グレ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 5 月 18 日

1　幾何，代数，アルゴリズム

2　グレブナ基底

3　消去理論

3.1　消去および拡張定理

グレブナ基底を lex 順序で計算すると、変数の消去が起こることをみた。このことを示す。そのために、「消去イデアル」を定義する。$k[x_1,\dots,x_n]$ のイデアル I について、「I の l 次の消去イデアル I_l」を $I_l := I \cap k[x_{l+1},\dots,x_n]$ と定める。これが $k[x_1,\dots,x_n]$ のイデアルになっていることを示す必要はある。

証明
I は $k[x_1,\dots,x_n]$ のイデアルであり、$k[x_{l+1},\dots,x_n]$ は $k[x_{l+1},\dots,x_n]$ のイデアルなので、イデアルの交わりがイデアルになることは使えない。個別にイデアルの条件を示す必要がある。

- 和で閉じる: $f,g \in I_l$ とする。$f,g \in I$ なので、$f+g \in I$ となる。また、$f,g \in k[x_{l+1},\dots,x_n]$ なので、$f+g \in k[x_{l+1},\dots,x_n]$ となっている。よって、$f+g \in (I \cap k[x_{l+1},\dots,x_n]) = I_l$ となっている。
- 積で飲み込む:$f \in I_l$ とし、$g \in k[x_{l+1},\dots,x_n]$ とする。$gf \in I_l$ であることを示す。$f \in k[x_{l+1},\dots,x_n]$ なので、$gf \in k[x_{l+1},\dots,x_n]$ となっている。また、I がイデアルであり $f \in I$ なので、$gf \in I$ となっている。よって、$gf \in I_l$ となっている。

(証終) さらに、l 次の消去イデアル I_l の 1 次の消去イデアル $(I_l)_1$ は I の $l+1$ 次の消去イデアル I_{l+1} になっている:$(I_l)_1 = I_{l+1}$ である。

証明
$I_l = I \cap k[x_{l+1},\dots,x_n]$ であり、$I_{l+1} = I \cap k[x_{l+2},\dots,x_n]$ であり、$(I_l)_1 = I_l \cap k[x_{l+2},\dots,x_n]$ である。よって、

$$\begin{aligned}(I_l)_1 &= I_l \cap k[x_{l+2},\dots,x_n] &(1)\\ &= (I \cap k[x_{l+1},\dots,x_n]) \cap k[x_{l+2},\dots,x_n] &(2)\\ &= I \cap k[x_{l+1},\dots,x_n] &(3)\\ &= I_l. &(4)\end{aligned}$$

示された。

(証終) つまり、高次の消去イデアルを考えたいときには、1 次ずつ消去イデアルを計算すればよいことがわかった。

消去イデアルはその定義から、イデアル I のうち文字を消したもののあつまりであり、G を I の基底とするなら、この G をたしひきかけ算して文字を消したもののあつまりとなっている。$\mathbf{V}(I)$ を考えると、これに属する点は I の式を 0 にしなくてはならず、特に I_l の式を 0 にしなくてはならない。これは、$\mathbf{V}(I)$ に点が属するには $k[x_{l+1},\dots,x_n]$ のなかではどうでなければならないかという必要条件を与える。I_l の式を 0 にするときを考えるには I_l の基底がわかっていれば必要十分なので、I_l の基底を求める方法を知りたいが、これには Groebner 基底が便利である。次のことが言え

る。これを消去定理とよぶ。「G を $I \subset k[x_1, \ldots, x_n]$ の lex 順序での Groebner 基底とすると、$G \cap k[x_{l+1}, \ldots, x_n]$ は I_l の Groebner 基底となる。」

証明

$G \cap k[x_{l+1}, \ldots, x_n] \subset I_l$ なので、$\langle \mathrm{LT}(G \cap k[x_{l+1}, \ldots, x_n]) \rangle = \langle \mathrm{LT}(I_l) \rangle$ となることを示せばよい。この $\subset$ は、$G \cap k[x_{l+1}, \ldots, x_n] \subset I_l$ は自明なので、生成元 $\mathrm{LT}(I_l)$ が $\langle \mathrm{LT}(G \cap k[x_{l+1}, \ldots, x_n]) \rangle$ に包まれることを示せばよい。$f \in I$ なので、$\mathrm{LT}(f) \in \mathrm{LT}(I) \subset \langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) \rangle$ となっていて、$\mathrm{LT}(g_i) | \mathrm{LT}(f)$ となる i が存在する。示したいのは $\mathrm{LT}(f)$ が $\mathrm{LT}(G \cap k[x_{l+1}, \ldots, x_n])$ のどれかで割り切れることであり、$\mathrm{LT}(G)$ である $\mathrm{LT}(g_i)$ で割り切れることは示したので、あとは $g_i \in k[x_{l+1}, \ldots, x_n]$ を示せばよい。

$f \in k[x_{l+1}, \ldots, x_n]$ なので、$\mathrm{LT}(f) \in k[x_{l+1}, \ldots, x_n]$ である。多項式順序の性質から、$\mathrm{LT}(g_i) \leq \mathrm{LT}(f)$ であり、いまは lex 順序を採用しているので、$\mathrm{LT}(g_i) \in k[x_{l+1}, \ldots, x_n]$ となる。さらに lex 順序を採用しているので、$g_i \in k[x_{l+1}, \ldots, x_n]$ となり、$g_i \in G \cap k[x_{l+1}, \ldots, x_n]$ となる。よって、$g_i \in G \cap k[x_{l+1}, \ldots, x_n]$ であり、$\mathrm{LT}(g_i) | \mathrm{LT}(f)$ であり、$\mathrm{LT}(f) \in \langle \mathrm{LT}(G \cap k[x_{l+1}, \ldots, x_n]) \rangle$ となっている。

(証終) これで消去のほうは議論できた。あとは後退代入に相当するところを考える。

文字を消した結果の式を満たすことは、多様体に点が属することの必要条件でしかない。それを満たす点のことを部分解という。つまり、「$(a_{l+1}, \ldots, a_n) \in k[x_{l+1}, \ldots, x_n]$ が $\mathbf{V}(I)$ の部分解である」とは、「$(a_{l+1}, \ldots, a_n) \in \mathbf{V}(I_l)$ となる」ことである。したがって、多様体に属するように整合性が取れるように他の点が取れるかどうかは分からない。そのような拡張ができるための十分条件として、次の拡張定理がある。「体は $k = \mathbb{C}$ で考えることにする。$(a_2, \ldots, a_n) \in \mathbf{V}(I_1)$ を部分解とする。I の Groebner 基底を G とする。$k[x_1, \ldots, x_n]$ の多項式について、その多項式を $(\mathbb{C}[x_2, \ldots, x_n])[x_1]$ の元、すなわち x_1 だけを不定元とみなした多項式とみなしたときの最高次の係数を LC' とよぶことにする。ただし、$\mathrm{LC}'(0)$ は考えないことにする。この条件のもとで、

$$(a_2, \ldots, a_n) \notin \mathbf{V}(\mathrm{LC}'(G)) \implies (a_1, a_2, \ldots, a_n) \in \mathbf{V}(I) \text{となる} a_1 (\in \mathbb{C}) \text{が存在する} \tag{5}$$

となる。証明は後の節でやる。先に、$(I_l)_1 = I_{l+1}$ であることは示したので、必要なら繰り返し使えばよい。

ここで、2 つの特徴的な条件がある。

- 体を $\mathbb{C}$ にしていること:$x^2 = z$, $x^2 = y$ を $\mathbb{R}$ 上で考えて先の定義をナイーブに適用すると、x を消去した $y = z$ 上、つまり (a, a) は、$\mathbf{V}(\mathrm{LC}'(x^2 - z), \mathrm{LC}'(x^2 - y)) = \mathbf{V}(1, 1) = \emptyset$ に入らない限り、つまりいつでも拡張できるということになるが、実際は $a \geq 0$ のときだけ拡張できる。
- $(a_2, \ldots, a_n) \notin \mathbf{V}(\mathrm{LC}'(G))$ としていること: $xy = 1$, $xz = 1$ を考える。

```
  − xy + (−1)
  − xz + (−1)
.
S(xy + (−1), xz + (−1)) = y + (−1)z.
Not enough. Appends
  − y + (−1)z
.
S(xy + (−1), y + (−1)z) = 0.
S(xz + (−1), y + (−1)z) = 0.
Enough for groebner basis. Result is
  − xy + (−1)
  − xz + (−1)
  − y + (−1)z
. ■ Minimalizes groebner basis
  − xy + (−1)
  − xz + (−1)
  − y + (−1)z
.
xy + (−1) is removed by y + (−1)z.
Minimalized groebner basis is
  − xz + (−1)
  − y + (−1)z
. ■
Reduce groebner basis
  − xz + (−1)
  − y + (−1)z
.
Reducing: overline(xz + (−1)) = xz + (−1).
Reducing: overline(y + (−1)z) = y + (−1)z.
Reduced groebner basis is
  − y + (−1)z
  − xz + (−1)
. ■
```

