零次元イデアルの根基の素イデアル分解と記号的固有値法

Prime decomposition of the radical of zero-dimensional 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]–[24])．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．我々の手法は代数拡大体での計算を用いないため効率的であるという特徴を持つ.

我々はこの手法を用いて，固有値法を用いた零次元根基イデアルの素イデアル分解の算法を提案した [19]. 本稿ではこれに基づき，同じアプローチを用いた零次元イデアルの根基の素イデアル分解の算法について議論する.

[*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

体 $K \subset \mathbb{C}$ を $\mathbb{C}$ の計算可能な部分体とする．本稿では $K = \mathbb{Q}$ とする．A を K 上の n 次正方行列とし，π_A を A の最小多項式とする．E を n 次単位行列とする．$\alpha \in \mathbb{C}$ を A の固有値とし，$V(\alpha) = \{\boldsymbol{p} \in \mathbb{C}^n \mid (A-\alpha E)\boldsymbol{p} = \boldsymbol{0}\}$ を α に附随する A の固有空間とする．$f(\lambda) \in K[\lambda]$ を α のモニックな定義多項式とする．

$\ker f(A) = \{\boldsymbol{u} \in K^n \mid f(A)\boldsymbol{u} = \boldsymbol{0}\}$ とする．対称多項式 $\psi_f(\mu, \lambda)$ を以下で定義する．

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

次が成り立つ．

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

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

$$L_A(\boldsymbol{w}) = \mathrm{span}_K\{\boldsymbol{w}, A\boldsymbol{w}, A^2\boldsymbol{w}, \ldots\}.$$

線型写像 A と $f(A)$ は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 基底と呼ぶ．

$\boldsymbol{u} \in \ker f(A)$ 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 α に附随する A の固有空間を与える．

3　零次元イデアルの根基の剰余環の倍写像行列の同時固有分解

本節では，零次元イデアルの剰余環に対する固有値法について述べ，倍写像行列の同時固有分解について述べる．

$\boldsymbol{x} = (x_1, \ldots, x_n)$ とする．$R = K[\boldsymbol{x}]$ を K 上の多項式環とし，$I \subset R$ を零次元イデアルとする．R/I を I の剰余環とする．このとき R/I は有限次元 K-ベクトル空間である．$\mathcal{M} = \{b_1, \ldots, b_m\}$ 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 における剰余類もまた 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 $r \circ s = s \circ r$ が成り立つ．よって，行列表現 M_r, M_s に対し，$M_rM_s = M_sM_r$ が成り立つ．したがって，M_r, M_s による同時固有分解が可能となる．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 $r(p)\boldsymbol{b}(p) = M_r(p)\boldsymbol{b}(p)$ と表す．こ

のとき $(M_r - r(p)E)\boldsymbol{b}(p) = \mathbf{0}$ 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，$(M_s - s(p)E)\boldsymbol{b}(p) = \mathbf{0}$ も成り立つので，$\boldsymbol{b}(p)$ は M_r と M_s の同時固有ベクトルである．

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 α, β 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 α に附随する M_r の固有ベクトルである．$\boldsymbol{p}_r(\alpha, \boldsymbol{u})$ が M_s との同時固有ベクトルであったとすると，

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

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．

我々は固有ベクトルの構成を K 上の Krylov 巡回部分空間の構成に帰着させ，$\mathbb{C}$ 上の計算を避けることで効率化を図る．また，素イデアル分解は $\mathbb{C}$ 上の固有ベクトルの関係に対応する K 上の Krylov 巡回部分空間の関係を用いることで行われる．以下では $\mathbb{C}$ 上の固有ベクトルの関係に対応する K 上の Krylov 巡回部分空間の関係に帰着させる．

I は一般の零次元イデアルであるため，R/I における倍写像は一般に一般固有空間を持つ．一方で，その部分空間である固有ベクトル空間は，I の根基 $\sqrt{I}$ の剰余環 $R/\sqrt{I}$ における倍写像の固有空間に対応することが期待される [12]．そこで，R/I における倍写像の一般固有空間に対し，その部分空間である固有ベクトル空間の同時固有分解を行うことにより，根基 $\sqrt{I}$ の素イデアル分解を行うことを目指す．

