対称イデアルの準素分解アルゴリズム

A Primary Decomposition Algorithm for Symmetric Ideals

東京理科大学　　石原侑樹 *1
Yuki Ishihara
Tokyo University of Science

Abstract

This article discusses primary decompositions of symmetric ideals. Let $K[X] = K[x_1, \ldots, x_n]$ be the n-variables polynomial ring over a filed K and $\mathfrak{S}_n$ the symmetric group of order n. Here, S_n acts on $K[X]$ by $\sigma(f(x_1, \ldots, x_n)) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$ for $f \in K[X]$ and $\sigma \in \mathfrak{S}_n$. An ideal I of $K[X]$ is called *a symmetric ideal* if $\sigma(I) = I$ for any $\sigma \in \mathfrak{S}$. For a primary decomposition $I = Q_1 \cap \cdots \cap Q_r$ of a symmetric ideal I, $I = \sigma(Q_1) \cap \cdots \cap \sigma(Q_r)$ is also a primary decomposition of I. We introduce an efficient algorithm to compute a primary decomposition of a symmetric ideal.

1　はじめに

対称性は数学の様々なところで登場する．例えば，2 変数多項式 $f(x, y) = xy + x + y + 1$ は x と y を入れ替えても変化せず，また $f(x, y) = 0$ を満たす点 (x, y) 全体の集合は直線 $x = y$ に関して対称である．同様のことが多項式イデアルに対しても成り立つ．対称式から生成されるイデアル $I = \langle x^2 + y^2 - 1, x + y + 1 \rangle$ は x と y の入れ替えに対して不変であり，その解，すなわち，$x^2 + y^2 - 1 = x + y + 1 = 0$ を満たす (x, y) 全体の集合も直線 $x = y$ に関して対称である．本稿ではより一般に，対称イデアル I の準素分解 $I = Q_1 \cap \cdots \cap Q_r$ に対し，準素成分同士の間にある種の対称性が存在することを紹介する．なお本稿の結果は [3] に基づく．

2　準備

本稿では，$\mathfrak{S}_n$ を n 次対称群とする．相異なる $i_1, \ldots, i_k \in \{1, \ldots, n\}$ に対し，$(i_1\, i_2\, i_3 \cdots i_k)$ を $i_1 \mapsto i_2$, $i_2 \mapsto i_3$, $\ldots$, $i_{k-1} \mapsto i_k$, $i_k \mapsto i_1$ となる置換とする．また，$\mathfrak{S}_n$ の置換 $\sigma_1, \ldots, \sigma_l$ から生成される部分群を $\langle\langle \sigma_1, \ldots, \sigma_l \rangle\rangle$ で表す．K を体，$K[X] = K[x_1, \ldots, x_n]$ を n 変数多項式環とすると，$\mathfrak{S}_n$ の $K[X]$ への作用，$\mathfrak{S}_n \times K[X] \ni (\sigma, f(x_1, \ldots, x_n)) \mapsto f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) \in K[X]$ が定義される．同様に，$\mathfrak{S}_n$ の部分群 G の $K[X]$ への作用も定義される．また，$K[X]$ のイデアル I に対し，$\sigma \in \mathfrak{S}_n$ による像 $\sigma(I) = \{\sigma(f) \mid f \in I\}$ も $K[X]$ のイデアルとなる．

以下，$K[X]$ の多項式およびイデアルについて考える．多項式 $f_1, \ldots, f_l$ から生成されるイデアルを $\langle f_1, \ldots, f_l \rangle$ で表す．また，イデアル I の根基 $\{f \in K[X] \mid$ ある自然数 m に対し，$f^m \in I\}$ を $\sqrt{I}$ と表記する．加えて，イデアル I, J に対し，$I : J = \{f \in K[X] \mid fJ \subset I\}$ をイデアル商，$I : J^\infty = \{f \in K[X] \mid$ ある自然数 m に対し，$fJ^m \subset I\}$ を飽和イデアルと呼ぶ．

*1 〒 162-8601 東京都新宿区神楽坂 1-3　E-mail: yishihara@rs.tus.ac.jp

さて，$K[X]$ の真のイデアル I に対し，準素イデアルの有限集合 $\{Q_1, \ldots, Q_k\}$ は $I = Q_1 \cap \cdots \cap Q_k$ を満たすとき，I の準素分解と呼ばれる．さらに，I の準素分解 $\{Q_1, \ldots, Q_k\}$ は

