Introduction to Algebra II, Field Theory

AnLei

Contents

1 Basics

1.1 Characteristic

Definition 1 (Characteristic)**.** Let F be a field. The characteristic of F is defined by

$$\operatorname{char} F := \begin{cases} \min\{n \in \mathbb{N} : n \cdot 1_F = \underbrace{1_F + \cdots + 1_F}_{n} = 0\} & \text{if such } n \text{ exists} \\ 0 & \text{otherwise} \end{cases}$$

Proposition 1. $\operatorname{char} F$ is a either a prime or 0.

Proof.

Suppose $p = \operatorname{char} F = ab$ for some $a, b \in \mathbb{N}_{\geq 1}$. Then $p1_F = (ab)1_F = (a1_F)(b1_F) = 0$. Since F is a integral domain, $(a1_F) = 0$ or $(b1_F) = 0$, which contradicts with the minimality of p. □

1.2 Field extensions

Definition 2 (Field Extension)**.** K is a **field extension** of F if K is a field containing a subfield F, denoted by K/F.

Examples:

1. $\mathbb{C}/\mathbb{R}/\mathbb{Q}$ ($\mathbb{C}$ is a field extension of $\mathbb{R}$ and $\mathbb{R}$ is a field extension of $\mathbb{Q}$)
2. For any squarefree integer $D \neq 1$, $\mathbb{C}/\mathbb{Q}(\sqrt{D})/\mathbb{Q}$.

我們有 $\mathbb{C} = \mathbb{R} + \mathbb{R}i$ 作為 $\mathbb{R}$ 的 field extension。對於任意 $a + bi \in \mathbb{C}$，我們可以將其視為以 $a, b \in \mathbb{R}$ 作為係數，$\{1, i\}$ 作為基底而得到的一個向量。事實上，可以觀察到若 K/F，則 $(K, F, +, \cdot)$ 是一個向量空間，其中加法使用兩個 K 的元素，而乘法為 K 中元素與 F 元素的係數積。

Definition 3 (Degree)**.** If K/F, the **degree** $[K : F]$ is defined by the dimension of K as an F-vector space.

$$[K : F] = \dim_F(K)$$

Examples:

1. $[\mathbb{C} : \mathbb{R}] = 2$ since $\mathbb{C}/\mathbb{R}$ has a basis $\{1, i\}$
2. $[\mathbb{Q}(\sqrt{D}) : \mathbb{Q}] = 2$ since $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$ has a basis $\{1, \sqrt{D}\}$
3. $[\mathbb{R} : \mathbb{Q}] = \infty$, since $\dim_{\mathbb{Q}}(\mathbb{R}) = \infty$.

Theorem 1 (Degree 的 Chain Rule)**.** *If $L/K/F$. Then $[L : F] = [L : K][K : F]$*

Definition 4 (Subfield generated by elements)**.** 假定 F 是一個 field，K/F。並且令：

$$\alpha_1 \dots \alpha_n \in K$$

由於 subfield 的交集還是 subfield，所以若令 $\mathcal{J}$ 為 K 中「同時包含 F 與 $\alpha_1 \dots \alpha_n$ 的 subfield 形成的搜集」，也就是：

$$\mathcal{J} = \{J \subseteq K \mid K/J, \text{ and } J/F \quad \text{and } \alpha_1 \dots \alpha_n \in J\}$$

則所有這樣的 subfield 形成的交集：

$$\bigcap_{J \in \mathcal{J}} J$$

仍然會是一個 K 中同時包含 F 與 $\alpha_1 \dots \alpha_n$ 的 subfield。且這是所有「K 中同時包含 F 與 $\alpha_1 \dots \alpha_n$ 的 subfield」中最小的 subfield，稱為 subfield generated by $\alpha_1 \dots \alpha_n$ over F，並且記成：

$$F(\alpha_1, \alpha_2 \dots \alpha_n) = \bigcap_{J \in \mathcal{J}} J$$

如果只有一個 α，則 $F(\alpha)$ 成為一個 simple extension，α 為一個 primitive element。

現在我們來看這個 extension $E = F(\alpha_1, \alpha_2 \dots \alpha_n)$ 實際上長什麼樣子。因為 $\alpha_1, \dots, \alpha_n \in E$ 而 E 有加法和乘法的封閉性，所以任何以 F 中元素為係數的 $\alpha_1, \dots, \alpha_n$ 的多項式都在 E 裡面。而 E 也有除法的封閉性 (因為乘法有逆)，所以應該包含所有這些多項式的分式：

$$F(\alpha_1, \dots, \alpha_n) \supseteq \left\{ \frac{f(\alpha_1, \dots, \alpha_n)}{g(\alpha_1, \dots, \alpha_n)} : f, g \in F[\alpha_1, \dots, \alpha_n], g \neq 0 \right\}$$

