数理解析研究所講究録
1138巻 2000年 28-42

拡張 Hensel 構成と多変数多項式の因数分解

筑波大学数学系　佐々木　建昭(Tateaki Sasaki)
筑波大学数学研究科　稲葉　大樹(Daiju Inaba) *

概　要

1993年、SasakiとKakoは一般Hensel構成が破綻する場合にも適用できる多変数多項式用Hensel構成法として拡張Hensel構成法を提案したが、主係数が特異な場合は考察しなかった。本稿では、まず拡張Hensel構成を主係数が特異な多項式にも適用できるよう拡張する。つぎに、初期因子を多項式とする拡張Hensel構成により、特異な多変数多項式が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できることを示す。最後に、拡張Hensel構成を使えば、非零代入をすることなく多変数多項式が因数分解できることを示す。

1　はじめに

多変数多項式の一般Hensel構成 [Mus71] は数式処理において非常に重要な演算であるが、一つの欠点を有する。$F(x, u_1, \ldots, u_\ell)$ を与えられた多項式、$(s_1, \ldots, s_\ell)$ を展開点とするとき、1変数多項式 $F(x, s_1, \ldots, s_\ell)$ が互いに素な多項式に分解できなければならない。この欠点は、2変数多項式に対しては1989年にKuoにより [Kuo89]、多変数多項式に対しては1993年にSasakiとKakoにより [SK99]、克服された。この拡張された方法をSasakiとKakoは**拡張Hensel構成**と命名した。

Sasaki-Kakoは主係数が“非特異”な場合のみを扱った。本稿ではまず、主係数が特異な場合にも適用できるよう、Sasaki-Kakoの方法を若干拡張する。

[SK99] は初期因子を代数関数で表した場合の拡張Hensel因子の性質を一般的に調べた。そのため、数学的には興味深いが、応用が限られるように思われる。そこで、本稿では、初期因子が多項式である場合に限定して拡張Hensel因子の性質を調べ、多項式を従変数の有理式級数を係数とする多項式因子に分解する定理を導出する。

この定理の直接的な応用は多変数多項式の因数分解であろう。多変数多項式の因数分解には非零代入問題という昔からよく知られた問題がある。1977年、Wangが一つの解決策を提示したが [Wan77]、Wangの方法は筆者らの目から見るとまだ不十分である。これに対し、本稿で提案する方法は非零代入問題の最終的解決法と言えるのではないかと思う。

*(sasaki,inaba)@math.tsukuba.ac.jp

2章では、一般 Hensel 構成が破綻する展開点（特異点と呼ぶ）を定義し、拡張 Hensel 構成を復習する。3章では、Sasaki-Kako の原論文では扱われなかった “特異な主係数” の場合の拡張 Hensel 構成を論じる。4章では、拡張 Hensel 構成の初期因子が多項式の場合の Hensel 因子の性質を調べ、本論の主定理である分解定理を導出する。5章では、拡張 Hensel 構成を用いた多変数多項式の因数分解法を説明する。

2 Hensel 構成の特異点と拡張 Hensel 構成

$\mathbf{K}$ を数体、$\mathbf{K}[u_1,\ldots,u_\ell]$, $\mathbf{K}(u_1,\ldots,u_\ell)$ をそれぞれ $\mathbf{K}$ 上の変数 $u_1,\ldots,u_\ell$ の多項式環、有理式体とする。また、$(s_1,\ldots,s_\ell)\in\mathbf{K}^\ell$ として、以下では変数と数値の組 $(u_1,\ldots,u_\ell)$, $(s_1,\ldots,s_\ell)$ をそれぞれ (u), (s) と略記する。与えられた多変数多項式 $F(x,u)\in\mathbf{K}[x,u]$ は無平方と仮定し次式と表す。

$$F(x,u)=f_n(u)x^n+f_{n-1}(u)x^{n-1}+\cdots+f_0(u)x^0,\quad f_0(u)\neq 0. \tag{1}$$

多項式 F の主変数 x に関する次数と主係数をそれぞれ $\deg(F),\mathrm{lc}(F)$ と表し、$f_i(u)$ の位数 (f_i の各項の全次数のなかで最小のもの) を $\mathrm{ord}(f_i)$ と表す。有理式 $f(u)/g(u)$ に対しては位数を $\mathrm{ord}(f/g)=\mathrm{ord}(f)-\mathrm{ord}(g)$ と定める。F と G の最大公約子を $\gcd(F,G)$ と表し、F の係因子と原始部分をそれぞれ $\mathrm{cont}(F)$, $\mathrm{pp}(F)$ と表す：$\mathrm{cont}(F)=\gcd(f_n,f_{n-1},\cdots,f_0)$, $\mathrm{pp}(F)=F/\mathrm{cont}(F)$。多項式 F と G の (主変数 x に関する) 剰余を $\mathrm{rem}(F,G)$、終結式を $\mathrm{res}(F,G)$ と表す。また、$p_1,\ldots,p_l$ から生成されるイデアルを $\langle p_1,\cdots,p_l\rangle$ と表す。$G(u)$ を以下のような有理式の (無限) 級数とする。

$$\begin{cases} G(u) \;=\; g_1(u)/d_1(u)+g_2(u)/d_2(u)+\cdots+g_k(u)/d_k(u)+\cdots, \\ g_k(u) \text{ and } d_k(u) \text{ are homogeneous w.r.t. } u_1,\ldots,u_\ell \quad (k=1,2,\ldots), \\ 0\le \mathrm{ord}(g_1/d_1)<\mathrm{ord}(g_2/d_2)<\cdots<\mathrm{ord}(g_k/d_k)<\cdots. \end{cases} \tag{2}$$

$G(u)$ のような非負位数の (無限) 級数全体の成す環を $\mathbf{K}\{(u)\}$ と表すことにする。

点 $(s_1,\ldots,s_\ell)\in\mathbf{K}^\ell$ が $f_1(s)=f_0(s)=0$ を満たせば、その点を **Hensel 構成の特異点**、略して特異点という。また、$f_n(s)=0$ なら、点 $(s_1,\ldots,s_\ell)$ で**主係数は特異**であるという。$f_n(s)\neq 0$, $f_m(s)\neq 0$, $(n\ge m\ge 2)$, かつ $f_{m-1}(s)=\cdots=f_0(s)=0$ となる場合には

$$\hat{F}^{(0)}(x)=x^m,\quad \tilde{F}^{(0)}(x)=f_n(s)x^{n-m}+\cdots+f_m(s)x^0,$$

を初期因子として $F(x,u)$ を一般 Hensel 構成することにより、

$$F(x,u)\equiv \hat{F}^{(k)}(x,u)\tilde{F}^{(k)}(x,u)\pmod{(u-s)^{k+1}}$$

を満たす $\hat{F}^{(k)}(x,u),\tilde{F}^{(k)}(x,u)\in\mathbf{K}[x,u]$ を構成できる。ここで、$\hat{F}^{(k)}(x,u)$ と $\tilde{F}^{(k)}(x,u)$ は点 (s) でそれぞれ特異、非特異な多項式である。

以下では一般性を失うことなく、原点 $(u)=(0)$ が特異点とする。さて、原点で特異だが主係数が特異でない多項式 $\hat{F}(x,u)$ に対して、Sasaki-Kako は次のように Hensel 構成を拡張することを提案した。まず、$u_i \mapsto tu_i$ $(i=1,\ldots,\ell)$ なる変換で、従変数 $u_1,\ldots,u_\ell$ に関する全次数変数 t を導入する。つぎに、$\hat{F}(x,u)$ に対する Newton 線と Newton 多項式を次のように定める。($\hat{F}(x,0)=x^m$ となることに注意)。

