簡介 Galois 理論

李華介

國立台灣師範大學數學系

Chapter 2

Galois Group 和 Fixed Field

Galois 理論主要探討的是 field extensions 之間的關係, 這些關係可以和 groups 之間的關係相連結. 本章主要是探討這些關係的基本定義及其基本性質.

2.1. Galois Group

當 L 是一個 field 時, 從 L 到 L 的 1-1 且 onto 的 ring homomorphism 稱為 L 的 automorphism. 我們用 $\mathrm{Aut}(L)$ 表示所有 L 的 automorphisms 所成的集合. 本節將討論 $\mathrm{Aut}(L)$ 相關的性質.

利用合成函數的運算我們可以將 $\mathrm{Aut}(L)$ 視成一個 group. 也就是說對任意 $\sigma, \tau \in \mathrm{Aut}(L)$, 我們考慮的運算為 $\sigma \circ \tau$, 在此運算之下 $\mathrm{Aut}(L)$ 會是一個 group. 要注意這裡的"$\circ$"指的是合成而不是乘法. 也就是說對任意 $\lambda \in L$, 我們有 $\sigma \circ \tau(\lambda) = \sigma(\tau(\lambda))$, 因此 $\sigma \circ \tau$ 仍為 L 到 L 的函數. 而且 σ 和 τ 都是 ring isomorphisms, 很容易驗證 $\sigma \circ \tau$ 仍為 ring isomorphism. 因此 $\sigma \circ \tau \in \mathrm{Aut}(L)$, 換句話說 $\mathrm{Aut}(L)$ 在 $\circ$ 的運算下是封閉的 (closed).

要證明 $\mathrm{Aut}(L)$ 在 $\circ$ 運算之下是一個 group 我們還須證明結合率 (associative law) 即 $\sigma \circ (\tau \circ \rho) = (\sigma \circ \tau) \circ \rho$ 以及存在 identity 和 inverse. 合成函數的結合率在一般的集合論中有介紹 (你也可以用元素代入自行驗證) 這裡不做驗證. 至於 identity 會是什麼呢? 大家很快猜出應該是 identity 這個函數. 這裡我們用 I 來表示, 也就是說 $I : L \to L$ 滿足對任意 $\lambda \in L$ 皆有 $I(\lambda) = \lambda$. 當然了 I 是 ring isomorphism 所以 $I \in \mathrm{Aut}(L)$. 又因為對任意 $\sigma \in \mathrm{Aut}(L)$ 皆有 $\sigma \circ I = I \circ \sigma = \sigma$, 所以 I 會是 $\mathrm{Aut}(L)$ 在 $\circ$ 的運算之下的 identity.

對任意的 $\sigma \in \mathrm{Aut}(L)$, 其 inverse 會是什麼呢? 從函數的觀點看來和 σ 合成後會是 I 的函數應就是 σ 的反函數. 又加上 σ 是 1-1 且 onto 其反函數 σ^{-1} 必存在, 所以我們找到"候選人"了: 就是 σ 的反函數 σ^{-1}. 最後我們僅要證明 $\sigma^{-1} \in \mathrm{Aut}(L)$ 即可. 首先我們要證明: $\sigma^{-1} : L \to L$ 仍為 ring isomorphism. σ^{-1} 是 1-1 且 onto 可由反函數定義推得, 所以

只要證明 σ^{-1} 為 ring homomorphism 即可. 也就是說對任意 $a, b \in L$ 我們要證明

$$\sigma^{-1}(a+b) = \sigma^{-1}(a) + \sigma^{-1}(b) \quad \text{且} \quad \sigma^{-1}(a \cdot b) = \sigma^{-1}(a) \cdot \sigma^{-1}(b).$$

因為 σ 是 ring homomorphism, 故得

$$\sigma(\sigma^{-1}(a) + \sigma^{-1}(b)) = \sigma(\sigma^{-1}(a)) + \sigma(\sigma^{-1}(b)) = a + b.$$

也就是說 $\sigma^{-1}(a+b)$ 和 $\sigma^{-1}(a) + \sigma^{-1}(b)$ 經由 σ 作用後皆得 $a+b$. 所以由 σ 是 1-1 得知 $\sigma^{-1}(a+b) = \sigma^{-1}(a) + \sigma^{-1}(b)$. 同理可得 $\sigma^{-1}(a \cdot b) = \sigma^{-1}(a) \cdot \sigma^{-1}(b)$. 由此知 $\sigma^{-1} \in \mathrm{Aut}(L)$ 從而得證 $\mathrm{Aut}(L)$ 在 $\circ$ 的運算之下是一個 group.

前面提過為了方便記, 當 L/K 是 field extensions 時我們可以直接假設 $K \subseteq L$. 在這個時候, 若 $\sigma : L \to L$ 是 L 的一個 automorphism 且對任意 $k \in K$ 皆滿足 $\sigma(k) = k$, 我們稱 σ 為 L 的一個 K-automorphism. 我們將 L 的所有 K-automorphisms 所成的集合用 $\mathrm{Aut}_K(L)$ 表示. 簡單來說 $\mathrm{Aut}_K(L)$ 的元素就是 L 的 automorphisms 中會將 K 的元素固定的那些 automorphisms.

$\mathrm{Aut}_K(L)$ 當然是 $\mathrm{Aut}(L)$ 的一個 subset, 事實上在 $\circ$ 的運算下 $\mathrm{Aut}_K(L)$ 會是 $\mathrm{Aut}(L)$ 的一個 subgroup. 要證明這件事, 依 group 的理論我們只要證明封閉性和 inverse 存在即可. 首先若 $\sigma, \tau \in \mathrm{Aut}_K(L)$, 由於對任意 $k \in K$ 我們皆有 $\sigma(k) = k$ 且 $\tau(k) = k$, 所以得到 $\sigma \circ \tau(k) = \sigma(\tau(k)) = \sigma(k) = k$. 也就是說 $\sigma \circ \tau \in \mathrm{Aut}_K(L)$. 最後對任意 $k \in K$, 由於 $\sigma(k) = k$ 故知 $\sigma^{-1}(k) = \sigma^{-1}(\sigma(k)) = k$. 因此 σ^{-1} 仍為 K-automorphism, 也就是說 $\sigma^{-1} \in \mathrm{Aut}_K(L)$.

$\mathrm{Aut}_K(L)$ 既然是一個 group 又和 L/K 這一個 extension 息息相關, 我們有以下的定義來突顯這兩件事.

Definition 2.1.1. 對任意的 extension L/K 我們稱 $\mathrm{Aut}_K(L)$ 為 L/K 的 *Galois group*. 通常我們會把 L/K 的 Galois group 記為 $\mathrm{Gal}(L/K)$.

$\mathrm{Aut}_K(L)$ 和 $\mathrm{Gal}(L/K)$ 是一樣的, 不過當我們要談論 Galois 的相關理論時我們會特別選用 $\mathrm{Gal}(L/K)$ 這個符號.

當 F/K 是 L/K 的 subextension, 即 F 是一個 field 且 $K \subseteq F \subseteq L$. 我們稱 F 是 L/K 的 *intermediate field*. 這時我們有兩個 groups 可以考慮: 一個是 $\mathrm{Gal}(L/F)$, 另一個是 $\mathrm{Gal}(F/K)$. 這兩個 groups 都和 $\mathrm{Gal}(L/K)$ 有關, 不過 $\mathrm{Gal}(L/F)$ 和 $\mathrm{Gal}(L/K)$ 的關係較直接, 所以我們先討論 $\mathrm{Gal}(L/F)$ 和 $\mathrm{Gal}(L/K)$ 的關係.

事實上若 $\sigma \in \mathrm{Gal}(L/F)$, 依定義我們當然有 $\sigma \in \mathrm{Aut}(L)$ 而且 σ 將 F 中的元素固定. 然而由於 $K \subseteq F$ 我們知 σ 當然也將 K 中的元素固定. 也就是說 $\sigma \in \mathrm{Aut}_K(L) = \mathrm{Gal}(L/K)$. 我們得證 $\mathrm{Gal}(L/F) \subseteq \mathrm{Gal}(L/K)$. 又由於 $\mathrm{Gal}(L/K)$ 和 $\mathrm{Gal}(L/F)$ 在 $\circ$ 的運算之下都是 group, 所以 $\mathrm{Gal}(L/F)$ 是 $\mathrm{Gal}(L/K)$ 的 subgroup.

若令 $\mathfrak{F}$ 是 L/K 的 intermediate fields 所成的集合且令 $\mathfrak{G}$ 是 $\mathrm{Gal}(L/K)$ 的 subgroups 所成的集合. 由以上的討論我們可以訂一個從 $\mathfrak{F}$ 到 $\mathfrak{G}$ 的函數 $\mathcal{G}$. 這個函數 $\mathcal{G} : \mathfrak{F} \to \mathfrak{G}$ 的定義如下: 對任意 L/K 的 intermediate field $F \in \mathfrak{F}$, 我們定義 $\mathcal{G}(F) = \mathrm{Gal}(L/F)$.

由定義我們知道 $\mathcal{G}(K) = \mathrm{Gal}(L/K)$. 另外 $\mathcal{G}(L) = \mathrm{Gal}(L/L) = \mathrm{Aut}_L(L)$, 也就是說 $\mathcal{G}(L)$ 中的元素 σ 必須是 L 到 L 的函數且滿足對任意 $\lambda \in L$ 皆有 $\sigma(\lambda) = \lambda$. 這表示 $\sigma = I$, 因此得知 $\mathcal{G}(L) = \{I\}$ 是由 identity 所成的 trivial group. 對於函數 $\mathcal{G}$, 我們還有以下的性質.

