記 号 処 理 34-3
(1 9 8 5.1 1.1 3)

ベキ級数イデアルのGröbner基底

GRÖBNER BASIS OF IDEAL OF CONVERGENT POWER SERIES

H. Kobayashi*), A. Furukawa**), T. Sasaki***)

*) Department of Mathematics, Nihon University
Kanda, Chiyoda-ku, Tokyo 101, Japan

**) Department of Mathematics, Tokyo Metropolitan University
Fukazawa, Setagaya-ku, Tokyo 158, Japan

***) The Institute of Physical and Chemical Research
Wako-shi, Saitama 351-01, Japan

Abstract

This paper develops a theory of Gröbner basis of ideal of convergent power series. The basis is constructed by calculating "S-power series" successively, where the S-power series is an analogue of S-polynomial and constructed so as to cancel the head terms of initial polynomials of two power series. By using the finite generation property of monoideal, it is proved that a finite number of successive constructions of S-power series provide us a Gröbner basis of power series ideal.

§1. Introduction

In discussing polynomial ideals and related problems, the Gröbner bases are very useful ideal bases [1]. The Gröbner bases allow us to solve the following problems within reasonable computation steps [2]: determine whether or not a given polynomial is an element of a given ideal, calculate the intersection of two polynomial ideals, simplify a polynomial with polynomial side-relations, solve a system of algebraic equations with/without parameters, calculate the polynomial solutions of a linear equation with polynomial coefficients, and so on.

A construction method of Gröbner basis for polynomials in $K[x_1,\ldots,x_n]$, with K a number field, was discovered by Buchberger in 1965 [1]. Lauer [3] extended the Buchberger's method to include the polynomials with coefficients in the ring of integers. However, as far as the authors know, no attempt was made to construct a Gröbner basis of an ideal in a ring of power series. In this paper, we construct a Gröbner basis on a ring of convergent power series $K\{x_1,\ldots,x_n\}$ and discuss some properties of it.

As we will see below, our construction is an almost straightforward extension of the method for polynomials, but we used some results of the theory of monoideal to prove the finite generation property of the Gröbner basis for power series. We follow to Hironaka [4] to use monoideals in discussing ideals of infinite power series. Because the theory of monoideal is essential in our extension, §2 is devoted to survey this theory briefly. The development of a theory of Gröbner basis of power series ideal is done in §4 and §5.

§2. Monoideal

Let Z_0 be the set of non-negative integers, and Z_0^n the Cartesian product of Z_0 with n a positive integer. An element A of Z_0^n is written as $(\alpha_1,\ldots,\alpha_n)$ and we define $|A| = \alpha_1 + \cdots + \alpha_n$.

Definition I-1 [monoideal]. A subset I_M of Z_0^n is a monoideal if

$$I_M + Z_0^n = I_M. \quad \square$$

Figure 1 illustrates a monoideal in Z_0^2, where all the lattice points inside the shaded area constitute the monoideal and the lattice points (1,3) and (2,2) are generators of the monoideal.

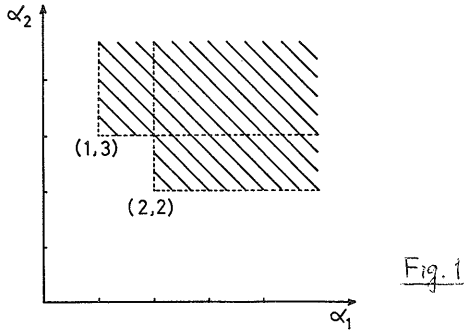

Fig. 1

Proposition I-1. A monoideal I_M is finitely generated. That is, there exist a finite number of elements $A_1, \ldots, A_s$ in I_M satisfying

$$I_M = \bigcup_{i=1}^{s} (A_i + Z_0^n). \quad \square$$

Proof. We use an induction on n. When $n = 1$, it is obvious that I_M is generated by a single element $A_1 = (\alpha_1)$, $\alpha_1 = \min\{|A| \mid A \in I_M\}$.

