グレ explorer . ブナ基底と代数多様体入門 (Ideals, Varieties, and Algorithms)

ashiato45 のメモ，著者は D.Cox, J.Little, D.O'Shea

2015 年 6 月 22 日

1　幾何，代数，アルゴリズム

2　グレブナ基底

3　消去理論

4　代数と幾何の対応

4.1　ヒルベルトの零点定理

問題 3:

(1)

$$
\begin{aligned}
f(x_1, x_2, \dots, x_n) &= f(\widetilde{x}_1, \widetilde{x}_2 + a_2\widetilde{x}_1, \dots, \widetilde{x}_n + a_n\widetilde{x}_1) && (1)\\
&= (\sum_{d=0}^{N} h_d)(\widetilde{x}_1, \widetilde{x}_2 + a_2\widetilde{x}_1, \dots, \widetilde{x}_n + a_n\widetilde{x}_1) && (2)\\
&= h_N(\widetilde{x}_1, \widetilde{x}_2 + a_2\widetilde{x}_1, \dots, \widetilde{x}_n + a_n\widetilde{x}_1) + (\text{ゴミ}) && (3)\\
&= (\sum_{|\alpha|=N} c_\alpha x^\alpha)(\widetilde{x}_1, \widetilde{x}_2 + a_2\widetilde{x}_1, \dots, \widetilde{x}_n + a_n\widetilde{x}_1) + (\text{ゴミ}) && (4)\\
&= \sum_{|\alpha|=N} c_\alpha \widetilde{x}_1^{\alpha_1}(\widetilde{x}_2 + a_2\widetilde{x}_1)^{\alpha_2} \dots (\widetilde{x}_n + a_n\widetilde{x}_1)^{\alpha_n} + (\text{ゴミ}) && (5)\\
&= \sum_{|\alpha|=N} c_\alpha \widetilde{x}_1^{\alpha_1}(a_2\widetilde{x}_1)^{\alpha_2} \dots (a_n\widetilde{x}_1)^{\alpha_n} + (\text{ゴミ}) && (6)\\
&= \widetilde{x}_1^N \sum_{|\alpha|=N} c_\alpha (1 \cdot a_2^{\alpha_2} \cdot \dots \cdot a_n^{\alpha_n}) + (\text{ゴミ}) && (7)\\
&= \widetilde{x}_1^N \sum_{|\alpha|=N} c_\alpha (1, a_2, \dots, a_n)^\alpha + (\text{ゴミ}) && (8)\\
&= \widetilde{x}_1^N h_N(1, a_2, \dots, a_n) + (\text{ゴミ}). && (9)
\end{aligned}
$$

問題 4: 代数的閉体 K を考える。これが仮に有限体であり、$a_1, \dots, a_n$ が K のすべての元であるとする。このとき、

$$(x - a_1) \dots (x - a_n) = 1 \qquad (10)$$

という方程式を考える。左辺は $a_\bullet$ のどれを入れても 0 になるので、$a_\bullet$ はどれも根にならない。しかし、K は代数的閉体なのでこの根は K に属さなければならないが、先の考察よりこれは $a_1, \dots, a_n$ のどれでもない。

弱系の零点定理:$I \subset k[x_1, \dots, x_n]$ は $\mathbf{V}(I) = \emptyset$ とする。このとき、I は全体になってしまう。証明する。まず 1 次元で考える。PID なので $I = \langle f \rangle$ なる f がある。$\deg f \geq 1$ のときには、代数的閉体で考えてるので解が出てしまって、

$\mathbf{V}(I)$ は空でなくなるので矛盾。よって、$\deg f = 0$ となり、f は定数になる。よって、$1 \in I$ である。次に n 次元で考える。$I = \langle f_1, \dots, f_s \rangle$ とする。変数変換

$$x_1 \mapsto \widetilde{x}_1, \quad x_i \mapsto \widetilde{x}_i + a_i \widetilde{x}_1 \tag{11}$$

をかけて、f_1 の $\widetilde{x}_1$ についての最高次の係数は定数であるとしてよい。変数変換の性質より、f が解を持つ $\iff$ $\widetilde{f}$ が解を持つので、$\mathbf{V}(f) = \emptyset \iff \mathbf{V}(\widetilde{f}) = \emptyset$ である。また、$\widetilde{\bullet}$ が定数に影響しないので $1 \in I \iff 1 \in \widetilde{I}$ となる。

$$\begin{aligned}
\mathbf{V}(\widetilde{I}_1) &= \pi_1(\mathbf{V}(\widetilde{I})) && (12)\\
& \boxed{f_1 \text{ の } \widetilde{x}_1 \text{ の係数は定数、拡張定理}} && (13)\\
&= \pi_1(\emptyset) && (14)\\
& \boxed{\mathbf{V}(I) = \emptyset \text{ で } \mathbf{V}(I) = \emptyset \iff \mathbf{V}(\widetilde{I}) = \emptyset} && (15)\\
&= \emptyset. && (16)
\end{aligned}$$

