数理解析研究所講究録
496巻 1983年 86-95


# 超越数論におけるMahlerの方法

慶応理工 塩川 宇賢 (Iekata Shiokawa)

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 $\Omega=(\omega_{ij})$ と,
$\underline{z}=(z_1,\cdots,z_k)\in\mathbb{C}^k$ に対して

$$\Omega\underline{z}=\left(\prod_{j=1}^{k}z_j^{\omega_{1j}},\cdots,\prod_{j=1}^{k}z_j^{\omega_{kj}}\right) \qquad (1)$$

とおく。いま関数 $f_1(\underline{z}),\cdots,f_n(\underline{z})$ があり, その $\underline{z}$ と $\Omega\underline{z}$ 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 $f_1(\underline{z}),\cdots,f_n(\underline{z})$ の $\mathbb{C}(\underline{z})$ 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 $\sum_{r=0}^{\infty}z^{2^r}$ や $\sum_{r=0}^{\infty}[r\omega]z^r$ $(\omega\in\mathbb{R}\setminus\mathbb{Q})$ 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。

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

$\omega$ 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、Loxton-van der Poorten は $\alpha_1, \cdots, \alpha_n \in \overline{\mathbb{Q}}$, $0 < |\alpha_i| < 1$, かつ $|\alpha_1|, \cdots, |\alpha_n|$ が乗法的に独立ならば $f(\alpha_1), \cdots, f(\alpha_n)$ が代数的に独立であることを証明した。ここで $\beta_1, \cdots, \beta_n$ が乗法的に独立とは、$\beta_1^{\mu_1} \cdots \beta_n^{\mu_n} = 1$, $\mu_i \in \mathbb{Z}$ が $\mu_1 = \cdots = \mu_n = 0$ 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) $\alpha_1, \cdots, \alpha_n \in \overline{\mathbb{Q}}$, $0 < |\alpha_i| < 1$ が相異なるならば $f(\alpha_1), \cdots, f(\alpha_n)$ は代数的に独立である。

$\omega$ が一般の場合、問題はより難しくなる。$\omega$ 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。$\omega$ 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，$\alpha_1, \cdots, \alpha_n \in \overline{\mathbb{Q}}$, $0<|\alpha_1|<|\alpha_2|<\cdots<|\alpha_n|<1$ 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 $\omega$ 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 $\pm\omega_1, \cdots, \pm\omega_n$ が $\bmod \mathbb{Z}$ で相異なる時，$\alpha \in \overline{\mathbb{Q}}$, $0<|\alpha|<1$ に対して $\sum_{r=1}^{\infty} [r\omega_1]\alpha^r, \cdots, \sum_{r=1}^{\infty} [r\omega_n]\alpha^r$ 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

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

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

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）はまた $|x|\cdot|y|^{\lambda+1}<1$, $|y|\cdot|x|^{\lambda}<1$

で成り立つ。

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

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

ここで $\omega_r=[0;a_{r+1},a_{r+2},\cdots]$ $(r\geqq 1)$, $\omega_0=\omega$,

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

とおくと (3), (4) より

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

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

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

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

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

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

さて (5) より $f(\alpha_i)=f(\omega;\alpha_i,1)$, $1\leq i\leq n$ の代数的独立性を示すには, $f(x;\alpha_i^p,\alpha_i^r)$, $1\leq i\leq n$ のそれを云えばよい。(厳密には $(x,y)=(\alpha_i,1)$ が $f(\omega;x,y)-(-1)^j f(x;x^p y^q, x^r y^s)\in\overline{\mathbb{Q}}(x,y)$ の極にならない事を確かめる必要があるが $\cdots$。)

今, $\alpha_1,\cdots,\alpha_n$ 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 $\alpha_1,\cdots,\alpha_n\in\overline{\mathbb{Q}}$, $0<|\alpha_i|<1$, に対して, 1の累乗根 $\zeta_1,\cdots,\zeta_n$ 乗法的に独立な

$\beta_1, \cdots, \beta_m \in \overline{\mathbb{Q}}$, $0<|\beta_i|<1$, 及び $m$ 変数の単項式 $M_1, \cdots, M_n$ が存在し $\alpha_i = \zeta_i M_i(\beta_1, \cdots, \beta_m)$, $1 \le i \le n$ と書ける。

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

$$f_i(\underline{z}) = f(X; \zeta_i^p M_i(\underline{x}), \zeta_i^r M_i(\underline{y})), \quad 1 \le i \le n \qquad (8)$$

を定義すれば

$$f(X; \alpha_i^p \alpha_i^r) = f_i(\underline{z}_0), \quad \underline{z}_0 = (\beta_1^p, \beta_1^r, \cdots, \beta_m^p, \beta_m^r). \qquad (9)$$

これで問題は1つの関数 $f(\underline{z})$ の $n$ 個の点 $\alpha_1, \cdots, \alpha_n$ における値の代数的独立性から $n$ 個の関数 $f_1(\underline{z}), \cdots, f_n(\underline{z})$ の1点 $\underline{z}_0$ における値の代数的独立性に置き換えられた。しかも $\underline{z}_0$ の座標は乗法的独立性をもつ。

まず各 $f_i(\underline{z})$ 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

$$f(\underline{z}) = f(X; \zeta^p M(\underline{x}), \zeta^r M(\underline{y}))$$

とおく。(7) で定義された $a, b, c, d$ によって

$$\text{Ⓗ}\underline{z} = (x_1^a y_1^b, x_1^c y_1^d, \cdots, x_m^a y_m^b, x_m^c, y_m^d)$$

