Vol. 27 No 4　　情　報　処　理　　Apr. 1986

解　説

多変数連立代数方程式の解法†

小　林　英　恒††

1. はじめに

連立代数方程式の解法として，三つの方法すなわち，グレブナ (Gröbner) 基底による方法，消去法，一般消去法がある．この三方法について解説し，さらに解法の実例を示す．最後に，連立代数方程式を解く上での問題点についてふれる．

2. 問題の設定

多変数連立代数方程式は，変数を消去していくことによって解けることは昔から知られていたが，実際に計算を実行して解を得ることは，今日と違って，昔はほとんどできなかったと言ってよい．実際，古典的な教科書であるファン・デル・ヴェルデンの現代代数学の一般消去法の一頁には，わざわざ「これに関連した実際的な計算は，ひじょうに複雑すぎて現実に実行することは，とても望めない」と脚注がついているほどである．この一般消去法というのは，連立代数方程式の解法の一つであって，われわれはこの解法を中心として，他の二つの解法すなわちグレブナ基底による方法，消去法を合わせて説明する．

まず問題を設定しよう．

有理数体を $\boldsymbol{Q}$ と書き，$\boldsymbol{Q}$ を係数に持つ n 変数 $x_1, \cdots, x_n$ の多項式の全体を $\boldsymbol{Q}[x_1, \cdots, x_n]$ と書く．$f_1, \cdots, f_n$ を $\boldsymbol{Q}[x_1, \cdots, x_n]$ の元とするとき，連立代数方程式

$$f_1 = \cdots = f_n = 0$$

をみたす解を複素数の範囲で全部求めるというのが問題である．

たとえば，連立代数方程式

$$\begin{cases} x^2+y^2+z^2-1=0 \\ xyz+x^3+y^3=0 \\ xy+yz+zx-1=0 \end{cases}$$

が与えられたとき，これをみたす解を複素数の範囲で求めようというのである．ここで複素数の範囲でというのは，解 $(\alpha_1, \alpha_2, \alpha_3)$ において，各 α_i が複素数である場合も許容するということである．

この問に答えるのに，連立代数方程式の持つ固有の性質，計算上の都合もあって，次のようにする．まず，$f_1, \cdots, f_n$ の中に独立でない*ものがあるときは，無限個の解を持つが，この場合は無限個の解を持つという判定をするにとどめる．次に，有限個の解を持つ場合，全部の解を求めるが**，特別な解以外は近似値で複素数の範囲で求める．

3. 解　法

これから述べる三つの解法は，一口で言えば「変数を消去する方法」であるが，具体的にはかなり異なる計算をすることになる．

3.1 グレブナ基底による方法

イデアル，イデアルの基底，グレブナ基底（以下G-基底と略す）なる用語はコンピュータ環論の稿を参照していただきたい．

この方法の鍵になるのは，「辞書式順序でイデアル $(f_1, \cdots, f_n)$ の G-基底を構成すると，1変数多項式を含む G-基底 $\{g_1, \cdots, g_s\}$ が取れる．そのような G-基底が存在しないなら，もともと連立方程式は無限個の解を持つ」という命題である[1]．辞書式順序の定義は後出の例1または定理1の直前を参照して欲しい．

この命題を利用して解が得られることを示すために，まずイデアル $(f_1, \cdots, f_n)$ とは，$h_1, \cdots, h_n$ を任意の多項式として，$h_1f_1+\cdots+h_nf_n$ の形の多項式全体であったことを思い出しておこう．G-基底というのは，$\{f_1, \cdots, f_n\}$ に一定の操作を加えてできる多項式の有限個の集まりであるが，今 $\{g_1, \cdots, g_s\}$ を G-基底とし，g_s が1変数多項式とすると，ある多項式 $h_1, \cdots, h_n$ が存在して，

† Solution of Systems of Algebraic Equations by Hidetsune KOBAYASHI (Dept. of Math. College of Sci. & Technology, Nihon Univ.).

†† 日本大学理工学部数学科

* 正確にはイデアル $(f_1, \cdots, f_n)$ の高さ $<n$

** 1変数代数方程式の全根は求められるものと仮定する．

$g_i=h_1f_1+\cdots+h_nf_n$

と書ける．$(\alpha_1,\cdots,\alpha_n)$ が $f_1=\cdots=f_n=0$ の解だとすれば，上の等式からこれは g_i の零点ともなっている．ところが g_i は，1変数，たとえば x_n の多項式だから，

$g_i(\alpha_1,\cdots,\alpha_n)=g_i(\alpha_n)=0$

となる．つまり解の第 n 番目の座標は1変数代数方程式 $g_i(x_n)=0$ の根でなければならない．このことから，元の連立方程式の第 n 変数に $g_i=0$ の解を代入してできる $n-1$ 変数の方程式を解けば，元の方程式が解けることになる．

