Weil 猜測

李文卿

余文卿 合著

第一節 方程式在有限體中解的個數

在這一節, 我們將討論代數曲線在有限體內的有理點的估計問題。這方面的工作由 Hua-Vandiver [12] 所提出, 另也由 Weil [13] 獨立發現, 在此我們採用 [13] 的講法, 而引導出有名的 Weil 猜測 (Weil conjecture)。

以 k 表示 q 個元素的有限體。考慮

$$a_0x_0^{n_0} + a_1x_1^{n_1} + \cdots + a_rx_r^{n_r} = b$$

一類的多項方程式, 其中 $a_0, a_1, \ldots, a_r$ 是 k 中的非零元素, $b \in k$ 且 $n_0, n_1, \ldots, n_r$ 是正整數, 我們想估計這方程式在 $(k)^{r+1}$ 中的解的個數。

首先討論 $b = 0$ 的特殊情形。給定 $u \in k$, 以 $N_i(u)$ 表示方程式

$$x^{n_i} = u$$

在 k 中解的個數。因而 $N_i(0) = 1$, $N_i(u) = d_i$, d_i =g.c.d. $(n_i, q-1)$, 這 u 也是 $k^\times$ 中元素的 d_i 次方; 而其他情形, $N_i(u) = 0$, 這乃由於 $k^\times$ 是秩爲 $q-1$ 的循環群。以 N 表示方程式

$$a_0x_0^{n_0} + a_1x_1^{n_1} + \cdots + a_rx_r^{n_r} = 0$$

在 $(k)^{r+1}$ 中解的個數, 則

$$N = \sum_{\substack{u_0,u_1,\ldots,u_r \in k \\ \sum a_iu_i = 0}} N_0(u_0)N_1(u_1)\ldots N_r(u_r),$$

注意到滿足 $\sum\limits_{i=0}^{n} a_iu_i = 0$ 的 $(r+1)$ 序對 $(u_0, u_1, \ldots, u_r)$ 形成一 r 維的子向量空間。

函數 N_i 可進一步表示爲 $k^\times$ 的特徵 (首先不看 0 的取值) 如下。以 H_i 表示 $k^\times$ 的子群 $(k^\times)^{n_i} = (k^\times)^{d_i}$, 這是秩爲 $(q-1)/d_i$ 的循環群。因 $H_i^\perp$ 是秩爲 d_i 的循環群且包含 k 中滿足 $\chi^{d_i} = 1$ 的所有特徵, 故

$$H_i^\perp = \{\chi \in \hat{k^\times} | \chi^{d_i} = 1\},$$

這裡 1 表示顯然特徵。對 $u \in k$, 我們發現

$$\sum_{u \in H_i^\perp} \chi(u) = \begin{cases} 1 & \text{若 } u = 0, \\ |H_i^\perp| = d_i & \text{若 } u \in H_i = (k^\times)^{d_i}, \\ 0 & \text{若 } u \in k^\times \backslash H_i, \\ & (\text{因 } (H_i^\perp)^\perp = H_i). \end{cases}$$

換句話說

$$N_i = \sum_{\chi \in H_i^\perp} \chi = \sum_{\chi \in \hat{k}^x, \chi^{d_i} = 1} \chi,$$

因此

$$N = \sum_{u_i \in k, \Sigma a_i u_i = 0} \sum_{\chi \in \hat{k}^x, \chi_i^{d_i} = 1} \chi_0(u_0)\chi_1(u_1)\dots\chi_r(u_r).$$

固定一 $(\chi_0, \chi_1, \dots, \chi_r) \in (\hat{k}^\times)^{r+1}$, $\chi_i^{d_i} = 1$ $(0 \le i \le r)$ 而讓 u_i 在 k 變動, 我們想由此得出 N 的進一步取值。若所有 χ_i 都是顯然特徵, 即對任意 $u_i \in k$, $\chi_i(u) = 1$, 對所有 $u_i \in k$, $\sum_{i=0}^{r} a_i u_i = 0$ 求和, 則和就是方程式 $\sum_{i=0}^{r} a_i u_i$ 在 $(k)^{r+1}$ 中解的個數, 是等於 q^r。其次, 若某些但非全部的 χ_i 是顯然特徵, 如 $\chi_{i_0} = 1$, 則 $\chi_{i_0}(u_{i_0}) = 1$ 是與 u_{i_0} 取值無關。則對所有 $\sum_{i=0}^{r} a_i u_i = 0$ 求和時, 得到的和是

$$\prod_{\substack{j \ne i_0 \\ 0 \le j \le r}} \left(\sum_{u_i \in k} \chi_j(u_i) \right)。$$

因某一 χ_j 是非顯然特徵, 故乘積是 0。到此我們得到

$$\begin{aligned} N &= q^r + \sum_{u_i \in k, \Sigma a_i u_i = 0} \sum_{\chi_i \in \hat{k}^x, \chi_i^{d_i} = 1, \chi_i \ne 1} \chi_0(u_0)\chi_1(u_1)\dots\chi_r(u_r) \\ &= q^r + \sum_{\chi_i^{d_i} = 1, \chi_i \ne 1} \chi_0(a_0)^{-1}\cdots\chi_r(a_r)^{-1} \sum_{u_i \in k, \Sigma a_i u_i = 0} \chi_0(a_0 u_0)\chi_1(a_1 u_1)\dots\chi_r(a_r u_r) \\ &= q^r + \sum_{\chi_i^{d_i} = 1, \chi_i \ne 1} \chi_0(a_0)^{-1}\cdots\chi_r(a_r)^{-1} \sum_{y_i \in k^\times, \Sigma y_i = 0} \chi_0(y_0)\chi_1(y_1)\dots\chi_r(y_r) \quad (y_i = a_i u_i) \\ &= q^r + \sum_{\chi_i^{d_i} = 1, \chi_i \ne 1} \chi_0(a_0)^{-1}\cdots\chi_r(a_r)^{-1} \sum_{\substack{y_0, v_1, \dots, v_r \in k^\times \\ v_1 + v_2 + \dots + v_r + 1 = 0}} (\chi_0\chi_1\dots\chi_r)(y_0)\chi_1(v_1)\dots\chi_r(v_r) \end{aligned}$$

$$
\begin{aligned}
&(y_i = y_0 v_i)\\
&= q^r + (q-1) \sum_{\chi_i^{d_i},\chi_i\neq 1,\Pi\chi_i=1} \chi_0(a_0)^{-1}\cdots\chi_r(a_r)^{-1} \sum_{v_i\in k^\times, v_1+v_2+\cdots+v_r+1=0} \chi_1(v_1)\ldots\chi_r(v_r)\\
&\quad \left(\text{因} \sum_{y_0\in k^\times} \chi_0\cdots\chi_r(y_0) = \begin{cases} 0 & \text{若 } \prod_{i=0}^{r}\chi_i \neq 1,\\ q-1 & \text{若 } \prod_{i=0}^{r}\chi_i = 1\text{。}\end{cases}\right)\\
&= q^r + (q-1) \sum_{\chi_i^{d_i}=1,\chi_i\neq 1,\Pi\chi_i=1} \chi_0(a_0)^{-1}\cdots\chi_r(a_r)^{-1} j(\chi_1,\ldots,\chi_r)\text{。}
\end{aligned}
$$

如第一章命題所證, 對任意 k 中的非顯然加法特徵 ψ, Jacobi 和 $j(\chi_1,\ldots,\chi_r)$ 等於

$$\frac{1}{q} g(\chi_0,\psi) g(\chi_1,\psi_1)\ldots g(\chi_r,\psi)\text{。}$$

其中 $\chi_0\chi_1\cdots\chi_r = 1$, 且其絕對值等於 $q^{(r-1)/2}$, 因而得證

定理1: 方程式

$$a_0 x_0^{n_0} + a_1 x_1^{n_1} + \ldots + a_r x_r^{n_r} = 0$$

在 k^{r+1} 中解的個數 N 是

$$
\begin{aligned}
N &= q^r + (q-1) \sum_{\chi_i^{d_i}=1,\chi_i\neq 1,\Pi\chi_i=1} \chi_0(a_0)^{-1}\cdots\chi_r(a_r)^{-1} j(\chi_1,\ldots,\chi_r)\\
&= q^r + \frac{q-1}{q} \sum_{\chi_i^{d_i}=1,\chi_i\neq 1,\Pi\chi_i=1} \chi_0(a_0)^{-1}\cdots\chi_r(a_r)^{-1} g(\chi_0,\psi) g(\chi_1,\psi)\cdots g(\chi_r,\psi),
\end{aligned}
$$

