平成２１年６月１２日　八起数学塾

ヒルベルトの零点定理

1　準備

次の定理はイデアルについての零点定理と考えることができる。(理由は定理 2.2 参照)

定理 1.1.

$\mathfrak{a}$ を可換環 A の (1) ではないイデアルとすれば $\sqrt{\mathfrak{a}} = \bigcap_{\mathfrak{p} \in V(\mathfrak{a})} \mathfrak{p}$ が成り立つ

証明.

$f \in \sqrt{\mathfrak{a}}$ とすると１以上の整数 n が存在して $f^n \in \mathfrak{a}$ である。$\mathfrak{p} \in V(\mathfrak{a})$ ならば $f^n \in \mathfrak{a} \subset \mathfrak{p}$ であって、$\mathfrak{p}$ が素イデアルであるから $f \in \mathfrak{p}$ が成り立つ。よって $\sqrt{\mathfrak{a}} \subset \bigcap_{\mathfrak{p} \in V(\mathfrak{a})} \mathfrak{p}$ である。

逆の包含関係を示すために $f \notin \sqrt{\mathfrak{a}}$ のとき $\exists \mathfrak{p} \in V(\mathfrak{a})$ で $f \notin \mathfrak{p}$ となることを示す。

その１：局所化を使わない直接的な証明

このような $\mathfrak{p}$ があれば、$\forall n$ に対して $f^n \notin \mathfrak{p}$ であることに着目して、積閉集合 $S = \{1, f, f^2, ...\}$ を考える。

イデアルの集合 $\mathfrak{I} = \{\mathfrak{b} | \mathfrak{a} \subset \mathfrak{b}$ かつ $S \cap \mathfrak{b} = \emptyset\}$ は $\mathfrak{a}$ を含むので、空集合ではない。さらに集合の包含関係を順序として帰納的であるから、Zorn の補題によって、極大元を持つ。その極大元の１つを $\mathfrak{p}$ とする。$\mathfrak{p} \in \mathfrak{I}$ だから $\mathfrak{a} \subset \mathfrak{p}$ かつ $f \notin \mathfrak{p}$ なので、後は $\mathfrak{p}$ が素イデアルであることを示せば良い。

$a, b \notin \mathfrak{p}$ かつ $ab \in \mathfrak{p}$ とする。$\mathfrak{p}$ の極大性によって $S \cap \{(a) + \mathfrak{p}\} \neq \emptyset, S \cap \{(b) + \mathfrak{p}\} \neq \emptyset$ なので、$\exists m, n, \exists x, y \in A, \exists p, q \in \mathfrak{p}$ で $f^m = xa + p, f^n = yb + q$ となるが、$f^{m+n} = xyab + xaq + ybp + pq \in \mathfrak{p}$ だから矛盾である。よって $\mathfrak{p}$ は素イデアルである。

その２：局所化を使う楽な証明

S は、上記その１と同じ積閉集合とし、自然な写像 $A \to A/\mathfrak{a}$ における f, S の像をそれぞれ $\bar{f}, \bar{S}$ とする。$f \notin \sqrt{\mathfrak{a}}$ だから $0 \notin \bar{S}$ であり、従って $(A/\mathfrak{a})_{\bar{f}}$ は零環ではないから、$\mathrm{Spec}(A/\mathfrak{a})_{\bar{f}} \neq \emptyset$。そこで $\mathfrak{q} \in \mathrm{Spec}(A/\mathfrak{a})_{\bar{f}}$ を自然な写像 $A \to A/\mathfrak{a} \to (A/\mathfrak{a})_{\bar{f}}$ で A に引き戻してそれを $\mathfrak{p}$ とすれば、$\mathfrak{p}$ は明らかに所望の条件を満たす。

Q.E.D.

