

2009 年度卒業論文

無限体上における Nullstellensatz について

早稲田大学理工学部数理科学科

1G06L048-5

手島 悠人

指導教員名 楫 元

概要

Nullstellensatz (強形の零点定理) は、代数閉体上の多項式環の根基イデアルとその零点集合により定義されるイデアルが等しい事を主張している。これは、アフィン多様体と根基イデアルの間に 1 対 1 の対応がある事を示しており、代数と幾何をつなぐ重要な定理である。その定理は代数閉体上におけるもので、例えば有理数体等の代数閉体でない体上では一般には成り立たない。では無限体上の多項式環において、代数閉体の場合と比べどのような差異が生じているのだろうか。無限体上の 2 変数以下の多項式環の単項イデアルについて、その零点集合により定義されるイデアルが等しくなるような条件を調べた。結果、イデアルを生成する多項式を分解したときの、それらの零点の個数が重要な役割を果たしている事が分かった。

1 序文

Nullstellensatz は、代数閉体 k 上の多項式環 $k[x_1, \dots, x_n]$ において、 I をそのイデアルとすると、

$$\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$$

が成り立つ事を主張している。つまり、Nullstellensatz によりアフィン多様体と根基イデアルに 1 対 1 の対応がある事が分かる。これは代数と幾何の対応を与える大変重要な定理である。この Nullstellensatz により、 k を代数閉体とし、その多項式環のイデアル I を根基イデアルと仮定すると

$$\mathbf{I}(\mathbf{V}(I)) = I \tag{1}$$

が成り立つ事が分かる。ただし、

$$\mathbf{V}(I) = \{(a_1, \dots, a_n) \in k^n \mid \forall f \in I \text{ に対して } f(a_1, \dots, a_n) = 0\}$$

$$\mathbf{I}(S) = \{f \in k[x_1, \dots, x_n] \mid \forall (a_1, \dots, a_n) \in S \subset k^n \text{ に対し } f(a_1, \dots, a_n) = 0\}$$

とする。

では、基礎体が代数閉体でない場合 (1) 式は成り立つのであろうか。代数閉体でなく、例えば実数体上で調べてみると、(1) 式は一般には成り立たない事がすぐに分かる (2, 3 章の例を参照)。では無限体上の多項式環で I が何か適当な条件を満たせば成立するのであろうか。いくつかの例を調べ、 I を生成する多項式が関係しているのではないかと考察した。このような動機から始まり、次の問題を考える事にした。

■問題提起 無限体上で $\mathbf{I}(\mathbf{V}(I)) = I$ が成り立つ必要十分条件はどのようなものであるか。

この“無限体上での Nullstellensatz”のような問題を軸に $\mathbf{I}(\mathbf{V}(I))$ が成り立つ I の条件を調べたところ、2 変数以下の多項式環の単項イデアルについて、いくつかの結果を得る事ができた。そして、 f を既約多項式の積に分解したときの分解とそれらの既約多項式の零点の個数が代数閉体のときと同様な状況のときに (1) 式が成り立つことがわかった。その意味は、それぞれのセクションで詳しく述べる事にしよう。

2 1 変数多項式環において

以下では特に断らない場合, k を無限体とする.

まず実数体上の多項式環上でいくつかの例を調べてみた.

例 1

$I = \langle x^2 + 1 \rangle \subset \mathbf{R}[x]$ のとき, $V(I) = \emptyset$ となり, $I(V(I)) = \mathbf{R}[x] \neq I$ である.

例 2

$I = \langle x^2 - 1 \rangle \subset \mathbf{R}[x]$ のとき, $I(V(I)) = I$ である. (参考文献 [1]4, 2, prop9, def10 参照)

I が根基イデアルであっても, 一般に (1) 式が成り立つとは限らない事が分かった. 一変数多項式環 $k[x]$ で先ほどの問題提起を調べたところ, その解答を得る事ができた. 主定理の紹介の前に, その証明の準備として命題を 2 つ用意する.

命題 2.1 $k[x]$ は単項イデアル整域である.