其中 d_i =g.c.d. $(n_i, q-1)$, 特別是它滿足

$$|N - q^r| \leq (q-1) q^{\frac{r-1}{2}} M,$$

其中 M 是滿足 $\chi_i^{d_i} = 1$, $\chi_i \neq 1$, $\Pi\chi_i = 1$ 之特徵 $(\chi_0,\chi_1,\ldots,\chi_r)$ 總數。

其次考慮不均勻方程式

$$a_0 x_0^{n_0} + a_1 x_1^{n_1} + \cdots + a_r x_r^{n_r} = b, \quad b\in k^\times\text{。}$$

把上面方程式的各項係數除以 $-b$, 而可設原來方程式是

$$a_0 x_0^{n_0} + a_1 x_1^{n_1} + \cdots + a_r x_r^{n_r} + 1 = 0$$

以 N_1 表示上面方程式在 k^{r+1} 中的解的個數, 且以 N' 表示方程式

$$a_0 x_0^{n_0} + a_1 x_1^{n_1} + \cdots + a_r x_r^{n_r} + x_{r+1}^{q-1} = 0$$

在 k^{r+2} 中解的個數, 則由定理 1 得出

$$N' = q^{r+1} + (q-1) \sum_{\chi_i^{d_i}=1, \chi_i \neq 1, \chi_0 \cdots \chi_{r+1}=1} \chi_0(a_0)^{-1} \cdots \chi_r(a_r)^{-1} j(\chi_1, \ldots, \chi_{r+1})$$

其中 $d_{r+1} = q-1$, 更進一步, N' 與 N 的關係式是

$$N' = N + (q-1)N_1$$

在此 N 表示 $x_{r+1} = 0$ 時解的個數, 且 $(q-1)N_1$ 表示 $x_{r+1} \neq 0$ 時解的個數, 因這時 $x_{r+1}^{q-1} = 1$。因此

$$\begin{aligned} N_1 &= \frac{1}{q-1}(N' - N) \\ &= q^r + \sum_{\chi_i^{d_i}=1, \chi_i \neq 1, \chi_0 \cdots \chi_{r+1}=1} \chi_0(a_0)^{-1} \cdots \chi_r(a_r)^{-1} j(\chi_1, \ldots, \chi_{r+1}) \\ &\quad - \sum_{\chi_i^{d_i}, \chi_i \neq 1, \chi_0 \cdots \chi_r = 1} \chi_0(a_0)^{-1} \cdots \chi_r(a_r)^{-1} j(\chi_1, \ldots, \chi_r) \end{aligned}$$

在上面的表現式中, 我們可以把第二個和視爲第一個和中 $\chi_{r+1} = 1$ 的情形。因 $d_{r+1} = q-1$, χ_{r+1} 唯一要考慮的條件是對給定的 $\chi_0, \ldots, \chi_r$, $\chi_i^{d_i} = 1$, $\chi_i \neq 1$, 滿足

$$\chi_0 \chi_1 \cdots \chi_{r+1} = 1$$

因此, 這樣的 $(\chi_0, \ldots, \chi_r)$ 的個數有 $(d_0 - 1) \cdots (d_r - 1)$ 個, 得證出

定理2: 滿足方程式

$$a_0 x_0^{n_0} + a_1 x_1^{n_1} + \ldots + a_r a_r^{n_r} = b, \qquad a_i \in k^\times,\ b \in k^\times$$

的解的個數 N_1 滿足

$$|N_1 - q^r| \leq (d_0 - 1) \ldots (d_r - 1) q^{r/2},$$

其中 d_i =g.c.d. $(n_i, q-1)$。

以 $P^r(k)$ 表示 k 上的 r 維投影空間 (projective space)。是由 $k^{r+1} \backslash \{0\}$, 把共線的點合而爲一而得, 換句話說, 它是由

$$(x_0 : x_1 : \ldots : x_r),\ x_i \in k,\ \text{不全爲零}$$

的點所組成, 且對 $t \in k^\times$,

$$(x_0 : x_1 : \ldots : x_r) = (tx_0 : tx_1 : \ldots : tx_r),$$

給定一齊次多項式 $f(x_0,\ldots,x_r)$。若 $(b_0, b_1,\ldots,b_r)$ 是方程式 $f=0$ 的解, 則對 $t\in k$, $(tb_0, tb_1,\ldots,tb_r)$ 也是方程式的解。因此, 我們可考慮一齊次多項方程式或一組齊次多方程式在投影空間的解, 其解集合稱爲投影曲體(projective variety)。

以 $\overline{N}$ 表示方程式

$$a_0x_0^m + a_1x_1^m + \ldots + a_rx_r^m = 0, \quad a_i \in k^\times$$

在投影空間 $P^r(k)$ 所定投影曲體的點的個數, 則

$$N = 1 + (q-1)\overline{N}$$

換句話說,

$$\overline{N} = 1 + q + \cdots + q^{r-1} + \sum_{\chi_i^{d_i}=1,\chi_i\neq 1,\chi_0\cdots\chi_r=1} \chi_0(a_0)^{-1}\ldots\chi_r(a_r)^{-1}j(\chi_1,\ldots,\chi_r),$$

其中 d =g.c.d. $(m, q-1)$。

第二節 Weil 猜想

對任意正整數 n, 以 k_n 表示 k 在其代數閉包 $\overline{k}$ 的 n 次擴充體。並以 $\overline{N}_n$ 表示方程式

$$a_0x_0^m + a_1x_1^m + \ldots + a_rx_r^m = 0$$

在 $P^r(k_n)$ 中解的個數; 定 $d(n)$ =g.c.d (m, q^n-1), 則 $|k_n| = q^n$, 且

$$\overline{N}_n = 1 + q^n + \cdots + (q^n)^{r-1} \sum_{\substack{\chi_i\in\hat{k}_n^\times,\chi_i^{d(n)}=1\\ \chi_i\neq 1,\chi_0\cdots\chi_r=1}} \chi_0(a_0)^{-1}\ldots\chi_r(a_r)^{-1}j(\chi_1,\ldots,\chi_r)。 \qquad (1)$$

現我們探討出現在上面和中的特徵。注意到 d =g.c.d. $(m, q-1)$ 可整除 $d(n)$。$k^\times$ 中滿足 $\chi^d=1$ 的特徵 χ 生成 $k_n^\times$ 中的特徵 $\mathbf{X}$= $\chi\cdot N_{k_n/k}$; 因 $N_{k_n/k}$ 是映成, 故 χ 與 $\mathbf{X}$ 有相同的秩。另一方面, $k_n^\times$ 中剛好有 d 個特徵的秩可整除 d; 故 $\hat{k}_n^\times$ 中滿足 $\chi^d=1$ 的特徵 χ 正好就是 $k^\times$ 的特徵與 Norm 的合成。利用以上的語言, 有時也把 $\chi\cdot N_{k_n/k}$ 寫爲 $\chi_\circ$ 設 ψ 是 k 的非顯然加法特徵, 則由第一章命題 5, 對 $\chi_0,\ldots,\chi_r\in\hat{k}^\times$, 滿足 $\chi_i^d=1$, $\chi_i\neq 1$, $\chi_0\cdots\chi_r=1$, 則有

$$\begin{aligned} &\chi_0\circ N_{k_n/k}(a_i)^{-1}\ldots\chi_r\circ N_{k_n/k}(a_r)^{-1}j(\chi_0\circ N_{k_n/k},\ldots,\chi_r\circ N_{k_n/k})\\ =\ &[\chi_0(a_0)^{-1}\ldots\chi_r(a_r)^{-1}]^n\frac{1}{q^n}g(\chi_0\circ N_{k_n/k},\psi\circ Tr_{k_n/k})\ldots g(\chi_r\circ N_{k_n/k},\psi\circ Tr_{k_n/k}) \end{aligned}$$

$$= [\chi_0(a_0)^{-1}\cdots\chi_r(a_r)^{-1}]^n\frac{1}{q^n}g(\chi_0,\psi)^n\cdots g(\chi_r,\psi)^n(-1)^{(n+1)(r+1)}$$
(利用 Davenport-Hasse 恆等式)
$$= [\chi_0(a_0)^{-1}\cdots\chi_r(a_r)^{-1}j(\chi_0,\chi_1,\ldots,\chi_r)]^n(-1)^{(r+1)(n+1)}。$$