Next, assuming that every monoideal in Z_0^n, $n < k$, is finitely generated, we consider the case of $n = k$. Let

$$\hat{I}_M = \{(\alpha_1,\ldots,\alpha_{k-1}) \mid (\alpha_1,\ldots,\alpha_{k-1},\alpha_k) \in I_M\},$$

then $\hat{I}_M$ is obviously a monoideal in Z_0^{k-1}. Hence, by induction assumtion, there exist a finite number of generators $\hat{A}_1, \ldots, \hat{A}_\ell$ such that $\hat{I}_M = \bigcup_{i=1}^{\ell} (\hat{A}_i + Z_0^{k-1})$. For $i=1,\ldots,\ell$, let $\hat{A}_i = (\alpha_{i1},\ldots,\alpha_{i,k-1})$ and $\alpha_{ik} = \min\{\alpha_k \mid (\alpha_{i1},\ldots,\alpha_{i,k-1},\alpha_k) \in I_M\}$. Denoting $(\alpha_{i1},\ldots,\alpha_{i,k-1},\alpha_{ik})$ by A_i, we decompose I_M as $I_M = \bigcup_{i=1}^{\ell} (A_i + Z_0^k) + I'_M$, with $I'_M \cap [\bigcup_{i=1}^{\ell} (A_i + Z_0^k)] = \phi$. Then, each element $(\alpha_1,\ldots,\alpha_k)$ of I'_M satisfies $\alpha_k < \bar{\alpha}_k = \max\{\alpha_{1k},\ldots,\alpha_{\ell k}\}$. For each α in $\{0,\ldots,\bar{\alpha}_k - 1\}$, let $\hat{I}_{M,\alpha} = \{(\alpha_1,\ldots,\alpha_{k-1}) \mid (\alpha_1,\ldots,\alpha_{k-1},\alpha) \in I'_M\} + Z_0^{k-1}$, then $\hat{I}_{M,\alpha}$ is a monoideal in Z_0^{k-1} and it is finitely generated by induction assumption. Therefore, I_M is finitely generated. $\square$

Corollary to Prop. I-1. Let $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_s \subseteq \cdots$ is an increasing sequence of monoideals, then there exists an integer T such that

$$I_T = I_{T+1} = \cdots. \quad \square$$

Proof. Let $I_\infty = \bigcup_{i=1}^{\infty} I_i$, then we can see that I_∞ is a monoideal. Prop. I-1 assures that there are a finite number of elements $A_1, \ldots, A_t$ of I_∞ such that $I_\infty = \bigcup_{i=1}^{t} (A_i + Z_0^n)$. For each i, $1 \leq i \leq t$, there is a number J(i) such that $A_i \in I_{J(i)}$. Let $T = \max\{J(1),\ldots,J(t)\}$, then $A_i \in I_T$ for $i=1,\ldots,t$. So $I_\infty = \bigcup_{i=1}^{t} (A_i + Z_0^n) \subseteq I_T$. Hence, we see $I_\infty \subseteq I_T \subseteq I_{T+1} \subseteq \cdots \subseteq I_\infty$. $\square$

Let $K[x_1,\ldots,x_n]$ be a ring of polynomials in n variables $x_1, \ldots, x_n$ with coefficients in a number field K. We abbreviate $K[x_1,\ldots,x_n]$ to $K[x]$. Let $f_1, \ldots, f_r$ be elements of $K[x]$, and I the ideal $(f_1,\ldots,f_r)$ in $K[x]$ generated by $f_1, \ldots, f_r$. We express f in $K[x]$ as $f = \sum_A a_A x^A$, where $A = (\alpha_1,\ldots,\alpha_n)$, $a_A \in K$, and x^A is an abbreviation of $x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$.

We call $\alpha_1 + \cdots + \alpha_n$ the degree of the term x^A, i.e., $\deg(x^A) = |A|$.

Definition I-2 [lexicographic order $\rangle$ in Z_0^n].

