線性代數與數論

余文卿

使用代數的語言, 線性代數即是探討向量空間及上面的同態 (homomorphisms), 構成向量空間的主體只是一加法交換群, 其元素通稱爲向量, 而副體是一代數體, 通常是複數體 $\mathcal{C}$ 或其子體 $\mathcal{R}$ 或 $\mathcal{Q}$, 有時也可能是有限體; 體中的元素通稱爲純量; 純量乘向量得出向量, 這乘法稱爲純量乘法。而向量空間即是一具有純量乘法的加法交換群。

向量空間中較重要的同態即是一般所稱的線性轉換, 即對所有向量 v_1, v_2 以及純量滿足

$$L(\alpha v_1 + \beta v_2) = \alpha L(v_1) + \beta L(v_2)。$$

當這向量空間的維數是有限時, 取定一特殊的基底 $u_1, u_2, \ldots, u_n$; 若

$$L(u_i) = \sum_{j=1}^{n} a_{ij} u_j, \quad i = 1, 2, \ldots, n.$$

則 L 對映一 $n \times n$ 方陣 $A = [a_{ij}]_{1 \le i,j \le n}$; 變換到另一組基底 $w_1, w_2, \ldots, w_n$,

$$w_j = \sum_{k=1}^{n} p_{jk} u_k \quad j = 1, 2, \ldots, n$$

定 $P = [p_{jk}]$, 則 L 所對應的方陣是 PAP^{-1}。

一向量空間中最重要的代數運算除向量加法以及純量乘法外, 就算內積(inner procuct) 了。內積把兩個向量映到純量, 是一雙線性函數。以 (v_1, v_2) 表示兩向量 v_1 與 v_2 的內積, 則對任意純量 α, β,

$$\begin{aligned} <\alpha u + \beta v, w> &= \alpha <u, w> + \beta <v, w>, \\ <u, \alpha v + \beta w> &= \bar{\alpha} <u, v> + \bar{\beta} <u, w> . \end{aligned}$$

利用向量的內積以及有名的 Cauchy-Schwartz 不等式

$$| < u, v > |^2 \le < u, u > < v, v >$$

可定出兩向量 u, v 的夾角 θ 爲

$$\cos\theta = < u, v > / < u, u >^{1/2} < v, v >^{1/2}$$

因而兩向量垂直的充要條件是內積爲零。

其實, 大部份的線性代數理論已見於高中的數學課程, 二維與三維向量空間見於高中的數學課程; 二維與三維向量空間見於高二的解析幾何學中, 矩陣與行列式的理論則見於高三理科數學。當然, 這基礎性的代數理論也引用於大學的相關課程。數論是代數的一主要分支, 自然處處可看到線性代數的痕

跡, 底下我們就從線性代數出發, 來引導出兩個數論上的重要主題。

A. Bernoulli 多項式

考慮定義在 $[0,1]$ 的平方可積分函數所形成的函數空間 $L^2([0,1])$, 其內積定義是

$$< f, g >= \int_0^1 f(x)\overline{g(x)}dx。$$

在這內積下, $L^2([0,1])$ 構成 一 Hilbert 空間, 亦即 complete inner product space。

在 $L^2([0,1])$ 中, 考慮

$$S = \{1, x, x^2, \ldots, x^n, \ldots\}.$$

S 是由 x 之所有單項式所集的集合, 這集合並非一垂直集合, 因

$$< x^i, x^j >= \int_0^1 x^{i+j}dx = \frac{1}{i+j+1} \neq 0.$$

但 Gram-Schmidt 步驟保證我們可以從 S 建構另一垂直集合 $T = \{B_0(x), B_1(x), \ldots, B_n(x), \ldots\}$ 使得 $B_n(x)$ 的次數是 n 且其領導係數是 1; 其建構方法如下:

$$\begin{aligned}
B_0(x) &= 1, \\
B_1(x) &= x - < x, 1 >= x - \frac{1}{2}, \\
B_2(x) &= x^2 - \frac{B_1(x)}{< B_1, B_1 >} < x^2, B_1(x) > \\
&\quad - < x^2, 1 > \\
&= x^2 - x + \frac{1}{6},
\end{aligned}$$

