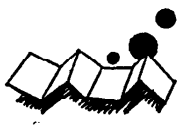
解　説



コンピュータ環論†

佐々木　建　昭††　　古　川　昭　夫†††

1. コンピュータ環論とは

1970年代の数式処理アルゴリズムの主役が多項式のGCDと因数分解，および初等関数を対象とするアルゴリズム（不定積分や微分方程式の求解）とするならば，1980年代のアルゴリズムの主役はコンピュータ環論，特に多項式イデアル論のアルゴリズムと言ってもさしつかえないであろう．$f_1, \cdots, f_s$ を多項式環 $K[x_1, \cdots, x_n]$ に属する多項式とするとき，$f_1, \cdots, f_s$ から生成されるイデアルとは多項式の集合

$$\{u_1 f_1 + \cdots + u_s f_s \mid u_i \in K[x_1, \cdots, x_n]\}$$

のことである．このイデアル（多項式イデアル）を $(f_1, \cdots, f_s)$ と表すならわしである．定義から分かるとおり，多項式イデアルで扱われるのは多項式であり，計算機処理に適した対象である．

数学の分野では環論は非常に進歩しており，その理論は高度に抽象的である．そのうちどの程度がコンピュータで扱えるのか，環論の専門家ではない筆者らには分かるべくもない．しかしながら，次章で述べるように，多項式イデアルに関する基本的演算は非常に明確であり，計算機屋にも十分に理解できるものである．数学者はイデアルの性質そのものに興味をもつが，われわれ計算機屋は計算のアルゴリズム化と効率化に大いに関心がある．計算機屋の目で数学者の作りあげた理論をながめるとき，われわれにも出番が残されていることに直ちに気付く…数学者の作ったアルゴリズムは効率性を欠くからである．Kronecker の因数分解アルゴリズムが実用的計算には全く無力であったように，数学者の考案したアルゴリズムを用いたのでは，コンピュータと言えども環論はまったく手に負えない．すなわち，コンピュータ環論とは環論の計算に対する効率的なアルゴリズムを開発し，それをインプリメントして，環論の諸量を計算するようなコンピュータ・システムを構築することである．

数学者は最近こう言ってよくこぼす：「20世紀に入って抽象数学が大発展をとげたのはよいが，理論が進歩しすぎて計算が追いつかない．理論の正しさを確かめるために簡単な例題を解くことさえ容易ではない」と．このような現状のため，構成的代数が見直されているという．コンピュータ環論は多くの数学者に待望されている．一方，初等的数学にあき足らなくなった多くの計算機代数屋のコンピュータ環論に対する思い入れは強い．ヨーロッパでは数学者と計算機代数屋の2人3脚が始まっている．遠からず，この分野は大発展をするだろう．その結果はめぐりめぐって，多くの代数計算法に多大な恩恵を及ぼすにちがいない．

本稿は夢多く，チャレンジングなテーマであるコンピュータ環論について，筆者らの最近の成果をおりまぜて平易に解説するものである．

2. 多項式イデアルの基本演算

本章では多項式イデアルに関する基本的な演算とその計算方法について述べる（参考文献1）参照）．

$R = Q[x_1, x_2, \cdots, x_n]$ を有理数係数の n 変数多項式全体の作る環とし，$I = (f_1, f_2, \cdots, f_s)$，$J = (g_1, g_2, \cdots, g_t)$ を多項式 $f_1, \cdots, f_s$，および $g_1, \cdots, g_t$ でおのおの生成される R のイデアルとする．

2.1 合同性の判定

二つの多項式 h_1, h_2 がイデアル I を法として合同であるとは，$h_1 - h_2 \in I$ なることであり，このとき $h_1 \equiv h_2 \pmod{I}$ と表すならわしである．合同な多項式を同一とみなすことにより，イデアル I による剰余環 R/I が構成される．合同性の判定は環論にとって最も基本的な計算であり，これは，今みたように，与えられた多項式 h がイデアル I に属するかどうかというメンバシップ問題に帰着される．すなわち，

$$h = y_1 f_1 + y_2 f_2 + \cdots + y_s f_s \qquad (1)$$

なる不定方程式の多項式解 $(y_1, y_2, \cdots, y_s)$ が存在する

† Computer Ring Theory by Tateaki SASAKI (The Institute of Physical and Chemical Research) and Akio FURUKAWA (Dept. of Mathematics, Tokyo Metropolitan University).

†† 理化学研究所
††† 東京都立大学理学部数学科

かどうかという問題に他ならない.

2.2 イデアルの和の計算

二つのイデアル I, J が与えられているとき，その和 $K=I+J$ は $(f_1, f_2, \cdots, f_s, g_1, g_2, \cdots, g_t)$ で定義される．したがって，K の生成元は特別な計算なしに I と J の生成元から求まるが，この中にはイデアルの生成元としては余分なものも含まれ，冗長になっている．たとえば，方程式

$$g_1=y_1f_1+\cdots+y_sf_s+y_{s+2}g_2+\cdots+y_{s+t}g_t \quad (2)$$

が多項式解をもつならば，g_1 は K の表現には不要である．(1)式と(2)式の多項式解の計算はそれぞれ mod I, mod K での多項式の“簡単化”と密接に関連している．これについては第5章で詳しく述べる．

2.3 イデアルの積の計算

イデアル I と J の積 K は

$$K=(f_1g_1, f_1g_2, \cdots, f_1g_t, f_2g_1, \cdots, f_2g_t, \cdots, f_sg_t) \quad (3)$$

で定義される．この生成元の簡約も(2)式と同様な方程式の求解に帰着される．

2.4 イデアルの共通集合の計算

イデアル I と J の共通部分 $K=I\cap J$ もイデアルとなる．このイデアル K の生成元は I の生成元と J の生成元の共通集合というわけにはいかない．

多項式 h がイデアル $K=I\cap J$ に属するための必要十分条件は

$$\begin{aligned} h&=y_1f_1+y_2f_2+\cdots+y_sf_s \\ &=z_1g_1+z_2g_2+\cdots+z_tg_t \end{aligned} \quad (4)$$

が多項式解 $(y_1, \cdots, y_s, z_1, \cdots, z_t)$ をもつ場合である．このような h の作るイデアル K の生成元 $(h_1, \cdots, h_l)$ を求めることを考えよう．それには

$$y_1f_1+\cdots+y_sf_s-z_1g_1-\cdots-z_tg_t=0 \quad (5)$$

なる線形不定方程式の解 $(y_1, \cdots, y_s, z_1, \cdots, z_t)$ の集合の生成元

$$\begin{aligned} &(\tilde{y}_{11}, \cdots, \tilde{y}_{s1}, \ \tilde{z}_{11}, \cdots, \tilde{z}_{t1}), \\ &(\tilde{y}_{12}, \cdots, \tilde{y}_{s2}, \ \tilde{z}_{12}, \cdots, \tilde{z}_{t2}), \\ &\quad \cdots\cdots\cdots\cdots \\ &(\tilde{y}_{1k}, \cdots, \tilde{y}_{sk}, \ \tilde{z}_{1k}, \cdots, \tilde{z}_{tk}) \end{aligned}$$

