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 11 月 06 日

零次元イデアルに関するアルゴリズム

- $k = \bar{k}$ の時，イデアル $I \subseteq k[\mathbf{X}]$ が零次元イデアルであるとは，次のいずれか一つを満たすことであった：
  1. $V(I)$ が有限集合
  2. $k[\mathbf{X}]/I$ が k-ベクトル空間として有限次元
  3. 各 x_i に対し，$\mathrm{LT}(g_i) = x_i^{m_i}$ となるような $m_i \geq 0$ および Gröbner 基底の元 $g_i \in G$ が存在する
- 今回は，この有限次元ベクトル空間の構造に着目したアルゴリズムを紹介する．
  1. $I \cap k[x_i]$ のモニックな生成元の計算アルゴリズム
  2. $\sqrt{I}$ の計算アルゴリズム
  3. $V(I)$ の点の個数の評価（次回）

消去イデアルの生成元 I

- $I \cap k[x_i] = \langle p_i \rangle$ となるような $p_i \in k[x_i]$ を求めたい
- x_i-以外全部消去順序で Gröbner 基底を計算すれば原理的には出来るが，いちいち計算しなおすのはとても非効率的

$\rightsquigarrow$ A の中での $[x_i^j]$ について調べてみよう

$$S := \{\, 1, [x_i], [x_i^2], \ldots \,\}$$

A は有限次元なので，S は k 上一次従属．

- そこで，m_i を $\{\, 1, [x_i], \ldots, [x_i^{m_i}] \,\}$ が一次従属となるような最小のものに取る．

$\rightsquigarrow$ $\sum_{j=0}^{m_i} c_i [x_i]^j = 0$ となるような $c_i \in k$ が取れ，特に m_i の最小性から $c_{m_i} \neq 0$ となる．

- 実は，この $p_i(x_i) = \sum_{j=0}^{m_i} c_j x_i^j \in I$ が $I \cap k[x_i]$ の生成元！

消去イデアルの生成元 II

Exercise 2-2

上の $p_i(x_i)$ が $I \cap k[x_i]$ の生成元となることを示し，それに基づいて零次元イデアルの消去イデアル $I \cap k[x_i]$ のモニックな生成元を求めるアルゴリズムを与えよ．

Proof.

$\langle p_i \rangle \subseteq I \cap k[x_i]$ は明らかなので，$\supseteq$ を示す．$c_{m_i} \neq 0$ より，特に p_i はモニックであるとしてよい．そこで $\langle q \rangle = I \cap k[x_i]$ とする．$p_i \in \langle q \rangle$ より，$p_i(x_i) = r(x_i)q(x_i)$ となるような $r \in k[x_i]$ が存在する．ここで，$\deg q < \deg p_i$ とすると，$q(x) \neq 0$ より $[q(x_i)]$ は $1, [x_i], \ldots, [x_i]^{m_i-1}$ の非自明な線形結合で和がゼロとなるものである．これは m_i の最小性に反するので，$\deg q = \deg p_i$ である．特に $\deg r(x_i) = 0$ であるので，$p_i(x_i)$ と $q(x_i)$ は k の単元倍の差を除いて等しい．よって $I \cap k[x_i] = \langle q \rangle = \langle p_i \rangle$ ∎

よって，生成元を求めるアルゴリズムは次のようになる．

消去イデアルの生成元 III

1. 基底 $B = \{ \mathbf{X}^{\alpha_0}, \ldots, \mathbf{X}^{\alpha_r} \}$ で次のように $[x_i]$ の冪を表す：

$$\begin{aligned}
[x_1]^0 &= a_{00}\mathbf{X}^{\alpha_0} + \cdots + a_{0r}\mathbf{X}^{\alpha_r} \\
[x_1]^1 &= a_{10}\mathbf{X}^{\alpha_0} + \cdots + a_{1r}\mathbf{X}^{\alpha_r} \\
&\vdots \\
[x_i]^r &= a_{r0}\mathbf{X}^{\alpha_0} + \cdots + a_{rr}\mathbf{X}^{\alpha_r}
\end{aligned}$$

