数理解析研究所講究録 1286 巻 2002 年 51-60

有限体上の多項式イデアルの素イデアル分解について

横山 和弘
九州大学大学院 数理学研究院
yokoyama@math.kyushu-u.ac.jp

1 はじめに

現在では、有理数体上の多項式環において、Gröbner 基底計算と多項式の因数分解計算を組合せることで、準素イデアル分解を実際に計算することが可能になっている。これらを一般化して、標数 0 の計算可能な体の上の多項式環でも原理的に準素イデアル分解は計算可能になっている。(最近の計算面での進捗については、 [4] を参照されたい。) 簡単のために、以下では準素イデアル分解の代わりに準素分解と言うことにする。

一方、正標数の場合では、準素分解とそれに密接に関係する根基計算に関して、一般的な形で計算可能性が議論されているが、実際の計算機でどのように実現するかは明確にされていない。そこで、実際の計算機で効率よい計算を実現させることは、大変興味深い問題となっている。さらに、純粋数学の研究や代数幾何符号の設計といった工学への応用も考えられ、ひとたび実現されれば、大きな広がりが期待できる。そこで、まず、最も基本である有限体上の多項式環でのイデアルの準素分解計算の効率的かつ実際的な実現が第 1 の目的となる。この実現には、素因子より対応する準素成分を抽出する効率的な方法である局所化計算技法 [12] が適用できる。局所化計算技法は Gröbner 基底計算をベースとし、標数には無関係であることから、準素分解の問題は、素因子の計算、すなわち素イデアル分解に帰着される。(これも簡単のため、素分解と呼ぶことにする。) しかし、素分解に関しては、標数 0 と正標数では、計算面において大きな差があり、通常の標数 0 の方法が直接に正標数の場合に適応できないという問題が生ずる。

そこで、本論文では、この素分解について、標数 0 の場合の最も基本的である有限体上の多項式環を考え、新たな計算アルゴリズムを提案するものである。実際的な計算のために、正標数で成功した Gianni-Trager-Zaccharias [7] の戦略を用い、正標数特有の状況に対応するために、分離的イデアルとイデアルの分離閉包という概念を導入する。提案するアルゴリズムのすべての計算は、極めて基本的といえる計算、すなわち、有限体上の Gröbner 基底計算と多項式の因数分解からなっており、全体としての効率性は個々の部品の効率性に依存している。残念ながら、今の段階では、実装がすべて終わっていないため、実際の有効性については今後の実験を待つことになる。その代わりとして、本論文では、実際の実装に関するいくつかの改良点を挙げることとする。注意として、素分解は、正標数での根基イデアル計算と密接な関係がある。この関係は、多項式の因数分解を考えれば、既約因子計算と無平方分解との関係に相当する。

2 数学的背景

ここでは、正標数での素分解における重要な点をまとめる。以下では、標数 p、位数 q の有限体 $K = GF(q)$ を係数体とする多項式環 $K[x_1, \ldots, x_n]$ を考える。変数全体の集合 $[x_1, \ldots, x_n]$ を X で表す。一般の記法として、ネーター環 R に対して、R の元 $f_1, \ldots, f_t$ で生成されるイデアルを $Id_R(f_1, \ldots, f_t)$ で表し、R

のイデアル I に対して、その根基イデアルを $\sqrt{I}$ で表し、I の R の元 f に対する商イデアルを $(I:f)$ で表すことにする。さらに、I の素因子全体の集合を $\mathrm{Ass}(I)$ で、孤立素因子全体の集合を $\mathrm{Ass}_{iso}(I)$ で表す。このとき、$\sqrt{I}=\cap_{P\in Ass_{iso}(I)}P$ であり、$\mathrm{Ass}(\sqrt{I})$ は $\mathrm{Ass}_{iso}(I)$ に一致する。つまり、I の素分解とは、$\mathrm{Ass}_{iso}(I)$ を計算することに他ならない。

K の任意の拡大体 L に対して、L を係数体とし、変数集合を Z とする多項式環 $L[Z]$ のイデアル J を考えたとき、J のアフィン多様体として L の代数閉包 $\bar{L}$ での J の零点全体の集合を考えることとする。さらに、$V_{\bar{L}}(J)$ で表す。逆に、アフィン多様体 W に対し、対応するイデアル $\{f\in L[Z]\mid f(\alpha)=0 \text{ for any } \alpha\in W\}$ を $I_{L[Z]}(W)$ で表す。