For any elements $A = (\alpha_1,\ldots,\alpha_n)$ and $B = (\beta_1,\ldots,\beta_n)$ of Z_0^n, we define $A \rangle B$ iff there is an integer i, $1 \leqq i \leqq n$, such that $\alpha_j = \beta_j$ for all j, $1 \leqq j < i$, and $\alpha_i > \beta_i$. □

Note. The following theory is valid if we use another definition of order so far as Z_0^n becomes a well-ordered Abelian semigroup by the order.

Definition I-3 [exponent set, leading exponent, head term].

Exponent set of f, leading exponent of f, and head term of f, which are abbreviated to exs(f), lex(f), and ht(f), respectively, are defined as follows:

$$\mathrm{exs}(f) = \{A \in Z_0^n \mid a_A \neq 0 \text{ in } f = \sum a_A x^A\},$$

lex(f) $\in$ exs(f), lex(f) $\rangle$ any other element of exs(f),

ht(f) = a term $a_A x^A$ of f, where $A = \mathrm{lex}(f)$. □

Definition I-4. The lex(I), with I a polynomial ideal, is a subset of Z_0^n defined by

$$\mathrm{lex}(I) = \{\mathrm{lex}(f) \mid f \neq 0,\ f \in I\}.$$ □

Proposition I-2. The set $E = \mathrm{lex}(I)$ is a monoideal. □

Proof. The relation $E \subseteq E + Z_0^n$ is trivial because $(0,\ldots,0) \in Z_0^n$, so we have only to show $E + Z_0^n \subseteq E$. Let $A + B$ be any element of $E + Z_0^n$ such that $A \in E$ and $B \in Z_0^n$. By definition, there exists a polynomial f in I such that $\mathrm{lex}(f) = A$. Since $\mathrm{lex}(x^B f) = A + B$ and I is an ideal, we have $x^B f \in I$. That is, $A + B \in E$. □

§4. Gröbner basis for truncated power series

Let $C\{z_1,\ldots,z_n\}$ be a ring of convergent power series with coefficients in the complex number field C. We abbreviate $C\{z_1,\ldots,z_n\}$ to $C\{z\}$. Let $f_1, \ldots, f_r$ be elements of $C\{z\}$, and I the ideal $(f_1,\ldots,f_r)$ in $C\{z\}$ generated by $f_1, \ldots, f_r$. We express f in $C\{z\}$ as $f = \sum_A a_A z^A$, where $A = (\alpha_1,\ldots,\alpha_n)$, $a_A \in C$, and z^A is an abbreviation of $z_1^{\alpha_1} z_2^{\alpha_2} \ldots z_n^{\alpha_n}$.

Before defining a Gröbner basis for power series, we consider in this section a power series ideal modulo $(z_1,\ldots,z_n)^{M+1}$. We call a Gröbner basis for this truncated power series an M-Gröbner basis. In this and the next sections, we omit several short proofs which are analogous to those given in §3.

Definition II-1 [order $\rhd$ in Z_0^n].

For any element A and B of Z_0^n, we define $A \rhd B$ iff either $|A| < |B|$ or $A \rangle B$ when $|A| = |B|$. □

Notes. We can formulate the following theory by using another definition of $\rhd$. For example, if we define $\rhd$ by using a weight function for variables, we obtain the theory in a quite general form. The important point in such a definition is that the lower degree terms are of higher order, and this is essential for power series.

Definition II-2 [initial polynomial].

The initial polynomial of f, which is abbreviated to in(f), is the sum of the lowest degree terms of f:

$$\mathrm{in}(f) = \sum_{|A| = \text{lowest}} a_A z^A.$$ □

Definition II-3 [order, leading exponent, head term].

Order of f, leading exponent of f, and head term of f, which are abbreviated to ord(f), lex(f), and ht(f), respectively, are defined as follows:

$$\mathrm{ord}(f) = \deg(\mathrm{in}(f)),$$
$$\mathrm{lex}(f) = \mathrm{lex}(\mathrm{in}(f)),$$
$$\mathrm{ht}(f) = \mathrm{ht}(\mathrm{in}(f)),$$

where the lex and ht in the right hand side are defined by Def. I-3. □

Definition II-4 [M-equality of power series].

