

局部體與大域體

李文卿·余文卿

第一節. 局部體

設 k 是一具 q 個元素的有限體，將有理函數體 $k(T)$ 表為 F 。設 x 是 k 上投影線 \mathbf{P}^1 上的一封閉點；研究 \mathbf{P}^1 上非零有理函數在 x 點附近的表現，即是想知道 x 到底是 f 的幾重零點或極點；而了解的方法是透過 x 所滿足的不可約多項式 $P(T)$ 。將 f 表為 $k(T)$ 中兩多項式 $g(T)$ 與 $h(T)$ 的商（若 x 是無窮遠點，則以 $\frac{1}{T}$ 取代 T ）。那麼 f 在 x 點之零位的重數等於 P 整除 g 的重數減去 P 整除 h 的重數。說得更透澈一點，以 \mathcal{P} 表示 $k(T)$ 中由 P 生成的理想； $P(T)$ 整除 $g(T)$ 的重數是滿足 $g(T)$ 落在 \mathcal{P}^m 的最高幕次 m 。最後這一描述法可擴充並適用於常數體是 k 的任意函數體 K 。事實上，在這種情形 K 中的位 (place) 即是 $k[T]$ 或 $k[\frac{1}{T}]$ 之整閉包 \mathcal{O} 的一最大理想 \mathcal{P} 。欲知 K 中非零有理函數在 \mathcal{P} 的情況，可先將 f 表為 g/h ，其中 g, h 落在 \mathcal{O} 。這種表示法可以做到是因為 K 是 \mathcal{O} 的商體。 g 在 \mathcal{P} 的重數 (order) 記做 $ord_{\mathcal{P}}g$ ，是使得 $g \in \mathcal{P}^m$ 的最高幕次 m ；那麼 f 在 \mathcal{P} 位的重數是

$$ord_{\mathcal{P}}f = ord_{\mathcal{P}}g - ord_{\mathcal{P}}h.$$

對 k 的每一位 \mathcal{P} ，利用重數 $ord_{\mathcal{P}}$ 可定義 K 上一賦值 (valuation) $| \cdot |_{\mathcal{P}}$ 如下：

$$\begin{cases} |0|_{\mathcal{P}} = 0, \\ |f|_{\mathcal{P}} = (N\mathcal{P})^{-ord_{\mathcal{P}}f} = (q^{-deg P})^{ord_{\mathcal{P}}f} \\ = |\mathcal{O}/\mathcal{P}|^{-ord_{\mathcal{P}}f}, f \in K^{\times}. \end{cases}$$

在有理數體 \mathbf{Q} 中，整數環 \mathbf{Z} 扮演的角色就像 $k[T]$ 在 $k(T)$ 中的一樣。 \mathbf{Z} 的每一質理想 $(p) = p\mathbf{Z}$ 即是 \mathbf{Q} 的一有限位 (finite place)。若 k 是 \mathbf{Q} 的有限 (代數) 擴充體， K 即稱為數體 (number field)，它的整數環 \mathcal{O} (ring of integers) 是 \mathbf{Z} 在 K 中的整閉包， \mathcal{O} 中的最大理想 \mathcal{P} 即是 K 的有限位。餘數體 \mathcal{O}/\mathcal{P} 是個有限體，其元素個數 $N\mathcal{P}$ 稱為 \mathcal{P} 的 norm。類似於上面的方法，我們可定 $ord_{\mathcal{P}}$ ，以及由 $ord_{\mathcal{P}}$ 定義 K 上的賦值 $| \cdot |_{\mathcal{P}}$ 為

$$\begin{cases} |0|_{\mathcal{P}} = 0, \\ |z|_{\mathcal{P}} = (N\mathcal{P})^{-ord_{\mathcal{P}}z} \\ = |\mathcal{O}/\mathcal{P}|^{-ord_{\mathcal{P}}z}, \text{ 若 } z \in K^{\times}. \end{cases}$$

上面定義在函數體或數體的賦值 $| \cdot |_{\mathcal{P}}$ 有下列的基本性質：設 $x, y \in K$ ，則

- (1) $|x|_{\mathcal{P}} \geq 0$ ，且 $|x|_{\mathcal{P}} = 0 \Leftrightarrow x = 0$ ，
- (2) $|xy|_{\mathcal{P}} = |x|_{\mathcal{P}}|y|_{\mathcal{P}}$ ，
- (3) $|x + y|_{\mathcal{P}} \leq \max(|x|_{\mathcal{P}}, |y|_{\mathcal{P}})$ 。

注意到由性質 (3) 可導出

(4) 三角不等式: $|x + y|_p \leq |x|_p + |y|_p$.

因此, $|\cdot|_p$ 定義了 K 上的一量度 (metric)。 K 對這量度的完備體 K_p 包含 K 當稠密子體。 K_p 中的整數是在 \mathcal{P} 沒有極點的元素; 由於 (1) 到 (3) 的性質, 使這些整數形成一環, 稱為 K_p 的整數環, 以 \mathcal{O}_p 表之。 換句話說,

$$\mathcal{O}_p = \{x \in K_p \mid |x|_p \leq 1\}$$

\mathcal{O}_p 中的乘法可逆元素稱為 \mathcal{P} -adic 單位 (\mathcal{P} -adic units), 形成一乘法子群 \mathcal{U}_p , 故

$$\mathcal{U}_p = \{x \in K_p \mid |x|_p = 1\}$$

而

$$\mathcal{P}_p = \mathcal{O}_p - \mathcal{U}_p = \{x \in K_p \mid |x|_p < 1\}$$

是 \mathcal{O}_p 中的唯一最大理想且 \mathcal{O}_p 中的非零理想只是 \mathcal{P} 的某一幕次方, 而商 $\mathcal{O}_p/\mathcal{P}_p$ 稱為 K_p 的餘數體 (residue field), 它與未完備前的餘數體 \mathcal{O}/\mathcal{P} 是同構的。 \mathcal{P}_p 是一主理想 (principal ideal) 由取值是最大值 $(N\mathcal{P})^{-1}$ 的任意元素 π_p 所生成; π_p 稱為在 \mathcal{P} 的 uniformizer。 $K_p^\times = \mathcal{U}_p \langle \pi_p \rangle$, 更進一步, 以 S 表示 \mathcal{O}_p 中餘數體的所有代表, 則任意 \mathcal{O}_p 的元素可表成係數落在 S 以 π_p 為幕次的泰勒展開式, 其中常數項不落在 \mathcal{P} 的元素構成單位群 \mathcal{U}_p 。 且任意 $-K_p$ 的元素則可表成係數落在 S 以 π_p 為幕次的 Laurent 級數。

例題 1: 設 $K = \mathbf{Q}$ 且 $\mathcal{P} = (p)$, 可選 $\pi_p = p$ 及 $S = \{i \mid 0 \leq i \leq p-1\}$, 則

$$\begin{aligned} \mathcal{O}_p &= \mathbf{Z}_p = \left\{ \sum_{i=0}^{\infty} a_i p^i \mid 0 \leq a_i \leq p-1 \right\}, \\ \mathbf{Q} \cap \mathbf{Z}_p &= \left\{ \frac{m}{n} \mid m, n \in \mathbf{Z}, p \nmid n \right\} \end{aligned}$$

$$\mathcal{P}_p = p\mathbf{Z}_p = \left\{ \sum_{i=1}^{\infty} a_i p^i \mid 0 \leq a_i \leq p-1 \right\},$$

$$\mathcal{U}_p = \left\{ \sum_{i=0}^{\infty} a_i p^i \mid 0 \leq a_i \leq p-1, \text{ 且 } a_0 \neq 0 \right\},$$

$$\mathbf{Q}_p = \left\{ \sum_{i>-\infty}^{\infty} a_i p^i \mid 0 \leq a_i \leq p-1 \right\},$$

餘數體是 $\mathbf{Z}_p/p\mathbf{Z}_p \cong \mathbf{Z}/p\mathbf{Z}$ 。

習題 1: 在例題 1 中, 將 -1 與 $\frac{1}{r}$, 其中 $p \nmid r$, 表示成係數在 S 變數為 p 的 Taylor 級數

例題 2: 設 $K = k(T)$ 且 \mathcal{P} 是次數為 1 的位, 它對應點 $a \in k$ 。 選定 $\pi_p = T - a$ 以及 $S = k$, 則整數環是由係數在 k 之 $T - a$ 的 Taylor 級數所組成; \mathcal{U}_p 是在 a 不為零的元素所組成。 在 \mathcal{P} 的餘數體與 k 同構, 而完備體 K_p 是形式幕級數 $k((T-a))$ 所形成的體, 這體與 $k((T))$ 同構。

現把 K_p 視為拓模群而觀察其拓模結構。 理想族 $\{\mathcal{P}_p^n\}_{n \geq 0}$ 形成 0 附近的鄰近系統 (neighborhood system)。 故看成加法拓模群時, K_p 是局部緊緻且完全不連結 (即每一點各自形成一連結分支)。 且 \mathcal{O}_p (及 $\mathcal{P}_p^n, n \geq 1$) 既是開集也是緊緻, 而單位群 \mathcal{U}_p 上有自然的 Filtration

$$\mathcal{U}_p \supset 1 + \mathcal{P}_p \supset 1 + \mathcal{P}_p^2 \supset \cdots \supset 1 + \mathcal{P}_p^n \supset$$

在上面這系列中, 第一個商群和餘數體的乘法群同構; 而其他剩下的連續商則與餘數體的加法群同構, 群 $\{1 + \mathcal{P}_p^n\}_{n \geq 1}$ 形成 1 的鄰近系統。 故乘法群 K_p^\times 也是局部緊緻, 而 \mathcal{U}_p 是開集也是緊緻。 注意到 K_p^\times 上的拓模是承襲 K_p 的拓模而來。