2.1 逐次計算と同時計算

素分解計算では、大きく2種類のアプローチがあり、ひとつは逐次計算法、他方は同時計算法と呼ぶことができる。Kalkbrener [8] は可換ネーター環 R に関して、R の素分解が計算可能であり、さらに、R の素イデアル P による剰余類環の商体 $Q(R/P)$ を係数体とする一変数多項式の因数分解が計算可能であるという条件のもとで、一変数多項式環 $R[x]$ の素分解が計算可能になるという、計算可能性に関する帰納的な証明を与えている。この方向に従えば、イデアルの同次元成分を計算すれことで ([7, 12, 3] を参照)、素分解計算を有理関数体を係数体とする 0 次元イデアルの素分解計算に帰着できることを使って、以下に翻訳できる。ある変数集合 $Y\subset X$ を抜き出して $L=K(Y)$ とすれば、L の代数拡大体上の一変数多項式の因数分解が計算できれば、消去イデアル $I\cap L[Z\cup\{z\}]$ の素分解が $I\cap L[Z]$ より計算できることになる。ここで $Z\subset X\setminus Y$ であり、$z\in X\setminus(Z\cup Y)$ とする。つまり、この方法は、有理関数体の代数拡大を逐次的に計算していく方法であり、逐次計算法と呼ぶことができる。

したがって、この逐次計算方式を採用するのであれば、有理関数体上の一変数多項式の因数分解の効率的計算が本質的となる。しかし、代数拡大体上の多項式の因数分解は基礎体上の多項式の因数分解に帰着して計算されることより、実際的な素分解の実現としては、素分解を逐次拡大として計算せずに基礎体の上の計算として同時に計算してしまう方法がより有効であるものと考える。ここでは、この方法を同時計算法と呼ぶことにする。

本論文では、この同時計算法を採用することとし、その実現として、標数 0 の場合に大変有効であった、戦略 [7]、すなわち、一般的な位置にある元を利用した分解、を改良して使用する。このとき提案する方式は、以下の特徴を持つ。

- 正標数の場合に生じる計算面での問題点を解決するために、イデアルの分離閉包という概念を導入する。
- 多項式の因数分解を考える場合は、いつでも基礎体、すなわち完全体である $K=GF(q)$ 上の多項式を扱い、これにより計算が大変単純化される。

2.2 分離性と一般の位置の点を利用した分解

計算のために、必要な概念を準備する。Y を変数集合 X の真の部分集合とし、$Z=X\setminus Y$、$L=K(Y)$ とおく。簡単のために、変数に順番を付け、$Z=\{x_1,\ldots,x_s\}$、$Y=\{x_{s+1},\ldots,x_n\}$ としておく。さらに、これ以外の新たな変数を t で表す。

定義 2.1 $L[Z]$ のイデアル J が分離的であるとは、J が以下を満たすときに言う。
(1) J は *0* 次元根基イデアルである。

(2) J のすべての素因子 P に対して、剰余類環 $L[Z]/P$ は体 L の分離拡大となる。

ここで定義した分離性は根基計算での逐次計算法 [5] で使われた分離性に対応する。

定義 2.2 L 上の一変数多項式 $f(x)$ が分離的であるとは、$f(x)$ が重根をもたないときに言う。ここで、根は L の代数閉包 $\tilde{L}$ で考えるものとする。一変数多項式 $f(x)$ に対して、ある分離的多項式 $h(x)$ が存在して、$f(x) = h(x^{p^e})$、ここで e はある非負整数、となるとき、$h(x)$ を $f(x)$ の分離閉包と呼び、$\mathrm{sc}(f)$ で表す。

定義 2.3 J を $L[Z]$ の *0* 次元イデアルとする。$L[Z]$ の多項式 $f(Z)$ に対して、$f(Z)$ の J に関する最小多項式 m_f を L 上のモニックな一変数多項式で、$h(f)$ が J に属するような多項式の中で次数が最小のものとして定義する。

Z に属する各変数 x に対して、x の J に関する最小多項式 m_x は消去イデアル $J \cap L[x]$ の生成元になっていることに注意しておく。

命題 2.4 J を $L[Z]$ の *0* 次元イデアルとする。もし、Z に属する各変数 x の J に関する最小多項式がすべて分離的であれば、J は分離的である。

証明： 分離性の定義より、Z に属するすべての変数 x に対して、$\gcd(m_x, dm_x/dx) = 1$ となる。Seidenberg の補題 92 [11] (Lemma 8.13 [2] を参照) により J は根基イデアルである。

次に $Ass(J)$ を考えよう。各素因子 $P \in Ass(J)$ に対して、$L' = L[Z]/P$ は L の拡大体であり、さらに、$V_{\tilde{L}}(P)$ の任意の元 $\alpha = (\alpha_1, \ldots, \alpha_s)$ に対し、$L' \cong L(\alpha_1, \ldots, \alpha_s)$ となる。一方、各 α_i は分離多項式 m_{x_i} の根であるので、各 α_i は L 上の分離元である。したがって、$L(\alpha_1, \ldots, \alpha_s)$ は L の分離拡大となる。∎

定義 2.5 J を $L[Z]$ の分離イデアルとする。$L[Z]$ に属する多項式 $g(Z)$ が J に関して一般的な位置にあるとは、J の各素因子 P に対して、$g(Z)$ は分離拡大の $L[Z]/P$ の原始元になっているときに言う。

