

Gröbner - Bases について

都立大数学科 古川 昭夫

(Akio Furukawa)

近年, 多項式イデアル論における有力な算法として Gröbner-Bases の方法が注目と浴び, それを利用してめざましい成果がでてゐる。本稿ではそれと紹介すると共に, 基本定理の別証明と与える論法を報告する。

体 K 上の多項式環 $R = K[x_1, x_2, \dots, x_n]$ 上のイデアル $I = (f_1, f_2, \dots, f_r)$ の剰余環 R/I における標準形を求めるために Buchberger によつて理論が開発された算法が, Gröbner-Bases の方法であり, SAC1 に実際に implement されている。近年, 1) 多項式係数の不定方程式の生成元の求解, 2) 代数方程式の求解, 3) 素イデアルの判定, 4) 準素イデアル分解 などの算法が次々と Gröbner-Bases を利用して開発されている。本稿では 1), 2) の算法と理論を紹介する。

§ 1 準備

まず, 次の様に用語を定める。

$$\mathbb{Z}_0^+ : \{ x \in \mathbb{Z} \mid x \geq 0 \}$$

K : 基礎体 (係数体)

R : $K[x_1, x_2, \dots, x_n]$ 多項式環

項 : $x_1^{e_1} x_2^{e_2} \dots x_n^{e_n}$, $e_i \in \mathbb{Z}_0^+$

指数 : $(e_1, e_2, \dots, e_n) \in (\mathbb{Z}_0^+)^n$

単項式 : 係数 $\times$ 項

多項式 : 単項式の和。但し, 同類項は簡約されるものもある。

Gröbner-Bases (以下, G-Bases と略す) とは, "順序" が本質的に重要な役割を果たす。

$$\mathbb{e} = (e_1, e_2, \dots, e_n), \mathbb{f} = (f_1, f_2, \dots, f_n) \in (\mathbb{Z}_0^+)^n$$

に於いて

① lexicographic ordering $\triangleright$

$$\mathbb{e} \triangleright \mathbb{f}$$

$$\Leftrightarrow e_1 > f_1 \vee (e_2, \dots, e_n) \triangleright (f_1, \dots, f_n)$$

① total degree ordering ▶

$$e \triangleright f$$

$$\iff e_1 + e_2 + \dots + e_n > f_1 + f_2 + \dots + f_n$$

$$\text{otherwise } e \triangleright f$$

例 $(3, 2, 1) \triangleright (3, 1, 2) \triangleright (2, 3, 5)$

$$(2, 3, 5) \blacktriangleright (3, 2, 1) \blacktriangleright (3, 1, 2)$$

以下, 順序としては ① と採用して話をする。但し, 次の性質の成立する $(\mathbb{Z}_0^+)^n$ の全順序ならば同様の話ができる。

性質 ①

$$\textcircled{1} \quad e_1 \triangleright f_1, e_2 \triangleright f_2 \Rightarrow e_1 \cdot e_2 \triangleright f_1 \cdot f_2$$

② 降下列は有限ととまる。

±, Notation を ± に次の様に定める。

$\exp(t)$: 項 t の指数 (exponent)。

$$\underline{t_1 \triangleright t_2} \iff \exp(t_1) \triangleright \exp(t_2)$$

$\text{term}(m)$: 単項式 m の項 (term)。

$\text{coef}(m)$: 単項式 m の係数 (coefficient)。

$$\underline{m_1 \triangleright m_2} \iff \text{term}(m_1) \triangleright \text{term}(m_2)$$

このようにして項, 単項式にも順序が定められる。

$E(P)$: 多項式 P に現れる項の指数の集合。

$\max \exp(P)$: $E(P)$ の最大元。

$\max(P)$: $\max \exp(P)$ に対応する項。

$\text{head}(P)$: $\max(P)$ に対応する P 中の単項式。

$\text{rest}(P)$: $P - \text{head}(P)$

例 $P = 3x_1^2x_2 + 4x_1x_2 + 6 \in \mathbb{Q}[x_1, x_2]$ に対し

$$E(P) = \{(2, 1), (1, 1), (0, 0)\},$$

$$\max \exp(P) = (2, 1), \quad \max(P) = x_1^2x_2$$

$$\text{head}(P) = 3x_1^2x_2, \quad \text{rest}(P) = 4x_1x_2 + 6$$

次に多項式 P_1, P_2 に対し

$$P_1 \triangleright P_2 \iff \max(P_1) \triangleright \max(P_2)$$

$$P_1 \trianglelefteq P_2 \iff \max(P_1) = \max(P_2) \vee P_1 \triangleright P_2$$