上面所定義的賦值 $|\cdot|_p$ 不具阿基米德性質, 稱為非阿基米德賦值 (nonarchimedean

valuation), 而位 \mathcal{P} 稱為非阿基米德位 (nonarchimedean place)。當 K 是函數體時, 所有的賦值都是非阿基米德, 但 K 是數體時, 也會有阿基米德賦值, 因而得出 K 的阿基米德 (無窮) 位。說得更精確一點; 設 K 是 \mathbf{Q} 的 n 次擴充體, 則 $k = \mathbf{Q}(\xi), \xi \in K$ 。 ξ 之有理係數不可約多項式的次數是 n , 設 ξ_1, \dots, ξ_{r_1} 是這多項式的實根, 而 $\xi_{r_1+1}, \bar{\xi}_{r_1+1}, \xi_{r_1+2}, \bar{\xi}_{r_1+2}, \dots, \xi_{r_1+r_2}, \bar{\xi}_{r_1+r_2}$ 是這多項式的複數根。在此 $n = r_1 + 2r_2$ 且 $\bar{\xi}_j$ 是 ξ_j 的共軛複數。則有 n 個從 K 到 \mathbf{C} 的嵌入 (embedding) 如下:

$$\begin{aligned} \sigma_i &: \xi \rightarrow \xi_i, \quad i = 1 \cdots, r_1 \\ \tau_j &: \xi \rightarrow \xi_{r_1+j}, \quad 1 \leq j \leq r_2 \\ \bar{\tau}_j &: \xi \rightarrow \bar{\xi}_{r_1+j}, \end{aligned}$$

故 $\sigma_i(K)$ 是 \mathbf{R} 的子體, 而 $\tau_j(K), \bar{\tau}_j(K)$ 則是 \mathbf{C} 的子體。

把 \mathbf{R} 或 \mathbf{C} 上的一般絕對值限制到 K 嵌入的映像, 則得到 K 上的賦值, 而這樣的賦值完備體則是 \mathbf{R} 或 \mathbf{C} 。另一方面, τ_j 與 $\bar{\tau}_j$ 得出同一個賦值, 且 $\sigma_1, \dots, \sigma_{r_1}, \tau_1, \dots, \tau_{r_2}$ 是 K 中不等價的相異賦值, 稱為 K 的阿基米德位, 因每一位都具有阿基米德性質, 我們稱 K 有 r_1 個實位 (real place) 與 r_2 個複位 (complex place)。

所謂的大域體 (global field) 是指數體或常數體為有限體的單變數函數體。若 v 是大域體 K 的一位, K 對 v 的完備體以 K_v 表示, 稱為局部體 (local field)。故 K_p, \mathbf{R} 與 \mathbf{C} 都是局部體, 其中 \mathbf{R} 與 \mathbf{C} 是阿基米德局部體,

而 K_p 是非阿基米德局部體, 這二者都局部緊緻 (locally compact)。 K_v 上的標準賦值定義為

$$|\cdot|_v = \begin{cases} |\cdot|_p & \text{若 } K_v = K_p \\ |\cdot|_{\mathbf{R}} & \text{若 } K_v = \mathbf{R} \\ |\cdot|_{\mathbf{C}} & \text{若 } K_v = \mathbf{C} \end{cases}$$

在最後一種情形, \mathbf{C} 上的賦值是平方, 原因是兩個複數嵌入只對應到一個位, 若 $|\cdot|$ 是體 K 上的非阿基米德賦值, 則 $|\cdot|$ 任意正幕次方也是 K 上的非阿基米德賦值, 但定出同樣的拓模結構, 我們稱這兩種賦值等價。大域體的每一非阿基米德位置對應到一賦值的等價類, 每一類中取一定為標準賦值。為什麼標準賦值要這樣選取? 在下一節的討論中可看出理由。可以證明: 大域體上的任一非顯然賦值一定等價於 $|\cdot|_{\mathbf{R}}, |\cdot|_{\mathbf{C}}$ 或標準的 p -adic 賦值。

下述引理是非常基本且常用的

Hensel 預備定理: 設 K 是一非阿基米德局部體, 其整數環是 \mathcal{O} 且最大理想是 \mathcal{P} 。 $F(x)$ 是係數在 \mathcal{O} 的多項式, 假設在 modulo \mathcal{P} 後, $\bar{F}(x)$ 可分解成係數在餘數體 \mathcal{O}/\mathcal{P} 的兩互質多項式 $g(x)$ 與 $h(x)$ 的乘積; 則存在有二係數在 \mathcal{O} 的多項式 $G(x), H(x)$, 分別是 $g(x)$ 與 $h(x)$ 的提升 (lifting), 使得 $F(x) = G(x)H(x)$ 且 $\deg G(x) = \deg g(x)$ 。

證明: 我們使用連續逼進法把 $F(x)$ 分解。設 $G_0(x)$ 與 $H_0(x)$ 是 $\mathcal{O}[x]$ 的兩多項式, 分別是 $g(x)$ 與 $h(x)$ 的提升且滿足

$$\deg G_0 = \deg g, \quad \deg H_0 = \deg h,$$

那麼

$$F(x) - G_0(x)H_0(x) = \pi F_1(x),$$

其中 π 是 \mathcal{P} 的 uniformizer 且 $F_1(x) \in \mathcal{O}[x]$ 。

其次解同餘方程式

$$F(x) \equiv [G_0(x) + \pi g_1(x)][H_0(x) + \pi h_1(x)] \pmod{\mathcal{P}^2}$$

其中 $g_1, h_1 \in \mathcal{O}[x]$; 這相當於解

$$F_1(x) \equiv g_1(x)H_0(x) + h_1(x)G_0(x) \pmod{\mathcal{P}}$$

換句話說, 視為 $\mathcal{O}/\mathcal{P}[x]$ 中的多項式, 它們滿足

$$\overline{F_1(x)} = \overline{g_1(x)}h(x) + \overline{h_1(x)}g(x)$$

因 $g(x)$ 與 $h(x)$ 互質, 上面的方程式對 $\overline{g_1}, \overline{h_1}$ 在 $\mathcal{O}/\mathcal{P}[x]$ 中有解。選擇 $\overline{g_1}, \overline{h_1}$ 使得 $\deg \overline{g_1} < \deg g$, 則 $\deg \overline{h_1} \leq \deg F - \deg g$ 。

設 g_1 與 h_1 分別是 $\overline{g_1}$ 與 $\overline{h_1}$ 在 $\mathcal{O}[x]$ 中的提升且次數不變。

$$\begin{aligned} \text{令 } G_1(x) &= G_0(x) + \pi g_1(x) \text{ 且} \\ H_1(x) &= H_0(x) + \pi h_1(x), \\ \text{則 } \deg G_1 &= \deg g, \overline{G} = g, \overline{H_1} = h, \text{ 且} \\ F - G_1(x)H_1(x) &= \pi^2 F_2, \end{aligned}$$

其中 $F_2(x) \in \mathcal{O}[x]$ 且 $\deg F_2 \leq \deg F$ 。

解同餘方程式

$$F(x) \equiv (G_1(x) + \pi^2 g_2(x))(H_1(x) + \pi^2 h_2(x)) \pmod{\mathcal{P}^3}$$

仿照上面的方法繼續下去, 最後得出二系列多項式

$$\{G_0(x), G_1(x), \dots, G_m(x), \dots\}$$

與 $\{H_0(x), H_1(x), \dots, H_n(x), \dots\}$ 滿足

$$G_{i+1}(x) \equiv G_i(x) \pmod{\mathcal{P}^{i+1}},$$

$$H_{i+1}(x) \equiv H_i(x) \pmod{\mathcal{P}^{i+1}}$$

$$\deg G_i = \deg g$$

$$\text{且 } F(x) \equiv G_i(x)H_i(x) \pmod{\mathcal{P}^{i+1}}.$$

故兩數列都是 Cauchy 系列, 設其分別收斂至 $G(x)$ 與 $H(x)$ 。則 $\deg G = \deg G_0 = \deg g, \overline{G} = g, \overline{H} = h$ 。從

$$F(x) \equiv G_n(x)H_n(x) \pmod{\mathcal{P}^{n+1}}, n \geq 1.$$

取極限, 則得出 $F(x) = G(x)H(x)$ 如所欲。

習題 2: 設 K 是一函數體, 其常數體是 k 。設 v 是 K 的 n 次位。對任意 K_v 的 uniformizer π_v , 證明 K 與形式冪級數 $k_n(|\pi_v|)$ 同構。

第二節. 賦值的擴充

設 K 是一非阿基米德局部體, 其賦值是 $|\cdot|_K$, 設 L 是 K 的一可分離 (separable) 擴充體, 次數為 $[L : K] = n$; 則有 n 個 L 到 K 之代數閉包 \overline{K} 的嵌入 $\sigma_1, \dots, \sigma_n$ 。利用這 n 個嵌入, 我們可定義 L 中的元素 z 的 trace 與 norm 為

$$\begin{cases} Tr_{L/K}(z) = \sigma_1(z) + \dots + \sigma_n(z), \\ N_{L/K}(z) = \sigma_1(z) \cdots \sigma_n(z). \end{cases}$$

可以證明: $Tr_{L/K}$ 是由加法群 L 到加法群 K 的同態 (homomorphism) 且 $N_{L/K}$ 是乘法群 L^\times 到乘法群 K^\times 的同態。更進一步, 若 M 是 L 中包含 K 的子體, 則

$$\begin{aligned} Tr_{L/K} &= Tr_{M/K} \circ Tr_{L/M} \\ \text{且 } N_{L/K} &= N_{M/K} \circ N_{L/M}. \end{aligned}$$

$Tr_{L/K}(z)$, $N_{L/K}(z)$ 與 z 之不可約多項式的關係與有限體的無異，見於有限體一文中的定理 5 與習題 2，細節留做習題。

現我們將 K 上的賦值 $|\cdot|_K$ 擴充到 L 上的賦值 $|\cdot|_L$ 。假設這可以做到。那麼當 L 是 K 的 Galois 擴充時， z 的所有共軛數應有一樣的取值，故

$$\begin{aligned} |z|_L^n &= |\sigma_1(z)|_L \cdots |\sigma_n(z)|_L \\ &= |N_{L/K}(z)|_L = |N_{L/K}(z)|_K \end{aligned}$$

這表示

$$|z|_L = |N_{L/K}(z)|_K^{1/n}.$$

而上式即使在 L 不是 K 的 Galois 擴充的情況下也有意義。這建議了下面的。

定理 1: 設 K 是一具賦值 $|\cdot|_K$ 的非阿基米德局部體， L 是 K 的 n 次可分離擴充體，則 $|\cdot|_K$ 可唯一擴充到 L 上的一賦值 $|\cdot|_L$ ，其定義為

$$|z|_L = |N_{L/K}(z)|_K^{1/n}, \quad z \in L$$

更進一步， L 對 $|\cdot|_L$ 是完備。

證明: 存在性。 對 $z \in L$ ，定義

$$|z|_L = |N_{L/k}(z)|_k^{1/n}.$$

顯然地，它滿足賦值的條件(1) 與 (2)。剩下要證的是對 $z, w \in L$,

$$|z + w|_L \leq \max(|z|_L, |w|_L).$$

由定義看來，這等價於證明若 $z \in L$ 滿足 $|N_{L/k}(z)|_k \leq 1$ ，則 $|N_{L/k}(1 + z)|_k \leq 1$ 。