由這樣導出的一系列多項式 $B_0, B_1(x), \ldots B_n(x), \ldots$, 即是數論上有名的 Bernoulli 多項式。在數論上, 這些多項式是由一特殊函數的級數展開而得出, 即

$$\frac{te^{xt}}{e^t - 1} = \sum_{n=0}^{\infty} \frac{B_n(x)t^n}{n!}, \quad |t| < 2\pi.$$

若先定 Bernoulli 數爲

$$\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} \frac{B_n t^n}{n!}, \quad |t| < 2\pi.$$

則

$$B_n(x) = \sum_{k=0}^{n} \binom{n}{k} B_k x^{n-k}$$

這的確是領導係數是 1 的 n 次多項式, 而 $B_n(x)$ 的常數項 $B_n(0) = B_n$。

Bernoulli數與 Bernoulli 多項式在數論上出盡鋒頭; 早 在 18世 紀 中 葉, Euler 即 能 用 Bernoulli 數表示出 Riemann Zeta函數在偶數的取值。Riemann Zeta 函數的定義是

$$\varsigma(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \quad \text{Re } s > 1.$$

Euler所得到的式子是

$$\varsigma(2m) = \frac{(-1)^{m-1}(2\pi)^{2m}B_{2m}}{2(2m)!},$$

特別是

$$1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{n^2} + \cdots = \frac{\pi^2}{6},$$
$$1 + \frac{1}{2^4} + \frac{1}{3^4} + \cdots + \frac{1}{n^4} + \cdots = \frac{\pi^4}{90}.$$

Bernoulli數也自然出現在古 典的 Poisson Maclaurin 求和公式裡: 若 $f \in S([0,\infty))$ 則

$$\sum_{n=1}^{\infty} f(n) = \int_0^{\infty} f(x)dx + \sum_{r=0}^{\infty} \frac{(-1)^r B_{r+1}}{(r+1)!} f^{(r)}(0)$$

這裡 $S([0,\infty))$ 表示由滿足對所有整數 n,

$$\lim_{\lambda \to \infty} \lambda^n |f^{(r)}(\lambda)| = 0$$

的所有無窮可微分之函數 f 所構成的函數空間。另一方面, Bernoulli多項式也是一些級數的取值:

$$\sum_{n=1}^{\infty} \frac{\cos 2\pi nx}{(2\pi n)^{2m}} = \frac{(-1)^{m-1}B_{2m}(x)}{2(2m)!}, \quad |x|<1,\ m\geq 1.$$

$$\sum_{n=1}^{\infty} \frac{\sin 2\pi nx}{(2\pi n)^{2m+1}} = \frac{(-1)^{m+1}B_{2m+1}(x)}{2(2m)!}, \quad |x|<1,\ m\geq 0.$$

當然從上面的表現式, 可很快看出 Bernoulli 多項式彼此之間的垂直性, 而這又回到了線性代數。

B. 二階方陣與模型群

在線性代數中, 每一 $\mathcal{R}^n$ 到本身的線性轉換都可表爲 $n \times n$ 的實方陣 $A = [a_{ij}]_{1\leq i,j\leq n}$ 而這線性轉換可逆的充要條件是 $\det A \neq 0$。現考慮行列式值是 1 的 2×2 實方陣

$$SL_2(\mathcal{R})=\left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \Big| a,b,c,d \in \mathcal{R},\ ad\text{–}bc\text{=}1 \right\}$$

$SL_2(\mathcal{R})$ 構成一乘法群, 而稱爲特別線性群, 其子群

$$SL_2(\mathcal{Z})=\left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \Big| a,b,c,d \in \mathcal{Z},\ ad\text{–}bc\text{=}1 \right\}$$

在數論上被稱爲模型群(modular group)。這群的生成元是

$$S=\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \quad 與 \quad T=\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

模型群及其子群在模型式理論上扮演了極其重要的角色。現舉出其中之一。

對任意複數平面上的方格點

$$L=\{uw_1+vw_2 | u,v\in\mathcal{Z}\}=\mathcal{Z}w_1+\mathcal{Z}w_2,$$

其中 $w_1,\ w_2,\ 0$ 在複數平面上不共線且 $\mathrm{Im}\ w_1/w_2>0$。在

$$\sigma:\begin{cases} w_1 \longrightarrow aw_1+bw_2 \\ w_2 \longrightarrow cw_1+dw_2 \end{cases}, \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathcal{Z})$$

