グレブナー基底入門：計算編
ーグレブナー基底の計算方法とその応用ー

神戸祐太（株式会社すうがくぶんか）

2021/12/26

目次

計算編：目次

自己紹介

グレブナー基底とは

まずは計算してみよう

三彩色問題に応用してみよう

整数計画法への応用

自己紹介

名前、所属、学位

- 名前：神戸祐太（かんべ　ゆうた）
- 所属：株式会社すうがくぶんか, 立教大学
- 学位：博士（学術）　（埼玉大学, 論文博士, 数学専攻）

研究テーマ：**グレブナー基底**とモジュライ空間, 耐量子計算暗号（超特異楕円曲線暗号）

最近の活動

- すうがくぶんか（統計・機械学習・数学・プログラミング）
- 耐量子計算暗号研究（Sage による実装・実験など）

グレブナー基底とは

グレブナー基底とは

$$\begin{cases} f_1 = z^5 + yz^4 - z^3 + y^2 + 2z^2 - x - 6z + 4 & = 0, \\ f_2 = y^2 + z^5 - z^3 & = 0, \\ f_3 = -2yz^4 - z^2 + 2x + 3z - 2 & = 0. \end{cases} \tag{1}$$

$\Downarrow$ $\langle f_1, f_2, f_3 \rangle$ のグレブナー基底を求めて，
= 0 の方程式を立てる

$$\begin{cases} g_1 = z^2 - 3z + 2 & = 0 \ (\Rightarrow z = 1, 2), \\ g_2 = y^2 + 24z - 24 & = 0, \\ g_3 = x + y(-15z + 14) & = 0. \end{cases} \tag{2}$$

実は...<u>(1) の解 $\Leftrightarrow$ (2) の解！</u>

$(x, y, z) = (0, 0, 1), (16\sqrt{-24}, \sqrt{-24}, 2), (-16\sqrt{-24}, -\sqrt{-24}, 2)$

グレブナー基底とは

$$\begin{cases} f_1 = z^5 + yz^4 - z^3 + y^2 + 2z^2 - x - 6z + 4 & = 0, \\ f_2 = y^2 + z^5 - z^3 & = 0, \\ f_3 = -2yz^4 - z^2 + 2x + 3z - 2 & = 0. \end{cases} \tag{1}$$

$\Downarrow$ $\langle f_1, f_2, f_3 \rangle$ のグレブナー基底を求めて,
= 0 の方程式を立てる

$$\begin{cases} g_1 = z^2 - 3z + 2 & = 0 \ (\Rightarrow z = 1, 2), \\ g_2 = y^2 + 24z - 24 & = 0, \\ g_3 = x + y(-15z + 14) & = 0. \end{cases} \tag{2}$$

実は...(1) の解 $\Leftrightarrow$ (2) の解!

$(x, y, z) = (0, 0, 1), (16\sqrt{-24}, \sqrt{-24}, 2), (-16\sqrt{-24}, -\sqrt{-24}, 2)$

グレブナー基底とは

$$\begin{cases} f_1 = z^5 + yz^4 - z^3 + y^2 + 2z^2 - x - 6z + 4 & = 0, \\ f_2 = y^2 + z^5 - z^3 & = 0, \\ f_3 = -2yz^4 - z^2 + 2x + 3z - 2 & = 0. \end{cases} \tag{1}$$

$\Downarrow$ $\langle f_1, f_2, f_3 \rangle$ のグレブナー基底を求めて，
= 0 の方程式を立てる

$$\begin{cases} g_1 = z^2 - 3z + 2 & = 0 \ (\Rightarrow z = 1, 2), \\ g_2 = y^2 + 24z - 24 & = 0, \\ g_3 = x + y(-15z + 14) & = 0. \end{cases} \tag{2}$$

実は...<u>(1) の解 $\Leftrightarrow$ (2) の解！</u>

$(x, y, z) = (0, 0, 1), (16\sqrt{-24}, \sqrt{-24}, 2), (-16\sqrt{-24}, -\sqrt{-24}, 2)$