Mahler-Manin 予想の解決と Mahler 関数

— Mahler の方法による超越性・代数的独立性の証明へのイントロダクション —

慶應義塾大学理工学部　田中 孝明 (Taka-aki Tanaka)

1　Mahler-Manin 予想について

モジュラー j 不変量 (或いは, 楕円モジュラー関数ともいう) $j(\tau)$ は, 上半平面 $\mathbb{H} = \{\tau \in \mathbb{C} \mid \mathrm{Im}\,\tau > 0\}$ で定義された正則関数[1]であり,

$$SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; a, b, c, d \in \mathbb{Z},\ ad - bc = 1 \right\}$$

の作用に関して不変である. すなわち, $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ の τ への作用を分数 1 次変換 $\sigma(\tau) = \dfrac{a\tau + b}{c\tau + d}$ により定義するとき 任意の $\sigma \in SL_2(\mathbb{Z})$ に対し $j(\sigma(\tau)) = j(\tau)$ をみたす. $SL_2(\mathbb{Z})$ は $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ により生成されるから, $j(\tau)$ は

$$j(\tau + 1) = j(\tau), \quad j\left(-\frac{1}{\tau}\right) = j(\tau)$$

をみたす関数であると定義しても同値である. 第 1 式より $j(\tau)$ は周期 1 をもつから, $z = e^{2\pi i \tau}$ の Fourier 級数に展開される :

$$j(\tau) = \frac{\left(1 + 240 \displaystyle\sum_{n=1}^{\infty} \frac{n^3 z^n}{1 - z^n}\right)^3}{z\left(\displaystyle\prod_{n=1}^{\infty}(1 - z^n)\right)^{24}} = \frac{1}{z} + 744 + \sum_{n=1}^{\infty} c(n) z^n. \tag{1}$$

以下, 本稿を通して (1) の右辺により原点の周りのローラン展開が与えられる解析関数を $J(z)$ と表す. $J(z)$ は $0 < |z| < 1$ で正則である. $c(n)$ はすべて正整数であり, 参考文献 [4] によると, $c(1) = 196884$, $c(2) = 21493760$, $c(3) = 864299970$, $c(4) = 20245856256$, $c(5) = 333202640600, \ldots$ である.

1937 年 Schneider は $\tau \in \mathbb{H}$ が 3 次以上の代数的数ならば $j(\tau)$ は超越数であることを証明した.

一方, 1969 年 Mahler は, $0 < |q| < 1$ をみたす代数的数 q に対して $J(q)$ は超越数であろうと予想した. また, 1971 年 Manin は, $J(z)$ を $\mathbb{C}_p$ 上の関数と考えた場合に上記と同様の結果が成立することを予想した. ただし, $\mathbb{C}_p$ は素数 p に対する p 進数体 $\mathbb{Q}_p$ の代数閉包の完備化である. これらを併

[1] $j(\tau)$ は $\mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$ で有理型である.

せて Mahler-Manin 予想と称する. この予想は K. Barré, G. Diaz, F. Gramain, G Philibert [1] により解決された:

定理 1. $0 < |q| < 1$ をみたす代数的数 q に対し $J(q)$ は超越数である.

[1] の証明は比較的長く self contained ではない部分もあったが, 天羽 雅昭 [3] により簡潔な証明が与えられた. 本稿の第 1 節から第 3 節では上記 Mahler の予想の証明を [3] にほぼ沿った形で解説する. 今回の講演に際し, 著書 [3] からの大幅な引用を快諾して下さった群馬大学工学部の天羽 雅昭先生への深い謝意をここに表したいと存じます.

2 証明のための準備

Mahler の方法による超越性・代数的独立性の証明には下記の基本不等式が用いられる. α を 0 でない代数的数, $n = [\mathbb{Q}(\alpha) : \mathbb{Q}]$, $\alpha^{(1)}(= \alpha), \alpha^{(2)}, \ldots, \alpha^{(n)}$ を α の共役とする. $\boxed{\alpha} = \max\{|\alpha^{(1)}|, |\alpha^{(2)}|, \ldots, |\alpha^{(n)}|\}$ と定義する. $d = \mathrm{den}(\alpha)$ とすると $N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(d\alpha) \in \mathbb{Z} \setminus \{0\}$ だから $1 \le |N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(d\alpha)| = d^n |\alpha^{(1)}||\alpha^{(2)}| \cdots |\alpha^{(n)}| \le d^n |\alpha| \boxed{\alpha}^{n-1}$. 故に,

$$|\alpha| \ge d^{-n} \boxed{\alpha}^{-n+1}.$$

両辺の対数をとると **Liouville** の基本不等式:

$$\log |\alpha| \ge -2n \max\{\log \boxed{\alpha}, \log \mathrm{den}(\alpha)\}$$

を得る.

補題 1 (A special case of Siegel's lemma)**.** $a_{ij} \in \mathbb{Z}$ $(i = 1, \ldots, r;\ j = 1, \ldots, 2r)$ は $|a_{ij}| \le A$ をみたすとする. ただし, $A \ge 1$. このとき, $x_1, \ldots, x_{2r}$ についての同次連立 1 次方程式 $\sum_{j=1}^{2r} a_{ij} x_j = 0 \quad (i = 1, \ldots, r)$ の非自明な整数解, 即ち, 少なくともひとつは 0 ではない $x_1, \ldots, x_{2r} \in \mathbb{Z}$ であって

$$|x_j| \le 2rA \qquad (j = 1, \ldots, 2r)$$

をみたすものが存在する.

この補題は Siegel's lemma の特別な場合であり, 証明は本報告集の若林 功 先生の「Thue の定理」を参照して頂きたい.

Mahler 予想の証明に用いる $j(\tau)$ の性質は次の 2 つである.

性質 1 (全射性) 写像 $j : \mathbb{H} \to \mathbb{C}$ は全射である.

性質 2 (モジュラー多項式) 任意の正整数 s に対し

$$\Phi_s(X) = \prod_{\substack{a,d \in \mathbb{N},\ ad=s, \\ b \in \mathbb{Z},\ 0 \le b \le d-1, \\ (a,b,d)=1}} \left(X - j\left(\frac{a\tau + b}{d} \right) \right) \tag{2}$$

とおく. このとき, X の多項式 $\Phi_s(X)$ の係数は $\mathbb{Z}[j]$ に属す. 従って, $\Phi_s(X) = \Phi_s(X, j) \in \mathbb{Z}[X, j]$. これを位数 s のモジュラー多項式という. (2) より $\Phi_s(j(s\tau), j(\tau)) = 0$. あるいは, $J(z)$ について書くと

$$\Phi_s(J(z^s), J(z)) = 0.$$

$\Phi_s(X) \in \mathbb{Z}[j][X]$ は $\mathbb{C}(j)$ 上既約である. $\psi(s) = \deg_X \Phi_s(X)$ は $\Phi_s(X)$ の定義より

$$\psi(s) = s \prod_{p|s} \left(1 + \frac{1}{p}\right)$$

で与えられることが分かる. ただし, 右辺の積は s のすべての素因数 p に亘る.

$$\prod_{p|s} \left(1 + \frac{1}{p}\right) \leq \sum_{k=1}^{s} \frac{1}{k} \leq 1 + \log s$$

だから

$$s \leq \psi(s) \leq s(1 + \log s). \tag{3}$$

今回の証明には, この粗い評価で十分である.

参考文献 [4] によると, 例えば,

$$\begin{aligned} \Phi_2(X, Y) &= -X^2Y^2 + X^3 + Y^3 + 2^4 \cdot 3 \cdot 31XY(X + Y) + 3^4 \cdot 5^3 \cdot 4027XY \\ &\quad -2^4 \cdot 3^4 \cdot 5^3(X^2 + Y^2) + 2^8 \cdot 3^7 \cdot 5^6(X + Y) - 2^{12} \cdot 3^9 \cdot 5^9 \end{aligned}$$

である. このように多項式 Φ_s の係数の絶対値は比較的大きいが, そのことは Mahler 予想の証明にはあまり影響を及ぼさない. しかし, $J(z)$ のローラン展開の係数 ($j(\tau)$ の Fourier 係数) $c(n)$ の増大度が大きいことは Mahler 予想の証明をやや複雑なものにしている. そこで, $J(z)$ と共通の性質を持ちながらテーラー展開の係数が比較的単純であり, 従って, Φ_s と比べ単純な関数方程式をみたす関数を例にとり, Mahler の方法による超越性の証明の骨格を説明する. $j(\tau)$ は実軸を自然境界とするから $J(z)(= J(e^{2\pi i\tau}))$ は単位円 $|z| = 1$ を自然境界としてもつ. 同様に 単位円を自然境界とする解析関数の例として Fredholm 級数

$$f(z) = \sum_{k=0}^{\infty} z^{d^k}$$

が知られている. ただし, d は 2 以上の整数である. 明らかに $f(z) \in \{0, 1\}[[z]]$ であり, 関数方程式

$$f(z) = f(z^d) + z$$

をみたす.

Proposition 1. $0 < |\alpha| < 1$ をみたす代数的数 α に対し $f(\alpha)$ は超越数である.

補題 **2.** Fredholm 級数 $f(z)$ は有理関数体 $\mathbb{C}(z)$ 上超越的である.

証明. 単位円 $|z| = 1$ が $f(z)$ の自然境界であることを示せば, $f(z)$ は代数関数 (の分枝) ではないから主張が従う. 任意に選んだ正整数 n に対し ζ を 1 の d^n 乗根のうちの任意のひとつとする.

$0 \le t < 1$ なる t に対し

$$f(t\zeta) = \sum_{k=0}^{n-1} (t\zeta)^{d^k} + \sum_{k=n}^{\infty} t^{d^k}$$

であるから $f(t\zeta)$ は $t \to 1-0$ のとき発散する. これは, $z = \zeta$ が $f(z)$ の特異点であることを意味する. このような ζ は単位円 $|z| = 1$ 上に稠密に分布するから, $f(z)$ は $|z| = 1$ の外部へは解析接続できない. 即ち, $|z| = 1$ は $f(z)$ の自然境界である. □

Prop. 1 の証明. m を正整数のパラメータとする. a_{ij} $(0 \le i, j \le m)$ を未知定数として

$$F(z) = \sum_{i=0}^{m} \sum_{j=0}^{m} a_{ij} z^i f(z)^j$$

とおく. $\mathrm{ord}_{z=0} F(z) > m^2$ をみたすよう a_{ij} を定める. 即ち,

$$F(z) = \sum_{l=0}^{\infty} b_l z^l$$

と冪級数で表したとき, a_{ij} についての整数係数の同次連立 1 次方程式

$$b_l = 0 \quad (l = 0, 1, \ldots, m^2)$$

をみたす a_{ij} を求める. 未知数 a_{ij} の個数 $(m+1)^2$ が方程式の個数 $m^2 + 1$ より大きいから非自明な有理数解 a_{ij} が存在する. 分母の最小公倍数を乗ずることにより a_{ij} は少なくともひとつは 0 ではない整数であるとしてよい. このような整数解 a_{ij} をとり固定すれば, 各 m に対して $F(z)(= F(z; m)) \in \mathbb{Z}[[z]]$ が定まり, 補題 2 より $F(z)$ は恒等的に 0 ではない.

