第2章　グレブナ基底
§6　グレブナ基底の性質

担当　乳井昌道

§6では、グレブナ基底の性質を調べ、与えられた基底がグレブナ基底になるかどうかを判定する方法を学ぶ。

命題1

$G=\{g_1,\ldots,g_t\}$ は $I\subset k\left[x_1,\ldots,x_n\right]$ のグレブナ基底であり, $f\in k\left[x_1,\ldots,x_n\right]$ とする. このとき, 次の2つの条件を満たす多項式 $r\in k\left[x_1,\ldots,x_n\right]$ がただ1つ存在する.

(ｉ) r のどの項も $LT(g_1),\ldots,LT(g_t)$ のどれでも割り切れない.

(ⅱ) $f=g+r$ となる $g\in I$ が存在する.

特に, 割り算アルゴリズムにおいて, Gの元がどのように並んでいても r は f を G で割ったときの余りである。

→グレブナ基底で割り算するときは余りはただ1つに決まる.

系2

$G=\{g_1,\ldots,g_t\}$をイデアル$I\subset k[x_1,\ldots,x_n]$のグレブナ基底とし, $f\in k[x_1,\ldots,x_n]$とする. このとき, $f\in I$ であることと f を G で割ったときの余りがゼロであることは同値である.

→イデアル所属問題が解ける. $f\in I$であるかどうかを決めるには, G による余りを計算するだけでいい.

証明(系2)

余りがゼロであるときには, $f \in I$ であることはすでに見た. 逆に, $f \in I$ が与えられたとき, $f = f + 0$ は命題1の2つの条件を満たす. これより, 0は f を G で割ったあまりであることが従う.

定義3

ｓ個の順序付けられた関数 $F=(f_1,\ldots,f_s)$ による ｆの割り算の余りを $\overline{f}^F$ と書く. Ｆが $\langle f_1,\ldots,f_s\rangle$ のグレブナ基底であるときには, 命題1によって, Ｆは(その元の順序とは関係ない)集合とみなせる.

例(定義3)

$F=\left(x^2y-y^2, x^4y^2-y^2\right)\subset k\left[x,y\right]$において, lex順序を使って,

$$\overline{x^5y}^F = xy^3$$

を得る. なぜなら

$$x^5y=\left(x^3+xy\right)\left(x^2y-y^2\right)+0\cdot\left(x^4y^2-y^2\right)+xy^3$$

先頭項の打ち消しあい

f_i の多項式係数の線型結合は, 必ずしも $LT(f_i)$ によって生成されたイデアルに入ってないことがある. 適当な結合

$$\alpha x^{\alpha} f_i - \beta x^{\beta} f_j$$

において先頭項が打ち消し合い, 低次の項だけが残る場合があるため.それでも $\alpha x^{\alpha} f_i - \beta x^{\beta} f_j \in I$ であって, その先頭項は $\langle LT(f) \rangle$ に入る.

定義4

$f,g\in k[x_1,\ldots,x_n]$ をゼロでない多項式とする.

(ⅰ) $multi\deg(f)=\alpha$ かつ $multi\deg(g)=\beta$ であるとする.
このとき, 各 i に対して, $\gamma_i=\max(\alpha_i,\beta_i)$と書き, $\gamma=(\gamma_1,\ldots,\gamma_n)$
とおく. この x^γ を$LM(f)$ と$LM(g)$ の最小公倍元と
呼び, $x^\gamma=LCM(LM(f),LM(g))$と書く.

(ⅱ) f と g の S 多項式とは,

$$S(f,g)=\frac{x^\gamma}{LT(f)}\cdot f-\frac{x^\gamma}{LT(g)}\cdot g$$

で与えられる多項式である.

例(定義4)

$R[x,y]$ におけるgrlex順序で $f = x^3y^2 - x^2y^3 + x$ と
$g = 3x^4y + y^2$ を考える. このとき, $\gamma = (4,2)$ であって,

$$S(f,g) = \frac{x^4y^2}{x^3y^2} \cdot f - \frac{x^4y^2}{3x^4y} \cdot g$$

$$= x \cdot f - \left(1/3\right) \cdot y \cdot g = -x^3y^3 + x^2 - \left(1/3\right) \cdot y^3$$

S多項式 $S(f,g)$ は, 先頭項の打ち消し合いが起こるように設計されている.