例を示そう．

例 1. $f_1=x^2+y^2+x-1$, $f_2=xy+x-1$ とし $f_1=f_2=0$ を解きたい．

これを，$x^ay^b\succ x^{a'}y^{b'}\Leftrightarrow a>a'$ または $a=a'$, $b>b'$ なる辞書式順序で，イデアル (f_1,f_2) の G-基底を求める計算をしてみよう．

$$S_p(f_1,f_2)=yf_1-xf_2=x-x^2+xy-y+y^3$$
$$\downarrow\quad f_1\text{ を加えて}$$
$$y^3+xy-y+y^2+x-1+x$$
$$\downarrow\quad f_2\text{ を引いて}$$
$$y^3+y^2-y+x=f_3\text{ とおく．}$$

計算によって，$S_p(f_1,f_3)\longrightarrow\!\!\!\!\!\rightarrow 0$ ($\longrightarrow\!\!\!\!\!\rightarrow$ は0に簡約できるという意味．コンピュータ環論参照のこと)．また $S_p(f_2,f_3)=-y^4-y^3+y^2+x-1\xrightarrow[-f_3]{}-y^4-2y^3+y-1=f_4$ とおく．作り方から f_4 はイデアル (f_1,f_2) に属すから，連立方程式の解の第2番目の座標は

$y^4+2y^3-y+1=0$

をみたさなければならない．この方程式の根を $\beta_1,\cdots,\beta_4$ とおき，これらを f_2 に代入すると，

$x=1/(\beta_i+1)$　　$(\beta_i\neq 1$ のとき$)$

が得られる．あとは，このようにして得られた解 (x,y) が，実際に方程式の解になっていることを確かめておけばよい．例を終る．

この方法が正しいことを示す鍵になるのは次の定理1である．

$x_1^{a_1}x_2^{a_2}\cdots x_n^{a_n}\succ x_1^{b_1}x_2^{b_2}\cdots x_n^{b_n}$ は，ある $i(1\leqq i\leqq n)$ が存在し $j<i$ に対しては，$a_j=b_j$, $a_i>b_i$ となるときとする．この順序 $\succ$ は辞書式順序と呼ばれるが，この順序で考えて

定理 1　F がイデアル (F) のグレブナ基底なら，

$$(F)\cap\boldsymbol{Q}[x_i,\cdots,x_n]=\{F\cap\boldsymbol{Q}[x_i,\cdots,x_n]\}\cdot\boldsymbol{Q}[x_i,\cdots,x_n]$$

が，$i=1,\cdots,n$ に対して成り立つ．

この定理によって

$$(F)\cap\boldsymbol{Q}[x_n]=\{F\cap\boldsymbol{Q}[x_n]\}\cdot\boldsymbol{Q}[x_n]$$

だから，与えられた連立方程式が有限個の解をもつなら，次の **3.2** に示す消去法から $(F)\cap\boldsymbol{Q}[x_n]\neq\phi$ が分かるから，定理の等式に当てはめれば，F の中に x_n のみを変数とする多項式が含まれる．無限個の解を持つ場合，$x_1,\cdots,x_n$ の順を変えて同様の操作をやれば，ある x_i のみを変数とする多項式が G-基底に含まれない．

この方法は，与えられた連立代数方程式の二つの式におのおの適当な単項式を掛けて足し引きして，余分な項を消して変数を消去していくわけで，筆算でよくやる方法の一般化となっている．

3.2 消 去 法

次に消去法による方法を示そう．ここでいう消去法とは狭い意味で変数を一個ずつ減らしていく方法のことを言う．

二つの多項式 f, $g\in\boldsymbol{Q}[x_1,\cdots,x_n]$ が与えられたとき，まずこれらを

$$f=a_0(x_1,\cdots,x_{n-1})x_n^{\,l}+\cdots+a_l(x_1,\cdots,x_{n-1}),$$
$$g=b_0(x_1,\cdots,x_{n-1})x_n^{\,m}+\cdots+b_m(x_1,\cdots,x_{n-1})$$

と書きなおす．

次に行列式

$$\left.\begin{matrix}m\\ \\ \\ \\ n\\ \\ \\ \\ \end{matrix}\right\{\begin{vmatrix} a_0 & a_1\cdots\cdots a_l & & \\ & a_0 & a_1\cdots a_l & 0 \\ & \cdots\cdots\cdots & \ddots & \\ 0 & \cdots\cdots a_0 & a_1\cdots & a_l \\ b_0 & b_1\cdots\cdots b_m & & \\ & b_0 & b_1\cdots b_m & 0 \\ & \ddots & \ddots & \ddots \\ 0 & & b_0 & b_1\cdots b_m \end{vmatrix}=R(f,g)$$

の最後の列の余因子を $\delta_1,\cdots,\delta_{l+m}$ とおくと，

$$(\delta_1x^{m-1}+\delta_2x^{m-2}+\cdots+\delta_l)f$$
$$+(\delta_{l+1}x^{l-1}+\delta_{l+2}x^{l-2}+\cdots+\delta_{l+m})g=R(f,g)$$