証明 参考文献 [1]1.5.cor5 参照

つまり, $k[x]$ の任意のイデアル I はある $f \in k[x]$ を用いて $I = \langle f \rangle$ と表わす事が出来る. また I に対し f は 0 でない定数倍を除いて一意的に定まる.

命題 2.2 $a \in k[x]$ が $f(x) \in k[x]$ の根 $\iff (x - a)$ が $f(x)$ の因子

証明 参考文献 [2] 命題 2.5 参照

以上の 2 つの命題は, どちらもいわゆる割り算アルゴリズムから得られる. これらを用いて以下の定理を示す事が出来た.

主定理 1

$f \in k[x]$ で生成されるイデアル $I = \langle f \rangle \subset k[x]$ に対し, 次が成り立つ.

$f = 0$ 又は $(V(I))^{\sharp} = \deg(f) \iff I(V(I)) = I$

ただし, $\deg(f)$ とは f の次数であり, f が 0 でない定数のとき $\deg(f) = 0$ とする. $f = 0$ のときの次数は

$-\infty$ とする事もあるが、この論文で特に用いる事はない。この定理は一見単項イデアルについてのみ言及しているようであるが、命題 2.1 より問題提起に対する 1 変数多項式環の場合の回答である。

主定理 1 の証明 まず $\Rightarrow$ について示す。 f を場合分けして示す事にする。

(i) $f \in k \setminus \{0\}$ のとき、 $I = \langle f \rangle = k[x]$ より、 $V(I) = \emptyset$ となる。従って、 $I(V(I)) = k[x]$ 。よって、 $I(V(I)) = I$ が成り立つ。

(ii) $f = 0$ のとき $I = 0$ より、 $V(I) = k$ となる。従って、 $I(V(I)) = 0$ 。よって、 $I(V(I)) = I$ が成り立つ。

(iii) $\deg(f) \geq 1$ のとき、 $(V(I))^\sharp = \deg(f) = m$ とする。 $V(I) = \{s_1, \dots, s_m\}$ とすれば、命題 2.2 より

$$f = a(x - s_1) \cdots (x - s_m) \quad (\text{ただし, } a \in k \setminus \{0\})$$

と書ける。ところで命題 2.1 より $I(V(I)) = \langle g \rangle$ を満たす $g \in k[x]$ が存在する。再び命題 2.2 より、

$$g = h(x - s_1) \cdots (x - s_m) \quad (\text{ただし, } h \in k[x] \setminus \{0\})$$

と表わせる。一般に $I \subset I(V(I))$ であるから $f \in I(V(I)) = \langle g \rangle$ 。よって、 $g \mid f$ であり、 f と h の次数を比べれば分かるように、 $h \in k$ でなくてはならない。よって、 $\langle f \rangle = \langle g \rangle$ なので、 $I = I(V(I))$ が成り立つ。

次に、 $\Leftarrow$ を示す。 $f \in k$ の時は明らかなので、 $\deg(f) = m \geq 1$ について示せば十分。

(i) $1 \leq (V(I))^\sharp \leq m - 1$ と仮定する。

$$V(I) = \{q_1, \dots, q_t\} \quad (1 \leq t \leq m - 1)$$

とする。 $I(V(I)) = \langle g \rangle$ とおけば、命題 2.2 より

$$g = b(x - q_1) \cdots (x - q_t) \quad (\text{ただし, } b \in k)$$

と書けるので、

$$I(V(I)) = \langle (x - q_1) \cdots (x - q_t) \rangle \neq \langle f \rangle = I$$

となり不適。

(ii) $(V(I))^\sharp = 0$ のときは、つまり、 $V(I) = \emptyset$ であるが、

$$I(V(I)) = k[x] \neq \langle f \rangle \quad (\langle f \rangle \neq k (\neq 0) \text{ より})$$

となり不適。 f は m 次式なので高々 m 個の根を持つ。つまり、 $(V(I))^\sharp \leq m$ である。よって、(i)、(ii) より、 $(V(I))^\sharp = m$ である。以上より、主定理 1 が証明された。 ■

