簡介 Galois 理論

李華介

國立台灣師範大學數學系

前言

本講義主要目的是要簡單的介紹 Galois 理論. 涉及的層面只是 Galois 理論的基本概念, 並不談其應用及推廣. 我們所需的預備知識是基本的線性代數及我的大學基礎代數講義中的第三部份 “Fields”. 這些預備知識基本上在本講義中是不會再給證明, 不過若牽涉一些概念上的問題我們會將其概念再詳述一遍.

Contents

前言 v

Chapter 1. Field Extensions 1

§1.1. 有關 Field Extension 的觀念 1

§1.2. Field Extension 的 Degree 4

§1.3. Field Extensions 的分類 5

Chapter 2. Galois Group 和 Fixed Field 11

§2.1. Galois Group 11

§2.2. Fixed Field 17

§2.3. Extension Degree 和 Galois Group 的 Order 之關係 20

Chapter 3. Normal Extension 和 Separable Extension 27

§3.1. Splitting Field 27

§3.2. Normal Extension 32

§3.3. Separable Polynomial 39

§3.4. Separable Extension 44

Chapter 4. Galois Extension 49

§4.1. Fundamental Theorem of Galois Theory 49

§4.2. Galois 理論的應用 55

§4.3. Galois 理論的例子 59

Chapter 1

Field Extensions

在本章中我們將回顧一些有關 field extension 的基本性質並介紹其和 Galois theory 相關的一些概念.

1.1. 有關 Field Extension 的觀念

在這一節中我們希望說明一些觀念, 這些觀念說實話不容易講清楚, 如果同學無法完全了解也沒有關係, 可以依你所知的概念繼續研讀以下其他的章節. 等到對這些理論有更深一層的體認後或許就能慢慢體會這些觀念了.

在談論 field extension 時有一個很重要的定理, 這個定理是說: 如果 K 是一個 field, $p(x) \in K[x]$ 是一個 irreducible polynomial, 則必存在一個 K 的 extension field L 使得 $p(x) = 0$ 在 L 中有解 (參見大學基礎代數講義 Theorem 10.3.4). 這個定理的證明大致上就是取 $L = K[x]/(p(x))$ 這個 field, 而 $a = \overline{x} \in L$ 就是 $p(x)$ 的一個根. 第一次看到這個證明大部分的同學會對這個簡單的證明充滿了疑惑, 大致上會有兩個疑問:

(1) 怎麼找一個多項式的根那麼簡單? 為什麼高中時還要學那麼多解多項式方程式的方法?

(2) 這裡的 K 真的包含於 $L = K[x]/(p(x))$ 嗎? $\overline{x}$ 真的是 $p(x) = 0$ 的一個解嗎?

第一個問題比較好回答. 這個定理主要是存在性問題: 只要求找到一個 field 使的 $p(x) = 0$ 在那個 field 中有解. 而從前高中找解是要求在特定的 field 中找解 (如 實數 $\mathbb{R}$ 或 複數 $\mathbb{C}$) 當然有其困難度. 別忘了這個世界不只有 $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ 這三個 fields.

至於第二個問題較難回答, 我們用一個例子說明一下. 我們都知道 $x^3 - 2$ 是 $\mathbb{Q}[x]$ 中的一個 irreducible polynomial. 如何找到一個 field 使得 $x^3 - 2 = 0$ 在其中有解呢? 假設你不知道這世上有 $\mathbb{R}$ 和 $\mathbb{C}$ 這個 field, 你會怎麼辦?

代數的方法就是先憑空找一個符號 a 假設是 $x^3 - 2$ 的根 (即 a 滿足 $a^3 = 2$). 因為要找到一個 field L 使得 a 和 $\mathbb{Q}$ 都在裡面, 所以我們要求 a 和 $\mathbb{Q}$ 的元素都相互運算後仍在 L 中. 當然 $\mathbb{Q}$ 本身的運算還要保持, 所以我們只要注意 a 本身的自己的運算以及 a 和 $\mathbb{Q}$ 的

運算即可. 首先對任意的 $r \in \mathbb{Q}$, $r+a$ 和 $r \cdot a$ 到底是什麼呢? 當 $r = 0$ 時 $r+a$ 和 $r \cdot a$ 當然須分別等於 a 和 0 這樣才能滿足結合率和分配率. 同樣的在結合率和分配率的要求之下當 $r \neq 0$ 時 $r+a$ 和 $r \cdot a$ 都不能屬於 $\mathbb{Q}$, 所以我們的 L 中還必須包含 $r+a$ 和 $r \cdot a$ 這兩種符號 (注意這仍只是符號而不是任何的數). 這裡要注意的是我們為了保持 1 仍為乘法單位元素所以必須把 $1 \cdot a$ 和 a 視為相同. 接下來我們看 a 本身的運算: $a+a$ 和 $a \cdot a$ 應該是多少呢? 在要求分配率仍成立的前提下由於 $a + a = 1 \cdot a + 1 \cdot a = (1+1) \cdot a = 2 \cdot a$, 我們不需要新的符號來代表 $a+a$, 它就是 $2 \cdot a$ (簡記為 $2a$). 同樣的任意 n 個 a 相加就是 $n \cdot a$. 至於 $a \cdot a$ 我們就需要新的符號, 按慣例就沿用指數的符號將 $a \cdot a$ 記為 a^2, 同樣的任意 n 個 a 相乘就記為 a^n. L 中若僅有這些符號還不夠成為一個 field (甚至連 ring 都不行), 我們還需要這些符號間的相加相乘. 很快的在分配率, 結合率以及交換率皆須符合的要求下我們發現 L 中必須有

$$r_0 + r_1 \cdot a + r_2 \cdot a^2 + \cdots + r_n \cdot a^n$$

這些符號, 其中 n 是任意非負整數, 而 $r_0, \ldots, r_n \in \mathbb{Q}$. 同樣的因為前述規律的要求這些符號之間的相加相乘就和多項式之間的相加相乘一樣 (現在應該可以看出前面那個定理的證明為何會和 $K[x]$ 這個 polynomial ring 有關了吧). 事實上, 我們不需要這麼多符號: 這是因為我們要求 $a^3 = 2$, 所以 $a^4 = 2a$, $a^5 = 2a^2, \ldots$ 這樣一直下去我們發現前面那些符號都可以用

$$r_0 + r_1 \cdot a + r_2 \cdot a^2$$

表示即可. 只用這些次數小於 3 的符號不止所用的符號少, 最重要的是它們的表法唯一. 換言之, 任兩個次數小於 3 的符號只要不相同它們就代表不同的數. 這方面前面任意次數的符號就沒有這優點 (比方說 $a^4 = 2a$). 令一方面它們又足夠代表所有的符號: 這是因為 $\mathbb{Q}$ 是一個 field 我們可以用長除法 (Euclid's Algorithm 參見大學基礎代數講義 Theorem 7.2.4) 對任意 $f(x) \in \mathbb{Q}[x]$ 都可找到 $h(x), r(x) \in \mathbb{Q}[x]$ 使得 $f(x) = (x^3 - 2)h(x) + r(x)$ 其中 $r(x) = 0$ 或其次數小於 3. 所以對任意的 $f(a)$ 我們都可以用 $r(a)$ 來表示 (現在大家應該可以看出當初為何會考慮 $L = K[x]/(p(x))$ 了). 只用到次數小於 3 的符號, 當定義加法時仍延用多項式的加法不會出問題 (因為兩次數小於 3 的多項式相加仍次數小於 3); 但是定義乘法若相乘後次數大於等於 3 怎麼辦? 當然我們就用上述長除法將次數大於等於 3 的符號用次數小於 3 的符號來表示了 (大家可以看出這裡的運算完全和 $\mathbb{Q}[x]/(x^3 - 2)$ 的運算相同). 所以集合

$$R = \{r_0 + r_1 \cdot a + r_2 \cdot a^2 \,|\, r_0, r_1, r_2 \in \mathbb{Q}\}$$

在前述的運算之下就是包含 a 和 $\mathbb{Q}$ 且滿足 $a^3 = 2$ 最小的 ring. 事實上 R 會是一個 field, 這是由於若 $f(x) \neq 0$, $f(x) \in \mathbb{Q}[x]$ 且 $\deg(f(x)) < 3$, 則因 $x^3 - 2$ 是 $\mathbb{Q}[x]$ 的 irreducible polynomial, $f(x)$ 和 $x^3 - 2$ 必互質. 故由輾轉相除法 (或由 $\mathbb{Q}[x]$ 是一個 principle ideal domain 參見大學基礎代數講義 Theorem 7.2.6) 知存在 $g(x), h(x) \in \mathbb{Q}[x]$ 其中 $\deg(g(x)) < 3$, 使得 $f(x)g(x) + (x^3 - 2)h(x) = 1$; 亦即 $f(a) \cdot g(a) = 1$. 也就是說對任意 $f(a) \neq 0$ 且 $f(a) \in R$ 皆存在 $g(a) \in R$ 使得 $f(a) \cdot g(a) = 1$. 所以 $L = R$ 就是我們要找的 field. 現在可以相信 $\mathbb{Q} \subseteq L$ 且 $a \in L$ 是 $x^3 - 2$ 的一個根了吧! 大家應該也可以看出這個 L 和

$\mathbb{Q}[x]/(x^3-2)$ 是 isomorphic. 但是要描述這個 L 裡元素間的運算多複雜啊! 還不如直接用 $\mathbb{Q}[x]/(x^3-2)$ 表示更簡明扼要.

了解了找到 extension 使的 x^3-2 有根的建構方法後, 大家或許會有新的疑問: 我們都知道 x^3-2 有 3 個根分別是

$$\sqrt[3]{2}, \quad \sqrt[3]{2}\,(\frac{-1+\sqrt{3}i}{2}) \quad \text{和} \quad \sqrt[3]{2}\,(\frac{-1-\sqrt{3}i}{2}),$$

前面創造出的 a 到底是哪一個呢? 事實上都可以, 就看你怎樣把 a 送到 $\mathbb{C}$ 了. 你可以任取上述三個複數之一和 $\mathbb{Q}$ 中元素進行運算, 你會發現和 a 與 $\mathbb{Q}$ 中元素運算相同. 所以若有另一個人用 b 來表示 x^3-2 的一個根, 然後用前述方法造出一個 field, 你不能說 $a=b$ 但是可以肯定的是這兩個 field 是 isomorphic (都 isomorphic to $\mathbb{Q}[x]/(x^3-2)$).

或許你會有另一個疑問: 從上述觀點 x^3-2 會有無窮多個根啊! 這不是和我們所認知的一個 n 次多項式至多有 n 個根 (大學基礎代數講義 Theorem 10.3.3) 相衝突嗎? 其實不然, 仔細看看大學基礎代數講義 Theorem 10.3.3 它其實是說在一個固定的 field 中至多有 n 個根. 這是一個很重要的概念: 在 Galois 理論中我們是要在一個固定的 field 中談問題. 雖然 field 是固定的但我們較不在意根長什麼樣子, 而重視的是在這 field 有幾個根. 例如 x^3-2 在 $\mathbb{C}$ 中有三個相異根, 我們就得知有三種方法將 a 送到 $\mathbb{C}$ 中. 又例如 x^3-2 在 $\mathbb{Q}(\sqrt[3]{2})$ 中僅有一個根 (因為 $\mathbb{Q}(\sqrt[3]{2})$ 中的元素都是實數, 但 x^3-2 在 $\mathbb{C}$ 中其他兩個根是虛數) 所以我們知道將 a 送到 $\mathbb{C}$ 後所得的三個 fields 是相異的.

從上述的情況得知, 有些代數的性質和它的元素在於哪個 field 其實是無關的, 不過有時將之擺在一個固定的 field 中討論確有其方便性. 就例如對於 irreducible polynomial $p(x)\in K[x]$ 我們考慮 $L=K[x]/(p(x))$ 使得 $p(x)$ 在 L 中有根. 在這裡 K 其實並不是真正包含於 L 中, 我們只是找到一個一對一的 ring homomorphism 將 K 送到 L 中. 因為這時候這個 ring homomorphism 的像 (image) 和 K 的代數結構是一樣的而且是 L 的 subfield 所以我們就視同 K 包含於 L. 事實上我們有以下一個比較正式的定義:

Definition 1.1.1. 假設 K 和 L 都是 fields 且 K 和 L 間存在一對一的 ring homomorphism $i: K\to L$, 則稱 L 是 K 的 extension. 通常我們會記作 L/K (唸成 L over K).

簡單來說就是當 K 並不包含於 L 時, 我們當然不能直接對 K 的元素和 L 的元素做運算. 不過如果存在一對一的 ring homomorphism $i: K\to L$, 那麼對任意的 $k\in K$ 和 $l\in L$, 我們可以定

$$k+l := i(k)+l \quad \text{and} \quad k\cdot l := i(k)\cdot l,$$

因為 $i(k)\in L$ 所以自然可以和 L 中的元素做運算了. 又因為 i 是一對一的, i 的像 $i(K)=\{i(k)\,|\,k\in K\}$ 中的元素和 K 中的元素有一個一對一的對應關係. 因此我們可以將 K 中的元素 ($k\in K$) 看成是是 L 的元素 ($i(k)\in L$). 也就是說我們將 K "identify" 成 L 的一個 subfield. 因此從今以後我們若提到 L 是 K 的 extension 為了方便我們還是省略提及存在一個 $i: K\to L$, 而直接假設 $K\subseteq L$.

Galois 理論簡單的說就是探討 field extensions 間的關係. 給定一個 field K, 事實上存在無窮多個 K 的 extensions, 我們自然會問兩個 extensions L_1/K 和 L_2/K 在什麼條件之

下可以看成是一樣的 extension 呢？這不是單純的兩個 fields L_1 和 L_2 間的關係, 還牽涉到 K 在 L_1 和 L_2 中的“角色” . 簡單來說, 我們不只希望 L_1 和 L_2 是 isomorphic 而且希望能保持 K 的運算. 因此我們有以下的定義:

Definition 1.1.2. 令 $i : K \to L_1$, $j : K \to L_2$ 是 K 的兩個 extensions. 如果存在 $\phi : L_1 \to L_2$ 是一個 isomorphism 滿足對任意的 $k \in K$ 皆有 $\phi(i(k)) = j(k)$, 則稱 L_1/K 和 L_2/K 是 isomorphic extensions over K.

這裡因為 $k \in K$ 所以 $i(k) \in L_1$. 因此 ϕ 可將 $i(k)$ 送到 L_2 中. 而 $\phi(i(k)) = j(k)$ 就是要求 ϕ 必須把在 L_1 中代表 k 的元素送到 L_2 中那個代表 k 的元素. 特別的是當我們將 K 分別看成是 L_1 和 L_2 的 subfield (即 $K \subseteq L_1$ 且 $K \subseteq L_2$), 此時 $i(k) = k$ 且 $j(k) = k$ 因此 ϕ 必須符合對於所有的 $k \in K$, 皆滿足 $\phi(k) = k$. 在這情況之下有這樣性質的 ϕ 就稱為 L_1 和 L_2 之間的一個 “K-isomorphism”. 特別是當 $L_1 = L_2$ 時我們稱 ϕ 為一個 “K-automorphism”. 一般為了方便起見, 兩個 extensions L_1/K 和 L_2/K 我們都直接看成 $K \subseteq L_1$ 和 $K \subseteq L_2$. 所以若 L_1/K 和 L_2/K 是 isomorphic extensions over K 我們就直接假設 L_1 和 L_2 之間存在一個 K-isomorphism.

