

Zariski位相における閉集合の基底・既約性・およびHilbertの零点定理

本稿では、複素アフィン空間 \mathbb{C}^n 上の Zariski 位相 (Zariski topology) における閉集合の構造、既約閉集合 (irreducible closed set) と多項式環の素イデアル (prime ideal) の対応関係、そしてそれらの根底を支える代数幾何学の基本定理である Hilbert の零点定理 (Hilbert's Nullstellensatz) について包括的かつ自己完結的 (self-contained) に解説します。

1. Zariski 位相と閉集合系の基底

まずは、 \mathbb{C}^n 上の Zariski 位相の定義と、その閉集合を生成する「基底」について導入します。

定義 1.1 (Zariski 位相の閉集合)

\mathbb{C}^n の部分集合 V が Zariski 位相において閉集合（または代数的集合）であるとは、ある多項式の集合 $S \subset \mathbb{C}[x_1, \dots, x_n]$ が存在して、次のように表されることである。

$$V = V(S) = \{x \in \mathbb{C}^n \mid \forall f \in S, f(x) = 0\}$$

定義 1.2 (閉集合系の基底)

位相空間の閉集合の族 \mathcal{B} が閉集合系の基底 (base for closed sets) であるとは、任意の閉集合が \mathcal{B} の元の共通部分として表せることである。

命題 1.3 (閉集合系の基底)

集合族 $\mathcal{B} = \{\{x \in \mathbb{C}^n \mid f(x) = 0\} \mid f \in \mathbb{C}[x_1, \dots, x_n]\}$ は \mathbb{C}^n の Zariski 位相における閉集合系の基底をなす。

証明

任意の閉集合 V をとる。定義 1.1 より、ある多項式の部分集合 $S \subset \mathbb{C}[x_1, \dots, x_n]$ が存在して $V = V(S)$ と表される。各多項式 $f \in \mathbb{C}[x_1, \dots, x_n]$ が単独で定める零点集合を $V(f) = \{x \in \mathbb{C}^n \mid f(x) = 0\}$ とおく。このとき、集合の共通部分の定義から次が成り立つ。

$$V(S) = \{x \in \mathbb{C}^n \mid \forall f \in S, f(x) = 0\} = \bigcap_{f \in S} \{x \in \mathbb{C}^n \mid f(x) = 0\} = \bigcap_{f \in S} V(f)$$

各 $V(f)$ は定義より族 \mathcal{B} の元である。したがって、任意の閉集合 V は \mathcal{B} の元の共通部分として表されるため、 \mathcal{B} は閉集合系の基底をなす。(証明終)

開集合系の基底（開基）との双対性

位相空間論における通常の「開集合系の基底（開基、base for open sets）」は、閉集合系の基底の補集合を考えるこ

とで自然に得られます。 $V(f)$ の補集合を $D(f)$ と表し、これを**主開集合 (principal open set)** と呼びます。

$$D(f) = \mathbb{C}^n \setminus V(f) = \{x \in \mathbb{C}^n \mid f(x) \neq 0\}$$

de Morgan の法則により、任意の開集合 $U = \mathbb{C}^n \setminus V(S)$ は、次のように主開集合の和集合として書き換えることができます。

$$U = \mathbb{C}^n \setminus \bigcap_{f \in S} V(f) = \bigcup_{f \in S} (\mathbb{C}^n \setminus V(f)) = \bigcup_{f \in S} D(f)$$

これは、任意の開集合が主開集合の和集合で表せることを意味しており、族 $\{D(f) \mid f \in \mathbb{C}[x_1, \dots, x_n]\}$ が Zariski 位相の開基をなすことと完全に同値です。また、Zariski 位相の重要な性質として、任意の多項式 f, g に対して $V(f) \cup V(g) = V(fg)$ が成り立ちます。これは、基底の元の有限和が再び基底の元に収まることを意味しており、有限和の操作を挟むことなく、純粋に共通部分（または開集合側では和集合）をとるだけで全体の位相が記述できる強力な構造を示しています。

