

多変数多項式の解析的因数分解アルゴリズム

岩見 真希

MAKI IWAMI

筑波大学数理解析科学研究所

GRADUATE SCHOOL OF PURE AND APPLIED SCIENCES, UNIVERSITY OF TSUKUBA*

1 はじめに

解析的因数分解とは、形式的べき級数環での因数分解のことであり、代数幾何で非常に重要な概念である。 K を標数 0 の数体、 $\bar{K}$ を K の代数閉体、 x を主変数、 $u_1, \dots, u_\ell$ (以下 $\mathbf{u}$ と略記) を従変数、 $K[x, \mathbf{u}]$, $K(x, \mathbf{u})$, $K\{x, \mathbf{u}\}$ をそれぞれ K 上の変数 $x, \mathbf{u}$ の多項式環、有理式体、形式的べき級数環とする。 $K\{x, \mathbf{u}\}$ の単元でない非零な多項式 $F(x, \mathbf{u}) \in \bar{K}[x, \mathbf{u}]$ が $\bar{K}\{x, \mathbf{u}\}$ で既約 (可約) であることを、解析的に既約 (可約) であるといい、 $\bar{K}\{x, \mathbf{u}\}$ で既約な因子の積に分解することを、解析的因数分解という。実際は、Weierstrass preparation theorem により、1 つの変数については多項式とみなすことができるため、 $\bar{K}\{\mathbf{u}\}[x]$ での因数分解としてよい。3 変数以上のことを多変数と、形式的べき級数環の因子のことを解析的因子とよぶ。

計算代数でよく知られているように、Hensel 構成により、多変数多項式を $\bar{K}\{\mathbf{u}\}[x]$ で分解することができる。したがって、Hensel 構成が破綻するところでの分解、すなわち、一般性を失うことなく $F(x, \mathbf{0}) = x^D$ ($D = \deg_x(F) \geq 2$) なる $F(x, \mathbf{u})$ の分解が問題となる ($\deg_x(F)$ は F の x の次数をあらわす)。Hensel 構成が破綻するこれらの因子は、その拡張として考案された拡張 Hensel 構成 [SK99] で分解することができる。拡張 Hensel 構成とは、与式から一意に定まる “Newton 多項式” を互いに素な因子の積に分解し、それらを初期因子として与式の因子を構成する方法であり、得られた因子を拡張 Hensel 因子とよぶ。

初期因子を多項式にとったときの拡張 Hensel 因子は、2 変数では解析的因子となるのに対し、多変数では主変数に関しては多項式であるが、一般に従変数に関しては有理式級数となる。2 章で定義するが、形式的べき級数環を含んだこの環を $\bar{K}\{(\mathbf{u})\}[x]$ と表記する。したがって、多変数では、最終目標は $\bar{K}\{\mathbf{u}\}[x]$ での因数分解であるものの、最初の目標は $\bar{K}\{(\mathbf{u})\}[x]$ での因数分解となる。

Newton 多項式を既約な多項式の積に分解したものが無平方の場合、2 変数では、拡張 Hensel 因子がそのまま解析的既約因子となる。多変数では $\bar{K}\{(\mathbf{u})\}[x]$ の既約因子となっており、有理式部分の分母に着目して因子をかけあわせることで、分母をキャンセルさせ、解析的既約因子を得ることができる ([SI00])。

Newton 多項式が無平方でない場合、拡張 Hensel 因子のうち、 g^m ($m \geq 2, g$ は既約多項式) を初期因子にもつような因子 ($g^m + \dots$) の解析的既約性判定および可約な場合の分解法が問題となる。2 変数に対しては、[Ab88, Ab89, Ab90, AM73] のアイデアに基づいて [Kuo89] そして [McC97] によって完成された “展開基底 (expansion base)” を用いた方法と、拡張 Hensel 構成を利用した方法 [Sas00] の 2 つがある。前者は、重複既約成分 g を新たな変数とし、これを主変数として展開する方法であるのに対し、後者は、分数べきをだすことで主変数に関して一次因子の積にまで分解し、これらの互いに素な因子を初期因子として拡張 Hensel 構成し、最後にかけあわせて解析的因子をつくるという方法である。

本稿では、多変数で Newton 多項式が無平方でない場合の解析的因数分解法として、上記 2 変数の 2 つの方法の多変数への拡張を述べる。まず 2 章で、初期処理として拡張 Hensel 構成を施したあと問題となる因子の型とその環を定義し、その解決方法として、3 章で拡張 Hensel 構成を用いた方法 [Iwa03] を、4 章で展開基底を用いた方法 [Iwa04] を述べる。特に後者の Lifting 部分は、展開基底と拡張 Hensel 構成を融合させたものといえる。

*maki@math.tsukuba.ac.jp

2 多変数の因子の環と問題となる型

与えられた多項式 $F(x, u)$ に Hensel 構成を施すことにより、一般性を失うことなく、 $F(x, 0) = x^D$ ($D = \deg_x(F) \geq 2$) なる $F(x, u)$ に帰着する。 $F(x, 0) = x^D$ は互いに素な因子の積に分解できないため Hensel 構成は破綻する。ここで、拡張 Hensel 構成を施す。まず、 $u_i \rightarrow tu_i$ ($i = 1, \dots, \ell$) とすることで、従変数に関する全次数変数 t を導入する。そして、横軸に x のべき、縦軸に t のべきをとった 2 次元平面上に $F(x, tu)$ の各項に対応する点をプロットする。凸包の 1 つの下辺を Newton 線、Newton 線上にある点に対応する項を足し合わせたものを Newton 多項式とよび、それぞれ $\mathcal{L}_{\text{New}}$, F_{New} とあらわす。この Newton 多項式 F_{New} を互いに素な因子の積に分解し、これらを初期因子として構成するのが拡張 Hensel 構成である。初期因子を多項式とする拡張 Hensel 構成により、従変数に関する有理式級数を係数とする多項式の積に分解することができる。次の例で、拡張 Hensel 因子 (拡張 Hensel 構成によって得られる因子) の形を示す。

