数理解析研究所講究録
第520巻 1984年 1-22



# 連立代数方程式のある種の解法について
## － 代数的・数値的算法による全解構成法 －

電気通信大学 電気通信学部 情報数理工学科
藤瀬 哲朗(Tetsuro Fujise)†
日本大学 理工学部 数学科
小林 英恒(Hidetsune Kobayashi)

## §1 動機

数式処理系において項関係規則が存在する下で多項式の canonical form を定めるためには，Gröbner-bases などによる代数的変形法[2]が用いられる．ところが，項関係規則は別の見方をすれば連立代数方程式ともみなせるわけであり，実際に解いて近似的に canonical form を求めることも考えられる．例えば，

$$xy=10,\ y-1=4$$

とすると

$$x=2,\ y=5$$

となって

$$xy-x=x(y-1)=8$$

と canonical form を定めることができる．この場合には簡単に方程式の解が求まったのだが，実際には難しい．方程式が有限個の解をもつならば，Bézout の定理[11]より解の個数が無限遠の解及び重複度も含めて方程式の次数の積に等しくなる性質をもつために canonical form は数個存在することが知られている．そのために例えばよく用いられるNewton- Rapson 法[4]により全解を求めることは難しい．これに対し有理数体$\mathbb{Q}$上の解をすべて計算する方法として Van der Waerden (以後 VdWと略す)の消去法[11]の利用がある．これは VdW のU-終結式を計算し，それを$\mathbb{Q}$上で因数分解した結果を用いる方法である．ところがこれは[11]の注釈にあるように“これに関連した実際的計算法は非常に複雑すぎて，現実に実行することなどはとても望めない”方法である．最近 Lazardによりこの U-終結式を modernな方法[7,8]で計算することが提案され，この注釈を修正可能とした(計算機が進歩したためでもある)．ところでこのU-終結式を係数体の代数的閉体上で因数分解すれば，その因子から元の方程式系のすべての解を求められることが知られている．そこでここでは初等幾何的性質を利用して複素数体$\mathbb{C}$上で数値的に因数分解し，その全解を求め

† 現在，(株)三菱総合研究所．

る方法を構築する．そして実際に計算機にimplementする．§２,３ではこのLazard の方法を説明する．§４ではこれを数値的に解く方法を述べ，§５以降でこの implementation と計算例及び問題点について述べる.つまり記号計算のための基礎理論を動機として代数的･数値的ハイブリッド算法を使った連立代数方程式の解法を述べる．

§2 Lazard の方法(基本定理)

n元連立代数方程式

$$(1)\quad \begin{cases} f_0(x_1,\cdots,x_n)=0 \\ \quad\cdots \\ f_{n-1}(x_1,\cdots,x_n)=0, \quad f_i \in K[x_1,\cdots,x_n], \quad K:\text{体} \end{cases}$$

が有限個の解を持つとき，そのすべての解を多重度も含めて求める．なおこの論文ではKをQもしくはQの拡大体と制限することにする.†

さて,この節では(1)の解を計算するための基本定理を示す．証明は Lazard [ 6,8 ], Kaplansky[5]を参照.

定義2.1

$B \equiv K[x_1,\cdots,x_n]/(f_0,\cdots,f_{n-1})$,

L : Kの拡大体,

$B_L \equiv L \otimes_K B = L[x_1,\cdots,x_n]/(f_0,\cdots,f_{n-1})$.

定理2.1

以下の条件は同値である．

(ｉ) (1)はKの代数的閉体K中に有限個の解をもつ

(ii) (1)はKのすべての拡大体Lに対してL中に有限個の解をもつ.

(iii) 環BはK上の有限次元ベクトル空間である.

ここで代数的性質を利用するために(1)を次のように変形する： deg $f_i$ を $f_i$の全次数とするとき,(1)の方程式系を同次化( homogenize )して

$$d_i \equiv \deg f_i,\quad F_i(x_0,\cdots,x_n) \equiv x_0^{d_i} f_i\left(\frac{x_1}{x_0},\cdots,\frac{x_n}{x_0}\right),$$

$$(2)\quad \begin{cases} F_0(x_0,\cdots,x_n)=0, \\ \quad\cdots \\ F_{n-1}(x_0,\cdots,x_n)=0, \quad F_i \in K[x_0,\cdots,x_n] \end{cases}$$

とする($F_i(1,x_1,\cdots,x_n)=f_i(x_1,\cdots,x_n)$ となることに注意する).以下この(2)

† [ 9 ]では有限体上の解も計算できる.また,方程式の数が変数の数よりも少くても計算可能である.

の方程式系の射影空間上での解を求めることを考える.さて(1)と同様に$F_i$から生成される ideal によって n+1 変数の多項式環の次数つき剰余環

$$A \equiv K[x_0,\cdots,x_n]/(F_0,\cdots,F_{n-1}),$$

$$A_L \equiv L \otimes_K A = L[x_0,\cdots,x_n]/(F_0,\cdots,F_{n-1})$$

を考える.このときAを(2)の環,もしくは(1)の次数つき環と呼ぶ.次数つき環または加群Xに対して,$X^d$をd次の要素からなる集合とする(例えば$A=\oplus_i A^i$となる).

定理2.2

以下の条件は同値である.

(i) (1)はKの代数的閉体$\bar{K}$中に有限個の射影解をもつ.

(ii) (1)はKのすべての拡大体Lに対してL中に有限個の射影解を持つ.

(iii) $^\forall d \geqq D$, $\dim_K A^d = \dim_K A^D$

となるような整数Dが存在する.

(iv) LをKの拡大体とするとき,次の条件を満足する.

"yの積写像"が$A_L^{D'-1}$から$A_L^{D'}$への全射になるような整数D'及び

$y \in A_L^1$が存在する.

系2.1

定理2.2の条件が満たされるときに限り以下のことが成り立つ.

(i) "yの積写像"は$^\forall d \geqq \max(D,D')$に対して $A_L^d$から$A_L^{d+1}$への全単射になる.

(ii) (1)の射影解の数は高々 $\dim_K A^D$である.

(iii) (1)は定理2.1の条件を満たす.

(iv) (2)は$A^D=0$のときに限り,K中に自明解しかもたない.

定理2.3

定理2.2の条件が成り立っているとき

$$D=D'=d_0+d_1+\cdots+d_n-n \qquad (d_n=1)$$

となる.

§3 Lazardの方法(構成法)

さて以後(1)が定理2.2の条件を満たすとし,そのときの(2)の解を求めることにする.

