４章§1の前半
代数と幾何の関係

担当：長谷川禎彦

2013/3/12

ヒルベルトの零点定理

- 多様体 V は，V 上で消える多項式からなるイデアルに関係付けられる

$$\mathbf{I}(V) = \{f \in k[x_1, \cdots, x_n] : f(x) = 0 \text{ for } \forall x \in V\}$$

$$\begin{array}{ccc} \text{affine variety} & & \text{ideal} \\ V & \rightarrow & \mathbf{I}(V) \end{array}$$

- 逆に，イデアルに対して，多様体 V を定義出来る．

$$\mathbf{V}(I) = \{x \in k^n : f(x) = 0 \text{ for } \forall f \in I\}$$

ヒルベルトの零点定理

ヒルベルトの基底定理により，任意のイデアルIは有限個の生成集合を持つ

$$\exists g_1, \cdots, g_t \in I \Rightarrow I = \langle g_1, \cdots, g_t \rangle$$

$$\mathbf{V}(I) = \mathbf{V}(g_1, \ldots, g_t)$$

ideal		affine variety
I	$\rightarrow$	$\mathbf{V}(I)$

ヒルベルトの零点定理

- イデアルと多様体は一対一にはなっていない
  - 異なるイデアルが同じ多様体にマップされることがある

$$f = x^2 - 1$$

例
$(x+1)(x^2-1)$

イデアル　$I_1 = \langle f \rangle \supsetneq \langle f^2 \rangle = I_2$

多様体　$\mathbf{V}(I_1) = \mathbf{V}(I_2) = \{1, -1\}$

- 代数的閉体でない場合は，もっと問題がある

（補足）代数的閉体

- 体 k が代数的閉体であるとは、一次以上の任意の k 係数一変数多項式が k 上に根を持つこと [wikipedia]

$$x^2 + x + 1 \in \mathbb{Z}[x]$$

$$x = -\frac{1}{2} + \frac{1}{2}\sqrt{3}i, -\frac{1}{2} - \frac{1}{2}\sqrt{3}i \notin \mathbb{Z}$$

Z は代数的閉体ではない

代数的閉体でない場合 $\mathbb{R}[x]$

$$I_1 = \langle 1 \rangle = \mathbb{R}[x]$$
$$I_2 = \langle 1 + x^2 \rangle$$
$$I_3 = \langle 1 + x^2 + x^4 \rangle$$

$$\mathbf{V}(I_1) = \mathbf{V}(I_2) = \mathbf{V}(I_3) = \emptyset$$

- k が代数的閉体の場合は，空な多様体を表すイデアルは一意に決まるか？

- 1変数，多変数どちらの場合もYES

一変数の場合の証明

一変数 $k[x]$ では，任意のイデアルは一つの多項式で生成される(1章§5の系4)

$$f \in k[x] \qquad I = \langle f \rangle$$

$$\mathbf{V}(I) = \{x \in k : f(x) = 0\}$$

k は代数的閉体なので，$\mathbf{V}(I)$ が空集合になるには f は定数で無ければならない．

$$I = \langle 1 \rangle = k[x] \qquad \square$$

定理1 弱形の零点定理
（*Nullstellensatz*）

定理 1 (弱形の零点定理) k を代数的閉体とし，$I \subset k[x_1, \ldots, x_n]$ を $\mathbf{V}(I) = \emptyset$ を満たすイデアルとする．このとき $I = k[x_1, \ldots, x_n]$ である．

- **前のページは1変数の場合であったが，多変数でも言えるということ**

証明

イデアル I に定数 1が含まれていることを示せば良い

$$1 \in I$$

なぜなら

$$\langle 1 \rangle = k[x_1, .., x_n]$$

証明は帰納法. $n = 1$ の場合は既に示した.

n-1で多項式環 $k[x_2, ..., x_n]$ に対して成立していると仮定する. $\mathbf{V}(I) = \emptyset$ を満たす任意のイデアルを考える. $I = \langle f_1, ..., f_s \rangle \subset k[x_1, ..., x_n]$

f_1が定数関数でないと仮定する. その場合の全次数は1以上である.