以下，A, B などで互いに可換で最小多項式が無平方となるような K 上の正方行列を表す．

定理 4
B の固有値 β の最小多項式を $g(\lambda)$ とする．このとき，$\boldsymbol{u} \in \ker g(B)$ が Krylov 巡回空間の包含関係 $L_A(\boldsymbol{u}) \subset L_B(\boldsymbol{u})$ を満たすならば，ベクトル $\boldsymbol{p} = \psi_f(B, \beta E)\boldsymbol{u}$ は A と B の同時固有ベクトルを与える．

命題 5
定理 4 において，A の固有値 α の最小多項式を $f(\lambda)$ とするとき，$\boldsymbol{u} \in \ker f(A)$ が成り立つ．

ここで「同時 Krylov 巡回部分空間」を定義する．

定義 6
$A_1, \ldots, A_m$ を可換な n 次正方行列，$\boldsymbol{u}$ を n 次元ベクトルとする．

$$L_{\{A_1,\ldots,A_m\}}(\boldsymbol{u}) = \mathrm{span}_K\{A_1^{e_1} \cdots A_m^{e_m}\boldsymbol{u} \mid e_1, \ldots, e_m \in \mathbb{Z}_{\geq 0}\}$$

を $A_1, \ldots, A_m$ に関する $\boldsymbol{u}$ の同時 Krylov 巡回部分空間という．

命題 7
$A_1, \ldots, A_m$ を可換な n 次正方行列，$\boldsymbol{u}$ を n 次元ベクトル，$F(x_1, \ldots, x_m) \in K[x_1, \ldots, x_m]$ とする．正方行列 $B = F(A_1, \ldots, A_m)$ が $L_{A_i}(\boldsymbol{u}) \subset L_B(\boldsymbol{u})$ $(i = 1, \ldots, m)$ を満たすならば，$L_{\{A_1,\ldots,A_m\}}(\boldsymbol{u}) = L_B(\boldsymbol{u})$ が成り立つ．

定理 4 から，行列 A, B の同時固有ベクトルを求めるためには，$L_A(\boldsymbol{u}) \subset L_B(\boldsymbol{u})$ を満たす $\boldsymbol{u} \in \ker g(B)$ を選ぶ必要があるが，それは一般には簡単ではない．しかしながら，特別な状況下では，選ぶことができる場合もある．その一つとして，Jordan-Krylov の意味で単項生成の概念を導入する．

定義 8
ベクトル空間 V と行列 A に対し，$V = L_A(\boldsymbol{u})$ となるベクトル $\boldsymbol{u}$ が存在するとき，V は *Jordan-Krylov* の意味で**単項生成**である．

定義 9 (最小消去多項式)
多項式環 $K[\lambda]$ の単項イデアル $\mathrm{Ann}_{K[\lambda]}(A,\boldsymbol{u}) = \{g(\lambda) \in K[\lambda] \mid g(A)\boldsymbol{u} = \boldsymbol{0}\}$ のモニックな生成元 $\pi_{A,\boldsymbol{u}}(\lambda)$ を，A に関する $\boldsymbol{u}$ の最小消去多項式という．

命題 10
B の最小多項式の既約因子 $g(\lambda)$ について，$\ker g(B)$ が Jordan-Krylov の意味で $\boldsymbol{u}$ で単項生成ならば，$L_A(\boldsymbol{u}) \subset L_B(\boldsymbol{u})$ である．さらに最小消去多項式 $\pi_{A,\boldsymbol{u}}(\lambda)$ を既約にできる．

上の命題より $\boldsymbol{u} \in \ker f(A) \cap \ker g(B)$ である．

定義 11
行列 B の最小多項式 $\pi_B(\lambda)$ の任意の既約因子 $g(\lambda)$ に対し，$\ker g(B)$ が Jordan-Krylov の意味で単項生成であるとき，B は**支配的**であるという．

倍写像 $x_1, \ldots, x_n \in R/I$ の表現行列をそれぞれ $A_1, \ldots, A_n$ とする．ある A_i が支配的ならば，$\ker f(A_i)$ の Jordan-Krylov 基底を用いて $A_1, \ldots, A_n$ の同時固有ベクトルがとれることになる．一方、どの A_i も支配的でなければ，確率的なアルゴリズムによって同時固有ベクトルを構成できると考えられる．つまり，倍写像 $r \in \mathbb{R}/I$ でその表現行列が支配的であるようなものをうまく選ぶ（その行列を B とする）．このとき，$\ker g(B)$ の Jordan-Krylov 基底から $A_1, \ldots, A_n$ および B の同時固有ベクトルが作れる．