2. 既約閉集合と素イデアルの特徴付け

2つの真の閉部分集合の和として表せないという幾何学的な性質（既約性）が、代数学におけるイデアルの性質（素イデアル）とどのように結びつくかを解説します。

定義 2.1 (既約閉集合)

位相空間の空でない閉集合 V が既約 (irreducible) であるとは、2つの真の閉部分集合の和として表せないこと、すなわち $V = V_1 \cup V_2$ (V_1, V_2 は閉集合) ならば $V = V_1$ または $V = V_2$ が成り立つことである。

定義 2.2 (素イデアル)

可換環 R の固有イデアル $\mathfrak{p} \subsetneq R$ が素イデアル (prime ideal) であるとは、任意の $f, g \in R$ に対して $fg \in \mathfrak{p} \implies f \in \mathfrak{p}$ または $g \in \mathfrak{p}$ が成り立つことである。

定義 2.3 (代数的集合のイデアル)

\mathbb{C}^n の部分集合 V に対し、 V 上のすべての点で 0 になる多項式全体からなる集合を $I(V)$ と定義する。

$$I(V) = \{f \in \mathbb{C}[x_1, \dots, x_n] \mid \forall x \in V, f(x) = 0\}$$

これは多項式環 $\mathbb{C}[x_1, \dots, x_n]$ のイデアルとなる。

命題 2.4 (既約性と素イデアルの同値性)

\mathbb{C}^n の空でない閉集合 V が既約であるための必要十分条件は、対応するイデアル $I(V)$ が $\mathbb{C}[x_1, \dots, x_n]$ の素イデアルとなることである。

証明

(\implies) V を既約閉集合とする。 $V \neq \emptyset$ より $I(V) \neq \mathbb{C}[x_1, \dots, x_n]$ である。いま、 $f, g \in \mathbb{C}[x_1, \dots, x_n]$ が $fg \in I(V)$ を満たすと仮定する。このとき、任意の $x \in V$ に対して $f(x)g(x) = 0$ が成り立つため、各点 $x \in V$ は $f(x) = 0$ または $g(x) = 0$ を満たす。ゆえに、包含関係 $V \subset V(f) \cup V(g)$ を得る。両辺と V との共

通部分をとることで、

$$V = (V \cap V(f)) \cup (V \cap V(g))$$

と表される。 $V(f)$ および $V(g)$ は Zariski 位相の閉集合であるため、それぞれの V との交わりも V の閉部分集合である。 V の既約性から、 $V = V \cap V(f)$ または $V = V \cap V(g)$ が成り立つ。 $V = V \cap V(f)$ の場合、 $V \subset V(f)$ であり、これは任意の $x \in V$ に対して $f(x) = 0$ 、すなわち $f \in I(V)$ を意味する。同様に $V = V \cap V(g)$ の場合は $g \in I(V)$ となる。したがって、 $I(V)$ は素イデアルである。

(\Leftarrow) $I(V)$ を素イデアルとする。 V が既約であることを示すために、 $V = V_1 \cup V_2$ (ただし V_1, V_2 は \mathbb{C}^n の閉集合) と仮定する。このとき、イデアルの定義から $I(V) = I(V_1 \cup V_2) = I(V_1) \cap I(V_2)$ が成り立つ。したがって、 $I(V_1) \cap I(V_2) \subset I(V)$ である。ここで、 $I(V_1) \subset I(V)$ または $I(V_2) \subset I(V)$ が成り立つことを示す。もし $I(V_1) \not\subset I(V)$ かつ $I(V_2) \not\subset I(V)$ と仮定すると、 $f \in I(V_1) \setminus I(V)$ および $g \in I(V_2) \setminus I(V)$ が存在する。このとき、 $fg \in I(V_1) \cdot I(V_2) \subset I(V_1) \cap I(V_2) \subset I(V)$ となるが、 $I(V)$ は素イデアルであるため $f \in I(V)$ または $g \in I(V)$ となり矛盾を生じる。ゆえに、 $I(V_1) \subset I(V)$ または $I(V_2) \subset I(V)$ である。一般に閉集合 W に対し $V(I(W)) = W$ が成り立つ。なぜなら、 W は閉集合であるからある多項式集合 S を用いて $W = V(S)$ と書け、 $S \subset I(V(S)) = I(W)$ から $V(I(W)) \subset V(S) = W$ となり、逆の包含関係 $W \subset V(I(W))$ は常に成り立つからである。これより、 $I(V_1) \subset I(V)$ のときは $V = V(I(V)) \subset V(I(V_1)) = V_1$ となり、仮定の $V_1 \subset V$ と合わせて $V = V_1$ を得る。同様に $I(V_2) \subset I(V)$ のときは $V = V_2$ となる。したがって、 V は既約である。(証明終)