となることが分かる．この式から $f(\alpha_1,\cdots,\alpha_n)=g(\alpha_1,\cdots,\alpha_n)=0$ なら，$R(f,g)(\alpha_1,\cdots,\alpha_n)=0$ でなければならないことが分かる．ところで，この $R(f,g)$ は $x_1,\cdots,x_{n-1}$ の多項式なので，与えられた f, g より変数が一つ少なくなっている．逆に $R(f,g)(\alpha_1,\cdots,\alpha_{n-1})=0$ のとき，$a_0(\alpha_1,\cdots,\alpha_{n-1})\neq 0$ または $b_0(\alpha_1,\cdots,\alpha_{n-1})\neq 0$ ならば，複素数 α_n で，$(\alpha_1,\cdots,\alpha_{n-1},\alpha_n)$ が，$f=g=0$ の共通根となるものが存在することが分かっているから，$R(f,g)=0$ の解から $f=g=0$ の解が与えられると思ってよい．$R(f,g)$ が恒等的に0なら $f=g=0$ の共通根は無限個存在する．

以上のことを使って，多変数連立代数方程式を解くには，適当に方程式を対にして上述の $R(f,g)$ を計算し変数を消去していけばよいということになる．前の例を消去法で解いてみよう．

例 2. $f_1=x^2+x+y^2-1$, $f_2=(y+1)x-1$.

$$R(f_1,f_2)=\begin{vmatrix}(y+1) & -1 & 0\\ 0 & (y+1) & -1\\ 1 & 1 & y^2-1\end{vmatrix}$$
$$=y^4+2y^3-y+1$$

これで前の例と同じ式が得られた．例終り．

行列式の計算は数値のみを要素に持つ場合と違って，数式を要素に持つ場合，現在ひいき目にみてもサイズ 20×20 の行列の行列式が求め得る最大のものと言ってよいであろう．したがって行列式の計算にはうまい工夫が必要である．その一つとして，次の方法がある[4]．

佐々木，金田，渡辺の方法

$f=a_0x^n+a_1x^{n-1}+\cdots+a_n$,

$g=b_0x^m+b_1x^{m-1}+\cdots+b_m$

が与えられたとする．$n>m$ とする．

$b_0^{n-m}f=q\cdot xg+\hat{f}$, $\deg(\hat{f})\leqq m$

と割り算した上で，

$$R(\hat{f},g)=\begin{vmatrix}\underbrace{A}_{m} & \underbrace{B}_{m}\end{vmatrix}\Big)m$$
$$\begin{vmatrix}\underbrace{C}_{m} & \underbrace{D}_{m}\end{vmatrix}\Big)m$$

と書く．すると，$R(\hat{f},g)=|A\cdot D-B\cdot C|$ となる．また

$R(\hat{f},g)=(-1)^{(n-m)m}b_0^{(n-m)(m-1)}R(f,g)$

なる関係が成立する．

以上二つの解法は，一度1変数代数方程式を解いてそれを元の式（あるいは元の式から引き出された式）に代入するのだから，近似解で済ませる限り，上記の例のように2変数の場合はともかく，変数が多くなると誤差が積もってしまうことは避けられない．

計算を実行することは困難でほとんど不可能なのだが，$\boldsymbol{Q}$ の有限次代数拡大体 K を一つ固定すると，K の元を係数にもつ多項式を因数分解するアルゴリズムは知られている[5]．このことから，連立代数方程式が有限個の解を持つ場合，どの解も $\boldsymbol{Q}$ 上代数的だから，十分大きな $\boldsymbol{Q}$ の拡大体上で各変数に関する1変数の方程式（変数を消去して得られる最終の式のこと）は，1次因子に完全に分解する．したがって完全に正確な解が求められるということになるが，実際には現在の計算機の記憶容量では，このような正確な解が得られる連立代数方程式は簡単な場合に限られる．

3.3 一般消去法

これまでに説明した二つの方法は，解の重複度に関する情報は与えない．ここに解の重複度とは，1変数代数方程式の2重根，3重根といった解の重複度の概念を多変数の場合に拡張したものであり，この概念を使って方程式の次数と解の個数に関するベズー (Bezout) の定理が示される．

この節は，**3.3.1** と **3.3.2** に分け，**3.3.1** では一般消去法の理論を紹介し，**3.3.2** で簡単な例を具体的に解くことによって実際のアルゴリズムを示すことにしたい．

3.3.1 で U-終結式 $D(U)$ なるものが定義され，この $D(U)$ は

$\Pi_i(a_{0i}U_0+\cdots+a_{ni}U_n)$

と書ける．このとき，$(a_{0i},\cdots,a_{ni})$ が与えられた方程式を斉次化したものの解となる．

3.3.1 一般消去法の理論

定理 2 $f_1,\cdots,f_r$ は1変数の多項式で，各多項式の係数は文字であるとする．このとき，これら係数として現れる文字の多項式 $D_1,\cdots,D_h$ が存在して，次のことが成立する：

多項式 $f_1,\cdots,f_r$ の係数の文字に有理数を割り当ててできる r 個の有理数係数の多項式を0と等しいとおいてできる連立方程式が共通根を持つか，あるいはどの多項式の最高次の係数も0となるためには，割り当てた値が $D_1=\cdots=D_h=0$ を満たすことが必要十分条件である．

この定理を n 変数 $x_1,\cdots,x_n$ の有理数を係数とする多項式に当てはめるとすれば，一つの変数，たとえば x_1 を主変数とし，各係数は $x_2,\cdots,x_n$ の多項式とみれば，$D_1,\cdots,D_h$ は $x_2,\cdots,x_n$ の多項式だから，元の連立方程式を解くことが一つ変数の個数が減った連立方程式を解くことに帰着されることが分かる．

