数式処理 *J.JSSAC (2005)*
Vol. 11, No. 3,4, pp. 21 - 28

Noda2005 論文

Dynamic Evaluation の実装について

野呂 正行*

神戸大学 理学部

概　要

In Dynamic Evaluation (DE) [1], the defining polynomial of an algebraic number to be newly added to a ring need not be irreducible. Such an extended ring may have zero divisors and we often get stuck when we try to compute the reciprocal of an element or to check that an element is zero or not. In this case the element is a zero divisor, and we can decompose the base ring by using the zero divisor. The existing DE method executes the Euclid algorithm to detect a zero divisor, but it often causes heavy intermediate coefficient swells. In this paper, we formulate the decomposition in terms of an ideal decomposition. Then we show that each component can be computed efficiently by modular computation.

1 Dynamic Evaluation

体 K の有限次代数拡大 L は，さまざまな方法で表現できる．例えば，K が標数 0 の場合，L は常に単拡大 $L = K(\alpha)$ として表現できる．この場合，原始元 α の K 上の最小多項式を $m(x)$ とすれば，$L = K[x]/(m(x))$ となり，L における計算は，右辺の一変数多項式環の剰余環における演算として実現できる．しかし，K 上代数的な元 α_i $(i = 1, 2, \ldots)$ を順次添加していく場合，原始元 α の K 上の最小多項式 $m(x)$ の係数は一般に増大し，それは $K[x]/(m(x))$ の計算の効（低下を招く．かわりに，$K_0 = K, K_i = K_{i-1}(\alpha_i)$ $(i = 1, 2, \ldots)$ で，α_i を $f_i(x) \in K_{i-1}[x]$ の根として与えるのが現実的である．この場合，$f_i(x)$ が K_{i-1} 上既約なら α_i は共役を除いて一意に定まるが，多項式の既約性判定あるいは既約因子分解は一般にコストが高く，多数の代数的数が添加される場合にはやはり現実的でない．Duval [1][2] による Dynamic Evaluation (DE) は，f_i に対し，無平方性のみを要求する．より正確には，

$$K_i = K[x_1, \ldots, x_i]/I, I = \langle f_1(x_1), f_2(x_1, x_2), \ldots, f_i(x_1, \ldots, x_i)\rangle$$

とし，I が 0 次元根基イデアルである場合を考える．この場合，$I = \cap_k P_k$ (P_k : 極大イデアル）と素因子分解すれば，

$$K_i = \oplus_k F_k, F_k = K[x_1, \ldots, x_i]/P_k$$

*noro@math.kobe-u.ac.jp

が成り立つ．すなわち，K_i は体 F_k の直和となる．各直和成分は，$f_1, \ldots, f_i$ のいずれかの根を K に添加した体を表しており，K_i を考えることは，これらをすべてまとめて扱っていることになる．こうしても，環演算については正しい結果を与える．問題は，K_i における逆元計算および零判定である．I が極大イデアルでない場合，K_i に零因子が存在する．a が零因子ならば，a の逆元は K_i においては存在しない．しかし，a が F_k において 0 でなければ F_k において逆元が存在する．よって，$Q_1 = \cap_{a \notin P_k} P_k$, $Q_2 = \cap_{a \in P_k} P_k$ とすれば，$K[x_1, \ldots, x_i]/Q_1$ において a の逆元が存在する．Q_1, Q_2 が因数分解を使わずに GCD 計算でできるというのが，DE のキーポイントである．すなわち，零因子が現れた時点で，GCD 計算により係数 '体'（実際には体の直和）を分解できるのである．

ここで，GCD に関していくつか注意が必要である．例えば，$a = a(x_1, \ldots, x_i)$ と $f_i(x_1, \ldots, x_i)$ から $K_{i-1}[x_i]$ における互除法を行う場合，K_{i-1} は体とは限らないため，K_{i-1} による除算が不可能になる場合がある．この場合には，K_{i-1} に零因子が見つかったことになり，この零因子を使って K_{i-1} を分解する．このような操作は一般に再帰的に必要となる可能性がある．また，よく知られているように，互除法は係数膨張を起こしやすい．このため，subresultant 法を始めとする種々の方法が考案されているが，代数体においては，modular 計算による方法が効率よい．以下で，DE を modular 計算により行う方法について述べる．