と順序を定める。従って $P_1 \trianglelefteq P_2 \wedge P_2 \trianglelefteq P_1$ なる同じ order の多項式はたくさん存在する。

さらに、多項式の組 $F = (P_1, P_2, \dots, P_e)$ に対し、

$$\max F = \max_{i=1}^e (\max P_i)$$

$$\overline{\max} F = \{P_i \mid \max P_i = \max F\}$$

と定める。2つの多項式の組 $F_1 = (P_1, P_2, \dots, P_e),$

$F_2 = (Q_1, Q_2, \dots, Q_e)$ に対し

$$F_1 \supset F_2 \iff \max F_1 \supset \max F_2$$

$$\text{or } \# \overline{\max F_1} = \# \overline{\max F_2}$$

$$F_1 \supseteq F_2 \iff \max F_1 \supseteq \max F_2$$

$$\text{or } \# \overline{\max F_1} = \# \overline{\max F_2}$$

(但し, $\#$ は集合の元の個数を表す。)

として順序関係も定める。

§2 M-reduction と G-Basis

指数 $\mathbf{e} = (e_1, e_2, \dots, e_n)$, $\mathbf{f} = (f_1, f_2, \dots, f_n)$ に対し,
別の順序関係 $\succcurlyeq$

$$\mathbf{e} \succcurlyeq \mathbf{f} \iff \forall i \quad e_i \geq f_i$$

として定める。すると,

$$t_1 \mid t_2 \iff \exp(t_1) \leq \exp(t_2)$$

である。多項式の組 $F = \{P_1, P_2, \dots, P_k\}$ に対し

$$M(F) = \{ \mathbf{e} \in (\mathbb{Z}_+^+)^n \mid \exists P_i \quad \mathbf{e} \succcurlyeq \max \exp(P_i) \}$$

と定める。一般に $(\mathbb{Z}_+^+)^n$ の部分集合 S は,

$$S + (\mathbb{Z}_+^+)^n = S$$

とみたとき, monomial ideal といわれる。 $M(F)$ も monomial ideal の例である。

すなわち, このとき,

多項式 f が $F = \{P_1, \dots, P_k\}$ について M -可約

$$\Leftrightarrow M(F) \cap E(f) \neq \emptyset$$

多項式 f が $F = \{P_1, \dots, P_k\}$ について M -既約

(あるいは M -正規)

$$\Leftrightarrow M(F) \cap E(f) = \emptyset$$

多項式 f が one-step M -reducible to $f^{(1)}$

w.r.t. P_i [記号としては $f \xrightarrow{i} f^{(1)}(F)$]

$$\Leftrightarrow \exists e \in E(f), \exists P_i \in F, \exists m: \text{単項式}$$

$$\text{s.t. } e \geq \max \exp(P_i),$$

$$f^{(1)} = f - m \cdot P_i, \quad f^{(1)} \triangleleft f$$

例 $P_1 = xy - 1, P_2 = x^2 - y, f = x^2y, g = y^2 + x$

$F = \{P_1, P_2\}$ のとき,

f は F に関して M 可約で,

$$x^2y \xrightarrow{1} x \quad (F)$$

$$x^2y \xrightarrow{2} y \quad (F)$$

こゝで, x, y は M -正規である。

g は F に関して M 既約で, M -正規である。

こゝとき,

$\text{hcoef}(P)$: 多項式 P の $\text{head}(P)$ の係数。

と定めると、上記の単項式 m は

$$m = (x^{\#} / \max(P_i)) \cdot (\text{hcoef}(f) / \text{hcoef}(P_i))$$

と表わされる。文脈で、今考えている多項式の組

$F = \{P_1, \dots, P_k\}$ が固定して自明なとき、

$$f \xrightarrow{i} f^{(i)}(F) \quad \text{は単に} \quad f \xrightarrow{i} f^{(i)}$$