1.2. Field Extension 的 Degree

在大學基礎代數講義的 Chapter 9 Section 4 中我們曾經說明若 L/K 是一個 field extension 那麼我們可以將 L 看成是一個 vector space over K. 這件事情在我們新的 field extension 的定義之下仍是對的. 也就是說若 $i : K \to L$ 是一個 field extension, 那麼仿照前面對任意的 $k \in K$ 及 $l \in L$ 我們定義 $k \cdot l := i(k) \cdot l$, 很容易就可以驗證在此定義之下 L 仍為一個 vector space over K. 既然 L 是一個 vector space over K, 很自然的會考慮到其維度 (dimension) 因此我們仍然有以下的定義:

Definition 1.2.1. 給定一個 field extension L/K, 我們用 $[L : K]$ 來表示 $\dim_K(L)$, 稱之為 the *degree* of L over K. 若 $[L : K]$ 是有限的 (即 L 是一個 finite dimensional vector space over K), 則稱 L 是 K 的一個 *finite extension*.

若 L_1/K 和 L_2/K 是兩個 isomorphic extensions over K, 由 extension degree 的定義大家應可理解 $[L_1 : K] = [L_2 : K]$. 這個證明很簡單不過我們仍將證明寫下讓大家了解當初要求 isomorphism 時要保持 K 的重要性.

Lemma 1.2.2. *若 L_1/K 和 L_2/K 是兩個 isomorphic extensions over K, 則 $[L_1 : K] = [L_2 : K]$.*

Proof. 大家可以直接假設 $K \subseteq L_1$ 和 $K \subseteq L_2$ 來處理, 這裡我們用比較正式的定義來證明.

假設 $i : K \to L_1$ 和 $j : K \to L_2$ 分別為 L_1/K 和 L_2/K 的 extension 且 $\phi : L_1 \to L_2$ 為 L_1 和 L_2 的 isomorphism over K. 依定義 ϕ 是一個 ring homomorphism, 如果我們能證明 ϕ 是 L_1 和 L_2 這兩個 vector space over K 的 K-linear map, 那麼再由假設 ϕ 是 1-1 且 onto (因已知 ϕ 是 isomorphism) 可得 $\dim_K(L_1) = \dim_K(L_2)$, 即 $[L_1 : K] = [L_2 : K]$.

要證明 ϕ 是 K-linear, 只要證明對任意的 $c \in K$ 且 $a, b \in L_1$, 皆有

$$\phi(c \cdot a + b) = c \cdot \phi(a) + \phi(b).$$

這裡的 $c \cdot a + b$ 需看成是 L_1 中元素的運算, 依定義是 $i(c) \cdot a + b$. 故利用 ϕ 是 L_1 到 L_2 的 ring homomorphism 知

$$\phi(c \cdot a + b) = \phi(i(c) \cdot a + b) = \phi(i(c) \cdot a) + \phi(b) = \phi(i(c)) \cdot \phi(a) + \phi(b).$$

另一方面, $c \cdot \phi(a) + \phi(b)$ 需看成是 L_2 中元素的運算, 依定義是 $j(c) \cdot \phi(a) + \phi(b)$. 然而 ϕ 滿足 $\phi(i(c)) = j(c)$ 故知 $\phi(c \cdot a + b) = c \cdot \phi(a) + \phi(b)$, 也就是說 ϕ 是一個 K-linear map. □

從這個證明我們了解到若 ϕ 是 L_1 到 L_2 的 ring homomorphism 且保持 K 的運算那麼 ϕ 就是一個 L_1 到 L_2 的 K-linear map. 不過反過來並不一定對. 也就是說如果 $\psi : L_1 \to L_2$ 是一個 K-linear map 並不一定保證 ψ 是一個 ring homomorphism. 這是由於 K-linear map 僅保持 K 中元素和 L_1 中元素的乘法運算但是 ring homomorphism 卻需保持任兩個 L_1 中元素的乘法運算. 因此要注意兩個 extensions L_1/K 和 L_2/K, 如果僅知 $[L_1 : K] = [L_2 : K]$ 並不表示 L_1 和 L_2 是 isomorphic extensions over K.

若 L, F 和 K 皆為 fields, 且 $i : K \to F$ 和 $j : F \to L$ 皆為 1-1 的 ring homomorphism, 則 $j \circ i : K \to L$ 當然也是 1-1 的 ring homomorphism. 所以如果 L/F 和 F/K 是 field extensions 則 L 當然也是一個 field extension of K. 我們有以下重要有關 extension degree 的性質. 事實上這是大學基礎代數講義的 Theorem 9.4.6 和 Corollary 9.4.7 的合併, 我們就不再證明了.

Lemma 1.2.3. *假設 L/F 和 F/K 是 field extensions. 若 F 是 K 的一個 finite extension 且 L 是 F 的一個 finite extension 則 L 也是 K 的一個 finite extension. 反之, 若 L 是 K 的一個 finite extension, 則 F 是 K 的一個 finite extension 且 L 是 F 的一個 finite extension.*

另外, 在這兩個等價條件之下皆有:

$$[L : K] = [L : F][F : K].$$

1.3. Field Extensions 的分類

要創造出一 field extension over K 通常就是在 K 中加入其他的元素. 當然不能隨便亂加東西, 因為我們要求 field extension 仍然要是一個 field 所以加入的東西至少和 K 之間要可以運算. 有一種情況我們是不必擔心加入的東西和 K 是否能運算, 就是當這些東西和 K 都可以在某個更大的 field L 之中, 在這情況之下我們當然可以把所有的元素看成是 L 的元素, 自然就可以運算了. 當然了加入的元素雖然可以運算最後還需成為一個 field, 要達到這個目的我們有以下這個定義：

Definition 1.3.1. 若 L 是一個 field, $K \subseteq L$ 是 L 的 subfield 且 $S \subseteq L$ 是 F 的一個子集合 (subset). 我們定義 $K(S)$ 為 L 中所有包含 K 和 S 的 subfields 的交集. 也就是說

$$K(S) = \bigcap_{\substack{F \text{ subfield of } L \\ K \subseteq F \text{ 且 } S \subseteq F}} F.$$

稱為 the *extension of K generated by S*.

這裡要注意：如同證明一個 ring 中的一些 subrings 的交集仍為 ring (參見大學基礎代數講義 Lemma 6.2.2) 的方法, 我們可以證得一個 field 中的一些 subfields 的交集仍為 field. 所以 $K(S)$ 也是一個 field. 由這個定義也可以看出 $K(S)$ 事實上是 L 中包含 K 和 S 最小的 field. 換句話說：如果 K' 是 L 的 subfield 且 $K \subseteq K'$ 以及 $S \subseteq K'$, 則可得 $K(S) \subseteq K'$.

當 $S = \{a_1, \ldots, a_n\}$ 是 F 的一個有限子集時, 我們通常會省略"{ }" 這個符號而將 $K(S)$ 記為 $K(a_1, \ldots, a_n)$. 特別是當 $S = \{a\}$ 只有一個元素時我們稱 $K(a)$ 是 K 的一個 *simple extension.*

不難理解 simple extensions 是了解 field extensions 的要素. Simple extension 不只是最簡單的 extension 而且我們這裡要學習的 extensions (特別是 finite extensions) 大部分都可以利用 simple extensions 一步一步 extend 上去而得到. 所以如果能了解 simple extensions 大致上就能了解一般的 extensions. 我們自然得花點時間了解一下 simple extensions.

利用 a 得到的 simple extension $K(a)$ 可以分成兩種情況: 一種是 $[K(a) : K]$ 是 finite 的情況; 另一種是 $[K(a) : K]$ 是 infinite 的情況.

Definition 1.3.2. 如果 $K(a)/K$ 是一個 finite extension 則稱 a 是 *algebraic* over K; 反之則稱 a 是 *transcendental* over K.

這個定義其實和以前學過 algebraic 的定義 (大學基礎代數講義 Definition 9.4.4) 是等價的. 這是由於我們有以下的性質.

Theorem 1.3.3. *假設 K 是一個 field, L 是 K 的一個 extension field 且 $a \in L$, 則下面任一敘述和 a 是 algebraic over K 是等價的.*

(1) *存在 $K[x]$ 中的一個非 0 的 polynomial $f(x)$ 滿足 $f(a) = 0$.*

(2) *存在一個 field M 滿足 $a \in M$, $K \subseteq M \subseteq L$ 且 $[M : K]$ 是有限的.*

(3) *在 L 中包含 K 和 a 最小的 ring (即 $K[a]$) 就是包含 K 和 a 最小的 field (即 $K[a] = K(a)$).*

Proof. (1), (2) 和 (3) 是等價的我們已在大學基礎代數講義 Theorem 10.1.9 中證明過了 (注意那時是用 (1) 來定義 algebraic). 這裡我們只要檢查 a 是 algebraic over K (即 $[K(a) : K]$ 是有限的) 和 (2) 是等價的即可.

如果 $[K(a) : K]$ 是有限的, 則令 $M = K(a)$, 故有 $a \in M$, $K \subseteq M \subseteq L$ 且 $[M : K]$ 是有限的.

反之, 如果 M 是一個 field 滿足 $a \in M$, $K \subseteq M \subseteq L$ 且 $[M : K]$ 是有限的, 則由 $K(a)$ 是 L 中包含 K 和 a 最小的 field 的定義知 $K \subseteq K(a) \subseteq M$. 也就是說 $K(a)$ 是 M over K 的一個 subspace. 所以由線性代數知其 over K 的 dimension 一定比較小, 也就是說 $[K(a) : K] \leq [M : K]$. 故知 $[K(a) : K]$ 是有限的. □

回顧一下, 當 a 是 algebraic over K 時滿足 Theorem 1.3.3 (1) 中所述次數最小的 monic polynomial (即最高次項係數為 1) 稱為 a over K 的*minimal polynomial*. (注意這裡一定要強調 over 哪一個 field 的 minimal polynomial, 因為 over 不同的 field 其 minimal polynomial 會不同.) 如果 a over K 的 minimal polynomial 為 $p(x)$ 且 $\deg(p(x)) = n$, 那麼我們有以下重要的結論:

(1) $K(a)$ 和 $K[x]/(p(x))$ 是 isomorphic extensions over K.

(2) $[K(a) : K] = n$.

(3) $K(a)$ 中的元素的可以唯一表示成

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

當 $b \in L$ 也滿足 $p(b) = 0$ 時, 不見得會有 $K(a) = K(b)$. 但由前面 (1) 得知 $K(a)$ 和 $K(b)$ 都和 $K[x]/(p(x))$ 是 isomorphic extensions over K, 所以我們知 $K(a)$ 和 $K(b)$ 是 isomorphic extensions over K. 事實上若我們定 $\phi : K(a) \to K(b)$ 滿足

$$\phi(c_0 + c_1 a + \cdots + c_{n-1} a^{n-1}) = c_0 + c_1 b + \cdots + c_{n-1} b^{n-1}, \forall c_0, c_1, \ldots, c_{n-1} \in K,$$

則 ϕ 就是一個 $K(a)$ 到 $K(b)$ 的 K-isomorphism. 要注意的是在更一般的情況, 如果 $q(x) \in K[x]$ 是 $c \in L$ 的 minimal polynomial over K 且 $p(x) \neq q(x)$, 那麼我們不能馬上斷言 $K(a)$ 和 $K(c)$ 是否 isomorphic over K. 當然了如果 $\deg(p(x)) \neq \deg(q(x))$, 由於 $[K(a) : K] \neq [K(c) : K]$ 利用 Lemma 1.2.2 我們立刻知 $K(a)$ 和 $K(c)$ 不可能是 isomorphic extensions over K. 但當 $\deg(p(x)) = \deg(q(x))$ 時, 雖然 $[K(a) : K] = K[(c) : K]$, 我們曾解釋過此時並不保證 $K(a)$ 和 $K(c)$ 是 isomorphic over K. 有很多種情況它們是不 isomorphic, 不過當 K 是 finite field 時, $K(a)$ 和 $K(c)$ 確實會 isomorphic over K (事實上是 $K(a) = K(c)$ 參見大學基礎代數講義 Theorem 10.4.8).

如果 L/K 是一個 extension 且 L 中所有的元素都是 algebraic over K, 我們便稱 L 是一個*algebraic extension* over K. 當 L/K 是 finite extension, 由 Theorem 1.3.3 (2) 知 L/K 必為 algebraic extension. 不過要注意 algebraic extension 不一定會是 finite extension. 比方說 $\mathbb{Q}(S)$ 其中 $S = \{\sqrt{n} \,|\, n \in \mathbb{N}\}$, 就是一個 algebraic extension over $\mathbb{Q}$ 但不是 finite extension over $\mathbb{Q}$. 另一方面當 S 是一個有限集合時, $K(S)/K$ 也未必是 finite extension, 除非 S 中的元素都是 algebraic over K. 我們有以下有關 finite extension 的充要條件.

Proposition 1.3.4. *若 S 是一個 finite set 且 S 中的元素皆 algebraic over K, 則 $L = K(S)$ 是一個 finite extension over K.*

反之, 若 L/K 是一個 finite extension, 則必存在一個 finite set S 其中 S 的元素皆 algebraic over K, 使得 $L = K(S)$.

Proof. 首先我們觀察若 F/K 是一個 extension 且 a 是 algebraic over K 則 a 是 algebraic over F. 這是由於 Theorem 1.3.3 告訴我們存在 $f(x) \neq 0$ 且 $f(x) \in K[x]$ 滿足 $f(a) = 0$. 但由於 $K \subseteq F$ 所以知 $f(x) \in F[x]$, 故再利用 Theorem 1.3.3 的等價關係知 a 仍為 algebraic over F.

現在如果 $S = \{a_1, \ldots, a_n\}$ 且 $a_1, \ldots, a_n$ 皆 algebraic over K, 對任意 $i \in \{1, \ldots, n\}$ 我們令 $F_i = K(a_1, \ldots, a_i)$. 由於 $L = K(a_1, \ldots, a_n) = F_n$ 以及 $F_i \subseteq F_{i+1}$, 利用 Lemma 1.2.3 我們有

$$[L : K] = [K(a_1, \ldots, a_n) : K] = [F_n : F_{n-1}] \cdots [F_2 : F_1] \cdot [F_1 : K].$$

由於 $F_1 = K(a_1)$ 且 a_1 是 algebraic over K 故知 $[F_1 : K]$ 是有限的. 同理, 當 $i \in \{1, \ldots, n-1\}$ 時, 由於 $F_{i+1} = F_i(a_{i+1})$ 且 a_{i+1} 是 algebraic over F_i (因 a_{i+1} 是 algebraic over K 且 $K \subseteq F_i$), 故知 $[F_{i+1} : F_i]$ 是有限的. 因此得到 $[L : K]$ 是有限的, 即 L/K 是一個 finite extension.

