簡介 Galois 理論

李華介

國立台灣師範大學數學系

Chapter 3

Normal Extension 和 Separable Extension

當$L = K(\alpha)$ 是一個 finite simple extension over K 時, 我們知道若 $\mathrm{Gal}(L/K)$ 的 order 要和 L/K 的 degree 相等, 則 α over K 的 minimal polynomial $f(x)$ 必須符合兩個要求: (1) $f(x)$ 所有的根全部在 L 中; (2) $f(x)$ 沒有重根. 符合 (1) 的 extension 就是所謂的 normal extension, 而符合 (2) 的 extension 就是所謂的 separable extension. 這一章中我們將探討這兩種 extensions 的基本性質.

3.1. Splitting Field

若多項式 $f(x) \in K[x]$, 在 L 中可以完全分解成一次式的乘積, 即 $f(x)$ 的根全部落在 L 中, 則我們稱 $f(x)$ 在 L 中 splits. 當然若 $L \subseteq L'$ 則 $f(x)$ 也在 L' 中 splits, 所以為了符合「經濟效益」我們只考慮讓 $f(x)$ splits 最小的 field, 稱之為 $f(x)$ 的 splitting field.

Definition 3.1.1. 假設 L/K 是一個 field extension, $f(x) \in K[x]$. 如果 $f(x)$ 在 $L[x]$ 中可完全分解成一次式的乘積, 即:

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

其中 $c, \alpha_1, \ldots, \alpha_n \in L$, 則稱 $f(x)$ *splits* over L.

如果 $f(x)$ splits over L 且對任意 L/K 的 proper intermediate field F (即 $F \subsetneq L$), $f(x)$ 都不 splits over F, 則稱 L 是 $f(x)$ over K 的 *splitting field*.

從以上定義我們可以看出若 L 是 $f(x)$ over K 的 splitting field 且 $\alpha_1, \ldots, \alpha_n \in L$ 是 $f(x)$ 所有的根, 則因為 $K(\alpha_1, \ldots, \alpha_n)$ 是包含 K 和 $\alpha_1, \ldots, \alpha_n$ 最小的 field, 我們得 $L = K(\alpha_1, \ldots, \alpha_n)$. 要注意雖然是同一個多項式 $f(x)$, 不過若 over 不同的 field 可能會有不同的 splitting field. 當然了若 $K \subseteq F \subseteq L$, 則 $L = K(\alpha_1, \ldots, \alpha_n) = F(\alpha_1, \ldots, \alpha_n)$, 所以此時 L 仍為 $f(x)$ over F 的 splitting field. 不過若 $K \subseteq F$ 但 $F \nsubseteq L$, 則 $F(\alpha_1, \ldots, \alpha_n)$ 是 $f(x) \in F[x]$ over F 的 splitting field, 但明顯的 $L = K(\alpha_1, \ldots, \alpha_n) \neq F(\alpha_1, \ldots, \alpha_n)$. 事實

上這時候 $K(\alpha_1,\ldots,\alpha_n)$ 甚至不 isomorphic to $F(\alpha_1,\ldots,\alpha_n)$. 所以一般來說要談 splitting field 必須說明是 over 哪一個 field 的 splitting field.

其實即使 over 同樣的 field K, $f(x)$ 的 splitting field 並不唯一. 這是由於找 $f(x)$ 的根的方法並不唯一. 也就是說當初我們在某一個 field L 中將 $f(x)$ 的所有的根 $\alpha_1,\ldots,\alpha_n$ 找出時, 有可能在另一個 field L' 找到另一組根 $\beta_1,\ldots,\beta_n$. 如果 L 和 L' 都包含於某個更大的 field M, 那麼我們可得 $\{\alpha_1,\ldots,\alpha_n\}=\{\beta_1,\ldots,\beta_n\}$ (否則會得到在 M 中 $f(x)$ 根的的個數大於 $\deg(f(x))$ 的矛盾). 因此知 $K(\alpha_1,\ldots,\alpha_n)=K(\beta_1,\ldots,\beta_n)$. 不過在一般的情形就不見得這麼幸運了. 假設 $f(x)$ 是 irreducible over K, 若找到 α 是 $f(x)$ 的一個根, 現若在另一個 field 找到 β 也是 $f(x)$ 的一個根, 我們僅知 $F_1=K(\alpha)$ 和 $F_2=K(\beta)$ 是 isomorphic. 若要得到 $f(x)$ over K 的 splitting field, 必須找到 $f(x)$ 其他的根. 由於 $\alpha\in F_1$ 是 $f(x)$ 的根, 知存在 $h(x)\in F_1[x]$ 使得 $f(x)=(x-\alpha)h(x)$, 同理知存在 $l(x)\in F_2[x]$ 使得 $f(x)=(x-\beta)l(x)$. 現在問題發生了 $h(x)$ 和 $l(x)$ 不只是不同的多項式, 它們的係數所在的 fields, F_1 和 F_2 也可能不同, 這樣一直找根下去所得的根差別也可能越來越大, 那麼這樣得到的 splitting field 會不會也差別很大呢? 要回答這個問題, 我們必須先了解這裡的 $h(x)$ 和 $l(x)$ 之間的關係. 首先我們要提醒的是在剛才 $f(x)$ 的分解中, 絕不能直接將 $f(x)$ 分解成 $(x-\alpha)(x-\beta)$ 乘上另一個多項式的形式. 這是因為 α 和 β 可能無法落在同一個 field 之中, 它們之間就不能運算, 在這時候 $(x-\alpha)(x-\beta)$ 是沒有意義的. 不管怎樣 F_1 和 F_2 之間是 K-isomorphic 的, 亦即存在 $\phi:F_1\to F_2$, 是 K-isomorphism, 且滿足 $\phi(\alpha)=\beta$. 現若 $h(x)=a_{n-1}x^{n-1}+a_{n-2}x^{n-2}+\cdots+a_1x+a_0$, 其中 $a_i\in F_1$, 即

$$f(x)=(x-\alpha)(a_{n-1}x^{n-1}+a_{n-2}x^{n-2}+\cdots+a_1x+a_0). \tag{3.1}$$

由於 ϕ 將 K 中元素固定, 若將 ϕ 作用在 $f(x)$ 的所有係數, 則所得的多項式仍為 $f(x)$. 另一方面將 ϕ 作用在等式 (3.1) 右邊的多項式的係數, 所得的多項式為

$$(x-\phi(\alpha))(\phi(a_{n-1})x^{n-1}+\phi(a_{n-2})x^{n-2}+\cdots+\phi(a_1)x+\phi(a_0)).$$

由於 $\phi(\alpha)=\beta$, 因此我們得

$$f(x)=(x-\beta)(\phi(a_{n-1})x^{n-1}+\phi(a_{n-2})x^{n-2}+\cdots+\phi(a_1)x+\phi(a_0)).$$

又因為 ϕ 是 F_1 到 F_2 的函數, 可知 $\phi(a_{n-1})x^{n-1}+\phi(a_{n-2})x^{n-2}+\cdots+\phi(a_1)x+\phi(a_0)\in F_2[x]$. 因此利用 $F_2[x]$ 的分解唯一性質知 $l(x)=\phi(a_{n-1})x^{n-1}+\phi(a_{n-2})x^{n-2}+\cdots+\phi(a_1)x+\phi(a_0)$. 所以我們很自然的有以下的定義.

Definition 3.1.2. 假設 $\phi:F_1\to F_2$, 是 ring isomorphism, 對任意

$$f(x)=a_nx^n+\cdots+a_1x+a_0\in F_1[x],$$

我們令

$$f^\phi(x)=\phi(a_n)x^n+\cdots+\phi(a_1)x+\phi(a_0)\in F_2[x].$$

簡單來說 $f^\phi(x)$ 就是將 $f(x)$ 這個多項式的係數用 ϕ 作用後所得的多項式. 由於 $f(x)$ 的係數落在 F_1, 所以 $f^\phi(x)$ 的係數會落在 F_2. 我們很自然的得到一個從 $F_1[x]$ 到 $F_2[x]$ 的函數.

Lemma 3.1.3. *假設 F_1 和 F_2 是 isomorphic fields, $\phi : F_1 \to F_2$ 是一 isomorphism. 定義 $\Phi : F_1[x] \to F_2[x]$, 使得對任意 $f(x) \in F_1[x]$ 皆有 $\Phi(f(x)) = f^{\phi}(x)$, 則 Φ 是一個 ring isomorphism.*

Proof. 首先檢驗 Φ 是一個 ring isomorphism. 若 $f(x), g(x) \in F_1[x]$, 依定義, 很容易驗證 $f^{\phi}(x) + g^{\phi}(x) = (f+g)^{\phi}(x)$, 所以知 $\Phi(f(x)+g(x)) = \Phi(f(x)) + \Phi(g(x))$. 至於乘法, 我們可以用 induction 來證明. 首先若 $f(x) = a_0 \in L_1$, $g(x) = b_m x^m + \cdots + b_1 x + b_0 \in L_1[x]$, 則 $f(x) \cdot g(x) = a_0 b_m x^m + \cdots + a_0 b_1 x + a_0 b_0$. 故知

$$\begin{aligned} \Phi(f(x) \cdot g(x)) &= \phi(a_0 b_m) x^m + \cdots + \phi(a_0 b_1) x + \phi(a_0 b_0) \\ &= \phi(a_0)\phi(b_m) x^m + \cdots + \phi(a_0)\phi(b_1) x + \phi(a_0)\phi(b_0). \end{aligned}$$

另一方面 $\Phi(f(x)) \cdot \Phi(g(x)) = \phi(a_0) \cdot (\phi(b_m) x^m + \cdots + \phi(b_1) x + \phi(b_0))$, 故知當 $\deg(f(x)) = 0$ 時 $\Phi(f(x)) \cdot \Phi(g(x)) = \Phi(f(x) \cdot g(x))$. 現假設當 $\deg(f(x)) < n$ 時對任意 $g(x) = b_m x^m + \cdots + b_1 x + b_0 \in L_1[x]$ 皆有 $\Phi(f(x)) \cdot \Phi(g(x)) = \Phi(f(x) \cdot g(x))$. 現若 $f(x) = a_n x^n + \cdots + a_1 x + a_0$, 可將 $f(x)$ 寫成 $f(x) = a_n x^n + f_1(x)$, 其中 $\deg(f_1(x)) < n$. 因此

$$f(x) \cdot g(x) = a_n b_m x^{n+m} + \cdots + a_n b_1 x^{n+1} + a_n b_0 x^n + f_1(x) \cdot g(x).$$

因此利用 Φ 保持加法的性質以及 induction 的假設知

$$\begin{aligned} &\Phi(f(x) \cdot g(x)) \\ &= \Phi(a_n b_m x^{n+m} + \cdots + a_n b_1 x^{n+1} + a_n b_0 x^n) + \Phi(f_1(x) \cdot g(x)) \\ &= \phi(a_n)\phi(b_m) x^{n+m} + \cdots + \phi(a_n)\phi(b_1) x^{n+1} + \phi(a_n)\phi(b_0) x^n + \Phi(f_1(x) \cdot g(x)) \\ &= \Phi(a_n x^n) \cdot \Phi(g(x)) + \Phi(f_1(x)) \cdot \Phi(g(x)) \\ &= \Phi(a_n x^n + f_1(x)) \cdot \Phi(g(x)) = \Phi(f(x)) \cdot \Phi(g(x)). \end{aligned}$$

故由 induction 得知 $\Phi(f(x)) \cdot \Phi(g(x)) = \Phi(f(x) \cdot g(x))$.

