代数幾何ゼミ

石井大海

早稲田大学基幹理工学部
数学科四年

2013 年 04 月 15 日

消去理論

消去定理と拡張定理

- 多項式系から変数を体系的に消去する手法を学ぶ.
- 主な戦略は次の二つの主定理（今回の発表範囲）
  - 消去定理
    - 講義や [CLO06] では辞書式順序について示しているが，ここでは一般化した形を紹介する.
  - 拡張定理
    - [CLO06] では終結式の理論を使うので最後に遅延されているが，ここでは [楫 13] での証明を紹介する.
    - 系の簡単な証明は恐らく次回以降

消去理論の例 I

方程式系

$$\begin{cases} x^2 + y + z = 1 \\ x + y^2 + z = 1 \\ x + y + z^2 = 1 \end{cases} \tag{3.1}$$

を解くために,

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

とおいて，辞書式順序で Gröbner 基底を計算すると,

$$\begin{cases} g_1 = x + y + z^2 - 1 \\ g_2 = y^2 - y - z^2 + z \\ g_3 = 2yz^2 + 4z^4 - z^2 \\ g_4 = z^6 - 4z^4 + 4z^3 - z^2 \end{cases} \tag{3.2}$$

消去理論の例 II

を得る．最後の式は z のみから成るので，これを解いて g_2, g_3, g_1 に代入すれば，

$$(1,0,0) \quad (0,1,0) \quad (0,0,1)$$
$$(-1+\sqrt{2}, -1+\sqrt{2}, -1+\sqrt{2})$$
$$(-1-\sqrt{2}, -1-\sqrt{2}, -1-\sqrt{2})$$

という解を得る．この解法は次の二つの段階に分けることが出来る．

消去ステップ 元の方程式系から x, y を消去して， z のみを含む式が得られた．

拡張ステップ 単純な方程式 $g_4 = 0$ の根を求めた後，それを元の方程式の解へと拡張出来た．

こうした操作が非常に一般的に行える，というのが消去理論．

消去定理について

消去イデアル

上でやった操作を一般化する.

Def. 1 (消去イデアル)

$k[X_1, \ldots, X_n]$ のイデアル $I = \langle f_1, \ldots, f_s \rangle$ の第 ℓ-消去イデアル I_ℓ とは,

$$I_\ell := I \cap k[X_{\ell+1}, \ldots, X_n]$$

で定義される $k[X_{\ell+1}, \ldots, X_n]$ のイデアルのことである.

これがイデアルとなることは非常に易しい（演習 1).
消去イデアルは Gröbner 基底を用いて簡単に計算することが出来る. その為に必要となるのが消去順序の概念.

消去順序 I

[CLO06] では演習問題 5 で ℓ-消去型単項式順序という概念が，
[楫 13] では ℓ-消去順序，または $\mathbf{X}$-消去順序が定義されている．
両者は若干違う概念であるので，両方を紹介する．

Def. 2 (消去型，消去順序)

1. ([CLO06]). 単項式順序 $>$ が ℓ-消去型（ℓ-elimination type）であるとは，$X_1, \ldots, X_\ell$ を含む単項式が，含まないような単項式より常に大となることである．
2. ([楫 13]). 単項式順序 $>$ が $\{X_1, \ldots, X_\ell\}$-消去順序，第 ℓ-消去順序であるとは，任意の $\alpha, \beta \in \mathbb{Z}_{\geq 0}^{\ell}, \gamma, \delta \in \mathbb{Z}_{\geq 0}^{n-\ell}$ に対し，

$$\mathbf{X}^{\alpha} > \mathbf{X}^{\beta} \Rightarrow \mathbf{X}^{\alpha}\mathbf{Y}^{\gamma} > \mathbf{X}^{\beta}\mathbf{Y}^{\delta}$$

となることである．この条件式の各辺を，
$(\alpha, 0) > (\beta, 0) \Rightarrow (\alpha, \gamma) > (\beta, \delta)$ と略記することがある．

消去順序 II

明らかに，(2) の方が (1) よりも強い条件である．即ち，次が成立する．

Prop.

単項式順序 $>$ が (2) の意味で ℓ-消去順序であれば，(1) の意味で ℓ-消去型となる．

Proof.