$F(x, 0, 0) = x^{18}$ かつ Newton 多項式が $F_{\text{New}} = (x^3 - t(u_1 + u_2))^3 (x^3 - tu_2)^3$ であるような $F(x, u_1, u_2) = ((x^3 - (u_1 + u_2))^2 (x^3 - u_2) + x^6 u_1^2 + x^3 u_1 u_2^2 + u_2^4 + x^6 (u_2^3 + u_1 u_2^2)) \times ((x^3 - (u_1 + u_2))(x^3 - u_2)^2 + x^3 u_1^3 + x^6 u_1^2 u_2^2)$
 $F_1^{(0)} \stackrel{\text{def}}{=} (x^3 - t(u_1 + u_2))^3$, $F_2^{(0)} \stackrel{\text{def}}{=} (x^3 - tu_2)^3$ を初期因子として拡張 Hensel 構成することで、次のような $F = F_1^{(\infty)} F_2^{(\infty)}$ なる因子 $F_1^{(\infty)}$, $F_2^{(\infty)}$ が得られる。

$$\begin{aligned} F_1^{(\infty)} &= F_1^{(0)} + t^2 x^6 (2u_1^2 + u_1 u_2 - u_2^2 - \frac{u_2^3}{u_1} - \frac{u_2^4}{u_1^2}) + t^3 x^3 (\dots + \frac{5u_2^4}{u_1} + \frac{2u_2^5}{u_1^2}) + \dots \\ F_2^{(\infty)} &= F_2^{(0)} + t^2 x^6 (-u_1^2 - u_1 u_2 + u_2^2 + \frac{u_2^3}{u_1} + \frac{u_2^4}{u_1^2}) + t^3 x^3 (\dots - \frac{2u_2^4}{u_1} - \frac{2u_2^5}{u_1^2}) + \dots \end{aligned}$$

このように、多変数では、主変数 x に関して多項式で従変数の全次数変数 t に関して正の整数べきだが、従変数に関しては有理式級数となる。(2 変数では、例えば $u_1 = u_2 = u$ として考えると、(*)-部分は $-u^2 - uu + u^2 + \frac{u^3}{u} + \frac{u^4}{u^2} = u^2$ のように、1 項にまとる。2 変数では、多項式を初期因子とした Hensel 因子は $\bar{K}\{u\}[x]$ の因子である。) この有理式級数を次で定義する。

定義 1 (多変数 Hensel 因子の環 $\bar{K}\{(u)\}[x]$)

$$\bar{K}\{(u)\} \stackrel{\text{def}}{=} \left\{ \sum_{k=0}^{\infty} \left[\frac{N_k(u)}{D_k(u)} \right] \mid \begin{array}{l} N_k(u) \text{ と } D_k(u) \text{ は } u \text{ の同次多項式 s.t.} \\ \text{tdeg}(N_k) - \text{tdeg}(D_k) = k \ (k = 0, 1, 2, \dots) \end{array} \right\}.$$

多変数では、初期因子を多項式としても、得られる Hensel 因子は $\bar{K}\{(u)\}[x]$ の因子である。したがって、多変数における解析的因数分解では、まず $\bar{K}\{(u)\}[x]$ で因数分解してから、因子をかけあわせて $\bar{K}\{u\}[x]$ の因数分解を得るという戦略をとることになる。

F_{New} の $\bar{K}[x, u]$ での因数分解を次とする。ここで、 $f_n(u)$ は F の主係数である。

$$F_{\text{New}} = f_n(0) x^{n_0} g_1(x, u) \cdots g_R(x, u) g_{R+1}(x, u)^{m_{R+1}} \cdots g_{R+R'}(x, u)^{m_{R+R'}},$$

$g_i(x, u) (i = 1, \dots, R + R')$ は $\bar{K}[x, u]$ の互いに素な既約因子, $0 \leq n_0 \in \mathbb{Z}$, $m_{R+j} \geq 2$ ($j = 1, \dots, R'$)).

ここで、 $F_0^{(0)} = f_n(0) x^{n_0}$, $F_1^{(0)} = g_1(x, u)$, $\dots$, $F_R^{(0)} = g_R(x, u)$, $F_{R+1}^{(0)} = g_{R+1}(x, u)^{m_{R+1}}$, $\dots$, $F_{R+R'}^{(0)} = g_{R+R'}(x, u)^{m_{R+R'}}$ とおき、これらを初期因子として次のように拡張 Hensel 構成する。(A を初期因子として拡張 Hensel 構成して得られた結果が B であるとき、 $A \Rightarrow B$ とあらわす)

$$\begin{array}{cccccccc} F_{\text{New}} & = & F_0^{(0)} & F_1^{(0)} & \cdots & F_R^{(0)} & F_{R+1}^{(0)} & \cdots & F_{R+R'}^{(0)} \\ \downarrow & \vdots & \downarrow & \downarrow & \cdots & \downarrow & \downarrow & \cdots & \downarrow \\ F(x, u) & = & F_0^{(\infty)} & F_1^{(\infty)} & \cdots & F_R^{(\infty)} & F_{R+1}^{(\infty)} & \cdots & F_{R+R'}^{(\infty)} \end{array}$$

このとき、各因子は次のように処理する。

$F_0^{(\infty)}(x, u)$: 原点に特異点をもつので、再帰的に拡張 Hensel 構成して分解する。

$F_1^{(\infty)}(x, u), \dots, F_R^{(\infty)}(x, u)$: 低次部分 $g_i(x, u)$ ($i = 1, \dots, R$) が既約ゆえ $\overline{K}\{(u)\}[x]$ の既約因子である。

