有限體的理論

李文卿

第一節 有限體的結構

所謂的有限體k是指非零元素皆具有乘法反元素的交換環; 它的特徵數 (characteristic) 是滿足

$$1+1+\cdots+1(n個)=0$$

的最小正整數n, 是個質數p。因此它包含$\mathbf{Z}/p\mathbf{Z}$做子體而可視爲佈於$\mathbf{Z}/p\mathbf{Z}$ 的有限維向量空間; 故k的元素個數$|k|$ $=$ q是質數p的冪次方p^d, 而指數d是k視爲佈於$\mathbf{Z}/p\mathbf{Z}$向量空間的維數, 這也表示: 把k看成加法群時, k是d個秩爲p之循環群的直和 (direct sum)。

其次考慮乘法群$k^\times = k-\{0\}$, 它的秩是$q-1$; 故$k^\times$中的每一元素都滿足

$$x^{q-1}=1,$$

即k^x中元素的秩都是$q-1$的因數。對任意$q-1$的正因數r, 設

$$\Omega(r)=\{x\in k^\times |\ x\text{ 的秩是 }r\}。$$

當r跑遍$q-1$的正因數時,$k^\times$可表爲$\Omega(r)$的不相交聯集, 現我們欲證明 $\Omega(q-1)\neq\phi$; 換句話說,

定理 1: $k^\times$是秩爲$q-1$的循環群。

想證明這定理, 首先觀察到底下的一般事實。

預備定理 1:任意係數在體F的n次多項式$f(x)$在F中至多有 n個相異零位。

證明:設α是$f(x)$在F中的一零位, 即$f(\alpha)=0$, 則

$$f(x)=f(x)-f(\alpha)=(x-\alpha)g(x),$$

其中$g(x)$是係數落在F的$n-1$次多項式, 若β是$f(x)$在F中另一異於 α 的零位, 則

$$0=f(\beta)=(\beta-\alpha)g(\beta),$$

但$\beta-\alpha\neq 0$, 故$g(\beta)=0$。利用數學歸納法, 若設$g(x)$在F中至多有$n-1$個相異零位時, 則推出$f(x)$在F中至多有n個相異零位。

由預備定理 1, 若$\Omega(r)\neq\phi$, 設y是$\Omega(r)$的元素, 則y生成一秩爲 r的循環子群, 是由方程式

$$x^r=1$$

在k中所有解組合而成, 又$\Omega(r)$正好是循環群$\langle y\rangle$的生成元 (generators) 所組成的集合,

即

$$\Omega(r) = \{y^i | 1 \le i \le r,\ \text{g.c.d.}(i, r) = 1\}。$$

這表$\Omega(r)$的元素個數是0或$\varphi(r)$; 其中$\varphi(n)$是 Euler φ–函數, 表示1到n之間與n互質的整數個數, 故得出

$$|k^\times| = q-1 = \sum_{r|(q-1)} |\Omega(r)| \le \sum_{r|(q-1)} \varphi(r)$$

其次, 我們需要另一事實。

預備定理2:對任意正整數$m, \sum_{r|m} \varphi(r) = m$。

假設預備定理2成立, 則由上面不等式可很快得到: 對任意$r|(q-1), |\Omega(r)| = \varphi(r)$。特別是$|\Omega(q-1)| = \varphi(q-1) \ge 1$, 而得證定理1。

現回來證明預備定理 2。 把集合$\{1, 2, \cdots, m\}$分割成

$$Y(r) = \{1 \le i \le m | \text{g.c.d.}(i, m) = \frac{m}{r}\}$$

的不相交聯集, 其中r跑遍m的所有正因數。對任意$i \in Y(r)$, 把i寫爲 $\frac{jm}{r}$, 則$1 \le j \le r$且

$$\text{g.c.d.}(i, m) = \text{g.c.d.}(\frac{jm}{r}, m) = \frac{m}{r}$$
$$\text{g.c.d.}(j, r) = \frac{m}{r}。$$

因而 g.c.d.$(j, r) = 1$。故$|Y(r)| = \varphi(r)$; 這證明了

$$m = \sum_{r|m} |Y(r)| = \sum_{r|m} \varphi(r)。$$

底下是能由上面論證馬上得出的一些推論。

推論1:設Ω_p是$\mathbf{Z}/p\mathbf{Z}$的一代數閉包 (algebraic closure), 則k是由方程 式$x^q - x = 0$在Ω_p中的所有解組合而成。

推論2:存在有元素$\xi \in k$, 使得$k = \mathbf{Z}/p\mathbf{Z}(\xi)$; 即$k$是質體$\mathbf{Z}/p\mathbf{Z}$的單擴張 (simple extension)。

推論3:對任意$|k^\times| = q - 1$的正因數r,$k^\times$中剛好有 $\varphi(r)$個秩爲r的元素。

推論4:給定任意正整數n, 在$\mathbf{Z}/p\mathbf{Z}$的代數閉包內, 存在有一唯一$\mathbf{Z}/p\mathbf{Z}$的n次擴充體。

證明:推論1 顯示:$\mathbf{Z}/p\mathbf{Z}$的n次擴充體要是存在的話, 一定是唯一; 即是由方程式

$$x^{p^n} = x$$

在代數閉包內的所有解組合而成。另一方面, 若α,β是方程式

$$x^{p^n} = x$$

的解, 則$\alpha - \beta$與$\alpha\beta^{-1}(\beta \ne 0$時) 也是方程的解, 故方程式的解確實形成一體, 而得證存在性。

推論5:給定任意正整數n, 則存在有一係數在$\mathbf{Z}/p\mathbf{Z}$的n次不可約 (irreducible) 多項式。

證明:設k是$\mathbf{Z}/p\mathbf{Z}$的n次擴充體, 則由推論2,

$$k = \mathbf{Z}/p\mathbf{Z}(\xi)。$$

設$f(x)$是ξ所滿足之$\mathbf{Z}/p\mathbf{Z}$係數不可約多項式。則

$$\begin{aligned} k &= \mathbf{Z}/p\mathbf{Z}(\xi) = \mathbf{Z}/p\mathbf{Z}[\xi] \\ &\cong \mathbf{Z}/p\mathbf{Z}[x]/(f(x)) \end{aligned}$$

故

$$\deg f = [k : \mathbf{Z}/p\mathbf{Z}] = n。$$

第二節 有限體的擴充

設k是一q個元素的有限體。k_n是k的n次擴充體。若k_m是介於 k與k_n之間之k的m次擴充體, 則k_n是佈於k_m的向量空間, 故 m可整除n。反之, 由推論1, 在k_n的代數閉包範圍內, 任意k的m次擴充體,$m|n$, 都是k_n的子體。

