Lecture Notes On Abstract Algebra (Week 11)

Guohua PENG (彭国华)
email: peng@scu.edu.cn

Contents

1 Lecture 20 (Nov 14, 2023): Algebraic Closure and Splitting Field

1.1 Algebraic Closure of A Field

Theorem 1.1 (Kronecker)**.** *Let $f(x) \in F[x]$ and $\deg f(x) \geq 1$. Then there exists an extension field K and $\alpha \in K$ such that $[K : F] \leq \deg f(x)$ and $f(\alpha) = 0$.*

Proof. Let $m(x)$ be an irreducible factor of $f(x)$. Then $F[x]/(m(x))$ is a field. The inclusion $F \to F[x]$ composed with the obvious epimorphism $\tau : F[x] \twoheadrightarrow F[x]/(m(x))$ induces a natural homomorphism η from F to $F[x]/(m(x))$:

$$\eta : F \hookrightarrow F[x] \twoheadrightarrow F[x]/(m(x)).$$

Then $\ker \eta = F \cap (m(x)) = 0$, and hence η must be a monomorphism. Notice the restriction of η on F is essentially the identity mao. Thus $K = F[x]/(m(x))$ may be regarded as an extension field of F and $[K : F] = \deg m(x) \leq \deg f(x)$.

Now focus on the obvious epimorphism

$$\tau : F[x] \to K = F[x]/(m(x))$$

and write $\overline{g(x)} = \tau(g(x))$. In particular, $\overline{x} = \tau(x) \in K$. Since $\overline{m(x)} = 0$ and $\overline{m(x)} = m(\overline{x})$, it follows $m(\overline{x}) = 0$. That is, $\alpha = \overline{x} \in K$ is a root of $m(x)$. Note that every root of $m(x)$ is a root of $f(x)$. This implies that $\alpha = \overline{x} \in K$ is a root of $f(x)$. In other words, $f(x)$ has a root in the extension field $K = F[x]/(m(x))$. □

Remark 1.1. Let $f(x)$ be an irreducible polynomial over F. Then $K = F[x]/(f(x))$ can be viewed as an extension of F. Let α be the imagine of x under the canonical map $F[x] \to K$. Then $\alpha \in K$ is a root of $f(x)$.

Example 1.1. We know that x^2+1 has no roots in $\mathbb{R}$. Hence x^2+1 is irreducible over $\mathbb{R}$. Consequently $\mathbb{R}[x]/(x^2+1)$ is an extension field of $\mathbb{R}$. Since $\overline{x^2+1} = \overline{x}^2 + \overline{1} = \overline{x}^2 + 1 = 0$ holds in $\mathbb{R}[x]/(x^2+1)$, we see that $\overline{x} \in \mathbb{R}[x]/(x^2+1)$ is a root of the polynomial X^2+1. In fact,

$$\mathbb{R}[x]/(x^2+1) = \{a + b\overline{x} \mid a, b \in \mathbb{R}\}.$$

Hence $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$ and $\overline{x}$ corresponds to $i = \sqrt{-1}$ or $-i$.

Example 1.2. Note that $\mathbb{F}_2 = \{0, 1\}$ denote the finite field with 2 elements. One can see that x^2+x+1 is irreducible over $\mathbb{F}_2$. Hence $\mathbb{F}_2[x]/(x^2+x+1)$ is an extension field of $\mathbb{F}_2$. Write α for the coset of x in $\mathbb{F}_2[x]/(x^2+x+1)$. Then $\alpha^2+\alpha+1 = 0$ and

$$K = \mathbb{F}_2[x]/(x^2+x+1) = \{0, 1, \alpha, \alpha+1\}.$$

It follows that K is a finite field of 4 elements, which is usually denoted by $\mathbb{F}_4$ or GF(4). Here "GF" stands for Galois field, since finite fields are also called **Galois fields**.

Remark 1.2. In general, let p be a prime integer. If $m(x)$ is an irreducible polynomial over the finite field $\mathbb{F}_p$ of p elements, then $\mathbb{F}_p[x]/(m(x))$ is a finite field of p^n elements. In other words, if there exists an irreducible polynomial of order n over $\mathbb{F}_p$, then we can construct a finite field with p^n elements. It's a basic fact that irreducible polynomials of any degree do exist over the finite field $\mathbb{F}_p$. So

$$\boxed{\text{a finite field with prime power order does exist.}}$$

Proposition 1.1. *If $f(x) \in F[x]$ has a root α in F, then there exist a polynomial $g(x) \in F[x]$ such that*

$$f(x) = (x - \alpha)g(x).$$

Definition 1.1. *A field F is called* **algebraically closed** (代数闭的) *if every polynomial $f(x) \in F[x]$ of degree ≥ 1 has a root in F.*

The real number field $\mathbb{R}$ is not algebraically closed, since $x^2+1 \in \mathbb{R}[x]$ has no roots in $\mathbb{R}$. The Fundamental Theorem of Algebra implies that $\underline{\mathbb{C}\text{ is algebraically closed}}$.