と F を略してかく。

また、

$$f \longrightarrow f^{(i)} \iff \exists P_i \in F, f \longrightarrow f^{(i)}$$

$$f \longrightarrow g \iff \exists f_0 = f, \exists f_1, \exists f_2, \dots, \exists f_n = g$$

$$\text{s.t. } f_0 \rightarrow f_1 \rightarrow f_2 \rightarrow \dots \rightarrow f_n$$

と定める。 ($\longrightarrow$ は $\rightarrow$ の transitive and reflexive

closure に他ならない。) このとき、 f は g に M -可約

であること、特に $g \neq f$ (従って、 $g \triangleleft f$) のとき、 f は g

に真に M -可約であること。

例 $F = \{xy - 1, x^2 - y\}$ のとき

$$x^2 y^2 + xy \xrightarrow{1} 2xy \xrightarrow{1} 1$$

$$x^2 y^2 + xy \xrightarrow{2} y^3 + xy \xrightarrow{1} y^3 + 1$$

から、 $x^2 y^2 + xy \twoheadrightarrow 1, x^2 y^2 + xy \twoheadrightarrow y^3 + 1$

$F = \{P_1, P_2, \dots, P_k\}$ で生成されるイデアルとは

$$\text{ideal}(F) = \{h_1 P_1 + h_2 P_2 + \dots + h_k P_k \mid h_i \in R\}$$

なる多項式の集合であり、

$$f \equiv g \pmod{\text{ideal}(F)}$$

とは、

$$f - g \in \text{ideal}(F)$$

のことであり、また、ここで $\pmod{\text{ideal}(F)}$ を単に、 $\pmod{F}$ と略すことにする。次の性質が成立する。

性質 1

$$(1) \quad f \longrightarrow g \Rightarrow f \equiv g \pmod{F} \wedge f \triangleright g$$

$$(2) \quad f \twoheadrightarrow g \Rightarrow f \equiv g \pmod{F} \wedge f \leq g$$

これはイデアルの基本性質から明らかである。ただし、
reduction の方法により、同じ f から派生する正規形でも
一般には等しくならないことに注意しよう。

性質 2

$$\left. \begin{array}{l} f_1 \twoheadrightarrow g \quad (g \text{ は正規}) \\ f_2 \twoheadrightarrow g \quad (\quad) \end{array} \right\} \Rightarrow f_1 \equiv f_2 \pmod{F}$$

は当然に成立するが、 $f_1 \equiv f_2$ でも、 $(f_1 = f_2 \text{ でも})$ 両者の
正規形は一致するとは限らない。

性質3

M -reduction は有限回の step で 停止する。

これは 順序 $\triangleright$ の Noether 性による。

また, 一般には $f \in \text{ideal}(F)$ でも, $f \rightarrow 0(F)$ とは言えない。しかし, F が 正しい条件をみたすとき,
 $f \in \text{ideal}(F) \iff f \rightarrow 0$ がいえることがある。このよ
 うな F が 正しい, 正しい。

Gröbner-Basis の定義

F が G-Basis

$\iff$ " $f \in \text{ideal}(F), f \neq 0 \Rightarrow f$ は F に関して M 可約

況の性質が容易に確かめられるので, G-Basis を構成する方法
 がわかれば, $K[x_1, x_2, \dots, x_n] / \text{ideal}(F)$ における標準形の問題
 は解決できることになる。

性質4. G-Basis の性質

$F = \{P_1, P_2, \dots, P_k\}$ が G-Basis ならば

1) $f \in \text{ideal}(F) \quad f \rightarrow 0 \quad (\text{reduction path})$
 による

2) $f - g \in \text{ideal}(F)$

$\exists h \quad f \rightarrow h, \exists g \rightarrow h$

±2, G -Basis は必ず存在する。 というのは, 一般に

Lemma 1
 $\text{monideal} \subseteq (\mathbb{Z}_0^+)^n$ は有限生成

が成立するので, $S = \{\max \exp(f) \mid f \in \text{ideal}(F)\}$ も monideal である。 S は有限生成である。 その生成元に対応する多項式 (一意には定まらない) の組を $G = \{Q_1, Q_2, \dots, Q_r\}$ とすれば $E(G) = S$ なので, 実際には G は G -Basis となる。

