グレブナー基底大好き bo 徒になろう

グレブナー基底大好き bot
@ groebner_basis

2016/09/18

- グレブナー基底の概略
- グレブナー基底の応用

グレブナー基底大好き bot とは

- グレブナー基底が大好きな bot
- 2015 年 9 月 20 日より Twitter で誕生
- 多項式環の精霊ぶなっしーという設定
- 語尾にぶながつく特徴的な話し方
- 「ぶなつい」でグレブナー基底についてわかりやすく解説
- 「ぶな本」を Kindle で売っている
- 最近では小説も書いている
- p 進大好き bot とは仲良し

グレブナー基底とは

定義 (グレブナー基底)

多項式環 $K[x_1, \ldots, x_n]$ のイデアル I に対して，有限集合 $G \subset I$ の先頭項から生成されるイデアルが，I の先頭項から生成されるイデアルに一致しているとき，G を I のグレブナー基底と呼ぶ．すなわち，

$$G \subset I \text{ がグレブナー基底} \underset{def}{\Leftrightarrow} \langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(G) \rangle.$$

ざっくり言うと

多項式の集合 $\{f_1, \ldots, f_r\}$ に対して，それをすごい性質のいいものに変えた多項式の集合 $\{f'_1, \ldots, f'_s\}$ のこと

グレブナー基底の具体例

問題 (連立方程式)

連立方程式

$$\begin{cases} x + y - 3 = 0 \\ x - y - 1 = 0 \end{cases}$$

の解は？

$$\begin{cases} x + y - 3 = 0 \\ x - y - 1 = 0 \end{cases} \longleftrightarrow I = \langle x + y - 3, x - y - 1 \rangle$$

$$\Downarrow \text{グレブナー基底}$$

$$x = 2, y = 1 \longleftrightarrow G = \{x - 2, y - 1\}$$

グレブナー基底の歴史

- 1965 年にオーストリア出身のブルーノ・ブッフベルガーによって発見される
- 博士論文で発表され，敬意を込めて彼の指導教官であるグレブナーから，「グレブナー基底」と名付けられた
- 1980 年代に数式処理ソフト Macaulay などに実装され，可換環論や代数幾何の計算に貢献することで脚光を浴びる
- 今や，Mathematica や GAP，Risa/Asir，Sage など多くの数式処理ソフトに組み込まれていて，他にも代数統計や微分方程式論，整数計画問題など様々な分野で応用されている

ざっくり言うと

グレブナー基底はコンピュータで計算できる，数学にすごく役に立つツール

グレブナー基底を理解するには，多項式環を理解することが必要

多項式の割り算

問題

$x^3 + x^2 + 1$ を $x^2 + 1$ で割ったときの商と余りは？

$$
\begin{array}{r}
x + 1 \\
\hline
x^2 + 1 \;\big)\; x^3 + x^2 \quad + 1 \\
\quad x^3 \quad + x \\
\hline
\qquad x^2 - x + 1 \\
\qquad x^2 \quad + 1 \\
\hline
\qquad\quad -x
\end{array}
$$

$$
x^3 + x^2 + 1 = \underset{\text{商}}{(x+1)}(x^2+1) + \underset{\text{余り}}{(-x)}
$$

一変数と二変数の違い

- 一変数：単項式の順序が，1 個しかない
  - $1, x, x^2, x^3, \ldots$
- 二変数：どう順序を入れればいいのか分からない
  - $x > y$ or $y > x$ ？
  - $x^2 > y$ or $y > x^2$ ？
  - $x^2 > xy$ or $xy > x^2$ ？

問題

x^2y を $x - xy$ で割ったときの商と余りは？

$$
\begin{array}{r|l}
 & xy + xy^2 + xy^3 + xy^4 + \cdots \\
\hline
x - xy & x^2y \\
 & x^2y - x^2y^2 \\
\hline
 & \quad x^2y^2 \\
 & \quad x^2y^2 - x^2y^3 \\
\hline
 & \quad\quad x^2y^3 \\
 & \quad\quad x^2y^3 - x^2y^4 \\
\hline
 & \quad\quad\quad x^2y^4 \\
 & \quad\quad\quad x^2y^4 - x^2y^5 \\
\hline
 & \quad\quad\quad\quad x^2y^5 \\
 & \quad\quad\quad\quad \ddots
\end{array}
$$

うまく順序を決めなければ，割り算が終わらない！

単項式順序

定義

多項式環 $K[x_1, \ldots, x_n]$

$x^\alpha := x_1^{\alpha_1} \cdots x_n^{\alpha_n}, \quad \alpha = (\alpha_1, \ldots, \alpha_n) \quad (\text{Ex. } x_1 x_2^2 = x^{(1,2)},\ n = 2)$