對體F的擴充體E, 以$\mathrm{Gal}(E/F)$表示固定F中每一元素之所有E的自同構 (automorphism) 所形成的群。考慮k_n中的函數$\sigma : x \longmapsto x^q$; 因

$$\begin{aligned} \sigma(x+y) &= (x+y)^q = x^q + y^q = \sigma(x) + \sigma(y), \\ \sigma(xy) &= (xy)^q = x^q y^q = \sigma(x)\sigma(y)。 \end{aligned}$$

故σ是k_n的自同態 (endomorphism)。更進一步, 若$\sigma(x) = x^q = 1$, 則 $x \neq 0$, 由這與

$$x^{q^n-1} = 1$$

得出$x = 1$, 原因是

$$\text{g.c.d. } (q, q^n - 1) = 1。$$

故σ是一對一。又k_n是有限體, 一對一必是映成; 故σ是k_n的自同構。最後$x \in k, \sigma(x) = x^q = x$, 這證明了$\sigma \in \mathrm{Gal}(k_n/k)$, 稱爲 Frobenius 自同構。設$\sigma$的秩是$r$, 則對任意$x \in k_n$,

$$\sigma^r(x) = x^{q^r} = x。$$

因$k^\times$是秩爲$q^n - 1$的循環群, 故$r = n$。因此$\mathrm{Gal}(k_n/k)$包含了秩是 n的循環群$\langle r \rangle$。另一方面, 每一$\mathrm{Gal}(E/F)$的自同構可視爲E上的F-線性轉換; 想決定$\mathrm{Gal}(k_n/k)$, 我們注意到下列事實:

預備定理3: $\mathrm{Gal}(E/F)$中的自同構是E-線性獨立的F-線性轉換。

證明:假設不然, 設

$$a_1\tau_1 + a_2\tau_2 + \ldots + a_r\tau_r = 0$$

是長度最短的線性關係式, 其中$a_1, a_2, \ldots, a_r \in E^\times$且 $\tau_1, \tau_2, \ldots, \tau_r \in \mathrm{Gal}(E/F)$; 則$r \geq 2$且 $\tau_1, \tau_2, \ldots, \tau_r$相異。設$y \in E$滿足$\tau_1(y) \neq \tau_2(y)$; 從 $\sum_{i=1}^{r} a_i\tau_i = 0$得出對每一$x \in k_n$,

$$\sum_{i=1}^{r} a_i\tau_i(yx) = \sum_{i=1}^{n} a_i\tau_i(y)\tau(x) = 0。$$

故

$$\sum_{i=1}^{r} a_i\tau_i(y)\tau_i = 0。$$

這產生了另一非顯然的關係式

$$\begin{aligned} &\sum_{i=1}^{r} a_i\tau_i(y)\tau_i - \tau_1(y)\sum_{i=1}^{r} a_i\tau_i \\ =\ &\sum_{i=2}^{r} a_i(\tau_i(y) - \tau_1(y))\tau_i \\ =\ &0。 \end{aligned}$$

這關係式比我們開始的關係式要短, 因而矛盾。

預備定理4:設E是體F的n次擴充體, 則$\mathrm{Gal}(E/F)$中至多有 n個相異的自同構。

證明:假設不然。設$m > n$且$\tau_1, \ldots, \tau_m$是$\mathrm{Gal}(E/F)$的相異自同構, 令$\{v_1, \ldots, v_n\}$是E佈於F的一組基底。設$(a_1, \ldots, a_m)$是 $n \times m$線性方程組

$$\begin{pmatrix} \tau_1(v_1) & \tau_2(v_2) & \cdots & \tau_m(v_1) \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ \tau_1(v_n) & \tau_2(v_n) & \cdots & \tau_m(v_n) \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} \doteq \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

的一組非零解。考慮$\sum_{i=1}^{m} a_i\tau_i$。由建構的過程,

$$\sum_{i=1}^{n} a_i\tau_i(v_j), \quad j = 1, \cdots, n$$

故對任意$x \in E, \sum_{i=1}^{m} a_i\tau_i(x) = 0$。換句話說, $\tau_1, \ldots, \tau_m$是E-線性相依, 但預備定理3告訴我們這不可能。

因此$|\mathrm{Gal}(k_n/k)| = |\langle\sigma\rangle| = n = [k_n, k]$。

這也是最大可能; 在這情況下, 我們稱k_n是k的 Galois 擴充。

定理2:設k_n是k的 Galois 擴充, 則$\mathrm{Gal}(k_n/k)$是由 Frobenius 自同構σ所生成的循環群, 其秩是 n。

注意到元素$x \in k_n$落在k的充要條件是x滿足方程式$x^q = x$。換句話說, 充要條件是被 Frobenius 自同構固定住, 或等同於被群$\mathrm{Gal}(k_n/k)$固定住。

利用$G = \mathrm{Gal}(k_n/k)$, 我們定義兩個從k_n到k的重要映象, 稱爲 trace 與 norm, 分別以$\mathrm{Tr}_{k_n/k}$與$\mathrm{N}_{k_n/k}$表示, 定義如下:

$$\mathrm{Tr}_{k_n/k} : x \longmapsto \sum_{\tau\in G} \tau(x) = \sum_{i=1}^{n} \sigma^i(x)$$
$$\mathrm{N}_{k_n/k} : x \longmapsto \prod_{\tau\in G} \tau(x) = \prod_{i=1}^{n} = \sigma(x)$$

從容易可驗證 trace 與 norm 的值域都落在k。顯然地,$\mathrm{Tr}_{k_n/k}$是加法群 k_n到加法群k的群同態, 又$\mathrm{N}_{k_n/k}$是乘法群$k_n^\times$到乘法群$k^\times$的群同態。底下我們考慮其值域。

定理3:(Hilbert 定理90) 從$k_n^\times$到$k^\times$的 norm 映象$\mathrm{N}_{k_n/k}$是映成函數, 其核$\ker \mathrm{N}_{k_n/k}$是

$$\ker \mathrm{N}_{k_n/k} = \{\frac{x}{\sigma(x)} | x \in k_n^\times\}。$$

證明:因

$$\begin{aligned} \mathrm{N}_{k_n/k}(\sigma(x)) &= \sum_{i=1}^{n} \sigma^{i+1}(x) = \sum_{i=1}^{n} \sigma^i(x) \\ &= N_{k_n/k}(x)。 \end{aligned}$$