しかし一般消去法はこの程度では満足しない．まず，後の議論の基本となる多項式の斉次化を説明しよう．$f(x_1,\cdots,x_n)$ が与えられた多項式とするとき，$F(X_0,\cdots,X_n)=X_0^r\cdot f(X_1/X_0,\cdots,X_n/X_0)$, $r=\deg(f)$, を f の斉次化という．実際 $F(X_0,\cdots,X_n)$ は斉次多項式となっていて，しかも $F(1,X_1,\cdots,X_n)=f(X_1,\cdots,X_n)$ である．ここに，$(X_0,\cdots,X_n)$ は斉次座標と呼ばれ，連比で点を表す座標で，

$x_1=X_1/X_0,\cdots,x_n=X_n/X_0$, $(X_0\neq 0)$

となっているものとする．

この斉次多項式 $F(X_0,\cdots,X_n)$ は

$F(tx_0, \cdots, tx_n)=t^r F(x_0, \cdots, x_n)$, $(r=\deg F)$,

を満たすから，$a_0, \cdots, a_n$ が $a_0 \neq 0$ であって，$F(a_0, \cdots, a_n)=0$ を満たすときは，

$F(1, a_1/a_0, \cdots, a_n/a_0)=f(a_1/a_0, \cdots, a_n/a_0)=0$

となる．また $F(0, \cdots, 0)=0$ だが，この $(0, \cdots, 0)$ は F の自明な解と呼ばれる．

このような斉次多項式 $F_1, , \cdots, F_r$ から決まる連立代数方程式 $F_1=\cdots=F_r=0$ の場合，定理2から次の定理が導かれる．

定理 3　$F_1, \cdots, F_r$ を X_0 を主変数とする多項式とみると，$X_1, \cdots, X_n$ を変数とする斉次多項式 $D_1, \cdots, D_h$ が存在して，$F_1=\cdots=F_r=0$ の自明でない解が存在することと $D_1=\cdots=D_h=0$ の自明でない解が存在することとが同値となる．

この定理では，前の定理2の形式的な最高次の項が実際に割り当てた有理数の値によって0になるかどうかに関する議論が不必要になっている．また，この定理から変数を順に消去していくと，$F_1, \cdots, F_r$ の係数を文字とすると，これらの文字の多項式 $b_1, \cdots, b_k$ が存在し，$F_1, \cdots, F_r$ の係数に有理数を割り当てたとき $b_1=\cdots=b_k=0$ となることと，$F_1=\cdots=F_r=0$ の自明でない解が存在することが同値となる．

実は，定理3を用いて順に変数を消去していくと最後にできるのは，

$b_1 X_n^{l_1}, \cdots, b_k X_n^{l_k}$

であり，これらが自明でない共通解を持つためには $b_1=\cdots=b_k=0$ となることが必要十分となるのである．

ここで変数を消去する方法は，前の消去法とほとんど同じ方法を用いるのであり，消去法のときと同様に $b_1 x_n^{l_1}, \cdots, b_k x_n^{l_k}$ はすべてイデアル $(F_1, \cdots, F_r)$ に属す．

一般に多項式 F がイデアル $(F_1, \cdots, F_r)$ に属することを，

$F \equiv 0 \ (F_1, \cdots, F_r)$

と書くが，この書き方に従えば

$b_1 x_n^{l_1} \equiv 0 \ (F_1, \cdots, F_r)$

と書ける．

上記では $F_1, \cdots, F_r$ の係数は単なる文字と考え，$b_1, \cdots, b_k$ はこれらの文字の多項式だった．いましばらく $F_1, \cdots, F_r$ の係数は文字だとする立場を続ける．

$F_1, \cdots, F_r$ の係数を変数とする多項式 T で

$T \cdot x_1^{\tau} \equiv 0 \ (F_1, \cdots, F_r)$　　(τ:自然数)

なる性質を持つものを惰性形式という．このような $F_1, \cdots, F_r$ に関する惰性形式すべてからなる集合を $\mathfrak{T}$ とおくと，$\mathfrak{T}$ に関して次の重要な定理が成り立つ．

定理 4　$F_0, \cdots, F_n$ を $X_0, \cdots, X_n$ の斉次多項式で，各係数は文字とする．$F_0, \cdots, F_n$ の惰性形式すべてからなる集合を $\mathfrak{T}$ とおく．このとき，$\mathfrak{T}$ は一つの多項式 R で生成される素イデアルである．

この R は，$F_0, \cdots, F_n$ の係数の文字を変数とする多項式だが，与えられた $F_0, \cdots, F_n$ の終結式と呼ばれる．

これで理論の紹介はほぼ終った．次にいよいよ最終の定理を示すことにするが，まず前処理をしておこう．

$f_1=f_2=\cdots=f_n=0$ が n 変数 $x_1, \cdots, x_n$ の有理数を係数とする連立代数方程式とする．これらを斉次座標 $(X_0, \cdots, X_n)$, $(x_i=X_i/X_0)$ で斉次化したものを $F_1, \cdots, F_n$ とする．$U_0, \cdots, U_n$ を別の変数とし，$L=U_0X_0+\cdots+U_nX_n$ とする．

