textbf{M}aximal \textbf{I}deals} \arrow[rr, bend left, dashed, "\text{generator}"] & & \text{\textbf{M}onic \textbf{I}rreducibles} \arrow[ll, bend left, dashed, "\text{principal ideal}"]
\end{tikzcd}$$

by (1) and (5) in the previous proposition.

1.2.2. *Polynomial ring over a field.*

Proposition 1.7. *If F is a field, then $F[x]$ is a ED.*

Proposition 1.8. *If R is a UFD, then $R[x]$ is also a UFD.*

We can summarize as:

$$\begin{tikzcd}
F \arrow[d] & F[x] \arrow[d] & F[x,y] \arrow[d] & F[x,y,z] \arrow[d] & \cdots \\
\text{Field} & \text{ED (hence PID)} & \text{UFD} & \text{UFD} & \cdots
\end{tikzcd}$$

1.3. **Characteristic.** Frobenius endomorphism.

2. Algebraic extensions

2.1. **Algebraic elements.** Finite simple extensions are the most basic examples of the field extensions that we should become perfectly familiar with them. An element that generates a finite simple extension field is called algebraic. For these elements, we can define minimal polynomials and conjugates for algebraic elements. The minimal polynomial is an essential tool to compute basic information of a given finite simple extension such as its degree. Conjugates are for useful when we construct a map between finite simple field extensions.

2.1.1. *Minimal polynomial.*

Definition 2.1. Let E/F be a field extension. An element $\alpha \in E$ is *algebraic over F* if the simple extension $F(\alpha)/F$ is finite. If α is not algebraic over F, we call it *transcendental* over F.

Proposition 2.1. *Let E/F be a field extension and $\alpha \in E$. TFAE:*

(1) *α is algebraic over F,*
(2) *there is a nonzero polynomial $f \in F[x]$ such that $f(\alpha) = 0$, in other words, an ideal given by the kernel of ring homomorphism*
$$\mathrm{eval}_\alpha : F[x] \to F[\alpha] : f(x) \mapsto f(\alpha)$$
is nonempty,
(3) *$F(\alpha) = F[\alpha]$, i.e. $F[\alpha]$ is a field.*

Proof. (1) ⇒ (2). Since $d = [F(\alpha) : F] < \infty$, we can find a linearly dependent finite subset of infinite set $\{1, \alpha, \alpha^2, \cdots\} \subset F(\alpha)$ over F. The coefficients on the linear dependency relation construct the polynomial.

(2) ⇒ (3). The kernel of eval_α is a prime ideal because the quotient $F[x]/\ker(\mathrm{eval}_\alpha) \cong \mathrm{im}(\mathrm{eval}_\alpha) = F[\alpha]$ is an integral domain. It is also maximal since $F[x]$ is a PID(Krull dimension 1). Therefore, the quotient $F[\alpha]$ is a field.

(3) ⇒ (2). There is $g \in F[x]$ such that $\alpha^{-1} = g(\alpha)$. Then, $f \in F[x]$ defined by $f(x) = xg(x) - 1$ satisfies $f(\alpha) = 0$.

(2)+(3) ⇒ (1). If there is $f \in F[x]$ with $f(\alpha) = 0$, then we can show every element $g(\alpha)$ of $F(\alpha) = F[\alpha]$ for some $g \in F[x]$ is represented as a linear combination of

$\{1, \alpha, \cdots, \alpha^{\deg f - 1}\}$ by the Euclidean algorithm; divide g by f. Therefore, a finite set spans $F(\alpha)$, so the dimension $F(\alpha)$ over F is finite. □

Since the ideal $\ker(\mathrm{eval}_\alpha) \subset F[x]$ for algebraic $\alpha \in E$ is maximal, the following definition makes sense:

Definition 2.2. Let E/F be a field extension and $\alpha \in E$ is algebraic. The unique monic irreducible polynomial $\mu_{\alpha,F} \in F[x]$ satisfying

$$\mu_{\alpha,F}(\alpha) = 0$$

is called the *minimal polynomial of* α *over* F.

Theorem 2.2. *Let* E/F *be a field extension and* $\alpha \in E$ *is algebraic. Then,*

$$F(\alpha) \cong F[x]/(\mu_{\alpha,F}).$$

In particular, $[F(\alpha) : F] = \deg \mu_{\alpha,F}$.