帰納法の仮定より、$\widetilde{I}_1 = k[\widetilde{x}_2, \dots, \widetilde{x}_n]$ である。よって、$1 \in \widetilde{I}_1 \subset \widetilde{I}$ となる。$1 \in \widetilde{I}$ なので、($\widetilde{I}$ で定数は変化しない。)$1 \in I$ である。よって、I は全体である。

ヒルベルトの零点定理

1. f は $f_1, \dots, f_s$ の共通零点 $\mathbf{V}(f_1, \dots, f_s)$ で消えるとする。
2. $f^m = \sum_{i=1}^s A_i f_i$ なる A_i たちを探す。
   (a) $\widetilde{I} = \langle f_1, \dots, f_s, 1 - yf \rangle \subset k[x_1, \dots, x_n, y]$ とする。
   (b) $\mathbf{V}(\widetilde{I}) = \emptyset$ となる。
      i. どの $(a_1, \dots, a_n, a_{n+1}) \in k^{n+1}$ も $\mathbf{V}(\widetilde{I})$ に属さなければよい。
      ii. 頭 n 個で作った点が $f_1, \dots, f_s$ のすべてで消えるとき、$1 - yf$ はこの点で消えない。yf がこの点で消えるからである。
      iii. そうでないとき、どこかで消えないときはその f_i をそのまま使えば消えない。
   (c) $1 \in \widetilde{I}$ が弱い零点定理からわかる。
   (d)
   $$1 = \sum_{i=1}^s p_i(x_1, \dots, x_n, y) f_i + q(x_1, \dots, x_n, y)(1 - yf) \tag{17}$$
   となるように p, q がとれる。
   (e) $y = 1/f$ とする。
   $$1 = \sum_{i=1}^s p_i(x_1, \dots, x_n, 1/f) f_i. \tag{18}$$
   (f) f^m をたくさんかければ、上の $1/f$ が消えてのぞむ式が得られる。

逆のほうは「強い」ほうで言ってる。

5 多様体上の多項式関数と有理関数

1. $V = \mathbf{V}(I)$, $V \neq \emptyset$
2. (V が既約のとき) ($I = \mathbf{I}(V)$ としてよい。)
   (a) ($l = 1$ のとき)
      i. $W_0 \subsetneq V$
      ii. $\exists$: $(a_1, \dots, a_n) \in V - W_0$
      iii. $\exists$: $f \in \mathbf{I}(W_0)$、$f(a_1, \dots, a_n) \neq 0$
      iv. (場合 1)

A. $m, g_\bullet$:

$$f = \sum_{i=0}^{m} g_i(x_2, \ldots, x_n) x_i^i \tag{19}$$

B. $W_1 = \mathbf{V}(I_1) \cap \mathbf{V}(g_0, \ldots, g_m)$
C. $(c_2, \ldots, c_n) \in \mathbf{V}(I_1) - W_1$
D. $\exists$: $c_1 \in k$、$f(c_1, \ldots, c_n) \neq 0$

v. (場合 2)

A. $\exists (b_2, \ldots, b_n) \in \mathbf{V}(I_1) \exists b_1 \in k$: $(b_1, \ldots, b_n) \notin V$
B. $\exists h \in I$: $h(b_1, \ldots, b_n) \neq 0$
C. $r, u_\bullet$:

$$h = \sum_{i=0}^{r} u_i(x_2, \ldots, x_n) x_1^i. \tag{20}$$

D.「(4)〜を示そう」

- $0 \leq j \leq r$, N_j, $v_{j0}, \ldots, v_{j,r-1}$:

$$u_r^{N_j} f^j = q_j h + \underbrace{v_{j0}}_{\in k[x_2, \ldots, x_n]} + v_{j1} x_1 + \cdots + v_{j,r-1} x_1^{r-1}. \tag{21}$$

- K: $k[\mathbf{V}(I_1)]$ の分数体
- $\exists\ \phi_0, \ldots, \phi_r \in K$(すべては 0 でない):

$$^\forall 0 \leq i \leq r-1\text{: } \sum_{j=0}^{r} \phi_j [v_{ji}] = [0] \tag{22}$$

あるいは、

$$\sum_{j=0}^{r} \phi_j([v_{j0}], \ldots, [v_{j,r-1}]) = ([0], \ldots, [0]). \tag{23}$$

- とりなおし:$\phi_\bullet \in k[x_2, \ldots, x_n]/I_1$
- $\exists w_j \in k[x_2, \ldots, x_n]$: $\phi_j = [w_j]$. うち少なくとも 1 つは $w_j \notin I_1$
- $v_j = w_j u_r^{N_j}$

E. $g = u_r v_0$
F. $W_1 = \mathbf{V}(g) \cap \mathbf{V}(I_1)$

(b) $l-1$ について:

3. (V は既約とはかぎらない)
4. $\exists$: $V_\bullet : V = V_1 \cup \ldots \cup V_m$. 既約
5. V_i': $\pi_l(V_i)$ のザリスキ閉包
6. $V_1' \not\subset V_i'$
7. W_1: V_1 と $\emptyset$ に定理を適用したもの。$V_1' - W_1 \subset \pi_l(V_1)$、$W_1 \subsetneq V_1'$。
8. $W = W_1 \cup V_2' \cup \ldots \cup V_m'$