$>$ を ℓ-消去順序とする．このとき，$>$ が単項式順序であることから任意の $0 \neq \alpha \in \mathbb{Z}^{\ell}_{\geq 0}$ について $(\alpha, 0) > (0, 0)$．よって，

$$(\alpha, \gamma) > (0, \delta)$$

となる．これは，$X_1, \ldots, X_\ell$ を含むような任意の単項式が含まない単項式より大である，ということである．よって $>$ は ℓ-消去型の単項式順序である． ∎

消去順序 III

逆は一般に不成立．それを見るため，消去順序の例を紹介する．

Example. (消去順序の例)

(a) $X_1 > \cdots > X_n$ で定まる辞書式順序は，任意の ℓ について (2) の意味で ℓ-消去順序となり，従って (1) の意味でも ℓ-消去型．

(b) $(\alpha, \gamma) >_\ell (\beta, \delta)$

$$\stackrel{\text{def}}{\Longleftrightarrow} |\alpha| > |\beta| \vee [|\alpha| = |\beta| \wedge (\alpha, \gamma) >_{\mathit{grevlex}} (\beta, \delta)]$$

により定まる順序は (1) の意味で ℓ-消去型だが，(2) の意味での消去順序にはならない（但し $|\alpha| = a_1 + \cdots + a_\ell$）．例えば，$x > y > z > w, \mathbf{X} = (x, y), \mathbf{Y} = (z, w)$ として上の順序を考えると，$x > y$ だが $xw < yz$ となる．

(c) $(\alpha, \gamma) >_{p,\ell} (\beta, \delta) \stackrel{\text{def}}{\Longleftrightarrow} \alpha >_{\mathit{grevlex}} \beta \vee [\alpha = \beta \wedge \gamma >_{\mathit{grevlex}} \delta]$ により定まる順序 $>_{p,\ell}$ は (2) の意味で ℓ-消去順序となるので，従って (1) の意味でも ℓ-消去型となる．

消去順序であることの証明 I

単項式順序については明らか．残った二つがそれぞれ消去型，消去順序でることを示す．まず単項式順序であることを示す為，次の定義をしておく（第二章四節演習問題 10, 12）．

Def. (重みつき順序，直積順序)

- $>_\sigma$ を単項式順序，$\mathbf{u} \in \mathbb{Z}^n_{\geq 0}$ とする．この時，重みつき順序 $>_{\mathbf{u},\sigma}$ を次のように定める．

$$\alpha >_{\mathbf{u},\sigma} \beta \overset{\text{def}}{\Longleftrightarrow} \mathbf{u}\cdot\alpha > \mathbf{u}\cdot\beta \vee [\mathbf{u}\cdot\alpha = \mathbf{u}\cdot\beta \wedge \alpha >_\sigma \beta]$$

- $>_\sigma, >_\tau$ を単項式順序とする．この時，直積順序 $>_{\sigma,\tau}$ を次のように定める．

$$(\alpha,\gamma) >_{\sigma,\tau} (\beta,\delta) \overset{\text{def}}{\Longleftrightarrow} \alpha >_\sigma \beta \vee [\alpha = \beta \wedge \gamma >_\tau \delta]$$

消去順序であることの証明 II

Claim

$>_{\mathbf{u},\sigma}, >_{\sigma,\tau}$ はそれぞれ単項式順序である.

Proof.

$\alpha >_{\mathbf{u},\sigma} \beta \Leftrightarrow (\mathbf{u}\cdot\alpha, \alpha) >_{lex,\sigma} (\mathbf{u}\cdot\beta, \beta)$ となっているので，直積順序 $<_{\sigma,\tau}$ が単項式順序となっていることを示せば十分である.

全順序性. σ, τ が全順序であることから明らか.

加法性. これも σ, τ の加法性から直ちに従う.