1. 任意の i に対し，$Q_i \not\supset \bigcap_{j \neq i} Q_j$
2. 任意の $i \neq j$ に対し，$\sqrt{Q_i} \neq \sqrt{Q_j}$

を満たすならば，I の最短準素分解と呼ばれる．I の最短準素分解 $\{Q_1, \ldots, Q_k\}$ に対し，Q_i は準素成分，その根基 $\sqrt{Q_i}$ は素因子と呼ばれる．本稿では I の素因子の集合 $\{\sqrt{Q_1}, \ldots, \sqrt{Q_k}\}$ を $\mathrm{Ass}(I)$ で表す．素因子の集合 $\mathrm{Ass}(I)$ の中で，包含関係に関し極小の素因子を孤立素因子，そうでない素因子を埋没素因子と呼ぶ．また，根基が孤立素因子，埋没素因子である準素成分をそれぞれ孤立準素成分，埋没準素成分と呼ぶ．

一般に I の最短準素分解は一意とは限らないが，素因子の集合 $\mathrm{Ass}(I)$ と孤立準素成分は分解に依らずに I から一意に定まることが知られている．例えば，任意の自然数 m に対し，$\{\langle x_1^2 \rangle, \langle x_1^3, x_1 x_2, x_2^m \rangle\}$ は $I = \langle x_1^3, x_1^2 x_2 \rangle$ の最短準素分解となるため，I は無限種類の最短準素分解を持つが，素因子の集合 $\mathrm{Ass}(I) = \{\langle x_1 \rangle, \langle x_1, x_2 \rangle\}$ や孤立準素成分 $\langle x_1^2 \rangle$ は一意に定まる．本稿では埋没準素成分に対してもある種の「一意性」を担保するために，「準素成分全体の集合」（準素類集合）を考える．

3　対称イデアルの基礎

この節では対称イデアルとその性質について説明する．対称イデアルは対称式をイデアルに拡張した概念である．

定義 1
イデアル I が $\mathfrak{S}_n$ の作用で不変であるとき，すなわち，任意の $\sigma \in \mathfrak{S}_n$ に対し，$\sigma(I) = I$ が成り立つとき，I を対称イデアルと呼ぶ．

例 1
$I = \langle x_1^3 - x_2^3, x_1 x_2 + 1 \rangle \subset \mathbb{Q}[x_1, x_2]$ は対称イデアルである．

対称式から生成されるイデアルは対称イデアルであるが，逆は成立するとは限らない．例えば，例 1 の $x_1^3 - x_2^3$ は対称式ではない．

注意 1
σ は可逆であるから，$\sigma(I) \subset I$ は $I \subset \sigma^{-1}(I)$ を意味する．したがって，定義 1 の “$\sigma(I) = I$” は “$\sigma(I) \subset I$” に置き換えることができる．

上記では作用する群として対称群 $\mathfrak{S}_n$ を考えていたが，下記のように $\mathfrak{S}_n$ の部分群に拡張することができる．

定義 2
G を $\mathfrak{S}_n$ の部分群とする．イデアル I が G の作用で不変であるとき，すなわち，任意の $\sigma \in G$ に対し，$\sigma(I) = I$ が成り立つとき，I を G-不変イデアルと呼ぶ．

例 2
群 $G = \{(1), (1\,2\,3), (1\,3\,2)\} \subset \mathfrak{S}_3$ とイデアル $I = \langle x_1^2 + x_2, x_2^2 + x_3, x_3^2 + x_1 \rangle \subset \mathbb{Q}[x_1, x_2, x_3]$ に対し，I は G-不変イデアルである．

与えられたイデアル I が対称イデアル（不変イデアル）か判定するために，イデアルの所属判定アルゴリズムを利用することができる．イデアルの所属判定はグレブナー基底を使った方法などが知られている．次の補題は具体的な対称イデアルの判定法を説明している．

補題 3
$I = \langle f_1, \ldots, f_k \rangle$ を $K[X]$ のイデアル，$G = \langle\langle \sigma_1, \ldots, \sigma_l \rangle\rangle$ を $\mathfrak{S}_n$ の部分群とする．このとき，次は同値である．

1. I は G-不変イデアル
2. 任意の $i \in \{1, \ldots, k\}$ と $\sigma \in G$ に対し，$\sigma(f_i) \in I$
3. 任意の $i \in \{1, \ldots, k\}$ と $j \in \{1, \ldots, l\}$ に対し，$\sigma_j(f_i) \in I$