と定義すれば，正整数 $h$ が存在して

$$f(\underline{z}) \equiv (-1)^{hl} f(\text{Ⓗ}^h \underline{z}) \mod \overline{\mathbb{Q}}(\underline{z}) \qquad (10)$$

実際. $f(i, j; \underline{z}) = f(X; \zeta^i M(\underline{x}), \zeta^j M(\underline{y}))$ とおくと (6) より

$$f(i, j; \underline{z}) \equiv (-1)^l f(ia+jb, ic+jd; \text{Ⓗ}\underline{z}) \mod \overline{\mathbb{Q}}(\underline{z}) \qquad (11)$$

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 $\zeta^N = 1$ なる

正整数とすると $N^4+1$ 個の行列 $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^r$ $(0 \leq r \leq N^4)$ のうち少くとも2個は $\bmod N$ 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 $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^h \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod N$ なる正整数 $h$ がある。$f(i,j;z)$ の定義において $i, j$ は $\bmod N$ で考えればよいから(11)を $h$ 回繰り返せば(10)が出る。

さて $(\zeta, M) = (\zeta_i, M_i)$ 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 $h_1, \cdots, h_n$ の個の公倍数とし，$\Omega z = \textcircled{H}^h z$ とおけば，

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

この型の関数方程式系には次の定理が適用出来る。

Lox ton - van der Poorten の定理　$\Omega = (\omega_{ij})$ を非負整数を成分とする $k \times k$ 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。$z = (z_1, \cdots, z_k)$ に対し(1)によって $\Omega z$ を定義する。$f_1(z), \cdots, f_n(z)$ 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。

$f_i(z) = a_i f(\Omega z) + b_i(z)$, $1 \leq i \leq n$, $a_i \in \bar{\mathbb{Q}}$, $b_i(z) \in \bar{\mathbb{Q}}(z)$.
$z_0 \in \bar{\mathbb{Q}}^k$ は $f_1(z), \cdots, f_n(z)$ 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)

をみたす。(A) $\xi=0$ の近傍で正則な任意の関数 $\phi(\xi)\not\equiv 0$ に対し $\phi(\Omega^j\xi_0)\neq 0$ が無限個の $j$ に対して成り立つ。(ここで $U(\Omega)$ の定義は省くが、一口で云って $\xi\in U(\Omega)$ ならば $\Omega^j\xi$ の各成分の絶対値は $j\to\infty$ なるとき $\rho^{r^j}$ $(0<\rho<1)$ の order で0に近づくことが保証される。ここで $r$ は $\Omega$ のスペクトル半径で1より大。) 以上の諸条件のもとで、もし $f_1(\xi),\cdots,f_m(\xi)$ が $\mathbb{C}(\xi)$ 上代数的に独立ならば $f_1(\xi_0),\cdots,f_m(\xi_0)$ は代数的に独立である。

証明は例によって結論を否定し補助関数をつくる。それが $\Omega^j\xi_0$ でとる値で数列 $\zeta_j\in\overline{\mathbb{Q}}$ を定義する。$\zeta_j$ は $j\to\infty$ なるとき十分速く0に収束するが、背理法の仮定より $|\zeta_j|\neq 0$ はそんなに小さくない。よって $\zeta_j=0$ $(\forall j>j_0)$。
他方 (A) より $\zeta_j\neq 0$ が無限回起り矛盾。

(8) で定義された関数 $f_1(\xi),\cdots,f_m(\xi)$, $\xi=(x_1,y_1,\cdots,x_m,y_m)\in\mathbb{C}^{2m}$, $\Omega=\text{Ⓗ}^t$ 但し Ⓗ は $2m$ 次正方行列で

$$\text{Ⓗ}=\begin{pmatrix} a & b & & & 0 \\ c & d & & & \\ & & \ddots & & \\ & & & a & b \\ 0 & & & c & d \end{pmatrix},$$

方程式系 (12), (9) で定義された代数的点 $\xi_0$ がこの定理の諸条件を満足することをチェックすればよい。関数の代数的独立性と (A) 以外は特に問題はない。前者の証明は簡単では

ない。(それ自体面白いが、少し煩かくなるので省く。)しかし本質的な困難は(A)の証明であり、そのためMasser以前には"$|\alpha_1|, \cdots, |\alpha_n|$ が乗法的に独立"という条件が落せなかった。(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, $\Omega^j z_0 \to 0$ $(j \to \infty)$ とするとき $\phi(\Omega^j z_0) = 0$ $(\forall j > j_0)$ が $\phi(z)$, $\Omega$, $z_0$ 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Mahler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 $k \geq 1$. $\Omega$ 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 $\Omega^j z_0 \to 0$ $(j \to \infty)$ 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と、上定理より2つの相異なる単項式 $M_1, M_2$ が存在し

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

が少くとも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

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

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

$$\beta_1^{i_1p+j_1r}\cdots\beta_m^{i_mp+j_mr}=1$$

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

$\beta_1,\cdots,\beta_m$ 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 $(i_\mu, j_\mu)$ の中の少くとも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 $\begin{pmatrix}t & u\\ r & w\end{pmatrix}$ 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 $\omega$ が非有界な連分数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

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

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だろうか。

問題 $\alpha_1, \cdots, \alpha_n \in \overline{\mathbb{Q}}$, $0<|\alpha_i|<1$ とする時 $n$ 個の数 $\sum_{k=1}^{\infty} \alpha_1^{k!}, \cdots, \sum_{k=1}^{\infty} \alpha_n^{k!}$ は $\alpha_1, \cdots, \alpha_n$ 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。