Lemma 2.1.2. *給定一 extension L/K, 若 $F_1, F_2 \in \mathfrak{F}$ 是 L/K 之兩個 intermediate fields 且滿足 $F_1 \subseteq F_2$, 則 $\mathcal{G}(F_2) \subseteq \mathcal{G}(F_1)$.*

Proof. 若 $\sigma \in \mathcal{G}(F_2) = \mathrm{Gal}(L/F_2)$, 即表示 σ 是 L 的 automorphism 且將 F_2 中的元素固定. 然而由於 $F_1 \subseteq F_2$, 可知 σ 當然也將 F_1 中的元素固定. 故得 $\sigma \in \mathrm{Gal}(L/F_1) = \mathcal{G}(F_1)$. 得證 $\mathcal{G}(F_2) \subseteq \mathcal{G}(F_1)$. □

這裡我們要強調: 必須先固定一個 extension L/K 才能定義出 $\mathcal{G}$ 這一個函數. 另外要注意的是 $\mathcal{G}$ 的定義域是一些 fields 所成的集合而不是 field. 更具體一點來說就是: 可以代入 $\mathcal{G}$ 的應該是 L/K 的 intermediate field 而不是 L 的元素. 同樣的將一個 intermediate field 代入 $\mathcal{G}$ 後所得的結果會是 $\mathrm{Gal}(L/K)$ 的 subgroup, 而不是 $\mathrm{Gal}(L/K)$ 中的元素. 千萬不要誤以為這裡定的 $\mathcal{G}$ 是從 L 送到 $\mathrm{Gal}(L/K)$ 的函數.

接下來我們要介紹一些 Galois groups 的例子. 因為我們舉的例子都是 simple extensions, 所以先介紹一下探討 simple extension 的 Galois group 的基本方法.

假設 L/K 是一個 simple extension of degree n, 即 $L = K(\alpha)$ 其中 α over K 的 minimal polynomial 為 $f(x) \in K[x]$ 且 $\deg(f(x)) = n$. 在前一章中我們提及對任意的 $\lambda \in K(\alpha)$ 都可唯一表示成:

$$\lambda = c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}, \quad \text{其中 } c_0, c_1 \ldots, c_{n-1} \in K.$$

現若 $\sigma \in \mathrm{Gal}(L/K)$, 則由於 σ 是 ring homomorphism 且將 K 中的元素固定, 可得

$$\sigma(\lambda) = \sigma(c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}) = c_0 + c_1\sigma(\alpha) + \cdots + c_{n-1}\sigma(\alpha)^{n-1}.$$

換言之, 對任意 $\lambda \in L$, $\sigma(\lambda)$ 的取值完全可由 $\sigma(\alpha)$ 決定. 所以要了解 $\mathrm{Gal}(L/K)$ 只要了解對任意 $\sigma \in \mathrm{Gal}(L/K)$, $\sigma(\alpha)$ 有哪些可能的取值. 這個概念對 simple extension 的 Galois group 相當重要, 我們不時的會用它來處理 simple extension.

那麼對任意的 $\sigma \in \mathrm{Gal}(L/K)$, $\sigma(\alpha)$ 有可能取哪些值呢? 首先我們觀察對任意的 $g(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0 \in K[x]$, 由於

$$g(\alpha) = a_m\alpha^m + a_{m-1}\alpha^{m-1} + \cdots + a_1\alpha + a_0,$$

以及 σ 是 ring homomorphism 且將 K 中的元素固定, 我們有

$$\begin{aligned} \sigma(g(\alpha)) &= \sigma(a_m\alpha^m + a_{m-1}\alpha^{m-1} + \cdots + a_1\alpha + a_0) \\ &= a_m\sigma(\alpha)^m + a_{m-1}\sigma(\alpha)^{m-1} + \cdots + a_1\sigma(\alpha) + a_0 \\ &= g(\sigma(\alpha)). \end{aligned} \tag{2.1}$$

現在由於 $f(x)$ 是 α over K 的 minimal polynomial, 我們有 $f(x) \in K[x]$ 且 $f(\alpha) = 0$, 套用等式 (2.1) 可得

$$f(\sigma(\alpha)) = \sigma(f(\alpha)) = \sigma(0) = 0.$$

也就是說 $\sigma(\alpha)$ 必為 $f(x)$ 的一個根. 又別忘了 σ 是 L 到 L 的 automorphism, 故知 $\sigma(\alpha) \in L$. 所以我們可以總結說: 若 $L = K(\alpha)$, $f(x) \in K[x]$ 為 α 的 minimal polynomial over K 且 $\sigma \in \mathrm{Gal}(L/K)$, 則 $\sigma(\alpha)$ 必為 $f(x)$ 在 L 中的一個根.

上一個結論只是說 $\sigma(\alpha)$ 必為 $f(x)$ 在 L 中的一個根. 並不表示對任意 $f(x)$ 在 L 中的一個根 β 皆存在 $\sigma \in \mathrm{Gal}(L/K)$ 使得 $\sigma(\alpha) = \beta$. 接下來我們要說明這是對的. 首先回顧一下: 若 $f(x) \in K[x]$ 是一個 irreducible polynomial 且 α 和 β 為其根, 從大學基礎代數講義的 Corollary 10.1.7 我們知道存在 K-isomorphisms $\phi : K[x]/(f(x)) \to K(\alpha)$ 和 $\psi : K[x]/(f(x)) \to K(\beta)$ 滿足 $\phi(\overline{x}) = \alpha$ 和 $\psi(\overline{x}) = \beta$. 考慮 $\rho = \psi \circ \phi^{-1} : K(\alpha) \to K(\beta)$, 很容易檢查 ρ 仍為 K-isomorphism 且滿足 $\rho(\alpha) = \beta$. 現若又知 $\beta \in L = K(\alpha)$, 由於 $K(\beta) \subseteq L$ 且 $[K(\beta) : K] = [L : K] = n$, 可得 $K(\beta) = L = K(\alpha)$. 換句話說在這情況下 ρ 為 L 的 K-automorphism, 也就是說 $\rho \in \mathrm{Gal}(L/K)$ 且滿足 $\rho(\alpha) = \beta$. 綜合以上的討論, 我們可以由 $f(x)$ 在 L 中相異根的個數得知 $\mathrm{Gal}(L/K)$ 的 order. (回顧一下所謂一個 finite group G 的 order 就是 G 中元素的個數, 記作 $|G|$.)

Proposition 2.1.3. *假設 $L = K(\alpha)$ 是一個 finite simple extension over K 且 $f(x) \in K[x]$ 為 α over K 的 minimal polynomial. 若 $f(x)$ 在 L 中共有 m 個相異根, 則 $|\mathrm{Gal}(L/K)| = m$.*

Proof. 令 $S = \{\beta \in L \mid f(\beta) = 0\}$ 為 L 中所有 $f(x)$ 的根所成的集合. 考慮一函數 $\chi : \mathrm{Gal}(L/K) \to S$ 使得對任意 $\sigma \in \mathrm{Gal}(L/K)$ 定義 $\chi(\sigma) = \sigma(\alpha)$. 從前面討論知對任意 $\sigma \in \mathrm{Gal}(L/K)$, 皆有 $\sigma(\alpha) \in S$, 所以 χ 是一個 well defined 的函數. 我們目的是要證明 χ 是 1-1 且 onto 由此可得 $\mathrm{Gal}(L/K)$ 和 S 的元素個數相等.

假設 $\sigma, \tau \in \mathrm{Gal}(L/K)$ 滿足 $\chi(\sigma) = \chi(\tau)$, 即 $\sigma(\alpha) = \tau(\alpha)$. 由前面討論知 σ 和 τ 對任意 L 中元素的取值完全由 $\sigma(\alpha)$ 和 $\tau(\alpha)$ 來決定. 因此由 $\sigma(\alpha) = \tau(\alpha)$ 得知 $\sigma = \tau$, 也就是說 χ 是 1-1. 另一方面對任意 $\beta \in S$ 由前面討論知必存在 $\sigma \in \mathrm{Gal}(L/K)$ 使得 $\sigma(\alpha) = \beta$, 也就是說 $\chi(\sigma) = \beta$. 故得證 χ 是 onto, 因此知 $\mathrm{Gal}(L/K)$ 的 order 為 m. □

由於一個多項式在一個 field 中其解的個數不超過此多項式的次數, 我們很容易得到以下之結果.

Corollary 2.1.4. *假設 L/K 是一個 finite simple extension, 則*

$$|\mathrm{Gal}(L/K)| \leq [L : K].$$

Proof. 假設 $L = K(\alpha)$ 且 α over K 的 minimal polynomial $f(x)$ 的次數為 n. 我們知在 L 中 $f(x)$ 的根的個數必小於或等於 n 而且 $[L : K] = n$, 故由 Proposition 2.1.3 知

$$|\mathrm{Gal}(L/K)| \leq n = [L : K].$$

□

這裡我們預告一下, 當 L/K 是 finite extension 時, 以後我們會知道即使 L/K 不是 simple extension, 仍然會有 $|\mathrm{Gal}(L/K)| \leq [L:K]$. 接下來我們來看兩個 simple extension 的例子.

Example 2.1.5. 利用 Eisenstain criterion 參見大學基礎代數講義Proposition 7.3.14 我們知道 x^4-2 是 $\mathbb{Q}[x]$ 中的 irreducible polynomial. 令 $\alpha = \sqrt[4]{2}$ 是 $x^4-2=0$ 唯一的正實數解, 我們有 α, $-\alpha$, αi 以及 $-\alpha i$ 是 $x^4-2=0$ 在 $\mathbb{C}$ 中的 4 個解. 現令 $L=\mathbb{Q}(\alpha)$, 我們考慮 $L/\mathbb{Q}$ 這一個 extension.

首先我們討論 $\mathrm{Gal}(L/\mathbb{Q})$ 是怎樣的 group. 由於 $\alpha \in \mathbb{R}$ 且 $L=\mathbb{Q}(\alpha)$ 是包含 $\mathbb{Q}$ 和 α 最小的 field, 故知 $L \subseteq \mathbb{R}$. 但 $\alpha i \notin \mathbb{R}$ 且 $-\alpha i \notin \mathbb{R}$, 我們得知 x^4-2 在 L 中的根為 α 和 $-\alpha$. 故由 Proposition 2.1.3 得知 $|\mathrm{Gal}(L/\mathbb{Q})| = 2 < 4 = [L:\mathbb{Q}]$.