基礎体 K の元の個数が十分あれば、以下に述べる命題 2.6 を効率的な判定条件として利用することで、一般の位置にある多項式 $g(Z)$ が一次式 $\sum_{x_i \in Z} a_i x_i$, $a_i \in K$ の中から効率よく探し出すことができる。(命題 2.6 は Proposition 8.69 [2] の特殊な形として考えられる。素因子の co-maximality より証明される。) 各係数の分母を払うことで、最小多項式 m_g は K 上の新しい変数 t と Y に関する多項式として扱うことができることに注意する。

命題 2.6 J を $L[Z]$ の分離的イデアルとする。多項式 $g(Z)$ が J に関して一般の位置にあるための必要十分条件は $g(Z)$ の J に関する最小多項式 m_g が $\deg(m_g) = \dim_L(L[Z]/J)$ を満たすことである。さらにこの場合、$m_g = m_1 \cdots m_r$ を最小多項式 m_g の L 上での因数分解とすると、各因子 m_i に対して、$P_i = Id_{L[Z]}(J, m_i(g))$ は J の素因子となり、$J = \cap_{i=1}^{r} P_i$ は J の素分解を与える。

以上により、分離的イデアルに対しては, ひとたび一般の位置の元 (多項式) が見つかれば、素分解は一般の位置の元の最小多項式の因数分解で計算できることがわかる。ここで、この計算手順を一般の位置の元を利用した分解と呼ぶことにする。基礎体 K の標数が 0 の場合には、各根基イデアルは分離的であり、ほとんどすべての一次式は一般の位置にある。しかし、正標数の場合では、この手順をそのままでは適用できないときがある。

- たとえ J が根基イデアルであっても、J は分離的であるとは限らない。つまり、一般の位置にある多項式の存在が保障できない場合がある。さらに、J が分離的であっても、K 上の一次式の中に一般の位置にある元が存在しない場合もある。

- 根基イデアル計算において Seidenberg の補題 [11] を利用できない。したがて、別の方法 [9, 5] を適用することになる。しかし、この場合、基礎体が完全体でない場合には、根基計算は非常に複雑になり、計算の効率が阻害される。さらに、この場合には、多項式の因数分解に関しても、無平方分解の段階で特殊な取り扱いが必要になり、計算がより複雑になってしまう。

例 2.7 $GF(p)(u,v)[x,y]$ において, $Id(x^p-u, y^p-v)$ は素イデアルであるが、分離的ではない。さらに、一般の位置にある元が存在しない。また、$GF(p)(z)[x,y]$ において $Id(x^p-z, y^p-z)$ は素イデアル $Id(x^p-z, x-y)$ に対応する準素イデアルであるが、各変数の最小多項式はみな既約になっている。

2.3 イデアルの分離閉包

定義 2.8 J を $L[Z]$ の 0 次元イデアルとする。$L[Z]$ のあるイデアル J' が次の条件を満たすとき、J' を J の分離閉包と呼び、$\mathrm{sc}(J)$ で表す。
(1) J' は $L[Z]$ の分離的イデアルである。
(2) J の零点 $(V_{\tilde{L}}(J))$ と J' の零点 $(V_{\tilde{L}}(J'))$ の間に以下の対応がある。J の各零点 $\alpha=(\alpha_1,...,\alpha_s)$ に対して、J' の零点 $\beta=(\beta_1,...,\beta_s)$ が一意的に存在し、各 i について $\beta_i=\alpha_i^{p^{e_i}}$ を満たす。ここで、e_i は非負整数で、α により定まる。

定理 2.9 $L[Z]$ の 0 次元イデアル J に対して、分離閉包 $\mathrm{sc}(J)$ が存在し、一意的に定まる。さらに、J の素因子 P は以下を満たす $\mathrm{sc}(J)$ の素因子 Q に対応する。非負整数 $e_1,\ldots,e_s$ が存在して、P の零点 $(\alpha_1,...,\alpha_s)$ は Q の零点 $(\alpha_1^{p^{e_1}},...,\alpha_s^{p^{e_s}})$ に一意的に対応する。

証明： J の素因子 P に対して、その零点 $\alpha^{(0)}=(\alpha_1^{(0)},\ldots,\alpha_s^{(0)})$ をひとつ取って固定する。このとき、$L[Z]/P\cong L(\alpha_1^{(0)},\ldots,\alpha_s^{(0)})$ である。さて、Z に属する各変数 x_i に対して、x_i の P に関する最小多項式 m_{x_i} を考える。P は極大イデアルであることより、m_{x_i} は既約であり、以下のように一意的に書き直すことができる。

$$m_{x_i}(t)=\mathrm{sc}(m_{x_i})(t^{p^{e_i}})$$

ここで、t を新たな変数とし、$\mathrm{sc}(m_{x_i})$ は m_{x_i} の分離閉包であり、e_i はある非負整数である。(m_{x_i}, e_i は $\alpha^{(0)}$ のとり方に依存しないことに注意する。) 各 $i=1,\ldots,s$ に対して、$\beta_i^{(0)}=(\alpha_i^{(0)})^{p^{e_i}}$ とおくと、$L(\beta_1^{(0)},\ldots,\beta_s^{(0)})$ は L の分離拡大となる。なぜならば、各元 $\beta_i^{(0)}$ は L 上の分離元である。