可以驗證由這些多項式分式的蒐集應該也是一個 field，所以也是 $\mathcal{J}$ 中的元素，但 E 又是其中最小的，所以"$\subseteq$" 也成立，於是等號成立。

1.3 Prime subfield

Definition 5 (Prime Subfield)**.** The prime subfield P of a field F is the minimal subfield of F containing 1_F:

$$P = \bigcap_{\substack{F/S \\ 1_F \in S}} S$$

i.e. the subfield generated by 1_F.

我們能夠定義一個 natural ring homomorphism。如果 $\operatorname{char} F = p > 0$，考慮 $\phi : \mathbb{Z} \to F, \phi(a) = a1_F$。$\phi$ 的 kernel 是

$$\ker \phi = \{a \in \mathbb{Z} : \phi(a) = a \cdot 1_F = 0_F\} = \{a \in \mathbb{Z} : p|a\} = p\mathbb{Z}$$

ϕ 的 image 就是 F 的 prime subfield。所以由 1st theorem of isomorphism 我們有 $P \cong \mathbb{Z}/p\mathbb{Z}$。

如果 $\operatorname{char} F = 0$，考慮 $\phi : \mathbb{Q} \to P, \phi(a/b) = (a1_F)(b1_F)^{-1}$。因為 $b \neq 0$ 所以 $(b1_F) \neq 0_F$，ϕ 是 well-defined。ϕ 是可逆的：

$$\phi^{-1}((a1_F)(b1_F)^{-1}) = \frac{a}{b}$$

所以 ϕ 是一個 ring isomorphism，$P \cong \mathbb{Q}$。可以總結如下

Proposition 2. Let P be prime subfield of a field F.

- If $\operatorname{char} F > 0$, then $P \cong \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$
- If $\operatorname{char} F = 0$, then $P \cong \mathbb{Q}$

1.4 Simple Extension

Definition 6 (Simple Extension)**.** If K/F, we say that K is a simple extension if $K = F(\alpha)$ for some $\alpha \in K$.

一個 extension 是否 simple 並不顯然，即使我們使用兩個以上的元素 extent 也可能得到一個 simple extension，比如 $\mathbb{Q}[\sqrt{2}, \sqrt{3}] = \mathbb{Q}[\sqrt{2} + \sqrt{3}]$。

Definition 7 (algebraic/transcendental)**.** Let K/F be a field extension. An element $\alpha \in K$ is said to be **algebraic over** F is α is a root of some nonzero polynomial over F. If no such polynomials exist, then we say α is **transcendental** over F. If every element of K is algebraic over F, then we say K is an **algebraic extension of** F.

Theorem 2. Let $p(x)$ be an irreducible polynomial in $F[x]$. Then there is an extension field K s.t. $p(x)$ has a root in K.

Proof.

Let $K = F[x]/(p(x))$. By Prop 15 of Chapter 9, K is a field. It contains F as a subfield. (To be more rigorous, K contains a subfield $\{a + (p(x)) : a \in F\}$ which is isomorphic to F.) It's clear $\alpha = x + (p(x)) \in K$ is a root of $p(x)$. $(p(\alpha) = p(x) + (p(\alpha)) = 0 + (p(x)))$ $\square$

Proposition 3 (Minimal Polynomial: **以特定元素為根的多項式存在唯一的最小元素**)**.** Assume α is algebraic over F. Then $\exists!$ monic irredubcible polynomial $m_{\alpha,F}(x) \in F[x]$ s.t.

$$\begin{cases} \alpha \text{ is a root of } m_{\alpha,F}(x) \\ \text{a polynomial } f(x) \text{ has } \alpha \text{ as a root } \Leftrightarrow m_{\alpha,F}(x) | f(x) \end{cases}$$

The polynomial $m_{\alpha,F}(x)$ is called the **minimal polynomial** of α over F. We define the **degree** of α over F to be $deg(m_{\alpha,F}(x))$.

