数理解析研究所講究録 1444 巻 2005 年 137-144



# 連立代数方程式の消去の理論と実際

野呂 正行
MASAYUKI NORO
神戸大学理学部
DEPARTMENT OF MATHEMATICS, KOBE UNIVERSITY *

## 1 はじめに

体 $K$ 上の $n$ 変数多項式 $f_i(x_1,\ldots,x_n)\in K[x_1,\ldots,x_n]$ に対して,

$$f_1(x_1,\ldots,x_n)=0,\ldots,f_m(x_1,\ldots,x_n)=0 \tag{1}$$

を連立代数方程式または代数方程式系とよぶ. (1) を解く, あるいは解の満たす性質を調べることは, 過去から今日に至るまで数学における中心的な課題の一つであり続けている. 解を実際に求める方法で最もポピュラーなものは消去法であろう. 各 $f_i$ が線形の場合には効率のよいアルゴリズム (Gauss 消去) があることは周知であるが, $f_i$ が高次項を含む場合には, 決定的といえる方法はなく, 現在でも種々の方法が提案されている. 本稿では, 関, Bézout により考案された終結式による消去法から始めて, 最近の方法である Gröbner 基底, 多重多項式終結式, 疎終結式などについて紹介する. さらに, 各方法による, 実際の方程式系の求解について, いくつかの実例をもとに解説する.

## 2 終結式

$$f(x) = a_nx^n+\cdots+a_0,\quad a_n\neq 0 \tag{2}$$
$$g(x) = b_mx^m+\cdots+b_0,\quad b_n\neq 0 \tag{3}$$

が共通零点 $\alpha$ を持つとき

$$\alpha^i f(\alpha) = 0\quad (i=0,\cdots m-1)$$
$$\alpha^j g(\alpha) = 0\quad (j=0,\cdots n-1)$$

が成り立つ. これは,

$$S(f,g)=\begin{pmatrix}
a_n & a_{n-1} & \cdots & a_1 & a_0 & & \\
 & a_n & a_{n-1} & \cdots & a_1 & a_0 & \\
 & & \ddots & \ddots & & \ddots & \ddots \\
 & & & a_n & a_{n-1} & \cdots & a_1 & a_0 \\
b_m & b_{m-1} & \cdots & b_1 & b_0 & & & \\
 & b_m & g_{m-1} & \cdots & b_1 & b_0 & & \\
 & & \ddots & \ddots & & \ddots & \ddots & \\
 & & & b_m & b_{m-1} & \cdots & b_1 & b_0
\end{pmatrix}$$

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

とおくとき, 線形方程式系 $S(f,g)x=0$ が $x={}^t(\alpha^{m+n-1},\ldots,1)$ なる非自明解をもつことを意味するから

$$\det S(f,g)=0 \tag{4}$$

が必要となる. (4) の左辺を $\mathrm{Res}_x(f,g)$ と書き $f,g$ の終結式 (resultant) と呼ぶ.

**定理 2.1**
(2), (3) に対し, $a(x),b(x)\in\mathbf{Z}[x,a_0,\ldots,a_{n-1},b_0,\ldots,b_{m-1}]$ が存在して

$$af+bg=\mathrm{Res}_x(f,g) \tag{5}$$

が成り立つ. $\mathrm{Res}_x(f,g)=0$ のとき, $f(x)$ と $g(x)$ は共通零点をもつ.

さて, $f(x,y),g(x,y)\in K[x,y]$ とする.

$$\begin{aligned} f(x,y) &= a_n(y)x^n+\cdots+a_0(y)\\ g(x,y) &= b_m(y)x^m+\cdots+b_0(y)\end{aligned}$$

と書くとき, $\mathrm{Res}_x(f(x,y),g(x,y))$ は $y$ の 1 変数多項式 $r(y)$ となる. このとき, (5) の $a,b$ は 2 変数多項式となる. すなわち $a(x,y),b(x,y)\in K[x,y]$ が存在して

$$a(x,y)f(x,y)+b(x,y)g(x,y)=r(y)$$

が成り立つ. よって $f(\alpha,\beta)=g(\alpha,\beta)=0$ となる $(\alpha,\beta)$ があるとすれば,

$$r(\beta)=0 \tag{6}$$

を満たさねばならない. (6) は, 2 変数の方程式系が解をもつ条件として得られた 1 変数の方程式であり, 消去法と呼ぶにふさわしい. この方法を繰り返し適用すれば, $n$ 変数の方程式系から最終的に 1 変数の方程式を得ることも可能である.