(2)に$K[x_0,\cdots,x_n]$の次数1の要素

$$y = u_0 x_0 + \cdots + u_n x_n$$

として $y=0$ をつけ加えることを考える．このとき環Aを $A'=A/yA$ と置き直すことにする．A'の性質について2つの場合が考えられる．

i） $y=0$となる(2)の解が存在するとき．

系2.1(iv)よりA'≠0となる．ところが$A'^D = A^D/yA^{D-1}$であるから

$$A^{D-1} \to A^D$$

は全射にならない．

ii） $y=0$となる解がないとき．

$A'^D=0$となり，“yの積”の写像は全射になる．

ここでyの代りに不定元$U_0,\cdots,U_n$を導入し

$$L=U_0 x_0+\cdots+U_n x_n$$

を考える．このとき

$R \equiv K[x_0,\cdots,x_n]$, $L \in R[U_0,\cdots,U_n]$,

V：K上のベクトル空間，$V_U \equiv K[U_0,\cdots,U_n] \otimes_K V$

$L \in (R^1)_U \subset R_U$

とし

$R^d_U \equiv (R_U)^d$, $A^d_U \equiv (A_U)^d$

と記号を定義すると

$$\begin{array}{ccc} R^{D-1}_U & \xrightarrow{L} & R^D_U \\ \downarrow{\scriptstyle p_U^{D-1}} & & \downarrow{\scriptstyle p_U^D} \\ A^{D-1}_U & \xrightarrow{L} & A^D_U \end{array}$$

となる．射影$p_u{}^D$は$p^D: R^D \to A^D$の拡張であるから，まず$p^D$について考える．

$p^D$の核は $G_0F_0+\cdots+G_{n-1}F_{n-1}$ ($G_i \in R^{D-d_i}$, $i=0,\cdots,n-1$)の集合となる．これは線形写像

$$\phi: R^{D-d_0} \times \cdots \times R^{D-d_{n-1}} \to R^D$$

に対し，$p^D$を施したときの核と考えられ

$$\phi(G_0,\cdots,G_{n-1}) \equiv \Sigma G_i F_i$$

となる．$\phi$を単項式を基底として行列$\Phi$で表わすことができる．すなわち

$\phi_i: R^{D-d_i} \to R^D$,

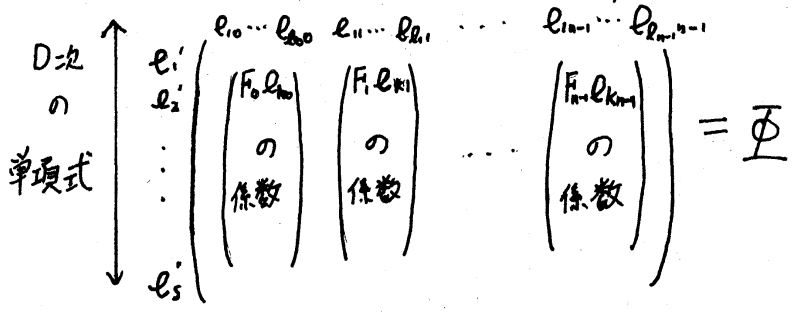
$e_{1i},\cdots,e_{\ell_i i}$: $D-d_i$次の単項式，$R^{D-d_i}$の基底，

$e_1', \cdots, e_s'$ : D次の単項式, $R^D$の基底

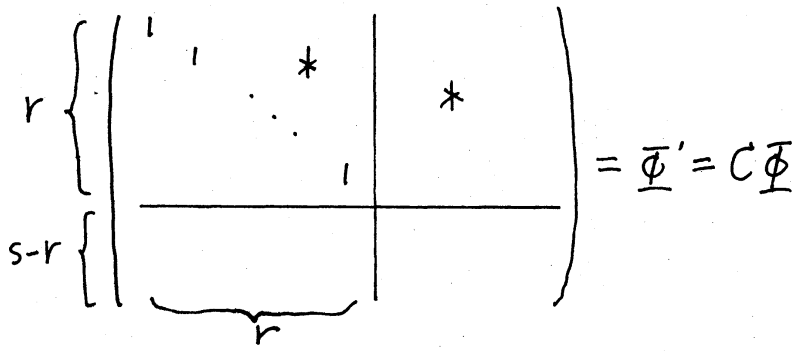
として

$\phi_i(e_{ki}) = \sum_j a_{jki} e_j'$ ($i=0,\cdots,n-1$; $a_{jki}$ : $F_i e_{ki}$中の項$e_j'$の係数)

とできる.よって行列




を$\phi(G)$の行列として考えることができる.この行列$\Phi$を Gauss の消去法で上3角化し, $\phi$の像の基底を$e_1', \cdots, e_s'$として R の新しい基底$e_1', \cdots, e_s'$上の行列




となるようにできる. $e_{r+1}', \cdots, e_s'$で生成されるベクトル空間が射影$p^D$を施した空間となることは明らかであり

$$\dim_K A^D = s - r$$

となる. $s = r$ならば非自明解をもたないことになる.

この性質を$p_u^D, K[U_0, \cdots, U_n]$加群について考えることにする. 単項式によって構成される基底の写像

$$L : R_U^{D-1} \to R_U^D$$

の行列(これもLで表わす)は,上と同様な方法で求まる.それをやはり Gaussの消去法で reduction して求まる新しい行列がCLとなる. 像$e_{r+1}', \cdots, e_s'$によって構成される$A_U^D$の基底上で写像 $p_u^D L = L p_u^{D-1}$に対応する行列はCL

$$\begin{cases} f_0 = x^2 + xy + 2x + y - 1 = 0 \\ f_1 = x^2 - y^2 + 3x + 2y - 1 = 0 \end{cases}$$

$$\Downarrow$$

$$\begin{cases} F_0 = -t^2 + 2tx + ty + x^2 + xy = 0 \\ F_1 = -t^2 + 3tx + 2ty + x^2 - y^2 = 0 \\ F_3 = Ut + Vx + Wy \end{cases}$$

$$\Downarrow$$

| | $t$ | $x$ | $y$ | $t$ | $x$ | $y$ | $t^2$ | $tx$ | $ty$ | $x^2$ | $xy$ | $y^2$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $t^3$ | -1 | 0 | 0 | -1 | 0 | 0 | U | 0 | 0 | 0 | 0 | 0 |
| $t^2x$ | 2 | -1 | 0 | 3 | -1 | 0 | V | U | 0 | 0 | 0 | 0 |
| $t^2y$ | 1 | 0 | -1 | 2 | 0 | -1 | W | 0 | U | 0 | 0 | 0 |
| $tx^2$ | 1 | 2 | 0 | 1 | 3 | 0 | 0 | V | 0 | U | 0 | 0 |
| $txy$ | 1 | 1 | 2 | 0 | 2 | 3 | 0 | W | V | 0 | U | 0 |
| $ty^2$ | 0 | 0 | 1 | -1 | 0 | 2 | 0 | 0 | W | 0 | 0 | U |
| $x^3$ | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | V | 0 | 0 |
| $x^2y$ | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | W | V | 0 |
| $xy^2$ | 0 | 0 | 1 | 0 | -1 | 0 | 0 | 0 | 0 | 0 | W | V |
| $y^3$ | 0 | 0 | 0 | 0 | 0 | -1 | 0 | 0 | 0 | 0 | 0 | W |