という計算で、この Groebner 基底が $y - z$, $xz - 1$ である。よって、$I_1 = \langle y - z \rangle$ である。よって、$\mathbf{V}(I_1) = \{(a, a); a \in \mathbb{C}\}$ となる。よって、これをナイーブに拡張すると、$(1/a, a, a)$ となる。

ここで先の条件を考えてみる。$\mathrm{LC}'(xz-1)=z$ なので、拡張できるための十分条件として $(a,a)\notin\mathbf{V}(z)$ が得られる。つまり、拡張できないかもしれない場合というのは、$(a,a)\in\mathbf{V}(z)$ になる。このときというのは、$a=0$ のときである。このときは実際、$1/a$ が考えられない。また図を考えて、$y=z$, $xz=1$ というときを考える。これは、平面 $y=z$ と双曲線 $xz=1$ を y 方向に延ばしたやつの共有点全体だが、この点のうち $z=0$ となっているものはあきらかに存在しない。

$\mathrm{LC}'(g_1),\ldots,\mathrm{LC}'(g_s)$ のうち定数があったときはあきらかに $\mathbf{V}(\mathrm{LC}'(g_1),\ldots,\mathrm{LC}'(g_s))=\emptyset$ となるので、部分解全体が拡張できることが保証される。つまり、系として「体は $k=\mathbb{C}$ とする。部分解 $(a_2,\ldots,a_n)\in\mathbf{V}(I_1)$ があったとする。さらに、G を I の Groebner 基底とし、$\mathrm{LC}'(G)$ のうち (当然非 0 の) 定数があったとすると、部分解 $(a_2,\ldots,a_n)$ は常に $(a_1,\ldots,a_n)\in\mathbf{V}(I)$ に拡張できる。」が得られる。仮に $g_1,\ldots,g_s$ に定数があったとすると、元の $\langle I\rangle$ が全体集合になり、$\mathbf{V}(I)$ は空集合になる。このときは、拡張もなにもなくなってしまうので自明に正しい。また、仮に $g_1,\ldots,g_s$ に 0 があったとすると、そのような 0 は外しておけばよいので考える必要がない。このときは LC' を考えることができなくなってしまう。

3.2 消去の幾何

頭 l 個落とす写像 $\pi_l\colon\mathbb{C}^n\to\mathbb{C}^{n-l}$ を射影写像 (projection map) という。すると、消去イデアルとについて、次の関係がある。「$f_\bullet\in k[x_1,\ldots,x_n]$ とする。

$$\pi_l(\mathbf{V}(f_1,\ldots,f_s))\subset\mathbf{V}(\langle f_1,\ldots,f_s\rangle_l)\tag{6}$$

となる。言い換えるなら、多様体の (l 次の) 射影は (l 次の) 部分解に包まれる。」

証明

$(a_1,\ldots,a_n)\in\mathbf{V}(f_1,\ldots,f_s)$ とする。$f_\bullet(a_1,\ldots,a_n)=0$ となっている。$\pi_l(a_1,\ldots,a_n)=(a_{l+1},\ldots,a_n)$ である。

一般に、$f\in k[x_{l+1},\ldots,x_n]$ のとき、これを $f\in k[x_1,\ldots,x_n]$ とみなすと、$f(\xi_1,\ldots,\xi_n)$ は $\xi_1,\ldots,\xi_l$ の値に依存せず、$\xi_{l+1},\ldots,\xi_n$ の値のみによって定まる。これは、$f\in k[x_1,\ldots,x_n]$ ではあるが、$k[x_{l+1},\ldots,x_n]$ からの埋め込みだったので、式のなかに $x_1,\ldots,x_n$ の文字があらわれず、これらに対応する値 $\xi_1,\ldots,\xi_l$ に値が依存しないからである。よって、$f(\pi(\xi_1,\ldots,\xi_n))$ と π_l による同値類で定めれば、これは well-defined である。

$f\in\langle f_1,\ldots,f_s\rangle_l$ とする。$f\in k[x_{l+1},\ldots,x_n]$ なので、先の考察より f のとる値は π_l の同値類で定まり、

$$f(a_{l+1},\ldots,a_n)=f(\pi_l(a_1,\ldots,a_n))=f(0,\ldots,0,a_{l+1},\ldots,a_n)\tag{7}$$

である。また、$f\in\langle f_1,\ldots,f_s\rangle$ なので、$f=\sum_i h_if_i$ となる $h_\bullet\in k[x_1,\ldots,x_n]$ が存在し、

$$f(a_{l+1},\ldots,a_n)\overset{\boxed{\text{頭 } l \text{ 個はなんでもいい (well-defined)}}}{=}f(a_1,\ldots,a_n)\tag{8}$$

$$=\sum_{i=1}^{s}h_i(a_1,\ldots,a_n)\underbrace{f_i(a_1,\ldots,a_n)}_{=0,\text{ はじめの設定}}\tag{9}$$

$$=0.\tag{10}$$

(証終) 言い換えるなら、多様体の射影は、部分解のうち拡張できるもの全体に一致する (そりゃそうだ、射影が部分解をはみ出ることがないというほうが重要情報っぽい。)。例えば、$(y=z,xy=1)$ を考えると、これの射影 $\pi_1(\mathbf{V}(y-z,xy-1))$ は $\{(a,a);a\neq0\}$ であり、消去イデアルのなす多様体は $\mathbf{V}(\langle y-z\rangle)$ になって、$\{(a,a)\}$ になる。

ただし、多様体の射影がかならず多様体になるとは限らない。実際先の例だと、$\pi_1(\mathbf{V}(y-z,xy-1))=\{(a,a);a\neq0\}$ であり、これは多様体でない。この状況を考えるために、次の分解を用意しておく。「$f_1,\ldots,f_s\in k[x_1,\ldots,x_n]$ について、

$$\mathbf{V}(f_1,\ldots,f_s)=\pi_1(\mathbf{V}(f_1,\ldots,f_s))\cup(\mathbf{V}(f_1,\ldots,f_s)\cap\mathbf{V}(\mathrm{LC}'(f_1),\ldots,\mathrm{LC}'(f_s))).\tag{11}$$

となる。」

証明

- $\supset$: $a = (a_1, \ldots, a_n)$ とする。$a \in \pi_1(\mathbf{V}(f_1, \ldots, f_s))$ のときは、先の「多様体の射影は部分解に含まれる」より、$a \in \mathbf{V}(f_1, \ldots, f_s)$ となる。$a \in \mathbf{V}(f_1, \ldots, f_s) \cap \mathbf{V}(\mathrm{LC}'(f_1), \ldots, \mathrm{LC}'(f_s))$ のときは自明に $a \in \mathbf{V}(f_1, \ldots, f_s)$ となる。
- $\subset$: $a \in \mathbf{V}(f_1, \ldots, f_s)$ とする。$a \notin \mathbf{V}(f_1, \ldots, f_s) \cap \mathbf{V}(\mathrm{LC}'(f_1), \ldots, \mathrm{LC}'(f_s))$ であるとする。このときは、$a \in \mathbf{V}(f_1, \ldots, f_s)$ なので、$a \notin \mathbf{V}(\mathrm{LC}'(f_1), \ldots, \mathrm{LC}'(f_s))$ なので、先の拡張定理により $a \in \pi_1(f_1, \ldots, f_s)$ となる。

(証終)

正確に多様体の射影と部分解との関係を記述するものとして、閉包定理がある:「$f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ として、

(a) $\pi_l(\mathbf{V}(f_1, \ldots, f_s))$ を包む最小の多様体は $\mathbf{V}(\langle f_1, \ldots, f_s \rangle_l)$ である。