定義 1 (Newton line $L_{\rm New}$ and Newton polynomial $\hat{F}_{\rm New}(x,u)$ for $\hat{F}(x,u)$) (the case of non-singular leading coefficient)

1. *For each monomial $cx^it^ju_1^{j_1}\cdots u_\ell^{j_\ell}$ of $\hat{F}(x,tu)$, with $c\in\mathbf{K}$ and $j=j_1+\cdots+j_\ell$, plot a dot at the point (i,j) in the (e_x,e_t)-plane ;*
2. *Let $L_{\rm New}$ be a straight line in (e_x,e_t)-plane, such that it passes the point $(m,0)$ and another dot plotted and that any dot plotted is not below $L_{\rm New}$;*
3. *Construct $\hat{F}_{\rm New}(x,tu)$ by summing all the monomials which are plotted on $L_{\rm New}$.*

Newton 線の傾きを $-\lambda$ とするとき、$F_{\rm New}(x,tu)$ は x と t^λ の同次多項式である。次に、イデアル $\hat{I}_k$ を次のように定める。Newton 線 $L_{\rm New}$ を $e_x/m+e_t/\mu=1$ とし ($(0,\mu)$ は $L_{\rm New}$ と e_t-軸の交点の座標である)、正整数 $\hat{m},\hat{\mu}$ を $\hat{\mu}/\hat{m}=\mu/m=\lambda$, $\gcd(\hat{m},\hat{\mu})=1$ を満たすように定めるとき、

$$\hat{I}_k \;=\; \langle\, x^m t^{(k+0)/\hat{m}},\; x^{m-1}t^{(k+\hat{\mu})/\hat{m}},\; \cdots,\; x^0 t^{(k+m\hat{\mu})/\hat{m}} \,\rangle.$$

Newton 多項式 $\hat{F}_{\rm New}(x,u)$ は二つ以上の項を持つから、次のように因数分解されるとする ($\hat{F}_{\rm New}(x,u)=\hat{G}(x,u)^m$ となる場合については [SK99] を参照されたい)。

$$\begin{cases} \hat{F}_{\rm New}(x,tu)=\hat{G}_1^{(0)}(x,tu)\cdots\hat{G}_r^{(0)}(x,tu), \quad r\geq 2, \\ \qquad \gcd(\hat{G}_i^{(0)},\hat{G}_j^{(0)})=1 \;\text{ for any }\; i\neq j. \end{cases}$$

($\hat{G}_i^{(0)}(x,tu)$ は通常 $tu_1,\ldots,tu_\ell$ の代数関数を係数とする x の多項式であるが、$tu_1,\ldots,tu_\ell$ の多項式になることもあり、4 章ではその場合を議論する)。このとき、次式を満たす $\hat{G}_i^{(k)}(x,tu)$ $(i=1,\ldots,r)$ が一般 Hensel 構成と同様な手順で構成できる (具体的な手順については [SK99] を参照されたい)。

$$\hat{F}(x,tu)\equiv \hat{G}_1^{(k)}(x,tu)\cdots\hat{G}_r^{(k)}(x,tu) \pmod{\hat{I}_{k+1}}, \quad k=1,2,\cdots.$$

3 拡張 Hensel 構成：主係数が特異な場合

主係数が特異な場合には Sasaki-Kako 法は直接的には適用できないが、以下のように若干拡張することにより、主係数が特異な場合にも適用可能になる。以下では、原点で $F(x,u)$

は特異、かつ主係数も特異であるとする：

$$\begin{cases} F(x,u) = f_n(u)x^n + \cdots + f_1(u)x + f_0(u), \\ \mathrm{ord}(f_n) = \nu > 0, \quad f_n(0) = f_1(0) = f_0(0) = 0. \end{cases} \tag{3}$$

定義 2 (Newton line L_{New} and Newton polynomial $F_{\mathrm{New}}(x,u)$ for $F(x,u)$) (the case of singular leading coefficient)

1. *For each monomial $cx^it^ju_1^{j_1}\cdots u_\ell^{j_\ell}$ of $F(x,tu)$, with $c \in \mathbf{K}$ and $j = j_1 + \cdots + j_\ell$, plot a dot at the point (i,j) in the (e_x,e_t)-plane ;*

2. *Let L_{New} be a straight line in (e_x,e_t)-plane, such that it passes the point (n,ν) and another dot plotted and that any dot plotted is not below L_{New} ;*

3. *Construct $F_{\mathrm{New}}(x,tu)$ by summing all the monomials which are plotted on L_{New} .*

図 1 に示すように、Newton 線には傾きが正、零、負の 3 種類の場合がありえる。

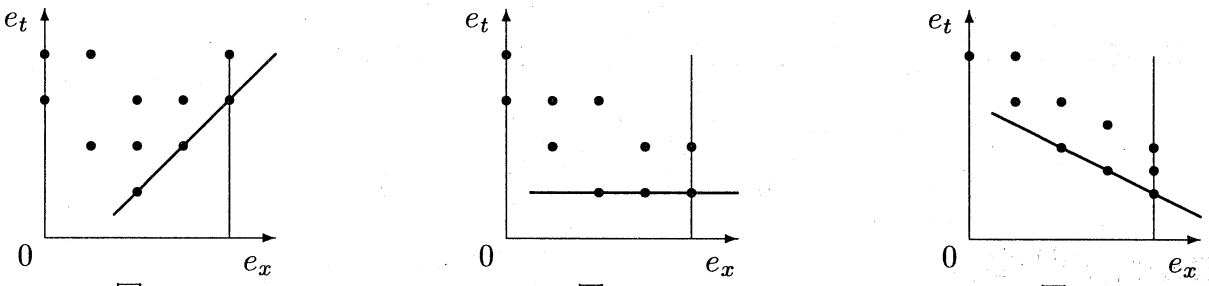

図 1-1　図 1-2　図 1-3

図 1　特異な主係数を持つ多項式に対する Newton 線：傾きが正、零、負の場合

Newton 線の傾きを、図 1-1 の場合は λ、図 1-3 の場合は $-\lambda$ とする。さて、正整数 $\hat{n},\hat{\nu}$ を $\hat{\nu}/\hat{n} = \lambda$, $\gcd(\hat{n},\hat{\nu}) = 1$ を満たすように決める。[SK99] の補題 1 によると、Newton 線 L_{New} を e_t-方向に $1/\hat{n}$ ずつ動かせば、(e_x,e_t)-平面上で L_{New} より上部にある全ての整数格子点が線上に乗る。そこで、多項式 $\bar{F}(x,u,t)$ とイデアル $\bar{I}_k$ を次のように定める。

$$\bar{F}(x,u,t) \stackrel{\mathrm{def}}{=} \begin{cases} \dfrac{F(x/t^\lambda, tu)}{t^{\nu-n\lambda}} & \text{図 1-1 の場合,} \\ F(x,tu) & \text{図 1-2 の場合,} \\ \dfrac{F(t^\lambda x, tu)}{t^{\nu+n\lambda}} & \text{図 1-3 の場合,} \end{cases} \tag{4}$$

$$\bar{I}_k = \langle\, t^{k/\hat{\nu}} \,\rangle, \quad k = 1,2,3,\cdots . \tag{5}$$

F から $\bar{F}$ への変換で Newton 線は図 1 のいずれの場合にも水平になる。

$\bar{F}(x,u,t)$ に対する Newton 多項式 $\bar{F}_{\mathrm{New}}(x,u,t)$ は二つ以上の項を持つから、次のように因数分解されるとする（$\bar{F}_{\mathrm{New}}(x,u,t)=\bar{G}(x,u,t)^m$ となる場合の処理は [SK99] と同じである）。

$$\begin{cases} \bar{F}_{\mathrm{New}}(x,u,t)=\bar{G}_1^{(0)}(x,u,t)\cdots\bar{G}_r^{(0)}(x,u,t), \quad r\geq 2, \\ \qquad \gcd(\bar{G}_i^{(0)},\bar{G}_j^{(0)})=1 \ \text{ for any } \ i\neq j. \end{cases} \tag{6}$$

