



# グレブナー基底はよい水

BV18051 千葉龍朗

令和元年 11 月 1 日

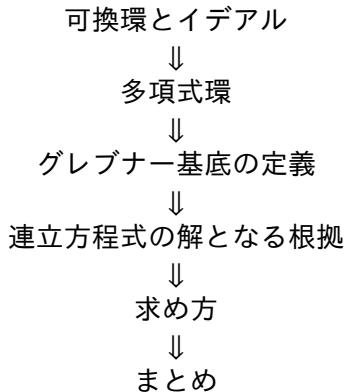
グレブナー基底という言葉を目にしたことがある人は多いだろう。とあるネット記事<sup>1</sup>などで紹介されているが、実際はどのようなものなのか興味があり、本研究に取り組んだ。

---

<sup>1</sup><http://groebner-basis.hatenablog.com/entry/2017/05/04/220248>, 「数学がよく分からない人のためのグレブナー基底 グレブナー基底にはポン酢が合う」 2019/10/20 最終閲覧 

# グレブナー基底って何?

多項式環のイデアルの生成系の中で優れたもの. Bruno Buchberger が発表した. グレブナーは彼の指導教授である Wolfgang Gröbner からきている.



$R$  を空でない集合とする.  $R$  に 2 つの二項演算, 加法  $+$ , 乗法  $\times$  が与えられており, 以下の条件を満たすとき,  $R$  を環という.

- ① 加法について可換群である. つまり, 以下の 4 つの条件が成り立つ.
  - (i) 任意の  $a, b, c \in R$  に対し,  $(a + b) + c = a + (b + c)$ .
  - (ii) 加法についての単位元  $e_+ \in R$  が存在し, 任意の  $a \in R$  に対して  $a + e_+ = e_+ + a = a$ .
  - (iii) 任意の  $a \in R$  に対し, 逆元  $b \in R$  が存在し,  $a + b = e_+$  である.
  - (iv) 任意の  $a, b \in R$  に対し,  $a + b = b + a$ .
- ② 乗法について結合法則が成り立ち, 単位元が存在する. また, 可換である. つまり, 以下の 2 つの条件が成り立つ.
  - (i) 任意の  $a, b, c \in R$  に対し,  $(ab)c = a(bc)$ .
  - (ii) 乗法についての単位元  $e_\times \in R$  が存在し, 任意の  $a \in R$  に対して  $a \times e_\times = e_\times \times a = a$ .
  - (iii) 任意の  $a, b \in R$  に対し,  $a \times b = b \times a$ .
- ③ 分配法則が成り立つ. つまり,  $a, b, c \in R$  で  $a \times (b + c) = a \times b + a \times c$  が成り立つ.

$R$  が乗法について可換群であった場合,  $R$  は体とよばれる.

可換環  $R$  の空でない部分集合  $I$  が次の条件を満たすとき,  $I$  を  $R$  のイデアルという.

- (i)  $a, b \in I$  なら  $a + b \in I$  である.
- (ii)  $r \in R, a \in I$  ならば  $ra \in I$  である.

可換環  $R$  に属する元からなる有限集合  $\mathcal{F} = \{y_\lambda\}_{\lambda \in \Lambda}$  があつたとき,

$$\sum_{\text{有限和}} r_\lambda y_\lambda, \quad r_\lambda \in R$$

なる表示をもつ元の全体は  $R$  のイデアルである. これを  $y_1, y_2, \dots, y_s$  が生成するイデアルといい,  $(\mathcal{F})$  とかく. 可換環  $R$  の任意のイデアル  $I$  について  $I = (\mathcal{F})$  となる  $R$  の元の集合  $\mathcal{F}$  が選べる. これを  $I$  の生成系とよぶ.