※ $multi\deg(f) = (3,2) \quad multi\deg(g) = (4,1)$

補題5

各ｉに対して, $c_i \in k$ で $multi\deg(f_i) = \delta \in Z_{\geq 0}^n$ であるような和 $\sum_{i=1}^{s} c_i f_i$ を考える. もし, $multi\deg\left(\sum_{i=1}^{s} c_i f_i\right) < \delta$ であれば, $\sum_{i=1}^{s} c_i f_i$ は $S(f_j, f_k)(1 \leq j,k \leq s)$ のｋ係数の線型結合である. さらに各 $S(f_j, f_k)$ の多重次数はδより真に小さい.

定理6

I を多項式環のイデアルとする.
I の基底 $G=\{g_1,\ldots,g_t\}$ が I のグレブナ基底であることは次と同値である:
すべての $i\neq j$ となる添字に対して, $S\left(g_i,g_j\right)$ を G (これはなんらかの順序が入っている)で割った余りはゼロである.

※定理6は, ブッフベルガーのSペア判定条件と呼ばれる.

証明(定理6)

$\Rightarrow$: もし、G がグレブナ基底であれば, $S\left(g_i, g_j\right) \in I$ であるから, G による割り算の余りは系2によりゼロである.

$\Leftarrow$: $f \in I$ をゼロでない多項式とする. S多項式すべての G による割り算の余りがゼロであるならば, $LT\left(f\right) \in \left\langle LT\left(g_1\right), \ldots, LT\left(g_t\right)\right\rangle$ であることを示す必要がある.

証明の方針(定理6)

与えられた $f \in I = \langle g_1, \ldots g_t \rangle$ に対して, $h_i \in k[x_1, \ldots, x_n]$ があって,

(2) $$f = \sum_{i=1}^{t} h_i g_i$$

となる. §2の補題8の(ii)により,

(3) $$multi\deg(f) \leq \max(multi\deg(h_i g_i))$$

が得られる. 等号が得られなければ, (2)において, 先頭項の間で打ち消し合いが起こっている.

補題5によって, これをS多項式を使って書き直すことができる.

S多項式の余りがゼロであるという仮定から, S多項式を, 項の打ち消し合いがより少ない式によって置き換えることができる.

先頭項の打ち消し合いがより少ない f の表示式が得られる.

証明の方針(定理6)

このようにして続けていくと, 最終的に(3)において等号が成立するような f の(2)の表示式が得られる.

$multi\deg(f) = multi\deg(h_i g_i)$ が適当な i に対して成り立つ.

$LT(f)$ が $LT(g_i)$ で割り切れることが従う.

これによって, $LT(f) \in \langle LT(g_1),\ldots,LT(g_t) \rangle$ となる.

証明(定理6)

f の表現式(2)に対して, $m(i) = multi\deg(h_i g_i)$ とし,
$\delta = \max(m(1), \ldots, m(t))$ と定義する. このとき, 不等式(3)は

$$multi\deg(f) \le \delta$$

となる.

f が(2)の形に書けるようなすべての表現の仕方を考える.

単項式順序は整列順序であるから, そのうちで, δ が最小になるように f の表現(2)を選ぶことができる.

証明(定理6)

いったん最小のδ が選ばれると $multi\deg(f)=\delta$ となることを証明する.
このとき, (3)において等号が成り立つ.
そして, $LT(f)\in\langle LT(g_1),\ldots,LT(g_t)\rangle$ が従う.

$multi\deg(f)=\delta$ の証明は背理法による.
等号が成り立たないということは $multi\deg(f)<\delta$ ということである.

証明(定理6)

f を次のように書き表す.

(4)
$$f = \sum_{m(i)=\delta} h_i g_i + \sum_{m(i)<\delta} h_i g_i$$
$$= \sum_{m(i)=\delta} LT(h_i) g_i + \sum_{m(i)=\delta} \left(h_i - LT(h_i)\right) g_i + \sum_{m(i)<\delta} h_i g_i$$

2行目の2番目と3番目の Σ の中に現れる単項式は, すべて多重次数が δ より真に小さい.

$multi\deg(f) < \delta$ という仮定から, 最初の Σ の項も多重次数が δ より真に小さい.

証明(定理6)

$LT(h_i)=c_i x^{\alpha(i)}$ とおく.
最初の和となる $\sum_{m(i)=\delta} LT(h_i) g_i = \sum_{m(i)=\delta} c_i x^{\alpha(i)} g_i$ は, ちょうど

$f_i = x^{\alpha(i)} g_i$ として補題5に記述した形をしている.
補題5よりこの和はS多項式 $S\left(x^{\alpha(j)} g_j, x^{\alpha(k)} g_k\right)$ の線型結合である.