**例 2.2**
$f(x,y,z)=g(x,y,z)=h(x,y,z)=0$ を解く場合, $r(z)=\mathrm{Res}_y(\mathrm{Res}_x(f,g),\mathrm{Res}_x(f,h))$ により, 解の満たすべき条件 $r(z)=0$ が得られる.

ただし, この方法はあまりに素朴である. すなわち, 一般に, 得られる多項式は解に対応しない零点を含む.

**例 2.3**

$$\begin{aligned} f(x,y,z) &= xyz-1=0\\ g(x,y,z) &= xy^2+y^2z+z^2x-1=0\\ h(x,y,z) &= x^3+(3y+3z)x^2+(3y^2+6zy+3z^2)x+y^3+3zy^2+3z^2y+z^3-1=0\end{aligned}$$

に対し,

$$\begin{aligned} \mathrm{Res}_x(f,g) &= z^3y^4-z^2y^2+(z^3+1)y\\ \mathrm{Res}_x(f,h) &= z^3y^6+3z^4y^5+(3z^5+3z^2)y^4+(z^6+5z^3)y^3+(3z^4+3z)y^2+3z^2y+1\\ r(z) &= \mathrm{Res}_y(\mathrm{Res}_x(f,g),\mathrm{Res}_x(f,h))=-z^{36}+12z^{33}+48z^{30}+97z^{27}+400z^{24}\\ &\quad +1091z^{21}+1088z^{18}+263z^{15}+33z^{12}+z^9\end{aligned}$$

となるが, $r(z)=0$ の解 $z=0$ は明らかに不適である.

Bézout[1] は, 与えられた方程式全てを用いて 1 変数を消去する方法を与えた. この方法はイデアルの言葉で言えば, 方程式系のイデアルから, 1 変数を消去した消去イデアルの元のうち, なるべく全次数の小さいものを求める方法である.

**例 2.4**

$$\begin{aligned} f(x,y,z) &= x^3 + a_2(y,z)x^2 + a_1(y,z)x + a_0(y,z) = 0 \\ g(x,y,z) &= x^3 + b_2(y,z)x^2 + b_1(y,z)x + b_0(y,z) = 0 \\ h(x,y,z) &= x^3 + c_2(y,z)x^2 + c_1(y,z)x + c_0(y,z) = 0 \end{aligned}$$

($f,g,h$ の全次数は 3) に対し, 全次数 4 の多項式 $F_1(x,y,z)$, $G_1(x,y,z)$, $H_1(y,z)$ ($\deg_x(F_1) = \deg_x(G_1) = 1$) を用いて全次数 7 の多項式 $r_1(y,z) = F_1 f + G_1 g + H_1 h$ を作る. 同様に, 全次数 4 の多項式 $F_2(x,y,z)$, $H_2(x,y,z)$, $G_2(y,z)$ ($\deg_x(F_2) = \deg_x(H_2) = 1$) を用いて全次数 7 の多項式 $r_2(y,z) = F_2 f + G_2 g + H_2 h$ を作る. $r(z) = \mathrm{Res}_y(r_1(y,z), r_2(y,z))$ は次数 49 の多項式である.

例 2.4 は, [1] において, それまで知られていた Euler および Cramer による, 消去により 81 次式が得られるという結果をより精密にする結果である. しかし, これは現在から見れば不十分な結果である.