Prop. 1 を背理法により証明する: $f(\alpha)$ は代数的数であると仮定する. $K = \mathbb{Q}(\alpha, f(\alpha))$ とおく. 以下, $c_1, c_2, \ldots$ は $\alpha, f(\alpha), f(z)$ のみに依存する正定数, $c_1(m), c_2(m), \ldots$ は $\alpha, f(\alpha), f(z)$ 及び m に依存する正定数とする. (このようにパラメータの依存関係を明確にしておくことが肝要である.) $f(z)$ のみたす関数方程式を繰り返し用いると $f(\alpha^{d^k}) = f(\alpha) - \alpha - \alpha^d - \cdots - \alpha^{d^{k-1}}$ が得られるから

$$F(\alpha^{d^k}) = \sum_{i=0}^{m} \sum_{j=0}^{m} a_{ij} \alpha^{d^k i} (f(\alpha) - \alpha - \alpha^d - \cdots - \alpha^{d^{k-1}})^j \in K$$

である. $c_1(m) = \max_{0 \le i,j \le m} |a_{ij}|$, $c_2 = \max\{\boxed{f(\alpha)}, \boxed{\alpha}, \mathrm{den}(\alpha)\} (> 1)$, $c_3 = c_2^2$ とすると, $k \ge c_4(m)$ のとき

$$\boxed{F(\alpha^{d^k})} \le (m+1)^2 c_1(m) c_2^{d^k m} \left((k+1) c_2^{d^{k-1}}\right)^m \le c_3^{d^k m},$$

$$\mathrm{den}\left(F(\alpha^{d^k})\right) \le c_2^{d^k m} \mathrm{den}\left(f(\alpha)\right)^m c_2^{d^{k-1} m} \le c_3^{d^k m}.$$

よって, Liouville の基本不等式より, $c_5 = 2[K : \mathbb{Q}] \log c_3$ とすると

$$\log |F(\alpha^{d^k})| \ge -2[K : \mathbb{Q}] d^k m \log c_3 \ge -c_5 d^k m \quad (k \ge c_4(m)). \tag{4}$$

次に, $\log |F(\alpha^{d^k})|$ の上界を求める. $N = \mathrm{ord}_{z=0} F(z) (> m^2)$ とすると $0 < |\alpha| < 1$ より

$$\lim_{k \to \infty} \alpha^{-d^k N} F(\alpha^{d^k}) = \lim_{k \to \infty} \sum_{l=0}^{\infty} b_{N+l} \alpha^{d^k l} = b_N$$

であるから $k \geq c_6(m)$ のとき $0 < |F(\alpha^{d^k})| \leq 2|b_N||\alpha|^{d^k N}$. よって, $c_7 = -\log|\alpha|$ とすると $N > m^2$ より

$$\log|F(\alpha^{d^k})| \leq \log 2 + \log|b_N| + d^k N \log|\alpha| \leq -c_7 d^k m^2 \quad (k \geq c_8(m)). \tag{5}$$

(4), (5) より $k \geq \max\{c_4(m), c_8(m)\}$ のとき $c_5 d^k m \geq c_7 d^k m^2$ となるから

$$c_5 c_7^{-1} \geq m.$$

最初から $m > c_5 c_7^{-1}$ なる m を選んで以上の議論を行えば矛盾である. □

注意 **(1)** 上記の証明を振り返ってみると m の選び方は

$$m > 4[K:\mathbb{Q}](-\log|\alpha|)^{-1} \log\max\{\boxed{f(\alpha)}, \boxed{\alpha}, \mathrm{den}(\alpha)\}$$

をみたすようにとれば十分であることが分かる.

(2) 上記の Mahler の方法は, 解析関数の特殊値が超越数であることを証明する方法の典型例である. 天羽先生の著書 [3] の 3.3 超越性の証明法 (22 頁 ~ 24 頁) において, このような証明のマインドが分かり易く解説されている.

補題 **3** (Mahler). $J(z)$ は有理関数体 $\mathbb{C}(z)$ 上超越的である.

証明 (解析的方法) z と $J(z)$ は $\mathbb{C}$ 上代数的独立であることを示せばよい. 変数変換し, $e^{2\pi i\tau}$ と $j(\tau)$ の代数的独立性を示す. 証明は背理法による. $P(x,y) = \sum_{k=0}^{m} P_k(x)y^k \in \mathbb{C}[x,y] \setminus \{0\}$ が存在して $P(e^{2\pi i\tau}, j(\tau)) = 0 \quad (\tau \in \mathbb{H})$ と仮定する. $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ を τ に作用させると,

$$\sigma(\tau) = \frac{a\tau + b}{c\tau + d} = \frac{a}{c} - \frac{1}{c(c\tau + d)}$$

より

$$P(e^{2\pi i a/c} e^{-2\pi i/c(c\tau+d)}, j(\tau)) = 0 \qquad (\tau \in \mathbb{H}). \tag{6}$$

ここで, $P_m(e^{2\pi i\theta}) \neq 0$ をみたす無理数 $\theta > 0$ をとり固定する. $\dfrac{p_n}{q_n} \to \theta \quad (p_n, q_n$ は互いに素な正整数) をみたす有理数列 $\{p_n/q_n\}_{n\geq 1}$ をとる. $p_n s_n - r_n q_n = 1$ をみたす $r_n, s_n \in \mathbb{Z}$ がとれるから

$$\begin{pmatrix} p_n & r_n \\ q_n & s_n \end{pmatrix} \in SL_2(\mathbb{Z}).$$

よって, (6) より

$$P(e^{2\pi i p_n/q_n} e^{-2\pi i/q_n(q_n\tau + s_n)}, j(\tau)) = 0 \qquad (\tau \in \mathbb{H}).$$

固定した τ ごとに $n \to \infty$ とすると,

$$\frac{1}{q_n(q_n\tau + s_n)} = \frac{1}{(q_n^2 \mathrm{Re}(\tau) + q_n s_n) + i(q_n^2 \mathrm{Im}(\tau))} \to 0$$

より

$$P(e^{2\pi i\theta}, j(\tau)) = \sum_{k=0}^{m} P_k(e^{2\pi i\theta}) j(\tau)^k = 0.$$

これが任意の $\tau \in \mathbb{H}$ に対して成り立つから, $j(\tau)$ が定数関数でないことと矛盾する. □

補題 **3** の証明 (代数的方法) 背理法による. $J(z) \in \mathbb{Q}((z))$ と考え

$$P(x,y) = \sum_{k=0}^{m} P_k(x)y^k = \sum_{l=0}^{n} Q_l(y)x^l \in \mathbb{C}[x,y] \setminus \{0\}$$

に対して

$$P(z, J(z)) = \sum_{k=0}^{m} P_k(z)J(z)^k = \sum_{l=0}^{n} Q_l(J(z))z^l = 0 \tag{7}$$

が成り立つと仮定する. 任意の正整数 s に対して $J_s(z) = J(z^s)$ とおき, 体 K_s を $K_s = \mathbb{C}(z, J, J_s)$ で定義する. これは $\mathbb{C}[[z]]$ の商体 $\mathbb{C}((z))$ の部分体である. 以下, 体の拡大次数 $[K_s : \mathbb{C}(J)]$ を 2 通りに評価することにより矛盾を導く.

まず, (7) より

$$[\mathbb{C}(z, J) : \mathbb{C}(J)] \leq n$$

であり, (7) に変換 $z \mapsto z^s$ を行うことにより

$$[K_s : \mathbb{C}(z, J)] \leq m$$

が分かる. よって,

$$[K_s : \mathbb{C}(J)] \leq [K_s : \mathbb{C}(z, J)][\mathbb{C}(z, J) : \mathbb{C}(J)] \leq mn.$$

他方, 関数方程式 $\Phi_s(J(z^s), J(z)) = 0$ 及び $\Phi_s(X, J)$ の $\mathbb{C}(J)$ 上での既約性より

$$[\mathbb{C}(J, J_s) : \mathbb{C}(J)] = \psi(s) \geq s$$

であるから

$$[K_s : \mathbb{C}(J)] \geq [\mathbb{C}(J, J_s) : \mathbb{C}(J)] \geq s.$$

以上より

$$s \leq mn.$$

s はいくらでも大きくとれるから, これは矛盾である. □

以下, $\tilde{J}(z) := zJ(z)$ とおく. さらに, 任意の正整数 k に対し

$$\tilde{J}(z)^k := \sum_{n=0}^{\infty} c_k(n)z^n$$

とおく. ただし, $c(n) = c_1(n+1)$ $(n = 1, 2, 3, \ldots)$ である.

補題 **4** (Mahler). $J(z)$ のみに依存する正定数 C_0 が存在して

$$0 \leq c_k(n) \leq e^{C_0\sqrt{kn}} \qquad (k = 1, 2, 3, \ldots;\ n = 0, 1, 2, \ldots)$$

が成り立つ.

証明. 以下, y は正の数を表す. (1) より

$$j(yi) = J(e^{-2\pi y}) = e^{2\pi y} + 744 + \sum_{n=1}^{\infty} c(n)e^{-2\pi yn}$$

だから, $c(n) > 0$ $(n \geq 1)$ に注意すると, $y \geq 1$ に対し

$$j(yi) \leq e^{2\pi y} + C \tag{8}$$

が成り立つ. ただし,

$$C = 744 + \sum_{n=1}^{\infty} c(n)e^{-2\pi n}$$

である. 同様にして, $0 < y \leq 1$ に対し

$$j(yi) = j\left(-\frac{1}{yi}\right) = j\left(\frac{1}{y}i\right) \leq e^{2\pi/y} + C. \tag{9}$$

また,

$$c_k(n)e^{-2\pi yn} \leq \tilde{J}(e^{-2\pi y})^k = (e^{-2\pi y}J(e^{-2\pi y}))^k = e^{-2\pi yk}j(yi)^k \tag{10}$$

である.

