数理解析研究所講究録
第 848 巻 1993 年 17-26

零因子をもつ環上の逆行列計算について

富士通国際研　竹島 卓 (Taku TAKESHIMA)[1)]
〃　横山 和弘 (Kazuhiro YOKOYAMA)[2)]

Abstract. ここでは、整域でない環、すなわち零因子を持つ環を成分とする行列の行列式・逆行列や線形方程式の解法について述べる。具体的には、整域でない環がよく知られた整域 (整数環・多項式環) の剰余環として与えられた場合について、いくつかの算法を与えている。

1. 整域上の行列演算と剰余環上の行列演算

$\mathcal{D}$ を整域とし、$\mathcal{Q}$ をその商体とする。ここでは整域でない環 $\mathcal{R}$ として、整域 $\mathcal{D}$ を素でないイデアル $\mathcal{I}$ で割った剰余環を考える。$\mathcal{R}$ の例として、よく数式処理で扱われるものを挙げる。

(i) 整数環 $\mathbb{Z}$ を素数でない整数 m で生成されるイデアル $< m >= m\mathbb{Z}$ で割った剰余環 $\mathbb{Z}/m\mathbb{Z}$

(ii) 一変数多項式環 $\mathbb{Q}[x]$ を既約でない多項式 $f(x)$ で生成されるイデアル $< f(x) >$ で割った剰余環 $\mathbb{Q}[x]/ < f(x) >$

(iii) 多変数多項式環 $\mathbb{Q}[x_1, ..., x_n]$ を素でないイデアル $\mathcal{I}$ で割った剰余環 $\mathbb{Q}[x_1, ..., x_n]/\mathcal{I}$、ここで素でないイデアルはいくつかの多項式 $f_1, ..., f_r$ で生成されている。

(i) と (ii) は（もとの整域が）単項イデアル環であり、(iii) は（もとの整域が）一意分解整域であるが、単項イデアル環ではない。

剰余環上の行列とその演算を扱うためには剰余環で四則演算が実行できなければならない。剰余環の四則演算自体は、一般にはもとの整域の四則演算から与えられる。そこで、「剰余環の元が一意的に表される」または、「剰余環の元の零判定ができる」ということが必要である。この一意表現は、もとの整域の元を用いて対応する剰余環の元を表すことであり、これによりもとの整域から剰余環への射影 p が表現できる。すなわち、

$$p : \mathcal{D} \in a \ \rightarrow p(a) \in \mathcal{R} = \mathcal{D}/\mathcal{I}$$

の p が計算可能であることが必要であり、$\mathcal{R}$ 上の演算はこの p により、

[1)] tak@iias.flab.fujitsu.co.jp
[2)] momoko@iias.flab.fujitsu.co.jp

$$p(a)+p(b)=p(a+b),\ \ p(a)\times p(b)=p(a\times b)$$

で与えられる。例の (i) と (ii) については、イデアルの生成元で割った余りで一意表現が与えられ、さらに一般化された (iii) については、イデアルの Gröbner 基底を用いた正規形 (normal form) で与えられる。(Buchberger, 1985, 1987 参照)

行列とその演算を考えよう。$\mathcal{D}$ 上の行列全体を $M(\mathcal{D})$ とおき、剰余環 $\mathcal{R}$ 上の行列全体を $M(\mathcal{R})$ とする。このとき、射影 p を自然に拡張することにより、$M(\mathcal{D})$ から $M(\mathcal{R})$ への全射準同型が得られる。これも同じ記号 p を使う。すなわち、$M=(m_{i,j})\in M(\mathcal{D})$ に対して、$p(M)=(p(m_{i,j}))$ となる。したがって、正方行列 $M=(m_{i,j})\in M(\mathcal{D})$ に対して、

$$\det(p(M))=p(\det(M))$$

であり、もし M の逆行列 M^{-1} が $M(\mathcal{D})$ 内に存在すれば、$p(M)$ の逆行列が $M(\mathcal{R})$ 内に存在し、

$$p(M)^{-1}=p(M^{-1})$$

となる。M の逆行列が $M(\mathcal{D})$ 内に存在しない場合でも、$\det(M)\neq 0$ であれば逆行列 M^{-1} が $M(\mathcal{Q})$ 内に存在し、さらに 分母を払った $\det(M)M^{-1}$ は $M(\mathcal{D})$ の元である。このことから次がいえる。(証明は易しい。)

