

Mahler の方法による代数的独立性の簡潔な証明

田中 孝明

定理. $f(z) = \sum_{k=0}^{\infty} z^{d^k}$ ($2 \leq d \in \mathbb{Z}$) とする.

$\alpha \in K$: 虚 2 次体, $0 < |\alpha| < 1 \implies \{f^{(l)}(\alpha) \mid l \geq 0\}$ は代数的独立.

証明. $f_l(z) = \left(z \frac{d}{dz}\right)^l f(z) = \sum_{k=0}^{\infty} d^{lk} z^{d^k}$ ($l \geq 0$) とおく. $\forall m \geq 0$ に対し, $\{f_l(\alpha) \mid 0 \leq l \leq m\}$ と $\{f^{(l)}(\alpha) \mid 0 \leq l \leq m\}$ は $\mathbb{Q}(\alpha)$ 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 $\exists m \geq 0$ s.t. $\{f^{(l)}(\alpha) \mid 0 \leq l \leq m\}$: 代数的従属 $\iff \{f_l(\alpha) \mid 0 \leq l \leq m\}$: 代数的従属
 $\implies \sum_{\substack{\mu=(\mu_0, \dots, \mu_m), \\ 0 \leq \mu_l \leq L}} \tau_{\mu} f_0(\alpha)^{\mu_0} \cdots f_m(\alpha)^{\mu_m} = 0$ ($\tau_{\mu} \in \mathbb{Z}$). ただし, τ_{μ} は not all 0.

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

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

とする.

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

$f_l(z)$ は

$$f_l(z) = d^l f_l(z^d) + z \quad (l \geq 0) \quad (1)$$

をみたま. (1) を iterate すると

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

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

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

とする. 即ち,

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

このとき,

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

従って,

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

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

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

定義 1.

$$V(\boldsymbol{\tau}) := \{Q(\mathbf{t}) \in K[\mathbf{t}] \mid Q(\mathbf{T}(\boldsymbol{\tau}; 1, d^k, \dots, d^{km}; y_0, \dots, y_m)) = 0 \text{ for } \forall k \geq 0\}.$$

さらに, $P(z; \mathbf{t}) = \sum_{n=0}^{\infty} P_n(\mathbf{t}) z^n \in K[\mathbf{t}][[z]]$ に対し,

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

ただし, $P_n \in V(\boldsymbol{\tau}) (\forall n \geq 0) \implies \text{ind } P(z; \mathbf{t}) := \infty$.

下記の Proposition 1 は補助関数の構成に関するものであり, 証明は後述する (6 頁参照). 以下, c_1, c_2, \dots は p, k に依存しない正定数, $c_1(p), c_2(p), \dots$ は p には依存するが k には依存しない正定数 とする.

Proposition 1. p を十分大きな正整数とする.

$$B_0(z; \mathbf{t}), \dots, B_p(z; \mathbf{t}) \in \mathcal{O}_K[z; \mathbf{t}], \quad \deg_z B_h, \deg_{t_{\boldsymbol{\mu}}} B_h \leq p \quad (0 \leq h \leq p, \boldsymbol{\mu})$$

であり, 次の (i), (ii) をみたすものが存在する.

(i) $\text{ind } B_0(z; \mathbf{t}) < \infty$.

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

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

Proposition 2. Prop. 1 の $E(z; \mathbf{t})$ に対し, $k > c_2(p)$ なら

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

証明. $b_l^{(k)}(\alpha) = f_l(\alpha) - d^{kl} f_l(\alpha^{d^k})$, $0 \leq l \leq m$ だから $f_l(\alpha^{d^k}) \rightarrow f_l(0)$ ($k \rightarrow \infty$) に注意すると, $c_4 > d^m$ とすれば, $|b_l^{(k)}(\alpha)| \leq c_4^k$ ($0 \leq l \leq m$) for $\forall k \gg 1$.

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

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

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

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

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

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 $E(z; \mathbf{t}) = \sum_{n=0}^{\infty} (\sum_{\lambda} g_{\lambda n} \mathbf{t}^\lambda) z^n$. $I = \text{ind } E(z; \mathbf{t})$ だから, k : 十分大 のとき

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

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

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

定理の証明の完結.

