# 零次元根基イデアルの素イデアル分解と記号的固有値法

# Prime decomposition of zero-dimensional radical ideals and symbolic eigenvalue method

筑波大学数理物質系　照井 章 [*1]
Akira Terui
Institute of Pure and Applied Sciences, University of Tsukuba

日本大学理工学部　石原 侑樹 [*2]
Yuki Ishihara
College of Science and Technology, Nihon University

金沢大学理工研究域　小原 功任 [*3]
Katsuyoshi Ohara
Faculty of Mathematics and Physics, Kanazawa University

新潟大学大学院自然科学研究科　田島 慎一 [*4]
Shinichi Tajima
Graduate School of Science and Technology, Niigata University

## 1　はじめに

多変数多項式環を零次元イデアルで割った剰余環は有限次元ベクトル空間である．剰余環における剰余類によって引き起こされる写像（倍写像）は線型写像であり，その表現行列の固有値から連立代数方程式の解を求める方法は固有値法と呼ばれ，多くの研究がなされている ([1]–[6], [8], [12])．また，固有値法を用いた準素イデアル分解の算法が提案されている [7].

我々はこれまでに，行列の最小消去多項式や最小消去多項式候補を用いて，固有空間，一般固有空間，スペクトル分解等を効率的に行うアルゴリズムを提案した．([10], [11], [13]–[23])．特に論文 [11] では一般固有空間を構成するアルゴリズムを提案した．我々の手法では代数拡大体での計算を用いないため効率的である．そこで，我々の方法を固有値法に適用することで，準素イデアル分解に対して新たなアプローチを行っていきたい．本稿では，特に零次元根基イデアルの素イデアル分解について考える.

[*1] 〒 305-8571 茨城県つくば市天王台 1-1-1　E-mail: terui@math.tsukuba.ac.jp
[*2] 〒 101-8308 東京都千代田区神田駿河台 1-8-14　E-mail: ishihara.yuki@nihon-u.ac.jp
[*3] 〒 920-1192 石川県金沢市角間町　E-mail: ohara@se.kanazawa-u.ac.jp
[*4] 〒 950-2181 新潟県新潟市西区五十嵐 2 の町 8050　E-mail: tajima@emeritus.niigata-u.ac.jp

## 2　行列 $A$ の固有空間と $\ker f(A)$ の Jordan-Krylov 基底

本節では，我々が先に書いた論文 [11] から，与えられた行列 $A$ の固有空間と $\ker f(A)$ の関係について復習する．なお，論文 [11] では一般固有空間の構成について述べられているが，本稿ではそのうち固有空間の構成のみを扱うことに注意する．

体 $K \subset \mathbb{C}$ を計算可能な部分体とする．行列 $A$ を $K$ 上の $n$ 次正方行列，$E$ を $n$ 次単位行列とし，$\alpha \in \mathbb{C}$ を $A$ の固有値とする．$\pi_A(\lambda) \in K[\lambda]$ を $A$ の最小多項式とし，$V_A(\alpha) = \{\boldsymbol{u} \in \mathbb{C}^n \mid (A - \alpha E)\boldsymbol{u} = \boldsymbol{0}\}$ を $\alpha$ に附随する $A$ の固有空間とする．$f(\lambda) \in K[\lambda]$ を $\alpha$ のモニックな定義多項式とする．対称多項式 $\psi_f(\mu, \lambda)$ を次で定義する．

$$\psi_f(\mu, \lambda) = \frac{f(\mu) - f(\lambda)}{\mu - \lambda} \in K[\mu, \lambda] \tag{1}$$

次が成り立つ．

**補題 1 ([11, Lemma 1])**
$\boldsymbol{u} \in \ker f(A)$ ならば $\psi_f(A, \alpha E) f(A)\boldsymbol{u} \in V(\alpha)$.

$\boldsymbol{w} \in K^n$ に対し，Krylov 巡回部分空間 $L_A(\boldsymbol{w})$ を次で定義する．

$$L_A(\boldsymbol{w}) = \mathrm{span}_K \{A^k \boldsymbol{w} \mid k = 0, 1, 2, \ldots\}$$

$A$ と $f(A)$ が可換であることから，$\boldsymbol{u} \in \ker f(A)$ に対し，$L_A(\boldsymbol{u}) \subset \ker f(A)$ が成り立つ．

**定理 2 ([11, Theorem 12])**
ある $\mathcal{B} \subset \ker f(A)$ が存在して $\ker f(A) = \bigoplus_{\boldsymbol{u} \in \mathcal{B}} L_A(\boldsymbol{u})$ が成り立つ．

