グレブナー基底はよい水

芝浦工業大学 数理科学研究会
BV18051　千葉龍朗

令和元年 11 月 1 日

目次

1　研究動機

グレブナー基底という言葉を耳にしたことがある人は多いだろう．とあるネット記事[*1]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.

2　グレブナー基底って何?

簡単に言うと, 多項式環のイデアルの生成系の中のとても優れたもの, である．1965 年にオーストリアの大学院生であった Bruno Buchberger が発表し, 当時の指導教授であった Wolfgang Gröbner の名前をとりグレブナー基底と名付けた．連立方程式を解くためのアルゴリズムや, 組み合わせ論, 可換代数などに使われる．また, グレブナー基底で多項式を割ると, 余りが一意に存在するという性質がある.

本研究では, グレブナー基底の定義の意味と, 使い方の一例について説明する.

3　可換環とイデアル

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．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 $e_\times$ が存在し, 任意の $a \in R$ に対して $a \times e_\times = e_\times \times a = a$.
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.

e_+ を R の零元, $e_\times$ を R の単位元と呼ぶ．$a \in R$ の逆元は $-a$ であり, $a - b = a + (-b)$ とかくことにする.

乗法の記号 $\times$ はよく省略される．乗法について可換だった場合, R を可換環という．また, 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．普通, 体は K で表す.

例 3.1.

- R が整数全体の集合 $\mathbb{Z}$, 有理数全体の集合 $\mathbb{Q}$, 実数全体の集合 $\mathbb{R}$, 複素数全体の集合 $\mathbb{C}$ のいず

[*1] 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.

れかとする. このとき, R の加法と乗法を通常の足し算, 掛け算で定義した場合, R は可換環である.

- R が 2 次正方行列の集合だった場合, R は環であるが, 可換環でない. 行列は一般に積について可換でないためである.

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.

例 3.2. $R = Z$ とし, R のイデアル I に 3 が含まれていたとする. このとき, イデアルの条件 (i) より $3 + 3 = 6 \in R$ でなければならない. 同様にして, $9, 12, 15, ..., 3n \in R \quad (n \in \mathbb{N})$ ということが分かる. また, $r = -1$ としたら, $3 \times (-1) = -3 \in R$ でなければならない. よって, $I = \{3n | n \in \mathbb{Z}\}$ ということが分かる.

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

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

なる表示をもつ元の全体は R のイデアルである. このとき, $(F) = (\{y_1, y_2, ..., y_s\})$ を $(y_1, y_2, ..., y_s)$ と略記し, $y_1, y_2, ..., y_s$ が生成するイデアルという. 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. 例は多項式を導入した後に載せる.

4 単項式と多項式

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 $x_1, x_2, ..., x_n$ 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. すると, 1 は次数 0 の単項式である. ここで, 煩雑な表現を避けるため, 変数のべき指数を成分とする n 項ベクトル

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

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. また, 単項式を u, v, w と表すこともある.

例 4.1. 変数を x_1, x_2, x_3, x_4 とする. 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.

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

$$K[x] = K[x_1, x_2, ..., x_n]$$

と表す. このとき, 変数 $x_1, x_2, ..., x_n$ の多項式とは線形空間 $K[x]$ に属する元 $f = f(x_1, x_2, ..., x_n)$ のことである. すると, f は

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

と表示できる. f に現れる単項式の次数がすべて d であるとき, f を次数 d の斉次多項式という.

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

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

と定義する. すると, 線形空間 $K[x]$ 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.

例 4.2. 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. $I = \{c_1(x_1 + 3) + c_2(x_2 - 2) | c_1, c_2 \in K[x]\}$ 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.

5 グレブナー基底

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

(i) 任意の $1 \neq u \in \mathcal{M}$ について $1 < u$ である
(ii) $u, v \in \mathcal{M}$ で $u < v$ ならば, 任意の $w \in \mathcal{M}$ について $uw < vw$ である

をみたすとき, $<$ を $K[x]$ の単項式順序という.

例 5.1. 単項式順序の代表例として, 辞書式順序と逆辞書式順序がある.

辞書式順序は次で定義される.

定義 5.1. 相違なる単項式 $\mathbf{x}^{\mathbf{a}}$, $\mathbf{x}^{\mathbf{b}}$ において

(i) $\mathbf{x}^{\mathbf{b}}$ の次数は $\mathbf{x}^{\mathbf{a}}$ の次数を超える.
(ii) $\mathbf{x}^{\mathbf{a}}$ と $\mathbf{x}^{\mathbf{b}}$ の次数が等しく, さらにベクトルの差 $b - a$ において, 最も左にある 0 でない成分が正.