次に、W_P を以下のように定める。

$W_P=\{(\beta_1,\ldots,\beta_s)\mid P$ のある零点 $\alpha=(\alpha_1,\ldots,\alpha_s)$ が存在して $i=1,\ldots,s$ に対して、$\beta_i=\alpha_i^{p^{e_i}}$ となる。$\}$

P は $L[Z]$ の極大イデアルであったので、$V_{\tilde{L}}(P)$ は $\alpha^{(0)}$ の代数的共役元全体の集合となる。したがって、W_P も $\beta^{(0)}=(\beta_1^{(0)},\ldots,\beta_s^{(0)})$ の代数的共役元全体よりなり、$(\tilde{L})^s$ の中で、すべての L-同型写像に関する最小の不変集合となる。そこで、

$$Q_P=I_{L[Z]}(W_P)=\{f(Z)\in L[Z]\mid f(\beta)=0 \text{ for every } \beta\in W_P\}$$

とおけば、Q_P は $L[Z]$ の素イデアルとなり、$L[Z]/P$ と $L[Z]/Q_P$ に対応する逐次拡大代数拡大 $(\cdots((L(\alpha_1^{(0)})(\alpha_2^{(0)})\cdots)(\alpha_s^{(0)})$ と $(\cdots((L(\beta_1^{(0)})(\beta_2^{(0)})\cdots)(\beta_s^{(0)})$ を考えることにより、$L(\beta_1^{(0)},\ldots,\beta_s^{(0)})\cong L[Z]/Q_P$ が成り立つ。よって、$J'=\cap_{P\in\mathrm{Ass}(J)}Q_P$ は定義 2.8 の条件を満たす。∎

以下、$E=(e_1,\ldots,e_s)$ を P の指数ベクトル と呼ぶ。上の対応は 1 対 1 とは限らない。すなわち、J の異なる素因子が $\mathrm{sc}(J)$ の同じ素因子に対応することがある。この場合、それらは、指数ベクトルによって

区別されることに注意しておく。一方、J が以下のような *special type* と呼ばれる時には、すべての素因子 J は皆同じ指数ベクトルを持ちことが直ちにわかる。従って、対応は 1 対 1 となる。

定義 2.10 J を $L[Z]$ の 0 次元イデアルとする。J が special type であるとは、Z に属するすべての変数 x_i に対して、x_i の J に関する最小多項式 m_{x_i} が既約のときにいう。

例 2.11 例 *2.7* の 2 番目の例では以下の対応がある。

$$\begin{aligned} J =< x^p - z, y^p - z > &\leftrightarrow \mathrm{sc}(J) =< x - z, y - z > \\ V(J) \ni (\sqrt[p]{z}, \sqrt[p]{z}) &\leftrightarrow (z, z) \in V(\mathrm{sc}(J)) \\ P =< x^p - z, x - y > &\leftrightarrow \mathrm{sc}(J) = Q =< x - z, y - z > \end{aligned}$$

ひとたび、分離閉包 $\mathrm{sc}(J)$ が計算されれば、$\mathrm{sc}(J)$ の素因子を一般の位置にある元を利用した分解により求めることができる。そして、これら素因子より J の素因子を計算することができる。

2.4 $\mathrm{sc}(J)$ の構成と Q から P の導出

提案する方法では、J から直接に分離閉包 $\mathrm{sc}(J)$ を計算するわけではない。別の special type のイデアル J_j で、$\sqrt{J} = \cap_{j=1}^{r} \sqrt{J_j}$ となるものを求める。(ここで、各 J_j' を J の中間イデアル と呼ぶことにする。) そして、各 J_j に対して、それらの分離閉包 $\mathrm{sc}(J_j)$ を計算する。

さて、中間イデアル J_j をひとつ取り固定する。簡単のために、それを H で表す。H は $L[Z]$ の 0 次元イデアルで special type である。定義より、Z に属するすべての x_i に対して、x_i の H に関する最小多項式 m_{x_i} は L 上既約となる。したがって、各多項式 m_{x_i} の分離閉包 $\mathrm{sc}(m_{x_i})$ を取れば、$m_{x_i}(t) = \mathrm{sc}(m_{x_i})(t^{q_i})$、ここで $q_i = p^{e_i}$、となる。さらに、*Frobenius map* を以下のように定義する。

$$\phi_E : L[Z] \ni f(x_1, \ldots, x_s) \to f(x_1^{q_1}, \ldots, x_s^{q_s}) \in L[Z],$$