$$\Downarrow$$

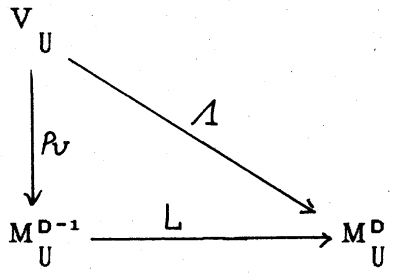
$$\begin{pmatrix} 1 & & & & & & & & & & & \\ & 1 & & & & & & & & & & \\ & & 1 & & & & & & & & & \\ & & & 1 & & & & & & & & \\ & & & & 1 & & & & & & & \\ & & & & & 1 & & & & & & \\ & & & & & & U+V-W & U+V-W & -U-V+W & U & -U & U \\ & & & & & & -V+W & -U+V & U & U-4V+W & V & 0 \\ & & & & & & -2V+3W & -2U+W & 3U+V & -3V & U+W & V \\ & & & & & & -V+2W & -U-V+W & 2U+V & -U & U & W \end{pmatrix}$$

図 2.1　reductionの流れの例（その1）

の最後のｓ－ｒ行によって構成される．

今後，reductionを再帰的に行う必要があるため，少々一般的な記号を使用する．

次数がＤ次未満の要素によって生成される次数つきＡ加群Ｍを考える．Ｍの$M^{D-1}$成分はＫ上ベクトル空間Ｖ(ここではＶ=$R^{D-1}$)の商(射影$p_u$)として表わされる．射影$p_u$($p:V\to M^{D-1}$)とＬの積で合成されてできる行列Λは




とできる．さて定理2.2の条件が成り立つと仮定すると，Ｋの適当な無限次拡大体Ｋ'に対して“ｙの積写像”が$M^{D-1}_{K'}$から$M^{D}_{K'}$への全射となるような

ｙが存在し，$^{\forall}d \geqq D$に対してそれが$M^{d}_{K'}$から$M^{d+1}_{K'}$への全単射になる．この条件を(Ｙ)とする．

補題2.1

もし，$x \in M^{D-1}_{K'}$，$z \in A^{1}_{U}$で(Ｙ)を満たせば

$$y\,x=0 \quad \Rightarrow \quad z\,x=0$$

となる．

命題2.1

もし(Ｙ)を満たせば，Ｋ上の係数をもつ行列ΓによりＬ$p_u$の行列Λは

$$\Lambda\,\Gamma=(\Lambda' \quad 0)$$

とでき，Λ'は正方行列となる．

定理2.4

ｋをΛの行数とし，(Ｙ)が成り立つと仮定する．すると次の(ａ)～(ｃ)が成り立つ．

(ａ) rank Λ=ｋ．

(ｂ) Λの列の組合せでできるｋ×ｋの行列式によって生成される ideal は単項idealである．そしてそれはΛ の行列式$G(U_0,\cdots,U_n)$によって生成される．また，Ｇは$U_0,\cdots,U_n$についてｋ次同次式である．

(ｃ) もしＭ=ＡならばＧはＫの代数的閉体上で１次因子の積になる．その因子のひとつを$\xi_0U_0+\cdots+\xi_nU_n$としたとき，$\xi_0\neq 0$ならば$(\xi_1/\xi_0,\cdots,\xi_n/\xi_0)$

が(1)の解になる($\xi_0=0$のとき無限遠の解になる).

さてΛ'を求めることを考える．ΛからΛ'への reduction はRの剰余環A加群M上で求められる．Λ中の$U_i$に対応する添字iを選ぶ．ここでは0が選べるとする．そこで$U_0$の係数行列をGaussの消去法により

$$\Gamma_1\Lambda=\begin{pmatrix} U_0\Lambda_0+\Lambda_1 & \Lambda_2 \\ \Lambda_3 & \Lambda_4 \end{pmatrix}$$

と$\Lambda_0$が上3角行列になるように変形する．$\Lambda_1,\Lambda_3,\Lambda_4$を$U_0$に独立，$\Lambda_2$を$U_0$に従属とする．2つの場合に分けて考えることにする．

1) $\Lambda_3,\Lambda_4$の行数が0のとき:

$$\Gamma_1\Lambda=(U_0\Lambda_0+\Lambda_1 \quad \Lambda_2).$$

$\Lambda_2'$がK上，$\Lambda_2''$が$K[U_0,\cdots,U_n]$上の係数をそれぞれとり

$$\Lambda_2=U_0\Lambda_2'+\Lambda_2''$$

と分離する．$I_1,I_2$を単位行列として

$$\Gamma_2=\begin{pmatrix} I_1 & -\Lambda_0^{-1}\Lambda_2' \\ 0 & I_2 \end{pmatrix}$$

ととれば

$$\Gamma_1\Lambda\Gamma_2=(U_0\Lambda_0+\Lambda_1 \quad \Lambda_2''-\Lambda_1\Lambda_0^{-1}\Lambda_2')$$

とできる．このとき次のことが成り立つ．

<u>補題2.2</u>　$\Lambda_2''-\Lambda_1\Lambda_0^{-1}\Lambda_2'=0$　.

2) $\Lambda_3,\Lambda_4$の行数が0でないとき，$(\Lambda_3 \quad \Lambda_4)$は条件(Y)を満たす加群Mに対応して

$$\Lambda:V_U \to M_U^D$$

の行列になる．すなわちΛ'を求める行列に対して

$$(\Lambda_3 \quad \Lambda_4)\Gamma=(\Lambda' \quad 0)$$

となるΓを求めることができる．この操作を再帰的に考える．まず残りの変数から例えば$U_1$を選び

$$\Gamma_1^1(\Lambda_3 \quad \Lambda_4)=\begin{pmatrix} U_1\Lambda_0^1+\Lambda_1^1 & \Lambda_2^1 \\ \Lambda_3^1 & \Lambda_4^1 \end{pmatrix}$$

とする.ただし$\Lambda_0^1$が上3角で$\Lambda_1^1,\Lambda_3^1,\Lambda_4^1$が$U_1$に独立とする.
$(\Lambda_3^1 \quad \Lambda_4^1)$の行数が0でなければ

$$\Gamma_1^2(\Lambda_3 \quad \Lambda_4)=\begin{pmatrix} U_2\Lambda_0^2+\Lambda_1^2 & \Lambda_2^2 \\ \Lambda_3^2 & \Lambda_4^2 \end{pmatrix}$$

$$\cdots$$

$$\Gamma_1^k(\Lambda_3^{k-1} \quad \Lambda_4^{k-1})= \quad (U_k\Lambda_0^k+\Lambda_1^k \quad \Lambda_2^k)$$

とできる(変数の数が有限であるから停止するのは自明である).