Proof. The kernel of $\mathrm{eval}_\alpha : F[x] \to F(\alpha)$ is characterized as the principal ideal generated by $\mu_{\alpha,F}$, so we find the isomorphism $F[x]/(\mu_{\alpha,F}) \cong F(\alpha)$.

Now we claim the dimension of $F[x]/(f)$ over F is the degree of $f \in F[x]$. It is enough to show $\{1, x, \cdots, x^{d-1}\}$ is a basis where $d = \deg f$. We can check this with the Euclidean algorithm. □

Example 2.1. Consider a field extension $\mathbb{C}/\mathbb{Q}$. The minimal polynomial of $\sqrt{2} \in \mathbb{C}$ over $\mathbb{Q}$ is $x^2 - 2$ since it is monic irreducible and has a root $\sqrt{2}$. Similarly, the minimal polynomial of $\frac{-1+\sqrt{-3}}{2} \in \mathbb{C}$ over $\mathbb{Q}$ is $x^2 + x + 1$.

Example 2.2. We can compute the degree of a field extension by finding minimal polynomial. Since the minimal polynomial $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$ is $x^4 - 10x^2 + 1$, we have $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = 4$.

On the other hand, recall that we have

$$\Big[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}\Big] = \Big[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})\Big] \cdot \Big[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}\Big] = 2 \cdot 2 = 4.$$

Also, $\sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ implies $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \leq \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Since the dimensions as vector spaces are equal, we get $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. We can also directly check

$$\sqrt{2} = \frac{1}{2}\left(\alpha - \frac{1}{\alpha}\right) \quad \text{and} \quad \sqrt{3} = \frac{1}{2}\left(\alpha + \frac{1}{\alpha}\right),$$

where $\alpha = \sqrt{2} + \sqrt{3}$. This kind of *dimension argument* is one of powerful tools to attack field theory. It will be discovered later that the dimension argument has an analogy with computation of group orders in finite group theory.

Example 2.3. The base field is important: we have

$$\mu_{\sqrt{2},\mathbb{Q}}(x) = x^2 - 2, \quad \text{but} \quad \mu_{\sqrt{2},\mathbb{Q}(\sqrt{2})}(x) = x - \sqrt{2}.$$

Example 2.4. Although $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(1 + \sqrt{2})$, the minimal polynomials of $\sqrt{2}$ and $1 + \sqrt{2}$ over $\mathbb{Q}$ are $x^2 - 2$ and $(x-1)^2 - 2$ respectively. Polynomials are usually used in order to be provided as a computational tool, so we frequently want to find a suitable minimal polynomial for a given field extension. However, note that a finite simple extension does not specify only one minimal polynomial as the above example. It is enough to find a suitable minimal polynomial that is easy to compute.

2.1.2. *Conjugates.*

Definition 2.3. Let E/F be a field extension and $\alpha, \beta \in E$ be algebraic over F They are said to be *conjugate over F* if they share a common minimal polynomial over F.

In other words, conjugates share the maximal ideal ker(eval), hence we get that $F(\alpha)$ and $F(\beta)$ are isomorphic. For the practical isomorphism map, we have the following theorem. It is also useful when we compute field automorphisms explicitly.

Theorem 2.3 (Conjugation isomorphism)**.** *Let E/F be a field extension and $\alpha, \beta \in E$. A map*

$$\phi : F(\alpha) \to F(\beta) : \alpha \mapsto \beta$$

fixing F is a well-defined field homomorphism iff they are conjugates over F. In addition, if that is the case, ϕ is in fact an isomorphism.

Proof. ($\Leftarrow$) Notice that the two conditions $\phi(\alpha) = \beta$ and $\phi|_F = \mathrm{id}_F$ force ϕ to be unique. Let $\mu \in F[x]$ be the common minimal polynomial of α and β over F and consider a map

$$\psi : F(\alpha) \xrightarrow{\sim} F[x]/(\mu) \xrightarrow{\sim} F(\beta) : \alpha \mapsto x + (\mu) \mapsto \beta.$$

The intermediate isomorphisms are given by the quotient of evaluation maps. Since $\psi(\alpha) = \beta$ and $\psi|_F = \mathrm{id}_F$, we have $\psi = \phi$. It shows that ϕ is a well-defined field isomorphism.