単項式の間の順序 $>$ が単項式順序とは，次の３つを満たすとき

1. 全順序である
2. $x^\alpha > x^\beta \Longrightarrow x^\alpha x^\gamma > x^\beta x^\gamma$
3. 整列順序である

ざっくり言うと

割り算するのに，いい感じの順序

1. 全順序

定義 (全順序)

順序 $>$ が全順序とは，任意の x^α, x^β に対し，

- $x^\alpha > x^\beta$
- $x^\alpha = x^\beta$
- $x^\alpha < x^\beta$

のいずれかが成り立つこと

ざっくり言うと

$x^3 + xy + 1$ のように，多項式の項が大きいものから順番に並べられるということ

2. 順番の保存

定義 (順番の保存)

順序 $>$ が，任意の $x^\alpha, x^\beta, x^\gamma$ に対し，

$$x^\alpha > x^\beta \Longrightarrow x^\alpha x^\gamma > x^\beta x^\gamma$$

が成り立つとき積の順番を保存するという．ここで，

$$x^\alpha x^\gamma = x_1^{\alpha_1+\gamma_1} \cdots x_n^{\alpha_n+\gamma_n}, \quad x^\beta x^\gamma = x_1^{\beta_1+\gamma_1} \cdots x_n^{\beta_n+\gamma_n}$$

ざっくり言うと

例えば，

$$x > y \Longrightarrow xy > y^2$$

つまり，$x^3 + xy + 1$ に，y をかけても，項の順番は変わらず，
$x^3y + xy^2 + y$ と書けるということ

3. 整列順序

定義 (整列順序)

順序 $>$ が整列順序とは，単項式の無限列

$$x^{\alpha_1} > x^{\alpha_2} > x^{\alpha_3} > x^{\alpha_4} > \cdots$$

対して，必ずある n が存在して，

$$x^{\alpha_n} = x^{\alpha_{n+1}} = x^{\alpha_{n+2}} = \cdots$$

となる時をいう

ざっくり言うと

無限に小さくすることはできないということ

単項式順序の例

例 (辞書式順序)

多項式環 $K[x, y]$
順序 $>$ を

$$x^a y^b > x^c y^d \underset{def}{\Leftrightarrow} \begin{cases} a > c \text{ または} \\ a = c \text{ かつ } b \geq d \end{cases}$$

ざっくり言うと

x の数が多い方が強い

辞書式順序

$>$ を辞書式順序とする

- $x > y$
- $x > y^2$
- $x > y^3$
- $x < xy$
- $x^2 > xy$
- $x > 1$
- $y > 1$
- $x^2 > xy^2$
- $x^3y^3 > x^3y^2$

辞書式順序での割り算

$x - xy \to -xy + x$

$$
\begin{array}{r}
-x \\
-xy + x \overline{\big)\ x^2y\ } \\
\underline{\ x^2y - x^2\ } \\
x^2
\end{array}
$$

よって,

$$x^2y = \underset{\text{商}}{(-x)}(-xy + x) + \underset{\text{余り}}{(x^2)}$$

辞書式順序での割り算

$x - xy \to -xy + x$ ⇐並べられる (1. 全順序)

$$
\begin{array}{r|l}
 & -x \\
\hline
-xy + x & x^2y \\
 & x^2y - x^2 \text{⇐順番が変わらない (2. 積の保存)} \\
\hline
 & x^2 \text{⇐無限に続かない（3. 整列順序）}
\end{array}
$$

よって,

$$
x^2y = \underset{\text{商}}{(-x)}(-xy + x) + \underset{\text{余り}}{(x^2)}
$$

命題

辞書式順序は単項式順序

証明.

次の３つを示せばいい

1. 全順序である
2. $x^a y^b > x^c y^d \Longrightarrow x^{a+e} y^{b+f} > x^{c+e} y^{d+f}$
3. 整列順序である

簡単なので割愛する □

ちなみに

n 変数でも同様に辞書式順序は定義できる
また，単項式順序は他にもたくさん（無限に）存在する

n 変数の辞書式順序

例 (辞書式順序)

多項式環 $K[x_1, \ldots, x_n]$

$x^\alpha := x_1^{\alpha_1} \cdots x_n^{\alpha_n}, \quad \alpha = (\alpha_1, \ldots, \alpha_n)$

$x^\beta := x_1^{\beta_1} \cdots x_n^{\beta_n}, \quad \beta = (\beta_1, \ldots, \beta_n)$

