

簡介 Galois 理論

李華介

國立台灣師範大學數學系

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) $|\text{Gal}(L/K)| = [L : K]$
- (2) $\text{Gal}(L/K)$ 的 *fixed field* 是 K .
- (3) L/K 是一個 *normal and separable extension*.

Proof. (1) $\Rightarrow$ (2): 假設 $\text{Gal}(L/K)$ 的 fixed field 是 F , 則我們有 $K \subseteq F \subseteq L$ 且 $|\text{Gal}(L/K)| = [L : F]$ (Theorem 2.3.4). 因此由 $|\text{Gal}(L/K)| = [L : K]$ 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 $\text{Gal}(L/K)$ 的 fixed field 的定義為 $\{\alpha \in L \mid \sigma(\alpha) = \alpha, \forall \sigma \in \text{Gal}(L/K)\}$. 所以 K 為 $\text{Gal}(L/K)$ 的 fixed field 不只是說 K 中的元素都會被所有的 $\sigma \in \text{Gal}(L/K)$ 固定, 也表示 L 中被所有的 $\sigma \in \text{Gal}(L/K)$ 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 $a = a_1, a_2, \dots, a_n$ 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 $a_1, a_2, \dots, a_n \in L$, 我們有 $f(x) \in L[x]$. 現假設 $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1x + c_0$, 其中 $c_i \in L$. 對任意 $\sigma \in \text{Gal}(L/K)$, 我們有

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

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 $\sigma \in \text{Gal}(L/K)$, 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 $\{a_1, a_2, \dots, a_n\} = \{\sigma(a_1), \sigma(a_2), \dots, \sigma(a_n)\}$. 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 $\sigma \in \text{Gal}(L/K)$ 皆有 $f(x) = f^\sigma(x)$. 故由式子 (4.1) 知對任意 $\sigma \in \text{Gal}(L/K)$ 皆有 $\sigma(c_i) = c_i$. 也就是說這些 c_i 都落在 $\text{Gal}(L/K)$ 的 fixed field 中. 因此由假設 K 是 $\text{Gal}(L/K)$ 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 $p(x) \mid f(x)$. 得知 $\deg(p(x)) \leq \deg(f(x))$, 因此由前面已知 $\deg(f(x)) \leq \deg(p(x))$ 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 $\text{Gal}(L/K) = \mathfrak{M}_K(L, N)$, 得證 $|\text{Gal}(L/K)| = [L : K]$. $\square$

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. $\square$

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 $a_1, \dots, a_n \in L$ 使得 $L = K(a_1, \dots, a_n)$. 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 $i \in \{1, \dots, n\}$, 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 $L = K(a_1, \dots, a_n) \subseteq F$, 而得證 $L = F$. 也就是說 L 是 $f(x)$ over K 的 splitting field.

(2) $\Rightarrow$ (1): 假設 $b_1, \dots, b_m \in L$ 是 $f(x)$ 所有的根. 因為 L 是 $f(x)$ over K 的 splitting field, 我們得 $L = K(b_1, \dots, b_m)$. 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. $\square$

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 $\text{Gal}(L/K)$ 的 subgroups 所成的集合, 即 $\mathfrak{G} = \{H \mid H \text{ 是 } \text{Gal}(L/K) \text{ 的 subgroup}\}$. 我們定義函數 $\mathcal{G} : \mathfrak{F} \rightarrow \mathfrak{G}$ 如下: 對任意 L/K 的 intermediate field F (即 $F \in \mathfrak{F}$), 我們定義 $\mathcal{G}(F) = \text{Gal}(L/F)$. 而函數 $\mathcal{F} : \mathfrak{G} \rightarrow \mathfrak{F}$ 的定義為: 對任意 $\text{Gal}(L/K)$ 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 $\mathcal{G} : \mathfrak{F} \rightarrow \mathfrak{G}$ 給了我們一個 L/K 的 *intermediate fields* 和 $\text{Gal}(L/K)$ 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 $\text{Gal}(L/F)$ 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 $\mathcal{G} : \mathfrak{F} \rightarrow \mathfrak{G}$, 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 $\mathcal{G} : \mathfrak{F} \rightarrow \mathfrak{G}$ 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 $\mathcal{G} : \mathfrak{F} \rightarrow \mathfrak{G}$ 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. $\square$