が求まればよい．実際，このとき，(4)式を満たす任意の h は適当な多項式 $u_1, u_2, \cdots, u_k$ を用いて

$$\begin{aligned} h&=(u_1\tilde{y}_{11}+\cdots+u_k\tilde{y}_{1k})f_1 \\ &\quad+\cdots+(u_1\tilde{y}_{s1}+\cdots+u_k\tilde{y}_{sk})f_s \\ &=u_1(\tilde{y}_{11}f_1+\cdots+\tilde{y}_{s1}f_s) \\ &\quad+\cdots+u_k(\tilde{y}_{1k}f_1+\cdots+\tilde{y}_{sk}f_s) \end{aligned}$$

とかけるので，$h_1=\tilde{y}_{11}f_1+\cdots+\tilde{y}_{s1}f_s, \cdots, h_k=\tilde{y}_{1k}f_1+\cdots+\tilde{y}_{sk}f_s$ が $K=I\cap J$ の生成元となることがわかる．

同様に，イデアル $I=(f_1, \cdots, f_s)$, $J=(g_1, \cdots, g_t)$, $K=(h_1, \cdots, h_l)$ が与えられたとき，これらの共通イデアル $I\cap J\cap K$ を計算することは

$$\begin{aligned} &y_1f_1+y_2f_2+\cdots+y_sf_s \\ &\quad=z_1g_1+z_2g_2+\cdots+z_tg_t \\ &\quad=w_1h_1+w_2h_2+\cdots+w_lh_l \end{aligned}$$

なる連立線形不定方程式の多項式解の計算に帰着されることになる．

2.5 イデアルの商の計算

イデアル I と J の商イデアル $K=I:J$ は

$$K=\{h \mid hJ\subseteq I\} \quad (6)$$

なる関係で定義されるイデアルである．$h\in K$ となる条件は，線形不定方程式

$$\begin{cases} hg_1=y_{11}f_1+\cdots+y_{1s}f_s, \\ hg_2=y_{21}f_1+\cdots+y_{2s}f_s, \\ \quad\cdots\cdots\cdots \\ hg_t=y_{t1}f_1+\cdots+y_{ts}f_s, \end{cases} \quad (7)$$

が多項式解をもつことである．(7)式を未知数 $(h, y_{11}, \cdots, y_{1s}, \ y_{21}, \cdots, y_{2s}, \cdots, y_{ts})$ についての連立方程式とみたときの解の生成元を

$$\begin{aligned} &(\tilde{h}_1, \tilde{y}_{111}, \tilde{y}_{121}, \cdots, \tilde{y}_{ts1}), \\ &(\tilde{h}_2, \tilde{y}_{112}, \tilde{y}_{122}, \cdots, \tilde{y}_{ts2}), \\ &\quad\cdots\cdots\cdots \\ &(\tilde{h}_k, \tilde{y}_{11k}, \tilde{y}_{12k}, \cdots, \tilde{y}_{tsk}) \end{aligned}$$

とすると，(6)式を満たす h は $\tilde{h}_1, \tilde{h}_2, \cdots, \tilde{h}_k$ の線形結合でかけるので，$(\tilde{h}_1, \tilde{h}_2, \cdots, \tilde{h}_k)$ が求める商 K の生成元となっている．

なお，イデアル I は

$$fg\in I \Rightarrow f\in I \text{ or } g\in I \quad (8)$$

を満足するとき**素イデアル**と呼ばれ，

$$fg\in I \Rightarrow {}^{\exists}m\in N(f^m\in I \text{ or } g^m\in I) \quad (9)$$

を満足するとき，**準素イデアル**といわれる．イデアル I が与えられたとき，I が素イデアル，あるいは準素イデアルかどうか判定することや，イデアル I を準素イデアル $P_1, P_2, \cdots, P_k$ によって $I=P_1\cap\cdots\cap P_k$ の形で表すこと（このことを準素イデアル分解という）は，連立代数方程式の解の様子を知る上で重要なことであるが，本稿の範囲を越える（興味ある読者は参考文献 2)を参照されたい）．なお，準素イデアル分解も連立線形方程式を何度も解くことによって実行できることを付加しておく．

3. 連立線形方程式の多項式解

前章で多項式イデアルに関する多くの基本的演算が連立線形方程式の多項式解の計算に帰着されることを見たから，その解法を考えよう．「それは Cramer の公式で計算できるではないか」と言わないでほしい．Cramer の公式は一般に有理式解を与え，多項式解の計算には使えない．「適当な初期値から出発し，反復解法で解くと多項式解が得られる」というのもよくない．われわれは方程式のすべての解を，すなわち一般解を計算したいのであるから．

この問題に最初の構成的解法を与えたのは女性数学者 Hermann[3] で，1926年のことである．解くべき連立方程式を

$$\begin{cases} P_{11}y_1+\cdots+P_{1s}y_s P=_{1,s+1}, \\ \cdots\cdots\cdots\cdots \\ P_{r1}y_1+\cdots+P_{rs}y_s=P_{r,s+1}, \end{cases} \tag{10}$$

とする．ただし $P_{ij}\in K[x_1,\cdots,x_n]$, K は数体，であり，$r<s$ と仮定する（そうでないと上の方程式は解をもつのが稀になる）．次に

$$\Delta\equiv\begin{vmatrix} P_{11}\cdots P_{1r} \\ \cdots\cdots\cdots \\ P_{r1}\cdots P_{rr} \end{vmatrix}\neq 0 \tag{11}$$

と仮定する．(10)の各式が線形独立である限り(11)式を仮定しても一般性を失わない（線形独立でなければ方程式の個数を減らして考えればよい）．(11)式の条件下では(10)式は次の連立方程式に等価である：

$$\begin{cases} \Delta y_1+\Delta_{1,r+1}y_{r+1}+\cdots+\Delta_{1s}y_s=\Delta_{1,s+1}, \\ \cdots\cdots\cdots\cdots\cdots \\ \Delta y_r+\Delta_{r,r+1}y_{r+1}+\cdots+\Delta_{rs}y_s=\Delta_{r,s+1}. \end{cases} \tag{12}$$

ただし，Δ_{ik} は次なる行列式である（これを **Cramer 行列式**と呼ぶことにする）：

$$\Delta_{ik}=\begin{vmatrix} P_{11}\cdots P_{1,i-1}\ P_{1k}\ P_{1,i+1}\cdots P_{1r} \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ P_{r1}\cdots P_{r,i-1}\ P_{rk}\ P_{r,i+1}\cdots P_{rr} \end{vmatrix}. \tag{13}$$

(12)式の一般解は斉次方程式（$\Delta_{1,s+1}=\cdots=\Delta_{r,s+1}=0$ と置いた式）の一般解と特解との和で与えられる．まず斉次方程式を考えると，それは次なる自明な $s-r$ 個の特解をもつことがすぐに分かる：

$$(y_1,\cdots,y_r,y_{r+1},\cdots,y_s)$$
$$=(\Delta_{1k},\cdots,\Delta_{rk},-\Delta,\cdots,-\Delta),\quad k=r+1,\cdots,s.$$

この解のことを **Cramer 解**と呼ぶ．よく知られていることであるが，斉次方程式の解のうちある次数以上のものはすべて Cramer 解の一次結合で表せる．まずこのことを示そう．

多項式 P の全次数を $\deg(P)$ で表し，

$$d=\max\{\deg(\Delta),\deg(\Delta_{ik})\,|\,i=1,\cdots,r,$$
$$k=r+1,\cdots,s\} \tag{14}$$