$\Lambda_2^k = U_k\Lambda_2'+\Lambda_2''$

とすれば

$$\Gamma_2=\begin{pmatrix} I_1 & -(\Lambda_0^k)^{-1}\Lambda_2^1 \\ 0 & I_2 \end{pmatrix},$$

$$\Gamma_1^k(\Lambda_3^{k-1} \quad \Lambda_4^{k-1})\Gamma_2=(U_k\Lambda_0^k+\Lambda_1^k \quad 0),\ \Gamma^i=\begin{pmatrix} I & 0 \\ 0 & \Gamma_1^i \end{pmatrix},$$

$$\Gamma^k\Gamma^{k-1}\cdots\Gamma^1\Gamma_1\Lambda\Gamma_2=\begin{pmatrix} \Lambda_2 & \Lambda^1 \\ U_k\Lambda_0^k+\Lambda_1^k & 0 \end{pmatrix}$$

となる．Λの行列式によって生成される ideal の生成元はこの$U_k\Lambda_0^k+\Lambda_1^k$の行列式とΛ¹中の正方行列の積となる.つまりΛ¹に対してここでのreductionをさらに再帰的に行えば最終的に

$$(\Lambda' \quad 0)=\left(\begin{array}{ccc|c} & & \cdots & \\ & & \cdots & \\ & U_{k'}\Lambda_0^{k'}+\Lambda_1^{k'} & & \\ U_k\Lambda_0^k+\Lambda_1^k & 0 & & \bigcirc \end{array}\right)$$

とΛをブロック３角化し,Λ'を求めることができる.

以上がLazardの方法である.

さて，このreductionの変数の選び方を考えると次のことがいえる.

命題2.2

この再帰的なreductionで最初に変数を$U_0$から選ぶことにより行列式Gからあらかじめ$U_0$を含まない因子(ブロック)を分離できる(変数$U_0$がないときはすでに分離されていることになる).

よって定理2.4の3)により(1)の解を求めるには無限遠の零点に対応する因子を含まないU-終結式G'を次節の方法で因数分解すればよい.

算法2.1 (Lazard)

1 初期化

図 2.1 より

$$\begin{pmatrix} U+V-W & U+V-W & -U-V+W & U & -U & U \\ -V+W & -U+V & U & U-4V+W & V & 0 \\ -2V+3W & -2U+W & 3U+V & -3V & -3V & V \\ -V+2W & -U-V+W & 2U+V & -U & U & W \end{pmatrix} \quad (=\Lambda)$$

$$\Downarrow$$

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

$$\Downarrow$$

$$\begin{pmatrix} V-W & U+V-W & 0 & 0 & 0 & 0 \\ -V+W & -V+W & -U+2V-W & V & 0 & 0 \\ -V+W & W & -2V & U-V+W & 0 & 0 \\ V-W & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \quad (=\Lambda')$$

$$\Downarrow$$

$$G(U,V,W) = (V-W)(U+V-W)(U-3V+W)(U+W)$$

$$\Downarrow$$

解 : $(1,-1)$, $(-3,1)$, $(0,1)$ .

図 2.2 reduction の流れの例(その2).

1.1　nを変数及び方程式の数とする.

1.2　$NL={}_{D+n}C_n$ .（$D=d_0+\cdots+d_{n-1}+1-n$ .）

1.2.1　NLが大きすぎれば，この環境では計算できないといって終る.

1.3　Φをつくる.

2　Φのreduction

2.1　Φを上3角化し，Λをつくる.

（ただし,実際には基本行列の積Cだけを記憶していればよい.つまりΦの数値部を1列ずつ求めながらreductionし，最後に非数値部に対して計算を行いΛを求める.）

3　Λのreduction(Gの計算，再帰的な計算(理論的には)を行う.)

3.1　i=0;

3.2　$U_i$の係数について対角化し$\Lambda^i$をつくる.

（$\Lambda^0=\Lambda_1$，上3角化でもよいが算法が簡単になる.）

3.3　もし($\Lambda_3^i$　$\Lambda_4^i$)の行数が0でなければ

3.3.1

もしi≠nならば，i:=i+1　として3.2へ戻る.

さもなければΛのrankがΛの行数と等しくなり，無限個の解をもつことになるので計算をやめる.

($\Lambda_3^i$　$\Lambda_4^i$)の行数が0ならば

3.3.2

もしΛ'の行数が0ならば，$U_i\Lambda_0^i+\Lambda_1^i$の行列式を値として終る.

さもなければ,Λ'をΛとして3を再帰的に計算して求めた値と$U_i\Lambda_0^i+\Lambda_1^i$の行列式の積を値として終る.

## §4　線形因子への分解

この節ではVdWのU-終結式から(1)の$U_0$を含まない因子を除き，それを$G(U_0,\cdots,U_n)$とする.

もし(1)の有理数体Q上の解だけを求めたければ[12]などの算法を使って因数分解をすればよい．しかし一般には因数分解できることは少ない．よって数値的にこの分解を行うことにする.

さてこの線形因子にまで分解される多項式

$$G(U_0,\cdots,U_n)=\prod_j(\alpha_{j0}u_0+\cdots+\alpha_{jn}u_n),\quad \alpha_{ji}\in K$$

はどんな性質をもっているのだろうか．初等幾何的性質に注目してみる．G=0は図2.1のように数枚の平面の方程式を表わしていると考えることができる．平面の方程式は平面上の１点$x_0=(a_0,\cdots,a_n)$とその

傾き$\left[\frac{\partial G}{\partial U_j}(x_0)\right]_{j=0,\cdots,n}$がわかれば

$$\frac{\partial G}{\partial U_0}(x_0)U_0+\cdots+\frac{\partial G}{\partial U_n}(x_0)U_n=0$$

と求めることができる(重複解については後述する)．よって$\frac{\partial G}{\partial U_i}(x_0)\equiv\alpha_i$とおけば

$(\alpha_1/\alpha_0,\cdots,\alpha_n/\alpha_0)$

が(1)の解になる($\alpha_0=0$の場合は分離してある)．さて，平面上の点と傾きを求めるにはどうすればよいのだろうか．これも初等幾何的問題で解くことができる．適当な直線を１本選ぶとそれは平面と平行でない限り１点だけで交わる．俗にいう“平面と直線の関係”という非常に美しい性質である.これを用いて交点を求め，傾きを計算すればよい．以上の方針に沿った２通りの算法を示す．なお，無限遠の解についても同様な方法で求まることは明らかである．