考慮 z 在 K 中的不可約多項式 $f(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_0$ ，則

$$[a_0(-1)^m]^{n/m} = N_{L/K}(z)$$

故 $|a_0|_K \leq 1$ 。換句話說， a_0 落在 K 的整數環 \mathcal{O}_K 裡，因

$$\begin{aligned} f(-1) &= (-1)^m N_{K(z)/K}(1 + z) \\ &= (-1)^m + (-1)^{m-1} a_{m-1} + \cdots + a_0, \end{aligned}$$

若有辦法證出所有的係數 $a_i \in \mathcal{O}_k$ ，則 $N_{K(z)/K}(1 + z)$ 的係數也一樣落在 \mathcal{O}_k ，自然地 $N_{L/K}(1 + z)$ 的係數也一樣，而得出 $|N_{L/K}(1 + z)|_K \leq 1$ 。

假設不然，令 j 表示滿足 $|a_j|_K \geq |a_i|_K, i = 0, \dots, m-1$ ，的最大指數，則有

$$|a_j|_K > 1, m-1 \geq j > 0$$

$$\text{且對 } i > j, |a_i|_K < |a_j|_K$$

以 \mathcal{P}_K 表示 \mathcal{O}_K 中的最大理想，則有 $a_j^{-1} \in \mathcal{P}_K$ 且對 $m-1 \geq i > j$ ，均有 $a_i a_j^{-1} \in \mathcal{P}_K$ 。多項式 $a_j^{-1} f(x)$ 落在 $\mathcal{O}_K[x]$ 中且 modulo \mathcal{P}_K 後得出 $\overline{a_j^{-1} f(x)} = \overline{g(x)h(x)}$ ，其中 $h(x) = 1$ 且 $g(x) = \overline{a_j^{-1} f(x)} = x^j + \cdots$ 是 $\mathcal{O}_K/\mathcal{P}_K[x]$ 中次數為 j 的多項式。注意到 $m > j > 0$ 。利用 Hensel 預備定理，得出

$$a_j^{-1} f(x) = G(x)H(x)$$

其中 G, H 是 $\mathcal{O}_K[x]$ 的多項式， $\deg G(x) = j$ 且

$\deg H > 0$ 。這與 f 是不可約的條件矛盾，從而證明 $a_i \in \mathcal{O}_K$ 。因此賦值的性質 (3) 成立。

唯一性: 視 L 是 K 上的 n 維向量空間。賦值 $|\cdot|_K$ 在 L 上的任意擴充賦值可定出 L 上的 norm $\|\cdot\|$ 。對所有 $\alpha \in K$ 以及 $x \in L$, 這 norm 滿足

$$\|\alpha x\| = |\alpha|_K \|x\|。$$

固定一組 L 對 K 的基底 $\{w_1, \dots, w_n\}$, 把 x 寫成 w_1, \dots, w_n 的 K -線性組合:

$$x = \alpha_1 w_1 + \dots + \alpha_n w_n, \alpha_i \in K。$$

定義

$$\|x\|_0 = \max_i |\alpha_i|_K,$$

則 $\|\cdot\|_0$ 是 L 上的 norm。假如兩個 norm $\|\cdot\|$ 與 $\|\cdot\|_0$ 是等價的 (即它們定義出相同的拓模), 那麼任意兩個 $|\cdot|_K$ 在 L 上的賦值擴充也會等價, 從而得證出唯一性。同時亦證出 L 對 $|\cdot|_L$ 的完備空間也是唯一的, 因這其實是對 $\|\cdot\|_0$ 的完備空間。故證出底下定理後, 本定理證明即完成。

定理 2: 設 K 是一賦值為 $|\cdot|_K$ 的局部體。 L 是 K 上的有限維向量空間。則任意滿足

$\|\alpha x\| = |\alpha|_K \|x\|, \alpha \in K, x \in L$ 的 norm $\|\cdot\|$ 等價於上面所定義的 norm $\|\cdot\|_0$ 。更進一步, L 對於 $\|\cdot\|$ 是完備空間。

證明: 我們必需證明存在有兩個正數 μ 與 ν , 使得對所有 $x \in L$,

$$\|x\| \leq \mu \|x\|_0 \text{ 且 } \|x\|_0 \leq \nu \|x\|$$

其中第一個不等式較容易導出。設 $x = \alpha_1 w_1 + \dots + \alpha_n w_n$, 由三角不等式得出

$$\|x\| \leq \|\alpha_1 w_1\| + \dots + \|\alpha_n w_n\|$$

$$\begin{aligned} &= |\alpha_1|_K \|w_1\| + \dots + |\alpha_n|_K \|w_n\| \\ &\leq \mu \max_i |\alpha_i|_K = \mu \|x\|_0, \end{aligned}$$

其中 $\mu = \|w_1\| + \dots + \|w_n\|$ 。為了證明另一不等式, 對 $x = \alpha_1 w_1 + \dots + \alpha_n w_n \in L, \alpha_i \in K$, 定義 n 個函數 $|\cdot|_i$ 如下:

$$|x|_i = |\alpha_i|_K$$

現只要證明存在有正數 ν_1, \dots, ν_n 使得 $|x|_i \leq \nu_i \|x\|$ 即可。在 $n = 1$ 時顯然成立。現歸納 n 加以證明。設 V 是由 w_1, \dots, w_{n-1} 所生成之 K 上的向量空間, 且令 $\|\cdot\|'$ 是 $\|\cdot\|$ 限制到 V 上的 norm, 由歸納假設, $\nu'_1, \dots, \nu'_{n-1}$ 存在, $\|\cdot\|'$ 與 $\|\cdot\|'_0$ 在 V 上等價且 V 具完備性。若 ν_n 存在, 則 ν_1, \dots, ν_{n-1} 也跟著存在。事實上, 將 x 記為 $x = x(V) + \alpha_n w_n$, 其中 $x(V) = \alpha_1 w_1 + \dots + \alpha_{n-1} w_{n-1}$ 。則對 $1 \leq i \leq n-1$

$$\begin{aligned} |x|_i &= |x(V)|_i \leq \nu'_i \|x(V)\|' \\ &\leq \nu'_i (\|x\| + \|\alpha_n w_n\|) \\ &\leq \nu'_i (\|x\| + |\alpha_n|_K \|w_n\|) \\ &\leq \nu'_i (1 + \nu_n \|w_n\|) \|x\| \end{aligned}$$

故可選定 $\nu_i = \nu'_i (1 + \nu_n \|w_n\|) (i = 1, \dots, n-1)$ 。假設 ν_n 不存在, 則存在有一序列 $\{x_j\}_{j \geq 1}$ 滿足 $|x_j|_n > j \|x_j\|$, 則 $x_j \notin V$, 注意到上不等式中, x_j 可換為非零的純量倍數時, 不等式依然成立, 故可設

$$x_j = \alpha_{j1} w_1 + \dots + \alpha_{jn-1} w_{n-1} + w_n, \alpha_{ji} \in K。$$

由這得出 $\|x_j\| < \frac{1}{j}$, 因此

$$\lim_{j \rightarrow \infty} x_j = 0 \text{ 且 } \lim_{j \rightarrow \infty} (x_j - w_n) = -w_n。$$

另一方面 $x_j - w_n$ 是封閉子空間 V 中的元素，這序列不可能收斂到 V 外的元素，因此 ν_n 確實存在，且 ν_1, \dots, ν_{n-1} 跟著存在，從而得所欲證。

註記： (1) 以 \mathcal{O}_L 表示 L 中對賦值 $|\cdot|_L$ 的整數環，在存在性的證明中已證明 \mathcal{O}_L 的元素是 \mathcal{O}_k 上的代數整數。反過來，若 $x \in L$ 是 \mathcal{O}_k 上的代數整數，則 x 的 norm 落在 \mathcal{O}_k 中，因而由 $|\cdot|_L$ 的定義知 $x \in \mathcal{O}_L$ ； \mathcal{O}_L 是由 L 中佈於 K 的整數所組合而成。換句話說，兩整數環合而為一。

(2) 若 K 是阿基米德局部體，定理 1 也成立，因

$$|z|_{\mathbf{C}} = |z\bar{z}|_{\mathbf{R}}^{1/2}, z \in \mathbf{C}$$

是 \mathbf{C} 上的一賦值，且唯一性在 \mathbf{C} 中成立。

設 $K, L, |\cdot|_K, |\cdot|_L$ 如定理 1 所示，以 $\mathcal{O}_K, \mathcal{O}_L$ 分別表示 K, L 中的整數環，且 $\mathcal{P}_K, \mathcal{P}_L$ 分別是 $\mathcal{O}_k, \mathcal{O}_L$ 中的最大理想。因 $\mathcal{O}_K \cap \mathcal{P}_L = \mathcal{P}_K$ 。 L 中的餘數體 $\mathcal{O}_L/\mathcal{P}_L$ 是 K 中餘數體 $\mathcal{O}_K/\mathcal{P}_K$ 的擴充體。設 w_1, \dots, w_f 是 \mathcal{O}_L 中的元素，modulo \mathcal{P}_L 後， $\bar{w}_1, \dots, \bar{w}_f$ 在 $\mathcal{O}_K/\mathcal{P}_K$ 是線性獨立，那麼 w_1, \dots, w_f 在 K 中也是線性獨立。若否；設 $\sum_{i=1}^f a_i w_i = 0$ 為一非顯然的關係式。我們可假設所有 $a_i \in \mathcal{O}_K$ ，但不全在 \mathcal{P}_K 中，Modulo \mathcal{P}_L 後得出 \bar{w}_i 在 $\mathcal{O}_K/\mathcal{P}_K$ 的一非顯然線性關係式，是為矛盾。這證明了 $\mathcal{O}_K/\mathcal{P}_K$ 是 $\mathcal{O}_L/\mathcal{P}_L$ 的一有限擴充體，且擴充次數 $f \leq n = [L : K]$ 。並且我們同時亦證： \mathcal{O}_L 中的任取 f 個元素，若在 modulo \mathcal{P}_L 後它們形成 $\mathcal{O}_L/\mathcal{P}_L$ 在 $\mathcal{O}_K/\mathcal{P}_K$ 之上的基底，則這 f 個元素在 K 中線性獨立。其次選定 K 中

