Galois Theory

IKHAN CHOI

Contents

1. Elementary field theory

1.1. Vector space over a subfield.

Theorem 1.1. *Let E/F be a field extension. Then, E is a vector space over F.*

Proof. Obvious. □

Definition 1.1. A *degree* of a field extension E/F is the dimension of the vector space E over F and denoted by $[E : F]$.

Definition 1.2. A field extension is called *finite* if its degree is finite.

Theorem 1.2 (Multiplicity of degree)**.** *If K is an intermediate field in a field extension E/F, then*

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

Proof. Boring basis counting. □

Corollary 1.3. *Finite extension of finite extension is finite.*

Last Update: June 3, 2019.

1.2. **Field homomorphisms.** Unlike general rings, field homomorphisms is extremely rigid. The following theorem deeply related to Schur's lemma in representation theory, and it holds for not only fields but also division rings.

Proposition 1.4. *A nontrivial field homomorphism is injective.*

Proof. The kernel should be either entire or zero. □

A nontrivial field homomorphism is also called *embedding* or *isomorphism onto a subfield of codomain.* A field isomorphism is just a nontrivial surjective field homomorphism.

1.3. **Simple extensions.** 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 1.3. 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.

2. Algebraic extensions

We do not prove the basic properties of polynomial ring over a field: they satisfy the axioms of ED, PID, and UFD, so every prime ideal is maximal and every irreducible element is prime.

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. Conjugates are for useful when we construct a map between finite simple field extensions.

2.1.1. *Minimal polynomials.* Let us get started from the minimal polynomials.

Definition 2.1 (Algebraic element)**.** 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.

We give some equivalent conditions for algebraicity.

Theorem 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 $f(\alpha) = 0$,*
(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 existence of $f \in F[x]$ such that $f(\alpha) = 0$ implies that the kernel of evaluation ring homomorphism $\mathrm{eval}_\alpha : F[x] \to F[\alpha]$ is nonempty. The kernel 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. □

Note that, due to the fact that $F[x]$ is a PID, there exists a one-to-one correspondence:

$$\begin{tikzcd}
\text{\textbf{M}aximal \textbf{I}deal in } F[x] \arrow[r, bend left, dashed, "\text{generator}"] & \text{\textbf{M}onic \textbf{I}rreducible polynomial in } F[x]. \arrow[l, bend left, dashed, "\text{principal ideal}"]
\end{tikzcd}$$

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

Definition 2.2 (Minimal polynomial)**.** 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.

The following theorem says that we can compute the degree of a finite simple extension via finding the minimal polynomial.

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 2.3. Let the base field is $\mathbb{Q}$. The minimal polynomial of $\sqrt{2}$ is $x^2 - 2$ since it is monic irreducible and has a root $\sqrt{2}$. Similarly, the minimal polynomial of $\frac{-1+\sqrt{-3}}{2}$ is $x^2 + x + 1$.

Example 2.4. The minimal polynomial $\sqrt{2}+\sqrt{3}$ over $\mathbb{Q}$ is x^4-10x^2+1. Therefore, $[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}]=4$.

On the other hand, we have

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

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

Actually, we have

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

where $\alpha=\sqrt{2}+\sqrt{3}$.

Remark. 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 while an element determines the unique minimal polynomial, a finite simple extension does not specify only one polynomial. For example, although $\mathbb{Q}(\sqrt{2})=\mathbb{Q}(1+\sqrt{2})$, the minimal polynomial of each generator over $\mathbb{Q}$ are x^2-2 and $(x-1)^2-2$ respectively. It is enough to find a suitable minimal polynomial that is easy to compute.

2.1.2. *Conjugates.* Now, we begin to define 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 great theorem.

Theorem 2.5 (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 provides a well-defined field isomomorphism iff they are conjugates over F.

Proof. ($\Leftarrow$) To prove well-definedness, since the two conditions that $\phi(\alpha)=\beta$ and ϕ fixes F determines ϕ uniquely, so we just need to show the existence of such ϕ.

Let $\mu\in F[x]$ be the common minimal polynomial of α and β over F. We will show that a map

$$\psi:F(\alpha)\overset{\sim}{\to}F[x]/(\mu)\overset{\sim}{\to}F(\beta)$$

is in fact ϕ. The intermediate isomorphisms are defined by the quotient of evaluation maps. Since we have $\psi(\alpha)=\beta$ and ψ fixes F clearly, ϕ is well-defined. The fact that ϕ is a field isomorphism is followed by ψ.

($\Rightarrow$) Suppose ϕ is an isomorphism 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 2.6. *Let $\phi : F \to F$ is a field automorphism. Then, α and $\phi(\alpha)$ are always conjugates.*

In the following examples, let $E = \mathbb{C}$ and $F = \mathbb{Q}$.