1. $W_1 = \mathbf{V}(I_l)$
2. Z_1: 閉包定理。$W_1 - Z_1 \subset \pi_l(V)$、$Z_1 \subsetneq W_1$
3. V_1:

$$V_1 = V \cap \{(a_1, \ldots, a_n) \in k^n; (a_{l+1}, \ldots, a_n) \in Z_1\} \tag{24}$$

$V_1 \subsetneq V$、$\pi_l(V) = (W_1 - Z_1) \cup \pi_l(V_1)$

4. W_2: $\pi_l(V_1)$ のザリスキ閉包
5. Z_2:閉包定理。$W_2 - Z_2 \subset \pi_l(V_1)$、$Z_2 \subsetneq W_2$
6. V_2:

$$V_2 = V_1 \cap \{(a_1, \ldots, a_n) \in k^n; (a_{l+1}, \ldots, a_n) \in Z_2\} \tag{25}$$

7. 3-4 を、できた $V_\bullet$ が $\emptyset$ になるまでくりかえす。

5.0.1 演習

(1) (a) $a, b \notin I \cap k[x_{l+1}, \ldots, x_n]$ とする。

- $a \notin I$ かつ $b \notin I$ のとき: I が素イデアルなので、$ab \notin I$ となる。よって、$ab \notin I_l$ となる。
- $a \notin I$ かつ $b \notin k[x_{l+1}, \ldots, x_n]$ のとき: b は $x_1, \ldots, x_l$ の 1 文字以上を含まなければならない。よって、ab も同様で、$ab \notin k[x_{l+1}, \ldots, x_n]$ となる。よって、$ab \notin I_l$ となる。
- $a \notin k[x_{l+1}, \ldots, x_n]$ かつ $b \notin I$ のとき: 上と同様。
- $a, b \notin k[x_{l+1}, \ldots, x_n]$ のとき: 上と同様。

(b) ?案。$\mathbf{V}(I_l)$ が既約でないとし、

$$\begin{aligned} \mathbf{V}(I_l) &= \mathbf{V}(fg, h_1, h_2, \ldots, h_s) && (26) \\ &= \mathbf{V}(f, h_1, \ldots, h_s) \cup \mathbf{V}(g, h_1, \ldots, h_s) && (27) \end{aligned}$$

であるとする。ただし、最後 2 つで $\mathbf{V}(I_l)$ を覆い、どちらかだけで全てを覆うということはない (既約でないから)。

$\mathbf{V}(I_l)$ は $k[x_{l+1}, \ldots, x_n]$ の subset だが、これを $k[x_1, \ldots, x_n]$ で捉えると、$\mathbf{V}(I)$ よりも広い (?)。したがて、

$$\begin{aligned} \mathbf{V}(I) &= \mathbf{V}(F_1, \ldots, F_s) && (28) \\ &= \mathbf{V}(F_1, \ldots, F_S) \cap \mathbf{V}(I_l) && (29) \\ &= \underbrace{(\mathbf{V}(F_1, \ldots, F_S) \cap \mathbf{V}(f, h_1, \ldots, h_s))}_{A} \cup \underbrace{(\mathbf{V}(F_1, \ldots, F_S) \cap V(g, h_1, \ldots, h_s))}_{B} && (30) \end{aligned}$$

A と B で $\mathbf{V}(I)$ が覆えていて、しかもどちらかだけで覆ってはいない。(後者は、先の「どちらかだけで全て $(\mathbf{V}(I_l))$ を覆うことはない」による。) よって、$\mathbf{V}(I)$ は既約でなく、対偶がしめされた。

(2) 体でやって戻せばいいと思っていた。つまり、h を u_r でわって先頭の x_1 に関する係数を 1 にしておく。このとき、わったあとの係数の分母はすべて u_r のべきになる。これで $k(x_2, \ldots, x_n)$ 係数で割り算して、最後に u_r のべきを解消する。

(3) (a) $x = (z, y) \in V_y$ とする。$\pi_1(x) = y$ となる。$(z, y) \in \mathbb{C} \times \{y\}$ はあきらか (実際はもっとせまい)。

$V_y \neq \emptyset$ とする $\pi_1(x) = y$ となる $x = (z, y) \in V$ が存在する。$\pi_1(x) = y$ なので、y にうつる V の元として x が見つかったことになり、$y \in \pi_1(V)$ である。逆に、$y \in \pi_1(V)$ とする。$\pi_1(x) = y$ となる $x \in V$ が存在する。すると、$x \in V_y$ である。よって、$V_y \neq \emptyset$ である。

(b) 場合 1 は

すべての $(b_2, \ldots, b_n) \in \mathbf{V}(I_1)$ とすべての $b_1 \in k$ にたいして、$(b_1, \ldots, b_n) \in V$ となる

ときだった。$\pi_1(V) \subset \mathbf{V}(I_1)$ は一般に成立するが、さらに部分解 $\mathbf{V}(I_1)$ から筒状に伸ばしたものが V であるというのがこの場合であるから、$\pi_1(V) = \mathbf{V}(I_1)$ である。

