対称群の作用をもつ連立方程式に関する一考察

A note on a system of polynomial equations with the action of the symmetric group

瀬賀 達也・張間忠人

Sega Tatsuya，Harima Tadahito

1 はじめに

自然数 k に対して，

$$p_k := p_k(x_1, x_2, \ldots, x_n) = x_1^k + x_2^k + \cdots + x_n^k$$
$$h_k := h_k(x_1, x_2, \ldots, x_n) = \sum_{a_1+a_2+\cdots+a_n=k} x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$$

とおく．p_k を n 変数 $x_1, x_2, \ldots, x_n$ に関する k 次のベキ乗和対称式，h_k を $x_1, x_2, \ldots, x_n$ に関する k 次の完全対称式という．どちらも代表的な対称式である．次の連立方程式を考える．

$$(*1)\ \begin{cases} p_{k_1}(x_1, x_2, \ldots, x_n) &= 0 \\ p_{k_2}(x_1, x_2, \ldots, x_n) &= 0 \\ & \vdots \\ p_{k_n}(x_1, x_2, \ldots, x_n) &= 0 \end{cases} \qquad (*2)\ \begin{cases} h_{k_1}(x_1, x_2, \ldots, x_n) &= 0 \\ h_{k_2}(x_1, x_2, \ldots, x_n) &= 0 \\ & \vdots \\ h_{k_n}(x_1, x_2, \ldots, x_n) &= 0 \end{cases}$$

どちらの方程式も自明解，すなわち $x_1 = x_2 = \cdots = x_n = 0$ を解に持つことは明らかである．

問 1.1 n 個の n 変数ベキ乗和対称式からなる連立方程式 $(*1)$ は，いつ，自明解しか持たないか？ そのときの $k_1, k_2, \ldots, k_n$ の値の組をすべて求めよ．

問 1.2 n 個の n 変数完全対称式からなる連立方程式 $(*2)$ は，いつ，自明解しか持たないか？ そのときの $k_1, k_2, \ldots, k_n$ の値の組をすべて求めよ．

どちらの問題も 3 変数以上の場合で未解決である．3 変数の場合ですら完全に解けていないようである．この問題は，たとえば，論文 [1], [6] において扱われている．その中から 2 変数と 3 変数の場合の結果をいくつか紹介する．

(1) a と b を自然数 $(a < b)$，d を a と b の最大公約数とする．このとき，連立方程式

$$\begin{cases} p_a(x_1, x_2) &= 0 \\ p_b(x_1, x_2) &= 0 \end{cases}$$

が自明解しか持たないための必要十分条件は，$\frac{a}{d}$ または $\frac{b}{d}$ が偶数であることである．

(2) a と b を自然数 $(a < b)$ とする．このとき，連立方程式

$$\begin{cases} h_a(x_1, x_2) &= 0 \\ h_b(x_1, x_2) &= 0 \end{cases}$$

が自明解しか持たないための必要十分条件は，$a+1$ と $b+1$ が互いに素であることである．

(3) $a < b < c$ とする．「$a = 1,\ 2 \le b \le 7$ で，bc は 6 で割り切れる」または「$a = 2$ かつ $b = 3$」であれば，連立方程式

$$(*3)\ \begin{cases} p_a(x_1, x_2, x_3) &= 0 \\ p_b(x_1, x_2, x_3) &= 0 \\ p_c(x_1, x_2, x_3) &= 0 \end{cases}$$

は自明解のみを持つ.

(4) $a=1,\ b=2$ のとき, $(*3)$ が自明解のみ持つための必要十分条件は, c は 3 の倍数であることである. また, $a=1,\ b=3$ のとき, $(*3)$ が自明解のみ持つための必要十分条件は, c は偶数であることである.

(5) 連立方程式

$$(*4)\quad \begin{cases} h_a(x_1,x_2,x_3) &= 0 \\ h_b(x_1,x_2,x_3) &= 0 \\ h_c(x_1,x_2,x_3) &= 0 \end{cases}$$

について次が成り立つ.

(i) $a=1,\ b=2$ のとき, $(*4)$ が自明解のみ持つための必要十分条件は, c は 3 の倍数であることである.

(ii) $a=1,\ b=3$ のとき, $(*4)$ が自明解のみ持つための必要十分条件は, c は 2 の倍数であることである.

(iii) $a=1,\ b=4$ のとき, $(*4)$ が自明解のみ持つための必要十分条件は, c は 3 の倍数であることである.

(iv) $a=2,\ b=3$ のとき, $(*4)$ が自明解のみ持つための必要十分条件は, c は 4 の倍数である, または c は 4 で割ると 1 余ることである.

また, n 変数の場合の代表的な結果として, 次が知られている.

(6) $k_1,k_2,\ldots,k_m$ が連続する自然数のとき, 連立方程式 $(*1)$ と $(*2)$ は自明解しか持たない.

(7) 連立方程式 $(*1)$ が自明解しか持たないとき, $n!$ は $k_1\times k_2\times\cdots\times k_n$ を割る. $(*2)$ についても同様である.

(7) は自明解を持つための必要条件を与えているが, その逆は成り立たないことが知られている. たとえば $k_1=1,\ k_2=3,\ k_3=5,\ k_4=8$ はその反例になっている ([1], Remark 2.16). しかし, 3 変数のときは反例があるかどうか知られていないようだ. また, 3 変数と 4 変数について問 1.1 と問 1.2 の部分的な結果は [1], [5], [6] で述べられている.