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

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

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 $\text{Gal}(L/K)$ 的 *subgroup*, 則

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

特別若 H_1 和 H_2 是 $\text{Gal}(L/K)$ 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 $|\text{Gal}(L/K)| = [L : K]$ 且 $|\text{Gal}(L/F)| = [L : F]$. 再利用 $[L : K] = [L : F][F : K]$, 得知 $[F : K] = [L : K]/[L : F] = |\text{Gal}(L/K)|/|\text{Gal}(L/F)|$.

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 $[F_2 : F_1] = |\text{Gal}(L/F_1)| / |\text{Gal}(L/F_2)| = |\mathcal{G}(F_1)| / |\mathcal{G}(F_2)|$.

(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 $[\mathcal{F}(H) : K] = |\text{Gal}(L/K)| / |H|$. 現若 $H_1 \subseteq H_2$, 則 $\mathcal{F}(H_2) \subseteq \mathcal{F}(H_1)$, 故知 $[\mathcal{F}(H_1) : \mathcal{F}(H_2)] = [\mathcal{F}(H_1) : K] / [\mathcal{F}(H_2) : K] = |H_2| / |H_1|$. $\square$

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 $\text{Gal}(L/K)$ 的 subgroup 之間的對應關係. 所以我們很自然的會問到 $\text{Gal}(L/K)$ 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 $\sigma \in \text{Gal}(L/K)$, 則 $\sigma(F)$ 為 L/K 的 intermediate field 且 $L/\sigma(F)$ 的 Galois group $\text{Gal}(L/\sigma(F))$ 為 $\sigma \circ \text{Gal}(L/F) \circ \sigma^{-1}$. 亦即 $\mathcal{G}(\sigma(F)) = \sigma \circ \mathcal{G}(F) \circ \sigma^{-1}$.

Proof. 依定義 $\sigma(F) = \{\sigma(\alpha) \mid \alpha \in F\}$, 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 $\sigma : L \rightarrow L$ 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 $\tau \in \text{Gal}(L/\sigma(F))$, 我們有 $\tau : L \rightarrow L$ 且對任意 $\alpha \in F$ 皆有 $\tau(\sigma(\alpha)) = \sigma(\alpha)$. 令 $\rho = \sigma^{-1} \circ \tau \circ \sigma : L \rightarrow L$. 因為 $\text{Gal}(L/K)$ 是一個 group 且 $\tau \in \text{Gal}(L/\sigma(F)) \subseteq \text{Gal}(L/K)$, 我們知 $\rho \in \text{Gal}(L/K)$. 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 $\rho \in \text{Gal}(L/F)$. 故得 $\tau = \sigma \circ \rho \circ \sigma^{-1} \in \sigma^{-1} \circ \text{Gal}(L/F) \circ \sigma^{-1}$.

反之, 若 $\tau \in \sigma \circ \text{Gal}(L/F) \circ \sigma^{-1}$, 表示存在 $\rho \in \text{Gal}(L/F)$ 滿足 $\tau = \sigma \circ \rho \circ \sigma^{-1}$. 因為 $\text{Gal}(L/K)$ 是一個 group 且 $\rho \in \text{Gal}(L/F) \subseteq \text{Gal}(L/K)$, 我們知 $\tau \in \text{Gal}(L/K)$. 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 $\tau \in \text{Gal}(L/\sigma(F))$. $\square$

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 $\text{Gal}(L/F)$ 是 $\text{Gal}(L/K)$ 的 *normal subgroup*. 而且當 F/K 是 *Galois extension* 時, $\text{Gal}(F/K)$ 和 $\text{Gal}(L/K)/\text{Gal}(L/F)$ 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 $\sigma \in \text{Gal}(L/K)$, 由於 $\sigma|_F : F \rightarrow L$ 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