定理 2 の $\mathcal{B}$ を $\ker f(A)$ の Jordan-Krylov 基底という．

$\boldsymbol{u} \in \ker f(A)$ に対し，$P_A(\lambda, \boldsymbol{u}) = \mathrm{span}_{\mathbb{C}}\{\psi_f(A, \lambda E)\boldsymbol{u}\}$ とおく．$\deg f = d$ とし，$\alpha_1, \ldots, \alpha_d \in \mathbb{C}$ を $f(\lambda)$ の根とする．$P_A(\boldsymbol{u}) = P_A(\alpha_1, \boldsymbol{u}) \oplus P_A(\alpha_2, \boldsymbol{u}) \oplus \cdots \oplus P_A(\alpha_d, \boldsymbol{u})$ とおく．補題 1 と定理 2 より，$\ker f(A)$ の Jordan-Krylov 基底が $A$ の固有空間を与えることがわかる．

**定理 3 ([11, Theorem 13])**
複素数 $\alpha_1, \ldots, \alpha_d \in \mathbb{C}$ を $f(\lambda)$ の根とする．このとき，以下が成り立つ．

1. $\boldsymbol{u} \in \ker f(A)$ ならば $P_A(\boldsymbol{u}) = \mathbb{C} \otimes_K L_A(\boldsymbol{u})$.
2. Jordan-Krylov 基底 $\mathcal{B} \subset \ker f(A)$ に対し，$\bigoplus_{\boldsymbol{b} \in \mathcal{B}} P_A(\alpha, \boldsymbol{b})$ は固有値 $\alpha$ に附随する $A$ の固有空間を与える．

## 3　零次元根基イデアルの剰余環の倍写像行列の同時固有分解

本節では，零次元根基イデアルの剰余環に対する固有値法について述べ，そこにおける倍写像行列の同時固有分解について説明する．

$\boldsymbol{x} = (x_1, \ldots, x_n)$ とする．$R = K[\boldsymbol{x}]$ を $K$ 上の多項式環とし，$I \subset R$ を $R$ の零次元根基イデアルとする．このとき $R/I$ は $K$ 上の有限次元ベクトル空間である．$\mathcal{B} = \{b_1, \ldots, b_m\}$ を $R/I$ の基底とする．$f(\boldsymbol{x}) \in R$ の $R/I$ における正規形は $I$ の Gröbner 基底を用いて計算される．

多項式 $r \in R$ の $R/I$ における剰余類をまた $r$ で表す．多項式 $r$ によって引き起こされる写像 $r : R/I \ni h \mapsto rh \in R/I$ は線型写像である．ここで，$\boldsymbol{b} = {}^t(b_1, \ldots, b_m)$ に対し，写像 $r$ の行列表現を $r\boldsymbol{b} = M_r\boldsymbol{b}$ で定める．このとき，この写像の合成は可換である．すなわち $r \circ s = s \circ r$. よって，行列表現 $M_r, M_s$ に対

し，$M_r M_s = M_s M_r$ が成り立つ．したがって，線形代数学でよく知られているように，$M_r$, $M_s$ による同時固有分解の理論が応用可能となる．いま，$r\boldsymbol{b} = M_r \boldsymbol{b}$ において，変数 $x_1, \ldots, x_n$ に $p \in V(I)$ の値を代入する操作を $r(p)\boldsymbol{b}(p) = M_r \boldsymbol{b}(p)$ と表す．このとき $(M_r - r(p)E)\boldsymbol{b}(p) = \boldsymbol{0}$ が成り立つ．すなわち，$r(p)$ は行列 $M_r$ の固有値であり，$\boldsymbol{b}(p)$ は $r(p)$ に附随する固有ベクトルである．しかも，多項式 $s \in R$ に対しても，$(M_s - s(p)E)\boldsymbol{b}(p) = \boldsymbol{0}$ であるので，$\boldsymbol{b}(p)$ は $M_r$ と $M_s$ の同時固有ベクトルであることがわかる．