故對所有 $x \in k_n^\times$,$x/\sigma(x)$ 落在 norm 映象$\mathrm{N}_{k_n/k}$的核。更進一步,

$$\frac{x}{\sigma(x)} = \frac{y}{\sigma(y)}$$

的充要條件是$xy^{-1} \in k^\times$, 因此集合

$$\{\frac{x}{\sigma(x)} | x \in k_n^\times\}$$

形成$k_n^\times$的乘法子群, 其秩是$(q^{n-1} - 1)/(q - 1)$。因而這集合是$\ker \mathrm{N}_{k_n/k}$全部的充要條件

是 norm 映象是映成函數。現證明$\mathrm{N}_{k_n/k}$是映成。觀察到對任意$x \in k_n^\times$

$$\begin{aligned} & \mathrm{N}_{k_n/k}(x) \\ = & \sum_{i=1}^{n} \sigma^i(x) = x \cdot x^q \cdot x^{q^2} \cdots x^{q^{n-1}} \\ = & x^{1+q+q^2+\cdots+q^{n-1}} = x^\alpha (\alpha = \frac{q^n-1}{q-1}) \end{aligned}$$

故對任意 $k_n^\times$ 的生成元 x,$\mathrm{N}_{k_n/k}(x)$ 的秩是 $q-1$, 這證明了 $\mathrm{N}_{k_n/k}(x)$是映成。

定理4: (Hilbert 定理90) 從k_n到k的 trace 映象 $\mathrm{Tr}_{k_n/k}$是映成函數, 而其核是

$$\ker(\mathrm{Tr}_{k_n/k}) = \{x - \sigma(x) | x \in k_n\}。$$

證明:任意$\mathrm{Gal}(k_n/k)$的元素都是k-線性映象, $\mathrm{Tr}_{k_n/k}$的值域是佈於k的向量空間, 故$\mathrm{Tr}_{k_n/k}(k_n) = 0$ 或k。若$\mathrm{Tr}_{k_n/k}(k_n) = 0$, 則 $\sum_{i=1}^{n} \sigma^i = 0$, 這是$\mathrm{Gal}(k_n/k)$中元素的一非顯然線性關係, 但由預備定理3, 這不可能發生; 因而$\mathrm{Tr}_{k_n/k}$是映成函數, 其核有 q^{n-1}個元素。顯然地

$$\mathrm{Tr}_{k_n/k}(\sigma(x)) = \mathrm{Tr}_{k_n/k}(x)。$$

故對所有$x \in k_n$,$x - \sigma(x)$落在核中。更進一步, $x - \sigma(x) = y - \sigma(y)$的充要條件是$x - y \in k$; 故群的秩是$q^n/q$; 因而等於核的全部。

注意事項: 爲norm 與 trace 的 Hilbert 定理90, 一般是利用 Galois的 first cohomology 證明 (à la Noether); 但當基底的體是有限體時, 我們可使用上面的計數法。

習題 1: 設k是有限體,k_m,k_{mn}分別是k的m次與mn次擴 充體, 證明

$$\mathrm{Tr}_{k_{mn}/k} = \mathrm{Tr}_{k_m/k} \circ \mathrm{Tr}_{k_{mn}/k_n}$$
且 $$\mathrm{N}_{k_{mn}/k} = \mathrm{N}_{k_m/k} \circ \mathrm{N}_{k_{mn}/k}。$$

給定$z \in k_n$, 它定義了k_n上的一線性轉換

$$\mathrm{L}_z : x \longmapsto zx。$$

即乘上z。選定k_n的一組基底, 把L_z表成n階方陣; 這方陣的 trace 與行列式值就稱爲L_z的 trace 與行列式。這兩者也就是$\mathrm{Tr}_{k_n/k}(z)$與 $\mathrm{N}_{k_n/k}(z)$。說得更精確一個, 我們有底下的定理。

定理5:設$z \in k_n$, 線性轉換L_z如上所定, 則

(1) $\mathrm{Tr}\,\mathrm{L}_z = \mathrm{Tr}_{k_n/k}(z)$且 $\det \mathrm{L}_z = \mathrm{N}_{k_n/k}(z)$

(2) 若$k(z) = k_n$且$f(x) = x^n + a_1 x_{n-1} + \ldots + a_n$是$z$所滿足的佈於$k$的不可約多項式, 則

$$a_1 = -\mathrm{Tr}_{k_n/k}(z)$$
且 $$a_n = (-1)^n \mathrm{N}_{k_n/k}(z)。$$

證明:在(2) 的$k(z) = k_n$假設下, 我們將證明 (1) 與 (2)。在 (1) 中, 當 $k(z)$是k_n的眞子體時的情形留做習題。對任意$\tau \in \mathrm{Gal}(k_n/k)$,

$$0 = \tau(f(z)) = f(\tau(z)),$$

故$\tau(z)$也是$f(x)$的根。更進一步, 若τ與τ'是

$\mathrm{Gal}(k_n/k)$的相異元素, 則$\tau(z) \neq \tau'(z)$ (否則它們在$k(z) = k_n$上相同)。這證明了z在$\mathrm{Gal}(k_n/k)$的作用下有n個相異值, 構成了$f(x)$的所有根。因此由根與係數的關係得出

$$-a_1 = f(x) = 0 \text{ 的根的總和 } = \mathrm{Tr}_{k_n/k}(z)$$

且

$$(-1)^n a_n = f(x) = 0 \text{ 的根的乘積 } = \mathrm{N}_{k_n/k}(z)。$$

這證明了 (2), 對於 (1), 我們知道L_z滿足$f(x) = 0$, 又$f(x)$在 k中不可約且$[k_n : k] = n$,$f(x)$其實是L_z的特徵多項式,L_z 的伴隨矩陣是

$$\begin{bmatrix} 0 & & & & -a_n \\ 1 & 0 & & & -a_{n-1} \\ & 1 & & & \vdots \\ & & \ddots & & \vdots \\ & & & 0 & \vdots \\ & & & 1 & -a_1 \end{bmatrix}$$

故trace $= -a_1$且行列式$= (-1)^n a_n$, 這證明了 (2)。

習題 2:設$z \in k_n$, 若$k(z) = k_m$是k_n的眞子體時, 證明

$$\mathrm{Tr}\,\mathrm{L}_z = \mathrm{Tr}_{k_n/k}(z) = \frac{n}{m}\mathrm{Tr}_{k_n/k}(z),$$

且

$$\det \mathrm{L}_z = \mathrm{N}_{k_n/k}(z) = \mathrm{N}_{k_m/k}(z)^{n/m}。$$

習題 3:

(1) (Normal Basis 定理) 存在有元素$z \in k_n$, 使得$\{\tau(z)|\tau \in \mathrm{Gal}(k_n/k)\}$是$k_n$佈於$k$的基底。(提示: 考慮 Frobenius 自同構σ的最小多項式)