このとき、次式を満たす $\bar{G}_i^{(k)}(x,u,t)$ $(i=1,\ldots,r)$ が構成できる。

$$\bar{F}(x,u,t)\equiv\bar{G}_1^{(k)}(x,u,t)\cdots\bar{G}_r^{(k)}(x,u,t) \pmod{\bar{I}_{k+1}}, \quad k=1,2,\cdots. \tag{7}$$

次章で使う必要上、$\bar{G}_i^{(k)}$ $(i=1,\ldots,r)$ の構成手順を簡単に述べる。まず、“Moses-Yun の補間式” $\bar{W}_i^{(l)}$ $(i=1,\ldots,r;\ l=0,1,\ldots,n-1)$ を計算する。

$$\begin{cases} \bar{W}_1^{(l)}\cdot\dfrac{\bar{F}_{\mathrm{New}}}{\bar{G}_1^{(0)}}+\cdots+\bar{W}_r^{(l)}\cdot\dfrac{\bar{F}_{\mathrm{New}}}{\bar{G}_r^{(0)}}=x^l, \\ \deg(\bar{W}_i^{(l)})<\deg(\bar{G}_i^{(0)}) \quad (i=1,\ldots,r). \end{cases} \tag{8}$$

次に、$\bar{G}_i^{(k')}$ $(k'=0,1,\ldots,k-1)$ を構成したとして、次式を計算する。

$$\begin{aligned} \bar{D}^{(k)} &\equiv \bar{F}-\bar{G}_1^{(k-1)}\cdots\bar{G}_r^{(k-1)} \pmod{\bar{I}_{k+1}} \\ &= \bar{d}_n^{(k)}x^n+\bar{d}_{n-1}^{(k)}x^{n-1}+\cdots+\bar{d}_0^{(k)}. \end{aligned} \tag{9}$$

最後に、$\bar{G}_i^{(k)} \stackrel{\mathrm{def}}{=} \bar{G}_i^{(k-1)}+\delta\bar{G}_i^{(k)}$ $(i=1,\ldots,r)$ は次式で構成すればよい。

$$\delta\bar{G}_i^{(k)}=\bar{W}_i^{(n)}\bar{d}_n^{(k)}+\bar{W}_i^{(n-1)}\bar{d}_{n-1}^{(k)}+\cdots+\bar{W}_i^{(0)}\bar{d}_0^{(k)}. \tag{10}$$

注釈 1　[SK99] が扱ったのは本質的に図 1-3 の場合と同じであるから、[SK99] に記述された拡張 Hensel 構成法も上記の方法に統一できる。

例 1　主変数が特異な次の 2 変数多項式 $F(x,y)$ の拡張 Hensel 構成の例。
分り易さのため、例においては全次数変数 t を明示せず、$\bar{}$ 付きの式 $\bar{F}(x,u,t)$ 等でなく、元の多項式 $F(x,u)$ 等のままで計算結果を示す。

$$\begin{aligned} F(x,y) &= x^4y^2+x^3(3y^2+y)+x^2(y^3-2y^2+3y-2) \\ &\quad +x(3y^3-9y^2-5y)+(-2y^4-5y^3+3y^2). \end{aligned} \tag{11}$$

$F(x,y)$ の Newton 多項式とその既約因数分解は次式となる。

$$F_{\mathrm{New}}(x,y)=x^4y^2+x^3y+2x^2=x^2\cdot(xy+2)\cdot(xy-1).$$

上式右辺の互いに素な三つの因子を $G_1^{(0)}=x^2$, $G_2^{(0)}=xy+2$, $G_3^{(0)}=xy-1$ とおき、

$$W_1^{(l)}\cdot F_{\mathrm{New}}/G_1^{(0)}+W_2^{(l)}\cdot F_{\mathrm{New}}/G_2^{(0)}+W_3^{(l)}\cdot F_{\mathrm{New}}/G_3^{(0)}=x^l \quad (l=0,1,2,3)$$

を満たす Moses-Yun の補間式 $W_i^{(l)}$ $(i=1,2,3)$ を計算する：

$$\begin{array}{lll} W_1^{(0)}=-(xy+2)/4, & W_2^{(0)}=-y^2/12, & W_3^{(0)}=y^2/3,\\ W_1^{(1)}=-x/2, & W_2^{(1)}=y/6, & W_3^{(1)}=y/6,\\ W_1^{(2)}=0, & W_2^{(2)}=-1/3, & W_3^{(2)}=1/3,\\ W_1^{(3)}=0, & W_2^{(3)}=2/(3y), & W_3^{(3)}=1/(3y). \end{array}$$

以下、$k=1,2$ に対し、$\delta G_i^{(k)}$ を順に計算する $(G_i^{(k)}=G_i^{(k-1)}+\delta G_i^{(k)})$。

$$\begin{aligned} k=1:\quad & D^{(1)}=3x^3y^2+3x^2y \;\Rightarrow\; d_3^{(1)}=3y^2,\ d_2^{(1)}=3y,\\ & \delta G_1^{(1)}=W_1^{(3)}(3y^2)+W_1^{(2)}(3y)=0,\\ & \delta G_2^{(1)}=W_2^{(3)}(3y^2)+W_2^{(2)}(3y)=y,\\ & \delta G_3^{(1)}=W_3^{(3)}(3y^2)+W_3^{(2)}(3y)=2y,\\ k=2:\quad & D^{(2)}=-4x^2y^2-5xy \;\Rightarrow\; d_2^{(2)}=-4y^2,\ d_1^{(2)}=-5y,\\ & \delta G_1^{(2)}=W_1^{(2)}(-4y^2)+W_1^{(1)}(-5y)=5xy/2,\\ & \delta G_2^{(2)}=W_2^{(2)}(-4y^2)+W_2^{(1)}(-5y)=y^2/2,\\ & \delta G_3^{(2)}=W_3^{(2)}(-4y^2)+W_3^{(1)}(-5y)=-3y^2. \end{aligned}$$

以上より、2 次の Hensel 因子として次式を得る。

$$G_1^{(2)}=x^2+5xy/2,\quad G_2^{(2)}=xy+2+y+y^2/2,\quad G_3^{(2)}=xy-1+2y-3y^2.$$

4 初期因子が多項式の場合

本章では初期因子 $G_i^{(0)}(x,tu)$ が x と $u_1,\ldots,u_\ell$ の多項式になる場合を考察する。簡単のため、(4) の変換を行なわず、$F(x,tu)$ 等を扱うことにする。まず、有理式係数の多項式 $G(x,u)\in\mathbf{K}\{(u)\}[x]$ に対して **Newton 多角形**を定義する。

定義 3 (Newton polygon for $G(x,u)$) *For each term $cx^it^ju_1^{j_1}\cdots u_\ell^{j_\ell}/D(tu)$ of $G(x,tu)$, where $c\in\mathbf{K}$, $j=j_1+\cdots+j_\ell$ and $D(u)$ is a homogeneous polynomial in $u_1,\ldots,u_\ell$ with $\mathrm{ord}(D)=d$, plot a dot at the point $(i,j-d)$ in the (e_x,e_t)-plane. The Newton polygon for $G(x,u)$ is a convex hull containing all the dots plotted.*