(b) $\mathbf{V}(f_1, \ldots, f_s) \neq \emptyset$ とする。$\pi_l(\mathbf{V}(f_1, \ldots, f_s))$ は、多様体 $\mathbf{V}(\langle f_1, \ldots, f_s \rangle_l)$ から、これに真に包まれる多様体 W を削ったものを包む:

$$^{\exists} W(\text{: 多様体}, \subsetneq \mathbf{V}(\langle f_1, \ldots, f_s \rangle_l)) \text{:} \underbrace{\mathbf{V}(\langle f_1, \ldots, f_s \rangle_l) - W}_{\neq \emptyset} \subset \pi_l(\mathbf{V}(f_1, \ldots, f_s)) \tag{12}$$

となる。

」

証明

(b) の $l = 1$ のときだけを証明する。$\mathbf{V}(f_1, \ldots, f_s)$ に関して、条件を満たす、この多様体に真に含まれる多様体を探す。

Algorithm 1 削る多様体を探す

```
1: list ⇐ [f_1, ..., f_s]
2: stop ⇐ false
3: while stop = false do
4:   if list ⊂ k[x_2, ..., x_n] then
5:     stop ⇐ true
6:     W ⇐ ∅
7:   else
8:     W ⇐ V(⟨list⟩_1) ∩ V(LC'(list))
9:     if V(⟨list⟩_1) − W ≠ ∅ then
10:      stop ⇐ true
11:    else
12:      list ⇐ [x ↦ x − LT'(x)](list) + LC'(list)
13:    end if
14:  end if
15: end while
```

ただし、LT' は、$k[x_2, \ldots, x_n][x_1]$ とみなしたときの先頭項とする。

- アルゴリズムは停止する: L.3 の停止条件から、L.3〜L.15 のループが 1 回実行されるごとに、必ず L.12 が実行される。この行について、$[x \mapsto x - \mathrm{LT}'(x)](list)$ は、$k[x_2, \ldots, x_n][x_1]$ での先頭項を消しており、$\mathrm{LC}'(list) \subset k[x_2, \ldots, x_n]$ なので、$list$ の最高の ($k[x_2, \ldots, x_n][x_1]$ での) 次数は、0 より大きければ真に減少する。
  このことから、$list$ の次数はあるところで 0 に到達する。つまり、$list$ の元がどれも $k[x_2, \ldots, x_n]$ に属することになる。すると、その次のループのなかで、L.4 の条件が真となり、L.5 で $stop = true$ となるので、L.4 の停止条件を満たすようになり、アルゴリズムは停止する。

- $\mathbf{V}(list)$ は変わらない: $list$ が変化するのは L.12 でのみであり、このときには、
  (a) $list_b \notin k[x_2, \ldots, x_n]$
  (b) $W_a = \mathbf{V}(\langle list_b \rangle_1) \cap \mathbf{V}(\mathrm{LC}'(list_b))$
  (c) $\mathbf{V}(\langle list_b \rangle_1) - W_a = \emptyset$
  (d) $list_a = [x \mapsto x - \mathrm{LT}'(x)](list_b) + \mathrm{LC}'(list_b)$
  となっている。
  まず、$\mathbf{V}(list_b) = \mathbf{V}(list_b + \mathrm{LC}'(list_b))$ を示す。(b),(c) より、
  $$\mathbf{V}(\langle list_b \rangle_1) \subset W_a = \mathbf{V}(\langle list_b \rangle_1) \cap \mathbf{V}(\mathrm{LC}'(list_b)) \subset \mathbf{V}(\mathrm{LC}'(list_b)) \tag{13}$$
  $\langle list_b \rangle \supset \langle list_b \rangle_1$ なので、$\mathbf{V}(list_b) \subset \mathbf{V}(\langle list_b \rangle_1)$ である。よって、
  $$\mathbf{V}(list_b) \subset \mathbf{V}(\mathrm{LC}'(list_b)) \tag{14}$$
  である。よって、
  $$\mathbf{V}(list_b) = \mathbf{V}(\mathrm{LC}'(list_b)) \cap \mathbf{V}(list_b) = \mathbf{V}(\mathrm{LC}'(list_b) + list_b) \tag{15}$$
  である。
  そして、
  $$\left\langle \mathrm{LC}'(list_b) + list_b \right\rangle = \left\langle \mathrm{LC}'(list_b) + ([x \mapsto x - \mathrm{LT}'(x)](list_b)) \right\rangle = \langle list_a \rangle \tag{16}$$
  なので、
  $$\mathbf{V}(list_a) = \mathbf{V}(\mathrm{LC}'(list_b) + list_b) = \mathbf{V}(list_b) \tag{17}$$
  である。
- $\pi_1(\mathbf{V}(list))$ は変わらない: $\mathbf{V}(list)$ が変わらないことから直ちに従う。
- $\mathbf{V}(\langle list \rangle_1)$ は変わらない: $list$ が変化する、すなわち L.12 が実行されるときを考えればよく、「$\mathbf{V}(list)$ は変わらない」の状況と同じとしてよい。閉包定理より、$\mathbf{V}(\langle list_a \rangle_1)$ は $\pi_1(\mathbf{V}(list_a))$ を包む最小の多様体である。また、$\mathbf{V}(list_b)$ は $\pi_1(\mathbf{V}(list_b))$ を包む最小の多様体である。しかし、先に示したことより、「$\pi_1(\mathbf{V}(list))$ は変わらない」ので、$\pi_1(\mathbf{V}(list_b)) = \pi_1(\mathbf{V}(list_a))$ である。よって、$\mathbf{V}(\langle list_a \rangle_1)$ も $\mathbf{V}(\langle list_b \rangle_1)$ も同じ多様体 $\pi_1(\mathbf{V}(list_b)) = \pi_1(\mathbf{V}(list_a))$ を包む最小の多様体なので、
  $$\mathbf{V}(\langle list_a \rangle_1) = \mathbf{V}(\langle list_b \rangle_1) \tag{18}$$
  である。
- 停止時点で、$W \subsetneq \mathbf{V}(\langle f_1, \ldots, f_s \rangle_1)$ となり、W は多様体である。
  - 停止直前に実行されたのが L.5 である: このとき $W = \emptyset$ なのであきらか。
  - 停止直前に実行されたのが L.10 である: このとき $W = \mathbf{V}(\langle list \rangle_1) \cap \mathbf{V}(\mathrm{LC}'(list))$ なので、多様体ではある。
    さらに、W のこの式より、$W \subset \mathbf{V}(\langle list \rangle_1)$ であることも保証される。
    最後に、$W \neq \mathbf{V}(\langle list \rangle_1)$ であることを示せばよいが、そうだとすると L.9 の条件が通過できず矛盾する。
- 停止時点で、W は $\mathbf{V}(\langle f_1, \ldots, f_s \rangle_1) - W \subset \pi_1(\mathbf{V}(f_1, \ldots, f_s))$ となる。
  - 停止直前に実行されたのが L.5 であるとき: $list \subset k[x_2, \ldots, x_n]$ となっている。よって、$\langle list \rangle_1 = \langle list \rangle$ となる。よって、$\mathbf{V}(list)$ は x_1 を使わずに定義されていることわかり、どの部分解 $\mathbf{V}(\langle list \rangle_1)$ も、拡張できること、すなわち $\mathbf{V}(\langle list \rangle_1) = \pi_1(\langle list \rangle)$ がわかる。これまで示してきた不変より、
    $$\begin{aligned} \mathbf{V}(\langle f_1, \ldots, f_s \rangle_1) - W &= \mathbf{V}(\langle f_1, \ldots, f_s \rangle_1) - W && (19)\\ &= \mathbf{V}(\langle list \rangle_1) - W && (20)\\ &= \mathbf{V}(\langle list \rangle_1) && (21)\\ &= \pi_1(\mathbf{V}(list)) && (22)\\ &= \pi_1(\mathbf{V}(f_1, \ldots, f_s)). && (23) \end{aligned}$$
    また、W はあきらかに $\mathbf{V}(\langle f_1, \ldots, f_s \rangle_1)$ に含まれる多様体であり、満たされた。

– 停止直前が L.10 のとき: $list$ に関して、部分解の分解を考えると、$W = \mathbf{V}(\langle list\rangle_1) \cap \mathbf{V}(\mathrm{LC}'(list))$ となるから、

$$\mathbf{V}(\langle list\rangle_1) = \pi_1(\mathbf{V}(list)) \cup W \tag{24}$$

となる。よって、$\mathbf{V}(\langle list\rangle_1) - W \subset \pi_1(\mathbf{V}(list))$ となる。これまで示してきたことより、

$$\begin{aligned}\mathbf{V}(\langle f_1,\dots,f_s\rangle_1) - W &= \mathbf{V}(\langle list\rangle_1) - W &(25)\\ &\subset \pi_1(\mathbf{V}(list)) &(26)\\ &= \pi_1(\mathbf{V}(f_1,\dots,f_s)). &(27)\end{aligned}$$