反之, 如果 L/K 是 finite extension, 我們對 extension degree 作 induction. 也就是對任意的 extension L'/K' 假設當 $[L' : K'] < m$ 時, 皆存在一個 finite set S', 使得 $L' = K'(S')$. 當 $[L : K] = 1$ 時, 由於 $L = K$, 我們可以令 $S = \{1\}$ 即可. 現若 $[L : K] = m$, 任取 $a \in L$ 但 $a \notin K$. 由於 $[L : K] = [L : K(a)][K(a) : K]$, 馬上得知 $[L : K(a)] < m$ (因 $a \notin K$, 故 $[K(a) : K] > 1$) 故由 induction 的假設知存在一個 finite set S' 使得 $L = K(a)(S')$. 故令 $S = S' \cup \{a\}$, 則知 S 是一個 finite set 且 $L = K(S)$. 這裡 S 中的元素必定會 algebraic over K, 這是因為 L/K 是 finite extension 所以 L 中的元素必皆 algebraic over K. □

在 Theorem 1.3.3 中我們提過: 當 a 是 algebraic over K 且 $L = K(a)$ 時, 包含 a 和 K 最小的 ring, $K[a]$ 事實上就是 L. 當 L/K 是 finite extension 時, 由 Proposition 1.3.4 知存在 $a_1, \ldots, a_n$ 皆 algebraic over K 使得 $L = K(a_1, \ldots, a_n)$. 我們自然會問: 是否包含 K 和 $a_1, \ldots, a_n$ 最小的 ring, $K[a_1, \ldots, a_n]$ 會是 L 呢? 由於 $K \subseteq K[a_1, \ldots, a_n] \subseteq L$, 我們知 $K[a_1, \ldots, a_n]$ 是 L over K 的 subspace, 故知 $\dim_K(K[a_1, \ldots, a_n]) \leq [L : K]$ 因此由大學基礎代數講義Theorem 9.3.7 馬上就知 $K[a_1, \ldots, a_n]$ 是一個 field, 故知 $K[a_1, \ldots, a_n] = L$. 這裡我們想用 induction 來證明, 讓大家更清楚這個結果.

Lemma 1.3.5. *假設 L/K 是一個 finite extension. 若 $L = K(a_1, \ldots, a_n)$, 則包含 K 和 $a_1, \ldots, a_n$ 最小的 ring, $K[a_1, \ldots, a_n]$ 等於 L. 也就是說對任意 $\lambda \in L$, 皆存在一個 n 個變數的 polynomial, $f(x_1 \ldots, x_n) \in K[x_1, \ldots, x_n]$ 滿足 $f(a_1, \ldots, a_n) = \lambda$.*

Proof. 我們對 n 做 induction. 當 $n = 1$ 時, 利用 Theorem 1.3.3 知對任意 $\alpha \in K(a_1)$ 都存在 $c_0, c_1, \ldots, c_r \in K$ 使得 $\alpha = c_0 + c_1 a_1 + \cdots + c_r a_1^r$. 令 $f(x) = c_0 + c_1 x + \cdots + c_r x^r$, 可得 $\alpha = f(a_1)$. 利用 induction, 假設 $F = K(a_1, \ldots, a_{n-1})$ 且對任意 F 中的元素 β 皆存在 $f(x_1, \ldots, x_{n-1}) \in K[x_1, \ldots, x_{n-1}]$ 滿足 $\beta = f(a_1, \ldots, a_{n-1})$. 考慮 $L = K(a_1, \ldots, a_{n-1}, a_n) = F(a_n)$. 由於 a_n 是 algebraic over $K \subseteq F$, 再利用 Theorem 1.3.3 知對任意 $\lambda \in L$ 都存在 $\beta_0, \beta_1, \ldots, \beta_s \in F$ 使得 $\lambda = \beta_0 + \beta_1 a_n + \cdots + \beta_s a_n^s$. 然而 $\beta_i \in F$, 由 induction 的假設知對每一個 β_i 皆存在 $f_i(x_1 \cdots, x_{n-1}) \in K[x_1, \ldots, x_{n-1}]$ 使得

$\beta_i = f_i(a_1, \ldots, a_{n-1})$. 故若令 $f(x_1, \ldots, x_{n-1}, x_n)$ 為

$$f_0(x_1, \ldots, x_{n-1}) + f_1(x_1, \ldots, x_{n-1})x_n + \cdots + f_s(x_1, \ldots, x_{n-1})x_n^s \in K[x_1, \ldots, x_{n-1}, x_n],$$

我們有 $\lambda = f(a_1, \ldots, a_{n-1}, a_n)$. □

當 L/K 不是 algebraic extension 時, 依定義在 L 中必存在一元素 a 是 transcendental over L. 換言之, $K(a)/K$ 不是 finite extension. 最後我們簡單的介紹一下這一種 simple extension. a 是 transcendental over K 意即對任意的非零的多項式 $f(x) \in K[x]$ 皆有 $f(a) \neq 0$. 由於 $K(a)$ 是一個包含 K 和 a 的 field, 對任意 $f(x) \in K[x]$, $f(a)$ 當然也在 $K(a)$ 中. 事實上

$$K[a] = \{f(a) \,|\, f(x) \in K[x]\} \subseteq K(a)$$

是包含 K 和 a 最小的 ring. 這個性質和 a 是 algebraic 或 transcendental over K 無關. 不過由於 a 是 transcendental over K, 若 $f(x), g(x) \in K[x]$ 且 $f(x) \neq g(x)$, 則 $f(a) \neq g(a)$. 這是因為 $f(x) - g(x)$ 是 $K[x]$ 中非 0 的多項式, 如果 $f(a) = g(a)$ 這表示 a 為 $f(x) - g(x)$ 的一個根, 此與 a 是 transcendental over K 相矛盾. 這和 algebraic over K 的情況不同, 因為若 b 是 algebraic over K 且 $p(x) \in K[x]$ 是其 minimal polynomial over K, 則對任意的 $f(x) \in K[x]$ 我們都可以找到 $g(x) = f(x) + p(x) \in K[x]$ 使得 $f(x) \neq g(x)$ 但是 $f(b) = g(b)$. 另一個 algebraic 和 transcendental 不同的是: 當 b 是 algebraic over K 時包含 K 和 b 最小的 ring 也會是一個 field (即 $K[b] = K(b)$); 不過若 a 是 transcendental over K, 那麼包含 K 和 a 最小的 ring (即 $K[a]$) 就不再是一個 field 了. 這是因為當 $f(x) \in K[x]$ 且 $\deg(f(x)) \geq 1$ 時, $f(a) \neq 0$ 且如果存在 $g(a) \in K[a]$ 使得 $f(a) \cdot g(a) = 1$ 表示 a 是 $f(x) \cdot g(x) - 1$ 的一個根, 再次和 a 是 transcendental over K 相矛盾. 因此我們知 $K[a]$ 不可能是 field. 那麼 $K(a)$ 到底是怎樣的 field 呢? 事實上若考慮

$$L = \{f(a)/g(a) \,|\, f(x), g(x) \in K[x] \text{ 且 } g(x) \neq 0\}$$

很容易驗證這是包含 K 和 a 最小的 field, 故有 $K(a) = L$.

同樣的道理, 如果 $L = K(a_1, \ldots, a_n)$, 其中某些 a_i 是 transcendental over K, 那麼 L 中的元素並不能全部用 $f(a_1, \ldots, a_n)$ 其中 $f(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$, 這種形式來表示. 但是要描述 L 中的元素, 我們仍可用 $f(a_1, \ldots, a_n)/g(a_1, \ldots, a_n)$, 其中 $f(x_1, \ldots, x_n), g(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ 且 $g(a_1, \ldots, a_n) \neq 0$ 來表示. 在本講義中我們僅探討 finite extension, 所以對於 transcendental extension 我們僅探討到此.

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

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

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 $S = \{\beta \in L \,|\, f(\beta) = 0\}$ 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 $F_1,F_3\nsubseteq\mathbb{R}$, 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

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

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, $|\mathrm{Gal}(L/K)|\le[L:K]$. 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. □

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:

$$\begin{cases}\sigma_1(a_1)x_1+\sigma_2(a_1)x_2+\cdots+\sigma_n(a_1)x_n &= 0\\ \sigma_1(a_2)x_1+\sigma_2(a_2)x_2+\cdots+\sigma_n(a_2)x_n &= 0\\ \qquad\vdots &\ \vdots\\ \sigma_1(a_m)x_1+\sigma_2(a_m)x_2+\cdots+\sigma_n(a_m)x_n &= 0\end{cases} \tag{2.4}$$

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 $a_1,\dots,a_m$ 是 L/K 的一組 basis, 對任意 $\lambda\in L$ 都存在一組 $r_1,\dots,r_m\in K$ 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 $c_1,\dots,c_n\in L$ 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 $\sigma_1,\dots,\sigma_n$ 是 linearly independent over L 相矛盾, 故得證 $|\mathrm{Gal}(L/K)|=n\le m=[L:K]$. □

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

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

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

假設 $H=\{\tau_1,\dots,\tau_n\}$, 其中 $\tau_1=I$ 是 identity. 任取 $a_1,\dots,a_{n+1}\in L$, 我們欲證明 $a_1,\dots,a_{n+1}$ 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:

$$\begin{cases}\tau_1(a_1)x_1+\tau_1(a_2)x_2+\cdots+\tau_1(a_{n+1})x_{n+1} &= 0\\ \tau_2(a_1)x_1+\tau_2(a_2)x_2+\cdots+\tau_2(a_{n+1})x_{n+1} &= 0\\ \qquad\vdots &\ \vdots\\ \tau_n(a_1)x_1+\tau_n(a_2)x_2+\cdots+\tau_n(a_{n+1})x_{n+1} &= 0\end{cases}\tag{2.6}$$

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:

$$\begin{cases} \tau_1(a_1) + \tau_1(a_2)c_2 + \cdots + \tau_1(a_m)c_m &= 0 \\ \tau_2(a_1) + \tau_2(a_2)c_2 + \cdots + \tau_2(a_m)c_m &= 0 \\ \qquad\qquad \vdots & \vdots \\ \tau_n(a_1) + \tau_n(a_2)c_2 + \cdots + \tau_n(a_m)c_m &= 0 \end{cases} \tag{2.7}$$

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

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

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:

$$\begin{cases} \tau_1(a_1) + \tau_1(a_2)\tau(c_2) + \cdots + \tau_1(a_m)\tau(c_m) &= 0 \\ \tau_2(a_1) + \tau_2(a_2)\tau(c_2) + \cdots + \tau_2(a_m)\tau(c_m) &= 0 \\ \qquad\qquad \vdots & \vdots \\ \tau_n(a_1) + \tau_n(a_2)\tau(c_2) + \cdots + \tau_n(a_m)\tau(c_m) &= 0 \end{cases}$$

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 $a_1 + c_2 a_2 + \cdots + c_m a_m = 0$, 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. □

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. □

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 $\mathcal{G}(\mathcal{F}(H)) = H$. □

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.

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.

Chapter 4

Galois Extension

在這最後一章中, 我們將介紹 Galois extension 以及其基本定理. 最後我們介紹一些應用以及例子

4.1. Fundamental Theorem of Galois Theory

我們首先介紹何謂 Galois extension, 從而得到 Galois extension 的 intermediate fields 以及其 Galois groups 的 subgroups 存在著一對一的對應關係.

在一般代數書中對於 Galois extension 的定義不盡相同, 不過這些定義其實是等價的. 我們首先來探討這些等價關係.

Theorem 4.1.1. *假設 L/K 是一個 finite extension. 下列敘述是等價的.*

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

(2) $\mathrm{Gal}(L/K)$ *的 fixed field 是* K.

(3) L/K *是一個 normal and separable extension.*

Proof. (1) $\Rightarrow$ (2): 假設 $\mathrm{Gal}(L/K)$ 的 fixed field 是 F, 則我們有 $K \subseteq F \subseteq L$ 且 $|\mathrm{Gal}(L/K)| = [L : F]$ (Theorem 2.3.4). 因此由 $|\mathrm{Gal}(L/K)| = [L : K]$ 得知 $[L : K] = [L : F]$. 又由於 $[L : K] = [L : F][F : K]$, 故得 $[F : K] = 1$. 亦即 $F = K$.

(2) $\Rightarrow$ (3): 回顧 $\mathrm{Gal}(L/K)$ 的 fixed field 的定義為 $\{\alpha \in L \,|\, \sigma(\alpha) = \alpha, \forall \sigma \in \mathrm{Gal}(L/K)\}$. 所以 K 為 $\mathrm{Gal}(L/K)$ 的 fixed field 不只是說 K 中的元素都會被所有的 $\sigma \in \mathrm{Gal}(L/K)$ 固定, 也表示 L 中被所有的 $\sigma \in \mathrm{Gal}(L/K)$ 固定的元素必定落在 K 中. 現任取 $a \in L$, 假設 a over K 的 minimal polynomial 為 $p(x)$. 令 $a = a_1, a_2, \ldots, a_n$ 為 $p(x)$ 在 L 中所有的相異根. 考慮 $f(x) = (x - a_1)(x - a_2) \cdots (x - a_n)$. 由於 n 為 $p(x)$ 在 L 中相異根的個數, 因此我們知 $\deg(f(x)) = n \leq \deg(p(x))$. 又由於 $a_1, a_2, \ldots, a_n \in L$, 我們有 $f(x) \in L[x]$. 現假設 $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$, 其中 $c_i \in L$. 對任意 $\sigma \in \mathrm{Gal}(L/K)$, 我們有

$$f^\sigma(x) = x^n + \sigma(c_{n-1})x^{n-1} + \cdots + \sigma(c_1)x + \sigma(c_0). \tag{4.1}$$

另一方面由於 $f(x)=(x-a_1)(x-a_2)\cdots(x-a_n)$, 利用 Lemma 3.1.3 知

$$f^\sigma(x)=(x-\sigma(a_1))(x-\sigma(a_2))\cdots(x-\sigma(a_n)).$$

由於 $\sigma\in\mathrm{Gal}(L/K)$, 我們知 $\sigma(a_i)$ 必會在 L 中且會是 $p(x)$ 的一個根. 因此由 σ 是 1-1 知 $\{a_1,a_2,\ldots,a_n\}=\{\sigma(a_1),\sigma(a_2),\ldots,\sigma(a_n)\}$. 也就是說

$$(x-a_1)(x-a_2)\cdots(x-a_n)=(x-\sigma(a_1))(x-\sigma(a_2))\cdots(x-\sigma(a_n)),$$

因此知對任意 $\sigma\in\mathrm{Gal}(L/K)$ 皆有 $f(x)=f^\sigma(x)$. 故由式子 (4.1) 知對任意 $\sigma\in\mathrm{Gal}(L/K)$ 皆有 $\sigma(c_i)=c_i$. 也就是說這些 c_i 都落在 $\mathrm{Gal}(L/K)$ 的 fixed field 中. 因此由假設 K 是 $\mathrm{Gal}(L/K)$ 的 fixed field 知 $c_i\in K$, 亦即 $f(x)\in K[x]$. 由於 a 是 $f(x)\in K[x]$ 的一個根, 故由 $p(x)$ 是 a over K 的 minimal polynomial 的性質知 $p(x)\,|\,f(x)$. 得知 $\deg(p(x))\le\deg(f(x))$, 因此由前面已知 $\deg(f(x))\le\deg(p(x))$ 我們得 $\deg(p(x))=\deg(f(x))$. 再加上 $p(x)$ 和 $f(x)$ 都是 monic polynomials 得知 $p(x)=f(x)$. 由於 $f(x)$ 在 L 中可以完全分解且其根皆相異, 得證 a over K 的 minimal polynomial 在 L 中 splits 且為 separable polynomial. 因為當初 $a\in L$ 是任取的, 故由 normal extension 和 separable extension 的定義得知 L/K 是 normal and separable extension.

(3) $\Rightarrow$ (1): 假設 L/K 是一個 normal and separable extension, 由 separable extension 的性質 (Theorem 3.4.5) 知若 N/K 是包含 L 的 finite normal extension, 則 $|\mathfrak{M}_K(L,N)|=[L:K]$. 但由於 L/K 是 normal extension, 由 Lemma 3.2.6 知 $\mathrm{Gal}(L/K)=\mathfrak{M}_K(L,N)$, 得證 $|\mathrm{Gal}(L/K)|=[L:K]$. □

我們對符合以上任一項的 finite extension 稱之為 Galois extension.