第 2 節と第 3 節では, 2 つの多項式の終結式（シルベスターの行列式）を利用して, 上の (1) と (2) の別証明を与える. また, グレブナー基底を計算するブッフベルガーのアルゴリズムを用いて, (1) と (2) の別証明を与えることもできる. 2 変数の場合の別証明を考えようと思った動機は, 未解決である 3 変数の場合にも適用する手法を探るためである. その結果, グレブナー基底を用いた手法は 3 変数の場合でも有効であることが分かってきたが, (1) と (2) の別証明とその有効性に関する説明は, 次の機会とする.

第 4 節では, 3 変数連立 2 次方程式の教材開発に向けた基礎研究として, 置換で移り合う方程式系に注目し, 解きやすい方程式を見つけることを目標とするオリジナルな問題 (問題 4.1) を設定した. 定理 4.5 と定理 4.9 では, ブッフベルガーのアルゴリズムを用いて, 次の 3 変数連立 2 次方程式

$$\begin{cases} x^2+ayz+b=0 \\ y^2+axz+b=0 \\ z^2+axy+b=0 \end{cases} \qquad \begin{cases} x^2+ay+az+b=0 \\ y^2+ax+az+b=0 \\ z^2+ax+ay+b=0 \end{cases}$$

について, その問に対する 1 つの解を与える.

2　2 変数べき乗和多項式からなる連立方程式

本節では，終結式を利用して, 次の定理の (2) ⇒ (1) の別証明を与える.

定理 2.1　a,b を自然数 $(a<b)$, d を a と b の最大公約数とする. 次は同値である.

(1)　連立方程式

$$(*5)\quad \begin{cases} x^a+y^a &= 0 \\ x^b+y^b &= 0 \end{cases}$$

は自明解しか持たない.

(2) $\frac{a}{d}$ または $\frac{b}{d}$ は偶数である.

まず, 連立方程式 $(*5)$ は自明解しか持たないことと次の連立方程式 $(*6)$ は解をもたないことが同値であることに注意しよう.

$$(*6)\ \begin{cases} x^a+1 &= 0 \\ x^b+1 &= 0 \end{cases}$$

2 つの多項式 x^a+1 と x^b+1 の終結式 $R(a,b)$ は

$$R(a,\ b)=\begin{vmatrix}
1 & 0 & \cdots & 0 & 1 & & & & & & \\
 & 1 & 0 & \cdots & 0 & 1 & & & & & \\
 & & \ddots & & & & \ddots & & & & \\
 & & & 1 & 0 & \cdots & 0 & 1 & & & \\
 & & & & 1 & 0 & \cdots & 0 & 1 & & \\
 & & & & & \ddots & & & & \ddots & \\
 & & & & & & 1 & 0 & \cdots & 0 & 1 \\
1 & 0 & & \cdots & \cdots & & 0 & 1 & & & \\
 & 1 & 0 & & \cdots & \cdots & & 0 & 1 & & \\
 & & \ddots & & & & & & & \ddots & \\
 & & & 1 & 0 & & \cdots & \cdots & & 0 & 1
\end{vmatrix}$$

で与えられる. よく知られた終結式の性質より, 「$R(a,b)\neq 0$ であれば, 方程式 $(*6)$ は解を持たない」ことが分かるので, 以下では, $\frac{a}{d}$ または $\frac{b}{d}$ は偶数であることを仮定して, $R(a,b)\neq 0$ を示そう.

上の終結式の右辺（シルベスターの行列式）の (i,j) 成分を c_{ij} とすれば, 行列式の定義から

$$R(a,b)=\sum_{\sigma\in S_{a+b}} \mathrm{sgn}(\sigma)\ c_{1\sigma(1)}c_{2\sigma(2)}\cdots c_{a+b\sigma(a+b)}$$

である. ここで, $(a+b)$ 次対称群 S_{a+b} の元 τ で, 各 $c_{i\tau(i)}$ が対角成分以外の 1 をとる置換はただ 1 つしかなく, それは,

$$\tau=\begin{pmatrix} 1 & 2 & \cdots & a & \cdots & b & b+1 & \cdots & a+b \\ a+1 & a+2 & \cdots & 2a & \cdots & a+b & 1 & \cdots & a \end{pmatrix}$$

である. この置換 τ の上下の関係は, $k\in\{1,2,\ldots,a+b\}$ に対して

$$\tau(k)\equiv k+a \mod a+b$$

で与えられる. ゆえに, $t\geq 1$ に対して

$$\tau^t(k)\equiv k+ta \mod a+b$$

を得る. よって, $k\equiv k+(\frac{a+b}{d})a \mod a+b$ であることに注意すると, $\tau^{\frac{a+b}{d}}$ は恒等置換であることが分かる. さらに, τ に対して $\tau^t(k)\neq k\ (0<t<\frac{a+b}{d})$, $\tau^i(k)\neq\tau^j(k)\ (0<i<j<\frac{a+b}{d})$ が言えるので, τ は長さ $\frac{a+b}{d}$ である d 個の巡回置換の積に分解する（ここで, 各巡回置換は互いに共通な文字を含まないことに注意しよう）. その巡回置換による分解を