図 2 は例 1 と後述の例 3 における多項式に対する Newton 多角形である。Newton 線は Newton 多角形の一辺であることに注意されたい。

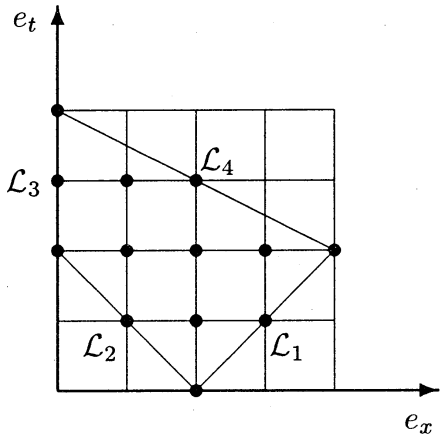

図 2 例 1 と例 3 の多項式に対する Newton 多角形

[SK99] によれば、初期因子 $G^{(0)}$ に対する Moses-Yun の補間式は $G^{(0)}$ と随伴初期因子 $H^{(0)} \stackrel{\text{def}}{=} F_{\text{New}}/G^{(0)}$ のみから一意的に定まり、対応する Hensel 因子 $G^{(k)}$ も、主項の係数部を定めれば、$G^{(0)}, H^{(0)}$ 及びそれらに対応する補間式で一意的に定まる。よって、理論解析では初期因子は $G^{(0)}, H^{(0)}$ の二つとする。

補題 4 拡張 Hensel 構成の初期因子の一つ $G^{(0)}(x,u)$ が多項式ならば、対応する補間式 $W^{(l)}$ $(l=0,1,\ldots,n-1)$ と Hensel 因子 $G^{(k)}$ $(k=1,2,\ldots)$ は $\mathbf{K}(u)[x]$ の要素である：

$$\begin{cases} W^{(l)}(x,u) \in \mathbf{K}(u)[x] & (l=0,1,\ldots,n-1), \\ G^{(k)}(x,u) \in \mathbf{K}(u)[x] & (k=1,2,3,\ldots). \end{cases} \tag{12}$$

そして、$W^{(l)}$ と $G^{(k)}$ の各係数部の分子と分母は $u_1,\ldots,u_\ell$ の同次式である。

証明 $W^{(l)}$ は $G^{(0)}$ と $H^{(0)}$ に拡張互除法と除算を適用して計算できる。これらの演算は $\mathbf{K}(u)$ 上の有理演算であるから、$W^{(l)} \in \mathbf{K}(u)[x]$ である。同様に、$G^{(k)}(x,u)$ は $F(x,u)$ と $G^{(0)}$, $H^{(0)}$、および対応する補間式に $\mathbf{K}(u)$ 上の加減乗算を適用して構成されるから、$G^{(k)} \in \mathbf{K}(u)[x]$ である。さらに、$G^{(0)}, H^{(0)}$ の各係数が $u_1,\ldots,u_\ell$ の同次式であり、拡張互助法と除算は係数部の同次性を保存するので、$W^{(l)}$ の各係数の分母部分が $u_1,\ldots,u_\ell$ の同次式となり、$G^{(k)}$ の各係数部もそうであることがいえる。 ■

補題 4 によると、$F(x,u)$ は次のように Hensel 因子に分解できる。

$$\begin{cases} F(x,tu) \equiv G^{(k)}(x,tu)\, H^{(k)}(x,tu) \pmod{I_{k+1}}, \\ G^{(k)}(x,u), H^{(k)}(x,u) \in \mathbf{K}(u)[x], \end{cases} \quad (k=1,2,\ldots). \tag{13}$$

上式において、F, $G^{(k)}$, $H^{(k)}$ の Newton 多角形をそれぞれ $\mathcal{N}, \mathcal{N}', \mathcal{N}''$ とし、これらの下辺を時計回りに順に $(\mathcal{L}_1,\cdots,\mathcal{L}_\rho)$, $(\mathcal{L}'_1,\cdots,\mathcal{L}'_\rho)$, $(\mathcal{L}''_1,\cdots,\mathcal{L}''_\rho)$ とする。ここで、$\mathcal{L}'_i$ と $\mathcal{L}''_i$

の対の一方は長さが0であってもよい（$\mathcal{L}'_i$ が長さ0のとき、$\mathcal{L}'_i$ は実質的には無である）。各 $i \in \{1,\ldots,\rho\}$ に対し、F, $G^{(k)}$, $H^{(k)}$ の各項でそれぞれ $\mathcal{L}_i$, $\mathcal{L}'_i$, $\mathcal{L}''_i$ 上にプロットされる項の和からなる多項式をそれぞれ $F_{\mathcal{L}_i}(x,u)$, $F'_{\mathcal{L}'_i}(x,u)$, $F''_{\mathcal{L}''_i}(x,u)$ と表す。辺 $\mathcal{L}_i$, $\mathcal{L}'_i$, $\mathcal{L}''_i$ の左端の座標をそれぞれ (n_i,ν_i), (n'_i,ν'_i), (n''_i,ν''_i) とし、$F_{\mathcal{L}_1}+\cdots+F_{\mathcal{L}_\rho}$ を次式とする。

$$F_{\mathcal{L}_1}+\cdots+F_{\mathcal{L}_\rho} \;=\; f_n^{(0)}(u)x^n+\cdots+f_{n_1}^{(0)}(u)x^{n_1}+\cdots+f_0^{(0)}(u). \tag{14}$$

補題 5 各 $i \in \{1,\ldots,\rho\}$ に対し、次式が成立する。

$$\begin{cases} \mathrm{length}(\mathcal{L}_i)=\mathrm{length}(\mathcal{L}'_i)+\mathrm{length}(\mathcal{L}''_i), \\ F_{\mathcal{L}_i}(x,u)=F'_{\mathcal{L}'_i}(x,u)\cdot F''_{\mathcal{L}''_i}(x,u). \end{cases} \tag{15}$$

ここで、$\mathrm{length}(\mathcal{L}'_i)=0$ ならば $F'_{\mathcal{L}'_i}(x,u)=1$ とおく。

証明 $G^{(k)}H^{(k)}$ に対する Newton 多角形は $\mathcal{N}$ である故、$G^{(k)}H^{(k)}$ は $F_{\mathcal{L}_1},\ldots,F_{\mathcal{L}_\rho}$ に対応する項を全て持つ。$F_{\mathcal{L}_i}$ に対応する $G^{(k)}H^{(k)}$ の項は $G^{(k)}$ と $H^{(k)}$ の Newton 多角形の同じ傾きの辺上に乗る必要がある（辺 $\mathcal{L}'_i$ と $\mathcal{L}''_j$ の傾きが異なれば、積 $F'_{\mathcal{L}_i}\cdot F''_{\mathcal{L}_j}$ の項が全体として一つの直線上に乗ることはない）。したがって、$\mathcal{N}$ の凸性より、$\mathcal{N}'$ と $\mathcal{N}''$ の各辺は $(\mathcal{L}'_1,\mathcal{L}''_1),\ldots,(\mathcal{L}'_\rho,\mathcal{L}''_\rho)$ と対にでき、各対に対して (15) が成立する。 ■

以下では、$\rho \geq 2$ と仮定し、$n_0=n$ とおく。また、$u_1,\ldots,u_\ell$ の有理式はたとえば部分分数分解などで一意的に簡約表現されると仮定する。