Definition 4.1.2. 假設 L/K 是一個 finite extension. 若 L/K 是 normal and separable extension, 則稱 L/K 是一個 *Galois extension.*

在這個定義中我們特別選 normal and separable extension 當成 Galois extension 的定義是希望加強印象. 以後大家若有機會探討不是 finite extension 的情況, 一般會用 normal and separable extension 來定義 Galois extension. 另一方面雖然 Theorem 4.1.1 中三個敘述是等價的, 但是一般我們都是利用檢查是否為 normal and separable extension 來判斷一個 extension 是否為 Galois extension. 例如我們可以利用 normal extension 和 separable extension 的性質得到以下的結果.

Proposition 4.1.3. *假設 L/K 是 finite normal extension 且 F 是 L/K 的 intermediate field. 則 L/F 是一個 Galois extension.*

Proof. 對任意 L/K 的 intermediate field F, 由於 L/K 是 normal 且 separable extension, 因此分別利用 Corollary 3.2.3 以及 Lemma 3.4.2 得知 L/F 也是 normal and separable extension. 也就是說 L/F 也是 Galois extension. □

要注意由於 F/K 不一定是 normal extension (參見 Example 3.2.4 (1)), 所以在 Proposition 4.1.3 中 F/K 不一定是 Galois extension.

在一般的情況如何檢查一個 extension 是否為 normal 和 separable extension 呢? 在 Theorem 3.2.2 和 Theorem 3.4.7, 我們分別介紹了檢查 normal extension 和 separable extension 的方法, 所以綜合這兩個定理, 我們得到了檢查 Galois extension 的方法.

Theorem 4.1.4. *假設 L/K 是一個 finite extension. 下列的敘述是等價的.*

(1) *L/K 是 Galois extension.*

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

Proof. (1) $\Rightarrow$ (2): 由於 L/K 是 finite extension, 知存在 $a_1, \ldots, a_n \in L$ 使得 $L = K(a_1, \ldots, a_n)$. 令 $p_i(x)$ 為 a_i over K 的 minimal polynomial, 由於 L/K 是 normal 且 separable extension, 故知 $p_i(x)$ splits over L 且為 separable polynomial. 要注意有可能 $i \neq j$ 但 $p_i(x) = p_j(x)$, 不過如果 $p_i(x) \neq p_j(x)$, 那麼 $p_i(x)$ 和 $p_j(x)$ 的根皆相異. 否則若 α 同時是 $p_i(x)$ 和 $p_j(x)$ 的根, 會造成 $p_i(x)$ 和 $p_j(x)$ 皆為 α 的 minimal polynomial 的矛盾. 故若去除掉重複的 $p_i(x)$ 後令 $f(x)$ 為所有這些相異的 $p_i(x)$ 的乘積, 則 $f(x) \in K[x]$ 為 separable polynomial 且 $f(x)$ splits over L. 現在證明 L 為 $f(x)$ 的 splitting field. 假設 $K \subseteq F \subseteq L$ 且 $f(x)$ splits over F. 由於對所有 $i \in \{1, \ldots, n\}$, a_i 的 minimal polynomial 是 $f(x)$ 的因式, 我們得 a_i 是 $f(x)$ 的一個根, 故得 $a_i \in F$. 因此 $L = K(a_1, \ldots, a_n) \subseteq F$, 而得證 $L = F$. 也就是說 L 是 $f(x)$ over K 的 splitting field.

(2) $\Rightarrow$ (1): 假設 $b_1, \ldots, b_m \in L$ 是 $f(x)$ 所有的根. 因為 L 是 $f(x)$ over K 的 splitting field, 我們得 $L = K(b_1, \ldots, b_m)$. 由於 $f(x)$ 是 separable polynomial, 每一個 b_i over K 的 minimal polynomial 因為整除 $f(x)$ 必也是 separable polynomial, 因此 b_i 皆為 separable element over K. 故由 Theorem 3.4.7 知 L/K 是 separable extension. 又因為 L 是 $f(x)$ over K 的 splitting field, 故由 Theorem 3.2.2 知 L/K 是 normal extension. 因此得 L/K 是 Galois extension. □

我們曾經提過, Galois 理論就是要探討一個 extension 其 Galois group 的 subgroups 以及這個 extension 的 intermediate fields 之間的關係. 我們曾介紹過兩個函數來探討它們之間的關係, 現在回顧一下這兩個函數. 假設 L/K 是 finite extension. 我們定義 $\mathfrak{F}$ 是 L/K 的 intermediate fields 所成的集合, 即 $\mathfrak{F} = \{F \mid F \text{ 是一個 field 且 } K \subseteq F \subseteq L\}$. 且令 $\mathfrak{G}$ 是 $\mathrm{Gal}(L/K)$ 的 subgroups 所成的集合, 即 $\mathfrak{G} = \{H \mid H \text{ 是 } \mathrm{Gal}(L/K) \text{ 的 subgroup}\}$. 我們定義函數 $\mathcal{G} : \mathfrak{F} \to \mathfrak{G}$ 如下: 對任意 L/K 的 intermediate field F (即 $F \in \mathfrak{F}$), 我們定義 $\mathcal{G}(F) = \mathrm{Gal}(L/F)$. 而函數 $\mathcal{F} : \mathfrak{G} \to \mathfrak{F}$ 的定義為: 對任意 $\mathrm{Gal}(L/K)$ 的 subgroup H (即 $H \in \mathfrak{G}$), 我們定義 $\mathcal{F}(H)$ 為 H 的 fixed field, 即 $\mathcal{F}(H) = L^H$.

對於一般的 finite extension L/K, Corollary 2.3.6 告訴我們 $\mathcal{F}$ 是 1-1 的函數且 $\mathcal{G}$ 是 onto 的函數. 當 L/K 是 Galois extension 時我們可得 $\mathcal{F}$ 是 onto 的(因此是 1-1 且 onto 的函數) 以及 $\mathcal{G}$ 是 1-1 的函數 (因此是 1-1 且 onto 的函數). 這就是所謂 Galois 理論的 fundamental theory. 這個 fundamental theory 事實上有兩部分, 我們將它們分開討論.

Theorem 4.1.5 (First Fundamental Theorem of Galois Theory)**.** *假設 L/K 是一個 finite Galois extension. 則對任意 $F \in \mathfrak{F}$, 我們有 $\mathcal{F}(\mathcal{G}(F)) = F$. 因此 $\mathcal{G} : \mathfrak{F} \to \mathfrak{G}$ 給了我們一個 L/K 的 intermediate fields 和 $\mathrm{Gal}(L/K)$ 的 subgroups 之間的一個一對一的對應關係.*

Proof. 對任意 L/K 的 intermediate field F, 由 Proposition 4.1.3 我們知 L/F 是一個 Galois extension. 所以利用 Theorem 4.1.1 可得 L/F 的 Galois group 的 fixed field 為 F. 由於 L/F 的 Galois group $\mathrm{Gal}(L/F)$ 就是 $\mathcal{G}(F)$, 而 $\mathcal{G}(F)$ 的 fixed field 就是 $\mathcal{F}(\mathcal{G}(F))$, 因此得證 $\mathcal{F}(\mathcal{G}(F)) = F$.

接著要說明 $\mathcal{G} : \mathfrak{F} \to \mathfrak{G}$, 給了 $\mathfrak{F}$ 到 $\mathfrak{G}$ 之間一個一對一的對應關係. 注意這裡提的一對一對應關係 (one to one correspondence) 指的是兩個集合間的對應關係, 也就是說 $\mathfrak{G}$ 中的每一個元素在 $\mathfrak{F}$ 中都可找到唯一的元素與之對應, 反之亦然. 因此我們不只要說明 $\mathcal{G} : \mathfrak{F} \to \mathfrak{G}$ 是 1-1 且要說明其為 onto. 現若 $F_1, F_2 \in \mathfrak{F}$ 滿足 $\mathcal{G}(F_1) = \mathcal{G}(F_2)$, 套用 $\mathcal{F}$ 於其上得 $\mathcal{F}(\mathcal{G}(F_1)) = \mathcal{F}(\mathcal{G}(F_2))$. 故由 $\mathcal{F}(\mathcal{G}(F)) = F$, 得知 $F_1 = F_2$. 另一方面任取 $H \in \mathfrak{G}$, 考慮 $F = \mathcal{F}(H)$, 則由 $\mathcal{G}(\mathcal{F}(H)) = H$ (Corollary 2.3.6) 知 $\mathcal{G}(F) = H$. 故得知 $\mathcal{G} : \mathfrak{F} \to \mathfrak{G}$ 確實給了 $\mathfrak{F}$ 和 $\mathfrak{G}$ 兩個集合之間一個一對一的對應關係. □

當 L/K 是 finite Galois extension, 由 Corollary 2.3.6 以及 Theorem 4.1.5 我們知道對所有 $H \in \mathfrak{G}$ 以及 $F \in \mathfrak{F}$ 皆有 $\mathcal{G}(\mathcal{F}(H)) = H$ 以及 $\mathcal{F}(\mathcal{G}(F)) = F$. 也就是說此時 $\mathcal{F}$ 和 $\mathcal{G}$ 互為反函數. 不過要注意若 $F_1, F_2 \in \mathfrak{F}$ 且 $F_1 \subseteq F_2$, 則 $\mathcal{G}(F_2) \subseteq \mathcal{G}(F_1)$ (Lemma 2.1.2). 也就是說較大的 intermediate field 對應到較小的 subgroup. 反之, 若 $H_1, H_2 \in \mathfrak{G}$ 且 $H_1 \subseteq H_2$, 則 $\mathcal{F}(H_2) \subseteq \mathcal{F}(H_1)$ (Lemma 2.2.2). 因此要注意較大的 subgroup 對應到較小的 intermediate field. 這樣大小顛倒的對應關係也可由以下 extension degree 和 group order 的關係看出.

Corollary 4.1.6. *假設 L/K 是 finite Galois extension.*

(1) *若 F 是 L/K 的 intermediate field, 則*

$$[F : K] = \frac{|\mathrm{Gal}(L/K)|}{|\mathrm{Gal}(L/F)|} = \frac{|\mathrm{Gal}(L/K)|}{|\mathcal{G}(F)|}.$$

特別若 F_1, F_2 是 L/K 的 intermediate fields 滿足 $F_1 \subseteq F_2$, 則

$$[F_2 : F_1] = \frac{|\mathcal{G}(F_1)|}{|\mathcal{G}(F_2)|}.$$

(2) *若 H 是 $\mathrm{Gal}(L/K)$ 的 subgroup, 則*

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

特別若 H_1 和 H_2 是 $\mathrm{Gal}(L/K)$ 的 subgroup 且滿足 $H_1 \subseteq H_2$, 則

$$[\mathcal{F}(H_1) : \mathcal{F}(H_2)] = \frac{|H_2|}{|H_1|}.$$

Proof. (1) 因為 L/K 是 finite Galois extension, 由 Proposition 4.1.3 我們知 L/F 是 Galois extension, 故由 Theorem 4.1.1 知 $|\mathrm{Gal}(L/K)| = [L : K]$ 且 $|\mathrm{Gal}(L/F)| = [L : F]$. 再利用 $[L : K] = [L : F][F : K]$, 得知 $[F : K] = [L : K]/[L : F] = |\mathrm{Gal}(L/K)| \,/\, |\mathrm{Gal}(L/F)|$.

現若 $F_1 \subseteq F_2$, 由於 $[F_2 : F_1] = [F_2 : K]/[F_1 : K]$, 故利用前面所得結果知 $[F_2 : F_1] = |\mathrm{Gal}(L/F_1)| \,/\, |\mathrm{Gal}(L/F_2)| = |\mathcal{G}(F_1)| \,/\, |\mathcal{G}(F_2)|$.

(2) 利用 Corollary 2.3.5 我們知 $[\mathcal{F}(H) : K] = [L : K]/\,|H|$, 故利用 L/K 是 Galois extension, 我們有 $[\mathcal{F}(H) : K] = |\mathrm{Gal}(L/K)| \,/\, |H|$. 現若 $H_1 \subseteq H_2$, 則 $\mathcal{F}(H_2) \subseteq \mathcal{F}(H_1)$, 故知 $[\mathcal{F}(H_1) : \mathcal{F}(H_2)] = [\mathcal{F}(H_1) : K]/[\mathcal{F}(H_2) : K] = |H_2| \,/\, |H_1|$. □

當 L/K 是 field extension 時, 我們曾提到過探討 L/K 的 intermediate field 是否能保持原來 L/K 的 extension 特質是重要的課題. 例如 Galois 理論的第一個 fundamental theory (Theorem 4.1.5) 就是利用到當 L/K 是 finite Galois extension 時, 對所有 L/K 的 intermediate field F, 皆有 L/F 也是 Galois extension (Proposition 4.1.3). 我們強調過這時 F/K 並不一定也是 Galois extension. 第二個 fundamental theorem 就是要回答何時 F/K 會是 Galois extension.

既然第一個 fundamental theorem 告訴我們 L/K 的 intermediate field 和 $\mathrm{Gal}(L/K)$ 的 subgroup 之間的對應關係. 所以我們很自然的會問到 $\mathrm{Gal}(L/K)$ 這個 group 的性質會不會影響到 L/K 的 intermediate field 的性質. 下一個 Lemma 就是告訴我們它們之間如何"互動".

Lemma 4.1.7. *假設 L/K 是一個 field extension 且 F 為 L/K 的 intermediate field. 若 $\sigma \in \mathrm{Gal}(L/K)$, 則 $\sigma(F)$ 為 L/K 的 intermediate field 且 $L/\sigma(F)$ 的 Galois group $\mathrm{Gal}(L/\sigma(F))$ 為 $\sigma \circ \mathrm{Gal}(L/F) \circ \sigma^{-1}$. 亦即 $\mathcal{G}(\sigma(F)) = \sigma \circ \mathcal{G}(F) \circ \sigma^{-1}$.*

Proof. 依定義 $\sigma(F) = \{\sigma(\alpha) \,|\, \alpha \in F\}$, 由於 F 是一個 field 且 σ 是 ring homomorphism 可得 $\sigma(F)$ 仍為一個 field. 又因為 $K \subseteq F \subseteq L$ 且 $\sigma : L \to L$ 是 K-monomorphism, 所以 $\sigma(K) = K \subseteq \sigma(F) \subseteq L$. 故知 $\sigma(F)$ 是 L/K 的 intermediate field.

現假設 $\tau \in \mathrm{Gal}(L/\sigma(F))$, 我們有 $\tau : L \to L$ 且對任意 $\alpha \in F$ 皆有 $\tau(\sigma(\alpha)) = \sigma(\alpha)$. 令 $\rho = \sigma^{-1} \circ \tau \circ \sigma : L \to L$. 因為 $\mathrm{Gal}(L/K)$ 是一個 group 且 $\tau \in \mathrm{Gal}(L/\sigma(F)) \subseteq \mathrm{Gal}(L/K)$, 我們知 $\rho \in \mathrm{Gal}(L/K)$. 又對於任意 $\alpha \in F$, 皆有

$$\rho(\alpha) = \sigma^{-1} \circ \tau \circ \sigma(\alpha) = \sigma^{-1}(\tau(\sigma(\alpha))) = \sigma^{-1}(\sigma(\alpha)) = \alpha,$$

因此得 $\rho \in \mathrm{Gal}(L/F)$. 故得 $\tau = \sigma \circ \rho \circ \sigma^{-1} \in \sigma^{-1} \circ \mathrm{Gal}(L/F) \circ \sigma^{-1}$.