Theorem 1.2 (Fundamental Theorem of Algebra, 代数基本定理)**.** *Every polynomial $f(x) \in \mathbb{R}[x]$ with $\deg f(x) \geq 1$ has a root in $\mathbb{C}$.*

Let

$$\overline{\mathbb{Q}} = \text{the set of all algebraic numbers.}$$

Then

$$\boxed{\overline{\mathbb{Q}} \text{ and } \mathbb{C} \text{ are algebraic closed.}}$$

Corollary 1.1. *Let F be an algebraic closed field. Then every polynomial over F can be decomposed as a product of linear factors in $F[x]$.*

Definition 1.2. *If the field extension K/F is algebraic and K is algebraically closed, then K is called an* **algebraic closure** (代数闭包) *of F.*

The Fundamental Theorem of Algebra shows that $\mathbb{C}$ is algebraically closed. But $\mathbb{C}$ is NOT an algebraic closure of $\mathbb{Q}$.

Actually, $\overline{\mathbb{Q}}$ is a proper subfield of $\mathbb{C}$. The extension $\mathbb{C}/\overline{\mathbb{Q}}$ is purely transcendental. Every complex number outside of $\overline{\mathbb{Q}}$ is transcendental over $\mathbb{Q}$.

Remark 1.3. 1. An algebraic closed field is an algebraic closure of itself.

2. An irreducible polynomial over an algebraic closed field must be of degree one. In other words, every polynomial of degree greater than 1 over an algebraic closed field is reducible.

3. For any field F, we can achieve its algebraic closure $\overline{F}$ by adjoining to F all algebraic elements (i.e, all roots of polynomials over F). Hence an algebraic closure of a field F is the "smallest" extension field in which every polynomial over F has a root.

   For example, $\overline{\mathbb{Q}}$ is obtained by adjoining all algebraic numbers to $\mathbb{Q}$.

4. An algebraic closure of a field does exist and is unique in the following sense: if K_1 and K_2 are two algebraic closures of F, then there exists an isomorphism (of rings) $\tau : K_1 \to K_2$ such that $\tau(a) = a$ for all $a \in F$.

Corollary 1.2. *Every polynomial over F can be factored as a product of linear polynomials over its algebraic closure.*

Corollary 1.3. *A polynomial of degree n over F has exactly n roots in its algebraic closure, counting multiplicity (重数计算在内).*

Exercises

1. Let $\overline{\mathbb{Q}}$ denote the set of all algebraic numbers.

   (a) For every $\alpha \in \mathbb{C}\backslash\overline{\mathbb{Q}}$, show that α is transcendental over $\mathbb{Q}$.

   (b) Show that $\overline{\mathbb{Q}}/\mathbb{Q}$ is an infinite extension.

   (c) Let $\alpha \in \mathbb{C}$ be a root of a polynomial $f(x) \in \overline{\mathbb{Q}}[x]$. Show that α is an algebraic number. Deduce that $\overline{\mathbb{Q}}$ is algebraically closed.

   (d) Show that $\overline{\mathbb{Q}}$ is the algebraically closure of $\mathbb{Q}$ in $\mathbb{C}$.

   (e) Let F be an intermediated field of $\overline{\mathbb{Q}}/\mathbb{Q}$ such that $[F : \mathbb{Q}]$ is finite. Show that $\overline{\mathbb{Q}}$ is also an algebraic closure of F.

2. Let $\alpha \in \overline{F}$ be a roof of $f(x) \in F[x]$. Show that $f(x) = (x - \alpha)g(x)$ for some polynomial $g(x)$ over $F(\alpha)$.

3. Let $f(x)$ be a polynomial of degree n over F. Show that $f(x)$ has at most n roots in an algebraic closure $\overline{F}$.

4. Let K be an algebraic closure of F and M be an intermediate subfield of K/F. Show that K is an algebraic closure of M.

1.2 Splitting Field of a polynomial

Recall Kronecker's Theorem: every nonconstant polynomial over a field has a root in some extension field.

Actually, if $p(x) \in F[x]$ is irreducible, we can take $K = F(\alpha)$, where α is the image of x via the canonical map $F[x] \to F[x]/(p(x))$. Then $K = F[x]/(p(x))$ is an extension field of F and α is a root of $p(x)$. Where is α? α is an element in some algebraic closure of F.

We say that a polynomial $f(x) \in F[x]$ **splits** (分裂) (or splits completely) over F if there exist elements $\alpha_1, \alpha_2, \ldots, \alpha_n \in F$ such that

$$f(x) = c(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n),$$

where $c \in F$ is the leading coefficient of $f(x)$. A polynomial $f(x) \in F[x]$ splits over an extension field K of F if and only if $f(x)$ factors in $K[x]$ as a product of constant or linear factors. Every polynomial over F splits over its algebraic closure $\overline{F}$. In particular, if F is an algebraic closed field, then every polynomial over F splits.

Remark 1.4. 1. Every polynomial over $\mathbb{R}$ splits over $\mathbb{C}$.

