大學基礎代數

李華介

國立台灣師範大學數學系

Chapter 10

中級 Field 的性質

在這一章中我們要更進一步探討 algebraic element 以及 algebraic extension 的性質. 另外我們也會利用所得的性質來探討一些有關 finite field 的基本性質.

10.1. Algebraic Elements

假設 F 是一個 field, L 是 F 的一個 extension. 要知道 F 中的一個元素 a 是否 algebraic over F, 依定義就必須驗證是否存在一個不為 0 的 $f(x) \in F[x]$ 使得 $f(a) = 0$. 一般來說用這種方法來驗證一個元素是否是 algebraic over F, 技術上是相當困難的. 這一節中我們將討論幾種和原先 algebraic element 的定義等價的性質, 這樣以後我們要驗證一個元素是否是 algebraic over F 就有多一點的方法來處理.

首先注意當 $a \in L$ 是 algebraic over F 時, 事實上滿足 $f(x) \in F[x]$ 且 $f(a) = 0$ 的多項式有無窮多個. 不過這其中有一個相當特別. 我們首先可以考慮滿足 $f(a) = 0$ 的 $f(x) \in F[x]$ 中 degree 最小的 polynomials. 這樣的 polynomials 有以下兩個重要的性質.

Lemma 10.1.1. 假設 F 是一個 *field,* L 是 F 的一個 *extension.* 若 $a \in L$ 是 *algebraic over* F 且 $f(x) \in F[x]$ 是 $F[x]$ 中滿足 $f(a) = 0$ 的非 0 多項式中 *degree* 最小的一個 *polynomial,* 則 $f(x)$ 有以下兩個性質*:*

(1) 若 $g(x) \in F[x]$ 且 $g(a) = 0$, 則存在 $h(x) \in F[x]$ 滿足 $g(x) = f(x) \cdot h(x)$.

(2) $f(x)$ 是 $F[x]$ 中的 *irreducible element.*

Proof. (1) 由於 F 是一個 field, 利用 Euclid's Algorithm (Theorem 7.2.4) 知存在 $h(x), r(x) \in F[x]$ 使得

$$g(x) = f(x) \cdot h(x) + r(x) \tag{10.1}$$

其中 $r(x) = 0$ 或 $\deg(r(x)) < \deg(f(x))$. 將 a 代入式子 (10.1) 得

$$g(a) = f(a) \cdot h(a) + r(a).$$

由於 $f(a) = g(a) = 0$, 我們得 $r(a) = 0$. 如果 $r(x) \neq 0$, 則得到 $r(x) \in F[x]$ 滿足 $\deg(r(x)) < \deg(f(x))$ 且 $r(a) = 0$. 這和 $f(x)$ 當初的選取相矛盾, 故知 $r(x) = 0$. 也就是說 $g(x) = f(x) \cdot h(x)$.

(2) 假設 $f(x)$ 在 $F[x]$ 中不是 irreducible, 即存在 $h(x), l(x) \in F[x]$ 滿足 $\deg(h(x)) < \deg(f(x))$, $\deg(l(x)) < \deg(f(x))$ 且 $f(x) = h(x) \cdot l(x)$. 將 a 代入上式, 由 $f(a) = 0$ 知 $h(a) \cdot l(a) = 0$. 由於 $h(x), l(x) \in F[x]$ 且 $a \in L$, 我們知 $h(a), l(a) \in L$. 故由 L 是 integral domain (Lemma 9.1.1) 得 $h(a) = 0$ 或 $l(a) = 0$. 這再次和 $f(x)$ 的選取相矛盾, 故知 $f(x)$ 是 $F[x]$ 中的 irreducible element. □

若 $f(x) \in F[x]$ 是 $F[x]$ 中符合 $f(a) = 0$ degree 最小的 polynomial 且 $g(x) \in F[x]$ 滿足 $g(a) = 0$, 則由 Lemma 10.1.1 (1) 知 $g(x) \in \big(f(x)\big)$. 現在如果 $g(x)$ 也是 $F[x]$ 中符合 $g(a) = 0$ degree 最小的 polynomial, 則可得 $\big(f(x)\big) = \big(g(x)\big)$. 由於 $F[x]$ 中的 unit 都是 F 中的非 0 元素 (Proposition 7.2.3) 利用 Lemma 8.1.3 知存在 $c \in F$ 使得 $f(x) = c \cdot g(x)$. 所以如果我們將這些次數最低而滿足 $f(a) = 0$ 的 polynomial 除以它們的最高次項係數所得的 monic polynomial 就唯一了. 因此我們有以下之定義.

Definition 10.1.2. 假設 F 是一個 field, L 是 F 的一個 extension field 且 $a \in L$ 是 algebraic over F. 若 $p(x) \in F[x]$ 是 $F[x]$ 的非 0 polynomial 中滿足 $p(a) = 0$ degree 最小的 monic polynomial, 則稱 $p(x)$ 是 a over F 的 *minimal polynomial.* 又如果 $\deg(p(x)) = n$, 則稱 a 是 algebraic over F of *degree* n.

我們知道當 $[L : F]$ 是有限的時候, L 中的元素都是 algebraic over F. 若 $[L : F] = n$ 且 $a \in L$, 則由於 $1, a, \ldots, a^n$ 一定 linearly independent over F, 故知存在 $f(x) \in F[x]$ 且 $\deg(f(x)) \leq n$ 使得 $f(a) = 0$ (詳見 Theorem 9.3.7 的証明) 故由 minimal polynomial 的定義知: 若 $p(x)$ 是 a 的 minimal polynomial, 則 $\deg(p(x)) \leq \deg(f(x)) \leq n$. 換言之我們得 a 的 degree 小於或等於 $[L : F]$. 我們將這個結果寫成以下之 Lemma.

Lemma 10.1.3. 假設 F 是一個 *field,* L 是 F 的一個 *finite extension,* 則 L 中任意的元素都是 *algebraic over* F 且其 *degree* 小於或等於 $[L : F]$.

當 L 不是 finite extension over F 時, L 中當然有可能存在元素是 algebraic over F. 如果 $a \in L$ 是 algebraic over F, 我們想知道 F 和 L 之間是否可以找到一個 field K 是 F 的一個 finite extension 滿足 $a \in K$?

Definition 10.1.4. 假設 F 是一個 field, L 是 F 的一個 extension field. 若 K 是 L 的一個 extension field 且 $F \subseteq K \subseteq L$, 則稱 K 是 L over F 的一個 *subextension* 或是 *intermediate field.*

Proposition 10.1.5. 假設 F 是一個 *field*, L 是 F 的一個 *extension field*. 若 $a \in L$ 是 *algebraic over* F 且其 *degree* 為 n, 則存在 L *over* F 的一個 *subextension* K 滿足 $a \in K$ 且 $[K : F] = n$.

Proof. 考慮 $\phi : F[x] \to L$ 其中對任意的 $f(x) \in F[x]$, $\phi(f(x)) = f(a)$. 由於 $a \in L$, 所以自然有 $\phi(f(x)) = f(a) \in L$, 因此 ϕ 確實是一個從 $F[x]$ 映射到 L 的函數. 很容易驗證 ϕ 是一個 ring homomorphism.

什麼是 $\ker(\phi)$ 呢? 由於 $F[x]$ 是一個 principle ideal domain 且 $\ker(\phi)$ 是 $F[x]$ 的一個 ideal, 我們知存在 $p(x) \in f[x]$ 使得 $\ker(\phi) = \big(p(x)\big)$. 事實上 我們可以有 $\ker(\phi) = \big(p(x)\big)$ 其中 $p(x)$ 是 a 的 minimal polynomial. 這是因為若 $f(x) \in \ker(\phi)$, 則知 $\phi(f(x)) = f(a) = 0$. 故由 Lemma 10.1.1 知 $f(x) \in \big(p(x)\big)$. 反之, 對任意 $f(x) \in \big(p(x)\big)$, 存在 $h(x) \in F[x]$ 使得 $f(x) = p(x) \cdot h(x)$, 因此由 $p(a) = 0$ 得 $f(a) = p(a) \cdot h(a) = 0$. 故得證 $\ker(\phi) = \big(p(x)\big)$, 其中 $p(x)$ 是 a 的 minimal polynomial.