$F_1, \cdots, F_n$ の各係数を文字で置き換え，$F_1, \cdots, F_n$, L の終結式を計算する．するとこの終結式はこれらの文字および $U_0, \cdots, U_n$ の多項式となるが，この多項式の文字に対応するもともとの有理数を代入してできる $U_0, \cdots, U_n$ の多項式を $D(U_0, \cdots, U_n)$ $(=D(U)$ と略記) とおく．この $D(U)$ は U-終結式と呼ばれている．

定理 5　$D(U)$ は，$F_1, \cdots, F_n, L$ の U 終結式とするとき，$D(U) \neq 0$ なら

$$D(U_0, \cdots, U_n) = \prod_{j=1}^{M} (a_{j0}U_0+\cdots+a_{jn}U_n), (a_{j*} \in \boldsymbol{C}, \ {}^{\forall}j)$$

となり，$(a_{j0}, \cdots, a_{jn})$ は $F_1, \cdots, F_n$ の共通零点であり，逆に $F_1, \cdots, F_n$ の自明でない共通零点はすべてこの積記号の中に表れる．ここで $M=(\deg F_1)\times\cdots\times(\deg F_n)$ である．また，積記号の中に $(a_{j0}, \cdots, a_{jn})$ が l 回表れる場合，$(a_{j0}, \cdots, a_{jn})$ の $F_1=\cdots=F_n=0$ の解としての重複度は l である．

上の定理で，$D(U) \equiv 0$ となる場合は，$F_1=\cdots=F_n=0$ が無限個の解を持つ場合で，このとき $f_1=\cdots=f_n=0$ が無限個の解を持つか否かは容易に判定できる．

この定理から，元の方程式の解は，

$(a_{j1}/a_{j0}, \cdots, a_{jn}/a_{j0})$, $(a_{j0} \neq 0)$

で与えられるとともに，この解も求められることが分かる．$a_{j0}=0$ の場合は無限遠解と呼ばれ元の方程式とは無関係と思ってよい．

これで，一般消去法の理論の紹介は終った．

3.3.2

ここから，具体的に $D(U)$ をどう計算するのか，

また $D(U)$ が求められたとして，どうすればその1次因子が求まるのかを説明したい．

$D(U)$ を求めるのに現在知られている最良のアルゴリズムはラザール (D. Lazard) の方法である[3]．この方法は理論的には斉次の場合のヒルベルトの零点定理を用いて解釈すれば分かりよいが，その理論を紹介するのは面倒なので，具体的に簡単な例を用いてその方法を4つの段に分けて示すことにする．

与えられた連立代数方程式は前の二つの方法の例と同じく，

$$\begin{cases} f_1 = x^2+y^2+x-1=0 \\ f_2 = xy+x-1=0 \end{cases}$$

↗とする．

第一段，f_1, f_2 を斉次化し，L を付け加える：

$$F_1 = X_0^2 \cdot f_1(X_1/X_0, X_2/X_0)$$
$$= X_1^2+X_2^2+X_0X_1-X_0^2,$$
$$F_2 = X_0^2 \cdot f_2(X_1/X_0, X_2/X_0) = X_1X_2+X_0X_1-X_0^2,$$
$$L = UX_0+VX_1+WX_2.$$

$d=(\deg F_1-1)+(\deg F_2-1)+1=3$ 次の X_0, X_1, X_2 に関する単項式を適当な順に縦に並べる．次に，$d-\deg F_1=1$ 次の単項式の一つ X_0 を F_1 に掛けて，各項の係数を次に示す行列の外側の単項式の列を参照して並べる．これを X_1F_1, X_2F_1, X_0F_2, X_1F_2, X_2F_2, $X_1^2L, X_1X_2L, \cdots, X_2^2L$ に関して繰返す．

	X_0F_1	X_1F_1	X_2F_1	X_0F_2	X_1F_2	X_2F_2	$(X_2^2,$	$X_0X_1,$	$X_0X_2,$	$X_1^2,$	$X_1X_2,$	$X_2^2)\times L$
X_0^3	−1	0	0	−1	0	0	U	0	0	0	0	0
$X_0^2X_1$	1	−1	0	1	−1	0	V	U	0	0	0	0
$X_0^2X_2$	0	0	−1	0	0	−1	W	0	U	0	0	0
$X_0X_1^2$	1	1	0	0	1	0	0	V	0	U	0	0
$X_0X_1X_2$	0	0	1	1	0	1	0	W	V	0	U	0
$X_0X_2^2$	1	0	0	0	0	0	0	0	W	0	0	U
X_1^3	0	1	0	0	0	0	0	0	0	V	0	0
$X_1^2X_2$	0	0	1	0	1	0	0	0	0	W	V	0
$X_1X_2^2$	0	1	0	0	0	1	0	0	0	0	W	V
X_2^3	0	0	1	0	0	0	0	0	0	0	0	W

第二段，掃き出し法で次のように整理する．

$$\begin{pmatrix} 1 & & & * & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & 2U+V+W & U+V+W & U+V & U & U & 0 \\ & & & -U-V & -U-V & W & -U & 0 & U \\ & 0 & & U+V+W & U & U & W & V+W & V \\ & & & -U-V & -U & 0 & -V-W & -V & W \end{pmatrix}$$

