代数閉体でない場合の代数的集合について

小野貴寛（岡山大学 自然科学研究科）

若手会の講演では [1] の Exercise となっている，“体 k が代数閉体でないなら, k^n の任意の代数的集合は 1 つの多項式で定義される.”を紹介した. この報告書はそれについてまとめたものである.

1 定義と Kunz の問題

$R = k[x_1, \ldots, x_n]$ を体 k 上 n 変数多項式環, $f \in R$ とする. すると代入写像

$$\begin{array}{ccc} k^n & \longrightarrow & k \\ \cup & & \cup \\ (\alpha_1, \ldots, \alpha_n) & \longmapsto & f(\alpha_1, \ldots, \alpha_n) \end{array} \tag{1.1}$$

を考えることができる. ここで次の記号, 定義を与える.

定義 1.1 (共通零点)**.** $f_1, \ldots, f_r \in R$ に対して

$$\mathrm{Var}(f_1, \ldots, f_r) \stackrel{\mathrm{def}}{=} \{(\alpha_1, \ldots, \alpha_n) \in k^n \mid f_i(\alpha_1, \ldots, \alpha_n) = 0 \text{ for } 1 \leq \forall i \leq r\}.$$

定義 1.2 (代数的集合)**.**

$$k^n \supseteq V \text{ が代数的集合} \stackrel{\mathrm{def}}{\Longleftrightarrow} \exists \mathfrak{a} : R \text{ のイデアル s.t. } \mathrm{V} = \mathrm{Var}(\mathfrak{a}).$$

注意 1.3.

- R は Noether 環なので, 任意の R のイデアルは有限生成である. 代数的集合を与えるイデアル $\mathfrak{a}$ の生成元を $f_1, \ldots, f_m$ とすれば $V = \mathrm{Var}(\mathfrak{a}) = \mathrm{Var}(f_1, \ldots, f_m)$ となる.
- つまり, 任意の代数的集合は有限個の多項式の共通零点.
- 代数的集合は $\mathfrak{a}$ の生成元の取り方によらない.

以上の定義を用いて, Kunz の問題を述べることができる.

定理 1.4 (Kunz の問題)**.** *k が代数閉体でないなら, k^n の任意の代数的集合はただ 1 つの多項式で定義される.*

2 具体例・証明

この章では代数閉体でない体として, 実数体, 有限体の場合で定理 1.4 の様子を見る. $n = 1$ の場合, $k[x]$ は PID であるから定理 1.4 は成り立つ.

例 2.1 (実数体の場合)**.** ここでは 2 変数として, $\mathbb{R}[x, y]$ で考える. 代数的集合を与えるイデアルの生成元が $f_1 = xy - 1, f_2 = x - y \in \mathbb{R}[x, y]$ であるとすると, 代数的集合の定義から, $\mathrm{Var}(f_1, f_2) = \{(-1, -1), (1, 1)\}$

である．このとき, $g=(xy-1)^2+(x-y)^2\in\mathbb{R}[x,y]$ とすれば, $\mathrm{Var}(f_1,f_2)=\mathrm{Var}(g)$ であることが確認できる．

例 **2.2** (有限体の場合)**.** 2 変数, $k=\mathbb{F}_2$ で考える．代数的集合を与えるイデアルが $f_1=x-1, f_2=y-1\in\mathbb{F}_2[x,y]$ で生成されているとする．すると $\mathrm{Var}(f_1,f_2)=\{(1,1)\}$ であり, $g=xy+1$ とおけば $\mathrm{Var}(g)=\{(1,1)\}$ が確かめられるので, $\mathrm{Var}(f_1,f_2)=\mathrm{Var}(g)$ となり 1 つにすることができる．

以上のことから次のことが観察される．

観察 2.3.