現由 First Isomorphism Theorem (6.4.2) 知

$$F[x]/\big(p(x)\big) \simeq \mathrm{im}(\phi).$$

然而 $p(x)$ 是 $F[x]$ 的一個 irreducible element (Lemma 10.1.1), 故由 $\big(p(x)\big)$ 是 $F[x]$ 的一個 maximal ideal (Lemma 8.3.2), 得知 $F[x]/\big(p(x)\big)$ 是一個 field (Theorem 6.5.11). 換言之 $\mathrm{im}(\phi)$ 是一個 field.

至於什麼是 $\mathrm{im}(\phi)$ 呢? 由定義知

$$\mathrm{im}(\phi) = \{f(a) \mid f(x) \in F[x]\}.$$

換言之, $\mathrm{im}(\phi)$ 裡的元素都是由某個 $F[x]$ 裡的 polynomial 代入 a 所得. 所以若 $c \in F$, 我們自然有 $\phi(c) = c \in \mathrm{im}(\phi)$, 故得 $F \subseteq \mathrm{im}(\phi) \subseteq L$. 另一方面將 a 代入 x 這一個 polynomial 得到 a: 也就是說 ϕ 將 x 送到 a (即 $\phi(x) = a$), 故知 $a \in \mathrm{im}(\phi)$. 所以若令 $K = \mathrm{im}(\phi)$, 則知 K 是 L over F 的一個 subextension 且 $a \in K$. 最後由假設 a over F 的 degree 是 n, 也就是說 a 的 minimal polynomial $p(x)$ 的 degree 是 n, 因此由 Lemma 9.3.6 知 $\dim_F(F[x]/\big(p(x)\big)) = \deg(p(x)) = n$. 故由 $K \simeq F[x]/\big(p(x)\big)$ 知 $[K : F] = n$. □

若僅由定義來看 Proposition 10.1.5 中的 $\mathrm{im}(\phi) = \{f(a) \mid f(x) \in F[x]\}$ 只是一個 ring, 那為何它會是 field 呢? 若你記得 Theorem 9.3.7 這就一點都不奇怪了. 因為 $\mathrm{im}(\phi) \subseteq L$ 自然是 integral domain, 而由 Proposition 10.1.5 的證明也知 $\dim_F(\mathrm{im}(\phi)) = n$.

我們也很容易檢查 $\{f(a) \mid f(x) \in F[x]\}$ 會是 L 中包含 F 以及 a 最小的 ring, 這是因為若 R 是一個 ring 且包含 F 以及 a, 則對任意的 $f(x) \in F[x]$, 由於 $f(a)$ 僅牽涉到 a 和 F 中的元素間的加法以及乘法, 別忘了這些都是 R 中元素的運算所以當然

得 $f(a) \in R$. 換言之我們得 $\{f(a) \mid f(x) \in F[x]\} \subseteq R$, 再加上 $\{f(a) \mid f(x) \in F[x]\}$ 本身是一個 ring 所以它自然是包含 F 以及 a 最小的 ring 了!

為了方便我們定以下之符號, 在一般的代數書上這個定義是標準的且常被使用的定義.

Definition 10.1.6. 假設 F 是一個 field, L 是 F 的一個 extension field 且 $a \in L$. 我們令 $F[a]$ 表示 L 中包含 F 以及 a 最小的 ring; 我們也令 $F(a)$ 表示 L 中包含 F 以及 a 最小的 field.

前面已知 $F[a]$ 就是 $\mathrm{im}(\phi) = \{f(a) \mid f(x) \in F[x]\}$. 那麼 $F(a)$ 中的元素又是怎樣呢? 利用 quotient field 的性質 (Proposition 7.4.2) 很容易驗證

$$F(a) = \{f(a)/g(a) \mid f(x), g(x) \in F[x] \text{ 且 } g(a) \neq 0\}.$$

由這裡可看出: 一般來說 $F[a]$ 和 $F(a)$ 是不相同的; 不過前面提過若 a 是 algebraic over F, 則 $F[a]$ 會是一個 field, 所以 $F[a]$ 自然是包含 F 以及 a 最小的 field. 換句話說當 a 是 algebraic over F 時, 我們有 $F[a] = F(a)$. 因此 $F(a)$ 就是 Proposition 10.1.5 中所要找的 K, 所以我們將 Proposition 10.1.5 重整以後可以得:

Corollary 10.1.7. 假設 F 是一個 *field,* L 是 F 的一個 *extension field. 若* $a \in L$ 是 *algebraic over* F 且 $p(x) \in F[x]$ 為 a *over* F 的 *minimal polynomial,* 則

$$F(a) \simeq F[x]/\big(p(x)\big) \quad \text{and} \quad [F(a) : F] = \deg(p(x)).$$

Remark 10.1.8. 同學或許會奇怪 $F[a]$ 裡的元素長的是 $f(a)$ 其中 $f(x) \in F[x]$ 這種樣子, 而 $F(a)$ 裡的元素長的是 $f(a)/g(a)$ 其中 $f(x), g(x) \in F[x]$ 這種樣子: 兩個樣子差這麼多, 怎麼可能會 $F[a] = F(a)$ 呢? 這是因為當 a 是 algebraic over F 時, $F[a]$ (或 $F(a)$) 裡的元素其表示法是不唯一的. 例如若 $p(x) \in F[x]$ 是 a 的 minimal polynomial, 如果令 $g(x) = f(x) + p(x)$, 則 $g(a) = f(a)$. 所以當然有可能用不同的形式寫下來的元素它們的值是相同的.

接下來我們就來看和 a 是 algebraic over F 等價的條件是什麼?

Theorem 10.1.9. 假設 F 是一個 *field,* L 是 F 的一個 *extension field* 且 $a \in L$, 則下面有關於 a 的敘述是等價的.

(1) a 是 *algebraic over* F.

(2) 存在 K 是 L *over* F 的 *subextension* 滿足 $a \in K$ 且 $[K : F]$ 是有限的.

(3) $F[a] = F(a)$.

Proof. 由前面 Proposition 10.1.5 可知 (1) $\Rightarrow$ (2), 所以我們僅要驗證 (2) $\Rightarrow$ (3) 以及 (3) $\Rightarrow$ (1).

(2) ⇒ (3): 若 K 是 L over F 的 subextension (即 $F \subseteq K \subseteq L$), 則由假設 $a \in K$ 知 $F[a] \subseteq K$. 再由假設 K 是 F 的一個 finite extension, 套用 Proposition 9.4.3 可得 $F[a]$ 是一個 field. 故知 $F[a] = F(a)$.

(3) ⇒ (1): 假設 $F[a] = F(a)$, 也就是說 $F[a]$ 是一個 field. 如果 $a = 0 \in F$, 那當然 a 是 algebraic over F (注意 F 中的元素當然是 algebraic over F). 如果 $a \neq 0$, 則由 $a \in F[a]$ 且 $F[a]$ 是一個 field 知 $a^{-1} \in F[a]$. 別忘了 $F[a]$ 裡的元素都是 $f(a)$, 其中 $f(x) \in F[x]$ 這種形式, 所以我們有 $a^{-1} = f(a)$, 其中

