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 4 月 17 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。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。