的模型變換下, 很明顯有 $\sigma(L)=L$ 且 $\sigma(0)=0$, 其逆轉換是

$$\sigma^{-1}:\begin{cases} w_1 \longrightarrow dw_1-bw_2, \\ w_2 \longrightarrow -cw_1+aw_2. \end{cases}$$

因而函數

$$G_k(L) = G_k(w_1,w_2)=\sum_{\lambda\in L,\lambda\neq 0}\lambda^{-k}$$
$$, k\geq 4 \text{ 是偶數}$$

滿足對所有模型轉換 σ

$$G_k(\sigma(L))=G_k(L)。$$

亦即對任意 $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathcal{Z})$,

$$G_k(aw_1+bw_2, cw_1+dw_2)=G_k(w_1,w_2)。$$

現令 $z=w_1/w_2$ 且

$$G_k(z) = w_2^k G_k(w_1,w_2) = \sum_{(c,d)\in\mathcal{Z}^2-(0,0)}(cz+d)^{-k}$$

則有

$$G_k\left(\frac{az+b}{cz+d}\right)=(cz+d)^k G_k(z)。$$

這 $G_k(z)$ 即是權爲 k 的模型式, 被稱爲 Eisenstin 級數。

利用複數平面上的同一方格點 L 也可建構另一有名的雙週期函數 − Weierstrass $\wp$− 函數

$$\wp(z,L)=\frac{1}{z^2}+\sum_{\lambda\in L,\lambda\neq 0}\left[\frac{1}{(z-\lambda)^2}-\frac{1}{\lambda^2}\right]$$

利用 $|z|<\lambda$ 時,

$$\begin{aligned}\frac{1}{(z-\lambda)^2} &= \frac{1}{\lambda^2}\left[\frac{1}{(1-z/\lambda)^2}\right]\\ &= \frac{1}{\lambda^2}\left(1+2\left(\frac{z}{\lambda}\right)+3\left(\frac{z}{\lambda}\right)^2\right.\\ &\quad \left.+\cdots+n\left(\frac{z}{\lambda}\right)^{n-1}+\cdots\right),\end{aligned}$$

得出 $\wp(z,L)$ 在 $z=0$ 附近的冪級數展開式爲

$$\begin{aligned}\wp(z,L) &= \frac{1}{z^2}+3G_4(L)z^2+5G_6(L)z^4\\ &\quad +\cdots+(2n-1)G_{2n}(L)z^{2n-2}+\cdots,\end{aligned}$$

設 $X=\wp(z,L)$, $Y=\wp'(z,L)$ 注意到

$$F(z)=Y^2-(4X^3-60\,G_4(L)X-140\,G_6(L))$$

在 $z=0$ 附近的展開式中不再含有 z 的負次項, 因而是 z 的解析函數, 而 $F(z)$ 又是一雙週期函數 故必是一全純函數, 其唯一可能是常函數。由此得出

$$Y^2=4X^3-60\,G_4(L)X-140\,G_6(L)。$$

上面方程式定義一同構於 $\mathcal{C}/L$ 的橢圓曲線。

橢圓曲線的理論因 Wiles 聲明證明 Taniyama-Shimura-Weil猜測而再度被炒熱, 這猜測斷言所有的半穩定橢圓曲線都是模型曲線。若這猜測成立, 則Fermat 最後定理也跟著成立, 對於 Fermat 最後定理的新近發展, 請參考 [1,2,3]。

對於給定的橢圓曲線

$$E: y^2=x^3+ax^2+bx+c,\quad a,b,c\in\mathcal{Q},$$

如何分辨 E 是否是模型曲線呢? 方法之一是考慮這橢圓曲線的 Hasse-Weil L-函數, 這是一具有無窮乘積的 Zeta 函數, 若這函數對應到一模型式的 Zeta 函數, 則稱這曲線是一模型曲線。底下我們說明模型式的 Zeta 函數以及 Hasse-Weil L-函數的建構方法。

一模型式 $f(z)$ 滿足轉換式

$$f\left(\frac{az+b}{cz+d}\right)=(cz+d)^k f(z),\ \begin{bmatrix}a & b\\ c & d\end{bmatrix}\in SL_2(\mathcal{Z})$$

