グレブナー基底をなんとか活用したい

BV18051 千葉龍朗

2020 年 11 月 15 日

1　動機

昨年私はグレブナー基底の概要を勉強した. そのときに参考にした本では, トーリック環なるものや, 代数多様体などにグレブナー基底が活用できると書いてあった. しかしそれらの分野を扱うには私の理解力と根気が足りなすぎるため, 身近なところから使えるようなグレブナー基底の応用例を考えてみた.

2　グレブナー基底とは

初めにグレブナー基底について軽く説明を与える. 次に出てくる定義や定理は以前私が研究したものから抜粋した. 与えられていない証明については参考文献を参照のこと. おおざっぱに説明すると,

$$\begin{cases} x+y & =2 \\ 2x+3y & =3 \end{cases}$$

を

$$\begin{cases} (x-3)+(y+1) & =0 \\ 2(x-3)+3(y+1) & =0 \end{cases}$$

と変形するときにグレブナー基底という概念が役に立つ.

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 2.1. 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 2.1. 相違なる単項式 $\mathbf{x^a}$, $\mathbf{x^b}$ において

(i) $\mathbf{x^b}$ の次数は $\mathbf{x^a}$ 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, 最も左にある 0 でない成分が正.

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

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.
また, 逆辞書式順序は次で定義される.

定義 2.2. 相違なる単項式 $\mathbf{x^a}$, $\mathbf{x^b}$ において

(i) $\mathbf{x^b}$ の次数は $\mathbf{x^a}$ 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, $x_1^3 x_2 x_3^3 <_{rev} x_1^2 x_2^4 x_3$ である.

定義 2.3. 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 2.2. $K[x] = K[x_1, x_2, x_3]$ と, 単項式順序 $<_{lex}$ において, 多項式 $f = x_2 x_3 + 4x_1 x_3 - 2x_1^2 x_2 + 3x_1^2 x_3$ のイニシャル単項式 $\mathrm{in}_{<_{lex}}(f)$ は $x_1^2 x_2$ である.

定義 2.4 (グレブナー基底)**.** 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 2.3. $K[x] = [x_1, x_2]$ 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, $\{x_1, x_2, x_1^2, x_1 x_2, x_2^2, x_1^3, ...\}$ 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, $x_1 - 1 = \frac{3}{7} f_1 + \frac{2}{7} f_2$, $x_2 - 2 = \frac{2}{7} f_1 - \frac{1}{7} f_2$ 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.

定義 2.5. $K[x]$ 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 2.6 (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.

定理 2.7. 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.

定理 2.8 (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.

定理 2.9. 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.

つぎにグレブナー基底を求めるアルゴリズムであるブッフベルガーアルゴリズムの説明をする.

定義 2.10. 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 2.4. $K[x]=K[x_1,x_2,x_3]$ 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 2.11. 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 2.5. $K[x]=K[x_1,x_2]$ 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 $S(f_1,f_2)=\dfrac{x_1^2x_2}{x_1^2}f_1-\dfrac{x_1^2x_2}{2x_1x_2}f_2=-\dfrac{x_1^2}{2}+2x_2$.

定理 2.12 (ブッフベルガーアルゴリズム)**.** 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, $S(f_i,f_j)\quad(1\leq i<j\leq s)$ 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. このアルゴリズムは手計算で行うことも出来るが, 項が増えてくると複雑な計算が求められるので, 今回は MATLAB という数式処理システムを使った.

3　活用例

グレブナー基底の一番わかりやすい使い方はは, 多項式の連立方程式の求め方であろう. これを一般の方程式にも使えないだろうか. 例えば, 三角関数や対数関数などが絡んだ方程式にもグレブナー基底は使うことはできるのだろうか. これについて私が思いついた方法は, テイラー展開やマクローリン展開を用いて多項式方程式に変換するものである. 一般に, 三角関数 $\sin x$ と $\cos x$ はマクローリン展開によって次のように表すことができる.

$$\sin x = \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n+1)!} x^{2n+1}$$
$$\cos x = \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n)!} x^{2n}$$

これを用いて, 次のような連立方程式を考えてみる.

$$\begin{cases} \sin x + 2\cos y & = -1 \\ -3\sin x + \cos y & = -4 \end{cases}$$

これの解は $\sin x = 1$, $\cos x = -1$ より, $0 \leq x, y < 2\pi$ の範囲では $x = \dfrac{\pi}{2}$, $y = \pi$ である. この連立方程式を次のように表してみる.

$$\begin{cases} \sum_{n=0}^{\infty} \frac{(-1)^{2n+1}}{(2n+1)!} x^{2n+1} + 2\sum_{n=0}^{\infty} \frac{(-1)^{2n}}{(2n)!} x^{2n} & = -1 \\ -3\sum_{n=0}^{\infty} \frac{(-1)^{2n+1}}{(2n+1)!} x^{2n+1} + \sum_{n=0}^{\infty} \frac{(-1)^{2n}}{(2n)!} x^{2n} & = -4 \end{cases}$$

試しに $n = 2$ で考えると

$$\begin{cases} \frac{x^5}{120} - \frac{x^3}{6} + x + \frac{y^4}{12} - y^2 + 2 & = -1 \\ -\frac{x^5}{40} + \frac{x^3}{2} - 3x + \frac{y^4}{24} - \frac{y^2}{2} + 1 & = -4 \end{cases}$$