ここでは、多項式環を導入するために、単項式と多項式を定義する。  
可換な変数  $x_1, x_2, \dots, x_n$  を用意する。変数の積

$$x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$$

を単項式と呼び、その次数を  $a_1 + a_2 + \cdots + a_n$  と定義する。ただし、各  $a_i$  は非負整数である。

$$\mathbf{a} = (a_1, a_2, \dots, a_n)$$

を用いて  $x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$  を  $\mathbf{x}^{\mathbf{a}}$  と略記する。

例えば、変数を  $x_1, x_2, x_3, x_4$  としたとき、単項式  $x_1 x_2^3 x_3^2$  の次数は  $1 + 3 + 2 + 0 = 6$  である。また、 $\mathbf{a} = (1, 3, 2, 0)$  として  $x_1 x_2^3 x_3^2$  を  $\mathbf{x}^{\mathbf{a}}$  とかける。



単項式を並べたもの. 定義は以下の通り.

体  $K$  を固定する. 変数  $x_1, x_2, \dots, x_n$  の単項式の全体を基底に持つ  $K$  上の線形空間を

$$K[x] = K[x_1, x_2, \dots, x_n]$$

と表す. 多項式とは, これに属するものである.  $f \in K[x]$  とすると

$$f = \sum_{\mathbf{a}} c_{\mathbf{a}}^{(f)} \mathbf{x}^{\mathbf{a}}, c_{\mathbf{a}}^{(f)} \in K$$

多項式の次数がすべて  $d$  のとき, 斉次多項式という.

単項式  $x^a, x^b$  の積  $x^a x^b$  を  $x^{a+b}$ , 多項式  $f = \sum_a c_a^{(f)} x^a$  と  $g = \sum_a c_a^{(g)} x^a$  の積  $fg$  を

$$fg = \sum_a \left( \sum_{a'+a''=a} c_{a'}^{(f)} c_{a''}^{(g)} \right) x^a$$

と定義する. このとき,  $K[x]$  は可換環になる. これを体  $K$  上の  $n$  変数多項式環という. 多項式環  $K[x]$  のイデアル  $I$  が斉次多項式からなる生成系をもつとき,  $I$  を斉次イデアルとよぶ. 多項式環  $K[x]$  のイデアル  $I$  が単項式からなる生成系をもつとき,  $I$  を単項式イデアルとよぶ.

多項式環  $K[x] = K[x_1, x_2, x_3, x_4]$  において,  $f = 3x_1x_3 + 4x_2^2x_4$  は  $K[x]$  の元である.  $I = \{c_1(x_1 + 3) + c_2(x_2 - 2) \mid c_1, c_2 \in K[x]\}$  としたとき,  $I$  はイデアルである. このとき,  $I$  は  $(x_1 + 3, x_2 - 2)$  が生成するイデアルである. また,  $(x_1 + 3, x_2 - 2)$  を  $I$  の生成系といえる. いま,  $x_1 + 3, x_2 - 2$  はどちらも次数が 1 なので,  $I$  は斉次イデアルである.

多項式環  $K[x] = K[x_1, x_2, \dots, x_n]$  の単項式全体の集合  $M$  における順序  $<$  が

- ❶ 任意の  $1 \neq u \in M$  について  $1 < u$  である
- ❷  $u, v \in M$  で  $u < v$  ならば, 任意の  $w \in M$  について  $uw < vw$  であることをみたすとき,  $<$  を  $K[x]$  の単項式順序という.

$x^a <_{rev} x^b$  とは

- $x^a$  の次数より,  $x^b$  のほうが大きい
- $x^a$  と  $x^b$  の次数が等しく, ベクトルの差  $b - a$  においてもとも右にある 0 でない成分が負

のいずれかが満たされているときをいう. これを逆辞書式順序という.

例えば,  $K[x] = K[x_1, x_2, x_3]$  において,  $x_1^3 x_2 x_3^3 <_{rev} x_1^2 x_2^4 x_3$  である.

$$(2, 4, 1) - (3, 1, 3) = (-1, 3, -2)$$

$x^a <_{lex} x^b$  とは

- $x^a$  の次数より,  $x^b$  のほうが大きい
- $x^a$  と  $x^b$  の次数が等しく, ベクトルの差  $b - a$  においてもとも左にある 0 でない成分が正

のいずれかが満たされているときをいう. これを辞書式順序という.

