

# 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

## 1 研究動機

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。

## 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優れたもの、である。連立方程式を解くために使われたり、組み合わせ論、可換代数などにも応用されている。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 定義

本節では、グレブナー基底に関する数学的用語の中で最も重要な部分を述べるので、詳細については資料を参照してほしい。読みたくない人は次節に進んでも問題ない。

多項式環  $K[x] = K[x_1, x_2, \dots, x_n]$  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。

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。

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  $\mathcal{G} = \{g_1, g_2, \dots, g_s\}$  が  $<$  に関する  $I$  のグレブナー基底であるとは、次が成立するときという:

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

これより、 $\mathbf{f} = \mathbf{y}_1 \mathbf{g}_1 + \mathbf{y}_2 \mathbf{g}_2 + \dots + \mathbf{y}_s \mathbf{g}_s$  をみたす  $\mathbf{y}_1, \dots, \mathbf{y}_s$  が存在することを表すという事実が示せる。

## 4 具体例

$f_1 = x + y + z - 6, f_2 = x^2 + x^2 + y^2 - 14, f_3 = x^3 + y^3 + z^3 - 36$  として、 $f_1 = f_2 = f_3 = 0$  という連立方程式を解くとする。普通にやるとしたら色々工夫が必要で計算が大変であるが、グレブナー基底の考え方をを用いることである程度簡単に解くことができる。前節で書いたように、グレブナー基底を  $\{g_1, g_2, \dots, g_s\}$  としたら、 $f = y_1 g_1 + y_2 g_2 + \dots + y_s g_s$  が成り立つ。つまり、 $g_1 = g_2 = \dots = g_s = 0$  ならば  $f = 0$  となる。 $g_1 = g_2 = \dots = g_s = 0$  という連立方程式は元の連立方程式と解が一致し、なおかつ解きやすいものになっている。

実際にグレブナー基底を求めてみよう。多項式環のイデアル  $I$  を  $\{C_1 f_1 + C_2 f_2 + C_3 f_3 \mid C_1, C_2, C_3 \in R[x, y, z]\}$ 、単項式順序を  $x > y > z$  とする。色々計算すると、 $I$  のグレブナー基底  $\mathcal{G}$  は、以下のようになる:

$$\begin{aligned} \mathcal{G} &= \{g_1, g_2, g_3, g_4, g_5\} \\ &= \{f_1, f_2, f_3, y^2 + z^2 + yz - 6y - 6z + 11, z^3 - 6z^2 + 11z - 6\}. \end{aligned}$$

このとき、方程式  $g_5 = z^3 - 6z^2 + 11z - 6 = 0$  は一変数多項式なので、解を簡単に求めることができる。 $g_5 = (z-1)(z-2)(z-3)$  より、 $z = 1, 2, 3$  という解が求まった。これを  $g_4 = y^2 + z^2 + yz - 6y - 6z + 11 = 0$  に代入すれば  $y$ 、さらにそれらを  $g_1 = f_1$  に代入すれば連立方程式の解が求まる。解は以下の通り:

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

このように、グレブナー基底を求めさえすれば解は簡単に求まる。また、グレブナー基底の求め方はブッフベルガーアルゴリズムと呼ばれ、機械的に求めることが可能なので、数式処理ソフトなどに実装されている。

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。

## 5 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ということは、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] 日比孝之, すうがくの風景 8 グレブナー基底, 朝倉書店, 2003.
- [2] 丸山正樹, グレブナー基底とその応用, 共立出版, 2002.

<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ボン酢が合う」, 2019/10/20 最終閲覧。