的 uniformizer π_K 以及 L 中的 uniformizer π_L 因 $\pi_K \in \mathcal{P}_L$ ，故可表 $\pi_K = u\pi_L^e$ ，其中 e 是正整數且 u 是 \mathcal{U}_L 的單位。亦即

$$|\pi_K|_L = |\pi_L|_L^e,$$

稱 e 是 L 在 K 之上的分歧指數 (ramification index)。

定理 3: 設 K, L 如定理 1 所述，且 e, f 如上面所定。則

$$[L : K] = n = ef.$$

證明： 設 \mathcal{S} 是餘數體 $\mathcal{O}_L/\mathcal{P}_L$ 在 \mathcal{O}_L 的任意一組代表。我們知道任意 L 中的元素皆可表為 π_L 的 Laurent 冪級數，而其係數落在 \mathcal{S} 中。此外因任意冪次 π_L^j 可表為 $u_j \pi_L^i \pi_K^m$ ，其中 u_j 是單位， i, m 是整數且 $0 \leq i \leq e-1$ ，故同樣步驟可把任意 L 中的元素表為

$$\sum_{i=0}^{e-1} \sum_{m>-\infty} s_{im} \pi_L^i \pi_K^m, s_{im} \in \mathcal{S}$$

設 \mathcal{S} 是餘數體 $\mathcal{O}_K/\mathcal{P}_K$ 在 \mathcal{O}_K 中的一組代表，且 w_1, \dots, w_f 是 \mathcal{O}_L 的元素，在 modulo \mathcal{P}_L 後形成

$\mathcal{O}_K/\mathcal{P}_K$ 上的一組基底。則可選擇 \mathcal{S} 為

$$\left\{ \sum_{j=1}^f s_j w_j \mid s_j \in \mathcal{S} \right\}.$$

這證明了 $w_j \pi_L^i, 1 \leq j \leq f, 0 \leq i \leq e-1$ 生成 L 在 K 上的所有元素。

剩下要證明的是 $w_j \pi_L^i$ 在 K 中是線性獨立。假設不然則存在有一非顯然關係式

$$\sum_{i=0}^{e-1} \sum_{j=1}^f a_{ij} w_j \pi_L^i = 0$$

我們可假設 a_{ij} 都落在 \mathcal{O}_k 中且某些 a_{ij} 是單位。設 i_0 是最小的下標 m 使得對某一 j , a_{mj} 是單位。那麼對所有 $i < i_0, 1 \leq j \leq f$, 我們都有 $a_{ij} \in \mathcal{P}_K$, 這證明了

$$\sum_{j=1}^f \sum_{\substack{i \neq i_0 \\ 1 \leq i \leq e-1}} a_{ij} w_j \pi_L^i \in \mathcal{P}_L^{i_0+1},$$

因此

$$\sum_{j=1}^f a_{i_0 j} w_j \pi_L^{i_0} \in \mathcal{P}_L^{i_0+1},$$

而這表示

$$\sum_{j=1}^f a_{i_0 j} w_j \in \mathcal{P}_L.$$

換句話說: modulo \mathcal{P}_L 後, 在 $\mathcal{O}_L/\mathcal{P}_L$ 中, $\sum_{j=1}^f \overline{a_{i_0 j} w_j} = \overline{0}$. 此為 $\mathcal{O}_L/\mathcal{P}_L$ 中的非顯然關係式, 與 $\overline{w_1}, \dots, \overline{w_f}$ 在 $\mathcal{O}_K/\mathcal{P}_K$ 上是線性獨立的事實不符。因此

$$w_j \pi_L^i, 1 \leq j \leq f, 0 \leq i \leq e-1$$

形成 L 在 K 之上的一組基底, 得證出 $[L : K] = n = ef$.

註記: L/K 在 $e=1$ 時稱為無分歧 (unramified) 擴張, 而在 $f=1$ 時稱為完全分歧 (totally ramified) 擴張。

以 q 表示餘數體 $\mathcal{O}_K/\mathcal{P}_K$ 的元素個數。設 $|\cdot|_K$ 是 K 上的標準賦值滿足

$$|\pi_K|_K = q^{-1}.$$

以 $|\cdot|$ 表示等價於 $|\cdot|_K$ 在 L 上的唯一擴充 $|\cdot|_L$ 的標準賦值。故

$$|\pi_L| = |\mathcal{O}_L/\mathcal{P}_L|^{-1} = q^{-f}$$

現我們要表現出 $|\cdot|$ 。由定理3知

$$|\pi_K| = |\pi_L|^e = q^{-ef} = q^{-n} = |\pi_K|_K^n$$

故 $|\cdot| = |\cdot|_K^n$, 這與定理1組合在一起, 得出下面的推論。

推論 1 設 K 是一非阿基米德局部體, 上有標準賦值 $|\cdot|_K$ 。設 L 是 K 的 n 次可分離擴充體。則 L 上等價於 $|\cdot|_K$ 在 L 上之唯一擴充 $|\cdot|_L$ 的標準賦值 $|\cdot|$ 可表為

$$|x| = |N_{L/K}(x)|_K, x \in L.$$

習題 3: 設 K 是一非阿基米德局部體且 L 是 K 的 n 次可分離擴充體。設 K 的餘數體有 q 個元素, L 的餘數體有 q^f 個元素, L/K 的分歧數為 e , 則 $n = ef$ 。

(1) 證明 L 含有 1 的 $q^f - 1$ 次方根 (提示: 利用 Hensel 預備定理)。

(2) 設 ξ 是 L 中的 1 的原始 $q^f - 1$ 次方根且令 $M = K(\xi)$ 。證明 M 是 K 的 f 次無分歧擴充, 且 L 是 M 的完全分歧擴充。

事實上, 任意 K 的無分歧擴充都包含在 M 中, 故 M 是 K 在 L 中的最大無分歧擴充。

(3) 設 π_L 是 \mathcal{P}_L 的 uniformizer, 又

$$f(x) = x^r + a_{r-1}x^{r-1} + \dots + a_0$$

是 π_L 在 M 中的不可約多項式, 證明 $a_i \in \mathcal{P}_M, a_0 \in \mathcal{P}_M - \mathcal{P}_M^2$ 且 $r = e$ 故 $L = M(\pi_L)$ 。

設 K 是一體, L 是 K 的 n 次擴充體, 並設 w_1, \dots, w_n 是 L 在 K 上的一組基底, 則

$$w_i w_j = \sum_{k=1}^n a_{ijk} w_k \quad (*)$$

其中 $a_{ijk} \in K$, 這組關係式決定 L 到同構階段。

設 A 是包含 K 的一環, 則張量乘積 (tensor product) $A \otimes_K L$ 是由 $\sum_{i=1}^n c_i w_i, c_i \in A$ 所組成。由代數觀點來講, 這環的加法是各分量相加, 而乘法則由 $(*)$ 所決定。注意到 A 與 L 都可嵌入 $A \otimes_K L$ 中, 若 A 上有拓樸結構, 則可在 $A \otimes_K L$ 藉由映射

$$(c_1, \dots, c_n) \in A^n \mapsto \sum_{i=1}^n c_i w_i \in A \otimes_K L$$

給出一個與 A^n 上乘積拓樸同態的拓樸。

很容易驗證 $A \otimes_K L$ 上的代數結構與拓樸結構皆和 L 在 K 上的基底 $\{w_1, \dots, w_n\}$ 的選取無關。

定理 1 描述局部體上賦值擴張的情形, 下面定理則描述大域體上賦值擴充的情況; 前者有唯一性, 後者則不然。

定理 4: 設 K 是一大域體且 L 是 K 的 n 次可分離擴充體 v 是 K 的一個位, 則 L 上至多有 n 個位整除 v , 即 K 上的賦值 $|\cdot|_v$ 可至多擴充為 n 個 L 上的相異 (因此不等價) 的賦值。設 $w_1, \dots, w_r (r \leq n)$ 是 L 上整除 v 的位, 以 K_v 表示 K 在 v 的完備空間, L_{w_i} 表示 L 在 w_i 的完備空間, 則

$$K_v \otimes_K L \cong L_{w_1} \oplus \dots \oplus L_{w_r} \quad (5)$$

為代數上的同構與拓樸上的同態, 此處右邊是賦予乘積拓樸。

證明: 存在有 L 中的元素 ξ 使得 $L = K(\xi)$ 。設 $f(x)$ 是 ξ 在 K 上的不可約多項式,

把 $f(x)$ 分解成 K_v 中之不可約多項式 $f_i(x)$ 的乘積:

$$f(x) = f_1(x) \cdots f_r(x)。$$

因 L 是 K 的可分擴充體, 因子 $f_i (1 \leq i \leq r)$ 兩兩互質; 而顯然地, $r \leq n$ 。由代數方面來看, 利用中國餘式定理, 則有下列同構

$$\begin{aligned} K_v \otimes_K L &\cong K_v \otimes_K K[x]/(f(x)) \\ &\cong K_v[x]/(f(x)) \cong \prod_{i=1}^r K_v[x]/(f_i(x)) \end{aligned}$$

在這裡, 每一 $K_v[x]/(f_i(x))$ 都是 K_v 的有限代數擴充體, 稱為 L_i 。在上面的同構中, 元素 ξ 先對應到 $K_v[x]/(f(x))$ 中的 $x + (f(x))$, 而再對應到 $\prod_{i=1}^r K_v[x]/(f_i(x))$ 中的 $(x + (f_1(x)), \dots, x + (f_r(x)))$ 。因此, 對每一 $1 \leq i \leq r$, 函數

$$\xi \mapsto x + (f_i(x))$$

是 $K[\xi]$ 到 $L_i = K_v[x]/(f_i(x))$ 的一非顯然同態。因 $K[\xi] = L$ 是一體, 這表示 L 可嵌入每一 L_i 中, 以 $|\cdot|_i$ 表示 K_v 上賦值 $|\cdot|_v$ 在 L_i 的唯一擴充。因 K 在 K_v 中具稠密性, $K \otimes_L L$ 在 $K_v \otimes_K L$ 也稠密, 故 L 在每一 L_i 稠密。 $|\cdot|_i$ 限制到 L 時對應於 L 中的位 w_i , 且 L_i 是對 $|\cdot|_i$ 的完備空間 L_{w_i} 。

