

超越数論における Mahler の方法

慶応理工 塩川 宇賢 (Iekata Shiohawa)

超越数論において Mahler の方法というのがある。非負整数を成分とする k 次正方行列 $Q = (w_{ij})$ と、
 $z = (z_1, \dots, z_k) \in \mathbb{C}^k$ に対して

$$\Omega z = \left(\prod_{j=1}^k z_j^{w_{1j}}, \dots, \prod_{j=1}^k z_j^{w_{kj}} \right) \quad (1)$$

とおく。いま関数 $f_1(z), \dots, f_n(z)$ があり、その z と Ωz での値がある種の関数方程式を満たすとする。Mahler の方法は、関数 $f_1(z), \dots, f_n(z)$ の $\mathbb{C}(z)$ 上代数的独立性からその代数的点での値の \mathbb{Q} 上代数的独立性を導こうとするもので 1929 ~ 30 年の Mahler の 3 つの論文にはじまる。例えば関数 $\sum_{r=0}^{\infty} z^r$ や $\sum_{r=0}^{\infty} [\omega] z^r$ ($\omega \in \mathbb{R} \setminus \mathbb{Q}$) の値はこの方法で扱える。1969 年になって Mahler は 3 つの問題を出し彼の方法を一般化することを提案した。以来 K. Kubota, Loxton, van der Poorten, Masser, 西岡等による多くの研究がある。最近の著しい結果は, Loxton-van der Poorten

による実代数的数の小数展開のランダムネスへの応用と、Masser の A vanishing theorem for power series. *Invent. Math.*, 67, 275-286 (1982) であろう。前者については、Mendes-France と釜江の講演を参照してほしい。このノートでは、Masser の定理が如何に強力なものであるかを彼の論文 *An algebraic independence theorem I* (未発表) に沿って紹介しよう。Mahler の方法は実に多くの関数に応用されるが、その最も典型的なのは次の関数である。

$$f(z) = \sum_{r=1}^{\infty} [\gamma \omega] z^r, \quad |z| < 1 \quad (2)$$

ω を実 2 次無理数とする。Mahler が $\alpha \in \overline{\mathbb{Q}}, 0 < |\alpha| < 1$, ならば $f(\alpha)$ が超越数であることを示し、Looten-van der Poorten は $\alpha_1, \dots, \alpha_n \in \overline{\mathbb{Q}}, 0 < |\alpha_i| < 1$, かつ $|\alpha_1|, \dots, |\alpha_n|$ が乗法的に独立ならば $f(\alpha_1), \dots, f(\alpha_n)$ が代数的に独立であることを証明した。ここで β_1, \dots, β_n が乗法的に独立とは、 $\beta_1^{\mu_1} \dots \beta_n^{\mu_n} = 1, \mu_i \in \mathbb{Z}$ が $\mu_1 = \dots = \mu_n = 0$ の時に限り成り立つこととする。Masser は彼の vanishing theorem を用いて、この条件を落すことに成功した。即ち、

定理 (Masser 1982) $\alpha_1, \dots, \alpha_n \in \overline{\mathbb{Q}}, 0 < |\alpha_i| < 1$ が相異なるならば $f(\alpha_1), \dots, f(\alpha_n)$ は代数的に独立である。

ω が一般の場合、問題はより難しくなる。 ω が有界な連分

数展開をもつ時, 超越性は Loxton-van der Poorten によって得られたが, 代数的独立性は Flicker による部分的結果しか知られていない。Masser はこの場合にも彼の方法を少し補足すれば定理が証明出来るとのべている。 ω の連分数展開が非有界の時, 超越性は容易だが代数的独立性が意外に難しい。今の所, $\alpha_1, \dots, \alpha_n \in \mathbb{Q}, 0 < |\alpha_1| < |\alpha_2| < \dots < |\alpha_n| < 1$ 即ち絶対値が相異なるという強い条件のもとでしか云えない。

最後に相異なる ω に対応する $f(z)$ の値の代数的独立性は今まで全く手がつかなかったが, Masser によれば $\pm\omega_1, \dots, \pm\omega_n$ が $\text{mod } \mathbb{Z}$ で相異なる時, $\alpha \in \mathbb{Q}, 0 < |\alpha| < 1$ に対して $\sum_{r=1}^{\infty} [r\omega_1] \alpha^r, \dots, \sum_{r=1}^{\infty} [r\omega_n] \alpha^r$ は代数的に独立である。但し証明には別のタイプの vanishing theorem が必要である。