<u>算法2.2</u>　(GCD計算を用いる方法)

1　Gを$G_1\cdot G_2^2\cdot\cdots\cdot G_s^s$と無平方分解し，重複する平面を分離する．Q上の解を求めることが目的ならばここで因数分解をしてもよい．

1.1　以後アフィン空間で考えるので（線形因子の$U_0$の係数は0にならないことが保証されているので）$G_i(1,U_1,\cdots,U_n)=g(U_1,\cdots,U_n)$とする($i=1,\cdots,s$)．

2　ある１点$(\lambda_1,\cdots,\lambda_n)$と原点$(0,\cdots,0)$を結ぶ(別に違う点でもよい)直線$(\lambda_1 t,\cdots,\lambda_n t)$を選ぶ(t:媒介変数)．

3　直線と平面との交点を求めるために直線の式をGに代入し，１変数代数方程式

$$g(\lambda_1 t,\cdots,\lambda_n t)\equiv\tilde{g}(t)=0$$

をつくる．

3.1　もし，$\tilde{g}$の次数がgの次数より小さくなれば，直線がある平面と平行になったことを示すので２に戻って直線を選び直す(図2.2)．

4　$\tilde{g}(t)$をさらに無平方分解する.このとき多重度をもつ因子があれば,直線が平面の交線を通っているので２へ戻って直線を選び直す(図2.3)．

5　$\tilde{g}(t)=0$の全解を数値的に求める．

6　解のひとつを$t_0$とし，$x_0=(1,\lambda_1 t_0,\cdots,\lambda_n t_0)$として

$[\frac{\partial G}{\partial U_i}(x_0)]\equiv \alpha_i$を計算して最終的に(1)の解

$(\alpha_1/\alpha_0,\cdots,\alpha_n/\alpha_0)$

を求める．

さて，この算法ではcostの高い多変数多項式の無平方分解を行う必要がある．これではQの拡大体上の係数の方程式やLazardの方法を数値的に計算する場合には意味がなくなる．そこで無平方分解を用いない方法を考える．

算法2.3

1　$G(1,U_1,\cdots,U_n)\equiv g(U_1,\cdots,U_n)$とする．

2　算法2.2の２と同じ．

3　算法2.2の３と同じ．

4　算法2.2の５と同じ．

5　解のひとつを$t_0$とする．

5.1　もし４の解がすべて単根ならば，算法2.2に帰着できる．

5.2　もし$t_0$が重根と判断できれば，1)(1)が重根をもつ,2)直線が平面の交点を通ったことに相当する.どちらにしても

$$\frac{\partial G}{\partial U_j}(1,\lambda_1 t_0,\cdots,\lambda_n t_0)=0$$

となるはずである.そこで点$x_0=(1,\lambda_1 t_0,\cdots,\lambda_n t_0)$でのtangent coneを考え

$$G'(U_0,\cdots,U_n)\equiv \frac{\partial^{\ell} G}{\partial U_0^{\ell}}(x_0)U_0^{\ell}+\frac{\partial^{\ell} G}{\partial U_0^{\ell-1}\partial U_1}(x_0)U_0^{\ell-1}U_1+\cdots+\frac{\partial^{\ell} G}{\partial U_n^{\ell}}(x_0)U_n^{\ell}$$

($\ell$は$\frac{\partial^{\ell} G}{\partial U_0^{\ell}}(x_0)$, $\frac{\partial^{\ell} G}{\partial U_0^{\ell-1}\partial U_1}(x_0)$, $\cdots$, $\frac{\partial^{\ell} G}{\partial U_n^{\ell}}(x_0)$のうち０でない項が初めて現れる数である)

を再度線形因子に分解することを考える．つまり別の直線$(\lambda_1' t,\cdots,\lambda_n' t)$を選び$((\lambda_1,\cdots,\lambda_n)\neq(\lambda_1',\cdots,\lambda_n'))$，$g'\equiv G'(1,U_1,\cdots,U_n)$との交点を求めるために