性質 1　$p(M)$ が $M(\mathcal{R})$ 内で逆行列を持つための必要十分条件は、

$$p(\det(M))=\det(p(M))$$

が $\mathcal{R}$ 上逆元を持つことである。

注意：整域でない環 $\mathcal{R}$ 上の行列 $p(M)$ に対してその逆行列は、存在すれば一意的であることが逆元の一意性同様に容易に示される。このことより、もとの整域 $\mathcal{D}$ 上での $p(M)$ の逆像 M の逆行列 M^{-1} の射影 が $p(M)$ の唯一の逆行列 $p(M)^{-1}$ である。

したがって、原理的には、$\mathcal{Q}$ 上の行列演算があれば $\mathcal{R}$ 上の行列演算ができるということになる。さらに、M の行列式や逆行列を求める方法として、division free (Kaltofen, 1992) や fraction free 掃き出し法 (Sasaki& Murao, 1982, または佐々木, 1981 参照) 小行列式法 (佐々木 1981 参照) といったなるべく整域 $\mathcal{D}$ の上の演算のみで求める方法が数多く研究され、いくつかの算法が提案され、効率的であると主張されている。また、連分数展開と関係付けられる linear recurrence を用いて、確率的ではあるが効率的な算法 (Wiedemann, 1986, Kaltofen& Saunders, 1991) も提案されている。連分数展開と linear recurrence は coding theory における Berlekamp-Massey の算法に帰着され、これらは ある種の extended GCD 算法と同じである点で大変興味深い。(Berlekamp, 1968, Mills, 1975, Dornstetter, 1987)

このような効率的算法があるような $\mathcal{Q}$ や $\mathcal{D}$ の行列が対象である場合で、M が（$\mathcal{Q}$ のみならず）$\mathcal{D}$ 上でも逆行列を持つ時には、$\mathcal{D}$ 上で求めてから射影をとり、$\mathcal{R}$ へ写すという方法は有効といえる。

しかし、場合によっては直接 $\mathcal{D}$ 上の計算をすることは、剰余環上の計算の有利さがなくなってしまうことがある。というのは、剰余環ではいつでも一定の縮約された形になっているので、中間式の膨張（整数は桁、多項式・有理式なら次数）と計算における通分が抑制されるからである。また、整域上の逆行列や行列式の計算にモジュラー法を使う試みがあること (佐々木, 1981, Krishnamurthy, 1985 参照）からも「剰余環の性質をうまく利用した計算」が重要かつ効率化への鍵と考えられる。

2. 剰余環の分解による方法

剰余環 $\mathcal{R}$ を定義するイデアル $\mathcal{I}$ の分解が剰余環の分解を与える時がある。このような場合には、各々の成分（環）における計算を利用して、$\mathcal{R}$ 上の計算を行なう方法がある。

2.1. 準素イデアル分解と中国剰余定理

$\mathcal{I}$ が準素イデアル分解され（$\mathcal{D}$ が Noether 環ならばいつでも可能である）、さらに2つの異なる準素成分が $\mathcal{D}$ を生成する時には、中国剰余定理により剰余環自体もさらに「小さな環」に分解される。（一般の多項式環のイデアルの準素イデアル分解に関しては、Gianni et al.,1988 や Buchberger, 1985, 1987, を参照されたい。）

いま、$\mathcal{I}$ が以下のように無駄なく準素イデアル分解されたとする。

$$\mathcal{I} = \mathcal{I}_1 \cap \cdots \cap \mathcal{I}_r.$$

ここで、$\mathcal{I}_i, i = 1, ..., r$ は準素イデアルとし、異なる i, j に対して、$< \mathcal{I}_i, \mathcal{I}_j >= \mathcal{D}$ とする。このとき、

$$\mathcal{R} = (\mathcal{D}/\mathcal{I}_1) \bigoplus \cdots \bigoplus (\mathcal{D}/\mathcal{I}_r) = \mathcal{R}_1 \bigoplus \cdots \bigoplus \mathcal{R}_r$$