反之, 若 $\tau \in \sigma \circ \mathrm{Gal}(L/F) \circ \sigma^{-1}$, 表示存在 $\rho \in \mathrm{Gal}(L/F)$ 滿足 $\tau = \sigma \circ \rho \circ \sigma^{-1}$. 因為 $\mathrm{Gal}(L/K)$ 是一個 group 且 $\rho \in \mathrm{Gal}(L/F) \subseteq \mathrm{Gal}(L/K)$, 我們知 $\tau \in \mathrm{Gal}(L/K)$. 然而對任意 $\alpha \in F$, 因為 ρ 固定 F 中的元素, 所以 $\rho(\alpha) = \alpha$. 因此對任意 $\alpha \in F$ 皆有

$$\tau(\sigma(\alpha)) = \sigma \circ \rho \circ \sigma^{-1}(\sigma(\alpha)) = \sigma(\rho(\alpha)) = \sigma(\alpha).$$

得證 $\tau \in \mathrm{Gal}(L/\sigma(F))$. □

要注意 Lemma 4.1.7 並不需假設 L/K 是 Galois extension. 當 L/K 是 finite Galois extension, 利用 Lemma 4.1.7 我們可得到第二個 fundamental theorem.

Theorem 4.1.8 (Second Fundamental Theorem of Galois Theory)**.** *假設 L/K 是 finite Galois extension 且 F 是 L/K 的一個 intermediate field. 則 F/K 是 Galois extension 若且唯若 $\mathrm{Gal}(L/F)$ 是 $\mathrm{Gal}(L/K)$ 的 normal subgroup. 而且當 F/K 是 Galois extension 時, $\mathrm{Gal}(F/K)$ 和 $\mathrm{Gal}(L/K)/\mathrm{Gal}(L/F)$ 是 isomorphic.*

Proof. 首先回顧 H 是一個 group G 的 normal subgroup 表示 H 是 G 的 subgroup 且對任意 $g \in G$ 皆有 $g \cdot H \cdot g^{-1} = H$.

現若 F/K 是 Galois extension, 則依定義知 F/K 是 finite normal extension. 對任意 $\sigma \in \mathrm{Gal}(L/K)$, 由於 $\sigma|_F : F \to L$ 是一個 F 到 L 的 K-monomorphism, 故由 Lemma 3.2.6 知 $\sigma|_F$ 是一個 F 到 F 的 K-monomorphism. 換句話說 $\sigma(F) = F$, 因此由 Lemma 4.1.7 知

$$\mathrm{Gal}(L/F) = \mathrm{Gal}(L/\sigma(F)) = \sigma \circ \mathrm{Gal}(L/F) \circ \sigma^{-1}.$$

又因為 $\mathrm{Gal}(L/F)$ 是 $\mathrm{Gal}(L/K)$ 的 subgroup, 故得證 $\mathrm{Gal}(L/F)$ 是 $\mathrm{Gal}(L/K)$ 的 normal subgroup.

反之, 若 $\mathrm{Gal}(L/F)$ 是 $\mathrm{Gal}(L/K)$ 的 normal subgroup, 表示對任意 $\sigma \in \mathrm{Gal}(L/K)$ 皆有 $\mathrm{Gal}(L/F) = \sigma \circ \mathrm{Gal}(L/F) \circ \sigma^{-1}$. 故由 Lemma 4.1.7 知 $\mathrm{Gal}(L/F) = \mathrm{Gal}(L/\sigma(F))$. 也就是說對任意 $\sigma \in \mathrm{Gal}(L/K)$ 皆有 $\mathcal{G}(F) = \mathcal{G}(\sigma(F))$. 由於 L/K 是 Galois extension, 故得 $\mathcal{G} : \mathfrak{F} \to \mathfrak{G}$ 是一對一的函數 (Theorem 4.1.5), 因此對任意 $\sigma \in \mathrm{Gal}(L/K)$ 皆有 $\sigma(F) = F$. 換言之, 對任意 $\sigma \in \mathrm{Gal}(L/K)$, 皆有 $\sigma|_F : F \to F$ 是 F 到 F 的 K-monomorphism, 因此知 $\sigma|_F \in \mathrm{Gal}(F/K)$. 現考慮函數 $\Psi : \mathrm{Gal}(L/K) \to \mathrm{Gal}(F/K)$, 使得對任意 $\sigma \in \mathrm{Gal}(L/K)$, 定義 $\Psi(\sigma) = \sigma|_F$. 很容易得知 Ψ 是一個 group homomorphism. 若 $\tau \in \mathrm{Gal}(F/K)$, 則由於 $F \subseteq L$ 可將 τ 視為 F 到 L 的 K-monomorphism. 又因為 L/K 是 normal extension, 故利用 Theorem 3.2.7 知存在 $\sigma \in \mathrm{Gal}(L/K)$ 使得 $\sigma|_F = \tau$. 也就是說, 對任意 $\tau \in \mathrm{Gal}(F/K)$ 皆存在 $\sigma \in \mathrm{Gal}(L/K)$ 使得 $\Psi(\sigma) = \tau$. 證得 $\Psi : \mathrm{Gal}(L/K) \to \mathrm{Gal}(F/K)$ 是 onto. 接著我們要探討 $\ker(\Psi)$ (即 Ψ 的 kernel) 為何. 若 $\sigma \in \ker(\Psi)$, 表示 $\Psi(\sigma) = \sigma|_F$ 是 $\mathrm{Gal}(F/K)$ 的 identity. 亦即對任意 $\lambda \in F$ 皆有 $\sigma(\lambda) = \sigma|_F(\lambda) = \lambda$. 因此知 $\sigma : L \to L$ 將 F 的元素固定, 也就是說 $\sigma \in \mathrm{Gal}(L/F)$. 另一方面若 $\sigma \in \mathrm{Gal}(L/F)$, 則依定義 σ 將 F 的元素固定, 故知 $\sigma|F : F \to F$ 是 identity. 也就是說 $\sigma \in \ker(\Psi)$, 得證 $\ker(\Psi) = \mathrm{Gal}(L/F)$. 因此利用 group 的 first isomorphism 定理 (參見大學基礎代數講義Theorem 2.6.1) 得知:

$$\mathrm{Gal}(F/K) \simeq \mathrm{Gal}(L/K)/\ker(\Psi) = \mathrm{Gal}(L/K)/\mathrm{Gal}(L/F).$$

最後利用已知 L/K 為 finite Galois extensions, 得到 L/F 亦為 finite Galois extensions, 所以 $|\mathrm{Gal}(L/K)| = [L : K]$ 以及 $|\mathrm{Gal}(L/F)| = [L : F]$. 因此得

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

故利用 Theorem 4.1.1 得證 F/K 是 Galois extension. □

要注意 Theorem 4.1.8 事實上就是證明在 L/K 是 finite Galois extension 的前提之下, F/K 是 normal extension 若且唯若 $\mathrm{Gal}(L/F)$ 是 $\mathrm{Gal}(L/K)$ 的 normal subgroup. 不過在 F/K 是 normal extension 推導得 $\mathrm{Gal}(L/F)$ 是 $\mathrm{Gal}(L/K)$ 的 normal subgroup 的過程中

我們僅需 L/K 是 normal extension 的假設 (即不需 L/K 是 separable extension). 不過由 $\mathrm{Gal}(L/F)$ 是 $\mathrm{Gal}(L/K)$ 的 normal subgroup 推導得 F/K 是 normal extension 的過程中我們需要 L/K 是 Galois extension 的假設 (即不只 L/K 是 normal extension 且需 L/K 是 separable extension). 比方說證明中我們用到了 $\mathcal{G}$ 是 1-1 的性質就需 L/K 是 Galois extension 才會對.

我們已經介紹完了在大學代數中需了解的 Galois 理論. 如果你只想知道 Galois 理論是什麼, 那麼原則上讀到這裡已經達到了這個目的, 可以不必繼續研讀下去. 不過若沒有探討一些相關的應用或例子, 或許大家無法理解如何運用這些理論以及其重要性. 從歷史的角度來看, Galois 理論的應用最好的例子, 就是解決了一般多項式方程式的公式解問題以及一些尺規作圖問題. 不過談論這些例子需要再探討一些 Group Theory 的問題. 一來我們不想將討論的東西複雜化以致掩蓋了我們要探討 Galois 理論的目的; 二來這些例子的結論在更進階的代數理論中並沒有太多的用處. 因此我們選擇不去探討這些古典的問題, 而在接下來幾節中談論一些在探討更進階的代數理論時可能比較需要的應用與例子.

4.2. Galois 理論的應用

這一節中我們介紹兩個 Galois 理論的應用: 一個是探討 finite separable extension 一定是 simple extension; 另一個我們介紹 trace 和 norm 的基本性質.

Galois Theory 雖然是針對 Galois extension, 不過在不是 Galois extension 時也能應用. 最常見的情況是在 finite separable extension 時, 我們可以取 normal closure 而得到 Galois extension 再加以應用.

Lemma 4.2.1. *假設 L/K 是 finite separable extension 且 N 是 L/K 的 normal closure. 則 N/K 是 finite Galois extension.*

Proof. 因為 L/K 是 finite extension, 存在 $a_1, \ldots, a_n \in L$ 使得 $L = K(a_1, \ldots, a_n)$. 假設 a_i over K 的 minimal polynomial 為 $p_i(x)$. 因為 L/K 是 separable extension, 這些 $p_i(x) \in K[x]$ 皆為 separable polynomials. 若令 $f(x) = p_1(x) \cdots p_n(x)$, 則由 normal closure 的定義知 N 為 $f(x)$ over K 的 splitting field 且知 N/K 是 finite normal extension (Proposition 3.2.9).

現假設 $\alpha_1, \ldots, \alpha_m \in N$ 為 $f(x)$ 所有的根, 則 $N = K(\alpha_1, \ldots, \alpha_m)$. 然而每一個 α_j 因為是 $f(x) = p_1(x) \cdots p_n(x)$ 的一個根, 所以其 over K 的 minimal polynomial 必為 $p_1(x), \ldots, p_n(x)$ 其中之一. 因此由 $p_1(x), \ldots, p_n(x)$ 皆為 separable polynomials 知 $\alpha_1, \ldots, \alpha_m$ 皆為 separable element over K. 故由 Theorem 3.4.7 知 N/K 是 separable extension. 因此 N/K 是 finite Galois extension. □

當然了若 L/K 本身已不是 separable extension, 表示 L 中存在元素不是 separable element over K, 因此不論怎麼作 L 的 extension 都不可能成為 separable extension. 所以在這情況之下取 L/K 的 normal closure N, 並無法使得 N/K 是 Galois extension.

4.2.1. Primitive Element Theorem. 我們曾經特別介紹 finite simple extension. 可以發現在 simple extension 的情況之下, 很多問題都可以簡單清楚的處理. 事實上我們證過很多有關 finite extension 問題都是先處理 simple extension 的情況, 再用 induction 處理. 總之, 若能事先知道一個 field extension 是 simple extension, 那麼很多問題就能輕鬆解決. 甚麼時候一個 extension 會是 simple extension 呢? primitive element theorem 就是在說明所有 finite separable extension 皆為 simple extension.

Theorem 4.2.2 (Primitive Element Theorem)**.** *假設 L/K 是一個 finite separable extension, 則 L/K 是一個 simple extension.*

Proof. 我們分 K 是 finite field 和 K 不是 finite field 兩種情況來討論.

首先考慮 K 是 finite field 的情況. 此時由於 L/K 是 finite extension, 故知 L 也是一個 finite field. 因為一個 finite field 中的非 0 元素所成的乘法群是一個 cyclic group (參見大學基礎代數講義Theorem 10.4.3), 所以存在 $\alpha \in L$ 使得 L 中的非 0 元素都可以用 α^i, 其中 $i \in \mathbb{N}$ 來表示. 換言之, $L = K(\alpha)$, 所以 L/K 是 simple extension.

現考慮 K 是 infinite 的情況. 因為 L/K 是 finite separable extension, 由 Lemma 4.2.1 知若取 L/K 的一個 normal closure, 則 N/K 是 finite Galois extension. 利用 First Fundamental Theorem 4.1.5, 我們知道 N/K 的 intermediate fields 和 $\mathrm{Gal}(N/K)$ 的 subgroups 之間有一個 1-1 correspondence. 又因為 N/K 是 finite extension, 所以 $\mathrm{Gal}(N/K)$ 是一個 finite group (事實上 $|\mathrm{Gal}(N/K)| = [N : K]$), 因此 $\mathrm{Gal}(N/K)$ 只有有限多個 subgroups. 推得 N/K 只有有限多個 intermediate fields. 但由於 $K \subseteq L \subseteq N$, 故知 L/K 只有有限多個 intermediate fields. 由於 $[L : K]$ 是有限的, 必存在 $a \in L$ 使得 $[K(a) : K]$ 是最大的, 也就是說 $a \in L$ 滿足 $[K(a) : K] \geq [K(b) : K], \forall b \in L$. 我們要證明 $L = K(a)$. 假設 $K(a) \neq L$, 表示存在 $b \in L$ 但 $b \notin K(a)$. 現考慮所有 $K(a + cb)$ 其中 $c \in K$, 這種形式的 L/K 的 intermediate fields. 因為 L/K 只有有限多個 intermediate fields 且 K 有無窮多個元素, 利用鴿籠原理, 必存在 $c_1, c_2 \in K$ 且 $c_1 \neq c_2$ 滿足 $K(a + c_1b) = K(a + c_2b)$. 所以利用 $a + c_2b \in K(a + c_1b)$ 可得

$$(c_1 - c_2)b = (a + c_1b) - (a + c_2b) \in K(a + c_1b).$$

又因為 $c_1 - c_2 \in K$ 且 $c_1 - c_2 \neq 0$ 得知 $b \in K(a + c_1b)$. 再利用 $a = (a + c_1b) - c_1b$ 得知 $a \in K(a + c_1b)$. 換言之 $K(a) \subseteq K(a + c_1b)$. 但由於 $b \in K(a + c_1b)$ 且 $b \notin K(a)$ 知 $K(a) \subsetneq K(a + c_1b)$. 也就是說

$$[K(a + c_1b) : K] = [K(a + c_1b) : K(a)][K(a) : K] > [K(a) : K].$$

此和當初 a 的選取矛盾, 故得證 $L = K(a)$. □

利用這個結果, 今後要探討 finite separable extension 的問題時就可以直接假設它是一個 simple extension, 這樣要處理的問題就簡單多了. 可知這是一個相當實用的定理.

4.2.2. Trace and Norm. Trace 和 norm 是談論 finite extension 時兩個重要的函數.

Definition 4.2.3. 假設 L/K 是一個 finite separable extension 且 N 是 L/K 的一個 normal closure. 令 $\mathfrak{M}_K(L,N)=\{\sigma_1,\dots,\sigma_n\}$ 為所有 L 到 N 的 K-monomorphisms 所成的集合. 若 $a\in L$, 我們定義

$$\mathrm{T}_{L/K}(a)=\sigma_1(a)+\cdots+\sigma_n(a)\quad\text{and}\quad \mathrm{N}_{L/K}(a)=\sigma_1(a)\cdots\sigma_n(a).$$

$\mathrm{T}_{L/K}(a)$ 和 $\mathrm{N}_{L/K}(a)$ 分別稱作 a 的 *trace* 和 *norm* for L/K.