同樣, 若 $k_n \supset k_{n'} \supset k$ 則 (1) 中由 $\chi_i \in \hat{k}_n^\times$ $i=0,1,\cdots,r$ 所造成的和是

$$[\chi_0(a_0)^{-1}\cdots\chi_r(a_r)^{-1}j(\chi_0,\chi_1,\ldots,\chi_r)]^{n/n'}(-1)^{(r+1)(\frac{n}{n'}+1)}$$

對 $(\chi_0,\ldots,\chi_r)\in(\hat{k}_n^\times)^{r+1}$, 以 $\mu=\mu(\chi_0,\ldots,\chi_r)$ 表示體擴充的次數, 使得所有 χ_i 首次皆出現在 $\hat{k}_\mu^\times$ 中, 則 (1) 可表示爲

$$\overline{N}_n = 1+q^n+\cdots+q^{n(r-1)} + \sum_{\chi_i^{d(n)}=1,\chi_i\neq1,\chi_0\cdots\chi_r=1}[\chi_0(a_0)^{-1}\cdots\chi_r(a_r)^{-1}j(\chi_0,\ldots,\chi_r)]^{n/\mu}(-1)^{(r+1)(\frac{n}{\mu}+1)}$$

注意到 n 趨近於無窮大時, 只會有有限多個 $d(n)$。事實上, 若 m' 是 m 的因數中與 q 互質的最大因數, 則 $d(n)$ 是 m 的因數。因此, 除掉與 Norm 的合成因素, 只有有限個 k 之有限擴充體, 其乘法特徵的秩可整除 m'; 因而形式冪級數

$$\sum_{n=1}^{\infty}\overline{N}_nU^{n-1}=\sum_{i=0}^{r-1}\frac{q^i}{1-q^iU}+(-1)^r\sum_{\chi_i^m=1,\chi_i\neq1,\chi_0,\cdots\chi_r=1}\frac{-c(\chi_0,\ldots,\chi_r)U^{\mu-1}}{1-c(\chi_0,\ldots,\chi_r)U^\mu}, \qquad (2)$$

其中

$$c(\chi_0,\ldots,\chi_r) = (-1)^{r+1}\chi_0(a_0)^{-1}\cdots\chi_r(a_r)^{-1}j(\chi_0,\ldots,\chi_r)$$
$$= (-1)^{r+1}\chi_0(a_0)^{-1}\cdots\chi_r(a_r)^{-1}\frac{1}{q^\mu}g(\chi_0,\psi\circ Tr_{k_\mu/k})\cdots g(\chi_r,\psi\circ Tr_{k_\mu/k})$$

設 $\tau\in\mathrm{Cal}(k_\mu/k)$ 是一自同構, 則 $\chi_i^\tau=\chi_i\circ\tau$ 是 χ_i 的同秩非顯然特徵且滿足 $\chi_0^\tau\cdots\chi_r^\tau=1$, 因此 $\mu(\chi_0,\ldots,\chi_r)=\mu(\chi_0^\tau,\ldots,\chi_r^\tau)$, 更進一步

$$g(\chi_i^\tau,\psi\circ Tr_{k_\mu/k}) = \sum_{x\in k_\mu^\times}\chi_i^\tau(x)\psi(Tr_{k_\mu/k}x)=\sum_{x\in k_\mu^\times}\chi_i(x)\psi(Tr_{k_\mu/k}\tau^{-1}(x))$$
$$= \sum_{x\in k_\mu^\times}\chi_i(x)\psi(Tr_{k_\mu/k}x)=g(\chi_i,\psi\circ Tr_{k_\mu/k}).$$

因 $a_i\in k^\times$, 故 $\chi_i^\tau(a_i)=\chi_i(a_i)$。這證明了對任意 $\tau\in\mathrm{Gal}(k_\mu/k)$,

$$c(\chi_0^\tau,\ldots,\chi_r^\tau)=c(\chi_0,\ldots,\chi_r).$$

給定$(\chi_0,\ldots,\chi_r)$, 則有 $\mu(\chi_0,\ldots,\chi_r)$ 個 $(\chi_0,\ldots,\chi_r)$ 的共軛, 而它們共有相同的 c 與 μ, 故 (2) 可重寫爲

$$\sum_{n=1}^{\infty}\overline{N}_nU^{n-1}=\sum_{i=0}^{r-1}\frac{q^i}{1-q^iU}+(-1)^r\sum_{(\chi_0,\ldots,\chi_r)\in\Lambda_r}\frac{-\mu(\chi_0,\ldots,\chi_r)c(\chi_0,\ldots,\chi_r)U^{\mu-1}}{1-c(\chi_0,\ldots,\chi_r)U^{\mu}} \quad (3)$$

其中 Λ_r 是 $\{(\chi_0,\ldots,\chi_r)|\chi_i^m=1,\ \chi_i\neq 1,\ \chi_0\ldots\chi_r=1\}$ 在 $\mathrm{Gal}(k_\mu/k)$ 作用下的等價類。觀察到 (3) 的分式中, 分子都是分母的微分乘上 ±1, 故得出

$$\sum_{n=1}^{\infty}\overline{N}_nU^{n-1}=\frac{d}{dU}\log Z(U)=\frac{Z'(U)}{Z(U)}。$$

$Z[U]$ 是一 U 的有理函數, 我們將選擇 $Z[U]$, 使其爲兩常數項是 1 之多項式的商, 這稱爲附在方程式

$$a_0x_0^m+a_1x_1^m+\ldots+a_rx_r^m=0$$

所定義曲體的 zeta 函數。

習題1: 若 $\tau\in\mathrm{Cal}(k_\mu/k)$ 是異於單位元素的同構, 則

$$(\chi_0^\tau,\ldots,\chi_r^\tau)\neq(\chi_0,\ldots,\chi_r)$$

這裡 $\mu=\mu(\chi_0,\ldots,\chi_r)$。

例題1: 設 V_1 是 q 個元素 的體 k 上, 由方程式 $x_0^2+x_1^2+x_2^2=0$ 所定義的投影曲體。設 q 是奇數, 則有 $r=2$ 且 $m=2=m'$。$\hat{k}^\times$ 中只有一個秩爲 2 的非顯然特徵 χ, 故唯一的選擇是 $\chi_i=\chi$, $i=0,1,2$; 但這時 $\chi_0\chi_1\chi_2=\chi^3=\chi\neq1$。當 q 是偶數時, $m'=1$; 故兩種情形下, 出現在 (3) 的第二個和的項數是空集合, 且

$$\sum_{n=1}^{\infty}\overline{N}_nU^{n-1}=\frac{1}{1-U}+\frac{q}{1-qU}=\frac{d}{dU}\log Z_{V_1}(U),$$

其中

$$Z_{V_1}(U)=\frac{1}{(1-U)(1-qU)}。$$

例題2: 設 V_2 是 $P^2(k)$ 中方程式 $x_0^3+x_1^3+x_2^3=0$ 所定義的投影曲體, $|k|=q$, 故 $m=3$, $r=2$, $a_0=a_1=a_2=1$。設 $q\equiv1\pmod 3$, 則 $m'=3$ 可整除 $q-1$, 以 η, $\overline{\eta}$ 表 $\hat{k}^\times$ 中秩爲 3 的特徵。滿足

$$\chi_i^3=1,\ \chi_i\neq1\ \text{且}\ \chi_0\chi_1\chi_2=1$$

的 (χ_0, χ_1, χ_2) 之唯一選擇是 (η, η, η) 與 $(\overline{\eta}, \overline{\eta}, \overline{\eta})$ 故 $\mu(\eta, \eta, \eta) = \mu(\overline{\eta}, \overline{\eta}, \overline{\eta}) = 1$, 且對 k 的任意非顯然特徵 ψ,

$$c(\eta, \eta, \eta) = -\frac{1}{q}\, g(\eta, \psi)^3,$$
$$c(\overline{\eta}, \overline{\eta}, \overline{\eta}) = -\frac{1}{q}\, g(\overline{\eta}, \psi)^3$$