と分解される。ここで、$\mathcal{D}/\mathcal{I}_i$ を $\mathcal{R}_i$ とおいた。$\mathcal{D}$ から $\mathcal{R}_i$ への射影を p_i とおけば、$\mathcal{D}$ から $\mathcal{R}$ への射影 p は上の同型より

$$p = p_1 \bigoplus \cdots \bigoplus p_r$$

と書ける。以上が成り立つ時、環 $\mathcal{R}$ において中国剰余定理が成り立つということにする。この射影は自然に行列の射影に拡張できる。すなわち、行列 $M \in M(\mathcal{D})$ に対して、

$$\begin{aligned} \det(p(M)) &= p(\det(M)) \\ &= p_1(\det(M)) \bigoplus \cdots \bigoplus p_r(\det(M)) \\ &= \det(p_1(M)) \bigoplus \cdots \bigoplus \det(p_r(M)) \end{aligned}$$

となる。ここで、行列環の射影も同じ記号を使うものとする。よって、次を得る。

性質 2　$p(M)$ が $M(\mathcal{R})$ で逆行列を持つための 必要十分条件 は、すべての $p_i(M)$ が $M(\mathcal{R}_i)$ で逆行列を持つことである。

そこで、各成分 $\mathcal{R}_i$ 上での逆行列 $(p_i(M))^{-1}$ が求まれば、射影の逆変換（存在すれば）より、$p(M)^{-1}$ が求まる。整域 $\mathcal{D}$ が単項イデアル環（例 (i), (ii)）であれば、射影の逆変換は補間に他ならない。一般の整域における逆変換については、整域が多変数多項式環に帰着できれば、Gröbner 基底を使う算法がある。(Becker& Weispfenning, 1991)

Becker& Weispfenning(1991) の方法は、準素イデアル分解したときに、$<\mathcal{I}_i, \mathcal{I}_j>=\mathcal{D}$ なる条件が成り立たたない場合にも「中国剰余定理もどき」を構成できる。整域を多変数多項式環とする。イデアル $\mathcal{I}$ は前述のように無駄なく準素イデアル分解されたとする。すなわち、

$$\mathcal{I} = \mathcal{I}_1 \cap \cdots \cap \mathcal{I}_r,$$

ここで、$\mathcal{I}_i, i = 1, ..., r,$ は準素イデアルとし、$\mathcal{D}/\mathcal{I}_i$ を $\mathcal{R}_i$ とおく。また、$\mathcal{D}$ から $\mathcal{R}_i$ への射影を p_i とおく。このとき、$\mathcal{R}$ から形式的な直積 $\mathcal{R}_1 \times \cdots \times \mathcal{R}_r$ への自然な写像 ϕ が定義できる。すなわち、$\mathcal{R}$ の元 f に対して、その $\mathcal{D}$ への逆像を $\tilde{f}$ とおけば、f の ϕ による像は以下で定義される。

$\phi(\tilde{f}) = (p_1(\tilde{f}), ..., p_r(\tilde{f}))$.

写像 ϕ は全射とは限らないが単射である。また $\phi(\mathcal{R})$ から $\mathcal{R}$ への逆写像は、Becker& Weispfenning(1991) の算法により与えられる。この写像を 行列の写像に拡張することにより次を得る。

性質 3　$p(M)$ が $M(\mathcal{R})$ で逆行列を持つための 必要十分条件 は、すべての $p_i(M)$ が $M(\mathcal{R}_i)$ で逆行列 $p_i(M)^{-1}$ を持ち、かつ $(p_1(M)^{-1}, ..., p_r(M)^{-1})$ の逆像が存在することである。また、この逆像は $p(M)$ の逆行列である。

以上の剰余環の分解についてその効率性（コスト）を考えると、2つの重要な問題がある。

第一の問題点は、一個の逆行列を求めるために r 個の逆行列を求める点である。もし、逆行列算法のステップ数（ここでは、環上の加減乗を1ステップとみなす）が環に依存しないならば、分解した場合のステップ数は、$\mathcal{R}$ 上で直接逆行列を求める方法に比べて、r 倍になる。したがって、分解した方が効率的である場合とは、その空間量の減少による効果（幾つかの小さい環に帰着させた効果で、先に述べた環上の加減乗算の1ステップの計算量が小さくなることが期待できる。）が全体でのステップ数の増大（r 倍）を打ち消している場合である。