從 group 的理論我們知只有兩個元素的 group 必 isomorphic to $\mathbb{Z}/2\mathbb{Z}$, 因此我們知 $\mathrm{Gal}(L/\mathbb{Q})$ 是一個 order 2 的 cyclic group. 事實上 $\mathrm{Gal}(L/\mathbb{Q})$ 有兩個元素: 一個是 identity I 將 α 送到 α, 另一個不為 identity 的元素 σ 將 α 送到 $-\alpha$. 由於 $\sigma(\alpha) = -\alpha$, 我們知

$$\sigma \circ \sigma(\alpha) = \sigma(\sigma(\alpha)) = \sigma(-\alpha) = -\sigma(\alpha) = \alpha.$$

得知 $\sigma \circ \sigma = I$, 也就是說 σ 的 order 確為 2. 因此 $\mathrm{Gal}(L/\mathbb{Q})$ 的確是一個 order 2 的 cyclic group.

因為 $\alpha^4 = 2$, 很容易看出 α^2 是 x^2-2 的一個根. 令 $F = \mathbb{Q}(\alpha^2)$. 由於 x^2-2 是 irreducible over $\mathbb{Q}$, 所以 $[F:\mathbb{Q}] = 2$, 又因為 $\alpha^2 \in L$, 我們知 $\mathbb{Q} \subsetneq F \subsetneq L$. 既然 F 是 L/K 的 intermediate field, 那麼 $\mathcal{G}(F) = \mathrm{Gal}(L/F)$ 是甚麼呢? 已知 $\mathrm{Gal}(L/F)$ 會是 $\mathrm{Gal}(L/\mathbb{Q})$ 的 subgroup, 又知 $\mathrm{Gal}(L/\mathbb{Q})$ 是一個 order 2 的 cyclic group, 所以 $\mathrm{Gal}(L/F)$ 要不是 identity 就是 $\mathrm{Gal}(L/\mathbb{Q})$. 因此我們只要檢驗 $\mathrm{Gal}(L/\mathbb{Q})$ 中不為 identity 的 σ (即 $\sigma(\alpha) = -\alpha$) 是否在 $\mathrm{Gal}(L/F)$ 中即可: 也就是要檢查 σ 是否將 $F = \mathbb{Q}(\alpha^2)$ 中的元素固定. 因為 σ 已將 $\mathbb{Q}$ 中元素固定, 所以若 σ 可將 α^2 固定, 則 σ 會將 $F = \mathbb{Q}(\alpha^2)$ 中所有的元素固定 (別忘了 $\mathbb{Q}(\alpha^2)$ 中的元素都是 $r_0 + r_1\alpha^2$ 其中 $r_0, r_1 \in \mathbb{Q}$ 這種形式). 然而

$$\sigma(\alpha^2) = \sigma(\alpha)^2 = (-\alpha)^2 = \alpha^2,$$

我們得知 $\sigma \in \mathrm{Gal}(L/F)$, 也就是說 $\mathrm{Gal}(L/F) = \mathrm{Gal}(L/\mathbb{Q})$. 用 $\mathcal{G}$ 這個函數來看就是 $\mathcal{G}(F) = \mathcal{G}(\mathbb{Q})$. 由於已知 $F \neq \mathbb{Q}$, 所以在這情況之下 $\mathcal{G}$ 不是一對一的函數.

Example 2.1.6. 令 $L = \mathbb{Q}(\alpha)$ 其中 $\alpha = \sqrt{2}+i$. 很容易驗證 $x^4-2x^2+9 \in \mathbb{Q}[x]$ 是 α over $\mathbb{Q}$ 的 minimal polynomial. 我們有

$$\alpha = \sqrt{2}+i, \quad -\alpha = -\sqrt{2}-i, \quad \overline{\alpha} = \sqrt{2}-i \quad \text{and} \quad -\overline{\alpha} = -\sqrt{2}+i$$

是 $x^4-2x^2+9=0$ 在 $\mathbb{C}$ 中的 4 個解.

由於 $(\sqrt{2}+i)\cdot(\sqrt{2}-i) = 3$, 知 $\overline{\alpha} = \sqrt{2}-i = 3(\sqrt{2}+i)^{-1} = 3\alpha^{-1} \in L$. 因此 x^4-2x^2+9 在 $\mathbb{C}$ 中的 4 個根 (即 α, $-\alpha$, $3\alpha^{-1}$ 和 $-3\alpha^{-1}$) 都在 L 中. 故由 Proposition 2.1.3 知 $|\mathrm{Gal}(L/\mathbb{Q})| = 4$.

由 group 的理論知 $\mathrm{Gal}(L/\mathbb{Q})$ 會 isomorphic to $\mathbb{Z}/4\mathbb{Z}$ 或 $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ 其中之一. 區分 $\mathbb{Z}/4\mathbb{Z}$ 和 $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ 這兩個 groups 的方法是: 由於 $\mathbb{Z}/4\mathbb{Z}$ 是一個 order 4 的 cyclic group, 所以其中必存在一個 order 4 的元素, 而 $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ 就沒有 order 4 的元素. 因此我們需檢查 $\mathrm{Gal}(L/\mathbb{Q})$ 中所有元素的 order. 已經知道 $\mathrm{Gal}(L/\mathbb{Q})$ 中將 α 送到 α 的元素就是 identity, 所以我們只要考慮其他三個元素 $\sigma_1,\sigma_2,\sigma_3\in\mathrm{Gal}(L/\mathbb{Q})$ 其中

$$\sigma_1(\alpha)=-\alpha,\quad \sigma_2(\alpha)=\overline{\alpha}=3\alpha^{-1}\quad\text{and}\quad \sigma_3(\alpha)=-\overline{\alpha}=-3\alpha^{-1}.$$

因為

$$\sigma_1\circ\sigma_1(\alpha)=\sigma_1(\sigma_1(\alpha))=\sigma_1(-\alpha)=-\sigma_1(\alpha)=-(-\alpha)=\alpha,$$

得知 $\sigma_1\circ\sigma_1=I$, 也就是說 σ_1 的 order 為 2. 另一方面

$$\sigma_2\circ\sigma_2(\alpha)=\sigma_2(\sigma_2(\alpha))=\sigma_2(3\alpha^{-1})=3\sigma_2(\alpha)^{-1}=3(3\alpha^{-1})^{-1}=\alpha,$$

以及

$$\sigma_3\circ\sigma_3(\alpha)=\sigma_3(\sigma_3(\alpha))=\sigma_3(-3\alpha^{-1})=-3\sigma_3(\alpha)^{-1}=-3(-3\alpha^{-1})^{-1}=\alpha,$$

所以 σ_2 和 σ_3 的 order 皆為 2. 得知 $\mathrm{Gal}(L/\mathbb{Q})\simeq\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$.

接下來我們看看 L/K 的 intermediate fields. 由於 $(\sqrt{2}+i)+(\sqrt{2}-i)=2\sqrt{2}$ 以及 $(\sqrt{2}+i)-(\sqrt{2}-i)=2i$, 我們知

$$\sqrt{2}=\frac{1}{2}(\alpha+3\alpha^{-1})\in L,\quad i=\frac{1}{2}(\alpha-3\alpha^{-1})\in L\quad\text{and}\quad \sqrt{2}i=\frac{1}{4}(\alpha^2-9\alpha^{-2})\in L.$$

令 $F_1=\mathbb{Q}(\sqrt{2}i)$, $F_2=\mathbb{Q}(\sqrt{2})$ 以及 $F_3=\mathbb{Q}(i)$. 很容易看出 $[F_1:\mathbb{Q}]=[F_2:\mathbb{Q}]=[F_3:\mathbb{Q}]=2$. 由於 $F_2\subseteq\mathbb{R}$ 但 $F_1,F_3\not\subseteq\mathbb{R}$, 我們知 $F_2\neq F_1$ 且 $F_2\neq F_3$. 又若假設 $F_1=F_3$, 即 $\sqrt{2}i\in F_3=\mathbb{Q}(i)$, 則 $\sqrt{2}=\sqrt{2}i/i\in F_3$. 得到 $F_2=F_3$ 之矛盾, 故知 $F_1\neq F_3$. 因此 F_1, F_2 和 F_3 是 $L/\mathbb{Q}$ 的三個相異的 intermediate fields.

要知道 $\mathcal{G}(F_1)$ (即 $\mathrm{Gal}(L/F_1)$) 是 $\mathrm{Gal}(L/\mathbb{Q})$ 的哪一個 subgroup, 我們需要探討在 σ_1, σ_2 和 σ_3 中哪些會固定 $F_1=\mathbb{Q}(\sqrt{2}i)$ 中所有的元素. 由於

$$\sigma_1(\sqrt{2}i)=\sigma_1(\frac{1}{4}(\alpha^2-9\alpha^{-2}))=\frac{1}{4}(\sigma_1(\alpha)^2-9\sigma_1(\alpha)^{-2})=\frac{1}{4}((-\alpha)^2-9(-\alpha)^{-2})=\sqrt{2}i,$$

$$\sigma_2(\sqrt{2}i)=\sigma_2(\frac{1}{4}(\alpha^2-9\alpha^{-2}))=\frac{1}{4}(\sigma_2(\alpha)^2-9\sigma_2(\alpha)^{-2})=\frac{1}{4}(9\alpha^{-2}-9(3\alpha^{-1})^{-2})=-\sqrt{2}i,$$

以及

$$\sigma_3(\sqrt{2}i)=\sigma_3(\frac{1}{4}(\alpha^2-9\alpha^{-2}))=\frac{1}{4}(\sigma_3(\alpha)^2-9\sigma_2(\alpha)^{-2})=\frac{1}{4}(9\alpha^{-2}-9(-3\alpha^{-1})^{-2})=-\sqrt{2}i,$$

我們知僅有 σ_1 會固定 F_1 中的元素, 因此知 $\mathcal{G}(F_1)=\mathrm{Gal}(L/F_1)=\{I,\sigma_1\}$. 同樣方法可得到 $\mathcal{G}(F_2)=\mathrm{Gal}(L/F_2)=\{I,\sigma_2\}$ 以及 $\mathcal{G}(F_3)=\mathrm{Gal}(L/F_3)=\{I,\sigma_3\}$. 要注意雖然 $\mathcal{G}(F_1)$, $\mathcal{G}(F_2)$ 以及 $\mathcal{G}(F_3)$ 都 isomorphic to $\mathbb{Z}/2\mathbb{Z}$, 但它們是 $\mathrm{Gal}(L/\mathbb{Q})$ 中三個相異的 subgroups. 事實上以後我們會知道在這個例子中 $\mathcal{G}$ 這個函數是 1-1 且 onto 的.