命題 12
$f(\lambda)$ は行列 A_1 の最小多項式の既約因子とし，$\ker f(A_1) = L_{A_1}(\boldsymbol{u})$ であるとする．$\pi_{A_i,\boldsymbol{u}}(\lambda) = f_i(\lambda)h_i(\lambda)$ $(i = 2, \ldots, n)$ とおき，

$$\boldsymbol{v} = h_2(A_2)h_3(A_3)\cdots h_n(A_n)\boldsymbol{u}$$

とする．このとき $\ker f(A_1) = L_{A_1}(\boldsymbol{v})$ かつ $\boldsymbol{v} \in \ker f(A_1) \cap \ker f_2(A_2) \cap \cdots \cap \ker f_n(A_n)$ が成り立つ．さらに $\ker f(A_1) = L_{\{A_1,\ldots,A_n\}}(\boldsymbol{v})$ である．

定義 13
倍写像 $x_1, \ldots, x_n \in R/I$ の表現行列をそれぞれ $A_1, \ldots, A_n$ とする．倍写像 $r \in R/I$ の表現行列を B とし，$g(\lambda)$ を B の最小多項式の既約因子とする．B は支配的であるとし，ある $\boldsymbol{u} \in \ker g(B)$ が存在して $\ker g(B) = L_B(\boldsymbol{u})$ とする．$f_i(\lambda)$ を行列 A_i に関する $\boldsymbol{u}$ の最小消去多項式の既約因子とし，$\pi_{A_i,\boldsymbol{u}}(\lambda) = f_i(\lambda)h_i(\lambda)$ とする．このとき，

$$\begin{aligned} &I_{\{(A_1,f_1),(A_2,f_2),\ldots,(A_n,f_n),(B,g),\boldsymbol{u}\}} \\ &\quad = I + \langle g(r)\rangle + \langle {}^t\boldsymbol{w}(A_i - x_iE)\psi_g(B,rE)h_1(A_1)h_2(A_2)\cdots h_n(A_n)\boldsymbol{u} \mid \boldsymbol{w} \in K^n, i = 1,\ldots,n\rangle \quad (1) \end{aligned}$$

を $\{(A_1,f_1),(A_2,f_2),\ldots,(A_n,f_n),(B,g),\boldsymbol{u}\}$ **に対応するイデアル**という．

式 (1) のイデアル $I_{\{(A_1,f_1),(A_2,f_2),\ldots,(A_n,f_n),(B,g),\boldsymbol{u}\}}$ は素イデアルであるであることが期待される．以上をアルゴリズムにまとめたものをアルゴリズム 1 に示す．

R/I の基底を $\mathcal{M} = \{b_1, \ldots, b_m\}$ とする．$R/I \ni f = a_1b_1 + \cdots a_mb_m$ $(a_i \in K)$ を $(b_1, \ldots, b_m) \cdot {}^t(a_1, \ldots, a_m)$ で表す．R/I の基底に関する線形写像による f の像をを行列 B を用いて $(b_1, \ldots, b_m)B\,{}^t(a_1, \ldots, a_m)$ で表すとき，B をこの線型写像の表現行列と呼ぶ．

アルゴリズム 1 (行列の同時固有分解による零次元イデアルの根基の素イデアル分解)
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)

