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 10 月 30 日

2.2 有限次元代数 I

- イデアル $I \subseteq k[\mathbf{X}]$ の Gröbner 基底 G に関する「剰余代数」を調べる．
- Gröbner 基底の基本性質：$f \in k[\mathbf{X}]$ を G で割る：

$$f = h_1 g_1 + \cdots + h_t g_t + \overline{f}^G$$

この時，次の性質が成立：

  - $\overline{f}^G$ は $\mathbf{X}^\alpha \notin \langle \mathrm{LT}(I) \rangle$ なる単項式の線形結合で書ける．
  - $\overline{f}^G$ は f, G に対し（g_i の並び順によらず）一意的に定まり，

$$\overline{f}^G = 0 \Leftrightarrow f \in I$$

$\rightsquigarrow$ $\overline{f}^G = \overline{g}^G \Leftrightarrow f - g \in I$

? f, g の和・積の剰余を $\overline{f}^G, \overline{g}^G$ で表せないか？

2.2 有限次元代数 II

観察

- 剰余の和は再び剰余となる事が基本性質からわかる：

$$\overline{f}^G + \overline{g}^G = \overline{f+g}^G$$

- 剰余の積は再び積になるとは限らない（反例：$I = \langle x^2+3 \rangle$ として $f = x, g = x+2$）．しかし，次は成立：

$$\overline{\overline{f}^G \cdot \overline{g}^G}^G = \overline{f \cdot g}^G$$

$\rightsquigarrow$ G による剰余には，自然に和と積が定まる．

$\star$ この「剰余算術」は剰余環 $k[\mathbf{X}]/I$ と密接に関連している！

2.2 有限次元代数 III

- 剰余環の著しい性質：$[f] = [g] \Leftrightarrow f - g \in I$

$\Rightarrow$ 次のような対応が得られる！

$$\text{剰余} \longleftrightarrow \text{商集合}$$

$$\overline{f}^G \longleftrightarrow [f]$$

$\rightsquigarrow$ $\overline{f}^G$ を $[f] \in k[\mathbf{X}]/I$ の代表元として扱え，更に次のように算術が対応する！

$$\overline{f}^G + \overline{g}^G \longleftrightarrow [f] + [g]$$

$$\overline{\overline{f}^G \cdot \overline{g}^G}^G \longleftrightarrow [f] \cdot [g]$$

2.2 有限次元代数 IV

- ⋆ $k[\mathbf{X}]/I$ の元には加法とスカラー倍（$c \in k$ を $[c]$ だと思って掛ける）があるので，k-ベクトル空間としての構造が入る．
- ⇝ $k[\mathbf{X}]/I$ は k-代数（あるいは k-多元環）になる！
- 以下では $A = k[\mathbf{X}]/I$ と書いて，そのベクトル空間としての性質を調べよう．
- 基本性質：剰余は $\mathbf{X}^\alpha \notin \langle \mathrm{LT}(I) \rangle$ の k-線型結合で書ける．
- 更に，こうした $\mathbf{X}^\alpha$ たちは一次独立！
- ⇝ $\mathbf{X}^\alpha \notin \langle \mathrm{LT}(I) \rangle$ は A の基底となる（基底単項式または標準単項式と呼ぶ）．

基底単項式を用いた演算の例 I

Example.

$G = \{ x^2 + \frac{3}{2}xy + \frac{y^2}{2} - \frac{3}{2}x - \frac{3}{2}y, xy^2 - x, y^3 - y \}$ を考える．G は $x > y$ なる grevlex に関して Gröbner 基底．
すると，$\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(G) \rangle = \langle x^2, xy^2, y^3 \rangle$ となることが判る．
これに属さない単項式は

$$B = \{ 1, x, y, xy, y^2 \}$$

の五つのみで，これが A の基底となることがわかる．

- B を用いて環演算の構造を解明出来ないか？
- 加法：ベクトル空間の加法として，成分毎に足せば OK ！

? 乗法はどうなるか？

- A の乗法は加法について分配する

$\rightsquigarrow$ 自然な方法：基底の乗算表を与えればよい！

基底単項式を用いた演算の例 II

Exercise 2-1

実際に剰余に関する乗算表が次のようになることを確かめよ：

$\cdot$	1	x	y	xy	y^2
1	1	x	y	xy	y^2
x	x	α	xy	β	x
y	y	xy	y^2	x	y
xy	xy	β	x	α	xy
y^2	y^2	x	y	xy	y^2

但し，

$\alpha = -3xy/2 - y^2/2 + 3x/2 + 3y/2, \beta = 3xy/2 + 3y^2/2 - 3x/2 - y/2$

零次元イデアル I

- ⋆ 先程の例は，A が k-ベクトル空間として有限次元だったから上手くいった．

? どんなときに有限次元になるか？

Th. (有限性定理)

$k = \bar{k}, I \subseteq k[\mathbf{X}], V = V(I)$ とし，単項式順序を一つ固定する．この時，次の四条件は同値：

(i) V は有限集合

(ii) 各 $1 \leq i \leq n$ に対し，$x_i^{m_i} \in \langle \mathrm{LT}(I) \rangle$ となる $m_i \geq 0$ がある．

(iii) G を I の *Gröbner* 基底とする．各 $1 \leq i \leq n$ について，$x_i^{m_i} = \mathrm{LM}(g_i)$ となるような $m_i \geq 0, g_i \in G$ が存在する．

(iv) $k[\mathbf{X}]/I$ は k-ベクトル空間として有限次元．

証明の方針；Ideals, Varieties and Algorithms より.