(2)對 (1) 中的 z, 則有 $\mathrm{Tr}_{k_n/k}(z) \neq 0$ (提示: 把 k_n 中的元素 表成 $\{\tau(z)|\tau \in \mathrm{Gal}(k_n/k)\}$的$k$-線性組合, 然後證明 $\mathrm{Tr}_{k_n/k}(k_n) = k\,\mathrm{Tr}_{k_n/k}(z)$)。

第三節 群的特徵

所謂拓樸群G的特徵(character) 是指G到複數平面上單位圓S^1的連續性同態 (continuous homomorphism)。若G是一有限群, 則群內賦有離散拓樸, 故特徵即是G到S^1的群同態。因S^1是可交換群, 故群的特徵其實是定義在G除以其交換子 (commutator) 所形成子群的商群上。把所有G的元素都送到 1的特徵稱爲G 的明顯特徵(trivial character), 以χ_0表之。

所有G的特徵, 在點態乘法下, 即

$$\chi_1\chi_2(x) = \chi_1(x)\chi_2(x),$$

形成一乘法交換群, 稱爲G的對偶群(dual group), 而以$\widehat{G}$ 表之。

例題1:設G是一有限循環群, 計算其對偶群$\widehat{G}$。

解答:設G的秩是n,g是G的生成元,ζ是 1的n次原始根。$\eta : G \longmapsto S^1$定成

$$\eta(g) = \zeta;$$

則η是G到S^1的同態且其秩是n, 故$\widehat{G}$包含循環群 $\langle\eta\rangle$。另一方面, 任一G上的特徵χ是由它在g的取值所決定。故 $\chi(g) = \zeta^k$,$k \in \mathbf{Z}$;

而這表示$\chi = \eta^k$。故$\widehat{G} = \langle\eta\rangle$是一秩爲$n$的循環群, 因而 $\widehat{G} \cong G$。

命題 1: 若G是一有限交換群, 則G與其對偶群$\widehat{G}$同構。

證明:由有限交換群的基本定理(Fundamental Theorem of finite abelian groups), 我們可以把G表成循環群的直積:

$$G = G_1 \times \ldots \times G_r。$$

對任意G上的特徵χ, 以χ_i表示χ在G_i的限制值, 則χ 是$\chi_1, \ldots, \chi_r$的乘積$\chi_1 \cdots \chi_r$且 $\widehat{G} = \widehat{G}_1 \times \ldots \times \widehat{G}_r$。但上面例題1告訴我們$\widehat{G}_i$與$G_i$同構, 故$\widehat{G}$與$G$同構。

注意事項:上面的同構$G \cong \widehat{G}$並非標準的, 因其取決於分解的形式與每一循環子群, 即這同構取決於生成元的選擇。然而,$\widehat{G}$的對偶群$\widehat{\widehat{G}}$很自然地與G同構。底下是一種不退化的配對。

$$\xi : G \times \widehat{G} \longrightarrow S^1$$

定義

$$\xi(g, \chi) = \chi(g)$$

(當固定其中一變數時,ξ是另一變數的群同態)。

習題 4:

(1) 證明上面所定義的ξ是不退化的, 即證明

(i) 若g不是G的單位元素, 則存在有一G的特徵χ, 使得 $\chi(g) \neq 1$。

(ii) 若χ不是G的顯然特徵χ_0, 則存在有一G的元素g, 使得 $\chi(g) \neq 1$。

(2) 證明ξ的不退化是G與$\widehat{\widehat{G}}$自然同構的充分條件。

對拓樸群 G 的封閉子群 (closed subgroup) H, 定

$$H^\perp = \{\chi \in \widehat{G} | \chi(H) = \{1\}\}$$

當G是交換子群時,$H^\perp$可簡化看成$\widehat{G/H}$。

定理6(Pontrjagin 對偶): 設G是一可交換拓樸群, 則對應

$$H \longmapsto H^\perp$$

建立了G的封閉子群與$\widehat{G}$封閉子群間的一一對應。更進一步, $(H^\perp)^\perp$自然地與H同構。

這裏, 我們只考慮這定理在G是有限交換群的特殊情形, 則拓樸沒扮演任何角色。再次利用有限交換群的基本定理, 我們可假設G是秩爲n的循環群;G的子群H可用n的因數d當指標, 使得H的秩$= d$。則$\widehat{G}$是秩爲n的循環群且$H^\perp$的秩爲 $\frac{n}{d}$。現$H \longmapsto H^\perp$的一一對應非常明顯。在 $\widehat{\widehat{G}} \cong G$的標準同構中, 我們可以把$(H^\perp)^\perp$看成子群

$$\widetilde{H} = \{g \in G | \text{對所有 } \chi \in H^\perp,\ \chi(g) = 1\}。$$

因對每一$\chi \in H^\perp$,χ在H的取值顯然都是1, 故群$\widetilde{H}$包含H。另一方面,$|\widetilde{H}| = |\widehat{G}|/|H^\perp|$ 且$|H^\perp| = |G|/|H|$, 得出 $|\widetilde{H}| = |H|$; 故$\widetilde{H} = H$, 即$(H^\perp)^\perp$ 自然與H同構。

設$\mathbf{C}[G]$是定義在有限交換群G上的所有複值函數。定義$\mathbf{C}[G]$上的內積 $\langle\cdot,\cdot\rangle$爲

$$\langle f, g\rangle = \frac{1}{|G|} \sum_{x \in G} f(x)\overline{g(x)}。$$

命題2: 設G是一有限交換群, 則G的特徵形成 $\mathbf{C}[G]$ 的一組垂直單一基底。

爲證明這命題, 我們需要下列。

預備定理5: 設G是一有限交換群,$g \in G$且$\chi \in \widehat{G}$, 則

(1) $\sum_{\chi\in G}\chi(x) = \begin{cases} 0 & \text{若 } \chi \neq \chi_0, \\ |G| & \text{若 } \chi = \chi_0。\end{cases}$

(2) $\sum_{\eta\in\widehat{G}}\eta(g) = \begin{cases} 0 & \text{若 } g \neq e, \\ |G| & \text{若 } g = e。\end{cases}$

其中e是G的單位元素。

證明:(1) 若$\chi = \chi_0$, 很明顯成立。設$\chi \neq \chi_0$且 $y \in G$使得 $\chi(y) \neq 1$, 由

$$\begin{aligned}\sum_{\chi\in G}\chi(x) &= \sum_{\chi\in G}\chi(xy) = \sum_{\chi\in G}\chi(x)\chi(y) \\ &= \chi(y)\sum_{\chi\in G}\chi(x)\end{aligned}$$