(証終) (a) は射影を多様体で上から抑え、(b) は多様体の差で下から抑えている。

この定理だと $\pi_1(\mathbf{V}(f_1,\dots,f_s))$ が正確にどういう形をしているかは分からない。実は

$$\pi_1(\mathbf{V}(f_1,\dots,f_s)) = \bigcup_{i=1}^{t}(A_i - B_i) \tag{28}$$

となる多様体 A_i, B_i が存在する、つまり多様体の射影は多様体の差の和で書けることがわかり、このような (？) 集合を構成可能という。あとでやる。

この節で π の記号を整備して、先の節での系を幾何学的に言い直すことができる。すなわち:「$\mathbf{V}(g_1,\dots,g_s)$ について、$\mathrm{LC}'(g_1),\dots,\mathrm{LC}'(g_s)$ のうちで定数 (当然非 0) があるならば、$\pi_1(\mathbf{V}(g_1,\dots,g_s)) = \mathbf{V}(\langle g_1,\dots,g_s\rangle_1)$ となる。」$g_1,\dots,g_s$ のうち 0 があるような場面は、その 0 を外しておけるので考える必要がない。このときは LC' を考えることができなくなってしまう。また、そもそも非 0 の定数があったときには、多様体は空集合をあらわすようになる。このときは射影しても空でありやはり成立している。

3.3 陰関数表示化

パラメタ表示された図形、つまり関数の像を陰関数表示することを考える。ここで、陰関数表示とは、パラメタ表示された図形を包む最小のアフィン多様体を求めることである。図形を包む最小のアフィン多様体ということで、先の閉包定理を利用したいが、そのためにパラメタ表示された図形というのを何かのアフィン多様体の射影として表現できると便利である。そこで、グラフを考える。

k^n 中で多項式で表示された図形を考える。この図形は、$F = (f_1,\dots,f_n)\colon k^m \to k^n$ であらわされており、$f_\bullet \in k[t_1,\dots,t_m]$ とする。グラフへの埋め込み $i\colon k^m \to k^{m+n}$ を、

$$i(t_1,\dots,t_m) = (t_1,\dots,t_m) \oplus F(t_1,\dots,t_m) \tag{29}$$

と定義する。この $i(k^m)$ は $k[t_1,\dots,t_m,x_1,\dots,x_n]$ のアフィン多様体であって、

$$i(k^n) = \mathbf{V}(f_1 - x_1,\dots,f_n - x_n) \tag{30}$$

である。なぜならグラフは、$t_\bullet$ のスロットには $t_\bullet$ がそのまま入っていてほしいし、$x_\bullet$ のスロットには $f(t_1,\dots,t_m)$ が入っていてほしいからである。$x_\bullet$ が F の値域側の文字であることには注意する。ただしここで、$x_\bullet$ は

$$x_i(t_1,\dots,t_m,x_1,\dots,x_n) = x_i \quad (i = 1,\dots,n) \tag{31}$$

という関数 $x_\bullet\colon k^{m+n} \to k$ であり、$f_\bullet$ は $f_\bullet \in k[t_1,\dots,t_m]$ でもあるが、

$$f_i(t_1,\dots,t_m,x_1,\dots,x_n) = f_i(t_1,\dots,t_m) \tag{32}$$

とみなしている。そして、グラフの射影はいままで通り、π_m を考える。すると、

$$\pi_m(t_1,\dots,t_m,x_1,\dots,x_n) = (x_1,\dots,x_n) \tag{33}$$

であるから、$F = \pi_m \circ i$ となった。よって、$F(k^n) = \pi_m \circ i(k^n) = \pi_m(i(k^n))$ となり、パラメタ付けされた図形 $F(k^n)$ は、アフィン多様体 $\mathbf{V}(x_1 - f_1,\dots,x_n - f_n) = i(k^n)$ の射影 $\pi_m(i(k^n))$ としてあらわせた。これで閉包定理を使う準備ができた。

多項式でパラメタ表示された図形を陰関数表示する手法として、次がある:「無限体 k 上の図形の多項式によるパラメタ表示 $F = (f_1, \ldots, f_n) \colon k^m \to k^n$ について、$F(k^m)$ を包む最小のアフィン多様体は $\mathbf{V}(\left\langle \underbrace{x_1 - f_1}_{k[t_1,\ldots,t_m,x_1,\ldots,x_n]}, \ldots, x_n - f_n \right\rangle_m)$ である。」

証明

k が代数的閉体であるときには、$F(k^m) = \pi_m(i(k^m)) = \pi_m(\mathbf{V}\langle f_1 - x_1, \ldots, f_n - x_n\rangle)$ を包む最小の多様体を考えればよいが、閉包定理よりこれは $\mathbf{V}(\langle f_1 - x_1, \ldots, f_n - x_n\rangle_m)$ である。

k を包む代数的閉体 K が存在するので、これをかんがえる (体論)。以降、係数を k とするイデアルを $\langle \bullet \rangle_k$ と書き、多様体を $\mathbf{V}_k(\bullet)$ と書く。また、K についても同様とする。$F(k^n)$ を包む最小の多様体を Z_k とする。このとき、$\pi_m(i(k^n)) \subset Z_k$ であることを示そう。

(証終)

やりなおし。$I = \langle x_1 - f_1, \ldots, x_n - f_n \rangle$ としてある。

証明

$V = \mathbf{V}(I)$ とする。

まず、$\mathbb{C}$ 上で考える。パラメタで表示された図形 $F(k^m)$ は、先のグラフの利用により $\pi_m(i(k^m)) = \pi_m(V)$ と表示される。V はアフィン多様体で、$\pi_m(V)$ はその射影なので、閉包定理によりこれを包む最小の多様体は $\mathbf{V}(I_m)$ である。$\mathbb{C}$ のときは証明おわり。

$k \subset \mathbb{C}$ 上で考える。k は $\mathbb{C}$ の 1 と $+$ を持つので、無限体である。$\mathbb{C}$ 上の多様体と k 上の多様体を区別するため、$\mathbf{V}_{\mathbb{C}}$, $\mathbf{V}_k$ を考える。$V_k = \mathbf{V}_k(I)$, $V_{\mathbb{C}} = \mathbf{V}_{\mathbb{C}}(I)$ としてある。

$$F(k^m) \overset{\boxed{\text{グラフの射影}}}{=} \pi_m(V_k) \overset{\boxed{\text{補題}}}{\subset} \mathbf{V}_k(I_m). \tag{34}$$

これで $F(k^m) \subset \mathbf{V}_k(I_m)$ は示された。あとは最小性を示せばよい。$F(k^m)$ を包もうとすると一緒に $\mathbf{V}_k(I_m)$ も包んでしまうことを示せばよい。$Z_k = \mathbf{V}_k(g_1, \ldots, g_s) \subset k^n$ を $F(k^m)$ を包む多様体とする。各 $i = 1, \ldots, s$ について、$F(k^m) \subset Z_k$ なので g_i は $F(k^m)$ 上消えてしまう。よって、$g_i \circ F$ は k^m を消す。$g_i \in k[x_1, \ldots, x_n]$ であり、$F \in k[t_1, \ldots, t_m]$ なので、$g_i \circ F \in k[t_1, \ldots, t_m]$ であり、$g_i \circ F \in k[t_1, \ldots, t_m]$ である。k は無限体だと先に言ったので、$g_i \circ F$ は多項式として 0 である。多項式として 0 なので、$(g_i \circ F)(\mathbb{C}^m) = 0$ であり、g_i は $F(\mathbb{C}^m)$ 上で消える。よって、$F(\mathbb{C}^m) \subset Z_{\mathbb{C}} = \mathbf{V}_{\mathbb{C}}(g_1, \ldots, g_s)$ である。$\mathbb{C}$ の場合の定理より、パラメタ表示 $F(\mathbb{C}^m)$ を包む最小の多様体は $\mathbf{V}_{\mathbb{C}}(I_m)$ であるから、$\mathbf{V}_{\mathbb{C}}(I_m) \subset Z_{\mathbb{C}}$ である。両方で k^n の結びをとって、

$$\mathbf{V}_k(I_m) = \mathbf{V}_{\mathbb{C}}(I_m) \cap k^n \subset Z_{\mathbb{C}} \cap k^n = Z_k \tag{35}$$