しかし, この存在証明は G -Basis の構成には役立たない。
 G -Basis の構成は多項式の組を多項式の項書換規則 (term rewriting rule) とみなし Knuth-Bendix の Completion-Algorithm をこの M -reduction に適用することにより, 2 とされる。

多項式 P, Q と生成元に含まれていない P, Q は $P=0, Q=0$ とみなせるので, P, Q は

$$\max P \rightarrow -\frac{\text{rest}(P)}{\text{hwef}(P)}, \quad \max Q \rightarrow -\frac{\text{rest}(Q)}{\text{hwef}(Q)}$$

なる書換則とみなせる。 すると, P と Q の両方の書換則を適用できる順序最小の項は $\text{L.C.M}(P, Q)$ である。

$\text{L.C.M}(P, Q)/P = t, \text{L.C.M}(P, Q)/Q = s$ とすると,

$$(tP, \frac{hcoef(P)}{hcoef(Q)} \leq Q)$$

ε P, Q a critical-pair ε " " ,

$$tP - \frac{hcoef(P)}{hcoef(Q)} \leq Q$$

ε $P \times Q$ a S -polynomial ε " " $Sp(P, Q)$ ε 素数。

例 $Sp(xy-1, x^2-y)$

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

$$Sp(x^2-y, -x+y^2)$$

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

$$= xy^2 - y$$

性質 5. S -polynomial ε G -basis

$$G = \{P_1, P_2, \dots, P_k\} \text{ is } G\text{-basis}$$

$$\Leftrightarrow \forall P_i, \forall P_j \quad Sp(P_i, P_j) \longrightarrow 0$$

この証明は簡単である。 M -reduction の

$$1) f \longrightarrow g \Rightarrow t \cdot f \longrightarrow t \cdot g$$

$$2) g_1 \longrightarrow g_2 \Rightarrow f[t \leftarrow g_1] \downarrow f[t \leftarrow g_2]$$

なる性質を用いるのが Buchberger の証明法である。本稿では性質6の証明の際、同様の証明をできることを後ほど示す。性質5を用いて G -basis 構成の算法が可能となる。

算法 1 G -basis

- 1° $G := F$ (F : given set of polynomials)
- 2° G の中から 2 つの f, g をとりだし
 $Sp(f, g)$ の正規形を G に加える。
- 3° すべて Check してなければ 2° へ。

但し、 F は最初から reduce しておくのがよい。

この算法が必ず停止することは、次の lemma に基づく。

LEMMA 2

$\sum (\subseteq (\mathbb{Z}_0^+)^n)$ のどの元も $\geq$ に関して
比較できないならば、 $\sum$ は有限集合。

さて、 $F = \{P_1, P_2, \dots, P_k\}$ とあるとき、 $f \rightarrow_i g$ とりうことは、 $f = g + m \cdot P_i$ なる単項式 m が存在することになる。従って、

$$f \rightarrow g \quad \text{ならば、} \quad f = g + \sum_{i=1}^k h_i P_i \quad \text{--- (*)}$$

とかけらる。 (*) で等号が成立するような多項式 h_i

は, unique ではないが, 1つの reduction-path を定めれば, それに対応する h_i は unique となる。このするとき,

$$f \Rightarrow g \oplus h_1 P_1 \oplus \dots \oplus h_k P_k$$

と書くことにする。すると,

性質 6. M-reduction と付随多項式

$$f \Rightarrow g \oplus h_1 f_1 \oplus \dots \oplus h_k f_k, \quad f \neq g$$

$$\Rightarrow f \geq g, \quad f \geq h_i f_i$$

の成立することは明らかであろう。

§3 代数方程式への応用

G -basis と辞書式順序 (1) と構成すると, 次の性質 7 が成立する。

性質 7. G -Basis と消去

$F \in G\text{-Basis}$ とするとき,

$$\text{ideal}(F) \cap K[x_i, x_{i+1}, \dots, x_n]$$

$$= \text{ideal}(F \cap K[x_i, x_{i+1}, \dots, x_n])$$

ideal $F = (P_1, P_2, \dots, P_k)$ は, 連立方程式

$$P_1 = 0 \wedge P_2 = 0 \wedge \dots \wedge P_k = 0 \quad \dots (4)$$

の零点集合と対応関係をもっている。 (4) が 基礎体 K の代数的閉体 $\overline{K}$ 上で解をもつとき, イテラル F のことを可解 (solvable) といい, その解を F の解と行うことにすると, 性質 7 を利用して可解性の判定・有限個の解の求算のアルゴリズムが構成される。