ここで、$E = (e_1, \ldots, e_s)$ とする。この時、$\mathrm{sc}(H)$ は以下により計算できる。

定理 2.12 H の分離閉包 $\mathrm{sc}(H)$ に対して、

$$\mathrm{sc}(H) = \phi_E^{-1}(H) = \{f \in L[Z] \mid \phi_E(f) \in H\}$$

となる。さらに、H の素因子 P と $\mathrm{sc}(H)$ の素因子 Q には 1 対 1 の関係があり、以下を満たす。

$$Q = \mathrm{sc}(P) = \phi_E^{-1}(P)$$

証明： $H' = \phi_E^{-1}(H)$ とおく。$\mathrm{sc}(m_{x_i})(x_i^{q_i}) = m_{x_i}$ は H に属するので、Z に属する各変数 x_i に対して、$\mathrm{sc}(m_{x_i})(x_i)$ は H' に属する。すると、Z に属するすべての変数 x_i に対して、最小多項式 $\mathrm{sc}(m_{x_i})$ が分離的であるので、H' は分離的となる。

一方、$V_{\bar{L}}(H)$ と $V_{\bar{L}}(\phi_E^{-1}(H)) = V_{\bar{L}}(H')$ の間には、1 対 1 関係がある。なぜならば、H の各零点 $\alpha = (\alpha_1, \ldots, \alpha_s)$ に対して、$\beta = (\alpha_1^{q_1}, \ldots, \alpha_s^{q_s})$ は H' の零点となり、逆に、H' の零点 $\beta = (\beta_1, \ldots, \beta_s)$ に対して、$\alpha = (\sqrt[q]{\beta_1}, \ldots, \sqrt[q]{\beta_s})$ は H の零点となるからである。したがって、2.8 の定義より, $H' = \mathrm{sc}(H)$ となる。また、上の零点の対応が $\mathrm{Ass}(H)$ と $\mathrm{Ass}(\mathrm{sc}(H))$ の 1 対 1 の対応を引き起こす。∎

さて、$\mathrm{sc}(H)$ のすべての素因子が求まっているとする。これから, 各素因子に対応する素因子もしくは準素成分を構成することができる。

命題 2.13 Q を $\mathrm{sc}(H)$ の素因子とし、P を対応する H の素因子とする。また、$P_0 = Id(\phi_E(Q))$ とおく。このとき、$\sqrt{P_0} = P$、すなわち P_0 は対応する素因子 P に一致するかそれの準素イデアルである。

証明： P_0 の各零点 $\alpha=(\alpha_1,\ldots,\alpha_s)$ を考える。$P_0=Id(\phi_E(Q))$ であるので、$(\alpha_1^{q_1},\ldots,\alpha_s^{q_s})$ は Q の零点となり、結果として、α は Q に対応する素因子 P の零点である。よって、$V_{\tilde{L}}(P_0)\subset V_{\tilde{L}}(P)$ を得る。一方、P は極大イデアルであるので、$V_{\tilde{L}}(P_0)=V_{\tilde{L}}(P)$ を得、$\sqrt{P_0}=P$ を得る。∎

Frobenius Map 計算: 逆 *Frobenius map* 計算 $\phi_E^{-1}(H)$ と *Frobenius map* 計算 $Id(\phi_E(Q))$ は消去イデアル計算により計算できる。(Chapter 2 [1] を参照。)

逆 *Frobenius map* については、消去順序 $x_i >> y_j$ を導入し、$Id(H\cup\{x_i^{p^{e_i}}-y_i|1\le i\le s\})$ の $L[x_1,\ldots,x_s,y_1,\ldots,y_s]$ の中での Gröbner 基底 G_0 を求める。このとき、(変数 y_i を変数 x_i に置き換えることで、) $G_0\cap L[y_1,\ldots,y_s]$ は $\phi_E^{-1}(H)$ の Gröbner 基底となる。(Proposition 2.5 [9] を参照。)

Frobenius map については、消去順序 $x_i >> y_j$ を導入し、$Id(Q\cup\{y_i^{p^{e_i}}-x_i|1\le i\le s\})$ の $L[x_1,\ldots,x_s,y_1,\ldots,y_s]$ の中での Gröbner 基底 G_1 を求める。このとき、(変数 y_i を変数 x_i に置き換えることで) $G_1\cap L[y_1,\ldots,y_s]$ は $Id(\phi_E(Q))$ の Gröbner 基底となる。これは、ϕ_E が環準同型写像であることから示すことができる。