$V_y \subset \mathbb{C} \times \{y\}$ は一般に成立する。$(z, y) \in \mathbb{C} \times \{y\}$ とする。$y \in \pi_1(V) = \mathbf{V}(I_1)$ であり、$z \in \mathbb{C}$ なので、$(z, y) \in V$ である (場合 1)。さらに、$\pi_1(z, y) = y$ なので、$(z, y) \in V_y$ となる。

(c) 場合 2 は

ある $(b_2, \ldots, b_n) \in \mathbf{V}(I_1)$ と $b_1 \in k$ に対して $(b_1, \ldots, b_n) \notin V$ となる

場合だった。$I = \mathbf{I}(V)$ としてあるので、(与えられた $b_\bullet$ を使って)$h(b_1, \ldots, b_n) \neq 0$ となる多項式 $h \in I$ が

存在する。h を x_1 の多項式として、

$$h = \sum_{i=0}^{r} u_i(x_2, \ldots, x_n)x_1^i \tag{31}$$

とあらわす。$h(b_1, \ldots, b_n) \neq 0$ より、ある i に対して $u_i(b_2, \ldots, b_n) \neq 0$ となり、$u_i \notin I_1$ となる*1。もし、$u_r \in I_1$ ならば $h - u_r x_1^r$ も $(b_1, \ldots, b_n)$ で消えない*2から、$h - u_r x_1^r$ で置き換えることができる。このおきかえを繰替えして (次数を下げて)$u_r \notin I_1$ と仮定してもよい。
$\widetilde{W} = \mathbf{V}(u_r)$ とする。まず、$\pi_1(V) \not\subset \widetilde{W}$ をしらべる。$u_r \notin I_1$ となるようにしておいたので、$u_r(b_2, \ldots, b_n) \neq 0$ である。すると、

$$h(x_1, b_2, \ldots, b_n) = \sum_{i=0}^{r} u_i(b_2, \ldots, b_n)x_1^i \tag{32}$$

という x_1 についての方程式が得られる。代数学の基本定理より、これをみたす $\widetilde{b}_1$ が存在する。?

(4)

$$\begin{aligned}
(\widetilde{\pi}_{l-1} \circ \pi_1)(x_1, \ldots, x_n) &= \widetilde{\pi}_{l-1}(x_2, \ldots, x_n) && (33)\\
&= (x_{n-l+1}, \ldots, x_n) && (34)\\
&= \pi_l(x_1, \ldots, x_n). && (35)
\end{aligned}$$

(5) (a)

$$\begin{aligned}
(V \subset V_1 \cup V_2) &\iff (\mathbf{I}(V) \supset \mathbf{I}(V_1 \cup V_2)) && (36)\\
&\iff (\mathbf{I}(V) \supset \mathbf{I}(V_1)\mathbf{I}(V_2)) && (37)\\
&\iff ((\mathbf{I}(V) \supset \mathbf{I}(V_1)) \vee (\mathbf{I}(V) \supset \mathbf{I}(V_2))) && (38)\\
&\iff ((V \subset V_1) \vee (V \subset V_2)). && (39)
\end{aligned}$$

(b) $n = 2$ のときは示されている。n で成立するとする。$n + 1$ のとき示す。

$$\begin{aligned}
(V \subset V_1 \cup \ldots \cup V_{n+1}) &\iff (V \subset (V_1 \cup \ldots \cup V_n) \cup V_{n+1}) && (40)\\
&\iff ((V \subset (V_1 \cup \ldots \cup V_n)) \vee (V \subset V_{n+1})) && (41)\\
&\iff ((V \subset V_1) \vee \ldots \vee (V \subset V_{n+1})). && (42)
\end{aligned}$$

(6)

(7) (a)

$$\begin{aligned}
Z_1 &= \mathbf{V}_{W_1}([\phi_1], \ldots, [\phi_s]) && (43)\\
&= \left\{(x_1, \ldots, x_{n-l}) \in W_1; {}^\forall[\phi] \in \langle[\phi_1], \ldots, [\phi_s]\rangle\colon [\phi](x_1, \ldots, x_{n-l}) = 0\right\} && (44)\\
&= \left\{(x_1, \ldots, x_{n-l}) \in W_1; {}^\forall\phi \in \langle\phi_1, \ldots, \phi_{n-l}\rangle\colon \phi(x_1, \ldots, x_{n-l}) = 0\right\}. && (45)
\end{aligned}$$

よって、

$$\begin{aligned}
\{(a_1, \ldots, a_n) \in k^n; (a_{l+1}, \ldots, a_n) \in Z_1\} &= \left\{(a_1, \ldots, a_n) \in k^n; {}^\forall\phi \in \langle\phi_1, \ldots, \phi_{n-l}\rangle\colon \phi(a_{l+1}, \ldots, a_n) = 0\right\} && (46)\\
&= \langle\phi_1, \ldots, \phi_{n-l}\rangle. && (47)
\end{aligned}$$

これはアフィン多様体になっている。V_1 はこれと V との交わりなので OK。

*1 これは最高次の x_1^r の係数ではないかもしれない

*2 最高次をつぶして h を置き換える。このとき、消えないのは $(b_2, \ldots, b_n) \in \mathbf{V}(I_1)$ という仮定が条件 2 でかかっていたから。