この主定理 1 の結果であるが、代数閉体上で考えたときの結果に良く似ている側面があることを説明しよう。代数閉体上で、 $I(V(I)) = I$ が成り立つのは I が根基イデアルの場合であった。1 変数なので

$$I = \langle f \rangle = \sqrt{\langle f \rangle}$$

が成り立つ。この時 f は無平方 (square-free) である事がわかっている (参考文献 [1]4, 2, prop9, def10 参照)。つまり、 f が m 次の多項式なら m 個の異なる根を持つということなので、 $(V(I))^\sharp = \deg(f)$ である。また、当然異なる m 個の 1 次多項式の積に分解できることが分かる。

無限体上では f が無平方だとしても, $\deg(f)$ 個の根を持つとは限らないので, 当然ながら代数閉体の場合とは異なる結果である. 具体的な例は例 1 をみてほしい. 既に分かっている事ではあるが, $I = \langle f \rangle$ が根基イデアルであっても, (1) は成り立たないのである.

主定理 1 と上記考察をまとめてみよう. 代数閉体上では f が異なる m 個の 1 次多項式の積に分解できる時に (1) が成り立つ. それは I が根基イデアルである事と同じである. 無限体上で考えると, やはり同様に f が m 個の 1 次多項式の積に分解できる時に (1) が成り立つ.

無限体上でも代数閉体の時と同様に f が異なる 1 次多項式の積に分解出来るときに (1) 式が成り立つのだ.

3 2 変数多項式環の単項イデアルについて

前章で 1 変数の場合は問題提起の解答を得る事が出来た. では 2 変数多項式環 $k[x, y]$ の場合はどうなるのだろうか. 2 章のときと同様, まずは実数体 $\mathbf{R}$ 上でいくつか例を調べてみた.

例 1

$I = \langle x^2 + y^2 \rangle \subset \mathbf{R}[x, y]$ のとき, $\mathbf{V}(I) = (0, 0)$ となり, $\mathbf{I}(\mathbf{V}(I)) = \langle x, y \rangle \neq I$ である.
ただし, $I = \langle x, y \rangle$ の時, $\mathbf{I}(\mathbf{V}(I)) = I$ である.

例 2

$I = \langle x^2 - y^3 \rangle \subset \mathbf{R}[x, y]$ のとき, 計算方法は後ほど示すが, $\mathbf{I}(\mathbf{V}(I)) = I$ が成り立っている.

よって, I が根基イデアルであっても, 一般に (1) 式が成り立つとは限らない事が分かる. この場合, 1 変数の場合の証明方法を応用して, $k[x, y]$ の単項式イデアルについて問題提起に対し (主定理 3) という結果を得た. しかし, $k[x, y]$ は $k[x]$ と異なり, 単項イデアル整域ではなく, 問題提起の解答は得る事は出来なかった.

補足として述べておくと, I を単項式イデアルとすると, $\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$ が成り立つ事は分かっている. (参考文献 [1] の 9.3.exercise10 参照)

以下の 2 つの結果を主定理として挙げておく.

主定理 2

$f \in k[x, y]$ を既約な多項式とし, $I = \langle f \rangle$ とする. このとき,

$$(\mathbf{V}(I))^{\#} = \infty \iff \mathbf{I}(\mathbf{V}(I)) = I$$

主定理 3

$f = f_1 \cdots f_s \in k[x, y]$ を既約な多項式の積で, 任意の異なる i と j において, $f_i \nmid f_j$ として, $I = \langle f \rangle$ とする. このとき,

$$1 \leq \forall l \leq s \text{ で } (\mathbf{V}(\langle f_l \rangle))^{\#} = \infty \iff \mathbf{I}(\mathbf{V}(I)) = I$$

主定理 3 は, 主定理 2 より強力な結果であるので, 本来「主定理 2」ではなく命題としておくべきかもしれない. しかし, 主定理 2 の証明法は本論文の主題の一つでなので主定理としておく. 主定理 3 は強い結果であるが, 主定理 2 からすぐに導かれる事も理由の一つである.

まず, 主定理 2 を証明するのだが, その準備として次の 2 つの命題を用意する.

命題 3.1 $f \in k[x_1, \dots, x_n]$ が既約で $h_1 \cdots h_s$ を割り切るならば, f は h_i のうちどれかを割り切る.