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

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

反之, 若 $\text{Gal}(L/F)$ 是 $\text{Gal}(L/K)$ 的 normal subgroup, 表示對任意 $\sigma \in \text{Gal}(L/K)$ 皆有 $\text{Gal}(L/F) = \sigma \circ \text{Gal}(L/F) \circ \sigma^{-1}$. 故由 Lemma 4.1.7 知 $\text{Gal}(L/F) = \text{Gal}(L/\sigma(F))$. 也就是說對任意 $\sigma \in \text{Gal}(L/K)$ 皆有 $\mathcal{G}(F) = \mathcal{G}(\sigma(F))$. 由於 L/K 是 Galois extension, 故得 $\mathcal{G} : \mathfrak{F} \rightarrow \mathfrak{B}$ 是一對一的函數 (Theorem 4.1.5), 因此對任意 $\sigma \in \text{Gal}(L/K)$ 皆有 $\sigma(F) = F$. 換言之, 對任意 $\sigma \in \text{Gal}(L/K)$, 皆有 $\sigma|_F : F \rightarrow F$ 是 F 到 F 的 K -monomorphism, 因此知 $\sigma|_F \in \text{Gal}(F/K)$. 現考慮函數 $\Psi : \text{Gal}(L/K) \rightarrow \text{Gal}(F/K)$, 使得對任意 $\sigma \in \text{Gal}(L/K)$, 定義 $\Psi(\sigma) = \sigma|_F$. 很容易得知 Ψ 是一個 group homomorphism. 若 $\tau \in \text{Gal}(F/K)$, 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 $\sigma \in \text{Gal}(L/K)$ 使得 $\sigma|_F = \tau$. 也就是說, 對任意 $\tau \in \text{Gal}(F/K)$ 皆存在 $\sigma \in \text{Gal}(L/K)$ 使得 $\Psi(\sigma) = \tau$. 證得 $\Psi : \text{Gal}(L/K) \rightarrow \text{Gal}(F/K)$ 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 $\text{Gal}(F/K)$ 的 identity. 亦即對任意 $\lambda \in F$ 皆有 $\sigma(\lambda) = \sigma|_F(\lambda) = \lambda$. 因此知 $\sigma : L \rightarrow L$ 將 F 的元素固定, 也就是說 $\sigma \in \text{Gal}(L/F)$. 另一方面若 $\sigma \in \text{Gal}(L/F)$, 則依定義 σ 將 F 的元素固定, 故知 $\sigma|_F : F \rightarrow F$ 是 identity. 也就是說 $\sigma \in \ker(\Psi)$, 得證 $\ker(\Psi) = \text{Gal}(L/F)$. 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:

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

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

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

故利用 Theorem 4.1.1 得證 F/K 是 Galois extension. $\square$

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 $\text{Gal}(L/F)$ 是 $\text{Gal}(L/K)$ 的 normal subgroup. 不過在 F/K 是 normal extension 推導得 $\text{Gal}(L/F)$ 是 $\text{Gal}(L/K)$ 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 $\text{Gal}(L/F)$ 是 $\text{Gal}(L/K)$ 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 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 $a_1, \dots, a_n \in L$ 使得 $L = K(a_1, \dots, a_n)$. 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 $\alpha_1, \dots, \alpha_m \in N$ 為 $f(x)$ 所有的根, 則 $N = K(\alpha_1, \dots, \alpha_m)$. 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 $p_1(x), \dots, p_n(x)$ 其中之一. 因此由 $p_1(x), \dots, p_n(x)$ 皆為 separable polynomials 知 $\alpha_1, \dots, \alpha_m$ 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. $\square$

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 $\text{Gal}(N/K)$ 的 subgroups 之間有一個 1-1 correspondence. 又因為 N/K 是 finite extension, 所以 $\text{Gal}(N/K)$ 是一個 finite group (事實上 $|\text{Gal}(N/K)| = [N : K]$), 因此 $\text{Gal}(N/K)$ 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

$$T_{L/K}(a) = \sigma_1(a) + \dots + \sigma_n(a) \quad \text{and} \quad N_{L/K}(a) = \sigma_1(a) \cdots \sigma_n(a).$$

$T_{L/K}(a)$ 和 $N_{L/K}(a)$ 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) $T_{L/K}(ka + b) = kT_{L/K}(a) + T_{L/K}(b)$ 且 $N_{L/K}(ab) = N_{L/K}(a)N_{L/K}(b)$.
- (2) $T_{L/K}(k) = nk$ 且 $N_{L/K}(k) = k^n$.