$$f(x) = c_n x^n + \cdots + c_1 x + c_0, \quad c_i \in F.$$

故由

$$a^{-1} = c_n \cdot a^n + \cdots + c_1 \cdot a + c_0$$

得

$$1 = c_n \cdot a^{n+1} + \cdots + c_1 \cdot a^2 + c_0 \cdot a.$$

因此若令

$$g(x) = c_n x^{n+1} + \cdots + c_1 x^2 + c_0 x - 1,$$

則 $g(a) = 0$. 由於 $g(x) \in F[x]$ 且 $g(x) \neq 0$, 故知 a 是 algebraic over F. □

Theorem 10.1.9 給了我們一個很好的方法來驗證 a 是否是 algebraic over F. 也就是說今後要檢查 a 是 algebraic over F 我們可以不必真的去找一個 $f(x) \in F[x]$ 使得 $f(a) = 0$. 當然了要用什們方法會因問題而有所差別. 比方說若 $a^2 \in L$ 且我們知 a^2 是 algebraic over F, 如果 $f(x) \in F[x]$ 滿足 $f(a^2) = 0$, 則令 $g(x) = f(x^2)$, 我們可得 $g(a) = f(a^2) = 0$. 因此知 a 也是 algebraic over F. 也就是當 a^2 是 algebraic over F 時, a 也會是 algebraic over F. 但是反過來, 如果已知 a 是 algebraic over F, 我們就無法利用滿足 a 的 polynomial 來製造一個滿足 a^2 的 polynomial 了. 同學或許會想若 $f(a) = 0$, 我們可以令 $g(x) = f(x^{1/2})$, 則 $g(a^2) = f(a) = 0$ 呀! 這是不對的, 因為 $f(x)$ 若有奇數次項, 則 $g(x) = f(x^{1/2})$ 就不再是一個 polynomial 了. 所以在這種狀況下就不可能利用找 polynomial 的方法來證明 a^2 是 algebraic over F. 其實當 a 是 algebraic over F 時利用 Theorem 10.1.9 知存在一個 field K 是 F 的 finite extension 且 $a \in K$. 然而 K 是一個 field 且 $a \in K$, 所以當然 $a^2 \in K$, 所以再用一次 Theorem 10.1.9 (或是利用 Lemma 10.1.3) 我們得證 a^2 也是 algebraic over F. 以後我們常會用類似的方法來處理相關的問題.

10.2. Algebraic Closure

當 F 是一個 field, L 是 F 的一個 extension 時, 我們可以將 L 中的元素分成 algebraic over F 和不是 algebraic over F 的兩種. 在這一節中我們將探討 L 中所有 algebraic over F 的元素所成之集合.

Definition 10.2.1. 假設 F 是一個 field 且 L 是 F 的一個 extension. 我們令

$$\overline{L_F} = \{a \in L \mid a \text{ 是 algebraic over } F\},$$

稱之為 F 在 L 的 *algebraic closure*.

F 中的元素當然是 algebraic over F, 所以由定義知 $F \subseteq \overline{L_F} \subseteq L$. 另外如果 L 是 F 的一個 finite extension, 則由 Lemma 9.4.5 知 L 中的元素都 algebraic over F, 所以在這個假設之下 $\overline{L_F} = L$.

接下來我們要證明 $\overline{L_F}$ 的一個重要性質, 即 $\overline{L_F}$ 是一個 field. 換言之, 我們要證明若 $a, b \in \overline{L_F}$, 其中 $b \neq 0$, 則 $a - b$ 以及 $a \cdot b^{-1}$ 皆在 $\overline{L_F}$ 中 (Lemma 9.1.4). 要如何證明這些元素都是 algebraic over F 呢? 當然不可能用找 polynomial 的方法, 我們必須藉助 Theorem 10.1.9. 在這之前我們先推廣一下 Definition 10.1.6.

Definition 10.2.2. 假設 F 是一個 field 且 L 是 F 的一個 extension. 若 $a_1, \ldots, a_n \in L$, 則定 $F(a_1, \ldots, a_n)$ 表示為 L 中包含 F 以及 $a_1, \ldots, a_n$ 最小的 field.

Lemma 10.2.3. 假設 F 是一個 *field* 且 L 是 F 的一個 *extension.* 若 $a_1, \ldots, a_n \in L$ 皆為 *algebraic over* F, 則 $F(a_1, \ldots, a_n)$ 是 F 的一個 *finite extension.* 事實上, 如果已知 $a_1, \ldots, a_n$ *over* F 的 *degree* 分別為 $m_1, \ldots, m_n$, 則

$$[F(a_1, \ldots, a_n) : F] \leq m_1 \cdots m_n.$$

Proof. 為了方便, 我們令

$$K_1 = F(a_1), K_2 = K_1(a_2) = F(a_1, a_2), \ldots, K_n = K_{n-1}(a_n) = F(a_1, \ldots, a_n).$$

對任意的 i, 我們有 $[K_i : K_{i-1}] = [K_{i-1}(a_i) : K_i] \leq m_i$. 這裡 $[K_{i-1}(a_i) : K_{i-1}]$ 會小於或等於 m_i 的原因是: 由 Corollary 10.1.7 知 $[K_{i-1}(a_i) : K_{i-1}]$ 的值剛好是 a_i over K_{i-1} 的 minimal polynomial $q_i(x) \in K_{i-1}[x]$ 的 degree. 然而由假設 a_i over F 的 minimal polynomial $p_i(x) \in F[x]$ 的 degree 為 m_i. 由於 $p_i(x) \in F[x] \subseteq K_{i-1}[x]$ 且 $p_i(a_i) = 0$, 故由 $q_i(x)$ 是 a_i over K_{i-1} 的 minimal polynomial 的假設知 $\deg(q_i(x)) \leq \deg(p_i(x)) = m_i$. 故知

$$[K_i : K_{i-1}] = [K_{i-1}(a_i) : K_{i-1}] = \deg(q_i(x)) \leq m_i.$$

現在由於每一段 $[K_i : K_{i-1}]$ 都是有限的, 所以我們可以連續套用 Theorem 9.4.6 得:

$$\begin{aligned} [F(a_1, \ldots, a_n) : F] &= [K_n : K_{n-1}][K_{n-1} : F] \\ &= [K_n : K_{n-1}][K_{n-1} : K_{n-2}][K_{n-2} : F] \\ &\vdots \\ &= [K_n : K_{n-1}] \cdots [K_1 : F] \leq m_n \cdots m_1. \end{aligned}$$

故得證 $F(a_1, \ldots, a_n)$ 是 F 的一個 finite extension. □

利用 Lemma 10.2.3 我們馬上可得知 $\overline{L_F}$ 是一個 field.

Theorem 10.2.4. 假設 F 是一個 *field* 且 L 是 F 的一個 *extension.* 若 $a, b \in L$, 其中 $b \neq 0$, 皆為 *algebraic over* F, 則 $a+b$, $a-b$, $a \cdot b$ 以及 $a \cdot b^{-1}$ 皆為 *algebraic over* F. 由此我們可得 $\overline{L_F}$ 是一個 *field.*

Proof. 由 Lemma 10.2.3 我們知 $F(a,b)$ 是 F 的一個 finite extension. 由於 $a, b \in F(a,b)$, $b \neq 0$ 且 $F(a,b)$ 是一個 field, 我們自然有 $a+b$, $a-b$, $a \cdot b$ 以及 $a \cdot b^{-1}$ 皆為 $F(a,b)$ 的元素. 故由 Theorem 10.1.9 (或 Lemma 10.1.3) 知這四個元素皆為 algebraic over F.

今若 $a, b \in \overline{L_F}$, 其中 $b \neq 0$, 則由定義知 a, b 皆為 algebraic over F. 故由前知 $a+b$, $a-b$, $a \cdot b$ 以及 $a \cdot b^{-1}$ 皆為 algebraic over F. 故知這四個元素皆在 $\overline{L_F}$ 中, 因此得證 $\overline{L_F}$ 是一個 field. □

假設 L 是 F 的一個 extension, 且 K 是 L over F 的 subextension (即 $F \subseteq K \subseteq L$). L 中是 algebraic over K 的元素未必是 algebraic over F. 不過 L 中是 algebraic over F 的元素就一定是 algebraic over K. 這是因為若 $a \in \overline{L_F}$ (即 $a \in L$ 是 algebraic over F), 表示在 $F[x]$ 中存在 $f(x) \neq 0$ 使得 $f(a) = 0$. 由於 $f(x) \in F[x] \subseteq K[x]$, 我們自然得 a 也是 algebraic over K. 故得 $a \in \overline{L_K}$, 換句話說我們總是有

$$\overline{L_F} \subseteq \overline{L_K}.$$

我們有興趣知道什麼時候 $\overline{L_F}$ 會等於 $\overline{L_K}$. 以下是一個例子.

