この記事では文字 $\mathbf{x}$ を一貫して不定元を表すために使う．$\mathbf{x} = (x_1, \ldots, x_d)$ とする．

1 The Statement

定理 1.1 (Hilbert's Nullstellensatz (weak form))**.** k を代数閉体とする．この時，以下で定まる対応 μ は全単射である．

$$\begin{array}{cccc} \mu: & k^d & \to & \mathrm{Max}(k[\mathbf{x}]) \\ & (a_1, \ldots, a_d) & \mapsto & (x_1 - a_1, \ldots, x_d - a_d) \end{array}$$

定理 1.2 (Hilbert's Nullstellensatz (strong form))**.** k を代数閉体とする．任意のイデアル $\mathfrak{a} \subsetneq k[\mathbf{x}]$ に対して

$$\mathcal{I}\mathcal{Z}(\mathfrak{a}) = \sqrt{\mathfrak{a}}$$

が成立する．

1.1 Another Forms of The Two Statements

以上の二つの定理が「弱形」「強形」と並べられる理由は今ひとつ理解りにくい．Terence Tao は自身のブログ "What's New"に Hilbert's Nullstellensatz を扱った記事を掲載している [2]．それによると，以上の二つのステートメントはそれぞれ次のように言い換えられる．

定理 1.3 (Hilbert's Nullstellensatz (weak form) by Terence Tao)**.** k を代数閉体とし，多項式 $P_1, \ldots, P_m \in k[\mathbf{x}]$ をとる．この時，以下のちょうど一方が成立する．

1. 方程式系 $P_1(\mathbf{x}) = \ldots = P_m(\mathbf{x}) = 0$ が解 $\mathbf{x} = (a_1, \ldots, a_d) \in k^d$ を持つ．
2. $P_1 Q_1 + \ldots + P_m Q_m = 1$ を満たす多項式 $Q_1, \ldots, Q_m \in k[x]$ が存在する．

定理 1.4 (Hilbert's Nullstellensatz (strong form) by Terence Tao)**.** k を代数閉体とし，多項式 $P_1, \ldots, P_m, R \in k[\mathbf{x}]$ をとる．この時，以下のちょうど一方が成立する．

1. 方程式系 $P_1(\mathbf{x}) = \ldots = P_m(\mathbf{x}) = 0, R(\mathbf{x}) \neq 0$ が解 $\mathbf{x} = (a_1, \ldots, a_d) \in k^d$ を持つ．
2. $P_1 Q_1 + \ldots + P_m Q_m = R^r$ を満たす多項式 $Q_1, \ldots, Q_m \in k[\mathbf{x}]$ と非負整数 r が存在する．

このように weak form は strong form で $R = 1$ とした場合であることは明白である．したがって strong form $\Longrightarrow$ weak form が分かる．

2 Prepare for The Proofs

補題 2.1 (Zariski's Lemma)**.** 体 k 上の有限生成代数 K が体ならば，K は k の有限次代数拡大体である．

■Noether normalization theorem を使うもの．

(証明). Noether normalization theorem により，有限生成代数 K が $R := k[y_1, \ldots, y_m]$ の整拡大となり，しかも k 上代数独立であるような元 $y_1, \ldots, y_m$ が存在する．

$m > 0$ とする．$y_1 \in K$ (::field) なので $y_1^{-1} \in K$．したがって y_1^{-1} は R 上整であるから，以下が成立するような $f \in R$ と非負整数 n が存在する．

$$(y_1^{-1})^n + f(y_1, \dots, y_m)(y_1^{-1})^{n-1} = 0$$

この両辺に y_1^n を掛けると，

$$1 + f(y_1, \dots, y_m)y_1 = 0$$

となり，これは $y_1, \dots, y_m$ が k 上代数独立[†1] であることに矛盾する．よって $m = 0$.