根基イデアル計算: $J\neq\sqrt{J}$ であるとき、Frobenius map 計算で求めたイデアル P は必ずしも素イデアルとはいえず、準素イデアルのこともある。したがって、その根基 $\sqrt{P}$ を計算する必要がある。しかし、ここでの目的は I の素因子であり、$(\sqrt{P})^c=\sqrt{P}\cap K[X]$ が求めるべき I の素因子であるので、直接 $(\sqrt{P})^c$ を $(\sqrt{P})^c=\sqrt{P^c}=\sqrt{P\cap K[X]}$ を利用して求める。ここで、P^c を P の *contraction* とする。このとき、基礎体 K は $GF(q)$ であるので、松本の方法 *[9]* を使って、根基イデアル $\sqrt{P^c}$ を効率良く求めることができる。松本の方法は、逆 Frobenius map 計算と体の元の p-乗根計算から成っているので、有限体の場合には、極めて効率良いと考えられる。さらに、P は J を含んでいるので、P^c の根基イデアル計算は、J^c の根基イデアル計算より効率良いとも考えられる。

3 素分解計算

ここでは、提案する方法の全体を示す。I をこれから分解する $K[X]$ のイデアルとする。

3.1 0 次元イデアルへの帰着

まず、I から同次元成分を *independent sets modulo* I の計算から抜き出す。(詳細は Chapter 8 [2] を参照。) とくに、Gröbner 基底を使って, *maximal strongly independent set* Y *modulo* $\sqrt{I}$ を計算し、これからイデアル I に対して、$K(Y)[Z]$ における *extension ideal* J を計算する。ここで、$Z=X\setminus Y$ とする。このとき、J の各素因子 P に対して、それに対応する素因子 $P\cap K[X]$ を *contraction* 計算により行う。結果として、次の素分解が得られる。

$$\sqrt{J}=\cap_{i=1}^r\sqrt{Q_i},\ \ \sqrt{I}=\cap_{i=1}^r(\sqrt{Q_i}\cap K[X])\cap\sqrt{I'},$$

ここで、$I'=Id_{K[X]}(I,f)$ であり、多項式 f は J より計算される。I' は I を真に含むので、上の分解を I' に適用して行くことで、有限回の手順で、I のすべての素因子が計算される。計算したいものは、I の素因子であるので、有効な分解 [3, 12] を取り込むことができる。例えば、以下は計算面では多いに有効である。$\sqrt{Id(I,fg)}=\sqrt{Id(I,f)}\cap\sqrt{Id(I,g)}$、$\sqrt{I}=\sqrt{(IR_f\cap R)}\cap\sqrt{Id(I,f)}$.

3.2 中間分解

ここでは、$L[Z]$ の 0 次元イデアル J を考える。ここで、$Y \subset X, L = K(Y)$、$Z = X \setminus Y$ とする。各変数 $x_i \in Z$ に対して、J に関する最小多項式 $m_{x_i}(t)$ を計算する。ここで、分母を払って、最小多項式を変数 t と Y とする K 上の多変数多項式とみなす。次に、最小多項式を K 上で因数分解する。

$$m_{x_i}(t) = \prod_j m_{i,j}(t)^{e_{i,j}}$$

ここで、各 $m_{i,j}$ は K 上既約であり、$K[Y]$ 上既約となる。Gauss の補題より、$m_{i,j}$ は L 上既約にもなる。多項式 $m_{i,j}$ たちを J に加えることで、以下の中間分解が計算できる。ここで、各 J_k は special type である。

$$\sqrt{J} = \cap_{k=1}^{r} \sqrt{J_k},$$

さて、各 i に対して、$\mathcal{F}_i$ を m_{x_i} の K 上の異なるすべての既約因子の集合とし、$n_i = \#\mathcal{F}_i$ とおく。中間イデアルは $Id_{L[Z]}(J, g_1, \ldots, g_s)$、ここで、各 g_i は $\mathcal{F}_i$ の元、という形をしているので、最悪 $n_1 \cdots n_s$ 個の $(g_1, \ldots, g_s)$ の組合せが必要となり、計算効率を悪くする。しかし、その中の多くが不要なもので、$L[Z]$ 全体と一致してしまうので、不要な組合せを排除する効率的な方法があれば、大変有効になる。この方法として、g_i の逐次添加 が有効と思われる。というのは、早い段階で不要な組合せを排除できるからである。

中間分解の逐次的構成:

1. Set $\mathcal{J} = \{J\}$.
2. For $i = 1$ to s, do the following.
   - 2.1. Set $\mathcal{J}_0 = \mathcal{J}$ and $\mathcal{J} = \emptyset$.
   - 2.1. For each H in $\mathcal{J}_0$, do the following.
     - 2.1.1. Take one factor h from $\mathcal{F}_i$.
     - 2.1.2. Compute the Gröbner basis of $Id_{L[Z]}(H, h)$.
     - 2.1.3. If $Id_{L[Z]}(H, h) \neq L[Z]$, then $\mathcal{J} = \mathcal{J} \cup \{Id_{L[Z]}(H, h)\}$.
     - 2.1.4. Go to Step 2.1.1.
3. Return $\mathcal{J}$.