(b)

$$\begin{aligned}
(W_1 - Z_1) \cup \pi_l(V_1) &= (W_1 - Z_1) \cup \pi_l(\{(a_1, \ldots, a_n) \in k^n; (a_{l+1}, \ldots, a_n) \in Z_1\} \cap V) && (48)\\
&= (W_1 - Z_1) \cup (Z_1 \cap \pi_l(V)) && (49)\\
&= ((W_1 - Z_1) \cup Z_1) \cap ((W_1 - Z_1) \cup \pi_l(V)) && (50)\\
&= W_1 \cap ((W_1 - Z_1) \cup \pi_l(V)) && (51)\\
&\boxed{Z_1 \subsetneq W_1} && (52)\\
&= W_1 \cap \pi_l(V) && (53)\\
&\boxed{W_1 - Z_1 \subset \pi_l(V)(\text{閉包定理})} && (54)\\
&= \mathbf{V}(V_1) \cap \pi_l(V) && (55)\\
&= \pi_l(V) && (56)\\
&\boxed{\pi_l(V)\ \text{のほうがせまい}}. && (57)
\end{aligned}$$

定理 1(閉包定理の後半) k を代数的閉体とし、$V = \mathbf{V}(I) \subset k^n$ とする。$V \neq \emptyset$ ならば、

$$\mathbf{V}(I_l) - W \subset \pi_l(V) \tag{58}$$

となるようなアフィン多様体 $W \subsetneq \mathbf{V}(I_l)$ が存在する。

1. ？？？ :$l = 1$ のときは済んでいる。
2. ？？？ :$l > 1$ を考える。
3. $V = \mathbf{V}(I)$ としていたが、$V = \mathbf{V}(\mathbf{I}(V))$ が成立しているので、$I = \mathbf{I}(V)$ としてもよい。(「V を定義するどのイデアル I も同じ $\mathbf{V}(I_l)$ を与える。)
4. V が既約なとき:
   (a) V は既約なので、$I = \mathbf{I}(V)$ は素イデアル
   (b) Fact: I が素イデアル $\implies$ I_l は素イデアル。演習 1。
   略証:$a, b \notin I \cap k[x_{l+1}, \ldots, x_n]$ とする。あとは 4 通りにわける。I が素イデアルであることを使うパートと、a, b が $x_1, \ldots, x_l$ を含んでしまうパートに分かれる。
   (c) Fact: V が既約 $\implies$ $\mathbf{V}(I_l)$ は既約。
   略証: (3) で $I = \mathbf{I}(V)$ とした。I は素イデアルなので (a)、I_l も素イデアルであり (b)、代数的閉体上では素イデアルと既約多様体が対応するので[*3]、$\mathbf{V}(I_l)$ は既約。
   (d)「$\mathbf{V}(I_l) - W \subset \pi_l(V)$ となる $W \subsetneq \mathbf{V}(I_l)$ が存在する」よりも強い、

任意の多様体 $W_0 \subsetneq V$ にたいして、

$$\mathbf{V}(I_l) - W_l \subset \pi_l(V - W_0) \tag{59}$$

となる多様体 $W_l \subsetneq \mathbf{V}(I_l)$ が存在する

を示す。
   i. $l = 1$ のとき
   ii. $\exists a_\bullet$: $W_0 \neq V$ なので、$(a_1, \ldots, a_n) \in V - W_0$ なる点が存在する。
   iii. $\exists f$: $f \in \mathbf{I}(W_0)(W_0$ できえる) で、$f(a_1, \ldots, a_n) \neq 0$ となる多項式が存在する。(なぜ？)
   iv. 場合 I: すべての $(b_2, \ldots, b_n) \in \mathbf{V}(I_l)$ とすべての $b_1 \in k$ に対して $(b_1, \ldots, b_n) \in V$ となる場合:

[*3] 4-5-Prop3 一般の体で、V が既約 $\iff$ $\mathbf{I}(V)$ は素イデアル。

A. $m, g_\bullet$: f を x_1 について m 次であり、

$$f = \sum_{i=0}^{m} g_i(x_2, \ldots, x_n) x_1^i \tag{60}$$

とかく。

B. $\exists W_1$: $W_1 = \mathbf{V}(I_1) \cap \mathbf{V}(g_0, \ldots, g_m)$ とする。(これが条件をみたす)

C. Fact: $W_1 \subsetneq \mathbf{V}(I_1)$ である。($\subset$ はあきらか。)

実際 $(a_2, \ldots, a_n) \in \mathbf{V}(I_1) \setminus W_1$ である。なぜなら、$f(a_1, \ldots, a_n) \neq 0$ なので (iii)、g_i のどれかは $(a_2, \ldots, a_n)$ で非零である。よって、$(a_2, \ldots, a_n) \notin W_1$ にはなっている。また、$(a_1, \ldots, a_n) \in V$ なので $(a_2, \ldots, a_n)$ はその部分解 $\mathbf{V}(I_1)$ になっている。

D. $\forall c_\bullet$: $(c_2, \ldots, c_n) \in \mathbf{V}(I_1) - W_1$ とする。

E. $(c_1, \ldots, c_n) \notin W_1 = \mathbf{V}(I_1) \cap \mathbf{V}(g_0, \ldots, g_m)$ なので、$g_0, \ldots, g_m$ のいずれかで消えない。