1. 原点のみに解を持つ $\phi\in k[X,Y]$ が存在して, $g=\phi(f_1,f_2)$ とすれば良いのではないか．実数体の例では $\phi=X^2+Y^2$.
2. $\mathbb{F}_2[X,Y]$ の場合, 原点のみに解をもつ多項式として, X^2-XY-Y^2 がある．
3. X^2-XY-Y^2 は X^2-X-1 を Y で斉次化すると得られる．
4. $X^2-X-1=0$ は $\mathbb{F}_2$ に解を持たない．

例 **2.4** (生成元が 3 つ以上の場合)**.** これまでの例では代数的集合を与えるイデアルの生成元の個数は 2 つの場合のみであったが, ここでは 3 つ以上の場合を有限体 $\mathbb{F}_q$ $(q=p^n, p:\text{素数}, n\in\mathbb{N})$ で考える．この状況では次の事が成り立つ．

1. $\forall\alpha\in\mathbb{F}_q$ に対して $\alpha^q=\alpha$.
2. $X^q-X-1=0$ は $\mathbb{F}_q$ に解を持たない．

新たな変数 Y で 2 の左辺を斉次化し $=0$ とした $X^q-XY^{q-1}-Y^q=0$ を考える．

$$\begin{cases} Y=Y^q\neq 0\Rightarrow \left(\frac{X}{Y}\right)^q-\left(\frac{X}{Y}\right)-1=0 \text{ は } \mathbb{F}_q\text{に解を持たない.} \\ Y=0\Rightarrow X=X^q=0.\ \therefore (X,Y)=(0,0). \end{cases}$$

2 の X に $X^q-XY^{q-1}-Y^q$ を代入にし $=0$ とした,

$$\left(X^q-XY^{q-1}-Y^q\right)^q-\left(X^q-XY^{q-1}-Y^q\right)-1=0$$

は 1 変数の場合と同様に $\mathbb{F}_q$ に解を持たない．これを Z で斉次化した

$$\left(X^q-XY^{q-1}-Y^q\right)^q-\left(X^q-XY^{q-1}-Y^q\right)Z^{q-1}-Z^q=0$$

の解は $(X,Y,Z)=(0,0,0)$ である．こうして原点のみに解を持つ多項式を帰納的に作ることができる．

観察 2.3, 例 2.4 をまとめることで, 定理 1.4 の証明方針を得る．

証明.

1. 生成元が 2 つの場合を示せば十分である．$\mathfrak{a}=(f_1,f_2), f_i\in R$ とする．
2. k が代数閉体でないことより, k に解を持たないような多項式

$$F(X)=a_0X^n+a_1X^{n-1}+\cdots+a_{n-1}X+a_n\in k[X],\ (a_i\in k, a_0,a_n\neq 0)$$

が存在する．

3. Y で斉次化した $\phi(X,Y)$ を考える.

$$\phi(X,Y) = a_0X^n + a_1X^{n-1}Y + \cdots + a_{n-1}XY^{n-1} + a_nY^n.$$

4. $\phi(X,Y) = 0$ は,

$$\begin{cases} Y \neq 0 \Rightarrow a_0\left(\frac{X}{Y}\right)^n + a_1\left(\frac{X}{Y}\right)^{n-1} + \cdots + a_n = 0 \text{ は仮定より } k \text{ に解を持たない.} \\ Y = 0 \Rightarrow X^n = 0 \therefore (X,Y) = (0,0) \text{ のみ解である.} \end{cases}$$

5.

$$g(x_1,\ldots,x_n) := \phi\left(f_1\left(x_1,\ldots,x_n\right), f_2\left(x_1,\ldots,x_n\right)\right).$$

とすると, ϕ の作り方と代数的集合の定義から $\mathrm{Var}(f_1,f_2) = \mathrm{Var}(g)$ となる.

□

注意 2.5. 証明方針や実数体の場合の例から分かるように, 1 つにする多項式は一意的でない. しかし, 次の章で述べるように特殊な状況を考えることで一意に定まる場合もある.

3 多項式と多項式関数

ここでは多項式とそれを (1.1) のように多項式関数とみた場合の両者の違いについて考察する. 多項式 $f \in R$ から得られる多項式関数を $F_f : k^n \to k\left((\alpha_1\ldots,\alpha_n) \mapsto f\left(\alpha_1\ldots,\alpha_n\right)\right)$ と書くことにする. 多項式関数の集合は演算を $F_f + F_g \overset{\text{def}}{=} F_{f+g}$, $F_f \cdot F_g \overset{\text{def}}{=} F_{f\cdot g}$ とすることで可換環になる. これをここでは $PF_n(k)$ と書くことにする. すると, 次の全射環準同型写像を考えられる.

$$\begin{array}{ccc} k[x_1,\ldots,x_n] & \twoheadrightarrow & PF_n(k) \\ \cup & & \cup \\ f & \longmapsto & F_f \end{array}$$

この Kernel を I とすると, まとめて以下のように短完全列で書ける.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & I & \longrightarrow & R & \longrightarrow & R/I & \longrightarrow & 0 \quad \text{(exact)} \\ & & & & \cup & & \cup & & \\ & & & & f & \longmapsto & \overline{f} & & \end{array} \tag{3.1}$$

命題 3.1. k が無限体ならば $I = 0$ である. つまり, 多項式と多項式関数に違いは無い.