3.3 イデアルの素分解計算

$\mathcal{J}$ を J の中間分解とする。$\mathcal{J}$ の各元 H に対して、その分離閉包 $\mathrm{sc}(H)$ を逆 Frobenius map 計算により計算できる。そして、$\mathrm{sc}(H)$ の素因子より、対応する H の素因子が計算される。(節 2.4 を参照). $\mathrm{sc}(H)$ の素分解については、$\mathrm{sc}(H)$ は $L[Z]$ の分離イデアルであるので、素因子は 一般の位置にある元による分解 により計算できる。

命題 2.6 により、多項式 g が一般の位置にある元かどうかを、その最小多項式 m_g が $\deg(m_g) = \dim_L(L[Z]/\mathrm{sc}(H))$ となるかどうかで判定できる。計算の効率化のために、一般の位置にある元として、1 次式 $g(Z)$ を取ることが望ましい。このために、次を利用する。

補題 3.1 (Theorem 4.2 [13]) $T = s \times \ell \times \dim_L(L[Z]/\mathrm{sc}(H))$ とおく。ここで、$s = \#Z$ であり、$\ell = \#\mathrm{Ass}(\mathrm{sc}(H))$ とする。このとき、もし $\#K > T$ であれば、一般の位置にある元 g として、K 上の Z に関する 1 次式の中から取れる。

補題 3.1 の条件は単に理論的なもので、仮に K が十分な元を持っていなくても、1 次式の中から一般の位置にある元を見付けることは可能である場合が多くあるものと考える。(実際性に関しては、次の論文で議論したい。)

次に、体 K を拡大しなくてはならない場合を考える。拡大した体を K_1 とおく。この場合、イデアルとして $J_1 = K_1 \otimes J$ of $K_1(Y)[Z]$ を考えることになり、一般の位置にある元による分解計算により、J_1 の素因子全体の集合 $\mathcal{P}'$ が計算できる。そして、contraction 計算により、$(J_1)^c$ の素因子全体の集合 $\mathcal{P}_{K_1}$ が得られる。Galois 群 $\mathcal{G} = Galois(K_1/K)$ の作用を考えれば、$\mathcal{P}_{K_1}$ は $\mathcal{G}$-orbit に分けられる。そこで、$P_{K_1,1}, P_{K_1,2}, \ldots, P_{K_1,r}$ がひとつの $\mathcal{G}$-orbit をなすとすれば、$W = V_{\tilde{K}}(P_{K_1,1}) \cup \cdots \cup V_{\tilde{K}}(P_{K_1,r})$ は $\mathcal{P}_{K_1}$ の $\mathcal{G}$ に関する *minimal invariant* 集合となる。(ここで、$\tilde{K} = \tilde{K}_1$ であることに注意しておく。) したがって、J^c の素因子 P がただひとつ存在して、$V_{\tilde{K}}(P) = W$ となる。

そこで、$\mathcal{P}_{K_1}$ の元 P_{K_1} をもう一度考える。K_1 は K の有限次拡大体であったので、K_1 は剰余類環 $K[T]/P_0$ として考えることができる。ここで、T は新しい変数の集合で、P_0 は $K[T]$ の極大イデアルである。P_{K_1} の Gröbner 基底 G_{K_1} を $K[T,X]$ の元と見て、$P' = Id_{K[T,X]}(P_0, G_{K_1})$ とおく。すると、P_{K_1} は $P' \cap K[X]$ を $K_1[X]$ の部分集合として含み、P_{K_1} のすべての $\mathcal{G}$-共役も $P' \cap K[X]$ を含む。この事実より、$P' \cap K[X]$ は J^c の素因子で P_{K_1} に対応することが示される。この素因子は消去順序 $T >> X$ に関する Gröbner 基底計算で求まる。

アルゴリズムの概略: まとめとして、アルゴリズムの概略を示す。(もし、$\#K$ が一般の位置の元を 1 次式から探すのには小さ過ぎる場合には、適当な代数拡大体 K_1 を代わりに使い、後で、正しい素因子を計算する。)

素分解アルゴリズム:

1. Compute the dimension of I and a maximal strongly independent set Y.
   Let $Z = X \setminus Y$ and $L = K(Y)$.
2. Compute the *extension* $J = I^e = IL[Z]$ of I.
   (We compute a Gröbner basis G^e with respect to some efficient ordering, and compute a polynomial f from all leading coefficients of elements of G^e. Then, $I = I^{ec} \cap (I : f^\infty)$, where $I^{ec} = J \cap K[X]$.)
3. Compute prime divisors of J. (Sometimes, we compute primary ideals associated with prime divisors of J.)
   3.1. Compute the minimal polynomial m_{x_i} of x_i w.r.t. J for each x_i in Z.
   3.2. Factorize each m_{x_i} as a polynomial over K.
   3.3. Compute the intermediate decomposition $\mathcal{J}$ by INCREMENTAL SEARCH.
   3.4. For each $J_i \in \mathcal{J}$, compute $\mathrm{sc}(J_i)$ by *inverse Frobenius map computation.*
   3.5. Compute the prime decomposition of $\mathrm{sc}(J_i)$ by *decomposition using generic position*, similarly as in the characteristic 0 case.
   3.6. Compute the prime divisors or its associated primary ideals of J from the prime divisors of $\mathrm{sc}(J_i)$ by *Frobenius map computation.*
4. Compute the prime divisors of I^{ec} from prime divisors or associated primary ideals of J_i's by *contraction* and by *radical ideal computation over K using Matsumoto's algorithm [9].*
5. Unless $(I : f^\infty) = K[X]$, go back to Step 1, where we apply $(I : f^\infty)$ instead of I.