Case 1：$k \geq n$ のとき. (8), (10) より, $y \geq 1$ に対し

$$c_k(n)e^{-2\pi yn} \leq e^{-2\pi yk}(e^{2\pi y} + C)^k = (1 + Ce^{-2\pi y})^k.$$

これに $y = \sqrt{k/n} \geq 1$ を代入すると

$$c_k(n) \leq e^{2\pi\sqrt{kn}}\left(1 + Ce^{-2\pi\sqrt{k/n}}\right)^k$$

が得られる. $h = e^{2\pi\sqrt{k/n}}$ とおくと $\dfrac{k}{n} \leq h$ かつ $\left(1 + \dfrac{C}{h}\right)^h \leq e^C$ が成り立つから

$$\left(1 + \frac{C}{h}\right)^k \leq \left(1 + \frac{C}{h}\right)^{hn} \leq e^{Cn}.$$

よって, $n \leq k$ に注意すれば

$$c_k(n) \leq e^{2\pi\sqrt{kn}+Cn} \leq e^{(2\pi+C)\sqrt{kn}}$$

であるから補題の主張が従う.

Case 2：$k \leq n$ のとき. (9), (10) より, $0 < y \leq 1$ に対し

$$c_k(n)e^{-2\pi yn} \leq e^{-2\pi yk}(e^{2\pi/y} + C)^k \leq (e^{2\pi/y} + C)^k.$$

これより

$$c_k(n) \leq e^{2\pi(yn+k/y)}(1 + Ce^{-2\pi/y})^k \leq e^{2\pi(yn+k/y)}(1 + C)^k.$$

$y = \sqrt{k/n} \leq 1$ を代入し, $k \leq n$ に注意すれば

$$c_k(n) \leq e^{4\pi\sqrt{kn}}(1 + C)^k \leq e^{(4\pi+\log(1+C))\sqrt{kn}}$$

が得られるから補題の主張が従う. □

上記の証明のうち Case 1 の部分は塩川宇賢氏から天羽氏に教示されたものであり, その他の部分は天羽氏により Mahler (1974) の証明が簡明化されたものである.

補題 5 (天羽). $0 < |q| < 1$ なる複素数 q であって $J(q)$ が $[\mathbb{Q}(J(q)) : \mathbb{Q}] = m$ である代数的数となるようなものが存在するならば, 任意の正整数 s に対し $J(q^s)$ は代数的数であり, かつ

(a) $[\mathbb{Q}(J(q^s)) : \mathbb{Q}] \le m\psi(s)$,

(b) $\mathrm{den}(J(q^s)) \le \mathrm{den}(J(q))^{m\psi(s)}$,

(c) $\left|J(q^s)\right| \le e^{C_1 s}$ $\quad (C_1 > 0$ は $J(q)$ と $J(z)$ のみに依存$)$.

証明. $\beta := J(q)$ の共役を $\beta^{(1)}(= \beta), \beta^{(2)}, \ldots, \beta^{(m)}$ とすると,

$$\Psi_s(X) := \mathrm{den}(\beta)^{m\psi(s)} \prod_{k=1}^{m} \Phi_s(X, \beta^{(k)})$$

について,

$$\Psi_s(X) \in \mathbb{Z}[X] \quad \text{かつ} \quad \Psi_s(J(q^s)) = 0 \tag{11}$$

が成り立つことを示す. $\Psi_s(X)$ の係数は, 整数係数の $\beta^{(1)}, \beta^{(2)}, \ldots, \beta^{(m)}$ の対称式だから, 有理数である. さらに,

$$\mathrm{den}(\beta^{(k)}) = \mathrm{den}(\beta) \ (2 \le k \le m)$$

より, $\Psi_s(X)$ の係数は代数的整数である. よって, $\Psi_s(X) \in \mathbb{Z}[X]$. また, $\Phi_s(J(q^s), \beta) = 0$ より $\Psi_s(J(q^s)) = 0$ が成り立つ. 以上より, (11) が示された.

$\deg \Psi_s(X) = m\psi(s)$ だから, (11) より (a) が従う. さらに, $\Psi_s(X)$ の最高次係数は $\mathrm{den}(\beta)^{m\psi(s)}$ だから, (11) より (b) も従う.

最後に, (c) を示す. 写像 $j : \mathbb{H} \to \mathbb{C}$ が全射だから,

$$\beta^{(k)} = j(\tau_k) \quad (\tau_k = A_k + iB_k \in \mathbb{H})$$

をみたす τ_k $(1 \le k \le m)$ が存在する. このとき, $\Phi_s(X)$ の定義より

$$\Phi_s(X, \beta^{(k)}) = \prod_{\substack{a,d \in \mathbb{N},\ ad=s,\\ b \in \mathbb{Z},\ 0 \le b \le d-1,\\ (a,b,d)=1}} \left(X - j\left(\frac{a\tau_k + b}{d} \right) \right) \qquad (1 \le k \le m).$$

$\Psi_s(X)$ の定義と (11) より

$$\left|J(q^s)\right| \le \max_{1 \le k \le m} \max_{\substack{a,d \in \mathbb{N},\ ad=s,\\ b \in \mathbb{Z},\ 0 \le b \le d-1,\\ (a,b,d)=1}} \left| j\left(\frac{a\tau_k + b}{d} \right) \right|. \tag{12}$$

これを評価するため, 不等式

$$|j(\tau)| \le e^{C_2(y + 1/y)} \qquad (\tau = x + iy \in \mathbb{H}) \tag{13}$$

を使う. ただし, C_2 は j のみに依存する (従って, J のみに依存する) 正定数である. 実際, $z = e^{2\pi i\tau}$ とおくと, (1) より

$$|j(\tau)| \leq \frac{1}{|z|} + 744 + \sum_{n=1}^{\infty} c(n)|z|^n = j(yi)$$

だから (8) と (9) より (13) が従う.

(12) の右辺に (13) を応用すると

$$\left| J(q^s) \right| \leq \max_{1\leq k\leq m} \max_{\substack{a,d\in\mathbb{N},\ ad=s,\\ b\in\mathbb{Z},\ 0\leq b\leq d-1,\\ (a,b,d)=1}} e^{C_2(aB_k/d+d/aB_k)}.$$

よって, $1 \leq a, d \leq s$ より

$$\left| J(q^s) \right| \leq \max_{1\leq k\leq m} e^{C_2(B_k+1/B_k)s}.$$

これより (c) が従う. □

3 Mahler-Manin 予想の証明

本節では 第 2 節 Prop. 1 の証明に用いた方法を発展させ Mahler-Manin 予想を証明する.

定理 1 の証明. 証明は背理法による. $J(q)$ が代数的数であると仮定する. 以下, L は偶数のパラメータとし, $C_3, \ldots, C_{11}$ は $q, J(q), J(z)$ には依存するが L には依存しない正定数とする.

ステップ 1. a_{kl} $(1 \leq k, l \leq L)$ を未知定数とし

$$F(z) = \sum_{k=1}^{L}\sum_{l=1}^{L} a_{kl} z^k \tilde{J}(z)^l$$

とおく. $\mathrm{ord}_{z=0}F(z) \geq L^2/2 + 1$ をみたすよう a_{kl} 達を定める.

$$b_n = \sum_{k=1}^{\min\{n,L\}}\sum_{l=1}^{L} c_l(n-k)a_{kl} \qquad (n \in \mathbb{N}) \tag{14}$$

とおくと $F(z) = \sum_{n=1}^{\infty} b_n z^n$ と書けるから a_{kl} 達についての同次連立 1 次方程式

$$b_n = 0 \quad (n = 1, \ldots, L^2/2)$$

を解けばよい. 未知数の個数は L^2, 方程式の個数は $L^2/2$ である. また, 補題 4 より

$$|\ \text{方程式の係数}\ | = c_l(n-k) \leq e^{C_0\sqrt{l(n-k)}} \leq e^{C_0\sqrt{Ln}} \leq e^{C_0 L^{3/2}}$$

である. よって, 補題 1 (Siegel's lemma) より, この連立 1 次方程式の非自明解 $a_{kl} \in \mathbb{Z}$ であって

$$|a_{kl}| \leq L^2 e^{C_0 L^{3/2}} \qquad (1 \leq k, l \leq L) \tag{15}$$

をみたすものが存在する.

以下, L に応じて (15) をみたす解をひとつ固定したものを $F(z)$ とする. 補題 3 より $F(z)(= F(z;L)) \not\equiv 0$ である.

$$M := \min\{n \in \mathbb{N} \mid b_n \neq 0\}$$

とおく. このとき, $C_3 > 0$ であって

$$|z| \leq \frac{1}{2} e^{-C_3} \tag{16}$$

のとき

$$|F(z)| \leq 2|z|^M e^{C_3\sqrt{LM}} \tag{17}$$

が成り立つようなものが存在することを示す.

(14), (15) 及び 補題 4 より

$$|b_n| \leq L^2 \cdot e^{C_0\sqrt{Ln}} \cdot L^2 e^{C_0 L^{3/2}}.$$

よって, 適当な C_3 をとれば, $n \geq M (> L^2/2)$ のとき

$$|b_n| \leq e^{C_3\sqrt{Ln}}.$$

また, $L \leq L^2/2 < M$ より 任意の正整数 m に対し

$$\sqrt{L(M+m)} \leq \sqrt{\sqrt{LM}(\sqrt{LM}+m)} \leq \sqrt{LM} + m$$

が成り立つから

$$|b_{M+m} z^{M+m}| \leq e^{C_3\sqrt{L(M+m)}} |z|^{M+m} \leq |z|^M e^{C_3\sqrt{LM}} \left(e^{C_3}|z|\right)^m.$$

よって, z が (16) をみたすとき

$$|F(z)| \leq |z|^M e^{C_3\sqrt{LM}} \sum_{m=0}^{\infty} \left(\frac{1}{2}\right)^m = 2|z|^M e^{C_3\sqrt{LM}}$$

が成り立つ.

補題 5 より $J(q)$ が代数的数であるという仮定の下で $J(q^k)$ $(k \in \mathbb{N})$ も代数的数となる. C_3 は q にも L にも依存しないから, 必要ならば q^k を q に置き換えて, $z = q$ は最初から (16) をみたすと仮定してよい. 以下, これを仮定する.

ステップ 2 .

$$S := \min\{s \in \mathbb{N} \mid F(q^s) \neq 0\}$$

とおく. このとき,

$$S^2 \leq C_4\sqrt{LM} \tag{18}$$

が成り立つことを示す. 証明には次の不等式を用いる： $S \geq 3$ のとき

$$\log|\tilde{F}(0)| \leq \max_{|z|=|q|} \log|\tilde{F}(z)| + \frac{(S-1)(S-2)}{2} \log|q|. \tag{19}$$

ただし, $\tilde{F}(z) := z^{-M} F(z)$.