第三段，右下の 4×6 行列は

$$\begin{pmatrix} U & U+V+W & U+V & 0 & 0 & 0 \\ 0 & -U-V & W & -U & 0 & 0 \\ W & 0 & U & -V & 0 & 0 \\ -V & -U & 0 & -W & 0 & 0 \end{pmatrix}$$

と変形できる．

第四段，上の行列の第5，第6列を取り去ってできる 4×4 行列の行列式が求める U-終結式である．

今の場合，U-終結式は

$$-UV^2W-UW^3-VW^3+4U^2VW+\cdots-W^4$$

となる．

一般の場合には，前記の行列としては縦に $d=\sum_{i=1}^{n}(\deg F_i-1)+1$ 次の単項式を並べ，各列は $(d-\deg F_i)$ 次の単項式を F_i に掛けたときの係数，および $(d-1)$ 次単項式を Lに掛けたときの係数で構成すればよい．最終的に行列式を求めるところでは，もう少し工夫↗

↘がしてあるのだが，基本的には，今やったのと同様である．これでラザールの方法についての説明を終る．

すでに説明したように，第4段で得られた U-終結式を D とおくと，a_{ij} は複素数として

$$D=(a_{10}U+a_1V+a_{12}W)$$
$$\times\cdots\times(a_{40}U+a_{41}V+a_{42}W)$$
$$=\prod_{j=1}^{4}(a_{j0}U+a_{j1}V+a_{j2}W)$$

となり，このとき (a_{j0}, a_{j1}, a_{j2}) が $F_1=F_2=0$ の解となる．今，たとえば $a_{10}\neq 0$ なら

$$0=F_1(a_{10}, a_{11}, a_{12})=a_{10}^2F_1(1, a_{11}/a_{10}, a_{12}/a_{10})$$

だから，$F_1(1, a_{11}/a_{10}, a_{12}/a_{10})=f_1(a_{11}/a_{10}, a_{12}/a_{10})=0$ となって，元の方程式の解が求まるというしくみになっている．

さて，U-終結式は，ラザールの方法の第4段で示したように，そのままでは

$$\Pi(a_{j0}U+a_{j1}V+a_{j2}W)$$

の形をしてはいない．そこで，このような複素数の組 (a_{j0}, a_{j1}, a_{j2}) を求めることが必要となる．その方法として，筆者の提案した次の方法がある．その基本的な考えは，U-終結式を $D(U)$ とおくと，$D(U)=0$ をみたす図形は複素射影空間内でいくつかの超平面から

なっているから，ある直線とこの図形との交点を求めて，各交点で接平面あるいは接錐を求めれば，結局 $D(U)=0$ を構成する超平面が得られるというものである．このことを，今の例に当てはめてみよう．

(U, V, W) を座標とする複素3次元空間の平面 $U=1$ 上で考えると，

$$D(1, V, W)=0$$

は，重複も考えて高々4本 $(=(\deg f_1)\times(\deg f_2))$ の直線 $l_1, l_2, , l_3, l_4$ を決定する．

そこで，適当な直線 l を図-1 のようにとれば，重複度も考えに入れて高々4個の図 $(D=0)$ との交点が存在する．

交点を与える式は，$l=(\alpha t, \beta t)$ とすると，

$$D(1, \alpha t, \beta t)=0$$

となって，(α, β) を決めておけば，1変数代数方程式となっている．細かく言うと交点のとり方によってはうまく接平面が計算されない場合があるし，さらに悪い場合には直線をどんなに選んでも接平面を計算できないことがあるが，この2点は，次のように解決することができる．

まず，図-2 のように，交点が図 $(D=0)$ を構成する二つ以上の直線の交点を通る場合．この場合は，l の十分近くに l と1次独立な直線を引けば，このような交点を避けることができる．最初からこのような点を避けられるわけではないが，一度解を求めて，その解が適切か否かを試してみればよく，一般の変数が多い場合でも，必ず高々変数の個数と同じ回数の試みで，このような点を避けるような直線が選べる．

次に，直線をどう選ぼうとも接平面が求められないのは，図-3 のように，たとえば l_1 と l_2 とが重なっている場合である．このときは，点Pでの接錐は，$(a+bV+cW)^r$ の形をしているから，$D(1, \alpha t, \beta t)=0$ の解として点Pは r 重根になっているので，この r さ

