

グレブナ基底と代数多様体入門

2-7章

ブッフベルガーのアルゴリズム

担当: 長谷川禎彦

<http://metabolomics.jp/mediawiki/index.php?title=User:Aritalab/Internal/Seminar>

2-7の内容

- 2-6でSペア判定条件によって, 多項式の集合がグレブナ基底か否かが判定可能であることが分かった
- 2-7ではSペア判定条件から導かれる, グレブナ基底の構成法を示す

記号

- \bar{f}^F : 順序づけられた関数 $F = (f_1, f_2, \dots, f_s)$ による f の割り算の余り
- $LT(f)$: 多項式 f の先頭項
- $LC(f)$: 先頭項の係数
- $\text{multideg}(f)$: 先頭項の次数

$$f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2 \quad \text{lex順序}$$

$$\text{multideg}(f) = (3, 0, 0)$$

$$LC(f) = -5, \quad LM(f) = x^3, \quad LT(f) = -5x^2$$

復習: グレブナ基底

$$I = \langle f_1, f_2, \dots, f_s \rangle \quad f_i \in k[x_1, x_2, \dots, x_n]$$

- $\langle \text{LT}(I) \rangle = \{ \text{LT}(f) \mid f \in I \}$
 - イデアル I に属する多項式全ての先頭項の集合
- $\langle \text{LT}(f_1), \text{LT}(f_2), \dots, \text{LT}(f_s) \rangle$
 - 生成元先頭項で作ったイデアル

$$\langle \text{LT}(f_1), \text{LT}(f_2), \dots, \text{LT}(f_s) \rangle = \left\{ \sum_{i=1}^s h_i \text{LT}(f_i) \mid h_i \in k[x_1, x_2, \dots, x_n] \right\}$$

- f_i がグレブナ基底の場合

$$\langle \text{LT}(I) \rangle = \langle \text{LT}(f_1), \text{LT}(f_2), \dots, \text{LT}(f_s) \rangle$$

復習: グレブナ基底

- グレブナ基底の条件が成立しない場合は, 先頭項の打ち消し合いによって, 余分な先頭項が $\langle \text{LT}(I) \rangle$ に含まれているとき

具体例

$$\{f_1, f_2\} = \{x^2y + x, xy^2\} \quad I = \langle f_1, f_2 \rangle$$
$$\langle \text{LT}(I) \rangle = \{\text{LT}(h_1f_1 + h_2f_2) \mid h_i \in k[x, y]\}$$



$$\text{LT}(y \cdot (x^2y + x) - x \cdot (xy^2)) = xy \in \langle \text{LT}(I) \rangle$$

$$xy \notin \langle \text{LT}(f_1), \text{LT}(f_2) \rangle = \langle x^2y, xy^2 \rangle$$

f_1, f_2 はグレブナ基底ではない 5

復習 : Sペア判定条件

Chapter 2-6, 定理6

- グレブナ基底の判定法

$$\text{multideg}(f) = \alpha, \quad \text{multideg}(g) = \beta$$

$$\gamma = (\max(\alpha_1, \beta_1), \max(\alpha_2, \beta_2), \dots)$$

$$S(f, g) = \frac{x^\gamma}{\text{LT}(f)} \cdot f - \frac{x^\gamma}{\text{LT}(g)} \cdot g \quad \text{先頭項の打ち消し}$$

$G = \{g_1, g_2, \dots, g_t\}$
がイデアル I のグレブナ基底



$$\overline{S(g_i, g_j)}^G = 0 \\ i \neq j$$

ブッフベルガー・アルゴリズム

- S ペア判定法を元にしたグレブナ基底構成法
- 基底に多項式を追加することで, S 多項式を強制的に0にしていく方法

例1

grlex順序

$$I = \langle f_1, f_2 \rangle = \langle x^3 - 2xy, x^2y - 2y^2 + x \rangle$$

$$\text{LT}(S(f_1, f_2)) = -x^2 \notin \langle \text{LT}(f_1), \text{LT}(f_2) \rangle$$

グレブナ基底の定義より, f_1, f_2 はグレブナ基底ではない

一方, S ペア判定条件を使うと

$$\overline{S(f_1, f_2)}^F = -x^2, \quad F = (f_1, f_2)$$

なので, 当然グレブナ基底でない結論が得られる.