証明(定理6)

$$S\left(x^{\alpha(j)}g_j, x^{\alpha(k)}g_k\right) = \frac{x^\delta}{x^{\alpha(j)}LT\left(g_j\right)}x^{\alpha(j)}g_j - \frac{x^\delta}{x^{\alpha(k)}LT\left(g_k\right)}x^{\alpha(k)}g_k$$

$$= x^{\delta-\gamma_{jk}}S\left(g_j, g_k\right) \quad \left(\because S\left(g_j, g_k\right) = \frac{x^{\gamma_{jk}}}{LT\left(g_j\right)}g_j - \frac{x^{\gamma_{jk}}}{LT\left(g_k\right)}g_k\right)$$

が成り立つ. ここで, $x^{\gamma_{jk}} = LCM\left(LM\left(g_j\right), LM\left(g_k\right)\right)$ である.

定数 $c_{jk} \in k$ が存在して,

(5) $$\sum_{m(i)=\delta} LT\left(h_i\right)g_i = \sum_{j,k} c_{jk}x^{\delta-\gamma_{jk}}S\left(g_j, g_k\right)$$

が成り立つ.

証明(定理6)

$S(g_j, g_k)$ を $g_1, \ldots, g_t$ で割り算したときの余りがゼロであるという仮定を使う. 割り算アルゴリズムを使うと, 各々のS多項式が

(6) $$S(g_j, g_k) = \sum_{i=1}^{t} a_{ijk} g_i \quad \left(a_{ijk} \in k[x_1, \ldots, x_n]\right)$$

という形に書ける. 割り算アルゴリズムは,

(7) $$multi\deg(a_{ijk} g_i) \leq multi\deg(S(g_j, g_k))$$

がすべての i, j, k に対して成り立つことも保証している.
(§3の定理3を参照)
先頭項がすべて打ち消されるわけではない.

証明(定理6)

$S(g_j, g_k)$ の表示に $x^{\delta-\gamma_{jk}}$ を掛けて,

$$x^{\delta-\gamma_{jk}} S(g_j, g_k) = \sum_{i=1}^{t} b_{ijk} g_i \qquad \left(b_{ijk} = x^{\delta-\gamma_{jk}} a_{ijk}\right)$$

を得る. このとき, (7)と補題5によって,

(8) $\quad multi\deg\left(b_{ijk} g_i\right) \le multi\deg\left(x^{\delta-\gamma_{jk}} S(g_j, g_k)\right) < \delta$

が導かれる. $x^{\delta-\gamma_{jk}} S(g_j, g_k)$ の表現式を(5)に代入して,

$$\sum_{m(i)=\delta} LT(h_i) g_i = \sum_{j,k} c_{jk} x^{\delta-\gamma_{jk}} S(g_j, g_k) = \sum_{j,k} c_{jk} \left(\sum_i b_{ijk} g_i \right) = \sum_i \tilde{h}_i g_i$$

を得る. これは(8)によって, すべての i に対して,

$multi\deg\left(\tilde{h}_i g_i\right) < \delta$ であるという性質を持つ.

証明(定理6)

$\sum_{m(i)=\delta} LT(h_i) g_i = \sum_i \tilde{h}_i g_i$ を, 方程式(4)に代入し, g_i の多項式係数の結合としての f の表現を得る.

$$f = \sum_i \tilde{h}_i g_i + \sum_{m(i)=\delta} \left(h_i - LT(h_i)\right) g_i + \sum_{m(i)<\delta} h_i g_i$$

ここに, 現れるすべての項は多重次数が δ より真に小さい.
これは, δ が最小であるという仮定に反する. したがって, 背理法により結論が導かれる.

例(定理6)

- Sペア判定条件を使えば, 与えられた基底がグレブナ基底であるかどうか簡単にわかる.

R^3 の捻れ3次曲線のイデアル $I = \left\langle y - x^2, z - x^3 \right\rangle$ を考える.

$G = \{y - x^2, z - x^3\}$ がlex順序 $y > z > x$ に関するグレブナ基底であることを証明する. S多項式

$$S\left(y - x^2, z - x^3\right) = \frac{yz}{y}\left(y - x^2\right) - \frac{yz}{z}\left(z - x^3\right) = -zx^2 + yx^3$$

割り算アルゴリズムを使って,

$$-zx^2 + yx^3 = x^3 \cdot \left(y - x^2\right) + \left(-x^2\right) \cdot \left(z - x^3\right) + 0$$

余りはゼロであるから, 定理6より, G は I のグレブナ基底である.