

グレブナー基底

内藤と大垣と国井と山口のセミナー

No.007

はじめに

グレブナー基底とは多項式のイデアルの基底の中で、ある種の計算を行うのに都合の良い基底である。本セミナーではグレブナー基底の定義、判定法、構成法を解説し、いくつかの具体的な応用例を扱う予定である。必要とする知識としては、多項式環やイデアル等の定義を知っていれば良い程度である。足りないと感じたところはセミナー中にでも指摘して頂ければ幸いである。

参考文献

- [1] David Cox, John Little, Donal O'Shea 『IDEALS, VARIETIES, AND ALGORITHMS』, U.T.M. Springer(1996)
- [2] David Cox, John Little, Donal O'Shea 『Using Algebraic Geometry』 G.T.M.185 Springer(2004)

1 定義

k を体とする。

定義 1.1. (整列集合)

順序集合 A が整列集合であるとは、任意の A の部分集合が最小元をもつことである。

定義 1.2. $X_1^{\alpha_1} \cdots X_n^{\alpha_n} \in k[X_1, \dots, X_n]$ を $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{Z}_{\geq 0}^n$ と同一視し、 X^α と書く。

定義 1.3. (項順序) 以下の 3 つをみたす順序 \geq を項順序 (monomial order) という。

- 1 \geq は $\mathbb{Z}_{\geq 0}^n$ 上の全順序
- 2 $\alpha \geq \beta, \gamma \in \mathbb{Z}_{\geq 0}^n$ のとき $\alpha + \gamma \geq \beta + \gamma$ を満たす。
- 3 \geq は $\mathbb{Z}_{\geq 0}^n$ 上の整列集合である。

以下の 3 つは代表的な項順序である。

定義 1.4. (Lexicographic Order)

$\alpha = (\alpha_1, \dots, \alpha_n), \beta = (\beta_1, \dots, \beta_n) \in \mathbb{Z}_{\geq 0}^n$ とする。 $\alpha - \beta = (\alpha_1 - \beta_1, \dots, \alpha_n - \beta_n)$ の 0 でない最も左の元が正のとき $\alpha \geq_{lex} \beta$ とする。

定義 1.5. (Graded Lex Order)

$\alpha, \beta \in \mathbb{Z}_{\geq 0}^n$ のとき $\alpha \geq_{grlex} \beta$ とは $|\alpha| = \sum_{i=1}^n \alpha_i > \sum_{i=1}^n \beta_i = |\beta|$ または $|\alpha| = |\beta|$ かつ $\alpha \geq_{lex} \beta$ となることである。

定義 1.6. (Graded Reverse Lex Order)

$\alpha, \beta \in \mathbb{Z}_{\geq 0}^n$ のとき $\alpha \geq_{grevlex} \beta$ とは $|\alpha| > |\beta|$ または $|\alpha| = |\beta|$ かつ $\alpha - \beta$ の 0 でない最も右の元が負であることである。

定義 1.7. \geq を項順序とし、 $f = \sum_{\alpha} a_{\alpha} X^{\alpha} \in k[X_1, \dots, X_n] \setminus \{0\}$ とする。

1. $\text{multideg}(f) := \max\{\alpha \in \mathbb{Z}_{\geq 0}^n \mid a_{\alpha} \neq 0\}$
2. $\text{LC}(f) := a_{\text{multideg}(f)} \in k$
3. $\text{LM}(f) := X^{\text{multideg}(f)} \in k[X_1, \dots, X_n]$
4. $\text{LT}(f) := \text{LC}(f) \cdot \text{LM}(f)$