2. Every polynomial over $\mathbb{Q}$ splits over $\overline{\mathbb{Q}}$.

Definition 1.3. *Let K/F be a field extension, and let $f(x) \in F[x]$ be a polynomial with coefficients in F. The field K is said to be a* **splitting field** (分裂域) *of $f(x)$ over F if the following conditions are satisfied:*

1. *the polynomial $f(x)$ splits over K;*
2. *the polynomial $f(x)$ does not split over any proper subfield of K that contains F.*

> 1. A splitting field of $f(x) \in F[x]$ is the smallest subfield of $\overline{F}$ (an algebraic closure of F) in which $f(x)$ splits completely.
> 2. A splitting field of $f(x) \in F[x]$ is the smallest subfield of $\overline{F}$ containing all roots of $f(x)$.

Example 1.3. 1. The field $\mathbb{Q}(\sqrt{2})$ is a splitting field for the polynomial $x^2 - 2$ over $\mathbb{Q}$.

2. Let $\omega = e^{\frac{2\pi i}{3}}$ be a 3rd root of unity. We know that $\sqrt[3]{5}, \sqrt[3]{5}\omega, \sqrt[3]{5}\omega^2$ are all roots of $x^3 - 5$ in $\mathbb{C}$. Hence $\mathbb{Q}(\sqrt[3]{5}, \sqrt[3]{5}\omega, \sqrt[3]{5}\omega^2)$ is the unique splitting field contained in $\mathbb{C}$. But $\mathbb{Q}(\sqrt[3]{5}, \sqrt[3]{5}\omega, \sqrt[3]{5}\omega^2) = \mathbb{Q}(\sqrt[3]{5}, \omega)$. So a splitting field for the polynomial $x^2 - 5$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt[3]{5}, \omega)$.

3. Let n be a positive integer and $\zeta_n = e^{\frac{2\pi i}{n}}$. Then $\mathbb{Q}(\zeta_n)$ is a splitting field of $x^n - 1 \in \mathbb{Q}[x]$.

4. let $x^2 + ax + b \in \mathbb{R}[x]$ and $a^2 - 4b < 0$. Then $\mathbb{C}$ is the splitting field of $x^2 + ax + b$ over $\mathbb{R}$.

Recall Proposition 1.1: if $f(x) \in F[x]$ has a root α in F, then there exist a polynomial $g(x) \in F[x]$ such that $f(x) = (x - \alpha)g(x)$.

Fix an algebraic closure $\overline{F}$ of F. Let $f(x) = x^n + \cdots \in F[x]$ be a monic polynomial of degree n. Then $f(x)$ has exactly n roots in $\overline{F}$ (Corollary 1.3). Let $\alpha_1 \in \overline{F}$ be a root of $f(x)$ and set $K_1 = F(\alpha_1)$. Then $[K_1 : F] \le n$. By Proposition 1.1, $f(x) = (x - \alpha_1)f_1(x)$ for some $f_1(x) \in K_1[x]$. Let α_2 be a root of $f_1(x)$, then α_2 is a root of $f(x)$. Replacing $f(x)$ by $f_1(x)$, we can add another root α_2 to K_1 to obtain $K_2 = K_1(\alpha_2) = F(\alpha_1, \alpha_2)$ and $f_1(x) = (x - \alpha_2)f_2(x)$ for some $f_2(x) \in K_2[x]$. Clearly $[K_2 : K_1] \le n - 1$. Inductively, let α_i be a root of $f_{i-1}(x) \in K_{i-1}[x]$, we have an extension field $K_i = K_{i-1}(\alpha_i)$ and

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_{i-1})(x - \alpha_i)f_i(x),$$

where $f_i(x) = \frac{f_{i-1}(x)}{x - \alpha_i} \in K_i[x], \deg f_i(x) = n - i$, $i \ge 2$. Hence

$$[K_i : K_{i-1}] = [K_{i-1}(\alpha_i) : K_{i-1}] \le n + 1 - i. \tag{1}$$

Let $K = K_n = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Then

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n),$$

where $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$ are all roots of $f(x)$. Clearly $K = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ is the smallest extension subfield of $\overline{F}$ such that $f(x)$ splits.

Based on our previous discussion, if $\alpha_1, \alpha_2, \ldots, \alpha_n$ are all roots of $f(x)$, then $F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ is a splitting field of $f(x)$. And we have

Proposition 1.2. *Let $f(x) \in F[x]$ be a polynomial with degree $n \geq 1$.*

1. *A splitting field of $f(x)$ over F does exist.*
2. *If K is a splitting field for $f(x)$ over F, then $[K : F] \leq n!$.*

The second result comes from (1) and the transitivity of extension degree.

One may adjoin all roots of a polynomial to the base field to achieve a splitting field of the polynomial.

Corollary 1.4. *Let M/F be a field extension. If a polynomial $f(x) \in F[x]$ splits over M, then there exists a unique subfield K of M which is a splitting field for $f(x)$ over F.*

Proof. Let K be the intersection of all subfields L of M containing F with the property that the polynomial f splits over L. One can readily verify that K is the unique splitting field for f over F contained in M. $\square$

The Fundamental Theorem of Algebra ensures that a polynomial $f(x) \in \mathbb{Q}[x]$ with rational coefficients always splits over the field $\mathbb{C}$ of complex numbers. Thus some unique subfield L of $\mathbb{C}$ is a splitting field for $f(x)$ over $\mathbb{Q}$.