Lemma 10.2.5. 假設 F 是一個 *field,* L 是 F 的一個 *extension,* 且 K 是 L *over* F 的 *subextension.* 若 K 是 F 的一個 *finite extension,* 則 $\overline{L_F} = \overline{L_K}$

Proof. 我們已知 $\overline{L_F} \subseteq \overline{L_K}$, 所以只要證明 $\overline{L_K} \subseteq \overline{L_F}$. 也就是要證明: 若 $a \in L$ 是 algebraic over K, 則 a 是 algebraic over F. 我們考慮 $K(a)$ 這一個 field. 由假設 a 是 algebraic over K, 故利用 Corollary 10.1.7 知 $K(a)$ 是 K 的一個 finite extension. 再加上 K 是 F 的一個 finite extension, 套用 Theorem 9.4.6 可得

$$[K(a) : F] = [K(a) : K][K : F],$$

因此 $K(a)$ 是 F 的一個 finite extension. 故利用 $a \in K(a)$ 以及 Theorem 10.1.9 (或 Lemma 10.1.3) 知 a 是 algebraic over F. □

我們可以將 Lemma 10.2.5 推廣到更一般的狀況. 回顧一下若 K 是 F 的一個 algebraic extension 表示 K 中的元素皆為 algebraic over F. 在 Lemma 10.2.5 中的假設 K 是 F 的 finite extension, 所以自然是 F 的一個 algebraic extension. 我們要將 Lemma 10.2.5 推廣到 K 是 F 的 algebraic extension 這個狀況.

Theorem 10.2.6. 假設 F 是一個 *field,* L 是 F 的一個 *extension,* 且 K 是 L *over* F 的 *subextension.* 若 K 是 F 的一個 *algebraic extension,* 則 $\overline{L_F} = \overline{L_K}$

Proof. 和 Lemma 10.2.5 相同的情形, 我們只要證明: 若 $a \in L$ 是 algebraic over K, 則 a 是 algebraic over F. 不過這裡碰到的狀況是 K 可能不是 finite extension over F, 所以我們不能直接套用 Lemma 10.2.5. 要克服這個困難, 我們必須想辦法找到一個 F 的 finite extension K' 且滿足 a 是 algebraic over K'. 如此再套用 Lemma 10.2.5 得證 a 是 algebraic over F.

由假設 a 是 algebraic over K, 知存在 $f(x) \neq 0$ 且 $f(x) \in K[x]$ 使得 $f(a) = 0$. 假設 $f(x) = a_n x^n + \cdots + a_0$. 由於 $a_n, \ldots, a_0 \in K$ 且 K 是 F 的一個 algebraic extension, 故知 $a_n, \ldots, a_0$ 皆為 algebraic over F. 令 $K' = F(a_n, \ldots, a_0)$, 由 Lemma 10.2.3 知 K' 是 F 的一個 finite extension. 故利用 Lemma 10.2.5 知 $\overline{L_{K'}} = \overline{L_F}$. 另外由於 $a_n, \ldots, a_0 \in F(a_n, \ldots, a_0) = K'$, 我們知 $f(x) \in K'[x]$. 故由 $f(a) = 0$ 知 a 是 algebraic over K'. 換言之, 我們有 $a \in \overline{L_{K'}}$, 故由 $\overline{L_{K'}} = \overline{L_F}$ 得知 $a \in \overline{L_F}$. 因此得證 a 是 algebraic over F. □

我們已知 $\overline{L_F}$ 是一個 filed (Theorem 10.2.4) 且 $F \subseteq \overline{L_F} \subseteq L$. 如果我們再收集 L 中是 algebraic over $\overline{L_F}$ 的元素會不會得到更大的 field 的呢? 換句話來說, 我們想知道 $\overline{L_{\overline{L_F}}}$ (不要被這符號嚇著了) 是什麼? 事實上所謂的 algebraic closure 就是說 L 中 algebraic over $\overline{L_F}$ 的元素所成的集合就是 $\overline{L_F}$ 自己.

Corollary 10.2.7. 假設 F 是一個 *field* 且 L 是 F 的一個 *extension,* 若 $a \in L$ 且 a 是 *algebraic over* $\overline{L_F}$, 則 a 是 *algebraic over* F. 也就是說, 我們有

$$\overline{L_{\overline{L_F}}} = \overline{L_F}.$$

Proof. 首先注意由定義 $\overline{L_F}$ 中的元素都是 algebraic over F, 故知 $\overline{L_F}$ 是 F 的一個 algebraic extension. 因此若令 $K = \overline{L_F}$, 則 K 符合 Theorem 10.2.6 的條件, 故知 $\overline{L_K} = \overline{L_F}$. 也因此若 $a \in L$ 是 algebraic over $\overline{L_F} = K$, 表示 $a \in \overline{L_K}$. 故由 $\overline{L_K} = \overline{L_F}$ 得知 $a \in \overline{L_F}$, 也就是說 a 是 algebraic over F. □

10.3. Roots of Polynomials

這一節中我們將討論一個 polynomial 在一個 field 中它的根的性質.

首先我們還是來看大家最熟悉的餘式定理.

Lemma 10.3.1. 假設 F 是一個 *field.* 若 $f(x) \in F[x]$, 其中 $\deg(f(x)) = n$, 且 $a \in F$ 滿足 $f(a) = 0$, 則存在 $h(x) \in F[x]$, 其中 $\deg(h(x)) = n - 1$, 使得 $f(x) = (x - a) \cdot h(x)$.

Proof. 由於 F 是一個 field, 考慮 $f(x) \in F[x]$ 以及 $(x - a) \in F[x]$, 利用 Euclid's Algorithm (Theorem 7.2.4) 知存在 $h(x), r(x) \in F[x]$ 滿足 $f(x) = (x-a) \cdot h(x) + r(x)$, 其中 $r(x) = 0$ 或 $\deg(r(x)) < \deg(x - a) = 1$. 如果 $r(x) \neq 0$ 由 $\deg(r(x)) < 1$ 知 $r(x) = c \in F$ 是一個常數. 但由於 $f(a) = 0$ 故將 a 代入 $f(x) = (x - a) \cdot h(x) + c$

得 $c = 0$, 此和 $r(x) \neq 0$ 相矛盾故知 $r(x) = 0$. 也就是 $f(x) = (x - a) \cdot h(x)$. 至於 $\deg(h(x)) = n - 1$, 可由 Lemma 7.2.2 直接得知. □

由於 $\deg(x - a) = 1$, 我們知道 $x - a$ 是 $F[x]$ 中的 irreducible element. 因此 Lemma 10.3.1 告訴我們若 $f(a) = 0$, 則 $x - a$ 會是 $f(x)$ 的一個 irreducible divisor. 利用 $F[x]$ 是 unique factorization domain (Theorem 7.2.14), 我們知存在 $k \in \mathbb{N}$ 以及 $q(x) \in F[x]$ 使得 $f(x) = (x - a)^k \cdot q(x)$, 其中 $q(a) \neq 0$ (即 $x - a$ 不是 $q(x)$ 的 divisor). 我們依此來定義 a 在 $f(x)$ 的重根數.

Definition 10.3.2. 假設 F 是一個 field. 若 $f(x) \in F[x]$ 且 $a \in F$ 滿足 $f(a) = 0$, 則稱 a 是一個 *root* of $f(x)$. 又如果 $f(x) = (x - a)^k \cdot q(x)$, 其中 $q(a) \neq 0$, 則稱 a 是一個 *root* of *multiplicity* k of $f(x)$.

接下來也是大家熟悉的定理: 一個 n 次多項式在一個 field 中計算重根在內至多有 n 個根. 這裡指的計算重根在內是說如果 a 是 k 重根, 則要算成是 k 個根.