$$\tau=\tau_1\tau_2\cdots\tau_d$$

としよう. ここで, 各 τ_i は長さ $\frac{a+b}{d}$ の巡回置換であり, $\frac{a}{d}$ と $\frac{b}{d}$ はともに偶数であることはないので, しかし, 仮定から $\frac{a}{d}$ と $\frac{b}{d}$ のどちらかは偶数なので, 結局, τ_i は長さが奇数の巡回置換であることが分かる. ゆえに

$$\mathrm{sgn}(\tau_i)=1.$$

従って, S_{a+b} の元 σ のうち, すべての i に対して $c_{i\sigma(i)}=1$ となる置換は, 恒等置換または τ を分解して得られた巡回置換 τ_i のいくつかの積で表される置換であるから,

$$\begin{aligned} R(a,b) &= \textstyle\sum_{\sigma\in S_{a+b}}\mathrm{sgn}(\sigma)\ c_{1\sigma(1)}c_{2\sigma(2)}\cdots c_{a+b\sigma(a+b)} \\ &= {}_dC_0+{}_dC_1+\cdots+{}_dC_{d-1}+{}_dC_d \\ &= (1+1)^d \\ &= 2^d \end{aligned}$$

が分かる. よって, 終結式 $R(a,b)$ の値は 0 でないので, 連立方程式 $(*5)$ は自明解しか持たない.

3　2 変数完全対称式からなる連立方程式

本節では，終結式を利用して, 次の定理の (2) ⇒ (1) の別証明を与える.

定理 3.1　a, b を自然数とする. 次は同値である.

(1)　連立方程式

$$(*7)\ \begin{cases} x^a + x^{a-1}y + \cdots + xy^{a-1} + y^a &= 0 \\ x^b + x^{b-1}y + \cdots + xy^{b-1} + y^b &= 0 \end{cases}$$

は自明解しか持たない.

(2)　$\gcd(a+1, b+1) = 1$. ここで gcd は 2 つの自然数の最大公約数を表す.

まず, 連立方程式 (∗7) は自明解しか持たないことと次の連立方程式 (∗8) は解をもたないことが同値であることに注意しよう.

$$(*8)\ \begin{cases} x^a + x^{a-1} + \cdots + x + 1 &= 0 \\ x^b + x^{b-1} + \cdots + x + 1 &= 0 \end{cases}$$

2 つの多項式 $x^a + x^{a-1} + \cdots + x + 1$ と $x^b + x^{b-1} + \cdots + x + 1$ の終結式 $R'(a, b)$ は

$$R'(a,\ b) = \begin{vmatrix} 1 & 1 & \cdots & 1 & 1 & & & & & & \\ & 1 & 1 & \cdots & 1 & 1 & & & & & \\ & & \ddots & & & & \ddots & & & & \\ & & & 1 & 1 & \cdots & 1 & 1 & & & \\ & & & & 1 & 1 & \cdots & 1 & 1 & & \\ & & & & & & \ddots & & & \ddots & \\ & & & & & & & 1 & 1 & \cdots & 1 & 1 \\ 1 & 1 & & \cdots & \cdots & & & 1 & 1 & & & \\ & 1 & 1 & & \cdots & \cdots & & & 1 & 1 & & \\ & & \ddots & & & & & & & & \ddots & \\ & & & 1 & 1 & & \cdots & \cdots & & & 1 & 1 \end{vmatrix}$$

で与えられる. よく知られた終結式の性質より, 「$R'(a, b) \neq 0$ であれば, 方程式 (∗8) は解を持たない」ことが分かるので, 以下では, $\gcd(a+1, b+1) = 1$ を仮定して, $R'(a, b) \neq 0$ を示そう. a と b に関する二重帰納法で証明する.

行列式と基本変形に関する性質等を用いると,

(3.1)　$R'(a, b) = \pm R'(b, a)$

(3.2)　$R'(a, a+1) = 1$

(3.3)　$b > a+1$ のとき, $R'(a, b) = R'(a, b-a-1)$

が分かる. また, 2 つの自然数 m, n $(m > n)$ について, 次の同値性に注意しておく.

(3.4)　$\gcd(m+1, n+1) = 1 \ \Leftrightarrow\ \gcd(m-n, n+1) = 1$

Step1 : $a = 1$ とする.

(Case 1) $a = 1, b = 1$ のとき, $\gcd(a+1, b+1) = \gcd\,(2, 2) = 2 \neq 1$ であるから問題にしなくてもよい.

$a = 1, b = 2$ のとき, $\gcd(a+1, b+1) = \gcd\,(2, 3) = 1$ であり,

$$R'(a,\ b) = \begin{vmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{vmatrix} = 1.$$

すなわち, 終結式 $R'(a, b)$ の値は 0 でない.

(Case 2) $b \leq k-1$ である全ての自然数 b に対して「$\gcd\,(2, b+1) = 1$ ならば $R'(1, b) \neq 0$」が成り立つと仮定する.

(SubCase 1) $\gcd(2, k+1) \neq 1$ のときは問題にしなくてよい.

(SubCase 2) $\gcd(2, k+1) = 1$ とする. $k > 2$ であるから (3.3) より, $R'(1,k) = R'(1,k-2)$. また, (3.4) より, $\gcd(2, k-1) = 1$ である. ゆえに, 帰納法の仮定より

$$R'(1,k) = R'(1,k-2) \neq 0.$$

よって, $\gcd(2, b+1) = 1$ であるような b について $R'(1,b) \neq 0$ が成り立つ.