第二の問題点は、逆写像が効率よく計算できるかどうかである。単項イデアル環または多項式環上の補間法は効率よく計算できる例であるが、前述した Becker& Weispfenning の方法は Gröbner 基底の計算を必要とし、そのコストは小さいとは言えない。（しかし、この場合には環 $\mathcal{R}$ 上の諸演算自体も複雑であり、環 $\mathcal{R}$ 上で直接計算する方が有利と直ちに結論できるものでもない。）

以上の2点より、環を分解して計算する方法は理論的には興味深いが、実際の計算において効率が上がるかどうかは環 $\mathcal{R}$ に依存するため、環ごとに得失をよく検討しなければな

らない。多変数多項式環の剰余環で環の分解が有効になるのは、イデアルの準素成分が極大イデアルである場合が挙げられる。

2.2. 準素イデアルによる剰余環上の方法：Hensel 構成

前節で、イデアルによる剰余環の行列計算が、そのイデアルの準素イデアル分解に対応する剰余環の行列計算に帰着される場合を述べたが、ここでは、各々の成分の上での行列計算が、さらに小さい環の上での計算から導かれる場合があること、およびその場合の計算法を述べる。基本的には、行列の Hensel 構成を実行するものである。行列の Hensel 構成は行列の各成分が多項式の場合にモジュラー算法として適用されており、ベキ級数環の上で逆行列を構成する技法である。そして、各ベキ級数を有理関数に変換することで、有理関数体上の逆行列を求めている。(Krishnamurthy, 1985 参照)

以下 $\mathcal{D}$ は Noether 整域、$\mathcal{I}$ は準素イデアルとし、それが属する素イデアル $\mathcal{J}$ のベキ乗とする。すなわち、$\mathcal{I}=\mathcal{J}^s$、と仮定する。(このような状況は必ずしも一般的とは言えない。一般のイデアルでは、素イデアルのベキは必ずしも準素イデアルにはならないし、必ずしも準素イデアルが素イデアルのベキになるものでもない。ただし、単項イデアル環ではいつでもいえる。) まず、$\mathcal{J}$ が単項イデアル、すなわち $\mathcal{J}=<a>$ のときを考える。このとき、$\mathcal{I}=<a^s>$ である。$\mathcal{D}$ から $\mathcal{D}/\mathcal{J}^k$ への射影を $q^{(k)}$ と書くことにする。このとき、$p=q^{(s)}$ である。また、簡単のため $q=q^{(1)}$ とおく。M を $\mathcal{D}$ 上の正方行列とする。このとき、次が成り立つ。

性質 4　$p(M)$ が $\mathcal{R}$ 上で逆行列を持つための必要条件は $q(M)$ が $\mathcal{D}/\mathcal{J}$ 上で逆行列を持つことである。

この性質は、「$p(\det(M))$ が $\mathcal{R}$ 上で可逆元であるための必要十分条件は $q(\det(M))$ が $\mathcal{D}/\mathcal{J}$ 上で可逆であることである。」と同値であり、それは det に注目して証明できるが、逆行列の構成法を示す意味で上の性質の方を構成的に証明する。

$p(M)$ が $\mathcal{R}$ 上で逆行列を持つとする。このとき、ある行列 $N\in M(\mathcal{D})$ で $p(M)p(N)=p(I)$ となるものが存在する。ここで、I は単位行列とする。このとき、$q(M)q(N)=q(I)$ となり $q(M)$ も $\mathcal{D}/\mathcal{J}$ 上で逆行列を持つ。逆に、$q(M)$ が逆行列を持つと仮定し、それは $q(N)$、$N\in M(\mathcal{D})$ であるとする。すると、$M=M_0+aM_1$, $N=N_0+aN_1$, $q(M)=q(M_0)$, $q(N)=q(N_0)$ となるように、$M_0,M_1,N_0,N_1\in M(\mathcal{D})$ がとれる。$q(M)q(N)=q(I)$ であることから、M_0N_0-I は $M(\mathcal{J})$ に属することがわかる。ここで、$M(\mathcal{J})$ はすべての成分がイデアル $\mathcal{J}$ に属する行列全体の集合とする。よって、$M_0N_0-I=aL_1$、L_1 は $M(\mathcal{D})$ の元、と書ける。そこで、$N_1'=-N_0(M_1N_0+L_1)$ とおけば、