($\Rightarrow$) Suppose ϕ is a field homomorphism fixing F. Then, ϕ commutes with a polynomial function with coefficients in F. From

$$\mu_{\alpha,F}(\beta) = \mu_{\alpha,F}(\phi(\alpha)) = \phi(\mu_{\alpha,F}(\alpha)) = \phi(0) = 0,$$

we get $\mu_{\beta,F} \mid \mu_{\alpha,F}$. The irreducibility of $\mu_{\alpha,F}$ implies $\mu_{\alpha,F} = \mu_{\beta,F}$. □

Corollary 2.4. *Let $\phi : F \to F$ is a field automorphism. Then, α and $\phi(\alpha)$ are always conjugates.*

Example 2.5. The base fields are important. There are two conjugates of $\sqrt{2} \in \mathbb{C}$ over $\mathbb{Q}$: $\pm\sqrt{2}$. However, there is only one conjugate of $\sqrt{2}$ over $\mathbb{Q}(\sqrt{2})$ or $\mathbb{C}$: itself.

Example 2.6. There are two conjugates of $\omega := \frac{-1+\sqrt{-3}}{2} \in \mathbb{C}$ over $\mathbb{Q}$: ω and $\overline{\omega}$. It means that there are only two automorphisms on $\mathbb{Q}(\omega)$: one is identity, and the other is the complex conjugation.

Example 2.7. Two different conjugates can define a same field homomomorphism. See Section 3.

Example 2.8. The isomorphism does not have to be an automorphism. There are four conjugates of $\sqrt[4]{2}$ over $\mathbb{Q}$: $\pm\sqrt[4]{2}$ and $\pm i\sqrt[4]{2}$. However, $\mathbb{Q}(\sqrt[4]{2}) \neq \mathbb{Q}(i\sqrt[4]{2})$ even though they are isomorphic. See Section 4.

2.2. **Algebraic extensions.**

Algebraic extension is a generalization of finite extensions, for instance, every finite extension. In Galois theory, which will be studied later, we will not care elements that are not algebriac. Therefore, it is natural to think of a field extension that only consists of algebraic elements, which is called also algebraic. The main interests in Galois theory will be restricted to algebraic extensions. To people who know the category theory, an algebraic extension is just a direct limit of finite simple extensions.

Definition 2.4. A field extension E/F is called *algebraic* if all elements $\alpha \in E$ are algebraic over F.

The easiest example of an algebraic extension is a finite extension. The relations between finite extensions and algebraic extension are as follows.

Proposition 2.5. *For finite extensions and algebraic extensions, we have:*

(1) *a finite extension is algebraic,*
(2) *a simple algebraic extension is finite.*

Proof. Easy. □

Now, we are going to get some basic criteria for determining or constructing algebraic extensions. If summarized, we can just say any basic operations of algebraic extensions are algebraic. Before that, we introduce a good notion about algebraic extensions: the set of all algebraic elements in a given field.

In the rest of this subsection, assume that we have fixed a sufficiently large ambient field L. Restricting the "domain of discourse" by assuming a large entire field is a greatly helpful idea in order not to be confused in the theory of extensions. For example, if we do not fix such a field L, we might be able to consider useless large fields which may grow without limits. Moreover, we cannot think about the number of field extensions satisfying particular properties.

Note that the following definition *depends on the choice of* L, and we will use it *only in this subsection.*

Definition 2.5. Let $\overline{F}$ denote the set of all algebraic elements in L over F.

Proposition 2.6. *The set $\overline{F}$ of F in L is always a field.*

Proof. An element is algebraic over F if and only if it is contained in a finite extension E/F because $\alpha \in E$ is equivalent to $F(\alpha) \leq E$.

Let $\alpha, \beta \in L$ be nonzero algebraic elements over a field F. Since $\alpha + \beta$, $\alpha\beta$, and α^{-1} are all in $F(\alpha, \beta)$, which is a finite extension of F with degree $\deg_F(\alpha)\deg_F(\beta)$, the set of algebraic elements over F in L is a field. □

Remark. The field $\overline{F}$ is called the *relative algebraic closure of F in L.* Since we have not defined algebraic closures yet, we will only adopt the notation. The reason of the word "relative" is explained later. Also, honestly, the notation $\overline{F}$ is not so good that it is often used to represent an algebraic closure, not a relative one. We, however, proceed with this notation to grasp concepts of algebraic extensions.