整列性. $\emptyset \neq S \subseteq \mathbb{Z}^{\ell}_{\geq 0} \times \mathbb{Z}^{n-\ell}_{\geq 0}$ として，これが最小元を持つことを示す. ここで,

$$\mu = \min_{\sigma} \left\{ \alpha \in \mathbb{Z}^{\ell}_{\geq 0} \,\middle|\, (\alpha, \beta) \in S \right\}, \nu = \min_{\tau} \left\{ \beta \in \mathbb{Z}^{n-\ell}_{\geq 0} \,\middle|\, (\mu, \beta) \in S \right\}$$

とおけば，$(\mu, \nu) \in S$ が S の $>_{\sigma,\tau}$ に関する最小元となる. よって，整列性も成立. ∎

消去順序であることの証明 III

これを使えば，次のように $(b), (c)$ を言い換えることが出来る．

- $\alpha >_\ell \beta \Leftrightarrow \alpha >_{\mathbf{u}_\ell, \mathit{grevlex}} \beta$ （ただし $\mathbf{u}_\ell = (\underbrace{1, \ldots, 1}_{\ell個}, 0, \ldots, 0)$）
- $\alpha >_{p,\ell} \beta \Leftrightarrow \alpha >_{\mathit{grevlex}(\ell), \mathit{grevlex}(n-\ell)} \beta$
  （ただし $\mathit{grevlex}(k)$ は $\mathbb{Z}^k_{\geq 0}$ 上の次数付き逆辞書式順序）

よって単項式順序となることは OK．あとはそれぞれ ℓ-消去型ないし消去順序であることを示せばよい．

消去順序であることの証明 IV

$>_\ell$ が ℓ-消去型であること.

$0 \neq \alpha \in \mathbb{Z}^\ell_{\geq 0}, \gamma, \delta \in \mathbb{Z}^{n-\ell}_{\geq 0}$ とすると,

$$\mathbf{u}_\ell \cdot (\alpha, \gamma) = (1, \ldots, 1) \cdot \alpha + 0 \cdot \gamma = |\alpha| > 0$$
$$\mathbf{u}_\ell \cdot (0, \delta) = (1, \ldots, 1) \cdot 0 + 0 \cdot \delta = 0 + 0 = 0$$

なので $(\alpha, \gamma) >_\ell (0, \delta)$. よって $>_\ell$ は ℓ-消去型の単項式順序. ∎

$>_{p,\ell}$ が ℓ-消去順序であること.

$(\alpha, 0) >_{p,\ell} (\beta, 0) \Leftrightarrow \alpha >_{grevlex} \beta$ であるので, 直積順序の定義から直ちに $(\alpha, \gamma) >_{p,\ell} (\beta, \delta)$ が従う. ∎

二つの順序の違いは？

- 異なる二つの「消去順序」の定義を見て，それらが実際に異なることを示した．
- どちらも，ある意味で辞書式順序の一般化になっている．
- 消去定理・拡張定理でそれぞれどういう役割を果すのか？
  - $\Rightarrow$ 消去定理では (1) の消去型の単項式順序を，拡張定理では (2) の消去順序を使えばいい（拡張定理の証明に (1) は使えない）

消去定理

以上を用いて，一般化された消去定理を証明出来る．

Th. 3 (消去定理)

$I : k[\mathbf{X}, \mathbf{Y}]$ のイデアル　$>$: (1) の意味での $\mathbf{X}$-消去型単項式順序
$G : >$に関する I の *Gröbner* 基底
$\Rightarrow G_s = G \cap k[\mathbf{Y}]$ は $I \cap k[\mathbf{Y}]$ の *Gröbner* 基底

Proof.

$G_\ell = G \cap k[\mathbf{Y}]$ が $I_\ell = I \cap k[\mathbf{Y}]$ の Gröbner 基底となっていることを示す．特に，$f \in I_\ell$ として $LT(f) \in \langle LT(g_\ell) \rangle$ を示せばよい．
$f \in I_\ell \subseteq I$ とすると，G が I の Gröbner 基底であることがら $LT(f) \in \langle LT(G) \rangle$ となる．よって，単項式イデアルの補題から $\exists g \in G$ s.t. $LT(g) \mid LT(f)$ となる．ここで $f \in k[\mathbf{Y}]$ より f は $\mathbf{X}$ を含まないので，それを割り切る $LT(g)$ も $\mathbf{X}$ を含まない．
今，$LT(g)$ は ℓ-消去型順序 $>$ に関する先頭項だったから，g の他の項は $LT(g)$ 未満であるので $\mathbf{X}$ を含まない．よって $g \in k[\mathbf{Y}]$ となり，$g \in G \cap k[\mathbf{Y}] = G_\ell$ となる．よって，$LT(f) \in \langle LT(G_\ell) \rangle$ となるので，G_ℓ は I_ℓ の Gröbner 基底となる． ∎