さて、$F_{\mathcal{L}_1}$ は $F_{\mathcal{L}_1}(x,u)=x^{n_1}F_1^{(0)}(x,u)$ の形をしているので、$F_1^{(0)}(x,u)$ を互いに素な多項式に分解することにより、$\mathbf{K}[x,u]$ において次のように分解できる。

$$\begin{cases} F_{\mathcal{L}_1}(x,u)=x^{n_1}\cdot\mathrm{cont}(F_{\mathcal{L}_1})\,G_{11}^{(0)}(x,u)\cdots G_{1r_1}^{(0)}(x,u), \\ \qquad \gcd(G_{1j}^{(0)},G_{1j'}^{(0)})=1 \text{ for any } j\neq j', \\ \qquad G_{1j}^{(0)}\text{の主数係数は1に規格化する}. \end{cases} \tag{16}$$

x^{n_1} と $G_{1j}^{(0)}(x,u)$ $(j=1,\ldots,r_1)$ を初期因子として拡張 Hensel を適用すると、$F(x,u)$ は次のように分解できる（$F_2(x,u)$ は初期因子 x^{n_1} に対応する Hensel 因子である）。

$$F(x,u)=F_2(x,u)\,\mathrm{cont}(F_{\mathcal{L}_1})\,G_{11}^{(\infty)}(x,u)\cdots G_{1r_1}^{(\infty)}(x,u).$$

補題5によると、$F_2(x,u)$ に対する Newton 多角形の下辺は $\mathcal{L}_2,\ldots,\mathcal{L}_\rho$ であるから、対応 $F_{\mathcal{L}_2}(x,u) \Longleftrightarrow$ [Newton polynomial for $F_2(x,u)$] が成立し、したがって次式が成立する。

$$F_{\mathcal{L}_2}(x,u)=[\text{Newton polynomial for } F_2(x,u)f_{n_1}^{(0)}(u)].$$

同様に $F_{\mathcal{L}_2}(x,u)$ を $\mathbf{K}[x,u]$ 内で因数分解し、この手順を続けると、次の定理を得る。

定理 6 (分解定理) $F(x,u)$ は $\mathbf{K}\{(u)\}[x]$ 内で次のように分解できる。

$$\left\{\begin{array}{c} F(x,u) \;=\; f_0^{(0)}(u)\prod_{i=1}^{\rho}\Big[\hat{g}_i(u)\cdot G_{i1}^{(\infty)}(x,u)\cdots G_{ir_i}^{(\infty)}(x,u)\Big], \\ \hat{g}_i(u)=\mathrm{cont}(F_{\mathcal{L}_i})/f_{n_i}^{(0)}(u)\quad (i=1,\ldots,\rho), \\ G_{i1}^{(0)}\cdots G_{ir_i}^{(0)}=\mathrm{pp}(F_{\mathcal{L}_i})\quad (i=1,\ldots,\rho), \\ \gcd(G_{ij}^{(0)},G_{ij'}^{(0)})=1 \text{ for any } j\neq j', \\ G_{ij}^{(\infty)}(x,u)\in\mathbf{K}\{(u)\}[x]\quad (j=1,\ldots,r_i). \end{array}\right. \tag{17}$$

証明 上述の議論より、$F(x,u)$ が (17) 第 1 ～ 第 4 式のように分解できることがいえる。問題は第 5 式の条件だけである。まず、任意の i と j に対し $G_{ij}^{(0)}(x,u)\in\mathbf{K}[x,u]$ である。さらに、拡張 Hensel 構成で $G_{ij}^{(0)}(x,u)$ に付け加わる項は $G_{ij}^{(0)}(x,u)$ に対する Newton 線の上側にのみプロットされるから、それらの位数は正である。ゆえに、任意の k に対して $G_{ij}^{(k)}(x,u)\in\mathbf{K}\{(u)\}[x]$ となる。 ■

上記手順では、$\mathcal{L}_1\Rightarrow\mathcal{L}_2\Rightarrow\cdots\Rightarrow\mathcal{L}_\rho$ の順に各辺上の Hensel 因子が決まる。$\mathcal{L}_\rho\Rightarrow\mathcal{L}_{\rho-1}\Rightarrow\cdots\Rightarrow\mathcal{L}_1$ の順に各辺上の Hensel 因子を決めるには次の変換をすればよい。

$$\mathcal{T}_{\mathrm{Rev}}:\; F(x,u_1,\ldots,u_\ell)\;\mapsto\; x^nF(1/x,u_1,\ldots,u_\ell). \tag{18}$$

さて、Hensel 因子として、右辺から左辺へと決めた (17) 式の因子 $G_{ij}^{(\infty)}$ と、左辺から右辺へと決めた次式の因子 $H_{ij}^{(\infty)}$ が得られた。

$$\left\{\begin{array}{c} F(x,u) \;=\; f_n^{(0)}(u)\prod_{i=1}^{\rho}\Big[\hat{h}_i(u)\cdot H_{i1}^{(\infty)}(x,u)\cdots H_{ir_i'}^{(\infty)}(x,u)\Big], \\ \hat{h}_i(u)=\mathrm{cont}(F_{\mathcal{L}_i})/f_{n_{i-1}}^{(0)}(u)\quad (i=1,\ldots,\rho). \end{array}\right. \tag{19}$$

定理 7 各 $i\in\{1,\ldots,\rho\}$ に対して、$G_{i1}^{(0)},\ldots,G_{ir_i}^{(0)}$ と $H_{i1}^{(0)},\ldots,H_{ir_i'}^{(0)}$ を $F_{\mathcal{L}_i}(x,u)$ の既約因数分解で決めれば、$r_i=r_i'$ で、かつ $G_{ij}^{(\infty)}(x,u)=U_{ij}(u)H_{ij}^{(\infty)}(x,u)$ $(j=1,\ldots,r_i)$ が成立する。ここで、U_{ij} は $\mathbf{K}\{(u)\}$ における単元である。

証明 $\mathbf{K}[x,u]$ における $F_{\mathcal{L}_i}(x,u)$ の既約因数分解は一意的ゆえ、$r_i=r_i'$ である。したがって、一般性を失うことなく、$G_{ij}^{(0)}=H_{ij}^{(0)}$ $(j=1,\ldots,r_i)$ としてよい。さて、$G_{ij}^{(\infty)}$ と $H_{ij}^{(\infty)}$ は共に $\mathbf{K}\{(u)\}[x]$ における $F(x,u)$ の因子であるが、任意の $i\neq i'$ あるいは $j\neq j'$ に対し、$G_{ij}^{(\infty)}\nmid H_{i'j'}^{(\infty)}$ である。なぜなら、$i\neq i'$ ならば、$G_{ij}^{(\infty)}$ と $H_{i'j'}^{(\infty)}$ の Newton 線は傾きが異なるし、$j\neq j'$ ならば、$\gcd(G_{ij}^{(0)},H_{i'j'}^{(0)})=1$ だからである。したがって、$G_{ij}^{(\infty)}|H_{ij}^{(\infty)}$ となるが、この除算を $G_{ij}^{(\infty)}$ の Newton 線に沿って行なうと、商は $1+\frac{g(u)}{h(u)}\in\mathbf{K}\{(u)\}$ となることが解る。すなわち、その商は $\mathbf{K}\{(u)\}$ における単元である。 ■

例2　次の多項式 (例1で用いたもの) で定理7を検証する（図2参照)。

$$\begin{aligned} F(x,y) &= x^4y^2 + x^3(3y^2+y) + x^2(y^3-2y^2+3y-2) \\ &\quad + x(3y^3-9y^2-5y) + (-2y^4-5y^3+3y^2). \end{aligned}$$

まず、(17) 流に6次まで拡張 Hensel 構成すると、次式を得る。

$$\begin{aligned} F_2^{(6)} &= x^2 + x(5y/2 + 33y^2/4 + 9y^3/2 - 259y^4/8 - 4537y^5/32) \\ &\quad - 3y^2/2 + y^3/4 + 19y^4/4, \\ G_{11}^{(6)} &= xy + 2 + y + y^2/2 - 5y^3/4 + y^4/2 + 3y^5/8 - 39y^6/32, \\ G_{12}^{(6)} &= xy - 1 + 2y - 3y^2 - 7y^3 - 5y^4 + 32y^5 + 143y^6. \end{aligned}$$