Lemma 2.7. *Let $E, F \leq L$ be fields. Then,*

(1) *$F \leq E$ implies $\overline{F} \leq \overline{E}$,*

(2) $\overline{\overline{F}} = \overline{F}$.

Proof. (1) Suppose $\alpha \in \overline{F}$ so that there is $f \in F[x]$ such that $f(\alpha) = 0$. Since $f \in F[x] \subset E[x]$, the element α is also algebraic over E, hence $\alpha \in \overline{E}$.

(2) It is enough to show $\overline{\overline{F}} \subset \overline{F}$. Let $\alpha \in \overline{\overline{F}}$ so that we can find $f \in \overline{F}[x]$ such that

$$f(\alpha) = \sum_{i=0}^{n} a_i \alpha^i = 0.$$

If we consider the field $E = F(a_0, \cdots, a_n)$ of coefficients, then $f \in E[x]$. In other words, α is algebraic over E.

The field extension E/F is finite since all generators a_i are algebraic over F, and $E(\alpha)/E$ is also finite since α is algebraic over E. Therefore, the field extension $E(\alpha)/F$ is finite, and $F(\alpha)/F$ is also finite, hence the algebraicity of α over F. □

Lemma 2.8. *Let $E, F \leq L$ be fields. A field extension E/F is algebraic iff $\overline{E} = \overline{F}$.*

Proof. If E/F is algebraic, then $F \leq E \leq \overline{F}$ implies $\overline{F} \leq \overline{E} \leq \overline{\overline{F}} = \overline{F}$. Conversely, if $\overline{E} = \overline{F}$, then $\alpha \in E$ implies $\alpha \in E \leq \overline{E} = \overline{F}$, hence E is algebraic over F. □

Theorem 2.9. *Let K be an intermediate field of a field extension E/F. Then, E/F is algebraic iff E/K and K/F are algebraic.*

Proof 1. Choose a big L. Since $\overline{E} \geq \overline{K} \geq \overline{F}$, we have $\overline{E} = \overline{F}$ iff $\overline{E} = \overline{K}$ and $\overline{K} = \overline{F}$. □

Proof 2. A direct proof uses the argument in the proof of above lemma as follows: if we take $\alpha \in E$ that is algebraic over K, and if a_i denotes the coefficients of $\mu_{\alpha,K}$, then the field extension $F(a_1, \cdots, a_n, \alpha)/F$ is finite, so α is algebriac over F. □

Theorem 2.10. *Let E_1/F and E_2/F are algebraic extensions in a superfield L. Then, the compositum E_1E_2/F is algebriac.*

Proof. Choose a big L. Since $E_1, E_2 \leq \overline{F}$, we have $E_1E_2 \leq \overline{F}$, so $\overline{E_1E_2} = \overline{F}$. □

Remark. An algebraic extension is a direct limit of finite extensions. In other words, a field E is algebraic over F if and only if there is a tower of fields $\{K_\alpha\}_\alpha$ such that K_α/F are all finite and the ascending union is E. We skip the proof.

Example 2.9. For a transcendental number such as π, an extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ is not algebraic since it contains an element that is not algebraif. To give another reason, that is because a simple extension is algebraic if and only if it is finite.

Example 2.10. Finite extensions are not only the algebraic extensions. For examples,

$$\mathbb{Q}(\sqrt{2}, \sqrt[4]{2}, \sqrt[8]{2}, \cdots), \quad \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \cdots)$$

are infinite algebraic extensions.

2.3. **Algebraic closures.**

Algebraic closure is intuitively a maximal algebraic extension. It is well described using the notion of algebraically closed fields. Although the existence will be proved later, we give definitions.

2.3.1. *Algebraically closed fields.*

Definition 2.6. A field F is called *algebraically closed* if it has no proper algebraic extension.

Proposition 2.11. *For a field F, TFAE:*

1. *F is algebraically closed,*
2. *every polynomial in $F[x]$ has a root in F,*
3. *every polynomial in $F[x]$ is linearly factorized in F; every root is in F.*

Proof. (1) ⇒ (2) If $f \in F[x]$ does not have root in F, then the proper finite extension $(F[x]/(f))/F$ shows that F is not algebraically closed.