< (19) の証明 > $R > 0,\ \alpha \in \mathbb{C},\ |\alpha| < R$ とする. 分数 1 次変換

$$g(z) = \frac{R(z-\alpha)}{R^2 - \overline{\alpha} z}$$

は $|z| = R$ のとき $R^2 = z\overline{z}$ より,

$$|g(z)| = \left|\frac{R(z-\alpha)}{z\overline{z} - \overline{\alpha}z}\right| = \left|\frac{R(z-\alpha)}{z(\overline{z} - \overline{\alpha})}\right| = 1$$

をみたす. また, $z = \alpha$ は $g(z)$ の 1 位の零点である. $R = |q|,\ \alpha = q^s\ (s = 2, \ldots, S-1)$ として,

$$G(z) = \tilde{F}(z) \prod_{s=2}^{S-1} \frac{|q|^2 - \overline{q}^s z}{|q|(z - q^s)}$$

とおくと, $|z| \leq |q|$ で $G(z)$ は正則だから最大値原理より

$$|G(0)| \leq \max_{|z|=|q|} |G(z)| = \max_{|z|=|q|} |\tilde{F}(z)|$$

が成り立つ. ここで,

$$|G(0)| = |\tilde{F}(0)| \prod_{s=2}^{S-1} |q|^{1-s} = |\tilde{F}(0)||q|^{-(S-1)(S-2)/2}$$

より,

$$|\tilde{F}(0)||q|^{-(S-1)(S-2)/2} \leq \max_{|z|=|q|} |\tilde{F}(z)|$$

となる. 両辺の対数をとれば (19) が得られる. < (19) の証明終り >

< (18) の証明 > (17) と (19) より

$$\log|\tilde{F}(0)| \leq \log 2 + C_3\sqrt{LM} + \frac{(S-1)(S-2)}{2}\log|q|.$$

$\tilde{F}(0) = b_M \in \mathbb{Z} \setminus \{0\}$ だから $\log|\tilde{F}(0)| \geq 0$. よって, $\log|q| < 0$ に注意すれば (18) が従う.

< (18) の証明終り >

$$\gamma := F(q^S) = \sum_{k=1}^{L}\sum_{l=1}^{L} a_{kl} q^{Sk} \left(q^S J(q^S)\right)^l$$

とおく. $0 \neq \gamma \in \mathbb{Q}(q, J(q^S))$ だから, 補題 5 (a) より

$$[\mathbb{Q}(\gamma) : \mathbb{Q}] \leq C_5\psi(S) \tag{20}$$

が成り立つ.

ステップ 3. $|\gamma|$ の下界:

$$\log|\gamma| \geq -C_6\psi(S)L(\psi(S) + L^{1/2}). \tag{21}$$

を Liouville の基本不等式を用いて証明する. 補題 5 (b) より

$$\mathrm{den}(\gamma) \leq \mathrm{den}(q)^{2SL}\mathrm{den}(J(q^S))^L \leq \left(\mathrm{den}(q)^{2S}\mathrm{den}(J(q))^{[\mathbb{Q}(J(q)):\mathbb{Q}]\psi(S)}\right)^L.$$

よって, $S \leq \psi(S)$ だから,

$$\log \mathrm{den}(\gamma) \leq C_7\psi(S)L.$$

次に, (15) と補題 5 (c) より

$$\begin{aligned}\lceil \gamma \rceil &\leq L^2 \cdot L^2 e^{C_0 L^{3/2}} (\max\{1, \lceil q \rceil\})^{2SL} (\max\{1, \lceil J(q^S) \rceil\})^L \\ &\leq L^2 \cdot L^2 e^{C_0 L^{3/2}} (\max\{1, \lceil q \rceil\})^{2SL} e^{C_1 SL}.\end{aligned}$$

よって,

$$\log \lceil \gamma \rceil \leq C_8(L^{3/2} + SL) \leq C_8 \left(L^{3/2} + \psi(S)L \right).$$

これらと (20) を使うと, Liouville の基本不等式より

$$\begin{aligned}\log|\gamma| &\geq -2[\mathbb{Q}(\gamma) : \mathbb{Q}] \max\left\{ C_7 \psi(S)L, C_8 \left(L^{3/2} + \psi(S)L \right) \right\} \\ &\geq -C_6 \psi(S)L(\psi(S) + L^{1/2}) \qquad (21)\end{aligned}$$

が得られる.

ステップ 4 . $|\gamma|$ の上界： $L \geq C_9$ のとき

$$\log|\gamma| \leq -C_{10} SM \qquad (22)$$

が成り立つ. 実際, (17) より

$$|\gamma| \leq 2|q^S|^M e^{C_3 \sqrt{LM}}$$

だから, $|q| < 1$ および $L < \sqrt{2M}$ より主張が従う.

ステップ 5 . $L \geq C_9$ の下で, (21) と (22) より

$$C_{10} SM \leq C_6 \psi(S)L(\psi(S) + L^{1/2}) \qquad (23)$$

となるが, L が十分大きいとき成り立たないことを示す. 実際, (23) の右辺に (3) を用いると

$$M \leq C_{10}^{-1} C_6 (1 + \log S)L \left(S(1 + \log S) + L^{1/2} \right).$$

よって, (18) および $L < \sqrt{2M}$ より

$$M \leq C_{11} M^{7/8} (\log M)^2$$

となるが, これは M が十分大きいとき成り立たない. 従って, (23) は L が十分大きいとき成り立たず, 矛盾が導かれる. □

4 Nesterenko の結果と代数的独立性

Mahler-Manin 予想解決の発表から程ない 1996 年, Nesterenko は次の定理を証明した.

$$P(z) = 1 - 24 \sum_{n=1}^{\infty} \frac{n z^n}{1 - z^n}, \quad Q(z) = 1 + 240 \sum_{n=1}^{\infty} \frac{n^3 z^n}{1 - z^n}, \quad R(z) = 1 - 504 \sum_{n=1}^{\infty} \frac{n^5 z^n}{1 - z^n}$$

とする.

定理 2 (Nesterenko [2])**.** $0<|q|<1$ をみたす任意の複素数 q に対し $q, P(q), Q(q), R(q)$ のうち少なくとも 3 つの数は $\mathbb{Q}$ 上代数的独立, すなわち

$$\mathrm{trans.deg}_{\mathbb{Q}}\,\mathbb{Q}\Big(q, P(q), Q(q), R(q)\Big) \geq 3$$

が成り立つ.

系 1. $0<|\alpha|<1$ をみたす代数的数 α に対し $P(\alpha), Q(\alpha), R(\alpha)$ は代数的独立である.

$$J(z) = 1728\frac{Q(z)^3}{Q(z)^3 - R(z)^2}$$

かつ

$$z\frac{d}{dz}P(z) = \frac{1}{12}(P(z)^2 - Q(z)), \qquad z\frac{d}{dz}Q(z) = \frac{1}{3}(P(z)Q(z) - R(z)),$$
$$z\frac{d}{dz}R(z) = \frac{1}{2}(P(z)R(z) - Q(z)^2)$$

より

$$\Delta = \frac{1}{1728}(Q^3 - R^2)$$

とすると

$$z\frac{d}{dz}\Delta = P\Delta, \quad J = \frac{Q^3}{\Delta}, \quad z\frac{d}{dz}J = -\frac{Q^2R}{\Delta}, \quad \left(z\frac{d}{dz}\right)^2 J = \frac{-PQ^2R + 4QR^2 + 3Q^4}{6\Delta}$$

であり, これらを逆に解いて

$$P = 6\frac{\left(z\frac{d}{dz}\right)^2 J}{z\frac{d}{dz}J} - 4\frac{z\frac{d}{dz}J}{J} - 3\frac{J}{J-1728}, \quad Q = \frac{\left(z\frac{d}{dz}J\right)^2}{J(J-1728)}, \quad R = -\frac{\left(z\frac{d}{dz}J\right)^2}{J^2(J-1728)}$$

となる. 従って, $0<|q|<1$ をみたす任意の複素数 q に対し

$$\mathbb{Q}\Big(q, J(q), J'(q), J''(q)\Big) = \mathbb{Q}\Big(q, P(q), Q(q), R(q)\Big)$$

であるから,

系 2. $0<|\alpha|<1$ をみたす代数的数 α に対し $J(\alpha), J'(\alpha), J''(\alpha)$ は代数的独立である. 特に, $J(\alpha)$ は超越数である. すなわち, Mahler-Manin 予想が成立する.

$J(z), J'(z), J''(z)$ は $\mathbb{C}(z)$ 上代数的独立であるが, 上記の関係式から

Proposition 2. $J(z), J'(z), J''(z), J^{(3)}(z)$ は $\mathbb{C}(z)$ 上代数的従属である.

一方, Fredholm 級数

$$f(z) = \sum_{k=0}^{\infty} z^{d^k}$$

(ただし, d は 2 以上の整数) に対しては

Proposition 3. $\{f^{(l)}(z) \mid l \geq 0\}$ は $\mathbb{C}(z)$ 上代数的独立である.

これは, gap theorem から導かれるが, 初等的に示すこともできる：

$$f_l(z) = \left(z\frac{d}{dz}\right)^l f(z) = \sum_{k=0}^{\infty} d^{lk} z^{d^k} \quad (l \geq 0)$$

とおくと $f_l(z)$ は

$$f_l(z) = d^l f_l(z^d) + z \qquad (l \geq 0) \tag{24}$$

をみたす. 任意の $m \geq 0$ に対し, $\{f_l(z) \mid 0 \leq l \leq m\}$ と $\{f^{(l)}(z) \mid 0 \leq l \leq m\}$ は $\mathbb{C}(z)$ 上同じベクトル空間を生成する. $\{f_l(z) \mid l \geq 0\}$ は $\mathbb{C}(z)$ 上代数的独立であることを (24) を用いて l に関する帰納法で初等的に証明できる:

補題 6. $\{f_l(z) \mid l \geq 0\}$ は $\mathbb{C}(z)$ 上代数的独立である.