由於 $\phi : F_1 \to F_2$ 是 isomorphism, 我們知 ϕ 的 inverse, $\phi^{-1} : F_2 \to F_1$ 存在且為 ring isomorphism. 現考慮 $\Psi : F_2[x] \to F_1[x]$, 定義為對任意 $g(x) = b_m x^m + \cdots + b_1 x + b_0 \in F_2[x]$, 皆有 $\Psi(g(x)) = \phi^{-1}(b_m) x^m + \cdots + \phi^{-1}(b_1) x + \phi^{-1}(b_0)$. 很容易驗證對任意 $f(x) \in F_1[x]$, $g(x) \in F_2[x]$ 皆有 $\Psi(\Phi(f(x))) = f(x)$ 且 $\Phi(\Psi(g(x))) = g(x)$, 故知 Φ 是 1-1 and onto, 得證 Φ 是一個 ring isomorphism. □

在一般 ring 的理論中我們知若 R_1 和 R_2 是 rings, $\Phi : R_1 \to R_2$ 是 ring homomorphism 且 I 是 R_1 的 ideal, 則 R_1/I 和 $R_2/\Phi(I)$ 看成 rings 仍為 isomorphic. 所以我們有以下之結果.

Corollary 3.1.4. *假設 F_1 和 F_2 是 isomorphic fields, $\phi : F_1 \to F_2$ 是一 isomorphism 且 $p(x) \in F_1[x]$. 則存在一 ring isomorphism $\tau : F_1[x]/(p(x)) \to F_2[x]/(p^{\phi}(x))$ 滿足 $\tau(\overline{x}) = \overline{x}$ 且對任意 $\lambda \in F_1$, $\tau(\overline{\lambda}) = \overline{\phi(\lambda)}$.*

Proof. 由 Lemma 3.1.3 我們知 $\Phi : F_1[x] \to F_2[x]$ 是一個 ring isomorphism. 現考慮 $\pi : F_2[x] \to F_2[x]/(p^\phi(x))$ 使得對任意 $g(x) \in F_2[x]$, 皆有 $\pi(g(x)) = \overline{g(x)}$ (modulo $(p^\phi(x))$). 我們知 π 是 onto 的 ring homomorphism, 故 $\pi\circ\Phi : F_1[x] \to F_2[x]/(p^\phi(x))$ 是一個 onto 的 ring homomorphism. 現若 $f(x) \in \ker(\pi\circ\Phi)$, 即 $\Phi(f(x)) = f^\phi(x) \in (p^\phi(x))$, 則存在 $h(x) \in F_2[x]$ 使得 $f^\phi(x) = p^\phi(x) \cdot h(x)$. 兩邊多項式的係數用 ϕ^{-1} 作用可得 $f(x) = p(x) \cdot h^{\phi^{-1}}(x)$. 由於 $h^{\phi^{-1}}(x) \in F_1[x]$, 故知 $f(x) \in (p(x))$, 得證 $\ker(\pi \circ \Phi) = (p(x))$. 因此利用 ring 的 first isomorphism 定理知 $\pi \circ \Phi$ induces 一個 ring isomorphism $\tau : F_1[x]/(p(x)) \to F_2[x]/(p^\phi(x))$, 其中對任意 $f(x) \in F_1[x]$, $\tau(\overline{f(x)}) = \pi \circ \Phi(f(x))$. 又因為依定義 $\pi \circ \Phi(x) = \pi(x) = \overline{x}$ 且對任意 $\lambda \in F_1$, $\pi \circ \Phi(\lambda) = \pi(\phi(\lambda)) = \overline{\phi(\lambda)}$, 故得 $\tau(\overline{x}) = \overline{x}$ 且對任意 $\lambda \in F_1$, $\tau(\overline{\lambda}) = \overline{\phi(\lambda)}$. □

這裡要特別強調: 既然 $\Phi : F_1[x] \to F_2[x]$ 是 ring isomorphism, 我們知若 $p(x) \in F_1[x]$ 是 irreducible polynomial, 則 $\Phi(p(x)) = p^\phi(x)$ 在 $F_2[x]$ 中亦為 irreducible polynomial. 因此我們有以下之性質.

Corollary 3.1.5. *假設 F_1 和 F_2 是 isomorphic fields, $\phi : F_1 \to F_2$ 是一 isomorphism 且 $p(x) \in F_1[x]$ 是 $F_1[x]$ 中的 irreducible polynomial. 若 α 是 $p(x)$ 的一個根, 而 β 是 $p^\phi(x)$ 的一個根, 則存在一 isomorphism $\rho : F_1(\alpha) \to F_2(\beta)$ 滿足 $\rho(\alpha) = \beta$ 且對任意 $\lambda \in F_1$, $\rho(\lambda) = \phi(\lambda)$.*

Proof. 由於 $p(x)$ 是 $F_1[x]$ 中的 irreducible polynomials, 我們知存在 ring isomorphism $\eta : F_1(\alpha) \to F_1[x]/(p(x))$ 滿足 $\eta(\alpha) = \overline{x}$ 以及對任意 $\lambda \in F_1$, $\eta(\lambda) = \overline{\lambda}$. 又由於 $p^\phi(x)$ 是 $F_2[x]$ 中的 irreducible polynomials, 我們知存在 ring isomorphism $\theta : F_2(\beta) \to F_2[x]/(p^\phi(x))$ 滿足 $\theta(\beta) = \overline{x}$ 以及對任意 $\zeta \in F_2$, $\theta(\zeta) = \overline{\zeta}$. 故利用 Corollary 3.1.4, 考慮 $\rho = \theta^{-1} \circ \tau \circ \eta : F_1(\alpha) \to F_2(\beta)$. 則 ρ 是一個 ring isomorphism, 且

$$\rho(\alpha) = \theta^{-1} \circ \tau \circ \eta(\alpha) = \theta^{-1}(\tau(\overline{x})) = \theta^{-1}(\overline{x}) = \beta$$

以及對任意 $\lambda \in F_1$,

$$\rho(\lambda) = \theta^{-1} \circ \tau \circ \eta(\lambda) = \theta^{-1}(\tau(\overline{\lambda})) = \theta^{-1}(\overline{\phi(\lambda)}) = \phi(\lambda).$$

□

在 Corollary 3.1.5 中, 由於 ρ 若定義域限制在 F_1 則和 ϕ 為同一函數 (即 $\rho|_{F_1} = \phi$). 通常我們就稱 $\phi : F_1 \to F_2$ 是*extendible* to $\rho : F_1(\alpha) \to F_2(\beta)$.

現在我們在回到當初要探討有關 splitting field 的唯一性. Corollary 3.1.5 大致上是說: 若找好相對應的根, 這樣一直 extend 上去的 fields 都會 isomorphic. 下一個定理就是要說明這件事. 這個定理是有關 splitting field 最重要的觀念, 以後我們要探討有關 splitting field 的理論都要用上這個定理. 為了強調它的重要性, 在這裡我們特別稱之為 splitting field 的 fundamental theorem (一般書並未如此稱呼).

Theorem 3.1.6 (The Fundamental Theorem for Splitting Fields)**.** *假設 F_1 和 F_2 是 isomorphic fields, $\phi : F_1 \to F_2$ 是一 isomorphism 且 $f(x) \in F_1[x]$. 若 L 是 $f(x)$ over F_1*

的 splitting field, 且 L'/F_2 是一個 field extension 使得 $f^\phi(x)$ splits over L', 則存在一個一對一的 ring homomorphism (即 monomorphism) $\sigma : L \to L'$ 滿足 $\sigma|_{F_1} = \phi$.

Proof. 利用 Corollary 3.1.5 我們當然可以每次都用 simple extension 將 ϕ extends 到 $L \to L'$ 的 monomorphism. 不過這樣的 argument 總是不容易說清楚, 最好的方法還是用 induction. 由於 L 是 $f(x)$ over F_1 的 splitting field, 所以 L/F_1 是 finite extension. 我們就針對 $[L : F_1] = n$ 作 induction.

假設 $[L : F_1] = 1$, 此時表示 $L = F_1$, 所以令 $\sigma = \phi$ 即可. 若 $[L : F_1] = n > 1$, 則由於此時 $L \neq F_1$, 必存在 $f(x)$ 的一個根 α 滿足 $\alpha \notin F_1$. 現若 $p(x) \in F_1[x]$ 是 α over F_1 的 minimal polynomial, 由 minimal polynomial 的性質知 $p(x) \mid f(x)$ in $F_1[x]$ (參見大學基礎代數講義Lemma 10.1.1). 故將 ϕ 作用在多項式的係數得 $p^\phi(x) \mid f^\phi(x)$ in $F_2[x]$. 現因 $f^\phi(x)$ splits over L', 故可找到 $\beta \in L'$ 為 $p^\phi(x)$ 的一個根. 現利用 Corollary 3.1.5 知存在 $\rho : F_1(\alpha) \to F_2(\beta)$ 是 isomorphism 且滿足 $\rho|_{F_1} = \phi$. 現在我們檢查一下 induction 的假設條件. 首先我們有一 field isomorphism $\rho : F_1(\alpha) \to F_2(\alpha)$. 再來由於 $F_1 \subseteq F_1(\alpha) \subseteq L$, 故知 L 仍為 $f(x)$ over $F_1(\alpha)$ 的 splitting field. 再加上 ϕ extends to ρ 且 $f(x) \in F_1[x]$, 我們有 $f^\rho(x) = f^\phi(x) \in F_2[x] \subseteq F_2(\beta)[x]$ 且 $L'/F_2(\beta)$ 為 field extension 滿足 $f^\rho(x)$ splits over L'. 最後因 $[F_1(\alpha) : F_1] > 1$, 故得 $[L : F_1(\alpha)] = [L : F_1]/[F_1(\alpha) : F_1] < n$. 所以可套用 induction 的假設知存在一 monomorphism $\sigma : L \to L'$ 滿足 $\sigma|_{F_1(\alpha)} = \rho$. 但由於 $F_1 \subseteq F_1(\alpha)$, 知

$$\sigma|_{F_1} = (\sigma|_{F_1(\alpha)})|_{F_1} = \rho|_{F_1} = \phi.$$

故得證本定理. □

這個定理主要是講如何可以把一個 isomorphism 的定義域 extends 到大一點的 field. 千萬要注意, 這個定理必需要求 L 是 $f(x)$ over F_1 的 splitting field. 不能僅假設 $f(x)$ splits over F_1 (因為若僅假設 $f(x)$ splits over F_1, 符合這樣的條件的 L 可能太大以致於無法將 ϕ extends to L). 另外要注意的是, 並不需要求 $f(x) \in F_1[x]$ 是 irreducible. 還有僅需要求 $f^\phi(x)$ splits over L', 而不需要求 L' 是 $f^\phi(x)$ over F_2 的 splitting field. 不過若 L' 剛好是 $f^\phi(x)$ over F_2 的 splitting field, 那麼 σ 就會是一個 isomorphism.

Corollary 3.1.7. *假設 F_1 和 F_2 是 isomorphic fields, $\phi : F_1 \to F_2$ 是一 isomorphism 且 $f(x) \in F_1[x]$. 若 L_1 和 L_2 分別是 $f(x)$ over F_1 和 $f^\phi(x)$ over F_2 的 splitting fields, 則存在一個 isomorphism $\sigma : L_1 \to L_2$ 滿足 $\sigma|_{F_1} = \phi$.*

Proof. 因 L_2 是 $f^\phi(x)$ over F_2 的 splitting field, 所以 $f^\phi(x)$ splits over L_2, 故套用 Theorem 3.1.6 得 $\sigma : L_1 \to L_2$ 是一個 monomorphism 且滿足 $\sigma|_{F_1} = \phi$. 令 $\mathrm{im}(\sigma)$ 為 σ 的 image, 則得 $[L_1 : F_1] = [\mathrm{im}(\sigma) : F_2] \leq [L_2 : F_2]$. 另一方面將 Theorem 3.1.6 套用於 $\phi^{-1} : F_2 \to F_1$, 可得 $[L_2 : F_2] \leq [L_1 : F_1]$. 故得 $[L_1 : F_1] = [\mathrm{im}(\sigma) : F_2] = [L_2 : F_2]$, 也就是說 $\mathrm{im}(\sigma) = L_2$, 得證 σ 是一個 isomorphism. □

特別當 $F_1 = F_2 = K$ 且 ϕ 是 K 的 identity map (即對任意 $a \in K$ 皆有 $\phi(a) = a$). 則對任意 $f(x) \in K[x]$, 由於 $f^\phi(x) = f(x)$ 故套用 Corollary 3.1.7 知: 若 L_1 和 L_2 都是

$f(x)$ over K 的 splitting field, 則存在一個 isomorphism $\sigma : L_1 \to L_2$ 滿足對任意 $a \in K$ 皆有 $\sigma(a) = \phi(a) = a$. 也就是說 $\sigma : L_1 \to L_2$ 是一個 K-isomorphism, 亦即 L_1 和 L_2 是 isomorphic over K. 我們將這個結果寫下.