1: $\mathcal{M} \leftarrow (K[\boldsymbol{x}]/I$ の基底$)$, $\quad m \leftarrow |\mathcal{M}|$ ▷ Gröbner 基底を使う，$i = 1, \ldots, n$
2: $M_i \leftarrow (\mathcal{M}$ に関する x_i 倍写像の表現行列$)$
3: $\mathcal{E} \leftarrow K^m$ の基底
4: $\pi_{M_1}(\lambda) \leftarrow g_1(\lambda) \cdots g_q(\lambda)$ ▷ M_1 の最小多項式
5: $P \leftarrow \emptyset$ ▷ 素イデアルのリスト
6: $\mathcal{B}_j \leftarrow (\ker g_j(M_1)$ の Jordan-Krylov 基底$) \quad (j = 1, \ldots, q)$
7: **if** $(|\mathcal{B}_1| = |\mathcal{B}_2| = \cdots = |\mathcal{B}_q| = 1)$ **then** ▷ M_1 は支配的
8: **for** $j = 1, \ldots, q$ **do**
9: $\boldsymbol{u} \in \mathcal{B}_j = \{\boldsymbol{u}\}$
10: $\pi_{M_i,\boldsymbol{u}}(\lambda)$ を計算 $\quad (i = 2, \ldots, n)$
11: **foreach** irreducible $(f_2, f_3, \ldots, f_n)$ s.t. $f_i \mid \pi_{M_i,\boldsymbol{u}}$ **do**
12: $\boldsymbol{v} \leftarrow (\ker g_j(M_1) \cap (\bigcap_{i=2}^{n} \ker f_i(M_i)))$ ▷ 命題 12 より
13: $\boldsymbol{p} \leftarrow \psi_{g_j}(M_1, x_1 E)\boldsymbol{v}$
14: $Q \leftarrow ((M_2 - x_2 E)\boldsymbol{p}, \ldots, (M_n - x_n E)\boldsymbol{p})$
15: $P \leftarrow P \cup \{\{$(関係式 $Q = O$ を簡約する)$\} \cup \{g_j(x_1)\}\}$
16: **end for**
17: **end for**
18: **else**
19: **repeat**
20: $r = r(x_1, \ldots, x_n)$ ▷ K 上のランダムな多項式
21: $M_r \leftarrow (\mathcal{M}$ に関する r 倍写像の表現行列$)$
22: $\pi_{M_r}(\lambda) \leftarrow g_1(\lambda) \cdots g_q(\lambda)$ ▷ M_r の最小多項式
23: $\mathcal{B}_j \leftarrow (\ker g_j(M_r)$ の Jordan-Krylov 基底$) \quad (j = 1, \ldots, q)$
24: **until** $(|\mathcal{B}_1| = |\mathcal{B}_2| = \cdots = |\mathcal{B}_q| = 1)$ ▷ M_r は支配的
25: $(M_r$ および $M_1, \ldots, M_n$ に対し，第 8 行から第 17 行までの処理を行う$)$
26: **end if**
27: **return** P

4 計算例

本節では，アルゴリズム 1 による計算例を示す．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 (x 倍写像が支配的な場合の例)
多項式環 $R = K[x, y]$ のイデアル I を以下の通り定義する．

$$I = \langle p_1^2, p_2 \rangle, \quad p_1 = x^2 + 4(y-2)^2 - 4, \quad p_2 = (2x + (y-2) - 2)(2x - (y+2) - 2)$$

$\sqrt{I} = \langle p_1, p_2 \rangle$ であり，あらかじめ得られている $\sqrt{I}$ の素イデアル分解は次式の通りである．

$$\sqrt{I} = \langle 17y^2 - 56y + 64, 2x + y - 4 \rangle \cap \langle 17y^2 - 72y + 64, 2x + y - 4 \rangle$$

単項式順序を $x > y$ とする辞書式順序 (Lex) とする。剰余環 R/I の基底 $\mathcal{M}$ は次の通りである．

$$\mathcal{M} = \{y^7, y^6, y^5, y^4, y^3, y^2, y, 1\}$$

倍写像の表現行列は 8 次正方行列である．剰余環 R/I における x 倍写像の表現行列を M_x，y 倍写像の表現行列を M_y とする．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，

$$\chi_{M_x}(\lambda) = f_1(\lambda)^2 f_2(\lambda)^2, \qquad f_1(\lambda) = 17x^2 - 96x + 140, \qquad f_3(\lambda) = 17y^2 - 72y + 64,$$
$$\chi_{M_y}(\lambda) = f_3(\lambda)^2 f_4(\lambda)^2, \qquad f_2(\lambda) = 17x^2 - 32x + 12 \qquad f_4(\lambda) = 17y^2 - 56y + 64$$

である．

$$\boldsymbol{u}_1 = {}^t(0, 4913, -57800, 280704, -725504, 1056768, -819200, 262144),$$
$$\boldsymbol{u}_2 = {}^t(0, 4913, -53176, 245888, -626176, 925696, -753664, 262144)$$

に対し，$\ker f_1(M_x) = L_{M_x}(\boldsymbol{u}_1)$, $\ker f_2(M_x) = L_{M_x}(\boldsymbol{u}_2)$ より M_x は支配的であることがわかる．

