Weak Nullstellensatz の証明

大塚美紀生

k を代数的閉体[注1]とし，多項式環 $k[x_1, x_2, \cdots, x_n]$ のイデアル[注2]を I とするとき，n 次元空間 k^n における Affine variety $V(I)$ は

$$V(I) = \left\{(a_1, a_2, \cdots, a_n) \,\middle|\, f(a_1, a_2, \cdots, a_n) = 0 \text{ for all } f \in I\right\}$$

により定められる。[注3]

Weak Nullstellensatz

$V(I) = \varnothing$ ならば $I = k[x_1, x_2, \cdots, x_n]$ である。

この定理は，理念としてはこうあるべきと理解できるが，直観的に明らかではない。何通りかの証明が知られているが，どれも意外と難しい。その中の一つに Elimination Theorem[注4]を(十分条件として)用いる証明があるが，Elimination Theorem 自体大定理であり，Weak Nullstellensatz だけ示すには大掛かりすぎる印象が否めない。2007 年，P. Schauenburg は Elimination Theorem に新しくシンプルな証明を与えた。それは，Elimination(変数の消去)の構造を(残った変数に)点の座標を代入して得られるイデアルで論じることと Gröbner Basis[注5]の性質を用いることによるものである。

本稿は，P. Schauenburg のアイデアを参考にして，Weak Nullstellensatz を易しく証明しようという試みである。Elimination Theorem を通さないで直接証明することにより，結果的には Gröbner Basis を使わないで済むことになった。

多変数表示を見やすくするために，本稿では

$$\boldsymbol{x} = (x_2, \cdots, x_n) \in k^{n-1},$$
$$(x_1, \boldsymbol{x}) = (x_1, x_2, \cdots, x_n) \in k^n$$

と表すことにする。

I を $k[x_1, x_2, \cdots, x_n]$ のイデアル[注2]とする。Hilbert Basis Theorem[注6]により，I は有限生成である。I の生成元を $f_1(x_1, \boldsymbol{x}),\ f_2(x_1, \boldsymbol{x}),\ \cdots,\ f_t(x_1, \boldsymbol{x})$ とするとき，

$$I = \langle f_1,\ f_2,\ \cdots,\ f_t \rangle$$

と表示し，$\boldsymbol{a} \in k^{n-1}$ に対して

$$I(\boldsymbol{a}) = \langle f_1(x_1, \boldsymbol{a}),\ f_2(x_1, \boldsymbol{a}),\ \cdots,\ f_t(x_1, \boldsymbol{a}) \rangle$$

と定める。

補題１　　$I(\boldsymbol{a}) = \left\{f(x_1, \boldsymbol{a}) \,\middle|\, f \in I\right\}$

(証明)　$f_i(x_1, \boldsymbol{x}) \in I\ (1 \leqq i \leqq t)$ より

$$f_i(x_1, \boldsymbol{a}) \in \left\{f(x_1, \boldsymbol{a}) \,\middle|\, f \in I\right\}$$

であるから，生成イデアルの最小性より

$$I(\boldsymbol{a}) \subset \left\{ f(x_1, \boldsymbol{a}) \,\middle|\, f \in I \right\}$$

$I = \langle f_1,\ f_2,\ \cdots,\ f_t \rangle$より，任意の $f \in I$ に対して

$$f(x_1, \boldsymbol{x}) = c_1 f_1(x_1, \boldsymbol{x}) + c_2 f_2(x_1, \boldsymbol{x}) + \cdots + c_t f_t(x_1, \boldsymbol{x}) \quad (c_i \in k)$$

と表される。$\boldsymbol{x} = \boldsymbol{a}$を代入すると

$$f(x_1, \boldsymbol{a}) = c_1 f_1(x_1, \boldsymbol{a}) + c_2 f_2(x_1, \boldsymbol{a}) + \cdots + c_t f_t(x_1, \boldsymbol{a}) \in I(\boldsymbol{a})$$

であるから，

$$\left\{ f(x_1, \boldsymbol{a}) \,\middle|\, f \in I \right\} \subset I(\boldsymbol{a})$$

■

補題２ $\left\{ f(x_1, \boldsymbol{a}) \,\middle|\, f \in I \right\} \neq \langle 0 \rangle$とする。$f_i(x_1, \boldsymbol{a})\ (1 \leqq i \leqq t)$ の中で(x_1 の)次数が最小のものを $f_0(x_1, \boldsymbol{a})$ とするとき，

$$\left\{ f(x_1, \boldsymbol{a}) \,\middle|\, f \in I \right\} = \langle f_0(x_1, \boldsymbol{a}) \rangle$$