Step2 : $1 \leq a \leq n-1$ とする.

(†1) $\gcd(a+1, b+1) = 1$ であるような b について, $R'(a,b) \neq 0$ が成り立つと仮定する.

(†2) さらに, $a = n$, $1 \leq b \leq m-1$ のとき, $\gcd(n+1, b+1) = 1$ であるような b について, $R'(n,b) \neq 0$ が成り立つと仮定する.

この状況の下で $a = n, b = m$ のとき, $\gcd(n+1, m+1) = 1$ であるような n と m について $R'(n,m) \neq 0$ であることを示そう.

(Case 1) $n > m$ とする. (3.1) より $R'(n,m) = \pm R'(m,n)$ である. ゆえに, 帰納法の仮定 (†1) より,

$$R'(m,n) \neq 0, \text{ i.e., } R'(n,m) \neq 0.$$

(Case 2) $m = n+1$ とする. (3.2) より

$$R'(n,m) = R'(n,n+1) = 1 \neq 0.$$

(Case 3) $m > n+1$ とする. (3.3) より $R'(n,m) = R'(n,m-n-1)$ が成り立つ. また, (3.4) から $\gcd(n+1, m-n) = 1$ である. ゆえに, 帰納法の仮定 (†2) より

$$R'(n,m) = R'(n,m-n-1) \neq 0.$$

よって, Step1 と Step2 より, $\gcd(a+1, b+1) = 1$ であるような a, b に対して, $R'(a,b) \neq 0$ であることが示された.

4 置換で移り合う 3 変数連立 2 次方程式について

体 K は数体とする. 多項式環 $K[x_1, x_2, \ldots, x_n]$ から有限個の多項式 $f_1, f_2, \ldots, f_l$; $g_1, g_2, \ldots, g_m$ をとり, 2 つの連立方程式

$$\begin{cases} f_1 &= 0 \\ f_2 &= 0 \\ &\vdots \\ f_l &= 0 \end{cases} \qquad \begin{cases} g_1 &= 0 \\ g_2 &= 0 \\ &\vdots \\ g_m &= 0 \end{cases}$$

を考える. これらが同じ解を持つための十分条件として

$$(f_1, f_2, \ldots, f_l) = (g_1, g_2, \ldots, g_m)$$

がある. 同じ解を持つ連立方程式は同値であるという. 連立方程式を解くことは, 同値な連立方程式で, 解きやすいものを見つけることに帰着する. すなわち, 与えられた方程式から定まるイデアル $(f_1, f_2, \ldots, f_l)$ に対して

$$(f_1, f_2, \ldots, f_l) = (g_1, g_2, \ldots, g_m)$$

をみたす解きやすい生成元 $\{g_1, g_2, \ldots, g_m\}$ を見つけることが解法の鍵である. そこで, 次の問題を考えたい.

問 4.1 $f_1, f_2, \ldots, f_l$ を整数係数の多項式とする. このとき, イデアル $(f_1, f_2, \ldots, f_l)$ に属する解きやすい多項式を見つけよ. ここでは, この解きやすい多項式を, 次の条件 (☆) をみたす多項式とした.

(☆) 整数係数の 1 変数多項式で 2 次式以下の整数係数の多項式の積として表される.

上の (☆) のような多項式 $=0$ の方程式は, 高校生であれば因数分解した後, 解くことができるであろう. この節では, 3 変数連立 2 次方程式の教材開発の基礎研究として, 問 4.1 に取り組む. ここでは, 連立方程式のクラスとして, 置換で移り合う方程式系に注目する.

定義 4.2　I を $K[x_1, x_2, \ldots, x_n]$ のイデアル, S_n を n 次対称群とする. いま, S_n は変数 $x_1, x_2, \ldots, x_n$ の置換として作用しているとする. 等式

$$I = \{ {}^{\sigma}f \mid {}^{\forall}f \in I, {}^{\forall}\sigma \in S_n \}$$

が成り立つとき, I は S_n 不変であるという.

補題 4.3　I を $K[X] = K[x_1, x_2, \ldots, x_n]$ のイデアル, $\{f_1, f_2, \ldots, f_l\}$ を I の生成系とする. どの生成元 f_i に対しても, 任意の $\sigma \in S_n$ について

$${}^{\sigma}f_i \in \{f_1, f_2, \ldots, f_l\}$$

であるとする. このとき, I は S_n 不変である.

(証明) イデアル I の任意の元 f は

$$f = g_1 f_1 + g_2 f_2 + \cdots + g_l f_l$$

とかける (ただし, 各 g_k は $K[X]$ の元). この f に S_n の任意の置換 σ を施すと,

$${}^{\sigma}f = {}^{\sigma}g_1^{\sigma} f_1 + {}^{\sigma}g_2^{\sigma} f_2 + \cdots + {}^{\sigma}g_l^{\sigma} f_l$$

となる. 仮定より, 各 ${}^{\sigma}f_i$ は $\{f_1, f_2, \ldots, f_l\}$ に属するから, イデアル I にも属する. もちろん, 各 ${}^{\sigma}g_i$ は $K[X]$ の元であるから, 結局

$${}^{\sigma}f \in I$$

となり, I は S_n 不変であることが分かる.