F. よって、$f(x_1, \ldots, c_2, \ldots, c_n) \in k[x_1]$ は非零な多項式。

G. $\exists c_1$: k は無限体なので、$f(c_1, \ldots, c_n) \neq 0$ となる $c_1 \notin k$ が存在する。

H. f は W_0 で消えるようにとっていたので (iii)、f で消えないやつ $(c_1, \ldots, c_n) \notin W_0$。

I. 場合 I の仮定の、ファイバーがちゃんとのびているというやつより、$(c_1, \ldots, c_n) \in V$。

J. $(c_1, \ldots, c_n) \in V - W_0$ となる。(H,I)

K. $(c_2, \ldots, c_n) \in \pi_1(V - W_0)$ となる。

v. 場合 II: ある $(b_2, \ldots, b_n) \in \mathbf{V}(I_1)$ とある $b_1 \in k$ に対して $(b_1, \ldots, b_n) \notin V$ となるとき。

A. $\exists h$: $(b_1, \ldots, b_n) \notin V$ なので、$h(b_1, \ldots, b_n) \neq 0$ となる $h \in I$ が存在する。(なぜ？)

B. r, u_i: h を x_1 について整理する。

$$h = \sum_{i=0}^{r} u_i(x_2, \ldots, x_n) x_1^i. \tag{61}$$

C. $h(b_1, \ldots, b_n) \neq 0$ なので、ある i について $u_i(b_2, \ldots, b_n) \neq 0$ となり ($(b_2, \ldots, b_n) \notin \mathbf{V}(I_1)$ なので)、$u_i \notin I_1$ となる。

D. $u_r \in I_1$(最高次) ならば、$h - u_r x_1^r$ も $(b_1, \ldots, b_n)$ で消えないのでこれを置き換えて、最高次 $u_r \notin I_1$ となるようにできる。

$v_i \in k[x_2, \ldots, x_n]$ で、

$$\sum_{i=0}^{r} v_i f^i \in I \text{かつ} v_0 \notin I_1 \tag{62}$$

なるものが存在することを示す。

E.

F. $q, v_\bullet$: $0 \leq j \leq r$ にたいして、

$$u_r^{N_j} f^j = q_j h + v_{j0} + v_{j1} x_1 + \cdots + v_{j,r-1} x_1^{r-1}. \tag{63}$$

とする。f を $k(x_2, \ldots, x_n)$ 係数で割り算して最後に払えばよい。

G. $I_1 = \mathbf{I}(\mathbf{V}(I_1))$ だたので、$k[x_2, \ldots, x_n]/I_1 \simeq k[\mathbf{V}(I_1)]$ となる。

H. K: $\mathbf{V}(I_1)$ は既約なので (a,b)、この環は整域で分数体 K が考えられる。

I. K を元とする $(r+1) \times r$ 行列

$$\begin{pmatrix} [v_{00}] & \ldots & [v_{0,r-1}] \\ \vdots & & \vdots \\ [v_{r0}] & \ldots & [v_{r,r-1}] \end{pmatrix} \tag{64}$$

を作る。横に先の割り算の結果が並んで、縦には $1, f, \ldots, f^r$ となっている。

J. $\exists\phi_\bullet$: 行は $r+1$ 個あり、その行たちは K^r に属しているので、線型従属であり、係数 $\phi_0,\dots,\phi_r \in K$ で、

$$0 \le i \le r-1 \implies \sum_{j=0}^{r} \phi_j [v_{ji}] = [0] \tag{65}$$

となるものがある。あるいは、

$$\sum_{j=0}^{r} \phi_j([v_{j0}],\dots,[v_{j,r-1}]) = ([0],\dots,[0]). \tag{66}$$

K. $\phi_\bullet$ たちの分母を払って、$\phi_\bullet \in k[x_2,\dots,x_n]_1$ と思ってよい。

L. $w_\bullet$: $\phi_j = [w_j]$ となる $w_j \in k[x_2,\dots,x_n]$ が存在する。

M. $\phi_\bullet$ すべては 0 ではないのだから、$w_\bullet$ の少なくとも 1 つは I_1 に入らない。

N. J を書き直せば、

$$\sum_{j=0}^{r} [w_j]([v_{j0}],\dots,[v_{j,r-1}]) = ([0],\dots,[0]). \tag{67}$$

O. 上は、

$$\sum_{j=0}^{r} w_j(v_{j0},\dots,v_{j,r-1}) \in (I_1)^r \tag{68}$$

であり、

$$^\forall i\colon \sum_{j=0}^{r} w_j v_{ji} \in I_1 \tag{69}$$

となっている。

P. 擬除算の式に w_j をかけて $\sum_{j=0}^{r}$ をとる。

$$\begin{aligned}
\sum_{j=0}^{r} w_j(u_r^{N_j} f^j) \mod I &= \sum_{j=0}^{r} w_j(q_j h + v_{j0} + v_{j1}x_1 + \cdots + v_{j,r-1}x_1^{r-1}) \mod I && (70)\\
&= \sum_{j=0}^{r} w_j(q_j h) \mod I && (71)\\
&\boxed{\mathrm{O}, \textstyle\sum w_j v_{ji} \in I_1} && (72)\\
&= 0 \mod I && (73)\\
&\boxed{\text{A より。} h \in I}. && (74)
\end{aligned}$$