そこで, F に他の元を足すことで, S 多項式が割り切れるようにする

例1

$S(f_1, f_2)$ のあまりを F の元に足すと当然割り切れる

$$\overline{S(f_1, f_2)}^F = 0 \quad F = (f_1, f_2, f_3 = -x^2)$$

但し, 今度は f_1, f_3 と f_2, f_3 のあいだのSペア判定が必要.

f_1, f_3 で行ってみると

$$\overline{S(f_1, f_3)}^F = -2xy \neq 0$$

よって, まだ F はグレブナ基底ではない. さらに $-2xy$ を F の元に追加する.

$$F = (f_1, f_2, f_3, f_4 = -2xy)$$

$$\overline{S(f_1, f_2)}^F = \overline{S(f_1, f_3)}^F = \overline{S(f_1, f_4)}^F = 0$$

例1

しかし, まだ f_2, f_3 の間では

$$\overline{S(f_2, f_3)}^F = -2y^2 + x \neq 0$$

$$F = (f_1, f_2, f_3, f_4 = -2xy)$$

F に $-2y^2 + x$ を追加すると

$$\overline{S(f_i, f_j)}^F = 0 \quad (1 \leq i < j \leq 5)$$

$$F = (f_1, f_2, f_3, f_4, f_5 = -2y^2 + x)$$

これから, イデアル I の grlex 順序に関するグレブナ基底は

$$F = \{x^3 - 2xy, x^2y - 2y^2 + x, -x^2, -2xy, -2y^2 + x\}$$

例1

ちなみに, lex順序の場合, グレブナ基底の元は6個になる

$$G = \{x^3 - 2xy, -2y^2 + x^2y + x, x^2, xy, x - 2y^2, y^3\}$$

invlex順序の場合, グレブナ基底の元は3個になる

$$G = \{x^3 - 2xy, -2y^2 + x^2y + x, x^2\}$$

以降, 簡約グレブナ基底を求めるが, 簡約グレブナ基底でも元の数は一項式順序によって一般に異なる

$$\langle g_1, g_2, \dots \rangle \supset \langle f_1, f_2, \dots \rangle$$

?

- グレブナ規定は余分な元を足しているのですが、グレブナ基底の張るイデアルの方が大きいように錯覚するが、足している元はもとのイデアルに含まれるので、**二つのイデアルは同じ**

グレ基 元の基底 余りの項

$$G = F \cup \{S_1, S_2, \dots\}$$

$$S_1, S_2, \dots \in I = \langle f_1, f_2, \dots, f_s \rangle$$



$$\langle g_1, g_2, \dots \rangle = \langle f_1, f_2, \dots \rangle$$

定理2

- 今の例をアルゴリズム化
- 例では, グレブナ基底を作れるっぽいのはわかるが, 停止するかどうかは自明ではない
 - 昇鎖条件 (ACC) を使うと停止することが分かる

復習：昇鎖条件 (ACC)

- $I_1 \subset I_2 \subset \cdots$ を $k[x_1, \dots, x_n]$ のイデアルの昇鎖とするとある N が存在して $I_N = I_{N+1} = I_{N+2} \cdots$
- これはヒルベルトの基底定理から導かれる

ヒルベルトの基底定理

全てのイデアル $I \subset k[x_1, \dots, x_n]$ は有限個の生成集合を持つ。つまり、ある $g_1, \dots, g_t \in I$ に対して $I = \langle g_1, \dots, g_t \rangle$

定理2

定理 2 $I = \langle f_1, \dots, f_s \rangle \neq \{0\}$ を多項式イデアルとする. I のグレブナ基底は, 次のアルゴリズムによって, 有限回のステップで構成することができる.