$F_{R+1}^{(\infty)}(x, u), \dots, F_{R+R'}^{(\infty)}(x, u)$: 低次部分 $g_i(x, u)^m$ ($i = R+1, \dots, R+R'$, $m \geq 2$) が互いに素な多項式因子の積に分解されていないため、同じ方法では分解できない。

よって、 $F_i^{(\infty)}(x, u)$ の低次部分 $g_i(x, u)^m$ ($i = R+1, \dots, R+R'$) が $\overline{K}\{(u)\}[x]$ でどのように高次項を取り込み、因数分解されるかが問題となる。

以後、一般性を失うことなく $F(x, u) = g^m + \dots$ (g は $\overline{K}[x, u]$ の既約因子、 $F_{\text{New}} = g^m$, $m \geq 2$) とし、まず $F(x, u)$ の $\overline{K}\{(u)\}[x]$ での因数分解、次に $\overline{K}\{u\}[x]$ での因数分解という順で解析的既約因子を求める。

3 拡張 Hensel 構成を用いた分解法 [Iwa03]

アルゴリズム 1 (拡張 Hensel 構成を用いた解析的因数分解)

1. $F_{\text{New}} = g^m$ の既約多項式 g を、代数関数 $\theta_1, \dots, \theta_{\hat{d}}$ を導入して互いに素な因子の積に分解し、 $\overline{K}(\theta_1, \dots, \theta_{\hat{d}})\{(u)\}[x]$ で拡張 Hensel 構成。 t は従変数の全次数変数。

$$\begin{aligned} F_{\text{New}} = g^m &= (x - t^{\hat{d}/\hat{d}}\theta_1)^m \cdots (x - t^{\hat{d}/\hat{d}}\theta_{\hat{d}})^m, \quad \hat{d}, \hat{\delta} \in \mathbb{N} \text{ s.t. } \hat{\delta}/\hat{d} = -|\mathcal{L}_{\text{New}} \text{ の傾き}| \text{ かつ } \gcd(\hat{d}, \hat{\delta}) = 1. \\ &= G_1^{(0)} \cdots G_{\hat{d}}^{(0)} \\ \text{拡張 Hensel 構成} &\quad \downarrow \quad \cdots \quad \downarrow \\ F(x, u) &= G_1^{(\infty)} \cdots G_{\hat{d}}^{(\infty)}, \quad G_i^{(\infty)} \in \overline{K}(\theta_i)\{(u)\}[x] \quad (i = 1, \dots, \hat{d}) \end{aligned}$$

$G_i^{(\infty)} \xrightarrow{\theta_i \rightarrow \theta_j} G_j^{(\infty)}$ ($G_1^{(\infty)}, \dots, G_{\hat{d}}^{(\infty)}$ は共役であるという) ゆえ、2., 3. はどれか 1 つの i について計算すれば十分。

2. $G_i^{(\infty)} \stackrel{\text{def}}{=} x^m + g_{i,m-1}(u)x^{m-1} + \dots + g_{i,0}(u)$ に変換 $T_{x\theta_i} : G_i(x, u) \mapsto H_i(x, u) \stackrel{\text{def}}{=} G_i(x - g_{i,m-1}(u)/m, u)$ を施す。
3. $H_{i\text{New}}$ の $\overline{K}(\theta_i)\{(u)\}[x]$ での因数分解を次とする。ただし $0 \leq r \in \mathbb{Z}$; $m_{R+1}, \dots, m_{R+R'} \geq 2$ 。

$$H_{i\text{New}} = x^r h_{i1}(x, u) \cdots h_{iR}(x, u) h_{iR+1}(x, u)^{m_{R+1}} \cdots h_{iR+R'}(x, u)^{m_{R+R'}}$$

- (a) $H_{i\text{New}} = h_{i1}(x, u)$ ならば、 F は $\overline{K}\{(u)\}[x]$ で既約。
- (b) $H_{i\text{New}} = h_{i1}(x, u)^{m_1}$ (i.e. $R = 0$) ならば、 $j \triangleq 1$, $H_{ij}^{(\infty)} \triangleq H_i$ として (c)iii. へ。
- (c) $H_{i0}^{(0)} = x^r$, $H_{ij}^{(0)} = h_{ij}(x, u)$ ($j = 1, \dots, R$), $H_{ij}^{(0)} = h_{ij}(x, u)^{m_j}$ ($j = R+1, \dots, R+R'$) とおいて拡張 Hensel 構成。

i. $H_{i0}^{(\infty)}$: 再帰的に拡張 Hensel 構成して分解する。

ii. $H_{ij}^{(\infty)}$ ($j = 1, \dots, R$): $\prod_{i=1}^{\hat{d}} [T_{x\theta_i}^{-1} \cdot H_{ij}^{(\infty)}]$ を計算。これが $\overline{K}\{(u)\}[x]$ の既約因子である。

iii. $H_{ij}^{(\infty)}$ ($j = R+1, \dots, R+R'$):

- $\deg_x(h_{ij}) = 1$ ならば、 $G_i^{(\infty)} \triangleq H_{ij}$, $m \triangleq m_j$ として 2. へ。
- $\deg_x(h_{ij}) \geq 2$ ならば、 $F \triangleq H_{ij}^{(\infty)}$, $g \triangleq h_{ij}(x, u)$, $m \triangleq m_j$ として 1. へ。

新たな代数関数 $\theta_{\hat{d}+1}, \dots, \theta_{\hat{d}+\deg_x(h_{ij})}$ を導入して $\overline{K}(\theta_i, \theta_{\hat{d}+1}, \dots, \theta_{\hat{d}+\deg_x(h_{ij})})\{(u)\}$ 上で再帰的に計算することで $\overline{K}(\theta_i)\{(u)\}[x]$ での因数分解 $H_{ij}^{(\infty)} = H_{ij1} \cdots H_{ij\lambda_j}$ を得る。