特別是 $f(z+1)=f(z)$, 故 f 是一特別的週期函數, 而有 Fourier 展開式

$$f(z)=\sum_{n=-\infty}^{\infty}a_n e^{2\pi inz}。$$

實際上, Fourier 係數 a_n 在 $n<0$ 時皆爲零。即 f 的 Fourier 展開式形式是

$$f(z)=\sum_{n=0}^{\infty}a_n e^{2\pi inz},$$

定義 f 所對應的 Zeta 函數是

$$Z(f;s)=\sum_{n=1}^{\infty}a_n n^{-s},$$

如以 $G_k(z)$ 爲例, 其 Fourier 展開式是

$$G_k(z)=-\frac{B_k}{2k}+\sum_{n=1}^{\infty}\left(\sum_{d|n}d^{k-1}\right)e^{2\pi inz},$$

而所對應的 Zeta 函數是

$$\sum_{n=1}^{\infty}\left(\sum_{d|n}d^{k-1}\right)n^{-s}=\zeta(s)\zeta(s-k+1)。$$

另一方面, 對任意質數 p 以及正整數 r, 以 N_r 表示方程式 $y^2 = x^3 + ax^2 + bx + c$ 在有限體 $\mathcal{F}_{p^r}$ 中解的個數, 這裡 $\mathcal{F}_{p^r}$ 表示具有 p^r 個元素的有限體。定義

$$Z(E/\mathcal{F}_f; T) = \exp\left(\sum_{r=1}^{\infty} N_r \frac{T^r}{r}\right),$$

亦即

$$\frac{d}{dT} Z(E/\mathcal{F}_p; T) = Z(E/\mathcal{F}_p; T)\left(\sum_{r=1}^{\infty} N_r T^{r-1}\right)$$

$Z(E/\mathcal{F}_r; T)$ 是 T 的有理函數, 對幾乎所有的質數 p,

$$Z(E/\mathcal{F}_p; T) = \frac{1 - a_{E,p}T + pT^2}{(1-T)(1-pT)}$$

而橢圓曲線 E 的 Hasse-Weil L-函數即定義爲

$$\prod_{p|N_E} (1 - a_{E,p}p^{-s})^{-1} \prod_{p\dagger N_E} (1 - a_{E,p}p^{-s} + p^{1-2s})^{-1}$$

其中 N_E 是橢圓曲線 E 的 conductor。

注意到 Hasse-Weil L-函數可表現爲無窮乘積, 但模型式的 Zeta 函數則不一定可表現爲無窮乘積, 其可表爲無窮乘積的充要條件是這模型式是 Hecke 算子的共同特徵函數。這裡的 Hecke 算子把權爲 k 的模型式映到權爲 k 的模型式, 定義是

$$T(n)f(z) = n^{k-1} \sum_{a\geq 1, ad=n} \sum_{0\leq b<d} d^{-k} f\left(\frac{az+b}{d}\right)$$

若存在有一複數 $\lambda(n)$ 使得對所有正整數 n,

$$T(n)f = \lambda(n)f,$$

則稱 f 是一共同特徵函數, 限制 f 的第一個 Fourier 係數是 1 時, 則 f 所對應的 Zeta 函數是

$$\prod_p (1 - a_p p^{-s} + p^{k-1-2s})^{-1}$$

設 p 是大於3的質數且設 Fermat 方程式 $x^p + y^p + z^p = 0$ 有不全爲零的非顯然解。取一組原始解 (a, b, c), 定 $A = a^p$, $B = b^p$ 且 $C = c^p$, 則橢圓曲線

$$E_{A,B}:\ y^2 = x(x - A)(x + B)$$

是一半穩定的橢圓曲線, 稱爲 Frey 曲線, 若 Taniyani-Shinura-Weil 猜測成立, 則 $E_{A,B}$ 背後有一權爲 2 的模型式, 使得$E_{A,B}$ 的 Hasse-Weil L-函數與這模型式的 Zeta 函數一樣, 但模型式的理論專家告訴我們根本沒有這樣的模型式, 這就推出 Fermat 最後定理成立。

參考資料

1. 余文卿, 費馬最後定理, 數學傳播 70, p.32-41, 1994。
2. 李文卿, 費馬最後定理: A.Wiles 的解決方法, 數學傳播 (70), p.42-66, 1994。
3. 余文卿, 費馬最後定理的過去, 現在與未來, 自然科學簡訊, p.19-21, 1995。
4. Neal Koblitz, Introduction to elliptic curver and modular forms, Springer-Verlag, 1984.
5. Richard O. Hill, Jr, Elementary linear algeba with applications Acalemic, Press, 1991.

—本文作者任教於國立中正大學數學系—