順序 $>$ を

$$x^\alpha > x^\beta \underset{def}{\Leftrightarrow} \begin{cases} \alpha_1 > \beta_1 \text{または} \\ \alpha_1 = \beta_1 \text{かつ} \alpha_2 \geq \beta_2 \text{または} \\ \alpha_1 = \beta_1 \text{かつ} \alpha_2 = \beta_2 \text{かつ} \alpha_3 \geq \beta_3 \text{または} \\ \vdots \\ \alpha_1 = \beta_1 \text{かつ} \alpha_2 = \beta_2 \text{かつ} \alpha_3 = \beta_3 \text{かつ} \cdots \alpha_n \geq \beta_n \end{cases}$$

ざっくり言うと

$x_1, x_2, \ldots$ の順に数が多い方が強い

先頭項 LT

定義 (先頭項 LT)

$>$ を単項式順序とする
f を多項式とする
f の項の中で，$>$ で比べて最も大きい項を先頭項と呼び $\mathrm{LT}(f)$ で表す

例 (先頭項 LT)

$>$ を辞書式順序とする
$f = 3x^2y + xy + 2y^2 + 1$ とすると，
$\mathrm{LT}(f) = 3x^2y$
$g = xy - 2xy^2 + x$ とすると，$g = -2xy^2 + xy + x$ なので，
$\mathrm{LT}(g) = -2xy^2$

イデアル

定義

$f_1, \ldots, f_s \in K[x_1, \ldots, x_n]$ とする

$$\langle f_1, \ldots, f_s \rangle := \{\Sigma_{i=1}^{s} h_i f_i \ | h_i \in K[x_1, \ldots, x_n]\}$$

を $f_1, \ldots, f_s$ から生成されるイデアルと呼ぶ
また，$\{f_1, \ldots, f_s\}$ を基底と呼ぶ

定義

単項式順序 $>$ を 1 つ決める
I をイデアル $\langle f_1, \ldots, f_s \rangle$ とする

$$\langle \mathrm{LT}(I) \rangle := \langle \mathrm{LT}(f) \ | f \in I \rangle$$

を I の先頭項から生成されるイデアルと呼ぶ

注意

$I = \langle f_1, \ldots, f_s \rangle$ とした時，一般に

$$\langle LT(I) \rangle \neq \langle LT(f_1), \ldots, LT(f_s) \rangle$$

例

$>$ を辞書式順序とする
$f_1 = x + y, f_2 = x - y$ とし，$I = \langle f_1, f_2 \rangle$ とすると，

$$\langle LT(f_1), LT(f_2) \rangle = \langle x, x \rangle = \langle x \rangle$$

しかし，$I = \langle x + y, x - y \rangle = \langle x, y \rangle$ なので，

$$\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(f) \mid f \in \langle x, y \rangle \rangle = \langle x, y \rangle$$

よって，

$$\langle \mathrm{LT}(I) \rangle \neq \langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s) \rangle$$

実は

$$\langle LT(I)\rangle = \langle LT(f_1), \ldots, LT(f_s)\rangle$$

の等号が成立するとき，I の基底 $\{f_1, \ldots, f_s\}$ はグレブナー基底

定義 (グレブナー基底)

多項式環 $K[x_1, \ldots, x_n]$ のイデアル I に対して，有限集合 $G \subset I$ の先頭項から生成されるイデアルが，I の先頭項から生成されるイデアルに一致しているとき，G を I のグレブナー基底と呼ぶ．すなわち，

$$G \subset I \text{ がグレブナー基底} \underset{def}{\Leftrightarrow} \langle \mathrm{LT}(I)\rangle = \langle \mathrm{LT}(G)\rangle.$$

例

$I = \langle x+y, x-y\rangle = \langle x, y\rangle$ とすると，
$\{x, y\}$ は I のグレブナー基底だが，
$\{x+y, x-y\}$ は I のグレブナー基底ではない

グレブナー基底の存在性

定理

任意のイデアルと単項式順序に対し，グレブナー基底は存在する

証明.

LT(f) は単項式なので，$\langle \mathrm{LT}(I) \rangle$ は単項式から生成される
よって，ディクソンの補題より，$\langle \mathrm{LT}(I) \rangle$ に基底 $\mathrm{LT}(G)$ が取れる
この G はグレブナー基底の条件を満たすので，OK □

事実 (ディクソンの補題)

単項式から生成されるイデアルは有限生成

グレブナー基底の計算アルゴリズム

定理 (ブッフベルガー)

グレブナー基底は有限回操作で計算可能である

証明 (概略).