$b_l^{(k)}(z) = \sum_{h=0}^{k-1} d^{lh} z^{d^h}$ だから $D = \text{den}(\alpha)$ とすると、 $\text{den}(b_l^{(k)}(\alpha)) = D^{d^{k-1}}$ ($0 \leq l \leq m$). Prop. 2 の証明と同様にして

$$\text{den}(T_{\boldsymbol{\mu}}(\boldsymbol{\tau}; 1, d^k, \dots, d^{km}; b_0^{(k)}(\alpha), \dots, b_m^{(k)}(\alpha))) \leq D^{(m+1)Ld^{k-1}}.$$

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

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

$B_0(z; \mathbf{t}) \in \mathcal{O}_K[z; \mathbf{t}]$, $\deg_z B_0, \deg_{t_{\boldsymbol{\mu}}} B_0 \leq p$, $\#\{\boldsymbol{\mu} = (\mu_0, \dots, \mu_m) \mid 0 \leq \mu_l \leq L\} = (L+1)^{m+1}$ だから

$$\begin{aligned} D^*(k) &:= \text{den}\left(E\left(\alpha^{d^k}; \mathbf{T}(\boldsymbol{\tau}; 1, d^k, \dots, d^{km}; \mathbf{b}^{(k)}(\alpha))\right)\right) \\ &\leq D^{pd^k + (m+1)L(L+1)^{m+1}pd^{k-1}} \\ &= c_{10}^{pd^k}. \quad \boxed{c_{10} = D^{1+(m+1)L(L+1)^{m+1}/d}} \end{aligned} \quad (2)$$

もし、 $E(\alpha^{d^k}; \mathbf{T}(\boldsymbol{\tau}; 1, d^k, \dots, d^{km}; \mathbf{b}^{(k)}(\alpha))) = B_0(\alpha^{d^k}; \mathbf{T}(\boldsymbol{\tau}; 1, d^k, \dots, d^{km}; \mathbf{b}^{(k)}(\alpha))) \neq 0$ ならば $D^*(k)E(\alpha^{d^k}; \mathbf{T}(\boldsymbol{\tau}; 1, d^k, \dots, d^{km}; \mathbf{b}^{(k)}(\alpha))) \in \mathcal{O}_K \setminus \{0\}$ であり、 K は虚 2 次体だから

$$D^*(k)|E(\alpha^{d^k}; \mathbf{T}(\boldsymbol{\tau}; 1, d^k, \dots, d^{km}; \mathbf{b}^{(k)}(\alpha)))| \geq 1. \quad (3)$$

Prop. 1 (i) より、 $\text{ind } B_0(z; \mathbf{t}) < \infty$ だから 下記の Prop. 3 より、 $\exists k_0 > c_2(p)$ (in Prop. 2) s.t. $B_0(\alpha^{d^{k_0}}; \mathbf{T}(\boldsymbol{\tau}; 1, d^{k_0}, \dots, d^{k_0 m}; \mathbf{b}^{(k_0)}(\alpha))) \neq 0$. (2), (3) と Prop. 2 より、 $1 \leq c_3^{p^2 d^{k_0}} c_{10}^{pd^{k_0}}$. よって、 $1 \leq c_3^p c_{10}$. 即ち、 $c_3^{-p} \leq c_{10}$. $0 < c_3 < 1$ だから、 p が十分大きいとき これは矛盾. \square

補題 1. $\{f_l(z) \mid l \geq 0\}$ は $\mathbb{C}(z)$ 上代数的独立.

Proposition 3. $P(z; \mathbf{t}) \in K[z; \mathbf{t}]$ に対し、

$$P(\alpha^{d^k}; \mathbf{T}(\boldsymbol{\tau}; 1, d^k, \dots, d^{km}; \mathbf{b}^{(k)}(\alpha))) = 0 \text{ for } \forall k \gg 1 \implies \text{ind } P(z; \mathbf{t}) = \infty.$$

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

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

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

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

となるから

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

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

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

とおける. このとき,

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

$G_h(z) = \sum_{n=0}^N \sum_{\boldsymbol{\lambda}=(\lambda_0, \dots, \lambda_m)} r_{n\boldsymbol{\lambda}h} z^n f_0(z)^{\lambda_0} \dots f_m(z)^{\lambda_m}$ とおくと, $G_h(z) \in \mathbb{C}[[z]]$.