命題 3.2. k が有限体 $\mathbb{F}_q$ の場合, $I = (x_1^q - x_1, \ldots, x_n^q - x_n)$ である.

例 3.3. $\mathbb{F}_2[x,y]$ において, 多項式 $x^2 + x$ から得られる多項式関数 $F_{x^2+x} : \mathbb{F}_2^2 \to \mathbb{F}_2$ は

$$\begin{array}{ccc} (0,0) & \longmapsto & 0 \\ (0,1) & \longmapsto & 0 \\ (1,0) & \longmapsto & 0 \\ (1,1) & \longmapsto & 0 \end{array}$$

なので多項式 0 から得られる F_0 と同じである. このように多項式としては異なっていても関数としては同じという場合がある.

以上のことから有限体において例 3.3 のようなことを除いた

$$\mathbb{F}_q[x_1,\ldots,x_n]/\left(x_1^q-x_1,\ldots,x_n^q-x_n\right) \tag{3.2}$$

を考えることにする. (3.2) は

$$\underbrace{\underbrace{\mathbb{F}_q[x_1]/(x_1^q-x_1)}_{q\text{次元}\,\mathbb{F}_q\text{ベクトル空間}}\otimes_{\mathbb{F}_q}\cdots\otimes_{\mathbb{F}_q}\underbrace{\mathbb{F}_q[x_n]/(x_n^q-x_n)}_{q\text{次元}\,\mathbb{F}_q\text{ベクトル空間}}}_{n\text{個}}$$

と書けるから多項式関数の個数は q^{q^n} 個である. 一方, $\mathbb{F}_q^n$ の巾集合の個数は

$$\#\left(\mathcal{P}\left(\mathbb{F}_q^n\right)\right)=2^{q^n}$$

なので $q=2$ の場合のみ両者の個数が等しいことが分かる.

定理 3.4. 次の写像は全単射. ((3.1) より well-defined.)

$$\begin{array}{ccc}\mathbb{F}_2[x_1,\ldots,x_n]/\left(x_1^2-x_1,\ldots,x_n^2-x_n\right) & \longrightarrow & \mathcal{P}(\mathbb{F}_2^n)\\ \cup & & \cup\\ f & \longmapsto & \mathrm{Var}(f)\end{array}$$

証明.

- これまでの議論より $q=2$ の場合は両者の個数は等しい. 全射であることを示す.
- $\mathcal{P}(\mathbb{F}_2^n)$ で 1 点のみの集合が全射であることを示せば十分である.
- それは定理 1.4 と 1 変数の場合の対応から作ることができる.

$$\begin{array}{ccc}k[x] & \longrightarrow & \mathcal{P}(\mathbb{F}_2)\\ \cup & & \cup\\ f & \longmapsto & \mathrm{Var}\left(f\right)\end{array}$$

$$\begin{array}{ccc}0 & \longmapsto & \{0,1\}\\ 1 & \longmapsto & \emptyset\\ x & \longmapsto & \{0\}\\ x+1 & \longmapsto & \{1\}\end{array}$$

□

系 3.5. $\mathbb{F}_2[x_1,\ldots,x_n]/(x_1^2-x_1,\ldots,x_n^2-x_n)$ の場合, 定理 1.4 により 1 つにする多項式は一意的に定まる. ($n=2$ の場合は表 1 のようになる.)

$\mathbb{F}_q[x_1,\ldots,x_n]$, $\mathbb{F}_q[x_1,\ldots,x_n]/\left(x_1^q-x_1,\ldots,x_n^q-x_n\right)$ での性質についてはこのこと以外にも多くのことが知られているようである. 例えば [6] や, その参考文献としてある [7] などがある.

定理 1.4 は次のように述べることもできる.