複素数 $\alpha, \beta \in \mathbb{C}$ をそれぞれ $M_r, M_s$ の固有値とし，多項式 $f(\lambda), g(\lambda) \in K[\lambda]$ をそれぞれ $\alpha, \beta$ のモニックな定義多項式とする．$\boldsymbol{u} \in \ker f(M_r)$ に対し，$\boldsymbol{p}_r(\alpha, \boldsymbol{u}) = \psi_f(M_r, \alpha E)\boldsymbol{u}$ は $\alpha$ に附随する $M_r$ の固有ベクトルである．この固有ベクトルが $M_s$ との同時固有ベクトルであったとすると，

$$(M_s - \beta E)\psi_f(M_r, \alpha E)\boldsymbol{u} = \boldsymbol{0}$$

となる．この式を $\alpha = r(p)$ と $\beta = s(p)$ の関係式とみなすことができる．十分多くの表現行列を用いることで，$p \in V(P)$ となる素イデアル $P$ を求めることが期待できる．

**予想 4**
$\boldsymbol{u} \in \ker f(M_r) \cap \ker g(M_s)$ かつ $L_{M_s}(\boldsymbol{u}) \subset L_{M_r}(\boldsymbol{u})$ と仮定する．このとき，$\boldsymbol{p}_r(\alpha, \boldsymbol{u})$ は $M_r$ と $M_s$ の同時固有ベクトルである．

予想 4 の条件「$\boldsymbol{u} \in \ker f(M_r) \cap \ker g(M_s)$ かつ $L_{M_s}(\boldsymbol{u}) \subset L_{M_r}(\boldsymbol{u})$」を満たす Krylov 巡回部分空間 $L_{M_s}(\boldsymbol{u})$, $L_{M_r}(\boldsymbol{u})$ を「同時 Krylov 巡回部分空間」と呼ぶ．予想 4 が正しければ，$M_r$ および $M_s$ に関する同時 Krylov 巡回部分空間を求めることで，同時固有ベクトルを求めることが期待できる．

予想 4 に基づく計算手順をまとめたものをアルゴリズム 1 に示す．単純な手順で同時 Krylov 巡回部分空間が見つからない場合は，無作為に生成された多項式 $r(x_1, \ldots, x_n)$ を用いて同時 Krylov 巡回部分空間を求めることで同時固有ベクトルを求める．

**アルゴリズム 1 (零次元根基イデアルの素イデアル分解)**
**Input:** $I$ の Gröbner 基底, 変数 $V = \{x_1, \ldots, x_n\}$
**Output:** $P = P_1 \cap P_2 \cap \cdots \cap P_k$ ($P_i$: 素イデアル)

$B \leftarrow (K[\boldsymbol{x}]/I$ の基底$)$, $\quad M_i \leftarrow (B$ に関する $x_i$ 倍写像の表現行列$)$ ▷ Gröbner 基底を使う，$i = 1, \ldots, n$
$\chi_{M_i}(\lambda) \leftarrow f_{i,1}(\lambda)^{m_{i,1}} \cdots f_{i,q_i}(\lambda)^{m_{i,q_i}}$ ▷ $M_i$ の特性多項式
$P \leftarrow \emptyset$ ▷ 素イデアルのリスト
**for** $\boldsymbol{j} = (j_1, j_2, \ldots, j_n)$ **do** ▷ $1 \le i < i' \le n$, $1 \le j_i \le q_i$, $1 \le j'_i \le q'_i$
  $\boldsymbol{u}_{\boldsymbol{j}} \leftarrow (\bigcap \ker f_{i,j_i}(M_i)$ の Jordan-Krylov 基底$)$, $\quad P' \leftarrow \emptyset$
  **if** $\boldsymbol{u}_{\boldsymbol{j}} \neq \boldsymbol{0}$ and $\exists i$ s.t. $L_{M_{i'}}(\boldsymbol{u}_{\boldsymbol{j}}) \subset L_{M_i}(\boldsymbol{u}_{\boldsymbol{j}})$ for all $i' \neq i$ **then**
    $\boldsymbol{v}_i(x_i) \leftarrow \psi_{f_{i,j_i}}(M_i, x_i E)\boldsymbol{u}_{\boldsymbol{j}}$
    $P' \leftarrow P' \cup \{(M_{i'} - x_{i'}E)\boldsymbol{v}_i(x_i)[k] \mid k = 1, \ldots, n\}$ ▷ $\boldsymbol{v}[k]$: $\boldsymbol{v}$ の第 $k$ 成分
    $P'$ の関係式を簡約, $\quad P \leftarrow P \cup \{P'\}$
  **else**
    (ランダムな多項式 $r$ から決まる行列 $M_r$ を加えてアルゴリズム 1 を再実行する)
  **end if**
**end for**
**return** $P$