このとき、 $\prod_{i=1}^{\hat{d}} [T_{x\theta_i}^{-1} \cdot H_{ij1}^{(\infty)}], \dots, \prod_{i=1}^{\hat{d}} [T_{x\theta_i}^{-1} \cdot H_{ij\lambda_j}^{(\infty)}]$ が F の $\overline{K}\{(u)\}[x]$ での既約因子。

4. $\overline{K}\{(u)\}[x]$ の既約因子を分母に着目してかけあわせ、 $\overline{K}\{u\}[x]$ の既約因子を得る。

4 展開基底を用いた分解法 [Iwa04]

$F_{\text{New}} = g^m$ (g は $\overline{K}[x, u]$ の既約因子、 $m \geq 2$) なる $F(x, tu)$ (t は従変数の全次数変数) に対して、 $G_{-1} \stackrel{\text{def}}{=} t$, $G_0 \stackrel{\text{def}}{=} x$, $G_1 \stackrel{\text{def}}{=} g$ とおく。 $\mathcal{G} = (G_{-1}, G_0, G_1)$ を展開基底とよぶ。 G_i の weight w_i ($i = -1, 0$)

をそれぞれ $w_{-1} \stackrel{\text{def}}{=} 1$, $w_0 \stackrel{\text{def}}{=} -|\text{Newton 線 } \mathcal{L}_{\text{New}} \text{ の傾き }|$ と定義する. F を G_1, G_0, G_{-1} の順に割ること
で、一意表現の $\mathcal{G}$ -adic expansion $F = \sum_{e_1=0}^m c_{(e_{-1}, e_0, e_1)} G_{-1}^{e_{-1}} G_0^{e_0} G_1^{e_1}$ ($c_{(e_{-1}, e_0, e_1)} \in \overline{K}\{(u)\}$) を得る. 横
軸に G_1 のべき, 縦軸に G_{-1} と G_0 の weight 付きのべきの和をとった 2 次元平面上に、各項に対応する
点 $(e_1, w_{-1}e_{-1} + w_0e_0)$ をプロットする (すなわち、重複既約多項式 $G_1 = g$ を新たな主変数とみなしてい
る). このときの Newton 線を $\mathcal{L}_{G_1\text{New}}$, Newton 多項式を $F_{G_1\text{New}}$ とあらわす. このとき、 G_1 の weight を
 $w_1 \stackrel{\text{def}}{=} -|\mathcal{L}_{G_1\text{New}} \text{ の傾き }|$ と定義する. 再び $F_{G_1\text{New}} = g_1^{m_1}$ (g_1 は既約多項式, $m_1 \geq 2$) の場合、 $G_2 \stackrel{\text{def}}{=} g_1$
として、展開基底に $\mathcal{G} = (G_{-1}, G_0, G_1, G_2)$ と追加、 G_2, G_1, G_0, G_{-1} の順に割ること
で $\mathcal{G}$ -adic expansion $F = \sum_{e_2=0}^{m_1} c_{(e_{-1}, e_0, e_1, e_2)} G_{-1}^{e_{-1}} G_0^{e_0} G_1^{e_1} G_2^{e_2}$ ($c_{(e_{-1}, e_0, e_1, e_2)} \in \overline{K}\{(u)\}$) を計算し、横軸に G_2 のべき, 縦軸に
 G_{-1}, G_0, G_1 の weight 付きのべきの和を取り、各項に対応する点 $(e_1, w_{-1}e_{-1} + w_0e_0)$ をプロットし、 $F_{G_2\text{New}}$
を $\overline{K}\{(u)\}$ 上で因数分解する. このステップを、新たな Newton 多項式が $\overline{K}\{(u)\}$ 上で互いに素な因子に
分解できるか、 $F_{G_s\text{New}} = g_s^{m_s}$ で $m_s = 1$ となるまで繰り返す. 結果として、 F が $\overline{K}\{(u)\}$ 上可約ならば、
Newton 多項式が互いに素な因子の積に分解され、後述する Lifting 方法により、 F の $\overline{K}\{(u)\}[x]$ での因数
分解を得る. 最後に、分母がキャンセルするように分母に着目してかけあわせて解析的既約因子を得る.

4.1 Newton 多項式の Pseudo Form への変形

展開基底 $\mathcal{G} = (G_{-1}, G_0, \dots, G_s)$, $\mathcal{G}$ -adic expansion $F = \sum_{e_s=0}^{D_s} c_{(e_{-1}, e_0, \dots, e_s)} G_{-1}^{e_{-1}} G_0^{e_0} \dots G_s^{e_s}$ ($D_s = \deg_x(F)/\deg_x(G_s)$), weight $\mathcal{W} = (w_{-1}, w_0, \dots, w_s)$ とする. このとき、 $F_{G_s\text{New}}$ は weight の違いを利用し
た項の書き換えにより (例 2 参照)、次のような、 G_s の重複部分 G_s^r と、 G_s^d と Δ_s の q 次同次多項式の積の
形 (pseudo form とよぶ) であらわすことができ、これを $F_{G_s\text{New}}^*$ と表す.

$$F_{G_s\text{New}}^* = G_s^r ((G_s^d)^q + \alpha_1 \Delta_s (G_s^d)^{q-1} + \dots + \alpha_q \Delta_s^q), \quad 0 \leq r \in \mathbb{Z}, d, q \in \mathbb{N}, \alpha_1, \dots, \alpha_q \in \overline{K}\{(u)\},$$

$$\exists^1 \Delta_s = G_{-1}^{\tilde{e}_{-1}} \dots G_{s-1}^{\tilde{e}_{s-1}} \text{ s.t. } \tilde{e}_{-1} > 0, 0 \leq \tilde{e}_i < \deg_x(G_{i+1})/\deg_x(G_i) \quad (i = 0, \dots, s-1), dw_s = \sum_{i=-1}^{s-1} w_i \tilde{e}_i.$$

これを $\overline{K}\{(u)\}$ 上因数分解したものを次とする.

