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 05 月 13 日

前回までの復習

- 消去理論：文字の消去と解の拡張
- 文字消去の為の単項式順序：ℓ-消去型 [CLO06] と ℓ-消去順序 [楫 13]
  - 単項式順序 $>$ が ℓ-消去型（ℓ-elimination type）$\Leftrightarrow X_1, \ldots, X_\ell$ 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
  - 単項式順序 $>$ が ℓ-消去順序（ℓ-elimination order）$\Leftrightarrow \mathbf{X}^\alpha > \mathbf{X}^\beta \Rightarrow \mathbf{X}^\alpha \mathbf{Y}^\gamma > \mathbf{X}^\beta \mathbf{Y}^\delta$
  - 消去定理には両方使えるが，[楫 13] での拡張定理の証明には消去順序しか使えない
  - 消去順序ならば消去型だが，逆は不成立.
  - 辞書式順序・直積による消去順序は消去順序．しかし重みによる順序は消去型だが消去順序ではない.

消去定理

消去型の単項式順序を用いれば，一般化された消去定理を証明出来るのだった.

Th. 1 (消去定理)

$I : k[\mathbf{X}, \mathbf{Y}]$ のイデアル　$>$: $\mathbf{X}$-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

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に対応した．
- 解の拡張がいつでも出来るとは限らない．
  1. 係数体が代数的閉体でない場合：
     $I = \langle x^2 - y, x^2 - z \rangle \subseteq \mathbb{R}[x, y, z]$ として辞書式順序で Gröbner 基底を計算すると，$I = \langle y - z, x^2 - z \rangle$ となり，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．
  2. 「先頭項」が消える場合：$I = \langle xy - 1, xz - 1 \rangle \subseteq \mathbb{R}[x, y, z]$ として辞書式順序で 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．

幾つかの定義と記号 I

以下，簡単のため ℓ-消去順序についてのみ考える．

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)

$\mathbf{X}$-消去順序を一つ固定する．この時,

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

この時，f は次のように書き下せる．

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

消去順序の性質

補題は既に示した．特に (ii) の (3.2) および (3.3) に関しては ℓ-消去型でも成立したのだった．

Lemma. (消去順序の補題)

$<$ を 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．

$$\deg g \leq \deg f \Rightarrow \deg_{\mathbf{X}} g \leq \deg_{\mathbf{X}} f \tag{3.1}$$

よって，

$$\deg g \leq \deg f, f \in k[\mathbf{Y}] \Rightarrow g \in k[\mathbf{Y}] \tag{3.2}$$

が成立し，特に次が云える．

$$LT(f) \in k[\mathbf{Y}] \Rightarrow f \in k[\mathbf{Y}] \tag{3.3}$$

(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，

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

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. 2 (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，

$$\begin{aligned} \deg \bar{S} &= deg(\overline{LC_X(g)}X^{M-m}\bar{h} - \overline{LC_X(h)}\bar{g}) \\ &= deg(\overline{LC_X(g)}X^{M-m}\bar{h}) \\ &= M - \deg_X h + \deg \bar{h} \end{aligned} \tag{3.4}$$

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,

$$\deg \bar{S} \leq \max_{A_p \neq 0}(\deg \bar{A}_p + \deg \bar{p}) < M - L \tag{3.5}$$

従って (3.4), (3.5) 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，

$$(\exists f \in I)\overline{LC_X(f)} \neq 0 \Rightarrow (\exists g \in G)\overline{LC_X(g)} \tag{3.6}$$

拡張定理の証明

I に関し，**??** 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 (3.6) 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．

∎

拡張定理の系

拡張定理の次の形の系はよく使うが，上とは異なる方法で証明することも出来る．

Cor. 17 (拡張定理；一変数・定数係数版)

$k = \bar{k}$　$I \subseteq k[X, \mathbf{Y}] : k[X, \mathbf{Y}]$ のイデアル として，
$V := V(I)$　$I_1 := I \cap k[\mathbf{Y}]$ とする．このとき，$\mathrm{LC}_X(f) \in k^\times$ を満たすような $f \in I$ が存在するならば，任意の部分解 $\mathbf{b} \in V(I_1)$ は完全解 $(a, \mathbf{b}) \in V(I)$ に拡張される．

系の証明 I

$\pi_1(V(I)) \supseteq Z(I_1)$ を示せばよい．以下では対偶を示す．すなわち，$\mathbf{b} \in \mathbb{A}^{n-1}$ を取って，

$$\mathbf{b} \notin \pi_1(V(I)) \Rightarrow \mathbf{b} \notin V(I_1)$$

を示す．それには結局，$\mathbf{b} \notin \pi_1(V(I))$ として，$g(\mathbf{b}) \neq 0$ となる $g \in I_1$ の存在を示せば十分である．
系の前提から，$\mathrm{LC}_X(f) \in k^\times$ となる $f \in I$ が存在し，イデアルの性質から f はモニックであるとしてよい．そこで $\mathrm{LT}(f) = X^N$ とする．この時，次が成立する．

Claim

任意の $h \in k[X, \mathbf{Y}]$ に対し，ある $g \in I$ と $h_i(\mathbf{b}) = 0$ を満たす $h_i \in k[\mathbf{Y}](1 \leq i \leq N-1)$ があって，次のように書ける．

$$h = g + h_0 + h_1 X + \cdots + h_{N-1} X^{N-1}$$

系の証明 II

主張の証明.