以下の変数変換を考える（係数aは上手く選ぶとする）

$$\left.\begin{aligned} x_1 &= \tilde{x}_1 \\ x_2 &= \tilde{x}_2 + a_2\tilde{x}_1 \\ &\vdots \\ x_n &= \tilde{x}_n + a_n\tilde{x}_1 \end{aligned}\right\} \text{座標変換(1)}$$

これをf_1に代入すると，

$$\begin{aligned} f_1(x_1,\ldots,x_n) &= f_1(\tilde{x}_1, \tilde{x}_2 + a_2\tilde{x}_1, \ldots, \tilde{x}_n + a_n\tilde{x}_1) \\ &= c(a_2,\ldots,a_n)\tilde{x}_1^N + (\tilde{x}_1 \text{ に関して } N \text{ 次未満の式}) \end{aligned}$$

$c(a_2,\ldots,a_n)$ は零関数ではない（演習3）．

代数的閉体は無限体（演習4）．無限体でありかつ零関数ではないので，　$c(a_2,\ldots,a_n) \neq 0$

となる $a_2,\ldots,a_n$ を選ぶことが出来る．

$c(a_2, \ldots, a_n)$をこのように選んで，座標変換(1)より，多項式 $f \in k[x_1, .., x_n]$ が写された多項式を $\tilde{f} \in k[\tilde{x}_1, .., \tilde{x}_n]$ と表す．集合 $\tilde{I} = \{\tilde{f} : f \in I\}$ はイデアルとなる(演習5)．

変換元の方程式が解を持たないので，変換後の方程式も解を持たない：$\mathbf{V}(\tilde{I}) = \emptyset$

また，変換は定数には影響を及ぼさないので

$$1 \in \tilde{I} \Rightarrow 1 \in I$$

以上より，$1 \in \tilde{I}$ を示せば十分．

$$\tilde{f}_1(\tilde{x}_1,\ldots,\tilde{x}_n) = c(a_2,\ldots,a_n)\tilde{x}_1^N + (\tilde{x}_1 \text{ に関して } N \text{ 次未満の式})$$

$c(a_2,\ldots,a_n) \neq 0$ であるので，3章§2系4の拡張定理を用いることが可能．これにより，消去イデアルと射影が関連付けられる．

射影　$\pi_1 : (x_1, x_2, .., x_n) \to (x_2, .., x_n)$

消去イデアル　$\tilde{I}_1 = \tilde{I} \cap k[\tilde{x}_2, .., \tilde{x}_n]$

$$\mathbf{V}(\tilde{I}_1) = \pi_1(\mathbf{V}(\tilde{I}))$$

ここは前提条件

$$\mathbf{V}(\tilde{I}_1) = \pi_1(\mathbf{V}(\tilde{I})) = \pi_1(\emptyset) = \emptyset$$

帰納法の仮定より，n-1変数の多項式環 $k[x_2, .., x_n]$ で結果が証明されているとしているので，

$$\mathbf{V}(\tilde{I}_1) = \emptyset \quad \Rightarrow \quad \tilde{I}_1 = \langle 1 \rangle = k[x_2, .., x_n]$$

$$1 \in \tilde{I}_1$$

一方で，$\tilde{I}_1$ は $\tilde{I}$ の部分空間であるので

$$1 \in \tilde{I}_1 \in \tilde{I} \qquad \square$$

整合性問題

- 以下の連立多項式が解を持つか

$$\begin{aligned} f_1 &= 0 \\ f_2 &= 0 \\ &\vdots \\ f_s &= 0 \end{aligned} \qquad \mathbb{C}^n$$