$$F_{G_s\text{New}}^* = G_s^r h_1(G_s^d, \Delta_s) \dots h_R(G_s^d, \Delta_s) h_{R+1}(G_s^d, \Delta_s)^{m_{R+1}} \dots h_{R+R'}(G_s^d, \Delta_s)^{m_{R+R'}}$$

$$h_i(G_s^d, \Delta_s) (i = 1, \dots, R + R') \text{ は } \overline{K}\{(u)\} \text{ 上の互いに素な既約因子.}$$

4.2 Lifting のテクニック

前式で $H_0^{(0)} = G_s^r$, $H_1^{(0)} = h_1(G_s^d, \Delta_s)$, $\dots$, $H_R^{(0)} = h_R(G_s^d, \Delta_s)$, $H_{R+1}^{(0)} = h_{R+1}(G_s^d, \Delta_s)^{m_{R+1}}$, $\dots$,
 $H_{R+R'}^{(0)} = h_{R+R'}(G_s^d, \Delta_s)^{m_{R+R'}}$ とおき、これらを初期因子として Lifting する. このとき、 G_s を主変数とみて
拡張 Hensel 構成と同じ方法で Lifting すると、得られる因子は、 G_s に関しては多項式となるものの、従変数扱
いの Δ_s がもともとの主変数 x を含むために、 x が分母にあらわれたり、 x の次数が膨張するということが起こ
りうる. x の次数膨張は、残差計算時に展開基底の定義 $G_{i+1} \stackrel{\text{def}}{=} (G_i^{d_i})^{\tilde{q}_i} + \tilde{a}_{1,i} \Delta_i (G_i^{d_i})^{\tilde{q}_i-1} + \dots + \tilde{a}_{\tilde{q}_i,i} \Delta_i^{\tilde{q}_i}$ ($i =$
 $0, \dots, s-1$), $\tilde{a}_{1,i}, \dots, \tilde{a}_{\tilde{q}_i,i} \in \overline{K}\{(u)\}$ より、 $(G_i^{d_i})^{\tilde{q}_i} \rightarrow G_{i+1} - (\tilde{a}_{1,i} \Delta_i (G_i^{d_i})^{\tilde{q}_i-1} + \dots + \tilde{a}_{\tilde{q}_i,i} \Delta_i^{\tilde{q}_i})$ と書き換
えることで回避することができる. 一方、分母に x があらわれるのは、補間式の方母が $\overline{K}\{(u)\}$ 上の Δ_s
の多項式であることによるもので、分母に Δ_s をもたないように変形した補間式 (Practical Interpolation
Polynomials とよぶことにする) を用いることで、回避することができる.

定義 2 (Moses-Yun の補間式の変形版 Practical Interpolation Polynomials)

MosesYun の補間式 $W_i^{(j)} \in \overline{K}\{(u)\}(\Delta_s)[G_s]$ s.t. $W_0^{(j)} \frac{F_{G_s\text{New}}^*}{H_0^{(0)}} + \dots + W_{R+R'}^{(j)} \frac{F_{G_s\text{New}}^*}{H_{R+R'}^{(0)}} = G_s^j$,

$\deg_{G_s}(W_i^{(j)}) < \deg_{G_s}(H_i^{(0)})$ ($i = 0, \dots, R + R'$; $j = 0, \dots, D_s - 1$; $D_s = \deg_x(F)/\deg_x(G_s)$) に対して、
次を満たす $\tilde{W}_i^{(j)} (= \Delta_s^{\tilde{m}_j} W_i^{(j)}) \in \overline{K}\{(u)\}[G_s, \Delta_s]$ を Practical Interpolation Polynomials とよぶ.

$$\tilde{W}_0^{(j)} \frac{F_{G_s\text{New}}^*}{H_0^{(0)}} + \dots + \tilde{W}_{R+R'}^{(j)} \frac{F_{G_s\text{New}}^*}{H_{R+R'}^{(0)}} = \Delta_s^{\tilde{m}_j} G_s^j, \quad \tilde{m}_j \text{ は } W_0^{(j)}, \dots, W_{R+R'}^{(j)} \text{ の分母の } \Delta_s \text{ の次数の最大値}$$

ただし、 $r=0$ すなわち $H_0^{(0)} = 1$ の場合、 $W_0^{(j)} = \widetilde{W}_0^{(j)} = 0$.

◁

次のように、 $F = H_0^{(\infty)} H_1^{(\infty)} \cdots H_R^{(\infty)} H_{R+1}^{(\infty)} \cdots H_{R+R'}^{(\infty)}$ を構成することができる。

$\hat{d}, \hat{\delta} \in \mathbb{N}$ s.t. $w_s = \hat{\delta}/\hat{d}$, $\gcd(\hat{d}, \hat{\delta}) = 1$, $D_s \stackrel{\text{def}}{=} \deg_x(F)/\deg_x(G_s)$,

ideal $S_{k+1} = (G_s^{D_s} \tilde{t}^{((k+1)+0)/\hat{d}}, G_s^{D_s-1} \tilde{t}^{((k+1)+\hat{\delta})/\hat{d}}, G_s^{D_s-2} \tilde{t}^{((k+1)+2\hat{\delta})/\hat{d}}, \dots, G_s^0 \tilde{t}^{((k+1)+D_s\hat{\delta})/\hat{d}})$, $k = 1, 2, 3, \dots$

$$\begin{aligned} f^{(k)} &\equiv F - H_0^{(k-1)} \cdots H_{R+R'}^{(k-1)} \pmod{S_{k+1}} \\ &\equiv \sum_{j=0}^{D_s-1} f_j^{(k)} \tilde{t}^{k/\hat{d}} \cdot \Delta^{\tilde{m}_j} G_s^j \tilde{t}^{(D_s-j)\hat{\delta}/\hat{d}} \pmod{S_{k+1}} \quad (G_s^j \text{の係数部に } \Delta^{\tilde{m}_j} \text{を作り出す}) \\ H_i^{(k)} &\equiv H_i^{(k-1)} + \sum_{j=0}^{D_s-1} f_j^{(k)} \tilde{t}^{k/\hat{d}} \cdot \widetilde{W}_i^{(j)} \quad (i = 0, \dots, R+R') \end{aligned}$$