例 2.5 (既約な閉集合の例)

\mathbb{C}^2 における放物線 $V = V(y - x^2)$ を考える。多項式 $y - x^2 \in \mathbb{C}[x, y]$ は既約多項式である。多項式環 $\mathbb{C}[x, y]$ は一意分解整域であるため、既約元が生成する主イデアル $(y - x^2)$ は素イデアルとなる。このとき対応する図形のイデアルも $I(V) = (y - x^2)$ と一致するため、命題 2.4 より放物線 V は既約閉集合である。

例 2.6 (可約な閉集合の例)

\mathbb{C}^2 における直線同士の交わり $V = V(xy)$ を考える。これは x 軸 $V(y)$ と y 軸 $V(x)$ の和集合として $V = V(x) \cup V(y)$ と表せる。 $V(x)$ も $V(y)$ も V の真の閉部分集合であるため、 V は既約ではなく可約 (reducible) である。代数的に見ても、対応するイデアル $I(V) = (xy)$ は素イデアルではない。実際、 $x \notin (xy)$ かつ $y \notin (xy)$ であるにもかかわらず、その積 $xy \in (xy)$ となるからである。

代数幾何学では、このような \mathbb{C}^n の既約閉集合のことを、特に**アフィン代数多様体 (affine algebraic variety)** と呼び、図形を構成する最も基本的なビルディングブロックとして扱います。

3. 根基イデアルの定義と性質

代数と幾何の対応関係をより精密にするために不可欠な、根基イデアルの概念について整理します。

定義 3.1 (根基イデアル)

可換環 R のイデアル I が根基イデアル (radical ideal) であるとは、任意の元 $f \in R$ と任意の正の整数 $n \geq 1$ に対して、次の条件を満たすことである。

$$f^n \in I \implies f \in I$$

定義 3.2 (イデアルの根基)

可換環 R の任意のイデアル I に対し、そのイデアルの根基 (radical of an ideal) \sqrt{I} を次のように定義する。

$$\sqrt{I} = \{f \in R \mid \exists n \geq 1, f^n \in I\}$$

このとき、 \sqrt{I} もまた R のイデアルとなる。この記法を用いると、 I が根基イデアルであることは $I = \sqrt{I}$ と等価である。

例 3.3 (根基イデアルの具体例)

1変数多項式環 $\mathbb{C}[x]$ においてイデアル $I = (x^2)$ を考える。 $f(x) = x$ とおくと、 $f^2 = x^2 \in I$ であるが、 $f = x \notin I$ である。したがって、 (x^2) は根基イデアルではない。このイデアルの根基を計算すると $\sqrt{(x^2)} = (x)$ となる。一方、イデアル $J = (x)$ については、 $f^n \in (x)$ ならば多項式 $f(x)$ 自身が必ず x を因子に持つため $f \in (x)$ が成り立ち、 $\sqrt{(x)} = (x)$ となって根基イデアルの定義を満たす。また、一般にすべての素イデアルは根基イデアルである。

幾何学的な意味

幾何学の点集合 (零点集合) は、多項式の「累乗 (重複度)」の情報を識別できません。例えば、方程式 $x = 0$ が定める図形と $x^2 = 0$ が定める図形は、集合として見ればどちらも全く同じ原点 $\{0\} \subset \mathbb{C}$ です。しかし代数的には、イデアル (x) と (x^2) は明確に区別されます。この幾何と代数の「ズレ」を解消するため、「同じ図形を与えるイデアル群の中から、累乗の元をすべて吸収した最大のもの (=根基イデアル) を代表として選ぶ」というアプローチが自然に要請されることとなります。