$$g'(\lambda_1' t,\cdots,\lambda_n' t)\equiv \tilde{g}'(t)=0$$

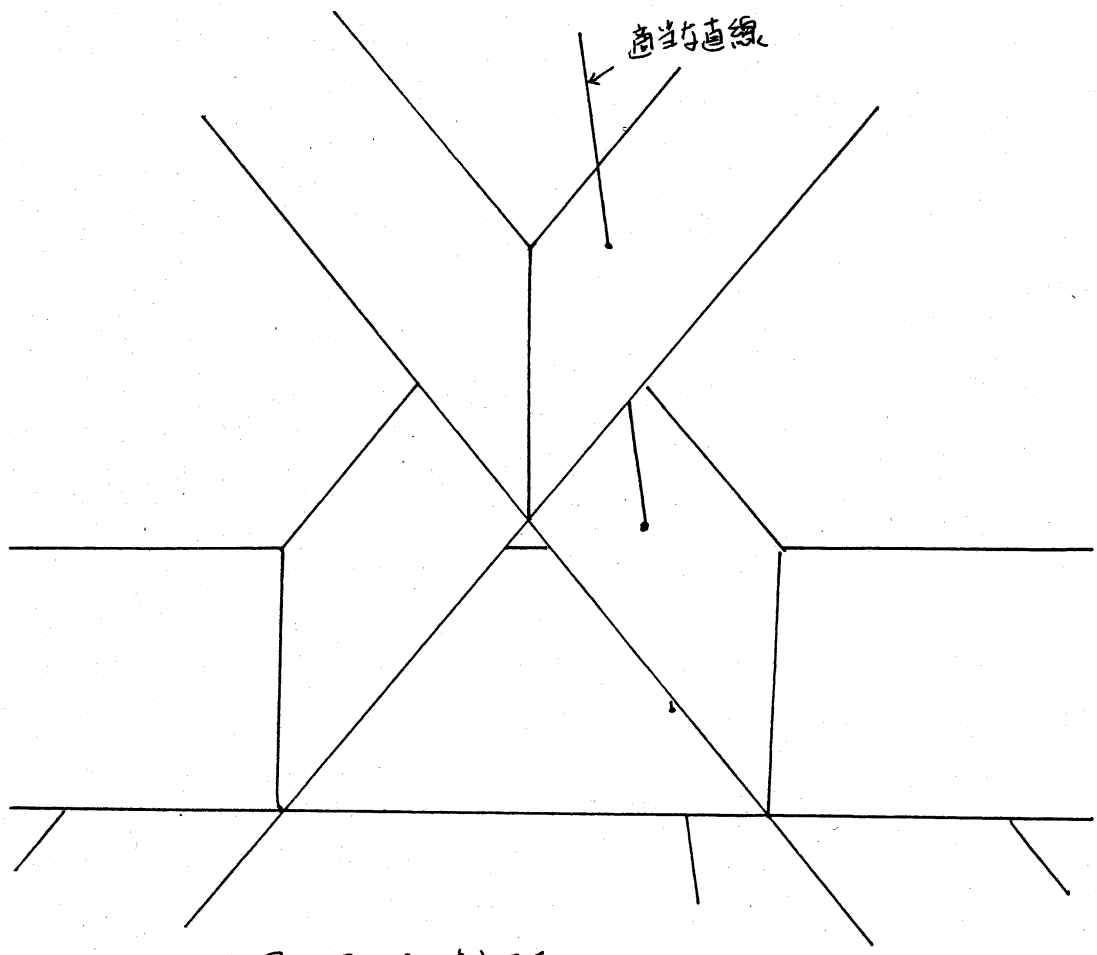



図 2.3 Gの表す平面の例

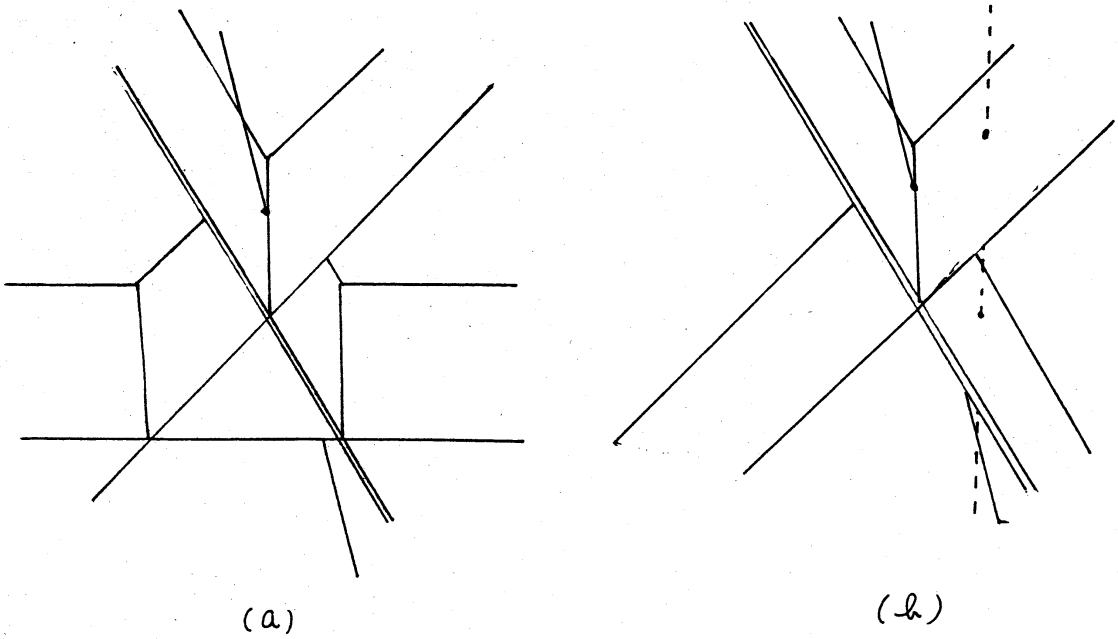



図 2.4 $\hat{g}=0$ が重根をもつ例

の全解を計算する．もし重根がないと判断できれば算法2.2の６に帰着できる．

もし重根があれば1)の場合であるから

$G''(U_0,\cdots,U_n)=(\alpha_0U_0+\cdots+\alpha_nU_n)^k$

として

$$\alpha_0U_0+\cdots+\alpha_nU_n=\frac{1}{\alpha_j{}^{k-1}\,k!}\cdot\frac{\partial^k}{\partial U_j{}^k}G''(U_0,\cdots,U_n)$$

とでき(jは計算可能なように適当に選ぶ)，

$(\alpha_1/\alpha_0,\cdots,\alpha_n/\alpha_0)$

を(1)の解にできる．

どちらの算法も（特に2.3は）１変数代数方程式の解の精度が(1)の解の精度を左右することがわかる.ここで用いたのが Durand-Kerner-Aberth 法である．Newton法の変形であるこの方法により１変数代数方程式の全解を同時に求めることができ，しかもAberthの初期値により収束性が半ば理論的に半ば経験的に保証される．また，この方法の弱点とすべき数値計算による重根の判定に対してもよい指針を与えてくれる(詳しくは[４]などを参照)．

例 ([4]より)

$f_0=x^2-2xy+3y^2-4x-6y-77,$

$f_1=x^2-9y^2-16.$

$G(u,v,w)$

$=$

$$\frac{3}{444928}(108u^4+1080u^3v+288u^3w-16236u^2v^2-5160u^2vw-1636u^2w^2-56808uv^3+4284uv^2w+7464uvw^2-476uw^3+554265v^4+40512v^3w-87650v^2w^2-3136vw^3+3465w^4).$$

(以下，係数を調整してある．)

直線 $(1,\lambda,0)$ を選ぶ．

$$\tilde{g}=\lambda^4-\frac{6312}{61585}\lambda^3-\frac{1804}{61585}\lambda^2+\frac{24}{12317}\lambda+\frac{12}{61585}=0,$$

$$\frac{\partial G}{\partial u}(1,\lambda,0)=\frac{6312}{61585}\lambda^3-\frac{3608}{61585}\lambda^2+\frac{72}{12317}\lambda+\frac{48}{61585},$$

$$\frac{\partial G}{\partial v}(1,\lambda,0)=4\lambda^3-\frac{18936}{61585}\lambda^2-\frac{3608}{61585}\lambda+\frac{24}{12317},$$

$$\frac{\partial G}{\partial w}(1,\lambda,0)=\frac{13504}{184755}\lambda^3+\frac{476}{61585}\lambda^2-\frac{344}{36951}\lambda+\frac{32}{61585}.$$

$\tilde{g}=0$ の解.

$\lambda$ = 0.16518300, 0.13747569, -0.13797874, -0.06218746

元の方程式系の解

(x,y)= (-6.0538916, 1.5147278), (-7.2474931,-2.0251548),
( 7.2474932,-2.0145625), ( 16.080412, 5.1916561).

これを代入してみる.

($f_0$,$f_1$)= (-0.00000005, 0.00000006),
( 0.00000007,-0.00000001),
( 0.00000009,-0.00000019),
(-0.00000061,-0.00000126).

