多項式の連立方程式を扱う魔術　–グレブナー基底–

丸 山 正 樹

以下は，市民講演会で使ったOHP原稿にほんの少しだけ手を加えたものである．有用な一般化が可能な個所が多々あるが，グレブナー基底を「連立方程式を解く」という視点のみから解説する事に特化し，雰囲気だけでも理解してもらうことを目指したものの故であると理解をして頂きたい．

まず次の方程式を考えてみよう．

$$\begin{cases} x^2+y+z=1 \\ x+y^2+z=1 \\ x+y+z^2=1 \end{cases}$$

最初の式から2番目の式を引いて因数分解すると

$$(x-y)(x+y-1)=0$$

$x=y$ の時は，$x^2+x+z=1$ と $2x+z^2=1$ を連立させて

$$z^4-4z^2+4z-1=0$$

これを解いて，

$$z=1 \text{ または } z=-1\pm\sqrt{2}$$

$x+y+1=0$ の場合は，$z=0$ となる．それぞれの場合に解を見つけるのは容易であろう．この解法は方程式の形の特殊性を使っているので，一般化することは難しい．例えば，方程式を

$$\begin{cases} x^2+y+z=1 \\ x+y^2+z=2 \\ x+y+z^2=3 \end{cases}$$

としてみると，最初の式から2番目の式を引いても

$$x^2-x-y^2+y+1=0$$

となり，これは因数分解できない．

「元の方程式から z のみについての方程式を導く一般的方法はあるか」

という問いに対する解答がYesであるということを説明するのが，此の講演の目的である．後で説明する方法により，最初の方程式の z についての解は

$$z^6-4z^4+4z^3-z^2=z^2(z-1)^2(z^2+2z-1)=0$$

の解であり，後に挙げた方程式の場合は

$$z^8 - 12z^6 + 4z^5 + 45z^4 - 16z^3 - 68z^2 + 16z + 37 = 0$$

の解であることが分かる．

1. 多項式の連立方程式

以下 K は有理数全体 $\mathbb{Q}$，実数全体 $\mathbb{R}$，又は複素数全体 $\mathbb{C}$ のいずれかとする．文字（変数）$X_1, \ldots, X_n$ を用意して $K[X_1, \ldots, X_n]$ で K に係数を持つ $X_1, \ldots, X_n$ についての多項式の全体とする．$K[X_1, \ldots, X_n]$ の元 $f_1(X_1, \ldots, X_n), \ldots, f_r(X_1, \ldots, X_n)$ を取って，連立方程式

$$(1) \qquad \begin{cases} f_1(X_1, \ldots, X_n) = 0 \\ f_2(X_1, \ldots, X_n) = 0 \\ \qquad\qquad \vdots \\ f_r(X_1, \ldots, X_n) = 0 \end{cases}$$

を考えよう．K の元の n 個の組 $(a_1, \ldots, a_n)$ の全体を K^n とおく：

$$K^n = \{(a_1, \ldots, a_n) \mid a_i \in K\}$$

(1) を解くとは，解の集合

$$V(f_1, \ldots, f_r) = \{(a_1, \ldots, a_n) \in K^n \mid f_1(a_i, \ldots, a_n) = \cdots = f_r(a_1, \ldots, a_n) = 0\}$$

を決めることである．

次の集合を考えよう．

$$\langle f_1, \ldots, f_r \rangle = \{f_1 g_1 + \cdots + f_r g_r \mid g_1, \ldots, g_r \in K[X_1, \ldots, X_n]\}$$

$\langle f_1, \ldots, f_r \rangle$ の「解の集合」を

$$V(\langle f_1, \ldots, f_r \rangle) = \{(a_1, \ldots, a_n) \in K^n \mid h(a_1, \ldots, a_n) = 0, {}^{\forall} h \in \langle f_1, \ldots, f_r \rangle\}$$