**定理 2.5**
$F_i(x_0,\ldots,x_n)$ を, 全次数が $d_i$ の斉次多項式とする.

$$F_1(x_0,\ldots,x_n) = \cdots = F_n(x_0,\ldots,x_n) = 0$$

の $\mathbf{P}^n$ における解が有限個の時, その個数は重複を込めて $d_1 d_2 \cdots d_n$ である.

Bézout 自身は $n = 2$ の場合のみを示したが, この定理はやはり Bézout の名を冠して呼ばれている. この定理によれば, 各変数の満たす最小次数の多項式の次数は, ジェネリックには $d_1 d_2 \cdots d_n$ となる. 例 2.4 の場合には 27 となり, 49 は過大である.

## 3 Gröbner 基底

終結式による消去法は, 消去により得られた多項式の零点の中に, 真の解に対応しないものが存在する可能性があることや, 消去された変数の値を求める手間が必要となるといった短所がある. 本節で述べる Gröbner 基底はイデアルの生成系の一つであるため, 零点集合は保たれる. また, 消去イデアルそのものを求めることができるので, 他の方法で求めた解の検証を行うのに便利である. 一般に Gröbner 基底の計算は, 特殊な場合を除いて計算量が知られていない. しかし, 種々の効率化も提案されていて, 特に有限体あるいは有理数体上の場合には, 計算機の能力向上もあって実用に耐えるものになりつつある. 以下, 体 $K$ 上の $n$ 変数多項式環を固定して考える.

**定義 3.1**
$T$ を係数 1 の単項式全体とする. $T$ の元を項と呼ぶ. $T$ の全順序 $<$ で次を満たすものを項順序とよぶ.

1. 任意 の $t \in T$ に対し $1 \leq t$.
2. $t, s \in T$ が $t \leq s$ を満たすなら, 任意の $u \in T$ に対し $tu \leq su$.

多項式 $f \neq 0$ に現れる項のうち $<$ に関して最高順序のものを $\mathrm{HT}(f)$ と書く.

**定義 3.2**
$I$ を多項式イデアルとし, $<$ を項順序とする. 有限集合 $G \subset I$ が $I$ の $<$ に関する *Gröbner* 基底であるとは, 任意の 0 でない $f \in I$ に対し, ある $g \in G$ が存在して $\mathrm{HT}(g) \mid \mathrm{HT}(f)$ が成り立つときをいう.

**定義 3.3**
$X=\{x_1,\ldots,x_n\}$, $X_i=\{x_{i+1},\ldots,x_n\}$ とする. イデアル $I\subset K[X]$ に対し, $I_i=I\cap K[X_i]$ を $(X,X_i)$ に関する $I$ の消去イデアルと呼ぶ.

消去イデアルは, イデアルの生成系から多項式係数の積和による消去で得られる全ての多項式を含む. 次の定理は, 消去イデアルが Gröbner 基底計算により得られることを意味する.

**定理 3.4**
$<$ を, $s\notin K[X_i]$, $t\in K[X_i]$ ならば $s>t$ となるような項順序とする. (このとき $X\setminus X_i >> X_i$ と書き, $<$ は $(X,X_i)$ に関する消去順序であるという.) $G$ をイデアル $I\subset K[X]$ の $<$ に関する *Gröbner* 基底とすると $G\cap K[X_i]$ は消去イデアル $I\cap K[X_i]$ の *Gröbner* 基底である.

$x_1>x_2>\cdots>x_n$ を満たす辞書式順序は, 任意の $(X,X_i)$ に関する消去順序である. また $K[x_1,\ldots,x_i]$, $K[X_i]$ の項順序を $<_1$, $<_2$ として, $t_1t_2<s_1s_2$ $(t_1,s_1\in K[x_1,\ldots,x_i]$, $t_2s_2\in K[X_i])$ を 「$t_1<_1 s_1$ または $(t_1=s_1$ かつ $t_2<_2 s_2)$」と定義すれば $<$ は $(X,X_i)$ に関する消去順序となる.

消去イデアルは, 前節で述べたような, 終結式あるいは Bézout の方法で得られるような多項式を全て含んでいる.