Two power series f and g in $C\{z\}$ are equal within degree M, and denoted by $f =_M g$, iff $\mathrm{ord}(f-g) > M$. □

Definition II-5 [M-reducibility of power series].

Let $F = \{f_1,\ldots,f_r\}$ be a subset of $C\{z\}$, and put $E = \bigcup_{i=1}^{r} [\mathrm{lex}(f_i) + Z_0^n]$. Let a power series h in $C\{z\}$ be decomposed as $h = h_d + h_{d+1} + \cdots$, where h_i is the sum of all terms of degree i of h. The h is called reducible within degree M (abbreviated to M-reducible) with respect to F if $\mathrm{exs}(h_i) \cap E \neq \phi$ for some $i \leqq M$, and h is called M-irreducible w.r.t. F if $\mathrm{exs}(h_i) \cap E = \phi$ for all $i \leqq M$. □

Definition II-6 [M-reduction of power series].

With the notations in Def. II-5, let $h' \in C\{z\}$. The h' is called an M-reduction of h w.r.t. F and written as $h \xrightarrow[F,M]{} h'$ if one of the followings holds:

(a) $h' = h$ when h is M-irreducible w.r.t. F,

(b) $h' = h - c \cdot x^A f_k$ when $\mathrm{exs}(h_i) \cap [\mathrm{lex}(f_k)+Z_0^n] \neq \phi$ for some $i \leqq M$, where c and A are determined as follows: let $\mathrm{ht}(f_k) = a_{A_k} x^{A_k}$, hence h contains a term proportional to x^{A_k} and let the term be $b_{A+A_k} x^{A+A_k}$, $|A+A_k| \leqq M$, then $c = b_{A+A_k} / a_{A_k}$. □

Definition II-7 [M-normal form of power series].

Suppose h in $C\{z\}$ is reduced successively as $h \xrightarrow[F,M]{} h' \xrightarrow[F,M]{} \cdots \xrightarrow[F,M]{} \tilde{h}$, and if $\tilde{h}$ is M-irreducible w.r.t. F then $\tilde{h}$ is called an M-normal form of h w.r.t. F. We denote the reduction of h to its normal form $\tilde{h}$ by $h \xrightarrow[F,M]{} \tilde{h}$. In particular, we write $h \xrightarrow[F,M]{} 0$ if $\tilde{h} =_M 0$. □

Proposition II-1. Let $F = \{f_1,\ldots,f_r\}$ be a subset of $C\{z\}$ and M a positive integer. Given a power series h in $C\{z\}$, we can reduce h to an M-normal form $\tilde{h}$ w.r.t. F by a finite sequence of reductions. □

Proof. In this proof, we denote the sum of all the k-th degree terms of h by h_k, so $h = h_d + h_{d+1} + \cdots$. If $d > M$ then h is already M-irreducible w.r.t. F, so we assume $d \leqq M$. We put $\mathrm{lex}(f_i) = A_i$, $i=1,\ldots,r$, and $E = \bigcup_{i=1}^{r} (A_i + Z_0^n)$.

Step 1. We show, by the transfinite induction w.r.t. $\mathrm{lex}(h_d)$, that there is a finite sequence of M-reductions

$$h_d \xrightarrow[F,M]{} \cdots \xrightarrow[F,M]{} \tilde{h}_d + h'_{d+1} + h'_{d+2} + \cdots,$$

where $\tilde{h}_d$ is either 0 or M-irreducible w.r.t. F.

Step 1-1. When $\mathrm{lex}(h_d) = (0,\ldots,0)$, or $d = 0$.

If $\mathrm{ord}(f_i) > 0$ for all i then h_0 is obviously M-irreducible w.r.t. F, otherwise there is a reduction such that $h_0 \xrightarrow[F,M]{} 0 +$ (terms of degree $\geqq$ 1). Hence, the claim in Step 1 is right in this case.