と定義する．$\{f_1, \ldots, f_r\}$ は $\langle f_1, \ldots, f_r \rangle$ の部分集合だから $V(\langle f_1, \ldots, f_r \rangle) \subset V(f_1, \ldots, f_r)$ は明らかである．逆に，$(a_1, \ldots, a_n) \in V(f_1, \ldots, f_r)$ とすると，$\langle f_1, \ldots, f_r \rangle$ の任意の元 $h = f_1 g_1 + \cdots + f_r g_r$ について

$$\begin{aligned} h(a_1, \ldots, a_n) &= f_1(a_1, \ldots, a_n) g_1(a_1, \ldots, a_n) + \cdots \\ &\qquad + f_r(a_1, \ldots, a_n) g_r(a_1, \ldots, a_n) \\ &= 0\, g_1(a_1, \ldots, a_n) + \cdots + 0\, g_r(a_1, \ldots, a_n) \\ &= 0 \end{aligned}$$

となるから，$(a_1, \ldots, a_n) \in V(\langle f_1, \ldots, f_r \rangle)$ となり，結局

$$V(\langle f_1, \ldots, f_r \rangle) = V(f_1, \ldots, f_r)$$

となる.

定義 連立方程式

$$\begin{cases} h_1(X_1,\ldots,X_n)=0 \\ h_2(X_1,\ldots,X_n)=0 \\ \qquad\vdots \\ h_s(X_1,\ldots,X_n)=0 \end{cases}$$

が (1) と同値であるとは, $\langle f_1,\ldots,f_r\rangle=\langle h_1,\ldots,h_s\rangle$ であるときに言う.

上で示したように, 連立方程式が同値であれば, 解の集合は一致する. $\langle f_1,\ldots,f_r\rangle$ が持つ性質を調べよう.

補題 u,v は $\langle f_1,\ldots,f_r\rangle$ の任意の元で, g は $K[X_1,\ldots,X_n]$ 任意の元であるとする. この時, 次のことが成り立つ.

(1) $u+v$ も $\langle f_1,\ldots,f_r\rangle$ の元である.
(2) gu も $\langle f_1,\ldots,f_r\rangle$ の元である.

此の補題は次の定義の動機づけである.

定義 $K[X_1,\ldots,X_n]$ の部分集合 I がイデアルであるとは, 補題の $\langle f_1,\ldots,f_r\rangle$ を I に置き換えて (1), (2) が成立するときに言う.

上の補題から $\langle f_1,\ldots,f_r\rangle$ はイデアルであるが, 次の Hilbert の基底定理によりイデアルはこのようなものしかない事が分かる.

定理 I をイデアルとすると, 多項式 $f_1,\ldots,f_r$ が存在して, $I=\langle f_1,\ldots,f_r\rangle$ となる.

定義 イデアル I について, $I=\langle f_1,\ldots,f_r\rangle$ となる多項式 $f_1,\ldots,f_r$ を I の生成元と言う.

従って, 多項式の連立方程式を考えることは, イデアルを考えることと同じことになり, 連立方程式を解くことは

「イデアルの生成元で解きやすいものを見つける」

ことに帰着する. 連立方程式をイデアルと考えたとき, 基本的な問題として次のものがある:

(1) f を多項式, I をイデアルとするとき, f が I の元であるかどうかを判定できるか,
(2) I,J をイデアルとするとき, $I=J$ であるかどうかを判定できるか,
(3) イデアルの解きやすい生成元を見つけることができるか.

(3) は我々の直接の目標であり, ある多項式が考えている連立方程式系に含まれるかどうかが (1) である. 連立方程式の同値性を判定するのが (2) である. 驚くべきことに, 上記の問題全てについて, 答えは Yes である.

2. 一変数の場合

$n=1$ の場合に上の問題 (1), (2), (3) を考えてみよう．一般の場合にどうすべきかについて，良い示唆を与えてくれる．以下この節では X_1 を X で表す．$f \in K[X]$ は

$$f = a_m X^m + a_{m-1}X^{m-1} + \cdots + a_1 X + a_0$$
$$a_i \in K,\ a_m \neq 0$$