(2) ⇒ (3) If f has a root α, then we can inductively apply this theorem for a new polynomial $f(x)/(x-\alpha)$ of a lower degree to make the complete linear factorization.

(3) ⇒ (1) If F is not algebraically closed so that there is a proper algebraic extension E/F, then the minimal polynomial $\alpha \in E \setminus F$ should be irreducible with degree bigger than 1. □

Remark. In particular, this proposition implies that algebraically closedness can be described in itself by factorizations. Namely, it is an internal property; it is preserved under isomorphisms.

Definition 2.7. A field $\overline{F}$ is called an *algebraic closure* of a field F if $\overline{F}$ is algebraically closed field and $\overline{F}/F$ is algebraic.

Proposition 2.12. *Let E/F be a field extension with E algebraically closed. Then the set of all algebraic elements in E over F is the only algebraic closure of F contained in E.*

Proof. For a while in this proof, let $\overline{F}$ denote the set of all algebraic elements of F in E.

Step 1: Algebraic closure. We will show that $\overline{F}$ is algebraically closed because the extension $\overline{F}/F$ is clearly algebraic. Let $f \in \overline{F}[x]$ and take a root $\alpha \in E$. Since both $\overline{F}(\alpha)/\overline{F}$ and $\overline{F}/F$ are algebraic, α is algebraic over F. Thus we have $\alpha \in \overline{F}$, and by the previous proposition, $\overline{F}$ is algebraically closed.

Step 2: Uniqueness. Suppose K is an algebraic closure of F in E. We have $\overline{F} \leq K$ since every algebraic element α with $f(\alpha) = 0$ for $f \in F[x] \subset K[x]$ should be contained in K. Also, $K/\overline{F}$ is algebraic because K/F is algebraic. Since $\overline{F}$ is algebraically closed, $K = \overline{F}$. □

This is a relation with relative algebraic closure: the relative algebraic closure in a algebraically closed field is really an algebraically closure. The proposition allows us to choose a standard algebraic closure when provided a large superfield like $\mathbb{C}$. In number theory, it is convenient for all algebraically closed fields to be considered that they are in $\mathbb{C}$.

Example 2.11. The set of all complex numbers $\mathbb{C}$ is an algebraically closed field by the fundamental theorem of algebra.

Example 2.12. The set of all algebraic numbers (over $\mathbb{Q}$) is an algebraically closed field by the proposition above and is a subfield of $\mathbb{C}$.

2.3.2. *Uniqueness and existence.* Here is a useful lemma that allows to apply the axiom of choice to field theory.

Theorem 2.13 (Isomorphism extension theorem)**.** *Let E/F be an algebraic extension. Let $\phi : F \cong F'$ be a field isomorphism. Let $\overline{F}'$ be an algebraic closure of F'. Then, there is an embedding $\widetilde{\phi} : E \to \overline{F}'$ which extends ϕ.*

$$\begin{tikzcd}
 & \overline{F}' \arrow[dd, dash] \\
E \arrow[ur, "\widetilde{\phi}"] \arrow[d, dash] & \\
F \arrow[r, "\phi"] & F'
\end{tikzcd}$$

Proof. Let S be the set of all field homomorphisms $K \to \overline{F}'$ which extends ϕ and satisfies $K \leq E$. The set S is nonempty since $\phi \in S$ and satisfies the chain condition since the increasing union defines the upper bound of chain. Use the Zorn lemma on S to obtain a maximal element $\widetilde{\phi} : K \to \overline{F}'$. We want to show $K = E$.

Suppose K is a proper subfield of E and let $\alpha \in E \setminus K$. Let $\alpha' \in \overline{F}'$ be a root of the pushforward polynomial $\phi_*(\mu_{\alpha,F}) \in F'[x]$. Then, we can construct a field homomorphism $K(\alpha) \to \overline{F}' : \alpha \mapsto \alpha'$. It leads a contradiction to the maximality of $\widetilde{\phi}$. Therefore, $K = E$. □

Theorem 2.14 (Uniqueness of algebraic closure)**.** *Algebraic closure is unique up to isomorphism.*

Proof. Suppose there are two algebraic closures $\overline{F}_1, \overline{F}_2$ of a field F. By the isomorphism extension theorem, we have a field homomorphism $\phi : \overline{F}_1 \to \overline{F}_2$ which extends the identitiy map on F. Since the image $\phi(F_1)$ is also algebraically closed and the field extension $F_2/\phi(F_1)$ is algebraic, we must have $\phi(F_1) = F_2$ by the definition of algebraically closedness. Thus, ϕ is surjective so that it is an isomorphism. □

Theorem 2.15 (Existence of algebraic closure)**.** *Every field has an algebraic closure.*

Proof. Let F be a field.