我們必需證明 $|\cdot|_i (1 \leq i \leq r)$ 兩兩相異, 且它們是 $|\cdot|_v$ 在 L 中的所有擴充賦值。設 $|\cdot|$ 是一 $|\cdot|_v$ 在 L 上的擴充賦值。則由連續性, $|\cdot|$ 可擴充為 $K_v \otimes_K L$ 上的實值函數並滿足

$$|\alpha\beta| = |\alpha||\beta|$$

以及

$$\begin{cases} |\alpha+\beta| \leq \max(|\alpha|, |\beta|), \text{ 若 } |\cdot|_v \text{ 是非阿基米德,} \\ \text{或} \\ |\alpha + \beta| \leq |\alpha| + |\beta|, \text{ 若 } |\cdot|_v \text{ 是阿基米德.} \end{cases}$$

將 $|\cdot|$ 限制到 L_i 上。若存在有元素 $\alpha \in L_i$, 使得 $|\alpha| \neq 0$, 則對任意 L_i 中的非零元素 β , 由關係式 $|\alpha| = |\beta||\alpha\beta^{-1}| \neq 0$ 得出 $|\beta| \neq 0$; 故 $|\cdot|$ 限制到 L_i 是 $|\cdot|_v$ 的擴充賦值, 利用定理 1, 它等於 $|\cdot|_i$ 。因 $|\cdot|$ 在 $K_v \otimes_K L$ 上非零, 故在某一 L_i 也非零, 這證明所有 L 上之 $|\cdot|_v$ 的擴充賦值皆落在 $|\cdot|_1, \dots, |\cdot|_r$ 之中。更進一步, 若 $|\cdot|_i = |\cdot|_j$, 選擇 $|\cdot| = |\cdot|_i = |\cdot|_j$, 會得出 $|\cdot|$ 限制到 L_i 與 L_j 上皆不為零。設 $\alpha \in L_i^\times$ 且 $\beta \in L_j^\times$, 視為 $K_v \otimes_K L$ 的元素, 則有

$$\begin{aligned} & \alpha\beta \\ &= (0, \dots, 0, \alpha, 0, \dots, 0)(0, 0, \dots, 0, \beta, 0, \dots, 0) \\ & \quad \quad \quad \uparrow \quad \quad \quad \uparrow \\ & \quad \quad \quad \text{第 } i \text{ 位置} \quad \quad \quad \text{第 } j \text{ 位置} \\ &= (0, \dots, 0) = 0 \end{aligned}$$

但 $0 = |0| = |\alpha\beta| = |\alpha||\beta| \neq 0$, 得出矛盾。這證明了代數部份同構。

剩下需證明 (5) 是拓樸同態。對 $x = (x_1, \dots, x_r) \in L_{w_1} \oplus \dots \oplus L_{w_r}$, 定義

$$\|x\|_0 = \max_{1 \leq i \leq r} |x_i|_i.$$

把 $L_{w_1} \oplus \dots \oplus L_{w_r}$ 視為 K_v 上的向量空間, 則 $\|\cdot\|_0$ 是其上的 norm, 且這 norm 引導出乘積拓樸。另一方面由定理 2 知, K_v 上之有限維向量空間的 norm 都等價, 故 $\|\cdot\|_0$ 也引導出 $K_v \otimes_K L$ 上的張量乘積拓樸, 定理證畢。

推論 2: 設 K 是一大域體且 L 是 K 的有限可分離擴充體。設 v 是 K 的一個位

且 w_1, \dots, w_r 是 L 中整除 v 的位。令 $\xi \in L$ 。則

$$\begin{aligned} N_{L/K}(\xi) &= \prod_{i=1}^r N_{L_{w_i}/K_v}(\xi) \\ \text{且 } Tr_{L/K}(\xi) &= \sum_{i=1}^r Tr_{L_{w_i}/K_v}(\xi) \end{aligned}$$

證明: 如上定理所述

$$\sum_{i=1}^r [L_{w_i} : K_v] = n = [L : K],$$

故推論對 $\xi \in K$ 成立。其次設 $K(\xi) = L$, 令 $f(x)$ 與 $f_i(x)$ 如上面證明所定, 則有

$$\begin{aligned} N_{L/K}(\xi) &= (-1)^n f(0) \\ \text{且 } N_{L_{w_i}/K_v}(\xi) &= (-1)^{[L_{w_i}:K_v]} f_i(0) \end{aligned}$$

又

$$Tr_{L/K}(\xi) = -(f \text{ 的 } x^{n-1} \text{ 係數}), \text{ 且}$$

$$\begin{aligned} & Tr_{L_{w_i}/K_v}(\xi) \\ &= -(f_i(x) \text{ 的 } x^{[L_{w_i}:K_v]-1} \text{ 係數}). \end{aligned}$$

因 $f(x) = f_1(x) \cdots f_r(x)$, ξ 的大域 norm 與 trace 與局部的 norm, trace 的關係式如推論所述。

最後討論當 $M = K[\xi]$ 為一中間體的情形。設 v_1, \dots, v_s 是 M 中的整除 v 的位, 則 w_1, \dots, w_r 是 L 中整除 v_1, \dots, v_s 的位, 固定 M 中的一個位 v_i , 則有

$$\begin{aligned} & \prod_{w_j|v_i} N_{L_{w_j}/M_{v_i}}(\xi) \\ &= \prod_{w_j|v_i} N_{M_{v_i}/K_v} \circ N_{L_{w_j}/M_{v_i}}(\xi) \end{aligned}$$

$$\begin{aligned}
 &= N_{M_{v_i}/K_v}(\xi)^{\sum_{w_j/v_i} [L_{w_j}:M_{v_i}]} \\
 &= N_{m_{v_i}/K_v}(\xi)^{[L:M]},
 \end{aligned}$$

故

$$\begin{aligned}
 &\prod_{w_j/v_i} N_{L_{w_j}/K_v}(\xi) \\
 &= \prod_{v_i|v} \prod_{w_j|v_i} N_{L_{w_j}/K_v}(\xi) \\
 &= \prod_{v_i|v} N_{M_{v_i}/K_v}(\xi)^{[L:M]} \\
 &= N_{M/K}(\xi)^{[L:M]} = N_{L/K}(\xi).
 \end{aligned}$$

類似方法可證 $Tr_{L/K}(\xi) = \sum_{i=1}^r Tr_{L_{w_i}/K_v}(\xi)$ 。

推論 3: 設 K 是一大域體且 L 是 K 的有限可分離擴充體。設 v 是 K 的一個位且 w_1, \dots, w_r 是 L 中整除 v 的位。以 $| \cdot |_v$ 和 $| \cdot |_w$ 分別表示 K_v 和 L_w 的標準賦值，則有

$$|N_{L/K}(\xi)|_v = \prod_{i=1}^r |\xi|_{w_i}.$$

證明: 當 v 是非阿基米德時，這由推論 2 與推論 3 得出。當 v 是阿基米德時，則可由推論 2 與標準的阿基米德賦值定義得出。

在這一段裡，我們考慮大域體中的非零元素在每個位的賦值。

定理 5: 設 K 是一大域體，令 $\xi \in K^\times$ ，則除有限多個位 w 外， $|\xi|_w = 1$ 。

證明: 若 $K = \mathbf{Q}$ 或有限體上的單變數函數體，這顯然成立。若 K 是函數體，但非有理函數體，則存在有一 K 的有理函數子體 F ，使得 K 是 F 的有限可分離擴充體。若 K 是一數

體，則選 $F = \mathbf{Q}$ ，於是 K 是 F 的有限可分離擴充體。

設

$$f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0$$

為 ξ 在 F 的不可約多項式。對每一 a_i ，除有限個 F 的位外，對其他位而言，它都是整數；故存在有一 F 中位置的有限集合 \mathcal{S} ，使得對 $v \notin \mathcal{S}$ 時，則有 $a_i \in \mathcal{O}_v$ 。因 $a_0 \neq 0$ ，必要時可擴充 \mathcal{S} ， $v \notin \mathcal{S}$ 時， $|a_0|_v = 1$ 。

設 \mathcal{S} 是由 K 中整除 \mathcal{S} 的位所構成的集合，由定理 4 知 \mathcal{S} 是一有限集。對任意 K 中落在 \mathcal{S} 之外的位 w ，則有 w 整除 F 中某一落在 \mathcal{S} 之外的位 v ， ξ 是佈於 \mathcal{O}_v 上的整數，故由定理 1 後的註記知它落在 \mathcal{O}_w 中，更進一步，由推論 1 與 3，得出

$$\begin{aligned}
 &|\xi|_w = |N_{K_w/F_v}(\xi)|_v \leq 1 \\
 &\text{且 } \prod_{w|v} |\xi|_w = |N_{K/F}(\xi)|_v = |a_0|_v^{[k:F(\xi)]} = 1.
 \end{aligned}$$