Theorem 10.3.3. 假設 F 是一個 *field.* 若 $f(x) \in F[x]$ 且 $\deg(f(x)) = n \geq 1$, 則在 F 中將 *multiplicity* 計算在內, $f(x)$ 至多有 n 個 *roots.*

Proof. 我們利用 induction. 如果 $\deg(f(x)) = 1$, 則 $f(x)$ 當然僅有 1 個根. 假設 degree 小於 n 的 polynomial 定理皆成立. 現考慮 $f(x) \in F[x]$ 且 $\deg(f(x)) = n$ 的情形. 如果 $f(x)$ 在 F 中沒有 root, 則定理當然成立. 如果 $a \in F$ 是 $f(x)$ 的一個 root of multiplicity k, 即表示存在 $q(x) \in F[x]$ 使得 $f(x) = (x - a)^k \cdot q(x)$, 其中 $q(a) \neq 0$. 利用 degree 的性質 (Lemma 7.2.2) 我們有 $\deg(q(x)) = n - k < n$, 故利用 induction 的假設知在 F 中將 multiplicity 計算在內, $q(x)$ 至多有 $n - k$ 個 roots. 然而若 $b \in F$ 是 $f(x)$ 的一個 root, 我們有

$$0 = f(b) = (b - a)^k \cdot q(b).$$

利用 F 是 integral domain, 我們知 $f(x)$ 的 roots 要不是 a 就是 $q(x)$ 的 roots. 因此在 F 中 $f(x)$ roots 的個數就是 k 加上 $q(x)$ 的 roots 的個數, 所以至多有 $k + (n - k) = n$ 個. □

我們要看一個元素 a 是否是 $f(x)$ 的一個根, 大家直覺的想法就是將 a 代入 $f(x)$ 看是否為 0. 事實上這是不對的, 要將 a 代入 $f(x)$ 牽扯上 a 和 $f(x)$ 的係數間的加法和乘法. 換言之如果 a 座落在一個包含 F 和 a 的 field L (至少要是 ring) 中, 這樣我們才可以將 a 和 $f(x)$ 的係數考慮成是 L 的元素而加以運算. 這樣 $f(a)$ (看成是 L 的元素) 才有意義. 這就是為甚麼我們前面的討論都會先給 F 的一個 extension L, 然後再談論 $a \in L$ 與 $F[x]$ 中的 polynomials 的關係. 所以我們自然會問: 給定任一非常數的 $f(x) \in F[x]$ 是否可以找到 F 的一個 extension L 使得 $f(x)$ 在 L 中有根? 答案是肯定的. 以下的定理就是回答這個問題. 我們將會建構一個 F 的 extension field 然後說明在其中可找到一個根. 這個定理的證明同學或許會覺得"虛

虛"的, 因為好像沒有真的在找根的感覺. 不過這就是數學在談存在性所關心的重點, 我們只要知道東西存在而不必真正告訴你東西是什麼.

Theorem 10.3.4. 假設 F 是一個 *field* 且 $p(x) \in F[x]$ 是 $F[x]$ 中的 *irreducible element,* 則存在一個 *field* L 是 F 的 *finite extension,* 其中 $[L:F] = \deg(p(x))$ 且 L 中存在 $a \in L$ 滿足 $p(a) = 0$.

Proof. 令 $L = F[x]/\big(p(x)\big)$. 由於 $p(x)$ 是 irreducible, 我們知 $\big(p(x)\big)$ 是 $F[x]$ 中的 maximal ideal, 故知 L 是一個 field.

首先我們要驗證 L 中存在一個 subfield 和 F 是 isomorphic 的, 因此我們可以將 L 看成是 F 的一個 extension. 事實上考慮 $\pi : F \to F[x]/\big(p(x)\big)$, 定義成 $\pi(c) = \overline{c}$, 很容易驗證 π 是一個 ring homomorphism. 也很容易驗證 π 是一對一的: 這是因為如果 $c \in \ker(\pi)$, 表示 $\overline{c} = \overline{0}$, 即 $c \in \big(p(x)\big)$. 但是 $\big(p(x)\big)$ 中除了 0 以外沒有其他的常數, 故得 $c = 0$ (也可套用 Proposition 9.1.5 (2) 得到 π 是一對一). 因此得證 $\mathrm{im}(\pi)$ 是 L 的 subfield 且和 F 是 isomorphic 的.

現在要證明 L 中存在一元素是 $p(x)$ 的根. 考慮 $a = \overline{x} \in L$, 我們要說明 $p(\overline{x}) = \overline{0}$ (注意 $\overline{0}$ 是 $L = F[x]/\big(p(x)\big)$ 的 0). 假設 $p(x) = a_n x^n + \cdots + a_1 x + a_0$, 其中 $a_i \in F$. 那麼 $p(a)$ 會是什麼呢? 別忘了我們提過這裡代入 a 必須用到的是 L 中的運算, 而在 L 中 $c \in F$ 是需經過 π 送到 L 的, 換句話說我們必須考慮的是 $\overline{c}$. 因此有

$$\begin{aligned} p(a) &= p(\overline{x}) \\ &= a_n \cdot \overline{x}^n + \cdots + a_1 \cdot \overline{x} + a_0 \\ &= \overline{a_n} \cdot \overline{x}^n + \cdots + \overline{a_1} \cdot \overline{x} + \overline{a_0} \quad (\text{依 } L \text{ 的運算定義}) \\ &= \overline{a_n x^n + \cdots + a_1 x + a_0} \\ &= \overline{p(x)} = \overline{0} \end{aligned}$$

所以 L 中真的存在一個元素代入 $p(x)$ 等於 L 中的 0.

最後由 Lemma 9.3.6 知 $[L:F] = \dim_F(L) = \dim_F(F[x]/\big(p(x)\big)) = \deg(p(x))$. □

由 Theorem 10.3.4 我們很容易得到以下一般的狀況.

Corollary 10.3.5. 假設 F 是一個 *field* 且 $f(x) \in F[x]$, 其中 $\deg(f(x)) = n \geq 1$, 則存在一個 *field* L 是 F 的 *finite extension,* 其中 $[L:F] \leq n$ 且 L 中存在 $a \in L$ 滿足 $f(a) = 0$.

Proof. 由於 $f(x) \in F[x]$ 而且 $\deg(f(x)) \geq 1$, 所以 $f(x)$ 不是 $F[x]$ 中的 unit. 利用 $F[x]$ 是 unique factorization domain, 我們知存在 $p(x) \in F[x]$ 是 $F[x]$ 中的 irreducible element 滿足 $p(x) \mid f(x)$. 注意如果 $p(a) = 0$, 則當然得 $f(a) = 0$. 因此由 Theorem 10.3.4 知存在 L, 其中 $[L:F] = \deg(p(x)) \leq \deg(f(x))$ 且 $a \in L$, 滿足 $f(a) = p(a) = 0$. □

我們可以一直套用 Corollary 10.3.5 找到一個 F 的 finite extension L' 使得 $f(x)$ 在 L' 中可以完全分解. 這裡所謂的 $f(x)$ 在 L' 完全分解就是說: 如果 $\deg(f(x)) = n$, 則 $f(x)$ 在 $L'[x]$ 中可以寫成 $f(x) = c \cdot (x - a_1) \cdots (x - a_n)$, 其中 $a_i \in L'$. 此時我們通常稱 $f(x)$ *splits into linear factors* in L'.

Theorem 10.3.6. 假設 F 是一個 *field* 且 $f(x) \in F[x]$, 其中 $\deg(f(x)) = n \geq 1$, 則存在一個 *field* L' 是 F 的 *finite extension,* 其中 $[L' : F] \leq n!$, 使得 $f(x)$ *splits into linear factors in* L'.

Proof. 利用 Corollary 10.3.5 知存在 L_1 是 F 的一個 extension 滿足 $[L_1 : F] \leq n$ 且 $a_1 \in L_1$ 使得 $f(a_1) = 0$. 故由 Lemma 10.3.1 知存在 $f_1(x) \in L_1[x]$ 且 $\deg(f_1(x)) = n - 1$ 使得 $f(x) = (x - a_1) \cdot f_1(x)$. 對 $f_1(x)$ 再套用一次 Corollary 10.3.5 知存在 L_2 是 L_1 的一個 extension 滿足 $[L_2 : L_1] \leq n - 1$ 且 $a_2 \in L_2$ 使得 $f_1(a_2) = 0$. 注意此時

$$[L_2 : F] = [L_2 : L_1][L_1 : F] \leq n(n - 1),$$

且存在 $f_2(x) \in L_2[x]$ 使得

$$f(x) = (x - a_1) \cdot (x - a_2) \cdot f_2(x).$$

所以這樣一直作下去 (或是對 degree 作 induction) 我們得證本定理. □

最後我們強調一下 Theorem 10.3.6 裡的 L' 當然會因 $f(x)$ 不同而不同, 不過事實上我們可以找到一個 F 的 extension $\tilde{F}$ 使得 $F[x]$ 中的所有 polynomial 在 $\tilde{F}$ 中都可以 splits into linear factors (當然此時 $\tilde{F}$ 有可能不是 F 的 finite extension). 不過由於這個定理的證明需用到所謂的 *Zorn's Lemma*, 我們就略去不證了.