要注意 trace 和 norm 的取值與 extension 有關. 例如若 F 是 L/K 的 intermediate field 且 $a\in F$, 則 $T_{L/K}(a)$ 和 $T_{F/K}(a)$ 可能不同; 同樣的 $N_{L/K}(a)$ 和 $N_{F/K}(a)$ 也可能不同. 接下來我們介紹一些 trace 和 norm 的基本性質.

Lemma 4.2.4. *假設 L/K 是一個 finite separable extension 且 $[L:K]=n$. 則對任意 $a,b\in L$ 以及 $k\in K$, 我們有以下的性質:*

(1) $\mathrm{T}_{L/K}(ka+b)=k\mathrm{T}_{L/K}(a)+\mathrm{T}_{L/K}(b)$ 且 $\mathrm{N}_{L/K}(ab)=\mathrm{N}_{L/K}(a)\mathrm{N}_{L/K}(b)$.

(2) $\mathrm{T}_{L/K}(k)=nk$ 且 $\mathrm{N}_{L/K}(k)=k^n$.

Proof. 假設 N 是 L/K 的一個 normal closure. 因為 L/K 是 finite separable extension, 由 Theorem 3.4.5 知 $|\mathfrak{M}_K(L,N)|=[L:K]=n$. 現假設 $\mathfrak{M}_K(L,N)=\{\sigma_1,\dots,\sigma_n\}$.

(1) 由於 σ_i 是 K-monomorphism, 我們有 $\sigma_i(ka+b)=k\sigma_i(a)+\sigma_i(b)$, 因此依定義得

$$\mathrm{T}_{L/K}(ka+b)=\sum_{i=1}^{n}\sigma_i(ka+b)=k\sum_{i=1}^{n}\sigma_i(a)+\sum_{i=1}^{n}\sigma_i(b)=k\mathrm{T}_{L/K}(a)+\mathrm{T}_{L/K}(b).$$

同理, 因為 $\sigma_i(ab)=\sigma_i(a)\sigma_i(b)$, 故得

$$\mathrm{N}_{L/K}(ab)=\sigma_1(ab)\cdots\sigma_n(ab)=(\sigma_1(a)\sigma_1(b))\cdots(\sigma_n(a)\sigma_n(b))=N_{L/K}(a)N_{L/K}(b).$$

(2) 由於 $\sigma_i(k)=k$, 故直接依定義知

$$T_{L/K}(k)=\sigma_1(k)+\cdots+\sigma_n(k)=nk\quad\text{and}\quad \mathrm{N}_{L/K}(k)=\sigma_1(k)\cdots\sigma_n(k)=k^n.$$

□

當 L/K 是 Galois extension 時, 因為 L/K 是 normal extension, 故由 Lemma 3.2.6 得 $\mathfrak{M}_K(L,N)=\mathrm{Gal}(L/K)$, 因此若 $\mathrm{Gal}(L/K)=\{\sigma_1,\dots,\sigma_n\}$, 則對任意$\tau\in\mathrm{Gal}(L/K)$, 由於 $\mathrm{Gal}(L/K)$ 是一個 group, 我們有 $\mathrm{Gal}(L/K)=\{\tau\circ\sigma_1,\dots,\tau\circ\sigma_n\}$. 因此依定義知

$$\tau(\mathrm{T}_{L/K}(a))=\tau(\sigma_1(a)+\cdots\sigma_n(a))=\tau(\sigma_1(a))+\cdots+\tau(\sigma_n(a))=\mathrm{T}_{L/K}(a).$$

同理知 $\tau(\mathrm{N}_{L/K}(a))=\mathrm{N}_{L/K}(a)$. 也就是說 $\mathrm{T}_{L/K}(a)$ 和 $\mathrm{N}_{L/K}(a)$ 皆落在 $\mathrm{Gal}(L/K)$ 的 fixed field 中. 但由於假設 L/K 是 Galois extension, 故由 Theorem 4.1.1 知 $\mathrm{Gal}(L/K)$ 的 fixed field 為 K, 得證 $\mathrm{T}_{L/K}(a)\in K$ 且 $\mathrm{N}_{L/K}(a)\in K$. 當 L/K 僅是 finite separable extension 時, 我們依然可利用 Galois 理論證得 $\mathrm{T}_{L/K}(a)\in K$ 且 $\mathrm{N}_{L/K}(a)\in K$.

Proposition 4.2.5. *假設 L/K 是 finite separable extension. 則對任意 $a \in L$, 皆有*

$$\mathrm{T}_{L/K}(a) \in K \quad \text{and} \quad \mathrm{N}_{L/K}(a) \in K.$$

Proof. 若 N 是 L/K 的一個 normal closure, 則由 Lemma 4.2.1 知 N/K 是 finite Galois extension. 假設 $\mathfrak{M}_K(L,N) = \{\sigma_1, \ldots, \sigma_n\}$. 對任意 $\tau \in \mathrm{Gal}(N/K)$, 由於 $\tau \circ \sigma_i : L \to N$ 是 K-monomorphism, 我們知 $\tau\sigma_i \in \mathfrak{M}_K(L,N)$. 又若 $\tau \circ \sigma_i = \tau \circ \sigma_j$, 則因 τ 是 1-1 可得 $\sigma_i = \sigma_j$. 因此我們知對任意 $\tau \in \mathrm{Gal}(N/K)$ 皆有 $\mathfrak{M}_K(L,N) = \{\tau \circ \sigma_1, \ldots, \tau \circ \sigma_n\}$. 所以依定義知對任意 $\tau \in \mathrm{Gal}(N,K)$ 皆有

$$\tau(\mathrm{T}_{L/K}(a)) = \tau(\sigma_1(a) + \cdots \sigma_n(a)) = \tau(\sigma_1(a)) + \cdots + \tau(\sigma_n(a)) = \mathrm{T}_{L/K}(a).$$

同理知 $\tau(\mathrm{N}_{L/K}(a)) = \mathrm{N}_{L/K}(a)$. 也就是說 $\mathrm{T}_{L/K}(a)$ 和 $\mathrm{N}_{L/K}(a)$ 皆落在 $\mathrm{Gal}(N/K)$ 的 fixed field 中. 故由 N/K 是 Galois extension 以及 Theorem 4.1.1 知 $\mathrm{T}_{L/K}(a) \in K$ 且 $\mathrm{N}_{L/K}(a) \in K$. □

若 L/K 是 finite separable extension 且 F 是 L/K 的 intermediate field, 則 L/F 和 F/K 皆為 finite separable extension (Lemma 3.4.2), 所以我們有 L/F 和 F/K 的 trace 和 norm. 現若 $a \in L$, 則由 Proposition 4.2.5 知 $\mathrm{T}_{L/F}(a)$ 和 $\mathrm{N}_{L/F}(a)$ 皆為 F 中的元素, 所以可以將它們代入 $\mathrm{T}_{F/K}$ 以及 $\mathrm{N}_{F/K}$ 中, 得 $\mathrm{T}_{F/K}(\mathrm{T}_{L/F}(a))$ 以及 $\mathrm{N}_{F/K}(\mathrm{N}_{L/F}(a))$. 事實上它們會分別等於 $\mathrm{T}_{L/K}(a)$ 以及 $\mathrm{N}_{L/K}(a)$, 這就是 trace 和 norm 的 transitive property.

Proposition 4.2.6. *假設 L/K 是 finite separable extension 且 F 是 L/K 的 intermediate field. 則對任意 $a \in L$, 皆有*

$$\mathrm{T}_{F/K}(\mathrm{T}_{L/F}(a)) = \mathrm{T}_{L/K}(a) \quad \text{and} \quad \mathrm{N}_{F/K}(\mathrm{N}_{L/F}(a)) = \mathrm{N}_{L/K}(a).$$

Proof. 若 N 是 L/K 的一個 normal closure, 則由於 N/K 是 normal extension 且 $F \subseteq L \subseteq N$, 利用 normal closure 的定義知存在 N' 是 F/K 的 normal closure 且 $N' \subseteq N$.

假設 $\mathfrak{M}_F(L,N) = \{\rho_1, \ldots, \rho_s\}$ 且 $\mathfrak{M}_K(F,N) = \{\psi_1, \ldots, \psi_t\}$, 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 知每一個 K-monomorphism $\psi_j : F \to N$ 都可以 extends 成一個 K-monomorphism $\phi_j : N \to N$ (即 $\phi_j|_F = \psi_j$). 在 Lemma 3.2.12 的證明中我們證得

$$\mathfrak{M}_K(L,N) = \{\phi_j \circ \rho_i \,|\, i = 1, \ldots, s \text{ 且 } j = 1, \ldots, t\}.$$

因此知

$$\mathrm{T}_{L/K}(a) = \sum_{j=1}^{t}\sum_{i=1}^{s} \phi_j(\rho_i(a)) = \sum_{j=1}^{t} \phi_j(\sum_{i=1}^{s} \rho_i(a)) = \sum_{j=1}^{t} \phi_j(\mathrm{T}_{L/F}(a)).$$

另一方面利用 Corollary 3.2.11 我們知 $\mathfrak{M}_K(F,N') = \mathfrak{M}_K(F,N) = \{\psi_1, \ldots, \psi_t\}$ 以及利用 Proposition 4.2.5 我們知 $\mathrm{T}_{L/F}(a) \in F$, 因此 $\phi_j(\mathrm{T}_{L/F}(a)) = \phi_j|_F(\mathrm{T}_{L/F}(a)) = \psi_j(\mathrm{T}_{L/F}(a))$. 故得

$$\mathrm{T}_{F/K}(\mathrm{T}_{L/F}(a)) = \sum_{j=1}^{t} \psi_j(\mathrm{T}_{L/F}(a)) = \sum_{j=1}^{t} \phi_j(\mathrm{T}_{L/F}(a)) = \mathrm{T}_{L/K}(a).$$

同理證得

$$\mathrm{N}_{F/K}(\mathrm{N}_{L/F}(a)) = \prod_{j=1}^{t} \psi_j(\mathrm{N}_{L/F}(a)) = \prod_{j=1}^{t}\prod_{i=1}^{s} \phi_j(\rho_i(a)) = \mathrm{N}_{L/K}(a).$$

□

因為一個 finite extension 的 normal closure 並不唯一, 由定義 trace 和 norm 的取值可能會和 normal closure 的選取有關. 我們最後就是要探討這個問題, 事實上我們得到一個元素的 trace 與 norm 和它的 minimal polynomial 有關, 也因此得知 trace 和 norm 和 normal closure 的選取無關.

Theorem 4.2.7. *假設 L/K 是 finite separable extension 且 $[L:K]=n$. 若 $a \in L$ 且 a over K 的 minimal polynomial 為 $f(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$, 則*

$$\mathrm{T}_{L/K}(a) = -\frac{n}{m}\, a_{m-1} \quad \text{and} \quad \mathrm{N}_{L/K}(a) = (-1)^n a_0^{n/m}.$$

Proof. 令 $F = K(a)$, 由於 $f(x)$ 是 a over K 的 minimal polynomial 且 $\deg(f(x)) = m$, 知 $[F:K] = m$, 故得 $[L:F] = [L:K]/[F:K] = n/m$. 因此由 $a \in F$ 以及 Lemma 4.2.4 (2) 知 $\mathrm{T}_{L/F}(a) = (n/m)a$ 以及 $\mathrm{N}_{L/F}(a) = a^{n/m}$. 接著我們要計算 $\mathrm{T}_{F/K}(a)$ 以及 $\mathrm{N}_{F/K}(a)$.

令 N 為 F/K 的一個 normal closure, 因為 L/K 是 finite separable extension, 故知 F/K 也是 finite separable extension (Lemma 3.4.2), 因此由 Theorem 3.4.5 知 $|\mathfrak{M}_K(F,N)| = [F:K] = m$. 假設 $\mathfrak{M}_K(F,N) = \{\sigma_1, \ldots, \sigma_m\}$. 由於 $F = K(a)$ 是一個 over K 的 simple extension, 每一個 F 到 N 的 K-monomorphism 都由 a 的取值唯一確定. 所以得 $\sigma_1(a), \ldots, \sigma_m(a)$ 皆相異. 又因為 $\sigma_i(a)$ 必為 $f(x)$ 的根, 所以得 $\sigma_1(a), \ldots, \sigma_m(a)$ 剛好就是 $f(x)$ 所有的根. 故得 $f(x) = (x-\sigma_1(a))\cdots(x-\sigma_m(a))$. 利用根與係數的關係, 我們得到

$$\mathrm{T}_{F/K}(a) = \sigma_1(a) + \cdots + \sigma_m(a) = -a_{m-1}$$

以及

$$\mathrm{N}_{F/K}(a) = \sigma_1(a)\cdots\sigma_m(a) = (-1)^m a_0.$$

因此利用 Proposition 4.2.6 以及 Lemma 4.2.4 (1) 得證

$$\mathrm{T}_{L/K}(a) = \mathrm{T}_{F/K}(T_{L/F}(a)) = \mathrm{T}_{F/K}(\frac{n}{m}\, a) = \frac{n}{m} T_{F/K}(a) = -\frac{n}{m}\, a_{m-1}$$

以及

$$\mathrm{N}_{L/K}(a) = \mathrm{N}_{F/K}(N_{L/F}(a)) = \mathrm{N}_{F/K}(a^{n/m}) = N_{F/K}(a)^{n/m} = ((-1)^m a_0)^{n/m} = (-1)^n a_0^{n/m}.$$

□

由 Theorem 4.2.7 可以看出, 不僅 $\mathrm{T}_{L/K}(a) \in K$ 且 $\mathrm{N}_{L/K}(a) \in K$ 而且 trace 和 norm 的取值和 L/K 的 normal closure 的選取無關.

4.3. Galois 理論的例子

在這最後一節中, 我們介紹兩種重要的 fields: finite fields 和 cyclotomic fields. 並介紹它們的 Galois groups.

4.3.1. Finite Fields. 首先我們簡單的回顧一下有關 finite field 的基本性質, 詳細情形可參考大學基礎代數講義Chapter 10 Section 4.

若 K 是一個 finite field 我們知 K 的 characteristic 一定是一個質數 p. 也就是說對任意 $a \in K$ 皆有 $pa = 0$, 由此可推出若 $a, b \in K$, 則 $(a+b)^p = a^p + b^p$ 甚而用 induction 得到對任意 $m \in \mathbb{N}$ 皆有 $(a+b)^{p^m} = a^{p^m} + b^{p^m}$. 由於 K 的 characteristic 為 p, 我們知 $\mathbb{F}_p = \{0, 1, \cdots, p-1\}$ 為一個 field (事實上 $\mathbb{F}_p \simeq \mathbb{Z}/p\mathbb{Z}$) 且包含於 K. 因此得 $K/\mathbb{F}_p$ 是一個 finite extension. 假若 $[K : \mathbb{F}_p] = n$, 則可得 $|K| = p^n$, 因此所有的 finite field 的元素個數都是 p^n 這種形式.