$I = \langle f_1, \ldots, f_s \rangle$ の基底 $\{f_1, \ldots, f_s\}$ に I の他の多項式を足していく
例えば，f_i と f_j の先頭項同士が打ち消しあってできる多項式
$S(f_i, f_j)$ を考えれば，これは新しい先頭項を持つ可能性がある
$(f_1 = x + y, f_2 = x - y$ なら，$S(f_1, f_2) = (x + y) - (x - y) = 2y)$
これをすべてのペア f_i, f_j に対して行い，どんどん足していけば，
ディクソンの補題から，単項式イデアルは有限生成なので，いつかは新しい先頭項が作れなくなる
そのとき，それはグレブナー基底になっている □

- グレブナー基底の概略
- グレブナー基底の応用

消去理論

定理 (消去定理)

$I \subset K[x_1, \ldots, x_n]$ をイデアル，$>$ を $x_1 > \cdots > x_n$ なる辞書式順序，G を I のグレブナー基底とする．このとき，任意の $0 \leq j \leq n-1$ に対して，

$$G \cap K[x_{j+1}, \ldots, x_n]$$

は $I \cap K[x_{j+1}, \ldots, x_n]$ のグレブナー基底

証明.

$\langle LT(G \cap K[x_{j+1}, \ldots, x_n]) \rangle \subset \langle LT(I \cap K[x, y, z]) \rangle$ は明らかなので，逆の包含を示す．$LT(f) \in LT(I \cap K[x_{j+1}, \ldots, x_n])$ に対して，G は I のグレブナー基底より $LT(f)$ を割り切る
$LT(g) \in K[x_{j+1}, \ldots, x_n]$，$g \in G$ が存在．ここで，$>$ は辞書式順序なので，$g \in K[x_{j+1}, \ldots, x_n]$ である．よって，
$LT(f) \in \langle LT(G \cap K[x_{j+1}, \ldots, x_n]) \rangle$ が言えた． □

消去理論

例

$I = \langle x^2 - 2, y^2 - 3, z - x - y \rangle \subset \mathbb{Q}[x_1, \ldots, x_n]$ の辞書式順序でのグレブナー基底をコンピュータで計算すると
$G = \{2x - z^3 + 9z, 2y + z^3 - 11z, z^4 - 10z^2 + 1\}$
つまり，$\langle LT(I) \rangle = \langle LT(G) \rangle = \langle x, y, z^4 \rangle$
こ z こで，

$$G \cap \mathbb{Q}[x, y, z] = \{2x - z^3 + 9z, 2y + z^3 - 11z, z^4 - 10z^2 + 1\}$$
$$G \cap \mathbb{Q}[y, z] = \{2y + z^3 - 11z, z^4 - 10z^2 + 1\}$$
$$G \cap \mathbb{Q}[z] = \{z^4 - 10z^2 + 1\}$$

であり，消去定理から，

$$I \cap \mathbb{Q}[z] = \langle z^4 - 10z^2 + 1 \rangle$$

が分かる

実は

消去理論使えば，連立方程式が解ける

証明.

$$\begin{cases} f_1 = 0 \\ \vdots \\ f_s = 0 \end{cases}$$

を連立方程式とする．このとき，$I = \langle f_1, \ldots, f_s \rangle$ のグレブナー基底を $G = \{g_1, \ldots, g_r\}$ とすると，$I = \langle G \rangle$ であるので，

$$\begin{cases} g_1 = 0 \\ \vdots \\ g_r = 0 \end{cases}$$

は上の連立方程式と同じ解を持つ．後は消去理論から OK $\square$

連立方程式と消去理論

例

$$\begin{cases} x+y-3=0 \\ x-y-1=0 \end{cases}$$

$I=\{x+y-3, x-y-1\}$ のグレブナー基底は $G=\{x-2, y-1\}$
よって，

$$\begin{cases} x-2=0 \\ y-1=0 \end{cases}$$

となって，$x=2, y=1$ で解けた

連立方程式と消去理論

例

$$\begin{cases} x^2+y^2-5=0 \\ xy+y^2-6=0 \end{cases}$$

$I=\{x^2+y^2-5, xy+y^2-6\}$ のグレブナー基底は
$G=\{6x+2y^3-11y, 2y^4-17y^2+36\}$ よって，

$$\begin{cases} 6x+2y^3-11y=0 \\ 2y^4-17y^2+36=0 \end{cases}$$

となって，$2y^4-17y^2+36=(y+2)(y-2)(y+\frac{3}{\sqrt{2}})(y-\frac{3}{\sqrt{2}})=0$
から $y=\pm 2, \pm\frac{3}{\sqrt{2}}$ を第一式に代入して解けば，

$$(x,y)=(1,2),(-1,-2),(\frac{1}{\sqrt{2}},\frac{3}{\sqrt{2}}),(-\frac{1}{\sqrt{2}},-\frac{3}{\sqrt{2}})$$