証明 参考文献 [1]3.5.Exercise5 参照

命題 3.2 $f, q \in k[x, y]$ で, $\deg_x(f) = l$ とする. このとき, 次を満たす $h, r \in k[x, y]$ が存在する.

$$\{\text{LC}_x(q)\}^l f = hq + r \text{ かつ, } \deg_x(r) < \deg_x(q)$$

ただし, $\deg_x(f) = l$ は f を $k[y]$ 上の x の多項式と見たときの次数である. また, $\text{LC}_x(q)$ は同様の見方をしたときの, 先頭項係数である. つまり, $\text{LC}_x(q) \in k[y]$ である.

この命題が何を意味するのか, 次の例を用いて説明しておこう.

例 $yx^2 + x + y^3 + 1$ を $(y^2 + 1)x + 1$ で x の多項式と見て “割り算” するという事を考えてみよう. もちろん, このままでは割り算が出来ない. これは $\text{LC}_x(q) = y^2 + 1 \in k[y]$ は逆元を持たない事による. つまり, x の多項式と見た時の係数 $k[y]$ は体でないので, 常に割り算できるとは限らないのである. しかしここで, 命題 3.2 を用いると,

$$(y^2 + 1)^2 (yx^2 + x + y^3 + 1) = \{y(y^2 + 1)x + y^2 - y + 1\} \times \{(y^2 + 1)x + 1\} + \{(y^3 + 1)(y^2 + 1)^2 - (y^2 - y + 1)\}$$

となる. 命題 3.2 の記号で書けば,

$$h = y(y^2 + 1)x + y^2 - y + 1, \quad r = (y^3 + 1)(y^2 + 1)^2 - (y^2 - y + 1)$$

であり, 確かに $\deg_x(r) < \deg_x(q)$ を満たしている. つまり, $\{\text{LC}_x(q)\}^l$ を f に乗じる事により, q での割り算が可能になるのだ.

では, 実際に命題 3.2 を証明する.

命題 3.2 の証明 $\{\text{LC}_x(q)\}^l f$ にたいして, いわゆる割り算アルゴリズムと同様の計算を実際に行っていけばよい. そして条件を満たす q と r が現れる事をみる. $\deg_x(r) = l'$ と置いておく. まず, $\{\text{LC}_x(q)\}^l f$ の先頭項を q を用いて消去する.

$$\{\text{LC}_x(q)\}^l f - \{\text{LC}_x(q)\}^{l-1} \{\text{LC}_x(f)\} x^{l-l'} q = \{\text{LC}_x(q)\}^{l-1} J_1(x, y) \quad (\text{ただし, } \deg_x(J_1(x, y)) < l \text{ である.})$$

とできる. これで, 先頭項を消去できたが, $\deg_x(J_1(x, y)) < l'$ なら,

$$h = \{\text{LC}_x(q)\}^{l-1} \{\text{LC}_x(f)\} x^{l-l'}, \quad r = \{\text{LC}_x(q)\}^{l-1} J_1(x, y)$$

で, 条件を満たす h と q がとれた. $\deg_x(J_1(x, y)) \geq l'$ のときは, $\{\text{LC}_x(q)\}^{l-1} J_1(x, y)$ の先頭項を q を用いて消去する.

$$\{\text{LC}_x(q)\}^{l-1} J_1 - \{\text{LC}_x(q)\}^{l-2} \{\text{LC}_x(J_1)\} x^{\deg_x(J_1)-l'} q = \{\text{LC}_x(q)\}^{l-2} J_2(x, y) \quad (\deg_x(J_2) < \deg_x(J_1))$$

とでき, 先頭項が消去できた. 先ほどと同様に, $\deg_x(J_2(x, y)) < l'$ なら,

$$h = \{\text{LC}_x(q)\}^{l-1} \{\text{LC}_x(f)\} x^{l-l'} + \{\text{LC}_x(q)\}^{l-2} \{\text{LC}_x(J_1)\} x^{\deg_x(J_1)-l'}, \quad r = \{\text{LC}_x(q)\}^{l-2} J_2(x, y)$$