因此

$$\sum_{n=1}^{\infty} \overline{N}_n U^{n-1} = \frac{1}{1-U} + \frac{q}{1-qU} + \frac{\frac{1}{q} g(\eta, \psi)^3}{1 + \frac{1}{q} g(\eta, \psi)^3 U} + \frac{\frac{1}{q} g(\overline{\eta}, \psi)^3}{1 + \frac{1}{q} g(\eta, \psi)^3 U} = \frac{d}{dU} Z_{V_2}(U)$$

而

$$Z_{V_2}(U) = \frac{[1 + \frac{1}{q} g(\eta, \psi)^3 U][1 + \frac{1}{q} g(\overline{\eta}, \psi)^3 U]}{(1-U)(1-qU)}$$

注意到上面兩個例題中的 zeta 函數滿足關於 $Z_V(\frac{1}{qU})$ 與 $Z_V(U)$ 的泛方程式。事實上, 在例題 1 中, 我們有

$$Z_{V_1}(\frac{1}{qU}) = \frac{1}{(qU^2)^{-1}} Z_{V_1}(U) = (qU^2) Z_{V_1}(U)。$$

而在例題 2 中定 $g(\eta, \psi) = \varepsilon\sqrt{q}$, $\varepsilon \in S^1$, 則

$$g(\overline{\eta}, \psi) = \eta(-1)\overline{\varepsilon}\sqrt{q} = \overline{\varepsilon}\sqrt{q},$$

因 $\eta(-1) = [\eta(-1)]^3 = 1$, 則有

$$Z_{V_2}(U) = \frac{(1 + \varepsilon^3\sqrt{q}U)(1 + \overline{\varepsilon}^3\sqrt{q}U)}{(1-U)(1-qU)}$$

且

$$\begin{aligned} Z_{V_2}(\frac{1}{qU}) &= \frac{(\sqrt{q}U)^2(\sqrt{q}U + \varepsilon^3)(\sqrt{q}U + \overline{\varepsilon}^3)}{(qU^2)^{-1}(1-U)(1-qU)} = (qU^2)^2 \frac{(1 + \overline{\varepsilon}^3\sqrt{q}U)(1 + \varepsilon^3\sqrt{q}U)}{(1-U)(1-qU)} \\ &= (qU^2)^2 Z_{V_2}(U)。 \end{aligned}$$

現考慮依附在方程式 $a_0 x_0^m + a_1 x_1^m + \ldots + a_r x_r^m = 0$ 所定義曲體 V 的 zeta 函數 $Z_V(U)$, 由 (3) 得出

$$Z_V(U) = \prod_{i=1}^{r-1} (1-qU)^{-1} \prod_{(\chi_0, \ldots, \chi_r) \in \Lambda_r} (1 - c(\chi_0, \ldots, \chi_r) U^{\mu})^{(-1)^r}。$$

注意到: 若 $(\chi_0,\ldots,\chi_r)$ 出現在上面的乘積中, 則 $(\overline{\chi}_0,\ldots,\overline{\chi}_r)$ 也會出現且 $\mu(\overline{\chi}_0,\ldots,\overline{\chi}_r)=\mu(\chi_0,\ldots,\chi_r)=\mu$, 又

$$\begin{aligned} c(\overline{\chi}_0,\ldots,\overline{\chi}_r) &= (-1)^{r+1}\overline{\chi}_0(a_0)^{-1}\cdots\overline{\chi}_r(a_r)^{-1}j(\overline{\chi}_1,\ldots,\overline{\chi}_r) \\ &= (-1)^{r+1}\chi_0(a_0)^{-1}\cdots\chi_r(a_r)^{-1}\overline{j(\chi_1,\ldots,\chi_r)}=\overline{c(\chi_0,\ldots,\chi_r)} \end{aligned}$$

由第一章的命題 5 得出 $j(\chi_1,\ldots,\chi_r)$ 的絕對值是 $q^{\mu(r-1)/2}$, 可定

$$c(\chi_0,\ldots,\chi_r)=\varepsilon(\chi_0,\ldots,\chi_r)q^{\mu(r-1)/2},\quad \varepsilon(\chi_0,\ldots,\chi_r)\in S^1,$$

則發現

$$\begin{aligned} 1-c(\chi_0,\ldots,\chi_r)(\frac{1}{q^{r-1}U})^{\mu} &= -(q^{\frac{r-1}{2}}U)^{-\mu}\varepsilon(\chi_0,\ldots,\chi_r)(1-\overline{\varepsilon(\chi_0,\ldots,\chi_r)}q^{\mu(r-1)/2}U^{\mu}) \\ &= -(q^{\frac{r-1}{2}}U)^{-\mu}\varepsilon(\chi_0,\ldots,\chi_r)(1-c(\overline{\chi}_0,\ldots,\overline{\chi}_r)U^{\mu})。 \end{aligned}$$

若$(\overline{\chi}_0,\ldots,\overline{\chi}_r)$不與$(\chi_0,\ldots,\chi_r)$共軛, 則$\varepsilon(\overline{\chi}_0,\ldots,\overline{\chi}_r)\varepsilon(\chi_0,\ldots,\chi_r)=1$, 否則$\varepsilon(\chi_0,\ldots,\chi_r)=\pm1$, 這證明了

$$\begin{aligned} Z_V(\frac{1}{q^{r-1}U}) &= (-1)^r q^{r(r-1)/2}U^r\prod_{i=0}^{r-1}(1-q^iU)^{-1}\prod_{(\chi_0,\ldots,\chi_r)\in\Lambda_r} \\ &\qquad -\varepsilon(\chi_0,\ldots,\chi_r)(q^{\frac{r-1}{2}}U)^{(-1)^{r+1}\mu}(1-c(\overline{\chi}_0,\ldots,\overline{\chi}_r)U^{\mu}) \\ &= \pm(q^{\frac{r-2}{2}}U)^e Z_V(U) \end{aligned}$$

其中指數 e 是 Z_V 的極點個數減去零點個數。而 $r-1$ 是曲體 V 的維數。

由上面對於曲線的計算結果, Weil 導出關於非奇異性不可約投影曲體 (nonsingular irreducible projective varieties) 之難以捉摸的猜測, 是有關定義在有限體之代數曲線的算術性質與定義在複數上之代數曲線的拓樸之間關連性。

設 V 是定義在 q 個元素之有限體 k 的 d 維非奇異性不可約投影曲體, 以 $\overline{N}_n$ 表示 V 在 k 之 n 次擴充體上的點的個數, 附在 V 的 zeta 函數定義成

$$Z_V(U)=\exp(\sum_{n=1}^{\infty}\overline{N}_n\frac{U^n}{n})$$

它是 U 之有理係數形式冪級數。在西元 1949 年, Weil 提出四個關於 $Z_V(U)$ 的四個猜測, 敍述如下:

(I) 有理性: $Z_V(U)$ 是 U 的有理數 (有理係數)。

(II) 泛方程式: 存在有整數 E, 稱爲 V 的 Euler-Poincáre 特徵數, 使得 $Z_V(U)$ 滿足泛方程式

$$Z_V(\frac{1}{q^dU}) = \pm(q^{\frac{d}{2}}U)^E Z_V(U)$$

(III) Riemann 假設: 存在有多項式 $P_i(U)$, $0 \leq i \leq 2d$, 滿足 $P_0(U) = 1 - U$ 且 $P_{2d}(U) = 1 - q^dU$, 使得

$$Z_V(U) = \frac{P_1(U)P_3(U)\dots P_{2d-1}(U)}{P_0(U)P_2(U)\dots P_{2d}(U)}。$$

更進一步, $P_i(U)$ 是整係數多項式且可分解爲

$$P_i(U) = \prod_{j=1}^{B_i}(1 - \alpha_{ij}U)$$

其中, α_{ij} 是代數整數, 滿足 $|\alpha_{ij}| = q^{i/2}$。注意到: 這樣的多項式要是存在時, 則由這些條件唯一確定。

(IV) Betti 數: $P_i(U)$ 的次數 B_i 定義成 V 的第 i 個 Betti 數, 則 (II) 中的 Euler-Poincáre 特徵數等於

$$\sum_{i=0}^{2d}(-1)^i B_i,$$

更進一步, 若 V 是由定義在數體之整數環上的曲體 $\widetilde{V}$ modulo - 質理想 (prime ideal) 而得, 則 B_i 等於一般餘調群 (cohomology group) $H^i(\widetilde{V}_k,\mathbf{Z})$ 的階數, 其中 $\widetilde{V}_n$ 是由定義 V 之同一方程式所定的複投影曲體, 而其拓樸是一般的拓樸。

例題 1 中的曲體是 P^2 上的投影線, 虧格數 (genus) 是 0, 它的 Euler-Poincáre 特徵數 $E = 2 = 1 - 0 + 1$, 滿足 (I)∼(IV) 的所有性質。例題 2 中的曲線 V_2 在 char $k \neq 2, 3$ 時是橢圓曲線 (elliptic curve), 即是虧格數是 1 的投影線。我們看出 Euler-Poincáre 特徵數 $E = 0 = 1 - 2 + 1$ 且 (I)∼(IV) 成立。

定義在有限體之非奇異性投影曲線的 zeta 函數是由 F. K. Schmidt 在西元 1931 年所引進, 他證明了: 對一定義在 q 個元素之有限體而虧格數是 g 的非奇異性投影曲線 C, 它的 zeta 函數形式是

$$Z_C(U) = \frac{P_1(U)}{(1 - U)(1 - qU)},$$

其中 $P_1(U)$ 是次數爲 $2g$ 的整係數多項式且 $P_i(0)=0$, 且更進一步, $Z_C(U)$ 滿足泛方程式

$$Z_C(\frac{1}{qU}) = \pm(qU)^{1-g} Z_C(U)$$

而對 C 的 Riemann 假設因此是: $P_1(U)$ 的零位的絕對值是 $q^{-1/2}$。這首先由 E. Artin 推測到, 他證明了特殊情形; $g=1$ 的情形由 Hasse 所證, 而 Weil 在 1940 年證出虧格數任意之曲線情形。

對方程式

$$a_0 x_0^m + a_1 x_1^m + \ldots + a_r x_r^m = 0$$

所定義的"Fermat 超曲面"而言, 其維數 $d = r-1$。當 r 是偶數且 d 是奇數時; 我們有

$$P_{2i}(U) \;=\; 1 - q^i U, \qquad 0 \le i \le d$$

且

$$P_d(U) \;=\; \prod_{(\chi_0,\ldots,\chi_r)\in\Lambda_r} (1 - c(\chi_0,\ldots,\chi_r) U^{\mu(\chi_0,\ldots,\chi_r)})$$

而 i 是其他奇數時, $P_i(U)=1$。

當 r 是奇數, d 是偶數時, 則有

$$P_{2i}(U) = 1 - q^i U, \quad 0 \le i \le d,\ i \ne \frac{d}{2}$$

且

$$P_d(U) = (1 - q^{\frac{d}{2}} U) \prod_{(\chi_0,\ldots,\chi_r)\in\Lambda_r} (1 - c(\chi_0,\ldots,\chi_r) U^{\mu(\chi_0,\ldots,\chi_r)})$$

而其他 $P_i(U)=1$。故 Z_V 滿足 Weil 猜測。

習題2: 證明定義在 q 個元素之有限體的非奇異性投影曲線 C 的 Riemann 假設等價於

$$|\overline{N}_n - q^n - 1| \le 2g \cdot g^{n/2}, \text{ 對所有 } n \ge 0,$$

其中 $\overline{N}_n$ 是 C 上的 k_n - 有理點個數。

習題3: 設 $V = P^d(k)$ 定義在 q 個元素的有限體。從定義出發驗證其 zeta 函數是

$$Z_V(U) = \frac{1}{(1-U)(1-qU)\cdots(1-q^dU)}$$

並證 Weil 猜測對 $V = P^d(k)$ 成立。

第三節 Weil 猜測的餘調代數解釋

如 Weil 自己所指出: 若賦予抽象曲體適當的餘調理論, 類似於定義在 $\mathbf{C}$ 上之曲體的普通餘調代數 (cohomology), 則由餘調代數理論的標準性質即可導出他的猜測。Dwork 利用 p-adic 分析, 成功地在有理性質與泛方程式方面推進了一步。有關 Weil 猜測的絕大部份工作集中在尋求好的餘調代數理論, 使能給出像 IV 的 Betti 數, 且其係數落在特徵數是 0 的體, 使得 Lefschetz 定點定理成立, 這裡有幾個嘗試。在 1963 年, Grothendieck 利用代數曲體的étale 拓樸而發展出 l-adic 餘調代數理論, 由此他得到 zeta 函數有理性質與泛方程式的另一證明。猜測最深的部份是 Riemann 假設, 而 Deligne 在西元 1973 年成功地利用 l-adic 餘調代數而加以證明。

在此我們簡短地解說 l-adic 餘調代數與 Weil 猜測的關連性。如上一節, 設 V 是非奇異性不可約的投影曲體, 維數是 d 且定義在 q 個元素的有限體 k, 以 $\overline{V}$ 表是 V 在代數閉包 $\overline{k}$ 上的所有點所成的集合。設 l 是不整除 q 的質數, 在 $\overline{V}$ 上賦予 étale 拓樸。對每一整數 $r \geq 1$, 則有 étale 餘調代數 $H^i_{\acute{e}t}(\overline{V}, \mathbf{Z}/l^r\mathbf{Z})$, $\overline{V}$ 上的 l-adic 餘調代數定義成

$$H^i(\overline{V}, \mathbf{Q}_l) = (\lim_{\infty \leftarrow r} H^i_{\acute{e}t}(\overline{V}, \mathbf{Z}/l^r\mathbf{Z})) \otimes_{\mathbf{Z}_l} \mathbf{Q}_l,$$

其中 $\mathbf{Z}_l$ 是 l-adic 整數環, 即

$$\mathbf{Z}_l = \{\sum_{i=0}^{\infty} a_i l^i | 0 \leq a_i \leq l-1\}。$$

是 r 趨近於無窮大時, $\mathbf{Z}/l^r\mathbf{Z}$ 的逆極限 (inverse limit), $\mathbf{Q}_l$是$\mathbf{Z}_l$的商體 (Quotient field), 也是 $\mathbf{Q}$ 在 l-adic 測度下的完備空間 (completion)。這 l-adic 餘調代數有下列的性質。

(a) 群 $H^i(\overline{V},\mathbf{Q}_l)$ 是佈於 $\mathbf{Q}_l$ 的有限維向量空間, 除 $0 \leq i \leq 2d$ 外, 其餘的都是 0。

(b) 對所有的 i, j, 存在有

$$H^i(\overline{V}, \mathbf{Q}_l) \times H^j(\overline{V}, \mathbf{Q}_l) \to H^{i+j}(\overline{V}, \mathbf{Q}_l)$$

的 cup-乘積構造。

(c) Poincáre 對偶性, 最高階的餘調群$H^{2d}(\overline{V}, \mathbf{Q}_l)$ 是一維的且對 $0 \leq i \leq 2d$, cup-乘積定義了不退化的配對

$$H^i(\overline{V}, \mathbf{Q}_l) \times H^{2d-i}(\overline{V}, \mathbf{Q}_l) \to H^{2d}(\overline{V}, \mathbf{Q}_l) \cong \mathbf{Q}_l。$$