10.4. Finite Fields

在這個講義的最後一節, 我們要簡單的介紹 finite field 的一些簡單的性質.

回顧一下所謂 F 是一個 finite field 就是說 F 是一個 field 且 F 的元素個數 (通常我們用 $|F|$ 來表示) 是有限多個. 由這個定義我們馬上知若 F 是 finite field, 則 F 的 characteristic 一定是一個質數 p (Lemma 9.2.3). 當初我們定 characteristic 是利用一個 ring homomorphism $\phi : \mathbb{Z} \to F$, 其中對任意 $n \in \mathbb{N}$ 我們定 $\phi(n) = n1$, 而 $\phi(-n) = n(-1)$. F 的 characteristic 是 p 表示 $\ker(\phi) = \big(p\big)$. 因此由 ring 的 1st Isomorphism Theorem 我們知 $\mathbb{Z}/\big(p\big) \simeq \mathrm{im}(\phi) \subseteq F$. 別忘了 p 是質數, 故知 $\big(p\big)$ 會是 $\mathbb{Z}$ 的一個 maximal ideal, 因此 $\mathbb{Z}/\big(p\big)$ 是一個 field. 又因 $\big|\mathbb{Z}/\big(p\big)\big| = p$, 我們得 F 中存在一個 subfield 和 $\mathbb{Z}/\big(p\big)$ 這個 p 個元素的 finite field 是 isomorphic 的. 為了方便我們將這個 p 個元素的 finite field 記為: $\mathbb{F}_p$.

既然 F 是 $\mathbb{F}_p$ 的一個 extension, 我們當然就可以把 F 看成是一個 vector space over $\mathbb{F}_p$. 那麼 F 會不會是 finite dimensional over $\mathbb{F}_p$ 呢? 大家可能都會猜想會, 但是怎麼證呢? 一般來說我們要證明一個 vector space V 是 finite dimensional over 一

個 field K, 我們只要證明 V 中可以找到有限多個元素 span V over K. 現在由於 F 是 finite field, 就假設 $|F| = n$ 吧, 那麼 F 中所有的元素當然 span F over $\mathbb{F}_p$ 了 (因為每個 $a \in F$ 都可以看成是 $a = 1 \cdot a$). 所以由 Lemma 9.3.4 (1) 知 $\dim_{\mathbb{F}_p}(F) \leq n$. 當然我們這個估計的 dimension 是非常粗略, 不過我們目前的目的只是要知道 F 是 $\mathbb{F}_p$ 的一個 finite extension. 綜合以上的結果我們可以得到以下 finite field 第一個重要的性質.

Theorem 10.4.1. 假設 F 是一個 *finite field* 且 $\mathrm{char}(F) = p$, 則 F 中存在一個 *subfield* $\mathbb{F}_p$, 其中 $|\mathbb{F}_p| = p$ 且和 $\mathbb{Z}/(p)$ *isomorphic,* 而且 F 是 $\mathbb{F}_p$ 的一個 *finite extension.* 若 $[F : \mathbb{F}_p] = k$, 則 $|F| = p^k$.

Proof. 我們前面已知 F 中存在一個 subfield $\mathbb{F}_p$ 滿足 $\mathbb{F}_p \simeq \mathbb{Z}/(p)$, 而且 F 是 $\mathbb{F}_p$ 的 finite extension. 所以我們僅剩下要證: 若 $[F : \mathbb{F}_p] = k$, 則 $|F| = p^k$.

這完全是一個線性代數的問題. 由 $\dim_{\mathbb{F}_p}(F) = [F : \mathbb{F}_p] = k$ 的假設知存在 $a_1, \ldots, a_k \in F$ 是一組 F over $\mathbb{F}_p$ 的 basis. 由 basis 的定義知對任意的 $\alpha \in F$, 存在一組唯一的 $c_1, \ldots, c_k \in \mathbb{F}_p$ 使得 $\alpha = c_1 \cdot a_1 + \cdots + c_k \cdot a_k$. (這裡的存在是因為 $a_1, \ldots, a_k$ span F over $\mathbb{F}_p$, 而唯一是因為 $a_1, \ldots, a_k$ 是 linearly independent over $\mathbb{F}_p$.) 注意這裡的 $a_1, \ldots, a_k$ 是固定的一組 basis, 而 $c_1, \ldots, c_k \in \mathbb{F}_p$ 會隨著 $\alpha \in F$ 的改變而改變. 換言之 F 中的任一個元素都由唯一的一組 $c_1, \cdots, c_k$ 所決定. 但由於這些 c_i 皆在 $\mathbb{F}_p$ 中而 $|\mathbb{F}_p| = p$, 因此對每個 $i \in \{1, \ldots, k\}$, c_i 都有 p 個選擇, 故知這些 $c_1, \ldots, c_k$ 共有 p^k 個選擇. 也就是說 F 中共有 p^k 個元素. □

Theorem 10.4.1 簡單來說就是告訴我們每一個 finite field 其元素的個數應該是 p^k 個這種形式. 所以不可能有 finite field 有 6 個元素; 不過 Theorem 10.4.1 也沒有告訴我們到底有沒有 finite field 有 9 個元素或 16 個元素等等. 馬上我們就要回答這個問題, 不過在此之前我們先談談 finite field 的乘法結構.

假設 F 是一個 finite field, 因為 F 是 field, 由 Corollary 9.1.2 知 $F^* = F \setminus \{0\}$ 在乘法之下是一個 abelian group. 又因為 F 只有有限個元素, 所以我們知道 F^* 是一個 finite abelian group. 既然 F^* 是一個 finite group, 利用 Lagrange's Theorem 我們有以下之結果.

Proposition 10.4.2. 假設 F 是一個 *finite field* 且 $|F| = p^k$. 令 $f(x) = x^{p^k} - x$, 則對任意 $a \in F$ 皆符合 $f(a) = 0$ 且 $f(x)$ *splits linear factors in* F. 事實上我們有

$$x^{p^k} - x = \prod_{a \in F} (x - a).$$

Proof. 首先我們考慮 F^* 這個 order 為 $p^k - 1$ 的 finite group. 利用 Lagrange's Theorem (Corollary 2.3.4), 我們知對任意 $a \in F^*$, 皆有 $a^{p^k - 1} = 1$ (注意 1 是 F^* 的 identity). 等式兩邊乘上 a 得 $a^{p^k} = a$, 故知 $f(a) = 0$. 另外當 $a = 0$ 時自然有 $f(a) = 0$, 所以我們得到對任意的 $a \in F$ 皆符合 $f(a) = 0$. 然而由 Theorem 10.3.3

我們知道 $f(x)$ 在 F 中最多只能有 $\deg(f(x)) = p^k$ 個根. 所以 F 中的元素剛好就是 $f(x)$ 所有的根. 因此 $f(x)$ 可以完全分解成

$$f(x) = \prod_{a \in F} (x - a),$$

也就是說 $f(x)$ splits linear factors in F. □

要注意 Lagrange's Theorem 是對一般的 finite group 都對的, 所以 Proposition 10.4.2 並沒有用到 F^* 是 abelian 的性質. 接下來我們要用到 finite abelian group 的重要性質來證明事實上 F^* 是一個 cyclic group. 回顧一下 finite abelian group 的 fundamental theorem (Theorem 3.3.11) 是說任意的 finite abelian group 都可寫成一些 cyclic groups 的 direct product. 另外要注意的是若 C_n 表示是一個 cyclic group of order n, 則 $C_n \times C_m$ 不見得會 isomorphic to C_{nm}, 除非 n 和 m 是互質的 (Proposition 3.2.2).

Theorem 10.4.3. 假設 F 是一個 *finite field,* 則 $F^* = F \setminus \{0\}$ 看成是一個乘法的 *group* 時是一個 *cyclic group.*

Proof. 由 Theorem 3.3.11 知存在 $n_1, \ldots, n_r \in \mathbb{N}$ 使得

$$F^* \simeq C_{n_1} \times \cdots \times C_{n_r},$$

其中 C_{n_i} 是一個 cyclic group of order n_i. 若我們能證明這些 n_i 都是兩兩互質的, 則重複運用 Proposition 3.2.2 可得

$$C_{n_1} \times \cdots \times C_{n_r} \simeq C_{n_1 \cdots n_r},$$

換言之 F^* 是 cyclic group.