Step 1-2. Assuming that the claim in Step 1 is right for any h'_d such that $\mathrm{lex}(h'_d) \lhd A$, we show the claim is right for h_d with $\mathrm{lex}(h_d) = A$. If $\mathrm{exs}(h_d) \cap E = \phi$ then there is nothing to prove, so we assume $\mathrm{exs}(h_d) \cap$

$E \neq \phi$. Let B be the highest order element of $exs(h_d) \cap E$ and assume that $B = lex(f_k) + C$, that is

$$h_d = \tilde{h}_d^{(1)} + c_B z^B + h^{(2)},$$

where [exponent of any term of $\tilde{h}_d^{(1)}$] $\rhd$ B and B $\rhd$ $lex(h^{(2)})$. By definition, we have either $\tilde{h}_d^{(1)} = 0$ or $exs(\tilde{h}_d^{(1)}) \cap E = \phi$. The rest part of h_d, or $c_B z^B + h^{(2)}$, can be reduced as

$$c_B z^B + h^{(2)} \xrightarrow[F,M]{} c_B z^B + h^{(2)} - (c_B / a_{A_k}) z^C \cdot f_k$$
$$= h^{(2)} - (c_B / a_{A_k}) z^C \cdot [f_k - ht(f_k)].$$

Writing the right hand side expression as $h'^{(2)}$, we see $lex(h'^{(2)}) \lhd B \trianglelefteq lex(h_d)$. By induction assumption, there exist a finite sequence of reductions $h'^{(2)} \xrightarrow[F,M]{} \cdots \xrightarrow[F,M]{} \tilde{h}^{(2)}$, where the d-th degree part of $\tilde{h}^{(2)}$ is either 0 or M-irreducible w.r.t. F. Thus, Step 1 is proved.

Step 2. By the Step 1, we have $h \xrightarrow[F,M]{} \cdots \xrightarrow[F,M]{} \tilde{h}_d + h'_{d+1} + h'_{d+2} + \cdots$, where $\tilde{h}_d$ is either 0 or M-irreducible w.r.t. F. Next, we apply the reduction procedure of Step 1 to h'_{d+1}. This procedure does not alter the terms of degree less than d+1, hence $h \xrightarrow[F,M]{} \cdots \xrightarrow[F,M]{} \tilde{h}_d + \tilde{h}_{d+1} + h''_{d+2} + \cdots$, where $\tilde{h}_{d+1}$ is either 0 or M-irreducible w.r.t. F. Continuing this procedure, we can reduce h to $\tilde{h}$. □

Definition II-8 [M-Gröbner basis of power series ideal].

Let $I = (f_1,\ldots,f_r)$ be an ideal in $C\{z\}$ and M a positive integer. A subset $G = \{g_1,\ldots,g_s\}$ of $C\{z\}$ is called an M-Gröbner basis of I if the following conditions are satisfied:

(1) $(g_1,\ldots,g_s) = I$,

(2) for any element f of I, $f \xrightarrow[G,M]{} 0$. □

Definition II-9 [S-power series].

Let f and g be power series in $C\{z\}$, and put $ht(f) = a_A x^A$ and $ht(g) = b_B x^B$. Let u and v be monomials satisfying $LCM(x^A,x^B) = u \cdot x^A = v \cdot x^B$, where LCM is the least common multiple. Then, S-power series of f and g, to be abbreviated to Sp(f,g), is defined by

$$Sp(f,g) = u \cdot f - (a_A / b_B) v \cdot g. \quad \square$$

Proposition II-2. (For the proof, refer to Corollary to Prop. I-4.)

Let G be an M-Gröbner basis of an ideal in $C\{z\}$, and h a power series in $C\{z\}$. Let $\tilde{h}_1$ and $\tilde{h}_2$ be M-normal forms of h w.r.t. G, then $\tilde{h}_1 = \tilde{h}_2$. □

Theorem 2. Let $I = (g_1,\ldots,g_s)$ be an ideal in $C\{z\}$, G the set $\{g_1,\ldots,g_s\}$, and M a positive integer. If

$$Sp(g_i,g_j) \xrightarrow[G,M]{} 0 \quad \text{for any pair } (g_i,g_j),\ i \neq j,\ 1 \leq i,j \leq s,$$

then G is an M-Gröbner basis of I. □

Proof. Let $E = \bigcup_{i=1}^{s} [lex(g_i) + Z_0^n]$ and f be any element of I with lex(f) = A. We have only to show $f \xrightarrow[G,M]{} 0$. If $A \in E$ then f can be reduced directly and we can replace f by f', $lex(f') \lhd A$, so we have only to consider the case of $A \notin E$.