F を体 k 上の多項式環 $k[x_1, x_2, ..., x_n]$ の部分集合とし、F が生成するイデアルは (1) でないとする。この場合 F を含む極大イデアルが存在するので、それを１つ取って固定し、それを $\mathfrak{m}$ とする。$K = k[x_1, x_2, ..., x_n]/\mathfrak{m}$ は k の拡大体と考えて良い。x_i の K における像を a_i とすると、$f \in k[x_1, x_2, ..., x_n]$ の K における像は $f(a_1, ..., a_n)$ である。ここで $f \in F$ とすると $f \in \mathfrak{m}$ だから、この場合には $f(a_1, ..., a_n) = 0$ が成り立つ。これは F が生成するイデアルが (1) ではない場合、k の適当な拡大体 K を取って、F の元の共通零点が K^n に存在するようにできることを示している。

ここで特に $n = 1$ の場合を考えると（(0) は $k[x_1]$ の極大イデアルではないので)、$0 \neq f \in \mathfrak{m}$ が存在し、$f(a_1) = 0$ であるから、$K = k(a_1)$ は k の代数拡大体である。

次の定理は $n = 1$ の場合に限らず、K が k の代数拡大体であることを主張する。この定理はヒルベルトの零点定理の代数的な表現である。

定理 1.2.

体上の有限生成代数が体ならば、それは有限生成加群、従って有限次の拡大体である。

証明.

k, K を体とし、K が k の有限生成代数になっているとすれば、ネーターの正規化定理によって、k 上代数独立で、$k[y_1, ..., y_m] \hookrightarrow K$ が整拡大となるような $y_1, ..., y_m \in K$ が存在する。ここで $m \geqq 1$ と仮定すると、$y_1 \in K$ だから $y_1^{-1} \in K$ であり、y_1^{-1} は $k[y_1, ..., y_m]$ 上整だから、$\exists f \in k[y_1, ..., y_m]$ で $y_1^{-n} + f(y_1, ..., y_m)y_1^{-(n-1)} = 0$ となるが、この両辺に y_1^n を掛けると $1 + f(y_1, ..., y_m)y_1 = 0$ となって、$y_1, ..., y_m$ が k 上代数独立であることに反する。よって $m = 0$ であるから、$k \hookrightarrow K$ は整拡大である。再び K が k の有限生成代数であることから、K は k 上代数的な元を有限個付け加えて得られることが分る。よって主張が証明された。

Q.E.D.

この定理によって、環 A が体 k 上の有限生成代数の場合に、先の定理 1.1 を改良することができる。

定理 1.3.

環 A が体 k 上の有限生成代数のとき、$\mathfrak{a}$ を A の (1) ではないイデアルとすれば $\sqrt{\mathfrak{a}} = \bigcap_{\mathfrak{m}\text{ は }\mathfrak{a}\text{ を含む極大イデアル}} \mathfrak{m}$ が成り立つ。

定理 1.3 の証明のために補題を示す。

補題 1.4.

B を整域、A を B の部分整域とする。B が A 上整ならば、A が体であることと B が体であることとは同値である。

証明.

A が体であるとする。$0 \neq b \in B$ は A 上整だから b を根に持つ A 係数のモニック多項式が存在する。このようなモニック多項式で次数が最小のものを $x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0$ とする。
仮に $a_0 = 0$ とすると $b(b^{n-1} + a_{n-1}b^{n-2} + ... + a_1) = 0$ だが、$b \neq 0$ であり、しかも B が整域だから、$b^{n-1} + a_{n-1}b^{n-2} + ... + a_1 = 0$ となって最小性に反する。よって $a_0 \neq 0$ である。
A は体だから $b \cdot (b^{n-1} + a_{n-1}b^{n-2} + ... + a_1)(-a_0^{-1}) = 1$。従って b は単元であり、B は体である。

B が体であるとする。$0 \neq a \in A$ は B において逆元を持ち、それは A 上整だから、$\exists a_i \in A$ で $a^{-n} + a_{n-1}a^{-(n-1)} + ... + a_1a^{-1} + a_0 = 0$ よって $a^{-1} = -(a_{n-1} + ... + a_1a^{n-2} + a_0a^{n-1}) \in A$。従って A は体である。

Q.E.D.

定理 1.3 の証明.