(d) 對兩個非奇異性曲體 X, Y, 有一自然的階代數同構

$$H^*(X, \mathbf{Q}_l) \otimes H^*(Y, \mathbf{Q}_l) \xrightarrow{\sim} H^*(X \times Y, \mathbf{Q}_l) \text{ (Künneth 公式)}$$

(e) Lefschetz 定點式。設 $f : \overline{V} \to \overline{V}$ 是一映型 (morphism), 有弧立定點且每一定點的重數是一, 亦即 f 在 $\overline{V} \times \overline{V}$ 的圖形與 $\overline{V} \times \overline{V}$ 的對角線元素作橫截性相交 (intersect transversally)。以 $L(f, \overline{V})$ 表示 f 的定點個數 (因 $\overline{V}$ 緊緻, 故 $L(F, \overline{V})$ 是一有限集合), 則

$$L(f, \overline{V}) = \sum_{i=0}^{2d} (-1)^i Tr(f^{(i)}; H^i(\overline{V}, \mathbf{Q}_l)),$$

其中 $f^{(i)}$ 是 f 在 H^i 導出的 pull-back 映象。

(f) 比較定理 (Comparison theorem)。若 $\overline{V}$ 是由定義在數體整數環的投影曲體 modulo 質理想而得出, 則

$$H^i(\overline{V}, \mathbf{Q}_l) \otimes_{\mathbf{Q}_l} \mathbf{C} \cong H^i(\widetilde{V}_n, \mathbf{C})$$

其中 $\widetilde{V}_n$ 是所對應的複曲體, 而賦予古典的拓樸。

(g) Cycle 的餘調類, 若 Z 是一 codimension 爲 i 的子曲體, 則對應於 Z, 有一餘調類 $\eta(Z) \in H^{2i}(\overline{V}, \mathbf{Q}_l)$, 這映象可線性化地擴充到所有的 cycles。有理等價之 cycles 具同樣的餘調類。Cycles 的交集變成餘調類的 cup- 乘積。更進一步, 若 P 是 V 的一封閉點 (closed point), 則 $\eta(P) \in H^{2d}(\overline{V}, \mathbf{Q}_l)$ 異於零。

這些性質是 $\mathbf{C}$ 上不可分非奇異性投影曲體的一般餘調代數所特有, 主要是由 Lefschetz 與 Hodge 發展出來。

現我們探討上面性質的一些推論。Frobenius 映型 $\Phi : \overline{V} \to \overline{V}$ 把坐標是 (a_i) 的點映至坐標是 (a_i^q) 的點。$\overline{V}$ 上的點 P, 其坐標落在 k_n 的充要條件是它被 Φ^n 固定住。因此

$$\overline{N}_n = \Phi^n \text{的定點數} = L(\Phi^n; V)$$

因 V 非奇異, 我們可用 Lefschetz 定點式計算 $\overline{N}_n$ 而得出

$$\overline{N}_n = \sum_{i=0}^{2d} (-1)^i Tr((\Phi^n)^{(i)}, H^i(\overline{V}, \mathbf{Q}_l))。$$

代入附著在 V 的 zeta 函數的定義中, 得出

$$Z_V(U) \;=\; \prod_{i=0}^{2d} [\exp(\sum_{n=1}^{\infty} Tr((\Phi^n)^{(i)}, H^i(\overline{V}, \mathbf{Q}_l)) \frac{U^n}{n})]^{(-1)^i}$$

$$= \prod_{i=0}^{2d}[\exp(\sum_{n=1}^{\infty} Tr(\Phi^{(i)^n}, H^i(\overline{N}, \mathbf{Q}_l))\frac{U^n}{n})]^{(-1)^i}$$

對每一固定 i, 我們利用下面線性代數的結果, 得出指數部份的值。

預備定理 1 設 f 是一佈於特徵數是 0 之體 K 的有限維向量空間的自同態, 視爲係在 K 而變數是 U 的形式冪級數, 則

$$\exp[\sum_{n=1}^{\infty} Tr(f^n; W)\frac{U^n}{n} = \det(1 - fU, W)^{-1}$$

證明: 若 W 的維數是 1, 則 f 只是乘上純量入, 且

$$\exp[\sum_{n=1}^{\infty} Tr(f^n, W)\frac{U^n}{n}] = \exp(\sum_{n=1}^{\infty} \frac{\lambda^n U^n}{n}) = \frac{1}{1-\lambda U} = \det(1 - fU; W)^{-1}。$$

對一般情形, 我們歸納 dim W 而證之。可假設 K 是代數封閉。故 f 有一固有向量, 因此 W 包含一維數是 1 的不變子空間 W', 因而有短的 exact 系列

$$0 \longrightarrow W' \longrightarrow W \longrightarrow W/W' \longrightarrow 0$$

式子的左邊 (右邊) 限制在 W' 與限制在 W/W' 的乘積等於是在 W 的情形。故所要結果由歸納法得證。

由預備定理馬上得出下面的定理

定理3: 附於定義在 k 之非奇異性不可約投影曲體 V 的 zeta 函數可表爲

$$Z_V(U) = \frac{P_1(U)P_3(U)\dots P_{2d-1}(U)}{P_0(U)P_2(U)\dots P_{2d}(U)},$$

其中 $P_i(U) = \det(1 - \Phi^{(i)}U; H^i(V; \mathbf{Q}_l))$ 且定義在 $H^i(V, \mathbf{Q_l})$ 的 $\Phi^{(i)}$ 是由 Frobenius 映型 $\Phi : \overline{V} \to \overline{V}$ 所引導出。

我們知道 $Z_V(U)$ 是係數在 $\mathbf{Q}$ 且是 U 的形式冪級數。上面定理告訴我們它的係數在 $\mathbf{Q}_l$ 且是 U 的有理函數。因此它的係數在 $\mathbf{Q}$ 且是 U 的有理函數。但這並不表示每一單一的 $P_i(U)$ 是有理係數, 也不知道定理中的 P_i 是否像 (III) 中的一樣。另一方面, 因 Φ^0 作用在 $H^0(\overline{V},\mathbf{Q}_l)$ 是恆等函數, 故 $P_0(U) = 1 - U$。更進一步, 因 Frobenius 映型是 q^d 次的有限映型, 故它引導出最高階餘調群 $H^{2d}(\overline{V},\mathbf{Q}_l)$ 上乘上 q^d 的乘法, 故 $P_{2d}(U) = 1 - q^dU$。

其次, 我們看出泛方程式 (II) 可由 Poincáre 對偶性 (c) 得出。事實上, 配對

$$H^i(V, \mathbf{Q}_l) \times H^{2d-i}(\overline{V}; Q_l) \longrightarrow H^{2d}(\overline{V}; \mathbf{Q}_l)$$

把 $(\Phi^{(i)}(v), \Phi^{(2d-i)}(w))$ 送到

$$\Phi^{(i)}(v) \vee \Phi^{(2d-i)}(w) = \Phi^{(2d)}(v \vee w) = q^d(v \vee w)$$

對所有的 $v \in H^i(\overline{V}, \mathbf{Q}_l)$ 與 $w \in H^{2d-i}(\overline{V}; \mathbf{Q}_l)$, 上面式子都成立。則由線性代數 (見注意事項) 得出

$$\begin{aligned} P_{2d-i}(U) &= \det(1 - \Phi^{(2d-1)}U; H^{2d-i}(\overline{V}; \mathbf{Q}_l) \\ &= \frac{(-1)^{B_i}(q^dU)^{B_i}}{\det(\Phi^{(i)}; H^i(\overline{V}; \mathbf{Q}_l)} \det(1 - \Phi^{(i)}/q^dU; H^i(\overline{V}; \mathbf{Q}_l) \\ &= \frac{(-q^dU)^{B_i}}{\det(\Phi^{(i)}; H^i(\overline{V}; \mathbf{Q}_l)} P_i(\frac{1}{q^dU}) \end{aligned}$$

且

$$\det(\Phi^{(i)}; H^i(\overline{V}; \mathbf{Q}_l)) \det(\Phi^{(2d-i)}; H^{2d-i}(\overline{V}; \mathbf{Q}_l)) = q^{dB_i}。$$