4. Hilbertの零点定理

代数 (多項式環のイデアル) と幾何 (Zariski 位相の閉集合) の間の完全な翻訳辞書を与える決定的な定理が、David Hilbert によって証明された **Hilbertの零点定理 (Hilbert's Nullstellensatz)** です。この定理は、基底となる体 k が代数閉体 (algebraically closed field) であるときに成立します (複素数体 \mathbb{C} は代数閉体です)。

4.1 弱零点定理 (Weak Nullstellensatz)

まず、連立多項式方程式の解の存在を保証する基礎的な形です。

定理 4.1 (弱零点定理)

k を代数閉体とする。多項式環 $k[x_1, \dots, x_n]$ のイデアル I が、環全体と一致しない ($I \neq k[x_1, \dots, x_n]$) ならば、その共通零点集合は空集合ではない。すなわち、

$$V(I) \neq \emptyset$$

これは1変数多項式における「代数学の基本定理」を、多変数および複数の方程式系へと一般化したものです。代数閉体上の多項式環において、代数的な矛盾 (例えば $1 = 0$ の導出など) を起こしていないイデアルであれば、それを満たす幾何学的な点 (共通解) が必ず存在することを約束します。

4.2 強零点定理 (Strong Nullstellensatz)

弱形式を基礎として、イデアルと図形の関係性を完全に決定づけたのが以下の強形式です。

定理 4.2 (強零点定理)

k を代数閉体とする。 $k[x_1, \dots, x_n]$ の任意のイデアル I に対して、次が成り立つ。

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

強零点定理は、「あるイデアル I から生成された図形 $V(I)$ を基に、再度多項式イデアル $I(V(I))$ を逆算すると、それはもとのイデアルの根基 \sqrt{I} に完全に一致する」という強力な事実を述べています。これにより、最初から I として**根基イデアル**を選んでおけば、 $I(V(I)) = I$ が成り立ち、代数的対象と幾何学的な対象が1対1で対応することになります。

4.3 代数と幾何の翻訳辞書

Hilbert の零点定理がもたらした最大の功績は、アフィン空間 k^n における幾何学性質と、多項式環 $k[x_1, \dots, x_n]$ における代数的性質を、包含関係を反転させた形で1対1に対応（ガロア接続）させた点にあります。その対応関係は以下の表のように美しく整理されます。

幾何学的対象 (k^n の Zariski 位相)	代数的対象 (多項式環 $k[x_1, \dots, x_n]$)
代数的集合 (閉集合)	根基イデアル
アフィン代数多様体 (既約閉集合)	素イデアル
点 (a_1, \dots, a_n)	極大イデアル $(x_1 - a_1, \dots, x_n - a_n)$
空集合 \emptyset	環全体 $k[x_1, \dots, x_n]$
包含関係 $V_1 \subset V_2$	逆向きの包含関係 $I(V_1) \supset I(V_2)$
2つの図形の交わり $V_1 \cap V_2$	イデアルの和の根基 $\sqrt{I(V_1) + I(V_2)}$

5. \mathbb{C} 上における Hilbert の零点定理の完全なる証明

ここからは、ベースの体を複素数体 \mathbb{C} に限定し、定理の完全な証明を与えます。 \mathbb{C} が代数閉体であることに加え、**非可算体 (uncountable field)** であるという強力な解析的・集合論的性質を利用することで、高度な可換環論を必要としない極めて自己完結的な証明を構築できます。まず、心臓部となる Zariski の補題の複素数版を示します。

補題 5.1 (Zariski の補題の \mathbb{C} 版)

L を \mathbb{C} 上有限生成な代数 (finitely generated algebra) であり、かつ L が体であるとする。このとき、 $L = \mathbb{C}$ である。

証明

L は \mathbb{C} 上有限生成な環であるから、ある有限個の元 $v_1, \dots, v_r \in L$ が存在して、 $L = \mathbb{C}[v_1, \dots, v_r]$ と表される。すべての多項式の単項式全体 $v_1^{e_1} \dots v_r^{e_r}$ ($e_i \geq 0$) は可算集合であり、これらが L を \mathbb{C} 上のベクトル空間として生成する。したがって、 L は \mathbb{C} 上のベクトル空間として高々可算な次元を持つ。