証明のスケッチ. 補題 2 より

$$f_0(z) = f(z) = \sum_{k=0}^{\infty} z^{d^k}$$

は $\mathbb{C}(z)$ 上超越的である. $f_0(z), f_1(z)$ が $\mathbb{C}(z)$ 上代数的独立であることを示す. $f_1(z)$ が体 $\mathbb{C}(z, f_0(z))$ 上超越的であることを示せばよい. 背理法により証明する. $f_1(z)$ が $\mathbb{C}(z, f_0(z))$ 上代数的であると仮定する. 即ち,

$$a_0(z, f_0(z))f_1(z)^m + a_1(z, f_0(z))f_1(z)^{m-1} + \cdots + a_m(z, f_0(z)) = 0 \tag{25}$$

となる $a_0(z, X), \ldots, a_m(z, X) \in \mathbb{C}[z, X]$, $a_0(z, X) \not\equiv 0$ が存在すると仮定する. ただし, m はこのような正整数のうち最小のものとする. (25) において z を z^d に変換し d^m を乗ずると

$$a_0(z^d, f_0(z^d))(df_1(z^d))^m + da_1(z^d, f_0(z^d))(df_1(z^d))^{m-1} + \cdots + d^m a_m(z^d, f_0(z^d)) = 0$$

となる. これに $f_0(z^d) = f_0(z) - z$, $df_1(z^d) = f_1(z) - z$ を代入して $f_1(z)$ の降べきの順に整理すると

$$a_0(z^d, f_0(z) - z)f_1(z)^m + (-mza_0(z^d, f_0(z) - z) + da_1(z^d, f_0(z) - z))f_1(z)^{m-1} + \cdots = 0 \tag{26}$$

を得る. (25), (26) 及び m の最小性から

$$\begin{aligned} & a_0(z^d, f_0(z) - z)a_1(z, f_0(z)) \\ = \quad & -mza_0(z, f_0(z))a_0(z^d, f_0(z) - z) + da_0(z, f_0(z))a_1(z^d, f_0(z) - z). \end{aligned} \tag{27}$$

$f_0(z)$ は $\mathbb{C}(z)$ 上超越的であるから, (27) は $f_0(z)$ に関する恒等式である. よって, $\deg_X a_0(z, X) \leq \deg_X a_1(z, X)$ であることが分かる. $a_0(z, X), a_1(z, X)$ の X に関する最高次係数をそれぞれ $p(z), q(z)$ とすると $p(z) \not\equiv 0$ であり,

$$p(z^d)q(z) = dp(z)q(z^d) \tag{28}$$

または

$$p(z^d)q(z) = -mzp(z)p(z^d) + dp(z)q(z^d) \tag{29}$$

が成り立つ. $\gcd(p(z), q(z)) = r(z)$ とすると (28), (29) ともに両辺は $r(z)r(z^d)$ で割り切れるから $p(z)/r(z), q(z)/r(z)$ をそれぞれあらためて $p(z), q(z)$ とおいて $p(z)$ と $q(z)$ には共通因子がないとしてよい. 従って, $A(z), B(z) \in \mathbb{C}[z]$ が存在して $A(z)p(z) + B(z)q(z) = 1$ となるから, $A(z^d)p(z^d) + B(z^d)q(z^d) = 1$. よって, $p(z^d)$ と $q(z^d)$ には共通因子がない. 従って, (28), (29) ともに $p(z^d)$ は $p(z)$ を割り切る. 故に, $\deg p = 0$, 即ち $p(z) \in \mathbb{C} \setminus \{0\}$. よって, $p(z) = 1$ としてよい. このとき, (28) は

$$q(z) = dq(z^d),$$

(29) は

$$q(z) = -mz + dq(z^d)$$

となる. 両辺の次数を比較して $q(z) \equiv k \in \mathbb{C}$. $\deg_X a_0(z, X) \leq \deg_X a_1(z, X)$ より $k \neq 0$ である. 従って, (28) のとき $d = 1$ となり, (29) のとき $mz = (d-1)k$ となる. これらはいずれも矛盾である.

以下, このようにして帰納的に $\{f_l(z) \mid l \geq 0\}$ が $\mathbb{C}(z)$ 上代数的独立であることが証明できる. □

$\{f^{(l)}(z) \mid l \geq 0\}$ は $\mathbb{C}(z)$ 上代数的独立であるから, これらの関数の代数的数における値の代数的独立性が問題となる. その証明には 第 2 節 Prop. 1 の証明 及び 第 3 節 Mahler-Manin 予想の証明と類似した方法が適用できる. 次節を通してそのことを解説する.

5 Mahler の方法による代数的独立性の証明

Fredholm 級数 $f(z) = \sum_{k=0}^{\infty} z^{d^k}$ に対して次が成り立つ. ただし, d は 2 以上の整数である.

定理 3. $0 < |\alpha| < 1$ をみたす代数的数 α に対し $\{f^{(l)}(\alpha) \mid l \geq 0\}$ は代数的独立である.

証明. 以下, $K = \mathbb{Q}(\alpha)$ とする. 任意の $m \geq 0$ に対し, $\{f_l(\alpha) \mid 0 \leq l \leq m\}$ と $\{f^{(l)}(\alpha) \mid 0 \leq l \leq m\}$ は K 上同じベクトル空間を生成する.

証明は背理法による. $\{f^{(l)}(\alpha) \mid l \geq 0\}$ は代数的従属と仮定すると 或る $m \geq 0$ に対して $\{f^{(l)}(\alpha) \mid 0 \leq l \leq m\}$ は代数的従属となる. これは $\{f_l(\alpha) \mid 0 \leq l \leq m\}$ が代数的従属であることと同値である. すなわち,

$$\sum_{\substack{\mu=(\mu_0,\ldots,\mu_m),\\ 0\leq\mu_l\leq L}} \tau_\mu f_0(\alpha)^{\mu_0} \cdots f_m(\alpha)^{\mu_m} = 0 \quad (\tau_\mu \in \mathbb{Z})$$

をみたす. ただし, τ_μ は少なくともひとつは 0 ではないものとする.

以下, t_μ $(\mu = (\mu_0, \ldots, \mu_m),\ 0 \leq \mu_l \leq L)$ を $(L+1)^{m+1}$ 個の独立変数とし,

$$F(z; \boldsymbol{t}) := \sum_{\substack{\mu=(\mu_0,\ldots,\mu_m),\\ 0\leq\mu_l\leq L}} t_\mu f_0(z)^{\mu_0} \cdots f_m(z)^{\mu_m} \in \mathbb{Z}[\boldsymbol{t}][[z]]$$

とする.

(注意. $F(z; \tau) = \sum_{\substack{\mu=(\mu_0,\ldots,\mu_m),\\ 0\leq\mu_l\leq L}} \tau_\mu f_0(z)^{\mu_0} \cdots f_m(z)^{\mu_m} \in \mathbb{Z}[[z]]$ は α を零点としてもつ.)

(24) を繰り返し用いると

$$f_l(z) = d^{kl} f_l(z^{d^k}) + \sum_{h=0}^{k-1} d^{lh} z^{d^h} \qquad (k \geq 0).$$

$b_l^{(k)}(z) = \sum_{h=0}^{k-1} d^{lh} z^{d^h}$ とおく. $x_0, \ldots, x_m, y_0, \ldots, y_m, w_0, \ldots, w_m$ を変数とし

$$\sum_{\substack{\mu=(\mu_0,\ldots,\mu_m),\\ 0\leq\mu_l\leq L}} t_\mu (x_0 w_0 + y_0)^{\mu_0} \cdots (x_m w_m + y_m)^{\mu_m} = \sum_{\substack{\mu=(\mu_0,\ldots,\mu_m),\\ 0\leq\mu_l\leq L}} T_\mu(\boldsymbol{t}; \boldsymbol{x}; \boldsymbol{y}) w_0^{\mu_0} \cdots w_m^{\mu_m}$$

とする. 即ち,

$$T_\mu(\boldsymbol{t}; \boldsymbol{x}; \boldsymbol{y}) = \sum_{\substack{\nu=(\nu_0,\ldots,\nu_m),\\ \nu_0\geq\mu_0,\ldots,\nu_m\geq\mu_m}} t_\nu \binom{\nu_0}{\mu_0} \cdots \binom{\nu_m}{\mu_m} x_0^{\mu_0} \cdots x_m^{\mu_m} y_0^{\nu_0-\mu_0} \cdots y_m^{\nu_m-\mu_m}.$$

このとき,

$$\begin{aligned} F(z; \boldsymbol{t}) &= \sum_{\substack{\mu=(\mu_0,\ldots,\mu_m),\\ 0\leq\mu_l\leq L}} t_\mu f_0(z)^{\mu_0} \cdots f_m(z)^{\mu_m} \\ &= \sum_{\substack{\mu=(\mu_0,\ldots,\mu_m),\\ 0\leq\mu_l\leq L}} t_\mu (f_0(z^{d^k}) + b_0^{(k)}(z))^{\mu_0} \cdots (d^{km} f_m(z^{d^k}) + b_m^{(k)}(z))^{\mu_m} \\ &= \sum_{\substack{\mu=(\mu_0,\ldots,\mu_m),\\ 0\leq\mu_l\leq L}} T_\mu(\boldsymbol{t}; 1, d^k, \ldots, d^{km}; \boldsymbol{b}^{(k)}(z)) f_0(z^{d^k})^{\mu_0} \cdots f_m(z^{d^k})^{\mu_m} \\ &= F(z^{d^k}; \boldsymbol{T}(\boldsymbol{t}; 1, d^k, \ldots, d^{km}; \boldsymbol{b}^{(k)}(z))) \end{aligned}$$

である. 従って,

$$0 = F(\alpha; \tau) = F(\alpha^{d^k}; \boldsymbol{T}(\tau; 1, d^k, \ldots, d^{km}; \boldsymbol{b}^{(k)}(\alpha))).$$

ただし, $T_\mu(\tau; 1, \ldots, 1; \boldsymbol{b}^{(0)}(\alpha)) = T_\mu(\tau; 1, \ldots, 1; 0, \ldots, 0) = \tau_\mu$ である.

(注意. $F\left(z; \boldsymbol{T}(\tau; 1, d^k, \ldots, d^{km}; \boldsymbol{b}^{(k)}(\alpha))\right) \in K[[z]]$ は α^{d^k} を零点としてもつ.)

定義 1.

$$V(\tau) = \{Q(\boldsymbol{t}) \in K[\boldsymbol{t}] \mid \text{任意の } k \geq 0 \text{ に対し } Q(\boldsymbol{T}(\tau; 1, d^k, \ldots, d^{km}; y_0, \ldots, y_m)) = 0\}$$

と定義する. さらに, $P(z; \boldsymbol{t}) = \sum_{n=0}^{\infty} P_n(\boldsymbol{t}) z^n \in K[\boldsymbol{t}][[z]]$ に対し,

$$\operatorname{ind} P(z; \boldsymbol{t}) := \min\{n \mid P_n \notin V(\tau)\}$$

と定義する. ただし, 任意の $n \geq 0$ に対し $P_n \in V(\tau)$ のときは $\operatorname{ind} P(z; \boldsymbol{t}) = \infty$ とする.

下記の Proposition 4 は補助関数の構成に関するものであり, 証明は後述する (19 頁参照). 以下, $c_1, c_2, \ldots$ は $p,\ k$ に依存しない正定数, $c_1(p), c_2(p), \ldots$ は p には依存するが k には依存しない正定数とする. K の整数環を $\mathbb{Z}_K$ と表す.

Proposition 4. p を十分大きな正整数とする.

$$B_0(z; \boldsymbol{t}), \ldots, B_p(z; \boldsymbol{t}) \in \mathbb{Z}_K[z; \boldsymbol{t}], \qquad \deg_z B_h, \deg_{t_\mu} B_h \leq p \ (0 \leq h \leq p,\ \mu)$$

であり, 次の (i), (ii) をみたすものが存在する.

(i) $\operatorname{ind} B_0(z;\boldsymbol{t}) < \infty$.