例 4.4　(1)　第 2 節と第 3 節で扱ったべき乗和多項式と完全対称式からなる連立方程式は S_n 不変である.

(2)　a, b を定数とする. 次の 3 変数連立 2 次方程式

$$(*9)\ \begin{cases} x^2 + ayz + b = 0 \\ y^2 + axz + b = 0 \\ z^2 + axy + b = 0 \end{cases} \qquad (*10)\ \begin{cases} x^2 + ay + az + b = 0 \\ y^2 + ax + az + b = 0 \\ z^2 + ax + ay + b = 0 \end{cases}$$

を考える.

$$\begin{cases} f_1 = x^2 + ayz + b \\ f_2 = y^2 + axz + b \\ f_3 = z^2 + axy + b \end{cases} \qquad \begin{cases} g_1 = x^2 + ay + az + b \\ g_2 = y^2 + ax + az + b \\ g_3 = z^2 + ax + ay + b \end{cases}$$

とおくと, 補題 4.3 より 2 つのイデアル (f_1, f_2, f_3) と (g_1, g_2, g_3) は S_3 不変であることが分かる.

この節の主定理では, Buchberger のアルゴリズムに登場する S 多項式を利用して, 上の連立 2 次方程式に対して, 条件 (☆) を満たす解きやすい多項式を与える. また, その証明では, 解きやすい多項式を導く手順も与えている. S_n 不変なイデアルに関する先行研究としては, [3], [4] などがある.

定理 4.5　例 4.4 で登場した $\{f_1, f_2, f_3\}$ で生成されるイデアルを I とする. このとき, I には z の 6 次式で, 次数 2 の多項式の積に分解される多項式

$$(a+1)\{(a+1)z^2 + b\}\{(a^2 - a + 1)z^2 + b\}\{(a^2 - a + 1)z^2 + (a-1)^2 b\}$$

が含まれる. また, I は S_3 不変なので,

$$(a+1)\{(a+1)x^2 + b\}\{(a^2 - a + 1)x^2 + b\}\{(a^2 - a + 1)x^2 + (a-1)^2 b\},$$
$$(a+1)\{(a+1)y^2 + b\}\{(a^2 - a + 1)y^2 + b\}\{(a^2 - a + 1)y^2 + (a-1)^2 b\}$$

も含まれる.

証明の前に, S 多項式について説明する.

定義 4.6 2 つの単項式 $u = x_1^{a_1}x_2^{a_2}\cdots x_n^{a_n}$, $v = x_1^{b_1}x_2^{b_2}\cdots x_n^{b_n}$ に対して, 単項式 $x_1^{c_1}x_2^{c_2}\cdots x_n^{c_n}$ を u と v の最小公倍単項式とよび, $\mathrm{lcm}\ (u, v)$ とかく. ここで $c_i = \max\{a_i, b_i\}$ である.

定義 4.7 多項式 f における $\mathrm{in}_<(f)$ の係数を c_f, 多項式 g における $\mathrm{in}_<(g)$ の係数を c_g とする. ここで, $\mathrm{in}_<$ は純辞書式順序による先頭項を表す. このとき, 多項式

$$S(f,g) = \frac{\mathrm{lcm}\ (\mathrm{in}_<(f), \mathrm{in}_<(g))}{c_f \cdot \mathrm{in}_<(f)} f - \frac{\mathrm{lcm}\ (\mathrm{in}_<(f), \mathrm{in}_<(g))}{c_g \cdot \mathrm{in}_<(g)} g$$

を f と g の S 多項式という.

例 4.8 $f = x^2 + y + z$, $g = x + y^2 + z$ とする. このとき, $\mathrm{in}_<(f) = x^2$, $\mathrm{in}_<(g) = x$ であるから f と g の S 多項式は

$$\begin{aligned} S(f,g) &= f - xg \\ &= -xy^2 - xz + y + z. \end{aligned}$$

(定理 4.5 の証明) 証明では, グレブナー基底に関する基本事項が必要である. それについては, たとえば, [2] に詳しい説明がある.

考える連立方程式は

$$\begin{cases} f_1 = 0 \\ f_2 = 0 \\ f_3 = 0 \end{cases}$$

である. $\{f_1, f_2, f_3\}$ で生成されるイデアル I について, 純辞書式順序によるグレブナー基底を求める. まず, S 多項式 $S(f_1, f_2)$ を求めると

$$\begin{aligned} S(f_1,f_2) &= az(x^2 + ayz + b) - x(y^2 + axz + b) \\ &= -xy^2 - bx + a^2yz^2 + abz. \end{aligned}$$

$S(f_1, f_2)$ を f_3 で割って

$$\begin{aligned} S(f_1,f_2) &= (-\tfrac{1}{a}y)(z^2 + axy + b) - bx + (a^2 + \tfrac{1}{a})yz^2 + \tfrac{b}{a}y + abz \\ &= 0 \cdot f_1 + 0 \cdot f_2 + (-\tfrac{1}{a}y)f_3 - bx + (a^2 + \tfrac{1}{a})yz^2 + \tfrac{b}{a}y + abz \end{aligned}$$