とする．次に，P の $x_n\equiv x$ に関する次数を $\deg_x(P)$ で表す．もしも $\deg_x(\Delta)=\deg(\Delta)$ ならばそれでよし，そうでなければ α_i を適当な数として $x_i\to x_i-\alpha_i x_n$, $i=1,\cdots,n-1$, なる変換により $\deg_x(\Delta)=\deg(\Delta)$ とすることができる．すなわち，

$$\Delta=c_d x_n^d+c_{d-1}x_n^{d-1}+\cdots+c_0$$

とおくと，Δ の主係数は K 上の数であると考えてよい．したがって，$y_1,\cdots,y_s$ が斉次方程式の任意の解であるとき，これらを x_n を主変数とみて Δ で割っても商と剰余は $K[x_1,\cdots,x_n]$ に入る：

$$y_i=Q_i\Delta+\bar{y}_i,\quad \deg_x(\bar{y}_i)<d,\quad i=r+1,\cdots,s. \tag{15}$$

これらを(12)式の斉次方程式に代入すると

$$\begin{cases} \Delta\bar{y}_1+\Delta_{1,r+1}\bar{y}_{r+1}+\cdots+\Delta_{1s}\bar{y}_s=0, \\ \cdots\cdots\cdots\cdots\cdots \\ \Delta\bar{y}_r+\Delta_{r,r+1}\bar{y}_{r+1}+\cdots+\Delta_{rs}\bar{y}_s=0, \end{cases} \tag{16}$$

を得る．ここで，$i=1,\cdots,r$ に対し

$$\bar{y}_i=y_i+Q_{r+1}\Delta_{i,r+1}+\cdots+Q_s\Delta_{is}$$

である．したがって，$(y_1,\cdots,y_s)$ から $(\bar{y}_1,\cdots,\bar{y}_s)$ への変換は Cramer 解に比例する部分を除くことに対応する．(15)式の定義より，(16)式の方程式の左辺第2項以降は x_n に関する次数が $2d$ より小である．したがって，$\deg_x(\bar{y}_i)<d$, $i=1,\cdots,r$, である．

以上より，(16)式の一般解は

$$\bar{y}_i=z_{i,d-1}x_n^{d-1}+\cdots+z_{i0}x_n^0,\quad i=1,\cdots,s,$$
$$\text{ただし } z_{ij}\in K[x_1,\cdots,x_{n-1}],$$

と表すことができる．この表式を(16)式に代入して変数 x_n に関して整理すると，sd 個の未知式 z_{ij} に関する約 rd 個の連立線形方程式を得る．ただし，この方程式系は変数 x_n を含まないから，$K[x_1,\cdots,x_n]$ 上の問題が $K[x_1,\cdots x_{n-1}]$ 上の同種の問題に帰着されたことになる．この手順を繰り返せば，問題は最後には K 上の連立方程式に帰着されて解ける．

同様な考察により，非斉次方程式の特解も x_n に関する次数が d より小さい範囲で解を探せばよいことが分かる．

以上が Hermann の方法の概略であるが，その数学的簡単さにもかかわらず，計算量が膨大になることは容易に想像できよう．さらに悪いことには，上記の方法では一般解の生成元の個数が極端に多くなってしまう．したがって，Hermann の方法は実際的計算には全く不適であると言わざるを得ない．しかし，純粋数学の分野では計算法の改善は重要視されず，1974年の Seidenberg の論文[2]においても Hermann の方法

が記述されている．なお，上記の方法は係数空間Kが体であるときのみ有効で，たとえば整数環Z上では使えないことに注意されたい．

4. $K(x_1, \cdots, x_{n-1})[x_n]$ における多項式解

線形方程式の多項式解の計算に対してはすでに決定版とも言える方法が発見されている（第 6〜7 章を参照）が，本章では解空間を $K(x_1, \cdots, x_{n-1})[x_n]$ にゆるめた場合のエレガントな方法を解説しよう．この方法は，筆者らが構築した副多項式剰余列の理論[4]に基づき，筆者の一人 (T.S.) が考案したものである[5]．

前章と同様 $x_n=x$ とおき，多項式 P の x に関する次数を $\deg_x(P)$ と表す．副多項式剰余列の理論によれば，F と G が互いに素な多項式であるとき，任意の多項式 H に対して

$$\begin{cases} A\cdot F+B\cdot G+\mathrm{res}_x(F,G)\cdot H=0, \\ \deg_x(A)\leqq\deg_x(G)-1, \\ \deg_x(B)\leqq\max\{\deg_x(F)-1,\ \deg_x(H)-\deg_x(G)\} \end{cases} \tag{17}$$

を満たす多項式 A と B が存在する．ただし，$\mathrm{res}_x(F,G)$ は F と G の x に関する終結式である．そして，F と G および H を x を主変数とする多項式とみなすとき，A と B は F, G, H の係数を要素とする行列式で表現できる．たとえば，

$$\begin{cases} F=f_l x^l+\cdots+f_0, & f_l\neq 0, \\ G=g_m x^m+\cdots+g_0, & g_m\neq 0, \\ H=h_k x^k+\cdots+h_0, & h_0\neq 0, \end{cases} \tag{18}$$

とし，$l+m>k$ であるとき，A と B の行列表現は次のようにシルベスタの行列式を拡張した形で与えられる：

$$A=\begin{vmatrix} f_l & f_{l-1} & \cdots & f_0 & & & x^{m-1} \\ & f_l & f_{l-1} & \cdots & f_0 & & x^{m-2} \\ & & \cdots & \cdots & \cdots & & \cdot \\ & & & f_l & f_{l-1} & \cdots\ f_0 & x^0 \\ g_m & g_{m-1} & \cdots & g_0 & & & 0 \\ & g_m & g_{m-1} & \cdots & g_0 & & 0 \\ & & \cdots & \cdots & \cdots & & \cdot \\ & & & g_m & g_{m-1} & \cdots g_0 & 0 \\ & & h_k & h_{k-1} & \cdots\cdots & h_0 & 0 \end{vmatrix} \begin{matrix} \\ \\ \\ \\ \\ \\ \\ \\ \\ \end{matrix} \begin{matrix} \\ \\ \\ \\ m\text{行} \\ \\ \\ \\ l\text{行} \\ \\ \end{matrix} \tag{19}$$

$B=[A$の最後列を $(0\cdots 0\ x^{l-1}\cdots x^0\ 0)$ とする$]$．

さて，本章でも(11)式なる条件を仮定し，連立方程式(10)式のかわりに(12)式を考える．さらに，本章では次なる条件を課する：

$$\mathrm{GCD}(\Delta, \Delta_{i,r+1})=1,\quad i=1,\cdots,r. \tag{20}$$

この条件は一般的にはもちろん成立しないが，

$$\mathrm{GCD}(\Delta, \Delta_{i,r+1}, \cdots, \Delta_{is})=1,\quad i=1,\cdots,r$$

であれば，λ_{ij} を適当な数値として

$$y_i\to y_i+\sum_{j=r+1}^{s}\lambda_{ij}y_j,\quad i=1,\cdots,r \tag{20'}$$

なる変換を施すことにより，(20)式が成立するようにできる．条件 (20′) 式が成立しない一般の場合は本稿では述べないので，興味ある読者は参考文献 5)を参照されたい．