Proposition 3.1.8. *假設 K 是一個 field 且 $f(x) \in K[x]$. 則所有 $f(x)$ over K 的 splitting fields 皆 isomorphic over K.*

一般來說, 若 $\sigma : L_1 \to L_2$ 是一個 K-isomorphism, 則 σ 會將 L_1/K 中任意的 intermediate field F 送到 L_2/K 的 intermediate field, $\sigma(F)$. 反之 $\sigma^{-1} : F_2 \to F_1$ 會將 L_2/K 的 intermediate field 送到 L_1/K 的 intermediate field. 另一方面若 $\tau \in \mathrm{Gal}(L_1/K)$, 則很容易驗證 $\sigma \circ \tau \circ \sigma^{-1} \in \mathrm{Gal}(L_2/K)$. 因此我們可利用 σ 定出一個 $\mathrm{Gal}(L_1/K)$ 到 $\mathrm{Gal}(L_2/K)$ 的 group isomorphism. 總而言之, 當 L_1 和 L_2 是 isomorphic over K 時, L_1/K 和 L_2/K 的 intermediate fields 之間有一個一對一的對應關係, 而且它們的 Galois groups, $\mathrm{Gal}(L_1/K)$ 和 $\mathrm{Gal}(L_2/K)$ 是 isomorphic. 因此當我們要探討 $f(x) \in K[x]$ over K 的 splitting field 其 Galois group 和 intermediate fields 的關係時, Proposition 3.1.8 告訴我們其實不必擔心是否會因所選的 splitting filed 不同而造成不同的結論.

3.2. Normal Extension

在這一節中我們要介紹 normal extension. 我們會了解 normal extension 和 splitting field 的關係, 進而幫助我們探討其 Galois group.

在 Proposition 2.1.3 中我們知道若 $L = K(\alpha)$ 是一個 finite simple extension, 要達到 $|\mathrm{Gal}(L/K)| = [L : K]$ 就必須要求 α 的 over K minimal polynomial 的所有的根都落在 L 中. 所以我們有以下之定義:

Definition 3.2.1. 假設 L/K 是一個 finite extension. 若所有在 L 中的元素其 over K 的 minimal polynomial 皆 splits over L, 則稱 L/K 是一個 *normal extension*.

要注意, 一般的書中大都定義: L/K 是 normal extension, 表示若 $p(x)$ 是 $K[x]$ 中的 irreducible polynomial 且 $p(x)$ 在 L 中有根, 則 $p(x)$ 在 L 中可完全分解. 其實這樣的定義和我們這裡的定義是一樣的. 因為不難看出 $K[x]$ 中的 irreducible polynomial $p(x)$ 若在 L 中有一根 a, 則 a over K 的 minimal polynomial 和 $p(x)$ 祇差個常數倍而已 (因為 minimal polynomial 需要求是 monic polynomial), 因此只要有一個可完全分解, 另一個也可完全分解. 我們不用這種定義是因為常常有同學忘了 irreducible 的條件誤以為 L/K 是 normal extension 表示若 $f(x) \in K[x]$ 在 L 有根, 則 $f(x)$ splits over L. 也有的同學忘了要先在 L 中有根的先決條件, 而誤以為 L/K 是 normal extension 表示所有 $K[x]$ 的 irreducible polynomial 皆 splits over K. 而我們的定義就不會有這種困擾.

要檢查一個 field extension L/K 是否為 normal extension, 依定義需要檢查所有 L 的元素, 不過以下的結果告訴我們只要檢查有限多個就可以了.

Theorem 3.2.2. *假設 L/K 是一個 field extension. 下列敘述是等價的.*

(1) L/K 是一個 *finite normal extension.*

(2) $L = K(a_1, \ldots, a_n)$ 其中這些 a_i *over* K 的 *minimal polynomial* 皆 *splits over* L.

(3) 存在 $f(x) \in K[x]$ 使得 L 是 $f(x)$ *over* K 的 *splitting field.*

Proof. (1) $\Rightarrow$ (2): 利用 Proposition 1.3.4, 由 L/K 是 finite extension 的假設知存在 $a_1, \ldots, a_n \in L$ 且 a_i 皆 algebraic over K 使得 $L = K(a_1, \ldots, a_n)$. 假設 $p_i(x) \in K[x]$ 是 a_i over K 的 minimal polynomial, 由 L/K 是 normal extension 的假設知 $p_i(x)$ splits over L.

(2) $\Rightarrow$ (3): 假設 $L = K(a_1, \ldots, a_n)$ 其中這些 a_i over K 的 minimal polynomial $p_i(x)$ 皆 splits over L. 現令 $f(x) = p_1(x) \cdots p_n(x)$, 我們知 $f(x)$ splits over L. 我們要說明 L 事實上是 $f(x)$ over K 的 splitting field. 假設 $K \subseteq F \subseteq L$, 且 F 是 $f(x)$ over K 的 splitting field. 由於對所有 $i \in \{1, \ldots, n\}$, a_i 皆為 $f(x)$ 的根, 故有 $a_i \in F$. 因此 $L = K(a_1, \ldots, a_n) \subseteq F$, 故得 $L = F$.

(3) $\Rightarrow$ (1): 若 $f(x) \in K[x]$ 且 L 是 $f(x)$ over K 的 splitting field, 則我們可以直接假設 $L = K(a_1, \ldots, a_n)$, 其中 $a_1, \ldots, a_n \in L$ 是 $f(x)$ 所有的根. 由 Proposition 1.3.4, 知 L/K 是 finite extension. 接著我們要證 L/K 是 normal extension. 若 $\alpha \in L$ 且其 over K 的 minimal polynomial 為 $p(x)$, 我們要證明 $p(x)$ 所有的根皆在 L 中. 任取 β 為 $p(x)$ 的另一個根. 由於 $p(x)$ 是 $K[x]$ 中的 irreducible polynomial 且 α, β 為其根, 我們知存在一個 K-isomorphism $\phi : K(\alpha) \to K(\beta)$. 由於 $f(x) \in K[x]$, 故有 $f(x) \in K(\alpha)[x]$. 再加上 ϕ 固定 K 中元素, 我們得 $f^{\phi}(x) = f(x)$. 現在將 $f(x)$ 考慮成 $K(\alpha)[x]$ 中的多項式, 我們知 $K(\alpha)(a_1, \ldots, a_m)$ 是 $f(x)$ over $K(\alpha)$ 的 splitting field. 另一方面將 $f^{\phi}(x) = f(x)$ 考慮成 $K(\beta)[x]$ 中的多項式, 我們知 $K(\beta)(a_1, \ldots, a_m)$ 是 $f^{\phi}(x)$ over $K(\beta)$ 的 splitting field. 由於 $K(\alpha)(a_1, \ldots, a_m) = K(a_1, \ldots, a_m)(\alpha) = L(\alpha)$ 以及 $\alpha \in L$, 可知 $K(\alpha)(a_1, \ldots, a_m) = L$. 另一方面我們有 $K(\beta)(a_1, \ldots, a_m) = K(a_1, \ldots, a_m)(\beta) = L(\beta)$. 重新整理後的結果是: 我們有一個 isomorphism, $\phi : K(\alpha) \to K(\beta)$ 以及一個 polynomial $f(x) \in K(\alpha)[x]$, 另外 L 和 $L(\beta)$ 分別是 $f(x)$ 和 $f^{\phi}(x)$ over $K(\alpha)$ 和 $K(\beta)$ 的 splitting fields. 所以直接套用 Corollary 3.1.7 知存在一個 isomorphism $\sigma : L \to L(\beta)$ 滿足 $\sigma|_{K(\alpha)} = \phi$. 由於 ϕ 將 K 的元素固定, 所以 σ 也將 K 的元素固定. 也就是說 σ 是 K-isomorphism, 亦即 L 和 $L(\beta)$ 是 isomorphic over K. 利用 Lemma 1.2.2 知 $[L : K] = [L(\beta) : K]$, 故由 $[L(\beta) : K] = [L(\beta) : L][L : K]$ 得 $[L(\beta) : L] = 1$. 也就是說 $L(\beta) = L$, 亦即 $\beta \in L$. 我們證得所有 $p(x)$ 的根必都在 L 中, 也就是說 $p(x)$ splits over L, 故由定義知 L/K 是一個 normal extension. □

談 extension 最常關心的是: 假設 L/K 是一個 filed extension 且 F 是 L/K 的 intermediate field. 那麼 L/K 的某些性質是否 L/F 或 F/K 會保持. 例如若 L/K 是 algebraic extension, 那麼 L/F 和 F/K 也是 algebraic extension. 另外在 Lemma 1.2.3 中我們也知 finite extension 的性質也會保持. 那麼 normal extension 的性質呢? 我們有以下的答案.

Corollary 3.2.3. *假設* L/K *是一個 finite extension 且* F *是* L/K *的 intermediate field. 若* L/K *是一個 normal extension, 則* L/F *也是一個 normal extension.*

Proof. 由 Theorem 3.2.2 ((1) ⇒ (3)) 我們知存在 $f(x) \in K[x]$ 使得 L 是 $f(x)$ over K 的 splitting field. 又因為 $K \subseteq F \subseteq L$, 將 $f(x)$ 看成是 over F 的 polynomial, 知 L 仍為 $f(x)$ over F 的 splitting field. 故再利用 Theorem 3.2.2 ((3) ⇒ (1)) 我們得 L/F 仍為一個 normal extension. □

要注意由 Corollary 3.2.3 的條件我們並不保證 F/K 是 normal extension. 另一方面 Corollary 3.2.3 反過來也未必正確, 也就是說若已知 L/F 是 normal extension, 也無法保證 L/K 是 normal extension. 甚至即使已知 L/F 和 F/K 是 normal extension, 也無法保證 L/K 是 normal extension. 以下就是一些例子.

Example 3.2.4. (1) 我們考慮 $x^3 - 2$ over $\mathbb{Q}$ 的 splitting field. 令 $\omega = (-1 + \sqrt{3}\,i)/2$ 為 1 的 3 次方根. 則 $x^3 - 2$ 在 $\mathbb{C}$ 上的 3 個根分別為 $\sqrt[3]{2}$, $\sqrt[3]{2}\,\omega$ 以及 $\sqrt[3]{2}\,\omega^2$. 因此 $L = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\,\omega, \sqrt[3]{2}\,\omega^2) = \mathbb{Q}(\sqrt[3]{2}, \omega)$ 為 $x^3 - 2$ over $\mathbb{Q}$ 的 splitting field. 當然得 $L/\mathbb{Q}$ 是 normal extension. 若令 $F = \mathbb{Q}(\sqrt[3]{2})$, 由於 $L = F(\omega)$ 仍是 $x^3 - 2$ over F 的 splitting field, 所以 L/F 也是 normal extension. 然而 $\sqrt[3]{2} \in F$ over $\mathbb{Q}$ 的 minimal polynomial 為 $x^3 - 2$, 但是 $x^3 - 2$ 在 F 中並未完全分解, 故知 $F/\mathbb{Q}$ 並不是 normal extension.