$$\mathbf{V}(f_1, \ldots, f_s) = \emptyset$$

$$1 \in \langle f_1, \ldots, f_s \rangle$$

任意の代数的閉体に適用可能

整合性問題

- 簡約グレブナ基底が{1}の場合共通ゼロ点を持たない．そうでない場合はもつ．
- 代数的閉体でなくとも，片方向には正しい

イデアルと多様体

- イデアルと多様体の間には1対1対応はない

$$\mathbf{V}(x) = \mathbf{V}(x^2) = \{0\}$$

- 多項式とそのべき乗は同じ集合上で消えるから

- 異なるイデアルが同じ多様体を定めるのはこの場合に限る

  – ヒルベルトのゼロ点定理

定理2 ヒルベルトの零点定理

定理 2 (ヒルベルトの零点定理) k を代数的閉体とする．多項式 f，f_1，$\ldots$，$f_s \in k[x_1, \ldots, x_n]$ が $f \in \mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$ を満たすとする．このとき，ある整数 $m \geq 1$ が存在して

$$f^m \in \langle f_1, \ldots, f_s \rangle$$

となる．逆も成立する．

証明

多項式 $f_1, f_2, .., f_s \in k[x_1, .., x_n]$ の共通ゼロ点で消える多項式fに対して，整数 $m \geq 1$ と多項式 $A_1, .., A_s$ で

$$f^m = \sum_{i=1}^{s} A_i f_i$$

を満たすものが存在することを示す必要がある．

そのために，イデアル

$$\tilde{I} = \langle f_1, ..., f_s, 1 - yf \rangle \subset k[x_1, ..., x_n, y]$$

を考える．まず以下を示す．

$$\mathbf{V}(\tilde{I}) = \emptyset$$

これを示すために，$(a_1, \ldots, a_n, a_{n+1}) \in k^{n+1}$をとると以下の2つの場合が考えられる．

1. $(a_1, \ldots, a_n)$ は $f_1, .., f_s$ の共通ゼロ点である
2. $(a_1, \ldots, a_n)$ は $f_1, .., f_s$ の共通ゼロ点でない

1.の場合，fが $f_1, .., f_s$ が共通零点で消えるから，

$f(a_1, \ldots, a_n) = 0$ となり，$(a_1, \ldots, a_n, a_{n+1})$では

$$1 - yf = 1 - a_{n+1} f(a_1, .., a_n) \neq 0$$

$$(a_1, \ldots, a_n, a_{n+1}) \notin \mathbf{V}(\tilde{I})$$

2.の場合はあるiに対して $f_i(a_1, .., a_n) \neq 0$

関数fをn+1変数の関数と捉えると,

$$f_i(a_1, .., a_n, a_{n+1}) \neq 0$$

$$(a_1, ..., a_n, a_{n+1}) \notin \mathbf{V}(\tilde{I})$$

$(a_1, ..., a_n, a_{n+1})$は任意なので $\mathbf{V}(\tilde{I}) = \emptyset$

弱形の零点定理より $1 \in \tilde{I}$

つまり, $1 = \sum_{i=1}^{s} p_i(x_1, ..., x_n, y) f_i + q(x_1, ..., x_n, y)(1 - yf)$

となるような多項式 $p_i, q \in k[x_1, .., x_n, y]$ が存在する.

ここで, $y = 1/f = 1/f(x_1, .., x_n)$ とおくと

$$1 = \sum_{i=1}^{s} p_1 \left(x_1, ..., x_n, \frac{1}{f(x_1, ..., x_n)} \right) f_i$$

分母を打ち消すような十分大きなf^mを両辺にかけると

$$f^m = \sum_{i=1}^{s} A_i f_i \qquad \square$$

定理の証明に必要な演習問題の（多分合っている）回答

演習問題3～5

（補足）斉次多項式

- **次数を揃えた多項式**

$$h_N(x_1,..,x_n) = \sum_{m_1+\cdots+m_n=N} \alpha_{m_1,..,m_n} x_1^{m_1} x_2^{m_2} \cdots x_n^{m_n}$$