条件(20)式の下では，(17)式によると

$$A_{ik}\Delta+B_{ik}\Delta_{i,r+1}+R_i\Delta_{ik}=0, \tag{21}$$

ただし $R_i=\mathrm{res}_x(\Delta, \Delta_{i,r+1})$,

を満たす多項式 A_{ik} と B_{ik} を，$i=1,\cdots,r$, $k=r+2,\cdots,s+1$ に対して計算できる．このとき，B_{ik} に対して次なる関係式が成立することを示せる：

$$B_{ik}/R_i=B_{jk}/R_j,\quad 1\leqq i,j\leqq r. \tag{22}$$

さて，(12)の第1式の $\Delta_{1,r+2},\cdots,\Delta_{1,s+1}$ を(21)式を用いて消去すると

$$\begin{aligned}\Delta(R_1y_1-A_{1,r+2}y_{r+2}-\cdots-A_{1s}y_s+A_{1,s+1}) \\ =-\Delta_{1,r+1}(R_1y_{r+1}-B_{1,r+2}y_{r+2} \\ -\cdots-B_{1s}y_s+B_{1,s+1})\end{aligned}$$

を得る．$\mathrm{GCD}(\Delta, \Delta_{1,r+1})=1$ ゆえ，上式は

$$\begin{cases} R_1y_1=\Delta_{1,r+1}u+A_{1,r+2}y_{r+2} \\ \qquad +\cdots+A_{1s}y_s-A_{1,s+1}, \\ R_1y_{r+1}=-\Delta u+B_{1,r+2}y_{r+2} \\ \qquad +\cdots+B_{1s}y_s-B_{1,s+1}, \end{cases} \tag{23}$$

なる連立方程式に等価である．ここで，uは未知の多項式であるが，$R_1\in K[x_1,\cdots,x_{n-1}]$ であるから(23)式は任意の多項式 $u, y_{r+2},\cdots,y_s$ に対して次のように解くことができる：

$$\begin{cases} y_1=(\Delta_{1,r+1}u+A_{1,r+2}y_{r+2} \\ \qquad +\cdots+A_{1s}y_s-A_{1,s+1})/R_1, \\ y_{r+1}=(-\Delta u+B_{1,r+2}y_{r+2} \\ \qquad +\cdots+B_{1s}y_s-B_{1,s+1})/R_1. \end{cases}$$

この解を(12)式の第 i 式，$i\geqq 2$, に代入すると，関係式(22)のため y_{r+1} は上記のままで，y_i を

$$\begin{aligned}y_i=(\Delta_{i,r+1}u+A_{i,r+2}y_{r+2} \\ +\cdots+A_{is}y_s-A_{i,s+1})/R_i\end{aligned}$$

とすればよいことが分かる．

以上より，$u=u_{r+1}$, $y_k=u_k$, $k=r+2,\cdots,s$, と置き換えれば，(12)式の一般解 $y=(y_1,\cdots,y_s)$ は斉次方程式の解 $y^{(j)}$, $j=r+1,\cdots,s$, と特解 $y^{(s+1)}$ で

$$y=u_{r+1}y^{(r+1)}+\cdots+u_sy^{(s)}+y^{(s+1)}, \tag{24}$$

ただし u_j は $K[x_1,\cdots,x_n]$の任意の要素，

と与えられることがわかる．ここで，

$$\begin{cases} \underline{y}^{(r+1)}=(\Delta_{1,r+1}/R_r,\cdots,\Delta_{r,r+1}/R_r,-\Delta/R_r,0\cdots0),\\ \underline{y}^{(r+2)}=(A_{1,r+2}/R_1,\cdots,A_{r,r+2}/R_r,B_{r,r+2}/R_r,1,0\cdots0),\\ \cdots\cdots\cdots\cdots\\ \underline{y}^{(s)}=(A_{1s}/R_1,\cdots,A_{rs}/R_r,B_{rs}/R_r,0\cdots0,1),\\ \underline{y}^{(s+1)}=(-A_{1,s+1}/R_1,\cdots,-A_{r,s+1}/R_r,\\ \qquad -B_{r,s+1}/R_r,0\cdots0), \end{cases} \tag{25}$$

である.

上記の A_{ik} と B_{ik} は Cramer 行列式(13)に対するシルベスタ型の行列式(19)で与えられるから，公式(25)は Cramer の公式の多項式解に対する拡張とみなせる．すなわち，$K(x_1,\cdots,x_n)$ と同様，$K(x_1,\cdots,x_{n-1})[x_n]$ においても，連立線形方程式の解はエレガントな行列式の公式で表されるのである.

5. 多項式イデアルの Gröbner 基底

多項式イデアルの計算に対する画期的方法は，1965年に Buchberger[6] によって考案された Gröbner 基底の計算アルゴリズムである（Buchberger の理論については参考文献 7)，8)が読みやすい).

理解を容易にするため，簡単な例を用いて説明しよう（下記の例は参考文献 11)に筆者の一人が与えたものである).

問題 1. $f=x^4+x^3+3x$, $f_1=x^3+x^2y+xy^2$, $f_2=x^2+y^3+3$ とするとき，$f\in(f_1,f_2)$ が成立するか否かを決定せよ.

問題 2. $f=2xy^2$, $f_1=x^3y+xy+1$, $f_2=x^2y^2-y^2+1$ とするとき，f からイデアル (f_1,f_2) に属する多項式を引いて最も簡単な残余を求めよ.

問題1においては，f が1変数多項式なのに f_1 と f_2 が2変数多項式なので $f\in(f_1,f_2)$ と思われるが，

$$f=(x-y)\cdot f_1+x\cdot f_2$$

なので $f\in(f_1,f_2)$ である．問題2においては，f の次数の方が f_1 と f_2 の次数より低いから f はこれ以上簡単にできそうになく思われるが，

$$f=y\cdot f_1-x\cdot f_2+(x-y)$$

であるから，f より簡単な残余が確かに存在する．なお，上問においては“簡単”の概念が定義されていないし，“最も簡単”な残余が一意的であるか否かも不明であることに注意されたい.

さて，第2章によれば，問題1は線形方程式に帰着させて解くことができるが，第3章で述べた方法は非効率的すぎる．ところが，問題1は次の方法で簡単に機械的に解けるのである：

① 任意の二つの単項式に対し，それらが等しいときのみ“=”が，そうでないときにはどちらかが高順位となる**順序**“$\succ$”を導入する；

② イデアルを $(f_1,\cdots,f_s)$ とするとき，f_i の項の中で最大順位のものを **head** (f_i)，残りの項をまとめて **rest** (f_i) とする：

$$f_i=\mathrm{head}(f_i)+\mathrm{rest}(f_i). \tag{26}$$

もしも多項式 f のどれかの項 T が $\mathrm{head}(f_i)$ の倍数ならば，T を次式で置き換える：

$$-(T/\mathrm{head}(f_i))\times\mathrm{rest}(f_i).$$

この操作を **M-簡約**と呼ぶ.

②の操作は f から f_i に比例する部分（=イデアルの成分）を引き去ることにほかならない．このことを

$$f\xrightarrow[f_i]{}$$

と図式的に表す.

問題1に M-簡約の手順を適用してみよう．ただし，項の順序づけには全次数一辞書式順序（項の全次数が高い方が順位が高く，全次数が同じときは辞書式に各変数の次数を比較して高いものを高順位とする）を用いる．たとえば

$$x^5\succ x^4y\succ x^3y^2\succ x^3yz\succ x^4.$$

この順序では $\mathrm{head}(f_1)=x^3$, $\mathrm{head}(f_2)=y^3$ であるから，問題1の f は次のように M-簡約される（M-簡約される項を下線で示す）：

$$\begin{aligned} f&=\underline{x^4}+x^3+3x\\ &\xrightarrow[f_1]{} x^3+3x-\underline{x^3y}-x^2y^2\\ &\xrightarrow[f_1]{} x^3+3x+\underline{xy^3}\\ &\xrightarrow[f_2]{} 0. \end{aligned}$$

すなわち，$f\in(f_1,f_2)$ が示された.