(2) 若令 $F = \mathbb{Q}(\sqrt{2})$, 則 F 是 $x^2 - 2$ over $\mathbb{Q}$ 的 splitting field, 所以 $F/\mathbb{Q}$ 是 normal extension. 若又令 $L = F(\sqrt[4]{2})$, 則 L 是 $x^2 - \sqrt{2}$ over $F = \mathbb{Q}(\sqrt{2})$ 的 splitting field, 所以 L/F 是 normal extension. 雖然 L/F 和 $F/\mathbb{Q}$ 都是 normal extensions, 不過 $L/\mathbb{Q}$ 並不是 normal extension. 這是因為 $\sqrt[4]{2} \in L$ 且 $x^4 - 2$ 是 $\sqrt[4]{2}$ over $\mathbb{Q}$ 的 minimal polynomial, 但是 $L = \mathbb{Q}(\sqrt[4]{2})$ 的元素皆為實數, 明顯的 $x^4 - 2$ 其他的虛根 $\pm\sqrt[4]{2}\,i$ 並不在 L 中. 也就是說 $x^4 - 2$ 並不 splits over L, 所以 $L/\mathbb{Q}$ 不是 normal extension.

當 L/K 是一個 finite extension 時 $\mathrm{Gal}(L/K)$ 只探討 L 到 L 的 K-isomorphisms. 其實為了考慮更一般的狀況我們也關心 L 到更大的 fields 的情況. 當然了從一個 field 到另一個 field 的 ring homomorphism, 除了是 0 mapping 的狀況外其他皆為 1-1 (參見大學基礎代數講義Proposition 9.1.5), 所以我們只要考慮 1-1 的 homomorphism.

Definition 3.2.5. 假設 L, M, 和 K 皆為 fields 其中 $K \subseteq L$ 且 $K \subseteq M$. 若 $\phi : L \to M$ 是 1-1 ring homomorphism 且對所有 $k \in K$ 皆有 $\phi(k) = k$, 則稱 ϕ 是一個 L 到 M 的 *K-monomorphism.* 為了方便起見, 我們將所有從 L 到 M 的 K-monomorphisms 所成的集合用 $\mathfrak{M}_K(L, M)$ 來表示.

我們要說明一下, 在這裡我們談論的 L 到 M 的 K-monomorphism, 都會只考慮 $L \subseteq M$ 的情況. 主要原因是我們希望 K-monomorphism 的像 (image) 和 L 仍有關係. 這裡有關係指的是元素之間仍可互相運算. 要達到這目的當然就需要 K-monomorphism 的像和 L 都落在某一個更大的 field 中. 由於擴大一個函數的對應域並沒有改變原來的函數, 所以為了方便起見就直接假設對應域包含 L.

當 L/K 是 finite normal extension 時, 下一個定理告訴我們一個從 L 到一個比 L 大的 field 的 K-monomorphism 它的 image 一定在 L 中. 也就是說在這情況下只考慮 $\mathrm{Gal}(L/K)$ 就足夠了.

Lemma 3.2.6. *假設 L/K 是一個 finite normal extension, 且 M 是一個 field 滿足 $L \subseteq M$. 若 $\phi : L \to M$ 是一個 K-monomorphism, 則 ϕ 是 L 的 K-automorphism. 亦即 $\mathfrak{M}_K(L, M) = \mathrm{Gal}(L/K)$.*

Proof. 首先我們證明對任意 $\alpha \in L$ 皆有 $\phi(\alpha) \in L$. 假設 $\alpha \in L$ 且 $p(x) \in K[x]$ 是其 over K 的 minimal polynomial. 由於 L/K 是 normal extension 知 $p(x)$ 在 L 中完全分解. 假設 $p(x) = (x-\alpha)(x-\alpha_2)\cdots(x-\alpha_n)$, 其中 $\alpha_i \in L$, 由於 $L \subseteq M$, 這也是 $p(x)$ 在 $M[x]$ 中的分解. 另一方面 ϕ 是 K-monomorphism, 故 $\phi(\alpha)$ 必為 $p(x)$ 在 M 中的一個根. 也就是說 $x - \phi(\alpha)$ 在 $M[x]$ 中必整除 $p(x)$. 由於 $M[x]$ 是一個 unique factorization domain (利用 M 是一個 field 以及大學基礎代數講義Theorem 7.2.14), 我們知 $\phi(\alpha) \in \{\alpha, \alpha_2, \ldots, \alpha_n\}$. 因此得證 $\phi(\alpha) \in L$. 故知 ϕ 是 L 的 K-automorphism.

前面是證得若 $\phi \in \mathfrak{M}_K(L, M)$, 則 $\phi \in \mathrm{Gal}(L/K)$, 也就是說 $\mathfrak{M}_K(L, M) \subseteq \mathrm{Gal}(L/K)$. 但由於 $L \subseteq M$, 若 $\sigma \in \mathrm{Gal}(L/K)$ 表示 σ 是 L 到 L 的 K-monomorphism 當然也就是 L 到 M 的 K-monomorphism. 因此有 $\mathrm{Gal}(L/K) \subseteq \mathfrak{M}_K(L, M)$, 故得 $\mathfrak{M}_K(L, M) = \mathrm{Gal}(L/K)$. □

既然一個 finite normal extension 是一個 polynomial 的 splitting field, 我們可以利用 The Fundamental Theorem for Splitting Field (Theorem 3.1.6) 得到以下有關 normal extension 重要的結果.

Theorem 3.2.7. *假設 L/K 是一個 finite normal extension, F 是 L/K 的一個 intermediate field 且 M 是一個 field 滿足 $L \subseteq M$. 若 $\tau : F \to M$ 是一個 K-monomorphism, 則存在 $\sigma \in \mathrm{Gal}(L/K)$ 滿足 $\sigma|_F = \tau$.*

Proof. 因 L/K 是一個 finite normal extension, 故存在 $f(x) \in K[x]$ 使得 L 是 $f(x)$ over K 的 splitting field. 因 $K \subseteq F \subseteq L$, 故若考慮 $f(x) \in F[x]$, 則 L 仍為 $f(x)$ over F 的 splitting field. 又因為 τ 將 K 的元素固定, 所以 $f^\tau(x) = f(x)$ 且 $f^\tau(x)$ splits over M (因 $L \subseteq M$). 因此將 $\tau : F \to \tau(F)$ 這一個 isomorphism 套用到 Theorem 3.1.6, 我們知存在 $\sigma : L \to M$ 是一個 monomorphism 使得 $\sigma|_F = \tau$. 又因為 τ 固定 K 的元素, 所以 σ 是一個 K-monomorphism, 因此由 Lemma 3.2.6 知 $\sigma \in \mathrm{Gal}(L/K)$. 得證本定理. □

當 L/K 不是 normal extension 時, 有可能一個 K-monomorphism 會將 L 的元素送到 L 以外的元素. 不過我們仍能控制其 image 的範圍. 首先介紹以下之定義.

Definition 3.2.8. 假設 L/K 是一個 field extension 且 N 是一個 field 滿足:

(1) $L \subseteq N$ 且 N/K 是一個 normal extension.

(2) 若 M 是一個 intermediate field of N/L 且 M/K 是一個 normal extension, 則 $M = N$.

則稱 N 是 L/K 的一個 *normal closure*.

簡單來說 N 是 L/K 的 normal closure 表示 N 是包含 L 的 field 中使得 N/K 是 normal extension 的最小的 field. 當然了, 如果 L/K 已是 normal extension, 那麼 L 本身自然是 L/K 的 normal closure.

我們自然會問 normal closure 的存在性及唯一性.

Proposition 3.2.9. *若 L/K 是一個 finite extension, 則 L/K 的 normal closure 必存在, 而且也是一個 finite extension over K. 若 N 和 N' 皆為 L/K 的 normal closure, 則 N 和 N' 是 isomorphic over K.*

Proof. 因 L/K 是 finite extension 由 Proposition 1.3.4 知存在 $a_1, \ldots, a_n \in L$ 且 a_i 皆 algebraic over K 使得 $L = K(a_1, \ldots, a_n)$. 令 $p_i(x) \in K[x]$ 為 a_i over K 的 minimal polynomial 且令 $f(x) = p_1(x) \cdots p_n(x)$. 若令 N 為 $f(x)$ over L 的 splitting field, 則 N/K 是 finite normal extension. 現在只需驗證 N/K 是包含 L 最小的 normal extension. 若 $L \subseteq M \subseteq N$ 且 M/K 是 normal extension. 由於 $a_i \in M$, 故由 M/K 是 normal extension 得 $p_i(x)$ splits over M, 也因此 $f(x)$ splits over M. 但由於 N 已是 $f(x)$ over K 的 splitting field 且 $M \subseteq N$, 故得 $M = N$.

前面已證明若 N 是 $f(x)$ over K 的 splitting field, 則 N 是 L/K 的 normal closure. 事實上反過來也是對的, 也就是說: 若 N 是 L/K 的 normal closure, 則 N 是 $f(x)$ over K 的 splitting field. 這是因為若 N 是 L/K 的 normal closure, 由於 $a_i \in L \subseteq N$ 且 N/K 是 normal extension 得 $p_i(x)$ splits over N, 因此 $f(x)$ splits over N, 所以若 $L \subseteq M \subseteq N$, 且 M 是 $f(x)$ over K 的 splitting field, 則由 Theorem 3.2.2 知 M/K 是一個 normal extension, 故由 N 是 L/K 的 normal closure 之假設得 $N = M$.

現假設 N 和 N' 都是 L/K 的 normal closure. 由於 N 和 N' 都是 $f(x)$ over K 的 splitting field, 故利用 Proposition 3.1.8 知 N 和 N' 是 isomorphic over K. □

再次強調 L/K 的 normal closure 並不唯一. 當然了如果 N 和 N' 都是 L/K 的 normal closure 且都包含於同一個 field, 那麼和 splitting field 的情形一樣, 可得 $N = N'$ (否則會有一個多項式在一個 field 中其根的個數大於其次數的矛盾發生).

接下來我們回到探討 K-monomorphism 的 image. 假設 L/K 是一個 finite extension, $\phi : L \to M$ 是一個 K-monomorphism, 其中 $L \subseteq M$. 由於 M 只是 ϕ 的對應域, 我們可以將 M 儘量擴大以方便討論 (這樣並沒有改變原來 ϕ 的 image). 由於假設 $L \subseteq M$, 不失一般性我們可以將 M 擴大到是 M/K 的一個 normal closure M', 擴大後的 M' 因為仍包含 L 且 M'/K 是 normal extension, 由 normal closure 的定義知 M' 會包含 L/K 的某個 normal closure (因為 L/K 的 normal closure 是包含 L 最小的 normal extension). 因此不失一般性我們可假設 ϕ 的對應域包含某個 L/K 的 normal closure.

Proposition 3.2.10. *假設 L/K 是一個 finite extension 且 $\phi : L \to M$ 是一個 K-monomorphism. 如果 M 包含 L/K 的某個 normal closure N, 則 ϕ 的 image 包含於 N, 亦即 $\phi : L \to N$.*

Proof. 由於 $L \subseteq N \subseteq M$, 且 N/K 是一個 finite normal extension. 將 L 視為是 N/K 的一個 intermediate field, 套用 Theorem 3.2.7, 知存在 $\sigma \in \mathrm{Gal}(N/K)$ 滿足 $\sigma|_L = \phi$. 由於 σ 是 N 到 N 的函數, 所以 $\phi = \sigma|_L$ 是一個 L 到 N 的函數. 故得證本定理. □

前面提到過不會有兩個不同的 L/K 的 normal closures 同時包含於一個 field. 因此在 Proposition 3.2.10 中的 N 會是唯一包含於 M 的 L/K 的 normal closure. 因此我們有以下之結果.