## §5 考察

Lazardの方法により連立代数方程式は連立線形方程式の拡張と考えることができ,さらにこの方法により1変数代数方程式に帰着できる. 当然のことながら実係数のときには実根は実根に共役根は共役根に対応することがわかる. また結果としてDKA法の精度が非常に重要になっていることもわかる.

## §6 implementationに関する注意

さて, 実際に最も時間がかかるのはGを求めるための行列式の計算である. 特に[ ]で述べられているように多変数の場合は非常に計算量が増える. §4の例ではGは15項であるが, gは5項である. そこで計算を楽にするためにはGを展開せずに行列のまま保ち, 直線の式を代入して1変数にしてから

$$\tilde{g}=\det\left(\left(\ \right)t+\left(\ \right)\right),\quad \frac{\partial G}{\partial v_j}(1,\lambda_1 t_0,\cdots,\lambda_n t_0)=\frac{\partial}{\partial v_j}\det\left(\left(\left(\ \right)v_j+\left(\ \right)\right)\Big|_{\substack{v_i=\lambda_i t_0\\ i\neq j}}\right)\Big|_{v_j=\lambda_j t_0}$$

としてBareiss法[ ]などで計算するとよい(後者の誤差については少々気になるが,ここではその解析を行わない). 同様に算法2.3での多変数の無平方分解も直線を数本選び1変数の式に帰着させてからGCD計算し, 重根の判定を行った方が効率的であろう.

§7　問題点

非常に明確である．ひとつはLazardの方法の行列Φの行数(D次の単項式の数)

$$NL = {}_{D+n}C_n,\ d_i \equiv \deg f_i,\ D = d_0+d_1+\cdots+d_n-n$$

が非常に大きくなるこである．また次の定理に注目する．

定理　(Bézoutの定理)

n変数n個の連立同次代数方程式が代数的閉体上で有限個の解をもてばその解の数は次数の積に等しい．

これからわかるように，例えば5変数5次ならば$5^5$個の解(無限遠の解も含む)をもつ．つまり連立代数方程式には本質的に解の個数が多いのに対し，この方法では"すべての解が求まってしまうという欠点"をもつのである．現実的には残念ながら小規模な方程式系を扱うことになる．とにかくVdWのU-終結式が求まりさえすれば解くことができるのは確かである．

参考文献

[ 1] Bareiss,E.H.: Sylvester's identity and multi-step integer-preserving Gaussian elimination, Math.Comp. No.22 (1968),pp.565-578.

[ 2] 古川 昭夫 他：Grobner-bases とその応用，本講究録(1984).

[ 3] Hearn,A.C.: Reduce-3 User's Manual, Rand Publication, 1983.

[ 4] 伊理 正夫: 数値計算法，朝倉書店，1981.

[ 5] Kaplansky,I.: Commutative rings, Univ. of Chicago Press, 1970.

[ 6] Lazard,D.: Algèbre lineaire sur $K[x_1,\cdots,x_n]$ et élimination, Bull.Soc.Math.France No.105 (1977), pp.165-190.

[ 7] Lazard,D.: Systems of algebraic equations, Proc.of EUROSAM'79 (Ed. Ng,E.W.), pp.88-94.

[ 8] Lazard,D.: Résolution des systèms d'équations algébraique, Theoretical Computer Science NO.15 (1981), pp.77-110.

[ 9] Martínez,J.M.: Solving nonlinear simultaneous equations with a generalization of Brent's method, BIT No.20 (1980), pp.501-510.

[10] Murao,H. et al.: efficient Gaussian elimination method for symbolic determinants and linear systems, Proc.of ACM SYMSAC'81 (Ed. Wang,P.S.), pp.155-159.

[11] Van der Waerden,B.L.: Modern algebra II (1st ed.), Springer, 1936 (邦訳 銀林 浩: 現代代数学III，東京図書，1960).

[12] Wang,P.S.: An improved multivariable polynomial factoring algorithm, Math.Comp. No.32 (1978), pp.1215-1231.

[13] Weinberger,P.J. et al.: Factoring polynomials over algebraic number fields, ACM TOMS Vol.2 No.4 (1976), pp.335-350.