以及$\chi(y) \neq 1$, 馬上得出$\sum_{\chi\in G}\chi(x) = 0$。

(2) 由 (1) 以及同構$G \cong \widehat{\widehat{G}}$得出。

現回到命題2的證明上。設χ_1,$\chi_2 \in \widehat{G}$, 則由預備定理5得出

$$\begin{aligned}\langle\chi_1,\chi_2\rangle &= \frac{1}{|G|}\sum_{x\in G}\chi_1(x)\overline{\chi_2(x)} \\ &= \frac{1}{|G|}\sum_{x\in G}(\chi_1\chi_2^{-1})(x) \\ &= \begin{cases}1 & \text{若 } \chi_1 = \chi_2, \\ 0 & \text{若 } \chi_1 \neq \chi_2。\end{cases}\end{aligned}$$

這證明了G的所有特徵形成一組垂直單一集, 故彼此之間線性獨立, 另一方面,

$$|\widetilde{G}| = |G| = \dim_{\mathbf{C}}\mathbf{C}[G],$$

故G所有特徵形成一組$\mathbf{C}[G]$的垂直單一基底。

第四節 有限體的特徵與 Gauss 和

設k是一q個元素的有限體, 如我們在第一節所見, 加法群k是d個秩爲p之循環群的直和, 故$q = p^d$。因而k的加法特徵所形成的對偶群$\widehat{k}$與k有相同結構。

例題1 $\widehat{\mathbf{Z}/p\mathbf{Z}} = \langle\psi\rangle$, 其中$\psi : \mathbf{Z}/p\mathbf{Z} \longmapsto S^1$定義爲

$$\psi(x) = e^{2\pi ix/p}。$$

我們已知道$\mathrm{Tr}_{k/\mathbf{Z}/p\mathbf{Z}} : k \longmapsto \mathbf{Z}/p\mathbf{Z}$是加法群同態, 故對每一$\varphi \in \widehat{\mathbf{Z}/p\mathbf{Z}}$ $\varphi \circ \mathrm{Tr}_{k/\mathbf{Z}/p\mathbf{Z}}$是$k$上的加法特徵。因 trace 是映成, 故對任一 $\mathbf{Z}/p\mathbf{Z}$的非顯然特徵與 trace 合成後會得出k的非顯然特徵。

命題3:設ψ是有限體k上的非顯然加法特徵 。對任意$a \in k$, 定義$\psi^a : k \longmapsto S^1$爲$\psi^a(x) = \psi(ax)$; 則$\psi^a$是$k$的加法特徵, 且$a \longmapsto \psi^a$建立了$k$到$\widehat{k}$的同構, 特別是

$$\widehat{k} = \{\psi^a | a \in k\}$$

且對所有$x \in k$,

$$\overline{\psi(x)} = \psi(x)^{-1} = \psi(-x) = \psi^{-1}(x)。$$

證明:以L_a表示, 表示乘上a之k上的線性轉換, 則 $\psi^a = \psi \circ L_a$。若$a = 0$, 則$L_a = 0$, 且ψ°是k上的顯然特徵。若 $a \neq 0$,L_a是乘法群$k^\times$的自同構, 故ψ^a是非顯然特徵, 對$a, b \in$

k,$\psi^{a+b}=\psi^a\psi^b$, 故$a\longmapsto\psi^a$是k到$\widehat{k}$的一對一同態; 因$|\widehat{k}|=|k|$, 故這同態也是映成。

例題2:以Ψ表示特徵$\psi\circ\mathrm{Tr}_{k/\mathbf{Z}/p\mathbf{Z}}$, 則由命題3得

$$\widehat{k}=\{\Psi^a|a\in k\}。$$

乘法群$k^\times$的對偶群$\widehat{k^\times}$是秩爲$q-1$的循環群。$k^\times$ 的特徵可視爲k上的函數, 而在0的取值定爲

$$\chi(0)=\begin{cases}0 & 若\ \chi\neq\chi_0,\\ 1 & 若\ \chi=\chi_0。\end{cases}$$

則$\chi\in\mathbf{C}[k]$; 因而由命題2, χ可寫成k之加法特徵的線性組合, 係數稱爲單一化的 Gauss 和 (normalized Gauss sum)。說得更精確一點, 對任意 $\chi\neq\chi_0$, 則有

$$\begin{aligned}(1)\ \chi&=\sum_{\psi\in\widehat{k}}\langle\chi,\overline{\psi}\rangle\overline{\psi}\\ &=\sum_{\psi\in\widehat{k},\psi\neq\psi_0}\langle\chi,\overline{\psi}\rangle\overline{\psi}\\ &=\tfrac{1}{|k|}\sum_{\psi\in\widehat{k},\psi\neq\psi_0}g(\chi,\psi)\overline{\psi},\end{aligned}$$

其中ψ_0是顯然加法特徵,$g(\chi,\psi)$稱爲χ對ψ的 Gauss 和。而

(2) $g(\chi,\psi)=|k|\langle\chi,\overline{\psi}\rangle=\sum_{x\in k}\chi(x)\psi(x)=\sum_{x\in k^\times}\chi(x)\psi(x)$。

(1) 可以看成χ對加法特徵的 Fourier 展開式, 而 Gauss 和是 Fourier 係數。

命題4:設$\chi\in\widehat{k^\times}$且$\psi\in\widehat{k}$是非顯然特徵, 則

(1) $g(\chi,\psi)g(\overline{\chi},\psi)=|k|\chi(-1)=q\chi(-1)$。

(2) $\overline{g(\chi,\psi)}=\chi(-1)(\overline{\chi},\psi)$, 故$g(\chi,\psi)$的絕對值是 $\sqrt{q}$。

證明:(1) 從定義得出

$$\begin{aligned}&g(\chi,\psi)g(\overline{\chi},\psi)\\ &=\sum_{x\in k^\times}\chi(x)\psi(x)\sum_{y\in k^\times}\overline{\chi(y)}\psi(y)\\ &=\sum_{x\in k^\times}\chi(x)\psi(x)\sum_{z\in k^\times}\overline{\chi}(xz)\psi(xz)\ (y=xz)\\ &=\sum_{z\in k^\times}\overline{\chi}(z)\sum_{x\in k^\times}\psi((1+z)x)\\ &=\sum_{z\in k^\times}\overline{\chi}(z)\left[\sum_{x\in k}\psi((1+z)x)-\psi(0)\right]\\ &=\sum_{z\in k^\times}\overline{\chi}(z)\left[\sum_{x\in k}\psi^{1+z}(x)-1\right)\\ &=\sum_{z\in k^\times}\overline{\chi}(z)\sum_{x\in k}\psi^{1+z}(x)\end{aligned}$$