(証明) f_0 は $f_1,\ f_2,\ \cdots,\ f_t$ の 1 つであるから，

$$\langle f_0(x_1, \boldsymbol{a}) \rangle \subset \langle f_1(x_1, \boldsymbol{a}),\ f_2(x_1, \boldsymbol{a}),\ \cdots,\ f_t(x_1, \boldsymbol{a}) \rangle$$

一方，任意の $i\ (1 \leqq i \leqq t)$ に対して，

$$f_i(x_1, \boldsymbol{a}) = f_0(x_1, \boldsymbol{a}) q_i(x_1) + r_i(x_1),\ \ \deg r_i(x_1) < \deg f_0(x_1, \boldsymbol{a})$$

を満たす多項式 $q_i(x_1),\ r_i(x_1)$ が存在する。

$f_i(x_1, \boldsymbol{a})$ も $f_0(x_1, \boldsymbol{a})$ も $\left\{ f(x_1, \boldsymbol{a}) \,\middle|\, f \in I \right\}$ に属するから，イデアルの性質より

$$r_i(x_1) \in \left\{ f(x_1, \boldsymbol{a}) \,\middle|\, f \in I \right\}$$

$f_0(x_1, \boldsymbol{a})$ の次数の最小性より

$$r_i(x_1) = 0$$

したがって，

$$\begin{aligned} &\langle f_1(x_1, \boldsymbol{a}),\ f_2(x_1, \boldsymbol{a}),\ \cdots,\ f_t(x_1, \boldsymbol{a}) \rangle \\ &= \langle f_0(x_1, \boldsymbol{a}) r_1(x_1),\ f_0(x_1, \boldsymbol{a}) r_2(x_1),\ \cdots,\ f_0(x_1, \boldsymbol{a}) r_t(x_1) \rangle \\ &\subset \langle f_0(x_1, \boldsymbol{a}) \rangle \end{aligned}$$

が成り立つから，

$$\langle f_1(x_1, \boldsymbol{a}),\ f_2(x_1, \boldsymbol{a}),\ \cdots,\ f_t(x_1, \boldsymbol{a}) \rangle = \langle f_0(x_1, \boldsymbol{a}) \rangle$$

補題１より

$$\left\{ f(x_1, \boldsymbol{a}) \,\middle|\, f \in I \right\} = \langle f_1(x_1, \boldsymbol{a}),\ f_2(x_1, \boldsymbol{a}),\ \cdots,\ f_t(x_1, \boldsymbol{a}) \rangle$$

であるから，

$$\left\{ f(x_1, \boldsymbol{a}) \,\middle|\, f \in I \right\} = \langle f_0(x_1, \boldsymbol{a}) \rangle$$

■

補題３ kを無限体[注1]，$f(x_1, x_2, \cdots, x_n) \in k[x_1, x_2, \cdots, x_n]$ とする。任意の $a_1, a_2, \cdots, a_n \in k$ に対して $f(a_1, a_2, \cdots, a_n) = 0$ となるのは，$f(x_1, x_2, \cdots, x_n) = 0$ の場合に限られる。

(証明) n についての数学的帰納法で示す。

$n = 1$ のとき，$f(a) = 0$ となる $a \in k$ の個数は $f(x)$ の次数以下しかないから，無限個の a に対して $f(a) = 0$ が成り立つなら $f(x)$ は零多項式である。

$n-1$ のとき正しいとして，$f \in k[x_1, x_2, \cdots, x_n]$ が任意の $a_1, a_2, \cdots, a_n \in k$ に対して $f(a_1, a_2, \cdots, a_n) = 0$ を満たすとする。

$$f = \sum_{i=0}^{d} g_i(x_1, \cdots, x_{n-1}) {x_n}^i, \quad g_i \in k[x_1, \cdots, x_{n-1}]$$

と表すことにし，$(a_1, \cdots, a_{n-1}) \in k^{n-1}$ を任意に選んで固定する。
任意の $x_n \in k$ に対して

$$f(a_1, \cdots, a_{n-1}, x_n) = \sum_{i=0}^{d} g_i(a_1, \cdots, a_{n-1}) {x_n}^i = 0$$