Since $f \in I$, there exist $h_1, \ldots, h_s$ in $C\{z\}$ satisfying

$$f = h_1 g_1 + \cdots + h_s g_s.$$

For i=1,...,s, put

$$ht(g_i) = a_{A_i} z^{A_i}, \quad ht(h_i) = b_{B_i} z^{B_i},$$

hence $lex(h_i g_i) = A_i + B_i$. Let D be the highest order element of $\{A_i+B_i \mid i=1,\ldots,s,\ h_i \neq 0\}$. Without loss of generality, we assume $D = A_1+B_1 = \cdots = A_\sigma+B_\sigma$, $D \rhd A_j+B_j$ for all $j > \sigma$. Then, putting $h_i =$

$b_{B_i} z^{B_i} + h_i'$, i=1,...,s, we decompose f as

$$f = f^{(1)} + f^{(2)},$$

$$f^{(1)} = \sum_{i=1}^{\sigma} b_{B_i} z^{B_i} g_i, \qquad f^{(2)} = \sum_{i=1}^{\sigma} h_i' g_i + \sum_{i=\sigma+1}^{s} h_i g_i.$$

We see $\mathrm{lex}(f^{(2)}) \lhd D$. If $\sigma = 1$ then $D = A \in E$, contradicting to the assumption $A \notin E$. Hence, $\sigma > 1$ and we can rewrite $f^{(1)}$ as

$$\begin{aligned} f^{(1)} = {} & (a_{A_1} b_{B_1}) \cdot (z^{B_1} g_1 / a_{A_1} - z^{B_2} g_2 / a_{A_2}) \\ & + (a_{A_2} b_{B_2} + a_{A_1} b_{B_1}) \cdot (z^{B_2} g_2 / a_{A_2} - z^{B_3} g_3 / a_{A_3}) \\ & + \cdots\cdots \\ & + (a_{A_{\sigma-1}} b_{B_{\sigma-1}} + \cdots + a_{A_1} b_{B_1}) \\ & \quad \times (z^{B_{\sigma-1}} g_{\sigma-1} / a_{A_{\sigma-1}} - z^{B_\sigma} g_\sigma / a_{A_\sigma}) \\ & + (a_{A_\sigma} b_{B_\sigma} + \cdots + a_{A_1} b_{B_1}) \cdot (z^{B_\sigma} g_\sigma / a_{A_\sigma}). \end{aligned}$$

We first note that the last term of the above expression is 0. To see this, we consider the sum of terms of exponent D in $f^{(1)}$, which is

$$\sum_{i=1}^{\sigma} a_{A_i} b_{B_i} z^{A_i+B_i} = (a_{A_1} b_{B_1} + \cdots + a_{A_\sigma} b_{B_\sigma}) \cdot z^D.$$

If this expression is not zero then $A = \mathrm{lex}(f) = A_1 + B_1$, contradicting to the assumption $A \notin E$. We next consider the j-th term, $j \leqq \sigma - 1$, of the r.h.s. expression. Remembering the definition of S-power series, we see [the j-th term] $= u \cdot \mathrm{Sp}(g_j, g_{j+1})$ with u a monomial. By the assumption of theorem, $\mathrm{Sp}(g_j, g_{j+1}) \xrightarrow[G,M]{} 0$. Hence, we find $f^{(1)} \xrightarrow[G,M]{} 0$.