$F_2^{(0)} = x^2$ ゆえ、$F_2^{(6)}$ をさらに拡張 Hensel 構成する（$F_2^{(6)}$ の精度では2次までしか構成できない)。

$$\begin{aligned} F_2^{(6)} &\equiv G_{21}^{(2)} \cdot G_{22}^{(2)} \pmod{\langle x^2y^2, xy^3, y^4\rangle}, \\ G_{21}^{(2)} &= x + 3y + 7y^2 + 5y^3, \\ G_{22}^{(2)} &= x - y/2 + 5/4y^2 - 1/2y^3. \end{aligned}$$

つぎに、(19) 流に拡張 Hensel 構成する。$F(x,y)$ に (18) の変換 $\mathcal{T}_{\mathrm{Rev}}$ を施すと、$\bar{F}(x,y)$ とその Newton 多項式 $\bar{F}_{\mathrm{New}}(x,y)$ として次式が得られる。

$$\begin{aligned} \bar{F}(x,y) &= x^4(3y^2-5y^3-2y^4) + x^3(-5y-9y^2+3y^3) \\ &\quad + x^2(-2+3y-2y^2+y^3) + x(y+3y^2) + y^2, \\ \bar{F}_{\mathrm{New}}(x,y) &= 3x^4y^2 - 5x^3y - 2x^2 = (3x^2)\cdot(xy+1/3)\cdot(xy-2). \end{aligned}$$

$\bar{F}_1^{(0)} = 3x^2$, $\bar{H}_{21}^{(0)} = xy + 1/3$, $\bar{H}_{22}^{(0)} = xy - 2$ とおいて $\bar{F}(x,y)$ の拡張 Hensel 構成を4次まで実行し、各 Hensel 因子に逆変換 $\mathcal{T}_{\mathrm{Rev}}^{-1}$ を施すと次式が得られる。

$$\begin{aligned} F_1^{(4)} &= -x^2(3y^2/2) - x(3y/2 + 17y^2/4 - 37y^3/4) + 3 - 5y - 2y^2, \\ H_{21}^{(4)} &= x(1/3 - 7y/9 + 34y^2/27 + 155y^3/81 + 250y^4/243) + y, \\ H_{22}^{(4)} &= -x(2 + 5y + 21y^2/2 + 79y^3/4 + 40y^4) + y. \end{aligned}$$

定理7によれば、$\{G_{21}^{(\infty)}, G_{22}^{(\infty)}\} \Longleftrightarrow \{H_{21}^{(\infty)}, H_{22}^{(\infty)}\}$ なる対応が成立するはずだが、単元 $U_{2j}(u)$ の不定性がある。そこで、この不定性を主係数を1に規格化することにより除く (それには $H_{2j}^{(\infty)}$ $(j=1,2)$ を主係数で割る … ただし、除算はべき級数除算！) :

$$\begin{aligned} G_{21}^{(4)} &:= H_{21}^{(4)}/\mathrm{lc}(H_{21}^{(4)}) = x + 3y + 7y^2 + 5y^3 - 32y^4, \\ G_{22}^{(4)} &:= H_{22}^{(4)}/\mathrm{lc}(H_{22}^{(4)}) = x - y/2 + 5y^2/4 - y^3/2 - 3y^4/8. \end{aligned}$$

$G_{2j}^{(k)}$ は左方向から構成した方が効率的であることに注意されたい。 ■

5 多変数多項式 ($\ell \geq 2$) の因数分解への応用

$\ell = 1$ の場合、(2) の $G(u)$ は u_1 のべき級数となって、$G^{(k)}(x, u_1)$ の係数部に有理式が現れることはない。そこで、本章では $\ell \geq 2$ とする。

さて、$F(x,u)$ が $\mathbf{K}[x,u]$ 内で $F(x,u) = G(x,u)H(x,u)$ と分解される場合を考える。定理 6 によると、主係数をうまく調節すれば、(17) の Hensel 因子のいくつかの積で $G(x,u)$ と $H(x,u)$ が表されるはずである ($f_0^{(0)}(u)$ と $\hat{g}_1(u), \ldots, \hat{g}_\rho(u)$ を含めた主係数の調節は通常の主係数処理法で行なえばよい)。これが拡張 Hensel 構成を用いた特異な多変数多項式の因数分解の原理であるが、この方法を実用化するには、Hensel 因子の効率的な組み合わせ方を考案する必要がある。特に、$G_{ij}^{(k)}(x,u)$ の係数部は一般に $u_1, \ldots, u_\ell$ の有理式なので、その場合の処理法を考えなければならない。

定義 8 (integral and rational Hensel factors) *If a Hensel factor* $G_{ij}^{(\infty)}(x,u)$ *in* (17) *is an integral power series in* $u_1, \ldots, u_\ell$ *then we call it* integral, *otherwise* rational.

$\mathbf{K}$ 上の $u_1, \ldots, u_\ell$ のべき級数環を $\mathbf{K}\{u\}$ と表すとき、$\mathbf{K}[x,u] \subset \mathbf{K}\{u\}[x] \subset \mathbf{K}\{(u)\}[x]$ ゆえ、一般に、[多項式因子] = [integral な因子の積]、[integral な因子] = [rational な因子の積]、となる。integral な因子を如何に組み合わせて多項式因子を作り出すかについては多くの研究がなされている。そこで、以下では、rational な因子を組み合わせて integral な因子を作り出すことを考える。

まず、拡張 Hensel 因子の分母項について調べる。前章と同様、一般性を失うことなく、初期因子は $G^{(0)}, H^{(0)}$ の二つとし、対応する補間式をそれぞれ $W^{(l)}, V^{(l)}$ とする。

$$\begin{cases} F_{\mathrm{New}}(x,u) = G^{(0)}(x,u)H^{(0)}(x,u), \\ G^{(0)} = g_{n'}x^{n'} + \cdots + g_0x^0, \\ H^{(0)} = h_mx^m + \cdots + h_0x^0, \end{cases} \quad n = n' + m, \tag{20}$$

$$\begin{cases} V^{(l)}G^{(0)} + W^{(l)}H^{(0)} = x^l, \\ \deg(V^{(l)}) < m, \ \ \deg(W^{(l)}) < n', \end{cases} \quad l = 0, 1, \ldots, n-1. \tag{21}$$

部分終結式理論によると、$V^{(0)}$ と $W^{(0)}$ は次のように行列式で表せる。

$$V^{(0)} = \begin{vmatrix} g_{n'} & \cdots & g_1 & g_0 & & x^{m-1} \\ & \ddots & \cdots & \ddots & \ddots & \vdots \\ & & g_{n'} & \cdots & g_1 & x^0 \\ h_m & \cdots & h_1 & h_0 & & 0 \\ & \ddots & \cdots & \ddots & \ddots & \vdots \\ & & h_m & \cdots & h_1 & 0 \end{vmatrix} / \operatorname{res}(G^{(0)}, H^{(0)}), \tag{22}$$

$$W^{(0)} = [\text{replace the last column by } (0, \cdots, 0, x^{n'-1}, \cdots, x^0)^{\mathrm{T}}]. \tag{23}$$

さらに、$l \geq 1$ のとき、$V^{(l)}$ と $W^{(l)}$ は次式で計算できる。

$$V^{(l)} = \mathrm{rem}(x^l V^{(0)}, H^{(0)}), \quad W^{(l)} = \mathrm{rem}(x^l W^{(0)}, G^{(0)}). \tag{24}$$