這表示 w 在 \mathcal{S} 之外時， $|\xi|_w = 1$ 。這證明了定理。

當 K 為一函數體時，上面的定理告訴我們：定義在有限體上之非奇異投影曲線上的非零有理函數，只會在有限多個封閉點上具零位或極點。

定理 6: (乘積式) 設 K 為一大域體且 $\xi \in K^\times$ 。又設 Σ 是由 K 的所有位所構成的集合，則

$$\prod_{w \in \Sigma} |\xi|_w = 1.$$

注意: 由定理 5 知無窮乘積 $\prod_{w \in \Sigma} |\xi|_w$ 事實上只是有限乘積，故定義上沒有收斂的問題。

證明: 情形 1. $K = \mathbf{Q}$. 可設 $\xi = n$ 非零整數, 將 n 分解成質因數乘積,

$n = \pm p_1^{e_1} \cdots p_r^{e_r}, e_i > 0, p_1, \dots, p_r$ 是相異質數。

由賦值定義知 $|n|_{p_i} = p_i^{-e_i} (i = 1, \dots, r)$, 當 $p \neq p_1, \dots, p_r$ 時, $|n|_p = 1$; 且 $|n|_R = n$, 故

$$\prod_{v \in \Sigma} |n|_v = 1.$$

情形 2. $K = k(T)$ 是 q 個元素有限體 k 上的有理函數體。可設 $\xi = g(T)$ 是 $k[T]$ 中的非零多項式。以 ∞ 表 K 中以 $\frac{1}{T}$ 當 uniformizer 的位。將 $g(T)$ 分解成不可約多項式的乘積

$$g(T) = a g_1(T)^{e_1} \cdots g_r(T)^{e_r},$$

其中 $a \in k^\times, e_i > 0, g_1, \dots, g_r$ 相異, 以 v_i 表示 K 中以 $g_i(T)$ 當 uniformizer 的位。則

$$|g(T)|_{v_i} = q^{-f_i e_i}$$

其中 $f_i = \deg g_i$; 而當 $v \neq v_1, \dots, v_r, \infty$ 時, $|g(T)|_v = 1$ 且

$$|g(T)|_\infty = q^{\sum_{i=1}^r f_i e_i},$$

這是因為 g 在 ∞ 的極點重數 = $\deg g = \sum_{i=1}^r f_i e_i$, 且 ∞ 是一次位, 故有

$$\prod_{v \in \Sigma} |\xi|_v = 1.$$

情形 3: K 是 $F = \mathbf{Q}$ 或 $k(T)$ 的有限可分離擴充體。令 Σ' 表示 F 中所有位的集合。設 $\xi \in K^\times$,

$$\prod_{w \in \Sigma} |\xi|_w = \prod_{v \in \Sigma'} \prod_{w|v} |\xi|_w$$

$$\begin{aligned} &= \prod_{v \in \Sigma'} |N_{k/F}(\xi)|_v \text{ (由推論 3)} \\ &= 1. \end{aligned}$$

因 $N_{k/F}(\xi) \in F^\times$ 且定理對 F 中的元素成立。

因 $N_{k/F}(\xi) \in F^\times$ 且定理對 F 中的元素成立。

在函數體的情形, 上面定理告訴我們: 非奇異投影曲線 C 上的任意非零有理函數 ξ , 重數照算的話, 其零位個數等於極點個數的總和。這裡個數的算法如下: 如封閉點 x 的次數是 f , 而 x 是 ξ 的重數為 e 的零位, 則 ξ 在 x 的零位個數是 ef 。

推論 4: 設 K 是常數體為 k 的函數體, $\xi \in K^\times$ 。若對 K 的所有位置 w , ξ 均落在 \mathcal{O}_w , 則 $\xi \in k^\times$ 。

證明: 因 ξ 沒有極點, 故也不會有零位。換句話說, 必是個非零常數。

第三節. Adèles 與 Idèles

給定一定義在大域體 K 的代數群 G , 我們想研究大域點 $G(K)$ 與局部點 $G(K_v)$ 之間的關係。最直覺的想法是考慮無窮乘積 $\prod_v G(K_v)$, 其中 v 跑遍所有 K 的位。不幸地, 這無窮乘積沒有很好的拓模性質。取而代之的想法是取 $G(K_v)$ 的“限制乘積”。在此我們就開始引介限制乘積的基本概念。

設 $\{G_v\}_{v \in \Sigma}$ 是一族局部緊緻的拓模群, 其指標集合是 Σ 。設 Σ_0 是 Σ 的有限子集合。對每一 $v \in \Sigma - \Sigma_0$, 我們固定一 G_v 的緊緻開子群 H_v , 對每一 Σ 中包含 Σ_0 的有限集合 S ,

定義

$$G_S = \prod_{v \in S} G_v \prod_{v \in \Sigma - S} H_v,$$

且賦予 G_S 乘積拓模。注意到 G_S 還是局部緊緻, 若 S_1 與 S_2 是兩個這樣的集合且滿足 $S_1 \supset S_2$, 則 $G_{S_1} \supset G_{S_2}$ 且 G_{S_2} 上的拓模是由 G_{S_1} 上的拓模限制下來的。定義 $\{G_v\}$ 對於 $\{H_v\}$ 的限制乘積 G 為 G_S 在包含關係下的直極限 (Direct limit) 而 S 跑遍所有 Σ 中包含 Σ_0 的有限子集。 G 中子集 U 是開集的充要條件是: 對所有包含 Σ_0 的有限子集 S , $U \cap G_S$ 都是 G_S 的開子集。因此, G 之單位元素 1 的任何開鄰域 (open neighborhood) 都會包含 $\prod_{v \in S} U_v \prod_{v \in \Sigma \setminus S} H_v$, 在此 S 是某一包含 Σ_0 的有限子集且 U_v 是 G_v 中包含 1 的開集。所以 G 是一個局部緊緻拓模群 (locally compact topological group), 其代數與拓模結構均與 Σ_0 的選取無關。

取一大域體 K , 令 $\Sigma = \Sigma_K$ 是 K 之所有位所形成的集合且 $\Sigma_0 = \Sigma_\infty$ 是 K 上的所有阿基米德位 (若 K 是函數體, 這集合是空集合)。首先考慮 $G = G_a$ 為加法群的情形。對 $v \in \Sigma$, $G_v = G(K_v) = K_v$ 且對 $v \in \Sigma - \Sigma_0$, 令 $H_v = G(\mathcal{O}_v) = \mathcal{O}_v$ 。那麼 $\{K_v\}_{v \in \Sigma}$ 對 $\{\mathcal{O}_v\}_{v \in \Sigma - \Sigma_0}$ 的限制乘積在各分量各自相乘與相加的運算下形成一環, 稱為 K 的 adèle - 環 (ring of adèles), 記為 A_K , 換句話說,

$$A_K = \{(x_v) \in \prod_{v \in \Sigma_k} K_v \mid \text{對幾乎所有位 } v, x_v \in \mathcal{O}_v\}.$$

定理 5 表示, 對幾乎所有 K 的位 v , K 的元素都落在 \mathcal{O}_v 故可將 K 的元素對角嵌入 A_K 中, 亦即 $x \mapsto (x, \dots, x, \dots)$ 。

考慮 K 的 n -次可分離擴充體 L 。

設 w_1, \dots, w_n 是 L 在 K 上的一組基底, 且 w_1, \dots, w_r 是 L 上整除 v 的位。定理 4 告訴我: 從代數上與拓模上看,

$$K_v \otimes_K L = K_v w_1 \oplus \dots \oplus K_v w_n \cong L_{w_1} \oplus \dots \oplus L_{w_r}.$$

現我們要探討 $\mathcal{O}_v w_1 \oplus \dots \oplus \mathcal{O}_v w_n$ 與 $\mathcal{O}_{w_1} \oplus \dots \oplus \mathcal{O}_{w_r}$ 之間的關係。很明顯地, $\mathcal{O}_{w_1} \oplus \dots \oplus \mathcal{O}_{w_r}$ 是由 $K_v \otimes_K L$ 中 \mathcal{O}_v 上的整數所組成。故除了有限個 v 之外, 由定理 5 知, w_1, \dots, w_n 都是 \mathcal{O}_v 的整數。因此, 對幾乎所有位 v , $\mathcal{O}_v w_1 \oplus \dots \oplus \mathcal{O}_v w_n$ 包含在 $\mathcal{O}_{w_1} \oplus \dots \oplus \mathcal{O}_{w_r}$ 中。反過來, 設 β 為 $K_v \otimes_K L$ 中 \mathcal{O}_v 上的整數, 將其表為

$$\beta = \alpha_1 w_1 + \dots + \alpha_n w_n, \quad \alpha_i \in K_v$$

設 $\sigma_1, \dots, \sigma_n$ 是 L 到 K 之代數閉包 \overline{K} 的 n 個嵌入。對 $K_v \otimes_K L$ 中的元素 $x = x_1 w_1 + \dots + x_n w_n$, $x_i \in K_v$, 以 $x^{(j)}$ 表示

$$x_i \sigma_j(w_1) + \dots + x_n \sigma_j(w_n) \in K_v \otimes_K \overline{K}, \\ j = 1, \dots, n.$$

那麼

$$\sum_{j=1}^n x^{(j)} = x_1 \text{Tr}_{L/K} w_1 + \dots + x_n \text{Tr}_{L/K} w_n \\ = \sum_{j=1}^n x_j \sum_{i=1}^r \text{Tr}_{L_{w_i}/K_v}(w_j) \text{ (推論 2)} \\ = \sum_{i=1}^r \text{Tr}_{L_{w_i}/K_v}(x).$$

現定義 $\text{Tr}_{L/K}(x)$ 為

$$\sum_{j=1}^n x^{(j)} = \sum_{i=1}^r \text{Tr}_{L_{w_i}/K_v}(x).$$

因此若 x 是 \mathcal{O}_v 上的整數 (integral over \mathcal{O}_v) 則 $Tr_{L/K}(x) \in \mathcal{O}_v$ 。關係式 $\beta = \alpha_1 w_1 + \dots + \alpha_n w_n$ 產生了下面的矩陣方程式

$$\begin{pmatrix} w_1^{(1)} & \dots & w_n^{(1)} \\ \vdots & & \vdots \\ w_1^{(n)} & \dots & w_n^{(n)} \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} \beta^{(1)} \\ \vdots \\ \beta^{(n)} \end{pmatrix}$$

因 w_1, \dots, w_n 是 K 一線性獨立, 故矩陣 $w = (w_j^{(i)})$ 的行列式值不為零, 利用 Cramer 法則, 解出

$$\alpha_i = \frac{\det B_i}{\det W} \quad (i = 1, \dots, n)$$

其中 B_i 是把 W 的第 i 行元素以 $\begin{pmatrix} \beta^{(1)} \\ \vdots \\ \beta^{(n)} \end{pmatrix}$ 取代而得。到此為止, 我們對 α_i 所知不多, 但對

$$\alpha_i^2 = \frac{\det({}^t B_i B_i)}{\det({}^t W W)}$$

知道的卻不少。這是因為矩陣

$${}^t W W = (Tr_{L/K} w_i w_j)$$

中各行列元素均為 \mathcal{O}_v 的元素, 且 ${}^t B_i B_i$ 亦然。更進一步, $d = \det({}^t W W)$ 是 K 中的非零元素。由定理 5 知, 對幾乎所有 K 的位 v 而言, 都有 $|d|_v = 1$, 因此 α_i^2 與 α_i 也落在 \mathcal{O}_v 中; 此我們得證了: 對幾乎所有的位 v , $\beta \in \mathcal{O}_v w_1 \oplus \dots \oplus \mathcal{O}_v w_n$ 這證明了下面的預備定理。