と書けるが，この時 m を f の次数と言い，$\deg f$ で表す．

I を $K[X]$ の $\{0\}$ でないイデアルとして，

$$d = \min\{\deg f \mid f \in I \setminus \{0\}\}$$

と置く．d の定義と I がイデアルであることにより，I の元 g で $\deg g = d$ であり，最高次の係数が 1 であるものが存在する：

$$g = X^d + b_{d-1}X^{d-1} + \cdots + b_0.$$

I の任意の元 f を g で割ることにより，

$$f = gh + r$$
$$\deg r < d \text{ または } r = 0$$

と書ける．$r = f + (-g)h$ であり，f と $-g$ が共に I の元であるから，イデアルの性質により r も I の元であることが分かる．$r \neq 0$ ならば，$\deg g < d$ で d の最小性に反する．従って，$r = 0$ であり，I の全ての元が g で割り切れることが分かった．逆に，g で割り切れる元が全て I の元であることは明らかだから，$I = \langle g \rangle$ となる．一方，最高次の係数が 1 の多項式 g_1, g_2 について $\langle g_1 \rangle = \langle g_2 \rangle$ ならば，$g_1 = ag_2$ であり $g_2 = bg_1$ であるから，2番目の式を1番目の式に代入して，両辺を g_1 で割ることにより $1 = ab$ を得る．故に，a は K の元となる．g_1 と ag_2 の最高次の係数を比較して，$a = 1$ が分かり，$g_1 = g_2$ となる．これにより上記の I に対する g は I によって一意的に定まることになる．

定理　I を一変数の多項式環 $K[X]$ のイデアルとすると，最高次の係数が 1 である多項式 g が存在して，$I = \langle g \rangle$ となる．この g は I によって一意的に定まる．

$I = \langle f_1, \ldots, f_r \rangle$ の時，定理の g は $f_1, \ldots, f_r$ の最大公約因子であることは容易に分かる．h_1 が f_1 と f_2 の最大公約因子であれば，$f_1, \ldots, f_r$ の最大公約因子と $h_1, f_3, \ldots, f_r$ の最大公約因子は一致する．従って，Euclid の互除法を $r-1$ 回繰り返すことにより，g は簡単に求まる．

前節の最後に挙げた問題は，上記の定理で解けたことになる．(1) は f を g で割って，割り切れるかどうかで判定できる．イデアル I, J に定理を適用して，$I = \langle g_1 \rangle$，$J = \langle g_2 \rangle$ とすると，$I = J$ であるための必要十分条件は，$g_1 = g_2$ となることである．(3) については $g = 0$ の解が I の解になる．

3. 辞書式順序と割り算

一変数の場合の取り扱いで鍵になったアイデアは，多項式（正確には，単項式の）次数による大小関係と多項式の割り算であった．これらを多変数の場合にそのまま一般化することは出来ないが，我々の目的に合う程度の一般化はある．

$\mathbb{Z}_{\geq 0}^n$ で負でない整数 n 個の組の集合とする．すなわち，

$$\mathbb{Z}_{\geq 0}^n = \{(\alpha_1, \ldots, \alpha_n) \mid \alpha_1, \ldots, \alpha_n \text{ は負でない整数}\}$$

$\mathbb{Z}_{\geq 0}^n$ の元 $\alpha = (\alpha_1, \ldots, \alpha_n)$ に対して単項式 $X^\alpha = X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ を対応させることにより，$\mathbb{Z}_{\geq 0}^n$ と単項式全体の集合との間に 1 対 1 対応がつく（$\alpha = (0, \ldots, 0)$ の時，$X^\alpha = 1$ とする）．$\mathbb{Z}_{\geq 0}^n$ の 2 元 $\alpha = (\alpha_1, \ldots, \alpha_n)$, $\beta = (\beta_1, \ldots, \beta_n)$ に対して

$$\alpha > \beta \Longleftrightarrow \begin{cases} \text{ある } i\ (1 \leq i \leq n) \text{ が存在して，} \\ \alpha_1 = \beta_1, \ldots, \alpha_{i-1} = \beta_{i-1} \text{ かつ } \alpha_i > \beta_i \end{cases}$$

と定義する．これで $\mathbb{Z}_{\geq 0}^n$ に順序が入るが，これを辞書式順序と言う．辞書式順序は次の性質を持っている：

(1) $\mathbb{Z}_{\geq 0}^n$ の任意の 2 元 α, β に対して，$\alpha > \beta, \alpha = \beta, \alpha < \beta$ の何れかが成り立つ，
(2) $\mathbb{Z}_{\geq 0}^n$ の任意の部分集合に，この順序での最小の元が存在する，
(3) $\alpha > \beta$ ならば，任意の $\mathbb{Z}_{\geq 0}^n$ の元 γ について，$\alpha + \gamma > \beta + \gamma$ となる．ここで，$\alpha = (\alpha_1, \ldots, \alpha_n)$, $\gamma = (\gamma_1, \ldots, \gamma_n)$ とするとき，$\alpha + \gamma = (\alpha_1 + \gamma_1, \ldots, \alpha_n + \gamma_n)$ と定義する．