4.3 各因子の処理

$H_0^{(\infty)}, \dots, H_{R+R'}^{(\infty)}$ は次のように処理する。

$H_0^{(\infty)}$: $F \equiv H_0^{(\infty)}$ とおき、再帰的に展開基底で分解する。

$H_1^{(\infty)}, \dots, H_R^{(\infty)}$: 低次部分 $h_i(G_s^d, \Delta_s)$ ($i = 1, \dots, R$) が既約ゆえ、 $\overline{K}\{(u)\}[x]$ の既約因子である。

$H_{R+1}^{(\infty)}, \dots, H_{R+R'}^{(\infty)}$: 各 $i = R+1, \dots, R+R'$ について $F \equiv H_i^{(\infty)}$, $D_s \equiv \deg_x(F)/\deg_x(G_s)$ とし、

低次部分 $h_i(G_s^d, \Delta_s)^{m_i}$ ($m_i \geq 2$) において、

• $d=1$ かつ $\deg_x(h_i)/\deg_x(G_s) = 1$ ならば、 $G_s \equiv h_i(G_s^1, \Delta_s)$ と再定義して

$F_{G_s \text{ New}}$ の $\overline{K}\{(u)\}$ 上での因数分解へ。

• それ以外ならば、 $G_{s+1} \equiv h_i(G_s^d, \Delta_s)$, $w_{s+1} \equiv D_s w_s / m_i$ と生成して $F_{G_{s+1} \text{ New}}$ の分解へ。

これにより、 $\overline{K}\{(u)\}[x]$ の因数分解を得る。あとは、分母に着目して因子をかけあわせることで $\overline{K}\{u\}[x]$ の因数分解を得ることができる。

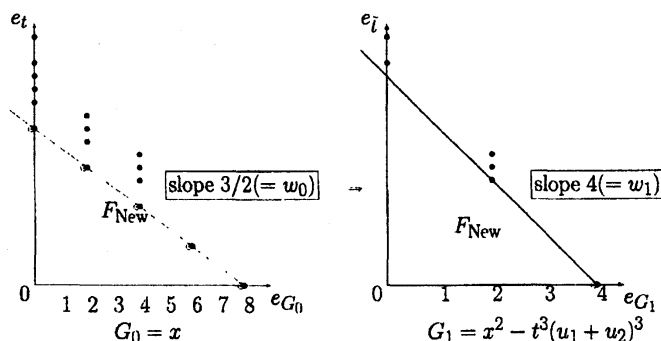
4.4 展開基底を用いた多変数の解析的因数分解の例

次のように解析的因数分解することのできる $F(x, u_1, u_2) = ((x^2 - (u_1 + u_2)^3)^2 + (u_1 + u_2)^7(u_1 + 2u_2)^2)((x^2 - (u_1 + u_2)^3)^2 - (u_1 + 2u_2)^8 - (u_1 + 3u_2)^{10}) \in \overline{K}[x, u_1, u_2]$ を考える。

$$\begin{aligned} F(x, tu_1, tu_2) &= (x^2 - t^3(u_1 + u_2)^3 + i \, xt^3(u_1 + u_2)^2(u_1 + 2u_2) - \frac{1}{2}t^6(u_1 + u_2)^4(u_1 + 2u_2)^2 - \cdots) \\ &\times (x^2 - t^3(u_1 + u_2)^3 - i \, xt^3(u_1 + u_2)^2(u_1 + 2u_2) - \frac{1}{2}t^6(u_1 + u_2)^4(u_1 + 2u_2)^2 + \cdots) \\ &\times ((x^2 - t^3(u_1 + u_2)^3)^2 - t^8(u_1 + 2u_2)^8 - t^{10}(u_1 + 3u_2)^{10}) \end{aligned}$$

F の Newton 多項式は $F_{\text{New}} = (x^2 - t^3(u_1 + u_2)^3)^4$ であり、互いに素な多項式因子に分解できない。

F の展開基底 $\mathcal{G} = (G_{-1}, G_0, G_1) = (t, x, x^2 - t^3(u_1 + u_2)^3)$, $\mathcal{G}$ -adic expansion $F = \sum_{e_1=0}^{D_1} c_{(e_{-1}, e_0, e_1)} G_{-1}^{e_{-1}} G_0^{e_0} G_1^{e_1}$, $c_{(e_{-1}, e_0, e_1)} \in \overline{K}\{(u)\}$, $D_1 = 4$ を計算し、 $G_{-1} \mapsto \tilde{t}^{w_{-1}} G_{-1}$, $G_0 \mapsto \tilde{t}^{w_0} G_0$ として 2次元平面の横軸に G_1 のべき、縦軸に $\tilde{t}$ のべきをとり、 $(e_1, 1 \cdot e_{-1} + \frac{3}{2} \cdot e_0)$ をプロットする。weight $\mathcal{W} = (w_{-1}, w_0, w_1) = (1, 3/2, 4)$.