Corollary 3.2.11. *假設 L/K 是一個 finite extension 且 M 是一個包含 L 的 field. 如果 M 包含 L/K 的某個 normal closure N, 則 $\mathfrak{M}_K(L, M) = \mathfrak{M}_K(L, N)$.*

Proof. 若 $\psi \in \mathfrak{M}_K(L, N)$, 表示 ψ 是一個 L 到 N 的 K-monomorphism, 由於 $N \subseteq M$, 故得 ψ 也是一個 L 到 M 的 K-monomorphism, 也就是說 $\psi \in \mathfrak{M}_K(L, M)$. 另一方面若 $\phi \in \mathfrak{M}_K(L, M)$, 則 Proposition 3.2.10 告訴我們 $\phi \in \mathfrak{M}_K(L, N)$. 故得 $\mathfrak{M}_K(L, M) = \mathfrak{M}_K(L, N)$. □

Corollary 3.2.11 告訴我們當擴大對應域 M 到包含 L/K 的某個 normal closure 後, 所有 L 到 M 的 K-monomorphisms 所成的集合 $\mathfrak{M}_K(L, M)$ 就不會再增加了. 因此我們只要考慮適當大的對應域就可以涵蓋所有情況了. 當然了最經濟的取法就是選定對應域是 L/K 的 normal closure. 不過由於以後我們要討論的 K-monomorphism 的定義域會在 L/K 的 intermediate fields 之間換來換去, 為了不必因為定義域的不同將對應域換來換去, 我們會將對應域固定為 N, 其中 $L \subseteq N$ 且 N/K 是 finite normal extension. 這樣一來不但有其方便性而且由 Corollary 3.2.11 知並沒有改變這些 K-monomorphisms 所成的集合.

從 Proposition 2.3.3 我們知道當 L/K 是 finite extension 時, 所有 L 到 L 的 K-monomorphisms (即 $\mathrm{Gal}(L/K)$) 的個數小於或等於 $[L : K]$. 現若 M 是一個包含 L 的 field, 那麼所有 L 到 M 的 K-monomorphism 的個數和 $[L : K]$ 會有什麼關係呢? 很明顯的由於對應域較大, L 到 M 的 K-monomorphisms 的個數有可能多於 L 到 L 的 K-monomorphisms 的個數, 所以我們無法直接知道其個數是否仍會小於或等於 $[L : K]$.

當初要探討 $\mathrm{Gal}(L/K)$ 和 $[L : K]$ 的關係時我們曾提過可以用 induction 來處理. 不過那時因為是討論 L 到 L 的 automorphism, 用歸納法比較不容易討論. 現在我們把對應域擴大了討論起來就方便多了, 我們主要是需要以下之 Lemma.

Lemma 3.2.12. *假設 L/K 是一個 finite extension, F 是一個 L/K 的 intermediate field 且 N 是一個 L 的 extension 滿足 N/K 是 finite normal extension. 則 $\mathfrak{M}_K(L, N)$, $\mathfrak{M}_F(L, N)$ 和 $\mathfrak{M}_K(F, N)$ 都是 finite sets 且*

$$|\mathfrak{M}_K(L, N)| = |\mathfrak{M}_F(L, N)|\,|\mathfrak{M}_K(F, N)|\,.$$

Proof. 首先注意我們有 $K \subseteq F \subseteq L \subseteq N$ 這樣的關係. 由於 N/K 是一個 finite normal extension 且 L 是 N/K 的一個 intermediate field, 利用 Theorem 3.2.7 知每一個 L 到 N 的 K-monomorphism (即 $\mathfrak{M}_K(L, N)$ 的元素) 都可 extends 成為 $\mathrm{Gal}(N/K)$ 的元素, 因此得 $|\mathfrak{M}_K(L, N)| \leq |\mathrm{Gal}(N/K)| \leq [N : K]$. 故知 $\mathfrak{M}_K(L, N)$ 是一個 finite set. 同理可得

$\mathfrak{M}_K(F,N)$ 也是 finite set. 另外由於 $K \subseteq F$ 所以一個 L 到 N 的 F-monomorphism 也是一個 L 到 N 的 K-monomorphism, 故知 $\mathfrak{M}_F(L,N)$ 是 $\mathfrak{M}_K(L,N)$ 的 subset, 因此 $\mathfrak{M}_F(L,N)$ 也是一個 finite set.

假設 $\mathfrak{M}_F(L,N) = \{\rho_1, \ldots, \rho_s\}$ 而 $\mathfrak{M}_K(F,N) = \{\psi_1, \ldots, \psi_t\}$, 亦即 $\rho_i : L \to N$ 是 F-monomorphism 且 $\psi_j : F \to N$ 是 K-monomorphism. 由於 N/K 是一個 finite normal extension 且 F 是 N/K 的一個 intermediate field, 利用 Theorem 3.2.7 每一個 K-monomorphism $\psi_j : F \to N$ 都可以 extends 成一個 K-monomorphism $\phi_j : N \to N$ (即 $\phi_j|_F = \psi_j$). 考慮 $\phi_j \circ \rho_i : L \to N$, 我們要驗證它是一個 K-monomorphism. 事實上由於 $K \subseteq F$ 且 ρ_i 是 F-monomorphism, 所以 ρ_i 當然也是 K-monomorphism, 再加上 ϕ_j 是 K-monomorphism, 因此對任意的 $k \in K$ 皆有 $\phi_j \circ \rho_i(k) = \phi_j(\rho_i(k)) = \phi_j(k) = k$. 故知對任意 $i \in \{1, \ldots, s\}$ 以及 $j \in \{1, \ldots, t\}$, $\phi_j \circ \rho_i$ 都是 L 到 N 的 K-monomorphism.

接著我們要說明對任意 K-monomorphism $\sigma : L \to N$, 皆可以找到 $i \in \{1, \ldots, s\}$ 以及 $j \in \{1, \ldots, t\}$ 使得 $\sigma = \phi_j \circ \rho_i$. 由於 $\sigma|_F : F \to N$ 是一個 K-monomorphism, 故利用 $\mathfrak{M}_K(F,N)$ 是所有 F 到 N 的 K-monomorphism 所成的集合知存在 $j \in \{1, \ldots, t\}$ 使得 $\psi_j = \sigma|_F$. 現考慮 $\phi_j^{-1} \circ \sigma : L \to N$, 由於對任意 $\lambda \in F$, 皆有 $\sigma(\lambda) = \psi_j(\lambda) = \phi_j(\lambda)$ (別忘了 $\phi_j|_F = \psi_j$). 故知 $\phi_j^{-1} \circ \sigma(\lambda) = \lambda$, 因此 $\phi_j^{-1} \circ \sigma$ 是一個 L 到 N 的 F-monomorphism. 故利用 $\mathfrak{M}_F(L,N)$ 是所有 L 到 N 的 F-monomorphism 所成的集合知存在 $i \in \{1, \ldots, s\}$ 使得 $\rho_i = \phi_j^{-1} \circ \sigma$. 換言之 $\sigma = \phi_j \circ \rho_i$.

我們已證得 $\mathfrak{M}_K(L,N) = \{\phi_j \circ \rho_i \,|\, i = 1, \ldots, s \text{ 且 } j = 1, \ldots, t\}$. 要說明 $|\mathfrak{M}_K(L,N)| = st = |\mathfrak{M}_F(L,N)|\,|\mathfrak{M}_K(F,N)|$, 我們還需驗證這些 $\phi_j \circ \rho_i$ 皆相異. 也就是說還要驗證: 若 $i, i' \in \{1, \ldots, s\}$, $j, j' \in \{1, \ldots, t\}$ 且 $\phi_j \circ \rho_i = \phi_{j'} \circ \rho_{i'}$, 則 $i = i'$ 且 $j = j'$. 對任意 $\lambda \in F$, 由於 $\rho_i, \rho_{i'}$ 是 F-monomorphisms, 我們得

$$\phi_j \circ \rho_i(\lambda) = \phi_j(\lambda) \quad \text{and} \quad \phi_{j'} \circ \rho_{i'}(\lambda) = \phi_{j'}(\lambda).$$

故由 $\phi_j \circ \rho_i = \phi_{j'} \circ \rho_{i'}$ 的假設知對任意 $\lambda \in F$ 皆有 $\phi_j(\lambda) = \phi_{j'}(\lambda)$. 換言之

$$\psi_j = \phi_j|_F = \phi_{j'}|_F = \psi_{j'},$$

故得 $j = j'$, 也因此知 $\phi_j = \phi_{j'}$. 再由 $\phi_j = \phi_{j'}$ 以及 $\phi_j \circ \rho_i = \phi_{j'} \circ \rho_{i'}$ 知

$$\rho_i = \phi_j^{-1} \circ (\phi_j \circ \rho_i) = \phi_{j'}^{-1} \circ (\phi_{j'} \circ \rho_{i'}) = \rho_{i'},$$

故得證 $i = i'$. □

接下來我們可以用 induction 來處理 monomorphism 的個數和 extension degree 的關係.

Proposition 3.2.13. *假設 L/K 是一個 finite extension 且 N 是一個 L 的 extension 滿足 N/K 是 finite normal extension. 則 $|\mathfrak{M}_K(L,N)| \leq [L:K]$.*

Proof. 我們對 $[L:K]$ 作 induction 證明: 假設 $[L:K] = 1$, 即 $L = K$, 此時所有 L 到 N 的 K-monomorphism 事實上就是 L 到 L 的 identity, 所以只有一個. 假設對所有 extension degree 小於 n 的 field extension 都成立. 現考慮 $[L:K] = n > 1$ 的情形. 任取 $\alpha \in L$

但 $\alpha \notin K$. 令 $F = K(\alpha)$, 此時我們有 $[F : K] > 1$ 故知 $[L : F] < n$. 假設 $p(x) \in K[x]$ 是 α over K 的 minimal polynomial. 由於 $F = K(\alpha)$ 是一個 simple extension over K, 每一個 K-monomorphism $\psi : F \to N$ 可由 $\psi(\alpha)$ 的取值唯一確定. 不過 $\psi(\alpha) \in N$ 必為 $p(x)$ 在 N 的一個根, 故由 $p(x)$ 在 N 的根的個數小於等於 $\deg(p(x)) = [F : K]$ 知 $|\mathfrak{M}_K(F, N)| \leq [F : K]$. 另一方面由於 $K \subseteq F \subseteq L \subseteq N$ 且 N/K 是一個 normal extension, 所以利用 Corollary 3.2.3 知 N/F 仍為 finite normal extension. 因此我們現在有一個 finite extension L/F 且 N 是一個 L 的 extension 滿足 N/F 是 finite normal extension. 又因為 $[L : F] < n$ 故套用 induction 的假設知 $|\mathfrak{M}_F(L, N)| \leq [L : F]$. 因此由 Lemma 3.2.12 知

$$|\mathfrak{M}_K(L, N)| = |\mathfrak{M}_F(L, N)|\,|\mathfrak{M}_K(F, N)| \leq [L : F][F : K] = [L : K].$$

□

最後我們強調 Proposition 3.2.13 我們無法得到所有 L 到 N 的 K-monomorphisms 的個數等於 $[L : K]$ 的主要原因是我們在考慮 $F = K(\alpha)$ 到 N 的 K-monomorphism 時, 雖然 α over K 的 minimal polynomial $p(x)$ 在 N 中可以完全分解 (因 N/K 是 normal extension), 不過由於 $p(x)$ 可能有重根, 所以 $p(x)$ 在 N 中根的個數仍有可能少於 $\deg(p(x)) = [F : K]$. 因此所有 F 到 N 的 K-monomorphisms 其個數仍有可能少於 $[F : K]$, 導致無法利用 induction 證得所有 L 到 N 的 K-monomorphisms 個數等於 $[L : K]$. 底下我們就是要探討 separable extension 的概念以幫助我們處理這個情況.