が成り立つから，

任意の i に対して $g_i(a_1, \cdots, a_{n-1}) = 0$

である。任意の $a_1, \cdots, a_{n-1}$ に対して成り立つから，帰納法の仮定より

すべての i に対して $g_i(x_1, \cdots, x_{n-1}) = 0$

であり，

$$f(x_1, \cdots, x_{n-1}, x_n) = \sum_{i=0}^{d} g_i(x_1, \cdots, x_{n-1}) {x_n}^i = 0$$

は零多項式となる。 ■

Weak Nullstellensatz の証明

$$I \subsetneqq k[x_1, x_2, \cdots, x_n] \implies V(I) \neq \varnothing$$

であることを，次元 n についての数学的帰納法で証明する。
$n = 1$ のとき，$I \neq k[x]$ とすると，補題 2 と同様の議論により

$$I = \langle g(x) \rangle \text{ for some } g(x) \in k[x]$$

と表されて，

$$g(x) = 0 \text{ または } \deg g(x) \geqq 1$$ [注7]

$g(x) = 0$ のときは，$V(I) = k$ である。
$\deg g(x) \geqq 1$ のときは，k が代数的閉体であることより

$$g(a) = 0$$

を満たす $a \in k$ が存在する[注8]から，

$$a \in V(I)$$

であり，いずれの場合も $V(I) \neq \varnothing$ である。
$n-1$ 次以下では定理が成り立つものとする。$k[x_1, x_2, \cdots, x_n]$ のイデアル I が

$$I = \langle f_1, f_2, \cdots, f_t \rangle \subsetneqq k[x_1, x_2, \cdots, x_n]$$

であるとすれば，

$$I_1 = I \cap k[x_2, \cdots, x_n] \subsetneqq k[x_2, \cdots, x_n]$$ [注9]

帰納法の仮定より $V(I_1) \neq \varnothing$ であるから，

$$\boldsymbol{a} = (a_2, \cdots, a_n) \in V(I_1)$$

が存在する。
すべての i に対して $f_i(x_1, \boldsymbol{x}) \in k[x_2, \cdots, x_n]$ であるとすれば，任意の $a_1 \in k$,

$f \in I$ に対して $f(a_1, \boldsymbol{a}) = 0,\ (a_1, \boldsymbol{a}) \in V(I)$ となるから，

$f_1(x_1, \boldsymbol{x})$ の x_1 についての次数は 1 以上

であるとしてよい。その次数を d として，

$$f_1(x_1, \boldsymbol{x}) = c(\boldsymbol{x}){x_1}^d + (x_1 \text{について } d-1 \text{次以下}) \qquad \big(c(\boldsymbol{x}) \in k[x_2, \cdots, x_n]\big)$$

と表すとき，

$$c(\boldsymbol{a}) \neq 0$$

としてよい。$f_1(x_1, \boldsymbol{x})$ の total degree を N として

$$\begin{aligned} x_1 &= \tilde{x}_1 \\ x_2 &= \tilde{x}_2 + b_2\tilde{x}_1 \quad (b_2 \in k) \\ &\vdots \\ x_n &= \tilde{x}_n + b_n\tilde{x}_1 \quad (b_n \in k) \end{aligned}$$

により変数変換すると，

$$\begin{aligned} f_1(x_1, \boldsymbol{x}) &= f_1(\tilde{x}_1, \tilde{x}_2 + b_2\tilde{x}_1, \cdots, \tilde{x}_n + b_n\tilde{x}_1) \\ &= p(b_2, \cdots, b_n){\tilde{x}_1}^N + (x_1 \text{について } N-1 \text{次以下}) \\ &\qquad \big(p(\boldsymbol{x}) \in k[x_2, \cdots, x_n]\big) \end{aligned}$$

ここで，$p(\boldsymbol{x})$ は零多項式ではないから，補題 3 より

$p(b_2, \cdots, b_n) \neq 0$ となる $\boldsymbol{b} = (b_2, \cdots, b_n) \in k^{n-1}$ が存在

する。このとき，

$$f(x_1, x_2, \cdots, x_n) = \tilde{f}(\tilde{x}_1, \tilde{x}_2, \cdots, \tilde{x}_n)$$

として

$$\tilde{I} = \{\tilde{f} : f \in I\}$$

を $k[\tilde{x}_1, \tilde{x}_2, \cdots, \tilde{x}_n]$ において考えると，

$$I \subsetneqq k[x_1, x_2, \cdots, x_n] \iff \tilde{I} \subsetneqq k[\tilde{x}_1, \tilde{x}_2, \cdots, \tilde{x}_n]^{\text{注9}}$$