この 3 性質を持つ順序は辞書式順序だけでなく，他にも沢山ある．実際，後述のグレブナー基底の計算には「斉次逆辞書式」と呼ばれる順序を使う場合が多い．しかし，連立方程式を解くという場合には，辞書式順序の斉次逆辞書式順序にはない特殊性を使うので，以下では，順序は辞書式であると仮定する．

$\mathbb{Z}_{\geq 0}^n$ と単項式の集合との 1 対 1 対応を使って，$\mathbb{Z}_{\geq 0}^n$ の順序を単項式の集合の順序と考える．この時，例えば (3) から X^α が X^β を割り切っていれば，$\alpha \leq \beta$ であることが分かる．$K[X_1, \ldots, X_n]$ の元 f を

$$f = \sum_\alpha a_\alpha X^\alpha$$

と書いた時，$a_\alpha \neq 0$ である α の内，辞書式順序で最大のものを，f の multidegree と呼び，$\mathrm{multideg}(f)$ で表す．$X^{\mathrm{multideg}(f)}$ を leading monomial と言い，$\mathrm{LM}(f)$ と書き，$a_{\mathrm{multideg}(f)}$ を leading coefficient と言い，$\mathrm{LC}(f)$ で表す．最後に，$\mathrm{LC}(f)\,\mathrm{LM}(f)$ を leading term と言い，$\mathrm{LT}(f)$ で表す．例えば，

$$f = 5\,X_1^4 X_2^5 X_3 + 2\,X_1^3 X_2^2 X_3 - 4\,X_1 X_2^2 X_3^4$$

ならば，

$$\begin{aligned}\mathrm{multideg}(f) &= (4,5,1)\\ \mathrm{LM}(f) &= X_1^4X_2^5X_3\\ \mathrm{LC}(f) &= 5\\ \mathrm{LT}(f) &= 5\,X_1^4X_2^5X_3\end{aligned}$$

である．

次に，多項式 f を多項式の集まり $\{f_1,\ldots,f_s\}$ で割ることを考える．一変数の場合，f を g で割ったとき，その余りの次数は $\deg g$ よりも小さい．これを「$\mathrm{LM}(g)$ が余りに現れるどの単項式も割り切らない」と理解して，一般の場合の割り算を次のように定義する．

定義　多項式 f を多項式の集まり $\{f_1,\ldots,f_s\}$ で割るとは
「多項式 $a_1,\ldots,a_s,r$ で

$$f = a_1f_1 + \cdots + a_sf_s + r$$

となり，$\mathrm{LM}(f_1),\ldots,\mathrm{LM}(f_s)$ のどれもが r に現れるどの単項式も割り切らないものを見つける」
ことであるとする．

上記の割り算はいつでも可能であるが，$a_1,\ldots,a_s,r$ は一意的に定まるとは限らないことが，一変数とは本質的に違うところである．割り算が可能であることは，次の例で感じ取って貰いたい．

$$\begin{array}{ll}a_1: & x+y\\ a_2: & 1\end{array}$$

$$\begin{array}{r|l}
xy-1 & x^2y+xy^2+y^2 \\
y^2-1 & x^2y-x \\
\hline
 & xy^2+x+y^2 \\
 & xy^2-y \\
\hline
 & x+y^2+y \\
\hline
 & y^2+y \\
 & y^2-1 \\
\hline
 & y+1 \\
\hline
 & 1 \\
\hline
 & 0
\end{array}$$

$$\begin{array}{l}r\\ \hline \\ \\ \\ \\ \\ \longrightarrow\ x\\ \\ \\ \longrightarrow\ x+y\\ \longrightarrow\ x+y+1\end{array}$$