$\sqrt{\mathfrak{a}} \subset \bigcap_{\mathfrak{m}\text{ は }\mathfrak{a}\text{ を含む極大イデアル}} \mathfrak{m}$ の証明は問題ないので、$\sqrt{\mathfrak{a}} \supset \bigcap_{\mathfrak{m}\text{ は }\mathfrak{a}\text{ を含む極大イデアル}} \mathfrak{m}$ を示す。

1.1 の「その 2」の記号をそのまま使う。$(A/\mathfrak{a})_{\bar{f}}$ は零環ではないから極大イデアルを持つ。それを $\mathfrak{n}$ として体 $K = (A/\mathfrak{a})_{\bar{f}}/\mathfrak{n}$ を考える。$(A/\mathfrak{a})_{\bar{f}} = (A/\mathfrak{a})[1/\bar{f}]$ に注意すれば、K が k の有限生成代数であることが分るから、定理 1.2 によって、K は k の有限次拡大体、従って整拡大である。

よって自然な写像 $A \to A/\mathfrak{a} \to (A/\mathfrak{a})_{\bar{f}} \to K$ の kernel を $\mathfrak{m}$ とすれば、$A/\mathfrak{m} \to K$ は単射かつ整であること

が分る。ここで K は体だから、補題 1.4 によって $A/\mathfrak{m}$ も体である。よって $\mathfrak{m}$ は A の極大イデアルであり、作り方から $\mathfrak{a} \subset \mathfrak{m}$ かつ $f \notin \mathfrak{m}$ である。

Q.E.D.

注意 1.5 (**Zariski 位相による証明の再構成**)**.**

定理 1.1 によって、$D(f) \neq \emptyset$ が $f \notin \sqrt{(0)}$ と同値であることに注意せよ。上記定理 1.3 の証明で $\mathfrak{a} = (0)$ の場合を考えれば分るように、環 A が体 k の有限生成代数ならば、任意の $D(f) \neq \emptyset$ に対して m-Spec $A \cap D(f) \neq \emptyset$ が成り立つ。

$\{D(f) | f \in A\}$ は Zariski 位相の開基底を成すから、これは環 A が体 k の有限生成代数の場合、Zariski 位相において、m-Spec A が Spec A の稠密集合であることを示している。この立場から定理 1.3 の証明を再構成すると次のようになる。

”$D(\bar{f})$ は空集合ではないから極大イデアルすなわち $\mathrm{Spec}(A/\mathfrak{a})$ の閉点を持つので、それを $\bar{\mathfrak{m}}$ とする。$\mathrm{Spec}(A/\mathfrak{a})$ が $V(\mathfrak{a})$ と位相同型であることに注意して、$\bar{\mathfrak{m}}$ に対応する $V(\mathfrak{a})$ の点を $\mathfrak{m}$ とする。$\mathfrak{m}$ は閉集合 $V(\mathfrak{a})$ の閉点であるから、Spec A の閉点すなわち極大イデアルである。しかも $\bar{\mathfrak{m}} \in D(\bar{f})$ だから $\mathfrak{m} \in V(\mathfrak{a}) \cap D(f)$ であり、$\mathfrak{m}$ が所望の極大イデアルである。”

2 ヒルベルトの零点定理（ Hilbert's Nullstellensatz ）

定理 2.1 (**ヒルベルトの零点定理（ weak form ）**)**.**

K を代数閉体、x_i を不定元とする。

対応 $k^n \ni (a_1, ..., a_n) \mapsto (x_1 - a_1, ..., x_n - a_n) \in \text{m-Spec}\, k[x_1, ..., x_n]$ は全単射である。

証明.

$(a_1, ..., a_n) \in k^n$ とする。$X_i = x_i - a_i$ と置くと、

$\forall f \in k[x_1, ..., x_n]$ について、$f(x_1, ..., x_n) = f(X_1 + a_1, ..., X_n + a_n) = X_i$たちの 1 次以上の項$+ f(a_1, ..., a_n)$ より $f(x_1, ..., x_n) \equiv f(a_1, ..., a_n) \pmod{(x_1 - a_1, ..., x_n - a_n)}$ が分る。

従って $k[x_1, ..., x_n]/(x_1 - a_1, ..., x_n - a_n) \simeq k$ だから、$(x_1 - a_1, ..., x_n - a_n) \in \text{m-Spec}\, k[x_1, ..., x_n]$ である。またこの対応が単射であることも明らかである。なお、これについては k が代数閉体であることを要しない。

k が代数閉体である場合には全射であることを示す。$\mathfrak{m} \in \text{m-Spec}\, k[x_1, ..., x_n]$ として、