$$(M_0+aM_1)(N_0+aN_1')=I-a^2(L_1M_1N_0+L_1^2+M_1N_0M_1N_0+M_1N_0L_1)$$

となり、

$$q^{(2)}(M_0+aM_1)q^{(2)}(N_0+aN_1')=q^{(2)}(I)$$

を得る。以下これを繰り返して、ある行列 $M_1,\ldots,M_k,N_1',\ldots,N_k'\in M(\mathcal{D})$ が存在して、$M=M_0+aM_1+\cdots+a^kM_k$ と書け、$N'=N_0+aN_1'+\cdots+a^kN_k'$ とおけば、

$$q^{(k+1)}(M_0 + aM_1 + \cdots + a^k M_k)q^{(k+1)}(N_0 + aN_1' + \cdots + a^k N_k') = q^{(k+1)}(I)$$

とできる。とくに、$k = s-1$ のときを考えれば、$p(M)p(N') = p(I)$ となり、$p(M)$ が $\mathcal{R}$ で逆行列を持つことがわかり、それは、$q(M)$ の逆行列より構成できる。この構成法は Hensel 構成に他ならない。ここでは、持ち挙げ (lift up) を線形、すなわち $a \to a^2 \to a^3 \to \cdots$、としたが、2乗で持ち挙げること、すなわち $a \to a^2 \to a^4 \to \cdots$、も可能である。

以上は $\mathcal{J}$ が単項イデアルであることを仮定したが、そうでない場合にも、$\mathcal{J}$ の正規 Gröbner 基底（極小基底）$\{a_1, ..., a_t\}$ をとれば、同様の Hensel 構成ができる（extended Zassenhaus 法に対応）。すなわち、上の aM_i のかわりに、$a_1M_{i,1} + a_2M_{i,2} + \cdots + a_tM_{i,t}$ を計算する。（ここの計算は、Gröbner 基底の性質を利用することで可能になる。）ここで、$M_{i,j}$ は $\mathcal{D}$ の上の行列である。これに対応して、N_i' の代わりに $N_{i,1}', ..., N_{i,t}'$ を求めるのである。したがって、次が成り立つ。

性質 5　性質 4 は $\mathcal{J}$ が有限個の極小基底をもち、$\mathcal{I} = \mathcal{J}^s$ のときにも成り立つ。

性質 4 が成り立つ時、環 $\mathcal{R}$ は Hensel 構成ができるということにする。

節 2.1 と節 2.2 を合わせると、

性質 6　環 $\mathcal{R}$ で中国剰余定理が成り立ち、かつ各々の成分で Hensel 構成ができるものとする。この時、$\mathcal{R}$ 上の行列 M が逆行列を持つための必要十分条件は各素因子による剰余環上で M の像が逆行列を持つことである。ここで、素因子とは、各準素イデアルの根基 (radical) のことをいう。

3. 掃き出し法

今までの議論では、行列の計算の前にもとのイデアルが分解されていることを前提にしている。しかし、一般にこの分解の操作は大きな計算量を必要とするので、同一の剰余環上の行列演算を多数の行列に対して多量に行なうときには、この分解が結果として全体の計算の効率化に役立つものとなるが、ごく小数の行列に対してのみ行なう場合には必ずしも効率的とは言えない。そこで、本節ではイデアルの分解が予めわかっている場合と予めは分かっていない場合の二つの場合に分けて、実際の行列演算（ここでは、掃き出し法）をどうするかについて述べる。

さて、行列式や逆行列の計算を効率よく行なう方法として掃き出し法が古くから使われている。前節では、剰余環上の行列演算をより小さい剰余環（整域）上の行列演算に帰着したが、より小さい剰余環上の逆行列計算には掃き出し法が有効である場合が多いと考えられる。そこで、まず整域上の掃き出し法について考える。