Example 1.4. Clearly $K_1 = \mathbb{Q}(\sqrt{-43})$ is a splitting field of $x^2 + 43$ over $\mathbb{Q}$ and $K_2 = \mathbb{Q}(\sqrt{47})$ is a splitting field of $x^2 - 47$ over $\mathbb{Q}$. Then $K = K_1K_2 = \mathbb{Q}(\sqrt{-43}, \sqrt{47})$ is the splitting of the reducible polynomial

$$(x^2 + 43)(x^2 - 47) = x^4 + 4x^2 - 2021.$$

One can check that $K = \mathbb{Q}(\sqrt{-43} + \sqrt{47}) = \mathbb{Q}(\sqrt{-43} + \sqrt{-2021}) = \mathbb{Q}(\sqrt{-2021} + \sqrt{47})$.

If we take $\alpha = \sqrt{-43} + \sqrt{47}$, then $\alpha^4 - 8\alpha^2 + 8100 = 0$. Therefore K is also a splitting field of the irreducible polynomial

$$x^4 - 8x^2 + 8100.$$

Remark 1.5. *Any two splitting fields of a given polynomial over a field F are F-isomorphic.* More precisely, if K_1 and K_2 are two splitting fields of $f(x) \in F[x]$, then there exists an isomorphism (of rings) $\tau : K_1 \to K_2$ such that $\tau(a) = a$ for all $a \in F$.

Exercises

1. Let K be a splitting field of a polynomial $f(x)$ over F and M is an intermediate field of K/F. Then K is a splitting field of $f(x)$ over M.
2. Let K_1, K_2 be the splitting fields for $x^2 + 3$ and $x^4 - 3$ over $\mathbb{R}$ respectively. Show that $K_1 = K_2$.

3. Let p be a prime and ζ_p a primitive p-th root of unity. Show that $\mathbb{Q}(\zeta_p)$ is a splitting field of $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$.

4. Construct a splitting field K of $f(x) = x^7 - 5$. What is $[K : \mathbb{Q}]$?

5. Construct a splitting field of $f(x) = x^4 - 4x^2 - 21$ explicitly.

6. Find out the minimal polynomial $m(x)$ of $\alpha = \sqrt{2}+\sqrt{-3}$. Then show that $K = \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt{-3})$ and that K is the splitting field of $m(x)$.

7. Let p be a prime integer and$f(x)$ be a polynomial of degree p over F with splitting field E. If $p \mid [E : F]$, show that $f(x)$ is irreducible over F.

8. Let F be a field and G a finite group of $F^\times$. Show that G is cyclic.

2 Lecture 21 (Nov 16, 2023): Galois Group and Extensions of an Isomorphism

2.1 Galois Group of a Field Extension

Let K_1/F and K_2/F be two extension fields of F. A ring homomorphism $\sigma : K_1 \to K_2$ is called an F-**homomorphism** (F-同态) if $\sigma(a) = a$ for all $a \in F$.

Remark 2.1.
1. An F-homomorphism is essentially a ring homomorphism that fixes every element of F.
2. An F-homomorphism must send 1 to 1, hence it is injective. So an F-homomorphism is also an F-**embedding** (F-嵌入).

Recall that an extension field K of F can be viewed as a vector space over F. So an F-homomorphism is a homomorphism as F-modules, hence a linear map between vector spaces over F.

$$\boxed{\begin{aligned} F\text{-homomorphism} &= F\text{-embedding} \\ &= F\text{-module homomorphism} + \text{preserving multiplication.} \end{aligned}}$$

Let $\sigma : K_1 \to K_2$ be an F-homomorphism. If σ is a bijection, then σ is called an F-**isomorphism** (F-同构) and we say that K_1 and K_2 are F-**isomorphic**. An F-homomorphism from K to K is called an F-**endomorphism** (F-自同态) and an F-isomorphism from K to K is called an F-**automorphism** (F-自同构).

$$\boxed{\text{An } F\text{-isomorphism is an isomorphism of } F\text{-modules.}}$$

Example 2.1. The field $\mathbb{R}[x]/(x^2+1) = \{a + b\overline{x} \mid a, b \in \mathbb{R}\}$ and $\mathbb{C}$ are extensions of $\mathbb{R}$. The isomorphism

$$\begin{aligned} \tau : \mathbb{R}[x]/(x^2+1) &\to \mathbb{C} \\ a + b\overline{x} &\mapsto a + bi \end{aligned}$$

is an $\mathbb{R}$-isomorphism.

Remark 2.2. Every ring homomorphism $\sigma : K_1 \to K_2$ has a canonical extension to polynomial rings

$$\begin{aligned} \sigma^* : K_1[x] &\to K_2[x] \\ \sum a_i x^i &\mapsto \sum \sigma(a_i) x^i. \end{aligned}$$

In particular, $\sigma^*(x) = x, \sigma\mid_{K_1} = \sigma$.

<u>**Basic Observation**</u> Let $K_1 = F(\alpha)$. Then an F-embedding $\sigma : K_1 \to K_2$ is completely determined by $\sigma(\alpha)$, the image of α. In other words, if σ, τ are two F-embeddings from K_1 to K_2 and $\sigma(\alpha) = \tau(\alpha)$, then $\sigma = \tau$.