となり, 条件を満たす h と q がとれた. $\deg_x(J_2(x, y)) \geq l'$ のときは, さらに上記のように先頭項を消去する. 以下同様にこの操作を繰り返す. ところで,

$$\deg_x(J_{i+1}) < \deg_x(J_i)$$

である事より, $\deg_x(f) = l$ 回以下の先頭項の消去により (その操作を m 回したとすれば) $\deg_x(J_m) < l'$ となる. この時,

$$r = \{\text{LC}_x(q)\}^{l-m} J_m(x, y)$$

で,

$$h = \{\text{LC}_x(q)\}^{l-1} \{\text{LC}_x(f)\} x^{l-l'} + \{\text{LC}_x(q)\}^{l-2} \{\text{LC}_x(J_1)\} x^{\deg_x(J_1)-l'} + \cdots + \{\text{LC}_x(q)\}^{l-m} \{\text{LC}_x(J_{m-1})\} x^{\deg_x(J_{m-1})-l'}$$

となる. これで, 題意を満たす h と r がとれた. ■

f に $\{\text{LC}_x(q)\}^l$ をかける事で, 1 変数多項式の割り算と全く同様の計算ができるのである. ここでは, $\{\text{LC}_x(q)\}$ の指数は l としているが, 実際は $l - l' + 1$ で十分であることが分かっている. 上記二つの命題を用いて, 主定理 2 を証明する.

主定理 2 の証明 まず, $\Rightarrow$ を示す.

$\mathbf{I}(\mathbf{V}(I)) \supseteq I$ は常に成り立つので, $\subseteq$ の包含関係を示せば良い.

まず,

$$\{b \in k \mid \exists a \in k \quad s.t. \quad (a, b) \in (\mathbf{V}(I))\}^\sharp = \infty \text{ 又は } \{a \in k \mid \exists b \in k \quad s.t. \quad (a, b) \in (\mathbf{V}(I))\}^\sharp = \infty$$

である事を示す. もし上の, 二つの条件が成り立たないとすると $(\mathbf{V}(I))^\sharp = \infty$ ののであるので,

$$\exists a \in k \quad s.t. \quad f(a, y) \in k[y] \text{ の根が無限個}$$

又は,

$$\exists b \in k \quad s.t. \quad f(x, b) \in k[x] \text{ の根が無限個}$$

となるが, いずれにせよ 0 でない 1 変数多項式の根は有限個である事に反する.

なので,

$$\{b \in k \mid \exists a \in k \quad s.t. \quad (a, b) \in (\mathbf{V}(I))\}^\sharp = \infty \quad (*)$$

が成り立つと仮定して示せば十分である. 必要なら x と y の役割を入れ替えれば良い. この時 $\deg_x(f) \geq 1$ になが成り立っていることが分かる. では, 包含関係を示す.

$$F \in \mathbf{I}(\mathbf{V}(I)), \quad \deg_x(F) = c, \quad \deg_x(f) = d$$

とする. $F \in \mathbf{I}(\mathbf{V}(I))$ を示せば良い.

まず, 命題 3.2 を用いて, F を f で “割り算” すると,

$$\{\text{LC}_x(f)\}^d F = h(x, y) f + r(x, y) \tag{2}$$

となる. ただし, $\deg_x(r) < \deg_x(f)$ である. ここで, 次を示す.

claim $r(x, y) = 0$ である.

これを示す. $\forall (a, b) \in \mathbf{V}(I)$ に対し, (2) 式に代入すれば分かるように, $r(a, b) = 0$ である.

(i) $\deg_x(f) = 0$ のとき

繰り返しになるが, $\forall (a, b) \in \mathbf{V}(I)$ に対し, $r(a, b) = 0$ となる. ここで, 仮定より $r(x, y) = r(y) \in k[y]$ となるが, (*) の仮定より, $r(y)$ は無限個の根を持つことになる. 無限体上で無限個の根を持つ多項式は 0 のみである. よって, $r(x, y) = 0$ が示された.