3.1. 整域上の掃き出し法

今、$\mathcal{R} = \mathcal{D}/\mathcal{I}$ は整域であると仮定する。その商体を $\mathcal{Q}(\mathcal{R})$ とおけば、$\mathcal{R}$ 上の行列 M の掃き出しは $\mathcal{Q}(\mathcal{R})$ での掃き出しを行なうことである。そこで、掃き出しを実行する方法として次が考えられる。

(i) 直接 $\mathcal{Q}(\mathcal{R})$ で効率的な掃き出し法を使って計算する。

(ii) 掃き出しの順番を制御しながら、掃き出す元が $\mathcal{R}$ で逆元を持つかどうか、を判定しながら掃き出しをすすめる。

(iii) さらに、$\mathcal{R}$ よりも小さい剰余環での掃き出しに帰着させる。

が挙げられる。(i) は結果的に最終ステップで、行列の行列式が算出され、そこで逆行列の存在（可逆性）が判定される。効率的な掃き出しとして、fraction-free 算法 (Sasaki& Murao, 1982) が挙げられる。

我々の設定では、途中の段階で行列が非可逆の場合に手続きを止めること（early detection）を採り入れる方法も考えられる。その例として (ii) について詳しく述べよう。

(ii) の計算が有効にできる場合として、$\mathcal{R}$ が単項イデアル整域（PID）であり、$\mathcal{R}$ 上の2元の GCD が効率的に計算できるときが挙げられる。そこで以下、$\mathcal{R}$ が単項イデアル整域であり、$\mathcal{R}$ 上の2元の GCD が効率的に計算できるものとする。(ii) の制御は単因子を求める算法とよく似ている。まず基本的な性質を挙げておく。

性質 7　一意分解整域（UFD）$\mathcal{R}$ 上の正方行列 M に対して、同一行（列）上のすべての元の GCD が可逆元でないならば、M は逆行列を持たない。さらに、行列 M がブロック化されている時、すなわち、

$$\begin{pmatrix} A & B \\ 0 & D \end{pmatrix}$$

である時、部分行列 A または D において、同一行（列）上のすべての元の GCD が可逆元でないならば、M は逆行列を持たない。

$n \times n$ 行列 $M = (m_{i,j})_{1 \le i,j \le n}$ が与えられたとしよう。掃き出し法では掃き出しを対角 $(1,1)$ より始める。i 回目の掃き出しにおいては、軸（pivot）m_{i_0,j_0} を選び必要ならば行・列を入れ換えて対角 (i,i) において、第 i 行で掃き出しを行なう。

(A) 軸 $m_{i,i}$ が可逆元であれば、正規化（すなわち、第 i 行全体に $m_{i,i}^{-1}$ を乗ずる）し、掃き出しを行なう。

(B) 軸 $m_{i,i}$ が非可逆元の場合には、第 i 列のすべての元が $m_{i,i}$ の倍元の場合にのみ掃き出しができる。しかし、この場合は性質 7 より、行列 M は $\mathcal{R}$ 上で逆行列を持たない。よって、この掃き出しは行列式を求める時のみ有効である。

(C) (A)(B) いずれでもない場合には、軸の変更を以下の手順で行なう。

(C-i) 第 i 列の第 $i+1$ 行以下に可逆元があれば、行を交換してその可逆元が軸にくるようにする。第 i 列の第 $i+1$ 行以下には可逆元がないが、第 $i+1$ 列以降の列で第 $i+1$ 行以下に可逆元がある場合は、列および行の交換を行ない、可逆元を軸に持ってきて掃き出しを行なう。

(C-ii) 第$i+1$列以降のすべての列で第$i+1$行以下に可逆元がない場合は、
第i列で第$i+1$行以下の元の全体の GCD （m' と置こう） を求める。すなわち、$m_{i,j_0}, m_{i,j_1}, ..., m_{i,j_r}$ を 0 でない第i列の第$i+1$行以下の元全体とすれば、

$$m' = GCD(m_{i,j_0}, ..., m_{i,j_r}).$$

この m' の構成すなわち extended GCD に対応する行の操作により、軸の値が m' になるようにできる。こうすると、第i列の第$i+1$行以下のすべての元は $m_{i,i} = m'$ の倍元となる。したがって、性質 7 より、m' が可逆元でなければ逆行列はもたないことが判定される。$m_{i,i} = m'$ が可逆元ならば、正規化して掃き出しを行なう。行列式を計算する場合には、上半三角化で十分であるので、$m_{i,i}$ による掃き出しを行なう。