2. そこで，掃き出し法を行列

$$\begin{bmatrix} a_{00} & \cdots & a_{0r} \\ \vdots & \ddots & \vdots \\ a_{r0} & \cdots & a_{rr} \end{bmatrix}$$

に適用し，一次従属になる最小の j を求める．

消去イデアルの生成元 IV

3. 次の連立方程式を解けば，$p(x_i) = x_i^j - (c_{j-1}x_i^j + \cdots + c_0)$ が解となる．

$$\begin{bmatrix} a_{j0} \\ \vdots \\ a_{jr} \end{bmatrix} = \begin{bmatrix} a_{00} & \cdots & a_{0j-1} \\ \vdots & \ddots & \vdots \\ a_{r0} & \cdots & a_{rj-1} \end{bmatrix} \begin{bmatrix} c_0 \\ \vdots \\ c_{j-1} \end{bmatrix}$$

⋆ このアルゴリズムは，一々 lex で計算するより遥かに効率がいい！

零次元イデアルの根基 I

- 数値解を求める際に重根が収束を劇的に遅くする.
- 一変数の時は p の代わりに $p_{red} = \frac{p}{\mathrm{GCD}(p,p')}$ を使えばよかった.（p の square-free part と云う）

⋆ $\sqrt{I}$ は p_{red} の一般化になっている！

Exercise 2-3

$p \in k[x], p \neq 0 \Rightarrow \sqrt{\langle p \rangle} = \langle p_{red} \rangle$

零次元イデアルの根基 II

Proof.

p はモニックであるとして一般性を失わない．p を $\bar{k}[x]$ で

$$p(x) = (x-\gamma_0)^{d_0} \cdot \cdots \cdot (x-\gamma_r)^{d_r}$$

と因数分解すれば，$p_{red}(x) = (x-\gamma_0) \cdot \cdots \cdot (x-\gamma_r)$ と表せる．
$f \in \langle p_{red} \rangle$ とすると，ある g があり $f = g(x-\gamma_0) \cdot \cdots \cdot (x-\gamma_r)$ と表せる．$d = \max_j d_j$ と置けば，
$f^d = g^d p(x-\gamma_0)^{d-d_0} \ldots (x-\gamma_r)^{d-d_r}$．ここで $p, f \in k[x]$ より，
$p | f^d$ となることが判る．よって $f \in \sqrt{\langle p \rangle}$．逆は明らか． ∎

- $k[x]$ で根基を計算するには p_{red} を計算すれば良い．
- 一般の多項式環 $k[\mathbf{X}]$ でイデアル I の根基を計算する方法は知られているが難しい．

$\leadsto$ I が零次元イデアルのときは簡単に計算できる！

零次元イデアルの根基 III

Prop. 7

$I \subseteq k[\mathbf{X}]$: 零次元イデアル, $k = \bar{k}$

p_i : $I \cap k[x_i]$ の生成元　$p_{i,red}$: p_iの *square-free part*

$\Rightarrow \sqrt{I} = I + \langle p_{1,red}, \ldots, p_{n,red} \rangle$

証明. $J = I + \langle p_{1,red}, \ldots, p_{n,red} \rangle$ と置く．まず J が根基イデアルであることを示そう．$p_{i,red} = (x_i - a_{i1}) \ldots (x_i - a_{id_i})$ と書こう．すると，$p_{1,red} \in J$ であり，異なる根を持つことから，

$$J = J + \langle p_{1,red} \rangle = \bigcap_j (J + \langle x_1 - a_{1j} \rangle)$$

と書けることがわかる．このことは簡単に示せるので事実として認める．これを繰り返せば，

$$J = J + \langle p_{1,red} \rangle = \bigcap_{j_1,\ldots,j_n} (J + \langle x_1 - a_{1j_1}, \ldots, x_n - a_{nj_n} \rangle)$$