注意事項: 設 A 與 B 是佈於體 K 的 r 維向量空間, 定義一配對

$$\langle\ ,\ \rangle : A \times B \longrightarrow K$$

設 f 與 g 分別是 A 與 B 上的自同態且存在有一非零元素 $\lambda \in K$ 滿足: 對所有 $a \in A$, $b \in B$

$$\langle f(a), g(b)\rangle = \lambda\langle a, b\rangle$$

則 f 與 g 都可逆, 更進一步 ${}^{\mathrm{t}}\mathrm{g}\, f = \lambda I_A$, 因此

$$\begin{aligned} \det(1 - {}^tg\, U; B) &= \det(1 - gU; B) \\ &= \det(1 - \lambda f^{-1}U; A) \\ &= \det(1 - \lambda f^{-1}U) \det(1 - \frac{f}{\lambda U}; A) = \frac{(-\lambda U)^r}{\det(f, A)} \det(1 - \frac{f}{\lambda U}; A) \end{aligned}$$

且

$$\det({}^{\mathrm{t}}\mathrm{g}\, f) = (\det g)(\det f) = \det \lambda I_A = \lambda^r。$$

事實上, $q^{-(2d-i)/2}\Phi^{(2d-i)}$ 的轉置是 $q^{-i/2}\ \Phi^{(i)}$ 的反元素。與定理 3 組合在一起, 得出 (II) 的泛方程式, 而

$$E = \sum_{i=0}^{2d}(-1)^i B_i。$$

最後, 若我們把定理 3 中的 zeta 函數做上面的解釋時, 則 (I), (III), (IV) 隨著 l-adic 餘調代數的性質得出, 而 Riemann 假設是 Deligne 在 1973 年利用更深的 l-adic 餘調代數得證出來。

定理4 (Deligne): 定理3中的多項式$P_i(U)$ 具有與 l 無關的整係數, 且可寫成

$$P_i(U) = \prod_{j=1}^{B_i}(1 - \alpha_{ij}U),$$

其中 α_{ij} 是絕對值爲 $q^{i/2}$ 的代數整數。

在此我們不列出 Deligne 的證明, 只稍微解釋爲什麼會成立。存在有一 codimension 是 1 的 cycle Z, 使得 $h = \eta(Z)$ 是 $H^2(\overline{V}, \mathbf{Q}_l)$ 的非顯然類且 $\Phi^{(2)}(h) = qh$, 與 h 作 $(d-i)$ 次的 cup-乘積得出一從 $H^i(\overline{V}, \mathbf{Q}_l)$ 到 $H^{i+2(d-i)}(\overline{V};\ \mathbf{Q}_l) = H^{2d-i}(\overline{V}; \mathbf{Q}_l)$ 的函數, 這配合 Poincáre 的對偶性, 得出 $H^i(\overline{V}; \mathbf{Q}_l) \times H^i(\overline{V}; \mathbf{Q}_l)$ 到 $H^{2d}(\overline{V}, Q_l)$ 的不退化配對。

當 V 對應有不可約且非奇異性的複投影曲體 $\widetilde{V}_h$。這就是 $H^i(\widetilde{V}_h; \mathbf{C}) \times H^i(\widetilde{V}_h, \mathbf{C})$ 到 $H^{2d}(\widetilde{V}_h; \mathbf{C})$ 的不退化配對。當 i 是偶數時, $H^i(\widetilde{V}, \mathbf{C})$ 包含一實子空間 $A^i(\widetilde{V}_h)$, 它在 $\Phi^{(i)}$ 作用下不變且佈於 $\mathbf{R}$ 的維數是 B_i; 又滿足: 在 $A^i(\widetilde{V}_h)$ 上, 這配對是不退化的純量積且 $q^{-i/2}\Phi^{(i)}$ 是這純量積下的么正轉換 (unitary transform)。這證明 i 是偶數時, $\Phi^{(i)}$ 的固有值的絕對值是 $q^{i/2}$。

對奇數 i, 我們考慮 $\overline{V} \times \overline{V}$, $\Phi^{(i)}$ 在 $H^i(\overline{V};\ \mathbf{Q}_l)$ 之固有值的大小則由 $H^{2i}(\overline{V} \times \overline{V}; \mathbf{Q}_l)$ 上的 Frobenius 映型所決定。

注意事項: 如上面所證, $\Phi^{(i)}$ 在 $H^{(i)}(\overline{V};\ \mathbf{Q}_l)$ 的固有值即是出現在 $P_i(U) = \prod_{j=1}^{B_j}(1 - \alpha_{ij}U)$ 中的 α_{ij}; 特別是 $\Phi^{(i)}$ 之固有值的絕對值是 $q^{i/2}$。

高斯是第一個考慮整係數多項式方程式在 modulo p 下的解的個數。特別是他想知道解的個數 N_p 隨 p 變化的情形。假設這多項式定義一維數是 d 的不可約且非奇異性投影曲體, 則 Weil 的猜測顯示

$$|N_p - (1 + p + \cdots + p^d)| \leq bp^{d/2},$$

其中 b 是同一多項式在 $\mathbf{C}$ 上所定義之投影曲體的第 d 個 Betti 數。

第四節 Zeta 函數的 Euler 乘積

設 k 是一體且 $P(T_1, \ldots, T_r)$ 是 $k[T_1, \ldots, T_r]$ 中的不可約多項式。方程式 $P(T_1, \ldots, T_r) = 0$ 在 k^r 的解集合稱爲仿射空間 k^r 中的仿射代數超平面(affine algebraic hypersurface)。

我們也可以考慮 $P(T_1,\ldots,T_r)=0$ 在 k 的任意有限代數充體的解。以 $\overline{k}$ 表示 k 的代數閉包, 而 V 是 $P(T_1,\ldots,T_r)=0$ 在 $\overline{k}^r$ 中的解集合, 我們稱 V 是定義在 k 之上 (defined over k)。給定 V 上的一點 $x=(x_1,\ldots,x_r)$, 以 $k(x)$ 表由 x 之坐標所成的體 $k(x_1,\ldots,x_r)$, 這是 k 的有限體, 且其次數稱爲 x 的次數 (degree)。

考慮 $k[T_1,\ldots,T_r]$ 到 $\overline{k}$ 的同態, 把 T_i 送到 x_i; 其核 $\mathfrak{m}$ 是 $k[T_1,\ldots,T_r]$ 的最大理想 (maximal ideal) 且包含 P. 商環 $k[T_1,\ldots,T_r]/\mathfrak{m}$ 與 $k(x)$ 同構。定義 $\deg\mathfrak{m}$ 爲 $\deg x$, 因而會有 $\deg x=[k(x):k]$ 個 $k(x)$ 到 $\overline{k}$ 的嵌入 (embedding)。對任意嵌入 σ , 點 $x^\sigma=(x_1^\sigma,\ldots,x_r^\sigma)$ 也落在 V 上。從 $k[T_1,\ldots,T_r]$ 到 $\overline{k}$ 而把 T_i 送到 x_i^σ 的同態的核也是$\mathfrak{m}$, 原因是$\mathfrak{m}$中多項式的係數都落在 k 中。因此每一最大理想 $\mathfrak{m}$ 對應到 V 上 $\deg\mathfrak{m}$ 個點。反過來, 給定一包含 P 的最大理想 $\mathfrak{m}$, 它對應了上面所說的 $\deg\mathfrak{m}$ 個點, 這些點稱爲 x 對所有 $k(x)$ 到 $\overline{k}$ 之嵌入的軌跡, 即

$$\{x^\sigma|\sigma\in\mathrm{Gal}(\overline{k}/k)\}$$

是 V 的一封閉點, 而可表現爲 $k[T_1,\ldots,T_r]$ 中的最大理想$\mathfrak{m}$。

當 k 是一有限體時, V 的 zeta 函數定義爲

$$Z_V(u)=\prod_{p\in m}(1-u^{\deg\mathfrak{m}})^{-1}=\prod_x(1-u^{\deg x})^{-1},$$