(ii) $E(z;\boldsymbol{t}) := \sum_{h=0}^{p} B_h(z;\boldsymbol{t})F(z;\boldsymbol{t})^h$ とおくと,

$$I := \operatorname{ind} E(z;\boldsymbol{t}) \geq c_1 p^2.$$

Proposition 5. Prop. 4 の $E(z;\boldsymbol{t})$ に対し, $k > c_2(p)$ なら

$$\left| E\left(\alpha^{d^k}; \boldsymbol{T}(\tau; 1, d^k, \ldots, d^{km}; \boldsymbol{b}^{(k)}(\alpha))\right)\right| \leq c_3^{p^2 d^k}, \qquad 0 < c_3 < 1.$$

証明. $b_l^{(k)}(\alpha) = f_l(\alpha) - d^{kl} f_l(\alpha^{d^k}),\ 0 \leq l \leq m$ だから $f_l(\alpha^{d^k}) \to f_l(0)\ (k \to \infty)$ に注意すると, $c_4 > d^m$ とすれば, 十分大きなすべての k に対し $|b_l^{(k)}(\alpha)| \leq c_4^k\ (0 \leq l \leq m)$ となる.

$$T_\mu(\boldsymbol{t};\boldsymbol{x};\boldsymbol{y}) = \sum_{\substack{\nu=(\nu_0,\ldots,\nu_m),\\ \nu_0 \geq \mu_0, \ldots, \nu_m \geq \mu_m}} t_\nu \binom{\nu_0}{\mu_0} \cdots \binom{\nu_m}{\mu_m} x_0^{\mu_0} \cdots x_m^{\mu_m} y_0^{\nu_0-\mu_0} \cdots y_m^{\nu_m-\mu_m}$$

だから, $T_\mu(\tau;\boldsymbol{x};\boldsymbol{y}) \in \mathbb{Z}[x_0, \ldots, x_m, y_0, \ldots, y_m],\ \deg_{x_l} T_\mu(\tau;\boldsymbol{x};\boldsymbol{y}), \deg_{y_l} T_\mu(\tau;\boldsymbol{x};\boldsymbol{y}) \leq L$. 従って, k が十分大きいとき

$$\begin{aligned} & |T_\mu(\tau; 1, d^k, \ldots, d^{km}; b_0^{(k)}(\alpha), \ldots, b_m^{(k)}(\alpha))| \\ \leq\ & c_5 d^{k\frac{m(m+1)}{2}L} c_4^{k(m+1)L} \ \leq\ c_5 c_4^{k\frac{m+1}{2}L} c_4^{k(m+1)L} \ =\ c_5 c_4^{\frac{3}{2}(m+1)Lk}. \end{aligned}$$

$E(z;\boldsymbol{t})$ は $\boldsymbol{t}$ については $\deg_{t_\mu} E(z;\boldsymbol{t}) \leq 2p$ の多項式で その係数は収束半径 1 の z の冪級数である. よって,

$$E(z;\boldsymbol{t}) = \sum_{\lambda} g_\lambda(z)\boldsymbol{t}^\lambda, \qquad g_\lambda(z) = \sum_{n=0}^{\infty} g_{\lambda n} z^n$$

とおくと, $|g_{\lambda n}| \leq c_6(p)2^n$. $g_\lambda(z)$ は単位円内で一様絶対収束するから $E(z;\boldsymbol{t}) = \sum_{n=0}^{\infty} \left(\sum_\lambda g_{\lambda n}\boldsymbol{t}^\lambda\right) z^n$. $I = \operatorname{ind} E(z;\boldsymbol{t})$ だから, k が十分大きいとき

$$\begin{aligned} & \left| E\left(\alpha^{d^k}; \boldsymbol{T}(\tau; 1, d^k, \ldots, d^{km}; \boldsymbol{b}^{(k)}(\alpha))\right)\right| \\ \leq\ & \sum_{n=I}^{\infty} \left(\sum_\lambda c_6(p) 2^n \left(c_5 c_4^{\frac{3}{2}(m+1)Lk}\right)^\lambda \right) |\alpha|^{d^k n} \\ & \left(\lambda = (\lambda_1, \ldots, \lambda_{(L+1)^{m+1}}),\ \ \deg_{t_\mu} E(z;\boldsymbol{t}) \leq 2p \text{ だから}\right) \\ \leq\ & \sum_{n=I}^{\infty} (2p+1)^{(L+1)^{m+1}} c_6(p) 2^n \left(c_5 c_4^{\frac{3}{2}(m+1)Lk}\right)^{2p(L+1)^{m+1}} |\alpha|^{d^k n} \\ =\ & \sum_{n=I}^{\infty} c_7(p) c_8^{pk} (2|\alpha|^{d^k})^n \quad \left(c_7(p) := (2p+1)^{(L+1)^{m+1}} c_6(p) c_5^{2p(L+1)^{m+1}},\ c_8 := c_4^{3(m+1)L(L+1)^{m+1}}\right) \\ =\ & c_7(p) c_8^{pk} \frac{(2|\alpha|^{d^k})^I}{1 - 2|\alpha|^{d^k}}. \\ & \left(1 - 2|\alpha|^{d^k} \geq \frac{1}{c_9},\ 2|\alpha|^{d^k} < 1,\ I \geq c_1 p^2\ (\because \text{Prop. 4}) \text{ だから}\right) \\ \leq\ & c_9 c_7(p) c_8^{pk} 2^{c_1 p^2} |\alpha|^{c_1 p^2 d^k}. \end{aligned}$$

ここで, $\boxed{|\alpha|^{c_1} < c_3 < 1}$ にとれば $k > c_2(p)$ のとき

$$\left| E\left(\alpha^{d^k}; \boldsymbol{T}(\tau; 1, d^k, \ldots, d^{km}; \boldsymbol{b}^{(k)}(\alpha))\right)\right| \leq c_3^{p^2 d^k}. \ \square$$

定理 3 の証明の完結. $b_l^{(k)}(z) = \sum_{h=0}^{k-1} d^{lh} z^{d^h}$ だから $D = \mathrm{den}(\alpha)$ とすると, $\mathrm{den}(b_l^{(k)}(\alpha)) = D^{d^{k-1}}$ $(0 \le l \le m)$. Prop. 5 の証明と同様にして

$$\mathrm{den}(T_\mu(\tau; 1, d^k, \ldots, d^{km}; b_0^{(k)}(\alpha), \ldots, b_m^{(k)}(\alpha))) \le D^{(m+1)Ld^{k-1}}.$$

$E(z; \boldsymbol{t}) = \sum_{h=0}^{p} B_h(z; \boldsymbol{t}) F(z; \boldsymbol{t})^h$, $F(\alpha^{d^k}; \boldsymbol{T}(\tau; 1, d^k, \ldots, d^{km}; \boldsymbol{b}^{(k)}(\alpha))) = 0$ だから,

$$E(\alpha^{d^k}; \boldsymbol{T}(\tau; 1, d^k, \ldots, d^{km}; \boldsymbol{b}^{(k)}(\alpha))) = B_0(\alpha^{d^k}; \boldsymbol{T}(\tau; 1, d^k, \ldots, d^{km}; \boldsymbol{b}^{(k)}(\alpha))).$$

$B_0(z; \boldsymbol{t}) \in \mathbb{Z}_K[z; \boldsymbol{t}]$, $\deg_z B_0, \deg_{t_\mu} B_0 \le p$, $\sharp\{\mu = (\mu_0, \ldots, \mu_m) \mid 0 \le \mu_l \le L\} = (L+1)^{m+1}$ だから

$$\begin{aligned} D^*(k) &:= \mathrm{den}\left(B_0(\alpha^{d^k}; \boldsymbol{T}(\tau; 1, d^k, \ldots, d^{km}; \boldsymbol{b}^{(k)}(\alpha)))\right) \\ &\le D^{pd^k + (m+1)L(L+1)^{m+1} pd^{k-1}} \\ &= c_{10}^{pd^k}. \qquad \boxed{c_{10} = D^{1+(m+1)L(L+1)^{m+1}/d}} \end{aligned} \tag{30}$$

もし, $B_0(\alpha^{d^k}; \boldsymbol{T}(\tau; 1, d^k, \ldots, d^{km}; \boldsymbol{b}^{(k)}(\alpha))) \ne 0$ ならば $D^*(k) E(\alpha^{d^k}; \boldsymbol{T}(\tau; 1, d^k, \ldots, d^{km}; \boldsymbol{b}^{(k)}(\alpha))) = D^*(k) B_0(\alpha^{d^k}; \boldsymbol{T}(\tau; 1, d^k, \ldots, d^{km}; \boldsymbol{b}^{(k)}(\alpha))) \in \mathbb{Z}_K \setminus \{0\}$ である.

以下では簡単のため α は虚 2 次体の数と仮定する. (α が一般の代数的数の場合には第 2 節冒頭の Liouville の基本不等式を用いて同様に証明できる.) このとき,

$$D^*(k) \left| E(\alpha^{d^k}; \boldsymbol{T}(\tau; 1, d^k, \ldots, d^{km}; \boldsymbol{b}^{(k)}(\alpha))) \right| \ge 1. \tag{31}$$

Prop. 4 (i) より, $\mathrm{ind}\, B_0(z; \boldsymbol{t}) < \infty$ だから 下記の Prop. 6 より, $k_0 > c_2(p)$ (in Prop. 5) が存在して $B_0(\alpha^{d^{k_0}}; \boldsymbol{T}(\tau; 1, d^{k_0}, \ldots, d^{k_0 m}; \boldsymbol{b}^{(k_0)}(\alpha))) \ne 0$. (30), (31) と Prop. 5 より, $1 \le c_3^{p^2 d^{k_0}} c_{10}^{pd^{k_0}}$. よって, $1 \le c_3^p c_{10}$. 即ち, $c_3^{-p} \le c_{10}$. $0 < c_3 < 1$ だから, p が十分大きいとき これは矛盾である. □

Proposition 6. $P(z; \boldsymbol{t}) \in K[z; \boldsymbol{t}]$ とする. 十分大きなすべての k に対し

$$P(\alpha^{d^k}; \boldsymbol{T}(\tau; 1, d^k, \ldots, d^{km}; \boldsymbol{b}^{(k)}(\alpha))) = 0$$

ならば

$$\mathrm{ind}\, P(z; \boldsymbol{t}) = \infty.$$

証明. $P(z; \boldsymbol{t}) = \sum_{n=0}^{N} Q_n(\boldsymbol{t}) z^n$ $(Q_n(\boldsymbol{t}) \in K[\boldsymbol{t}])$ とする.

$$Q_n(\boldsymbol{T}(\tau; 1, d^k, \ldots, d^{km}; f_0(\alpha) - w_0, f_1(\alpha) - d^k w_1, \ldots, f_m(\alpha) - d^{km} w_m) = \sum_{\lambda = (\lambda_0, \ldots, \lambda_m)} R_{n\lambda}(k) \boldsymbol{w}^\lambda$$