(ii) $\deg_x(f) > 0$ のとき

命題 3.2 を用いて, 今度は f を r で “割り算” する.

$$\{\mathrm{LC}_x(r)\}^d f = h_1(x, y)r + r_1(x, y) \quad (\deg_x(r_1) < \deg_x(r))$$

となる. ここで,

$$\left\{ \begin{array}{l} \deg_x(r_1) = 0 \text{ のとき, (i) と同様にして, } r_1(x, y) = 0 \text{ であるが, } f \text{ が既約な多項式なので, 命題 3.1 より} \\ f \mid h_1 \text{ 又は } f \mid r \text{ であるが, } \deg_x(r) < \deg_x(f) \text{ かつ, } \deg_x(h_1) < \deg_x(f) \text{ であるので, 矛盾.} \end{array} \right\}$$

つまり, $\deg_x(r_1) > 0$ である. 今度は命題 3.2 を用いて f を r_1 で割り算する.

$$\{\mathrm{LC}_x(r_1)\}^d f = h_2(x, y)r_1 + r_2(x, y) \quad (\deg_x(r_2) < \deg_x(r_1))$$

となる. ここで, もし $\deg_x(r_2) = 0$ であったとすると, 上記 $\{\}$ 内の r_1 を r_2 に置き換えて全く同様に議論すれば, 矛盾が生じる. つまり, $\deg_x(r_2) > 0$ である. 今度は, f を r_2 で割り算する, そして上と同様の議論により, $\deg_x(r_3) = 0$ で矛盾が生じ, $\deg_x(r_3) > 0$ が分かる. 以下この議論を繰り返していくのだが,

$$\deg_x(r_1) > \deg_x(r_2) > \deg_x(r_3) > \dots$$

であるので, ある $t > 0$ において, $\deg_x(r_t) = 0$ となる. しかし, やはり上記 $\{\}$ 内と同様の議論により, 矛盾が生じる. つまり, $\deg_x(r) > 0$ でない.

以上 (i), (ii) より, $r(x, y) = 0$ が示された.

claim が示されたところで, もう一度 (2) 式をみてほしい. f が既約で, $f \mid \{\mathrm{LC}_x(f)\}^d F$ なので, 命題 3.1 より, $f \mid \mathrm{LC}_x(f)$ 又は $f \mid F$ である. ところが, $\deg_x(\mathrm{LC}_x(f)) = 0$ と, $\deg_x(f) > 0$ であることから, $f \mid F$ となる. 即ち,

$$F \in \langle f \rangle = I$$

となり, $\Rightarrow$ が示された.

あとは, $\Leftarrow$ を示せば良い.

背理法で示す. $(\mathbf{V}(I))^\sharp < \infty$ と仮定すれば,

$$\mathbf{V}(I) = \{(a_1, b_1), \dots, (a_s, b_s)\}$$

とおける. このとき, $\mathbf{I}(\mathbf{V}(I)) = \mathbf{I}\{(a_1, b_1), \dots, (a_s, b_s)\}$ なので,

$$(x - a_1) \cdots (x - a_s) \in \mathbf{I}(\mathbf{V}(I))$$

である. 仮定より, $\mathbf{I}(\mathbf{V}(I)) = \langle f \rangle$ なので,

$$f \mid (x - a_1) \cdots (x - a_s)$$

となる. f が既約なので, 命題 3.1 より,

$$f \mid (x - a_1) \quad \text{or} \cdots \text{or} \quad f \mid (x - a_s)$$

である. 逆に $x - a_i$ は既約なので,

$$(x - a_1) \mid f \quad \text{or} \cdots \text{or} \quad (x - a_s) \mid f$$

である. よって,

$$\langle f \rangle = \langle x - a_1 \rangle \quad \text{or} \cdots \text{or} \quad \langle f \rangle = \langle x - a_s \rangle$$

が成り立つ. 従って,

$$\mathbf{V}(\langle f \rangle) = \mathbf{V}(I) \neq \{(a_1, b_1), \dots, (a_s, b_s)\}$$

となるが, これは仮定に矛盾. 以上より $(\mathbf{V}(I))^\sharp = \infty$ が示された. ■

ところで, 例 2 で計算方法は後に示すと書いたが, それはこの主定理 2 の証明法と全く同様なものである. 即ち, $x^2 - y^3$ が既約である事を示し, $\mathbf{I}(\mathbf{V}(I))$ から任意にとった元 F が $I = \langle x^2 - y^3 \rangle$ に入っている事を示せば良い. $x^2 - y^3$ が無限個の根を持つことにより, F を $x^2 - y^3$ で割り算して上記証明と同様にしてそれを示す事が出来る. この主定理 2 の証明法は, 具体的な多項式で生成されるイデアルで, $\mathbf{I}(\mathbf{V}(I)) = I$ を満たすものを調べる際に発見した手法を一般化したものである.