いま、 $L \neq \mathbb{C}$ と仮定する。このとき、 \mathbb{C} に属さない元 $t \in L \setminus \mathbb{C}$ が存在する。各複素数 $\alpha \in \mathbb{C}$ に対して、 $t - \alpha \in L$ を考える。 $t \notin \mathbb{C}$ より $t - \alpha \neq 0$ である。 L は体であるから、各 $\alpha \in \mathbb{C}$ に対して逆元 $(t - \alpha)^{-1} \in L$ が存在する。ここで、次の元からなる集合 S を定義する。

$$S = \{(t - \alpha)^{-1} \in L \mid \alpha \in \mathbb{C}\}$$

\mathbb{C} は非可算集合であるため、 S もまた非可算集合である（実際、 $\alpha \neq \beta$ ならば $(t - \alpha)^{-1} = (t - \beta)^{-1} \implies t - \alpha = t - \beta \implies \alpha = \beta$ となり矛盾するため、すべての元は相異なる）。

次に、この集合 S が \mathbb{C} 上線形独立 (linearly independent) であることを示す。有限個の相異なる $\alpha_1, \dots, \alpha_m \in \mathbb{C}$ と、 $c_1, \dots, c_m \in \mathbb{C}$ に対し、次の線形結合が 0 になると仮定する。

$$\sum_{i=1}^m \frac{c_i}{t - \alpha_i} = 0$$

この両辺に共通の分母 $\prod_{j=1}^m (t - \alpha_j)$ を掛けることで、次の等式を得る。

$$\sum_{i=1}^m c_i \prod_{j \neq i} (t - \alpha_j) = 0$$

ここで、複素数係数多項式 $P(x) = \sum_{i=1}^m c_i \prod_{j \neq i} (x - \alpha_j) \in \mathbb{C}[x]$ を導入する。各 $k = 1, \dots, m$ について、 $P(x)$ に $x = \alpha_k$ を代入すると、 $j \neq k$ を含む項はすべて消滅するため、次が残る。

$$P(\alpha_k) = c_k \prod_{j \neq k} (\alpha_k - \alpha_j)$$

α_i たちはすべて相異なるため、積の部分は 0 にならない。したがって、もしある k について $c_k \neq 0$ であるならば、 $P(\alpha_k) \neq 0$ となり、 $P(x)$ は恒等的に 0 ではない多項式 (0 多項式ではない) である。しかし、仮定より L において $P(t) = 0$ が成り立っている。 $P(x)$ が 0 多項式でないことは、 t が \mathbb{C} 上代数的 (algebraic) であることを意味する。 \mathbb{C} は代数閉体であるから、 \mathbb{C} 上代数的な元は \mathbb{C} 自身に属さねばならないが、これは $t \notin \mathbb{C}$ という選択に矛盾する。ゆえに、すべての c_i は 0 でなければならず、集合 S は \mathbb{C} 上線形独立である。

これは、 L が \mathbb{C} 上に非可算個の線形独立な元を持つことを意味し、 L の複素ベクトル空間としての次元が非可算次元であることを示す。しかし、これは冒頭で述べた「 L は高々可算次元である」という事実と矛盾する。したがって、最初の仮定 $L \neq \mathbb{C}$ は誤りであり、 $L = \mathbb{C}$ でなければならない。(証明終)

補題 5.1 を用いて、まず弱零点定理の証明を行います。なお、多項式環が固有イデアルから極大イデアルを構成できる (極大イデアルの存在性) という点については、環が可算生成であることから、Zorn の補題 (選択公理) に依存せずとも、多項式の全単項式を順に走査する可算ステップの議論によって容易に示されます。

定理 4.1 (弱零点定理) の証明

$\mathbb{C}[x_1, \dots, x_n]$ の任意の極大イデアルを \mathfrak{m} とおく。商環 $L = \mathbb{C}[x_1, \dots, x_n]/\mathfrak{m}$ は、 \mathfrak{m} の極大性より体である。また、各変数 x_i の商環における像を \bar{x}_i とおけば、 $L = \mathbb{C}[\bar{x}_1, \dots, \bar{x}_n]$ となり、 L は \mathbb{C} 上有限生成な環 (代