我們利用反證法, 為了方便就假設 n_1 和 n_2 不互質好了 (其他的狀況都是用相同的證明). 這表示存在一質數 q 是 n_1 和 n_2 的公因數. 因為 $q \mid n_1$ 且 q 是質數, Cauchy's 定理 (Theorem 3.3.2 或 Theorem 4.2.1) 告訴我們存在 $a \in C_{n_1}$ 滿足 $\mathrm{ord}(a) = q$. 也就是說 $a, a^2, \ldots, a^{q-1}, a^q = e_1$ 是 C_{n_1} 中 q 個相異的元素 (這裡我們用 e_i 來表示 C_{n_i} 的 identity). 同理我們知在 C_{n_2} 中存在 $b \in C_{n_2}$ 滿足 $\mathrm{ord}(b) = q$. 現考慮

$$\alpha = (a, e_2, \ldots, e_r), \beta = (e_1, b, \ldots, e_r) \in C_{n_1} \times C_{n_2} \times \cdots \times C_{n_r}.$$

當 $i, j \in \{1, \ldots, q\}$ 且 $i \neq j$ 時, 我們知

$$\alpha^i = (a^i, e_2, \ldots, e_r) \quad \text{and} \quad \alpha^j = (a^j, e_2, \ldots, e_r),$$

故由於 $a^i \neq a^j$, 我們知 $\alpha^i \neq \alpha^j$. 同理 $\beta^i \neq \beta^j$. 另外對任意的 $i, j \in \{1, \ldots, q-1\}$, 由於 $a^i \neq e_1$ 且 $b^j \neq e_2$, 我們也知

$$\alpha^i = (a^i, e_2, \ldots, e_r) \neq (e_1, b^j, \ldots, e_r) = \beta^j.$$

換句話說

$$\alpha, \alpha^2, \ldots, \alpha^{q-1}, \beta, \beta^2, \ldots, \beta^{q-1}$$

以及

$$\alpha^q = \beta^q = (e_1, e_2, \ldots, e_r)$$

是 $C_{n_1} \times \cdots \times C_{n_r}$ 中相異的 $2q-1$ 個元素. 由於 $a^q = e_1$ 且 $b^q = e_2$, 這 $2q-1$ 個元素 α^i 以及 β^j 都符合

$$(\alpha^i)^q = (\beta^j)^q = (e_1, e_2, \ldots, e_r). \tag{10.2}$$

別忘了 $(e_1, \ldots, e_r)$ 是 $C_{n_1} \times \cdots \times C_{n_r}$ 中的 identity, 所以 $C_{n_1} \times \cdots \times C_{n_r}$ 和 F^* 間的 isomorphism 會將 $(e_1, \ldots, e_r)$ 送到 F^* 的 identity 1. 而且這個 isomorphism (因為是一對一) 也會將 α^i 和 β^j 這 $2q-1$ 個相異的元素送到 F^* 中 $2q-1$ 個相異的元素. 由式子 (10.2) 我們知這 $2q-1$ 個 F^* 中的元素都符合 $x^q - 1 = 0$. 但是 Theorem 10.3.3 告訴我們 $x^q - 1$ 在 F 中至多只能有 q 個根, 因此得到矛盾. 也就是說 $F^* \simeq C_{n_1} \times \cdots \times C_{n_r}$ 中的 $n_1, \ldots, n_r$ 都兩兩互質, 故得證 F^* 是一個 cyclic group. □

F^* 是 cyclic 表示存在 $a \in F^*$ 使得所有 F^* 中的元素都是 a^i 這種形式, 所以我們有以下這個重要的性質.

Corollary 10.4.4. 假設 F 是一個 *finite field* 且 $|F| = p^k$, 則存在 $a \in F$ 滿足 $\mathbb{F}_p(a) = F$ 且 a *over* $\mathbb{F}_p$ 的 *degree* 為 k.

Proof. 令 $a \in F^* \subseteq F$ 產生 F^* 這一個 cyclic group. 回顧一下 $\mathbb{F}_p(a)$ 是 F 中包含 a 和 $\mathbb{F}_p$ 最小的 filed, 因此我們自然有 $\mathbb{F}_p(a) \subseteq F$. 另一方面任取 $b \in F$, 如果 $b = 0$, 則自然 $b \in \mathbb{F}_p(a)$; 如果 $b \neq 0$, 表示 $b \in F^*$, 故存在 $i \in \mathbb{N}$ 使得 $b = a^i$. 由於 $\mathbb{F}_p(a)$ 是一個 field, 故此時 $b = a^i \in \mathbb{F}_p(a)$. 因此證得 $F \subseteq \mathbb{F}_p(a)$, 故知 $F = \mathbb{F}_p(a)$.

由於已知 $|F| = p^k$, 故利用 Theorem 10.4.1 知 $[\mathbb{F}_p(a) : \mathbb{F}_p] = [F : \mathbb{F}_p] = k$. 因此由 Corollary 10.1.7 知 a over $\mathbb{F}_p$ 的 minimal polynomial 的 degree 為 k, 故由定義知 a over $\mathbb{F}_p$ 的 degree 為 k. □

接下來我們要證 finite field 的存在性, 即給定任一質數 p 以及 $k \in \mathbb{N}$, 我們要找到一個 finite field F 其元素個數剛好是 p^k. 首先注意當 $k = 1$ 時 $\mathbb{Z}/(p)$ 就是一個元素個數為 p 的 finite filed, 為了方便我們將此 filed 記為 $\mathbb{F}_p$. Theorem 10.4.1 告訴我們一個元素個數為 p^k 的 finite filed F 若存在, 則 F 一定會是 $\mathbb{F}_p$ 的一個 extension. 另外 Proposition 10.4.2 告訴我們在此情形 $x^{p^k} - x$ 在 F 中必定 splits into linear factors. 因此要尋找 F 必須從這兩個觀點出發.

Theorem 10.4.5. 給定任一質數 p 以及 $k \in \mathbb{N}$, 一定存在一個 *finite field* F 滿足 $|F| = p^k$.

Proof. 考慮 $x^{p^k} - x \in \mathbb{F}_p[x]$, Theorem 10.3.6 告訴我們存在一個 filed L 是 $\mathbb{F}_p$ 的一個 finite extension 使得 $x^{p^k} - x$ 在 L 中 splits into linear factors. 現在考慮

$$F = \{a \in L \mid a^{p^k} = a\},$$

也就是說 F 是 L 中 $x^{p^k}-x$ 所有的根所成的集合.

我們首先證明 F 是一個 filed. 利用 Lemma 9.1.4, 我們只要檢查對任意 $a,b\in F$ 且 $b\neq 0$ 皆有 $a-b\in F$ 以及 $a/b\in F$ 即可. $a-b$ 以及 a/b 當然都是 L 的元素, 再加上由 Lemma 9.2.5 我們有

$$(a-b)^{p^k}=a^{p^k}-b^{p^k}\quad\text{and}\quad(a/b)^{p^k}=a^{p^k}/b^{p^k},$$

故因 $a,b\in F$ (即 $a^{p^k}=a$ 且 $b^{p^k}=b$) 得知 $(a-b)^{p^k}=a-b$ 以及 $(a/b)^{p^k}=a/b$. 也就是說 $a-b$ 以及 a/b 都是 F 的元素.