次に主定理 3 を示す. これは主定理 2 からすぐに導かれる.

主定理 3 の証明

まず, $\Rightarrow$ を示す.

$$\mathbf{I}(\mathbf{V}(I)) = \mathbf{I}(\mathbf{V}(f_1 \cdots f_s)) = \mathbf{I}(\mathbf{V}(f_1) \cup \cdots \cup \mathbf{V}(f_s)) = \mathbf{I}(\mathbf{V}(f_1)) \cap \cdots \cap \mathbf{I}(\mathbf{V}(f_s))$$

となる. 仮定と主定理 2 より, 任意の i で $\mathbf{I}(\mathbf{V}(f_i)) = \langle f_i \rangle$ が成り立つので,

$$\mathbf{I}(\mathbf{V}(I)) = \langle f_1 \rangle \cap \cdots \cap \langle f_s \rangle = \langle f_1 \cdots f_s \rangle$$

となり, $\Rightarrow$ が示された.

次に, $\Leftarrow$ を示す. 背理法で示す事とする. $(\mathbf{V}(\langle f_1 \rangle))^\sharp \neq \infty$ と仮定し, 矛盾が生じる事を示せば十分である. その背理法の仮定より,

$$\mathbf{V}(\langle f_1 \rangle) = \{(a_1, b_1), \dots, (a_t, b_t)\}$$

とできる. この時,

$$(x - a_1) \cdots (x - a_t) f_2 \cdots f_s \in \mathbf{I}(\mathbf{V}(I))$$

である. 仮定より,

$$\mathbf{I}(\mathbf{V}(I)) = I = \langle f_1 \cdots f_s \rangle.$$

なので,

$$f_1 \cdots f_s \times h = (x - a_1) \cdots (x - a_t) f_2 \cdots f_s \quad (h \in k[x, y])$$

と表わせる. 両辺を $f_2 \cdots f_s$ で割れば,

$$f_1 \times h = (x - a_1) \cdots (x - a_t).$$

即ち,

$$f_1 \mid (x - a_1) \cdots (x - a_t)$$

となる. 後は, 主定理 2 の証明方法と全く同様にして, 矛盾が生じる事が言える. これで $\Leftarrow$ が示された.

以上で, 主定理 3 が証明された. ■

主定理 3 によって, ある多項式が無数個の零点を持つ異なる既約多項式の積に分解できる時, それによって生成されるイデアルは (1) 式を満たす事が分かった.

これも, やはり代数閉体の場合と同じである. 代数閉体上では, 自然と多項式が無数個の零点を持つ既約多項式の積に分解できる. そして, それらの分解された多項式が全て異なる時に, 即ち I が根基イデアルになる時に, (1) が成り立つ. そして, 無限体上でも同じように f が分解できる時に限り, (1) が成り立つ事を主定理 3 は主張してるのである.

主定理 2 の方法は 3 変数以上の多項式環には適用できない. なぜなら, claim の証明の (i) を見ると, ここで「無限体上の 1 変数多項式が無数個の根を持つとき, その多項式は 0」という命題を使っている. なので, このような証明方法は適用できない.

3 変数以上の多項式環上の単項イデアルについては調べる事ができなかった. どうやら 1 変数のときと同様に, イデアルを定義する多項式の根の個数が重要になっているようなので, イデアルによって定まる適当な不変量が必要なのかもしれない. 主定理 3 を単に拡張したものがその答えなのか, あるいは何か別の条件が必要なのか. 今後の研究課題としたいと思う.

謝辞

本論文を執筆するにあたって、内容や構成など様々な点においてご指導いただいた楫元先生、そして研究室の先輩、同輩に心より感謝致します。

参考文献

- [1] D.Cox J.Little D.O'shea *Ideals, Varieties, and Algorithms* Springer
- [2] 酒井 文雄, 環と体の理論, 共立出版株式会社