補題 1 より, $r_{n\boldsymbol{\lambda}h}$ ($0 \leq n \leq N$, $\boldsymbol{\lambda}$) が not all 0 $\implies G_h(z) = c_{hl_h} z^{l_h} + c_{hl_{h+1}} z^{l_h+1} + \dots$, $c_{hl_h} \neq 0$. $G_h(z)$ の係数は $O(d^{mk})$ だから $G_h(\alpha^{d^k}) = c_{hl_h} \alpha^{l_h d^k} + o(\alpha^{l_h d^k})$.

$$M = \min_{0 \leq h \leq H} l_h, \quad H^* = \max\{h \mid c_{hM} \neq 0\}$$

とすると

$$\begin{aligned} & P(\alpha^{d^k}; \mathbf{T}(\boldsymbol{\tau}; 1, d^k, \dots, d^{km}; \mathbf{b}^{(k)}(\alpha))) \\ &= \sum_{h=0}^H d^{hk} \left(c_{hl_h} \alpha^{l_h d^k} + o(\alpha^{l_h d^k}) \right) \\ &= c_{H^*M} d^{H^*k} \alpha^{M d^k} + o(d^{H^*k} \alpha^{M d^k}), \quad c_{H^*M} \neq 0, \quad \text{for } \forall k \gg 1. \end{aligned}$$

これは矛盾. 従って,

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

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

以下, Prop. 1 の証明に用いる補題を述べる.

補題 2. $V(\boldsymbol{\tau})$ は $K[\mathbf{t}]$ の素イデアル.

証明. イデアルであることは明らか. $Q_1, Q_2 \in K[\mathbf{t}]$, $Q_1 Q_2 \in V(\boldsymbol{\tau})$ **i.e.** $Q_1(\mathbf{T}(\boldsymbol{\tau}; 1, d^k, \dots, d^{km}; y_0, \dots, y_m)) Q_2(\mathbf{T}(\boldsymbol{\tau}; 1, d^k, \dots, d^{km}; y_0, \dots, y_m)) = 0$ for $\forall k \geq 0$ とすると, Q_1, Q_2 の少なくとも一方, それを Q_1 としてよい, は $Q_1(\mathbf{T}(\boldsymbol{\tau}; 1, d^k, \dots, d^{km}; y_0, \dots, y_m)) = 0$ for ∞ -many $k \geq 0$.

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

だから $Q_1(\mathbf{T}(\boldsymbol{\tau}; 1, d^k, \dots, d^{km}; y_0, \dots, y_m)) \in K[d^k, y_0, \dots, y_m]$. Q_1 が y_0, \dots, y_m の多項式として $\neq 0 \implies Q_1$ の少なくともひとつの係数は d^k の多項式 $\neq 0$. しかし, ∞ -many $k \geq 0$ 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, $Q_1(\mathbf{T}(\boldsymbol{\tau}; 1, d^k, \dots, d^{km}; y_0, \dots, y_m)) \equiv 0$. すなわち, $Q_1 \in V(\boldsymbol{\tau})$.

\square

補題 3. $\text{ind } P_1(z; \mathbf{t}) P_2(z; \mathbf{t}) = \text{ind } P_1(z; \mathbf{t}) + \text{ind } P_2(z; \mathbf{t})$.

証明. $\text{ind } P_1(z; \mathbf{t}) = I$, $\text{ind } P_2(z; \mathbf{t}) = J$ とする. $P_1(z; \mathbf{t}) = \sum_{n=0}^{\infty} P_n(\mathbf{t}) z^n$, $P_2(z; \mathbf{t}) = \sum_{m=0}^{\infty} Q_m(\mathbf{t}) z^m$ とすると, $P_1(z; \mathbf{t}) P_2(z; \mathbf{t}) = \sum_{k=0}^{\infty} (\sum_{n+m=k} P_n(\mathbf{t}) Q_m(\mathbf{t})) z^k$ だから, $I = \infty$ or $J = \infty \implies \text{ind } P_1(z; \mathbf{t}) P_2(z; \mathbf{t}) = \infty$ は明らか. $I, J < \infty$ のとき,

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

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

$$\begin{aligned} \sum_{n+m=I+J} P_n(\mathbf{t})Q_m(\mathbf{t}) &= \sum_{n=0}^{I-1} P_n(\mathbf{t})Q_{I+J-n}(\mathbf{t}) + P_I(\mathbf{t})Q_J(\mathbf{t}) + \sum_{m=0}^{J-1} P_{I+J-m}(\mathbf{t})Q_m(\mathbf{t}) \\ &\in V(\boldsymbol{\tau}) \qquad \notin V(\boldsymbol{\tau}) \quad (\because \text{補題 2}) \qquad \in V(\boldsymbol{\tau}) \\ &\notin V(\boldsymbol{\tau}). \quad \square \end{aligned}$$

定義 2. p を正整数とする.