因對$\chi=\chi_0$, $\sum_{z\in k^x}\overline{\chi}(z)=0$。應用預備定理5到$G=k$, 得出

$$\begin{aligned}&\sum_{x\in k}\psi^{1+z}(x)\\ &=\begin{cases}0 & 若\ \psi^{1+z}\neq\psi^0,\ 即\ 1+z\neq0\\ q & 若\ \psi^{1+z}=\psi^0,\ 即\ 1+z=0\end{cases}\end{aligned}$$

因此$g(\chi,\psi)g(\overline{\chi},\psi)=g(-1)$。得所欲證。

(2) 這是因爲

$$\begin{aligned}&\overline{g(\chi,\psi)}=\sum_{x\in k^x}\overline{\chi}(x)\overline{\psi(x)}\\ &=\sum_{x\in k^x}\overline{\chi}(x)\psi(-x)=\chi(-1)\sum_{x\in k^x}\overline{\chi}(x)\psi(x)\\ &=\chi(-1)g(\overline{\chi},\psi)。\end{aligned}$$

一般想計算$g(\chi,\psi)/\sqrt{q}$的值是一非常困難的問題。

習題5: 設 N 是正整數, 所謂 $\mathbf{Z}$ 上 $\bmod N$ 的特徵是指 $\mathbf{Z}/N\mathbf{Z}$ 中可逆元素 $(\mathbf{Z}/N\mathbf{Z})^\times$ 上的特徵。若 χ 是 $(\mathbf{Z}/N\mathbf{Z})^\times$

的原始特徵 (primitive character)(即不能找到 N 的眞因數 m, 使得 g.c.d$(n,m)=1$, g.c.d$(n',m)=1, n\equiv n'(\mathrm{mod}\, m) \Longrightarrow \chi(n)=\chi(n')$) 則稱$N$是$\chi$的 conductor。設$\psi_N$是$\mathbf{Z}/N\mathbf{Z}$的加法特徵, 定爲 $\psi_N(x)=e^{2\pi ix/N}$

(1)設χ是$\mathbf{Z}$上mod N的 特 徵,conductor是N, 證明 Gauss和

$$g(\chi,\psi_N)=\sum_{\chi(\mathrm{mod}\, N),(\chi,N)=1}\chi(x)\psi_N(x)$$

的絕對值是$\sqrt{N}$。

(2)設χ_1,χ_2是$\mathbf{Z}$上分別mod N_1,N_2 的特徵,χ_i的 conductor 是$N_i, i=1,2$。假設N_1與N_2互質, 則

$$(\mathbf{Z}/N_1N_2\mathbf{Z})^\times \simeq (\mathbf{Z}/N_1\mathbf{Z})^\times\times(\mathbf{Z}/N_2\mathbf{Z})^\times$$

以 $\chi_1\chi_2$ 表示 $\mathbf{Z}$ 上 mod N_1N_2 的特徵, 它限制到 $(\mathbf{Z}/N_1\mathbf{Z})^\times$ 等於 χ_i; 找出 $g(\chi_1\chi_2, \psi_{N_1N_2})$與 $g(\chi_1,\psi_{N_1})$,$g(\chi_2,\psi_{N_2})$ 之間的關係式。

Gauss和$g(\chi,\psi)$視爲χ與ψ的函數時, 隨ψ的變化非常簡單。事實上, 固定 k上的任一非顯然特徵ψ, 則其他的非顯然特徵皆可表爲ψ^t,$t\in k^\times$, 則有

$$\begin{aligned} g(\chi,\psi^t) &= \sum_{x\in k^\times}\chi(x)\psi^t(x) \\ &= \sum_{x\in k^\times}\chi(x)\psi(tx) = \chi(t)^{-1}\sum_{x\in k^\times}\chi(tx)\psi(tx) \\ &= \chi(t)^{-1}g(\chi,\psi)。 \end{aligned} \tag{3}$$

因此, 式子 (1) 可寫爲

$$\begin{aligned} \chi &= \frac{1}{|k|}\sum_{t\in k^\times} g(\chi,\psi^t)\overline{\psi^t} \\ &= \frac{1}{|k|}g(\chi,\psi)\sum_{t\in k^\times}\chi(t)^{-1}\overline{\psi^t}。 \end{aligned} \tag{4}$$

把$g(\chi,\psi)$看成χ的函數, 則比較複雜。若 χ_1,χ_2與$\chi_1\chi_2$ 都非顯然特徵, 則可證明

$$\begin{aligned} &\frac{g(\chi_1,\psi)g(\chi_2,\psi)}{g(\chi_1\chi_2,\psi)} = \sum_{s,t\in k, s+t=1}\chi_1(s)\chi_2(t) \\ &= \chi_1\chi_2(-1)\sum_{s,t\in k, s+t+1=0}\chi_1(s)\chi_2(t)。 \end{aligned}$$

注意到右邊的式子與ψ無關。左式稱爲附著在χ_1與χ_2 的 Jacobi 和。Jacobi 和可擴充爲r個。設$\chi_1,\ldots,\chi_r$ 是$k^\times$上的非顯然特徵, 則附著在$\chi_1,\ldots,\chi_r$ 的 Jacobi 和定義爲

$$\begin{aligned} &j(\chi_1,\ldots,\chi_r) \\ &= \sum_{\substack{v_1,\ldots,v_r\in k^\times \\ v_1+\ldots+v_r+1=0}}\chi_1(v_1)\ldots\chi_r(v_r) \\ &= (q-1)^{-1}\sum_{\substack{u_0,\ldots u_r\in k^\times \\ u_0+u_1+\ldots+u_r=0}}\chi(u_0)\chi_1(u_1)\ldots\chi_r(u_r)。 \end{aligned}$$

其中$\chi=(\chi_1\ldots\chi_r)^{-1}$。

我們需要

命題5:設$\chi,\chi_1,\ldots,\chi_r$是$k^\times$上的非顯然特徵, 滿足$\chi\chi_1\ldots\chi_r = 1$。則對$k$上的任一非顯然特徵 ψ,

$$\begin{aligned} &j(\chi_1,\ldots,\chi_r) \\ &= \frac{1}{q}g(\chi,\psi)g(\chi_1,\psi)\ldots g(\chi_r,\psi)。 \end{aligned}$$