**例 3.5**
例 *2.3* に対し, イデアル $I=\langle f,g,h\rangle$ の, $x>y>z$ なる辞書式順序に関する *Gröbner* 基底 $G=\langle g_1,g_2,g_3\rangle$ が,

$$\begin{aligned}
g_1(x,z) &= 817369228x+45454973z^{25}-552616591z^{22}-2086838465z^{19}-4183022954z^{16}\\
&\quad -17821406012z^{13}-47327708297z^{10}-44817461739z^7-11457564962z^4\\
&\quad -3111506477z\\
g_2(y,z) &= -7233356y+1740585z^{25}-20859119z^{22}-83871961z^{19}-170311198z^{16}\\
&\quad -699433340z^{13}-1910797353z^{10}-1927410739z^7-498196514z^4-69656837z\\
g_3(z) &= z^{27}+12z^{24}+48z^{21}+97z^{18}+400z^{15}+1091z^{12}+1088z^9+263z^6+33z^3+1
\end{aligned}$$

で与えられる. よって, 消去イデアルは $I_1=\langle g_2,g_3\rangle$, $I_2=\langle g_3\rangle$ となる. 例 *2.3* で計算した $r(z)$ は, $r(z)=-z^9g_3(z)$ を満たし, 確かに $r(z)\in I_2$ であることが分かる.

この例では, さらに詳しいことが分かる. すなわち,

$$\begin{aligned}
g_1(x,z) &= 817369228x+u_1(z)\\
g_2(y,z) &= -7233356y+u_2(z)
\end{aligned}$$

とおくと, $I$ の零点 $V(I)$ は

$$V(I)=\{(-\frac{u_1(\alpha)}{817369228},\frac{u_2(\alpha)}{7233356},\alpha)\mid g_3(\alpha)=0\}$$

と書ける. この場合の Gröbner 基底は, 変数の消去だけではなく, 解そのものも与えていることになる. これは特殊なことではなく, より一般な状況のもとで成り立つ.

**定理 3.6 (Shape Lemma)**
イデアル $I$ が根基イデアル, すなわち $\sqrt{I}=I$ のとき, 適当な線形変数変換のもとで, $I$ の辞書式順序による *Gröbner* 基底 $G$ は

$$G=\{z_1-g_1(z_n),\ldots,z_{n-1}-g_{n-1}(z_n),g_n(z_n)\}$$

となる.

このように, 辞書式順序による Gröbner 基底は, 代数方程式系の解を (ほぼ) 与えるが, 実際の計算の点からは問題がある. 例 2.3 にも現れているように, $g_1$, $g_2$ の係数が $g_3$ のそれに比べて大きい. これは, 一般に言えることで, 計算を困難にする一つの原因となる. これを改良するものとして次がある.

**定理 3.7 (Generalized Shape Lemma; GSL)**
イデアル $I$ が根基イデアルのとき, 適当な線形変数変換のもとで, $I$ の零点は

$$\{(\frac{h_1(\alpha)}{g_n'(\alpha)},\ldots,\frac{h_{n-1}(\alpha)}{g_n'(\alpha)},\alpha) \mid g_n(\alpha)=0\}$$

となる. ここで $g_n(z_n)$ は *Shape Lemma* と同じ *1* 変数多項式で, $g_n'(z_n)$ は $g_n(z_n)$ の微分である.

$I$ が根基であることから $g_n(z_n)$ が重複因子を持たないことが従う. よって, この定理は, Shape Lemma の系としてただちに言えるが, このように解を表現する理由は, $h_i$ の係数が, $g_i$ の係数に比べて著しく小さくなるからである.