数) である。したがって、補題 5.1 より $L = \mathbb{C}$ が成り立つ。

これにより、自然な全射環準同型 (ring homomorphism) $\pi : \mathbb{C}[x_1, \dots, x_n] \rightarrow \mathbb{C}[x_1, \dots, x_n]/\mathfrak{m} = \mathbb{C}$ が得られる。各変数に対して、その像を $a_i = \pi(x_i) \in \mathbb{C}$ ($i = 1, \dots, n$) とおく。任意の多項式 $f \in \mathbb{C}[x_1, \dots, x_n]$ に対し、 π が環準同型であることから次が従う。

$$\pi(f(x_1, \dots, x_n)) = f(\pi(x_1), \dots, \pi(x_n)) = f(a_1, \dots, a_n)$$

多項式 f が \mathfrak{m} に属することは $\pi(f) = 0$ と同値であるため、 $f \in \mathfrak{m} \iff f(a_1, \dots, a_n) = 0$ を得る。特に、一次式 $x_i - a_i$ について、 $\pi(x_i - a_i) = a_i - a_i = 0$ であるから、 $x_i - a_i \in \mathfrak{m}$ である。ゆえに、これらの一次式が生成するイデアルを考えると、包含関係 $(x_1 - a_1, \dots, x_n - a_n) \subset \mathfrak{m}$ が成り立つ。

$(x_1 - a_1, \dots, x_n - a_n)$ もまた、その商環が \mathbb{C} となることから極大イデアルであるため、極大性から両者は完全に一致する。

$$\mathfrak{m} = (x_1 - a_1, \dots, x_n - a_n)$$

任意の固有イデアル $I \subsetneq \mathbb{C}[x_1, \dots, x_n]$ は、ある極大イデアル \mathfrak{m} に包まれる。その極大イデアルは上述の議論からある点 $(a_1, \dots, a_n) \in \mathbb{C}^n$ を用いて $(x_1 - a_1, \dots, x_n - a_n)$ と書ける。このとき、任意の $f \in I \subset \mathfrak{m}$ に対して $f(a_1, \dots, a_n) = 0$ となる。これは点 (a_1, \dots, a_n) が共通零点集合 $V(I)$ に属することを意味しており、ゆえに $V(I) \neq \emptyset$ である。(証明終)

最後に、弱零点定理から強零点定理を鮮やかに導く **Rabinowitsch のトリック (Rabinowitsch's trick)** を用いた証明を展開します。変数を1つ追加することで、根基 (累乗) の計算を弱形式の「解の存在性」へと落とし込む手法です。

定理 4.2 (強零点定理) の証明

I を $\mathbb{C}[x_1, \dots, x_n]$ のイデアルとし、 $g \in I(V(I))$ とする。定義より、 $V(I)$ のすべての点で g は 0 になる。 $g = 0$ のときは明らかに $g \in \sqrt{I}$ となるため、以下 $g \neq 0$ と仮定する。

新しく変数 y を1つ導入し、 $n + 1$ 変数の多項式環 $\mathbb{C}[x_1, \dots, x_n, y]$ を考える。この拡大された環において、次のイデアル J を構成する。

$$J = I \cdot \mathbb{C}[x_1, \dots, x_n, y] + (1 - yg)$$

このイデアル J が定める \mathbb{C}^{n+1} 内の共通零点集合 $V(J)$ について考察する。もし、ある点 $(x_1, \dots, x_n, y) \in \mathbb{C}^{n+1}$ が $V(J)$ に属すると仮定すると、その点は J のすべての元を 0 にする。まず $I \subset J$ より、すべての $f \in I$ に対し $f(x_1, \dots, x_n) = 0$ であるから、前半の n 座標を切り出した点 (x_1, \dots, x_n) は $V(I)$ に属さねばならない。ここで、 $g \in I(V(I))$ という仮定を適用すると、この点で $g(x_1, \dots, x_n) = 0$ となる。