命題 1.8. \geq を $\mathbb{Z}_{\geq 0}^n$ 上の項順序とし、 $f_1, \dots, f_s \in k[X_1, \dots, X_n]$ を順序づけられた s 個の多項式とする ($f_1 > f_2 > \dots > f_s$)。このとき任意の多項式 $f \in k[X_1, \dots, X_n]$ は

$$F = a_1 f_1 + \dots + a_s f_s + r$$

と書ける。ただし、 $a_1, \dots, a_s, r \in k[X_1, \dots, X_n]$ であり、 $r = 0$ もしくは r は $\text{LT}(f_1), \dots, \text{LT}(f_s)$ のどれでも割り切れない。 r を f_1, \dots, f_s による f の余りという。さらに任意の i に対して

$$\text{multideg}(f) \geq \text{multideg}(a_i f_i)$$

が成り立つ。

定理 1.9. (Division Algorithm in $k[X_1, \dots, X_n]$) 命題 1.8 の a_1, \dots, a_s, r は次のアルゴリズムで求められる。

Input: f_1, \dots, f_s, f

Output: a_1, \dots, a_s, r

$a_1 := 0, \dots, a_s := 0, r := 0$

$p := f$

WHILE($p \neq 0$) {

$i := 1$

divisionoccurred:=false

WHILE($i \leq s$ AND divisionoccurred =false){

IF($LT(f_i)$ divides $LT(p)$) {

$a_i := a_i + LT(p)/LT(f_i)$

$p := p - (LT(p)/LT(f_i))f_i$

divisionoccurred:=true

}

ELSE {

$i := i + 1$

}

}

IF(divisionoccurred = false){

$r := r + LT(p)$

$p := p - LT(p)$

}

}

定義 1.10. (単項式イデアル)

単項式が生成するイデアル、すなわち $\mathbb{Z}_{\geq 0}^n$ の部分集合 A に対して $I = \langle X^\alpha \mid \alpha \in A \rangle \subset k[X_1, \dots, X_n]$ を単項式イデアルという。

補題 1.11. 単項式イデアル $I = \langle X^\alpha \mid \alpha \in A \rangle$ に対して $X^\beta \in I$ であることの必要十分条件はある $\alpha \in A$ に対して X^α が X^β を割り切ることである。

補題 1.12. (Dickson's Lemma)

$k[X_1, \dots, X_n]$ の任意の単項式イデアルは有限生成である。

定義 1.13. 0 でないイデアル $I \in k[X_1, \dots, X_n]$ に対して

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

定義 1.14. (グレブナー基底)

\geq を項順序とする。0 でないイデアル $I \subset k[X_1, \dots, X_n]$ に対して $G = \{g_1, \dots, g_s\} \subset I$ が I のグレブナー基底であるとは

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

が成り立つことである。

命題 1.15. I を 0 でない $k[X_1, \dots, X_n]$ のイデアルとする。

- (1) $\langle \text{LT}(I) \rangle$ は単項式イデアルである。
- (2) I のグレブナー基底が存在する。
- (3) グレブナー基底は I の基底である。

定理 1.16. (Hilbert Basis Theorem)

$k[X_1, \dots, X_n]$ の任意のイデアルは有限生成である。

2 Buchberger's Algorithm

定義 2.1. $f_1, \dots, f_s \in k[X_1, \dots, X_n]$ を s 個の順序づけられた多項式とする ($f_1 > \dots > f_s$)。 $f \in k[X_1, \dots, X_n]$ を $F = (f_1, \dots, f_s)$ で割った余り、すなわち割算アルゴリズムを実行して求まる余りの多項式を \bar{f}^F と書く。

命題 2.2. I を $k[X_1, \dots, X_n]$ のイデアルとし、 $G = \{g_1, \dots, g_s\}$ を I のグレブナー基底とする。このとき、任意の $f \in k[X_1, \dots, X_n]$ に対して以下を満たす $r \in k[X_1, \dots, X_n]$ が唯一つ存在する。

- (1) r のどの項も $\text{LT}(g_1), \dots, \text{LT}(g_s)$ で割り切れない
- (2) $f = g + r$ を満たす $g \in I$ が存在する

特に、余り r は G 内の順序に依らない。

系 2.3. $f \in k[X_1, \dots, X_n]$ がイデアル $I \subset k[X_1, \dots, X_n]$ の元であるための必要十分条件は $\bar{f}^F = 0$ である。