パラメタ消去と消去型単項式順序

- 以上の結果から，$>_{lex}, >_{\ell}, >_{p,\ell}$ のいずれを用いても，方程式系からパラメータを消去することが出来る．
- どの順序を用いるのがよいのか？
  - 一般に重み付き順序による ℓ-消去型順序を用いるのが最も効率がよく，綺麗な基底が求まる．
  - 場合によっては辞書式順序の方が速い場合もある．
  - （ここでベンチマークのグラフを出す）

解の拡張

$V(I)$ の点を計算するために，座標を一つずつ求めていくことは，$V(I_\ell)$ の点を求めてからそれを $V(I_{\ell-1})$ に拡張していくということ．つまり，

$$I_{\ell-1} = \langle g_1, \ldots, g_r \rangle \subseteq k[X_\ell, \ldots, X_n]$$

として，既に持っている解 $a_{\ell+1}, \ldots, a_n$ について，

$$g_1(a_\ell, x_{\ell+1}, \ldots, x_n) = \cdots = g_r(a_\ell, x_{\ell+1}, \ldots, x_n) = 0$$

となるような x_ℓ を求めるような操作．解を代入してしまえば $g_1, \ldots, g_r \in k[X_\ell]$ となって，1 変数多項式環は PID だったから，これらの GCD を取ってその零点を求めればよい．

解の拡張が出来ない例

解の拡張がいつでも出来るとは限らない.

Example.

$I = \langle xy - 1, xz - 1 \rangle \subseteq \mathbb{R}[x, y, z]$ として $x > y > z$ なる辞書式順序で Gröbner 基底を計算すると,

$$I = \langle y - z, xz - 1 \rangle$$

となる. 最初の方程式から $y = z$ が得られるが, このうち部分解 $y = z = 0$ は $xz = 1$ を満たすように拡張出来ない.

Example.

$I = \langle x^2 - y, x^2 - z \rangle \subseteq \mathbb{R}[x, y, z]$ として同様に辞書式順序で Gröbner 基底を計算すると,

$$I = \langle y - z, x^2 - z \rangle$$

となる. 最初の方程式から $y = z$ が得られるが, このうち $y = z < 0$ のとき $x^2 = z < 0$ は実数解を持たず, $\mathbb{R}$ の範囲では部分解を完全解に拡張出来ない.

幾つかの定義と記号 I

こうした状況を一般的に述べる為に，幾つかの定義と記号を導入しておく．

Def. (部分解，完全解)

$\pi_\ell : \mathbb{A}^n \to \mathbb{A}^{n-\ell}; (a_1, \ldots, a_n) \mapsto (a_{\ell+1}, \ldots, a_n)$ とする．このとき $\pi_\ell(V(I)) \subseteq V(I_s)$ に注意する．

- $\mathbf{b} = (b_{\ell+1}, \ldots, b_n) \in V(I_\ell)$ を I の部分解と云う．$\mathbf{a} \in \mathbb{A}^\ell$ によって $(\mathbf{a}, \mathbf{b}) \in V(I)$ と出来るとき，$(\mathbf{a}, \mathbf{b})$ を I の完全解 といい，$\mathbf{b}$ は 完全解 $(\mathbf{a}, \mathbf{b})$ に拡張されると云う．
- $\mathbf{b} \in \mathbb{A}^{n-\ell}$ が固定されているとき，$h \in k[\mathbf{X}, \mathbf{Y}]$ に対し，$\bar{h} := h(\mathbf{X}, \mathbf{b}) \in k[\mathbf{X}]$ と書く．同様にイデアル $I \subseteq k[\mathbf{X}, \mathbf{Y}]$ についても $\bar{I} := \left\{ \bar{h} \,\middle|\, h \in I \right\}$ と定める．これは $\mathbf{b}$ の代入により引き起こされる全射準同型 $\vartheta : k[\mathbf{X}, \mathbf{Y}] \to k[\mathbf{X}]$ の像であり，従って $k[\mathbf{X}]$ のイデアルとなる．

幾つかの定義と記号 II

Notation. ($\mathbf{X}$ に関する多重次数)