3.3. Separable Polynomial

簡單來說一個 separable polynomial 是一個沒有重根的多項式. 由於要談一個多項式有沒有重根牽涉到一個多項式的分解, 所以在這一節中我們先簡單的複習一些多項式分解的相關性質, 再探討有關 separable polynomial 的性質.

假設 K 是一個 field, 則 $K[x]$ 這一個 polynomial ring 是一個 principle ideal domain (參見大學基礎代數講義Theorem 7.2.6), 因此也是一個 unique factorization domain (參見大學基礎代數講義Theorem 7.2.14). 簡單來說就是每一個 $K[x]$ 中的非常數多項式都可以寫成一些 irreducible polynomials 的乘積. 在 unique factorization domain 中任兩個元素的 gcd (greatest common divisor) 是存在的. 事實上假設 $f(x), g(x) \in K[x]$ 且 $f(x)$ 和 $g(x)$ 的質因式分解分別為

$$f(x) = cp_1(x)^{m_1} \cdots p_r(x)^{m_r} \quad \text{and} \quad g(x) = c'p_1(x)^{n_1} \cdots p_r(x)^{n_r},$$

其中 $c, c' \in K$ 且 $p_i(x)$ 是 $K[x]$ 中的 irreducible polynomial. 若令 $d_i = \min\{m_i, n_i\}$ 則 $p_1(x)^{d_1} \cdots p_r(x)^{d_r}$ 就是 $f(x)$ 和 $g(x)$ 的 gcd. 另一個大家熟悉求 gcd 的方法就是用輾轉相除法. 事實上 $K[x]$ 是一個 principle ideal domain, 輾轉相除法可以幫助我們找到 ideal 的 generator. 也就是說 $f(x)$ 和 $g(x)$ 的 gcd 就是 $(f(x), g(x))$ 這個 ideal (即由 $f(x)$ 和 $g(x)$ 產生的 ideal) 的 generator. 因此 $d(x)$ 是 $f(x)$ 和 $g(x)$ 的 gcd 若且唯若 $(d(x)) = (f(x), g(x))$. 故知存在 $m(x), n(x) \in K[x]$ 使得 $d(x) = m(x)f(x) + n(x)g(x)$. 由於兩個多項式的 gcd 並不是唯一的, 會差個常數倍 (參見大學基礎代數講義Lemma 8.1.6), 因此為了方便起見, 在

這裡我們要求取的 gcd 一定要 monic (即最高次項係數為1), 如此一來就唯一了. 我們將 $f(x)$ 和 $g(x)$ 之 gcd 用 $\gcd(f(x),g(x))$ 表示. 特別當 $\gcd(f(x),g(x))=1$ 時, 我們稱 $f(x)$ 和 $g(x)$ 是互質 (relatively prime).

假設 L/K 是一個 field extension 且 $f(x),g(x)\in K[x]$. 此時我們可以將 $f(x)$ 和 $g(x)$ 看成是 $L[x]$ 中的元素. 從多項式的分解的角度來看在 $K[x]$ 中分解和在 $L[x]$ 中分解是不一樣的. 比方說 $f(x)$ 在 $K[x]$ 中有可能是 irreducible polynomial 但在 $L[x]$ 中就不是. 因此我們會問是否 $f(x)$ 和 $g(x)$ 在 $K[x]$ 中的 gcd 和在 $L[x]$ 中的 gcd 會不一樣? 其實它們是一樣的, 理由如下: 假設 $f(x)$ 和 $g(x)$ 在 $K[x]$ 和在 $L[x]$ 的 gcd 分別為 $d_K(x)$ 和 $d_L(x)$. 由於 $K[x]\subseteq L[x]$, 所以 $d_K(x)\in L[x]$ 且在 $L[x]$ 中整除 $f(x)$ 以及 $g(x)$. 因此依 $d_L(x)$ 是 $f(x)$ 和 $g(x)$ 在 $L[x]$ 的 gcd 知 $d_K(x)$ 在 $L[x]$ 中整除 $d_L(x)$. 另一方面由於存在 $m(x),n(x)\in K[x]$ 滿足 $m(x)f(x)+n(x)g(x)=d_K(x)$, 又 $d_L(x)$ 在 $L[x]$ 中整除 $f(x)$ 以及 $g(x)$, 因此知 $d_L(x)$ 在 $L[x]$ 中整除 $d_K(x)$. 也就是說在 $L[x]$ 中 $d_L(x)\mid d_K(x)$ 且 $d_K(x)\mid d_L(x)$, 所以利用 $d_K(x)$ 和 $d_L(x)$ 都是 monic polynomials 的假設知 $d_K(x)=d_L(x)$. 因此以後我們用 $gcd(f(x),g(x))$ 這個符號時不必擔心是 $f(x)$ 和 $g(x)$ 在 $K[x]$ 中或是在 $L[x]$ 中的 gcd.

由上面討論得知, 要探討 $f(x)$ 和 $g(x)$ 在 $K[x]$ 中是否互質和在 $L[x]$ 中探討其實是一樣的. 因此當要驗證 $f(x)$ 和 $g(x)$ 是否互質時, 我們可以考慮夠大的 extension L/K, 使得 $f(x)$ 和 $g(x)$ 在 L 中可以完全分解. 這樣就很容易判斷 $f(x)$ 和 $g(x)$ 是否互質了.

Lemma 3.3.1. *假設 L/K 是一個 field extension, $f(x),g(x)\in K[x]$ 且 $f(x)$ 和 $g(x)$ split over L. 則 $\gcd(f(x),g(x))=1$ 若且唯若 $f(x)$ 和 $g(x)$ 在 L 中沒有相同的根.*

Proof. 從上面的討論中我們知到可以將 $f(x)$ 和 $g(x)$ 考慮成 $L[x]$ 中的 polynomials.

假設 $\gcd(f(x),g(x))=1$, 表示存在 $m(x),n(x)\in L[x]$ 使得 $m(x)f(x)+n(x)g(x)=1$. 若 $\alpha\in L$ 是 $f(x)$ 和 $g(x)$ 在 L 中相同的根, 則將 α 代入得 $1=m(\alpha)f(\alpha)+n(\alpha)g(\alpha)=0$. 造成矛盾故知 $f(x)$ 和 $g(x)$ 在 L 中沒有相同的根.

另一方面, 假設$f(x)$ 和 $g(x)$ 在 L 中沒有相同的根. 首先將 $f(x)$ 和 $g(x)$ 在 L 中分別完全分解成

$$f(x)=a(x-a_1)\cdots(x-a_m)\quad\text{and}\quad g(x)=b(x-b_1)\cdots(x-b_n).$$

由於一次多項式一定是 irreducible, 所以利用唯一分解性質以及 $\{a_1,\ldots,a_m\}\cap\{b_1,\ldots,b_n\}=\emptyset$ 的假設, 得知 $f(x)$ 和 $g(x)$ 是互質的. □

接下來我們要探討 separable polynomial 的性質.

Definition 3.3.2. 假設 K 是一個 field, $f(x)\in K[x]$ 且 L 是 $f(x)$ over K 的 splitting field. 如果 $f(x)$ 在 L 中無重根, 則稱 $f(x)$ 是一個 *separable polynomial*.

要注意雖然 $f(x)$ over K 的 splitting field 並不唯一, 不過由於 splitting fields 之間是 K-isomorphic (Proposition 3.1.8) 所以 $f(x)$ 是否有重根和 splitting field 的選取無關. 這是因為若 L_1 和 L_2 皆為 $f(x)$ over K 的 splitting field, 則存在一個 K-isomorphism $\phi:L_1\to L_2$.

假設 $f(x)$ 在 $L_1[x]$ 中完全分解成 $f(x)=a(x-a_1)\cdots(x-a_n)$, 則 $f(x)$ 在 $L_2[x]$ 可分解成 $f(x)=f^{\phi}(x)=\phi(a)(x-\phi(a_1))\cdots(x-\phi(a_n))$. 由於 ϕ 是 1-1, 可得 $f(x)$ 在 L_1 中無重根若且唯若在 L_2 中無重根.

要判斷一個多項式有沒有重根, 大家都知道可以用微分來處理. 也就是如果 $f(x)$ 和 $f'(x)$ 沒有相同的根, 則 $f(x)$ 不會有重根. 可惜的是當初微分的定義是用極限的概念, 在這裡我們談的是一般的 field, 元素間沒有距離的概念, 所以無法談極限. 因此我們要用純代數的方法處理. 這裡所用的處理方法其實和以後理論的推廣無關, 所以大家若能接受原本判別重根的方法在一般的 field 都對的話, 可以直接跳過這一段, 而從 Lemma 3.3.5 繼續研讀下去.

Definition 3.3.3. 假設 K 是一個 field 且 $f(x)=a_nx^n+\cdots+a_2x^2+a_1x+a_0\in K[x]$. 我們定義 $f(x)$ 的微分為 $f'(x)=na_nx^{n-1}+\cdots+2a_2x+a_1$.

要注意這裡和微積分學的不同的是, 在微積分中我們是用極限定義微分, 再依定義推得 $f'(x)$ 為何. 在這裡我們直接定義 $f'(x)$ 為何, 所以大家熟悉(用極限推得)的微分性質並不一定成立. 我們必須驗證多項式在此定義之下微分的加法原理 (addition rule) 和乘法原理 (product rule) 是否成立.

Lemma 3.3.4. *假設 K 是一個 field 且 $f(x),g(x)\in K[x]$. 則*

$$(f+g)'(x)=f'(x)+g'(x)\quad\text{and}\quad(f\cdot g)'(x)=f'(x)\cdot g(x)+f(x)\cdot g'(x).$$

Proof. 假設 $f(x)=a_nx^n+\cdots+a_1x+a_0$ 且 $g(x)=b_nx^n+\cdots+a_1x+a_0$ ($f(x)$ 和 $g(x)$ 不一定次數相同, 不過我們不妨將它們寫成同次的形式, 只要將多餘項係數以 0 表示即可). 則 $(f+g)(x)=(a_n+b_n)x^n+\cdots+(a_1+b_1)x+(a_0+b_0)$. 故依定義知

$$\begin{aligned}(f+g)'(x) &= n(a_n+b_n)x^{n-1}+\cdots+(a_1+b_1)\\ &= (na_nx^{n-1}+\cdots+a_1)+(nb_nx^{n-1}+\cdots+b_1)\\ &= f'(x)+g'(x).\end{aligned}$$

至於 product rule 我們可以用 induction 處理. 給定 $g(x)=b_mx^m+\cdots+b_1x+b_0$, 我們對 $\deg(f(x))=n$ 作 induction, 證明對任意 $f(x)\in K[x]$, $(f\cdot g)'(x)=f'(x)\cdot g(x)+f(x)\cdot g'(x)$. 若 $\deg(f(x))=0$, 此時 $f(x)=a\in K$, 故 $(f\cdot g)(x)=ab_mx^m+\cdots+ab_1x+ab_0$. 由於 $f'(x)=0$, 因此得

$$(f\cdot g)'(x)=mab_mx^{m-1}+\cdots+ab_1=a(mb_mx^{m-1}+\cdots+b_1)=f'(x)\cdot g(x)+f(x)\cdot g'(x).$$

假設當 $\deg(f(x))<n$ 時, $(f\cdot g)'(x)=f'(x)\cdot g(x)+f(x)\cdot g'(x)$. 現若 $\deg(f(x))=n$, 則將 $f(x)$ 寫成 $f(x)=a_nx^n+f_1(x)$, 其中 $\deg(f_1(x))<n$. 故有 $(f\cdot g)(x)=(a_nx^n\cdot g(x))+(f_1\cdot g)(x)$. 將 $a_nx^n\cdot g(x)$ 乘開取微分可得

$$(a_nx^n\cdot g(x))'=na_nx^{n-1}\cdot g(x)+a_nx^n\cdot g'(x).$$

又因為 $\deg(f_1(x)) < n$ 利用 induction 的假設知

$$(f_1 \cdot g)'(x) = f_1'(x) \cdot g(x) + f_1(x) \cdot g'(x).$$

因此套用前面已證得的 addition rule, 我們有

$$\begin{aligned}(f \cdot g)'(x) &= (a_n x^n \cdot g(x))' + (f_1 \cdot g)'(x) \\ &= n a_n x^{n-1} \cdot g(x) + a_n x^n \cdot g'(x) + f_1'(x) \cdot g(x) + f_1(x) \cdot g'(x) \\ &= (n a_n x^{n-1} + f_1'(x)) \cdot g(x) + (a_n x^n + f_1(x)) \cdot g'(x) \\ &= f'(x) \cdot g(x) + f(x) \cdot g'(x).\end{aligned}$$

□

既然 product rule 成立我們就可以利用 product rule 得到我們熟悉的判斷一個多項式是否有重根的方法. 這裡我們仍選用比較代數的說法.