計算の仕方

例

WolframAlpha(https://www.wolframalpha.com/) で

$$\text{GroebnerBasis}[\{\text{ 多項式 }\},\{\text{ 変数 }\}]$$

を入力．例えば，

$$\mathit{GroebnerBasis}[\{x^2+y^2-5, x*y+y^2-6\},\{x,y\}]$$

と入力すれば

$$\{2y^4-17y^2+36, 6x+2y^3-11y\}$$

と出てくる
皆さんも，実際に好きな連立方程式を解いてみるぶなっ！！

不動点

命題

$\phi : K^n \to K^n$ を多項式写像とする．つまり，ある多項式 $f_1, \ldots, f_n \in K[x_1, \ldots, x_n]$ があって，

$$\phi(a_1, \ldots, a_n) = (f_1(a_1, \ldots, a_n), \ldots, f_n(a_1, \ldots, a_n))$$

と書ける．このとき，ϕ の不動点，つまり，$\phi(a) = a$ なる点は，連立方程式

$$\begin{cases} f_1(x_1, \ldots, x_n) = x_1 \\ \vdots \\ f_n(x_1, \ldots, x_n) = x_n \end{cases}$$

で求まる．つまり，イデアル $J = \langle f_1 - x_1, \ldots, f_n - x_n \rangle \subset K[x_1, \ldots, x_n]$ のグレブナー基底を計算すれば良い．

不動点

命題

多項式写像を $\phi : \mathbb{R}^2 \to \mathbb{R}^2$

$$\phi(x, y) = (x^2 - y, y^2 - x)$$

とする．この ϕ の不動点は，

$$J = \langle x^2 - y - x, y^2 - x - y \rangle \subset K[x, y]$$

のグレブナー基底を計算すれば，

$$GroebnerBasis[\{x^2 - y - x, -x + y^2 - y\}, \{x, y\}]$$

$$\{y^4 - 2y^3, x - y^2 + y\}$$

よって，不動点は

$$(0, 0), (2, 2)$$

イデアルの共通部分

命題

イデアル $I, J \subset K[x_1, \ldots, x_n]$ に対し，新しい変数 t を用いて，

$$H = I \cdot t + J \cdot (1 - t) \subset K[t, x_1, \ldots, x_n]$$

とすると，

$$I \cap J = H \cap K[x_1, \ldots, x_n]$$

が成り立つ．つまり，イデアルの共通部分はグレブナー基底で計算できる．

証明.

$f \in I \cap J \subset K[x_1, \ldots, x_n]$ に対し，$f = f \cdot t + f \cdot (1 - t) \in H$ なので，$f \in H \cap K[x_1, \ldots, x_n]$．よって，$I \cap J = H \subset K[x_1, \ldots, x_n]$．逆に，$f \in H \cap K[x_1, \ldots, x_n]$ なら，$f = a \cdot t + b \cdot (1 - t)(a \in I, b \in J)$ であるが，f は t に無関係なので，t に 0 や 1 を代入しても f は変わらず，$f = a = b \in I \cap J$ が言える． □

イデアルの共通部分

例

$I = \langle x + y, y^2 - 1 \rangle, J = \langle x - 1 \rangle \subset \mathbb{Q}[x, y]$ のとき，見た目では $I \cap J$ は分からないが，$H = I \cdot t + J \cdot (1 - t)$ から t を消去すれば，つまり，

$$GroebnerBasis[\{t * (x + y), t * (y^2 - 1), (1 - t) * (x - 1)\}, \{t, x, y\}]$$

を計算すれば，

$$\{xy - x - y + 1, x^2 - 1, ty + t + x - 1, tx - t - x + 1\}$$

が出てきて，このうち，t が関係ない部分は，

$$\{xy - x - y + 1, x^2 - 1\}$$

よって，

$$\langle x + y, y^2 - 1 \rangle \cap \langle x - 1 \rangle = \langle (x - 1)(y - 1), x^2 - 1 \rangle$$

最大公約元 gcd

命題

$f, g \in K[x_1, \ldots, x_n]$ と $I = \langle f \rangle$, $J = \langle g \rangle$ に対して，

$$I \cap J = \langle \frac{fg}{gcd(f, g)} \rangle$$

が成り立つ.

証明.