Proof.

Let $I_\alpha := \{f(x) \in F[x], f(\alpha) = 0\}$. It's straightforward to check that I is an ideal of $F[x]$. By the assuumption that α is algebraic over F, $I_\alpha \neq \{0\}$. Let $p(x)$ be a polynomial s.t. $I_\alpha = (p(x))$. Check $p(x)$ is irreducible. Assume $p(x) = a(x)b(x), a(x), b(x) \in F[x]$. We want to show that one of $a(x), b(x)$ is a unit, i.e. one of $a(x), b(x)$ is a nonzero constant polynommial. Now we have

$$a(\alpha)b(\alpha) = p(\alpha) = 0$$

$$\Rightarrow a(\alpha) = 0 \text{ or } b(\alpha) = 0$$

If $a(\alpha) = 0$, then $a(x) \in I_\alpha = (p(x))$

$$\Rightarrow p(x)|a(x)$$

$$deg(a(x)) \geq deg(p(x)) \geq deg(a(x))$$

$$\Rightarrow deg(a(x)) = deg(p(x)) = deg(b(x)) = 0$$

$\Rightarrow b(x)$ is a nonzero constant polynomial, i.e. $b(x) \in F[x]^\times$. Likewise, if $b(\alpha) = 0$, then $a(x) \in F[x]^\times$. This proves that $p(x)$ is irreducible. Set

$$m_{\alpha,F}(x) = \frac{1}{(\text{leading coefficients of } p(x))} p(x)$$

Then $m_{\alpha,F}(x)$ is the polynomial with the claimed properties. $\square$

Theorem 3. Given a simple extension $F(\alpha)$ of F, where α is algebraic over F with minimal polynomial $m(x)$. Then

$$F(\alpha) \cong F[x]/(m(x))$$

Proof.

Consider the surjective ring homomorphism (evalutation at α) $\psi : F[x] \to F(\alpha)$, $p(x) \mapsto p(\alpha)$. The kernel is the set of polynomials having α as a root, which is simple the ideal $(m(x))$ of multiples of m. By the first isomorphism theorem

$$F(\alpha) \cong F[x]/(m(x))$$

$\square$

Corollary 1 (Extension as a vector space)**.** If α is algebraic over F, then $[F(\alpha), F] = \deg m_{\alpha,F}$ and $F(\alpha)$ is spanned (as an F-vector space) by $\{1, \alpha, \ldots, \alpha^{\deg m - 1}\}$ and is thus $F[\alpha]$.

Proof.

Let $n = \deg m$, then the coset representatives are the remainders in the division by $m(x)$,

$$F[x]/(m(x)) = \{a_0 + a_1 x + \bar{\ldots}\, a_{n-1}x^{n-1} : a_i \in F\}$$

Equivalently, this says that the set $1, \bar{x}, \ldots, \bar{x}^{n-1}$ forms an F-basis for $F(x)/(m(x))$. Applying the isomorphism to $F(\alpha)$ shows that the set $\{1, \cdots, \alpha^{n-1}\}$ is an F-basis for $F(\alpha)$. Therefore, we have $[F(\alpha) : F] = n$. Furthermore, we see immediately that $F(\alpha) = F[a]$. $\square$

Thus, for example, if K is a finite extension of $\mathbb{F}_p$,

Corollary 2. (Algebraic Equivalence) If α and β are two elements in K/F have the same minimal polynomials, then the fields $F(\alpha)$ and $F(\beta)$ are isomorphic as fields. Explicitly, there is an isomorphism $\phi : F(\alpha) \to F(\beta)$ that fixes F (i.e. sends every element in F to itself) and sends α to β

Proof.

Let $m(x)$ be the common minimal polynomials. $F(\alpha)$ and $F(\beta)$ are both isomorphic to $F[x]/(m(x))$. Thus $F(\alpha)$ and $F(\beta)$ are isomorphic. $\square$

2 Splitting fields and algebraic closures

3 Separable Extensions