よって、

$$\sum_{j=0}^{r} w_j(u_r^{N_j} f^j) \in I. \tag{75}$$

Q. $v_\bullet$: $v_j = w_j u_r^{N_j}$

R. $u_r \notin I_1$ であり (擬除算「分母」にするためだった。D より。) 、ある j に対し $w_j \notin I_1$ であるから (線型従属より。M。) 、I_1 が素イデアルであること (既約と仮定している。a,b) より、$v_j \notin I_1$ となる。いまのところ、多項式として

$$\sum_{v_j f^j} \tag{76}$$

まで作った。うちどれか $v_j \notin I_1$ までわかっている。

S. $(1 = f^0$ の係数 $v_0 \notin I_1$ となるようにとりなおす。)

T. $\exists t$: $v_0, \dots, v_{t-1} \in I_1$ かつ $v_t \notin I_1$ とする。

U.

$$f^t \sum_{j=t}^{r} v_t f^{j-t} \in I \tag{77}$$

を考える。$f \notin I$ なので (iii。f は $(a_1, \dots, a_n)$ で消えず、この点は $V - W_0$ の元だった。)、

$$\sum_{j=t}^{r} v_t f^{j-t} \in I. \tag{78}$$

これは定数の係数 v_t が (T より)$v_t \notin I_1$ となっている。

V. D おわり。$v_i \in k[x_2, \dots, x_n]$ で、$\sum_{i=0}^{r} v_i f^i \in I$ かつ $v_0 \notin I_1$ となるものが存在する。

W. 次を示す:

$$\pi_1(V) \cap (k^{n-1} - \mathbf{V}(v_0)) \subset \pi_1(V - W_0). \tag{79}$$

実際、$\sum_{i=0}^{r} v_i f^i \in I$ なので、任意の $(c_1, \dots, c_n) \in V$ に対して、

$$v_0(c_2, \dots, c_n) + f(c_1, \dots, c_n) \sum_{i=1}^{r} v_i(c_2, \dots, c_n) f(c_1, \dots, c_n)^{i-1} = 0 \tag{80}$$

となる。したがって、$v_0(c_2, \dots, c_n) \neq 0$ ならば $f(c_1, \dots, c_n) \neq 0$ となり $(ab = 0 \implies a = 0 \vee b = 0)$、(iii より、$f$ は W_0 上消えるので)$(c_1, \dots, c_n) \notin W_0$ である。(まず V をとって、そこから射影を考え、引き算の条件をならばにして示した。)

X. g: $u_r \notin I_1$(D より。最高次係数はこうしておいた。) であり、$v_0 \notin I_1$(U より。定数の係数はこうしておいた) であり、I_1 は素イデアルなので、$g = u_r v_0$ とすると $g \notin I_1$ である。

Y. W_1: $W_1 = \mathbf{V}(g) \cap \mathbf{V}(I_1)$ とする。

Z. X の $g \notin I_1$ より、$W_1 \subsetneq \mathbf{V}(I_1)$ である。

AA 示したいのは、(d) の

$$\mathbf{V}(I_1) - W_1 \subset \pi_1(V - W_0) \tag{81}$$

だった。$(c_2, \dots, c_n) \in \mathbf{V}(I_1) - W_1$ をとる。$(c_2, \dots, c_n) \notin W_1$ なので、「u_r で消えるか v_0 消える」の否定で、u_r, v_0 のどちらでも消えない。

AB $\exists f_\bullet$: $I = \langle f_1, \dots, f_s \rangle$ とする。

AC $h \in I$ なので (A)、$I = \langle h, f_1, \dots, f_s \rangle$ となる。

AD $\exists c_1$: 拡張定理と、h の先頭係数 $u_r(c_2, \dots, c_n) \neq 0$ であること (AA)、より、ある $c_1 \in k$ で、$(c_1, \dots, c_n) \in V$ となるものが存在する。

AE W の式 (の左側から自由にとって), $v_0(c_2, \dots, c_n) \neq 0$ より、$(c_2, \dots, c_n) \in \pi_1(V - W_0)$ となり、AA、あるいは (d) の式が示される。($\pi(I_1) - W_1$ から元をとると、それは自動的に $\mathbf{V}(I_1) - W_1$ に入り、AA の式が使える。)

vi. $l = 1$ のときは示したので、$l - 1$ で成立を仮定する。

vii. $\forall W_0$: $W_0 \subset\neq V$ を自由にとる。

viii. $\exists W_1$: $l = 1$ のときは示したので適用する。

$$W_1 \subsetneq \mathbf{V}(I_1) \text{かつ} \mathbf{V}(I_1) - W_1 \subset \pi_1(V - W_0) \tag{82}$$