$$F_{G_0 \text{ New}} = (x^2 - t^3(u_1 + u_2)^3)^4 \quad F_{G_1 \text{ New}} = G_1^4 (G_1 - \tilde{t}^4(u_1 + 2u_2)^4 G_{-1}^4)(G_1 + \tilde{t}^4(u_1 + 2u_2)^4 G_{-1}^4)$$

$$\begin{array}{ccccccc} \text{Lifting} & & \Downarrow & & \Downarrow & & \Downarrow \\ F & = & H_0^{(\infty)} & & H_1^{(\infty)} & & H_2^{(\infty)} \end{array}$$

$$\begin{aligned} H_0^{(\infty)} &= G_1^2 + (u_1 + u_2)^7 (u_1 + 2u_2)^2 G_{-1}^9 \\ H_1^{(\infty)} &= G_1 - (u_1 + 2u_2)^4 G_{-1}^4 - \frac{(u_1 + 3u_2)^{10}}{2(u_1 + 2u_2)^4} G_{-1}^6 + \frac{(u_1 + 3u_2)^{20}}{8(u_1 + 2u_2)^{12}} G_{-1}^8 - \dots \\ H_2^{(\infty)} &= G_1 + (u_1 + 2u_2)^4 G_{-1}^4 + \frac{(u_1 + 3u_2)^{10}}{2(u_1 + 2u_2)^4} G_{-1}^6 - \frac{(u_1 + 3u_2)^{20}}{8(u_1 + 2u_2)^{12}} G_{-1}^8 + \dots \end{aligned}$$
$$\begin{aligned}
H_0 \ G_1^{\text{New}} &= G_1^2 + (u_1 + u_2)^7(u_1 + 2u_2)^2 G_{-1}^{-9} \\
&= G_1^2 + (u_1 + u_2)^7(u_1 + 2u_2)^2 G_{-1}^{-6} \boxed{G_{-1}^3} \\
&= G_1^2 + (u_1 + u_2)^7(u_1 + 2u_2)^2 G_{-1}^{-6} \boxed{\frac{G_0^2}{(u_1 + u_2)^3} - \frac{G_1}{(u_1 + u_2)^3}} \\
&= \frac{G_1^2 + (u_1 + u_2)^4(u_1 + 2u_2)^2 G_{-1}^{-6} G_0^2 - (u_1 + u_2)^4(u_1 + 2u_2)^2 G_{-1}^{-6} G_1}{9} \\
(\text{weights}) \quad &\qquad \qquad \qquad 9 \qquad \qquad \qquad 10.5) \\
&\equiv G_1^2 + (u_1 + u_2)^4(u_1 + 2u_2)^2 G_{-1}^{-6} G_0^2 \pmod{S_1} \stackrel{+}{=} H_0^* G_1^{\text{New}}
\end{aligned}$$
$$\begin{aligned}
H_{0 \ G_1 \text{New}}^* &= G_1^2 + (u_1 + u_2)^4 (u_1 + 2u_2)^2 \Delta_{H_0}^2, \quad \Delta_{H_0} = G_{-1}^3 G_0^1 \\
&= (G_1 + i (u_1 + u_2)^2 (u_1 + 2u_2) \Delta_{H_0}) (G_1 - i (u_1 + u_2)^2 (u_1 + 2u_2) \Delta_{H_0}), \quad i = \sqrt{-1}, \\
\text{を得る. } H_{01}^{(0)} &= (G_1 + i (u_1 + u_2)^2 (u_1 + 2u_2) \Delta_{H_0}), \quad H_{02}^{(0)} = (G_1 - i (u_1 + u_2)^2 (u_1 + 2u_2) \Delta_{H_0}) \text{ とおき、} \\
W_{01}^{(j)} H_{02}^{(0)} + W_{02}^{(j)} H_{01}^{(0)} &= G_1^j \text{ をみたす Moses-Yun の補間式 } W_{0i}^{(j)} \ (i = 1, 2; j = 0, 1) \text{ を計算する.}
\end{aligned}$$

このとき $\widetilde{W}_{01}^{(j)} H_{02}^{(0)} + \widetilde{W}_{02}^{(j)} H_{01}^{(0)} = \Delta_{H_0}^{\tilde{m}_j} G_1^j$ をみたす Practical Interpolation Polynomials $\widetilde{W}_{0i}^{(j)} \in \overline{K}(\mathbf{u})[\Delta_{H_0}, G_1]$ ($i = 1, 2; j = 0, 1$) は $\widetilde{W}_{0i}^{(0)} = \Delta_{H_0} W_{0i}^{(0)}$, $\widetilde{W}_{0i}^{(1)} = W_{0i}^{(1)}$ ($\tilde{m}_j = 1 - j$, $\Delta_{H_0} = G_{-1}^3 G_0$).

$$\begin{aligned} f^{(1)} &\equiv H_0 - H_{01}^{(0)} H_{02}^{(0)} \pmod{S_2} = 0, & f^{(2)} &\equiv H_0 - H_{01}^{(1)} H_{02}^{(1)} \pmod{S_3} = 0 \\ f^{(3)} &\equiv H_0 - H_{01}^{(2)} H_{02}^{(2)} \pmod{S_4} = -(u_1 + u_2)^4 (u_1 + 2u_2)^2 G_{-1}^6 \cdot \Delta_{H_0}^0 G_1 \quad (\because \tilde{m}_1 = 0) \text{ よって} \end{aligned}$$

$$f^{(4)} \equiv H_0 - H_{01}^{(3)} H_{02}^{(3)} \pmod{S_5} = 0, \quad f^{(5)} \equiv H_0 - H_{01}^{(4)} \tilde{H}_{02}^{(4)} \pmod{S_6} = 0$$

$$\equiv -\frac{1}{4}(u_1+u_2)^5(u_1+2u_2)^4 G_{-1}^6 G_0^1 \cdot \Delta_{H_0}^1 G_1^0 \quad (\because \tilde{m}_0=1) \text{ よって}$$

$$H_{0j}^{(\infty)} = G_1 + (-1)^{j+1} i (u_1 + u_2)^2 (u_1 + 2u_2) G_{-1}^3 G_0 - \frac{1}{2} (u_1 + u_2)^4 (u_1 + 2u_2)^2 G_{-1}^6 + (-1)^j \frac{1}{8} i (u_1 + u_2)^3 (u_1 + 2u_2)^3 G_{-1}^6 G_0 + \dots$$