**例 3.8**
例 *2.3* に対し, イデアル $I$ の *GSL* による解の表現は, 次の通り.

$$\{(\frac{h_1(\alpha)}{g_3'(\alpha)},\frac{h_2(\alpha)}{g_3'(\alpha)},\alpha) \mid g_3(\alpha)=0\}$$

$$\begin{aligned} h_1(z) &= 9z^{24}-249z^{21}-204z^{18}-1281z^{15}-8634z^{12}-11739z^9-1212z^6+21z^3+9 \\ h_2(z) &= -36z^{24}+117z^{21}+372z^{18}-1467z^{15}-5484z^{12}-6837z^9-4200z^6-669z^3-36 \end{aligned}$$

# 4 多重多項式終結式, 疎終結式

複数の多変数多項式から, 終結式によりトーナメント式に変数を消去していく方法は, 既に見たように最良の方法とは言えない. ここでは, ある意味で, 変数を一度に消去する方法である多重多項式終結式 (multipolynomial resultant), および疎終結式 (sparse resultant) について概説する. (本節は [2] の極めて大雑把な紹介である. 詳細は [2] を参照してほしい.)

**定理 4.1**
$F_0(x_0,\ldots,x_n)$, ...,$F_n(x_0,\ldots,x_n)$ を, 全次数がそれぞれ $d_i>0$ であるような斉次多項式とする. このとき, $F_0,\ldots,F_n$ の係数の絶対既約な整数係数多項式 $\mathrm{Res}(F_0,\ldots,F_n)$ がただ一つ存在して

1. $F_0,\ldots,F_n$ が $\mathbf{P}^n$ に共通零点を持つ $\Leftrightarrow \mathrm{Res}(F_0,\ldots,F_n)=0$
2. $\mathrm{Res}(x_0^{d_0},\ldots,x_n^{d_n})=1$

定理 4.1 を用いて代数方程式系の求解を行う方法として少くとも 2 つの方法: $u$-終結式 [3] および hidden variable による方法がある. ここでは後者について概説する.

一般に, 非斉次多項式 $f_0(x_1,\ldots,x_n)$ $(i=0,\ldots,n-1)$ が与えられ, その共通零点を求めたいとする. hidden variable による方法では, いずれかの変数, 例えば $x_n$ を定数とみなす. これにより $n-1$ 変数多項式が $n$ 個あると考える. これらを斉次化したものを

$$F_0(x_0,\ldots,x_{n-1}),\ldots,F_{n-1}(x_0,\ldots,x_{n-1})$$

($x_0$ は斉次化変数) とする. もし, もとの $f_0,\ldots,f_{n-1}$ に共通零点があれば, 解の $x_n$ 座標を代入したものは共通零点を持つ. よって, それを斉次化した $F_0,\ldots,F_{n-1}$ も $\mathbf{P}^{n-1}$ に共通零点を持つ. よって, $\mathrm{Res}(F_0,\ldots,F_{n-1})$ を計算することにより, $x_n$ の満たすべき 1 変数方程式が得られる.

ここで定義した多重多項式終結式は, 全次数 $d_i$ の多項式の全ての係数の関数となっていて, 全次数が大きくなると, 終結式自体が巨大化する. 実際の応用では, 入力多項式は疎な多項式であることが多く, いわゆる疎終結式 [4] が有効である. 疎終結式は, 各 $F_i$ に対して, 全次数ではなく, その support, すなわち, 係数が 0 でないような項の集合を与えた場合に, それらが $\mathbf{C}^n \setminus \{0\}$ に共通零点をもつ条件を与える $F_i$ の係数の多項式である. 多重多項式終結式, 疎終結式ともに, ある場合には行列式の商として計算できる. 特に, hidden variable の方法で, 変数の満たす必要条件を求めたい場合には, 終結式の厳密な計算は必要でなく, 分子の行列式を計算するだけで済む.