2 準備

2.1 零因子による分解

K を体，$R = K[x_1, \ldots, x_n]$ とし，$I \subset R$ を 0 次元根基イデアルとする．P_i $(i = 1, \ldots, m)$ を I の素因子とする．すなわち P_i は $I \subset P_i$ を満たす R の極大イデアルで，$I = \cap_{i=1}^{m} P_i$ が成り立つとする．このとき，

$$R/I = \oplus_{i=1}^{m} F_i, \quad F_i = R/P_i \tag{1}$$

が成り立つ．すなわち，R/I は体 F_i の直和である．$\pi : R \to R/I$，$\pi_i : R \to R/P_i$ を標準的射影とする．

命題 1

$f \in R$ とし，$A = \{i \mid f \in P_i\}$, $B = \{i \mid f \notin P_i\}$ とおけば，次が成り立つ．

1. $I : f = \cap_{i \in B} P_i$.
2. $I + \langle f \rangle = \cap_{i \in A} P_i$.
3. $I = (I + \langle f \rangle) \cap (I : f)$.
4. f は $R/(I : f)$ の単元である．

証明　(1) より，

$$g \in I : f \Leftrightarrow gf \in I \Leftrightarrow \pi_i(gf) = 0 \quad (i = 1, \ldots, m) \tag{2}$$

が成り立つ．定義により，$i \in A$ ならば $\pi_i(f) = 0$，また $i \in B$ ならば $\pi_i(f)$ は可逆である．よって，

$$(2) \Leftrightarrow \pi_i(g) = 0 \quad (i \in B) \Leftrightarrow g \in \cap_{f \notin P_i} P_i \tag{3}$$

より 1. が成り立つ． また，$f \in \cap_{i\in A} P_i, I \subset \cap_{i\in A} P_i$ より $g \in I + \langle f \rangle$ ならば $g \in \cap_{i\in A} P_i$． 逆に，$g \in \cap_{i\in A} P_i$ ならば，$h_i = 0\ (i \in A)$，$h_i = \pi_i(f)^{-1}\pi_i(g)\ (i \in B)$ とおき，$\pi_i(h) = h_i$ となる $h \in R$ をとると，$\pi_i(hf) = \pi_i(g) = 0\ (i \in A), \pi_i(hf) = \pi_i(g)\ (i \in B)$ より $\pi(hf) = \pi(g)$． すなわち $g \in I + \langle f \rangle$. よって， 2. が成り立つ．1.， 2. より 3. は明らかである． 4. も定義より明らか． ∎

2.2 イデアル商の線形方程式による計算

同型（1）のもとで，f が R/I の単元であることと，$I : f = I$ であることは同値である． よって， f の R/I における逆元計算に失敗した場合， $I : f, I + \langle f \rangle$ を求めることにより， R/I の自明でない分解が得られる． 実際には， 逆元計算と $I : f$ の計算は同時に行うことができる．以下， 多項式 f における， 項順序に関して最大の項を $\mathrm{HT}(f)$， 多項式 f の，グレブナー基底 G に関する正規形を $\mathrm{NF}_G(f)$ と書く．

命題 2

$<$ を R の項順序とし，G を 0 次元イデアル I の $<$ に関するグレブナー基底とする．S を G に関する標準単項式集合，すなわち G のどの元の頭項でも割り切れない，係数 1 の単項式の集合とし，$H = \{g \in \mathrm{Span}_K(S) \,|\, \mathrm{NF}_G(fg) \in K\}$ とおく．もし $\mathrm{NF}_G(fH) \neq \{0\}$ ならば $g_0 \in H$ で $\mathrm{NF}(fg_0) = 1$ なるものが存在する．このとき g_0 は f の逆元である．もし $\mathrm{NF}_G(fH) = \{0\}$ ならば有限次元 K-線形空間 H の K-基底 $G_H = \{g_1, \ldots, g_m\}$ を， $\mathrm{HT}(g_i)$ が全て異なるようにとれば， $G \cup G_H$ が $I : f$ のグレブナー基底となる．