を得る. 余りをグレブナー基底の候補に加えるわけであるが, 後の計算のために余りに $-a$ をかけた式を

$$f_4 = abx - (a^3 + 1)yz^2 - by - a^2bz$$

とする. ゆえに, $\{f_1, f_2, f_3, f_4\}$ が I のグレブナー基底の候補となる. 次に $S(f_1, f_4)$ を求めると

$$\begin{aligned} S(f_1,f_4) &= ab(x^2 + ayz + b) - x\{abx - (a^3 + 1)yz^2 - by - a^2bz\} \\ &= (a^3 + 1)xyz^2 + bxy + a^2bxz + a^2byz + ab^2. \end{aligned}$$

$S(f_1, f_4)$ を f_3 で割って

$$S(f_1,f_4) = (\frac{a^3+1}{a}z^2 + \frac{b}{a})(z^2 + axy + b) + a^2bxz + a^2byz - \frac{a^3+1}{a}z^4 - \frac{a^3b+2b}{a}z^2 + ab^2 - \frac{b^2}{a}.$$

さらに, 得られた余りを f_2 で割ると

$$\begin{aligned} S(f_1,f_4) &= ab(y^2 + axz + b) + (\tfrac{a^3+1}{a}z^2 + \tfrac{b}{a})(z^2 + axy + b) \\ &\qquad -aby^2 + a^2byz - \tfrac{a^3+1}{a}z^4 - \tfrac{a^3b+2b}{a}z^2 - \tfrac{b^2}{a} \\ &= 0 \cdot f_1 + abf_2 + (\tfrac{a^3+1}{a}z^2 + \tfrac{b}{a})f_3 + 0 \cdot f_4 \\ &\qquad -aby^2 + a^2byz - \tfrac{a^3+1}{a}z^4 - \tfrac{a^3b+2b}{a}z^2 - \tfrac{b^2}{a}. \end{aligned}$$

その余りをグレブナー基底の候補に加えるわけであるが, 後の計算のために余りに $-a$ をかけた式

$$f_5 = a^2by^2 - a^3byz + (a^3 + 1)z^4 + (a^3b + 2b)z^2 + b^2$$

を考える．ゆえに，$\{f_1, f_2, f_3, f_4, f_5\}$ が I のグレブナー基底の候補となる．次に，$S(f_2, f_4)$ を求めると

$$\begin{aligned} S(f_2, f_4) &= b(y^2 + axz + b) - z\{abx - (a^3+1)yz^2 - by - a^2bz\} \\ &= by^2 + (a^3+1)yz^3 + byz + a^2bz^2 + b^2. \end{aligned}$$

$S(f_2, f_4)$ を f_5 で割って

$$\begin{aligned} S(f_2, f_4) &= \tfrac{1}{a^2}\{a^2by^2 - a^3byz + (a^3+1)z^4 + (a^3b+2b)z^2 + b^2\} \\ &\quad +(a^3+1)yz^3 + (b + \tfrac{a^3b}{a^2})yz - \tfrac{a^3+1}{a^2}z^4 + (a^2b - \tfrac{a^3b+2b}{a^2})z^2 + b^2 - \tfrac{b^2}{a^2} \\ &= 0 \cdot f_1 + 0 \cdot f_2 + 0 \cdot f_3 + 0 \cdot f_4 + \tfrac{1}{a^2}f_5 \\ &\quad +(a^3+1)yz^3 + (b + \tfrac{a^3b}{a^2})yz - \tfrac{a^3+1}{a^2}z^4 + (a^2b - \tfrac{a^3b+2b}{a^2})z^2 + b^2 - \tfrac{b^2}{a^2} \end{aligned}$$

を得る．余りをグレブナー基底の候補に加えるわけであるが，後の計算のために余りに a^2 をかけた式を

$$f_6 = (a^5 + a^2)yz^3 + (a^3b + a^2b)yz - (a^3+1)z^4 + (a^4b - a^3b - 2b)z^2 + a^2b^2 - b^2$$

とする．よって，$\{f_1, f_2, f_3, f_4, f_5, f_6\}$ が I のグレブナー基底の候補となる．さらに，$S(f_3, f_4)$ を求めると

$$\begin{aligned} S(f_3, f_4) &= b(z^2 + axy + b) - y\{abx - (a^3+1)yz^2 - by - a^2bz\} \\ &= (a^3+1)y^2z^2 + by^2 + a^2byz + bz^2 + b^2. \end{aligned}$$

$S(f_3, f_4)$ を f_5 で割って

$$\begin{aligned} S(f_3, f_4) &= (\tfrac{a^3+1}{a^2b}z^2 + \tfrac{1}{a^2})\{a^2by^2 - a^3byz + (a^3+1)z^4 + (a^3b+2b)z^2 + b^2\} \\ &\quad +\tfrac{(a^3+1)(a^3b)}{a^2b}yz^3 + (a^2b + \tfrac{a^3b}{a^2})yz - \tfrac{(a^3+1)^2}{a^2b}z^6 \\ &\quad -\{\tfrac{(a^3+1)(a^3b+2b)}{a^2b} + \tfrac{a^3+1}{a^2}\}z^4 + \{b - \tfrac{(a^3+1)b^2}{a^2b} - \tfrac{a^3b+2b}{a^2}\}z^2 + b^2 - \tfrac{b^2}{a^2}. \end{aligned}$$