とおく. $w_0 = f_0(\alpha^{d^k}), \ldots, w_m = f_m(\alpha^{d^k})$ とすると,

$$\begin{aligned} & Q_n(\boldsymbol{T}(\tau; 1, d^k, \ldots, d^{km}; f_0(\alpha) - w_0, f_1(\alpha) - d^k w_1, \ldots, f_m(\alpha) - d^{km} w_m) \\ = \; & Q_n(\boldsymbol{T}(\tau; 1, d^k, \ldots, d^{km}; \boldsymbol{b}^{(k)}(\alpha))) \end{aligned}$$

となるから, 十分大きなすべての k に対し

$$\begin{aligned} & P(\alpha^{d^k}; \boldsymbol{T}(\tau; 1, d^k, \ldots, d^{km}; \boldsymbol{b}^{(k)}(\alpha))) \\ = & \sum_{n=0}^{N} \left(\sum_{\lambda=(\lambda_0,\ldots,\lambda_m)} R_{n\lambda}(k) f_0(\alpha^{d^k})^{\lambda_0} \cdots f_m(\alpha^{d^k})^{\lambda_m} \right) \alpha^{d^k n} \ = \ 0. \end{aligned}$$

$R_{n\lambda}(k) \in K(f_0(\alpha), \ldots, f_m(\alpha))[d^k]$ だから

$$R_{n\lambda}(k) = \sum_{h=0}^{H} r_{n\lambda h} d^{hk}, \qquad r_{n\lambda h} \in K(f_0(\alpha), \ldots, f_m(\alpha)) \subset \mathbb{C}$$

とおける. このとき,

$$\begin{aligned} & P(\alpha^{d^k}; \boldsymbol{T}(\tau; 1, d^k, \ldots, d^{km}; \boldsymbol{b}^{(k)}(\alpha))) \\ = & \sum_{h=0}^{H} d^{hk} \left(\sum_{n=0}^{N} \sum_{\lambda=(\lambda_0,\ldots,\lambda_m)} r_{n\lambda h} \alpha^{d^k n} f_0(\alpha^{d^k})^{\lambda_0} \cdots f_m(\alpha^{d^k})^{\lambda_m} \right). \end{aligned}$$

$G_h(z) = \sum_{n=0}^{N} \sum_{\lambda=(\lambda_0,\ldots,\lambda_m)} r_{n\lambda h} z^n f_0(z)^{\lambda_0} \cdots f_m(z)^{\lambda_m}$ とおくと, $G_h(z) \in \mathbb{C}[[z]]$ である. 補題 6 より, $r_{n\lambda h}$ $(0 \le n \le N,\ \lambda)$ の少なくともひとつが 0 でなければ $G_h(z) = c_{h\,m_h} z^{m_h} + c_{h\,m_h+1} z^{m_h+1} + \cdots,\ c_{h\,m_h} \neq 0$ と表せる. 冪級数 $G_h(z)$ の係数は有界だから $G_h(\alpha^{d^k}) = c_{h\,m_h} \alpha^{m_h d^k} + o(\alpha^{m_h d^k})$.

$$M = \min_{0 \le h \le H} m_h, \qquad H^* = \max\{h \mid m_h = M\}$$

とすると, 十分大きなすべての k に対し

$$\begin{aligned} P(\alpha^{d^k}; \boldsymbol{T}(\tau; 1, d^k, \ldots, d^{km}; \boldsymbol{b}^{(k)}(\alpha))) &= \sum_{h=0}^{H} d^{hk} \left(c_{h\,m_h} \alpha^{m_h d^k} + o(\alpha^{m_h d^k}) \right) \\ &= c_{H^* M} d^{H^* k} \alpha^{M d^k} + o(d^{H^* k} \alpha^{M d^k}), \quad c_{H^* M} \neq 0 \end{aligned}$$

となる. これは矛盾である. 従って,

$$r_{n\lambda h} = 0 \quad (0 \le n \le N,\ \lambda,\ 0 \le h \le H).$$

即ち, $Q_n(\boldsymbol{T}(\tau; 1, d^k, \ldots, d^{km}; f_0(\alpha) - w_0, f_1(\alpha) - d^k w_1, \ldots, f_m(\alpha) - d^{km} w_m) \equiv 0 \quad (0 \le n \le N)$. よって, $Q_n(\boldsymbol{T}(\tau; 1, d^k, \ldots, d^{km}; y_0, \ldots, y_m) \equiv 0 \quad (0 \le n \le N)$. 即ち, $Q_n(\boldsymbol{t}) \in V(\tau) \quad (0 \le n \le N)$.

□

以下, Prop. 4 の証明に用いる補題を述べる.

補題 **7.** $V(\tau)$ は $K[\boldsymbol{t}]$ の素イデアルである.

証明. イデアルであることは明らかである. $Q_1, Q_2 \in K[\boldsymbol{t}]$ が $Q_1 Q_2 \in V(\tau)$ であるとする. すなわち, 任意の $k \ge 0$ に対し $Q_1(\boldsymbol{T}(\tau; 1, d^k, \ldots, d^{km}; y_0, \ldots, y_m)) Q_2(\boldsymbol{T}(\tau; 1, d^k, \ldots, d^{km}; y_0, \ldots, y_m)) = 0$ とする. このとき, Q_1, Q_2 の少なくとも一方, それを Q_1 としてよい, は無限に多くの $k \ge 0$ に対し

$Q_1(\boldsymbol{T}(\tau;1,d^k,\ldots,d^{km};y_0,\ldots,y_m))=0$ となる.

$$\begin{aligned}&T_\mu(\tau;1,d^k,\ldots,d^{km};y_0,\ldots,y_m)\\ =&\sum_{\substack{\nu=(\nu_0,\ldots,\nu_m),\\ \nu_0\geq\mu_0,\ldots,\nu_m\geq\mu_m}}\tau_\nu\binom{\nu_0}{\mu_0}\cdots\binom{\nu_m}{\mu_m}d^{k\mu_1}\cdots d^{km\mu_m}y_0^{\nu_0-\mu_0}\cdots y_m^{\nu_m-\mu_m}\end{aligned}$$

だから $Q_1(\boldsymbol{T}(\tau;1,d^k,\ldots,d^{km};y_0,\ldots,y_m))\in K[d^k,y_0,\ldots,y_m]$ である. Q_1 が $y_0,\ldots,y_m$ の多項式として恒等的に 0 でなければ Q_1 の少なくともひとつの係数は d^k の多項式として恒等的に 0 ではない. しかし, 無限に多くの $k\geq 0$ に対して, これが 0 となるから, 多項式の根は有限個であることに反する. 従って, $Q_1(\boldsymbol{T}(\tau;1,d^k,\ldots,d^{km};y_0,\ldots,y_m))$ は恒等的に 0 である. すなわち, $Q_1\in V(\tau)$ である. □

補題 8. $\operatorname{ind}P_1(z;\boldsymbol{t})P_2(z;\boldsymbol{t})=\operatorname{ind}P_1(z;\boldsymbol{t})+\operatorname{ind}P_2(z;\boldsymbol{t})$.

証明. $\operatorname{ind}P_1(z;\boldsymbol{t})=I,\ \operatorname{ind}P_2(z;\boldsymbol{t})=J$ とする.

$$P_1(z;\boldsymbol{t})=\sum_{n=0}^{\infty}P_n(\boldsymbol{t})z^n,\quad P_2(z;\boldsymbol{t})=\sum_{m=0}^{\infty}Q_m(\boldsymbol{t})z^m$$

とすると,

$$P_1(z;\boldsymbol{t})P_2(z;\boldsymbol{t})=\sum_{k=0}^{\infty}\left(\sum_{n+m=k}P_n(\boldsymbol{t})Q_m(\boldsymbol{t})\right)z^k$$

だから, $I=\infty$ または $J=\infty$ ならば $\operatorname{ind}P_1(z;\boldsymbol{t})P_2(z;\boldsymbol{t})=\infty$ は明らか. 一方, $I,J<\infty$ のとき,

$$P_0(\boldsymbol{t}),\ldots,P_{I-1}(\boldsymbol{t}),Q_0(\boldsymbol{t}),\ldots,Q_{J-1}(\boldsymbol{t})\in V(\tau),\quad P_I(\boldsymbol{t}),Q_J(\boldsymbol{t})\notin V(\tau)$$

である. よって, $k<I+J\implies n<I$ または $m<J\implies P_n(\boldsymbol{t})\in V(\tau)$ または $Q_m(\boldsymbol{t})\in V(\tau)\implies\sum_{n+m=k}P_n(\boldsymbol{t})Q_m(\boldsymbol{t})\in V(\tau)$. また,

$$\begin{aligned}\sum_{n+m=I+J}P_n(\boldsymbol{t})Q_m(\boldsymbol{t}) &= \sum_{n=0}^{I-1}\underbrace{P_n(\boldsymbol{t})}_{\in V(\tau)}Q_{I+J-n}(\boldsymbol{t})+\underbrace{P_I(\boldsymbol{t})Q_J(\boldsymbol{t})}_{\notin V(\tau)\ (\because\text{補題 }7)}+\sum_{m=0}^{J-1}P_{I+J-m}(\boldsymbol{t})\underbrace{Q_m(\boldsymbol{t})}_{\in V(\tau)}\\ &\notin V(\tau).\ \square\end{aligned}$$

定義 2. p を正整数とする.

$$R(p)=\{g(\boldsymbol{t})\in K[\boldsymbol{t}]\mid \deg_{t_\mu}g(\boldsymbol{t})\leq p\text{ for }\forall\mu\}$$

とおく. これは K-vector space である.

$$\overline{R}(p):=R(p)/(R(p)\cap V(\tau)),\qquad d(p):=\dim_K\overline{R}(p)$$

と定義する. $f(\boldsymbol{t})\in R(p)$ に対し,

$$\overline{f(\boldsymbol{t})}:=f(\boldsymbol{t})+(R(p)\cap V(\tau))$$

と表す.

補題 9. $d(2p) \le 2^{(L+1)^{m+1}} d(p)$.