であるとき, $\mathbf{x}^{\mathbf{a}} <_{lex} \mathbf{x}^{\mathbf{b}}$ とする.

例えば, $K[x] = K[x_1, x_2, x_3]$ において, $x_1^2x_2^4x_2 <_{lex} x_1^3x_2x_3^3$ である.

また, 逆辞書式順序は次で定義される.

定義 5.2. 相違なる単項式 $\mathbf{x}^{\mathbf{a}}$, $\mathbf{x}^{\mathbf{b}}$ において

(i) $\mathbf{x}^{\mathbf{b}}$ の次数は $\mathbf{x}^{\mathbf{a}}$ の次数を超える.

(ii) $\mathbf{x^a}$ と $\mathbf{x^b}$ の次数が等しく, さらにベクトルの差 $b-a$ において, 最も右にある 0 でない成分が負.

であるとき, $\mathbf{x^a} <_{rev} \mathbf{x^b}$ とする.

先の例でいうと, $x_1^3x_2x_3^3 <_{rev} x_1^2x_2^4x_3$ である.

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, $\mathrm{in}_<(f)$ と表す. また, $K[x]$ 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 $\mathrm{in}_<(I)$ と表す. つまり, $\mathrm{in}_<(I) = \{\mathrm{in}_<(f) | f \in I\}$

例 5.2. $K[x] = K[x_1, x_2, x_3]$ と, 単項式順序 $<_{lex}$ において, 多項式 $f = x_2x_3 + 4x_1x_3 - 2x_1^2x_2 + 3x_1^2x_3$ のイニシャル単項式 $\mathrm{in}_{<_{lex}}(f)$ は $x_1^2x_2$ である.

さて, いよいよグレブナー基地の定義に入ろう. 多項式環 $K[x]$ の単項式順序 $<$ と $K[x]$ のイデアル $I \neq \{0\}$ について, I に属する 0 でない多項式の有限集合 $\mathcal{G} = \{g_a, g_2, ..., g_s\}$ が $<$ に関する I のグレブナー基底であるとは, 次が成立するときにいう.

$$\mathrm{in}_<(I) = (\mathrm{in}_<(g_1), \mathrm{in}_<(g_2), ..., \mathrm{in}_<(g_s))$$

例 5.3. $K[x] = [x_1, x_2]$ と単項式順序 $<_{lex}$ において, $f_1 = x_1 + 2x_2 - 5$, $f_2 = 2x_1 - 3x_2 + 4$ が生成するイデアル I のグレブナー基底は, $\{x_1 - 1, x_2 - 2\}$ である. 実際, I のイニシャルイデアルは, $\{x_1, x_2, x_1^2, x_1x_2, x_2^2, x_1^3, ...\}$ であり, $\mathrm{in}_<(x_1 - 1) = x_1$, $\mathrm{in}_<(x_2 - 2) = x_2$, これらは $\mathrm{in}_<(I)$ を生成し, $x_1 - 1 = \dfrac{3}{7}f_1 + \dfrac{2}{7}f_2$, $x_2 - 2 = \dfrac{2}{7}f_1 - \dfrac{1}{7}f_2$ より $x_1 - 1, x_2 - 2 \in I$ である. また, このイデアルにおいては辞書式順序と逆辞書式順序でのイニシャル単項式は同じ値をとるので, $<_{rev}$ においてのグレブナー基底も $\{x_1 - 1, x_2 - 2\}$ である.

ここで, $K[x]$ のイデアルについていくつかの定理を紹介しよう. 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. まず, 次の Dickson の補題というのを説明するため, 新しい順序を導入する. $K[x]$ 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, $au = v, a \in R \Rightarrow u \leq v$.

定理 5.3 (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.

この定理により, 次の定理が導ける.

定理 5.4. 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 には最小限が存在する.

この定理により, 任意のイデアルと単項式順序 $<$ において $\cdot < u_{j-1} < u_j < u_{j+1} < \cdots < u_1 < \mathrm{in}_<(f)$ 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 5.5 (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, 次の重要な定理が分かる.

定理 5.6. 多項式環 $K[x]$ の単項式順序 $<$ と $K[x]$ のイデアル $I \neq \emptyset$ について, $\mathcal{G} = \{g_1, g_2, ..., g_s\}$ が $<$ に関する I のグレブナー基底であるならば $\mathcal{G}$ は I の生成系である.

これにより, $f \in I$ としたとき, $f = y_1g_1 + y_2g_2 + \cdots + y_sg_s(y_i \in K[x], i = 1, 2, ...)$ と分解できる. よって, $g_1 = g_2 = \cdots = g_s$ なら $f = 0$ が成り立つ. これが連立方程式の解となる理論的根拠である[*2].