**例 4.2**
例 2.3 に対して, $z$ を *hidden variable* として疎終結式を計算すると $g_3(z)$ そのものが得られる. すなわち余分な成分は生じない.

## 5 実行例 — 4 つの長方形

関孝和, 建部賢明, 賢弘による大成算経第 19 巻 [5] にある, 4 つの長方形の面積および辺の長さの和をいくつか与えて辺の長さを求める問題について, 消去法の実行例を示す. 方程式は次の通りである.

$$\begin{aligned}
f_1 &= rs+tu+vw+p-a=0\\
f_2 &= pq+tu+vw+r-b=0\\
f_3 &= pq+rs+vw+t-c=0\\
f_4 &= pq+rs+tu+v-d=0\\
f_5 &= r+t+v+q-e=0\\
f_6 &= p+t+v+s-f=0\\
f_7 &= p+r+v+u-g=0\\
f_8 &= p+r+t+w-h=0
\end{aligned}$$

$p,q,r,s,t,u,v,w$ が変数, $a,b,c,d,e,f,g,h$ が定数である. 原著では, 著者らの消去法により変数を逐次消去し, $p$ に関する 50 次式を得ているそうである. 残念ながら, 本稿の筆者はそこに書かれている式を解読することはできず, 小松先生によればまだ読んだ人は誰もいないのではないか, ということである.

さまざまな方法を試した結果, 次の手順により $p$ の満たす方程式を比較的容易に求めることができる.

1. $w$, $u$, $s$, $v$ の消去

   $f_i$ $(i=1,\ldots,4)$ から $f_8$ により $w$ を, $f_7$ により $u$ を, $f_6$ により $s$ を消去したのち, $f_5$ により $v$ を消去したものを $\tilde{f}_i$ とする.

$$\begin{aligned}
\tilde{f}_1 &= 2t^2+(2q+2r-2e+g-h)t+(q-e+1)p+(2r-h)q+2r^2\\
&\quad +(-2e+f-h)r-a+he\\
\tilde{f}_2 &= 2t^2+(2q+2r-2e+g-h)t+(2q+r-e)p+(r-h)q+r^2\\
&\quad +(-e-h+1)r-b+he\\
\tilde{f}_3 &= t^2+(p+q+2r-e-h+1)t+(2q-e)p+(2r-h)q+2r^2\\
&\quad +(-2e+f-h)r-c+he\\
\tilde{f}_4 &= t^2+(-p+q-e+g-1)t+(q-r)p+(r-1)q+r^2\\
&\quad +(-e+f-1)r-d+e
\end{aligned}$$

2. $t$ の消去

$I=\langle \tilde{f}_1,\tilde{f}_2,\tilde{f}_3,\tilde{f}_4\rangle$ に対し, $\{t\} >> \{r,q,p,a,b,c,d,e,f,g,h\}$ かつ, 後半の変数には全次数逆辞書式順序を適用する消去順序を設定して Gröbner 基底 $G$ を計算すると,

$$G=\{g_1(p,q),g_2(p,q,r),\ldots,g_7(p,q,r),g_8(p,q,r,t),\ldots,g_{16}(p,q,r,t)\}$$

($a,\ldots,h$ は省略した.) すなわち,

$$I\cap \mathbf{Q}[p,q,r]=\langle g_1,\ldots,g_7\rangle$$

3. $r$ の消去

$h(p,q)=\mathrm{Res}_r(g_2(p,q,r),g_3(p,q,r))$ を計算する.

$$g_2=3r^2+(3q-3p-3e+3f-3)r-q+p-a+2b-c-d+e$$

で, $\deg_r(g_3)=1$ だから, 実際には $g_3=0$ を $r$ について解いて $g_2$ に代入して分母を払うことに相当する.

4. $q$ の消去

$$g_1=(3p-1)q-2p+2a-b-c-d+e$$

と, 3. の $h(p,q)$ から $R(p)=\mathrm{Res}_q(g_1(p,q),h(p,q))$ を求める. これも $g_1$ を $q$ について解いて代入して分母を払うことに相当する.

$$\begin{aligned}\deg_p(R) &= 12\\ \deg_a(R) &= \deg_b(R)=\deg_c(R)=\deg_d(R)=\deg_e(R)=5\\ \deg_f(R) &= \deg_g(R)=\deg_h(R)=4\end{aligned}$$

で, $a,b,c,d,e,f,g,h$ に関する $R$ の全次数は 12 である.