— 算法 2. 方程式系の可解性の判定 —

イテラル $F = (P_1, P_2, \dots, P_k)$ が与えられたとき,
 F から, F の Gröbner-basis G と順序 ① で
 構成する。(このとき, $G := GB(F)$ とかく。)

$$F \text{ が 非可解} \iff 1 \notin G$$

但し, G -basis の各多項式は $hcoef$ と 1 に正規化してあるものとする。

— 算法 3. 無限可解性の判定 —

$$G := GB(F), \quad F \subseteq K[x_1, x_2, \dots, x_n]$$

F が 有限個の解をもつ。

$$\iff \forall_i (1 \leq i \leq n) \quad x_i^{i_i} \text{ と head term に } \text{多項式が } G \text{ に存在する。}$$

算法4 代数方程式の全根の求解

- $F = (P_1, P_2, \dots, P_k) \subseteq \mathbb{Q}[x_1, x_2, \dots, x_m]$ given
- $G := \{Q_1, Q_2, \dots, Q_m\} := \text{GB}(F)$,
(但し, 各 Q_i は $(Q_1, Q_2, \dots, \check{Q}_i, \dots, Q_m)$ に関して既約になるよう, 必要に応じて $Q_i \in (Q_1, \dots, \check{Q}_i, \dots, Q_m)$ に関する正規形 $\tilde{Q}_i$ ととりかえておくものとする。
このような G -Basis は reduced-Gröbner-Basis といわれる。)
- $Q \in G \cap K[x_m]$ なる $Q(x_m) \in G$ とする。
(算法3より, 有限個の解をもつときは, このような $Q(x_m) \in G$ は必ず存在し, しかも reduced- G -Basis ならば, このような $Q(x_m)$ は唯一つである。)
- $Q(x_m) = 0$ を解き, 解 $x_m = a_m$ を, $Q_1, Q_2, \dots, Q_m$ に代入して得られる多項式を $Q_1^{(m-1)}, \dots, Q_m^{(m-1)}$ とする。
- $Q(x_{m-1}) \in \{Q_1^{(m-1)}, \dots, Q_m^{(m-1)}\} \cap K[x_{m-1}]$
なる $Q(x_{m-1})$ をとり, それらの共通解 $x_{m-1} = a_{m-1}$ を $Q_1^{(m-1)}, \dots, Q_m^{(m-1)}$ に代入して得られる多項式を $Q_1^{(m-2)}, \dots, Q_m^{(m-2)}$ とし, 以下, 恒次 $x_{m-2}, x_{m-3}, \dots$ と消去し, 最終解を得る。

§4 線形不定方程式への応用

$$P_1, P_2, \dots, P_k \in K[x_1, \dots, x_m], \quad f \in K[x_1, \dots, x_m]$$

のとき、線形不定方程式

$$f_1 P_1 + f_2 P_2 + \dots + f_k P_k = f \quad \text{--- (A)}$$

の多項式解 $(f_1, f_2, \dots, f_k)$ について考察しよう。

$F = \{P_1, P_2, \dots, P_k\}$ から reduced G-Basis $G = GB(F)$
 $= \{Q_1, Q_2, \dots, Q_m\}$ と取ると、各 Q_i は

$$Q_i = g_{i1} P_1 + g_{i2} P_2 + \dots + g_{ik} P_k$$

とかけられるので、(A) の解の構造を知りたいには

$$\begin{cases} h_1 Q_1 + h_2 Q_2 + \dots + h_m Q_m = f \\ \{Q_1, Q_2, \dots, Q_m\} \text{ は reduced G-Basis.} \end{cases} \quad \text{--- (B)}$$

の解の構造がわかればよい。従って、以下では (B) の形の線形不定方程式を考えよう。

算法 5 特殊解の構成

$f, G = \{Q_1, Q_2, \dots, Q_m\}$ (reduced G-Basis) が

与えられたとき、(B) の特殊解 $(h_1, \dots, h_m)$ は、

$f \rightarrow 0$ のときのみ存在し、

$$\text{このとき、} \quad f \rightarrow 0 \oplus h_1 P_1 \oplus h_2 P_2 \oplus \dots \oplus h_m P_m$$