# 4 計算例

以下では，アルゴリズム 1 による具体的な計算例を示す．以下の計算には数式処理システム Risa/Asir を用いている．

**例 1 (Cyclic-3** [8, Example 3]**)**
多項式環 $R = K[x, y, z]$ において，$I$ を以下の多項式で生成されるイデアルとする．

$$p_1 = x + y + z, \quad p_2 = xy + yz + zx, \quad p_3 = xyz - 1$$

あらかじめ得られている $I$ の素イデアル分解は次の通りである．

$$I = \langle y^2 + y + 1, x + y + 1, z - 1\rangle \cap \langle z^2 + z + 1, x - 1, y + z + 1\rangle \cap \langle z^2 + z + 1, x + z + 1, y - 1\rangle$$

単項式順序を $x > y > z$ とする全次数逆辞書式順序 (DegRevLex) とする．剰余環 $R/I$ の基底 $\mathcal{B}$ は次の通りである．

$$\mathcal{B} = \{yz^2, yz, z, y, z, 1\}$$

倍写像の表現行列は 6 次正方行列である．倍写像行列 $M_x, M_y, M_z$ の同時固有分解を求める．$M_x, M_y, M_z$ の特性多項式をそれぞれ $\chi_x(\lambda), \chi_y(\lambda), \chi_z(\lambda)$ とすると，

$$\chi_x(\lambda) = \chi_y(\lambda) = \chi_z(\lambda) = (\lambda^2 + \lambda + 1)^2(\lambda - 1)^2$$

である．$f_1(\lambda) = \lambda^2 + \lambda + 1$，$f_2(\lambda) = \lambda - 1$ とする．

$\ker f_i(M_x) \cap \ker f_j(M_y) \cap \ker f_k(M_z) \neq \{\mathbf{0}\}$ $(i, j, k \in \{1, 2\})$ に含まれる Krylov 巡回部分空間を求める．（以下，$\boldsymbol{u}_{ijk} \in \ker f_i(M_x) \cap \ker f_j(M_y) \cap \ker f_k(M_z)$ とする．）

1. $\ker f_1(M_x) \cap \ker f_1(M_y) \cap \ker f_2(M_z) \ni \boldsymbol{u}_{112} = {}^t(1, 1, 0, 1, 0, 0)$ とおくと，$L_{M_x}(\boldsymbol{u}_{112}) = L_{M_y}(\boldsymbol{u}_{112}) \supset L_{M_z}(\boldsymbol{u}_{112})$ が成り立つ．$\boldsymbol{u}_{112}$ を用いて $M_x$ の固有ベクトルを求めると

$$\boldsymbol{v}_{112x}(\lambda) = \psi_{f_1}(M_x, \lambda E)\boldsymbol{u}_{112} = {}^t(\lambda + 1, \lambda + 1, 1, \lambda + 1, 1, 1)$$

を得る．$\boldsymbol{v}_{112x}(\lambda)$ が $M_y$ の固有値 $y$ および $M_z$ の固有値 $z$ に附随する固有ベクトルであることを用いると，以下の関係式を得る．

$$\begin{aligned}
&(M_y - yE)\boldsymbol{v}_{112x}(x) \\
&= {}^t(-(x+1)y - x, -(x+1)y - x, -y - x - 1, -(x+1)y - x, -y - x - 1, -y - x - 1) = \mathbf{0}, \\
&(M_z - zE)\boldsymbol{v}_{112x}(x) \\
&= {}^t((x+1)(1-z), (x+1)(1-z), -z + 1, (x+1)(1-z), -z + 1, -z + 1) = \mathbf{0}.
\end{aligned}$$

これに $M_x$ の固有値 $x$ の定義多項式 $f_1(x) = x^2 + x + 1$ を加えてから関係式を整理すると，固有値 $x, y, z$ に関する関係式として

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

を得る．

2. $\ker f_1(M_x) \cap \ker f_2(M_y) \cap \ker f_1(M_z) \ni \boldsymbol{u}_{121} = {}^t(-1, 0, -1, 1, 1, 0)$ とおくと，$L_{M_x}(\boldsymbol{u}_{121}) = L_{M_y}(\boldsymbol{u}_{121}) \supset L_{M_z}(\boldsymbol{u}_{121})$ が成り立つ．$\boldsymbol{u}_{121}$ を用いて $M_x$ の固有ベクトルを求めると

$$\boldsymbol{v}_{121x}(\lambda) = \psi_{f_1}(M_x, \lambda E)\boldsymbol{u}_{121} = {}^t(-\lambda, -1, -\lambda - 1, \lambda + 1, \lambda, 1)$$