となる. この連立方程式を求めるため, 次のようなイデアルと単項式順序 $<_{lex}$ を考える.

$$I = \left\langle \frac{x^5}{120} - \frac{x^3}{6} + x + \frac{y^4}{12} - y^2 + 3, -\frac{x^5}{40} + \frac{x^3}{2} - 3x + \frac{y^4}{24} - \frac{y^2}{2} + 5 \right\rangle$$

$f_1 = \dfrac{x^5}{120} - \dfrac{x^3}{6} + x + \dfrac{y^4}{12} - y^2 + 3$, $f_2 = -\dfrac{x^5}{40} + \dfrac{x^3}{2} - 3x + \dfrac{y^4}{24} - \dfrac{y^2}{2} + 5$ とする. $S(f_1, f_2)$ を考える.

$$\begin{aligned} S(f_1, f_2) &= \frac{x^5}{\frac{x^5}{120}} f_1 - \frac{x^5}{\frac{x^5}{40}} f_2 = 120 f_1 + 40 f_2 \\ &= x^5 - 20x^3 + 120x + 10y^4 - 120y^2 + 360 - x^5 + 20x^3 - 120x + \frac{5}{3}y^4 - 20y^2 + 200 \\ &= \frac{35}{3}y^4 - 140y^2 + 560 = \frac{35}{3}(y^4 - 12y^2 + 48) \end{aligned}$$

$f_3 = y^4 - 12y^2 + 48$ とする. また,

$$\begin{aligned} f_1 - \frac{1}{12} f_3 &= \frac{x^5}{120} - \frac{x^3}{6} + \frac{y^4}{12} - y + 3 - \frac{y^4}{12} + y^2 - 4 \\ &= \frac{x^5}{120} - \frac{x^3}{6} + x - 1 = \frac{1}{120}(x^5 - 20x^3 + 120x - 120) \end{aligned}$$

$f_4 = x^5 - 20x^3 + 120x - 120$ とする. グレブナー基底の性質などにより, $I = \langle f_1, f_2 \rangle = \langle f_4, f_3 \rangle$ である. $f_3 = f_4 = 0$ をとくと実数解は次のようになる. 計算には MATLAB を用いた.

$$
\begin{aligned}
x \simeq & 1.4913201862260734659300986146501 \\
& 1.6945891766777537111869580103181 \\
& 3.6809841929847214378308420126325 \\
& -3.4334467779442743074739493188003 \pm 1.0541410148822538705740251121561i \\
y \simeq & \pm 2.5424597568374124782712259820421 \pm 0.6812500386332132803887884880756 6i
\end{aligned}
$$

y は複合同順ではない. 実部のみをみると, x は $\dfrac{\pi}{2}$ と, y は π と大きく離れてはいない. n を増やして計算したものが次の表である.

n	解の一部
1	$1.42366105093153631975945812327 53 \pm 0.28360600102688122282340658269 62i$
2	$1.4913201862260734659300986146501$
3	$1.56990689986954391753845906435 99 \pm 0.01765188090323510299293051195 1834i$
4	$1.56815894641110787592556907493 7$
5	$1.57079586203100728262424696506 33 \pm 0.00033543595901027078524256344 846082i$
6	$1.57075992487149364432194017319 13$
7	$1.57079632672976300875707131650 48 \pm 0.00000347085607688783217841718 61184546i$
8	$1.57079603178772188424190788781 74$
9	$1.57079632679489319983080024765 65 \pm 0.00000002262224219579978906208 1692666968i$
10	$1.57079632520784383232487189380 69$

表 1　$\sin x$ についての多項式の解

n	解の一部
1	± 2
2	$\pm 2.5424597568374124782712259820421 \pm 0.6812500386332132803887884880756 6i$
3	$\pm 3.5358512901488188969143280303023 \pm 1.1349901120762673856336025213004i$
4	$\pm 3.0813198896520597687893019424138 \pm 0.1914572255595679663455244266581 2i$
5	$\pm 3.0870830936139405367229293627 79$
6	$\pm 3.1411485506891669637201816814611 \pm 0.0141553400230411319377458486732 05i$
7	$\pm 3.1445011695040588898040758998222$
8	$\pm 3.1415918808081123508642041010143 \pm 0.0005201145629369182709369694029 4057i$
9	$\pm 3.1415086631450208914685119880321$
10	$\pm 3.1415926530608746202250555963953 \pm 0.0000123004751912886945255879079 98238i$

表 2　$\cos x$ についての多項式の解

この表より, n の値が増えるごとに x の実部の値は $\dfrac{2}{\pi} \simeq 1.5708$ に, y の値は $\pi \simeq 3.1415$ の値に近いものに

なっている.

4　今後やってみたいこと

今回は簡単な例で検証をしてみたが, 思いのほかうまくいったので複雑な例でも試してみたい. また, ここでやったことが微分方程式やフーリエ解析などに応用できるかも検証したい. 課題としては, x だけの式から解を求める際, 解が複数あるので我々が期待する解がどれなのかをはっきりさせられるようなシステムをつくりたい.

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.