其中$\mathfrak{m}$ 是 $k(T_1,\ldots,T_r)$ 的最大理想且 x 是 V 的封閉點。

V 在 k_n^r 上的點是次數整除 n 的點, 故至少有 q^{nr} 個最大理想 $\mathfrak{m}$ 使得 $P\in\mathfrak{m}$ 且 $\deg\mathfrak{m}$ 整除 n, 這裡 q 是 k 的元素個數, 這證明上面的無窮乘積在 u 非常小時會收斂。更進一步, 對足夠小的 u, 則有

$$\begin{aligned}\frac{Z_V(u)'}{Z_V(u)} &= \sum_{P\in\mathfrak{m},\,\mathfrak{m}:\text{最大}}\frac{(\deg\mathfrak{m})u^{\deg\mathfrak{m}-1}}{1-u^{\deg\mathfrak{m}}}=\sum_{l=1}^{\infty}\sum_{P\in\mathfrak{m},\,\mathfrak{m}:\text{最大}}(\deg\mathfrak{m})u^{l\deg\mathfrak{m}-1}\\ &= \sum_{\nu=1}^{\infty}N_\nu u^{\nu-1},\end{aligned}$$

其中 $N_\nu=\sum_{\deg\mathfrak{m}|\nu}\deg\mathfrak{m}$ 是 V 在 k_ν^r 中的點的個數。

一般, 若 V 是定義在有限體的非奇異性投影曲體, 它是多個仿射曲體的聯集; 像第二節利用 V 在 k 之有限充體之元素個數所定的 Zeta-函數 $Z_\nu(u)$ 具有 Euler 乘積

$$\begin{aligned}Z_\nu(u) &= \exp(\sum_{\nu=1}^{\infty}\overline{N}_\nu\frac{u^\nu}{\nu})\\ &= \prod_x(1-u^{\deg x})^{-1}\,(x:V\text{的封閉點})。\end{aligned}$$

例題1: 設 C 是有限體的投影線, 它有"無窮遠點", 而其他點在 k 的仿射線上。仿射線上的封閉點以 $k[T]$ 的首一不可約多項式或 $k(T)$ 的最大理想當參數, 則有

$$Z_C(u) = [\prod_{f\in k[T]}(1-u^{\deg f})^{-1}](1-u)^{-1} f \in k[T] \text{ 是首一不可約。}$$

例題2: 設 $\mathcal{C}$ 是由係數落在 q 個元素之有限體的均勻多項式 $P(T_0,T_1,T_2)$ 所定義的非奇異性投影曲線。解集合中的所有點 $\{x_0,x_1,x_2)|x_0\neq 0\}$ 可視爲由 $P(T,Y)=P(1,\frac{T_1}{T_0},\frac{T_2}{T_0})$ 所決定的仿射曲線, 其中 $T=\frac{T_1}{T_0}$, $Y=\frac{T_2}{T_0}$, 設 $P(T,Y)$ 對 Y 是首一多項式。以 F 表示體 $k(T)$ 且以 K 表示 $F[Y]/(P(T,Y))$, 它是 F 的有限擴充體, 稱爲 $\mathcal{C}$ 的有理函數體。設 $\mathcal{O}$ 是$k[T]$在K的整閉包 (integral closure)。$k[T,\,Y]$ 中包含 P 的最大理想 椹 即是 $\mathcal{O}$ 的最大理想 $\mathcal{P}$。更進一步, 若 $\mathcal{P}$ 對應到 $\mathcal{C}$ 的封閉點 x, 則 $\mathcal{O}/\mathcal{P}$ (稱爲 $\mathcal{P}$ 的餘數體) 同構於 $k(x)$。定義

$$\deg \mathcal{P} = \deg x = [\mathcal{O}/\mathcal{P};k]$$

故餘數體 $\mathcal{O}/\mathcal{P}$ 的元素個數是 $q^{\deg \mathcal{P}}$, 這也是 $\mathcal{P}$ 的範數 $N\mathcal{P}$, 附於仿射曲線 $\mathcal{C}$ 的 zeta 函數是

$$Z_{\mathcal{C}}(u)=\prod_{\mathcal{P}}(1-u^{\deg\mathcal{P}})^{-1},$$

稱這些質理想 $\mathcal{P}$ 是 $\mathcal{C}$ 或 K 的"有限位置"(finite places)。

在 $\mathcal{C}\backslash C$ 的點是解集合 $\{(x_0,x_1,x_2)|x_0=0\}$, 視爲選定之仿射子曲體的無窮遠點, 只有有限多個點。可表示爲 $k(\frac{1}{T})$ 在 K 的整閉包 $\mathcal{O}'$ 除以由 $\frac{1}{T}$ 所生成之最大主理想 $\mathcal{P}_\infty$, 這可看成"無窮位置"(infinite place)。再者$\deg \mathcal{P}_\infty=[\mathcal{O}/\mathcal{P}_\infty;\,k]$ 且餘數體 $\mathcal{O}'/\mathcal{P}_\infty$ 的元素個數是 $N\mathcal{P}_\infty$, 亦即 $q^{\deg\mathcal{P}_\infty}$。

有限與無限位置一起表示 $\mathcal{C}$ 的所有封閉點, 且有

$$Z_{\mathcal{C}}(u)=\prod_{\mathcal{P}:K\text{的位置}}(1-u^{\deg\mathcal{P}})^{-1}\text{。}$$

體 $F=k(T)$ 稱爲 k 上一個變數的有理函數體。$k(T)$ 的有限充體 K 稱爲函數體, 它是定義在 k_ν 之非奇異性投影曲體的有理函數體, 而含在 K 中之 k 的最大擴充體稱爲 K 的常數體(fields of constants)。

參考資料

[1] P. Deligne, La conjecture de Weil I, Inst. Hautes Etudes Sci. Publ. Math. 43 (1974), 273-307.

[2] P. Deligne, La conjecture de Weil II, Inst. Hautes Etudes Sci. Publ. Math. 52 (1980), 137-252.

[3] J. A. Dieudonné, On the history of the Weil conjecture, The Mathematical Intelligencer 10, Springer-Verlag, Berlin-Heidelkerg-New York (1975).

[4] B. Dwork, On the rationality of the zeta function of an algebraic variety, Amer. J. Math. 82 (1960), 631-648.

[5] E. Freitag and R. Kiehl, Etale Cohomology and the Weil conjecture, Springer-Verlag, Berlin-Heidelbery-New York (1988).

[6] A. Grothendieck (with M. Artin and J. L. Verdier), Théorie des topis et cohomologie étale des schémas (1963-1964), Lecture Notes in Math. 269, 270, 305, Springer-Verlag, Berlin-Heidelberg-New York, 1972-1973.

[7] A. Grothendieck, Formule de Lefschetz et rationalité des fonctions L, Séminaire Boubaki 1964/65, Exposé 279. W. A. Benjamin, New York, (1966).

[8] A. Grothendieck (by P. Deligne with J. F. Boutot, L. Illusie and J. L. Verdier), Cohomologie étale, Lecture Notes in Math. 569, Springer-Verlag, Berlin-Heidelberg, New York, (1977).

[9] A. Grothendieck, Cohomologie l-adique et fonćtions L (1965-1966), Lecture Notes in Math. 589, Springer-Verlag, Berlin-Heidelkerg, New York, (1977).

[10] R. Hartshorne, Algebraic Geometry, Springer-Verlag, Berlin-Heidelberg, New York, (1977).

[11] H. Hasse, Beweis des Analogons der Riemannschen Vermutung für die Artinschen und F. K. Schmidtschen Kongruenz zeta funktionen in gewissen elliptischen Fällen. Ges. d. Wiss. Nachrichten. Math. Phys. Klarse, (1933), Heft 3, 253-262.

[12] L. K. Hua and H. S. Vandiver, Characters over certain types of rings with applications to the theory of equations in a finite field, Proc. Nat, Acad. Sci. U.S.A., vol. 35 (1949), 94-99.

[13] A. Weil, Numbers of solutions of equations in finite fields, Bulletin of Amer. Math. Sic. 55 (1949), 497-508.

[14] A. Weil, Sur les courbes algébriques et les variétés qui sén déduisent, Hermann, Paris, (1948).

—本文作者分別任教於美國賓州州立大學數學系與國立中正大學數學系—