を得る．$\boldsymbol{v}_{121x}(\lambda)$ が $M_y$ の固有値 $y$ および $M_z$ の固有値 $z$ に附随する固有ベクトルであることを用いると，以下の関係式を得る．

$$(M_y - yE)\boldsymbol{v}_{121x}(x) = {}^t(x(y-1), y-1, (x+1)(y-1), (x+1)(1-y), x(1-y), -y+1) = \mathbf{0},$$
$$(M_z - zE)\boldsymbol{v}_{112x}(x) = {}^t(xz-1, z+x+1, (x+1)z+x, (-x-1)z-x, -xz+1, -z-x-1) = \mathbf{0}.$$

これに $M_x$ の固有値 $x$ の定義多項式 $f_1(x) = x^2+x+1$ を加えてから関係式を整理すると，固有値 $x, y, z$ に関する関係式として

$$\{y-1, -z-x+1, z^2+z+1\} \tag{3}$$

を得る．

3. $\ker f_2(M_x) \cap \ker f_1(M_y) \cap \ker f_1(M_z) \ni \boldsymbol{u}_{211} = {}^t(-1,0,1,1,0,-1)$ とおくと，$L_{M_y}(\boldsymbol{u}_{211}) = L_{M_z}(\boldsymbol{u}_{211}) \supset L_{M_z}(\boldsymbol{u}_{121})$ が成り立つ．$\boldsymbol{u}_{211}$ を用いて $M_y$ の固有ベクトルを求めると

$$\boldsymbol{v}_{211y}(\lambda) = \psi_{f_1}(M_y, \lambda E)\boldsymbol{u}_{211} = {}^t(-\lambda, -1, \lambda, \lambda+1, 1, -\lambda-1)$$

を得る．$\boldsymbol{v}_{211y}(\lambda)$ が $M_x$ の固有値 $x$ および $M_z$ の固有値 $z$ に附随する固有ベクトルであることを用いると，以下の関係式を得る．

$$(M_x - xE)\boldsymbol{v}_{211y}(y) = {}^t((x-1)y, x-1, (-x+1)y, (-x+1)(y+1), -x+1, (x-1)(y+1)) = \mathbf{0},$$
$$(M_z - zE)\boldsymbol{v}_{211y}(y) = {}^t(yz-1, y+z+1, -yz+1, (-z-1)y-z, -y-z-1, (z+1)y+z) = \mathbf{0}.$$

これに $M_x$ の固有値 $x$ の定義多項式 $f_1(x) = x^2+x+1$ を加えてから方程式を整理すると，固有値 $x, y, z$ に関する関係式として

$$\{-y-z-1, -x+1, z^2+z+1\} \tag{4}$$

を得る．

上の計算結果 (2), (3), (4) より，イデアル $I$ の素イデアル分解として

$$\langle z-1, x+y+1, y^2+y+1\rangle \cap \langle y-1, -z-x+1, z^2+z+1\rangle \cap \langle -y-z-1, -x+1, z^2+z+1\rangle$$

を得る．▮

**例 2**
多項式環 $R = K[x,y]$ において，$I$ を以下の多項式で生成されるイデアルとする．

$$p_1 = x^2 + 4(y-2)^2 - 4, \quad p_2 = \{2x + (y-2) - 2\}\{2x - (y+2) - 2\}$$

あらかじめ得られている $I$ の素イデアル分解は次の通りである．

$$I = \langle 17x^2 - 32x + 12, 2x + y - 4\rangle \cap \langle 17x^2 - 96x + 140, -2x + y + 4\rangle$$

単項式順序を $y > x$ とする全次数逆辞書式順序 (DegRevLex) とする．剰余環 $R/I$ の基底 $\mathcal{B}$ は次の通りである．

$$\mathcal{B} = \{xy, y, x, 1\}$$

倍写像の表現行列は 4 次正方行列である．倍写像行列 $M_x, M_y$ の同時固有分解を求める．$M_x, M_y$ の特性多項式をそれぞれ $\chi_x(\lambda), \chi_y(\lambda)$ とすると，

$$\begin{aligned}
\chi_x(\lambda) &= f_{x,1}(\lambda)f_{x,2}(\lambda), & f_{x,1}(\lambda) &= (17\lambda^2 - 96\lambda + 140), & f_{x,2}(\lambda) &= (17\lambda^2 - 32\lambda + 12), \\
\chi_y(\lambda) &= f_{y,1}(\lambda)f_{y,2}(\lambda), & f_{y,1}(\lambda) &= (17\lambda^2 - 72\lambda + 64), & f_{y,2}(\lambda) &= (17\lambda^2 - 56\lambda + 64)
\end{aligned}$$