問題2は，f_1 と f_2 の全次数が f のそれより大きいから，単なる M-簡約では解けない．Buchberger は問題2も M-簡約の方法で解くために，イデアルの生成元を増やすことを考えた.

$$f_3=a\cdot f_1+b\cdot f_2,\quad a,b\in Q[x,y],$$

とすれば，$f_3\in(f_1,f_2)$ であるから

$$(f_1,f_2)=(f_1,f_2,f_3)$$

が成立する（f_3 を生成元として追加してもイデアルは不変)．f_3 には種々の選び方があるが，M-簡約の観点からは次数の低い方がよい．そこで Buchberger は f_3 を次のように定義した：

③ $$f_3=\frac{\mathrm{lcm}}{\mathrm{head}(f_1)}\cdot f_1-\frac{\mathrm{lcm}}{\mathrm{head}(f_2)}\cdot f_2, \tag{27}$$

ただし $\mathrm{lcm}=\mathrm{LCM}(\mathrm{head}(f_1),\ \mathrm{head}(f_2))$,

LCM は最小公倍数.

f_3 を f_1 と f_2 の **S-多項式**と呼び，$\mathrm{Sp}(f_1,f_2)$ と表す.

上記の定義を言い換えると，$\mathrm{Sp}(f_1, f_2)$ とは $\mathrm{head}(f_1)$ と $\mathrm{head}(f_2)$ をキャンセルさせるように f_1 と f_2 を最も簡単に組み合わせた多項式にほかならない．

問題2の f_1 と f_2 に対して S-多項式は

$$f_3=\mathrm{Sp}(f_1, f_2)=y\cdot f_1-x\cdot f_2$$
$$=2xy^2-x+y$$

と計算される．この f_3 を用いれば，

$$f\xrightarrow[f_3]{} x-y$$

が直ちに得られる．

以上の解法によると，問題2の簡単な残余とは順位が低い残余であると定義できる．したがって“簡単”の概念は順序の定義に依存する．以下では，多項式の集合 $F=\{f_1, \cdots, f_t\}$ の任意の要素に対して f がもはや M-簡約できないとき，f は F に関して**既約**であるという．f を F に関して既約な要素 $\tilde{f}$ に M-簡約することを以下のように表す：

$$f\xrightarrow[F]{*}\tilde{f}. \tag{28}$$

また，項 t_1 と t_2 が K 上の因子を除いて同じとき

$$t_1\sim t_2 \tag{29}$$

と表す．

さて，問題2では $(f_1, f_2)=(f_1, f_2, f_3)$ となるように f_3 を追加したが，このような生成元はさらに追加できるはずである．すなわち，$F_0=\{f_1, \cdots, f_t\}$ を最初に与えられたイデアルの生成元の集合，l 個の生成元を追加した集合を $F_l=\{f_1, \cdots, f_s, \cdots, f_{s+l}\}$ とするとき，F_{l+1} を次のように構成する：F_l のどれか二つの要素 f_i と f_j に対して S-多項式を計算し，

$$\mathrm{Sp}(f_i, f_j)\xrightarrow[F_l]{*} f_{s+l+1}$$

とする．もしも $f_{s+l+1}=0$ ならばその f_{s+l+1} は消去し，そうでなければ $F_{l+1}=F_l\cup\{f_{s+l+1}\}$ とする．

この手順を繰り返すと，生成元の個数は無限に増え続けるか，あるいは $F_k=\{f_1, \cdots, f_s, \cdots, f_{s+k}\}$ の任意の二つの要素 f_i と f_j に対して

$$\mathrm{Sp}(f_i, f_j)\xrightarrow[F_k]{*} 0$$

となって停止する，のいずれかであるが，実際は後者が成立する．このとき F_k をイデアル $(f_1, \cdots, f_s)$ の**Gröbner 基底と呼ぶ。**

例として，問題2のイデアル (f_1, f_2) の Gröbner 基底を上記の方法で計算すると以下のようになる．

$$\mathrm{Sp}(f_2, f_3)=2\cdot f_2-x\cdot f_3$$
$$=x^2-xy-2y^2+2=f_4,$$
$$\mathrm{Sp}(f_1, f_3)=2y\cdot f_1-x^2\cdot f_3\xrightarrow[F_4]{*} 0.$$
$$\mathrm{Sp}(f_3, f_4)=x\cdot f_3-2y^2\cdot f_4$$
$$\xrightarrow[F_4]{} 4y^4+xy-7y^2+2=f_5.$$

$F_5=\{f_1, \cdots, f_5\}$ の任意の対 f_i と f_j に対して，$\mathrm{Sp}(f_i, f_j)\xrightarrow[F_5]{*} 0$ となり計算は停止する．

注意 1. Gröbner 基底は S-多項式を作る順序に依存する．たとえば，$\mathrm{Sp}(f_2, f_3)$ より先に $\mathrm{Sp}(f_1, f_3)$ を計算すると，x^3-x^2y+x+y も基底の要素になる．

注意 2. 上記の手順で構成される Gröbner 基底は一般に冗長な表現になる．実際，f_1 は f_4, f_2, f_3 で0に M-簡約され，f_2 は f_4 と f_3 で f_5 に M-簡約される．したがって，(f_1, f_2) の Gröbner 基底は (f_3, f_4, f_5) で十分である．このように，0あるいは他の要素に M-簡約可能な生成元を除いた Gröbner 基底を**縮小された基底**と呼ぶ．

Gröbner 基底の構成アルゴリズムの停止性を証明することはやっかいだが，興味ある読者は参考文献7)あるいは9)，10)を参照されたい．次に，Gröbner 基底の最も重要な性質を示そう．

（1） イデアル $(f_1, \cdots, f_s)$ の Gröbner 基底を $G=\{g_1, \cdots, g_t\}$ とする．このとき，$f\in(f_1, \cdots, f_s)$ なる任意の多項式に対し $f\xrightarrow[G]{*} 0$ となる．

（2） $f\in K[x_1, \cdots, x_n]$ なる任意の多項式 f に対し $f\xrightarrow[G]{*}\bar{f}$ とすると，$\bar{f}$ は一意的である（M-簡約の順序によらない）．

（1）の証明. $(f_1, \cdots, f_s)=(g_1, \cdots, g_t)$ であり，f はイデアルの要素であるから，

$$f=h_1g_1+\cdots+h_tg_t \tag{30}$$

を満たす多項式 $h_i\in K[x_1, \cdots, x_n]$，$i=1, \cdots, t$，が存在する．$i=1, \cdots, t$ に対し

$$\mathrm{head}(g_i)=a_i\hat{g}_i,\quad \mathrm{head}(h_i)=b_i\hat{h}_i \tag{31}$$

とおく．ただし，$\hat{g}_i$ と $\hat{h}_i$ は変数 $x_1, \cdots, x_n$ のみの単項式で，a_i と b_i は K の要素である．$\hat{p}$ を単項式とし，一般性を失うことなく

$$\hat{p}\sim\hat{h}_1\hat{g}_1\sim\cdots\sim\hat{h}_k\hat{g}_k\succ\hat{h}_l\hat{g}_l,\quad l\geqq k+1$$