2.2. Fixed Field

當 L 是一個 field, $\sigma \in \mathrm{Aut}(L)$ 若 $\lambda \in L$ 滿足 $\sigma(\lambda) = \lambda$, 我們就稱 λ 被 σ 固定 (fixed). 我們用 L^σ 表示在 L 中所有被 σ 固定的元素所成的集合. L^σ 事實上是一個 field, 我們稱之為 σ 的 fixed field. 這一節中我們主要是介紹 fixed field 以及其和 Galois group 的關係.

首先我們來看 L^σ 為何是一個 field. 若 $\lambda_1, \lambda_2 \in L^\sigma$, 且 $\lambda_2 \neq 0$ 則由於 $\sigma(\lambda_1) = \lambda_1$, $\sigma(\lambda_2) = \lambda_2$ 以及 $\sigma \in \mathrm{Aut}(L)$, 可得

$$\sigma(\lambda_1 - \lambda_2) = \sigma(\lambda_1) - \sigma(\lambda_2) = \lambda_1 - \lambda_2 \quad \text{and} \quad \sigma(\lambda_1\lambda_2^{-1}) = \sigma(\lambda_1)\sigma(\lambda_2)^{-1} = \lambda_1\lambda_2^{-1}.$$

因此 $\lambda_1 - \lambda_2 \in L^\sigma$ 以及 $\lambda_1\lambda_2^{-1} \in L^\sigma$, 故知 L^σ 是一個 field. 特別當 L/K 是一個 field extension 且 $\sigma \in \mathrm{Gal}(L/K)$, 則由於 K 中的元素皆被 σ, 固定我們有 $K \subseteq L^\sigma \subseteq L$, 換言之 L^σ 是 L/K 的 intermediate field.

在前一節中我們定義了一個函數 $\mathcal{G}$ 將 L/K 的 intermediate fields 送到 $\mathrm{Gal}(L/K)$ 的 subgroups. 一般來說 $\mathcal{G}$ 不一定是 1-1 (參見 Example 2.1.5), 為了探討何時 $\mathcal{G}$ 會 1-1, 以下我們引進了一個反向的函數將 $\mathrm{Gal}(L/K)$ 的 subgroups 送到 L/K 的 intermediate fields.

首先若 H 是 $\mathrm{Gal}(L/K)$ 的一個 subgroup 我們定義

$$L^H = \{\lambda \in L \,|\, \sigma(\lambda) = \lambda, \forall\, \sigma \in H\} = \bigcap_{\sigma \in H} L^\sigma.$$

利用 fields 的交集仍是 field 以及對任意 $\sigma \in H \subseteq \mathrm{Gal}(L/K)$ 皆有 $K \subseteq L^\sigma$, 我們知 L^H 仍為一個 field 且 $K \subseteq L^H \subseteq L$. 故得 L^H 仍為 L/K 的 intermediate field.

Definition 2.2.1. 當 L/K 是一個 field extension 且 H 是 $\mathrm{Gal}(L/K)$ 的一個 subgroup, 我們稱 $L^H = \{\lambda \in L \,|\, \sigma(\lambda) = \lambda, \forall\, \sigma \in H\}$ 為 H 的 fixed field.

回顧上一節中當 L/K 是一個 field extension, 我們令 $\mathfrak{F}$ 是 L/K 的 intermediate fields 所成的集合且令 $\mathfrak{G}$ 是 $\mathrm{Gal}(L/K)$ 的 subgroups 所成的集合. 現在我們可以定義一個函數 $\mathcal{F} : \mathfrak{G} \to \mathfrak{F}$ 使得對任意 $\mathrm{Gal}(L/K)$ 的 subgroup H (即 $H \in \mathfrak{G}$), 我們定義 $\mathcal{F}(H) = L^H$. 從前面的討論我們知 L^H 是 L/K 的一個 intermediate field, 也就是說 $\mathcal{F}(H) \in \mathfrak{F}$, 因此 $\mathcal{F}$ 確實是一個 well-defined 函數.

當 I 是 $\mathrm{Gal}(L/K)$ 的 identity 時, 當然有 $L^I = L$, 因此由定義知 $\mathcal{F}(\{I\}) = L$. 要注意的是雖然 $\mathrm{Gal}(L/K)$ 將 K 的元素都固定, 但是 $\mathrm{Gal}(L/K)$ 的 fixed field 可能比 K 還大, 所以一般的情形不見得有 $\mathcal{F}(\mathrm{Gal}(L/K)) = K$ (後面我們會舉一個例子). 對於函數 $\mathcal{F}$ 我們有和 $\mathcal{G}$ 相對應的性質 (Lemma 2.1.2).

Lemma 2.2.2. *給定一 extension L/K, 若 $H_1, H_2 \in \mathfrak{G}$ 是 $\mathrm{Gal}(L/K)$ 之兩個 subgroups 且滿足 $H_1 \subseteq H_2$, 則 $\mathcal{F}(H_2) \subseteq \mathcal{F}(H_1)$.*

Proof. 若 $\lambda \in \mathcal{F}(H_2) = L^{H_2}$, 表示對任意 $\sigma \in H_2$ 皆滿足 $\sigma(\lambda) = \lambda$. 現任取 $\tau \in H_1$, 由於 $H_1 \subseteq H_2$, 我們有 $\tau \in H_2$, 故由 $\lambda \in \mathcal{F}(H_2)$ 的假設知 $\tau(\lambda) = \lambda$, 因此 $\lambda \in L^{H_1} = \mathcal{F}(H_1)$. 得證 $\mathcal{F}(H_2) \subseteq \mathcal{F}(H_1)$. □

再次強調: $\mathcal{G}$ 是將 L/K 的 intermediate fields 送到 $\mathrm{Gal}(L/K)$ 的 subgroups, 而 $\mathcal{F}$ 是將 $\mathrm{Gal}(L/K)$ 的 subgroups 送到 L/K 的 intermediate fields. 以下是這兩個函數相互的關係.

Proposition 2.2.3. 令 L/K 是一個 *field extension,* F 是 L/K 的 *intermediate field* 且 H 是 $\mathrm{Gal}(L/K)$ 的 *subgroup.* 我們有以下的性質:

(1) $F \subseteq \mathcal{F}(\mathcal{G}(F))$ 且 $H \subseteq \mathcal{G}(\mathcal{F}(H))$.

(2) $\mathcal{G}(F) = \mathcal{G}(\mathcal{F}(\mathcal{G}(F)))$ 且 $\mathcal{F}(H) = \mathcal{F}(\mathcal{G}(\mathcal{F}(H)))$.

Proof. (1) 首先觀察若 F 是 L/K 的 intermediate field, 則 $\mathcal{G}(F) = \mathrm{Gal}(L/F)$, 換言之對任意的 $\sigma \in \mathcal{G}(F)$ 都會將 F 中的元素固定. 因此若 $\lambda \in F$, 則對任意 $\sigma \in \mathcal{G}(F)$ 皆滿足 $\sigma(\lambda) = \lambda$, 也就是說 $\lambda \in L^{\mathcal{G}(F)} = \mathcal{F}(\mathcal{G}(F))$. 故得證 $F \subseteq \mathcal{F}(\mathcal{G}(F))$. 另一方面, 若 H 是 $\mathrm{Gal}(L/K)$ 的 subgroup, 則 $\mathcal{F}(H)$ 中的元素都會被 H 固定住. 因此若 $\sigma \in H$, 則 $\sigma \in \mathrm{Aut}_{\mathcal{F}(H)}(L) = \mathrm{Gal}(L/\mathcal{F}(H)) = \mathcal{G}(\mathcal{F}(H))$. 故得證 $H \subseteq \mathcal{G}(\mathcal{F}(H))$.

(2) 由於 F 和 $\mathcal{F}(\mathcal{G}(F))$ 皆為 L/K 的 intermediate fields, 利用 (1) $F \subseteq \mathcal{F}(\mathcal{G}(F))$ 以及 Lemma 2.1.2 我們得到 $\mathcal{G}(\mathcal{F}(\mathcal{G}(F))) \subseteq \mathcal{G}(F)$. 然而 $\mathcal{G}(F)$ 是 $\mathrm{Gal}(L/K)$ 的 subgroup, 故將 (1) 的 H 用 $\mathcal{G}(F)$ 取代, 可得 $\mathcal{G}(F) \subseteq \mathcal{G}(\mathcal{F}(\mathcal{G}(F)))$. 因此得證 $\mathcal{G}(F) = \mathcal{G}(\mathcal{F}(\mathcal{G}(F)))$. 另一方面因為 H 和 $\mathcal{G}(\mathcal{F}(H))$ 皆為 $\mathrm{Gal}(L/K)$ 的 subgroups, 利用 (1) $H \subseteq \mathcal{G}(\mathcal{F}(H))$ 以及 Lemma 2.2.2 我們得到 $\mathcal{F}(\mathcal{G}(\mathcal{F}(H))) \subseteq \mathcal{F}(H)$. 然而 $\mathcal{F}(H)$ 是 L/K 的 intermediate field, 故將 (1) 的 F 用 $\mathcal{F}(H)$ 取代, 可得 $\mathcal{F}(H) \subseteq \mathcal{F}(\mathcal{G}(\mathcal{F}(H)))$. 因此得證 $\mathcal{F}(H) = \mathcal{F}(\mathcal{G}(\mathcal{F}(H)))$. □

在一般的情形 Proposition 2.2.3 (1) 的等式有可能不成立 (即 $F \subsetneq \mathcal{F}(\mathcal{G}(F))$ 和 $H \subsetneq \mathcal{G}(\mathcal{F}(H))$ 的情形有可能發生). 以後我們會知道當 L/K 是 finite extension 時, 對任意 $\mathrm{Gal}(L/K)$ 的 subgroup H 皆有 $H = \mathcal{G}(\mathcal{F}(H))$ 的性質. 不過對於 L/K 的 intermediate field F, 仍可能有 $F \neq \mathcal{F}(\mathcal{G}(F))$ 的情形發生 (下面我們會給一個例子). Galois 的理論就是要探討在哪些 extension L/K, 對任意的 L/K 的 intermediate field F 皆有 $F = \mathcal{F}(\mathcal{G}(F))$ 的性質.