Theorem 2.1. *Let $\sigma : K_1 \to K_2$ be an F-embedding and let $\alpha \in K_1$ be an algebraic element over F. Then*

1. *the imagine $\sigma(\alpha)$ in K_2 is also algebraic over F;*
2. *$\sigma(\alpha)$ and α have the the same minimal polynomial over F.*

Two algebraic elements α, β are called F-**conjugate** (F-共轭) if their minimal polynomials over F are the same. We also simply say that β is a *conjugate* (共轭元) of α if the base field F is clear. In other words, two roots of the same irreducible polynomial over F are called conjugate over F. For example, $\sqrt{2}$ and $-\sqrt{2}$ are conjugate over $\mathbb{Q}$, because they are the two roots of $x^2 - 2 \in \mathbb{Q}[x]$. Similarly, $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$ and $\sqrt[3]{2}\omega^3$ are conjugate over $\mathbb{Q}$, where $\omega = \frac{-1+\sqrt{-3}}{2}$. They have the same minimal polynomial $x^3 - 2$ over $\mathbb{Q}$.

If α is an algebraic element of degree n over F, then its minimal polynomial is of degree n. Consequently α has at most n conjugates.

$$\boxed{\text{An } F\text{-embedding must send an algebraic element to one of its } F\text{-conjugates.}}$$

Example 2.2. Let $\alpha = \sqrt[3]{2}$ and $\sigma : \mathbb{Q}(\alpha) \to \mathbb{C}$ an $\mathbb{Q}$-embedding. Then σ is completely determined by the image of α. Note that x^3-2 is the minimal polynomial of α over $\mathbb{Q}$. By Theorem 2.1, $\sigma(\alpha) \in \{\alpha, \alpha\omega, \alpha\omega^2\}$, where $\omega = \frac{-1+\sqrt{-3}}{2}$ and $\alpha, \alpha\omega, \alpha\omega^2$ are all roots of $x^3 - 2$. It follows that there are at most three $\mathbb{Q}$ embedding from $\mathbb{Q}(\alpha)$ to $\mathbb{C}$. Actually, there are exact three!

Example 2.3. The quadratic extensions $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$ are not isomorphic. In fact, if $\sigma : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{3})$ is an isomorphism, then σ must be a $\mathbb{Q}$-isomorphism. Let $\alpha = \sigma(\sqrt{2}) \in \mathbb{Q}(\sqrt{3})$. By Theorem 2.1, the minimal polynomial of α is $x^2 - 2$. Hence $\sigma(\sqrt{2}) = \pm\sqrt{2}$. It follows that $\sqrt{2} \in \mathbb{Q}(\sqrt{3})$. Impossible!

If K/F is an extension of fields, then an F-isomorphism from K to K is called an F-automorphism of K. An F-automorphism of K is also called an automorphism of the field extension K/F. Let <u>$\mathrm{Gal}\,(K/F)$</u> denote the set of all F-automorphisms on K, or the set of all automorphism of K/F. The composition of two F-automorphisms on K is still an F-automorphisms. It follows that $\mathrm{Gal}\,(K/F)$ becomes a multiplicative group, called the **Galois group of** K/F (域扩张K/F 的伽罗瓦群).

We can also define <u>$\mathrm{Aut}(K)$</u> to be the set of all automorphisms on K. Then $\mathrm{Aut}(K)$ becomes a group with respect to the composition of maps, called the **automorphism group of** K (K的自同构群).

$$\boxed{\text{The Galois group } \mathrm{Gal}\,(K/F) \text{ is a subgroup of } \mathrm{Aut}\,(K).}$$

Remark 2.3. Let $\sigma \in \mathrm{Aut}\,(K)$. Then $\sigma \in \mathrm{Gal}\,(K/F)$ if and only if the restriction of σ on F is the identity map (i.e. $\sigma|_F = \mathrm{id}_F$).

Example 2.4. 1. One can see that $\mathrm{Aut}(\mathbb{Q}) = \{1\}$ and $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{1, \sigma\} \cong \mathbb{Z}/2\mathbb{Z}$, where σ is the complex conjugate.

2. Let $K(x)$ be the field of rational functions in x over a field K and $\theta \in \mathrm{Gal}\,(K(x)/K)$. Then there exist $a, b, c, d \in K$ such that $ad-bc \neq 0$ and $\theta(x) = \frac{ax+b}{cx+d}$ (exercise!). Hence $\mathrm{Gal}\,(\mathbb{C}(x)/\mathbb{C}) \cong \mathrm{SL}_2(\mathbb{C})$.

3. Let $F = \mathbb{Q}(\sqrt{2})$. Then $\mathrm{Gal}\,(F/\mathbb{Q}) = \{1, \sigma\}$, where 1 refers to the identity map and σ is the map given by $\sigma(\sqrt{2}) = -\sqrt{2}$.

4. Let $\alpha = \sqrt[3]{2}$. Based on the above example and Theorem 2.1, we have $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) = 1$.