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

これは K -vector space.

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

$f(\mathbf{t}) \in R(p)$ に対し,

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

補題 4. $d(2p) \leq 2^{(L+1)^{m+1}} d(p)$.

証明. $R(2p) \ni \forall Q(\mathbf{t}) = \sum_{\varepsilon} \left(\prod_{\mu} t_{\mu}^{\varepsilon(\mu)p} \right) Q_{\varepsilon}(\mathbf{t})$, $Q_{\varepsilon}(\mathbf{t}) \in R(p)$ とかける. ただし, $\varepsilon(\cdot)$ は $\{\boldsymbol{\mu} = (\mu_0, \dots, \mu_m) \mid 0 \leq \mu_l \leq L\}$ 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. $\{\overline{Q_1(\mathbf{t})}, \dots, \overline{Q_{d(p)}(\mathbf{t})}\}$ を $\overline{R}(p)$ の K 上の basis とすると, $\left\{ \left(\prod_{\mu} t_{\mu}^{\varepsilon(\mu)p} \right) Q_i(\mathbf{t}) \mid 1 \leq i \leq d(p), \varepsilon \right\}$ は K 上で $\overline{R}(2p)$ を生成するから

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

補題 5. $\text{ind } F(z; \mathbf{t}) < \infty$.

証明. 補題 1 より, $f_0(z), \dots, f_m(z)$ は $\mathbb{Q}(\subset \mathbb{C}(z))$ 上代数的独立だから,

$$F(z; \boldsymbol{\tau}) = \sum_{\substack{\boldsymbol{\mu}=(\mu_0, \dots, \mu_m), \\ 0 \leq \mu_l \leq L}} \tau_{\boldsymbol{\mu}} f_0(z)^{\mu_0} \cdots f_m(z)^{\mu_m} \neq 0 \quad (\because \tau_{\boldsymbol{\mu}} \in \mathbb{Z}).$$

一致の定理より, $\exists k_0 \in \mathbb{N}$ s.t. $F(\alpha^{d^{k_0}}; \boldsymbol{\tau}) \neq 0$. $\text{ind } F(z; \mathbf{t}) = \infty$ とすると, $F(z; \mathbf{t}) = \sum_{n=0}^{\infty} P_n(\mathbf{t})z^n$ とおくと, $\forall n \geq 0$ に対し $P_n(\mathbf{t}) \in V(\boldsymbol{\tau})$. すなわち, $P_n(\mathbf{T}(\boldsymbol{\tau}; 1, d^k, \dots, d^{km}; y_0, \dots, y_m)) = 0$ for $\forall k \geq 0$. 従って, $0 \neq F(\alpha^{d^{k_0}}; \boldsymbol{\tau}) = \sum_{n=0}^{\infty} P_n(\boldsymbol{\tau})\alpha^{d^{k_0}n} = \sum_{n=0}^{\infty} P_n(\mathbf{T}(\boldsymbol{\tau}; 1, \dots, 1; 0, \dots, 0))\alpha^{d^{k_0}n} = 0$. これは矛盾. \square

Prop. 1 の証明. $B_h(z; \mathbf{t}) = \sum_{l=0}^p B_{hl}(\mathbf{t})z^l$ とすると $B_{hl}(\mathbf{t}) \in R(p)$ だから, $\{\overline{Q_1^{(p)}(\mathbf{t})}, \dots, \overline{Q_{d(p)}^{(p)}(\mathbf{t})}\}$ を $\overline{R(p)}$ の K 上の basis とすれば

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

と表せる.