零次元イデアルの根基 IV

を得る．ここで，各 $\langle x_1 - a_{1j_1}, \ldots, x_n - a_{nj_n} \rangle$ は極大イデアルなので，$J + \langle x_i - a_{ij_i} \mid 1 \le i \le n \rangle$ は $k[\mathbf{X}]$ か $\langle x_i - a_{ij_i} \mid 1 \le i \le n \rangle$ のどちらか一方と一致する．よって，J は高々有限個の極大イデアルの共通部分として書ける．極大イデアルは根基イデアルであり，根基イデアルの共通部分は根基イデアルとなるので，J は根基イデアルである．

最後に，$J = \sqrt{I}$ を示す．$I \subseteq J$ は明らか．$p_{i,red}$ は $V(I)$ 上の任意の点で消えるので，$k = \bar{k}$ より零点定理が使えて
$p_{i,red} \in I(V(I)) = \sqrt{I}$ となる．よって $I \subseteq J \subseteq \sqrt{I}$ となり，根基を取れば $J = \sqrt{J} = \sqrt{I}$ となる． ∎

- ⋆ 上の証明では $k = \bar{k}$ を用いたが，例えば入力が全て $\mathbb{Q}[\mathbf{X}]$ ならば演算じたいは $\mathbb{Q}$ の中で出来る．

これまでの例 I

Example.

$I = \langle y^4x + 3x^3 - y^4 - 3x^2, x^2y - 2x^2, 2y^4x - x^3 - 2y^4 + x^2 \rangle$
このとき，$I \cap k[x], I \cap k[y]$ および $\sqrt{I}$ を求めよ．

$k[x,y]/I$ の基底は $B = \{ xy^3, y^3, xy^2, y^2, xy, y, x^2, x, 1 \}$ であることがわかる．これを使って x, y の冪を表現すると，

$$\begin{array}{c} \\ 1 \\ x \\ x^2 \end{array} \begin{array}{c} \begin{array}{cccc} 1 & x & x^2 & x^3 \end{array} \\ \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & 1 & 1 \end{bmatrix} \end{array}$$

$$\begin{array}{c} \\ 1 \\ x \\ x^2 \\ y \\ xy \\ y^2 \\ xy^2 \\ y^3 \end{array} \begin{array}{c} \begin{array}{cccccc} 1 & y & y^2 & y^3 & y^4 & y^5 \end{array} \\ \begin{bmatrix} 1 & & & & & \\ & & & & & \\ & & & & 16 & 32 \\ & 1 & & & & \\ & & & & & \\ & & 1 & & & \\ & & & & & \\ & & & 1 & & \end{bmatrix} \end{array}$$

これまでの例 II

よって $I \cap k[x] = \langle x^3 - x^2 \rangle$，$I \cap k[y] = \langle y^5 - 2y^4 \rangle$．このとき，$p_{1,red} = x^2 - x$，$p_{2,red} = y^2 - 2y$ なので，$\sqrt{I}$ は次のようになる：

$$\sqrt{I} = \left\langle \begin{array}{c} y^4x + 3x^3 - y^4 - 3x^2, x^2y - 2x^2, \\ 2y^4x - x^3 - 2y^4 + x^2, x^2 - x, y^2 - 2y \end{array} \right\rangle$$

Exercise 2-4

$\mathbb{C}[x,y]/I$ および $\mathbb{C}[x,y]/\sqrt{I}$ の次元を較べてみよ．$V(I)$ の異なる点の個数はどうなるか？

$\mathbb{C}[x,y]/I$ の次元は 9 だった．$C[x,y]/\sqrt{I}$ の次元を計算したいので，$\mathbb{C}[x,y]/\sqrt{I}$ の基底を計算すると，$B' = \langle 1, y \rangle$ の二つなので，二次元であることがわかる．ここで $\sqrt{I}$ の Gröbner 基底を計算すると，$G = \{ 2x - y, y^2 - 2y \}$ であるので，これを解けば $V(I) = \{ (0,0), (1,2) \}$ となることが判る．