をみたすものがある。

ix. $I = l = (I_1)_{l-1}$ である。

x. $\mathbf{V}(I_1)$ は既約である。(a,b,c)

xi. $\exists W_l$: 帰納法の仮定を使う。

$$W_l \subsetneq \mathbf{V}(I_l)\text{かつ}\mathbf{V}(I) - W_1 \subset \widetilde{\pi}_{l-1}(\mathbf{V}(I_1) - W_1) \tag{83}$$

なるものが存在する。

xii. ここで、$\widetilde{\pi}_{l-1}\colon k^{n-1} \to k^{n-l}$ は射影であるが、domain が違ったので区別している。$\pi_l = \widetilde{\pi}_{l-1} \circ \pi_1$ なので

$$\mathbf{V}(I_l) - W_l \overset{\boxed{\text{xi}}}{\subset} \widetilde{\pi}_{l-1}(\mathbf{V}(I_1) - W_1) \overset{\boxed{\text{viii}}}{\subset} \pi_l(V - W_0). \tag{84}$$

となる。

xiii. l 全体で示され、既約な多様体について、定理 1(の強いやつ) が成立する。

5. 既約でない（！！ ）場合に示す。
6. $V_\bullet$:

$$V = V_1 \cup \ldots \cup V_m \tag{85}$$

と分解する。$V_\bullet$ は既約。

7. $V'_\bullet$: $\pi_l(V_\bullet)$ のザリスキ閉包。$V'_\bullet = \mathbf{V}(\mathbf{I}(\pi_l(V_\bullet)))$。

$$\mathbf{V}(I_l) = V'_1 \cup \ldots \cup V'_m \tag{86}$$

8. を示す。
   (a) $V'_1 \cup \ldots \cup V_m 7$ は $\pi_l(V_1) \cup \ldots \cup \pi_l(V_m) = \pi_l(V)$ を含む多様体である。
   (b) $\mathbf{V}(I_l)$ は $\pi_l(V)$ のザリスキ閉包なので (代数的閉体、閉包定理)

$$\mathbf{V}(I_l) \subset V'_1 \cup \ldots \cup V'_m. \tag{87}$$

   (c) 逆を示す。各 i にたいし、

$$\pi_l(V_i) \subset \pi_l(V) \subset \mathbf{V}(I_l). \tag{88}$$

   (d) V'_i は $\pi_l(V_i)$ のザリスキ閉包なので、

$$V'_i \subset \mathbf{V}(I_l). \tag{89}$$

   (e)

$$V'_1 \cup \ldots V'_m \subset \mathbf{V}(I_l). \tag{90}$$

9. 4-4-定理 3 によれば、$\mathbf{V}(I_l)$ は $\pi_l(V)$ のザリスキ閉包なので、(代数的閉体だし)

$$V'_i = (\pi_l(V_i)\text{のザリスキ閉包}) = \mathbf{V}(\mathbf{I}(V_i)_l). \tag{91}$$

10. V_i は既約としておいたので $\mathbf{I}(V_i)$ は既約で、$\mathbf{I}(V_i)_l$ も既約で、V'_i も既約になる。よって、(7) の分解は既約分解である。
11. 他のものには含まれない $V'_\bullet$ があるはずなので、それを番号をつけかえて V'_1 が他のものに含まれないということにしておく。
    すべての $V'_\bullet$ が等しいということはおこらない。なぜなら、すべてが等しいとしたら $\mathbf{V}(I_l)$ が既約ということになる。すると、I_l は素イデアルになる。5 により、V は既約でないとしたのだから、I は素イデアルでなく、I_l も素イデアルでない？？

12. W_1: V_1 にいままでの「既約にたいする強い定理」を使って、定理の $W_0 = \emptyset$ とすることで、

$$\mathbf{V}(\mathbf{I}(V_1)_l) - W_1 \subset \pi_l(V_1) \tag{92}$$

となる $W_1 \subsetneq V_1'$ が存在する。

13. 9 と上より、

$$V_1' - W_1 \subset \pi_l(V_1). \tag{93}$$

14. W: $W = W_1 \cup V_2' \cup \ldots \cup V_m'$ とする。(これがみたす！)
15. $W \subset \mathbf{V}(I_l)$ となる。($W_1 \subsetneq V_1'$ だし、$\mathbf{V}(I_l)$ の分解がある。)
16.

$$\begin{aligned}
\mathbf{V}(I_l) - W &= (V_1' \cup \ldots \cup V_m') - (W_1 \cup V_2' \cup \ldots \cup V_m') && (94)\\
&= V_1' - (W_1 \cup V_2' \cup \ldots \cup V_m') && (95)\\
&\subset V_1' - W_1 \subset \pi_l(V_1) \subset \pi_l(V). && (96)
\end{aligned}$$

17. $W \neq \mathbf{V}(I_l)$ を示す。$W = \mathbf{V}(I_l)$ とする。

    (a)

$$W_1 \cup V_2' \cup \ldots \cup V_m' = \mathbf{V}(I_l) = V_1' \cup \ldots \cup V_m'. \tag{97}$$

    (b)

$$V_1' \subset W_1 \cup V_2' \cup \ldots \cup V_m'. \tag{98}$$

    (c) V_1' は既約なので、W_1, V_2', ..., V_m' のどれかに含まれなければならない。矛盾。