$\mathbf{b} \notin \pi_1(V(I))$ なので，$(\pi_1|_V)^{-1}(\mathbf{b}) = \emptyset$ となる．
$(\pi_1|_V)^{-1}(\mathbf{b}) = V(\bar{I}) \times \{\mathbf{b}\}$ だったので，$V(\bar{I}) = \emptyset$ となる．すると，一変数における弱零点定理により，$\bar{I} = k[X]$ となる．よって，任意の $h \in k[X, \mathbf{Y}]$ に対し，$\bar{h} \in k[X] = \bar{I}$ となるので，ある $g' \in I$ により $\bar{h} = \bar{g'}$ とできる．そこで，$h' = h - g'$ とおけば，$h = h' + g'$ であり，g' の取り方から $\bar{h'} = \bar{h} - \bar{g'} = 0$ となる．h' を $k[\mathbf{Y}]$ 上の X についての多項式とみなして f で割り算する：

$$h' = qf + \sum_{i=1}^{N-1} h_i X^i$$

∎

系の証明 III

証明のつづき.

ここで， $\mathbf{Y} \mapsto \mathbf{b}$ という代入により $\bar{h}' = 0$ となるので， $k[X]$ における等式

$$-\bar{q}\bar{f} = \sum_{i=1}^{N-1} h_i(\mathbf{b}) X^i$$

が得られる．$\deg(\bar{f}) = N$ であり，右辺の次数は高々 $N-1$ 次であるので， $\bar{q} = 0$ でないと矛盾．よって必然的に $h_i(\mathbf{b}) = 0$ となる．今，定義より

$$h = g' + h' = g' + qf + \sum h_i X^i$$

であるので， $g = g' + qf$ と置けばこれが求めるものである．

∎

系の証明 IV

これで証明の準備は整った．上の主張において
$h = 1, X, X^2, \ldots, X^{N-1}$ とおいて，それぞれに対して次を満たすような $g_i \in I, h_{ij} \in k[\mathbf{Y}]$ $(1 \leq i, j \leq N-1, h_{ij}(\mathbf{b}) = 0)$ を取る：

$$
\begin{array}{ccccccccc}
1 & = & h_{00} & + & \cdots & + & h_{0N-1}X^{N-1} & + & g_0 \\
X & = & h_{10} & + & \cdots & + & h_{1N-1}X^{N-1} & + & g_1 \\
 & & \vdots & & \vdots & \ddots & \vdots & & \vdots \\
X & = & h_{10} & + & \cdots & + & h_{1N-1}X^{N-1} & + & g_1
\end{array}
$$

行列を使って書き直せば，次のようになる．

$$
E \begin{bmatrix} 1 \\ X \\ \vdots \\ X^{N-1} \end{bmatrix} = \underbrace{\begin{bmatrix} h_{00} & h_{01} & \cdots & h_{0N-1} \\ h_{10} & h_{11} & \cdots & h_{1N-1} \\ \vdots & \vdots & \ddots & \vdots \\ h_{N-10} & h_{N-11} & \cdots & h_{N-1N-1} \end{bmatrix}}_{=H} \begin{bmatrix} 1 \\ X \\ \vdots \\ X^{N-1} \end{bmatrix} + \begin{bmatrix} g_0 \\ g_1 \\ \vdots \\ g_{N-1} \end{bmatrix}
$$

系の証明 V

移項して,

$$(E - H) \begin{bmatrix} 1 \\ X \\ \vdots \\ X^{N-1} \end{bmatrix} = \begin{bmatrix} g_0 \\ g_1 \\ \vdots \\ g_{N-1} \end{bmatrix}$$

両辺に $E - H$ の余因子行列（教科書では「随伴行列」となっているが間違い？(それだと ${}^t\bar{A}$？)） $\tilde{H}$ を掛ければ,

$$\det(E - H) \begin{bmatrix} 1 \\ X \\ \vdots \\ X^{N-1} \end{bmatrix} = \tilde{H} \begin{bmatrix} g_0 \\ g_1 \\ \vdots \\ g_{N-1} \end{bmatrix} \tag{3.7}$$

系の証明 VI

となる．実は，$g = \det(E - H)$ とすると，これが求める g であることがわかる．$h_{ij} \in k[\mathbf{Y}]$ より $g \in k[\mathbf{Y}]$ である．また，式 (3.7) の一行目を展開すれば,

$$\det(E - H) = \tilde{h_0}0 \underbrace{g_0}_{\in I} + \cdots + \tilde{h_0}_{N-1} \underbrace{g_{N-1}}_{\in I} \in I$$

となるので $g \in I$．よって， $g \in k[\mathbf{Y}] \cap I = I_1$ となる．また，主張より各 $h_{ij} = 0$ となるので,

$g(\mathbf{b}) = \det(E - O) = \det E = 1 \neq 0$．よって示された． ∎

消去順序と拡張定理に関する注意

- 上の証明において $\mathrm{LC}_X(f)$ を取る所では，[楫 13] の意味での X-消去順序を用いなくてはいけない.
  - しかし，これは単に「代入する前に X についての次数が最大のものの係数を選べばよい」ということ.
  - 証明の中で取っているのであって，実際の計算には消去順序の種類の差は関与しない.
  - 系の証明においては，そもそも性質を用いていない.
- なので，消去イデアルの計算に関しては [CLO06] の意味での 1-消去型を用いればよい.
  - もちろん，複数の文字を消去して一つずつ計算していくような場合は，辞書式順序を使うことになるが.

参考文献

[CLO06] David Cox, John Little, and Donal O'Shea.
Ideals, Varieties, and Algorithms.
Undergraduate Texts in Mathematics. Springer, third edition, 2006.

[楫 13] 楫元.
グレブナー基底は面白い！
講義録, 2013.