これにより、次のような $\overline{K}\{u\}[x]$ での因数分解を得る.

$$(j = 1, 2)$$

$$\begin{aligned}
F = & (G_1 + i(u_1 + u_2)^2(u_1 + 2u_2)G_{-1}^3G_0 - \frac{1}{2}(u_1 + u_2)^4(u_1 + 2u_2)^2G_{-1}^6 - \frac{1}{8}i(u_1 + u_2)^3(u_1 + 2u_2)^3G_{-1}^6G_0 + \cdots) \\
& \times (G_1 - i(u_1 + u_2)^2(u_1 + 2u_2)G_{-1}^3G_0 - \frac{1}{2}(u_1 + u_2)^4(u_1 + 2u_2)^2G_{-1}^6 + \frac{1}{8}i(u_1 + u_2)^3(u_1 + 2u_2)^3G_{-1}^6G_0 + \cdots) \\
& \times (G_1 - (u_1 + 2u_2)^4G_{-1}^4 - \frac{(u_1 + 3u_2)^{10}}{2(u_1 + 2u_2)^4}G_{-1}^6 + \frac{(u_1 + 3u_2)^{20}}{8(u_1 + 2u_2)^{12}}G_{-1}^8 - \cdots) \\
& \times (G_1 + (u_1 + 2u_2)^4G_{-1}^4 + \frac{(u_1 + 3u_2)^{10}}{2(u_1 + 2u_2)^4}G_{-1}^6 - \frac{(u_1 + 3u_2)^{20}}{8(u_1 + 2u_2)^{12}}G_{-1}^8 + \cdots)
\end{aligned}$$

分母に着目して 3 番目と 4 番目の因子をかけあわせることで、次のような $\overline{K}\{u\}[x]$ の因数分解を得る.

$$\begin{aligned}
F(x, u_1, u_2) = & (x^2 - (u_1 + u_2)^3 + i x(u_1 + u_2)^2(u_1 + 2u_2) - \frac{1}{2}(u_1 + u_2)^4(u_1 + 2u_2)^2 - \cdots) \\
& \times (x^2 - (u_1 + u_2)^3 - i x(u_1 + u_2)^2(u_1 + 2u_2) - \frac{1}{2}(u_1 + u_2)^4(u_1 + 2u_2)^2 - \cdots) \\
& \times ((x^2 - (u_1 + u_2)^3)^2 - (u_1 + 2u_2)^8 - (u_1 + 3u_2)^{10})
\end{aligned}$$

5 おわりに

解析的因数分解で最終的に問題となるのは $F = g^m + \cdots$ (g は既約多項式, $m \geq 2$, $F_{\text{New}} = g^m$) の形であり、多変数を、主変数 x と従変数の全次数変数 t の 2 変数とみなして 2 変数のアルゴリズムを修正・適用することで、 $\overline{K}\{(u)\}[x]$ での因数分解を得ることができ、最後に分母をみて因子をかけあわせることで解析的既約因子を得ることができた. 4 章での展開基底を用いた分解法では、3 章の拡張 Hensel 構成を用いた分解法のように代数関数や t の分数べきがでてこないため、実装上有利であると思われる. また、最後の例で、1 番目と 2 番目の因子をかけあわせることで $F(x, u_1, u_2) = ((x^2 - (u_1 + u_2)^3)^2 + (u_1 + u_2)^7(u_1 + 2u_2)^2)((x^2 - (u_1 + u_2)^3)^2 - (u_1 + 2u_2)^8 - (u_1 + 3u_2)^{10})$ なる多項式環での因数分解を得ることができるように、Newton 多項式が無平方でない場合の多項式環での因数分解も可能となる.

参 考 文 献

- [Ab88] S. S. Abhyankar: What is the difference between a parabola and a hyperbola? *Math. Intelligencer* 10, pp. 37–43 (1988).
- [Ab89] S. S. Abhyankar: Irreducibility Criterion for Germs of Analytic Functions of Two Complex Variables. *Advances in Math.*, 74, pp. 190–257 (1989).
- [Ab90] S. S. Abhyankar: *Algebraic Geometry for Scientists and Engineers*. Number 35 in Mathematical Surveys and Monographs. Providence, RI: American Mathematical Society (1990).
- [AM73] S. S. Abhyankar and T. T. Moh: Newton-Puiseux expansion and generalized Tschirnhausen transformation II. *J. reine und angew. Math.* 261, pp.29–pp.54 (1973).
- [Iwa03] M. Iwami: Analytic Factorization of the Multivariate Polynomial. *Proc. of the 6th International Workshop on Computer Algebra in Scientific Computing*. pp.213–225 (2003).
- [Iwa04] M. Iwami: Extension of Expansion Base Algorithm to Multivariate Analytic Factorization. *Proc. of the 7th International Workshop on Computer Algebra in Scientific Computing*. pp.269–281 (2004).
- [Kuo89] T. C. Kuo: Generalized Newton-Puiseux Theory and Hensel's Lemma in $C[[x, y]]$. *Can. J. Math.*, Vol.XLI, No. 6, pp. 1101–1116 (1989).
- [McC97] S. McCallum: On Testing a Bivariate Polynomial for Analytic Reducibility. *J. Symb. Comput.* 24, pp. 509–535 (1997).
- [SI00] T. Sasaki and D. Inaba: Hensel Construction of $F(x, u_1, \dots, u_l)$, $l \geq 2$, at a Singular Point and Its Applications. *SIGSAM Bulletin*, Vol. 34, pp.9–17 (2000).
- [SK99] T. Sasaki and F. Kako: Solving Multivariate Algebraic Equation by Hensel Construction. *Japan J. Indus. Appl. Math.*, 16, 257–285 (1999).
- [Sas00] T. Sasaki: Properties of Extended Hensel Factors and Application to Approximate Factorization. Preprint (unpublished), Univ. Tsukuba (2000).