$\frac{fg}{gcd(f,g)} = lcm(f, g)$ であり，$lcm(f, g)$ は f, g で割れる最小の多項式なので，等号は明らか. □

最大公約元 gcd

例

$I = \langle (x+y)(x-y) \rangle, J = \langle (x+y)^2 \rangle \subset \mathbb{Q}[x,y]$ のとき，見た目では $I \cap J$ を計算すると，

$$GroebnerBasis[\{t*(x+y), t*(y^2-1), (1-t)*(x-1)\}, \{t,x,y\}]$$

を計算すれば，

$$\{x^3+x^2y-xy^2-y^3, 2txy+2ty^2-x^2-2xy-y^2, tx^2-ty^2\}$$

が出てきて，よって，

$$lcm((x+y)(x-y)), (x+y)^2) = x^3+x^2y-xy^2-y^3$$

で，

$$gcd((x+y)(x-y), (x+y)^2) = x+y$$

が計算できた

陰関数表示

定理

K^n の曲線 C がパラメータ $t_1, \ldots, t_s$ でパラメータ付けられているとする．つまり，ある多項式 $g_1, \ldots, g_n \subset K[t_1, \ldots, t_s]$ が存在して，曲線の座標 $(x_1, \ldots, x_n)$ は

$$x_1 = g_1(t_1, \ldots, t_s)$$
$$\vdots$$
$$x_n = g_n(t_1, \ldots, t_s)$$

と書ける．このとき，
$I = \langle x_1 - g_1(t_1, \ldots, t_s), \ldots, x_n - g_n(t_1, \ldots, t_s) \rangle$ とすれば，

$$J = I \cap K[x_1, \ldots, x_n]$$

は，C の陰関数表示，つまり，$V(J)$ は C を含む最小の代数多様体．ただし，K は無限体とする．

陰関数表示

例

$\mathbb{R}^2$ の曲線 C が

$$x = t$$
$$y = t^2$$

でパラメータ表示されているとすると，$I = \langle x - t, y - t^2 \rangle$ のグレブナー基底は，

$$\{x^2 - y, t - x\}$$

よって，

$$J = I \cap \mathbb{R}[x, y] = \langle x^2 - y \rangle$$

であり，C の陰関数表示は，

$$y = x^2$$

陰関数表示

例

$\mathbb{R}^2$ の曲線 C が

$$x = \frac{1-t^2}{1+t^2}$$
$$y = \frac{2t}{1+t^2}$$

でパラメータ表示されているとすると，
$I = \langle (1+t^2)x - (1-t^2), (1+t^2)y - 2t \rangle$ のグレブナー基底は，

$$\{x^2 + y^2 - 1, ty + x - 1, tx + t - y\}$$

よって，

$$J = I \cap \mathbb{R}[x, y] = \langle x^2 + y^2 - 1 \rangle$$

であり，C の陰関数表示は，

$$x^2 + y^2 = 1$$

ヒルベルト多項式

命題

$I \subset K[x_1, \ldots, x_n]$ イデアル.
$K[x_1, \ldots, x_n]_{\leq s} := \{f | tdeg(f) \leq s\}$, $I_{\leq s} := I \cap K[x_1, \ldots, x_n]_{\leq s}$
ヒルベルト多項式 $HP_I^a(s) := dim_K(K[x_1, \ldots, x_n]_{\leq s}/(I_{\leq s})$
（ただし，s は十分大きい）
このとき，

$$HP_I^a(s) = HP_{\langle LT(I)\rangle}^a(s)$$

が成り立つ. つまり，I のグレブナー基底 G に対し，

$$HP_I^a(s) = HP_{\langle LT(G)\rangle}^a(s)$$

ただし，単項式順序は，次数付とする. （射影空間のヒルベルト多項式の場合，単項式順序はなんでも良い）

ヒルベルト多項式

例

$I = \langle x^2 - y, x^3 - z \rangle \subset \mathbb{R}[x, y, z]$
I の次数付辞書式順序でのグレブナー基底は,

$$GroebnerBasis[\{x^2 - y, x^3 - z\}, \{x, y, z\}, MonomialOrder -> DegreeReverseLexicographic]$$

と入力すると,

$$\{y^2 - xz, xy - z, x^2 - y\}$$

と出るので,

$$LT(G) = \{x^2, xy, y^2\}$$

でヒルベルト多項式 $HP^a_{\langle LT(G) \rangle}(s) = 3s + 1$ から,

$$HP^a_I(s) = HP^a_{\langle LT(G) \rangle}(s) = 3s + 1$$

よって, $dim(V(I)) = deg(HP^a_{I(V)}) = 1.$

ヒルベルトの零点定理

定理

$I \subset \mathbb{C}[x_1, \ldots, x_n] = \mathbb{C}[X]$:イデアルに対し,
$V(I) := \{a \in \mathbb{C} | f(a) = 0, \forall f \in I\}$,
$I(V) := \{f \in \mathbb{C}[X] | f(a) = 0, \forall a \in V\}$
$\sqrt{I} = \{g \in \mathbb{C}[X] | g^n \in I, \exists n \in \mathbb{N}\}$ とすると,