証明　$\mathrm{NF}_G(fH) = \{0\}$ とすれば，$H = \{g \in \mathrm{Span}_K(S) \,|\, \mathrm{NF}_G(fg) = 0\}$ より $I : f = I + \langle H \rangle$ が成り立つ．$g \in I : f$ とする． $\mathrm{HT}(g)$ が， $\mathrm{HT}(G \cup G_H)$ のいずれかで割り切れることをいう．$g' = \mathrm{NF}_G(g)$ とすると， $g' \in \mathrm{Span}_K(S)$ かつ $g' \in I : f$ より $g' \in H$ である．$\mathrm{HT}(g)$ がどの $\mathrm{HT}(h)$ $(h \in G)$ でも割り切れなければ，$\mathrm{HT}(g) = \mathrm{HT}(g')$ が成り立つ．$g' \in H$ より g' は G_H の K-線形結合で書けるが，仮定より $\mathrm{HT}(g')$ はいずれかの $HT(g_i)$ と一致する． よって， $G \cup G_H$ は $I : f$ のグレブナー基底である． ∎

H は以下のように線形方程式系の求解により計算できる．$f \in R$ とする． $a_s\ (s \in S), a$ を未定係数とし，$g = \sum_{s\in S} a_s s$ とおく．$\mathrm{NF}_G(fg - a \cdot 1) = \sum_{s\in S} a_s \mathrm{NF}_G(fs) - a \cdot 1 = \sum_{s\in S} l_s s$ とすれば， l_s は a_s， a の線形形式となる． 線形方程式系 $l_s = 0 (s \in S)$ の解で， $a \neq 0$ なるものがあれば， f は R/I の単元で， その解から f の逆元が求まる． また， 解において常に $a = 0$ ならば，f は逆元を持たないことがわかり，その解は $fg \in I$ となる $g \bmod I$ をすべて与える． すなわち $\{g \bmod I \,|\, g \in I : f\}$ が求まる．この場合，解はいくつかの多項式 $G_H = \{g_1, \ldots, g_m\}$ により，$g = \sum_{i=1}^{m} c_i g_i$ （c_i は任意定数） として与えられる． この g_i を， 頭項が相異なるように選べば $G \cup G_H$ が $I : f$ のグレブナー基底を与える．

2.3 分解成分の modular 計算

f が単元でない場合， $I = (I + \langle f \rangle) \cap (I : f)$ となる．これらの分解成分を用いて計算を続行する場合， それぞれのイデアルのグレブナー基底が必要となる． $I : f$ については既にグレブナー基底が得られている．$I + \langle f \rangle$ のグレブナー基底計算は一種の GCD 計算と考えてよいが，互除法

あるいは Buchberger アルゴリズムいずれを用いても，Q 上の場合，係数膨張などにより計算が困難になる場合がある．これを避けるため，modular 計算を応用することを考える．まず，次の補題は明らかである．

補題 3
I を 0 次元イデアル，J を $I \subset J$ なるイデアルとすると，J も 0 次元イデアルで，$\dim_K R/I \geq \dim_K R/J$ が成り立つ．さらに，$I = J$ と $\dim_K R/I = \dim_K R/J$ は同値．

命題 4
I を 0 次元根基イデアル，$f \in R$ とする．$I + \langle f \rangle \subset I'$ なるイデアル I' に対し，$\dim_K R/I = \dim_K R/I' + \dim_K R/(I : f)$ ならば，$I' = I + \langle f \rangle$.