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

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

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

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

(2) 由於 $\sigma_i(k) = k$, 故直接依定義知

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

□

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

$$\tau(T_{L/K}(a)) = \tau(\sigma_1(a) + \dots + \sigma_n(a)) = \tau(\sigma_1(a)) + \dots + \tau(\sigma_n(a)) = T_{L/K}(a).$$

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

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

$$T_{L/K}(a) \in K \quad \text{and} \quad N_{L/K}(a) \in K.$$

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 $\mathfrak{M}_K(L, N) = \{\sigma_1, \dots, \sigma_n\}$. 對任意 $\tau \in \text{Gal}(N/K)$, 由於 $\tau \circ \sigma_i : L \rightarrow N$ 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 $\tau \in \text{Gal}(N/K)$ 皆有 $\mathfrak{M}_K(L, N) = \{\tau \circ \sigma_1, \dots, \tau \circ \sigma_n\}$. 所以依定義知對任意 $\tau \in \text{Gal}(N, K)$ 皆有

$$\tau(T_{L/K}(a)) = \tau(\sigma_1(a) + \dots + \sigma_n(a)) = \tau(\sigma_1(a)) + \dots + \tau(\sigma_n(a)) = T_{L/K}(a).$$

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

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 $T_{L/F}(a)$ 和 $N_{L/F}(a)$ 皆為 F 中的元素, 所以可以將它們代入 $T_{F/K}$ 以及 $N_{F/K}$ 中, 得 $T_{F/K}(T_{L/F}(a))$ 以及 $N_{F/K}(N_{L/F}(a))$. 事實上它們會分別等於 $T_{L/K}(a)$ 以及 $N_{L/K}(a)$, 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

$$T_{F/K}(T_{L/F}(a)) = T_{L/K}(a) \quad \text{and} \quad N_{F/K}(N_{L/F}(a)) = N_{L/K}(a).$$

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

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

因此知

$$T_{L/K}(a) = \sum_{j=1}^t \sum_{i=1}^s \phi_j(\rho_i(a)) = \sum_{j=1}^t \phi_j\left(\sum_{i=1}^s \rho_i(a)\right) = \sum_{j=1}^t \phi_j(T_{L/F}(a)).$$

另一方面利用 Corollary 3.2.11 我們知 $\mathfrak{M}_K(F, N') = \mathfrak{M}_K(F, N) = \{\psi_1, \dots, \psi_t\}$ 以及利用 Proposition 4.2.5 我們知 $T_{L/F}(a) \in F$, 因此 $\phi_j(T_{L/F}(a)) = \phi_j|_F(T_{L/F}(a)) = \psi_j(T_{L/F}(a))$. 故得

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

同理證得

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

□

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 $f(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_1x + a_0$, 則

$$T_{L/K}(a) = -\frac{n}{m} a_{m-1} \quad \text{and} \quad N_{L/K}(a) = (-1)^n a_0^{n/m}.$$

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 $T_{L/F}(a) = (n/m)a$ 以及 $N_{L/F}(a) = a^{n/m}$. 接著我們要計算 $T_{F/K}(a)$ 以及 $N_{F/K}(a)$.

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 $\mathfrak{M}_K(F, N) = \{\sigma_1, \dots, \sigma_m\}$. 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 $\sigma_1(a), \dots, \sigma_m(a)$ 皆相異. 又因為 $\sigma_i(a)$ 必為 $f(x)$ 的根, 所以得 $\sigma_1(a), \dots, \sigma_m(a)$ 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

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

以及

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

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

$$T_{L/K}(a) = T_{F/K}(T_{L/F}(a)) = T_{F/K}\left(\frac{n}{m}a\right) = \frac{n}{m}T_{F/K}(a) = -\frac{n}{m}a_{m-1}$$