(2) の意味での $\mathbf{X}$-消去順序を一つ固定する．この時,

$$\deg_{\mathbf{X}}(f) := \left(\text{先頭項 } LM(f) \text{ の } \mathbf{X} \text{ に関する多重次数}\right)$$
$$LC_{\mathbf{X}}(f) := \left(f \in (k[\mathbf{Y}])[\mathbf{X}] \text{ と見た時の } \deg_X(f) \text{ 次の係数}\right)$$

この時，f は次のように書き下せる.

$$f = LC_{\mathbf{X}}(f)\mathbf{X}^{\deg_{\mathbf{X}}(f)} + \left(\mathbf{X} \text{ についての多重次数} < \deg_{\mathbf{X}}(f) \text{ の項}\right)$$

消去順序の性質

証明に先立って次の補題を証明しておく.

Lemma. (消去順序の補題)

$<$ を (2) の意味での ℓ-消去順序とする. この時以下が成立.

(i) $f \in k[\mathbf{X}, \mathbf{Y}], \mathbf{b} \in \mathbb{A}^{n-\ell}$ について, $\deg \bar{f} \leq deg_{\mathbf{X}} f$. 特に,

$$\overline{LC_{\mathbf{X}}(f)} \neq 0 \Leftrightarrow \deg \bar{f} = \deg_{\mathbf{X}} f$$

(ii) $f, g \in k[\mathbf{X}, \mathbf{Y}]$ に対し次が成立.

$$\deg g \leq \deg f \Rightarrow \deg_{\mathbf{X}} g \leq \deg_{\mathbf{X}} f \tag{3.3}$$

よって,

$$\deg g \leq \deg f, f \in k[\mathbf{Y}] \Rightarrow g \in k[\mathbf{Y}] \tag{3.4}$$

が成立し, 特に次が云える.

$$LT(f) \in k[\mathbf{Y}] \Rightarrow f \in k[\mathbf{Y}] \tag{3.5}$$

(iii) $f_1, \ldots, f_s \in k[\mathbf{X}, \mathbf{Y}](f_i \neq 0) \quad f = \sum_{i=1}^{s} f_i \neq 0$ のとき,

$$\deg f = \max_{1 \leq i \leq s} \deg(f_i) \Rightarrow \deg_{\mathbf{X}}(f) = \max_{1 \leq i \leq s} \deg(f_i)$$

消去順序の補題の証明 I

Proof.

(1) $LC_{\mathbf{X}}(f)$ は先頭項の次数の $\mathbf{Y}$ を含む係数だったから自明.

(2) (3.3) の対偶が正に消去順序の定義だった．条件 (3.4) に関しては (1) の消去型の定義の対偶であり，消去順序は消去型の単項式順序となるので成立．(3.5) は (3.4) から従う．よって示された.

(3) $\deg f \geq \deg f_i$ なので (2) の (3.4) から $\deg_{\mathbf{X}} f \geq \deg_{\mathbf{X}} f_i$ となる．よって $\deg_{\mathbf{X}} f \geq \max_{1 \leq i \leq s} \deg_{\mathbf{X}} f_i$ となる．逆向きの順序関係は自明.

∎

消去順序の補題の証明 II

Rem.

上の証明から，(*i*) および (*ii*) の (3.4) および (3.5) は (1) の意味での消去型単項式順序でも成立することがわかる．
しかし，(*ii*) の (3.3) および (*iii*) は不成立．前者の例は既に見た．後者については $f = yz + xw$ として，重み付き消去順序を考えてやれば $\deg(f) = yz = \max\{yz, xw\}$ だが $\deg_X(f) = \deg_{\mathbf{X}}(yz) = y \neq x = \max\{y, x\} = \max\{\deg_{\mathbf{X}}(yz), \deg_{\mathbf{X}}(xw)\}$

拡張定理の証明

遂に拡張定理を示す．1 変数の場合を示すが，演習問題 1 から順次拡張出来るのでこれで問題はない．

Th. 4 (拡張定理（一変数版）)

$k = \bar{k}, I : k[X, \mathbf{Y}]$ のイデアル, $V := V(I) \subseteq \mathbb{A}^n, I_1 := I \cap k[\mathbf{Y}]$ とする．
部分解 $\mathbf{b} = (b_2, \ldots, b_n) \in V(I_1)$ に対し，$\overline{LC_X(f)} \neq 0$ を満たすような $f \in I$ が存在するなら， $\mathbf{b}$ は完全解に拡張される．
すなわち，$f(X, \mathbf{Y}) = c_N(\mathbf{Y})X^N + \cdots + c_0(\mathbf{Y})$ $(c_k \in k[\mathbf{Y}])$ かつ $c_N(\mathbf{b}) \neq 0$ となるような f があれば，$\mathbf{a}$ により $(\mathbf{a}, \mathbf{b}) \in V(I)$.