特別是$j(\chi_1,\ldots,\chi_r)$的絕對值是$q^{\frac{r-1}{2}}$。

證明:固定k的一非顯然特徵ψ, 像 (4), 把χ_i表爲 ψ^t的線性組合:

$$\chi_i = \frac{1}{q} g(\chi_i, \psi) \sum_{t \in k^x} \overline{\chi}_i(t) \overline{\psi^t}。$$

代入$j(X_1, \ldots, X_r)$的定義中得出

$$\begin{aligned} & (q-1) j(\chi_1, \ldots, \chi_r) \\ = \; & q^{-r-1} g(\chi, \psi) g(\chi_1, \psi) \ldots g(\chi_r, \psi) \\ & \cdot \sum_{u_i \in k, \Sigma u_i = 0} \sum_{t_i \in k^\times} \overline{x}(t_0) \overline{x}(t_1) \ldots \overline{x}(t_r) \\ & \cdot \overline{\psi}(t_0 u_0 + t_1 u_1 + \ldots + t_r u_r) \end{aligned}$$

但對固定的$t_0, t_1, \ldots, t_r$,

$$\begin{aligned} & \sum_{u_i \in k, \Sigma u_i = 0} \overline{\psi}(t_0 u_0 + \ldots + t_r u_r) \\ = & \sum_{u_i \in k, \Sigma u_i = 0} \overline{\psi}(t_0(u_0 + \ldots + u_r) + u_1(t_1 - t_0) \\ & + \ldots + u_r(t_r - t_0)) \\ = & \sum_{u_1, \ldots, u_r \in k} \overline{\psi}(u_1(t_1 - t_0) + \ldots + u_r(t_r - t_0)) \\ = & \begin{cases} q^r & \text{若 } t_0 = t_1 = \ldots = t_r \\ \\ 0 & \text{其他} \end{cases} \end{aligned}$$

因此

$$\begin{aligned} & (q-1) j(\chi_1, \ldots, \chi_r) \\ = \; & \frac{1}{q} g(\chi, \psi) g(\chi_1, \psi) \ldots g(\chi_r, \psi) \\ & \sum_{t_0 \in k^x} \overline{\chi}\, \overline{\chi}_1 \ldots \overline{\chi}_r(t_0) \\ = \; & \frac{q-1}{q} g(\chi, \psi) g(\chi_1, \psi) \ldots g(\chi_r, \psi) \end{aligned}$$

原因是$\chi \chi_1 \ldots \chi_r = \chi_0$, 這證明了命題。

第五節 Davenport-Hasse 恆等式

如第四節, 以k表示一q個元素的有限體,χ是$k^\times$ 上的非顯然 (乘法) 特徵, 而ψ是k上的非顯然加法特徵。對任意固定的整數ν, 以k_ν表示k的ν次擴充體。Trace 映象$\mathrm{Tr}\, k_v/k$與 Norm 映象$\mathrm{N}_{k_u/k}$如第二節所定, 分別對於體的加法群與乘法群, 它們是映成函數, 利用合成得出

$$\mathbf{X} = \chi \circ N_{k_\nu/k} \text{ 與 } \Psi = \psi \circ \mathrm{Tr}_{k_\nu/k}$$

分別是$k_\nu^\times$與k_ν的非顯然特徵, 兩個 Gauss 和

$$\begin{aligned} g(\chi, \psi) &= \sum_{y \in k^x} \chi(y) \psi(y) \\ g(\mathbf{X}, \Psi) &= \sum_{y \in k^x} \mathbf{X}(y) \Psi(y) \end{aligned}$$

的關係如下:

定理6 (Davenport-Hasse) —$g(\mathbf{X}, \Psi) = [-g(\chi, \psi)]^\nu$。

底下的證明是 A. Weil 所提出。對任意首一多項式 (monic polynomial)

$$f(x) = x^n + a_{n-1} x^{n-1} + \ldots + a_0,\ a_i \in k$$

其中常數項$a_0 = f(0) \neq 0$, 定義

$$\lambda(f) = \chi(a_0) \psi(a_{n-1})$$

很容易可看出: 若f_1與f_2是兩個這類的多項式, 則

$$\lambda(f_1 f_2) = \lambda(f_1) \lambda(f_2)$$

因常數項不爲零的首一多項式是常數項不爲零的首一不可約多項式的乘積, 故有

$$\sum_{f \in S} \lambda(f) u^{\deg f} = \sum_{p \in T} (1 - \lambda(p) u^{\deg p})^{-1}$$

其中

$S = \{f(x) \in k[x] |$ $f(x)$是首一多項式且$f(0) \neq 0\}$,

$T = \{p(x) \in k[x] |$ 是首一不可約多項式且$p(0) \neq 0\}$。

首先我們計算左邊的和。考慮$k[x]$中的d次多項式且其係數$a_{d-2}, \ldots, a_0 \neq 0$固定住。$x^{d-1}$的係數$a_{d-1}$可以是$k$的任意元素, 故和中的 $\lambda(f)$對所有這樣的f求和是0; 故對$d \geq 2$,u^d的係數是0,u^0的係數是1。且左邊之一次首一多項式是$x+a$,$a \in k^\times$的形式。故u的係數是

$$\sum_{a \in k^x} \lambda(x+a) = \sum_{a \in k^x} \chi(a)\psi(a) = g(\chi, \psi)。$$

我們已證明

$$1 + g(x, \psi)u = \prod_{p \in T} (1 - \lambda(p)u^{\deg p})^{-1} \quad (5)$$

同樣, 對多項式$F(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in k_\nu(x)$,$a_0 \neq 0$定義

$$\wedge(F) = \mathbf{X}(a_{n-1})\Psi(a_0)$$

則有

$$1 + g(\mathbf{X}, \Psi)U = \prod_{p(x) \in \widetilde{T}} (1 - \wedge(P)U^{\deg P})^{-1},$$

$\widetilde{T} = \{P(x) \in k_\nu[x] | P(x)$是首一不可約多項式且$P(0) \neq 0\}$。 (6)