例　$h_2(x_1,x_2,x_3) = x_1^2 + 3x_2x_3 - 2x_3^2$

演習問題3

全次数Nの多項式 $f_1(x_1, \ldots, x_n)$

座標変換

$$\tilde{f}_1 = c(a_2, \ldots, a_n)\tilde{x}_1^N + (\tilde{x}_1 \text{ degree less than } N)$$

この時 $c(a_2, \cdots, a_n) \neq 0$

復習：全次数

$$x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$$

$$|\alpha| = \alpha_1 + \alpha_2 + \cdots + \alpha_n$$

a.

fを斉次多項式として表すと

$$f(x_1, .., x_n) = h_N(x_1, .., x_n) + ... + h_0(x_1, .., x_n)$$

座標変換(1)により

$$\tilde{f} = c(a_2, ..., a_n)\tilde{x}_1^N + (\tilde{x}_1 \text{ degree less than } N)$$

この時，以下を示せ

$$c(a_2, ..., a_n) = h_N(1, a_2, ..., a_n)$$

証明

今，$h_N(x_1, ..., x_n)$ を以下の形に表す．

$$h_N(x_1, .., x_n) = \sum_{m_1+\cdots+m_n=N} \alpha_{m_1,..,m_n} x_1^{m_1} x_2^{m_2} \cdots x_n^{m_n}$$

座標変換(1)を代入すると

$$= \sum_{m_1+\cdots+m_n=N} \alpha_{m_1,..,m_n} \tilde{x}^{m_1} (\tilde{x}_2 + a_2\tilde{x}_1)^{m_2} \cdots (\tilde{x}_n + a_n\tilde{x}_1)^{m_n}$$

$$= \tilde{x}_1^N \sum \alpha_{m_1,..,m_n} a_2^{m_2} \cdots a_n^{m_n} + (\tilde{x}_1 \text{ degree less than } N)$$

$$= \tilde{x}_1^N \underbrace{h(1, a_2, ..a_n)}_{\| \; c(a_2, ..., a_n)} + \quad (\tilde{x}_1 \text{ degree less than } N) \quad \square$$

b.

斉次多項式 $h(x_1, .., x_n) \in k[x_1, .., x_n]$が零多項式であることと，$h(1, x_2, .., x_n) \in k[x_2, .., x_n]$ が零多項式であることは同値である．

[証明]

h_mをx_1に関して以下のように書く

$$h_m(x_1,..,x_n) = x_1^m g_0(x_2,..,x_n) + x_1^{m-1} g_1(x_2,..,x_n) + \cdots + x_1^0 g_m(x_2,..,x_n)$$

この時

$$h_m(1,x_2,..,x_n) = g_0(x_2,..,x_n) + g_1(x_2,..,x_n) + \cdots + g_m(x_2,..,x_n)$$

ここで，g_m は $x_2,..,x_n$ に関してm次の斉次多項式なので，g_mと g_k の項は$m \neq k$の場合同じ次数の項を含まない．

$$g_m(x_2,..,x_n) = \sum_{k_2+..+k_n=m} \alpha_{k_2,..,k_n} x_2^{k_2} \cdots x_n^{k_n}$$

よって $h_m(1, x_2, .., x_n)$ が零多項式になる時も，$h_m(x_1, x_2, .., x_n)$ が零多項式になる時も，gが零多項式である．よって示された．□

相殺してしまいそうなパターン

$$h_m(x_1, .., x_n) = x_1^m g_0(x_2, .., x_n) + x_1^{m-1} g_1(x_2, .., x_n) + \cdots + x_1^0 g_m(x_2, .., x_n)$$

$$h_m(1, x_2, .., x_n) = g_0(x_2, .., x_n) + g_1(x_2, .., x_n) + \cdots + g_m(x_2, .., x_n)$$

$$\| \qquad\qquad \| \qquad\qquad -$$

$$x_2 \qquad\qquad -x_2$$

というパターンは起きないということ

c.