以上より，K は k の整拡大，すなわち代数拡大となる．再び K が k 上有限生成代数な体であることから，K は k の有限次代数拡大体. ∎

■整従属性を使うもの． ([1], Ex5.18 と [3] を参照)

(証明). k 代数としての K の生成元を $x_1, \dots, x_n$ とする．すなわち，

$$K = k[x_1, \dots, x_n].$$

$n = 1$ ならば定理の成立は自明なので $n > 1$ としよう．示したいことは $x_1, \dots, x_n$ のすべてが k 上代数的であること．なので帰納的に考えて，$x_2, \dots, x_n$ が $k(x_1)$ [†2]上代数的ならば $x_1, \dots, x_n$ が k 上代数的であることを示せば良い[†3]．そこで，x_1 が k 上代数的でなく同時に $x_2, \dots, x_n$ が $k(x_1)$ 上代数的であると仮定し，背理法を用いる．

$x_2, \dots, x_n$ が $k[x_1]_f (= k[x_1][1/f])$ 上代数的であるような $f \in k[x_1]$ が存在する．実際，x_i が $k(x_1)$ 上代数的であることから，次の式を満たす $f_j^{(i)}, g_j^{(i)} \in k[x_1]$ が存在する．

$$x_i^{d_i} + \left(\frac{g_{d_i-1}^{(i)}}{f_{d_i-1}^{(i)}}\right) x_2^{d_i-1} + \cdots + \left(\frac{g_0^{(i)}}{f_0^{(i)}}\right) = 0 \text{ where } d_i > 0, f_j^{(i)}, g_j^{(i)} \in k[x_1], g_j^i \neq 0.$$

$\frac{g_{d_i-1}^{(i)}}{f_{d_i-1}^{(i)}}$ から $\frac{g_0^{(i)}}{f_0^{(i)}}$ までを通分すると，各 x_i は $k[x_1]\left[1/\prod_{j=0}^{d_i} f_j^{(i)}\right]$ 上整であることが分かる．したがって

$$f = \prod_{i=2}^{n} \prod_{j} f_j^{(i)} \in k[x_1]$$

とおくと，$x_2, \dots, x_n$ は $k[x_1]\,[1/f] = k[x_1]_f$ 上代数的であると言える．

$K = k[x_1][x_2, \dots, x_n]$ であり，$x_2, \dots, x_n$ は $k[x_1]_f$ 上整だから，K は $k[x_1]_f$ 上整．この整従属関係と K が体であることから $k[x_1]_f$ も体 ([1], Prop5.7)．$k[x_1] \subseteq k[x_1]_f \subseteq k(x_1)$ かつ $k(x_1)$ が $k[x_1]$ を含む最小の体（商体）であることから $k(x_1) = k[x_1]_f$．しかし実際は $k[x_1]_f \neq k(x_1)$ となる[†4]．よって矛盾が生じた． ∎

[†1] 「$y_1, \dots, y_m$ が k 上代数独立」の定義: $f(y_1, \dots, y_m) = 0$ となる 0 でない多項式 $f \in k[x_1, \dots, x_m]$ が存在しない.

[†2] $k(x_1)$ は k と x_1 を含む明らかな体.

[†3] 言い換えれば $K = k(x_1, \dots, x_{n-2})(x_{n-1})[x_n] \implies K = k(x_1, \dots, x_{n-3})(x_{n-2})[x_{n-1}, x_n] \implies \cdots \implies K = k(x_1)[x_2, \dots, x_n]$.

[†4] 実際，仮定から x_1 は k 上超越的だから，f は $k[x_1]$ の有限個の既約多項式の積に分解され，$k[x_1]$ は無数の既約多項式を持つ．なので f と互いに素な既約多項式 $g \in k[x_1]$ が存在する．$1/g = h/f^n$ となる $n > 0, h \in k[x_1]$ が存在すれば，$gh = f^n = f \cdot f^{n-1} \in (g)$．$g$ は素元だから $f \in (g)$ となり，f, g が互いに素であることに反する．よって $1/g \notin k[x_1]_f$.

3 Proof of The Weak Form

3.1 From Zariski Lemma.

■$(x_1 - a_1, \ldots, x_d - a_d) \in \mathrm{Max}(k[\mathbf{x}])$. 各 x_i を $x_i \mapsto a_i$ と写す写像を考える．明らかにこれは全射で，$\ker = (x_1 - a_1, \ldots, x_d - a_d)$．準同型定理から $k[\mathbf{x}]/(x_1 - a_1, \ldots, x_d - a_d) \cong k$ が得られる．剰余環が体になったので，$(x_1 - a_1, \ldots, x_d - a_d)$ は $\mathrm{Max}(k[\mathbf{x}])$ の元.