ある $(h_1, h_2, \dots, h_e)$ を与える。

従って特殊解を求めることができることばかりでなく、たいてい、

③の一般解を求めるには、

$$\begin{cases} h_1 Q_1 + h_2 Q_2 + \dots + h_m Q_m = f \\ \{Q_1, Q_2, \dots, Q_m\} \text{ は reduced G-Basis.} \end{cases} \quad \text{--- (A)}$$

の一般解がわかればよいことになる。

算法 6. 一般解の構成

③の一般解は

$$Sp(Q_i, Q_j) = t_i Q_i - \frac{c_j}{c_i} t_j P_j$$

(c_i, c_j は Q_i, Q_j の head coefficients)

$$\leadsto 0 \oplus \bar{h}_1 Q_1 \oplus \dots \oplus \bar{h}_m Q_m$$

とあるとき、

$$(\bar{h}_1, \bar{h}_2, \dots, \bar{h}_i - t_i, \dots, \bar{h}_j + \frac{c_j}{c_i} t_j, \dots, \bar{h}_m) \quad \text{--- (D)}$$

ある $m C_2$ 個の生成元で生成される。

この算法は Buchberger 氏によるものであるが、氏はこの証明を公表してはいない。従って以下の証明は筆者によるものである。

(算法 6 の証明)

④の一般解 $(h_1, h_2, \dots, h_m)$ が, ⑤の形の生成元によつて生成されることを $(h_1 Q_1, h_2 Q_2, \dots, h_m Q_m)$ の order に関する帰納法によつて示す。

$(h_1 Q_1, h_2 Q_2, \dots, h_m Q_m) = (0, 0, \dots, 0)$ のとき,

たしかに ⑤の元で生成される。

$(h_1 Q_1, h_2 Q_2, \dots, h_m Q_m)$ の order L 未満の ④の解 $(h_1, h_2, \dots, h_m)$ が ⑤の元で生成されるるとき,
 $(h_1 Q_1, h_2 Q_2, \dots, h_m Q_m)$ の order が L のときも, ④の解 $(h_1, h_2, \dots, h_m)$ が ⑤の元で生成されることを示そう。

$(h_1, h_2, \dots, h_m)$ は ④の解で, $(h_1 Q_1, h_2 Q_2, \dots, h_m Q_m)$ の order が $L (> (0, 0, \dots, 0))$ とする。

$$h_1 Q_1 \geq h_2 Q_2 \geq \dots \geq h_m Q_m \quad \text{--- ①}$$

と仮定しても一般性を失わない。

$h_i Q_i$ の order を $\bar{L}_i$ とし,

$h_i Q_i$ の head monomial は $e_i \cdot M_i$ ($e_i \in K$)

h_i の head monomial は $d_i \cdot m_i$ ($d_i \in K$)

Q_i の head monomial は $c_i \cdot f_i$ ($c_i \in K$)

とする。 (従つて $M_i = m_i \cdot f_i$, $e_i = c_i \cdot d_i$)

$$h_1 Q_1 + h_2 Q_2 + \dots + h_m Q_m = 0 \quad \text{--- ②}$$

の左辺に形式的に表わしたとき、項のうち最大の order のものは、①の仮定より $M_1 = m_1 \cdot g_1$ とある。一方、②の右辺を考えると、 M_1 の係数の和は 0 とななければならない。

従って $h_i Q_i$ ($i=2, \dots, n$) の中には M_1 と head term にもっとも少なくとも 1 つある。①の仮定より $h_2 Q_2$ の head term M_2 は M_1 と一致する。

$$\left. \begin{aligned} h_1 Q_1 &= d_1 \cdot c_1 \cdot m_1 \cdot g_1 + R_1, & R_1 &\triangleleft h_1 Q_1, \\ h_2 Q_2 &= d_2 \cdot c_2 \cdot m_2 \cdot g_2 + R_2, & R_2 &\triangleleft h_2 Q_2, \\ h_3 Q_3 &= d_3 \cdot c_3 \cdot m_3 \cdot g_3 + R_3, & R_3 &\triangleleft h_3 Q_3, \\ && & \\ h_m Q_m &= d_m \cdot c_m \cdot m_m \cdot g_m + R_m, & R_m &\triangleleft h_m Q_m, \end{aligned} \right\} \quad (3)$$