その余りは f_6 で割れるから，これまで通りであればそのまま割るのだが，係数に分数が多く式が煩雑になるだけであるから，ここでは余りに a^2b をかけて（余りの全体を $\frac{1}{a^2b}$ でくくって）得られた式

$$\begin{aligned} g = &(a^6b + a^3b)yz^3 + (a^4b^2 + a^3b^2)yz \\ &-(a^3+1)^2z^6 - (a^6b + 4a^3b + 3b)z^4 + (-2a^3b^2 + a^2b^2 - 3b^2)z^2 + a^2b^3 - b^3 \end{aligned}$$

を考え，それを f_6 で割ると

$$\begin{aligned} g &= abf_6 - (a^3+1)^2z^6 + \{ab(a^3+1) - (a^6b + 4a^3b + 3b)\}z^4 \\ &\quad +\{(-2a^3b^2 + a^2b^2 - 3b^2) - ab(a^4b - a^3b - 2b)\}z^2 + a^2b^3 - b^3 - a^3b^3 + ab^3 \\ &= abf_6 - (a^3+1)^2z^6 + (-a^6b + a^4b - 4a^3b + ab - 3b)z^4 \\ &\quad +(-a^5b^2 + a^4b^2 - 2a^3b^2 + a^2b^2 + 2ab^2 - 3b^2)z^2 + a^2b^3 - b^3 - a^3b^3 + ab^3 \end{aligned}$$

となる．この余りをグレブナー基底の候補に加えても問題はないが，ここでは -1 をかけた式を

$$\begin{aligned} f_7 &= (a^3+1)^2z^6 + (a^6b - a^4b + 4a^3b - ab + 3b)z^4 \\ &\quad +(a^5b^2 - a^4b^2 + 2a^3b^2 - a^2b^2 - 2ab^2 + 3b^2)z^2 + a^3b^3 - a^2b^3 - ab^3 + b^3 \end{aligned}$$

とする．よって，$\{f_1, f_2, f_3, f_4, f_5, f_6, f_7\}$ が I のグレブナー基底の候補となり，f_7 は I に含まれる．この f_7 は次のように 2 次式の積に因数分解できる，

$$f_7 = (a+1)\{(a+1)z^2 + b\}\{(a^2 - a + 1)z^2 + b\}\{(a^2 - a + 1)z^2 + (a-1)^2b\}.$$

定理 4.9　例 4.4 で登場した $\{g_1, g_2, g_3\}$ で生成されるイデアルを I とする．このとき，I には z の 6 次式で，次数 2 の多項式の積に分解される多項式

$$(z^2 + a^2 + b)(z^2 - 2az + 2a^2 + b)(z^2 + 2az + b)$$

が含まれる．また，I は S_3 不変なので，

$$\begin{aligned} &(x^2 + a^2 + b)(x^2 - 2ax + 2a^2 + b)(x^2 + 2ax + b), \\ &(y^2 + a^2 + b)(y^2 - 2ay + 2a^2 + b)(y^2 + 2ay + b) \end{aligned}$$

も含まれる．

(証明) 考える連立方程式は

$$\left\{\begin{array}{lcl} g_1 &=& 0 \\ g_2 &=& 0 \\ g_3 &=& 0 \end{array}\right.$$

である. Buchberger のアルゴリズムに登場した S 多項式を求めながら, $\{g_1, g_2, g_3\}$ で生成されるイデアル I に属する多項式を考えていく. まず, S 多項式 $S(g_2, g_3)$ を求めると,

$$\begin{array}{rcl} S(g_2, g_3) &=& (y^2 + ax + az + b) - (z^2 + ax + ay + b) \\ &=& y^2 - ay - z^2 + az. \end{array}$$

$g_4 := y^2 - ay - z^2 + az \in I$ とおく. 次に, S 多項式 $S(g_1, g_3)$ を求めると

$$\begin{array}{rcl} S(g_1, g_3) &=& a(x^2 + ay + az + b) - x(z^2 + ax + ay + b) \\ &=& -axy - xz^2 - bx + a^2y + a^2z + ab. \end{array}$$

$S(g_1, g_3)$ を g_3 で割って

$$\begin{array}{rcl} S(g_1, g_3) &=& (-y - \frac{1}{a}z^2 - \frac{b}{a})(z^2 + ax + ay + b) \\ && +ay^2 + 2yz^2 + (a^2 + 2b)y + \frac{1}{a}z^4 + \frac{2b}{a}z^2 + a^2z + ab + \frac{b^2}{a}. \end{array}$$

さらに, 余りは g_4 で割れるので

$$\begin{array}{rcl} S(g_1, g_3) &=& (-y - \frac{1}{a}z^2 - \frac{b}{a})(z^2 + ax + ay + b) + a(y^2 - ay - z^2 + az) \\ && +2yz^2 + (2a^2 + 2b)y + \frac{1}{a}z^4 + (\frac{2b}{a} + a)z^2 + ab + \frac{b^2}{a}. \end{array}$$

その余りはそのままでも I に含まれるが, 後の計算のために a をかけた式

$$g_5 = 2ayz^2 + (2a^3 + 2ab)y + z^4 + (a^2 + 2b)z^2 + a^2b + b^2 \in I$$

を考える. $S(g_4, g_5)$ を求めると

$$\begin{array}{rcl} S(g_4, g_5) &=& 2az^2(y^2 - ay - z^2 + az) \\ && -y\{2ayz^2 + (2a^3 + 2ab)y + z^4 + (a^2 + 2b)z^2 + a^2b + b^2\} \\ &=& -(2a^3 + 2ab)y^2 - yz^4 - (3a^2 + 2b)yz^2 - (a^2b + b^2)y - 2az^4 + 2a^2z^3. \end{array}$$