以下我們利用前一節的例子, 來探討 Galois groups 和 fixed fields 之間的關係.

Example 2.2.4. 我們沿用 Example 2.1.5 的 extension, 即 $L = \mathbb{Q}(\alpha)$ 其中 α 是 $x^4 - 2$ 唯一的正實根. 此時我們知 $\mathrm{Gal}(L/\mathbb{Q}) = \{I, \sigma\}$, 其中 $\sigma(\alpha) = -\alpha$. 又 $F = \mathbb{Q}(\alpha^2)$ 為 $L/\mathbb{Q}$ 的 intermediate field 且 $\mathbb{Q} \subsetneq F \subsetneq L$.

$\mathrm{Gal}(L/\mathbb{Q})$ 只有兩個 subgroups: 即 $\{I\}$ 和 $\mathrm{Gal}(L/\mathbb{Q})$. 已知 $\mathcal{F}(\{I\}) = L$, 我們來探討 $\mathcal{F}(\mathrm{Gal}(L/\mathbb{Q}))$ 應該是哪一個 field. 由於

$$\mathcal{F}(\mathrm{Gal}(L/\mathbb{Q})) = L^I \cap L^\sigma = L \cap L^\sigma = L^\sigma,$$

我們只要探討 σ 的 fixed field 即可.

由於對任意 L 中的元素 λ 都可唯一表示成 $\lambda = r_0 + r_1\alpha + r_2\alpha^2 + r_3\alpha^3$, 其中 $r_1, r_2, r_3, r_4 \in \mathbb{Q}$. 若 $\lambda \in L^\sigma$, 我們有

$$\lambda = \sigma(\lambda) = r_0 + r_1\sigma(\alpha) + r_2\sigma(\alpha)^2 + r_3\sigma(\alpha)^3 = r_0 - r_1\alpha + r_2\alpha^2 - r_3\alpha^3.$$

因此得知 $r_1 = r_3 = 0$, 也就是說 L^σ 中的元素必可寫成 $r_0 + r_2\alpha^2$, 其中 $r_0, r_2 \in \mathbb{Q}$ 這種形式. 故得 $L^\sigma \subseteq \mathbb{Q}(\alpha^2) = F$. 另一方面在 Example 2.1.5 中我們知 F 中的元素都被 σ 固定, 故得 $F \subseteq L^\sigma$. 因此得證 $L^\sigma = F$, 也就是說 $\mathcal{F}(\mathrm{Gal}(L/\mathbb{Q})) = F$. 要注意, 我們曾經提過在一般的情形 $\mathrm{Gal}(L/K)$ 的 fixed field 不一定是 K, 在我們這個例子 $\mathcal{F}(\mathrm{Gal}(L/\mathbb{Q})) = F \neq \mathbb{Q}$, 就是這種情形.

在 Example 2.1.5 我們已知 $\mathcal{G}(\mathbb{Q}) = \mathcal{G}(F) = \mathrm{Gal}(L/\mathbb{Q})$ 以及 $\mathcal{G}(L) = \{I\}$. 因此我們有

$$\mathcal{F}(\mathcal{G}(\mathbb{Q})) = \mathcal{F}(\mathcal{G}(F)) = \mathcal{F}(\mathrm{Gal}(L/\mathbb{Q})) = F \quad \text{and} \quad \mathcal{F}(\mathcal{G}(L)) = \mathcal{F}(\{I\}) = L.$$

因此知

$$\mathbb{Q} \subsetneq \mathcal{F}(\mathcal{G}(\mathbb{Q})), \quad F = \mathcal{F}(\mathcal{G}(F)) \quad \text{and} \quad L = \mathcal{F}(\mathcal{G}(L)).$$

要注意 $\mathbb{Q} \subsetneq \mathcal{F}(\mathcal{G}(\mathbb{Q}))$ 就是 Proposition 2.2.3 (1) 等式不成立的一個例子.

另一方面我們有 $\mathcal{G}(\mathcal{F}(\{I\})) = \mathcal{G}(L)$ 且 $\mathcal{G}(\mathcal{F}(\mathrm{Gal}(L/\mathbb{Q}))) = \mathcal{G}(F)$ 因此知

$$\{I\} = \mathcal{G}(\mathcal{F}(\{I\})) \quad \text{and} \quad \mathrm{Gal}(L/\mathbb{Q}) = \mathcal{G}(\mathcal{F}(\mathrm{Gal}(L/\mathbb{Q}))).$$

Example 2.2.5. 在這個例子我們沿用 Example 2.1.6 的 extension, 即 $L = \mathbb{Q}(\alpha)$ 其中 $\alpha = \sqrt{2} + i$. 此時我們知 $\mathrm{Gal}(L/\mathbb{Q}) = \{I, \sigma_1, \sigma_2, \sigma_3\}$, 其中 $\sigma_1(\alpha) = -\alpha$, $\sigma_2(\alpha) = 3\alpha^{-1}$ 以及 $\sigma_3(\alpha) = -3\alpha^{-1}$. 另外 $L/\mathbb{Q}$ 有三個相異的 nontrivial intermediate fields, 分別為 $F_1 = \mathbb{Q}(\sqrt{2}i)$, $F_2 = \mathbb{Q}(\sqrt{2})$ 以及 $F_3 = \mathbb{Q}(i)$.

在 Example 2.1.6 我們已知 $\mathrm{Gal}(L/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ 所以 $\mathrm{Gal}(L/\mathbb{Q})$ 共有 5 個 subgroups: $\{I\}$, $\mathrm{Gal}(L/\mathbb{Q})$, $H_1 = \{I, \sigma_1\}$, $H_2 = \{I, \sigma_2\}$ 以及 $H_3 = \{I, \sigma_3\}$. 我們先探討 $\mathcal{F}$ 在這 5 個 subgroups 的取值. 首先我們已知 $\mathcal{F}(\{I\}) = L$. 對於 $\mathcal{F}(H_1)$, 由於

$$\mathcal{F}(H_1) = L^{H_1} = L^I \cap L^{\sigma_1} = L^{\sigma_1},$$

我們只要探討 σ_1 的 fixed field 即可. 不過在 Exampel 2.1.6, 我們知道 σ_1 會固定 F_1 的所有元素, 因此知 $F_1 \subseteq L^{\sigma_1}$. 如果 $F_1 \neq L^{\sigma_1}$, 即 $[L^{\sigma_1} : F_1] > 1$, 由 Lemma 1.2.3 知

$$2 = [L : F_1] = [L : L^{\sigma_1}][L^{\sigma_1} : F_1] > [L : L^{\sigma_1}],$$

這迫使 $[L : L^{\sigma_1}] = 1$, 也就是說 $L = L^{\sigma_1}$. 不過這是不可能的因為 $\alpha \in L$ 但 $\sigma_1(\alpha) = -\alpha \neq \alpha$, 也就是說 $\alpha \notin L^{\sigma_1}$. 由此矛盾知 $F_1 = L^{\sigma_1} = L^{H_1} = \mathcal{F}(H_1)$. 同理可得 $F_2 = \mathcal{F}(H_2)$ 以及 $F_3 = \mathcal{F}(H_3)$. 至於 $\mathcal{F}(\mathrm{Gal}(L/\mathbb{Q}))$, 由定義以及前面結果知

$$\mathcal{F}(\mathrm{Gal}(L/\mathbb{Q})) = L^{\mathrm{Gal}(L/\mathbb{Q})} = L^I \cap L^{\sigma_1} \cap L^{\sigma_1} \cap L^{\sigma_3} = F_1 \cap F_2 \cap F_3.$$

如果 $F_2 = F_1 \cap F_2 \cap F_3$, 表示 $F_2 \subseteq F_1 \cap F_3 \subseteq F_3$, 這是不可能的 (因為 $[F_2 : \mathbb{Q}] = [F_3 : \mathbb{Q}] = 2$, 因此 $F_2 \subseteq F_3$ 會導致 $F_2 = F_3$). 故知 $F_2 \neq F_1 \cap F_2 \cap F_3$, 也就是說 $[F_2 : \mathcal{F}(\mathrm{Gal}(L/\mathbb{Q}))] > 1$. 再次利用 Lemma 1.2.3 知

$$2 = [F_2 : \mathbb{Q}] = [F_2 : \mathcal{F}(\mathrm{Gal}(L/\mathbb{Q}))][\mathcal{F}(\mathrm{Gal}(L/\mathbb{Q})) : \mathbb{Q}] > [\mathcal{F}(\mathrm{Gal}(L/\mathbb{Q})) : \mathbb{Q}],$$

故得 $[\mathcal{F}(\mathrm{Gal}(L/\mathbb{Q})) : \mathbb{Q}] = 1$, 也就是說 $\mathcal{F}(\mathrm{Gal}(L/\mathbb{Q})) = \mathbb{Q}$. 因此我們知 $\mathcal{F}$ 這個函數對 $\mathrm{Gal}(L/\mathbb{Q})$ 的 subgroups 取值分別為:

$$\mathcal{F}(\{I\}) = L, \quad \mathcal{F}(H_1) = F_1, \quad \mathcal{F}(H_2) = F_2, \quad \mathcal{F}(H_3) = F_3 \quad \text{and} \quad \mathcal{F}(\mathrm{Gal}(L/\mathbb{Q})) = \mathbb{Q}.$$