The $f^{(2)}$ is of the same form as f, so we can continue the above reduction making $f \xrightarrow[G,M]{} \cdots \xrightarrow[G,M]{} f'$, $\mathrm{lex}(f') \lhd \mathrm{lex}(g_i)$, i=1,...,s. That is $f \xrightarrow[G,M]{} 0$. □

Because the M-Gröbner basis is for truncated power series, it can be constructed by a finite number of steps. In fact, the following procedure allows us to calculate the M-Gröbner basis:

Procedure BUCHBERGER

input: an ideal $I = (f_1, \ldots, f_r)$ in $K[x]$.

output: a Gröbner basis $G = \{g_1, \ldots, g_s\}$ of I.

```
G := {g_1:=f_1 , ..., g_r:=f_r};
P := {(g_i,g_j) | g_i,g_j ε G, i ≠ j};
while P ≠ φ do begin
    p_ij := a pair (g_i,g_j) in P;
    P := P - {p_ij};
g̃ := an M-normal form of Sp(g_i,g_j) w.r.t. G;
    if g̃ ≠ 0 then begin
        P := P ⋃ {(g,g̃) | g ε G};
        G := G ⋃ {g̃};
        end;
    end.
```

In the above procedure, we must calculate M-normal form and S-power series as truncated power series, of cource. The M-Gröbner basis will be useful when we use truncated power series for approximate calculations.

§5. Gröbner basis of power series ideal

Now, we investigate the Gröbner basis of power series ideal for which we must consider the terms of arbitrarily high degree. This poses us an interesting problem when we stand on a viewpoint of constructive algebra. We discuss this point in the next section, and we first define a Gröbner basis of a power series ideal and investigate the properties generally.

Definition III-1 [tangential ideal].

Let $I = (f_1,\ldots,f_r)$ be an ideal in $C\{z\}$. The tangential ideal of I, to be abbreviated to $\bar{I}$, is defined as

$$\bar{I} = in(I) = \{in(f) \mid 0 \neq f \in I\}C[x]. \quad \square$$

Definition III-2 [Gröbner basis of power series ideal].

Let $I = (f_1,\ldots,f_r)$ be an ideal in $C\{z\}$. A subset $G = \{g_1,\ldots,g_s\}$ of I is called a Gröbner basis of I if the following conditions are satisfied:

(1) $(g_1,\ldots,g_s) = I$,

(2) for any f in I and for any positive integer M, $f \xrightarrow[G,M]{} 0$. $\square$

Note that the Gröbner basis of power series is defined in terms of M-Gröbner basis which is constructive.

Now, we consider the following procedure.

Procedure PS-GRÖBNER

input: an ideal $I = (f_1,\ldots,f_r)$ in $C\{z\}$.

output: a Gröbner basis $G = \{g_1,\ldots,g_s\}$ of I.

$G_0 := \{f_1,\ldots,f_r\}$; $M := 0$;

LOOP: $M := M+1$; $G_M := G_{M-1}$;

$P := \{(g_i,g_j) \mid g_i,g_j \in G_M,\ g_i \neq g_j\}$;

while $P \neq \phi$ do begin

$p_{ij} :=$ a pair (g_i,g_j) in P;

$P := P - \{p_{ij}\}$;

$\tilde{g} :=$ an M-normal form of $Sp(g_i,g_j)$ w.r.t. G_M;

if $\tilde{g} \neq_M 0$ then begin

$P := P \cup \{(g,\tilde{g}) \mid g \in G_M\}$;

$G_M := G_M \cup \{\tilde{g}\}$;

end;

end;

(**) if $G_M = G_{M-1}$ and

[termination condition] is satisfied then return G_M;

goto LOOP.

Note that, in the line (**), the [termination condition] is not specified yet. In the following, we use the notation G_M defined above.