Step 1: Construct an algebraically closed field containing F. At first we want to construct a field $K_1 \geq F$ such that every $f \in F[x]$ has a root in K_1. This is satisfied by $K_1 := R/\mathfrak{m}$, where a ring R and its maximal ideal $\mathfrak{m}$ is defined as follows: Let S be the set of all nonconstant irreducibles in $F[x]$. Define $R := F[\{x_f\}_{f \in S}]$. Let I be an ideal in R generated by $f(x_f)$ as f runs through all S. It has a maximal ideal $\mathfrak{m} \supset I$ in R since I does not contain constants. If $f \in F[x]$, then $\alpha = x_f + \mathfrak{m} \in K_1$ satisfies $f(\alpha) = f(x_f) + \mathfrak{m} = \mathfrak{m}$.

Construct a sequence $\{K_n\}_n$ of fields inductively such that every nonconstant $k \in K_n[x]$ has a root in K_{n+1}. Define $K := \lim_{\to} K_n$ as the inductive limit. It is in other word just the directed union of K_n through all $n \in \mathbb{N}$. Then, K is easily checked to be algebraically closed.

Step 2: Construct the algebraic closure of F. Let $\overline{F}$ be the set of all algebraic elements of K over F. Then, this is an algebraic closure. □

Remark. In fact, this K_1 is already algebraically closed, but it is hard to prove directly, so we are going to construct another algebraically closed field, K.

3. Separable extensions

3.1. Separable polynomials.

Definition 3.1. Let F be a field. A polynomial $f \in F[x]$ is called *separable* if it is square-free in $\overline{F}[x]$. An element $\alpha \in \overline{F}'$ is called *separable* over F if $\mu_{\alpha,F}$ is separable.

The separability of a polynomial does not depend on coefficient fields, but their characteristic. We can consider the algebraic closure of the smallest field containing coefficients of the polynomial and its characteristic when we check separability of a polynomial.

3.1.1. *Formal derivatives.*

Definition 3.2. Let $f \in F[x]$ for a field F such that

$$f(x) = \sum_{i=0}^{n} a_i x^i$$

The *formal derivative* of f is defined as a polynomial $f' \in F[x]$ such that

$$f'(x) := \sum_{i=1}^{n} i a_i x^{i-1}.$$

We can easily check that this definition satisfies the Leibniz rule.

Proposition 3.1. *Let $f \in F[x]$ for a field F. Then, f is separable iff f and f' are coprime in F.*

Proof. The polynomials f, f' is linearly factorized in $\overline{F}$.

($\Leftarrow$) Suppose f is not separable so that it has a multiple root $\alpha \in \overline{F}$ and

$$f(x) = (x-\alpha)^m g(x)$$

for an integer $m \geq 2$ and a polynomial $g \in F[x]$. Its derivative is

$$f'(x) = m(x-\alpha)^{m-1} g(x) - (x-\alpha)^m g'(x).$$

Since $f(\alpha) = f'(\alpha) = 0$, we have $\mu_{\alpha,F} \mid \gcd(f, f')$. They are not coprime in F.

($\Rightarrow$) Suppose f and f' are not coprime in F so that they has a common factor. Let $\alpha \in \overline{F}$ be a root of the common factor. If we write

$$f(x) = (x-\alpha)g(x), \qquad f'(x) = g(x) + (x-a)g'(x),$$

then we can see $g(\alpha) = 0$ and $(x-\alpha) \mid g$ in $\overline{F}[x]$. Hence $(x-\alpha)^2 \mid f$, so f is not separable. □

Remark. This is a powerful checking tool because the proposition do not requires that f and f' are coprime in $\overline{F}$, but in just F.

Example 3.1. Let $f(x) = x^{p^n} - x$ be a polynomial over a field of characteristic $p > 0$. Since $f'(x) = -1$, f is separable.