由 Example 2.1.6 我們知

$$\mathcal{G}(L)=\{I\},\quad \mathcal{G}(F_1)=H_2,\quad \mathcal{G}(F_2)=H_2,\quad \mathcal{G}(F_3)=H_3\quad\text{and}\quad \mathcal{G}(\mathbb{Q})=\mathrm{Gal}(L/\mathbb{Q}),$$

因此我們有

$$L=\mathcal{F}(\mathcal{G}(L)),\quad F_1=\mathcal{F}(\mathcal{G}(F_1)),\quad F_2=\mathcal{F}(\mathcal{G}(F_2)),\quad F_3=\mathcal{F}(\mathcal{G}(F_3))\quad\text{and}\quad \mathbb{Q}=\mathcal{F}(\mathcal{G}(\mathbb{Q})),$$

以及

$$\begin{gathered}\{I\}=\mathcal{G}(\mathcal{F}(\{I\})),\quad H_1=\mathcal{G}(\mathcal{F}(H_2)),\quad H_2=\mathcal{G}(\mathcal{F}(H_2)),\\ H_3=\mathcal{G}(\mathcal{F}(H_3))\quad\text{and}\quad \mathrm{Gal}(L/\mathbb{Q})=\mathcal{G}(\mathcal{F}(\mathrm{Gal}(L/\mathbb{Q}))).\end{gathered}$$

以後我們會知道 $L/\mathbb{Q}$ 的 intermediate fields 只有 $\mathbb{Q}$, F_1, F_2, F_3 以及 L, 因此知 $\mathcal{G}:\mathfrak{F}\to\mathfrak{G}$ 和 $\mathcal{F}:\mathfrak{G}\to\mathfrak{F}$ 互為反函數, 也就是說 $\mathcal{G}$ 和 $\mathcal{F}$ 都是 1-1 且 onto. 這種 extension 就是所謂的 Galois Extension.

2.3. Extension Degree 和 Galois Group 的 Order 之關係

當 L/K 是 finite extension 時 $\mathrm{Gal}(L/K)$ 會是一個 finite group 而且 $\mathrm{Gal}(L/K)$ 的 order 和 L/K 的 degree 相關. 這一節中我們就是要探討 $|\mathrm{Gal}(L/K)|$ 和 $[L:K]$ 的關係.

在 Corollary 2.1.4 中我們知道當 L/K 是 finite simple extension 時, $|\mathrm{Gal}(L/K)|\leq[L:K]$. 所以知道在這情形時 $\mathrm{Gal}(L/K)$ 是一個 finite group. 事實上不需 simple 的假設, 當 L/K 是 finite extension 時 $\mathrm{Gal}(L/K)$ 必是一個 finite group.

Lemma 2.3.1. *若 L/K 是一個 finite extension, 則 $\mathrm{Gal}(L/K)$ 是一個 finite group.*

Proof. 利用 Proposition 1.3.4, 我們知存在 $a_1,\dots,a_n\in L$, 其中這些 a_i 皆 algebraic over K, 使得 $L=K(a_1,\dots,a_n)$. 由 Lemma 1.3.5, 我們知對任意 $\lambda\in L$, 皆存在 $f(x_1,\dots,x_n)\in K[x_1,\dots,x_n]$ 使得 $\lambda=f(a_1,\dots,a_n)$. 因此若 $\sigma\in\mathrm{Gal}(L/K)$, 則由於 $f(x_1,\dots,x_n)$ 的係數都在 K 中, 可得

$$\sigma(\lambda)=\sigma(f(a_1,\dots,a_n))=f(\sigma(a_1),\dots,\sigma(a_n)).$$

也就是說 σ 對 L 中元素的取值完全可由 $\sigma(a_1),\dots,\sigma(a_n)$ 來決定. 換句話說若 $\sigma,\tau\in\mathrm{Gal}(L/K)$ 且對於所有的 $i=1,\dots,n$, 皆有 $\sigma(a_i)=\tau(a_i)$, 則 $\sigma=\tau$.

當 $\sigma\in\mathrm{Gal}(L/K)$ 時, $\sigma(a_i)$ 有哪些可能的取值呢? 若 $f_i(x)\in K[x]$ 是 a_i over K 的 minimal polynomial, 且 $\deg(f_i(x))=m_i$, 則由於

$$f_i(\sigma(a_i))=\sigma(f_i(a_i))=\sigma(0)=0,$$

我們知 $\sigma(a_i)$ 仍為 $f_i(x)$ 在 L 中的一個根. 因此每個 $\sigma(a_i)$ 最多只有 m_i 個選擇. 所以對任何 $\sigma\in\mathrm{Gal}(L/K)$ 這些 $\sigma(a_1),\dots,\sigma(a_n)$ 最多有 $m_1\cdots m_n$ 種選擇, 故知 $\mathrm{Gal}(L/K)$ 最多只能有 $m_1\cdots m_n$ 個元素. $\square$

要注意如果 $f_i(x)$ 在 L 中有 s_i 個根, 並不能像 simple extension 的情況得到 $|\mathrm{Gal}(L/K)|=s_1\cdots s_n$. 這是因為任意給定 $\alpha_1,\dots,\alpha_n\in L$ 分別為 $f_1(x)=0,\dots,f_n(x)$ 在 L 的根, 並不能保證存在 $\sigma\in\mathrm{Gal}(L/K)$ 會同時滿足 $\sigma(a_1)=\alpha_1,\dots,\sigma(a_n)=\alpha_n$.

利用 Corollary 2.1.4 以及 induction 我們可以推導出, 若 L/K 是 finite extension, 則 $|\mathrm{Gal}(L/K)| \leq [L:K]$. 例如若 $L = K(a_1, a_2)$, 我們令 $F = K(a_1)$, 則知 $L = F(a_2)$. 因此由 L/F 和 F/K 都是 finite simple extensions, 利用 Corollary 2.1.4 可得

$$|\mathrm{Gal}(L/F)|\,|\mathrm{Gal}(F/K)| \leq [L:F][F:K] = [L:K].$$

接著我們只要再探討 $|\mathrm{Gal}(L/K)|$ 和 $|\mathrm{Gal}(L/F)|\,|\mathrm{Gal}(F/K)|$ 的關係就可得所要的結論. 要得到 $|\mathrm{Gal}(L/K)|$ 和 $|\mathrm{Gal}(L/F)|\,|\mathrm{Gal}(F/K)|$ 的關係其實並不直接, 不過由於我們想更精準的得到 Galois groups 和 fixed fields 之間的關係, 在此我們就不去探討而選擇另外的方法來處理.

既然 $[L:K]$ 是用 vector space 的 dimension 來定義, 要找到 $|\mathrm{Gal}(L/K)|$ 和 $[L:K]$ 的關係, 我們也要想辦法將 $\mathrm{Gal}(L/K)$ 和 vector space 扯上關係. 我們考慮的 vector space 是所有從 L 到 L 的函數所成的集合, 即考慮 $V = \{f : L \to L\}$. 雖然 $\mathrm{Gal}(L/K)$ 中的元素不只是 L 到 L 的函數, 還必須是 ring homomorphism 且是 1-1 and onto, 不過兩個 ring homomorphisms 相加有可能不再是 ring homomorphism, 而兩個 1-1 and onto 的函數相加也可能不再是 1-1 and onto. 所以我們不能考慮所有 ring homomorphisms 所成的集合, 也不能考慮所有 1-1 and onto 的函數所成的集合. 它們都無法保持加法封閉, 當然無法形成 vector space. 因此我們必須把條件放寬到考慮所有 L 到 L 的函數. 這時候對於 $f, g \in V$ 和 $c \in L$, 若我們定義 $f+g$ 和 $c \cdot f$ 這兩個函數為: 對任意 $\lambda \in L$, $f+g$ 這個函數在 λ 的取值為 $f(\lambda)+g(\lambda)$ (即 $(f+g)(\lambda) = f(\lambda)+g(\lambda)$); 而 $c \cdot f$ 這個函數在 λ 的取值為 $c \cdot f(\lambda)$ (即 $(c \cdot f)(\lambda) = c \cdot f(\lambda)$), 則很容易看出 $f+g$ 和 $c \cdot f$ 仍為 L 到 L 的函數 (即 $f+g, c \cdot f \in V$), 且 V 確實為一個 over L 的 vector space.

Lemma 2.3.2. *假設 L 為一個 field 且 $\sigma_1, \ldots, \sigma_n \in \mathrm{Aut}(L)$ 為一組兩兩相異的 L 的 automorphisms. 若考慮 $\sigma_1, \ldots, \sigma_n$ 是 $V = \{f : L \to L\}$ 這個 vector space over L 的元素, 則 $\sigma_1, \ldots, \sigma_n$ 是 linearly independent over L.*

Proof. 考慮 $W = \langle \sigma_1, \ldots, \sigma_n \rangle$ 為以 $\sigma_1, \ldots, \sigma_n$ over L span 而成的 subspace of V. 既然 $\sigma_1, \ldots, \sigma_n$ 可展成 W, 要證明 $\sigma_1, \ldots, \sigma_n$ 是 linearly independent over L, 只要證明 $\dim_L(W) = n$ 即可.