Input: $F = (f_1, \dots, f_s)$

Output: a Groebner basis $G = (g_1, \dots, g_t)$ for I , with $F \subset G$

$G := F$

REPEAT

$G' := G$

 FOR each pair $\{p, q\}, p \neq q$ in G' DO

$S := \overline{S(p, q)}_{G'}$

 IF $S \neq 0$ THEN $G := G \cup \{S\}$

UNTIL $G = G'$

記号

G を多項式集合 $G = (g_1, \dots, g_t)$ とした場合,

$$\langle G \rangle = \langle g_1, \dots, g_t \rangle$$

$$\langle \text{LT}(G) \rangle = \langle \text{LT}(g_1), \dots, \text{LT}(g_t) \rangle$$

注意. イデアルでも似た記号が使われていたが
 I がイデアルの場合は

$$\langle \text{LT}(I) \rangle = \{ \text{LT}(f) \mid f \in I \}$$

各ステップで G は $G \subset I$

$G' := G$

FOR each pair $\{p, q\}, p \neq q$ in G' DO

$S := \overline{S(p, q)}^{G'}$

IF $S \neq 0$ THEN $G := G \cup \{S\}$

最初は $G = F$ であるので, $G \subset I$ は明らか.

各ステップ前で $G \subset I$ とする.

$p, q \in G' \subset I$ であるので, $S(p, q) \in I$

さらに, $G' \subset I$ であるので, $S = \overline{S(p, q)}^{G'} \in I$ 注(A)

以上から, $G \cup \{S\} \subset I$

G は I の基底である F を含むので, G 自身が I の基底. さらに
停止するとき, S 多項式は常に 0 $\Rightarrow G$ はグレブナ基底

各ステップで G は $G \subset I$

注(A)の部分の補足

$G' = (g'_1, g'_2, \dots, g'_t) \subset I$ とする.

$S(p, q)$ を G' で割ると, 余り r は以下を満たす.

$$S(p, q) = a_1 g'_1 + a_2 g'_2 + \dots + a_t g'_t + r$$

$$S(p, q) - (a_1 g'_1 + a_2 g'_2 + \dots + a_t g'_t) = r \in I$$

よって, $S(p, q)$ を G' で割った余りはイデアル I の元である.

アルゴリズムは停止する

$$G' := G$$
$$\text{FOR each pair } \{p, q\}, p \neq q \text{ in } G' \text{ DO}$$
$$S := \overline{S(p, q)}^{G'}$$
$$\text{IF } S \neq 0 \text{ THEN } G := G \cup \{S\}$$

G' は G に余りを足しているので $G' \subset G$

また $\langle \text{LT}(G') \rangle \subset \langle \text{LT}(G) \rangle$

さらに $G \neq G'$ であるならば $\langle \text{LT}(G') \rangle \subsetneq \langle \text{LT}(G) \rangle$

を示したい. 今 G' に新たに余り r が加わって G になったと

する: $G = G' \cup \{r\}$

r は G' の余りなので $\text{LT}(r)$ は $\text{LT}(G')$ で割り切れない. $\text{LT}(r) \notin \langle \text{LT}(G') \rangle$

一方で $\text{LT}(r)$ は $\text{LT}(G)$ で割り切れる. $\text{LT}(r) \in \langle \text{LT}(G) \rangle$

$$\langle \text{LT}(G') \rangle \subsetneq \langle \text{LT}(G) \rangle$$

アルゴリズムは停止する

これより, G のイデアル $\langle \text{LT}(G) \rangle$ は昇鎖を成す.
昇鎖条件より, 途中でイデアルは安定し, $\langle \text{LT}(G) \rangle = \langle \text{LT}(G') \rangle$
となる. $\langle \text{LT}(G) \rangle = \langle \text{LT}(G') \rangle$ の場合 $G = G'$ であるので,
これよりグレブナ基底アルゴリズムは必ず有限回で停止する.

補題3

- 先ほどのグレブナ基底は無駄がある
- 不必要な生成元を消去し, 最小のグレブナ基底を作る

補題 3 G を多項式イデアル I のグレブナ基底とする. $p \in G$ を $\text{LT}(p) \in \langle \text{LT}(G - \{p\}) \rangle$ となる多項式とする. このとき, $G - \{p\}$ は I のグレブナ基底でもある.