証明. 任意の $Q(\boldsymbol{t}) \in R(2p)$ は $Q(\boldsymbol{t}) = \sum_{\varepsilon} \left(\prod_{\mu} t_{\mu}^{\varepsilon(\mu)p} \right) Q_{\varepsilon}(\boldsymbol{t}), \quad Q_{\varepsilon}(\boldsymbol{t}) \in R(p)$ とかける. ただし, $\varepsilon(\cdot)$ は $\{\mu = (\mu_0, \ldots, \mu_m) \mid 0 \le \mu_l \le L\}$ から $\{0,1\}$ への関数で $\sum$ はそのような ε 全部にわたって動く. $\{\overline{Q_1(\boldsymbol{t})}, \ldots, \overline{Q_{d(p)}(\boldsymbol{t})}\}$ を $\overline{R}(p)$ の K 上の basis とすると, $\left\{ \overline{\left(\prod_{\mu} t_{\mu}^{\varepsilon(\mu)p} \right) Q_i(\boldsymbol{t})} \;\middle|\; 1 \le i \le d(p),\ \varepsilon \right\}$ は K 上で $\overline{R}(2p)$ を生成するから

$$\dim_K \overline{R}(2p) \le 2^{\sharp\{\mu=(\mu_0,\ldots,\mu_m) \mid 0 \le \mu_l \le L\}} d(p) = 2^{(L+1)^{m+1}} d(p). \quad \square$$

補題 10. $\operatorname{ind} F(z;\boldsymbol{t}) < \infty$.

証明. 補題 6 より, $f_0(z), \ldots, f_m(z)$ は $\mathbb{Q}(\subset \mathbb{C}(z))$ 上代数的独立だから,

$$F(z;\tau) = \sum_{\substack{\mu=(\mu_0,\ldots,\mu_m),\\ 0 \le \mu_l \le L}} \tau_{\mu} f_0(z)^{\mu_0} \cdots f_m(z)^{\mu_m} \not\equiv 0 \quad (\tau_{\mu} \in \mathbb{Z}).$$

一致の定理より, 正整数 k_0 が存在して $F(\alpha^{d^{k_0}};\tau) \ne 0$. $\operatorname{ind} F(z;\boldsymbol{t}) = \infty$ とすると, $F(z;\boldsymbol{t}) = \sum_{n=0}^{\infty} P_n(\boldsymbol{t}) z^n$ とおくとき, 任意の $n \ge 0$ に対し $P_n(\boldsymbol{t}) \in V(\tau)$. すなわち, 任意の $k \ge 0$ に対し $P_n(\boldsymbol{T}(\tau; 1, d^k, \ldots, d^{km}; y_0, \ldots, y_m) = 0$. 従って, $0 \ne F(\alpha^{d^{k_0}};\tau) = \sum_{n=0}^{\infty} P_n(\tau) \alpha^{d^{k_0}} = \sum_{n=0}^{\infty} P_n(\boldsymbol{T}(\tau; 1, \ldots, 1; 0, \ldots, 0)) \alpha^{d^{k_0}} = 0$ となるが, これは矛盾である. $\square$

Prop. 4 の証明. $B_h(z;\boldsymbol{t}) = \sum_{l=0}^{p} B_{hl}(\boldsymbol{t}) z^l$ とすると $B_{hl}(\boldsymbol{t}) \in R(p)$ だから, $\{\overline{Q_1^{(p)}(\boldsymbol{t})}, \ldots, \overline{Q_{d(p)}^{(p)}(\boldsymbol{t})}\}$ を $\overline{R}(p)$ の K 上の basis とすれば

$$\overline{B_{hl}(\boldsymbol{t})} = \sum_{i=1}^{d(p)} g_{hli} \overline{Q_i^{(p)}(\boldsymbol{t})} \quad (g_{hli} \in K)$$

と表せる.

$$\begin{aligned} E(z;\boldsymbol{t}) &= \sum_{h=0}^{p} B_h(z;\boldsymbol{t}) F(z;\boldsymbol{t})^h \\ &= \sum_{h=0}^{p} \sum_{l=0}^{p} B_{hl}(\boldsymbol{t}) z^l \left(\sum_{\substack{\mu=(\mu_0,\ldots,\mu_m),\\ 0 \le \mu_l \le L}} t_{\mu} f_0(z)^{\mu_0} \cdots f_m(z)^{\mu_m} \right)^h \\ &= \sum_{n=0}^{\infty} E_n(\boldsymbol{t}) z^n. \end{aligned} \tag{32}$$

$E_n(\boldsymbol{t}) \in R(2p)$ だから $\{\overline{Q_1^{(2p)}(\boldsymbol{t})}, \ldots, \overline{Q_{d(2p)}^{(2p)}(\boldsymbol{t})}\}$ を $\overline{R}(2p)$ の K 上の basis とすると

$$\overline{E_n(\boldsymbol{t})} = \sum_{j=1}^{d(2p)} f_{nj} \overline{Q_j^{(2p)}(\boldsymbol{t})} \quad (f_{nj} \in K)$$

と表せる. 従って, $(K[\boldsymbol{t}]/V(\tau))[[z]]$ において (32) より

$$\sum_{h=0}^{p} \sum_{l=0}^{p} \left(\sum_{i=1}^{d(p)} g_{hli} \overline{Q_i^{(p)}(\boldsymbol{t})} \right) z^l \left(\sum_{\substack{\mu=(\mu_0,\ldots,\mu_m),\\ 0 \le \mu_l \le L}} \overline{t_{\mu}} f_0(z)^{\mu_0} \cdots f_m(z)^{\mu_m} \right)^h = \sum_{n=0}^{\infty} \left(\sum_{j=1}^{d(2p)} f_{nj} \overline{Q_j^{(2p)}(\boldsymbol{t})} \right) z^n$$

となるから $\overline{R}(2p)[[z]]$ において $\{\overline{Q_1^{(2p)}(\boldsymbol{t})},\dots,\overline{Q_{d(2p)}^{(2p)}(\boldsymbol{t})}\}$ の係数を比較すると

$$f_{nj}=\sum_{h=0}^{p}\sum_{l=0}^{p}\sum_{i=1}^{d(p)}c_{nhlij}g_{hli}\quad(c_{nhlij}\in K;\ n\geq 0,\ 1\leq j\leq d(2p)).$$

$J=[2^{-(L+1)^{m+1}}p^2]$ とおくと, 補題 9 より

$$\begin{aligned}&\sharp\{g_{hli}\mid 0\leq h\leq p,\ 0\leq l\leq p,\ 1\leq i\leq d(p)\}\ =\ (p+1)^2d(p)\\ >\ & p^2d(p)\ \geq\ J2^{(L+1)^{m+1}}d(p)\\ \geq\ & Jd(2p)\ =\ \sharp\{f_{nj}\mid 0\leq n\leq J-1,\ 1\leq j\leq d(2p)\}.\end{aligned}$$

よって, $f_{nj}=0$ $(0\leq n\leq J-1,\ 1\leq j\leq d(2p))$ をみたす少なくともひとつは 0 ではない g_{hli} $(0\leq h\leq p,\ 0\leq l\leq p,\ 1\leq i\leq d(p))$ が存在する. $f_{nj}=0$ $(1\leq j\leq d(2p))\iff\overline{E_n(\boldsymbol{t})}=0\iff E_n(\boldsymbol{t})\in V(\tau)$ だから, このような g_{hli} をとれば, $I\geq J$ かつ 或る h $(0\leq h\leq p)$ が存在して $\operatorname{ind}B_h(z;\boldsymbol{t})<\infty$.

$r:=\min\{h\mid \operatorname{ind}B_h(z;\boldsymbol{t})<\infty\}$ とし, $E_0(z;\boldsymbol{t}):=\sum_{h=r}^{p}B_h(z;\boldsymbol{t})F(z;\boldsymbol{t})^{h-r}$ とおくと,

$$\begin{aligned}I\ &=\ \operatorname{ind}\left(\underbrace{\sum_{h=0}^{r-1}B_h(z;\boldsymbol{t})F(z;\boldsymbol{t})^h+F(z;\boldsymbol{t})^rE_0(z;\boldsymbol{t})}_{\in V(\tau)[[z]]}\right)\\ &=\ \operatorname{ind}\left(F(z;\boldsymbol{t})^rE_0(z;\boldsymbol{t})\right)\\ &=\ r\operatorname{ind}F(z;\boldsymbol{t})+\operatorname{ind}E_0(z;\boldsymbol{t})\qquad(\because\text{補題 }8).\end{aligned}$$

$I\geq J$ だから

$$\operatorname{ind}E_0(z;\boldsymbol{t})\geq J-r\operatorname{ind}F(z;\boldsymbol{t})\geq 2^{-(L+1)^{m+1}}p^2-1-p\operatorname{ind}F(z;\boldsymbol{t})$$

である. 補題 10 より $\operatorname{ind}F(z;\boldsymbol{t})<\infty$ だから $\boxed{2^{-(L+1)^{m+1}}>c_1}$ かつ p を十分大きくとれば $\operatorname{ind}E_0(z;\boldsymbol{t})\geq c_1p^2$ となる. よって, $E_0(z;\boldsymbol{t})$ にその係数達の共通公分母をかけたものを $E(z;\boldsymbol{t})$ とすればよい. □

参考. 定理 3 の証明における p は以下のように具体的に定められる.
$|\alpha|^{2^{-(L+1)^{m+1}}}<|\alpha|^{c_1}<c_3<1$ より $c_3=|\alpha|^{2^{-(L+1)^{m+1}-1}}$ とすれば

$$-p\log c_3=2^{-(L+1)^{m+1}-1}p(-\log|\alpha|),\quad \log c_{10}=\left(1+(m+1)L(L+1)^{m+1}d^{-1}\right)\log D$$

だから

$$p>2^{1+(L+1)^{m+1}}\left(1+(m+1)L(L+1)^{m+1}d^{-1}\right)(-\log|\alpha|)^{-1}\log D$$

をみたす p をとれば矛盾が導かれる. □

注意. 上記の計算によると m が大きいほど p を大きくとる必要があり, これは自然である. また, d が大きいほど p は小さくとれる. 一方 α に関して, $|\alpha|$ が 1 に近いほど, また, D が大きいほど p を大きくとる必要がある.

参考文献

[1] K. Barré-Sirieix, G. Diaz, F. Gramain, G. Philibert: Une preuve de la conjecture de Mahler-Manin, *Invent. Math.* **124** (1996), pp. 1–9.

[2] Y.V. Nesterenko: Modular functions and transcendence questions, *Math. Sb.* **187** (9) (1996), pp. 65–96 (Russian). Engl. transl., Sbornik Math. **187** (9–10) (1996), pp. 1319–1348.

和書

[3] 天羽 雅昭: 超越数論入門 — マーラー - マニン予想の証明 —, Seminar on Math. Sci. No. 26 (1998), Department of Math., Keio Univ.

[4] J.H. シルヴァーマン (Silverman) 著, 鈴木 治郎 訳: 楕円曲線論概説 上, 2003, シュプリンガー・フェアラーク東京.

田中 孝明
慶應義塾大学理工学部
〒 223–8522
横浜市港北区日吉 3 丁目 14 − 1
e-mail: takaaki@math.keio.ac.jp

Taka-aki Tanaka
Department of Mathematics
Keio University
Hiyoshi 3–14–1, Kohoku-ku
Yokohama, 223–8522 JAPAN