Masser の定理の証明をスケッチしよう。 $\lambda > 0$ に対して

$$f(\lambda; x, y) = \sum_{r=1}^{\infty} \sum_{s=1}^{[r\lambda]} x^r y^s$$

とおくと $f(z) = f(\omega; z, 1)$. $f(\lambda; x, y)$ は x, y の関数として領域 $|x| < 1, |x||y|^\lambda < 1$ で正則かつ関数等式

$$f(\lambda+a; x, y) = f(\lambda; xy^a, y) + \frac{xy(1-y^a)}{(1-x)(1-y)(1-xy^a)} \quad (3)$$

$$f(\lambda^{-1}; x, y) = -f(\lambda; y, x) + \frac{xy}{(1-x)(1-y)} \quad (4)$$

を満たす。更に (4) より領域 $|x| \cdot |y|^\lambda < 1$

に解析接続され, (3), (4) は夫々 $|x| \cdot |y|^{\lambda+1} < 1, |y| \cdot |x|^\lambda < 1$

で成り立つ。

(1) より $0 < \omega < 1$ と仮定してよい。 ω は 2 次無理数だから周期的連分数に展開される。即ち

$$\omega = [0; a_1, a_2, \dots, a_{j-1}, a_j, a_{j+1}, \dots, a_{j+l}]$$

$$\text{そこで } \omega_r = [0; a_{r+1}, a_{r+2}, \dots] \quad (r \geq 1), \quad \omega_0 = \omega,$$

$$x = \omega_j = \omega_{j+l} = \omega_{j+2l} = \dots$$

とおくと (3), (4) より

$$f(\omega_{r-1}; x, y) \equiv -f(\omega_r; x^{a_r} y, x) \pmod{\bar{\mathbb{Q}}(x, y)}$$

但し $\bar{\mathbb{Q}}(x, y)$ は x, y の \mathbb{Q} 係数有理関数体。これより

$$f(\omega; x, y) \equiv (-1)^j f(x; x^p y^q, x^r y^s) \pmod{\bar{\mathbb{Q}}(x, y)} \quad (5)$$

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix} = \begin{pmatrix} a_j & 1 \\ 1 & 0 \end{pmatrix} \dots \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix}$$

$$f(x; x, y) \equiv (-1)^l f(x; x^a y^b, x^c y^d) \pmod{\bar{\mathbb{Q}}(x, y)} \quad (6)$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a_{j+l} & 1 \\ 1 & 0 \end{pmatrix} \dots \begin{pmatrix} a_{j+1} & 1 \\ 1 & 0 \end{pmatrix} \quad (7)$$

さて (5) より $f(d_i) = f(\omega; d_i, 1)$, $1 \leq i \leq n$ の代数的独立性を示すには, $f(x; d_i^p, d_i^r)$, $1 \leq i \leq n$ のそれを云えばよい。(厳密には $(x, y) = (d_i, 1)$ が $f(\omega; x, y) - (-1)^j f(x; x^p y^q, x^r y^s) \in \bar{\mathbb{Q}}(x, y)$ の極にならない事を確かめる必要があるが ---。) 今, d_1, \dots, d_n を乗法的に独立な数の単項式で表わす。

Lemma (Loxton-van der Poorten), 任意の $d_1, \dots, d_n \in \bar{\mathbb{Q}}$, $0 < |d_i| < 1$, に対して, 1 の累乗根 S_1, \dots, S_n 乗法的に独立な

$\beta_1, \dots, \beta_m \in \bar{\mathbb{Q}}, 0 < |\beta_i| < 1$, 及 w m 変数の単項式 M_1, \dots, M_n が存在し $\alpha_i = S_i M_i(\beta_1, \dots, \beta_m), 1 \leq i \leq n$ と書ける。