上の計算の結果

$$x^2y+xy^2+y^2=(x+y)(xy-1)+1\cdot(y^2-1)+x+y+1$$

となり，余りの $x+y+1$ に現れるどの単項式も $\mathrm{LM}(xy-1)=xy$ でも $\mathrm{LM}(y^2-1)=y^2$ でも割り切れない．また，$xy-1$ と y^2-1 の順序を変えて上と同じ計算をすると，

$$x^2y+xy^2+y^2=(x+1)(y^2-1)+x(xy-1)+2x+1$$

となり，余りの一意性さえも成り立たないことが分かる．

4. グレブナー基底

第 1 節に挙げた問題を解く方法として，イデアルの良い生成元を見つけることを考えてみよう．一変数の場合は非常によい生成元が存在した．素朴に考えて，例えば最も数の少ない生成元はどうだろうか．イデアルを扱った経験のある人ならば，それが凡そ使いものにならないものであることを知っている．B. Buchberger は彼の学位論文で全く違った生成元を導入した（1965年）．1970 年代になってその有効性と重要性が認識されるに及んで，Buchberger はこの生成元のことを，彼の指導教授の名に因んで Gröbner 基底と名付けた．

第 1 節に挙げた Hilbert の基底定理を見直してみよう．$\{f_\lambda \mid \lambda\in\Lambda\}$ を，必ずしも有限とは限らない多項式の集合とする．

$$\langle f_\lambda \mid \lambda\in\Lambda\rangle=\left\{\sum_{\text{有限和}} g_i f_{\lambda_i} \;\middle|\; g_i \text{ は多項式}, \lambda_i\in\Lambda\right\}$$

と置く．$\langle f_\lambda \mid \lambda\in\Lambda\rangle$ がイデアルであることは容易に分かる．従って，Hilbert の基底定理により，有限個の多項式 $h_1,\dots,h_s$ が存在して

$$\langle f_\lambda \mid \lambda\in\Lambda\rangle=\langle h_1,\dots,h_s\rangle$$

となる．各 h_i は $\langle f_\lambda \mid \lambda\in\Lambda\rangle$ の元であるから，

$$h_i=\sum_{j=1}^{r_i} g_{ij}f_{\lambda_{ij}},\ \lambda_{ij}\in\Lambda$$

と書ける．右辺に現れる $f_{\lambda_{ij}}$ を使うと

$$\begin{aligned}\langle f_\lambda \mid \lambda\in\Lambda\rangle=\langle h_1,\dots,h_s\rangle &\subset \langle f_{\lambda_{ij}} \mid 1\le i\le s, 1\le j\le r_i\rangle\\ &\subset \langle f_\lambda \mid \lambda\in\Lambda\rangle\end{aligned}$$

と成るが，これは $\langle f_\lambda \mid \lambda\in\Lambda\rangle$ の有限個の生成元として $\{f_\lambda \mid \lambda\in\Lambda\}$ の中から取ることが出来ることを意味している．

さて，$K[X_1,\dots,X_n]$ のイデアル $I\neq\{0\}$ を取って，上の注意をイデアル $\langle \mathrm{LM}(I)\rangle=\langle \mathrm{LM}(f) \mid f\in I\rangle$ に適用してみよう．有限個の I の元 $f_1,\dots,f_s$ が存在して $\langle \mathrm{LM}(I)\rangle=\langle \mathrm{LM}(f_1),\dots,\mathrm{LM}(f_s)\rangle$ となる．

定義 $K[X_1,\ldots,X_n]$ のイデアル $I \neq \{0\}$ について，$\langle \mathrm{LM}(I)\rangle = \langle \mathrm{LM}(f_1),\ldots,\mathrm{LM}(f_s)\rangle$ と成る I の元の集合 $\{f_1,\ldots,f_s\}$ を I のグレブナー基底と呼ぶ．

$\{f_1,\ldots,f_s\}$ を I のグレブナー基底として，I の任意の元 f を此の $f_1,\ldots,f_s$ で割ってみると

$$f = a_1f_1 + \cdots + a_sf_s + r$$

となり，$\mathrm{LM}(f_1),\ldots,\mathrm{LM}(f_s)$ のどれもが r に現れるどの単項式も割り切らない．$r = f - (a_1f_1 + \cdots + a_sf_s)$ は I の元であるから，$\mathrm{LM}(r) = b_1\,\mathrm{LM}(f_1) + \cdots + b_s\,\mathrm{LM}(f_s)$ と書ける．もし $r \neq 0$ ならば，$b_1,\ldots,b_s$ のどれかは 0 でなく，$\mathrm{LM}(f_1),\ldots,\mathrm{LM}(f_s)$ のどれかが $\mathrm{LM}(r)$ を割り切ることになり，r の性質に反する．故に，$r = 0$ となり，f が $\langle f_1,\ldots,f_s\rangle$ に含まれることになる．