である。これで、$F(k^m)$ を含む多様体のうち最小のものは $\mathbf{V}_k(I_m)$ であることが示された。

一般の体については、その代数閉体を考えればよい。

(証終) 登場人物:

- k:無限体
- $F = (f_1, \ldots, f_n) \colon k^m \to k^n$:図形のパラメタ。
- $I = \langle x_1 - f_1, \ldots, x_n - f_n \rangle$
- $V = \mathbf{V}(I) \subset k^{n+m}$、$F$ のグラフ
- $V_k = \mathbf{V}_k(I)$:体 k をとったときの F のグラフ (k 多様体)
- $V_{\mathbb{C}} = \mathbf{V}_{\mathbb{C}}(I)$:体 $\mathbb{C}$ をとったときの F のグラフ ($\mathbb{C}$ 多様体)
- Z_k:$F(k^m)$ を包む自由な多様体。
- $g_1, \ldots, g_s \in k[t_1, \ldots, t_m]$:$Z_k$ を定義する自由な多項式。
- $Z_{\mathbb{C}}$:同じ $g_1, \ldots, g_s$ で定義される、Z_k に付随する多様体。Z_k より大きい。

次に有理パラメタ表示の陰関数表示を考える。

$$x_1 = \frac{f_1}{g_1}, \ldots, x_n = \frac{f_n}{g_n} \tag{36}$$

の陰関数表示を考える。分母を処理するために、$g = g_1 \ldots g_n$ とし、パラメタ y を次のように導入し、$k[y, t_1, \ldots, t_m, x_1, \ldots, x_n]$ で考える。「$g(x)$ は 0 になる $\iff$ $g_1(x), \ldots, g_n(x)$ の 1 つ以上は 0 になる」であり、「$g(x)$ は nonzero $\iff$ $g_1(x), \ldots, g_n(x)$ はどれも 0 にならない」となる。$W = \mathbf{V}(g)$ とする。

$$J = \langle g_1 x_1 - f_1, \ldots, g_n x_n - f_n, 1 - gy \rangle \tag{37}$$

とする ($1 - gy$ で W を避ける)。

$$j(t_1, \ldots, t_m) = (\frac{1}{g(t_1, \ldots, t_m)}, t_1, \ldots, t_m, \frac{f_1(t_1, \ldots, t_m)}{g_1(t_1, \ldots, t_m)}, \ldots, \frac{f_n(t_1, \ldots, t_m)}{g_n(t_1, \ldots, t_m)}). \tag{38}$$

こうしておくと、実は $j(k^m - W) = \mathbf{V}(J)$ となる。

証明

- $\subset$: あきらか。実際、$(t_1, \ldots, t_m) \in k^m - W$ とする。

$$j(t_1, \ldots, t_m) = (\underbrace{\frac{1}{g(t_1, \ldots, t_m)}}_{\Rightarrow y}, t_1, \ldots, t_m, \underbrace{\frac{f_1(t_1, \ldots, t_m)}{g_1(t_1, \ldots, t_m)}}_{\Rightarrow x_1}, \ldots, \underbrace{\frac{f_n(t_1, \ldots, t_m)}{g_n(t_1, \ldots, t_m)}}_{\Rightarrow x_n}). \tag{39}$$

  これは J の生成元を考えれば、$\mathbf{V}(J)$ に属する。
- $\supset$: $(y, t_1, \ldots, t_m, x_1, \ldots, x_n) \in \mathbf{V}(J)$ とする。$yg(t_1, \ldots, t_m) = 1$ となるので $g(t_1, \ldots, t_m)$ が nonzero で、$g_1(t_1, \ldots, t_m), \ldots, g_n(t_1, \ldots, t_m)$ はどれも nonzero になる。よって割り算が考えられて、$x_i = \frac{f_i(t_1, \ldots, t_m)}{g_i(t_1, \ldots, t_m)}$ を考えられる。すると、$j(t_1, \ldots, t_m) = (y, t_1, \ldots, t_m, x_1, \ldots, x_n)$ となり、$(y, t_1, \ldots, t_m, x_1, \ldots, x_n) \in j(k^m - W)$ となる。

(証終) $F = \pi_{m+1} \circ j$ なので、

$$F(k^m - W) = \pi_{m+1}(j(k^m - W)) = \pi_{m+1}(\mathbf{V}(J)) \tag{40}$$

となる。これで、パラメタ表示の図形をアフィン多様体の射影であらわせたので閉包定理が使える。有理陰関数表示化:「k を無限体とする。$F \colon k^m - W \to k^n$ を有理関数によるパラメタ付けとする。J をイデアル

$$J = \langle g_1 x_1 - f_1, \ldots, g_n x_n - f_n, 1 - gy \rangle \subset k[y, t_1, \ldots, t_m, x_1, \ldots, x_n] \tag{41}$$

とする。$g = g_1 \ldots g_n$ とした。$J_{m+1} = J \cap k[x_1, \ldots, x_n]$ を $(m+1)$ 次消去イデアルとする。このとき、$\mathbf{V}(J_{m+1})$ は $F(k^m - W)$ を含む k^n の最小の多様体である。」

証明

$k = \mathbb{C}$ のときには $\pi_{m+1}(\mathbf{V}(J)) = F(k^m - W)$ と閉包定理よりあきらか。

$k \subsetneq \mathbb{C}$ とする。k は無限体である。$\mathbb{C}$ 上の多様体と k 上の多様体を区別するため、$\mathbf{V}_{\mathbb{C}}, \mathbf{V}_k$ を考える。$V_k = \mathbf{V}_k(J)$, $V_{\mathbb{C}} = \mathbf{V}_{\mathbb{C}}(J)$ とする。

$$F(k^m - W) \overset{\text{さっきの}}{=} \pi_m(V_k) \overset{\text{射影が小さい補題}}{\subset} \mathbf{V}_k(J_{m+1}). \tag{42}$$

これで $F(k^m - W) \subset \mathbf{V}_k(J_{m+1})$ は示された。あとは最小性を示せばよい。$Z_k = \mathbf{V}_k(h_1, \ldots, h_s) \subset k^n$ を $F(k^m - W)$ を包む多様体とする。各 $i = 1, \ldots, s$ について、$F(k^m - W) \subset Z_k$ なので、h_i は $F(k^m - W)$ 上消えてしまう。よって、$h_i \circ F$ は $k^m - W$ 上消える。仮に $h_i \circ F$ が 0 多項式でないとする。g は 0 多項式ではないので、$(h_i \circ F) \cdot g$ は 0 多項式ではない。しかし、$h_i \circ F$ は $k^m - W$ 上消え、g は W 上消えるので、$(h_i \circ F) \cdot g$ は k^m で消える。無限体上で 0 関数になる多項式は 0 多項式なので $(h_i \circ F) \cdot g$ は 0 多項式である。これは矛盾であり、$h_i \circ F$ は 0 多項式である。

よって、$(h_i \circ F)(\mathbb{C}^m) = 0$ であり、h_i は $F(\mathbb{C}^m)$ 上で消える。よって、$F(\mathbb{C}^m) \subset Z_{\mathbb{C}} = \mathbf{V}_{\mathbb{C}}(I_m) \subset Z_{\mathbb{C}}$ である。両方で k^n の結びをとって、

$$\mathbf{V}_k(J_{m+1}) = \mathbf{V}_{\mathbb{C}}(J_{m+1}) \cap k^n \subset \mathbb{Z}_{\mathbb{C}} \cap k^n = Z_k \tag{43}$$

である。これで、$F(k^m)$ を含む多様体のうち最小のものは $\mathbf{V}_k(J_{m+1})$ であることが示された。

(証終)

3.4 特異点と包絡線

略

3.5 因数分解の一意性と終結式

定義 1: k を体とする。$f \in k[x_1, \ldots, x_n]$ が既約であるとは、f が定数でない $k[x_1, \ldots, x_n]$ の 2 つの積で書けないことである[*1]。