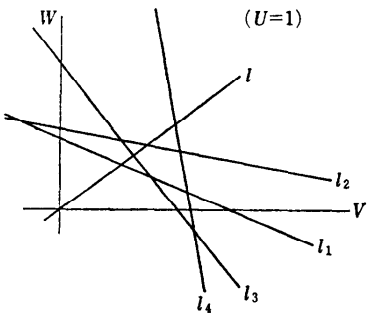

図-1

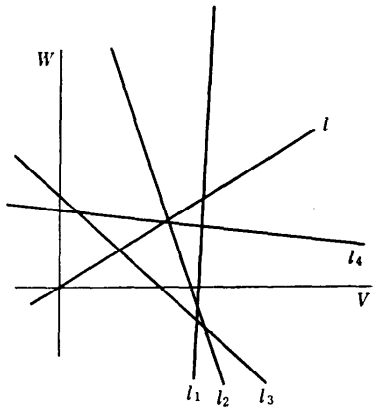

図-2

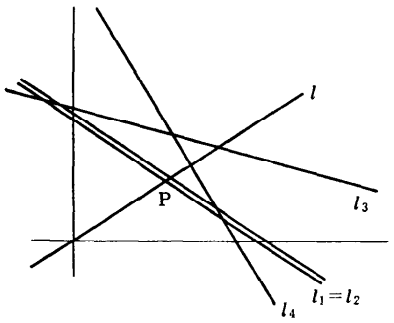

図-3

え正確に求めておけば次に示すように，(a, b, c) は求まる．

まず，点Pが良い点で，図-3 $(D=0)$ への接線が求まる場合には，求める接線は

$$\frac{\partial D}{\partial U}(P)\cdot U+\frac{\partial D}{\partial V}(P)\cdot V-\frac{\partial D}{\partial W}(P)\cdot W=0$$

で与えられる．Pが図-3 のように r 重根の場合には，点Pでの接錐の式は射影空間で考えて $(aU+bV+cW)^r$ となっているから，

$$a=\frac{1}{r!}\frac{\partial^r D}{\partial U^r}(P)$$

で与えられる．b, c も同様にして容易に求まる．

以上をまとめると，一般消去法によるアルゴリズムは，次のようになる．

A1　連立代数方程式 $f_1=\cdots=f_n=0$ の各 f_i を斉次化し，それを F_i とおく．

A2　$U_0, \cdots, U_n$ を変数とし，$L=U_0X_0+\cdots+U_nX_n$ とおく．

A3　$F_1, \cdots, F_n, L$ の U-終結式をラザールの方法

で求める.

A4 筆者の方法で, U-終結式の1次因子を得る.

これに従って, 前記の例を解くと次のようになる. ISIT (1, 1) は一番目の方程式に一番目の解を代入した値である.

```
ALGEQ(1)=X**2+Y**2+X-1
ALGEQ(2)=X*Y+X-1
.....
X=1.0537558*I-1.1219644
Y=-4.447718E-1*I-1.4735615
.....
X=-1.0537558*I-1.1219644
Y=4.447718E-1*I-1.4735615
.....
X=1.877304E-1*I+6.219644E-1
Y=-4.447718E-1*I+4.735615E-1
.....
X=-1.877304E-1*I+6.219644E-1
Y=4.447718E-1*I+4.735615E-1
.....
ISIT(1,1)=1.37443623E-8*I-3.09592714E-8
ISIT(2,1)=-5.15577792E-8*I+8.13703821E-9
```

4. 一般消去法で解いた例の説明

付録として, 一般消去法で解いた例を載せるが, これの説明をしよう.

一般消去法による解法のプログラムは藤瀬哲朗氏(現在三菱総研に所属) が大学院生のときに作成したもので, ほとんどの部分が REDUCE (及び RLISP) で書かれている. 一部分 FORTRAN で書かれているが, それは, 1次因子を求める際に, 1変数代数方程式を数値的に解くところである. この部分の数値解法のアルゴリズムは D.K.A. 法である. 計算は日大理工数学科の日立 M 240D で行われた.

例3では, 最初の F_1, F_2, F_3 (3章の説明では f_1, f_2, f_3 となっていたもの) が, 与えられた方程式であり, LINE $T*(1,0,0)$ は U-終結式の1次因子を求めるためにとった直線である. この例では原点は解であるが, その重複度は正確に8である. ほかに 10 組の解が求まっている. 解は, ベズーの定理から $3\times2\times3=18$ 個あるはずで, 実際に, $8+10=18$ 個の解が得られている. 今の例では無限遠解は一つもない. ISIT(1, 1) は第1番目の解を F_1 に代入して得られた値である. しかし, 今の場合には, この値はあまりにも大きく, 第1番目の解はとても解と呼べるしろものではないことが分かる. 実は, これは直線 $t(1,0,0)$ の取り方が悪かったからで, 次の例4では前例と同じ連立代数方程式に対して直線を取り直して, $t(1,1,1)$ とすると良い解が得られることが分かる.

5. 問 題 点

連立方程式を解く上での問題点は大雑把に言って次の二つにまとめることができよう.

1. 変数の個数や次数が大きくなると, 計算量が膨大になり, 計算不可能となる.

2. 無限個の解を持つ場合どのようにしたら良いか.

問題点1は, たとえば与えられた方程式系が5変数, 各3次の多項式からなるとしよう. すると, 解は最も多い場合 243 個存在する. この解を得るためには, 243×243 次の文字を要素とする行列式の計算を行わなければならないが, 通常どんなにくふうしても, このような行列式は計算できない. このような大きい系に対しては, 現在グレブナ基底による方法が有効だとされているが, この方法は1変数代数方程式の数値解を元の方程式に代入して変数を減らすか, 各変数についての1変数代数方程式を作り, それらから得られる数値解を組み合わせて解を得るかのどちらかであるから, 結局, 解の個数がいくつかといった問に対してすら確実な答を与えない.