系 3.6. A を整域, その商体 $Q(A)$ が代数閉体でないとする. このとき, $f\in A[x_1,\ldots,x_n]$ に対して k の場合と同様に $F_f:A^n\to A\left((\alpha_1,\ldots,\alpha_n)\mapsto f\left(\alpha_1,\ldots,\alpha_n\right)\right)$ を考える. このとき, 任意の代数的集合はただ 1 つの多項式で定義される.

表 1　$\mathbb{F}_2[x,y]/\left(x^2-x, y^2-y\right)$ の場合

$PF_2(\mathbb{F}_2)$	$\mathrm{Var}(-)$	図	$PF_2(\mathbb{F}_2)$	$\mathrm{Var}(-)$	図
0	$\{(0,0),(1,0),(0,1),(1,1)\}$		x	$\{(0,0),(0,1)\}$	
1	$\emptyset$		$x+1$	$\{(1,0),(1,1)\}$	
xy	$\{(0,0),(1,0),(0,1)\}$		$x+xy$	$\{(0,0),(0,1),(1,1)\}$	
$xy+1$	$\{(1,1)\}$		$x+xy+1$	$\{(1,0)\}$	
y	$\{(0,0),(1,0)\}$		$x+y$	$\{(0,0),(1,1)\}$	
$y+1$	$\{(0,1),(1,1)\}$		$x+y+1$	$\{(1,0),(0,1)\}$	
$y+xy$	$\{(0,0),(1,0),(1,1)\}$		$x+y+xy$	$\{(0,0)\}$	
$y+xy+1$	$\{(0,1)\}$		$x+y+xy+1$	$\{(1,0),(0,1),(1,1)\}$	

4 最後に

この報告書では代数閉体でないとき, 任意の代数的集合は 1 つの多項式で定義されることを示してきた. 一般に代数的集合（つまり有限個の多項式で与えられた連立方程式の解集合）を求める際には Gröbner 基底の理論が使われる. それは生成元を減らすというよりもむしろ増やすことでイデアル全体として良い性質を得ようとするものである. これについては第 14 回代数学若手研究会において飯間 圭一郎 先生により『連立方程式の解法とグレブナー基底』と題して発表されており, その報告書が公開されている [8].

参考文献

[1] Ernst Kunz, Introduction to Commutative Algebra and Algebraic Geometry, Birkhäuser 1985.

[2] D. Cox, J. Little and D. O'Shea, Ideals, Varieties, and Algorithms, 2nd edition, Springer-Verlag, New York, 1997.

[3] David Eisenbud, Commutative Algebra with a View Toward Algebraic Geometry, Springer, 1999.

[4] Martin Kreuzer and Lorenzo Robbiano, Computational commutative algebra 2, Springer-Verlag, Berlin, 2005.

[5] Srikanth B. Iyengar, Graham J. Leuschke, Anton Leykin, Claudia Miller, Ezra Miller, Anurag K. Singh, and Uli Walther, Twenty-four hours of local cohomology, Graduate Studies in Mathematics, 87, American Mathematical Society, 2007.

[6] Sicun Gao, Counting Zeros over Finite Fields Using Gröbner Bases, MS Thesis in Logic and Computation, 2009.

[7] R. Germundsson, Basic Results on Ideals and Varieties in Finite Fields, Technical Report LiTH-ISY-I-1259, Linköping University, S-581 83, 1991.

[8] 飯間 圭一郎, 『連立方程式の解法とグレブナー基底』, 第 14 回代数学若手研究会報告集, http://kissme.shinshu-u.ac.jp/wakate/2009/iima.pdf

[9] JST CREST 日比チーム編, 『グレブナー道場』, 共立出版, 2011.

[10] M. F. Atiyah and I. G. MacDonald, 新妻弘（訳）『可換代数入門』, 共立出版, 2006.

[11] 松村英之, 『復刊 可換環論』, 共立出版, 2000.

[12] 桂利行, 『代数学 III 体とガロア理論』, 東京大学出版会, 2005.

[13] 桂利行, 『代数幾何入門, 共立講座 21 世紀の数学 (17) 』, 共立出版, 1998.

[14] 広中平祐（講義）, 森重文（記録）, 丸山正樹, 森脇淳, 川口周（編）, 『代数幾何学』, 京都大学学術出版会, 2004.