簡介 Galois 理論

李華介

國立台灣師範大學數學系

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.