自然な写像 $k \hookrightarrow k[x_1, ..., x_n] \to k[x_1, ..., x_n]/\mathfrak{m}$ を考えると、体 $k[x_1, ..., x_n]/\mathfrak{m}$ は k 上有限生成代数だから、定理 1.2 によって k の代数拡大体である。ところが k は代数閉体なので、$k \simeq k[x_1, ..., x_n]/\mathfrak{m}$ である。この同型対応で x_i に対応する k の元 a_i をとすると、$(x_1 - a_1, ..., x_n - a_n) \subset \mathrm{Ker}(k[x_1, ..., x_n] \to k[x_1, ..., x_n]/\mathfrak{m}) = \mathfrak{m}$ となるが、$(x_1 - a_1, ..., x_n - a_n)$ は極大だから $(x_1 - a_1, ..., x_n - a_n) = \mathfrak{m}$

Q.E.D.

定理 2.2 (**ヒルベルトの零点定理（ strong form ）**)**.**

k を代数閉体、x_i を不定元、$\mathfrak{a}$ を $k[x_1, ..., x_n]$ のイデアルとすると $IZ(\mathfrak{a}) = \sqrt{\mathfrak{a}}$ が成り立つ。

証明.

$f \in \sqrt{\mathfrak{a}}$ ならば $\exists n$ で $f^n \in \mathfrak{a}$ であるから、f^n は $Z(\mathfrak{a})$ 上で零である。よって f も $Z(\mathfrak{a})$ 上で零だから $IZ(\mathfrak{a}) \supset \sqrt{\mathfrak{a}}$ である。これについては k が代数閉体であることを要しない。

k が代数閉体である場合に、逆の包含関係が成り立つことを示す。$\mathfrak{a} = (1)$ なら明白だから $\mathfrak{a} \neq (1)$ とする。定理 2.1 と定理 1.3 によって $f \in IZ(\mathfrak{a})$ のとき、$\forall(x_1 - a_1, ..., x_n - a_n) \supset \mathfrak{a}$ に対して $f \in (x_1 - a_1, ..., x_n - a_n)$ であることを示せばよい。

定理 2.1 の証明の初めの部分から、$\forall g \in k[x_1, ..., x_n], \forall(b_1, ..., b_n) \in k^n$ に対して、
$g(b_1, ..., b_n) = 0$ と $g \in (x_1 - b_1, ..., x_n - b_n)$ とは同値であることが分る。このことに注意せよ。
$(x_1 - a_1, ..., x_n - a_n) \supset \mathfrak{a}$ ならば $(a_1, ..., a_n) \in Z(\mathfrak{a})$ だから、$f(a_1, ..., a_n) = 0$
従って $f \in (x_1 - a_1, ..., x_n - a_n)$ である。

Q.E.D.

注意 2.3 (逆の包含関係を定理 1.2 から直接示す方法).
上記の証明では逆の包含関係を、定理 2.1 と定理 1.3 から証明したが、定理 1.2 から直接証明することもできる。$A = k[x_1, ..., x_n]$ とすれば定理 1.3 の証明と全く同じ議論によって、次の条件を満たす体 K と A のイデアル $\mathfrak{m}$ の存在が分る。

1. $k \hookrightarrow A/\mathfrak{m} \hookrightarrow K$ で K は k の代数拡大体
2. $\mathfrak{a} \subset \mathfrak{m}$ かつ $f \notin \mathfrak{m}$

さらに今回は k が代数閉体なので $k \simeq K$ であるから、$k \simeq A/\mathfrak{m}$ も分る。（なお、以上の議論に関して補題 1.4 は不要である。）

ここで $a_i \equiv x_i \pmod{\mathfrak{m}}$ となる $a_i \in k$（一意的に存在する）を取る。$\forall g \in k[x_1, ..., x_n]$ に対して $g \in \mathfrak{m}$ と $g(a_1, ..., a_n) = 0$ とが同値であることに注意せよ。$\mathfrak{a} \subset \mathfrak{m}$ から $(a_1, ..., a_n) \in Z(\mathfrak{a})$、また $f \notin \mathfrak{m}$ から $f(a_1, ..., a_n) \neq 0$ が分る。従って $f \notin IZ(\mathfrak{a})$ であり、逆の包含関係が成り立つことが分った。