Lemma 3.3.5. *假設 K 是一個 field 且 $f(x) \in K[x]$. 則 $f(x)$ 是一個 separable polynomial 若且唯若* $\gcd(f(x), f'(x)) = 1$.

Proof. 假設 L/K 是一個 extension 使得 $f(x)$ 和 $f'(x)$ 皆 split over L. 利用 Lemma 3.3.1 我們只要探討 $f(x)$ 和 $f'(x)$ 在 L 中有沒有相同的根.

假設 $f(x)$ 和 $f'(x)$ 在 L 中有相同的根 α (即 $\gcd(f(x), f'(x)) \neq 1$), 表示在 $L[x]$ 中 $f(x) = (x - \alpha) \cdot g(x)$ 其中 $g(x) \in L[x]$. 因此利用 product rule (Lemma 3.3.4) 得 $f'(x) = g(x) + (x - \alpha) \cdot g'(x)$. 但由於 $f'(\alpha) = 0$, 代入得 $g(\alpha) = 0$, 也就是 $x - \alpha$ 在 $L[x]$ 中也整除 $g(x)$. 故得 α 是 $f(x)$ 的一個重根. 因此 $f(x)$ 不是 separable polynomial.

反之, 如果 $f(x)$ 不是 separable polynomial, 表示存在 $\alpha \in L$ 以及 $h(x) \in L[x]$ 使得 $f(x) = (x - \alpha)^2 \cdot h(x)$. 因為 $(x - \alpha)^2 = x^2 - 2\alpha x + \alpha^2$, 再次利用 product rule 得 $f'(x) = 2(x - \alpha) \cdot h(x) + (x - \alpha)^2 \cdot h'(x)$. 因此知 α 也為 $f'(x)$ 在 L 的一個根. 因此由 Lemma 3.3.1 知 $\gcd(f(x), f'(x)) \neq 1$. □

前面提過, 以前大家熟悉的微分性質在一般的 field 並不一定是對的. 例如 $f'(x) = 0$ 若且唯若 $f(x)$ 是一個常數就不一定對. 事實上我們有以下之結果.

Lemma 3.3.6. *假設 K 是一個 field 且 $f(x) \in K[x]$.*

(1) *假設 K 是一個 characteristic 為 0 的 field. 則 $f'(x) = 0$ 若且唯若 $f(x) = c$ 是一個常數.*

(2) *假設 K 是一個 characteristic 為 p 的 field. 則 $f'(x) = 0$ 若且唯若存在一個 $g(x) \in K[x]$ 使得 $f(x) = g(x^p)$.*

Proof. 首先回顧一下一個 field K 的 characteristic 只有兩種情形: 當 characteristic 為 0 時表示, 若 $a \in K$ 且 $a \neq 0$, 則對任意正整數 n, na 皆不為 0; 而 characteristic 為 p 時表示, 對任意 $a \in K$, pa 皆為 0.

(1) 假設 K 的 characteristic 為 0 且 $f(x) = a_n x^n + \cdots + a_1 x + a_0$. 則 $f'(x) = na_n x^{n-1} + \cdots + a_1$. 如果 $f'(x) = 0$ 表示 $na_n, (n-1)a_{n-1}, \ldots, a_1$ 皆為 0. 由 K 的 characteristic 為 0 的假設知 $a_n, \ldots, a_1$ 皆為 0. 故 $f(x) = a_0$ 是一個常數. 反之, 如果 $f(x) = c$ 是一個常數, 自然由定義知 $f'(x) = 0$.

(2) 假設 K 的 characteristic 為 p 且 $f(x) = a_n x^n + \cdots + a_1 x + a_0$, 其中 $a_n \neq 0$. 則對於 $i \in \{1, \ldots, n\}$, $f'(x)$ 的每一個 x^{i-1} 項的係數為 ia_i. 因此若 $f'(x) = 0$ 且 $a_i \neq 0$, 則由 $ia_i = 0$ 知 $p \mid i$. 也就是說只有在 $i = pt$, 其中 t 為非負整數時, $f(x)$ 的 x^i 項的係數才可能不為 0. 特別因假設 $a_n \neq 0$, 所以知 $n = pm$. 因此若令 $b_t = a_{pt}$ 且 $g(x) = b_m x^m + \cdots + b_1 x + b_0$, 則

$$f(x) = \sum_{t=0}^{m} a_{pt} x^{pt} = \sum_{t=0}^{m} b_t (x^p)^t = g(x^p).$$

反之, 若 $g(x) = b_m x^m + \cdots + b_1 x + b_0 \in K[x]$ 且 $f(x) = g(x^p)$, 則 $f(x) = \sum_{t=0}^{m} b_t (x^p)^t = \sum_{t=0}^{m} b_t x^{pt}$, 故得

$$f'(x) = \sum_{t=1}^{m} (pt) b_t x^{pt-1} = \sum_{t=1}^{m} p(tb_t) x^{pt-1} = 0.$$

□

在下一節中我們要關心的是一個 irreducible polynomial 是否為 separable polynomial. 所以我們特別看一下 Lemma 3.3.5 特別在 $f(x)$ 是 irreducible 時的情形.

Proposition 3.3.7. *假設 K 是一個 field 且 $f(x) \in K[x]$ 是 $K[x]$ 中的 irreducible polynomial.*

(1) *假設 K 是一個 characteristic 為 0 的 field. 則 $f(x)$ 一定是一個 separable polynomial.*

(2) *假設 K 是一個 characteristic 為 p 的 field. 則 $f(x)$ 不是 separable polynomial 若且唯若存在一個 $g(x) \in K[x]$ 使得 $f(x) = g(x^p)$.*

Proof. 由於一個 polynomial 乘上一個非 0 的常數並不影響這裡所述的性質, 所以我們直接假設 $f(x) \in K[x]$ 是一個 monic irreducible polynomial. 若 $d(x) = \gcd(f(x), f'(x))$, 由於 $d(x)$ 是 $f(x)$ 的一個 monic 的因式, 而 $f(x)$ 是 irreducible 其 monic 的因式只有 1 和 $f(x)$ 本身, 故得 $d(x) = 1$ 或 $d(x) = f(x)$. 特別要注意, 如果 $f'(x) \neq 0$, 則由於 $\deg(f'(x)) < \deg(f(x))$, 此時 $f(x)$ 不可能整除 $f'(x)$. 因此若 $f'(x) \neq 0$, 則 $\gcd(f(x), f'(x))$ 不可能為 $f(x)$, 故得 $\gcd(f(x), f'(x)) = 1$.

(1) 假設 K 是一個 characteristic 為 0 的 field. 因為 $f(x)$ 是 irreducible, 故 $\deg(f(x)) > 1$, 因此由 Lemma 3.3.6 知 $f'(x)$ 不可能為 0. 由上面的討論知 $\gcd(f(x), f'(x)) = 1$, 因此由 Lemma 3.3.5 得知 $f(x)$ 是一個 separable polynomial.

(2) 假設 K 是一個 characteristic 為 p 的 field. 若 $f(x)$ 不是 separable polynomial, 則由 Lemma 3.3.5 知 $\gcd(f(x), f'(x)) \neq 1$. 故由前面討論得知 $f'(x) = 0$ 也就是說存在一個 $g(x) \in K[x]$ 使得 $f(x) = g(x^p)$ (Lemma 3.3.6). 反之若存在一個 $g(x) \in K[x]$ 使得

$f(x) = g(x^p)$, 則 $f'(x) = 0$. 故得 $\gcd(f(x), f'(x)) = f(x) \neq 1$. 因此再由 Lemma 3.3.5 得知 $f(x)$ 不是 separable polynomial. □

3.4. Separable Extension

在這一節中我們介紹另一個重要的 extension, separable extension. 首先我們會發現幾乎在大學代數中談的 extension 都是 separable extension, 然後我們會進一步討論 separable extension 重要的性質.

在前面我們提過當 $L = K(\alpha)$ 是 K 的 finite simple extension 時, 若 α 的 minimal polynomial 沒有重根時, 我們就可以由其 minimal polynomial degree 確實知道有關 L 的 K-monomorphisms 的個數. 所以我們有以下之定義.

Definition 3.4.1. 假設 L/K 是一個 finite extension. 若 $a \in L$ 且 a over K 的 minimal polynomial 是 separable polynomial, 則稱 a 是一個 *separable element* over K. 如果 L 中所有元素皆為 separable element over K, 則稱 L/K 是一個 *separable extension.*

要注意要談一個元素是否是一個 separable element, 仍必須說明是 over 哪一個 field. 有可能在 $K \subseteq F$ 的情形, a 是一個 separable element over F 但不是 separable over K. 不過反過來如果已知 a 是一個 separable element over K 那麼 a 一定是一個 separable element over F. 這是因為如果 $m_K(x) \in K[x]$ 和 $m_F(x) \in F[x]$ 分別為 a over K 的 minimal polynomial 和 a over F 的 minimal polynomial, 則 $m_F(x)$ 在 $F[x]$ 中必整除 $m_K(x)$. 因此如果 $m_K(x)$ 沒有重根, 當然 $m_F(x)$ 也不會有重根.

當 L/K 是一個 finite extension, 前面提過我們很關心一些 L/K 的性質是否在 intermediate fields 之間保持. 事實上 separable extension 和 algebraic extension 一樣是會被保持的.

Lemma 3.4.2. *假設 L/K 是一個 finite separable extension 且 F 是 L/K 的 intermediate field. 則 L/F 和 F/K 都是 separable extension.*

Proof. 任取 $a \in F$, 由於 $a \in L$ 且 L/K 是 separable extension, 得知 a 是一個 separable element over K. 因此由定義知 F/K 是 separable extension. 另外任取 $a \in L$, 由於 $K \subseteq F$ 且 a 是一個 separable element over K, 由前面討論知 a 也是一個 separable element over F. 因此知 L/F 也是一個 separable extension. □

事實上以後我們會知道如果 L/F 和 F/K 都是 separable extension 則 L/K 也會是一個 separable extension (再一次強調 normal extension 就沒有這麼好).

要檢查 L/K 是否為 separable extension, 依定義就得檢查 L 中所有元素是否為 separable element over K. 我們自然希望有一個等價但比較容易檢查的條件 (就像前面提的 normal extension). 以後等我們了解更多 separable extension 的性質之後, 我們會發現和 normal extension (Theorem 3.2.2) 一樣只要檢查有限多個元素就可以了. 不過事實上在目前大學代數大家所熟悉的 field extension 都是 separable extension.