である．$\ker f_{x,i}(M_x) \cap \ker f_{y,j}(M_y) \neq \{\mathbf{0}\}$ $(i, j \in \{1, 2\})$ に含まれる Krylov 巡回部分空間を求める．

1. $\ker f_{x,1}(M_x) \cap \ker f_{y,2}(M_y) \ni \boldsymbol{u}_{12} = {}^t(0, -1, -2, 4)$ とおくと，$L_{M_x}(\boldsymbol{u}_{12}) \subset L_{M_y}(\boldsymbol{u}_{12})$ が成り立つ．$\boldsymbol{u}_{12}$ を用いて $M_y$ の固有ベクトルを求めると

$$\boldsymbol{v}_{12y}(\lambda) = \psi_{f_{y,2}}(M_y, \lambda E)\boldsymbol{u}_{12} = {}^t(-34, -17\lambda + 60, -34\lambda + 128, 68\lambda - 192)$$

を得る．$\boldsymbol{v}_{12y}(\lambda)$ が $M_x$ の固有値 $x$ に附随する固有ベクトルであることを用いると，以下の関係式を得る．

$$\begin{aligned}
(M_x - xE)\boldsymbol{v}_{12y}(y) = {}^t(&-17y + 34x - 68, (17x - 32)y - 60x + 152, (34x - 60)y - 128x + 320, \\
&(-68x + 152)y + 192x - 512) = \mathbf{0}.
\end{aligned}$$

上の関係式を整理すると，固有値 $x$, $y$ に関する関係式として

$$\{-y + 2x - 4, -17x^2 + 96x - 140\} \tag{5}$$

を得る．

2. $\ker f_{x,2}(M_x) \cap \ker f_{y,1}(M_y) \ni \boldsymbol{u}_{21} = {}^t(0, 1, -2, 4)$ とおくと，$L_{M_x}(\boldsymbol{u}_{21}) \subset L_{M_y}(\boldsymbol{u}_{21})$ が成り立つ．$\boldsymbol{u}_{21}$ を用いて $M_y$ の固有ベクトルを求めると

$$\boldsymbol{v}_{21y}(\lambda) = \psi_{f_{y,1}}(M_y, \lambda E)\boldsymbol{u}_{21} = {}^t(-34, 17\lambda + 60, -34\lambda + 128, 68\lambda - 320)$$

を得る．$\boldsymbol{v}_{21y}(\lambda)$ が $M_x$ の固有値 $x$ に附随する固有ベクトルであることを用いると，以下の関係式を得る．

$$\begin{aligned}
(M_x - xE)\boldsymbol{v}_{21y}(y) = {}^t(&17y + 34x - 68, (-17x - 32)y - 60x + 152, \\
&(34x - 60)y - 128x + 192, (-68x + 152)y + 320x - 512) = \mathbf{0}.
\end{aligned}$$

上の関係式を整理すると，固有値 $x$, $y$ に関する関係式として

$$\{y + 2x - 4, 17x^2 - 32x + 12\} \tag{6}$$

を得る．

上の計算結果 (5), (6) より，イデアル $I$ の素イデアル分解として

$$\langle 2x - y - 4, -17x^2 + 96x - 140\rangle \cap \langle 2x + y - 4, 17x^2 - 32x + 12\rangle$$

を得る．∎

**例 3**

多項式環 $R = K[x, y]$ において，$I$ を以下の多項式で生成されるイデアルとする．

$$p_1 = x^2 - 2, \quad p_2 = y^2 - 2$$

あらかじめ得られている $I$ の素イデアル分解は次の通りである．

$$I = \langle x^2-2, -x+y\rangle \cap \langle x^2-2, -x-y\rangle$$

単項式順序を $y > x$ とする全次数逆辞書式順序 (DegRevLex) とする．剰余環 $R/I$ の基底 $\mathcal{B}$ は次の通りである．

$$\mathcal{B} = \{xy, y, x, 1\}$$

倍写像の表現行列は 4 次正方行列である．倍写像行列 $M_x, M_y$ の同時固有分解を求める．$M_x, M_y$ の特性多項式をぞれぞれ $\chi_x(\lambda), \chi_y(\lambda)$ とすると，