証明　分解 (1) および命題 1 より，$\dim_K R/I = \dim_K R/(I + \langle f \rangle) + \dim_K R/(I : f)$ が成り立つから，$\dim_K R/I' = \dim_K R/(I + \langle f \rangle)$, が成り立つ．よって前補題により $I' = I + \langle f \rangle$. ∎

一般に，$\mathbf{Q}$ 上のイデアル $I = \langle f_1, \ldots, f_l \rangle$ のグレブナー基底候補を次の方法により求めることができる．

アルゴリズム 5
$H \leftarrow \emptyset$
loop
　$p \leftarrow$ 未使用の素数
　$G_p \leftarrow I_p = \langle f_1 \bmod p, \ldots, f_l \bmod p \rangle$ の簡約グレブナー基底
　$H_p \leftarrow G_p$ の頭項集合
　if $H = \emptyset$ or $H \neq H_p$ then $H \leftarrow H_p, G \leftarrow G_p$
　else $G \leftarrow G$ と G_p を中国剰余定理で結合
　$G_Q \leftarrow G$ の係数を整数-有理数変換
　if G_Q がグレブナー基底 and $I \subset \langle G_Q \rangle$ then return G_Q
end loop

アルゴリズム 5 において，$I \subset \langle G_Q \rangle$ は，$f_1, \ldots, f_l$ を G_Q により簡約することでチェックできる．この方法で求まるのは $I \subset I'$ なるイデアル I' のグレブナー基底であり，$I = I'$ を示すのは一般には困難である．しかし，I が 0 次元で $I = (I + \langle f \rangle) \cap (I : f)$ なる分解成分のグレブナー基底の計算においては，$I + \langle f \rangle$ のグレブナー基底候補を上の方法で計算し，命題 4 の条件をチェックすることで得られた候補が正しいことを示すことができる．実際には，素数 p として，$I + \langle f \rangle$ の $\bmod p$ でのグレブナー基底から求めた線形次元が $\dim_K R/I - \dim_K R/(I : f)$ に等しいもののみを中国剰余定理のデータとして使うのがよいであろう．

2.4　三角形式でないグレブナー基底による分解

通常，イデアル I の生成元は，三角形式，すなわち $g_i(x_1, \ldots, x_i) = x_i^{m_i} + \cdots$ という形で与えられる，しかし，零因子による分解の途中で，この形をもたない多項式が，グレブナー基底の元として現われる可能性がある．この場合，係数環の分解が得られる．

命題 6

I を 0 次元根基イデアルとし，G を $x_n > x_{n-1} > \cdots > x_1$ なる辞書式順序 $<$ に関する I の簡約グレブナー基底とする．ある $g \in G$ が

$$g(x_1, \ldots, x_k, x_{k+1}) = c(x_1, \ldots, x_k)x_{k+1}^m + \{x_{k+1}\text{について } m-1 \text{ 次以下の項}\}$$

と書け，c が定数でなければ，c は R_k/I_k （$R_k = [x_1, \ldots, x_k], I_k = I \cap R_k$） の零因子.

証明　仮定より I_k は R_k の 0 次元根基イデアルである．よって，もし $c \in R_k$ が零因子でなければ R_k/I_k の単元となる．すなわち，ある $d \in R_k, f \in I_k$ が存在して $cd = 1 + f$．このとき，$g = cx_{k+1}^m +$ 低次項 とすれば $dg = (1 + f)x_{k+1}^m +$ 低次項 より $x_{k+1}^m +$ 低次項 $\in I$．よって，ある $g' = x_{k+1}^{m'} +$ 低次項 $\in G$ が存在して $\mathrm{HT}(g') \mid x_{k+1}^m \mid \mathrm{HT}(g)$．$G$ が簡約グレブナー基底だから $g = g'$ となるが，これは c が定数でないことに反する． ∎

I_k のグレブナー基底は $G \cap R_k$ で与えられるから，この命題を繰り返し適用することで，$I = \cap I_i$ かつ I_i のグレブナー基底 G_i が全て三角形式となるように分解できる．

3 実装

3.1 定義多項式からの根基イデアルの構成

前節の方法を適用するためには，K の逐次代数拡大 $K_k = K(\alpha_1, \ldots, \alpha_k)$ を表現する 0 次元根基イデアル I_k およびそのグレブナー基底 G_k が必要となる．実際には，根を添加していく途中で分解する可能性があるため，0 次元根基イデアルの木を構成していくことになる．これは次のように，やはり前節の方法を応用しながら帰納的に実行することができる．