証明 $\langle \text{LT}(G) \rangle = \langle \text{LT}(I) \rangle$ であることはわかっている. $\text{LT}(p) \in \langle \text{LT}(G - \{p\}) \rangle$ であるとすれば, $\langle \text{LT}(G - \{p\}) \rangle = \langle \text{LT}(G) \rangle$ である. 定義により, $G - \{p\}$ は I のグレブナ基底でもある. \square

補題3の証明を式で書き下す

$p \in G$ なので $G = (g_1 = p, g_2, \dots, g_t)$ とすると,

$$\langle \text{LT}(G - \{p\}) \rangle = \langle \text{LT}(g_2), \dots, \text{LT}(g_t) \rangle = \left\{ \sum_{i=2}^t h_i \text{LT}(g_i) \mid h_i \in k[x_1, \dots, x_n] \right\}$$

$$\langle \text{LT}(G) \rangle = \langle \text{LT}(p = g_1), \text{LT}(g_2), \dots, \text{LT}(g_t) \rangle$$

$$= \left\{ h_1 \text{LT}(p) + \sum_{i=2}^t h_i \text{LT}(g_i) \mid h_i \in k[x_1, \dots, x_n] \right\}$$

$$= \left\{ h_1 \sum_{i=2}^t \tilde{h}_i \text{LT}(g_i) + \sum_{i=2}^t h_i \text{LT}(g_i) \mid h_i, \tilde{h}_i \in k[x_1, \dots, x_n] \right\}$$

$\text{LT}(p) \in \langle \text{LT}(G - \{p\}) \rangle$
に由来

$$= \left\{ \sum_{i=2}^t (h_1 \tilde{h}_i + h_i) \text{LT}(g_i) \mid h_i, \tilde{h}_i \in k[x_1, \dots, x_n] \right\}$$

以上より $\langle \text{LT}(G - \{p\}) \rangle = \langle \text{LT}(G) \rangle$

定義4 極小グレブナ基底

minimal Groebner basis

1. 全ての $p \in G$ に対して $LC(p) = 1$
 2. 全ての $p \in G$ に対して $LT(p) \notin \langle LT(G - \{p\}) \rangle$ である
- $p \in G$ の先頭項が互いに割り切れない

例1で求めたグレブナ基底を極小化する

$$f_1 = x^3 - 2xy$$

$$f_2 = x^2y - 2y^2 + x$$

$$f_3 = -x^2$$

$$f_4 = -2xy$$

$$f_5 = -2y^2 + x$$

極小グレブナ基底の例

$$\text{LT}(f_1) = x^3 = -x \cdot \text{LT}(f_3)$$

$$\text{LT}(f_2) = x^2y = -(1/2)x \cdot \text{LT}(f_4)$$



$$\tilde{f}_3 = x^2, \tilde{f}_4 = xy, \tilde{f}_5 = y^2 - (1/2)x$$

極小グレブナ基底は一意には決まらない。

例えば、以下も極小グレブナ基底である。

$$\tilde{f}_3 = x^2 + axy, \tilde{f}_4 = xy, \tilde{f}_5 = y^2 - (1/2)x$$

演習問題7

- G と \tilde{G} を I の極小グレブナ基底とする.
 - $\text{LT}(G) = \text{LT}(\tilde{G})$ を証明せよ

$G = (g_1, \dots, g_s)$ $\tilde{G} = (\tilde{g}_1, \dots, \tilde{g}_t)$ とすると

$\text{LT}(G) = (\text{LT}(g_1), \dots, \text{LT}(g_s))$ $\text{LT}(\tilde{G}) = (\text{LT}(\tilde{g}_1), \dots, \text{LT}(\tilde{g}_t))$

両方はイデアル I のグレブナ基底なので、同じ空間を張る。

$\langle \text{LT}(I) \rangle = \langle \text{LT}(g_1), \dots, \text{LT}(g_s) \rangle = \langle \text{LT}(\tilde{g}_1), \dots, \text{LT}(\tilde{g}_t) \rangle$



$$\left\{ \sum_{i=1}^s h_i \text{LT}(g_i) \mid h_i \in k[\mathbf{x}] \right\} = \left\{ \sum_{i=1}^t \tilde{h}_i \text{LT}(\tilde{g}_i) \mid \tilde{h}_i \in k[\mathbf{x}] \right\}$$