1. $\boldsymbol{u}_1 \in \ker f_1(M_x) \cap \ker f_4(M_y)$ かつ $\ker f_1(M_x) = L_{M_x}(\boldsymbol{u}_1) = L_{\{M_x, M_y\}}(\boldsymbol{u}_1)$ より，$\boldsymbol{v}_1(\lambda) = \psi_{f_1}(M_x, \lambda E)\boldsymbol{u}_1$ は M_x と M_y の同時固有ベクトルである．

$$\begin{aligned}\boldsymbol{v}_1(x) = \psi_{f_1}(M_x, xE)\boldsymbol{u}_1 = {}^t(&83521, 167042x - 1591812, -1965200x + 11939168,\\ &9543936x - 47140864, -24667136x + 107927552, 35930112x + 1144965632,\\ &-27852800x + 106037248, 8912896x - 32505856)\end{aligned}$$

とおく．$\boldsymbol{v}_1(x)$ が M_y の固有値 y に附随する固有ベクトルであることを用いて関係式を求め，M_x の固有値 x の定義多項式 $f_1(x)$ を加えて関係式を整理すると，固有値 x, y に関する関係式として

$$\{17y^2 - 56y + 64, -y + 2x - 4\} \tag{2}$$

を得る．

2. $\boldsymbol{u}_2 \in \ker f_2(M_x) \cap \ker f_3(M_y)$ かつ $\ker f_2(M_x) = L_{M_x}(\boldsymbol{u}_2) = L_{\{M_x, M_y\}}(\boldsymbol{u}_2)$ より，$\boldsymbol{v}_2(\lambda) = \psi_{f_2}(M_x, \lambda E)\boldsymbol{u}_2$ は M_x と M_y の同時固有ベクトルである．

$$\begin{aligned}\boldsymbol{v}_2(x) = \psi_{f_2}(M_x, xE)\boldsymbol{u}_2 = {}^t(&-83521, 167042x + 923644, -1807984x - 4392800,\\ &8360192x + 11628544, -21289984x - 18241536, 31473664x + 16515072,\\ &-25624576x - 7471104, 8912896x + 1048576)\end{aligned}$$

とおく．$\boldsymbol{v}_2(x)$ が M_y の固有値 y に附随する固有ベクトルであることを用いて関係式を求め，M_x の固有値 x の定義多項式 $f_2(x)$ を加えて関係式を整理すると，固有値 x, y に関する関係式として

$$\{-17y^2 + 72y - 64, y + 2x - 4\} \tag{3}$$

を得る．

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

$$\sqrt{I} = \langle 17y^2 - 56y + 64, 2x - y - 4\rangle \cap \langle -17y^2 + 72y - 64, 2x + y - 4\rangle$$

を得る．

例 2 (x 倍写像の表現行列が支配的でない場合の例)
多項式環 $R = K[x, y]$ のイデアル I を以下の通り定義する．

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

$\sqrt{I} = \langle p_1, p_2 \rangle$ であり，あらかじめ得られている $\sqrt{I}$ の素イデアル分解は次式の通りである．

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

単項式順序を $x > y$ とする辞書式順序 (Lex) とする。剰余環 R/I の基底 $\mathcal{M}$ は次の通りである．

$$\mathcal{M} = \{x^3y, x^3, x^2y, x^2, xy, x, y, 1\}$$

倍写像の表現行列は 8 次正方行列である．剰余環 R/I における x 倍写像の表現行列を M_x，y 倍写像の表現行列を M_y とする．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，

$$\chi_{M_x}(\lambda) = \chi_{M_y}(\lambda) = f_1(\lambda)^4, \quad f_1(\lambda) = (\lambda^2 - 2)$$

である．

$$\boldsymbol{u}_1 = {}^t(1, 0, 0, 0, -2, 0, 0, 0), \quad \boldsymbol{u}_2 = {}^t(0, 1, 0, 0, 0, -2, 0, 0)$$

に対し，$\ker f_1(M_x) = L_{M_x}(\boldsymbol{u}_1) \oplus L_{M_x}(\boldsymbol{u}_2)$ より M_x は支配的でないことがわかる．

そこで $r = 4x + y$ とおき，剰余環 R/I における r 倍写像の表現行列を M_r とする．M_r の特性多項式を $\chi_r(\lambda)$ とすると，

$$\chi_r(\lambda) = f_{r,1}(\lambda)^2 f_{r,2}(\lambda)^2, \quad f_{r,1}(\lambda) = \lambda^2 - 200, \quad f_{r,2}(\lambda) = \lambda^2 - 72$$