Exercises

1. Let F_1, F_2 be two fields and let $\sigma : F_1 \to F_2$ be a ring homomorphism such that $\sigma(1) = 1$. Show that σ is injective and $\sigma(\frac{a}{b}) = \frac{\sigma(a)}{\sigma(b)}$ for all $a, b \in F_1, b \neq 0$.

2. Let K/F be a finite extension and σ an F-embedding of K. Show that $[K : F] = [\sigma(K) : F]$.

3. Let K/F be a finite extension. Show that every F-endomorphism on K is an F-automorphism.

4. Let $\alpha \in K$ be an algebraic element over F. Show that an F-automorphism σ of $F(\alpha)$ is completely determined by $\sigma(\alpha)$. In other words, if τ is another F-automorphism of $F(\alpha)$ such that $\sigma(\alpha) = \tau(\alpha)$, then $\sigma(x) = \tau(x)$ for all $x \in F[\alpha]$.

5. Prove $\mathrm{Gal}(\mathbb{C}(x)/\mathbb{C}) \cong \mathrm{SL}_2(\mathbb{C})$.

6. Prove $\mathrm{Gal}(\mathbb{R}/\mathbb{Q}) = \mathrm{Aut}(\mathbb{R}) = 1$.

2.2 Extensions of an Isomorphism

To determine the basic property of $\mathrm{Gal}(K/F)$ of a field extension K/F, we need to discuss the extensions of an embedding. Notice a ring homomorphism between fields must be an embedding.

Definition 2.1. *Let K_1/F_1 and K_2/F_2 be two extension fields and assume $\tau : F_1 \to F_2$ is a ring homomorphism. If $\sigma : K_1 \to K_2$ is a ring homomorphism such that $\sigma|_{F_1} = \tau$, i.e. $\sigma(\alpha) = \tau(\alpha)$ for all $\alpha \in F_1$, then σ is called an* **extension** (扩张) *of τ. And τ is called the* **restriction** (限制) *of σ to F_1.*

$$\begin{tikzcd} K_1 \arrow[r, "\sigma"] \arrow[d, dash] & K_2 \arrow[d, dash] \\ F_1 \arrow[r, "\tau"] & F_2 \end{tikzcd} \qquad \sigma|_{F_1} = \tau$$

Remark 2.4. An extension of τ is a ring homomorphism σ that makes the following diagram commute ($\tau \circ \iota_2 = \iota_1 \circ \sigma$):

$$\begin{tikzcd} K_1 \arrow[r, "\sigma"] & K_2 \\ F_1 \arrow[u, "\iota_1"] \arrow[r, "\tau"] & F_2 \arrow[u, "\iota_2"'] \end{tikzcd}$$

Here the vertical maps are inclusions.

Recall that an isomorphism σ between two extension fields of F are F-isomorphism if only if $\sigma(a) = a$ for all $a \in F$, or equivalently $\sigma\mid_F = \mathrm{id}\mid_F$.

An F-isomorphism is an extension of the identity map on F.

Consequently, $\mathrm{Gal}(K/F)$ is the group of extensions of the identity on F.

Example 2.5. The $\mathbb{Q}$-isomorphism

$$\sigma : K_1 = \mathbb{Q}(\sqrt[4]{2}) \to K_2 = \mathbb{Q}(i\sqrt[4]{2})$$
$$\sqrt[4]{2} \mapsto i\sqrt[4]{2}$$

is an extension of the $\mathbb{Q}$-isomorphism

$$\tau : F_1 = \mathbb{Q}(\sqrt{2}) \to F_2 = F_1 = \mathbb{Q}(\sqrt{2})$$
$$\sqrt{2} \mapsto -\sqrt{2}.$$

Consequently, σ is a extension of τ, and τ is the restriction of σ:

$$\begin{tikzcd}
\mathbb{Q}(\sqrt[4]{2}) \arrow[r, "\sigma"] \arrow[d, dash] & \mathbb{Q}(i\sqrt[4]{2}) \arrow[d, dash] \\
\mathbb{Q}(\sqrt{2}) \arrow[r, "\tau"] \arrow[d, dash] & \mathbb{Q}(\sqrt{2}) \arrow[d, dash] \\
\mathbb{Q} \arrow[r, "\mathrm{id}_{\mathbb{Q}}"] & \mathbb{Q}
\end{tikzcd}$$

Consider the $\mathbb{Q}$-isomorphism $\eta : K_1 \to K_2$ given by $\eta(\sqrt[4]{2}) = -i\sqrt[4]{2}$. One can check that η is also an extension of τ.

Given a homomorphism $\tau : F \to K$ of fields, we define

$$\tau^* : F[x] \to K[x]$$
$$f(x) = a_0 + a_1x + \cdots + a_nx^n \mapsto \tau^*(f)(x) = \tau(a_0) + \tau(a_1)x + \cdots + \tau(a_n)x^n.$$

Note that $\tau^*(1) = 1$ and

$$\tau^*(f+g) = \tau^*(f) + \tau^*(g),\ \tau^*(fg) = \tau^*(f)\tau^*(g)$$

for all $f, g \in F[x]$. Hence τ^* is a homomorphism from $F[x]$ to $K[x]$. In particular, if $f \mid g$, then $\tau^*(f) \mid \tau^*(g)$.

$$\begin{tikzcd}
F_1[x] \arrow[r, "\tau^*"] & F_2[x] \\
F_1 \arrow[r, "\tau"] \arrow[u] & F_2 \arrow[u]
\end{tikzcd}$$

A homomorphism between two rings can be canonically extended to a homomorphism between their polynomial rings.