特に、$H^{(0)} = x^m$ の場合には $V^{(l)}$ と $W^{(l)}$ は次式となる。

$$l \geq m \text{ のとき} \quad \begin{cases} V^{(l)} = 0, \\ W^{(l)} = x^{l-m}, \end{cases} \tag{25}$$

$$l < m \text{ のとき} \quad \begin{cases} V^{(l)} = x^l \cdot G^{(0)}_{\mathrm{Inv}\langle x^{m-l}\rangle}, \\ W^{(l)} = [G^{(0)}_{\mathrm{Inv}\langle x^{m-l}\rangle} \cdot G^{(0)} - 1]/x^{m-l}, \end{cases} \tag{26}$$

$$\text{ここで} \quad G^{(0)}_{\mathrm{Inv}\langle x^{m-l}\rangle} = [\,\text{Inverse of } G^{(0)} \text{ modulo } x^{m-l}\,]. \tag{27}$$

命題 9 拡張 Hensel 因子 $G^{(\infty)}, H^{(\infty)}$ が rational な場合、それらの有理式係数の分母に現れる因子は $\mathrm{res}(G^{(0)}, H^{(0)})$, $g_{n'}$, h_m, およびそのべき乗のみである。特に、$H^{(0)} = x^m$ の場合には、$G^{(\infty)}$ と $H^{(\infty)}$ の分母に現れるのは g_0 のべき乗のみである。

証明 拡張 Hensel 構成の出発時には $F, G^{(0)}, H^{(0)} \in \mathbf{K}[x, u]$ で、補間式 $V^{(l)}, W^{(l)}$ の係数部のみが $u_1, \ldots, u_\ell$ に関する有理式になりえる。そして、拡張 Hensel 構成ではこれ以外に有理式が現れる余地はない。(22), (23) によると、$V^{(0)}, W^{(0)}$ の分母には $\mathrm{res}(G^{(0)}, H^{(0)})$ が現れ、$V^{(l)}, W^{(l)}$ $(l \geq 1)$ の分母には $H^{(0)}, G^{(0)}$ による除算でそれぞれ $h_m, g_{n'}$ のべき乗が現れる。特に、$H^{(0)} = x^m$ の場合には $\mathrm{res}(x^m, G^{(0)}) = g_0^m$ で、$G^{(0)}_{\mathrm{Inv}\langle x^{m-l}\rangle}$ は分母因子として g_0 のみを含む（$G^{(0)}_{\mathrm{Inv}\langle x^{m-l}\rangle}$ は $G^{(0)}$ の定数項を最高順位項として、すなわち $G^{(0)}$ を x のべき級数とみなして、1 を $G^{(0)}$ で割った商であり、分母には g_0 のべき乗のみが現れる。たとえば、$G^{(0)}_{\mathrm{Inv}\langle x\rangle} = 1/g_0$, $G^{(0)}_{\mathrm{Inv}\langle x^2\rangle} = -g_1 x/g_0^2 + 1/g_0$、等である）。 ■

注釈 2　上記命題 9 によると、定理 6 において、辺 $\mathcal{L}_i$ 上の拡張 Hensel 因子の分母項は辺 $\mathcal{L}_{i+j}$ $(j \geq 1)$ 上の Hensel 因子には伝搬せず、伝搬するのは $f^{(0)}_{n_i}$ のみである。

命題 10 一方が integral で他方が rational な拡張 Hensel 因子の積が integral になることはなく、分母の因子が本質的に異なる（すなわち、多重度と共通因子を除いたとき異なる）rational な拡張 Hensel 因子の積が integral になることはない。

証明 $G^{(\infty)}$ が integral で $H^{(\infty)}$ が rational とし、$H^{(\infty)}$ に最初に現れる有理式項を T/h とする。$G^{(\infty)}H^{(\infty)}$ が integral なら、まず $G^{(0)}T/h$ において h がキャンセルしなければならないが、T は h に関して簡約済みなので、$G^{(0)}$ が h で割り切れる必要がある。ところが、仮定より $G^{(0)}$ は原始的ゆえ、それは不可能である。

つぎに、$G^{(\infty)}$ と $H^{(\infty)}$ が rational な場合、これらに最初に現れる分母項をそれぞれ g, h とし、次式のように表す。

$$G^{(\infty)} = G^{(0)} + \cdots + S/g + \cdots, \quad H^{(\infty)} = H^{(0)} + \cdots + T/h + \cdots.$$

ただし、$g,h \in \mathbf{K}[u]$, $S,T \in \mathbf{K}[x,u]$, S/g と T/h は簡約済みで、当面 $\gcd(g,h)=1$ とする。$G^{(0)}$ と $H^{(0)}$ をそれぞれ h と g で可能な限り簡約したとき、$G^{(0)} = hQ_G + \hat{G}^{(0)}$, $H^{(0)} = gQ_H + \hat{H}^{(0)}$、$Q_G, Q_H \in \mathbf{K}[x,u]$ とする。さて、$G^{(\infty)}H^{(\infty)}$ が integral なら、

$$G^{(0)}\,T/h + H^{(0)}\,S/g \in \mathbf{K}[x,u] \implies \hat{G}^{(0)}\,T/h + \hat{H}^{(0)}\,S/g \in \mathbf{K}[x,u]$$

でなければならない。$\hat{G}^{(0)}$ と T が h に関して簡約済み、$\hat{H}^{(0)}$ と S が g に関して簡約済みゆえ、上式が成立するには $\deg(\hat{G}^{(0)}T) = \deg(\hat{H}^{(0)}S)$ と $g\cdot\mathrm{lc}(\hat{G}^{(0)}) = -h\cdot\mathrm{lc}(\hat{H}^{(0)})$ がまず必要である。この式と $\gcd(g,h)=1$ の仮定より、$g \,|\, \mathrm{lc}(\hat{H}^{(0)})$, $h \,|\, \mathrm{lc}(\hat{G}^{(0)}) \implies g \,|\, \mathrm{lc}(H^{(0)})$, $h \,|\, \mathrm{lc}(G^{(0)})$ を得る。同様の論法で $G^{(0)}$ と $H^{(0)}$ の他の係数も順に h と g の倍数となり、$h \,|\, G^{(0)}$, $g \,|\, H^{(0)}$ でなければならない。ところが、仮定より $G^{(0)}$ と $H^{(0)}$ は原始的ゆえ、分母因子 g,h が消えることはありえない。

最後に、$g = c\hat{g}$, $h = c\hat{h}$, $\gcd(\hat{g},\hat{h})=1$ の場合も、$G^{(\infty)}H^{(\infty)}$ が integral ならば、まず因子 $\hat{g},\hat{h}$ がキャンセルされねばならないから、上記の議論がそのまま適用できる。 ■

注釈 3　上記命題 10 において、integral (rational) な Hensel 因子とは、積が integral (resp., rational) になる一群の因子でもよい。

命題 10 から、拡張 Hensel 因子の組み合わせに対して次の戦略を得る。

1. まず、各 $i \in \{1,\ldots,\rho\}$ に対し、辺 $\mathcal{L}_i$ 上の拡張 Hensel 因子が固有の分母因子を持てば、同じ分母を持つ Hensel 因子を組み合わせて、固有の分母因子を消去する。
2. 次に、異なる辺上の拡張 Hensel 因子が同じ分母を持てば、分母因子の多い順から Hensel 因子を組み合わせて、その分母を消去する。

例 3　次の 3 変数多項式 $F(x,y,z)$ で上述の組み合わせ方を見る（図 2 参照）。

$$\begin{aligned} F(x,y,z) \;=\; & x^4(y^2-z^2) + x^3(y+3z+3y^2+3z^2) \\ & + x^2(-2+3y-4z-2y^2+4yz-2z^2+y^3+5y^2z+3z^3) \\ & + x^1(-5y-9y^2-5yz-5z^2+3y^3+y^2z-5z^3) \\ & + (3y^2-5y^3-7y^2z-yz^2-2y^4-3y^2z^2-3yz^3-2z^4). \end{aligned} \tag{28}$$