定理 イデアル I のグレブナー基底は，I の生成元である．

グレブナー基底は割り算に対して非常に良く振る舞う．

定理 $\{f_1,\ldots,f_s\}$ を I のグレブナー基底とする．$K[X_1,\ldots,X_n]$ 任意の元 g に対して次の性質を持つ f,r が一意的に存在する：

(1) $g = f + r$,
(2) $f \in I$,
(3) $\mathrm{LM}(f_1),\ldots,\mathrm{LM}(f_s)$ のどれもが r に現れるどの単項式も割り切らない．

上の定理の g を $\{f_1,\ldots,f_s\}$ で割って $g = a_1f_1 + \cdots + a_sf_s + r$ と書くと，$f = a_1f_1 + \cdots + a_sf_s$ と r が定理にある性質 (1)，(2)，(3) を持つ．従って，余り r が一意的に決まることになる．

系 $\{f_1,\ldots,f_s\}$ を I のグレブナー基底とする．多項式 g が I の元であるための必要十分条件は，$\{f_1,\ldots,f_s\}$ で g を割ったときの余りが 0 に成ることである．

グレブナー基底に一意性が無いのは定義から明らかであろう．実際，$\{f_1,\ldots,f_s\}$ が I のグレブナー基底ならば，I の任意の元 f について，$\{f_1,\ldots,f_s,f\}$ もグレブナー基底である．一意性をのためにグレブナー基底に条件を付けよう．

定義 イデアル $I \neq \{0\}$ のグレブナー基底 $\{f_1,\ldots,f_s\}$ を I が被約であるとは

(1) 全ての i について，$\mathrm{LC}(f_i) = 1$,
(2) 全ての i について，$\mathrm{LM}(f_i)$ は f_j $(j \neq i)$ に現れるどの単項式も割り切らない，

時に言う.

次の定理は，それほど難しくなく証明できるが，驚くべき結果である.

定理 イデアル $I \neq \{0\}$ に対して被約グレブナー基底は必ず存在して，一意的である.

与えられたものから目的のものを導く手続きのことを algorithm という. Buchberger のグレブナー基底についての最大の貢献は

Buchberger's Algorithm
イデアルが有限個の生成元で与えられたとき，グレブナー基底を決定する，有限回で終わり，かつ有効な（簡単な場合には手計算でも可能であり，コンピュータを使えば，少し複雑でもそれほど時間のかからない）algorithm が存在する．また，グレブナー基底から被約グレブナー基底を決定することも容易である

の発見であろう.

第 1 節の最後に挙げた問題 (1), (2) はイデアルが有限個の生成元で与えられれば解ける．実際，まず，Buchberger's Algorithm で被約グレブナー基底を決定する．(1) については与えられた多項式を，このグレブナー基底で割ってみて，割り切れるかどうかを見ればよい（上の系を参照）．(2) については，I と J の被約グレブナー基底を比較して，それらが一致するかどうかによって判定できることになる（上の最後の定理を参照）.

5. グレブナー基底と多項式の連立方程式

多項式環 $K[X_1, \ldots, X_n]$ のイデアル $I = \langle g_1, \ldots, g_r \rangle$ を連立方程式と見なして，それを解くことを考える．もう少し正確に言うと，一変数の方程式を解くことに帰着させる.

定義 整数 m（$1 \leq m \leq n-1$）に対して，

$$I_m = K[X_{m+1}, \ldots, X_n] \cap I$$

と置き，m-th elimination ideal と呼ぶ.

次の結果が方程式を扱う基本定理である.

定理 $G = \{f_1, \ldots, f_s\}$ を I のグレブナー基底とする.

$$G_m = K[X_{m+1}, \ldots, X_n] \cap G$$

は m-th elimination ideal I_m のグレブナー基底である.

G が被約であれば，G_m もそうである．従って，第 2 節の結果を使えば，G が被約であれば，G_{n-1} は空集合であるか，唯一つの元から成る.