1. $k = 1$ の場合
   α_1 は $f_1(x_1) \in K[x_1]$ の根として与えられる．$f_1(x_1)$ の無平方因子を $g_1(x_1)$ とし，$I_1 = \langle g_1 \rangle$ とすれば，$G_1 = \{g_1\}$.
2. $I_{k-1} = \langle G_{k-1} \rangle$ まで構成できたとする．
   α_k が $f_k(x_1, \ldots, x_k) \in K[x_1, \ldots, x_k]$ により，$f_k(\alpha_1, \ldots, \alpha_{k-1}, x_k)$ の根として与えられているとする．$f_k \in K[x_1, \ldots, x_{k-1}][x_k]$ と見て，$f_k(x_1, \ldots, x_k) = c(x_1, \ldots, x_{k-1})x_k^m + \cdots$ とする．
   (a) c が $K[x_1, \ldots, x_{k-1}]/I_{k-1}$ の単元の場合
   $c^{-1}f_k$ をあらためて f_k とすることで，f_k をモニックにできる．このとき，$G = G_{k-1} \cup \{f_k\}$ はグレブナー基底だから，$K[x_1, \ldots, x_k]/\langle G \rangle$ における x_k の最小多項式 $m(x_k) \in K[x_k]$ が計算できる．もし，$m(x_k)$ が無平方なら $G_k = G, K_k = \langle G_k \rangle$ とすればよい．もし $m(x_k)$ が無平方でなければ $m(x_k)$ の無平方因子 $m_{sqfr}(x_k)$ を求め，$I_k = \langle G \cup \{m_{sqfr}\} \rangle$ とし，そのグレブナー基底を G_k とする．
   (b) c が $K[x_1, \ldots, x_{k-1}]/I_{k-1}$ の単元でない場合
   c は $K[x_1, \ldots, x_{k-1}]/I_{k-1}$ の零因子なので，$I_{k-1} = (I_{k-1} + \langle c \rangle) \cap (I_{k-1} : c)$ と分解できる．$I_{k-1} + \langle c \rangle$ 上では f_k の主係数 c が消えるので，その f_k について同様の手順を繰り返す.
   $I_{k-1} : c$ 上では c が単元なので，前項と同様の操作を行う.

この操作の中で，2-(a) の $\langle G \cup \{m_{sqfr}\}\rangle$ のグレブナー基底の計算は現状では中国剰余定理による計算が適用できない．したがって通常の Buchberger アルゴリズムで計算する必要がある．

3.2 modular dynamic evaluation

$R = K[x_1, \ldots, x_k]$ の 0 次元根基イデアル I およびそのグレブナー基底 G が与えられているとする．$f \in R$ の R/I における可逆性が不明の場合，前節の方法により，a を未知列ベクトルとするある斉次線形方程式系 $Aa = 0$ の求解により，可逆性の判定および，可逆でない場合の $I : f$ のグレブナー基底の計算が行える．$Aa = 0$ の求解も modular 計算により行うことができる．

1. 適当な素数 p を選び，$A \bmod p$ を簡約化する．
2. 行列 A'，B' を次のように選ぶ:
   (a) 1. で得た簡約行列の主成分，すなわち簡約化に用いたピボットがある行，列を A から取り出し A' とする．$\det(A') \bmod p \neq 0$ より $\det(A') \neq 0$ である．
   (b) A の，A' を選んだ残りの列を集め，A' で選ばれた行を取り出したものを B' とする．
3. $Aa = 0$ の解は，$[A' \mid B']a' = 0$ を満たす（a' は a の要素をしかるべく入れ換えたもの）．この解は $[E \mid A'^{-1}B']a' = 0$ により求まる．
4. 3. で得た解が $Aa = 0$ を満たせば解が得られたことになる．さもなくば，1. に戻る．

3. の求解は，Hensel 構成または中国剰余定理と，整数-有理数変換により計算できる [3][4]．いずれの方法を選ぶかは，$\dim \mathrm{Ker}(A)$ に依存する．f が単元の場合，$\dim \mathrm{Ker}(A) = 1$ となる．少なくともこの場合は Hensel 構成が有利であろう．