預備定理 1: 設 L 是大域體 K 的 n 次可分離擴充體, w_1, \dots, w_n 是 L 在 K 上的一組基底。對幾乎所有 K 的位 v , 均有

$$\mathcal{O}_v w_1 \oplus \dots \oplus \mathcal{O}_v w_n = \mathcal{O}_{w_1} \oplus \dots \oplus \mathcal{O}_{w_r}$$

其中 w_1, \dots, w_r 是 L 上整除 v 的位。

結合定理 4 與預備定理 1, 得到

預備定理 2: 設 L 是大域體 K 的 n 次可分離擴充體, 則從代數上與拓樸上而言, $A_K \otimes_K L$ 與 A_L 同構且同態, 並且 $L = K \otimes_K L$ 可對角嵌入 A_L 中。

現我們已做好證明下面定理的準備工作

定理 7: 設 K 是一大域體, 則 K 是 A_K 的離散子群, 且 A_K/K 在商拓樸 (quotient topology) 下是緊緻的。

證明: 設 F 是 \mathbf{Q} 或是常數體為 k 的有理函數體, 使得 K 為 F 的 n 次可分離擴充體。設 w_1, \dots, w_n 是 K 在 F 上的一組基底, 則看成加法群時,

$$A_K = A_F \otimes_F K = A_F w_1 \oplus \dots \oplus A_F w_n.$$

假設我們可證明 F 是 A_F 的離散子群且有一 A_F 的緊緻集 Ω 使得 $A_F = F + \Omega$, 那麼 K 是 $A_F \otimes_F k = A_k$ 的離散子群。更進一步令

$$\tilde{\Omega} = \Omega w_1 + \dots + \Omega w_n$$

則其為 A_K 上的一緊緻集, 並使得 $A_K = K + \tilde{\Omega}$, 從而

$$A_K/K \cong \tilde{\Omega}/K \cap \tilde{\Omega}$$

是一緊緻集。故定理 7 的證明變成只需證 $K = \mathbf{Q}$ 與 $K = k(T)$ 的情形。

情形一: $K = k(T)$ 。令 $\Omega = \prod_{v \in \Sigma_K} \mathcal{O}_v$, 則 Ω 是 A_K 中的開緊緻集。對每一位 v , 選取在 v 的 uniformizer π_v 如下: 若 $v \neq \infty$ 令 π_v 是 $k[T]$ 中在 v 為零的不可約多項式。若 $v = \infty$, 取 $\pi_v = 1/T$ 。選定 v 之餘

數體的代表 S_v 為 $k[T]$ 中次數小於 $\deg \pi_v$ 的多項式, 則每一 K_v 的元素 x_v 可寫成

$$x_v = \sum_{i > -\infty} s_i \pi_v^i, \quad s_i \in S_v.$$

以 $\langle x_v \rangle$ 表示 $\sum_{i < 0} s_i \pi_v^i$, 稱為 x_v 的極 (polar) 部份。給定 A_k 中的元素 $x = (x_v)_{v \in \Sigma_k}$, 則只有有限個位 v , $\langle x_v \rangle$ 才不為零, 且對所有位 $w \neq v$, $\langle x_v \rangle \in \mathcal{O}_w$ 。令

$$\gamma = \sum_v \langle x_v \rangle$$

則 $\gamma \in K$ 且 $x - \gamma$ 在所有都是整數, 這證明 $A_K = K + \Omega$ 。更進一步, 由推論 4, 可知 $K \cap \Omega = k$ 是有限集。故 K 在 A_K 中離散且 $A_K/K \cong \Omega/k$ 是緊緻。

情形二: $K = \mathbf{Q}$ 。設 $\Omega = [-\frac{1}{2}, \frac{1}{2}] \times \prod_p \mathbf{Z}_p$ 。在 \mathbf{Q} 的有限位置 p , 選定 uniformizer $\pi_p = p$ 且在 p 的餘數體的代表 S_p 選定為 $\{0, 1, \dots, p-1\}$ 對 $x_p \in \mathbf{Q}_p$, 定義 x_p 的極 (polar) 部份 $\langle x_p \rangle$ 如情形一所述。對任意 $x = (x_v) \in A_{\mathbf{Q}}$, 都有對幾乎所有的 p , $\langle x_p \rangle = 0$, 故 $\gamma = \sum_p \langle x_p \rangle$ 是一有理數且對所有的 p , $x - \gamma \in \mathbf{Z}_p$ 。最後, 有一整數 $n \in \mathbf{Z}$, 使得 $x - \gamma - n$ 的絕對值落在 $[-\frac{1}{2}, \frac{1}{2}]$ 。這證明 $A_{\mathbf{Q}} = \mathbf{Q} + \Omega$ 。注意到 $(-\frac{1}{2}, \frac{1}{2}) \times \prod_p \mathbf{Z}_p$ 是 0 的開一鄰域且不包含其他的有理數, 故 \mathbf{Q} 可嵌入 $A_{\mathbf{Q}}$ 為一離散子群。最後 $A_{\mathbf{Q}}/\mathbf{Q} \cong \mathbf{R} \times \prod_p \mathbf{Z}_p/\mathbf{Z} \cong (\mathbf{R}/\mathbf{Z}) \times \prod_p \mathbf{Z}_p$ 是緊緻集。

其次取 G 為乘法群 G_m 。同樣地令 $\Sigma = \Sigma_k$ 且 $\Sigma_0 = \Sigma_{\infty}$ 則對 $v \in \Sigma_K$, $G_v = G(K_v) = K_v^{\times}$, 且對 $v \in \Sigma - \Sigma_0$, 令 $H_v =$

$G(\mathcal{O}) = \mathcal{U}_v \cdot \{K_v^{\times}\}$ 對 $\{\mathcal{U}_v\}$ 的限制乘積稱為 Idèle 群 (group of idèles), 以 I_K 表之, 因此

$$I_K = \{(x_v) \in \prod_{v \in \Sigma_k} K_v^{\times} \mid \text{對幾乎所有 } v, x_v \in \mathcal{U}_v\}.$$

注意到 I_K 在代數上而言是 A_K 的單位群, 但其上之拓模比由 A_K 得來的限制拓模還細。

習題 3: 證明在 I_K 上的自同構 $x \mapsto x^{-1}$ 在限制拓模下並不連續。事實上, 我們加在 I_K 上的拓模是使 I_K 成為拓模群的最弱拓模。

定理 5 顯示 K^{\times} 可以對角嵌入 I_K 中。商群 I_K/K^{\times} 稱為 K 的 idèle 類群 (idèle class group)。利用 K 在 v 之完備體 K_v 的標準賦值 $|\cdot|_v$, 我們定義從 I_K 到正實數群的函數 $|\cdot|$, 稱為 I_K 上之 norm 函數, 如下

$$|x| = \prod_v |x_v|_v, \quad x = (x_v) \in I_K.$$

因對幾乎所有的位 v , x_v 都是單位, 故上面的乘積事實上是有限乘積。注意到 $|\cdot|$ 是一連續同態, 其核 I_K^1 是由 norm 是 1 的 idèles 組合而成。對一數體 K , $|\cdot|$ 的映象都是正實數, 且有

$$I_K = I_K^1 \times (\mathbf{R}_{>0}^{\times})_w \cong I_K^1 \times \mathbf{R}_{>0}^{\times}.$$

其中 w 是 K 的阿基米德位且 $(\mathbf{R}_{>0}^{\times})_w$ 是 K_w 的子群。而對常數體是 q 個元素的函數體 K , $|\cdot|$ 的映象是 $\mathbf{R}_{>0}^{\times}$ 的一無窮循環子群, 它由 q 的某一幕次 q^r 所生成, 我們有

$$I_K = I_K^1 \times \langle x \rangle \cong I_K^1 \times \mathbf{Z},$$

其中 x 是一 idèle 滿足 $|x| = q^r$ 。

乘積式 (定理 6) 顯示 K^{\times} 是 I_K^1 的子群。由定理 7, 我們知道 K 是 A_K 的離散子

群。又因 I_K 上的拓模比 A_K 的限制拓模還強，故 K^\times 是 I_K 的離散子群，因而也是 I_K^1 的離散子群。

定理 8: 設 K 是一大域體，則 K^\times 是 I_K^1 的離散子群且 I_K^1/K^\times 在商拓模下是緊緻的。

現只剩下要證明第二個斷言。為此，我們需要一幾何預備定理。給定一 idèle $a = (a_v)$ 。定義“邊長是 a 的平行多面體”為

$$P_a = \{x = (x_v) \in A_k \mid |x_v|_v \leq |a_v|_v\}.$$

則有 $P_a = aP_1$ ，且 P_1 是 A_k 的緊緻集，因 A_K/K 是緊緻集，以 $\overline{\mu_K}$ 表示 A_K/K 上全測度為 1 的 Haar 測度，令 μ_K 為 A_K 的 Haar 測度，使得其限制到 K 上得出 counting 測度，引出 A_K/K 上的 $\overline{\mu_K}$ 。因此 P_a 的體積為有限且滿足

$$\mu_K(P_a) = |a| \mu_K(P_1).$$

下面預備定理告訴我們：若 P_a 的體積足夠大的話，則 P_a 至少包含 K 中的兩相異元素。這是 Minkowski 定理的一個特殊情形，以 adèlic 語言表達出來。

預備定理 3: 存在有一常數 $c > 0$ ，使得對每一 idèle a 滿足 $|a| > \frac{1}{c}$ ，都有 $P_a \cap K^\times \neq \emptyset$ 。

證明: 選定 K 的 idèle $b = (b_v)$ 滿足

$$\begin{cases} b_v = 1 & \text{若 } v \text{ 是非阿基米德位} \\ b_v = \frac{1}{4} & \text{若 } v \text{ 是阿基米德位} \end{cases}$$

則 $P_b - P_b \subseteq P_1$ 。假設 $P_a \cap K^\times = \emptyset$ ，那麼 P_{ab} 與 K ， A_k 中的任意平移至多交於一次。因若 y_1, y_2 是 $(x + K) \cap P_{ab}$ 的兩相異元素，則 $\alpha = y_1 - x, \beta = y_2 - x$ 是 K 的相異元素