現假設 K 是 finite field 且 $|K| = p^n$. 由於 $K^* = K \setminus \{0\}$ 是一個 order 為 $p^n - 1$ 的乘法群故由 Lagrange theorem 知對任意 $a \in K^*$ 皆有 $a^{p^n-1} = 1$, 因此 K 中元素 (包括 0) 都滿足 $x^{p^n} - x = 0$. 但由於 $x^{p^n} - x$ 至多只有 p^n 個根, 所以 K 中元素剛好就是 $x^{p^n} - x$ 的所有的根. 得知 K 是 $x^{p^n} - x$ over $\mathbb{F}_p$ 的 splitting field. 由於 splitting filed 的唯一性 (Proposition 3.1.8) 而後提到 $q = p^n$ 個元素的 finite field 我們都用 $\mathbb{F}_q$ 來表示.

假如 $L/\mathbb{F}_q$ 是一個 finite extension 且 $[L : \mathbb{F}_q] = m$, 則知 $|L| = q^m$, 換言之 $L = \mathbb{F}_{q^m}$. 現考慮一個函數 $\varphi_q : \mathbb{F}_{q^m} \to \mathbb{F}_{q^m}$ 定義為 $\varphi_q(\alpha) = \alpha^q, \forall\, \alpha \in \mathbb{F}_{q^m}$. 由於對任意 $\alpha, \beta \in \mathbb{F}_{q^m}$ 皆有

$$\varphi_q(\alpha + \beta) = (\alpha + \beta)^q = \alpha^q + \beta^q = \varphi_q(\alpha) + \varphi_q(\beta)$$

以及

$$\varphi_q(\alpha\beta) = (\alpha\beta)^q = \alpha^q\beta^q = \varphi_q(\alpha)\varphi_q(\beta),$$

我們得知 φ_q 是一個 $\mathbb{F}_{q^m}$ 到 $\mathbb{F}_{q^m}$ 的 ring homomorphism. 又因為 $\mathbb{F}_{q^m}$ 是一個 field 且對任意 $a \in K$ 皆有 $\varphi_q(a) = a^q = a$, 故知 φ_q 是一個 $\mathbb{F}_{q^m}$ 到 $\mathbb{F}_{q^m}$ 的 $\mathbb{F}_q$-monomorphism. 也就是說 $\varphi_q \in \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$. 我們稱 φ_q 為 $\mathbb{F}_{q^m}/\mathbb{F}_q$ 的*Frobenius automorphism.*

Theorem 4.3.1. *假設 $L/\mathbb{F}_q$ 是一個 finite extension, 則 $L/\mathbb{F}_q$ 是一個 Galois extension. 若 $\varphi_q : L \to L$ 滿足 $\varphi_q(\alpha) = \alpha^q, \forall\, \alpha \in L$ 為 $L/\mathbb{F}_q$ 的 Frobenius automorphism, 則 $\mathrm{Gal}(L/\mathbb{F}_q)$ 是一個 cyclic group generated by φ_q.*

Proof. 假設 $[L : \mathbb{F}_q] = m$. 前面已知 $\varphi_q \in \mathrm{Gal}(L/\mathbb{F}_q)$. 考慮 $H = \langle \varphi_q \rangle$ 為 $\mathrm{Gal}(L/\mathbb{F}_q)$ 的一個 generated by φ_q 的 cyclic subgroup. 若能證得 φ_q 的 order 為 m, 則知 $|H| = m$ 且由 Proposition 2.3.3 知

$$m = [L : \mathbb{F}_q] \geq |\mathrm{Gal}(L/\mathbb{F}_q)| \geq |H| = m,$$

因而得證 $[L : \mathbb{F}_q] = |\mathrm{Gal}(L/\mathbb{F}_q)| = |H|$. 因此若能證得 φ_q 的 order 為 m, 則我們同時證得 $L/\mathbb{F}_q$ 是 Galois extension (Theorem 4.1.1) 且 $\mathrm{Gal}(L/\mathbb{F}_q) = H = \langle \varphi_q \rangle$.

現在要計算 φ_q 的 order. 首先因為 $|L| = q^m$, 因此 $L^* = L \setminus \{0\}$ 是一個 order 為 $q^m - 1$ 的 cyclic group. 假設 β 為其 generator. 若 φ_q 的 order 為 r, 則 φ_q^r 是 identity, 也就是說 $\varphi_q^r(\beta) = \beta$. 注意 $\varphi_q^2 = \varphi_q \circ \varphi_q$, 亦即

$$\varphi_q^2(\beta) = \varphi_q(\varphi_q(\beta)) = \varphi_q(\beta^q) = \beta^{q^2}.$$

因此利用 induction 知 $\varphi_q^r(\beta)=\beta^{q^r}$, 故由 $\varphi_q^r(\beta)=\beta$ 得 $\beta^{q^r}=\beta$. 也就是說 $\beta^{q^r-1}=1$. 但是 β 的 order 為 q^m-1, 得知 $q^r-1\geq q^m-1$, 亦即 $r\geq m$. 另一方面對任意 $\alpha\in L$, 由於 $\varphi_q^m(\alpha)=\alpha^{q^m}=\alpha$ (別忘了 $|L|=q^m$), 我們知 φ_q^m 是 identity, 故利用 φ_q 的 order 為 r 的假設知 $r\leq m$. 我們證得 φ_q 的 order 為 m, 故得證本定理. □

當一個 field extension 是 Galois extension 且其 Galois group 是 cyclic group 時, 我們稱此 extension 為 *cyclic extension*. Theorem 4.3.1 就是告訴我們任意 finite field 的 finite extension 都是 cyclic extension.

一般來說當 L/K 是一個 cyclic extension 且 $[L:K]=m$ 時, 我們知 $\mathrm{Gal}(L/K)$ 是一個 order m 的 cyclic group. 由 cyclic group 的性質知, 對任意滿足 $s\,|\,m$ 的正整數 s 皆存在唯一的 subgroup $H\subseteq\mathrm{Gal}(L/K)$ 滿足 $|H|=s$. 反之若 H 是 $\mathrm{Gal}(L/K)$ 的 subgroup, 由 Lagrange Theorem 知 $|H|\,|\,m$. 另外因為 $\mathrm{Gal}(L/K)$ 是 cyclic group, 所以 $\mathrm{Gal}(L/K)$ 的 subgroup H 都是 normal subgroup, 而且 H 以及 $\mathrm{Gal}(L/K)/H$ 都是 cyclic groups. 綜合這些結果, 由 First Fundamental Theorem 4.1.5 我們知道對任意 $s\,|\,m$, 存在唯一的 L/K 的 intermediate field F 滿足 $[L:F]=s$, 而且我們知 $\mathrm{Gal}(L/F)$ 是一個 cyclic group of order s. 另外因為 $\mathrm{Gal}(L/F)$ 是 $\mathrm{Gal}(L/K)$ 的 normal subgroup, 所以由 Second Fundamental Theorem 4.1.8 知 F/K 也是 Galois extension, 而且 $\mathrm{Gal}(F/K)$ isomorphic to $\mathrm{Gal}(L/K)/\mathrm{Gal}(L/F)$ 也是一個 cyclic group. 這些結果都可套用到 $K=\mathbb{F}_q$ 的情形, 而且當 F 是 $L/\mathbb{F}_q$ 的 intermediate field 時, 將 L/F 以及 $F/\mathbb{F}_q$ 套用 Theorem 4.3.1 的結果是和我們以上的討論結果相吻合的.

4.3.2. Cyclotomic Fields. 當 n 為大於 2 的整數, 則 x^n-1 over $\mathbb{Q}$ 的 splitting field 稱之為 n-th *cyclotomic field*.

假如 L 是 n-th cyclotomic field, 則由 Theorem 4.1.4 知 $L/\mathbb{Q}$ 是 Galois extension, 我們要探討 $L/\mathbb{Q}$ 的 Galois group $\mathrm{Gal}(L/\mathbb{Q})$ 為何. 首先注意所有 x^n-1 的根在乘法群之下形成一個 cyclic group of order n, 事實上若令 $\zeta_n=\cos(2\pi/n)+i\sin(2\pi/n)$ 則知 ζ_n 是其 generator. 換言之若 C_n 是所有 x^n-1 的根所成的集合, 則 $C_n=\{\zeta_n^t\,|\,1\leq t\leq n\}$. 因此我們知 $L=\mathbb{Q}(\zeta_n)$.

現若 $\sigma\in\mathrm{Gal}(L/\mathbb{Q})$, 則 $\sigma(\zeta_n)^n=\sigma(\zeta_n^n)=1$, 故知 $\sigma(\zeta_n)$ 仍為 x^n-1 的一個根. 另一方面若 $\sigma(\zeta_n)^m=1$, 表示 $\sigma(\zeta_n^m)=1$, 故由 σ 是 1-1 知 $\zeta_n^m=1$. 但由於 ζ_n 的 order 為 n, 得證 $n\,|\,m$. 也就是說 $\sigma(\zeta_n)$ 的 order 也是 n. 在 C_n 中 order 是 n 的元素, 我們稱之為*primitive* n-th root of 1. 也就是說若 $\sigma\in\mathrm{Gal}(L/\mathbb{Q})$, 則 $\sigma(\zeta_n)$ 是一個 primitive n-th root of 1.

那麼 C_n 中有多少 primitive n-th root of 1 呢? 現若 ζ_n^t 是一個 primitive n-th root of 1, 則由於 ζ_n^t 的 order 為 $n/\gcd(t,n)$ (參見大學基礎代數講義Proposition 2.3.3) 我們得知 $\gcd(t,n)=1$. 也就是說 primitive n-th root of 1 的個數就是 1 到 n 之間和 n 互質的整數個數. 這個數在整數論中我們用 $\phi(n)$ 來表示, 其中 ϕ 我們稱之為 Euler ϕ-function.

事實上 1 到 n 之間和 n 互質的整數在 $\mathbb{Z}/n\mathbb{Z}$ 中形成一個乘法群, 通常我們都用 $(\mathbb{Z}/n\mathbb{Z})^*$ 來表示. 千萬不要將 $\mathbb{Z}/n\mathbb{Z}$ 和 $(\mathbb{Z}/n\mathbb{Z})^*$ 搞混. 要注意 $\mathbb{Z}/n\mathbb{Z}$ 是一個 order 為 n 的加法群, 而 $(\mathbb{Z}/n\mathbb{Z})^*$ 是一個 order 為 $\phi(n)$ 的乘法群. 另外 $\mathbb{Z}/n\mathbb{Z}$ 是 cyclic group 但 $(\mathbb{Z}/n\mathbb{Z})^*$ 有

可能不是 cyclic group, 不過當然仍是 abelian group. 例如 $\mathbb{Z}/12\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{11}\}$ 是一個 cyclic group generated by $\overline{1}$. 但

$$(\mathbb{Z}/12\mathbb{Z})^* = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\} \quad \text{且} \quad \overline{5}^{\,2} = \overline{25} = \overline{1}, \quad \overline{7}^{\,2} = \overline{49} = \overline{1}, \quad \overline{11}^{\,2} = \overline{121} = \overline{1},$$

所以 $(\mathbb{Z}/12\mathbb{Z})^*$ 是一個 order 為 $\phi(12) = 4$ 的 abelian group 但不是 cyclic group.

要了解 $\mathrm{Gal}(L/\mathbb{Q})$ 首先就需要知道 $[L : \mathbb{Q}]$ 為何, 由於 $L = \mathbb{Q}(\zeta_n)$, 所以我們要知道 ζ_n over $\mathbb{Q}$ 的 minimal polynomial 的 degree 為何. 前面已知若 $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$, 則 $\sigma(\zeta_n) = \zeta_n^t$, 其中 $1 \le t \le n$ 且滿足 $\gcd(t, n) = 1$, 又由於 $\sigma(\zeta_n)$ 必為 ζ_n over $\mathbb{Q}$ 的 minimal polynomial 的一個根, 所以我們很自然會考慮以下的多項式:

$$f_n(x) = \prod_{1 \le t \le n,\, \gcd(t,n)=1} (x - \zeta_n^t).$$

這個多項式我們稱為 n-th cyclotomic polynomial. 以下我們要證明 $f_n(x) \in \mathbb{Q}[x]$ 且是 $\mathbb{Q}[x]$ 中的 irreducible polynomial, 因而得知 $f_n(x)$ 是 ζ_n over $\mathbb{Q}$ 的 minimal polynomial. 這個證明點煩雜, 我們需要好幾個步驟來證明. 若接受這事實, 可以直接跳過從 Theorem 4.3.5 繼續研讀.

首先我們要證明 $f_n(x) \in \mathbb{Z}[x]$, 再利用 $\mathbb{Z}[x]$ 上的分解性質證明 $f_n(x)$ 是 $\mathbb{Q}[x]$ 中的 irreducible polynomial.

Lemma 4.3.2. *若 $f_n(x)$ 是 n-th cyclotomic polynomial, 則 $f_n(x) \in \mathbb{Z}[x]$.*

Proof. 我們要利用和 Theorem 4.1.1 (2) $\Rightarrow$ (3) 的證明類似的方法先證明 $f_n(x) \in \mathbb{Q}[x]$. 若令 $L = \mathbb{Q}(\zeta_n)$, 則 $f_n(x) \in L[x]$. 對任意 $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$, 由於 $\sigma(\zeta_n) = \zeta_n^s$ 其中 $\gcd(s, n) = 1$, 我們知當 $\gcd(t, n) = 1$ 時 $\sigma(\zeta_n^t) = \sigma(\zeta_n)^t = \zeta_n^{st}$ 仍為 primitive n-th root of 1 (因為 $\gcd(st, n) = 1$). 也就是說

$$f_n^\sigma(x) = \prod_{1 \le t \le n,\, \gcd(t,n)=1} (x - \sigma(\zeta_n^t)) = f(x).$$

換言之, $f_n(x)$ 每一項的係數會被 σ 固定住. 也就是說 $f_n(x)$ 每一項的係數會落在 $\mathrm{Gal}(L/\mathbb{Q})$ 的 fixed field 中. 但已知 $L/\mathbb{Q}$ 是 Galois extension, 所以 $\mathrm{Gal}(L/\mathbb{Q})$ 的 fixed field 就是 $\mathbb{Q}$, 故得證 $f_n(x) \in \mathbb{Q}[x]$.

現在我們要證明 $f_n(x) \in \mathbb{Z}[x]$. 由於 $x^n - 1 = \prod_{1 \le t \le n}(x - \zeta_n^t)$, 所以存在 $g(x) \in L[x]$ 使得 $x^n - 1 = f_n(x)g(x)$. 對任意 $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$, 將 σ 作用到兩邊多項式的係數, 得 $x^n - 1 = f_n^\sigma(x)g^\sigma(x) = f_n(x)g^\sigma(x)$. 因此由 $\mathbb{Q}[x]$ 上的唯一分解性質, 得知對任意 $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ 皆有 $g^\sigma(x) = g(x)$. 故知 $g(x) \in \mathbb{Q}[x]$. 現因為 $f_n(x)$ 和 $g(x)$ 都是 $\mathbb{Q}[x]$ 中的 monic polynomial, 所以存在 $c_1, c_2 \in \mathbb{N}$ 使得 $c_1 f_n(x), c_2 g(x) \in \mathbb{Z}[x]$ 且 $c_1 f_n(x)$ 和 $c_2 g(x)$ 皆為 primitive polynomials (即各項係數的最大公因數為 1). 因此由 $(c_1 f_n(x))(c_2 g(x)) = c_1 c_2 (x^n - 1) \in \mathbb{Z}[x]$, 利用 Gauss Lemma (參見大學基礎代數講義Lemma 7.3.5) 可得 $c_1 c_2 = 1$, 故知 $f_n(x), g(x) \in \mathbb{Z}[x]$. 因此證得 $f_n(x) \in \mathbb{Z}[x]$. □

接著我們要證明 $f_n(x)$ 在 $\mathbb{Q}[x]$ 是 irreducible polynomial. 不過在證明之前我們需要一個滿技巧性的 Lemma. 首先介紹一下 notation. 若 p 是一個質數 且 $a \in \mathbb{Z}$, 則令 $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ 且 $\overline{a}$ 表示 a 在 $\mathbb{F}_p$ 中的值 (即 a modulo p). 同時若 $f(x) = a_m x^m + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, 則我們令 $\overline{f}(x) = \overline{a}_m x^m + \cdots + \overline{a}_1 x + \overline{a}_0 \in \mathbb{F}_p[x]$.