A の各列は，前節の記号を用いれば $\mathrm{NF}_G(fs)$ $(s \in S)$ および -1 を表している．A の掃き出しを左から右に行う場合，簡約形からただちに $I : f$ のグレブナー基底を得るために，$S = \{s_1, \ldots, s_m\}$ $(m = \dim_K R/I,\ s_1 < s_2 < \cdots < s_m)$ とし，$\mathrm{NF}_G(fs_i)$ を左から順にならべ，最も右に -1 を置くのがよい．この場合，線形方程式の最も右の変数が，解におけるパラメタになっていれば，f は単元で，それを 1 とおいた解が f^{-1} を表す．そうでない場合，f は零因子であり，$(I : f) \bmod I$ の K-基底 $\{g_1, \ldots\}$ を得る．これらのうち，$\mathrm{HT}(g_i)$ が他の $\mathrm{HT}(g_j)$ で割り切れるものを除いたものを G に添加したものが $I : f$ のグレブナー基底となる．これにより $\dim_K R/(I : f)$ が分かるから，$I + \langle f\rangle$ のグレブナー基底は前節の中国剰余定理による方法で計算できる．この後，必要があれば，f の $R/(I : f)$ における逆元を計算すればよい．また，分解後のイデアルが三角形式になっていなければ，それを用いてさらにイデアルを分解することができる．

4 実行例

以下で，計算時間は Pentium M 1.3GHz （メモリ 1GB） 上でのものである．

$$g_1 = x^9 - 4x^8 - 30x^7 + 142x^6 + 79x^5 - 680x^4 - 247x^3 + 998x^2 + 716x + 104$$

とし，$g_1(\alpha_1) = 0$ とする．α_2, α_3 を

$$g_2(\alpha_1, x_2) = g_1(x_2)/(x_2 - \alpha_1), \quad g_2(\alpha_1, \alpha_2) = 0$$

$$g_3(\alpha_1, \alpha_2, x_3) = g_2(\alpha_1, x_3)/(x_3 - \alpha_2), \quad g_3(\alpha_1, \alpha_2, \alpha_3) = 0$$

を満たすものとする． $R = \mathbf{Q}[x_1, x_2, x_3]$ として，$G = \{g_1(x_1), g_2(x_1, x_2), g_3(x_1, x_2, x_3)\}$, $I = \langle G \rangle$ とおけば， G は I の $x_3 > x_2 > x_1$ なる辞書式順序に関するグレブナー基底であり， I は 0 次元根基イデアルである． $g_1(x)$ は $\mathbf{Q}$ 上既約だが，$g_2(\alpha_1, x)$, $g_3(\alpha_1, \alpha_2, x)$ は可約のため， R/I は零因子をもつ． 既に知られている $g_3(\alpha_1, \alpha_2, x)$ の 2 次の因子 $f(\alpha_1, \alpha_2, x)$ から，

$$F(x_1, x_2, x_3) = \mathrm{NF}_G((x_1^{10} + x_2^{10} + x_3^{10} + 1) f(x_1, x_2, x_3))$$

とすれば， $F(\alpha_1, \alpha_2, \alpha_3)$ は零因子となるはずである．($x_1^{10} + x_2^{10} + x_3^{10} + 1$ は， 計算を複雑化するための因子である．）この F を用いて I の分解を行ってみる．