環 $\mathcal{R}$ が一意分解整域（UFD）であるが PID でない場合には、GCD に対応する行列操作が一般には存在しないので、その制御は難しくなる。(iii) と (ii) の中間でさらに剰余環をとって PID を構成することも考えられる。

$\mathcal{R}$ が UFD でさえない場合には、さらに困難になる。GCD に相当する元（元が生成するイデアルの別の生成元等）を計算することが必要であることに加えて、Property 5 が一般には成立しないからである。よってその制御は難しく、(ii) の方法は適さない。

(iii) は前節の中国剰余定理もしくは Hensel 構成を利用する方法で、一般のモジュラー算法に対応する。例えば、$\mathcal{R}$ の極大イデアルが複数個取れる場合に、$\mathcal{M}_1, ..., \mathcal{M}_r$ とする、

$$\mathcal{R}/\mathcal{M}_1 \cap \cdots \cap \mathcal{M}_r = \mathcal{R}/\mathcal{M}_1 \bigoplus \cdots \bigoplus \mathcal{R}/\mathcal{M}_r$$

となり、各剰余環は体になる。したがって、行列演算が体上の演算となり、さらには、各々の体が $\mathcal{Q}$ に比べて小さいことより、計算の効率化が可能になる（ただし、$\mathcal{R}/\mathcal{M}_1 \cap \cdots \cap \mathcal{M}_r$ から $\mathcal{R}$ への引き戻しが可能であることが前提になる)。

3.2. 一般の環の掃き出し法：動的掃き出し

体でない環の上で掃き出しを行なうには、節 3.1 の整域上の掃き出しで見たように、GCD の演算が必要になる。整域ではない環は一般には UFD・PID ではないので、GCD 演算はのぞめない。すなわち、$\mathcal{R}$ 上の行列の掃き出しの制御は大変難しい。そこで、もとの整域 $\mathcal{D}$ に戻って掃き出しを行なうことになる。このとき、(I) $\mathcal{D}$ が PID であれば、節 3.1. (ii) を用いることができ、$\mathcal{R}$ 用に少し変更を加えればよいことになり、(II) PID でない場合には、節 3.1. (i) または (iii) を行なって、最終的に射影をとって $\mathcal{R}$ 上の行列に戻すことになる。以下では、(I) の場合について考える。

節 3.1. (ii) の方法に対して、$\mathcal{R}$ 上の計算に変更する点は可逆元の判定とその計算である。$\mathcal{D}$ は PID であるので、イデアル $\mathcal{I}$ は単項イデアル $< a >$ である。a が既約因子分解されているならば、節 2 により、さらに小さい環の上の行列演算に帰着されるので、a は既約因子分解されていないものとする。（既約因子分解の計算量が、GCD の計算量と比べて大変大きい状況はよくあるものといえる。）

節 3.1 と同様に、$n \times n$ 行列 $M = (m_{i,j})_{1 \leq i,j \leq n}$ が与えられたとしよう。

(A) 軸 $m_{i,i}$ が可逆元であれば、正規化（すなわち、i 行全体に $m_{i,i}^{-1}$ を乗ずる）し、掃き出しを行なう。

(B) 軸 $m_{i,i}$ が零でない非可逆元の場合には、$GCD(a, m_{i,i})$ は自明ではない。そこで、$a, m_{i,i}$ を用いて以下が計算できる。

$$a = a_1^{e_1} a_2^{e_2} \cdots a_r^{e_r} a_{r+1}^{e_{r+1}} \cdots a_{r+s}^{e_{r+s}}$$
$$m_{1,1} = a_1^{e'_1} a_2^{e'_2} \cdots a_r^{e'_r}$$

ここで、$a_1, ..., a_{r+s}$ は $\mathcal{D}$ の元である。

この計算は GCD 計算のみで、無平方分解の算法と同様の方法により計算できる。そこで、

$$\mathcal{R} = \mathcal{D}/ < a >= \mathcal{D}/ < a_1^{e_1} > \bigoplus \cdots \bigoplus \mathcal{D}/ < a_{r+s}^{e_{r+s}} >$$