且 $\alpha - \beta$ 落在 $P_{ab} - P_{ab} \subset P_a$ 中，與原先假設矛盾。以 f, \overline{f} 分別表示 $P_{ab}, (P_{ab} + K)/K$ 上的示性函數，則有

$$\begin{aligned} \mu_K(P_{ab}) &= \int_{A_K} f(x) d\mu_K(x) \\ &= \int_{A_K/K} \sum_{\alpha \in K} f(x + \alpha) d\overline{\mu_K}(\overline{x}) \\ &= \int_{A_K/K} \overline{f}(\overline{x}) d\overline{\mu_K}(\overline{x}) \quad (\text{因對所有 } x \in A_K, \\ &\quad \text{card}((x + K) \cap P_{ab}) \leq 1) \\ &\leq \int_{A_K/K} d\overline{\mu_K}(\overline{x}) = 1 \end{aligned}$$

因此，若 $c = \mu(P_0)$ ，則有 $c|a| \leq 1$ 。因此對任意 idèle a 滿足 $|a| > \frac{1}{c}, P_a \cap K^\times \neq \emptyset$ 。

現我們證明定理 8。設 a_0 是滿足 $|a_0| > \frac{1}{c}$ 的 idèle，則對任意 $a \in I_K^1$ ，則有

$$|a^{-1}a_0| = |a_0| > \frac{1}{c}.$$

依據預備定理 3，存在有非零元素 $\alpha \in K^\times$ 落在 $P_{a^{-1}a_0}$ ，亦即 $\alpha a \in P_{a_0}$ 。更進一步，因 $\alpha a \in I_K^1$ ，存在有 $\beta \in K^\times$ 使得 $\beta(\alpha a)^{-1} \in P_{a_0}$ ，組合後兩個敘述得出 $\beta \in P_{a_0^2}$ 。另一方面， $P_{a_0^2} \cap K$ 同時是緊緻且離散，故是有限集，設為

$$P_{a_0^2} \cap K = \{0, \gamma_1, \dots, \gamma_s\}.$$

現已經證明 $\alpha a \in P_{a_0}$ 且 $(\alpha a)^{-1} \in \cup_{i=1}^s \gamma_i^{-1} P_{a_0}$ ，定

$$\begin{aligned} B &= P_{a_0} \cup (\cup_{i=1}^s \gamma_i^{-1} P_{a_0}) \\ \text{且 } B^* &= \{x \in I_K \mid x, x^{-1} \in B\} \end{aligned}$$

存在有一 K 之位的有限集 S 使得在 S 之外的位 v ， $(a_0)_v$ 與 $(\gamma_i)_v$ 都是單位， $i = 1, \dots, s_0$ 因此 B^* 是 $\prod_{v \in S} K_v^\times$ 與 $\prod_{v \notin S} \mathcal{U}_v$ 乘積上之緊緻

集, 故亦為 I_K 的緊緻集。而我們已得出: 對任意 $a \in I_K^1$, 存在有 $\alpha \in K^\times$ 使得 $a\alpha \in B^\times$ 。因為 I_K^1/K^\times 是 $I_K^1 \cap B^*$ 的商, 所以必是緊緻。定理證畢。

在此, 我們提出定理 8 的一些推論。首先考慮 K 是函數體的情形。由 K 之位所生成的自由交換群 (free abelian group) 稱為 K 的除子群 (group of divisor), 以 $Div(K)$ 表之。除子 $D = \sum n_\nu V$ 的次數定義為

$$\deg D = \sum_\nu n_\nu \deg \nu,$$

在此對幾乎所有的 $\nu, n_\nu = 0$ 。這次數函數 $\deg : Div(K) \rightarrow \mathbf{Z}$ 是一同態, 其核 $Div^\circ(K)$ 是次數為零的除子子群, 我們將在第五章第四節證明次數函數的值域是 \mathbf{Z} 。

對 $\xi \in K^\times$, ξ 的除子 $div \xi = \sum n_\nu \nu$, 其中 n_ν 是 ξ 在 ν 的重數 (order)。由定理 5 與 6 我們知道對幾乎所有的 $\nu, n_\nu = 0$ 且

$$\deg(div \xi) = \sum n_\nu \deg \nu = 0.$$

因此 $div \xi$ 落在 $Div^\circ(K)$ 中, 稱為主除子 (principal divisors), 以 $Prin(K)$ 表示由主除子所形成的子群, 商群 $Div^\circ(K)/Prin(K)$ 稱為 K 的 Jacobian, 以 $Jac(K)$ 表之。

對 I_K 中的 idèle $x = (x_\nu)$, 對應 $div x = \sum_\nu (\text{ord}_\nu x_\nu) \nu$ 。因對幾乎所有的 ν, x_ν 都是單位, 故有 $div x \in Div(K)$, 賦予 $Div(K)$ 離散拓樸, 則

$$div : I_K \mapsto Div(K)$$

是連續同態且為映成 (onto), 其核是 $\prod_v \mathcal{U}_v$ 。norm 是 1 的子群 I_K^1 映到子群 $Div^\circ(K)$ 且為

映成; 又 K^\times 映成到 $Prin(K)$ 。因此 div 函數在代數與拓樸上引導出同構

$$\begin{aligned} I_K^1/K^\times \prod_v \mathcal{U}_v &\cong Div^\circ(K)/Prin(K) \\ &= Jac(K). \end{aligned}$$

由於 I_K^1/K^\times 是緊緻, 我們發現 $Jac(K)$ 同時是緊緻且離散, 因而是有限, 這證明了下面的推論。

推論 5: 設 K 是一函數體, 則

$$\begin{aligned} Jac(K) &= Div^\circ(K)/Prin(K) \\ &\cong I_K^1/K^\times \prod_v \mathcal{U}_v \end{aligned}$$

是一有限群。

其次考慮 K 是數體的情形。對每一 K 的非阿基米德位 v , 以 \mathcal{P}_v 表示對應於 v 之 K 的整數環 \mathcal{O}_K 的最大理想。以 $\mathcal{J}(K)$ 表示由 \mathcal{O}_K 的最大理想們所生成的自由交換群且以 $Prin(K)$ 表示由非零主理想所生成的自由交換群。因 \mathcal{O}_K 的每一理想且在不考慮乘積次序的前提下, 此唯一都可表為最大理想的乘積, 故 $Prin(K)$ 是 $\mathcal{J}(K)$ 的子群。而商群 $\mathcal{J}(K)/Prin(K)$ 稱為 K 的理想類群 $Cl(K)$ (ideal class group)。

對一 idèle $x = (x_\nu) \in I_K^1$, 以 $I(x)$ 表示理想

$$\prod_{v:\text{非阿基米德}} \mathcal{P}_v^{\text{ord}_v x_\nu}.$$

因對幾乎所有的位 v, x_ν 的次數是 0, 故 $I(x)$ 是 $\mathcal{J}(K)$ 的元素, 函數 $I : I_K^1 \rightarrow \mathcal{J}(K)$ 將 x 送到 $I(x)$ 是群同態。給定一 $\mathcal{J}(K)$ 的元

素 $\prod_{v:\text{非阿}} \mathcal{P}_v^{n_v}$, 現建構一 idèle $x = (x_v) \in I_k^1$ 使得 $\prod_{v:\text{非阿}} \mathcal{P}_v^{n_v}$, 如下。在每一非阿基米德位 v , 選擇一 uniformizer π_v 且令 $x_v = (\pi_v)^{n_v}$, 則對幾乎所有 v , $x_v = 1$ 。固定一阿基米德位 w , 對其他的阿基米德位 $v \neq w$ 時, 定 $x_v = 1$, 且令 x_w 是 K_w 中的元素使得

$$\prod_{v:\text{所有位}} |x_v|_v = 1.$$

故 $x = (x_v)$ 具有所要的性質。現賦予 $\mathcal{J}(K)$ 離散拓撲, 則 I 是一連續同態且映成, 其核等於 $I_\infty^1 \prod_{v:\text{非阿}} \mathcal{U}_v$, 其中 I_∞^1 是由 $\prod_{v \in \Sigma_\infty} K_v^\times$ 中滿足 $\prod_{v \in \Sigma_\infty} |x_v|_v = 1$ 的元素組成。更進一步, I 把 K^\times 映至 $Prin(K)$; 因此引導出同構

$$I_K^1 / K^\times \cdot I_\infty^1 \prod_{v:\text{非阿}} \mathcal{U}_v \cong \mathcal{J}(K) / Prin(K)$$

因 I_K^1 / K^\times 是緊緻, 這證明 $\mathcal{J}(K) / Prin(K)$ 是離散且緊緻, 因此是有限群, 從而得證下面的推論。

推論 6 (Minkowski): 設 k 是一數體, 則

$$\begin{aligned} Cl(K) &= \mathcal{J}(K) / Prin(K) \\ &\cong I_K^1 / K^\times \cdot I_\infty^1 \prod_{v:\text{非阿}} \mathcal{U}_v \end{aligned}$$

是一有限群。

落在 $K^\times \cap I_\infty^1 \prod_{v:\text{非阿}} \mathcal{U}_v$ 的元素稱為數體 K 的單位。Dirichlet 證明: 單位元素所形成的子群是由落在 K 中 1 的方根所成的有限群與階數是 $r_1 + r_2 - 1$ 之自由交換群的乘積。在此, r_1 與 r_2 分別是 K 的實位與複位一個數。

對一定義在大域體 K 的一般代數群 G , 其 adèle 點 $G(A_k)$ 即是 $\{G(K_v)\}_{v \in \Sigma_K}$ 對 $\{G(\mathcal{O}_v)\}_{v \in \Sigma_K - \Sigma_0}$ 的限制乘積。

參考資料

1. E. Artin and J. Tate: Class field theory, Harvard (1961)。
2. J.W.S. Cassels and A. Fröhlich: Algebraic Number Theory, Thompson, Washington (1967)。
3. S. Iyanaga: The theory of Numbers. North-Holland, Amsterdam-Oxford (1969)。
4. A. Weil: Basic Number Theory, Springer-Verlag, New York-Heidelberg-Berlin (1973)。
5. 李文卿: 有限體的理論, 數學傳播, 十七卷一期, 82年3月, 43~54。

—本文作者分別任教於美國賓州州立大學數學系及國立中正大學應數所—