例えば,  $K[x] = K[x_1, x_2, x_3]$  において,  $x_1^2 x_2^4 x_2 <_{lex} x_1^3 x_2 x_3^3$  である.

$$(3, 1, 3) - (2, 4, 1) = (1, -3, 2)$$

多項式環  $K[x]$  の任意の多項式  $f \neq 0$  について,  $f$  に現れる単項式の中で  $<$  に関して最大のものを  $f$  の  $<$  に関するイニシャル単項式とよび,  $\text{in}_<(f)$  と表す. また, 多項式環  $K[x]$  の任意のイデアル  $I \neq \{0\}$  について,  $I$  に属するすべての多項式のイニシャル単項式を集めたものを  $I$  の  $<$  に関するイニシャルイデアルとよび  $\text{in}_<(I)$  と表す.

例えば...

辞書式順序において,  $f = x^2y + y^3 + x^2 - 3$  のイニシャル単項式  $\text{in}_<(f)$  は  $x^2y$

$I$  に属する 0 でない多項式の有限集合  $\mathcal{G} = \{g_1, g_2, \dots, g_s\}$  が単項式順序  $<$  に関する  $I$  のグレブナー基底であるとは、次が成立するときをいう。

$$\text{in}_<(I) = (\text{in}_<(g_1), \text{in}_<(g_2), \dots, \text{in}_<(g_s))$$



$f_1 = x_1 + 2x_2 - 5$ ,  $f_2 = 2x_1 - 3x_2 + 4$  が生成するイデアル  $I$  の  
グレブナー基底は

$$\mathcal{G} = \{x_1 - 1, x_2 - 2\}$$

実際,  $\text{in}_<(x_1 - 1) = x_1$ ,  $\text{in}_<(x_2 - 2) = x_2$  だが,  
 $\text{in}_<(I) = \{x_1, x_2, x_1^2, x_1x_2, x_2^2, x_1^3, \dots\}$ . かつ  $x_1 - 1$  と  $x_2 - 2$  は  $G$  が生成するイ  
デアルに属する.

ここで,  $K[x]$  のイデアルについていくつかの定理を紹介する. これらはグレブナー基底が連立方程式の解となることに深く関わっている.

## 定義

多項式環  $K[x]$  に属する単項式からなる集合  $M$  を考える. いま,  $u$  と  $v$  が  $M$  に属するとき,  $u \leq v$  を  $u$  が  $v$  を割り切る, と定義する. つまり,  
 $au = v, a \in R \Rightarrow u \leq v.$

これを整除関係による順序という.

## 定理 (Dickson の補題)

多項式環  $K[x]$  に属する単項式からなる空でない集合  $M$  に整除関係による順序  $\leq$  が定まっているとき, 順序  $\leq$  に関する  $M$  の最小限は有限個存在する.

帰納法で証明.

## 定理

多項式環  $K[x]$  の任意の単項式順序において,  $K[x]$  の部分集合  $N \neq \emptyset$  には最小限が存在する.

整除関係による順序を単項式順序に拡張したもの. Dickson の補題から, 無限減少数列  $\cdots < u_2 < u_1 < u_0$  が存在しないことを用いる. この定理により, 任意のイデアルと単項式順序  $<$  において

$\cdot < u_{j-1} < u_j < u_{j+1} < \cdots < u_1 < \text{in}_<(f)$  なる無限減少列は存在しないことが分かる.

よって、次のことが示せる.

## 定理 (Hilbert 基底定理)

多項式環  $K[x]$  の任意のイデアルは有限生成である.

この証明では,  $K[x]$  のイデアル  $I$  において  $\text{in}_<(I) = (\text{in}_<(g_1), \text{in}_<(g_2), \dots, \text{in}_<(g_s))$  となる  $g_1, g_2, \dots, g_s$  をみつけたとき,  $g_1, g_2, \dots, g_s$  は  $I$  を生成することを示している.

$\mathcal{G} = \{g_1, g_2, \dots, g_s\}$  が  $\langle \cdot \rangle$  に関する  $I$  のグレブナー基底である

↓

$f \in I$  としたとき,  $f = y_1 g_1 + y_2 g_2 + \dots + y_s g_s (y_i \in K[x], i = 1, 2, \dots)$  となる  $y_i$  が存在する.