証明の準備

拡張定理の証明で重要な役割を果たすのが次の命題である.

Prop. 16

$I : k[X, \mathbf{Y}]$ のイデアル, $< : X$-消去順序 として,
$G : <$による I の *Gröbner* 基底 とする. $\mathbf{b} \in \mathbb{A}^{n-1}$ として,
$\vartheta : \mathbb{A}^n \to \mathbb{A}^{n-1}$ を $\mathbf{b}$ の代入が引き起こす準同型とする. $\bar{I} := \vartheta[I]$ と置くとき, 次が成立する.

$$\exists g \in G \left[\overline{LC_X(g)} \neq 0 \right]$$

$$\Rightarrow \begin{cases} \overline{LC_X(g)} \neq 0 \text{ で } \deg_X g \text{ が最小となるような} \\ g \in G \text{ があって} \bar{I} = \langle \bar{g} \rangle \end{cases}$$

補題の証明 I

$T := \left\{ g \in G \,\middle|\, \overline{LC_X(g)} \neq 0 \right\}$ は仮定より空ではないので，
$\deg_X g$ が最小となるような g が確かに取れる．そこで
$M := \min_{g \in T} \deg_X g$ とおく．証明に入る前に，この時，次が成立す
ることを帰納法により示す．

$$(\forall L \in \mathbb{N})(\forall h \in G)\left[\deg_X h < M \Rightarrow \deg \bar{h} \leq \deg_X h - L\right] \qquad (*)$$

つまり，$\deg_X h < M$ ならば必然的に $\bar{h} = 0$ でなくてはならない，
ということである．

(i) $L = 1$ のとき．消去順序の補題 (i) より $\deg \bar{h} < \deg_X h$ であり，$\deg_X h < M$ とすると M の T 上の最小性より $\overline{LC_X(h)} = 0$ となる．よって再び補題より $\deg \bar{h} < \deg_X h$. よって $\deg \bar{h} \leq \deg_X h - 1$ となる．

補題の証明 II

(ii) $L+1$ のとき．帰納法の仮定は，

$$(\forall h \in G)\, \deg_X h < M \Rightarrow \deg \bar{h} \leq \deg_X h - L$$

である． $m := \deg_X h < M$ とする．M の T 上の最小性より $\overline{LC(h)} = 0$．ここで，

$$S := LC_X(g)X^{M-m}h - LC_X(h)g \in I$$

を考えると，これにより g, h の先頭項同士が打消し合うので，$\deg_X$ は下がる．よって $\deg_X S < M$．$\overline{LC_X(g)} \in k \setminus \{0\}$ なので，

$$\begin{aligned} \deg \bar{S} &= deg(\overline{LC_X(g)}X^{M-m}\bar{h} - \overline{LC_X(h)}\bar{g}) \\ &= deg(\overline{LC_X(g)}X^{M-m}\bar{h}) \\ &= M - \deg_X h + \deg \bar{h} \end{aligned} \tag{3.6}$$

補題の証明 III

また，S を基底 G によって割り算した結果を，

$$S = \sum_{p \in G} A_p p \quad (\deg(A_p p) \leq \deg S)$$

とすると，G は X-消去順序に関する基底だったから，消去順序の補題 (*iii*) より，

$$M > \deg_X S \geq \deg_X(A_p p) = \deg_X A_p + \deg_X p \geq \deg_X p$$

よって帰納法の仮定から，

$$\deg \bar{p} \leq \deg_X p - L$$

となる．一方，$\deg \overline{A_p} \leq \deg_X A_p$ だったから，

$$\deg \overline{A_p} + \deg \bar{p} \leq \deg_X A_p + \deg_X p - L < M - L$$

補題の証明 IV

よって,

$$\deg \bar{S} \leq \max_{A_p \neq 0}(\deg \bar{A}_p + \deg \bar{p}) < M - L \tag{3.7}$$