$$I(V) = \sqrt{I}$$

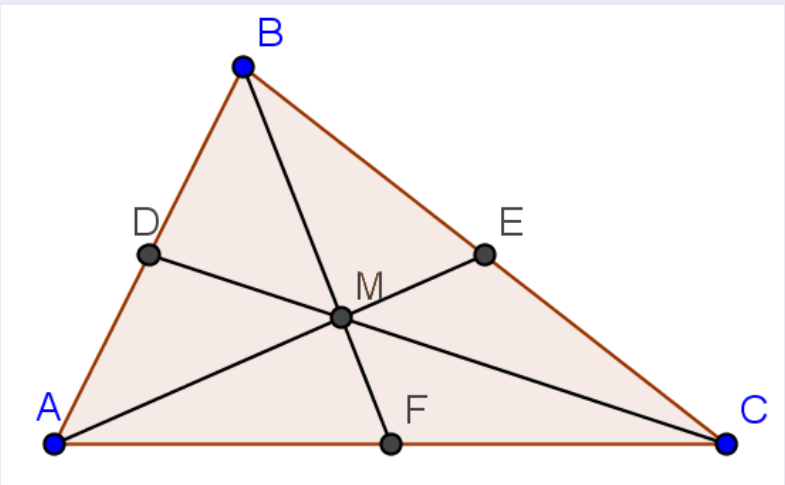
が成り立つ. さらに,

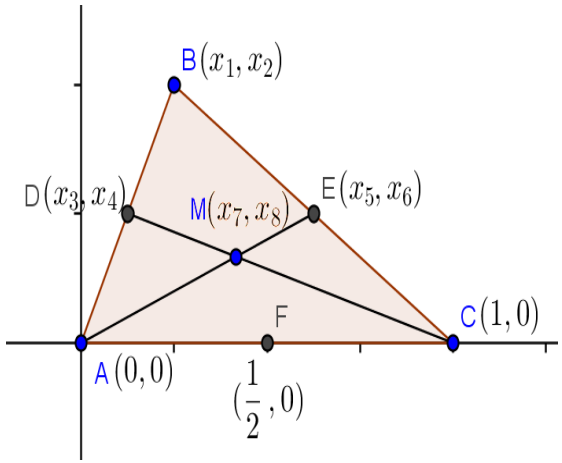
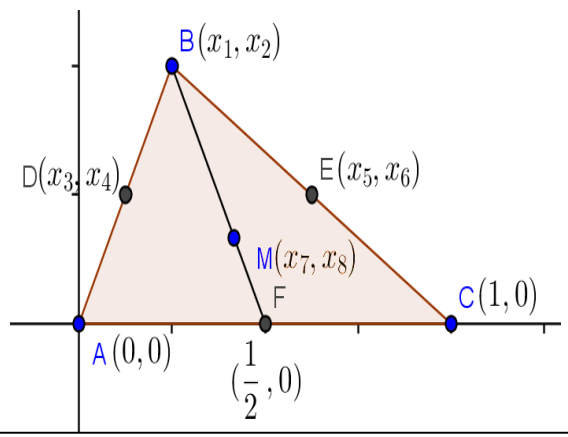
$$\begin{aligned} f \in \sqrt{I} &\iff 1 \in (I + (1 - tf)) \\ &\iff (I + (1 - tf)) \text{ のグレブナー基底は } \{1\} \end{aligned}$$

ヒルベルトの零点定理

定理 (三角形の重心定理)

三角形の各辺の中点と，向かい合う頂点を結んだ直線は，一点で交わる．つまり，重心は存在する．



状態	幾何の世界	多項式の世界
仮定		$\begin{cases} f_1 = a \cdot x_2 - 1 = 0 & (x_2 \neq 0) \\ f_2 = x_1 - 2x_3 = 0 & (\text{中点 D}) \\ f_3 = x_2 - 2x_4 = 0 & (\text{中点 D}) \\ f_4 = (1 + x_1) - 2x_5 = 0 & (\text{中点 E}) \\ f_5 = x_2 - 2x_6 = 0 & (\text{中点 E}) \\ f_6 = x_5 x_8 - x_6 x_7 = 0 & (\text{線分 AME}) \\ f_7 = (x_3 - 1)x_8 - x_4(x_7 - 1) = 0 & (\text{線分 DMC}) \end{cases}$
結論		$g = (2x_1 - 1)x_8 - x_2(2x_7 - 1) = 0 \quad (\text{線分 BMF})$

証明.