我們用反證法. 假設 $\dim_L(W) = l < n$, 由線性代數的性質知可在 $\sigma_1, \ldots, \sigma_n$ 中找到 l 個元素成為 W over L 的一組 basis. 經過重排, 我們假設 $\sigma_1, \ldots, \sigma_l$ 就是 W over L 的一組 basis. 因為 $\sigma_n \in W$, 利用 basis 的性質, 我們知道存在唯一的一組 $c_1, \ldots, c_l \in L$ 使得

$$\sigma_n = c_1 \cdot \sigma_1 + \cdots + c_l \cdot \sigma_l. \tag{2.2}$$

因為 σ_n 不為 0 函數, 一定存在一 $c_i \in \{c_1, \ldots, c_l\}$ 滿足 $c_i \neq 0$, 為了方便記, 我們就假設 $c_1 \neq 0$. 由於 $\sigma_1 \neq \sigma_n$, 必存在 $\lambda \in L$ 使得 $\sigma_1(\lambda) \neq \sigma_n(\lambda)$. 注意因為 σ_1 和 σ_n 是 ring homomorphism, 所以 $\lambda \neq 0$ (否則會造成 $\sigma_1(\lambda) = 0 = \sigma_n(\lambda)$). 現在對任意 $\beta \in L$, 我們將

$\lambda\beta$ 代入 σ_n 以及 $c_1\cdot\sigma_1+\cdots+c_l\cdot\sigma_l$ 中, 由於它們是相等的函數, 我們得

$$\begin{aligned}\sigma_n(\lambda)\sigma_n(\beta) &= \sigma_n(\lambda\beta)\\ &= c_1\cdot\sigma_1(\lambda\beta)+\cdots+c_l\cdot\sigma_l(\lambda\beta)\\ &= c_1\cdot\sigma_1(\lambda)\sigma_1(\beta)+\cdots+c_l\cdot\sigma_l(\lambda)\sigma_l(\beta)\end{aligned}$$

因為 σ_n 是 ring isomorphism 且 $\lambda\neq 0$, 我們知 $\sigma_n(\lambda)\neq 0$. 上式兩邊同除 $\sigma_n(\lambda)$, 得

$$\sigma_n(\beta)=\frac{c_1\cdot\sigma_1(\lambda)}{\sigma_n(\lambda)}\sigma_1(\beta)+\cdots+\frac{c_l\cdot\sigma_l(\lambda)}{\sigma_n(\lambda)}\sigma_l(\beta).$$

由於這個等式是對所有 $\beta\in L$ 都成立, 所以看成 L 到 L 的函數, 我們有

$$\sigma_n=\frac{c_1\cdot\sigma_1(\lambda)}{\sigma_n(\lambda)}\cdot\sigma_1+\cdots+\frac{c_l\cdot\sigma_l(\lambda)}{\sigma_n(\lambda)}\cdot\sigma_l. \tag{2.3}$$

由於 $\sigma_1(\lambda)\neq\sigma_n(\lambda)$ 且 $c_1\neq 0$, 故知

$$\frac{c_1\cdot\sigma_1(\lambda)}{\sigma_n(\lambda)}\neq c_1.$$

比較 (2.2) 和 (2.3) 兩式, 我們得到 $\sigma_n\in W$ 有兩種不同用 $\sigma_1,\ldots,\sigma_l$ 的線性組合的表示法. 這和 $\sigma_1,\ldots,\sigma_l$ 是 W 的一組 basis 相違背, 故知 $\dim_L(W)=l=n$. □

當 L/K 是一個 finite extension, 由 Lemma 2.3.1 我們知 $\mathrm{Gal}(L/K)$ 是 $\mathrm{Aut}(L)$ 中的一個 finite subgroup, 再利用 Lemma 2.3.2 知 $\mathrm{Gal}(L/K)$ 的元素是 linearly independent over L. 由此我們可推得以下重要的性質.

Proposition 2.3.3. *假設 L/K 是一個 finite extension, 則*

$$|\mathrm{Gal}(L/K)|\leq[L:K].$$

Proof. 假設 $\mathrm{Gal}(L/K)=\{\sigma_1,\ldots,\sigma_n\}$ 以及 $a_1,\ldots,a_m\in L$ 是 L/K 的一組 basis. 我們利用反證法: 即假設 $n>m$ 而推得矛盾. 對於任意的 $i\in\{1,\ldots,n\}$, $j\in\{1,\ldots,m\}$, 由於 $\sigma_i\in\mathrm{Aut}(L)$ 且 $a_j\in L$, 我們有 $\sigma_i(a_j)\in L$. 因此可以考慮以下係數在 L 的 n 個變數, m 個線性方程式的聯立方程式:

$$\left\{\begin{array}{rcl}\sigma_1(a_1)x_1+\sigma_2(a_1)x_2+\cdots+\sigma_n(a_1)x_n &=& 0\\ \sigma_1(a_2)x_1+\sigma_2(a_2)x_2+\cdots+\sigma_n(a_2)x_n &=& 0\\ \vdots & & \vdots\\ \sigma_1(a_m)x_1+\sigma_2(a_m)x_2+\cdots+\sigma_n(a_m)x_n &=& 0\end{array}\right. \tag{2.4}$$

因為變數的個數 n 大於方程式的個數 m, 由線性代數知在 L 中必存在一組不全為 0 的解 $c_1,\ldots,c_n\in L$ 使得 $x_1=c_1,\ldots,x_n=c_n$ 滿足聯立方程式 (2.4). 也就是說

$$c_1\sigma_1(a_j)+c_2\sigma_2(a_j)+\cdots+c_n\sigma_n(a_j)=0,\ \forall\, j\in\{1,\ldots,m\}. \tag{2.5}$$

現因為 $a_1,\ldots,a_m$ 是 L/K 的一組 basis, 對任意 $\lambda\in L$ 都存在一組 $r_1,\ldots,r_m\in K$ 使得 $\lambda=r_1a_1+\cdots+r_ma_m$. 若將 λ 代入 $c_1\cdot\sigma_1+\cdots+c_n\cdot\sigma_n$ 這個函數中可得:

$$\begin{aligned}(c_1\cdot\sigma_1+\cdots+c_n\cdot\sigma_n)(\lambda) &= c_1\cdot\sigma_1(\lambda)+\cdots+c_n\cdot\sigma_n(\lambda)\\ &= c_1\cdot\sigma_1(\sum_{j=1}^m r_ja_j)+\cdots+c_n\cdot\sigma_n(\sum_{j=1}^m r_ja_j)\\ &= \sum_{j=1}^m c_1\sigma_1(r_ja_j)+\cdots+c_n\sigma_n(r_ja_j).\end{aligned}$$

由於 $\sigma_i\in\mathrm{Gal}(L/K)$ 將 K 中的元素都固定以及式子 (2.5), 我們得

$$\begin{aligned}\sum_{j=1}^m c_1\sigma_1(r_ja_j)+\cdots+c_n\sigma_n(r_ja_j) &= \sum_{j=1}^m c_1r_j\sigma_1(a_j)+\cdots+c_nr_j\sigma_n(a_j)\\ &= \sum_{j=1}^m r_j(c_1\sigma_1(a_j)+\cdots+c_n\sigma_n(a_j))\\ &= 0.\end{aligned}$$

也就是說對任意 $\lambda\in L$ 代入 $c_1\cdot\sigma_1+\cdots+c_n\cdot\sigma_n$ 這個函數後都得到 0, 故得 $c_1\cdot\sigma_1+\cdots+c_n\cdot\sigma_n$ 是一個零函數 (即 $c_1\cdot\sigma_1+\cdots+c_n\cdot\sigma_n=0$). 由於 $c_1,\ldots,c_n\in L$ 是 L 中一組不全為 0 的數, $c_1\cdot\sigma_1+\cdots+c_n\cdot\sigma_n=0$ 和 Lemma 2.3.2 所知 $\sigma_1,\ldots,\sigma_n$ 是 linearly independent over L 相矛盾, 故得證 $|\mathrm{Gal}(L/K)|=n\leq m=[L:K]$. □

利用類似的方法, 我們可以得到以下更好的結果, 讓我們更清楚 Galois group 和 fixed field 之間的關係.

Theorem 2.3.4. *假設 L/K 是一個 finite extension 且 H 是 $\mathrm{Gal}(L/K)$ 的 subgroup. 則*

$$|H|=[L:\mathcal{F}(H)].$$

Proof. 回顧一下 $\mathcal{F}(H)=L^H$ 是 H 的 fixed field 而且是 L/K 的 intermediate field. 若考慮 $L/\mathcal{F}(H)$ 這一個 extension, 當然也是 finite extension, 故套用 Proposition 2.3.3, 得 $|\mathrm{Gal}(L/\mathcal{F}(H))|\leq[L:\mathcal{F}(H)]$. 依定義 $\mathrm{Gal}(L/\mathcal{F}(H))=\mathcal{G}(\mathcal{F}(H))$, 故由 Proposition 2.2.3 知 $H\subseteq\mathrm{Gal}(L/\mathcal{F}(H))$, 而得

$$|H|\leq|\mathrm{Gal}(L/\mathcal{F}(H))|\leq[L:\mathcal{F}(H)].$$

假設 $|H|=n$, 若我們能證明任取 L 中 $n+1$ 個元素必定 linearly dependent over $\mathcal{F}(H)$, 則知 $[L:\mathcal{F}(H)]\leq n=|H|$. 故得證 $|H|=[L:\mathcal{F}(H)]$.

假設 $H=\{\tau_1,\ldots,\tau_n\}$, 其中 $\tau_1=I$ 是 identity. 任取 $a_1,\ldots,a_{n+1}\in L$, 我們欲證明 $a_1,\ldots,a_{n+1}$ 是 linearly dependent over $\mathcal{F}(H)$. 首先我們考慮以下係數在 L 的 $n+1$ 個變數, n 個線性方程式的聯立方程式:

$$\left\{\begin{array}{rcl}\tau_1(a_1)x_1+\tau_1(a_2)x_2+\cdots+\tau_1(a_{n+1})x_{n+1} &=& 0\\ \tau_2(a_1)x_1+\tau_2(a_2)x_2+\cdots+\tau_2(a_{n+1})x_{n+1} &=& 0\\ \vdots & & \vdots\\ \tau_n(a_1)x_1+\tau_n(a_2)x_2+\cdots+\tau_n(a_{n+1})x_{n+1} &=& 0\end{array}\right. \tag{2.6}$$

注意因 $\tau_1 = I$ 所以聯立方程式 (2.6) 中的第一個式子其實是

$$a_1x_1 + a_2x_2 + \cdots + a_{n+1}x_{n+1} = 0.$$

若我們能證明聯立方程式 (2.6) 在 $\mathcal{F}(H)$ 中存在一組不全為 0 的解 $c_1, \ldots, c_{n+1} \in \mathcal{F}(H)$, 則得

$$c_1a_1 + c_2a_2 + \cdots + c_{n+1}a_{n+1} = 0,$$

故知 $a_1, \ldots, a_{n+1}$ 是 linearly dependent over $\mathcal{F}(H)$.