得られた $p$ の 12 次式 $R(p)$ は $\mathbf{Q}$ 上既約であり, $p$ の満たす最小次数の多項式であることが分かる. これは, 実際に消去イデアルを計算することでも確かめられる. よって, 関らの得た 50 次式は $R(p)$ で割り切れるはずであるが, 残念ながらこれを確かめることは現状ではできない. $R(p)$ は, $p$ およびパラメタ $a,b,c,d,e,f,g,h$ の多項式としては 22858 項ある巨大な多項式である. 関らの 50 次式もやはりパラメタを係数に含むが, 部分式に名前をつけて展開していないのが, 比較的コンパクトな表示が得られている理由と推測される.

ここで述べた方法では, ステップ 2 で $t$ の消去を消去イデアルにより行ったことにより, $g_1$, $g_2$ という小さな多項式が得られたことが, 後の計算を容易にしたが, この結果を手本にして, 逆に次のような解法を導くこともできる.

まず, $g_1(p,q)$ は, そのパラメタに関する部分に注目することにより

$$g_1=2f_1-f_2-f_3-f_4+f_5$$

であることが分かる. また, $l=\tilde{f}_1-\tilde{f}_2$ とおけば,

$$l=r^2+(q-p-e+f-1)r-pq+p-a+b$$

である. $m=\mathrm{Res}_t(\tilde{f}_3,\tilde{f}_4)$ とおいて $p,q,r$ の多項式 $l$, $m$ から $n(p,q)=\mathrm{Res}_r(l,m)$ を作る. 最後に $\mathrm{Res}_q(n,g_1)$ を作ればこれは定数倍を除いて $R(p)$ に等しい.

見通しのよい人ならこれくらいの解法を思いつくのは容易かもしれないが, (筆者のように) 見通しがよくない人でも, 計算機の助けを借りればこのような解法が得られる. ただし, 実際の計算はせいぜい $m$ の計算までで, 方法が違うとはいえ, 手で最後まで消去を遂行した関らの計算力は驚異的である.

## 6 おわりに

本稿は, 数学史の門外漢が, 偉大な先人の足跡をほんの少し辿ってみた (しかも計算機と最新アルゴリズムという「とび道具」を援用して) というだけの報告であるが, もし彼らが計算機を手にしていたら, どのようなことになっていたか, 想像するだけでも楽しいことである. 計算代数は, その性格上, 古典的な, 多項式を直接操作する代数幾何と親和性が高いが, この分野では 19 世紀から 20 世紀初頭の数学者の業績の再発見あるいは再評価が相次いでいる. 終結式については, 現在最先端の研究成果である [4] が Cayley の仕事に基づいている. また, Gröbner 基底は, 多項式イデアルの性質を単項式イデアルの性質に帰着する Macaulay のアイディアのアルゴリズム化とも言える. GSL は, Kronecker により既に発見されていたらしい. これらは数学史から計算代数への贈り物といえそうだが, 逆に, 数学史の研究に数学ソフトウェアを用いることにより, 新たな展開が期待できそうに思える. たとえば, 関らの記法を文法として定義して構文解析器を作ることで, 原典 [5] にある式を自動的に読みとり, 通常の式に変換することは, フォントの問題を克服すれば可能そうである. それにより, 今回できなかった結果の比較も直接チェックでき, より興味深い考察が可能になるのではないか.

## 参 考 文 献

[1] M. Bézout, Recherches sur le degré des équations résultantes de l'évanouissement des inconnues. M'emoires de l'Académie Royale 288-338 (1764).

[2] D.A. Cox, J.B. Little, D. O'Shea, Using Algebraic Geometry. GTM 185, Springer-Verlag (1999).

[3] B.L. van der Waerden, Algebra. Springer-Verlag (1990).

[4] I.M. Gelfand, M.M.Kapranov, A.V. Zelevinsky, Discriminants, Resultants, and Multidimensional Determinants. Mathematics: Theory and Applications, Birkhäuser (1994).

[5] 関孝和, 建部賢明, 建部賢弘, 大成算経, 二十巻中巻之十九.