であり，

$$\tilde{f}_1(\tilde{x}_1, \tilde{x}_2, \cdots, \tilde{x}_n) = p(\boldsymbol{b}){\tilde{x}_1}^N + (x_1 \text{について } N-1 \text{次以下})$$

について論じることになるから，はじめから

$$c(\boldsymbol{a}) \neq 0$$

としてよいことになる。

特に，$f_i(x_1, \boldsymbol{a})\ (1 \leqq i \leqq t)$ の中で（x_1 の）次数が最小である $f_0(x_1, \boldsymbol{a})$ について，

$$\deg f_0(x_1, \boldsymbol{a}) \geqq 1$$

である。k は代数的閉体であるから，

$f_0(a_1, \boldsymbol{a}) = 0$ を満たす $a_1 \in k$ が存在

する。補題 2 より

$$\big\{f(x_1, \boldsymbol{a}) \,\big|\, f \in I\big\} = \langle f_0(x_1, \boldsymbol{a})\rangle$$

であるから，

$$(a_1, \boldsymbol{a}) \in V(I)$$

であり，n のときも定理が成り立つ。 ■

注1　**体**(たい)とは，有理数の集合 $\boldsymbol{Q}$ や実数の集合 $\boldsymbol{R}$ のように，和と積が定義され，その2つの演算には整合性があり，0以外は逆数をもつような集合のことである。**代数的閉体**とは，その体を係数とする多項式の方程式の解がすべてその体に属するような体のことである。高校生以下の読者であれば，$k = \boldsymbol{C}$(複素数の集合)と思って本稿を読むとイメージしやすいだろう。

注2　整数の集合 $\boldsymbol{Z}$ のように，和と積が定義され，2つの演算に整合性があるような集合を**環**といい，環の部分集合で倍数の概念を一般化した集合を**イデアル**という。初歩から学ぶのであれば，文献[5]などを参照するとよいだろう。

注3　affine variety (アファイン代数多様体)が図形であるという立場では，いくつかの多項式 $f_1,\ f_2,\ \cdots,\ f_r$ の零点集合として

$$V(f_1, \cdots, f_r) = \left\{(a_1, \cdots a_n) \,\middle|\, f_i(a_1, \cdots, a_n) = 0\,,\ 1 \leqq i \leqq r\right\}$$

と定める方が自然であるが，Hilbert Basis Theorem (注6) により $k[x_1, x_2, \cdots, x_n]$ の任意のイデアルは有限生成であるから，初めから affine variety がイデアルで定義されていると考えてよい。

注4　Elimination Theorem 自体は本稿では用いないので，触れないことにする。関心を持たれた方は，文献[1]で学ばれるとよいだろう。

注5　Gröbner Basis 自体は本稿では用いないので，触れないことにする。関心を持たれた方は，文献[1]で学ばれるとよいだろう。

注6　Hilbert Basis Theorem については，文献[1]の Chapter 2 または文献[5]の Chapter 13 などを参照していただきたい。[1]の証明は Gröbner Basis を用いることで n 変数のまま簡潔に説明する手法であり，[5]の証明は，直接には R が有限生成ならば $R[x]$ も有限生成であることを示すことで，数学的帰納法により完結する。

注7　ここでは $\langle g(x)\rangle \neq k[x]$ が前提である。$g(x)$ が0でない定数であるとすれば，$\langle g(x)\rangle = k[x]$ となってしまう。

注8　代数的閉体である仮定から明らかであるが，k を複素数体 $\boldsymbol{C}$ のつもりで読んでいる人には，複素数体が代数的閉体であることを知っておく必要がある。複素数体が代数的閉体であるという定理を**代数学の基本定理**という。文献[4]にある証明は，高校数学の知識だけで理解することができる。

注9　環 R のイデアル I について，

$$I = R \iff 1 \in I$$

と言い換えれば，容易に示せるであろう。

参考文献

［1］ D.Cox and J.Little and D.O'Shea,
Ideals, Varieties, and Algorithms, Fourth Edition, Springer-Verlag (2015)

［2］ 前原潤，直観トポロジー，共立出版 (1993)

［3］ 大塚美紀生，整数係数多項式環$\boldsymbol{Z}[x_1, \cdots, x_n]$のイデアルについて，
早稲田数学フォーラム (2015),
http://wasmath.la.coocan.jp/hilbert-basis-theorem.pdf

［4］ 高木貞治，代数学講義(改訂新版)，共立出版 (1989)

［5］ J.J.Watkins, *Topics in commutative ring theory*,
Princeton University Press (2007)

2018.8.20