1. $I : F$ の計算
   まず， $(I : F)$ mod I の $\mathbf{Q}$-基底の計算を前節の modular 計算を用いて行うと， 70 秒で x_3 の 5 次式 $g(x_1, x_2, x_3) = c(x_1, x_2)x_3^5 + \cdots$ が得られる．$c(x_1, x_2)$ が定数でないため， これも零因子である．$I : c$ の計算を行ってみると， 0.3 秒で x_2 の 3 次式 $h(x_1, x_2)$ が得られる． これは x_2^3 の係数が定数のため， これで三角形式のグレブナー基底が得られる． この 3 次式は， 実際に $g_2(\alpha_1, x_2)$ の既約因子であることが確かめられる．
   一方で， $I : f = (I \cap \langle f \rangle)/f$ より， $I \cap \langle f \rangle$ を計算すれば $I : f$ が計算できる． これは $I \cap \langle f \rangle = ((1 - t)I + t\langle f \rangle) \cap R$ により計算できるが， これを Buchberger アルゴリズム（例えば斉次化 trace アルゴリズム） で計算しても， 5 時間たっても終らない．
2. $I + \langle f \rangle$ の計算
   $\dim_{\mathbf{Q}} R/I = 504$, $\dim_{\mathbf{Q}} R/(I : F) = 450$ なので, $\dim_{\mathbf{Q}} R/(I + \langle f \rangle) = 54$ が分かる． modular 計算により $I + \langle f \rangle \subset I'$ なるイデアル I' のグレブナー基底が 3 秒ほどで計算できるが, $\dim_{\mathbf{Q}} R/I' = 54$ なので， $I' = I + \langle f \rangle$ が分かる． こちらも， Buchberger アルゴリズムで 2000 秒かかる．

5 まとめ

これまで提案されている DE の計算法は，単に零因子 f と代数的数の定義多項式の GCD 計算の過程でイデアルが分解されていく， というものであったが， 代数体上の GCD を互除法で計算すると， 係数膨張が特にひどく， 途中で計算不能に陥ることが多い． このような困難を回避するために，modular 計算法がいくつか提案されている．ここで述べた方法の原型は， 代数体上の GCD の modular 計算 [5] [6] である． これらの場合， 係数環が体であることが modular 計算の正当性を保証するが， 係数環の定義イデアルの条件を根基イデアルにまで緩めることで, modular 計算をする上での困難が生ずる． ここでは零因子 f に対し， $I : f$ および $I + \langle f \rangle$ をまとめて考え， 線形次元による制約を与えることで， $I + \langle f \rangle$ のグレブナー基底候補が実際に求めるものであることを示すことができた．

逆元計算， あるいは $I : f$, $I + \langle f \rangle$ の計算は GCD 計算の一種であり，係数を考えなければその手間は $d = \dim_K R/I$ とすれば $O(d^2)$ 程度のはずである．一方で，線形方程式による計算は $O(d^3)$ となる．実際， 結果の係数がそれほど大きくない場合には， 通常の互除法あるいは Buchberger

アルゴリズムによる計算のほうが高速な場合もある．線形方程式求解において，Hensel 構成を用いれば，$O(d^3)$ の部分は $\bmod p$ での逆行列（LU 分解）計算に限定されるので，結果の係数が大きい場合には，結果の係数のビット長を M として Hensel 構成の $O(Md^2)$ が支配的になると期待できる．（実際には，整数-有理数変換の頻度が影響する．）前節の例で見たように，Buchberger アルゴリズムの適用が困難な例は容易につくることができる． このような場合にも， 本論文で述べた方法は安定して結果を出せるという点で有用であると考える．

参 考 文 献

[1] J. Della Dora, C. Discrescenso, D. Duval (1985). About a new method for computing in algebraic number fields, In Proc. Eurocal'85 (LNCS 204), Springer-Verlag, 289-290.

[2] D. Duval (1994). Algebraic Numbers: An Example of Dynamic Evaluation. J. Symb. Comp. 18, 429-445.

[3] J. C. Faugère (1999). A new efficient algorithm for computing Groebner bases (F_4). Journal of Pure and Applied Algebra (139) 1-3, 61-88.

[4] 野呂 正行, 横山 和弘 (2003)． グレブナー基底の計算 基礎篇．東京大学出版会.

[5] 野呂 正行 (1995) 逐次代数拡大体上での 1 変数多項式の GCD について．京大数理研講究録 920, 1-8.

[6] M. v. Hoeij, M. Monagan (2002). A modular GCD algorithm over Number Fields presented with Multiple Extensions. In Proc. ISSAC2002, ACM Press, 297-304.