とする．以下，f が $\hat{p}$ より低順位の多項式で表現できることを示す．$\mathrm{head}(f)\sim\hat{p}$ ならば $\mathrm{head}(f)$ は g_1 で M-簡約でき，f はより低順位の多項式で(30)式のように表現できる．したがって，$\mathrm{head}(f)\prec\hat{p}$ の場合を考える．この場合，$k\geqq 2$ でなければならない．f を次のように分離する：

$$\begin{cases} f=f'+f'', \\ f'=\sum_{i=1}^{k} b_i\hat{h}_ig_i,\quad f''=f-f'. \end{cases} \tag{32}$$

$k\geqq 2$ ゆえ，f' は次のように変形できる：

$$\begin{aligned}f'=&(a_1b_1)\cdot(\hat{h}_1g_1/a_1-\hat{h}_2g_2/a_2)\\&+(a_2b_2+a_1b_1)\cdot(\hat{h}_2g_2/a_2-\hat{h}_3g_3/a_3)\\&+\cdots\cdots\\&+(a_{k-1}b_{k-1}+\cdots+a_1b_1)\\&\times(\hat{h}_{k-1}g_{k-1}/a_{k-1}-\hat{h}_kg_k/a_k)\\&+(a_kb_k+\cdots+a_1b_1)\cdot\hat{h}_kg_k/a_k.\end{aligned}\qquad(33)$$

仮定より f においては $\hat{p}$ と同順位の項はキャンセルしているから，この式の最後の項は0である．上式の第 i 番目の項は $\mathrm{Sp}(g_i, g_{i+1})$ の倍数であるから，仮定により0に M-簡約される．すなわち，

$$f\xrightarrow[G]{}\cdots\xrightarrow[G]{}f''.$$

(32)式によると

$$f''=h_1''g_1+\cdots+h_t''g_t$$

と表せるが，$\mathrm{head}(h_i''g_i)\prec\hat{p}$, $i=1,\cdots,t$, である．したがって，上述の簡約を続けると $f\xrightarrow[G]{}\!\!\!\!\rightarrow 0$ となる．

(2)の証明. f を G によって二通りに M-簡約し，

$$f\xrightarrow[G]{}\!\!\!\!\rightarrow f^{(1)},\quad f\xrightarrow[G]{}\!\!\!\!\rightarrow f^{(2)}$$

になるとすれば，$f'=f^{(1)}-f^{(2)}$ も G に関して既約である．一方，f' はイデアルの要素となるから $\mathrm{head}(f)$ は G で M-簡約できる．よって $f'=0$ である．

以上の理論化により，本章の初めに与えた問題1と2は完全に，かつ効率よく解けることがわかるだろう．問題1はイデアルのメンバシップ問題である．問題2は {多項式$=0,\cdots,$多項式$=0$} の条件下での多項式の簡単化とみなすこともでき，単にイデアルの残余にとどまらず，数式の簡単化においても重要な計算である．

Gröbner 基底はそのほかにも種々の計算に使える（参考文献 8) 参照）が，特に連立代数方程式の解の判定解の有無，解の個数の有限性）や効率的解法に重要な役割を演ずる．これに関しては，本特集号の小林英恒氏の解説を参照されたい．しかし，コンピュータ環論の立場から最も重要な応用は，次章と次々章に述べる多項式係数線形方程式の多項式解の計算であろう．なお，上述の理論においては K は数体としたが，係数も含めて順序を定義すれば $K=Z$（整数環）でもよい．

6. 線形方程式の多項式解の効率的算法

Gröbner 基底を利用すれば線形方程式の多項式解を効率よく計算できることが，1978年 Zacharias によって見い出された（参考文献 8)を参照)．解くべき方程式を次のものとする：

$$f_1y_1+\cdots+f_sy_s=0,\quad f_i\in K[x_1,\cdots,x_n].\qquad(34)$$

（斉次方程式が解けさえすれば，非斉次方程式はイデアルのメンバシップ決定計算を若干拡張した方法で解ける．したがって，本章と次章では斉次方程式だけを考察する)．イデアル $(f_1,\cdots,f_s)$ の Gröbner 基底を $G=\{g_1,\cdots,g_t\}$ とする．前章に述べた基底構成法によれば，$i=1,\cdots,t$ に対し

$$g_i=\sum_{j=1}^{s}\alpha_{ij}f_j\qquad(35)$$

なる多項式の組 $\{\alpha_{ij}\}$ を容易に計算できる．また，f_j を G で M-簡約すれば0になるから，

$$f_j=\sum_{i=1}^{t}\beta_{ji}g_i\qquad(36)$$

なる多項式の組 $\{\beta_{ji}\}$ も容易に計算できる．

まず，次の線形方程式を考える：

$$g_1z_1+\cdots+g_tz_t=0.\qquad(37)$$

Gは Gröbner 基底であるから，$1\leqq i,\ j\leqq t$ なる任意の i と j に対し次式が成立する：

$$\mathrm{Sp}(g_i,g_j)\xrightarrow[G]{}\!\!\!\!\rightarrow 0.$$

$\mathrm{Sp}(g_i,g_j)=u_{ij}g_i-v_{ij}g_j$ とおくと，上式は

$$\begin{cases}u_{ij}g_i-v_{ij}g_j=\sum_{l=1}^{t}w_{ij,l}g_l\\ \mathrm{head}(u_{ij}g_i)=\mathrm{head}(v_{ij}g_j)\\ \qquad\succ\mathrm{head}(w_{ij,l}g_l),\quad l=1,\cdots,t,\end{cases}\qquad(38)$$

とかける．したがって，$i>j$ とするとき

$$\begin{aligned}\underset{\sim}{z}^{(ij)}=&(w_{ij,1},\cdots,w_{ij,i}-u_{ij},\cdots,\\&w_{ij,j}+v_{ij},\cdots,w_{ij,t})\end{aligned}\qquad(39)$$

は(37)式の特解である．この特解が(38)式の形式の解としては最も低順位の解であることは直ちに分かる．以下，方程式(37)の任意の解は(39)式で与えられる特解（最大で $t(t-1)/2$ 個存在する）の線形結合で表されることを示そう．

(37)式の任意の多項式解を $(z_1=h_1,\cdots,z_t=h_t)$ とし，$i=1,\cdots,t$ に対し

$$\mathrm{head}(g_i)=a_i\hat{g}_i,\quad \mathrm{head}(h_i)=b_i\hat{h}_i$$

とする．ただし，$\hat{g}_i$ と $\hat{h}_i$ は変数 $x_1,\cdots,x_n$ だけの単項式で，a_i と b_i は K の要素である．$\hat{p}$ を単項式とし，一般性を失うことなく

$$\hat{p}\sim\hat{g}_1\hat{h}_1\sim\cdots\sim\hat{g}_k\hat{h}_k\succ\hat{g}_l\hat{h}_l,\quad l\geqq k+1,$$

とする．もしも $k=1$ であるならば(37)式は明らかに成立しないから，$k\geqq 2$ でなければならない．前章の(32)式と同様，Σh_ig_i を次のように分離する：

$$\sum_{i=1}^{t}h_ig_i=\sum_{i=1}^{k}b_i\hat{h}_ig_i+\sum_{i=1}^{t}h_i''g_i.\qquad(40)$$

右辺第2項は $\mathrm{head}(h_i''g_i)\prec\hat{p}$, $i=1,\cdots,t$, を満たす. $k\geqq 2$ であるから, 右辺第1項は(33)式と同じ形に変形できる. 方程式(37)の左辺に現れる最高順位項は今の場合 $\hat{p}$ と同順位であるから, その係数の和は0でなければならない. よって, (33)式の右辺最後の項は0である. 次に, (33)式の右辺第 i 項を考える.

$$(\hat{h}_ig_i/a_i-\hat{h}_{i+1}g_{i+1}/a_{i+1})=m_i\cdot\mathrm{Sp}(g_i,g_{i+1}),$$

ただし m_i は単項式,

であるから, 特解 $z^{(i,i+1)}$ をさし引くと

$$(\hat{h}_ig_i/a_i-\hat{h}_{i+1}g_{i+1}/a_{i+1})\longrightarrow m_i\cdot\sum_{l=1}^{t}w_{i,i+1,l}g_l.$$

(38)式の順位関係によれば, 右辺の各項は $\mathrm{head}(\hat{h}_ig_i)$ より低順位であることが分かる.