命題 2:すべての定数でない多項式 $f \in k[x_1, \ldots, x_n]$ は、k 上で既約な多項式の積に分解できる。

証明

(1) Define f: $f \in k[x_1, \ldots, x_n]$ とする。既約ならば終わっているので、既約でないとする。
(2) Define g, h: 定数でない $g, h \in k[x_1, \ldots, x_n]$ で $f = gh$ と分解する。
(3) $\deg g < \deg f$ かつ $\deg h < \deg f$ となっている。
(4) g, h が既約でないならさらに (2) のように分解する。これを繰替えすると次数が落ちていくので、どこかで停止し既約に分解される。

(証終)

定理 3: $f \in k[x_1, \ldots, x_n]$ を k 上既約な多項式とし、f は積 gh を割り切ると仮定する。ここで、$g, h \in k[x_1, \ldots, x_n]$ である。このとき、f は g か h かのどちらかを割り切る。

証明

(1) $\Longrightarrow$: 帰納法にする。$n = 1$ であるとする。
(2) f は gh を割り切るとする (仮定)。
(3) Define p: $p = \mathrm{GCD}(f, g)$ とする。
(4) $\Longrightarrow$: p が定数でないとする。
(5) (3) で p は GCD なので、$p|f$ であり、仮定より f は既約なので p は定数か f かだが、(4) より f は p の定数倍 ($f \simeq p$) である。
(6) (3) で p は GCD なので $p|g$ であり、(5) より $f|g$ である。
(7) (4) おわり。
(8) $\Longrightarrow$: p は定数とする。$p = 1$ としてよい[*2]。
(9) Get A, B: (3) より、$Af + Bg = 1$ となる $A, B \in k[x_1]$ が存在する。
(10) (9) に h をかける。

$$h = h(Af + Bg) = Ahf + Bgh. \tag{44}$$

(11) (2) より $f|gh|Bgh$ で、$f|Ahf$ なので、(9) より $f|h$ となる。
(12) (8) おわり。
(13) (1) おわり。$n = 1$ で示された。
(14) $\Longrightarrow$: $n - 1$ で成立すると仮定する。

[*1] $f = gh$ と書いたとき $g = const.$ か $h = const.$ となること。
[*2] GCD は定数倍はどうでもいい。

(15) Def u: $u \in k[x_2, \ldots, x_n]$ は既約で、$u|gh$ とする。(u という特殊な f について結論「$u|g$ または $u|h$ を示す。」)
(16) $a_\bullet, b_\bullet$: を $g = \sum_{i=0}^{l} a_i x_1^i$ とし、$h = \sum_{i=0}^{m} x_1^i$ とする。
(17)

(証終)

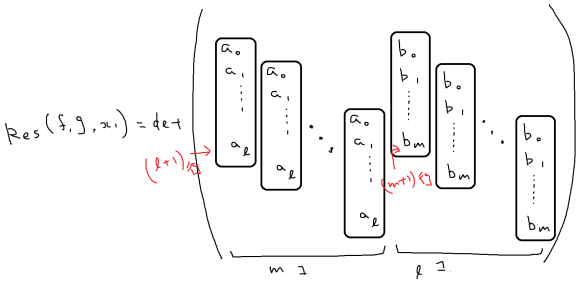
3.6 終結式と拡張定理

終結式の定義: $f, g \in k[x_1, \ldots, x_n]$ として、

$$f = a_0 x_1^l + \cdots + a_l, \quad a_0 \neq 0 \tag{45}$$
$$g = b_0 x_1^m + \cdots + b_m, \quad b_0 \neq 0 \tag{46}$$

とする。これについて、終結式を (図 1)1431709536336.png 参照.

図 1　1431709536336.png



とする。
命題 1: $f, g \in k[x_1, \ldots, x_n]$ の x_1 に関する次数が正であると仮定する[*3]。

(i) $\mathrm{Res}(f, g, x_1)$ は x_1 を消去した 1 次の消去イデアル $\langle f, g \rangle \cap k[x_2, \ldots, x_n]$ に含まれる。
(ii) $\mathrm{Res}(f, g, x_1) = 0$ であることと、f と g が $k[x_1, \ldots, x_n]$ において x_1 に関する次数が正の共通因子を持つことは同値である。

証明
(i) を示す。

(1) Get $l, m, a_\bullet, b_\bullet$:

$$f = a_0 x^l + \cdots + a_l \tag{47}$$
$$g = b_0 x^m + \cdots + b_m \tag{48}$$

ただし、$a_\bullet, b_\bullet \in k[x_2, \ldots, x_n]$ と書く。
(2) 終結式 $\mathrm{Res}(f, g, x_1)$ は定義より $a_\bullet, b_\bullet$ の積と和なので、$\mathrm{Res}(f, g, x_1) \in k[x_2, \ldots, x_n]$ である。
(3) Get A, B: $Af + Bg = \mathrm{Res}(f, g, x_1)$ となる $A, B \in (k[x_2, \ldots, x_n])[x_1]$ が存在する[*4] 。
(4) (3) より、$\mathrm{Res}(f, g, x_1) = Af + Bg \in \langle f, g \rangle$ である。

[*3] $\deg(f; x_1) > 0$?

[*4] $\mathrm{Res}(f, g, x_1) = 0$ のときは $A = B = 0$ でよい。$\mathrm{Res}(f, g, x_1) \neq 0$ のときには、$f, g \in k(x_2, \ldots, x_n)[x_1]$ とする。$A = c_0 x^{l-1} + \cdots + c_{l-1}$, $B = d_0 x^{m-1} + \cdots + d_{m-1}$ と、1 つ低い次数で $c_\bullet, d_\bullet \in k(x_2, \ldots, x_n)$ の変数で表しておく。$Af + Bg = 1$ という方程式を考え、係数比較して $\mathrm{Syl}(f, g, x_1)(c_0, \ldots, c_{l-1}, d_0, \ldots, d_{m-1})^T = (0, \ldots, 1)^T$ という線型方程式を得る。$\mathrm{Res}(f, g, x_1) \neq 0$ なのでこれは一意に解けて、クラメールの公式より各 $c_\bullet$, $d_\bullet$ は $\det(\mathrm{Syl}(f, g, x_1)$のある行を$(0, \ldots, 1)^T$に交換)$/\mathrm{Res}(f, g, x_1)$ である。よって、A, B の係数はすべて $(\mathrm{Syl}(f, g, x_1)$の積と和)$/\mathrm{Res}(f, g, x_1)$ である。よって、$A = \widetilde{A}/\mathrm{Res}(f, g, x_1)$, $B = \widetilde{B}/\mathrm{Res}(f, g, x_1)$ で、$\widetilde{A}, \widetilde{B}$ は $\mathrm{Syl}(f, g, x_1)$ の積と和となるものがある。よって、$Af + Bg = 1$ にこれを入れて $\widetilde{A}f + \widetilde{B}g = \mathrm{Res}(f, g, x_1)$ となる。

(5) (2)(4) より、$\mathrm{Res}(f,g,x_1) \in \langle f,g\rangle \cap k[x_2,\ldots,x_n]$ となる。

(ii) を示す。

(1) Section5-Prop8 [*5]を $f,g \in k[x_1,\ldots,x_n] \subset k(x_2,\ldots,x_n)[x_1]$ に適用し、「$\mathrm{Res}(f,g,x_1)=0 \iff f$ と g は x_1 に関して正の次数を持つ $k(x_2,\ldots,x_n)[x_1]$ の多項式を共通因子として持つ」となる。
(2) Section5-Cor4 を適用して、「f,g は $k(x_2,\ldots,x_n)[x_1]$ で共通因子を持つ $\iff$ f,g は $k[x_1,\ldots,x_n]$ で共通因子を持つ」となる。
(3) (1),(2) より、「$\mathrm{Res}(f,g,x_1)=0 \iff$ f,g は $k[x_1,\ldots,x_n]$ で共通因子を持つ」となる。

(証終)

系 2:$f,g \in \mathbb{C}[x]$ とする。このとき、$\mathrm{Res}(f,g,x)=0$ であることと、f と g が $\mathbb{C}$ において共通根を持つことは同値である。」

証明

$\mathbb{C}[x]$ で 2 つの共通因子を持つことと、共通根を持つことは同値である。

(証終)

命題 3:$f,g \in \mathbb{C}[x_1,\ldots,x_n]$ に対して、$a_0,b_0 \in k[x_2,\ldots,x_n]$ を

$$f = a_0x^l + \cdots + a_l, \quad a_0 \neq 0 \tag{49}$$
$$g = b_0x^m + \cdots + b_m, \quad b_0 \neq 0. \tag{50}$$