現由於聯立方程式 (2.6) 變數的個數 $n+1$ 大於方程式的個數 n, 由線性代數知在 L 中必存在一組不全為 0 的解. 我們考慮所有聯立方程式 (2.6) 的解中不等於 0 的項數最少的一組解. 經過重排我們假設 $x_1 = b_1, \ldots, x_{n+1} = b_{n+1}$ 是聯立方程式 (2.6) 的一組解, 其中這些 $b_i \in L$ 且 $b_1, \ldots, b_m \neq 0$ 以及 $b_{m+1}, \ldots, b_{n+1} = 0$. 依我們的找法知若在 L 中找到一組解且其不等於 0 的項數少於 m, 則這一組解必全等於 0. 又因為 $b_1 \neq 0$, 且聯立方程式 (2.6) 是線性的, 同除以 b_1 我們知

$$x_1 = 1, x_2 = b_2/b_1, \ldots, x_m = b_m/b_1, x_{m+1} = 0, \ldots, x_{n+1} = 0$$

仍然是聯立方程式 (2.6) 的一組不全為 0 的解. 為了方便我們將 b_i/b_1 記為 c_i, 也就是說我們有以下的等式:

$$\left\{\begin{array}{rcl} \tau_1(a_1) + \tau_1(a_2)c_2 + \cdots + \tau_1(a_m)c_m & = & 0 \\ \tau_2(a_1) + \tau_2(a_2)c_2 + \cdots + \tau_2(a_m)c_m & = & 0 \\ \vdots & & \vdots \\ \tau_n(a_1) + \tau_n(a_2)c_2 + \cdots + \tau_n(a_m)c_m & = & 0 \end{array}\right. \tag{2.7}$$

這些 $c_2, \ldots, c_m$ 是在 L 中皆不為 0 的數, 我們要證明這些 $c_2, \ldots, c_m$ 事實上是在 $\mathcal{F}(H)$ 中. 依定義 $\mathcal{F}(H)$ 是被所有 H 的元素固定的 L 中的元素所成的集合, 因此要證明 $c_i \in \mathcal{F}(H)$, 我們只要證明對任意 $\tau \in H$ 皆有 $\tau(c_i) = c_i$. 所以對任意 $\tau \in H$ 我們將之作用於式子 (2.7) 中的每一個式子得到對任意 $j \in \{1, \ldots, n\}$, 皆有

$$\begin{array}{rcl} 0 & = & \tau(\tau_j(a_1) + \tau_j(a_2)c_2 + \cdots + \tau_j(a_m)c_m) \\ & = & \tau(\tau_j(a_1)) + \tau(\tau_j(a_2))\tau(c_2) + \cdots + \tau(\tau_j(a_m))\tau(c_m) \\ & = & \tau \circ \tau_j(a_1) + \tau \circ \tau_j(a_2)\tau(c_2) + \cdots + \tau \circ \tau_j(a_m)\tau(c_m) \end{array}$$

由於 H 是一個 group 且 $\tau \in H$, 故對任意 $j = \{1, \ldots, n\}$ 皆存在唯一的 $j' \in \{1, \ldots, n\}$ 滿足 $\tau \circ \tau_j = \tau_{j'}$. 因此我們可以將上式改寫成

$$\tau_{j'}(a_1) + \tau_{j'}(a_2)\tau(c_2) + \cdots + \tau_{j'}(a_m)\tau(c_m) = 0.$$

再加上若 $j \neq k$, 則 $\tau \circ \tau_j \neq \tau \circ \tau_k$, 因此當 j 跑遍所有的 $1, \ldots, n$ 時, 所對應的 j' 也跑遍所有的 $1, \ldots, n$. 因此上式的是對任意的 $j' \in \{1, \ldots, n\}$ 都成立的, 也就是說我們有以下的等式:

$$\left\{\begin{array}{rcl} \tau_1(a_1) + \tau_1(a_2)\tau(c_2) + \cdots + \tau_1(a_m)\tau(c_m) & = & 0 \\ \tau_2(a_1) + \tau_2(a_2)\tau(c_2) + \cdots + \tau_2(a_m)\tau(c_m) & = & 0 \\ \vdots & & \vdots \\ \tau_n(a_1) + \tau_n(a_2)\tau(c_2) + \cdots + \tau_n(a_m)\tau(c_m) & = & 0 \end{array}\right.$$

換言之對任意 $\tau \in H$,

$$x_1 = 1, x_2 = \tau(c_2), \ldots, x_m = \tau(c_m), x_{m+1} = 0, \ldots, x_{n+1} = 0$$

是聯立方程式 (2.6) 的一組解. 由於

$$x_1 = 1, x_2 = c_2, \ldots, x_m = c_m, x_{m+1} = 0, \ldots, x_{n+1} = 0$$

已是聯立方程式 (2.6) 的一組解且聯立方程式 (2.6) 是線性的, 所以知

$$x_1 = 1 - 1 = 0, x_2 = c_2 - \tau(c_2), \ldots, x_m = c_m - \tau(c_m), x_{m+1} = 0, \ldots, x_{n+1} = 0$$

也是聯立方程式 (2.6) 的一組解. 很顯然的這一組解不等於 0 的項數少於 m, 但當初我們假設 m 是所有不全為 0 的解中不為 0 的項數最少的. 因此知這組解應全為 0, 也就是說 $\tau(c_2) = c_2, \ldots, \tau(c_m) = c_m$. 又這是對任意 $\tau \in H$ 都成立的, 故得 $c_2, \ldots, c_m \in \mathcal{F}(H)$. 故再由 $c_2, \ldots, c_m \neq 0$ 以及 $a_1 + c_2a_2 + \cdots + c_ma_m = 0$, 知 $a_1, \ldots, a_m$ 是 linearly dependent over $\mathcal{F}(H)$. 所以當然 $a_1, \ldots, a_m, \ldots, a_{n+1}$ 是 linearly dependent over $\mathcal{F}(H)$, 得證本定理. $\square$

利用 Theorem 2.3.4 我們馬上可推導出一些有用的性質.

Corollary 2.3.5. *假設 L/K 是一個 finite extension 且 H 是* $\mathrm{Gal}(L/K)$ *的 subgroup, 則*

$$[\mathcal{F}(H) : K] = [L : K]/|H|.$$

Proof. 由於 $K \subseteq \mathcal{F}(H) \subseteq L$, 利用 Lemma 1.2.3 我們知 $[L : K] = [L : \mathcal{F}(H)][\mathcal{F}(H) : K]$. 再利用 Theorem 2.3.4 我們知 $[L : \mathcal{F}(H)] = |H|$, 故得證. $\square$

Corollary 2.3.6. *假設 L/K 是一個 finite extension 且 H 是* $\mathrm{Gal}(L/K)$ *的 subgroup, 則*

$$\mathcal{G}(\mathcal{F}(H)) = H.$$

Proof. 由 Proposition 2.2.3 我們知 $H \subseteq \mathcal{G}(\mathcal{F}(H))$, 因此若要證得 $H = \mathcal{G}(\mathcal{F}(H))$ 只要檢查是否 $|H| = |\mathcal{G}(\mathcal{F}(H))|$. 由於 $\mathcal{G}(\mathcal{F}(H))$ 仍為 $\mathrm{Gal}(L/K)$ 的 subgroup, 故由 Theorem 2.3.4 知 $|\mathcal{G}(\mathcal{F}(H))| = [L : \mathcal{F}(\mathcal{G}(\mathcal{F}(H)))]$. 又由於 $\mathcal{F}(\mathcal{G}(\mathcal{F}(H))) = \mathcal{F}(H)$ (Proposition 2.2.3) 故知 $|\mathcal{G}(\mathcal{F}(H))| = [L : \mathcal{F}(H)] = |H|$. 得證 $\mathcal{G}(\mathcal{F}(H)) = H$. $\square$

回顧一下, 當 L/K 是一個 finite extension, 我們令 $\mathfrak{F}$ 是 L/K 的 intermediate fields 所成的集合且令 $\mathfrak{G}$ 是 $\mathrm{Gal}(L/K)$ 的 subgroups 所成的集合, 而 $\mathcal{G} : \mathfrak{F} \to \mathfrak{G}$ 是一個從 $\mathfrak{F}$ 到 $\mathfrak{G}$ 的函數, 且 $\mathcal{F} : \mathfrak{G} \to \mathfrak{F}$ 是一個從 $\mathfrak{G}$ 到 $\mathfrak{F}$ 的函數. Corollary 2.3.6 告訴我們當 $H \in \mathfrak{G}$ 時 $\mathcal{G}(\mathcal{F}(H)) = H$, 也就是說 $\mathcal{G} \circ \mathcal{F} : \mathfrak{G} \to \mathfrak{G}$ 是一個從 $\mathfrak{G}$ 送到 $\mathfrak{G}$ 的 identity map. 因此我們知 $\mathcal{F}$ 這個函數是 1-1 (因為若 $\mathcal{F}(H_1) = \mathcal{F}(H_2)$, 將之代入 $\mathcal{G}$ 得 $H_1 = H_2$) 而 $\mathcal{G}$ 是 onto (對任意 $H \in \mathfrak{G}$, 取 $F = \mathcal{F}(H) \in \mathfrak{F}$, 可得 $\mathcal{G}(F) = H$). 在 Example 2.1.5 中我們知一般來說 $\mathcal{G}$ 不一定是 1-1, 以後我們將探討何時 $\mathcal{G}$ 會是 1-1.