問題点2については, 局所表示を求めることになるだろうが, まだ体系的には手が付けられていない.

また, 問題点1, 2の両方に有効な方法として, イデアルの準素分解があるが, これを含めて, 環論のいろいろな性質をコンピュータにのせることができるかどうか, 現在研究が進められている.

参 考 文 献

1) Buchberger, B.: A Survey on the Method of Groebner Bases for Solving Problems in Connecttion with Systems of Multi-variate Polynomials, Proc. of RSYMSAC pp. 7-1〜7-15 (1984).
2) Fujise, T., Kobayashi, H. and Furukawa, A.: Solving Algebraic Equations by General Elimination Method, Submitted to Jorn. of Symb. Computation.
3) Lazard, D.: Résolutions des Systèmes d'Equations Algébriques, Theoretical Computer Science 15 pp. 77-110 (1981).
4) Sasaki, T., Kanada, Y. and Watanabe, S.: Calculation of Discriminants of High Degree Equations, Tokyo Journ. of Math. Vol. 4, No. 2, pp. 493-500 (1981).
5) Lenstra, A.K.: Factoring Polynomials over Algebraic Number Fields, Eurocal '83 Lecture Notes in Computer Sci. 162, Springer.
6) Van der Waerden, B.L.: Moderne Algebra

(銀林浩訳，ファン・デル・ヴェルデン：現代代数学，東京図書)．

付　録

例 3

```
ALGEQ(1)=X*Y**2-Z**2
ALGEQ(2)=X**2+Y**2-Z**2
ALGEQ(3)=X*Y+X**3+Y**3
LINE T*(1,0,0)
ORIGIN IS 8-UPLE ROOT
.....
X=1.69E-5*I+2.3537494
Y=-1.72E-5*I-2.0229495
Z=0
.....
X=1.2471492*I-1.857771E-1
Y=5.050074E-1*I+8.178292E-1
Z=0
.....
X=1.2471548*I-1.857925E-1
Y=5.050139E-1*I+8.178325E-1
Z=0
.....
X=-1.69E-5*I+2.3538114
Y=1.72E-5*I-2.0230128
Z=0
.....
X=-1.2471548*I-1.857889E-1
Y=-5.050123E-1*I+8.178323E-1
Z=0
.....
X=-1.2471492*I-1.857807E-1
Y=-5.050089E-1*I+8.178294E-1
Z=0
.....
X=-9.07564E-2*I+5.089023E-1
Y=7.052947E-1*I+1.936408E-1
Z=0
.....
X=-9.08224E-2*I+5.088868E-1
Y=7.054385E-1*I+1.936786E-1
Z=0
.....
X=9.07865E-2*I+5.089272E-1
Y=-7.053621E-1*I+1.93588E-1
Z=0
.....
X=9.07923E-2*I+5.088619E-1
Y=-7.05371E-1*I+1.937314E-1
Z=0
.....
ISIT(1,1)=2.32956443E-4*I+9.63230676
ISIT(2,1)=1.49146193E-4*I+9.63246092
ISIT(3,1)=-4.95138243E-6*I+1.00099918E-5
```

例 4

```
ALGEQ(1)=X*Y**2-Z**2
ALGEQ(2)=X**2+Y**2-Z**2
ALGEQ(3)=X*Y+X**3+Y**3
LINE T*(1,1,1)
ORIGIN IS 8-UPLE ROOT
.....
X=-1.247152*I-1.857848E-1
Y=-5.050106E-1*I+8.178309E-1
Z=-1.0658324*I+1.701125E-1
.....
X=2.3537804
Y=(-2.0229811)
Z=3.1036648
.....
X=1.247152*I-1.857848E-1
Y=5.050106E-1*I+8.178309E-1
Z=-1.0658324*I-1.701125E-1
.....
X=-9.07894E-2*I+5.088946E-1
Y=7.053666E-1*I+1.936597E-1
Z=4.928936E-1*I+1.834044E-1
.....
X=1.247152*I-1.857848E-1
Y=5.050106E-1*I+8.178309E-1
Z=1.0658324*I+1.701125E-1
.....
X=9.07894E-2*I+5.088946E-1
Y=-7.053666E-1*I+1.936597E-1
Z=-4.928936E-1*I+1.834044E-1
.....
X=2.3537804
Y=(-2.0229811)
Z=(-3.1036648)
.....
X=-1.247152*I-1.857848E-1
Y=-5.050106E-1*I+8.178309E-1
Z=1.0658324*I-1.701125E-1
.....
X=9.07894E-2*I+5.088946E-1
Y=-7.053666E-1*I+1.936597E-1
Z=4.928936E-1*I-1.834044E-1
.....
X=-9.07894E-2*I+5.088946E-1
Y=7.053666E-1*I+1.936597E-1
Z=-4.928936E-1*I-1.834044E-1
.....
ISIT(1,1)=-5.28311102E-8*I-1.37185143E-7
ISIT(2,1)=5.10541193E-8*I-2.07699968E-9
ISIT(3,1)=-1.37358485E-7*I+1.43151596E-7
```

(昭和 60 年 12 月 4 日受付)