注意 3.2 素因子を計算したいので、$(I : f^\infty)$ の代わりに、$(I : f)$ を使う。また、節 *3.1* で述べた分解を利用すれば、さらに効率的となる。

4 結論

本論文では、有限体上の多項式位イデアルの素分解の具体的なアルゴリズムを与えた。アルゴリズムは有限体上の Gröbner 基底計算をベースとしたいくつかの計算と多項式の因数分解から成っているので、ある程度の実際的な効率性を持っているものと考えている。真の実際性の計算機実験による検証は今後の課題である。実際の検証のためには、当然個々の部分計算や全体の計算の戦略の改良が必要であり、以下に有効であるものや今後の課題と思われるいくつかの改良点をあげる。

- I の素因子計算が目的であるので、有効な部分分解 [3, 12] を適用する。
- 因数分解すべき多項式の次数は大きくなる傾向があるので、効率的な多項式の因数分解が大変重要となる。(実際面の実装における実験 [10] を参考にされたい。) また、小さい体では、体演算の高速化も全体の効率アップに大変有効である。
- 分離的でない場合を扱うために導入した特別な操作は、極めて小さい標数、例えば、$p = 2, 3, 5$ のような場合にのみ有効になると考える。というのは、実際には、$\dim_L(L[Z]/J)$ が大きくなってしまうような J を扱うのは大変困難であるからである。(もし、標数 p がそんなに小さくなければ、計算可能になるイデアルは分離的になってしまい、標数 0 の場合と変わらずに、単に一般の位置にある元による分解を適用すればよいことになる。) したがって、標数の小ささをより一層利用した方法が効率アップに役立つものと考える。
- 項順序の選択は全体の効率に大きく関与する。そこで、実際にどのような項順序が有効かを計算機実験により検証することが大事である。もし、辞書式順序を選んだ場合には、計算全体は結果として、逐次計算法 と本質的に似通ってくる。というのは、計算の意味として、代数拡大を逐次的に行うこと、代数拡大体上での多項式の因数分解を行うことになるからである。

参考文献

[1] Adams, W.W., Loustaunau, P. (1994) *An Introduction to Gröbner Bases.* Graduate Studies in Mathematics **3**, American Mathematical Society.

[2] Becker, T., Weispfenning, V. (1993). *Gröbner Bases.* Springer-Verlag, New York.

[3] Caboara, M., Conti, P., Traverso, C. (1997) Yet another ideal decomposition algorithm. Proceedings of AAECC 12, L.N.C.S. **1255**, Springer, 39-54.

[4] Decker, D., Greuel, G.-M., Pfister, P. (1999) Primary decomposition: algorithms and comparisons. *Algorithmic Algebra and Number Theory*, Springer, 187-220.

[5] Fortuna E., Gianni P., Trager B. (2001) Computation of the radical of polynomial ideals over fields of arbitrary characteristic. Proceedings of ISSAC'01, ACM Press.

[6] Gianni, P., Trager, B. (1996) Square-free algorithms in positive characteristic. *Appl. Alg. in Eng. Comm. and Comp*, **7**, 1-14.

[7] Gianni, P., Trager, B., Zacharias, G. (1988). Gröbner bases and primary decomposition of polynomial ideals. *J. Symb. Comp.* **6**, 149-167.

[8] Kalkbrener, M. (1994) Prime decomposition of Radicals in Polynomial Rings. *J. Symb. Comp.* **18**, 365-372.

[9] Matsumoto R. (2001) Computing the radical of an ideal in positive characteristic. *J. Symb. Comp.* **32**, 263-271.

[10] Noro, M., Yokoyama, K. (2002). Yet another practical implementation of polynomial factorization over finite fields. to appear in the proceedings of ISSAC'02.

[11] Seidenberg, A. (1974) Constructions in algebra. *Trans. Amer. Math. Soc.* **197**, 272-313.

[12] Shimoyama, T., Yokoyama, K. (1996). Localization and primary decomposition of polynomial ideals. *J. Symb. Comp.* **22**, 247-277.

[13] Yokoyama, K., Noro, M., Takeshima, T. (1992). Solution of systems of algebraic equations and linear maps on residue class rings. *J. Symb. Comp.* **14**, 399-417.