$$\chi_x(\lambda) = \chi_y(\lambda) = (\lambda^2-2)^2$$

である．この例では $\ker f_1(M_x) \cap \ker f_1(M_y) \ni \boldsymbol{u}$, かつ $L_{M_x}(\boldsymbol{u}) \subset L_{M_y}(\boldsymbol{u})$ または $L_{M_y}(\boldsymbol{u}) \subset L_{M_x}(\boldsymbol{u})$ を満たす $\boldsymbol{u}$ が（存在はするが）容易には見つからない．そこで $r = 2y + x$ とおく．$M_r$ の特性多項式を $\chi_r(\lambda)$ とすると，

$$\chi_r(\lambda) = (\lambda^2-2)(\lambda^2-18)$$

である．$f_1(\lambda) = \lambda^2 - 2$, $f_2(\lambda) = \lambda^2 - 18$ とする．

1. $\ker f_1(M_r) \ni \boldsymbol{u}_{r1} = {}^t(1,0,0,2)$ とおくと，$L_{M_x}(\boldsymbol{u}_{r1}) = L_{M_y}(\boldsymbol{u}_{r1}) = L_{M_r}(\boldsymbol{u}_{r1}) \subset \ker f_1(M_x) \cap \ker f_1(M_y)$ が成り立つ．$\boldsymbol{u}_{r1}$ を用いて $M_y$ の固有ベクトルを求めると

$$\boldsymbol{v}_{r1y}(\lambda) = \psi_{f_1}(M_y, \lambda E)\boldsymbol{u}_{r1} = {}^t(\lambda, 2, 2, 2\lambda)$$

を得る．$\boldsymbol{v}_{r1y}(\lambda)$ が $M_x$ の固有値 $x$ に附随する固有ベクトルであることを用いると，以下の関係式を得る．

$$(M_x - xE)\boldsymbol{v}_{r1y}(y) = {}^t(-xy+2, 2(x-y), 2(x-y), -2(xy-2) = \mathbf{0}.$$

上の関係式を整理すると，固有値 $x$, $y$ に関する関係式として

$$\{x-y, x^2-2\} \tag{7}$$

を得る．

2. $\ker f_2(M_r) \ni \boldsymbol{u}_{r2} = {}^t(-1,0,0,2)$ とおくと，$L_{M_x}(\boldsymbol{u}_{r1}) = L_{M_y}(\boldsymbol{u}_{r1}) = L_{M_r}(\boldsymbol{u}_{r1}) \subset \ker f_1(M_x) \cap \ker f_1(M_y)$ が成り立つ．$\boldsymbol{u}_{r2}$ を用いて $M_y$ の固有ベクトルを求めると

$$\boldsymbol{v}_{r2y}(\lambda) = \psi_{f_2}(M_y, \lambda E)\boldsymbol{u}_{r2} = {}^t(-\lambda, 2, -2, 2\lambda)$$

を得る．$\boldsymbol{v}_{r2y}(\lambda)$ が $M_x$ の固有値 $x$ に附随する固有ベクトルであることを用いると，以下の関係式を得る．

$$(M_x - xE)\boldsymbol{v}_{r2y}(y) = {}^t(xy+2, -2(x+y), 2(x+y), -2(xy+2)) = \mathbf{0}.$$

上の関係式を整理すると，固有値 $x$, $y$ に関する関係式として

$$\{x+y, x^2-2\} \tag{8}$$

を得る．

上の計算結果 (7), (8) より，イデアル $I$ の素イデアル分解として

$$\langle x-y, x^2-2\rangle \cap \langle x+y, x^2-2\rangle$$

を得る．∎

# 参 考 文 献

[1] W. Auzinger and H. J. Stetter. An elimination algorithm for the computation of all zeros of a system of multivariate polynomial equations. In *Numerical Mathematics Singapore 1988*, pages 11–30. Springer Basel AG, 1988.

[2] D. Cox, J. Little, and D. O'Shea. Unsing Algebraic Geometry. Springer, 2005.

[3] D. Lazard. Resolution des systemes d'equations algebriques. *Theoretical Computer Science*, 15(1):77–110, 1981.

[4] H. M. Möller. Systems of algebraic equations solved by means of endomorphisms. Lecture Notes in Computer Science 673, Springer, 43–56, 1993.

[5] H. M. Möller and Hans J. Stetter. Multivariate polynomial equations with multiple zeros solved by matrix eigenproblems. *Numerische Mathematik*, 70(3):311–329, 1995.