以及

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

□

由 Theorem 4.2.7 可以看出, 不僅 $T_{L/K}(a) \in K$ 且 $N_{L/K}(a) \in K$ 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 $\mathbb{F}_p = \{0, 1, \dots, p-1\}$ 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 field 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 $\varphi_q : \mathbb{F}_{q^m} \rightarrow \mathbb{F}_{q^m}$ 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 $\varphi_q \in \text{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$. 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 $\varphi_q : L \rightarrow L$ 滿足 $\varphi_q(\alpha) = \alpha^q, \forall \alpha \in L$ 為 $L/\mathbb{F}_q$ 的 Frobenius automorphism, 則 $\text{Gal}(L/\mathbb{F}_q)$ 是一個 cyclic group generated by φ_q .

Proof. 假設 $[L : \mathbb{F}_q] = m$. 前面已知 $\varphi_q \in \text{Gal}(L/\mathbb{F}_q)$. 考慮 $H = \langle \varphi_q \rangle$ 為 $\text{Gal}(L/\mathbb{F}_q)$ 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

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

因而得證 $[L : \mathbb{F}_q] = |\text{Gal}(L/\mathbb{F}_q)| = |H|$. 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 $\text{Gal}(L/\mathbb{F}_q) = H = \langle \varphi_q \rangle$.

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. $\square$

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 $\text{Gal}(L/K)$ 是一個 order m 的 cyclic group. 由 cyclic group 的性質知, 對任意滿足 $s \mid m$ 的正整數 s 皆存在唯一的 subgroup $H \subseteq \text{Gal}(L/K)$ 滿足 $|H| = s$. 反之若 H 是 $\text{Gal}(L/K)$ 的 subgroup, 由 Lagrange Theorem 知 $|H| \mid m$. 另外因為 $\text{Gal}(L/K)$ 是 cyclic group, 所以 $\text{Gal}(L/K)$ 的 subgroup H 都是 normal subgroup, 而且 H 以及 $\text{Gal}(L/K)/H$ 都是 cyclic groups. 綜合這些結果, 由 First Fundamental Theorem 4.1.5 我們知道對任意 $s \mid m$, 存在唯一的 L/K 的 intermediate field F 滿足 $[L : F] = s$, 而且我們知 $\text{Gal}(L/F)$ 是一個 cyclic group of order s . 另外因為 $\text{Gal}(L/F)$ 是 $\text{Gal}(L/K)$ 的 normal subgroup, 所以由 Second Fundamental Theorem 4.1.8 知 F/K 也是 Galois extension, 而且 $\text{Gal}(F/K)$ isomorphic to $\text{Gal}(L/K)/\text{Gal}(L/F)$ 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 $\text{Gal}(L/\mathbb{Q})$ 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 $C_n = \{\zeta_n^t \mid 1 \leq t \leq n\}$. 因此我們知 $L = \mathbb{Q}(\zeta_n)$.

現若 $\sigma \in \text{Gal}(L/\mathbb{Q})$, 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 $n \mid m$. 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 $\sigma \in \text{Gal}(L/\mathbb{Q})$, 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 $\mathbb{Z}/12\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \bar{11}\}$ 是一個 cyclic group generated by $\bar{1}$. 但

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

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 $\text{Gal}(L/\mathbb{Q})$ 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 $\sigma \in \text{Gal}(L/\mathbb{Q})$, 則 $\sigma(\zeta_n) = \zeta_n^t$, 其中 $1 \leq t \leq n$ 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:

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

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 $\sigma \in \text{Gal}(L/\mathbb{Q})$, 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

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

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 $\text{Gal}(L/\mathbb{Q})$ 的 fixed field 中. 但已知 $L/\mathbb{Q}$ 是 Galois extension, 所以 $\text{Gal}(L/\mathbb{Q})$ 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 $x^n - 1 = \prod_{1 \leq t \leq n} (x - \zeta_n^t)$, 所以存在 $g(x) \in L[x]$ 使得 $x^n - 1 = f_n(x)g(x)$. 對任意 $\sigma \in \text{Gal}(L/\mathbb{Q})$, 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 $\sigma \in \text{Gal}(L/\mathbb{Q})$ 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 $f_n(x) \in \mathbb{Z}[x]$. $\square$

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 $\bar{a}$ 表示 a 在 $\mathbb{F}_p$ 中的值 (即 a modulo p). 同時若 $f(x) = a_mx^m + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$, 則我們令 $\bar{f}(x) = \bar{a}_mx^m + \cdots + \bar{a}_1x + \bar{a}_0 \in \mathbb{F}_p[x]$.