↓

$$\forall i, g_i = 0 \Rightarrow f = 0$$

# グレブナー基底をもとめよう

$K[x] = K[x, y, z]$  と単項式順序  $<_{lex}$  を固定し, 多項式

$f_1 = x + y + z - 6, f_2 = x^2 + x^2 + y^2 - 14, f_3 = x^3 + y^3 + z^3 - 36$  が生成するイデアル  $I$  の  $<_{lex}$  に関するグレブナー基底を求めたい... がそれは一般には難しい.

グレブナー基底を求める方法... ブッフベルガーアルゴリズム

多項式を多項式の集合で割ることを考える.

## 定義

多項式環  $K[x]$  において, 単項式順序  $<$  を固定し,  $F = \{f_1, f_2, \dots, f_s\}$  を 0 でない  $K[x]$  の相違なる多項式の集合とする. このとき,  $f \in K[x]$  を  $F$  で割るとは, 次の条件をみたすときにいう.

- ❶  $f = g_1 f_1 + g_2 f_2 + \dots + g_s f_s + r$  となる  $g_1, g_2, \dots, g_s, r \in K[x]$  が存在する.
- ❷  $r$  は単項式イデアル  $(\text{in}_<(f_1), \text{in}_<(f_2), \dots, \text{in}_<(f_s))$  に属さない.

このときの  $r$  を  $f$  の  $F$  に関する余りという.



$K[x] = K[x_1, x_2, x_3]$  とし,  $f = x_1^3 - x_1^2x_2 - x_1^2 - 1$  の  
 $f_1 = x_1^2 - x_3, f_2 = x_1x_2 - 1$  に関する余りを求める.

$$f = (x_1 - x_2 - 1)f_1 + (x_1x_3 - x_2x_3 - x_3 - 1)$$

$$f = (x_1 - 1)f_1 - x_1f_2 + (x_1x_3 - x_1 - x_3 - 1)$$

となるので,  $x_1x_3 - x_2x_3 - x_3 - 1$  と  $x_1x_3 - x_1 - x_3 - 1$  はいずれも  $f$  の  $f_1, f_2$  に関する余り. 実際,  $\text{in}_<(f_1) = x_1^2, \text{in}_<(f_2) = x_1x_2$  であるのでいずれの余りもこのイニシャル単項式が生成するイデアルに属さない.

$f$  を  $f_1, f_2, \dots, f_s$  で割ることを考える. まず,  $g_1 = g_2 = \dots = g_s = r = 0$  とし,  $d_f$  を  $\text{in}_<(f)$  の実数の係数とする.

①  $D = \{i | c \in K[x], c \times \text{in}_<(f_i) = \text{in}_<(f)\}$  とする.

②  $j = \min D$  とし,  $f - \frac{d_f \text{in}_<(f)}{d_f \text{in}_<(f_j)} f_j$  を新しい  $f$ ,  $g_j + \frac{d_f \text{in}_<(f)}{d_f \text{in}_<(f_j)}$  を新しい  $g_j$  とする.

③  $f - d_f \text{in}_<(f)$  を新しい  $f$ ,  $r + d_f \text{in}_<(f)$  を新しい  $r$  とする.

初めに (i) を実行し,  $D \neq \emptyset$  なら (ii),  $D = \emptyset$  なら (iii) を行うと,  $f$  の項数が減っていく. 最終的に 0 になったらこの手順は終了で,

$f = g_1 f_1 + g_2 f_2 + \dots + g_s f_s + r$  となる.

$K[x] = K[x_1, x_2, x_3]$  とし,  $f = x_1^3 - x_1^2x_2 - x_1^2 - 1$  の

$f_1 = x_1x_2 - 1, f_2 = x_1^2 - x_3$  に関する余りを求める.  $<$  は辞書式順序とする.

$f$  はそのまま,  $g_1 = g_2 = r = 0$ , イニシャル単項式は  $f : x_1^3, f_1 : x_1x_2, f_2 : x_1^2$ .