Lemma 2.1. *Let $\tau : F_1 \to F_2$ be an isomorphism between F_1 and F_2 and let α be a root of a polynomial $f(x) \in F_1[x]$. Fix an algebraic closure $\overline{F}_2$ of F_2.*

1. *The isomorphism τ can be naturally extended to be a ring isomorphism τ^* from $F_1[x]$ to $F_2[x]$. Consequently, $f(x) \in F_1[x]$ is irreducible over F_1 if and only if $\tau^*(f)(x)$ is irreducible over F_2.*

2. *If $\sigma : F_1(\alpha) \hookrightarrow \overline{F}_2$ is an embedding extending τ, then $\sigma(\alpha)$ is root of $\tau^*(f) \in F_2[x]$.*

3. *If $f(x)$ is irreducible and $\beta \in \overline{F}_2$ is a root of $\tau^*(f)(x) \in F_2[x]$, then there exists an extension $\sigma : F_1(\alpha) \to F_2(\beta)$ of τ such that $\sigma(\alpha) = \beta$.*

Proof. 1. Clear.

2. This is all because of $\sigma(g(\alpha)) = \tau^*(g)(\sigma(\alpha))$ for any $g(x) \in F_1[x]$ and $\alpha \in F_1$.

3. Define
$$\begin{aligned} \sigma : F_1(\alpha) &\to F_2(\beta) \\ \sum a_i\alpha^i &\mapsto \sum \tau(a_i)\beta^i. \end{aligned}$$
Direct check shows that σ is as required.

$$\begin{array}{ccc} F_1(\alpha) & \xrightarrow{\sigma} & F_2(\beta) \\ \updownarrow & & \updownarrow \\ F_1[x]/(f) & \xrightarrow{\tau^*} & F_2[x]/\left(\tau^*(f)\right) \\ \uparrow & & \uparrow \\ F_1[x] & \xrightarrow{\tau^*} & F_2[x] \\ \uparrow & & \uparrow \\ F_1 & \overset{\tau}{\leftrightsquigarrow} & F_2 \end{array}$$

□

If $F_1 = F_2$, we can take τ to be the identity map in the above lemma and obtain the following

Theorem 2.2. Let α, β be algebraic elements over F. Then there exists an F-isomorphism $\sigma : F(\alpha) \to F(\beta)$ such that $\sigma(\alpha) = \beta$ if and only if α and β are conjugate over F.

A splitting field of a polynomial can be achieved by adjoining roots successively. Applying the above results to the identity map, we have

Corollary 2.1. *Two splitting fields of a polynomial over F must be F-isomorphic. That is, if K_1/F and K_2/F are two splitting fields of $f(x)$ over F, then there exists an isomorphism $\theta : K_1 \to K_2$ such that $\theta\mid_F = \mathrm{id}_F$.*

An algebraic closure of a filed F can be achieved by adjoining all algebraic elements to F, so we can prove

Corollary 2.2. *Every automorphism of a field can be lifted to an automorphism of its algebraic closure. Hence two algebraic closures of a field F are F-isomorphic.*

It follows that an algebraic closure of a field does exist and the algebraic closure is essentially unique. We always use $\overline{F}$ or F^{ac} to denote the algebraic closure of F.

If K/F is an algebraic extension, then K can be obtained from F by adjoining a series if algebraic element. By Lemma 2.1, there is a subfield K' of $\overline{F}/F$ such that K' is F-isomorphic to K. In other words, every algebraic extension of F can be F-embedded in $\overline{F}/F$. Therefore, every algebraic extension of F can be regarded as a subextension of $\overline{F}/F$. Consequently, if K/F is algebraic, $\overline{K} = \overline{F}$.

Theorem 2.3. **Let $\tau : F_1 \to F_2$ be an embedding from F_1 to F_2.**

1. **Let α be an algebraic element of degree n over F_1. Then there are at most n embeddings from $F_1(\alpha)$ to $\overline{F}_2$ that extend τ.**

   Moreover, there are exactly n such embeddings if and only if the minimal polynomial of α over F_1 has no multiple roots.

2. **If K/F_1 is an extension of degree n, then there are at most n embeddings from K to $\overline{F}_2$ that extend τ.**

Proof. 1. Let $m(x)$ be the minimal polynomial of α over F_1. Clearly $\deg \tau^*(m(x)) = n$ and $\tau^*(m(x))$ has at most n distinct roots in $\overline{F}_2$. For each root β of $\tau^*(m(x))$, we can define an embedding $\sigma : F_1(\alpha) \hookrightarrow F_2(\beta) \subset \overline{F}_2$ so that $\sigma(\alpha) = \beta$ and $\sigma(a) = \tau(a)$ for all $a \in F_1$ by Lemma 2.1. Moreover, every embedding from $F_1(\alpha)$ to $\overline{F}_2$ must be of this form. It follows that there are at most n embeddings from $F_1(\alpha)$ to $\overline{F}_2$ extending τ and there are exact n such embeddings if and only if $m(x)$ has exactly n roots.