と置く。

$Sp(Q_1, Q_2)$ に対応する ④ の解を

$$(\bar{h}_1 - t_1, \bar{h}_2 + \frac{c_2}{c_1} t_2, \bar{h}_3, \dots, \bar{h}_m) \quad \dots (4)$$

但し、 $g_1 = \max(Q_1)$, $g_2 = \max(Q_2)$, $G = \text{G.C.D.}(g_1, g_2)$

と置くとき、 $t_1 = g_2/G$, $t_2 = g_1/G$ 。

と置く。このとき、 M -reduction の性質より

$$\forall_i \quad \max(t_1 Q_1) = \max(t_2 Q_2) \triangleright \bar{h}_i \cdot Q_i \quad \dots (5)$$

特に、 $t_1 \triangleright \bar{h}_1$, $t_2 \triangleright \bar{h}_2$

が成立してゐる。(ここぞ $\geq$ ではなく $\triangleright$ に注意!)

すなわち、 $M_1 = m_1 g_1 = m_2 g_2$ なる z 、 m_1, m_2 は t_1, t_2

の倍数で、従って $m_1 g_1 = m_2 g_2 = st_1 g_1 = st_2 g_2$ とおける。

$$d_1 s \quad (\bar{h}_1 - t_1, \bar{h}_2 + \frac{c_2}{c_1} t_2, \bar{h}_3, \dots, \bar{h}_m) \quad \dots \textcircled{6}$$

は $\textcircled{6}$ の解を α と、 $(\tilde{h}_1, \tilde{h}_2, \tilde{h}_3, \dots, \tilde{h}_m)$

$$= (h_1 - d_1 s \cdot t_1 + d_1 s \cdot \bar{h}_1, h_2 + \frac{c_2}{c_1} d_1 s \cdot t_2 + d_1 s \cdot \bar{h}_2, \\ h_3 + d_1 s \cdot \bar{h}_3, h_4 + d_1 s \cdot \bar{h}_4, \dots) \quad \dots \textcircled{7}$$

も $\textcircled{6}$ の解である。 $\textcircled{7}$ の order を考えよと

$$(\underline{h_1 - d_1 s \cdot t_1 + d_1 s \cdot \bar{h}_1}) \cdot Q_1 \triangleleft M_1$$

($\because h_1 = d_1 m_1, m_1 = st_1$ より $\underline{\hspace{1cm}}$ は 0 に等しく、

$$s \bar{h}_1 \triangleleft st_1 \text{ より } s \bar{h}_1 g_1 \triangleleft st_1 g_1 = M_1) \quad /$$

$$(h_2 + \frac{c_2}{c_1} d_1 s t_2 + d_1 s \bar{h}_2) \cdot Q_2 \triangleleft M_1$$

$$(\because h_2 g_2 = M_1, st_2 g_2 = M_1, s \bar{h}_2 g_2 \triangleleft st_2 g_2 \triangleleft M_1)$$

$$(h_3 + d_1 s \bar{h}_3) Q_3 \begin{cases} \triangleleft M_1 & (m_3 g_3 = M_1 \text{ のとき}) \\ \triangleleft M_1 & (m_3 g_3 \triangleleft M_1 \text{ のとき}) \end{cases}$$

$$(\because s \bar{h}_3 g_3 \triangleleft st_1 g_1 = M_1)$$

$$(h_4 + d_1 s \bar{h}_4) Q_4 \begin{cases} \triangleleft M_1 & (m_4 g_4 = M_1 \text{ のとき}) \\ \triangleleft M_1 & (m_4 g_4 \triangleleft M_1 \text{ のとき}) \end{cases}$$

が成立しているのぞ、仮定 $\textcircled{1}$ と order の定義より

$$(h_1 Q_1, h_2 Q_2, \dots, h_m Q_m) \triangleright (\underline{\tilde{h}_1 Q_1, \tilde{h}_2 Q_2, \dots, \tilde{h}_m Q_m})$$

$\textcircled{7}$ の解に対応

が成立する。従って、帰納法の仮定により

$(\widetilde{h}_1, \widetilde{h}_2, \dots, \widetilde{h}_m)$ は $\textcircled{D}$ の元で生成される。