[6] H. M. Möller and R. Tenberg. Multivariate polynomial system solving using intersections of eigenspaces. *Journal of Symbolic Computation*, 32(5):513–531, 2001.

[7] C. Monico. Computing the Primary Decomposition of Zero-dimensional Ideals. *Journal of Symbolic Computation*, 34(5):451–459, 2002.

[8] S. Moritsugu and K. Kuriyama. A Equations Linear Algebra Method for Solving Systems of Algebraic Equations. 数式処理, 7(4): 2–22, 2000.

[9] S. Tajima, K. Ohara, and A. Terui. Fast Algorithm for Calculating the Minimal Annihilating Polynomials of Matrices via Pseudo Annihilating Polynomials. preprint, 27 pages. `https://arxiv.org/abs/1801.08437`

[10] S. Tajima, K. Ohara, and A. Terui. Fast Algorithms for Computing Eigenvectors of Matrices via Pseudo Annihilating Polynomials. preprint, 17 pages. `https://arxiv.org/abs/1811.09149`

[11] S. Tajima, K. Ohara, and A. Terui. Exact algorithms for computing generalized eigenspaces of matrices via annihilating polynomials, 2022. preprint, 23 pages. `https://arxiv.org/abs/2209.04807`

[12] K. Yokoyama, M. Noro, and T. Takeshima. Solutions of systems of algebraic equations and linear maps on residue class rings. *Journal of Symbolic Computation*, 14(4):399–417, 1992.

[13] 小原功任, 田島慎一. 最小消去多項式を用いた行列スペクトル分解計算の並列化. Computer Algebra: Design of Algorithms, Implementations and Applications, 数理解析研究所講究録, 第 1815 巻, pp. 21–28. 京都大学数理解析研究所, 2012.

[14] 小原功任, 田島慎一. 最小消去多項式候補を用いた行列の一般固有空間の構造の計算法について. 数式処理研究と産学研究の新たな発展, MI レクチャーノート, 第 49 巻, pp. 113–118. 九州大学マス・フォア・インダストリ研究所, 2013.

[15] 小原功任, 田島慎一. 最小消去多項式候補を用いた行列の一般固有空間の構造の計算アルゴリズム. 数式処理とその周辺分野の研究, 数理解析研究所講究録, 第 1907 巻, pp. 62–70. 京都大学数理解析研究所, 2014.

[16] 小原功任, 田島慎一. 最小消去多項式を用いた一般固有ベクトル空間の基底計算法. 数式処理とその周辺分野の研究, 数理解析研究所講究録, 第 1955 巻, pp. 198–204. 京都大学数理解析研究所, 2015.

[17] 田島慎一. 一般固有ベクトル空間の構造を求める計算法について. Computer Algebra: The Algorithms, Implementations and the Next Generation, 数理解析研究所講究録, 第 1843 巻, pp. 146–154. 京都大学数理解析研究所, 2013.

[18] 田島慎一, 小原功任, 照井章. 最小消去多項式を用いた Jordan 細胞の構造の効率的な計算. Computer Algebra — Foundations and Applications, 数理解析研究所講究録, 第 2280 巻, pp. 186–194. 京都大学数理解析研究所, 2024.

[19] 田島慎一, 照井章. 行列の最小消去多項式候補を利用した固有ベクトル計算. 数式処理とその周辺分野の研究, 数理解析研究所講究録, 第 1815 巻, pp. 13–20. 京都大学数理解析研究所, 2012.

[20] 田島慎一, 照井章. 行列の最小消去多項式候補を利用した固有ベクトル計算 (II). 数式処理研究と産学研究の新たな発展, MI レクチャーノート, 第 49 巻, pp. 119–127. 九州大学マス・フォア・インダストリ研究所, 2013.

[21] 田島慎一, 照井章. 行列の最小消去多項式候補を利用した固有ベクトル計算 (III). 数式処理とその周辺分野の研究, 数理解析研究所講究録, 第 1907 巻, pp. 50–61. 京都大学数理解析研究所, 2014.

[22] 田島慎一, 照井章. 行列の最小消去多項式候補を利用した固有ベクトル計算 (IV). 数式処理とその周辺分野の研究, 数理解析研究所講究録, 第 1955 巻, pp. 188–197. 京都大学数理解析研究所, 2015.

[23] 田島慎一, 奈良洸平. 最小消去多項式候補とその応用. In *Computer Algebra — Design of Algorithms, Implementations and Applications*, 数理解析研究所講究録, 第 1815 巻, pp. 1–12. 京都大学数理解析研究所, 2012.