ととる。もし $\mathrm{Res}(f,g,x_1) \in \mathbb{C}[x_2,\ldots,x_n]$ が $(c_2,\ldots,c_n) \in \mathbb{C}^{n-1}$ において消えるとすると次が成立する。

(i) a_0 または b_0 が $(c_2,\ldots,c_n) \in \mathbb{C}^{n-1}$ で消える。
(ii) $c_1 \in \mathbb{C}$ が存在して、f と g は $(c_1,\ldots,c_n) \in \mathbb{C}^n$ で消える。

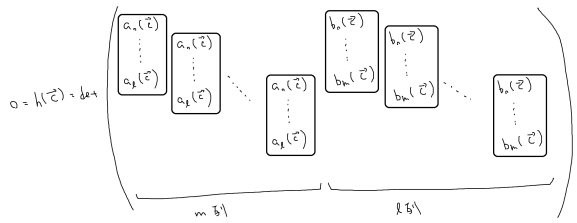
証明

(1) Def $\mathbb{c}$: $\mathbb{c} = (c_2,\ldots,c_n)$ とする。
(2) $\Longrightarrow$: $a_0(\mathbb{c}) \neq 0$ かつ $b_0(\mathbb{c}) \neq 0$ だとする。(結論の片方を持ってくる。)
(3) (2) の仮定より、

$$f(x_1,\mathbb{c}) = a_0(\mathbb{c})x_1^l + \cdots + a_l(\mathbb{c}), \quad a_0(\mathbb{c}) \neq 0 \tag{51}$$
$$g(x_1,\mathbb{c}) = b_0(\mathbb{c})x_1^m + +b_m(\mathbb{c}), \quad b_0(\mathbb{c}) \neq 0 \tag{52}$$

となっている。
(4) Def h: $h = \mathrm{Res}(f,g,x_1)$ とする。
(5) 仮定より $h = \mathrm{Res}(f,g,x_1) = 0$ となる。
(6) (図 2)1431792619123.png 参照.

図 2　1431792619123.png



(7) f,g の $a_\bullet, b_\bullet$ の表現より、$f(x_1,\mathbb{c})$ と $g(x_1,\mathbb{c})$ の終結式は、上の行列式である。

[*5] 1 変数多項式について、共通因子と終結式が消えることの同値

(8) 上 2 つより、

$$0 = h(\mathbb{c}) = \mathrm{Res}(f(x_1, \mathbb{c}), g(x_1, \mathbb{c}), x_1). \tag{53}$$

(9) Get c_1: 系 2 より、$f(x_1, \mathbb{c})$ と $g(x_1, \mathbb{c})$ は共通根を持つ。この x_1 を $c_1 = x_1$ とおく。
(10) (9) より、$f(c_1, \mathbb{c}) = g(c_1, \mathbb{c}) = 0$ となる。c_1 が求めるものだった。
(11) (2) おわり。前件を後ろに否定して「または」で結論を得る。

(証終)

定理 4(2 つの多項式に対する拡張定理): $I = \langle f, g \rangle \subset \mathbb{C}[x_1, \ldots, x_n]$ とし、I_1 を I の 1 次の消去イデアルとする。また、$a_0, b_0 \in \mathbb{C}[x_2, \ldots, x_n]$ を

$$f = a_0 x^l + \ldots a_l, \quad a_0 \neq 0 \tag{54}$$
$$g = b_0 x^m + \ldots b_m, \quad b_0 \neq 0 \tag{55}$$

のものとする。部分解 $(c_2, \ldots, c_n) \in \mathbf{V}(I_1)$ があるとする。もし、$(c_2, \ldots, c_n) \notin \mathbf{V}(a_0, b_0)$ ならば、$c_1 \in \mathbb{C}$ が存在して $(c_1, \ldots, c_n) \in \mathbf{V}(I)$ となる[*6]。

証明

(1) Def $\mathbb{c}$: $\mathbb{c} = (c_2, \ldots, c_n)$ とする。
(2) 命題 1 より、$\mathrm{Res}(f, g, x_1) \in I_1$ となる。
(3) 上より、$\mathbb{c} = (c_2, \ldots, c_n) \in \mathbf{V}(I_1)$ なので、終結式 $\mathrm{Res}(f, g, x_1)$ は $\mathbb{c}$ で消える。
(4) $\Longrightarrow$: $a_0(\mathbb{c}) \neq 0$ かつ $b_0(\mathbb{c}) \neq 0$ とする。
(5) Get c_1: 命題 3 より拡張した c_1 がある。$(c_1, \mathbb{c}) \in \mathbf{V}(f, g)$ となる。
(6) (3) おわり。
(7) $\Longrightarrow$: $a_0(\mathbb{c}), b_0(\mathbb{c})$ の一方が 0 でもう一方が 0 でないとする。$a_0(\mathbb{c}) \neq 0$ かつ $b_0(\mathbb{c}) = 0$ として一般性をうしなわない。
(8) Def N: N を十分大きいとする。$x_1^N f$ の x_1 についての次数は g の x_1 についての次数より大きい。
(9) $\langle f, g \rangle = \langle f, g + x_1^N \rangle$ となる。
(10) $g + x_1^N f$ の x_1 についての LT は a_0 になっている。この係数は (7) より $a_0(\mathbb{c}) \neq 0$ である。
(11) Get c_1: 上より (4)-(6) が $f, g + x_1^N f$ に適用でき、$(c_1, \mathbb{c}) \in \mathbf{V}(f, g + x_1^N f)$ となる。
(12) 上と (9) より、$(c_1, \mathbb{c}) \in \mathbf{V}(f, g)$ となる。
(13) (7) おわり。
(14) (4)-(6),(7)-(13) が示されたものだった。

(証終)

一般終結式を定義する。3 変数以上に対する終結式を定義したかった。$f_1, \ldots, f_s$ の一般終結式を、変数 $x_1, \ldots, x_n$ に $u_2, \ldots, u_s$ を追加して、

$$\mathrm{Res}(f_1, u_2 f_2 + \cdots + u_s f_s, x_1) = \sum_{\alpha} h_\alpha(x_2, \ldots, x_n) u^\alpha \tag{56}$$

と書いたときの h_α たちと定義する[*7]。

定理 5: 拡張定理。イデアル $I = \langle f_1, \ldots, f_s \rangle \subset k[x_1, \ldots, x_n]$ をとり、I_1 を I の 1 次の消去イデアルとする。各 $1 \leq i \leq s$ にたいして、f_i を次の形に書く[*8]。

$$f_i = g_i(x_2, \ldots, x_n) x_1^{N_i} + (x_1\text{の次数が} < N_i\text{である項}). \tag{57}$$

ここで、$N_i \geq 0$ であり、$g_i \in \mathbb{C}[x_2, \ldots, x_n]$ は 0 でない。部分解 $(c_2, \ldots, c_n) \in \mathbf{V}(I_1)$ であると仮定する。もし $(c_2, \ldots, c_n) \notin \mathbf{V}(g_1, \ldots, g_s)$ であるならば、$c_1 \in \mathbb{C}$ が存在して、$(c_1, \ldots, c_n) \in \mathbf{V}(I)$ となる。

[*6] 拡張できた。
[*7] f_1, f_2 なら u_2 だけ追加する。α は 1 個になって、$\mathrm{Res}(f_1, u_2 f_2, x_1) = h_{e_2}(x_2, \ldots, x_n) u^{\alpha_2}$ となる。
[*8] $g_i \in k[x_2, \ldots, x_n]$ は f の x_1 に関する最高次

証明

(1) Def $\mathbb{c}$: $\mathbb{c} = (c_2, \ldots, c_n)$ とする。

(2) $(f_1(x_1, \mathbb{c}), \ldots, f_s(x_1, \mathbb{c})$ の共通根を求めたい。$)$

(3) $\Longrightarrow$: $s \geq 3$ とする。

(4) 仮定の「多様体に属さない」の仮定より、$\mathbb{c} \notin \mathbf{V}(g_1, \ldots, g_s)$ とする。一般性を失なわず、$g_1(\mathbb{c}) \neq 0$ と仮定してよい[*9]。

(5) Get h_α: $f_1, \ldots, f_s$ の一般終結式を名付ける。

$$\mathrm{Res}(f_1, u_2 f_2 + \cdots + u_s f_s, x_1) = \sum_\alpha h_\alpha u^\alpha \tag{58}$$