演習問題7

同じ空間を張るので, $LT(g)$ を $LT(\tilde{g})$ で表せる

$$LT(g_a) = \sum_{i=1}^t \tilde{q}_i^a LT(\tilde{g}_i) \quad \tilde{q}_i^b \in k[\mathbf{x}]$$

$$x^3y^5 = \frac{1}{2}x^2 \cdot xy^5 + \frac{1}{2}y \cdot x^3y^4$$

同様に, 逆に $LT(\tilde{g})$ を $LT(g)$ で表せる

$$LT(\tilde{g}_b) = \sum_{i=1}^s q_i^b LT(g_i) \quad q_i^a \in k[\mathbf{x}]$$

上の式を代入すると, $LT(g)$ は $LT(g)$ 自身で表される.

$$LT(g_a) = \sum_{i=1}^t \sum_{j=1}^s \tilde{q}_i^a q_j^i LT(g_j)$$

演習問題7

$LT(p) \notin \langle LT(G - \{p\}) \rangle$ の条件から $a = j$ 以外の場合はない。
仮に $a \neq j$ の場合, $LT(g_a)$ を $LT(g_j)$ で割り切れてしまう。よって

$$LT(g_a) = \sum_{i=1}^t \tilde{q}_i^a q_a^i LT(g_a) \quad \tilde{q}_i^a q_a^i \in k$$

$$\tilde{q}_i^a q_a^i \in k \text{ から } \tilde{q}_i^a \in k$$

$LT(p) \notin \langle LT(G - \{p\}) \rangle$ の条件から, 同様に

$$LT(g_a) = \tilde{q}_c^a LT(\tilde{g}_c)$$


$LC(p) = 1$ の条件より, $LT(g_a) = LT(\tilde{g}_c)$. G と \tilde{G} の元には一体一の関係が存在する. 故に $LT(G) = LT(\tilde{G})$

定義4 簡約グレブナ基底

reduced Groebner basis

1. 全ての $p \in G$ に対して $LC(p) = 1$
2. 全ての $p \in G$ に対してどの単項式も $\langle LT(G - \{p\}) \rangle$ に含まれない

例

$$\tilde{f}_3 = x^2 + axy, \tilde{f}_4 = xy, \tilde{f}_5 = y^2 - (1/2)x$$


割れるので、これは極小であっても
簡約ではない

命題6

- $I \neq \{0\}$ を多項式イデアルとする. 与えられた単項式順序に関して, I は唯一の簡約グレブナ基底を持つ.

証明

G を I の極小グレブナ基底とする. g' と G' を以下で定義する.

$$g' = \overline{g}^{G-\{g\}} \quad G' = (G - \{g\}) \cup \{g'\}$$

そうすると, $\text{LT}(g) = \text{LT}(g')$ となっている.

$\langle \text{LT}(G) \rangle = \langle \text{LT}(G') \rangle$ かつ $G' \in I$ であることから, G' はグレブナ基底である. さらに, g' は G' に対して簡約されている.

極小グレブナ基底 $G = (g_1, g_2, g_3)$ に対して (grlex順序)

$$\begin{array}{ll} g_1 = x^2 + xy & g'_1 = \overline{g_1}^{G-\{g_1\}} = x^2 - \frac{1}{2}x \\ g_2 = xy + y^2 & g_2 = xy + y^2 \\ g_3 = y^2 - \frac{x}{2} & g_3 = y^2 - \frac{x}{2} \\ G = (g_1, g_2, g_3) & G' = (g'_1, g_2, g_3) \end{array}$$

証明

$$G' = (G - \{g\}) \cup \{g'\}$$

を次々計算すると, グレブナ基底自体が変化するが,
その先頭項は常に同じ.

$$g_1 = x^2 + xy$$

$$g_2 = xy + y^2$$

$$g_3 = y^2 - \frac{x}{2}$$

$$G = (g_1, g_2, g_3)$$



$$g'_1 = \frac{g_1}{g_1} = x^2 - \frac{1}{2}x$$

$$g_2 = xy + y^2$$

$$g_3 = y^2 - \frac{x}{2}$$

$$G = (g'_1, g_2, g_3)$$

割り算は
grlex順序



$$g_1 = x^2 - \frac{1}{2}x$$

$$g'_2 = \frac{g_2}{g_2} = xy + \frac{1}{2}x$$

$$g_3 = y^2 - \frac{x}{2}$$

$$G = (g_1, g'_2, g_3)$$



$$g_1 = x^2 - \frac{1}{2}x$$

$$g_2 = xy + \frac{1}{2}x$$

$$g'_3 = \frac{g_3}{g_3} = y^2 - \frac{x}{2}$$

$$G = (g_1, g_2, g'_3)$$

最終的には簡約グレブナ基底が得られる.