■μ :: injective. 自明である．

■μ :: surjective. $\mathfrak{m} \in \mathrm{Max}(k[\mathbf{x}])$ を任意に取る．この時 $L = k[\mathbf{x}]/\mathfrak{m}$ は体．しかも $\tilde{a}_i = x_i + \mathfrak{m}$ とおけば $L = k[\{\tilde{a}_i\}_{i=1}^d]$ と書けるから，L は有限生成 k-代数．Zariski's Lemma より，L/k は有限代数拡大である．k は代数的閉体であったから，$L \cong k$ となり，よって各 $\tilde{a}_i$ は k の元 a_i に対応する．こうして点 $\mathbf{a} = (a_1, \ldots, a_d)$ が得られた．再び $x_i \mapsto a_i$ という写像 (像は $k[\{a_i\}_{i=1}^d] = k$) に準同型定理を用いれば,

$$k[\mathbf{x}]/\mu(\mathbf{a}) \cong k[\{a_i\}_{i=1}^d] \cong k[\{\tilde{a}_i\}_{i=1}^d] = k[\mathbf{x}]/\mathfrak{m}$$

という同型が構成できる．したがって $\mathfrak{m} = \mu(\mathbf{a})$.

4 Proof of The Strong Form

4.1 From Zariski Lemma.

$\sqrt{\mathfrak{a}} \subseteq \mathcal{I}\mathcal{Z}(\mathfrak{a})$ は明らか．逆に $f \notin \sqrt{\mathfrak{a}}$ として $f \notin \mathcal{I}\mathcal{Z}(\mathfrak{a})$ を示す．

■素イデアル $\mathfrak{p}$ の存在. $\sqrt{\mathfrak{a}}$ は $\mathfrak{a}$ を含む素イデアル全体の共通部分であるから，この時 $\mathfrak{a} \subseteq \mathfrak{p}, f \notin \mathfrak{p}$ なる素イデアル $\mathfrak{p}$ が存在する．

■体 L の構成. $\bar{f} = f + \mathfrak{p} (\neq 0)$ とし，$C = (k[\mathbf{x}]/\mathfrak{p})_f = (k[\mathbf{x}]/\mathfrak{p})[1/\bar{f}]$ とする．さらに $\mathfrak{m}$ を C の極大イデアルとおく．すると体 $L = C/\mathfrak{m} = (k[\mathbf{x}]/\mathfrak{p})_f/\mathfrak{m}$ は $\tilde{a}_i = \frac{x_i + \mathfrak{p}}{1} + \mathfrak{m}$ で生成される有限生成 k-代数.

■$\mathbf{a} \in \mathcal{Z}(\mathfrak{a})$ かつ $f(\mathbf{a}) \neq 0$ なる点 $\mathbf{a}$ を得る. Zariski's Lemma より，L/k は有限代数拡大である．k は代数的閉体であったから，$L \cong k$ となり，よって各 $\tilde{a}_i$ は k の元 a_i に対応する．こうして点 $\mathbf{a} = (a_1, \ldots, a_d)$ が得られた．ここで以下の準同型を考える．

$$\phi : k[\mathbf{x}] \to k[\mathbf{x}]/\mathfrak{p} \to (k[\mathbf{x}]/\mathfrak{p})_f = C \to C/\mathfrak{m} \cong k; \quad x_i \mapsto x_i + \mathfrak{p} \mapsto \frac{x_i + \mathfrak{p}}{1} \mapsto \frac{x_i + \mathfrak{p}}{1} + \mathfrak{m} = \tilde{a}_i \mapsto a_i.$$

これは代入写像．繋いでいる写像はすべて準同型なので，$g \in \mathfrak{p}$ は C の零元 $\frac{0+\mathfrak{p}}{1}$ へ写り，最終的に零元 0 へ写る．同様に，f は C の単元 $\frac{f+\mathfrak{p}}{1}$ へ写り，最終的に単元へ写る．つまり $g \in \mathfrak{p}$ について $\phi(g) = g(\mathbf{a}) = 0$ で，$\phi(f) = f(\mathbf{a})$ は単元．よって $\mathbf{a} \in \mathcal{Z}(\mathfrak{p}) \subset \mathcal{Z}(\mathfrak{a})$ かつ $f(\mathbf{a}) \neq 0$.

参考文献

[1] M.F.Atiyah, I.G.MacDonald ”Introduction to Commutative Algebra”

[2] Terence Tao (2007/11/27) "Hilbert' s nullstellensatz" `https://terrytao.wordpress.com/2007/11/26/hilberts-nullstellensatz/`

[3] Alborz Azarang "A one-line undergraduate proof of Zariski's lemma and Hilbert's nullstellensatz" `http://arxiv.org/abs/1506.08376`