最初の仮定より，f_1の全次数Nは1以上であると仮定した．これより $h_N(x_1, .., x_n) \neq 0$

b.の結果から，直ちに $c(a_2, .., a_n) \neq 0$ □

これは零関数でないという意味

bで示したこと

$$h(x_1, .., x_n) \text{ is not zero poly} \Leftrightarrow h(1, x_2.., x_n) \text{ is not zero poly}$$

aで示したこと

$$0 \neq h(1, a_2, .., a_n) = c(a_2, .., a_n)$$

演習問題4

代数的閉体 k は無限体である

（証明）

仮に k は有限体であると仮定し，その全ての元を以下で表す（ここでは簡単のため二個で示すが，N個の場合でも全く証明は同じ）

$$k = \{a_1, a_2\}$$

（演習問題のヒントを使って）

関数 $f(x)$ を以下で定義する

$$f(x) = (x - a_1)(x - a_2) + 1 = x^2 - \overbrace{(a_1 + a_2)}^{\in k} x + \overbrace{a_1 a_2}^{\in k} + 1$$

この関数の係数は k の元で，k は代数的閉体と仮定したので $f(x)=0$ の解は k 上にあるはずである．

しかし，f は全ての k の元において

$$f(a_1) = f(a_2) \neq 0$$

であるので，体 k 上にはなく，代数的閉体であるとした仮定に反する．

よって，代数的閉体は無限体．□

演習問題5

多項式 $f \in k[x_1, \ldots, x_n]$ が座標変換(1)によって移された多項式を $\tilde{f} \in k[\tilde{x}_1, \ldots, \tilde{x}_n]$ と表す.

この時,

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

が $k[\tilde{x}_1, \ldots, \tilde{x}_n]$ のイデアルとなることを示せ.

復習:イデアルの条件(§1参照)

(i) $0 \in \tilde{I}$

(ii) $\tilde{f}, \tilde{g} \in \tilde{I} \to \tilde{f} + \tilde{g} \in \tilde{I}$

(iii) $\tilde{f} \in \tilde{I} \wedge \tilde{h} \in k[\tilde{x}_1, .., \tilde{x}_n] \to \tilde{h}\tilde{f} \in \tilde{I}$

(i)は自明. ここでは(ii) (iii)を示す.

変数変換の写像をTと表すと逆写像も定義できて

$$T \circ T^{-1} = 1$$

$$T\begin{cases} x_1 &= \tilde{x}_1 \\ x_2 &= \tilde{x}_2 + a_2\tilde{x}_1 \\ &\vdots \\ x_n &= \tilde{x}_n + a_n\tilde{x}_1 \end{cases} \qquad T^{-1} = \begin{cases} \tilde{x}_1 &= x_1 \\ \tilde{x}_2 &= x_2 - a_2 x_1 \\ &\vdots \\ \tilde{x}_n &= x_n - a_n x_1 \end{cases}$$

$$\tilde{f}, \tilde{g} \in \tilde{I} \qquad T^{-1}(\tilde{f} + \tilde{g}) = f + g \in I$$

$$\tilde{f} + \tilde{g} = T(f + g) \in \tilde{I}$$

これより(ii)が成立することが示された.

(iii)を示す.

$\tilde{h} \in k[\tilde{x}_1, .., \tilde{x}_n] \quad \tilde{f} \in \tilde{I}$

とした時, Tの逆写像の操作を見れば,

$$T^{-1}(\tilde{h}) \in k[x_1, ..x_n]$$

は明らかである.

$$T^{-1}(\tilde{h}\tilde{f}) = T^{-1}(\tilde{h})f \in I$$

これから, $\tilde{h}\tilde{f} \in \tilde{I}$

これで(iii)が示された. □