Proposition 3.4.3. *假設 K 是一個 field. 則在以下兩個狀況之下的 finite extension 都是 separable extension.*

(1) *當 K 的 characteristic 是 0 時;*

(2) *當 K 是 finite field 時.*

Proof. (1) 當 K 的 characteristic 是 0 時, 由 Proposition 3.3.7 我們知所有 $K[x]$ 中的 irreducible polynomial 皆為 separable polynomial. 若 L/K 是 finite extension, 因為任意 $a \in L$ over K 的 minimal polynomial 都是 $K[x]$ 中的 irreducible polynomial, 故得 a 皆為 separable element over K. 得證 L/K 是 separable extension.

(2) 當 K 是 finite field 時, 首先我們複習一下 finite field 的性質. 我們知道 K 的 characteristic 必為一質數 p (參見大學基礎代數講義Lemma 9.2.3) 且 K 中元素個數必為 p^n, 其中 $n \in \mathbb{N}$ (參見大學基礎代數講義Theorem 10.4.1). 由於 $K \setminus \{0\}$ 共有 $p^n - 1$ 個元素且在乘法之下是一個 group, 因此利用 Lagrange Theorem 我們知對任意 $a \in K$ 且 $a \neq 0$ 皆有 $a^{p^n-1} = 1$. 兩邊各乘上 a, 得 K 中任意元素 a 皆滿足 $a^{p^n} = a$. 因此若令 $b = a^{p^{n-1}}$, 則 $b^p = (a^{p^{n-1}})^p = a^{p^n} = a$. 換言之, 對任意 $a \in K$, 皆存在 $b \in K$ 使得 $b^p = a$. 另外由於 K 的 characteristic 為 p, 當 $a, b \in K$ 時我們有 $(a+b)^p = a^p + b^p$ (參見大學基礎代數講義 Lemma 9.2.5). 因此若 $f(x) = \sum_{i=0}^{n} a_i x^i$, 則 $f(x)^p = \sum_{i=0}^{n} a_i^p x^{ip}$ (參見大學基礎代數講義 Lemma 9.2.6).

現假設 L/K 是一個 finite extension, 且假設存在 $a \in L$ 不是一個 separable element over K. 換言之, 若 a over K 的 minimal polynomial 為 $f(x)$, 則 $f(x) \in K[x]$ 不是一個 separable polynomial. 因此由 Proposition 3.3.7 (2) 我們知存在 $g(x) = \sum_{t=0}^{m} a_t x^t \in K[x]$ 使得 $f(x) = g(x^p)$. 由前面討論知, 對任意 $t \in \{0, 1, \ldots, m\}$ 皆存在 $b_t \in K$ 使得 $b_t^p = a_t$. 因此

$$f(x) = g(x^p) = \sum_{t=0}^{m} a_t (x^p)^t = \sum_{t=0}^{m} b_t^p (x^t)^p = (\sum_{t=0}^{m} b_t x^t)^p.$$

換言之, 若令 $h(x) = \sum_{t=0}^{m} b_t x^t \in K[x]$, 則 $f(x) = h(x)^p$. 這和 $f(x)$ 在 $K[x]$ 中是 irreducible polynomial 相矛盾, 因此 L 中每個元素皆為 separable element over K. 得證 L/K 是 separable extension. □

由此結果我們知, 以後若是談論 $\mathbb{Q}$ 的 finite extension 或是 finite field 的 finite extension, 我們都可以直接說是 separable extension. 雖然 Proposition 3.4.3 幾乎涵蓋了我們常見的 extension, 但並沒有涵蓋所有的情形. 接下來我們簡單的介紹一個 finite extension 但不是 separable extension 的例子.

Example 3.4.4. 令 $\mathbb{F}_2$ 為一個只有兩個元素的 finite field, α 是 transcendental over $\mathbb{F}_2$ 且令 $K = \mathbb{F}_2(\alpha)$. 要注意 K 雖然不再是 finite field 但是其 characteristic 仍為 2. 考慮 $x^2 - \alpha \in K[x]$, 而令 $L = K(\beta)$ 是 $x^2 - \alpha$ over K 的 splitting field, 其中 β 滿足 $\beta^2 = \alpha$. 首先觀察 $\beta \notin K$. 這是因為若 $\beta \in K$, 即表示存在 $f(x), g(x) \in \mathbb{F}_2[x]$, 其中 $g(x) \neq 0$ 使得 $\beta = f(\alpha)/g(\alpha)$. 換言之, $f(\alpha)^2/g(\alpha)^2 = \alpha$. 這會造成 α 是 $f(x)^2 - x \cdot g(x)^2 \in \mathbb{F}_2[x]$

的一個根, 和 α 是 transcendental over $\mathbb{F}_2$ 相矛盾. 故知 $x^2-\alpha$ 是 $K[x]$ 中的 irreducible polynomial. 又因若令 $h(x)=x-\alpha$, 則 $x^2-\alpha=h(x^2)$, 故由 Proposition 3.3.7 知 $x^2-\alpha$ 不是 separable polynomial. 因此 β 不是一個 separable element over K, 進而得知 $L=K(\beta)$ 不是一個 separable extension over K.

大家應該不難將這個例子推廣到一般 characteristic p 的例子.

接下來我們就來看看當初要介紹 separable extension 最主要的原因. 這也是有關 separable extension 最重要的性質.

Theorem 3.4.5. *假設 L/K 是一個 finite extension 且 N 是一個 L 的 extension 滿足 N/K 是 finite normal extension. 則 L/K 是一個 separable extension 若且唯若 $|\mathfrak{M}_K(L,N)|=[L:K]$.*

Proof. 首先我們用類似 Proposition 3.2.13 的證明方法對 $[L:K]$ 作 induction, 證明若 L/K 是一個 finite separable extension 且 N 是一個 L 的 extension 滿足 N/K 是 finite normal extension, 則 $|\mathfrak{M}_K(L,N)|=[L:K]$. 當 $[L:K]=1$ 時, 因為 L 到 N 的 K-monomorphism 只有 identity, 所以自然成立. 假設對所有 extension degree 小於 n 的 separable extensions 皆成立. 現考慮 $[L:K]=n>1$ 的情形. 任取 $\alpha\in L$ 但 $\alpha\notin K$. 令 $F=K(\alpha)$, 此時我們有 $[F:K]>1$ 故知 $[L:F]<n$. 假設 $p(x)\in K[x]$ 是 α over K 的 minimal polynomial. 由於 $\alpha\in L$ 且 L/K 是 separable extension, 所以 α 是一個 separable element over K, 也就是說 $p(x)$ 是一個 separable polynomial. 然而 N/K 是 normal extension, 故 $p(x)$ 在 N 中完全分解, 再加上 $p(x)$ 沒有重根, 故得 $p(x)$ 在 N 中的根的個數等於 $\deg(p(x))=[F:K]$. 因此利用所有 $K(\alpha)$ 到 N 的 K-monomorphisms 的個數等於 $p(x)$ 在 N 中根的個數, 得知 $|\mathfrak{M}_K(F,N)|=[F:K]$. 另一方面因為 $[L:F]<n$, N/F 是 normal extension (Corollary 3.2.3) 且 L/F 是 separable extension (Lemma 3.4.2), 故套用 induction 的假設知 $|\mathfrak{M}_F(L,N)|=[L:F]$. 因此利用 Lemma 3.2.12 得知

$$|\mathfrak{M}_K(L,N)|=|\mathfrak{M}_F(L,N)|\,|\mathfrak{M}_K(F,N)|=[L:F][F:K]=[L:K].$$

反之, 如果 L/K 不是 separable extension, 由定義知存在 $\beta\in L$ 不是 separable element over K. 換言之, 若 β over K 的 minimal polynomial 為 $h(x)$, 則 $h(x)$ 在 N 中有重根. 因此若令 $F=K(\beta)$ 則 $|\mathfrak{M}_K(F,N)|<\deg(h(x))=[F:K]$. 另一方面由 Proposition 3.2.13 我們知 $|\mathfrak{M}_F(L,N)|\le[L:F]$. 故套用 Lemma 3.2.12 得知

$$|\mathfrak{M}_K(L,N)|=|\mathfrak{M}_F(L,N)|\,|\mathfrak{M}_K(F,N)|<[L:F][F:K]=[L:K].$$

□

利用 Theorem 3.4.5 我們便可以回答當初談到 Lemma 3.4.2 的反向為何也是對的.

Proposition 3.4.6. *假設 L/K 是一個 finite extension 且 F 是 L/K 的 intermediate field. 則 L/K 是 separable extension 若且唯若 L/F 和 F/K 都是 separable extension.*

Proof. 在 Lemma 3.4.2 中我們已證得若 L/K 是 separable extension 則 L/F 和 F/K 都是 separable extension.

至於另一方向, 首先令 N 為 L/K 的 normal closure. 我們得 N 是 L 的一個 extension 且 N/K 以及 N/F 是 finite normal extensions. 因此若 L/F 和 F/K 是 separable extensions, 則利用 Theorem 3.4.5 知 $|\mathfrak{M}_F(L,N)| = [L:F]$ 且 $|\mathfrak{M}_K(F,N)| = [F:K]$. 故利用 Lemma 3.2.12 得到 $|\mathfrak{M}_K(L,N)| = [L:F][F:K] = [L:K]$. 因此再次利用 Theorem 3.4.5 得知 L/K 是 separable extension. □

最後我們得到一個判別 separable extension 的好方法.

Theorem 3.4.7. *假設 L/K 是一個 field extension. 下列敘述是等價的.*

(1) *L/K 是 finite separable extension.*

(2) *$L = K(a_1, \ldots, a_m)$, 其中 $a_1, \ldots, a_m$ 皆為 algebraic 且 separable element over K.*

Proof. (1) ⇒ (2) 由於 L/K 是 finite extension, 由 Proposition 1.3.4 知存在 $a_1, \ldots, a_m$ 是 algebraic over K 使得 $L = K(a_1, \ldots, a_m)$. 又因為 L/K 是 separable extension, 所有 L 中的元素都是 separable element over K, 故知 a_i 皆為 separable element over K.

(2) ⇒ (1) 因為 $a_1, \ldots, a_m$ 皆為 algebraic over K, 所以 $L = K(a_1, \ldots, a_m)$ 是 finite extension over K. 我們對 $[L:K]$ 作 induction. 假設 $[L:K] = 1$, 此時 $L = K$ 所以 L/K 當然是 separable extension. 假設對於所有 degree 小於 n 的 extension 皆成立. 現若 $[L:K] = n > 1$, 故存在 a_i 滿足 $a_i \notin K$. 不失一般性我們假設 $a_1 \notin K$. 令 $F = K(a_1)$, 則由於 $[F:K] > 1$, 我們有 $[L:F] < n$. 因為 a_1 是 separable element over K, 所以 a_1 over K 的 minimal polynomial $p(x)$ 為 separable polynomial. 若令 N 為 L/K 的 normal closure, 我們得所有 F 到 N 的 K-monomorphisms 的個數等於 $\deg(p(x)) = [F:K]$. 因此由 Theorem 3.4.5 知 F/K 是 finite separable extension. 另一方面由於 $L = K(a_1, a_2, \ldots, a_m) = K(a_1)(a_2, \ldots, a_m) = F(a_2, \ldots, a_m)$ 且 $a_2, \ldots, a_m$ 皆為 separable element over K, 當然也都是 separable element over F (因為 $K \subseteq F$), 故由 $[L:F] < n$ 套用 induction 的假設知 L/F 是 finite separable extension. 因此利用 Proposition 3.4.6, 由 F/K 是 finite separable extension 以及 L/F 是 finite separable extension 得知 L/K 是一個 finite separable extension. □

簡單來說 Theorem 3.4.7 告訴我們只要加入的元素都是 separable element 那麼所得的 extension 就是 separable extension. 因此只要檢查加入的元素而不必檢查所有的元素.

最後我們要說明一點. 由於在這裡我們只談 finite extension, 所以我們只討論在 finite extension 之下的 normal extension 和 separable extension. 事實上 normal extension 和 separable extension 的性質在一般的 algebraic extension 中也都可以討論.