2. Let $\alpha_1, \ldots, \alpha_m \in K$ such that $K = F_1(\alpha_1, \ldots, \alpha_m)$. Set $L_0 = F_1$, $L_i = F_1(\alpha_1, \ldots, \alpha_i)$, $1 \le i \le m$. Then

$$L_1 = F_1(\alpha_1), L_i = L_{i-1}(\alpha_i), L_m = K.$$

Let $[L_1 : F_1] = n_1$ and $[L_i : L_{i-1}] = n_i$, $i \ge 2$. Then α_1 is an algebraic element of degree n_1 over F_1, α_i is an algebraic element of degree n_i over L_{i-1}. Hence, for each embedding from L_{i-1} to $\overline{F}_2$, there are at most n_i extensions form L_i to $\overline{F}_2$ by the previous claim. Note that $n_1 n_2 \cdots n_m = n$ by the Tower Law (Transitivity of Extension Degree). It follows that there are at most n embeddings from K to $\overline{F}_2$ extending τ.

$$\begin{tikzcd}
L_i = L_{i-1}(\alpha_i) = F_1(\alpha_1, \ldots, \alpha_i) \arrow[r, "\tau_i"] \arrow[d, dash, "n_i"'] & M_i = M_{i-1}(\beta_i) = F_2(\beta_1, \ldots, \beta_i) \hookrightarrow \overline{F}_2 \arrow[d, dash] \\
L_{i-1} \arrow[r, "\tau_{i-1}"] \arrow[d, dash, "n_{i-1}"'] & M_{i-1} \hookrightarrow \overline{F}_2 \arrow[d, dash] \\
\vdots \arrow[d, dash, "n_3"'] & \vdots \arrow[d, dash] \\
L_2 = L_1(\alpha_2) = F_1(\alpha_1, \alpha_2) \arrow[r, "\tau_2"] \arrow[d, dash, "n_2"'] & M_2 = M_1(\beta_2) = F_2(\beta_1, \beta_2) \hookrightarrow \overline{F}_2 \arrow[d, dash] \\
L_1 = F_1(\alpha_1) \arrow[r, "\tau_1"] \arrow[d, dash, "n_1"'] & M_1 = F_2(\beta_1) \hookrightarrow \overline{F}_2 \arrow[d, dash] \\
F_1 \arrow[r, "\tau"] & F_2
\end{tikzcd}$$

□

Let $\tau : F_1 \to F_2$ be an embedding from F_1 to F_2 and α an algebraic element over F_1 with minimal polynomial $m(x)$. If $m(x)$ has totally n distinct roots in $\overline{F}_1$, then there are exactly n extensions of τ from $F_1(\alpha)$ into $\overline{F}_2$.

$$\begin{array}{ccc}
F_1(\alpha) & \overset{\sigma}{\hookrightarrow} & \overline{F}_2 \\
| & & | \\
F_1 & \overset{\tau}{\hookrightarrow} & F_2
\end{array}$$

Recall that $\mathrm{Gal}\,(K/F)$ denotes the group of all F-automorphisms on K. By Theorem 2.3, we immediately have

Theorem 2.4. **If K/F is a finite extension, then $|\mathrm{Gal}\,(K/F)| \leq [K : F]$.**

Corollary 2.3. *Let K/F be a field extension of degree n. Then the identity map on F has at most n extensions to K.*

$\boxed{\text{If } F(\alpha) \text{ contains exactly } m \text{ conjugates of } \alpha, \text{ then } |\mathrm{Gal}\,(K/F)| = m.}$

Exercises

1. Let $F(x)$ be the rational function field in one variable. Let
$$\begin{aligned} \tau : F(x) &\to F(x) \\ f(x) &\mapsto f(x^2). \end{aligned}$$
Show that τ is an F-endomorphism, but not surjective (hence not an F-automorphism).

2. Let K/F be a finite extension. Show that an F-homomorphism from K to itself must be an F-automorphism. Is this true for infinite extension?

3. Let K/F be an algebraic extension. Then every F-homomorphism from K to itself is an F-automorphism.

4. Let $\sigma \in \mathrm{Aut}(K)$ and $\alpha \in K^*$. Is it true that $\sigma^{-1}(\alpha) = \sigma(\alpha^{-1})$?

5. Determine the structure of $\mathrm{Gal}(K/\mathbb{Q})$ for
   (a) $K = \mathbb{Q}(\sqrt{2}, \sqrt{-2})$;
   (b) $K = \mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$;
   (c) K is a spliting field of $x^3 - x - 1$;
   (d) K is a spliting field of $x^4 + 2x^2 - 3$.
   (e) K is a spliting field of $x^4 + x^2 - 1$.

Homework Exercise 9, 10(1), 11, 13, 27 on page 242-244. Exercise 2, 4 on page 314-315.