付録　計算例（Brown-Conte[9]）

$$\begin{cases} 2z^2+3x+y-3=0 \\ 5y^2+2xz+3x-1=0 \\ 25xy+20z+1=0 \end{cases}$$

U-終結式 G(TT, X, Y, Z)

```
                    7              6              6              5
ZZZ2 := (2343750*TT  - 1171875*TT *X - 3515625*TT *Z - 1781250*TT *

          2            5                5                5  2
         X  + 5062500*TT *X*Y - 7265625*TT *X*Z - 187500*TT *Y  -

                  5                  5  2             4  3
        14062500*TT *Y*Z - 10546875*TT *Z  + 2171875*TT *X  -

                4  2               4  2               4    2
        9187500*TT *X *Y + 28500000*TT *X *Z - 11156250*TT *X*Y

                   4                  4    2            4  3
         - 39375000*TT *X*Y*Z + 13359375*TT *X*Z  + 3600000*TT *Y

                4  2               4    2            4  3
         - 3656250*TT *Y *Z + 28500000*TT *Y*Z  + 9843750*TT *Z

                3  4             3  3               3  3
         + 10200000*TT *X  + 18525000*TT *X *Y + 41081250*TT *X *Z

                3  2  2            3  2                  3
         - 15697500*TT *X *Y  + 24300000*TT *X *Y*Z - 16968750*TT

          2  2            3    3             3    2
        *X *Z  - 5175000*TT *X*Y  + 27075000*TT *X*Y *Z + 51281250

           3      2            3    3            3  4
        *TT *X*Y*Z  + 52593750*TT *X*Z  - 2966250*TT *Y  -

                3  3               3  2  2             3  4
        15525000*TT *Y *Z + 30881250*TT *Y *Z  + 24656250*TT *Z

                2  5             2  4               2  4
         - 5370000*TT *X  + 37035000*TT *X *Y - 9325000*TT *X *Z

                2  3  2            2  3                  2
         + 11076250*TT *X *Y  + 15690000*TT *X *Y*Z - 8503125*TT *
```

```
 3  2              2  2  3              2  2  2
X *Z  + 6264000*TT *X *Y  + 37477500*TT *X *Y *Z +

           2  2    2              2  2  3             2
72277500*TT *X *Y*Z  + 80606250*TT *X *Z  - 4024875*TT *X*

 4              2    3                2    2  2
Y  + 30105000*TT *X*Y *Z + 15339375*TT *X*Y *Z  + 63703125

   2      3              2    4            2  5
*TT *X*Y*Z  - 57328125*TT *X*Z  + 406800*TT *Y  + 8098875*

  2  4                2  3  2              2  2  3
TT *Y *Z + 33615000*TT *Y *Z  - 48740625*TT *Y *Z  -

           2    4             2  5                6
21065625*TT *Y*Z  - 3431250*TT *Z  - 14520000*TT*X  +

            5                  5                 4  2
7228000*TT*X *Y + 2550000*TT*X *Z + 9600000*TT*X *Y  +

              4                    4  2               3  3
10578000*TT*X *Y*Z + 25567500*TT*X *Z  + 14901600*TT*X *Y

                3  2                  3    2
 + 15033750*TT*X *Y *Z + 53151250*TT*X *Y*Z  + 30219375*TT

  3  3               2  4                2  3
*X *Z  + 5170350*TT*X *Y  + 20628000*TT*X *Y *Z + 27897750

     2  2  2               2    3               2  4
*TT*X *Y *Z  - 60033750*TT*X *Y*Z  - 47932500*TT*X *Z  +

              5                   4                    3  2
2004300*TT*X*Y  + 18014625*TT*X*Y *Z - 23746500*TT*X*Y *Z

                  2  3                  4
 - 30166875*TT*X*Y *Z  - 74120625*TT*X*Y*Z  + 30318750*TT*

   5              6              5                  4  2
X*Z  + 518400*TT*Y  + 440100*TT*Y *Z - 5326875*TT*Y *Z  -

              3  3                2  4                   5
28957500*TT*Y *Z  + 34104375*TT*Y *Z  + 19603125*TT*Y*Z

                6           7           6             6
 - 33721875*TT*Z  - 4998400*X  - 3115200*X *Y + 8712000*X

              5  2             5                5  2
*Z - 440400*X *Y  + 14526000*X *Y*Z + 1028000*X *Z  +
```

```
          4  3              4  2                4     2
4137000*X *Y  + 9163400*X *Y *Z - 1519500*X *Y*Z  + 808500

   4  3             3  4             3  3              3  2
*X *Z  + 3282715*X *Y  + 2464200*X *Y *Z + 2751675*X *Y *

 2             3    3             3  4             2  5
Z  - 34281375*X *Y*Z  - 8781250*X *Z  + 1633212*X *Y  +

          2  4                2  3  2             2  2  3
2791380*X *Y *Z - 12068100*X *Y *Z  - 26757000*X *Y *Z  +

           2    4             2  5              6
19480500*X *Y*Z  + 2499000*X *Z  + 483408*X*Y  + 240480*X*

 5                  4  2              3  3               2
Y *Z - 10430100*X*Y *Z  + 4671000*X*Y *Z  + 13144500*X*Y *

 4                  5                 6           7
Z  + 16641000*X*Y*Z  - 14242500*X*Z  + 79488*Y  - 261360*

 6             5  2           4  3            3  4
Y *Z - 504900*Y *Z  + 777375*Y *Z  + 9004500*Y *Z  -

          2  5             6            7
8542125*Y *Z  - 8656875*Y*Z  + 16593750*Z )/2343750
```

118項ある。これと直線(1,5,5,5)との交点を求める。

```
                7                   6                    5
YYY2 := (52333*S )/390625 + (36011*S )/9375 + (1692707*S )/15625 +

                4                3                2
       (59803*S )/625 + (3616*S )/375 + ( - 307*S )/25 - 2*S + 1
```

以下，x方向，y方向，z方向，t方向の傾きの式を求める。

```
         6                    5                   4                   3
(36011*S )/9375 + (3385414*S )/15625 + (179409*S )/625 + (14464*S )

                2
/375 + ( - 307*S )/5 - 12*S + 7
```

```
          6                          5                          4
(6491267*S )/2343750 + (5968666*S )/46875 + (927719*S )/3750 + (

          3                 2
   87643*S )/625 + (17*S )/5 + ( - 123*S)/50 + ( - 1)/2


          6                          5                          4
(379297*S )/1171875 + (2091712*S )/46875 + (1704908*S )/9375 + (

          3                 2
   27909*S )/625 + ( - 2074*S )/125 - 4*S


          6                          5                          4
( - 8083*S )/3750 + ( - 6980048*S )/46875 + (2107831*S )/18750 + (

          3                 2
   24732*S )/125 + (1053*S )/25 + ( - 181*S)/10 + ( - 3)/2
```

数式の準備が終ったので，元の方程式系の解を数値的に構成する．

まず，1変数代数方程式の解(複素数体上の)を求める．
ただし，S=(実部，虚部)とする．

```
I= 1 , S= (  0.245628538673351812,  0.902101694235117046E-01)
I= 2 , S= (  0.245628538673351812, -0.902101694235117185E-01)
I= 3 , S= ( -0.409304332371273186,  0.268193704908770841)
I= 4 , S= ( -0.581188349172691188, -0.212798854058726672E-12)
I= 5 , S= ( -0.409304332370566709, -0.268193704909060845)
I= 6 , S= (-13.8814105137560837,  -24.3024673604901444)
I= 7 , S= (-13.8814105137557637,   24.3024673604901587)
```

これと傾きの式より，元の方程式系の解を求める．
これも(実部，虚部)とする．

```
T1= (1.0000000000000000,   0.0)
X1= (-1.0973333434859124,  1.21364440801285700)
Y1= (-0.585391751865234317,-0.330664073237274161)
Z1= (-1.90459868521453823,  0.434509582716715193)

T2= (1.0000000000000000,  0.0)
X2= (-1.0973333434859235,-1.21364440801285678)
Y2= (-0.585391751865234400,0.330664073237274536)
Z2= (-1.90459868521453890,-0.434509582716714471)

T3= (1.0000000000000000,  0.0)
X3= (0.938079623585398981, 0.962819216404950773)
Y3= (-0.288072766676130312,1.09802355095440651)
Z3= (1.05929031197648960, -0.940839105516718122)

T4= (1.0000000000000000,  0.0)
X4= (-1.32570474360258173,-0.329160618273517284E-12)
Y4= (1.37227352541755354,  0.254869240725757838E-11)
Z4= (1.67404119144681740,  0.156041453507957078E-11)

T5= (1.0000000000000000,   0.0)
X5= (0.938079623581094715, -0.962819216394252692)
Y5= (-0.288072766666708530,-1.09802355094677750)
Z5= (1.05929031197096646,   0.940839105517520674)

T6= (1.0000000000000000,   0.0)
X6= (0.572108139281499423, -0.723733946866960548E-01)
Y6= (0.187326380727244834,  0.856580846382267724E-01)
Z6= (-0.741712895000152417,-0.443102993018122818E-01)

T7= (1.0000000000000000,  0.0)
X7= (0.572108139281500186, 0.723733946866950278E-01)
Y7= (0.187326380727244543,-0.856580846382261896E-01)
Z7= (-0.741712895000151390,0.443102993018106564E-01)
```

共役根が当然対応する.