$D = \{2\}$  より  $f - \frac{x_1^3}{x_1^2}f_2 = -x_1^2x_2 - x_1^2 + x_1x_3 - 1$  を新しい  $f, g_2 + \frac{x_1^3}{x_1^2} = x_1$  を

新しい  $g_2$ . このとき,  $\text{in}_<(f) = x_1^2x_2$

$D = \{1, 2\}$  より  $f - \frac{-x_1^2 x_2}{x_1 x_2} f_1 = -x_1^2 + x_1 x_3 - x_1 - 1$  を新しい  $f$ ,

$g_1 + \frac{-x_1^2 x_2}{x_1 x_2} = -x_1$  を新しい  $g_1$ . このとき,  $\text{in}_<(f) = x_1^2$

$D = \{2\}$  より  $f - \frac{-x_1^2}{x_2} f_2 = x_1 x_3 - x_1 - 1$  を新しい  $f$ ,  $g_2 + \frac{-x_1^2}{x_2} = x - 1$  を新しい  $g_1$ . このとき,  $\text{in}_<(f) = x_1 x_3$

いま,  $f$  に現れる単項式について,  $D = \emptyset$  となるものしかないので,  $r = f$  として終了. 結果は  $f = g_1 f_1 + g_2 f_2 + r = (x_1 - 1) f_1 - f_2 + x_1 x_3 - x_1 - x_3 - 1$ .

次に,  $S$  多項式というものを定義する. これは, 2つの多項式のそれぞれのイニシャル単項式を打ち消しあうものである. 定義は次の通り.

### 定義

多項式環  $K[x]$  に属する  $0$  でない多項式  $f, g$  について,  $m(f, g)$  を  $\text{in}_<(f)$  と  $\text{in}_<(g)$  の最小公倍単項式とする. このとき,  $f$  と  $g$  の  $S$  多項式  $S(f, g)$  は以下で計算される.

$$S(f, g) = \frac{m(f, g)}{d_f \text{in}_<(f)} f - \frac{m(f, g)}{d_g \text{in}_<(g)} g$$

$K[x] = K[x_1, x_2]$  として,  $K[x]$  に属する多項式を

$f_1 = x_1^2 + 2, f_2 = 2x_1x_2 + x_1$  とする. このとき,  $f_1$  と  $f_2$  の  $S$  多項式は

$$S(f_1, f_2) = \frac{x_1^2x_2}{x_1^2}f_1 - \frac{x_1^2x_2}{2x_1x_2}f_2 = -\frac{x_1^2}{2} + 2x_2.$$

次に紹介するのは、イデアルの生成元が分かっているときに有効な手段である。

## 定理

多項式環  $K[x]$  と単項式順序  $<$  を固定し、 $K[x]$  のイデアル  $I$  の生成元が  $F = \{f_1, f_2, \dots, f_s\}$  であったとする。このとき、 $I$  のグレブナー基底が  $F$  である必要十分条件は、 $S(f_i, f_j)$  ( $1 \leq i < j \leq s$ ) を  $F$  で割った余りが  $0$ 、である。

もし余りが  $0$  でなかった場合、その余りを  $F$  に加えれば余りは  $0$  になる。これを繰り返していくのがブッフベルガーアルゴリズムである。

$K[x] = K[x, y, z]$  と単項式順序  $<_{lex}$  を固定し, 多項式  $f_1 = x + y + z - 6, f_2 = x^2 + x^2 + y^2 - 14, f_3 = x^3 + y^3 + z^3 - 36$  が生成するイデアル  $I$  の  $<_{lex}$  に関するグレブナー基底を求める.  $F = (f_1, f_2, f_3)$  とし,  $<_{lex}$  を単に  $<$  とかく.

- まず,  $S(f_1, f_2)$  を求める.

$$S(f_1, f_2) = xf_1 - f_2 = xy + xz - 6x - y^2 - z^2 + 14$$

- これを  $F$  で割ったときの余りを求める. すると,  $y^2 + z^2 + yz - 6y - 6z + 11$  である. これを  $f_4$  とし,  $F$  に加える. これにより,  $S(f_1, f_4)$  と  $S(f_2, f_4)$  は  $F$  で割った余りがそれぞれ 0 になる.
- $S(f_2, f_3)$  を求める. すると,  $xy^2 + xz^2 - 14x - y^3 - z^3 + 36$  となる.