従って (3.6), (3.7) より,

$$\begin{aligned} \deg \bar{h} &= \deg \bar{S} + \deg_X h - M \\ &< M - L + \deg_X h - M = \deg_X h - L \\ \therefore \deg \bar{h} &\leq \deg_X h - (L+1) \end{aligned}$$

以上から示された. ∎

これを用いて $\bar{I} = \langle \bar{g} \rangle$ を示す. それには特に I の基底 G の元について考えればよいので, $h \in G$ を取って, $\bar{h} \in \langle \bar{g} \rangle$ を示せば十分である. $m := \deg_X h$ についての帰納法で示そう (一変数について考えているので自然数についての変則的な完全帰納法).

補題の証明 V

(i) $m < M$ の時．$(*)$ より $\bar{h} = 0$ でなければ矛盾．よって $\bar{h} = 0 \in \langle \bar{g} \rangle$．

(ii) $m \geq M$ の時．$S := LC_X(g)h - LC_X(h)X^{m-M}g \in I$ とおくと，これは g, h よりも $\deg_X$ が小さくなるので，$\deg_X S < m$．基底により $S = \sum_{p \in G} A_p p$ と標準表示されているとする．$(*)$ の証明と同様にして，$\deg_X p \leq \deg_X S < m$ となる．よって，帰納法の仮定より $\bar{p} \in \langle \bar{g} \rangle$ となる．よって，$\bar{S} = \sum_{p \in G} \overline{A_p} \bar{p} \in \langle \bar{g} \rangle$ であり，S の定義から，$\overline{LC_X(g)}\bar{h} = \underbrace{\bar{S}}_{\in \langle \bar{g} \rangle} + \underbrace{\overline{LC_X(h)}X^{m-M}\bar{g}}_{\in \langle \bar{g} \rangle} \in \langle \bar{g} \rangle$ となる．

今，g の取り方から $k \ni \overline{LC_X(g)} \neq 0$ であるので，$\bar{h} \in \langle \bar{g} \rangle$ である．

以上より示された． ∎

証明の準備そのに

次の補題も用いる．これは簡単な背理法で示せるので，証明は省略する．

Lemma.

前の定理と同じ記号法の下で，

$$(\exists f \in I)\overline{LC_X(f)} \neq 0 \Rightarrow (\exists g \in G)\overline{LC_X(g)} \tag{3.8}$$

拡張定理の証明

I に関し，1 の意味での X-消去順序（例えば辞書式順序や直積によるもの）に関する Gröbner 基底 G を取る．$f \in I$ が $\overline{LC_X(f)} \neq 0$ を満たすとすると，補題の (3.8) より $g \in G$ で $\overline{LC_X(g)} \neq 0$ となるものが取れる．すると，命題より特に $\bar{I} = \langle \bar{g} \rangle$ であり $\deg_X$ が最小であるとして構わない．
$\deg_X g = 0$ とすると，$g \in k[\mathbf{Y}]$ となるので $g \in I_1$ となるが，$\mathbf{b} \in V(I_1)$ なので $\overline{LC_X(g)} = \bar{g} = g(b) = 0$ となり矛盾．よって $\deg_X g > 0$ である．$\overline{LC_X(g)} \neq 0$ より消去順序の補題 (i) から $\deg \bar{g} = \deg_X g > 0$ となる．よって，k が代数閉体であることから，$\bar{g} \in k[X]$ は k に少なくとも根を一つ持つ．そこで $\bar{(g)}(a) = 0$ とすると，$a \in V(\bar{g}) = V(\bar{I})$ なので，$(a, \mathbf{b}) \in V(\bar{I}) \times \{\mathbf{b}\} = (\pi_1|_V)^{-1}(\mathbf{b})$．よって $(a, \mathbf{b}) \in V$ となる．

∎

参考文献

[CLO06] David Cox, John Little, and Donal O'Shea. Ideals, Varieties, and Algorithms. Ed. by S. Axler and K.A. Ribet. Third. Undergraduate Texts in Mathematics. Springer, 2006.

[楫 13] 楫元. “グレブナー基底は面白い！. ——「代数幾何学入門」への入門——”. 講義録. 2013.