定義 2.4. $f, g \in k[X_1, \dots, X_n]$ とし、 $\text{multideg}(f) = \alpha, \text{multideg}(g) = \beta$ とする。 $\gamma = (\gamma_1, \dots, \gamma_n)$ を各 i に対し、 $\gamma_i = \max\{\alpha_i, \beta_i\}$ とするとき

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

を f と g の S 多項式という。また、このとき X^γ を $\text{LM}(f)$ と $\text{LM}(g)$ の最小公倍数といい、 $\text{LCM}(\text{LM}(f), \text{LM}(g))$ と書く。

例 2.5. $f = x^3y^2 - x^2y^3 + x, g = 3x^4y + y^2$ を $\mathbb{R}[x, y]$ の元とし、 grlex order を与える。このとき $\gamma = (4, 2)$ であるから、 S 多項式は

$$\begin{aligned} S(f, g) &= \frac{x^4y^2}{x^3y^2} \cdot f - \frac{x^4y^2}{3x^4y} \cdot g \\ &= x \cdot f - (1/3) \cdot y \cdot g \\ &= -x^3y^3 + x^2 - (1/3)y^3. \end{aligned}$$

補題 2.6. $f = \sum_{i=1}^s c_i f_i$ とおく。ただし、各 i に対し $c_i \in k$ かつ $\text{multideg}(f_i) = \delta \in \mathbb{Z}_{n \geq 0}^n$ とする。このとき、 $\text{multideg}(f) < \delta$ ならば f は $1 \leq l \leq m \leq s$ に対し $S(f_l, f_m)$ の k 上の線形結合で書ける。さらに、各 l, m に対し $\text{multideg}(S(f_l, f_m)) < \delta$ である。

定理 2.7. $G = \{g_1, \dots, g_s\} \subset k[X_1, \dots, X_n]$ が $k[X_1, \dots, X_n]$ のイデアル I のグレブナー基底であるための必要十分条件は任意の相異なる i, j に対して $\overline{S(g_i, g_j)}^G = 0$ が成り立つことである。

定理 2.8. (Buchberger's Algorithm)

0 でない多項式イデアル $I = (f_1, \dots, f_s)$ のグレブナー基底 $G = \{g_1, \dots, g_r\}$ は次のアルゴリズムで得られる。

Input: $F = \{f_1, \dots, f_s\}$

Output: a Groebner basis $G = \{g_1, \dots, g_r\}$ for I , with $F \subset G$

$G := F$

DO{

$G' := G$

 FOR(each pair $\{p, q\}$ in G') {

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

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

 }

 }WHILE($G \neq G'$)

}

3 reduced Groebner basis

補題 3.1. G を $k[X_1, \dots, X_n]$ のイデアル I のグレブナー基底とする。 $p \in G$ が $\text{LT}(p) \in \langle \text{LT}(G - \{p\}) \rangle$ を満たすとき、 $G - \{p\}$ は I のグレブナー基底である。

定義 3.2. (minimal Groebner basis)

I のグレブナー基底 G が以下の条件を満たすとき G を最小グレブナー基底 (minimal Groebner basis) という。

- (1) 任意の $p \in G$ に対して $\text{LC}(p) = 1$
- (2) 任意の $p \in G$ に対して $\text{LT}(p) \notin \langle \text{LT}(G - \{p\}) \rangle$

定義 3.3. (reduced Groebner basis)

I のグレブナー基底 G が以下の条件を満たすとき G を簡約グレブナー基底 (reduced Groebner basis) という。

- (1) 任意の $p \in G$ に対して $\text{LC}(p) = 1$
- (2) 任意の $p \in G$ に対して p の全ての単項式が $\langle \text{LT}(G - \{p\}) \rangle$ に含まれない

命題 3.4. $k[X_1, \dots, X_n]$ の 0 でないイデアル I に対し、項順序を一つ定めると簡約グレブナー基底は一意に定まる。