- これを  $F$  で割ったときの余りを求める. すると,  $z^3 - 6z^2 + 11z - 6$  となる. これを  $f_5$  とし,  $F$  に加える.
- ここで,  $S(f_3, f_4) = y^2 f_3 - x^3 f_4$  であるが,  $f_3, f_4$  は  $F$  で割り切れるので  $S(f_3, f_4)$  を  $F$  で割った余りは  $0$  になる. 同様にして  $S$  多項式を  $F$  で割った余りが  $0$  であることがいえる. よってグレブナー基底は  $F = \{f_1, f_2, f_3, f_4, f_5\} = \{x + y + z - 6, x^2 + x^2 + y^2 - 14, x^3 + y^3 + z^3 - 36, y^2 + z^2 + yz - 6y - 6z + 11, z^3 - 6z^2 + 11z - 6\}$  である.

以上より,  $f_1 = f_2 = f_3 = 0$  の連立方程式

$$\begin{cases} x + y + z & = 6 \\ x^2 + y^2 + z^2 & = 14 \\ x^3 + y^3 + z^3 & = 36 \end{cases}$$

の解を求めることができる.  $f_5 = z^3 - 6z^2 + 11z - 6 = (z-1)(z-2)(z-3)$  より,  $f_5 = 0$  とすれば  $z = 1, 2, 3$ . これを  $f_4$  に代入し  $y$ ,  $f_1$  に代入し  $x$  の値が求まる.

$$(x, y, z) = (1, 2, 3), (1, 3, 2), (2, 1, 3), (2, 3, 1), (3, 1, 2), (3, 2, 1)$$

グレブナー基底はイデアル  $I$  を生成するという性質より,  $f_2, f_3$  は  $f_1, f_4, f_5$  で書き換えることができる. すると,  $F' = \{f_1, f_4, f_5\}$  もグレブナー基底である. このように, 単項式順序  $<$  とイデアル  $I$  についてのグレブナー基底は複数ある. そのなかで, 最も単純なものを被約グレブナー基底という. 定義は以下の通り.

## 定義

$G = \{g_1, g_2, \dots, g_s\}$  をグレブナー基底として,

- (i)  $d_i = 1$
- (ii)  $i \neq j$  のとき,  $g_i$  に現れる単項式は  $g_j$  で割り切れないとき  $G$  を被約グレブナー基底という.

先の例でいうと,  $F'$  は被約グレブナー基底である.

# まとめ

$$\begin{cases} x + y + z & = 6 \\ x^2 + y^2 + z^2 & = 14 \\ x^3 + y^3 + z^3 & = 36 \end{cases}$$

# まとめ

$$\begin{cases} x + y + z & = 6 \\ x^2 + y^2 + z^2 & = 14 \\ x^3 + y^3 + z^3 & = 36 \end{cases}$$



# まとめ

$$\begin{cases} x + y + z & = 6 \\ x^2 + y^2 + z^2 & = 14 \\ x^3 + y^3 + z^3 & = 36 \end{cases}$$



$$\begin{cases} x + y + z - 6 = 0 \\ x^2 + x^2 + y^2 - 14 = 0 \\ z^3 - 6z^2 + 11z - 6 = 0 \end{cases}$$

グレブナー基底で多項式で割ると余りが一意に存在する. 例えば,  
 $G = \{x - 1, y - 2\}$  はグレブナー基底の一つであるが,  $f = x^2 + 3y^2 - xy + 5$   
 を  $G$  で割ると,  $g_1 = x - 1, g_2 = y - 2$  としたら

$f = (x - y + 1)g_1 + (3y + 5)g_2 + 16, g_1 = y - 2, g_2 = x - 1$  としたら  
 $f = (3y - x + 6)g_1 + (x - 1)g_2 + 16$  となり, 確かに一致している. これより,  
 余りによって多項式環を分解できるのではないかと思ったので, それを考  
 えてみたい.

- 桂利行, 代数学 I 群と環, 大学数学の入門, 東京大学出版社, 2018.
- 日比孝之, すうがくの風景 8 グレブナー基底, 2003
- 丸山正樹, グレブナー基底とその応用, 共立出版, 2002.