接下來要證明 $|F|=p^k$. 要注意由假設 $x^{p^k}-x$ splits into linear factors in L, 我們只能知 F 的元素個數至多有 p^k 個, 除非能證得 $x^{p^k}-x$ 沒有重根. 要證明 $x^{p^k}-x$ 沒有重根, 我們先任取 $a\in L$ 是 $x^{p^k}-x$ 的一個根, 由 Lemma 10.3.1 知存在 $h(x)\in L[x]$ 使得 $x^{p^k}-x=(x-a)\cdot h(x)$. 若得 $h(a)\neq 0$, 則知 a 不是重根. 然而利用 Lemma 9.2.6, 我們知道 $(x-a)^{p^k}-(x-a)=x^{p^k}-a^{p^k}-x+a$. 由於 $a^{p^k}=a$ (因假設 a 是 $x^{p^k}-x$ 的一個根), 故得

$$x^{p^k}-x=(x-a)^{p^k}-(x-a)=(x-a)\cdot h(x),$$

其中 $h(x)=(x-a)^{p^k-1}-1$. 因為 $h(a)=-1\neq 0$, 故知任意 $x^{p^k}-x$ 的根都不是重根. 因此得證 F 是一個有 p^k 個元素的 finite field. □

利用 finite field 的存在性以及Corollary 10.4.4, 我們馬上有以下的應用.

Corollary 10.4.6. 假設 $\mathbb{F}_p$ 是一個有 p 個元素的 *finite field,* 則對任意 $k\in\mathbb{N}$, 皆存在 $g(x)\in\mathbb{F}_p[x]$ 在 $\mathbb{F}_p[x]$ 中是 *irreducible* 且 $\deg(g(x))=k$.

Proof. 利用 Theorem 10.4.5 知存在一個 finite field F 滿足 $[F:\mathbb{F}_p]=k$. 故由 Corollary 10.4.4 知存在 $a\in F$ 使得 $F=\mathbb{F}_p(a)$, 且由於 $[\mathbb{F}_p(a):\mathbb{F}_p]=k$ 知 a over $\mathbb{F}_p$ 的 minimal polynomial 的 degree 為 k. 由於 minimal polynomial 一定是 irreducible (Lemma 10.1.1), 故得證本定理. □

接下來我們來看在 $\mathbb{F}_p[x]$ 中的 irreducible element 的特性.

Lemma 10.4.7. 假設 $\mathbb{F}_p$ 是一個有 p 個元素的 *finite field* 且 $g(x)\in\mathbb{F}_p[x]$ 在 $\mathbb{F}_p[x]$ 中是 *irreducible.* 若 $\deg(g(x))=k$, 則在 $\mathbb{F}_p[x]$ 中 $g(x)\mid x^{p^k}-x$.

Proof. 由於 $\deg(g(x))=k$, 利用 Theorem 10.3.4 知存在一個 $\mathbb{F}_p$ 的 extension L 滿足 $[L:\mathbb{F}_p]=k$ 且 $a\in L$ 滿足 $g(a)=0$. 換言之, L 是一個 finite field 且 $|L|=p^k$. 然而 Proposition 10.4.2 告訴我們 L 中的元素都會是 $f(x)=x^{p^k}-x$ 的根, 因此由 $a\in L$ 知 $f(a)=0$. 要注意事實上 $g(x)$ 會和 a over $\mathbb{F}_p$ 的 minimal polynomial $h(x)$ associates. 這是因為 $g(a)=0$ 故利用 Lemma 10.1.1 (1) 知 $h(x)\mid g(x)$, 但 $g(x)$ 又假設是 irreducible, 故得 $h(x)$ 和 $g(x)$ associates (注意 $h(x)$ 不可能是 unit). 又由於 $f(a)=0$, 再利用一次 Lemma 10.1.1 (1) 知 $h(x)\mid f(x)$ (即 $f(x)\in\big(h(x)\big)$). 故由 $g(x)$ 和 $h(x)$ associates 知 $\big(g(x)\big)=\big(h(x)\big)$, 因此得證 $f(x)\in\big(g(x)\big)$ 即 $g(x)\mid f(x)$. □

最後我們來看有關 finite field 的唯一性. 我們將證明若 K 和 L 都是 finite field 且 $|K| = |L|$ 則 $K \simeq L$. 首先要強調的是這裡的 isomorphic 指的是 ring 的 isomorphism. 大家或許還記得在線性代數中兩個 vector space 若 dimension 相同, 則它們之間是 isomorphic. 不過這裡的 isomorphic 是指 vector space 間的 isomorphism, 要求的函數是 linear transformation, 僅保持加法的結構. 另外 K^* 和 L^* 是元素個數相同的 cyclic group, 從 Theorem 3.1.1 知 K^* 和 L^* 也是 isomorphic. 不過這裡的 isomorphic 指的是 group 的 isomorphism, 僅保持乘法的結構. 這兩種 isomorphic 都不能保證 K 和 L 間存在著 ring isomorphism. 我們的證明不是真的找到 K 的 L 的 ring isomorphism. 而是想找到一個 field F 滿足 $K \simeq F$ 且 $F \simeq L$, 則利用 isomorphism 的 transitivity 性質得證 $K \simeq L$.

Theorem 10.4.8. 假設 K 和 L 都是 *finite field* 且 $|K| = |L|$, 則 K 和 L 之間存在一個 *ring isomorphism.* 也就是說 $K \simeq L$ *as rings.*

Proof. 首先觀察當 $|K| = |L| = p$ 時, 由 Theorem 10.4.1 知 K 存在一個 subfield 和 $\mathbb{Z}/\big(p\big)$ isomorphic. 不過由於 $|K| = \big|\mathbb{Z}/\big(p\big)\big| = p$, 故得知 $K \simeq \mathbb{Z}/\big(p\big)$. 同理得 $L \simeq \mathbb{Z}/\big(p\big)$, 故知 $K \simeq L$.

現在看一般 $|K| = |L| = p^k$ 的情形. 由於所有元素個數為 p 的 finite field 皆 isomorphic, 所以我們可以假設 K 和 L 都是 $\mathbb{F}_p$ 的 extension, 其中 $\mathbb{F}_p$ 就是元素個數為 p 的 finite field. 由於 $|K| = p^k$, 利用 Corollary 10.4.4 知存在 $a \in K$ 使得 $\mathbb{F}_p(a) = K$ 且 a over $\mathbb{F}_p$ 的 minimal polynomial $g(x)$ 的 degree 是 k. 因此由 Corollary 10.1.7 得

$$K = \mathbb{F}_p(a) \simeq \mathbb{F}_p[x]/\big(g(x)\big).$$

或許同學們會想對 L 如法泡製得到 $L \simeq \mathbb{F}_p[x]/\big(g(x)\big)$. 事實上這是不行的, 因為雖然 Corollary 10.4.4 告訴我們存在 $a' \in L$ 使得 $L = \mathbb{F}_p(a')$, 不過 a' over $\mathbb{F}_p$ 的 minimal polynomial 不見得就是 $g(x)$. 要克服這個困難我們得利用 Lemma 10.4.7. 首先, 由於 $|L| = p^k$, Proposition 10.4.2 告訴我們 $x^{p^k} - x$ splits into linear factors in L. 不過由於 $g(x)$ 在 $\mathbb{F}_p[x]$ 中是 irreducible (Lemma 10.1.1), 因此由 Lemma 10.4.7 得知 $g(x) \mid x^{p^k} - x$. 所以 $g(x)$ 也 splits into linear factors in L. 換言之在 L 中存在 $b \in L$ 滿足 $g(b) = 0$. 當然了 $g(x)$ 是 b over $\mathbb{F}_p$ 的 minimal polynomial. 原因是 b over $\mathbb{F}_p$ 的 minimal polynomial 一定是 $g(x)$ 的 divisor (Lemma 10.1.1) 但 $g(x)$ 是 irreducible 且兩者皆為 monic polynomial, 故得證 $g(x)$ 是 b over $\mathbb{F}_p$ 的 minimal polynomial. 因此由 Corollary 10.1.7 知

$$\mathbb{F}_p[x]/\big(g(x)\big) \simeq \mathbb{F}_p(b).$$

不過由於 $\mathbb{F}_p(b) \subseteq L$ 且 $[L : \mathbb{F}_p] = [\mathbb{F}_p(b) : \mathbb{F}_p] = k$, 我們得證 $L = \mathbb{F}_p(b)$. 故知

$$L \simeq \mathbb{F}_p[x]/\big(g(x)\big) \simeq K.$$

□

關於大學基礎代數中 field 的性質, 我們就介紹至此. 我們並沒有觸及所謂的 Galois Theory, 不過已有足夠的預備知識. 若同學們對本講義中的 field 理論很清楚了, 應該可以更進一步的去了解 Galois Theory.