次のような形で示す（代数閉を使うのは $*$ の部分）：

$$
\begin{tikzcd}
\text{(i)} \arrow[rr, Rightarrow, "*"] & & \text{(ii)} \arrow[r, Leftrightarrow] \arrow[dl, Rightarrow] & \text{(iii)} \\
& \text{(iv)} \arrow[ul, Rightarrow] & &
\end{tikzcd}
$$

$\blacksquare$

証明. $\underline{(i) \Rightarrow (ii)}$. $V = \emptyset$ ならば弱零点定理より $1 \in I$ となるので，$m_i = 0$ に取れば良い．そこで $V \neq \emptyset$ とする．以下，i を一

零次元イデアル III

つ固定する．V の点の第 i-座標に現れる相異なる k の元を $a_1, \ldots, a_k$ と置き，一変数多項式 $f(x_i)$ を次で定める：

$$f(x_i) = \prod_{j=1}^{k} (x_i - a_j)$$

すると，構成より $f(x_i)$ は I 上の任意の点で消える．今，$k = \bar{k}$ より零点定理から $I(V(I)) = \sqrt{I}$ であることに気を付ければ，$f \in I(V) = \sqrt{I}$ となる．よってある $m \geq 0$ があって $f^m \in I$ とあるので，f の定義より $x_i^{km} = \mathrm{LT}(f) \in \langle \mathrm{LT}(I) \rangle$ となる．

<u>$(ii) \Leftrightarrow (iii)$</u>．$x_i^{m_i} \in \langle \mathrm{LT}(I) \rangle$ とする．G が Gröbner 基底であることから $x_i^{m_i} \in \langle \mathrm{LT}(G) \rangle$ となり，単項式イデアルの補題より $\mathrm{LT}(g_i) \mid x_i^{m_i}$ となる．これは，g_i の先頭項が x_i の冪であることを意味するので (iii) が成立．逆も同様．

<u>$(ii) \Rightarrow (iv)$</u>．　$x_i^{m_i} \in \langle \mathrm{LT}(I) \rangle$ とすると，$d_i \geq m_i$ ならば $x_1^{d_1} \cdot \cdots \cdot x_n^{d_n}$ となってしまう．今，任意の i に対し $x_i^{m_i} \in \langle \mathrm{LT}(I) \rangle$

零次元イデアル IV

であるので，$x_1^{d_1} \cdot \cdots \cdot x_n^{m_n} \notin \langle \mathrm{LT}(I) \rangle \Rightarrow d_i < m_i$ となる．よって，$\mathbf{X}^{\alpha} \notin \langle \mathrm{LT}(I) \rangle$ となるような $\alpha = (d_1, \ldots, d_n)$ は高々 $m_1 \cdot \cdots \cdot m_n$ 個しかない．これまでの議論から，これらの単項式が A の基底であったので，A は有限次元である．

$\underline{(iv) \Rightarrow (i)}$．$V$ が有限であることを示すには，特に V の点の各成分の取り得る値がそれぞれ有限個しかない事を示せば十分である．そこで，i を一つ固定し，剰余類 $[x_i^j] \in A\,(j = 0, 1, \ldots)$ を考えよう．A が有限次元であることから，$\left\{ [x_i^j] \,\middle|\, j < \omega \right\}$ は k 上一次従属である．よって，ある m と $c_j \in k, (c_0, \ldots, c_m) \neq 0$ があって，

$$\sum_{j=1}^{m} c_j [x_i^j] = \left[\sum_{j=1}^{m} c_j x_i^j \right] = [0]$$

零次元イデアル V

となる．これは $\sum_{j=1}^{m} c_j x_i^j \in I$ を意味し，この多項式は零多項式ではないから，k では根を高々有限個しか持たない．よって $V(I)$ は有限集合となる． $\blacksquare$

Def. (零次元イデアル)

上の定理の条件を満たすようなイデアル $I \subseteq k[\mathbf{X}]$ の事を，零次元イデアルと呼ぶ．

- ⋆ A : 有限次元代数 $\Leftrightarrow$ I : 零次元イデアル
- I が零次元 $\Leftrightarrow$ 各 i について $I \cap k[x_i] \neq 0$
  - $\Rightarrow$ については，x_i が一番後ろにくるような Gröbner 基底について前の定理を適用してやれば，$x_i = \mathrm{LM}(g_i)$ となる $g_i \in G$ が取れ，これが求めるものになる．

零次元イデアル VI

- $(\Leftarrow)$．$I \cap k[x_i] = \langle p \rangle$ とし，$m_i = \deg p$ と置く．すると，どんな単項式順序を選んだとしても，$x_i^{m_i} \in \langle \mathrm{LT}(I) \rangle$ となる．よって，$\mathbf{X}^\alpha \notin \langle \mathrm{LT}(I) \rangle$ となるためには，α は

$$R := \left\{ (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n_{\geq 0} \;\middle|\; \forall i (0 \leq \alpha_i < m_i) \right\}$$

の元でなくてはならない．よって A は有限次元.

$\leadsto$ 零次元イデアルについて，$k[\mathbf{X}]/I$ の基底を求めるアルゴリズムは簡単！

- 上の R の元 $\alpha \in R$ を適当な順番に列挙して，$\overline{\mathbf{X}^\alpha}^G = \mathbf{X}^\alpha$ を満たすものだけを選び出せばよい！

⋆ 来週以降，このベクトル空間としての構造を使って計算を楽する方法を紹介.

1. 零次元イデアルの消去イデアルのモニックな生成元の計算法
2. 零次元イデアルの根基イデアルの計算法
3. 根の個数の評価