$$\begin{aligned} E(z; \mathbf{t}) &= \sum_{h=0}^p B_h(z; \mathbf{t})F(z; \mathbf{t})^h \\ &= \sum_{h=0}^p \sum_{l=0}^p B_{hl}(\mathbf{t})z^l \left(\sum_{\substack{\mu=(\mu_0, \dots, \mu_m), \\ 0 \leq \mu_l \leq L}} t_{\mu} f_0(z)^{\mu_0} \cdots f_m(z)^{\mu_m} \right)^h = \sum_{n=0}^{\infty} E_n(\mathbf{t})z^n. \end{aligned} \quad (4)$$

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

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

と表せる. 従って, $(K[\mathbf{t}]/V(\boldsymbol{\tau}))[[z]]$ において (4) より

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

となるから $\overline{R(2p)}[[z]]$ において $\{\overline{Q_1^{(2p)}(\mathbf{t})}, \dots, \overline{Q_{d(2p)}^{(2p)}(\mathbf{t})}\}$ 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 4 より

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

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. $f_{nj} = 0$ ($1 \leq j \leq d(2p)$) $\iff \overline{E_n(\mathbf{t})} = 0 \iff E_n(\mathbf{t}) \in V(\boldsymbol{\tau})$ だから, このような g_{hli} をとれば, $I \geq J$ かつ $\exists h$ ($0 \leq h \leq p$) s.t. $\text{ind } B_h(z; \mathbf{t}) < \infty$.

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

$$\begin{aligned} I &= \text{ind} \left(\sum_{h=0}^{r-1} B_h(z; \mathbf{t})F(z; \mathbf{t})^h + F(z; \mathbf{t})^r E_0(z; \mathbf{t}) \right) \\ &\quad \in V(\boldsymbol{\tau})[[z]] \\ &= \text{ind} (F(z; \mathbf{t})^r E_0(z; \mathbf{t})) \\ &= r \text{ind } F(z; \mathbf{t}) + \text{ind } E_0(z; \mathbf{t}) \quad (\because \text{補題 3}). \end{aligned}$$

$I \geq J$ だから $\text{ind } E_0(z; \mathbf{t}) \geq J - r \text{ind } F(z; \mathbf{t}) \geq 2^{-(L+1)^{m+1}} p^2 - 1 - p \text{ind } F(z; \mathbf{t})$. 補題 5 より $\text{ind } F(z; \mathbf{t}) < \infty$ だから $\boxed{2^{-(L+1)^{m+1}} > c_1}$, p : 十分大にとれば $\text{ind } E_0(z; \mathbf{t}) \geq c_1 p^2$. よって, $E_0(z; \mathbf{t})$ にその係数達の共通公分母をかけたものを $E(z; \mathbf{t})$ とすればよい. \square

参考 : 定理の証明における 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 $-p \log c_3 = 2^{-(L+1)^{m+1}-1} p (-\log |\alpha|)$, $\log c_{10} = 1 + (m+1)L(L+1)^{m+1} d^{-1} \log D$ だから

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

をみたす p をとれば矛盾. \square

※ $|\alpha| \sim 1$ かつ $D \gg 0$ なる α ほど p を大きくする.

★ 定理は $\alpha \in \overline{\mathbb{Q}}$ に対しても成り立つ. 証明は下記の基本不等式を用いる :

$\beta \in \overline{\mathbb{Q}}, \beta \neq 0, \boxed{n = \deg \beta}, \beta = \beta^{(1)}, \beta^{(2)}, \dots, \beta^{(n)} : \beta$ の共役.
 $\overline{|\beta|} := \max\{|\beta^{(1)}|, |\beta^{(2)}|, \dots, |\beta^{(n)}|\}, d := \text{den}(\beta). N_{\mathbb{Q}(\beta)/\mathbb{Q}}(d\beta) \in \mathbb{Z} \setminus \{0\}$ だから
 $1 \leq |N_{\mathbb{Q}(\beta)/\mathbb{Q}}(d\beta)| = d^n |\beta^{(1)}| |\beta^{(2)}| \dots |\beta^{(n)}| \leq d^n |\beta| \overline{|\beta|}^{n-1}$. 故に,

$$|\beta| \geq d^{-n} \overline{|\beta|}^{n+1}.$$

両辺の対数をとると 基本不等式 :

$$\log |\beta| \geq -2n \max\{\log \overline{|\beta|}, \log \text{den}(\beta)\}$$

を得る.