6 ブッフベルガーアルゴリズム

一般に, イデアル I が与えられていたとき, そのグレブナー基底を求めるのは難しい. だが, グレブナー基底を求めるアルゴリズムが存在する. それはブッフベルガーアルゴリズムとよばれ, 数式処理ソフトなどにも実装されている. それがどういったものなのかを説明するため, まずは必要な知識を導入する.

定義 6.1. 多項式環 $K[x]$ において, 単項式順序 $<$ を固定し, $F = \{f_1, f_2, ..., f_s\}$ 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.

(i) $f = g_1f_1 + g_2f_2 + \cdots g_sf_s + r$ となる $g_1, g_2, ..., g_s, r \in K[x]$ が存在する.
(ii) r は単項式イデアル $(\mathrm{in}_<(f_1), \mathrm{in}_<(f_2), ..., \mathrm{in}_<(f_s))$ に属さない.

このときの r を f の F に関する余りという.

例 6.1. $K[x] = K[x_1, x_2, x_3]$ 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. すると,

$$f = (x_1 - x_2 - 1)f_1 + (x_1x_3 - x_2x_3 - x_3 - 1)$$
$$f = (x_1 - 1)f_1 - x_1f_2 + (x_1x_3 - x_1 - x_3 - 1)$$

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 に関する余りである. 実際, $\mathrm{in}_<(f_1) = x_1^2$, $\mathrm{in}_<(f_2) = x_1x_2$ 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.

この割り算をアルゴリズムとして実行する方法はいくつかあるが, その一つを紹介しよう. f を $f_1, f_2, ..., f_s$ で割ることを考える. まず, $g_1 = g_2 = \cdots = g_s = r = 0$ とし, d_f を $\mathrm{in} < (f)$ の実数の係数とする.

(i) $D = \{i | c \in K[x], c \times \mathrm{in}_<(f_i) = \mathrm{in}_<(f)\}$ とする.
(ii) $j = \min D$ とし, $f - \dfrac{d_f\mathrm{in}_<(f)}{d_f\mathrm{in}_<(f_j)}f_j$ を新しい f, $g_j + \dfrac{d_f\mathrm{in}_<(f)}{d_f\mathrm{in}_<(f_j)}$ を新しい g_j とする.
(iii) $f - d_f\mathrm{in}_<(f)$ を新しい f, $r + d_f\mathrm{in}_<(f)$ 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, $f = g_1f_1 + g_2f_2 + \cdots g_sf_s + r$ となる. このアルゴリズムを割り算ア

[*2] 証明は理解できてないので略

ルゴリズムという.

次に, S 多項式というものを定義する. これは, 2 つの多項式のぞ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 6.2. 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 $\mathrm{in}_<(f)$ と $\mathrm{in}_<(g)$ 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.

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

例 6.2. $K[x] = K[x_1, x_2]$ 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 $S(f_1, f_2) = \dfrac{x_1^2 x_2}{x_1^2} f_1 - \dfrac{x_1^2 x_2}{2x_1x_2} f_2 = -\dfrac{x_1^2}{2} + 2x_2$.

さて, いよいよブッフベルガーアルゴリズムを紹介する. ただし, これ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 6.3. 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 $F = \{f_1, f_2, ..., f_s\}$ であったとする. このとき, I のグレブナー基底が I 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.

この証明は難しくて理解できていない.

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.

7 具体例

$K[x] = K[x, y, z]$ 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.

(1) まず, $S(f_1, f_2)$ を求める.

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

(2) 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.

(3) $S(f_2, f_3)$ を求める. すると, $xy^2 + xz^2 - 14x - y^3 - z^3 + 36$ となる.

(4) 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.

(5) 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.

ここで, 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.

$G = \{g_1, g_2, ..., g_s\}$ 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' はグレブナー基底である.

実は, これは次の連立方程式

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

の解を求めるのに役に立つ. $f_5 = z^3 - 6z^2 + 11z - 6 = (z-1)(z-2)(z-3)$ より, $f_5 = 0$ とすれば $z = 1, 2, 3$ という解が出てくる. これを f_4, f_1 に代入すると, すべての解は

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

となる. これは, グレブナー基底は I を生成する, つまり f_1, f_2, f_3 は f_1, f_4, f_5 で表すことができることを利用している. また, f_1, f_4, f_5 のイニシャル単項式は違う変数で表されるので, 比較的解きやすい.

以上より, グレブナー基底の有効性が理解できただろう. まとめると, グレブナー基底は複雑な多項式を薄めて分かりやすくする水のようなものであると言える.

8 気になったこと

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.

参考文献

[1] 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.
[2] 日比孝之, すうがくの風景 8 グレブナー基底, 2003.
[3] 丸山正樹, グレブナー基底とその応用, 共立出版, 2002.