とする。

(6) Get A, B: 命題 1 の終結式の性質より、$A, B \in \mathbb{C}[u_2, \ldots, u_s, x_1, \ldots, x_n]$ で

$$A f_1 + B(u_2 f_2 + \cdots + u_s f_s) = \mathrm{Res}(f_1, u_2 f_2 + \cdots + u_s f_s, x_1) \tag{59}$$

となるものが存在する。

(7) Get $A_\bullet, B_\bullet$: $A = \sum_\alpha A_\alpha u^\alpha, \quad B = \sum_\beta B_\beta u^\beta$ とおく。ここで、$A_\alpha, B_\beta \in \mathbb{C}[x_1, \ldots, x_n]$ である。

(8) $(h_\alpha \in \langle f_1, \ldots, f_s \rangle = I$ を示す。$)$

(9) Def $e_\bullet$:

$$e_2 = (1, 0, \ldots, 0), \ldots, e_s = (0, \ldots, 0, 1) \tag{60}$$

とする。ここで長さは $n - 1$。

(10) (9) の定義を使って、

$$u_2 f_2 + \cdots + u_s f_s = \sum_{i \geq 2} u^{e_i} f_i. \tag{61}$$

(11)

$$\sum_\alpha h_\alpha u^\alpha \overset{\boxed{(5),(6),(10)}}{=} (\sum_\alpha A_\alpha u^\alpha) f_i + (\sum_\beta B_\beta u^\beta)(\sum_{i \geq 2} u^{e_i} f_i) \tag{62}$$

$$= \sum_\alpha (A_\alpha f_1) u^\alpha + \sum_{i \geq 2,} B_\beta f_i u^{\beta + e_i} \tag{63}$$

$$= \sum_\alpha (A_\alpha f_1) u^\alpha + \sum_\alpha (\sum_{\substack{i \geq 2, \beta \\ \beta + e_i = \alpha}} B_\beta f_i) u^\alpha \tag{64}$$

$$= \sum_\alpha (A_\alpha f_1 + \sum_{\substack{i \geq 2, \beta \\ \beta + e_i = \alpha}} B_\beta f_i) u^\alpha. \tag{65}$$

(12) Fix α.

(13) 上の両辺の u^α 係数を比較し[*10]、

$$h_\alpha = A_\alpha f_1 + \sum_{\substack{i \geq 2, \beta \\ \beta + e_i = \alpha}} B_\beta f_i. \tag{66}$$

(14) $I = \langle f_1, \ldots, f_s \rangle$ だったので、上の式は h_α をこれらの結合であらわしていることから $h_\alpha \in I$ である。

(15) Free (12), α。任意の $\alpha \in \mathbb{Z}_{\geq 0}^{n-1}$ について、$h_\alpha \in I$ となる。

(16) (5) より、$h_\alpha \in \mathbb{C}[x_2, \ldots, x_n]$ だったので、上とあわせて $h_\alpha \in I_1$ となる。

(17) 仮定 (部分解) より、$\mathbb{c} \in \mathbf{V}(I_1)$ なので、上より $h_\alpha(\mathbb{c}) = 0$ である。

[*9] $g_1(\mathbb{c}) = \cdots = g_s(\mathbb{c}) = 0$ だとするとおかしいので少なくとも 1 個は nonzero でないといけず、それを 1 番にした。

[*10] decode

(18) Def h: $h = \mathrm{Res}(f_1, u_2 f_2 + \cdots + u_s f_s, x_1)$ とする。

(19)

$$h(\mathfrak{c}) \overset{\boxed{(18)}}{=} \mathrm{Res}(f_1, u_2 f_2 + \cdots + u_s f_s, x_1)(\mathfrak{c}) \overset{\boxed{(5)}}{=} \sum_{\alpha} (h_\alpha u^\alpha)(\mathfrak{c}) \overset{\boxed{(17)}}{=} 0. \tag{67}$$

すなわち、終結式が $\mathfrak{c}$ で消える。

(20) Def $h(\mathfrak{c}, u_2, \ldots, u_n)$:$\mathbb{C}[x_1, u_2, \ldots, u_s]$ の多項式 $h(\mathfrak{c}, u_2, \ldots, u_n)$ を、終結式 h に $(x_2, \ldots, x_n) \leftarrow \mathfrak{c}$ を代入して得られた多項式と定義する。(実際は x_1 もないよね？)

(21) (19),(20) より、$h(\mathfrak{c}, u_2, \ldots, u_n) = 0$ となる。

(22) $\Longrightarrow$: $g_2(\mathfrak{c}) \neq 0$ かつ f_2 は変数 x_1 に関する次数が $f_3, \ldots, f_s$ のどれよりも大きいとする。

(23)

$$h(\mathfrak{c}, u_2, \ldots, u_n) = \mathrm{Res}(f_1(x_1, \mathfrak{c}), u_2 f_2(x_1, \mathfrak{c}) + \cdots + u_s f_s(x_1, \mathfrak{c}), x_1). \tag{68}$$

(「終結式を計算してから代入」と「代入してから終結式」が一致する) これは、仮定より f_1 の最高次が $\mathfrak{c}$ で消えないこと、(22) の仮定より $u_2 f_2 + \cdots + u_s f_s$ の最高次が $u_2 g_2$ であり、再び (22) の仮定より $g_2(\mathfrak{c} \neq 0$ であることから従う。

(24) (19) と (23) より、

$$\mathrm{Res}(f_1(x_1, \mathfrak{c}), u_2 f_2(x_1, \mathfrak{c}) + \cdots + u_s f_s(x_1, \mathfrak{c}), x_1) = 0. \tag{69}$$

(25) Get F: $f_1(x_1, \mathfrak{c})$ も $u_2 f_2(x_1, \mathfrak{c}) + \cdots + u_s f_s(x_1, \mathfrak{c})$ もどちらも $k[x_1, u_2, \ldots, u_s]$ の元なので、命題 1 が使えて (24) より、この 2 式に x_1 について正の次数を持った共通因子 F が得られる。

(26) F の定義より、F は $f_1(x_1, \mathfrak{c})$ を割り切る。よって、$F \in \mathbb{C}[x_1]$ である。

(27) F は $u_2 f_2(x_1, \mathfrak{c}) + \cdots + u_s f_s(x_1, \mathfrak{c})$ を割り切るが、$f_\bullet(x_1, \mathfrak{c}) \in \mathbb{C}[x_1]$ であることと、$u_\bullet \in \mathbb{C}[u_2, \ldots, u_n]$ であることから (正確には係数比較して)、F は $f_2(x_1, \mathfrak{c}), \ldots, f_s(x_1, \mathfrak{c})$ をすべて割り切る。

(28) (26),(27) より、F は $f_1(x_1, \mathfrak{c}), \ldots, f_s(x_1, \mathfrak{c})$ すべての、x_1 について正の次数を持つ共通因子である。

(29) Def c_1: (25) より F は x_1 について正の次数を持つので、F の根 $c_1 \in \mathbb{C}$ が存在する (代数閉体)。

(30) (27),(28) より、c_1 は $f_i(x_1, \mathfrak{c})$ すべての共通根であり、部分解 $\mathfrak{c}$ が拡張されて $(c_1, \mathfrak{c})$ となった。

(31) (22) おわり。

(32) $\Longrightarrow$: (22) がみたされないとき:

(33) Get N: 十分大きい

(34) (33) より、$f_2 + x_1^N f_1$ の x_1 に関する最高次の係数は g_1 である。

(35) (33) より、$f_2 + x_1^N f_1$ の x_1 に関する次数は $f_3, \ldots, f_s$ のどれよりも大きい。

(36) Get c_1: 上 2 つより、(22)-(31) の議論が $f_1, f_2 + x_1^N f_1, f_3, \ldots, f_s$ に適用でき、これに関する $\mathfrak{c}$ の拡張 c_1 を得る。

(37) 上より、

$$f_1(x_1, \mathfrak{c}) = 0 \tag{70}$$
$$(f_2 + x^N f_1)(x_1, \mathfrak{c}) = 0 \tag{71}$$
$$\vdots \tag{72}$$
$$f_s(x_1, \mathfrak{c}) = 0 \tag{73}$$

となっている。引き算して、$f_2(x_1, \mathfrak{c}) = 0$ も得られ、c_1 は $\mathfrak{c}$ の拡張になっている。

(38) (32) おわり。

(39) (31),(38) より、示された。

(証終)