上記の操作を続行すると, 解 $(z_1=h_1,\cdots,z_t=h_t)$ はその順位が $z^{(ij)}$ の head よりも低くできる. 一方, $z^{(ij)}$ は(38)式の形の解としては最低順位のものなので, 結局(37)式の任意の多項式解は特解(39)式の倍数を引きさることにより0になる.

以上より, 方程式(37)の多項式解の一般解の生成元が Gröbner 基底から計算できることが分かった. (37)式の一般解が分かれば, 公式(35)で変換することにより(34)式の一般解が容易に得られる. この方法では, 一般解の生成元の個数は Gröbner 基底の要素の個数の2乗より少ないが, 2乗におよそ比例する.

Hermann の方法に比べると, 本章の Gröbner 基底を利用する方法ははるかに効率的であることが容易に想像できよう. 加えて, 新しい方法では一般解の生成元の個数がほぼ最少におさえられる. このことは実際計算上非常に大きな利点である.

7. 連立方程式の多項式解の効率的算法*

1個の線形方程式が解けるならば, その解を残りの方程式に代入することにより, 連立方程式は (原理的には容易に) 解ける(逐次代入法). しかし, 体上の解の公式として Cramer の公式があるように, また第3章に述べた Cramer の公式の拡張があるように, 連立方程式に対しては方程式全部を同時に扱うことにより効率的に解く方法があるのでは, と予想できる. 実際その予想が正しいことを筆者らは最近実証した(参考文献 9)を参照). 筆者らの方法は, 前章に述べた Gröbner 基底を利用する方法の拡張であり, 証明も前章のそれとほぼ同じである. したがって, 本章では多項式イデアルをどのように拡張すればよいかを中心に, 効率的解法を説明しよう.

解くべき連立方程式を

$$\begin{cases}f_{11}y_1+\cdots+f_{1s}y_s=0,\\ \cdots\cdots\\ f_{r1}y_1+\cdots+f_{rs}y_s=0,\end{cases}\tag{41}$$

とする. ただし, $f_{ij}\in K[x_1,\cdots,x_n]$ である. f_{1i}, $f_{2i},\cdots,f_{ri}$ をまとめてベクトル化し,

$$\vec{f}_i=(f_{1i},f_{2i},\cdots,f_{ri})\tag{42}$$

とすると, (41)式は

$$\vec{f}_1y_1+\cdots+\vec{f}_sy_s=0\tag{43}$$

となり, (34)式と同形になる. 解 $y=(y_1,\cdots,y_s)$ は $y_i\in K[x_1,\cdots,x_n]$ なる多項式であるから, われわれは $F=\{\vec{f}_1,\cdots,\vec{f}_r\}$ を生成元とする加群

$$\vec{I}=\{u_1\vec{f}_1+\cdots+u_s\vec{f}_s\,|\,u_i\in K[x_1,\cdots,x_n]\}\tag{44}$$

を扱っていることになる.

もしも加群 $\vec{I}$ に対しても Gröbner 基底が定義できるならば, 連立方程式(41)は方程式(34)と同様に解けることが予想される. そこで, Gröbner 基底の概念を加群 $\vec{I}$ に拡張することを考える. 今の場合ベクトルを扱って複雑なので, 新しい記号を導入して定義を明確にする.

単項式 $T=x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n}$ の順序はその指数の組のみで決定されるから,

$$\mathrm{ex}(T)=(\alpha_1,\alpha_2,\cdots,\alpha_n)\tag{45}$$

と定義する. 指数の組に対して順序 "$\succ$" を定義すれば, 項の順序は指数の組の順序に帰着できる. 非負整数の集合を Z_0 で表すと, 指数の組 $(\alpha_1,\cdots,\alpha_n)$ は Z_0 のカルテシアン積 Z_0^n の要素である. 同様に, 単項式のベクトル $\vec{T}=(T_1,T_2,\cdots,T_r)$ の順序を定義するには, Z_0^n のカルテシアン積 $(Z_0^n)^r$ の要素

$$(\mathrm{ex}(T_1),\mathrm{ex}(T_2),\cdots,\mathrm{ex}(T_r))\tag{46}$$

を考えればよい.

$(Z_0^n)^r$ の要素に対する順序を "$|\succ$" とする. $|\succ$ の定義には種々のものが考えられるが, 連立方程式を解くのに最適な順序は次のものである:

定義 [最高順序-最小インデックス順序 $|\succ$].

$\vec{A}=(A_1,\cdots,A_r)$ と $\vec{B}=(B_1,\cdots,B_r)$ を $(Z_0^n)^r$ の要素とする. $\vec{A}$ の成分を並べかえて $\vec{A}'=(A_{i_1},\cdots,A_{i_r})$ を次のように作る ($\{i_1,\cdots,i_r\}=\{1,\cdots,r\}$):

$A_{i_l}\geqq A_{i_{l+1}}$, $l=1,\cdots,r-1$

$A_{i_l}=A_{i_{l+1}}$ なるときは $i_l<i_{l+1}$.

---

* 本章に述べるものとほとんど同じアイデアに基づく Gröbner 基底の加群への拡張が最近ヨーロッパとアメリカでなされたことを, 本稿の脱稿後に知った.

したがって，A_{i1} は $A_1, \cdots, A_r$ の中で ($\succ$ の意味で) 最高順序の成分であり，しかも同一順序の成分の中では最小インデックスのものである．同様に $\vec{B}$ の成分を並べかえて $\vec{B}'=(B_{j_1}, \cdots, B_{j_r})$ を作る．このとき，以下の2条件を満たす整数 k, $1 \leqq k \leqq r$, が存在するとき $\vec{A} \mid\succ \vec{B}$ と定める：

① $1 \leqq l < k$ なるすべての整数 l に対し
$$A_{i_l}=B_{j_l} \text{ かつ } i_l=j_l,$$

② $A_{i_k} \succ B_{j_k}$, あるいは $A_{i_k}=B_{j_k}$ かつ $i_k<j_k$.