である．

$$\boldsymbol{u}'_1 = {}^t(0, 1, 1, 0, 0, -2, -2, 0), \quad \boldsymbol{u}'_2 = {}^t(0, 1, -1, 0, 0, -2, 2, 0)$$

に対し，$\ker f_{r,1}(M_r) = L_{M_r}(\boldsymbol{u}'_1)$, $\ker f_{r,2}(M_r) = L_{M_r}(\boldsymbol{u}'_2)$ より M_r は支配的であることがわかる．

1. $\boldsymbol{u}'_1 = {}^t(0, 1, 1, 0, 0, -2, -2, 0)$ に対し，$\pi_{M_x, \boldsymbol{u}'_1}(\lambda) = \pi_{M_y, \boldsymbol{u}'_1}(\lambda) = f_1(\lambda) = \lambda^2 - 2$, $\ker f_{r,1}(M_r) = L_{M_r}(\boldsymbol{u}'_1) = L_{\{M_x, M_y\}}(\boldsymbol{u}'_1)$ より，$\boldsymbol{u}'_1 \in \ker f_{r,1}(M_r) \cap \ker f_1(M_x) \cap \ker f_1(M_y)$ であり，$\boldsymbol{v}_{r,1}(\lambda) = \psi_{f_{r,1}}(M_r, \lambda E)\boldsymbol{u}'_1$ は M_r, M_x および M_y の同時固有ベクトルである．$\boldsymbol{v}_{r,1}(r)$ に $r = 4x + y$ を代入すると
$$\boldsymbol{v}_{r,1}(x, y) = {}^t(5, 4x + y, 4x + y, 10, -10, -8x - 2y, -8x - 2y, -20)$$
を得る．$\boldsymbol{v}_{r,1}(x, y)$ が M_x の固有値 x および M_y の固有値 y に附随する固有ベクトルであることを用いて関係式を求め，M_r の固有値 $r = 4x + y$ の定義多項式 $f_{r,1}(r)$ を加えて関係式を整理すると，固有値 x, y に関する関係式として
$$\{-y^2 + 2, -x + y\} \tag{4}$$
を得る．

2. $\boldsymbol{u}'_2 = {}^t(0, 1, -1, 0, 0, -2, 2, 0)$ に対し，$\pi_{M_x, \boldsymbol{u}'_2}(\lambda) = \pi_{M_y, \boldsymbol{u}'_2}(\lambda) = f_1(\lambda) = \lambda^2 - 2$, $\ker f_{r,2}(M_r) = L_{M_r}(\boldsymbol{u}'_2) = L_{\{M_x, M_y\}}(\boldsymbol{u}'_2)$ より，$\boldsymbol{u}'_2 \in \ker f_{r,2}(M_r) \cap \ker f_1(M_x) \cap \ker f_1(M_y)$ であり，$\boldsymbol{v}_{r,2}(\lambda) = \psi_{f_{r,2}}(M_r, \lambda E)\boldsymbol{u}'_2$ は M_r, M_x および M_y の同時固有ベクトルである．$\boldsymbol{v}_{r,2}(r)$ に $r = 4x + y$ を代入すると
$$\boldsymbol{v}_{r,2}(x, y) = {}^t(-3, 4x + y, -4x - y, 6, 6, -8x - 2y, 8x + 2y, -12)$$

を得る．$\boldsymbol{v}_{r,2}(x,y)$ が M_x の固有値 x および M_y の固有値 y に附随する固有ベクトルであることを用いて関係式を求め，M_r の固有値 $r=4x+y$ の定義多項式 $f_{r,2}(r)$ を加えて関係式を整理すると，固有値 x, y に関する関係式として

$$\{-y^2+2, x+y\} \tag{5}$$

を得る．

上の計算結果 (4), (5) より，イデアル $\sqrt{I}$ の素イデアル分解として

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

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, 小原功任, 照井章. 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. Computer Algebra — Foundations and Applications, 数理解析研究所講究録, 第 2320 巻, pp. 132–144. 京都大学数理解析研究所, 2025.

[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. 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.

[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 (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.

[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 (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.

[23] 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.

[24] 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.