一方で、その点はイデアル J のもう1つの生成元である $1 - yg$ も 0 にしなければならない。しかし、ここに先ほどの $g(x_1, \dots, x_n) = 0$ を代入すると、

$$1 - y \cdot 0 = 1 = 0$$

となり、代数的な矛盾が生じる。したがって、このような点 (x_1, \dots, x_n, y) は \mathbb{C}^{n+1} 上に存在し得ず、共通零点集合は空集合となる。

$$V(J) = \emptyset$$

ここで、既に証明された弱零点定理 (定理 4.1) の対偶を適用する。共通零点集合が空集合 $V(J) = \emptyset$ であるな

らば、イデアル J は環全体と一致していなければならない。

$$J = \mathbb{C}[x_1, \dots, x_n, y]$$

特に、乗法の単位元 1 が J に属することになる ($1 \in J$)。イデアル J の定義に立ち返ると、ある有限個の多項式 $f_i \in I$ と、 $n+1$ 変数多項式環の元 $h_i(x_1, \dots, x_n, y), q(x_1, \dots, x_n, y)$ が存在して、次の代数的な恒等式が成立する。

$$1 = \sum_{i=1}^m f_i(x_1, \dots, x_n) h_i(x_1, \dots, x_n, y) + q(x_1, \dots, x_n, y)(1 - yg(x_1, \dots, x_n))$$

この恒等式に対し、有理関数体 (rational function field) $\mathbb{C}(x_1, \dots, x_n)$ において、新変数 y に $\frac{1}{g(x_1, \dots, x_n)}$ を代入する ($g \neq 0$ であるため、この有理式の代入は正当化される)。すると、右辺の最右項の因子は $1 - \frac{1}{g}g = 0$ となり、多項式 q を巻き込んで完全に消滅する。その結果、次の有理式の関係式が残る。

$$1 = \sum_{i=1}^m f_i(x_1, \dots, x_n) h_i \left(x_1, \dots, x_n, \frac{1}{g(x_1, \dots, x_n)} \right)$$

各 $h_i(x, \frac{1}{g})$ は、各項の分母に g のいくつかの累乗を持つ有理関数である。これら有限個の多項式 h_i の中で、変数 y (すなわち $\frac{1}{g}$) に関する最高の次数を N と定める。このとき、等式の両辺に $g(x_1, \dots, x_n)^N$ を掛け合わせることで、すべての分母を払うことができる。

$$g(x_1, \dots, x_n)^N = \sum_{i=1}^m f_i(x_1, \dots, x_n) H_i(x_1, \dots, x_n)$$

ここで、 $H_i(x_1, \dots, x_n) = g^N h_i(x, \frac{1}{g})$ は分母が完全に相殺されたため、純粋な多項式環 $\mathbb{C}[x_1, \dots, x_n]$ の元となる。各 f_i はもともとイデアル I の元であったため、イデアルの定義 (多項式倍の和を再び含むこと) から、この右辺全体の多項式は I に属する。したがって、

$$g^N \in I$$

が成立し、根基イデアルの定義 (定義 3.2) より $g \in \sqrt{I}$ が示された。逆の包含関係 $\sqrt{I} \subset I(V(I))$ は、 $g \in \sqrt{I} \implies g^n \in I \implies \forall x \in V(I), g(x)^n = 0 \implies g(x) = 0$ より自明に成り立つ。ゆえに、 $I(V(I)) = \sqrt{I}$ である。(証明終)

参考文献 (References)

- [1] D. Hilbert, "Ueber die vollen Invariantensysteme," [Mathematische Annalen](#), vol. 42, no. 3, pp. 313–373, 1893.
- [2] J. L. Rabinowitsch, "Zum Hilbertschen Nullstellensatz," [Mathematische Annalen](#), vol. 102, pp. 520, 1930.
- [3] M. F. Atiyah and I. G. Macdonald, [Introduction to Commutative Algebra](#), Addison-Wesley, 1969.
- [4] R. Hartshorne, [Algebraic Geometry](#), Graduate Texts in Mathematics, vol. 52, Springer-Verlag, 1977.