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 $\bar{f}(x) \in \mathbb{F}_p[x]$ 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 $\bar{a}^p = \bar{a}$. 因此若 $l(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_1x + a_0$, 則

$$\begin{aligned} \bar{l}(x^p) &= (x^p)^m + \bar{a}_{m-1}(x^p)^{m-1} + \cdots + \bar{a}_1x^p + \bar{a}_0 \\ &= (x^m)^p + \bar{a}_{m-1}^p(x^{m-1})^p + \cdots + \bar{a}_1^p x^p + \bar{a}_0^p \\ &= (x^m + \bar{a}_{m-1}x^{m-1} + \cdots + \bar{a}_1x + \bar{a}_0)^p \\ &= \bar{l}(x)^p. \end{aligned}$$

故得 $\bar{l}(x)^p = \bar{e}(x)\bar{h}(x)$. 要注意 $\bar{h}(x)$ 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 $\bar{h}(x)$, 又因為 $\bar{h}(x)$ 整除 $\bar{l}(x)^p$, 所以 $q(x)$ 也整除 $\bar{l}(x)^p$. 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 $\bar{l}(x)$. 換言之, 存在 $d_1(x), d_2(x) \in \mathbb{F}_p[x]$ 使得 $\bar{h}(x) = d_1(x)q(x)$ 且 $\bar{l}(x) = d_2(x)q(x)$. 這會導致

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

所以 $\bar{f}(x)$ 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 $\bar{f}_n(x) \in \mathbb{F}_p[x]$ 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 $x^n - 1 = \bar{f}_n(x)\bar{g}(x)$ 知 $\bar{f}_n(x)$ 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 $\bar{n}x^{n-1}$, 其中因 $p \nmid n$, 所以 $\bar{n} \neq 0$. 因此我們知在 $\mathbb{F}_p[x]$ 中 $\gcd(x^n - 1, \bar{n}x^{n-1}) = 1$, 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.

現今 $h(x)$ 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 $1 \leq t \leq n$ 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 $h(\zeta_n^{p_1 p_2}) = 0$. 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. $\square$

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 $\text{Gal}(L/\mathbb{Q})$ 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 $\Psi : \text{Gal}(L/\mathbb{Q}) \rightarrow (\mathbb{Z}/n\mathbb{Z})^*$, 其定義為: 若 $\sigma \in \text{Gal}(L/\mathbb{Q})$, 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 $\bar{t} - \bar{t}' = \overline{t - t'} = \bar{0}$. 因此知 $\bar{t} = \bar{t}'$. 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 $\sigma, \tau \in \text{Gal}(L/\mathbb{Q})$ 且 $\sigma(\zeta_n) = \zeta_n^t$ 以及 $\tau(\zeta_n) = \zeta_n^s$. 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

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

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 $\text{Gal}(L/K)$ 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 $H \subseteq \text{Gal}(L/K)$ 滿足 $|H| = s$. 反之若 H 是 $\text{Gal}(L/K)$ 的 subgroup, 由 Lagrange Theorem 知 $|H| \mid m$. 另外因為 $\text{Gal}(L/K)$ 是 abelian group, 所以 $\text{Gal}(L/K)$ 的 subgroup H 都是 normal subgroup, 而且 H 以及 $\text{Gal}(L/K)/H$ 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 $\text{Gal}(L/F)$ 是一個 abelian group of order s . 另外因為 $\text{Gal}(L/F)$ 是 $\text{Gal}(L/K)$ 的 normal subgroup, 所以由 Second Fundamental Theorem 4.1.8 知 F/K 也是 Galois extension, 而且 $\text{Gal}(F/K)$ isomorphic to $\text{Gal}(L/K)/\text{Gal}(L/F)$ 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.