3.1.2. *Relation to irreducibles.*

Definition 3.3. A *perfect field* is a field over which every irreducible is separable.

Corollary 3.2. *A polynomial over a perfect field is separable iff it is a product of distinct irreducibles.*

Proposition 3.3. *Let F be a field of characteristic 0. Then, F is perfect.*

Proof. Let $f \in F[x]$ be an irreducible of degree n. Notice that f and g are not coprime iff $f \mid g$. Since F has characteristic 0, f' has degree $n-1$ and is nonzero, so we have $f \nmid f'$. Hence f is separable. □

Proposition 3.4. *Let F be a field of characteristic $p > 0$. Then, F is perfect iff F has the Frobenius automorphism.*

Proof. ($\Leftarrow$) Let $f \in F[x]$ be an inseparable irreducible. Since we must have $f' = 0$ by the irreducibility of f, we can find $g \in F[x]$ such that $f(x) = g(x^p)$. The coefficients of g are p-powers of elements of F, so there is $h \in F[x]$ such that $g(x^p) = h(x)^p$. It is a contradiction to the irreducibility of f. □

Corollary 3.5. *The rational field $\mathbb{Q}$ and every finite fields are perfect.*

Proposition 3.6. *Let F be a field of characteristic $p > 0$. For an irreducible $f \in F[x]$, there is a unique separable irreducible $f_{\mathrm{sep}} \in F[x]$ such that $f(x) = f_{\mathrm{sep}}(x^{p^k})$ for some k.*

Example 3.2. The Frobenius endomorphism is not surjective in the field of rational functions $\mathbb{F}_p(t)$, where t is not algebraic over $\mathbb{F}_p$. For example, t is not in the image of $\mathbb{F}_p(t) \to \mathbb{F}_p(t) : x \mapsto x^p$. Then, the polynomial $x^p - t \in \mathbb{F}_p(t)[x]$ is inseparable irreducible since it is factorized as

$$x^p - t = (x - t^{\frac{1}{p}})^p$$

in $\overline{\mathbb{F}_p(t)}[x]$.

3.2. **Separable extensions.**

Definition 3.4. A field extension E/F is called *separable* if all elements in E is separable over F.

Theorem 3.7 (Primitive element theorem)**.** *A finite separable extension is simple.*

3.3. **Separable closures.**

Definition 3.5. Let E/F be a field extension. The *separable degree* of E/F is the number $[\overline{F}^{\mathrm{sep}} : F]$.

3.3.1. *Field embeddings.*

Theorem 3.8. *The separable degree of a field extension E/F is the number of field embeddings $E \hookrightarrow \overline{F}$ fixing F.*

Lemma 3.9. *All roots of an irreducible polynomial has same multiplicity.*

Proof. □

Theorem 3.10. *Let K be an intermediate field of a finite extension E/F. Then,*

$$[E:F]_{\text{sep}} \mid [E:F]$$

Proof. □

Theorem 3.11. *A finite field extension E/F is separable if and only if*

$$[E:F]_{\text{sep}} = [E:F].$$

Proof. □

multiplcation formula

4. Normal extensions

4.1. **Automorphism group.**

4.2. **Normal extensions.**

5. Galois theory

5.1. **Galois correspondence.**

5.2. **Insolvability of quintics.**

5.3. **Finite fields.**

Lemma 5.1 (Frobenius endomorphism)**.** *Let F be a field of characteristic p. Then, the map $\sigma : x \mapsto x^p$ is a field endomorphism on F.*

Theorem 5.2. *Let L denote an algebraically closed field of characteristic $p > 0$. In L, the set of all finite subfields is described as a totally ordered set*

$$\{\mathbb{F}_p, \mathbb{F}_{p^2}, \mathbb{F}_{p^3}, \cdots\},$$

where $\mathbb{F}_q$ denotes a field of order q.

Proof. Step 1: Non-existence. The identity 1 is contained in every finite subfield of L, so is the field $\mathbb{F}_p$, hence the finite dimensional vector space over $\mathbb{F}_p$. Thus, the order of a finite field of characteristic p is a power of p.

Step 2: Existence. Let $q = p^n$ for $n \in \mathbb{Z}_{>0}$. Consider the set F of roots of the polynomial

$$f(x) = x^q - x$$

in L. We claim that F forms a field, the splitting field of f.