そこで新しい変数 $x = (x_1, \dots, x_m), y = (y_1, \dots, y_m), z = (x_1, y_1, \dots, x_m, y_m) \in \mathbb{C}^{2m}$ を用い n 個の関数

$$f_i(z) = f(x; S_i^P M_i(x), S_i^R M_i(y)), 1 \leq i \leq n \quad (8)$$

を定義すれば

$$f(x; \alpha_i^P, \alpha_i^R) = f_i(z_0), z_0 = (\beta_1^P, \beta_1^R, \dots, \beta_m^P, \beta_m^R). \quad (9)$$

これで問題は 1 つの関数 $f(z)$ の n 個の点 $\alpha_1, \dots, \alpha_n$ における値の代数的独立性から n 個の関数 $f_1(z), \dots, f_n(z)$ の 1 点 z_0 における値の代数的独立性に置き換えられた。しかも z_0 の座標は無法的独立性をもつ。

まず各 $f_i(z)$ がある種の関数方程式を満足することを示す。簡単のため i を取り除き

$$f(z) = f(x; S^P M(x), S^R M(y))$$

とおく。(7) で定義された a, b, c, d によって

$$\textcircled{H} z = (x_1^a y_1^b, x_1^c y_1^d, \dots, x_m^a y_m^b, x_m^c y_m^d)$$

と定義すれば, 正整数 h が存在して

$$f(z) \equiv (-1)^{hl} f(\textcircled{H}^h z) \pmod{\bar{\mathbb{Q}}(z)} \quad (10)$$

実際, $f(i, j; z) = f(x; S^i M(x), S^j M(y))$ とおくと (6) より

$$f(i, j; z) \equiv (-1)^l f(ia+jb, ic+jd; \textcircled{H} z) \pmod{\bar{\mathbb{Q}}(z)} \quad (11)$$

ここで $\begin{pmatrix} ia+jb \\ ic+jd \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} i \\ j \end{pmatrix}$ に注意。今 N を $S^N = 1$ なる

正整数とすると $N^k + 1$ 個の行列 $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^r$ ($0 \leq r < N^k$) のうち
 少くとも 2 個は $\text{mod } N$ で成分ごとに等しい。しかも (7) より
 $\det \begin{pmatrix} a & b \\ c & d \end{pmatrix}^r = \pm 1$ 。よって $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^h \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N}$

なる正整数 h がある。 $f_i(z_j; z)$ の定義において i, j は
 $\text{mod } N$ で考えればよいから (11) を h 回繰り返せば (10) が出る。

さて $(S, M) = (S_i, M_i)$ とすると、正整数 h_i が存在して
 (10) が $h = h_i$ として $f_i(z)$ に対して成り立つ。 h を $h_1, \dots,$
 h_n の偶の公倍数とし、 $\Omega z = \bigoplus_{i=1}^n H_i z$ とおけば、

$$f_i(z) = f_i(\Omega z) + R_i(z), \quad 1 \leq i \leq n. \quad (12)$$

この型の関数方程式系には次の定理が適用出来る。

Laxton-van der Poorten の定理 $\Omega = (\omega_{ij})$ を非負整数を成分とする $R \times R$ 正則行列で、スペクトル半径 (即ち固有値の絶対値の最大値 - Frobenius の定理からそれ自身 1 つの固有値になる) に属する (各成分が) 正の固有ベクトルをもち、かつ 1 の累乗根を固有値としてもたないとする。 $z = (z_1, \dots, z_k)$ に対し (1) によって Ωz を定義する。 $f_1(z), \dots, f_n(z)$ は $z=0$ の近傍で代数的数を係数としてテーラー展開され、次の関数等式を満たす。

$f_i(z) = a_i f(\Omega z) + b_i(z), \quad 1 \leq i \leq n, \quad a_i \in \bar{\mathbb{Q}}, \quad b_i(z) \in \bar{\mathbb{Q}}(z)$
 $z \in \bar{\mathbb{Q}}^k$ は $f_1(z), \dots, f_n(z)$ 及び $b_i(\Omega^j z)$ ($1 \leq i \leq n, j \geq 0$) の正則点で $z=0$ のある近傍 $U(\Omega)$ に属し、次の性質 (A)