一方、今、

$$(h_1, h_2, \dots, h_m) = (\widetilde{h}_1, \widetilde{h}_2, \dots, \widetilde{h}_m) \\ - d_1 S(\underbrace{\widetilde{h}_1 - t_1, \widetilde{h}_2 + \frac{C_2}{C_1} t_2, \widetilde{h}_3, \dots, \widetilde{h}_m}_{\textcircled{D} \text{ の元}})$$

なので、 $(h_1 \theta_1, h_2 \theta_2, \dots, h_m \theta_m)$ の order が L のときも題意は成立する。order $\triangleright$ は多項式の組 $(f_1, \dots, f_m)$ に関して有限の降級列しかもたないのと、従って、order についての帰納法により任意の order $(h_1 \theta_1, \dots, h_m \theta_m)$ に対応する任意の $\textcircled{D}$ の解 $(h_1, h_2, \dots, h_m)$ が $\textcircled{D}$ の type の元で生成されることが示された。(証明終わり)

全く同じ論法で、 $G = \{P_1, P_2, \dots, P_k\}$ に関し、

$$\forall \text{Sp}(P_i, P_j) \Rightarrow 0 \oplus f_1 P_1 \oplus \dots \oplus f_k P_k$$

$$\Rightarrow \forall (g_1, g_2, \dots, g_k) \quad \exists (h_1, h_2, \dots, h_k)$$

$$g_1 P_1 + g_2 P_2 + \dots + g_k P_k \Rightarrow 0 \oplus h_1 P_1 \oplus \dots \oplus h_k P_k''$$

(すなわち性質5) を $(g_1 P_1, g_2 P_2, \dots, g_k P_k)$ の order $\triangleright$ に関する帰納法で示すことができる。また、この論法が Euclid 環上の G -Basis の存在と構成証明とすることができる。

[REFERENCES]

- [1] B.Buchberger, Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems, Aequationes Mathematicae, Vol 4/3.S. 374-383, 1970.
- [2] B.Buchberger, A Theoretical Basis for the reduction of polynomials to canonical forms, ACM SIGSAM Bulletin 39, 19-29, 1976.
- [3] L.Bachmir and B.Buchberger, A Simplified Proof of the Characterization theorem for the Gröbner-bases, ACM SIGSAM Bulletin ,29-34, 1980. Vol 14. No 4.
- [4] B.Buchberger and R.Loos, Algebraic Simplification in Computer Algebra, Springer, 11-43, 1982.
- [5] C.Kollreider and B.Buchberger, An improved Algorithmic Construction of Gröbner bases for Polynomial ideals, Techn. Rep. Nr. 110, Inst. für MATH, Univ. Linz, Austria, 1979.
- [6] B.Buchberger, A criterion for detecting unnecessary reductions in the construction of Groebner bases, Eurosam 79, Springer Lec.Note. in Comp.Sci. No 72, 3-21, 1979.
- [7] B.Buchberger, Grobner Bases: An algorithmic method in Polynomial ideal Theory, CAMP-Publ-Nr83-29.0, Chap6, 1983.
- [8] A.Kandri Rody and Deepak Kapur, Algorithms for computing Gröbner Bases of Polynomil ideals over various Euclidean rings, Proc. of EUROSAM84, 1984.

- [9] A.Kandri Rody and B.D.Saunders, Primality of ideals in polynomial rings, Proc of MACSYMA USER'S CONFERENCE84, 1984.

[1], [2] は Gröbner-Basis に関する オリジナル論文であるが、両者とも記法・証明がわかりにくい。[3], [4] は証明もあり、よりして読むやすい。Gröbner-Basis の構成の効率化については [5], [6] をみると良い。代数方程式の求解の算法とその理論の証明は [7] が詳しい。[7] は参考文献も豊富で Gröbner-Basis について詳しく調べたい人にはお薦めたい。Euclid 環と係数にする多項式イデアルについて同様の理論が成立すること示したのが [8] である。[9] はイデアルの既約性の判定と G-Basis の関連を示している。

Gröbner-Basis の implement は、Buchberger を中心に数式処理システム SAC1 上で行なわれている。このプログラムは東大センターにもある。日本では、藤瀬哲朗（電通大…当時、現三菱総研）が REDUCE 2.0 上に、筆者が muSIMP/muMATH 83 上に implement している。