証明

簡約グレブナ基底はただ一つ

練習問題7より, イデアル I の二つの極小グレブナ基底 G, \tilde{G} は

$$\text{LT}(G) = \text{LT}(\tilde{G})$$

$g \in G$ に対して $\text{LT}(g) = \text{LT}(\tilde{g})$ となる $g \in \tilde{G}$ が存在する.
 $g = \tilde{g}$ が示せれば, $G = \tilde{G}$ が言えるので, 一意性が言える.

$g - \tilde{g}$ を考えると $g - \tilde{g} \in I$ であるので $\overline{g - \tilde{g}}^G = 0$

$\text{LT}(g) = \text{LT}(\tilde{g})$ であり, かつ G と \tilde{G} に対して簡約されているため, $g - \tilde{g}$ の先頭項は打ち消し合い, かつ残りの項は $\text{LT}(g), \text{LT}(\tilde{g})$ で割ることが出来ない. よって,

$$\overline{g - \tilde{g}}^G = g - \tilde{g} = 0$$

イデアル一致のアルゴリズム

- 二つの多項式集合 $\{f_1, f_2, \dots\}$, $\{g_1, g_2, \dots\}$ が張るイデアルが同じかどうか

$$I_1 = \langle f_1, f_2, \dots \rangle$$

$$I_2 = \langle g_1, g_2, \dots \rangle$$

- 命題6より, **簡約グレブナ基底が一致する場合に限り**, 二つのイデアルが等しい

$$I_1 = I_2$$

ガウスの消去法と ブッフベルガーアルゴリズム

線形代数のガウス消去法

$$\begin{aligned} 3x - 6y - 2z &= 0, \\ 2x - 4y + 4w &= 0, \\ x - 2y - z - w &= 0. \end{aligned}$$

$$\begin{pmatrix} 1 & -2 & -1 & -1 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

$$\begin{pmatrix} 1 & -2 & 0 & 2 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

イデアルとグレブナ基底

lex順序 $x > y > z > w$

$$I = \left\langle \begin{array}{l} 3x - 6y - 2z \\ 2x - 4y + 4w \\ x - 2y - z - w \end{array} \right\rangle \subset k[x, y, z, w]$$

極小グレブナ基底

$$I = \langle x - 2y - z - w, z + 3w \rangle$$

簡約グレブナ基底

$$I = \langle x - 2y + 2w, z + 3w \rangle$$

Maxima (1960s~)

<http://maxima.sourceforge.net/>

- 実行はShift + Return

```
(%i1) x:100;      xに100を代入. ;は自動で入る. $を行末に入れるとechoしない.  
(%o1) 100
```

```
(%i2) f(x):=sin(x)+x;      関数定義  
(%o2) f(x):=sin(x)+x
```

```
(%i3) ? sin;           ヘルプ  
-- Function: sin (<x>)  
   - Sine.  
   There are also some inexact matches for `sin'.  
   Try `?? sin' to see them.  
(%o3) true
```

Maxima

Groebner basis demo

(%i1) load(grobner);

Loading maxima-grobner \$Revision: 1.6 \$ \$Date: 2009-06-02 07:49:4

(%o1) C:/PROGRA~2/MAXIMA~1.0/share/maxima/5.27.0/share/contrib/

(%i2) poly_monomial_order:lex; 単項式順序:lex, grlex, 等

(%o2) Lex

(%i3) poly_pseudo_divide(x^2*y+x*y^2+y^2,[x*y-1,y^2-1],[x,y]);

(%o3) [[y+x,1],y+x+1,1,3] 多項式の割り算

(%i4) poly_grobner([x^3-2*x*y,x^2*y-2*y^2+x],[x,y]);

(%o4) [x^3-2xy,-2y^2+x^2y+x,x^2,xy,x-2y^2,y^3] グレブナ基底

(%i5) poly_reduced_grobner([x^3-2*x*y,x^2*y-2*y^2+x],[x,y]);

(%o5) [x-2y^2,y^3] 簡約グレブナ基底(但し教科書と異なり, LCは1に正規化されていない)