$S(g_4, g_5)$ を g_4 で割って

$$\begin{array}{rcl} S(g_4, g_5) &=& -(2a^3 + 2ab)(y^2 - ay - z^2 + az) - yz^4 - (3a^2 + 2b)yz^2 \\ && -(2a^4 + 3a^2b + b^2)y - 2az^4 + 2a^2z^3 - (2a^3 + 2ab)z^2 + (2a^4 + 2a^2b)z. \end{array}$$

さらに, 余りは g_5 で割れるので

$$\begin{array}{rcl} S(g_4, g_5) &=& -(2a^3 + 2ab)(y^2 - ay - z^2 + az) + (-\frac{1}{2a}z^2 - \frac{2a^2+b}{2a})\{2ayz^2 + (2a^3 + 2ab)y \\ && +z^4 + (a^2 + 2b)z^2 + a^2b + b^2\} + \frac{1}{2a}z^6 + (\frac{a}{2} + \frac{b}{a} - 2a + \frac{2a^2+b}{2a})z^4 + 2a^2z^3 \\ && +(\frac{ab}{2} + \frac{b^2}{2a} - 2a^3 - 2ab + \frac{2a^4+5a^2b^2+2b^2}{2a})z^2 + (2a^4 + 2a^2b)z + \frac{2a^4b+3a^2b^2+b^3}{2a}. \end{array}$$

この余りはそのままでも I に含まれるが, $2a$ をかけた式

$$g_6 = z^6 + (-a^2 + 3b)z^4 + 4a^3z^3 + (-2a^4 + 2a^2b + 3b^2)z^2 + (4a^5 + 4a^3b)z + 2a^4b + 3a^2b^2 + b^3 \in I$$

を考える. この g_6 は次のように 2 次式の積に因数分解できる,

$$g_6 = (z^2 + a^2 + b)(z^2 - 2az + 2a^2 + b)(z^2 + 2az + b).$$

注意 4.10 I を $K[x, y, z]$ の S_3 不変な 2 次式イデアルとする. すなわち, I は 2 次式で生成され, S_3 不変である. このとき, $J := I \cap K[z]$ は $K[z]$ のイデアルであり, 1 変数多項式環の性質より, $J \neq (0)$ であれば, J に含まれる多項式で次数が最小のもの g を取ってくると $J = (g)$ が成り立つ. そして, グレブナー基底の消去定理より, g は I の無駄のないグレブナー基底のメンバーであることが分かる. 残念ながら, 定理 4.5 と定理 4.9 で求めた z の 6 次式は, いつも I の無駄のないグレブナー基底のメンバーとは限らない. 実際,

$$\left\{\begin{array}{lcl} f_1 &=& x^2 + yz + 1 \\ f_2 &=& y^2 + xz + 1 \\ f_3 &=& z^2 + xy + 1 \end{array}\right.$$

で生成されるイデアル I の無駄のないグレブナー基底は,

$$\{2z^5+3z^3+z,\ yz^3+yz-z^4-z^2,\ y^2-yz+2z^4+3z^2+1,\ x-2yz^2-y-z\}$$

となる. z の 5 次式が登場し, 定理 4.5 で求めた 6 次式 $2z^6+3z^4+z^2$ は, それに含まれない. しかし, 定理 4.5 と 4.9 の結果から, 次は自然な問いかけであろう.

問 4.11　K を有理数体, I を $K[x,y,z]$ の S_3 不変な 2 次式イデアルとする. このとき, I の無駄のないグレブナー基底に含まれる 1 変数 z のみの整数係数多項式で, 2 次以下の整数係数の多項式の積に分解できるものが存在するか？

条件「S_3 不変」を外すと次のような反例がある.

例 4.12　連立方程式

$$\begin{cases} x^2+yz+3 &= 0 \\ y^2+2xz+2 &= 0 \\ z^2+3xy+1 &= 0 \end{cases}$$

について, $\{x^2+yz+3, y^2+2xz+2, z^2+3xy+1\}$ で生成されるイデアル I の純辞書式順序に関するグレブナー基底を求めると z のみの式として

$$343z^8+490z^6+1680z^4+8878z^2+2809$$

が得られる. これは K 上既約多項式である.

参考文献

[1] A. Conca, C. Krattenthaler and J. Watanabe, Regular sequences of symmetric porynomials, Rend. Semin. Mat. Univ. Padova 121 (2009), 179-199.

[2] D. コックス, J. リトル, D. オシー (大杉英史, 北村知徳, 日比孝之 訳), グレブナー基底, 丸善出版, 2012.

[3] A. V. Geramita, A. Hoefel and D. Wehlau, Hilbert functions of S_n-stable artinian Gerenstein algebras, J. Algebra 458 (2016), 53-70.

[4] T. Harima, A. Wachi and J. Watanabe, The quadratic complite intersections associated with the action of the symmetric group, Illinois J. Math. 59 (2015), 99-113.

[5] N. Kumar, Prime ideals and regular sequences of symmetric polynomials, Preprint, arXiv:1309.1098, 2013.

[6] N. Kumar and I. Martino, Regular sequences of power sums and complete symmetric polynomials, Preprint, arXiv:1110.6813, 2013.