上の定理を方程式を解くという視点から眺めてみよう．G_m は I の部分集合であるから，$V(I) \subset V(G_m)$ である．従って，$(a_1, \ldots, a_n)$ が I の解ならば，$(a_{m+1}, \ldots, a_n)$ は I_m の解である．このことを理解した上で考えれば，方程式を解く手続きは以下の通りである.

(i) I の被約グレブナー基底 G を決定する.
(ii) G_{n-1} が空集合でなければ, その解の一つ a_n を取る. G_{n-1} が空集合ならば a_n は何でも良い.
(iii) $g_1,\ldots,g_r$ の X_n に a_n を代入した式を $\bar{g}_1,\ldots,\bar{g}_r$ として, $K[X_1,\ldots,X_{n-1}]$ のイデアル $\bar{I}=\langle\bar{g}_1,\ldots,\bar{g}_r\rangle$ を考えて, (i) に戻る.

注意 (1) $G_{n-2}\setminus G_{n-1}=\{f_1,\ldots,f_t\}$ とする. f_i $(1\leq i\leq t)$ を X_{n-1} の多項式として整理して

$$f_i=A_{im_i}(X_n)X_{n-1}^{m_i}+A_{im_i-1}(X_n)X_{n-1}^{m_i-1}+\cdots+A_{i0}(X_n)$$

と書こう. G_{n-1} の解 a_n を取ると,

$$A_{1m_1}(a_n)=A_{2m_2}(a_n)=\cdots=A_{tm_t}(a_n)=0$$

であるか, $f_1(X_{n-1},a_n),\ldots,f_t(X_{n-1},a_n)$ が正の次数の共通因子を持つ.
(2) G_{n-1} が空集合ならば, (1) の $f_1,\ldots,f_t$ は X_{n-1} について正の次数の共通因子を持つ.

例 最初に挙げた方程式のイデアル

$$\langle x^2+y+z-1,x+y^2+z-1,x+y+z^2-1\rangle$$

の被約グレブナー基底は

$$\{x+y+z^2-1,\ yz^2+\frac{z^4-z^2}{2},\ y^2-y-z^2+z,\ z^6-4z^4+4z^3-z^2\}$$

であり, 2番目の連立方程式のイデアル

$$\langle x^2+y+z-1,x+y^2+z-2,x+y+z^2-3\rangle$$

の被約グレブナー基底は

$$\{x+\frac{z^6}{2}-5z^4+2z^3+13z^2-4z-\frac{21}{2},\ y-\frac{z^6}{2}+5z^4-2z^3-12z^2+4z+\frac{15}{2},\ z^8-12z^6+4z^5+45z^4-16z^3-68z^2+16z+37\}$$

である.

最後に, グレブナー基底の計算に使える, パソコン上のソフトの例を挙げておく.
(1) 市販のソフトでは, Mathematica と Maple がある. これらのソフト上での, 多項式についての函数, 命令の多くが, グレブナー基底の計算を基礎にしている.

(2) 富士通のグループが開発した Asir は上記の市販ソフトに比べると格段に速いパッケージである．Mathematica や Maple で何十分もかかる計算が，数秒ですむこともある．公開されているソフトであって，

endeavor.fujitsu.co.jp (164.71.131)

から，ftp で入手できる．UNIX 版，DOS 版，Windows 版，Macintosh 版があるが，最後のMacintosh 版は 68K 用で，PPC 用は無いようである．

(3) ドイツの Kaiserslautern 大学の計算機代数のグループが開発している Singular というソフトがある．これは特異点の計算に特化したパッケージであるが．グレブナー基底の強力な計算力を持っている．上記の Asir とは違った計算機で試行したので，単純比較は出来ないが，数倍速い場合もあるようである．これも公開されていて，

http://www.mathematik.uni-kl.de/~zca/Singular/

からダウンロード出来る．UNIX 版，DOS 版，Macintosh 版があるが，Macintosh 版には MPW が必要である．最近，version-up された．

(4) 上記のほか PARI, MuPad, Macaulay など多くのソフトがあるが，全く使った経験が無いか，最新版は知らないものなので，無責任なことは言わないことにする．上記 (2), (3) のソフトのマニュアルなどで，入手方法を見つけることは，それほど難しく無い．

（まるやま まさき，京都大学大学院理学研究科）