Example 2.7. There are two conjugates of $\sqrt{2}$ over $\mathbb{Q}$: $\pm\sqrt{2}$. However, there is only one conjugate of $\sqrt{2}$ over $\mathbb{Q}(\sqrt{2})$: itself.

Example 2.8. There are two conjugates of $\omega := \frac{-1+\sqrt{-3}}{2}$ over $\mathbb{Q}$: ω and $\overline{\omega}$. It means that there are only two automorphisms on $\mathbb{Q}(\omega)$: one is identity, the other is complex conjugation.

Example 2.9. Two different conjugates can define the same isomomorphism. See Section 3.

Example 2.10. 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.** In Galois theory, we will not care an element that is not algebriac. Therefore, it is natural to think 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 $\alpha \in E$ is 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.

Theorem 2.11. *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 criteria for determining or constructing algebraic extensions. For example, the intersection of algebraic extensions is algebraic. Before that, we introduce a good notion about algebraic extensions, and it is just the set of all algebraic elements in a given field.

Definition 2.5. The set of all algebraic elements in E over F is called *relative algebraic closure* and denoted by $\overline{F}|_E$.

Proposition 2.12. *A relative algebraic closure is a field.*

Proof. □

Lemma 2.13. *Let E/F be a field extension and $L > E$. Then,*

(1) $\overline{F}|_L < \overline{E}|_L$,
(2) $\overline{(\overline{F}|_E)}|_E = \overline{F}|_E$.

Proof. □

Lemma 2.14. *A field extension E/F is algebraic iff $\overline{E}|_L = \overline{F}|_L$ for all field $L > E$.*

Proof. □

Remark. In fact, it is sufficient to check $\overline{E}|_L = \overline{F}|_L$ just for one algebraically closed field L in Lemma 2.14, but since we have not defined the algebraically closed fields yet, we let L be all superfields of E.

Theorems what we want to know are given as follows. They are all obviously proved from the lemmas above, so we give elementary proofs here.

Theorem 2.15. *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. One direction is clear. Suppose E/K and K/F are algebraic. Take $\alpha \in E$ and let L be a field generated by F and the coefficients of $\mu_{\alpha,K}$ so that $\mu_{\alpha,K} \in L[x]$ and $L(\alpha)/L$ is finite. The extension L/F is finite since K/F is algebraic. Since $L(\alpha)/F$ is finite, $F(\alpha)/F$ is finite. □

Theorem 2.16. *Let E/F and E'/F are algebraic extensions in a superfield L. Then, the compositum EE'/F is algebriac.*

Proof. □

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.

There is another important characterization of algebraically closed fields.

Proposition 2.17. *A field F is algebraically closed iff every polynomial in $F[x]$ has a root in F.*

Proof. Easy. □

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. In particular, the theorem implies that algebraically closedness is a 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 2.18. *Let E/F be a field extension with algebraically closed field E. Then the set of all algebraic elements in E over F is the only algebraic closure of F contained in E.*

Proof. The set of algebraic elements is algebraically closed. □

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, algebraically closed fields are all considered to be in $\mathbb{C}$.

Example 2.19. The set of all complex numbers $\mathbb{C}$ is an algebraically closed field by the fundamental theorem of algebra.

Example 2.20. 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 an extremely useful lemma that allows to apply the axiom of choice to field theory.

Theorem 2.21 (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.*

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

Proof. Let S be the set of all field homomorphisms $K \to \overline{F}'$ which extends ϕ and satisfies $K < E$. 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's 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 2.22 (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 2.23 (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 $K_1 > F$ such that every $f \in F[x]$ has a root in K_1. This is satisfied by $K_1 := R/\mathfrak{m}$, where R and $\mathfrak{m}$ is defined as follows: Let S be the set of all irreducibles and nonconstant polynomials 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.

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 union of K_n for 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

Definition 3.1. 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.

Definition 3.2. A field extension E/F is called *separable* if all elements in E is separable over F.

Definition 3.3. The *index* of a field extension E/F is the number of field homomorphisms $E \to \overline{F}$ fixing F. It is denoted by $\{E : F\}$.

Proposition 3.1. *All roots of an irreducible polynomial has same multiplicity.*

Proof. □

Theorem 3.2. *Let K be an intermediate field of a finite extension E/F. Then,*

$$\{E : F\} \mid [E : F]$$

Proof. □

3.1. Separable closures.

3.2. Perfect fields.

4. Normal extensions

5. Computation of Galois groups

* 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 $\mathbb{F}_p$)

5.1. 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 5.1. *There are only five isomorphic types of transitive subgroups of the symmetric group S_4.*

Corollary 5.2. $G \cong S_4,\ A_4,\ D_4,\ V_4,$ *or* C_4.

Proposition 5.3. *Two groups A_4 and V_4 are only transitive normal subgroups of S_4.*

Now we define our resolvent polynomial.

Proposition 5.4. *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 5.1. 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 5.5. *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 $G \cong C_4$. □

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