Lemma 4.3.3. *假設 $L/\mathbb{Q}$ 是一個 field extension 且 p 是一個質數. 又假設 $h(x), l(x)$ 為 $\mathbb{Z}[x]$ 中的 monic polynomials 其中 $h(x)$ 是 $\mathbb{Q}[x]$ 中的 irreducible polynomial. 令 $f(x) = h(x)l(x)$, 若存在 $\alpha \in L$ 滿足 $h(\alpha) = 0$ 且 $l(\alpha^p) = 0$, 則 $\overline{f}(x) \in \mathbb{F}_p[x]$ 不是一個 separable polynomial.*

Proof. 因為 $h(x)$ 是 $\mathbb{Q}[x]$ 中的 irreducible polynomial 且 $h(\alpha) = 0$, 知 $h(x)$ 是 α over $\mathbb{Q}$ 的 minimal polynomial. 令 $g(x) = l(x^p) \in \mathbb{Z}[x]$, 因為 $l(\alpha^p) = 0$, 我們知 $g(\alpha) = 0$, 故由 $h(x)$ 是 α over $\mathbb{Q}$ 的 minimal polynomial 知 $h(x)$ 在 $\mathbb{Q}[x]$ 中整除 $g(x)$. 又由於 $h(x)$ 為 $\mathbb{Z}[x]$ 中的 monic polynomial, 利用 Gauss Lemma 我們知 $h(x)$ 也在 $\mathbb{Z}[x]$ 中整除 $g(x)$ (參見大學基礎代數講義Lemma 7.3.7). 也就是說存在 $e(x) \in \mathbb{Z}[x]$ 使得 $l(x^p) = g(x) = e(x)h(x)$.

回顧一下因為 $\mathbb{F}_p$ 是一個 p 個元素的 finite field, 所以 $\mathbb{F}_p$ 的 characteristic 為 p 且對任意 $a \in \mathbb{Z}$ 皆有 $\overline{a}^p = \overline{a}$. 因此若 $l(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$, 則

$$\begin{aligned}
\overline{l}(x^p) &= (x^p)^m + \overline{a}_{m-1}(x^p)^{m-1} + \cdots + \overline{a}_1 x^p + \overline{a}_0 \\
&= (x^m)^p + \overline{a}_{m-1}^p (x^{m-1})^p + \cdots + \overline{a}_1^p x^p + \overline{a}_0^p \\
&= (x^m + \overline{a}_{m-1}x^{m-1} + \cdots + \overline{a}_1 x + \overline{a}_0)^p \\
&= \overline{l}(x)^p.
\end{aligned}$$

故得 $\overline{l}(x)^p = \overline{e}(x)\overline{h}(x)$. 要注意 $\overline{h}(x)$ 未必是 $\mathbb{F}_p[x]$ 中的 irreducible polynomial, 不過一定存在一個 $\mathbb{F}_p[x]$ 中的 irreducible polynomial $q(x)$ 整除 $\overline{h}(x)$, 又因為 $\overline{h}(x)$ 整除 $\overline{l}(x)^p$, 所以 $q(x)$ 也整除 $\overline{l}(x)^p$. 因此利用 $\mathbb{F}_p[x]$ 是一個 unique factorization domain 以及 $q(x)$ 是 $\mathbb{F}_p[x]$ 中的 irreducible polynomial, 可得 $q(x)$ 整除 $\overline{l}(x)$. 換言之, 存在 $d_1(x), d_2(x) \in \mathbb{F}_p[x]$ 使得 $\overline{h}(x) = d_1(x)q(x)$ 且 $\overline{l}(x) = d_2(x)q(x)$. 這會導致

$$\overline{f}(x) = \overline{h}(x)\overline{l}(x) = q(x)^2 d_1(x)d_2(x),$$

所以 $\overline{f}(x)$ 不可能是 separable polynomial. □

現在我們可以利用 Lemma 4.3.3 來證明 $f_n(x)$ 是 $\mathbb{Q}[x]$ 中的 irreducible polynomial.

Proposition 4.3.4. *若 $f_n(x)$ 是 n-th cyclotomic polynomial, 則 $f_n(x)$ 是 $\mathbb{Q}[x]$ 中的 irreducible polynomial.*

Proof. 首先觀察若 p 是一個質數且 $p \nmid n$, 則 $\overline{f_n}(x) \in \mathbb{F}_p[x]$ 是一個 separable polynomial. 這是因為在 Lemma 4.3.2 的證明中我們知存在 $g(x) \in \mathbb{Z}[x]$ 使得 $x^n - 1 = f_n(x)g(x)$, 因此由 $x^n - 1 = \overline{f_n}(x)\overline{g}(x)$ 知 $\overline{f_n}(x)$ 在 $\mathbb{F}_p[x]$ 中整除 $x^n - 1$. 但是 $x^n - 1$ 在 $\mathbb{F}_p[x]$ 中的微分是 $\overline{n}x^{n-1}$, 其中因 $p \nmid n$, 所以 $\overline{n} \neq 0$. 因此我們知在 $\mathbb{F}_p[x]$ 中 $\gcd(x^n - 1, \overline{n}x^{n-1}) = 1$, 故由

Lemma 3.3.5 知 x^m-1 在 $\mathbb{F}_p[x]$ 中是 separable polynomial. 也因此由 $\overline{f_n}(x)$ 在 $\mathbb{F}_p[x]$ 中是 x^n-1 的因式, 得知 $\overline{f_n}(x)$ 是 $\mathbb{F}_p[x]$ 中的 separable polynomial.

現令 $h(x)$ 為 ζ_n over $\mathbb{Q}$ 的 minimal polynomial, 由於 $f_n(\zeta_n)=0$, 知 $h(x)$ 在 $\mathbb{Q}[x]$ 中整除 $f_n(x)$. 但因為 $f_n(x)$ 是 $\mathbb{Z}[x]$ 中的 monic polynomial, 由 Gauss Lemma 我們知 $h(x)\in\mathbb{Z}[x]$ 且存在 $l(x)\in\mathbb{Z}[x]$ 使得 $f_n(x)=h(x)l(x)$ (參見大學基礎代數講義Lemma 7.3.8). 我們要證明若 $1\le t\le n$ 且 $\gcd(t,n)=1$, 則 $h(\zeta_n^t)=0$.

假設 t 的質因數分解為 $t=p_1\cdots p_r$ (這裡 p_i 未必相異), 由於 $\gcd(t,n)=1$, 我們知 $p_i\nmid n$. 由於 $\gcd(p_1,n)=1$, 知 $\zeta_n^{p_1}$ 是一個 primitive n-th root of 1, 故知 $f_n(\zeta_n^{p_1})=0$, 但因為 $h(\zeta_n)=0$ 且 $\overline{f_n}(x)$ 在 $\mathbb{F}_{p_1}[x]$ 中是 separable polynomial, 由 Lemma 4.3.3 知 $\zeta_n^{p_1}$ 不可能是 $l(x)$ 的一個根, 故得 $h(\zeta_n^{p_1})=0$. 同理由於 $\gcd(p_2,n)=1$, 我們知 $(\zeta_n^{p_1})^{p_2}$ 也是 primitive n-th root of 1. 故由 $f_n((\zeta_n^{p_1})^{p_2})=0$, $h(\zeta_n^{p_1})=0$ 以及 $\overline{f_n}(x)$ 在 $\mathbb{F}_{p_2}[x]$ 中是 separable polynomial, 再次利用 Lemma 4.3.3, 我們得知 $h(\zeta_n^{p_1p_2})=0$. 因此用 induction, 我們知 $h(\zeta_n^t)=h(\zeta_n^{p_1\cdots p_r})=0$.

我們證得了所有的 primitive n-th root of 1 都是 $h(x)$ 的根, 而這些 primitive n-th root of 1 又剛好是 $f_n(x)$ 所有的根, 故由 $h(x)$ 和 $f_n(x)$ 都是 monic polynomial 且 $h(x)$ 整除 $f_n(x)$ 得證 $h(x)=f_n(x)$. 也就是說 $f_n(x)$ 是 $\mathbb{Q}[x]$ 中的 irreducible polynomial. □

事實上在 Proposition 4.3.4 中我們證得了 $f_n(x)$ 就是 ζ_n over $\mathbb{Q}$ 的 minimal polynomial.

Theorem 4.3.5. *若 L 是 n-th cyclotomic field, 則 $L/\mathbb{Q}$ 是一個 degree 為 $\phi(n)$ 的 Galois extension 且 $\mathrm{Gal}(L/\mathbb{Q})$ 是一個 isomorphic to $(\mathbb{Z}/n\mathbb{Z})^*$ 的 abelian group.*

Proof. 我們已知 $L/\mathbb{Q}$ 是一個 Galois extension. 又因為 $L=\mathbb{Q}(\zeta_n)$ 且 $f_n(x)$ 為 ζ_n over $\mathbb{Q}$ 的 minimal polynomial, 所以 $[L:\mathbb{Q}]=\deg(f_n(x))=\phi(n)$.

現考慮函數 $\Psi:\mathrm{Gal}(L/\mathbb{Q})\to(\mathbb{Z}/n\mathbb{Z})^*$, 其定義為: 若 $\sigma\in\mathrm{Gal}(L/\mathbb{Q})$, 且 $\sigma(\zeta_n)=\zeta_n^t$, 則定 $\Psi(\sigma)=\bar{t}\in\mathbb{Z}/n\mathbb{Z}$. 首先檢查 Ψ 是一個 well-defined 函數. 假設 $\sigma(\zeta_n)=\zeta_n^t$ 且 $t'\in\mathbb{Z}$ 使得 $\zeta_n^t=\zeta_n^{t'}$, 得 $\zeta_n^{t-t'}=1$. 由於 ζ_n 的 order 為 n, 故得 $n\mid t-t'$, 也就是 $\bar{t}-\overline{t'}=\overline{t-t'}=\bar{0}$. 因此知 $\bar{t}=\overline{t'}$. 另一方面因為 $\sigma(\zeta_n)$ 必為 primitive n-th root of 1, 故若 $\sigma(\zeta_n)=\zeta_n^t$, 則 $\gcd(t,n)=1$, 因此知 $\Psi(\sigma)=\bar{t}\in(\mathbb{Z}/n\mathbb{Z})^*$.

接下來檢查 Ψ 是一個 group homomorphism. 假設 $\sigma,\tau\in\mathrm{Gal}(L/\mathbb{Q})$ 且 $\sigma(\zeta_n)=\zeta_n^t$ 以及 $\tau(\zeta_n)=\zeta^s$. 則

$$\tau\circ\sigma(\zeta_n)=\tau(\sigma(\zeta_n))=\tau(\zeta_n^t)=\tau(\zeta_n)^t=(\zeta_n^s)^t=\zeta_n^{st}.$$

我們知若 $\Psi(\sigma)=\bar{t}$ 且 $\Psi(\tau)=\bar{s}$, 則 $\Psi(\tau\circ\sigma)=\overline{st}=\bar{s}\bar{t}$. 故得 $\Psi(\tau\circ\sigma)=\Psi(\tau)\Psi(\sigma)$. 得證 Ψ 是一個 group homomorphism.

現假設 $\sigma\in\ker(\Psi)$, 表示 $\Psi(\sigma)=\bar{1}$. 現若 $\sigma(\zeta_n)=\zeta_n^t$, 知 $\Psi(\sigma)=\bar{t}=\bar{1}$. 因而得知存在 $m\in\mathbb{Z}$ 使得 $t=mn+1$. 故知 $\sigma(\zeta_n)=\zeta_n^t=\zeta_n^{mn+1}=\zeta_n$. 也就是說 σ 是 L 到 L 的 identity. 得證 Ψ 是 1-1. 最後由於 $L/\mathbb{Q}$ 是 Galois extension, 我們有

$|\mathrm{Gal}(L/\mathbb{Q})| = [L:\mathbb{Q}] = \phi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$. 故由 $\Psi : \mathrm{Gal}(L/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^*$ 是 1-1 得證 Ψ 是 onto. 因此得證 $\mathrm{Gal}(L/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^*$. □

當一個 field extension 是 Galois extension 且其 Galois group 是 abelian group 時, 我們稱此 extension 為 *abelian extension*. Theorem 4.3.5 就是告訴我們當 L 是一個 cyclotomic field 時, $L/\mathbb{Q}$ 一定是一個 abelian extension. 特別當 p 是一個質數且 L 是 p-th cyclotomic field, 由於 $\mathbb{Z}/p\mathbb{Z}$ 是 finite field 知 $(\mathbb{Z}/p\mathbb{Z})^*$ 是一個 cyclic group, 所以 $L/\mathbb{Q}$ 是一個 cyclic extension.

一般來說當 L/K 是一個 abelian extension 且 $[L:K] = m$ 時, 我們知 $\mathrm{Gal}(L/K)$ 是一個 order m 的 abelian group. 由 abelian group 的性質知, 對任意滿足 $s \mid m$ 的正整數 s 皆存在一個 (不一定唯一) subgroup $H \subseteq \mathrm{Gal}(L/K)$ 滿足 $|H| = s$. 反之若 H 是 $\mathrm{Gal}(L/K)$ 的 subgroup, 由 Lagrange Theorem 知 $|H| \mid m$. 另外因為 $\mathrm{Gal}(L/K)$ 是 abelian group, 所以 $\mathrm{Gal}(L/K)$ 的 subgroup H 都是 normal subgroup, 而且 H 以及 $\mathrm{Gal}(L/K)/H$ 都是 abelian groups. 綜合這些結果, 由 First Fundamental Theorem 4.1.5 我們知道對任意 $s \mid m$, 皆存在一個 L/K 的 intermediate field F 滿足 $[L:F] = s$, 而且我們知 $\mathrm{Gal}(L/F)$ 是一個 abelian group of order s. 另外因為 $\mathrm{Gal}(L/F)$ 是 $\mathrm{Gal}(L/K)$ 的 normal subgroup, 所以由 Second Fundamental Theorem 4.1.8 知 F/K 也是 Galois extension, 而且 $\mathrm{Gal}(F/K)$ isomorphic to $\mathrm{Gal}(L/K)/\mathrm{Gal}(L/F)$ 也是一個 abelian group. 這些結果都可套用到 L 是 cyclotomic field 且 $K = \mathbb{Q}$ 的情形. 因此當 F 是 $L/\mathbb{Q}$ 的 intermediate field 時, 我們得 L/F 以及 $F/\mathbb{Q}$ 都是 abelian extension.

我們知道了每一個 cyclotomic field 的 subfield 都是 finite abelian extension over $\mathbb{Q}$. 事實上反過來也是對的: 任意 finite abelian extension over $\mathbb{Q}$ 都會是某一個 cyclotomic field 的 subfield. 這就是所謂的*Kronecker-Weber Theorem*. 當然了這個定理的證明超出了這個講義的範圍, 不過相信若你已熟悉了 Galois 理論, 要探索這些進階的理論已不是難事.