この定義は複雑そうに見えるが，$\vec{A}$ と $\vec{B}$ の順序関係が最高順序-最小インデックスの成分 A_{i_1} と B_{j_1} によって主に決定されることを考えれば分かりやすかろう．

例. $n=3$, $r=2$ のとき，

$$((1,1,1),\ (0.2,0)) \mid\succ ((2,0,0),\ (1,1,1)) \mid\succ$$
$$((0,2,0),\ (1,1,1)) \mid\succ ((0,3,0),\ (0,2,1)) \mid\succ$$
$$((2,0,0),\ (1,1,0)) \mid\succ ((2,0,0),\ (0,0,1)).$$

ただし，順序 $\succ$ は全次数-辞書式とした．

定義 [head とその位置，および rest]

$\vec{f}=(f_1, \cdots, f_r)$ を多項式のベクトルとする．$i=1, \cdots, r$ に対し，head (f_i) の指数の組を $\vec{A}$ とし，$\vec{A}=(A_1, \cdots, A_r)$ とする．$\vec{A}$ の成分中，最高順序-最小インデックスのものを A_k とする (A_k は上記の順序の定義における A_{i_1} に等しい)．このとき，

$$\mathrm{head}(\vec{f})=\mathrm{head}(f_k), \tag{47}$$
$$\mathrm{hp}(\vec{f})=k, \tag{48}$$
$$\mathrm{rest}(\vec{f})=\vec{f}-(0, \cdots, 0, \underset{\substack{\uparrow \\ k\text{番目の成分}}}{\mathrm{head}(\vec{f})}, 0, \cdots, 0), \tag{49}$$

と定義し，それぞれ $\vec{f}$ の head, head の位置, $\vec{f}$ の rest と呼ぶ．

定義 [$\vec{g}$ による $\vec{f}$ の簡約]．

$\vec{f}=(f_1, \cdots, f_r)$, $\vec{g}=(g_1, \cdots, g_k)$ を多項式のベクトルとし，$\mathrm{hp}(\vec{g})=k$, $\mathrm{head}(\vec{g})=T_k$ とする．$\vec{f}$ を $\vec{g}$ により簡約するとは，$\vec{f}$ の k 番目の成分 f_k が T_k の倍数である項 T を含むとき，

$$\vec{f}'=\vec{f}-(T/T_k)\vec{g} \tag{50}$$

を構成することである．

例. $G=\{\vec{g}_1, \vec{g}_2\}$, ただし (下線は head を表わす)

$$\vec{g}_1=(\underline{xy^4}-1,\ x^2y^2,\ xy^4-x),$$
$$\vec{g}_2=(xy^4-y,\ \underline{x^2x^3}-1,\ xy^4-1),$$

で $\vec{f}=(xy^4,\ x^2y^3,\ xy^4)$ を簡約すると

$$\vec{f} \xrightarrow[\vec{g}_1]{} (1,\ x^2y^3-x^2y^2,\ x)$$
$$\xrightarrow[\vec{g}_2]{} (-xy^4+y+1,\ -x^2y^2+1,\ x-y^4+x+1)$$
$$\xrightarrow[\vec{g}_1]{} (y,\ 1,\ 1).$$

定義 [加群 $\vec{I}$ の Gröbner 基底]．

$\vec{I}$ を (44) 式で定義される加群とし，$\vec{g}_1, \cdots, \vec{g}_t$ を多項式のベクトルとする．$G=\{\vec{g}_1, \cdots, \vec{g}_t\}$ が次の2条件を満たすとき，G を $\vec{I}$ の Gröbner 基底という：

① $(\vec{g}_1, \cdots, \vec{g}_t)=\vec{I}$,

② $\vec{I}$ の任意の要素 $\vec{f}$ に対し，$\vec{f} \xrightarrow[G]{} (0, \cdots, 0)$.

したがって，加群 $\vec{I}$ の Gröbner 基底は多項式イデアルのそれの直接的な拡張になっている．

詳しいことは参考文献 9) を参照していただくとして，上記の Gröbner 基底を構成するには，S-多項式を次に述べるように定義して，第5章で述べたイデアルに対する基底構成法で計算すればよい．

定義 [$\vec{f}$ と $\vec{g}$ に対する S-多項式]．

$\mathrm{head}(\vec{f})=h_f$, $\mathrm{head}(\vec{g})=h_g$, $\mathrm{hp}(\vec{f})-\mathrm{hp}(\vec{g})=\delta p$ とし，$\mathrm{LCM}(h_f, h_g)=\mathrm{lcm}$ とおくと，

$$\mathrm{Sp}(\vec{f}, \vec{g})=\begin{cases}(\mathrm{lcm}/h_f)\cdot\vec{f}-(\mathrm{lcm}/h_g)\cdot\vec{g}, \\ \qquad \delta p=0 \text{ のとき}, \\ 0,\ \delta p \neq 0 \text{ のとき}.\end{cases} \tag{51}$$

この定義において，$\delta p \neq 0$ のときには S-多項式が0とされることに注意されたい．このため，$\mid\succ$ として最高順序-最小インデックス順序をとる限り，$\vec{I}$ の Gröbner 基底の計算は予想よりもずっと早く収束する．

順序 $\mid\succ$ は，0でない最小インデックスの成分を主成分とするように決めることもできる．この場合にも (51) の定義式でよいが，Gröbner 基底の生成元の個数はずっと多くなる ($\delta p \neq 0$ となる場合が少なくなるからである)．この順序で連立方程式を解くことは第1の方程式を解いて残りの方程式に代入する逐次代入法に等しいから，最高順位-最小インデックス順序を用いる方法により，解法は大幅に効率化されることになる (具体例は参考文献 9) に記載されている)．

参 考 文 献

1) van der Wärden, B. L.: *Moderne Algebra I.* 2nd Edition (1937). (銀林 浩訳「現代代数学 1, 2, 3」, 東京図書, 1974).

2) Seidenberg, A.: *Constructions in Algebra,* Trans. Amer. Math. Soc. 197. pp. 273-313 (1974).

3) Hermann, G.: *Die Frage der Endlich Vielen Schritte in der Theorie der Polynomideale,* Math. Ann. 95, pp. 736-788 (1926).

4) Sasaki, T. and Furukawa, A.: *Secondary Polynomial Remainder Sequence and an Extension of Subresultant Theory*, J. Inf. Process. 7, pp. 175–184 (1984).
5) Sasaki, T.: *Cramer-type Formula for the Polynomial Solutions of Coupled Linear Equations with Polynomial Coefficients*, Publ. RIMS (Kyoto Univ.), 21, pp. 237-254 (1985).
6) Buchberger, B.: *An Algorithm for Finding a Basis for the Residue Class Ring of a Zero-dimensional Polynomial Ideal* (*German*), Ph. D. Thesis, Univ. of Innsbruck (Austria), Math. Inst. (1965).
7) Buchberger, B.: *A Theoretical Basis for the Reduction of Polynomials to Canonical Forms*, ACM SIGSAM Bull. 10, pp. 19-29 (1976).
8) Buchberger B.: "Gröbner Bases: An Algorithmic Method in Polynomial Ideal Theory", in *Recent Trends in Multidimensional Systems Theory*, edited by N. K. Bose, D. Reidel Publ. Comp. (1985). 本記事は約50編の Gröbner 基底に関する論文を参考文献として載せている.
9) Furukawa, A., Sasaki, T. and Kobayashi. H.: *Gröbner Basis of a Module over* $K[x_1,\cdots,x_n]$ *and Polynomial Solutions of a System of Linear Equations*, Preprint, 17 (1985).
10) Kobayashi, H., Furukawa, A. and Sasaki, T.: *Gröbner Basis of Ideal of Convergent Power Series*, Preprint, 20 (1985).
11) 佐々木建昭, 元吉文男, 渡辺隼郎:「数式処理システム」(ソフトウェア講座・第36巻), 昭晃堂 (1986).

(昭和60年12月6日受付)