ない。(それ自体面白いが、少し粗^まくなるので省く。)しかし本質的な困難は (A) の証明であり、そのための Masser 以前には " $|d_1|, \dots, |d_n|$ が乗法的に独立" という条件が落とせなかった。(A) の証明はいわゆる vanishing theorem であって、 $f(z)$ を $z=0$ の近傍で正則な関数、 $\Omega^j z_0 \rightarrow 0$ ($j \rightarrow \infty$) とするとき $\phi(\Omega^j z_0) = 0$ ($\forall j > j_0$) が $\phi(z)$, Ω , z_0 の如何なる条件のもとで成り立つかを特徴づけることである。これが Maher の問題 1 であって、次の Masser の定理はその完全な解答といえよう。

Masser の vanishing theorem $k \geq 1$. Ω は非負整数を成分とする $k \times k$ 正則行列で 1 の累乗根を固有値としてもたない。 $z_0 \in \bar{\mathbb{Q}}^k$ の各座標は 0 でなく $\Omega^j z_0 \rightarrow 0$ ($j \rightarrow \infty$) とする。この時、次の 2 条件は同値である。

(i) \mathbb{C}^k の原点で正則な関数 $\phi(z)$ が存在して $\phi(\Omega^j z_0) = 0$
($\forall j > j_0$)

(ii) 2 つの k 変数の単項式 M_1, M_2 が存在して $M_1(\Omega^j z_0) = M_2(\Omega^j z_0)$ がある算術級数に属するすべての j に対して成り立つ。

(A) の証明。今 z_0 が (A) をみたさないとする、上定理より 2 つの相異なる単項式 M_1, M_2 が存在し

$$M_1(\Omega^j z_0) = M_2(\Omega^j z_0) \quad (13)$$

が少なくとも2つの $j = g, j = g + e$ ($g \geq 0, e \geq 1$) で成り立つ。(A)の証明にはこれで十分。) そこで

$$M_1(\Omega^g \mathbb{Z}) / M_2(\Omega^g \mathbb{Z}) = x_1^{i_1} y_1^{j_1} \cdots x_m^{i_m} y_m^{j_m},$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{ke} = \begin{pmatrix} t & u \\ v & w \end{pmatrix} \text{ とおけば (13) より.}$$

$$\beta_1^{i_1 P + j_1 r} \cdots \beta_m^{i_m P + j_m r} = 1$$

$$\beta_1^{i_1 (Pt + ru) + j_1 (Pv + rw)} \cdots \beta_m^{i_m (Pt + ru) + j_m (Pv + rw)} = 1.$$

β_1, \dots, β_m の乗法的独立性より

$$i_\mu P + j_\mu r = i_\mu (Pt + ru) + j_\mu (Pv + rw) = 0, \quad 1 \leq \mu \leq m.$$

しかも (i_μ, j_μ) の中の少なくとも1つは $(0, 0)$ ではない。よって $\begin{pmatrix} P \\ r \end{pmatrix}$ と $\begin{pmatrix} Pt + ru \\ Pv + rw \end{pmatrix} = \begin{pmatrix} t & u \\ v & w \end{pmatrix} \begin{pmatrix} P \\ r \end{pmatrix}$ とは1次従属。即ち $\begin{pmatrix} t & u \\ v & w \end{pmatrix}$ は有理数の固有値をもつ。しかし(7)よりこれは不可能である。これで(A)が云えた。

最後に ω が非有界な連分展開をもつ場合について補足しておく。この場合には Mahler の方法が使えそうにない。そこで(5), (6)を用いて

$$\sum_{r=0}^{\infty} [rw] z^r = \sum_{n=0}^{\infty} (-1)^n \frac{z^{i_n + j_n - 1}}{(1 - z^{i_n})(1 - z^{j_n - 1})}$$

と展開する。 a_n が非有界であるから右辺の級数は、超越性や代数的独立性に関する限り *Lacunary series* と思ってよい。従って超越性は容易に出る。しかし代数的独立性は全く別である。例えば次の問題はどうかだろうか。

問題 $\alpha_1, \dots, \alpha_n \in \overline{\mathbb{Q}}, 0 < |\alpha_i| < 1$ とする時 n 個の数 $\sum_{k=1}^{\infty} \alpha_1^{k!}, \dots, \sum_{k=1}^{\infty} \alpha_n^{k!}$ は $\alpha_1, \dots, \alpha_n$ の如何なる条件のもとで代数的に独立となるか?

Liouville 数 $\sum_{k=1}^{\infty} 10^{-k!}$ の印象からこの種の問題がもう済んだと思うのは早合点である。