Clearly F is nonempty: $0 \in F$. Let $\alpha, \beta \in F$. Since $\sigma^n : x \mapsto x^q$ gives a field homomorphism, we have

$$(\alpha - \beta)^q = \alpha^q - \beta^q = (\alpha - \beta)$$

and

$$(\alpha\beta)^q = (\alpha\beta).$$

Also, we have $\alpha\alpha^{-1} = \alpha^{-1}\alpha = 1$ if we define $\alpha^{-1} := \alpha^{q-2}$ for nonzero $\alpha \in F$. Therefore, F is a field.

Step 3: Uniqueness. Let F be a finite subfield of L of order q. Then, every nonzero element $\alpha \in F$ satisfies $\alpha^{q-1} = 1$ since q is contained in a group $\mathbb{F}^\times$ of order $q - 1$, and it implies α satisfies $x^q - x = 0$ for all $\alpha \in F$. Since the number of roots of $x^q - x = 0$ is less or equal than q, we can conclude every finite subfield of L is characterized as the splitting field of a polynomial of the form $x^q - x$. □

Theorem 5.3. *The multiplicative group of $\mathbb{F}_{p^n}^{\times}$ is cyclic.*

Theorem 5.4. *The Galois group $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is cyclic.*

5.4. Cyclotomic fields.

6. Computational techniques

6.1. General strategies.

- reducible case, irreducible<=>transitivity
- resolvent polynomial1: discriminant
- resolvent polynomial2: cubic resolvent
- double quadratic, reciprocal equation: finding symmetry
- number of imaginary roots=2n: composition of n transpositions
- $x^n - \alpha$: Jacobson-Velez
- reduction modulo p (over $\mathbb{F}_p$)

6.2. Quartic.

In this section, we assume the following setting:

- F is a perfect field,
- f is an irreducible quartic over F,
- E is the splitting of f over F,
- $G = \mathrm{Gal}(E/F)$,
- $H = G \cap V_4$.

Theorem 6.1. *There are only five isomorphic types of transitive subgroups of the symmetric group S_4.*

Corollary 6.2. *$G \cong S_4,\ A_4,\ D_4,\ V_4,$ or C_4.*

Proposition 6.3. *Two groups A_4 and V_4 are only transitive normal subgroups of S_4.*

Now we define our resolvent polynomial.

Proposition 6.4. *Let K be the fixed field of H. Then,*

$$K = F(\alpha_1\alpha_2 + \alpha_3\alpha_4,\ \alpha_1\alpha_3 + \alpha_2\alpha_4,\ \alpha_1\alpha_4 + \alpha_2\alpha_3).$$

Definition 6.1. Let K be the fixed field of H. A *resolvent cubic* is a cubic R_3 that has K as the splitting field over F.

Theorem 6.5. *We have*

1. *$G \cong S_4$ if R_3 is irreducible and ,*
2. *$G \cong A_4$ if R_3 is irreducible and ,*
3. *$G \cong D_4$ if R_3 has only one root in K and f is irreducible over K,*
4. *$G \cong C_4$ if R_3 has only one root in K and f is reducible over K,*
5. *$G \cong V_4$ if R_3 splits in K.*

Proof. There are five possible cases:

$$(G,H) = (S_4,V_4),\ (A_4,V_4),\ (D_4,V_4),\ (V_4,V_4),\ (C_4,C_2).$$

We have

$$[K:F] = |G/H|, \qquad [E:K] = |H|.$$

If f is reducible over K, then $\mathrm{Gal}(E/K)$ is no more a transitive subgroup of S_4 so that $H \neq V_4$ and $G \cong C_4$. □

$$\begin{tikzcd}
E \arrow[rrrr] & & & & 1 \arrow[d, dashed, "2"] & \\
& & & & C_2 \arrow[dl, dashed, "2"'] \arrow[dr, dashed, "2"] & \\
K = F_{V_4 \cap G} \arrow[uu, dashed] & & & V_4 \arrow[dl, dashed, "3"'] \arrow[dr, dashed, "2"] & & C_4 \arrow[dl, dashed, "2"] \\
F \arrow[u, dashed] \arrow[r] & ? & A_4 \arrow[dr, dashed, "2"'] & & D_4 \arrow[dl, dashed, "3"] & \\
& & & S_4 & &
\end{tikzcd}$$