其次我們考慮 (5) 與 (6) 的無窮乘積。設 $p(x)$ 是 $k[x]$ 中的首一不可約多項式, 且設 $P(x)$ 是$k_\nu[x]$ 中整除 $p(x)$ 的首一不可約多項式。則對任意 $\tau \in \mathrm{Gal}(k_\nu/k)$,$\tau(P(x))$可整除 $\tau(p(x)) = p(x)$, 而且 $\tau(P(x))$ 也是 $k_\nu[x]$ 中的首一不可約多項式。若 $\tau_1(P(x)), \ldots, \tau_r(P(x))$ 是 $P(x)$ 在 $\mathrm{Gal}(k_\nu/k)$ 作用下的不同影像。則它們是$p(x)$在$k_\nu[x]$中的相異不可約因式, 而乘積

$$q(x) = \tau_1(p(x)) \ldots \tau_\nu(p(x))$$

可除盡$p(x)$且是$\mathrm{Gal}(k_\nu/k)$作用下的不變量, 故$q(x) \in k[x]$。因$p(x)$ 不可約且$p(x)$與$q(x)$都是首一多項式, 故得出$p(x) = q(x)$, 即

$$p(x) = \tau_1(P(x)) \ldots \tau(P(x)),$$

是$p(x)$在$\mathrm{Gal}(k_\nu/k)$作用下之共軛多項式的乘積。這證明了每一$k[x]$中的首一不可約多項式在$k_\nu[x]$中可分解成相異不可約多項式, 這些多項式在 $\mathrm{Gal}(k\nu/k)$作用下互爲共軛, 且每一$k_\nu[x]$的首一不可約多項式可唯一整除一$k[x]$中的首一不可約項式, 故我們可寫爲

$$1 + g(X, \Psi)U = \prod_{P \in T} \prod_{P|p, P \in \widetilde{T}} (1 - \wedge(P)U^{\deg P})^{-1}$$

其次固定一個$k[x]$中的首一不可約多項式$p(x)$,$\deg p(x) = n$且 $p(0) \neq 0$。 設$P(x)$是$k_\nu[x]$中$p(x)$的首一不可約因式, 我們要探討 $\lambda(p)$與$\wedge(P)$之間的關係。設$-\xi$是$P(x)$在k_ν之代數閉包 $\overline{k}_\nu$的一個根, 則$p(x)$是$-\xi$在$k[x]$中的不可約多項式且$p(x)$是$-\xi$在$k_\nu[x]$中的不可約多項式, 因而

$[k(\xi) : k] = n$ 且 $[k_\nu(\xi) : k_\nu] = \deg P(x)$。

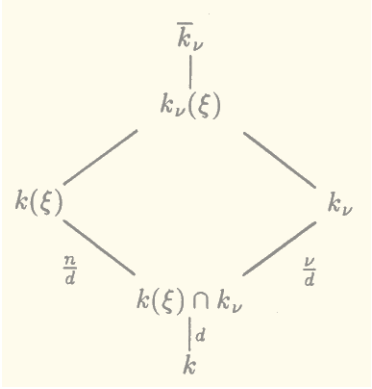
設交集$k(\xi)\cap k_\nu$是k的d次擴充。因爲在$\overline{k}_\nu$中, 對任意次數只有一k的擴充體是這次數, 故得出

$$d=\text{g.c.d.}(n,\nu),(\frac{n}{d}\text{與}\frac{\nu}{d}\text{互質})。$$

因此

$$\begin{aligned}[k_\nu(\xi):k_\nu] &= [k(\xi):k(\xi)\cap k_\mu]=\frac{n}{d}\\ &= \deg P(x)。\end{aligned}$$

且$p(x)$在$k_\nu[x]$中有d個相異不可約因式



把$P(x)$與$p(x)$分別寫成

$$\begin{aligned}p(x) &= x^{n-1}+bx^{x-1}+\ldots+a\\ \text{且 } P(x) &= x^{n/d}+Bd^{(n/d)-1}+\ldots+A\end{aligned}$$

由定理5, 則有

$$\begin{aligned}&b=-\text{Tr}_{k(\xi)/k}(-\xi)=\text{Tr}_{k(\xi)/k}(\xi),\\ &a=(-1)^n\text{N}_{k(\xi)/k}(-\xi)=\text{N}_{k(\xi)/k}(\xi)\\ &B=-\text{Tr}_{k_\nu(\xi)/k_\nu}(-\xi)=\text{Tr}_{k_\nu(\xi)/k_\nu}(\xi)\text{且}\\ &A=(-1)^{n/d}\text{N}_{k_\nu(\xi)/k_\nu}(-\xi)=\text{N}_{k_\nu(\xi)/k_\nu}(\xi)\end{aligned}$$

因此

$$\begin{aligned}\lambda(p) &= \chi(a)\psi(a)\\ &= \chi(\text{N}_{k(\xi)/k}(\xi))\psi(\text{Tr}_{k(\xi)/k}(\xi))\end{aligned}$$

且

$$\begin{aligned}\wedge(P) &= \mathbf{X}(A)\Psi(B)\\ &= \chi(\text{N}_{k_\nu/k}(A))\psi(\text{Tr}_{k_\nu/k}(B))\\ &= \chi(\text{N}_{k_\nu(\xi)/k}(\xi))\psi(\text{Tr}_{k_n u(\xi)/k}(\xi))\\ &= \chi(\text{N}_{k(\xi)/k}(\xi))^{\nu/d}\psi(\text{Tr}_{k(\xi)/k}(\xi))^{\nu/d}\\ &= \lambda(p)^{\nu/d}\end{aligned}$$

故

$$\begin{aligned}&\prod_{P|p,P\in\widetilde{T}}(1-\wedge(P)U^{\deg U})^{-1}\\ =\ &(1-\lambda(p)^{\nu/d}U^{n/d})^{-d}\end{aligned}$$

把U換成u^ν, 則有

$$\begin{aligned}[1-\lambda(p)^{\nu/d}U^{n/d}]^{-1} &= \prod_{\nu/d}[1-\lambda(p)^{\nu/d}u^{n\nu/d}]^{-d}\\ &= \prod_{i=1}^{\nu}[1-\lambda(p)\zeta_{\nu/d}^i u^n]^{-d}\\ &= \prod_{i=1}^{\nu}[1-\lambda(p)(\zeta_\nu^i u)^n]^{-1}\end{aligned}$$

其中ζ_m是1的m次原始方根。我們得證了

$$\begin{aligned}&1+g(\mathbf{X},\Psi)u^\nu\\ =\ &\prod_{p\in T}\prod_{i=1}^{\nu}[1-\lambda(p)(\zeta_\nu^i u)^{\deg p}]^{-1}\\ =\ &\prod_{i=1}^{\nu}[1-g(x,\psi)\zeta_\nu^i u]\\ =\ &1-[-g(x,\psi)]^\nu u^\nu\end{aligned}$$

這證明了定理。

參考文獻

1. N. Jacobson: Basic Algebra I, Freeman, San Francisco (1980).
2. S. Lang: Algebra, Addison-Wesley, Reading, Mass (1967).
3. A. Weil: Numbers of solutions of equation in finite fields, Bulletin of Amer. Math. Soc. 55, 497-508 (1949).

—本文本文作者爲美國賓州州立大學數學系教授, 現正訪問國立台灣大學數學系—