三角形の重心定理

$$\iff (f_1 = \cdots f_7 = 0 \Longrightarrow g = 0)$$
$$\iff g \in \sqrt{\langle f_1, \cdots, f_7 \rangle}$$
$$\iff (\langle f_1, \cdots, f_7 \rangle + (1 - tg)) \text{ のグレブナー基底は } \{1\}$$

がヒルベルトの零点定理から成り立つので,

$$\langle a \cdot x_2 - 1, x_1 - 2x_3x_2 - 2x_4, (1 + x_1) - 2x_5, x_2 - 2x_6, x_5x_8 - x_6x_7,$$
$$(x_3 - 1)x_8 - x_4(x_7 - 1), 1 - t((2x_1 - 1)x_8 - x_2(2x_7 - 1))\rangle$$

のグレブナー基底を計算すればいい. 実際, 計算すると, $\{1\}$ なので, $\mathbb{C}^2$ において, 三角形の重心定理が成り立つ. よって, $\mathbb{R}^2$ においても三角形の重心定理は成り立つ. □

ちなみに

この方法では、$\mathbb{C}$ 上の幾何の定理しか完全に証明できない。しかし、$\mathbb{R}$ 上でも解けるアルゴリズムが存在する。それは、

定理 (タルスキー)

実閉体（実数体）上のすべての一階述語論理式は，限量記号（$\forall, \exists$）のない等価な論理式に変形できる（これを *QE*（限量記号消去）するという）．しかも、これはアルゴリズムが存在して計算できる.

というもので，つまり，実数体でも幾何の問題は証明できるということ．現在では，そのアルゴリズムは実装，実用化されていて，国立情報学研究所の「ロボットは東大に入れるか。」プロジェクトでは，大学の入試問題を解くのに応用されている．ちなみに，*CGS-QE* という包括的グレブナー基底系という，グレブナー基底を利用したものもある.

まとめ

- 単項式順序は割り算ができるための順序
- 割り算ができると，グレブナー基底が求められる
- グレブナー基底はイデアルの本質的な情報を持つ基底
- グレブナー基底で連立方程式が解ける
- グレブナー基底で，可換環論や代数幾何の種々の演算ができる
- 他にも，統計や D 加群などに応用される

計算機代数

ちなみに

グレブナー基底を研究する分野には計算機代数がある.
計算機代数とは，*Computer Algebra* の訳語で，グレブナー基底の生みの親であるブッフベルガーさんがその名を付けたと言われる.
計算機代数では，グレブナー基底の計算量やアルゴリズムの改良など，実用的にコンピュータで計算できるかどうかも重視される.
従来の数値計算との違いは，正確に代数的な演算をコンピュータで計算することで，数学的構造を明らかにする点である.
例えば，因数分解のアルゴリズムにおいて，方程式の近似的な根ではなく，数学的に正確な根が計算機代数では求められる.
すなわち，コンピュータ上での数学の実現を目指す分野であり，数学とコンピュータの融合分野といえる.

グレブナー基底とは
イデアルの DNA

by グレブナー基底大好き bot

参考文献

- D. Cox, J. Little, and D. O'Shea, *IDEALS, VARIETIES, AND ALGORITHMS*. Undergraduate Texts in Mathematics. Springer Science+Business Media, New York, third edition, 2006. An Introduction to Computational Algebraic Geometry and Commutative Algebra.
- D. コックス, J. リトル, D. オシー, 『グレブナ基底と代数多様体入門（上・下)』（落合啓之ほか訳）, 丸善出版, 2000 年
- JST CREST 日比チーム編, 『グレブナー道場』, 共立出版, 2012 年
- 丸山正樹, 『グレブナー基底とその応用』, 共立出版, 2006 年
- 大阿久俊則, 『D 加群と計算数学』, 朝倉書店, 2002 年
- 野呂正行, 『計算機代数入門』, 2005 年, http://www.math.kobe-u.ac.jp/Asir/ca.pdf


Thomas Becker, Volker Weispfenning, *Gröbner Bases*, Graduate Texts in Mathematics. Springer-Verlag, New York, 1993. A Computational Approach to Commutative Algebra.


穴井宏和, 横山和弘, 『QE の計算アルゴリズムとその応用』, 東京大学出版会, 2011 年


ぶなぶなくん，『５分で分かるグレブナー基底』，Amazon，Kindle，2015 年


ぶなぶなくん，『グレブナー基底と初等幾何の定理の自動証明』，Amazon，Kindle，2016 年


『グレブナー基底大好き bot さん の togetter まとめ』 http://togetter.com/id/groebner_basis


グレブナー基底大好き bot，『最近、妹がグレブナー基底に興味を持ち始めたのだが。』，カクヨム，https://kakuyomu.jp/works/1177354054880542193