Proposition III-1. With the above notations, let f be any element of I. Then, for any positive integer L, $L \leqq M$, we have $f \xrightarrow[G_M,L]{} 0$. $\square$

Proof. The case $L = M$ is trivial, so we assume $L < M$. By the construction, $G_L \subseteq G_M$, so we write $G_L = \{g_1,\ldots,g_\ell\}$ and $G_M = \{g_1,\ldots,g_\ell,\ldots,g_m\}$. Then, for all j in $\{\ell+1,\ldots,m\}$, there exist h'_{j1}, ..., $h'_{j\ell}$ in $C\{z\}$ satisfying

$$g_j = h'_{j1}g_1 + \cdots + h'_{j\ell}g_\ell.$$

Since $f \in I$, there exists h_1, ..., h_ℓ, .., h_m in $C\{z\}$ satisfying

$$\begin{aligned} f &= h_1g_1 + \cdots + h_\ell g_\ell + \cdots + h_m g_m \\ &= (h_1 + \textstyle\sum_j h'_{j1})g_1 + \cdots + (h_\ell + \sum_j h'_{j\ell})g_\ell. \end{aligned}$$

Reducing f w.r.t. G_L as in the proof of Th. 2, we find $f \xrightarrow[G_M,L]{} 0$. $\square$

Theorem 3. With the above notations, there exists a positive integer T such that G_T is a Gröbner basis of I. $\square$

Proof. By virtue of Th. 2, we have only to show the existence of G_T such that $Sp(g_i,g_j) \xrightarrow[G_T,L]{} 0$ for any g_i and g_j in G_T and for any positive integer L. We put $E_M = \bigcup_{i=1}^{m} [lex(g_i) + Z_0^n]$. Since $E_1 \subseteq E_2 \subseteq \cdots$ is an increasing sequence of monoideals, Corollary to Prop. I-1 assures

that there exists an integer T such that $E_T = E_{T+1} = \cdots$. Prop. III-1 assures that our claim is right for $L \leqq T$. So, we consider the case $L > T$. Suppose $Sp(g_i,g_j) \xrightarrow[G_T,L]{} \tilde{g}$, $lex(\tilde{g}) \notin E_L$. Then, by the construction, there is an integer ℓ, $\ell > L$, such that $\tilde{g} \in G_\ell$. This means $lex(\tilde{g}) \in E_\ell$, but $E_\ell = E_T$ by definition of T, so we are lead to a contradiction. □

Theorem 4. Let $I = (f_1,\ldots,f_r)$ be an ideal in $C\{z\}$ and $\bar{I} = in(I)$ a tangential ideal of I. Let $G = \{g_1,\ldots,g_s\}$ be a Gröbner basis of I, and put $E = \bigcup_{i=1}^{s} [lex(g_i) + Z_0^n]$, then $lex(\bar{I}) = E$. (The lex in this equation is for polynomials.) □

Proof. Put $\bar{E} = lex(\bar{I})$, then $E \subseteq \bar{E}$ because $lex(g_i) \in \bar{E}$ for all i in $\{1,\ldots,s\}$. Next, we show $A \in E$ for any element A of $\bar{E}$. Since $A \in \bar{E}$, there exists a homogeneous polynomial $\bar{f}$ in $\bar{I}$ such that $lex(\bar{f}) = A$. Since $\bar{I} = in(I)$, $\bar{f}$ can be expressed as $\bar{f} = in(h_1f_1 + \cdots + h_rf_r)$, with h_1, ..., h_r in $C\{z\}$. Putting $f = \sum h_if_i$, we see $f \in I$ and $lex(f) = A$. Since G is a Gröbner basis of I, we have $f \xrightarrow[G,M]{} 0$ for any integer $M \geq |A|$. This means $A = lex(f) \in E$, because if not so then ht(f) cannot be reduced w.r.t. G. □

§6. On constructivity of a Gröbner basis for infinite power series

紙面の都合で省略するが、この部分には今後なすべき仕事が残っている。

References

[1] B. Buchberger, "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.

[2] B. Buchberger, "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., 1984.

[3] M. Lauer, "Canonical representations for the residue classes of a polynomial ideal (German)", Diploma Thesis, Univ. of Kaiserslautern (FRG), Dept. of Mathematics, 1976.

[4] H. Hironaka, "Resolution of singularities of an algebraic variety over a field of characteristic zero: I, II", Annals of Math. 79, 1964, pp. 109-326.