$F(x,y,z)$ の Newton 多項式 $F_{\mathcal{L}_1}$ とその既約因数分解は次式となる。

$$F_{\mathcal{L}_1} = x^4(y^2-z^2) + x^3(y+3z) - 2x^2 = x^2\cdot[x(y-z)+2]\cdot[x(y+z)-1].$$

$F_2^{(0)} = x^2$, $G_{11}^{(0)} = x(y-z)+2$, $G_{12}^{(0)} = x(y+z)-1$ とおく。$F_2^{(0)}$, $G_{11}^{(0)}$, $G_{12}^{(0)}$ に対する

Moses-Yun の補間式 $V_2^{(l)}, W_{11}^{(l)}, W_{12}^{(l)}$ $(l=0,1,2,3)$ は次式となる。

$$\begin{array}{lll} V_2^{(0)} = -[x(y+3z)+2]/4, & W_{11}^{(0)} = -(y-z)^3/(12y+4z), & W_{12}^{(0)} = (y+z)^3/(3y+z), \\ V_2^{(1)} = -x/2, & W_{11}^{(1)} = (y-z)^2/(6y+2z), & W_{12}^{(1)} = (y+z)^2/(3y+z), \\ V_2^{(2)} = 0, & W_{11}^{(2)} = -(y-z)/(3y+z), & W_{12}^{(2)} = (y+z)/(3y+z), \\ V_2^{(3)} = 0, & W_{11}^{(3)} = 2/(3y+z), & W_{12}^{(3)} = 1/(3y+z). \end{array}$$

見て解るとおり、$W_{1j}^{(l)}$ は従変数 y,z に関して有理式となっている。

拡張 Hensel 構成を実行すると 2 次の因子から有理式係数が現われる：

$$\begin{aligned} F_2^{(2)} &= x^2 + 5xy/2, \\ G_{11}^{(2)} &= x(y-z) + 2 + (y+2z) + (y^2/2 - yz/6 - 4z^2/9) + \frac{4z^3/9}{3y+z}, \\ G_{12}^{(2)} &= x(y+z) - 1 + (2y-z) - (3y^2 + 10yz/3 + 2z^2/9) + \frac{2z^3/9}{3y+z}. \end{aligned}$$

$G_{11}^{(2)} \times G_{12}^{(2)}$ では、当然、位数 2 までの項では有理式の係数は分子と分母がキャンセルして消える。上式 $G_{11}^{(2)}$ と $G_{12}^{(2)}$ は $\mathcal{L}_1$ 上の Hensel 因子である。つぎに $\mathcal{L}_2$ 上の Hensel 因子を調べる。(28) より、$\mathcal{L}_2$ 上の Newton 多項式 $F_{\mathcal{L}_2}$ とその既約因数分解は次式となる。

$$F_{\mathcal{L}_2} = -2x^2 - 5xy + 3y^2 = -2(x+3y)\,(x-y/2).$$

$G_{21}^{(0)} = x+3y$, $G_{22}^{(0)} = x-y/2$ とおくと、対応する補間式 $W_{2j}^{(l)}$ $(j=1,2)$ は次式となる。

$$\begin{array}{ll} W_{21}^{(0)} = -2/(7y), & W_{22}^{(0)} = 2/(7y), \\ W_{21}^{(1)} = 6/7, & W_{22}^{(1)} = 1/7. \end{array}$$

これから、$\mathcal{L}_2$ 上の Hensel 因子 $G_{2j}^{(k)}$ の分母項に現れる可能性のある因子は y のべき乗であることが解る。したがって、$\mathcal{L}_1$ 上の Hensel 因子に現れる分母因子 $(3y+z)$ を消去するには $\mathcal{L}_1$ 上の因子 $G_{11}^{(2)}$ と $G_{12}^{(2)}$ を掛けるしかない。そこで、改めて $G_1^{(0)} = G_{11}^{(0)} G_{12}^{(0)}$ と $G_2^{(0)}$ を初期因子として拡張 Hensel 構成を 3 次まで行なうと、Hensel 因子 $G_1^{(\infty)}, G_2^{(\infty)}$ は無限級数となることが解り、上記 $F(x,y,z)$ は既約多項式であることが解る。 ■

例 4　異なる辺上での Hensel 因子を組み合わせる例。

$$\begin{aligned} F(x,y,z) &= x^4(y^2-z^2) + x^3(y+3z+3y^2+3z^2) \\ &\quad + x^2(-2+3y-4z-2y^2+5yz-2z^2+y^3+6y^2z+3z^3) \\ &\quad + x^1(-5y-9y^2-5yz-5z^2+3y^3+y^2z-5z^3) \\ &\quad + (3y^2-5y^3-7y^2z-yz^2-2y^4-3y^2z^2-3yz^3-2z^4). \end{aligned} \tag{29}$$

上式は例3の多項式の二つの項 $4x^2yz$, $5x^2y^2z$ の係数を少し変えたものであり、初期因子も Moses-Yun の補間式も例3のそれと同じである。例3と同じ記号を用い、拡張 Hensel 構成を4次まで実行すると、分母因子が魔法のようにキャンセルして次式を得る。

$$F_2^{(4)} = x^2 + x(5y/2 + 33y^2/4 - 5yz/2 + 5z^2/2 + 9y^3/2 - \cdots - 5z^3/2) - 3y^2/2,$$
$$G_{11}^{(4)} = x(y-z) + 2 + y + 2z + y^2/2 - yz/2 - 5y^3/4 - \cdots + z^3/2 + y^4/2 + \cdots - z^4/2,$$
$$G_{12}^{(4)} = x(y+z) - 1 + 2y - z - 3y^2 - 3yz - 7y^3 - \cdots - 2z^3 - 5y^4 + \cdots + 2z^4.$$

$G_{11}^{(4)}$ と $G_{12}^{(4)}$ は integral ゆえ、$F_2^{(k)}$ の $\mathcal{L}_2$ 上での拡張 Hensel 因子が integral なら、それらと組み合わせて多項式因子を作れる可能性がある。拡張 Hensel 構成してみると、$F_2^{(k)}$ の因子 $G_{2j}^{(3)}$ $(j=1,2)$ は integral となり、$G_{1j}^{(3)}G_{2j}^{(3)}$ $(j=1,2)$ から多項式因子が得られる。

6 おわりに

上述の理論をみると、拡張 Hensel 構成は奥が深いことがうかがえる。今までに解明したことはほんの表層だけで、多変数多項式の特異性との関連など、数学的に解明すべき点が多々ある。また、実用面、たとえば因数分解への応用でもさらなる研究が望まれる。今後は、算法をインプリメントしつつ、種々の観点から研究を進め、日本生まれのこの算法を是非とも数式処理の基本算法の一つにしていきたい。

参 考 文 献

[Kuo89] T.-C. Kuo: *Generalized Newton-Puiseux theory and Hensel's lemma in* $\mathbf{C}[[x,y]]$, Can. J. Math., Vol. XLI, 1101-1116 (1989).

[Mus71] D. R. Musser: *Algorithms for polynomial factorizations*, Ph.D. Thesis, University of Wisconsin, 1971.

[SK99] T. Sasaki & F. Kako: *Solving multivariate algebraic equation by Hensel construction*, Japan J. Indus. Appl. Math., **16**, 257-285 (1999). (This paper was submitted in March, 1993, and the authors recieved referees' reports in Sep., 1996 and the letter of acceptance in June, 1998.)

[Wan77] P. S. Wang: *Preserving sparseness in multivaraite polynomial factorization*, Proc. 1977 MACSYMA Users Conference (1977), 55-61.