と分解して、さらに小さい環 $\mathcal{D}/ < a_j^{e_j} >$, $j = 1, ..., r+s$, 上の計算に帰着させる。この分解によって、行列 M は $M_1 \bigoplus \cdots \bigoplus M_{r+s}$ と書ける。ここで M_i は M の $\mathcal{D}/ < a_i^{e_i} >$ への射影である。このとき、$M_1, ..., M_r$ の (i,i) 成分は 0 または ベキ零元であり、$M_{r+1}, ..., M_{r+s}$ の (i,i) 成分は可逆元となっている。そこで、$M_1, ..., M_r$ に対しては、軸の変更が必要となる。節 2.2 の Hensel 構成を用いれば、各々の剰余環 $\mathcal{D}/ < a_i^{e_i} >$ に対しては、まず $\mathcal{D}/ < a_i >$ を考えることになるので、まさしく M_j, $j = 1, ..., r$ の (i,i) 成分 は $\mathcal{D}/ < a_i^{e_i} >$ 上で 0 となる。

注意：非可逆元に対する GCD 操作と軸の変更はつまるところ、a と同一行（または列）上の元の GCD 操作に他ならない。

以上の掃き出しに関する制御の特徴は、掃き出しながら環の分解を与えていく点にある。一般に環の分解はコストがかかるので、このように動的に分解していく方法は有効であると考えられる。さらに、固定した環上の多くの行列に関して逆行列を求めていく場合には、次第に環の分解が得られる点（すなわち、次第に小さい環の計算に帰着できる点）で、その有効性が顕著になると考えられる。

4. まとめ

本稿では動的掃き出し法を念頭におき、それに必要となる要素アルゴリズムとして、中国剰余アルゴリズムと Hensel 構成とを検討した。しかし、動的掃き出し法がどの程度効率的かについては未検討であり今後の課題である。

動的掃き出し法と類似の方法、すなわち計算の進行につれて環をより小さい成分に分解し、各々の環上で計算を行なったのちもとの環に復元するという動的な技法は、線形計算ばかりでなく一般に剰余環上の計算において広く利用できる方法である。

次の機会には線形演算のなかで今回述べなかった固有値問題についての研究結果を発表する予定である。

参 考 文 献

[1] T.Becker, V.Weispfenning, The Chinese remainder problem multivariate interpolation, and Gröbner bases, in the proceedings of ISSAC'91, ACM PRESS, 64-69, 1991.

[2] E.R.Berlekamp, *Algebraic Coding Theory*, McGraw-Hill, 1968.

[3] B.Buchberger, Gröbner bases: An algorithmic method in polynomial idael theory, in Recent Trends in Multidimensional System Theory, Chapter 6, D.Reidel Publ. Comp., 1985.

[4] B.Buchberger, Applications of Gröbner bases in non-linear computational geometry, in Trends in Computer Algebra, LNCS 296, 52-80. 1987.

[5] J.L.Dornstetter, On the equivalence between Berlekamp's and Euclid's, IEEE Trans. Inform. Theory, vol. IT-33, 428-431, 1987.

[6] P.Gianni, B.Trager, G.Zacharias, Gröbner bases and primary decomposition of polynomial ideals, J. Symbolic Computation, Vol.6, 149-168.

[7] E.Kaltofen, On computing determinants of matrices without divisions, in the proceeding of ISSAC'92, ACM PRESS, 342-349, 1992.

[8] E.Kaltofen, B.D.Saunders, On Wiedemann's method of solving linear systems, in the proceedings of AAECC-8, LNCS 536, 29-38, 1991.

[9] E.V.Krishnamurthy, *Error-Free Polynomial Matrix Computations*, Springer-Verlag, 1985.

[10] W.H.Mills, Continued fractions and linear recurrences, Math. Comp. Vol.29, 173-180, 1975.

[11] 佐々木建昭, 数式処理（情報処理叢書7）, 情報処理学会, 1981.

[12] T.Sasaki, H.Murao, Efficient Gaussian elimination method for symbolic determinants and linear systems, ACM Trans. Math. Software, Vol.8, 277-289, 1982.

[13] D.H.Wiedemann, Solving sparce linear equations over finite fields, IEEE Trans. Inform. Theory, Vol.IT-32, 54-62, 1986.