証明 (1) ならば (2)，(2) ならば (3) は明らかであるため，(3) ならば (1) のみ示す．任意の $i \in \{1, \ldots, k\}$ と $j \in \{1, \ldots, l\}$ に対し，$\sigma_j(f_i) \in I$ が成り立つと仮定する．任意の $\sigma \in G$ と $f \in I$ をとる．すると，ある $\sigma_{a_1}, \ldots, \sigma_{a_m}$ $(1 \leq a_1, \ldots, a_m \leq l)$ が存在して，$\sigma = \sigma_{a_1} \cdots \sigma_{a_m}$ となる．また，ある $h_1, \ldots, h_k \in K[X]$ が存在して，$f = h_1 f_1 + \cdots + h_k f_k$ となる．ここで，$\tau \in G$ に対し

$$\tau(f) = \tau\left(\sum_{i=1}^{k} h_i f_i\right) = \sum_{i=1}^{k} \tau(h_i f_i) = \sum_{i=1}^{k} \tau(h_i)\tau(f_i)$$

であるから，任意の f_i に対し $\tau(f_i) \in I$ であらば $\tau(f) \in I$ となる．また，各 i に対し

$$\sigma(f_i) = (\sigma_{a_1} \cdots \sigma_{a_m})(f_i) = (\sigma_{a_1} \cdots \sigma_{a_{m-1}})(\sigma_{a_m}(f_i))$$

であるから，$\sigma(f_i) \in I$ が成り立つ．したがって，$\sigma(f) \in I$ である． ∎

例 3
n 次対称群 $\mathfrak{S}_n$ は $(1\,2)$ と $(1\,2\,3 \cdots n)$ から生成されるため，I が対称イデアルであることと，$(1\,2)(I) = I$ かつ $(1\,2\,3 \cdots n)(I) = I$ が成り立つことは同値である．

アルゴリズム 1 (不変イデアルの判定)
入力：$\{f_1, \ldots, f_k\}$: $K[X]$ の多項式，$\sigma_1, \ldots, \sigma_l$: $\mathfrak{S}_n$ の置換
出力：$\langle f_1, \ldots, f_k \rangle$ が $\langle\langle \sigma_1, \ldots, \sigma_l \rangle\rangle$-不変イデアルならば 1，それ以外は 0

1. 各 $i = 1, \ldots, k$ と各 $j = 1, \ldots, l$ に対し，$\sigma_j(f_i) \in I$ が成り立つか判定．
2. すべての i, j に対し $\sigma_j(f_i) \in I$ が成り立てば 1 を返す．そうでなければ 0 を返す．

4 対称イデアルの準素分解

この節では対称イデアルの準素分解が持つ対称性について紹介する．まず置換 $\sigma \in \mathfrak{S}_n$ は同型写像であるため，代数的な構造を変化させない．例えば，イデアル I が（準）素イデアルであれば $\sigma(I)$ も（準）素イデアルである．また，σ はイデアル和 $I + J$，イデアル積 $I \cdot J$，共通部分 $I \cap J$，根基 $\sqrt{I}$ などのイデアルの演算操作とも可換である．よって，I の準素分解 $I = Q_1 \cap \cdots \cap Q_r$ に対し，$\sigma(I) = \sigma(Q_1) \cap \cdots \cap \sigma(Q_k)$ は $\sigma(I)$ の準素分解となる．したがって，$I = \sigma(I)$ が成り立てば，$\sigma(Q_1) \cap \cdots \cap \sigma(Q_k)$ は I の準素分解でもある．すなわち，次の補題が成り立つ．

補題 4 ([3], Lemma 3.11)
I を G-不変イデアルとし，$\sigma \in G$ とする．I の準素分解 $\mathcal{Q} = \{Q_1, \ldots, Q_k\}$ に対し，$\sigma(\mathcal{Q}) = \{\sigma(Q_1), \ldots, \sigma(Q_k)\}$ も I の準素分解となる．特に，$\mathcal{Q}$ が最短準素分解であれば $\sigma(\mathcal{Q})$ も最短準素分解である．

次の命題のように，対称イデアル I の素因子の集合 $\mathrm{Ass}(I) = \{\sqrt{Q_1}, \ldots, \sqrt{Q_r}\}$ には G による作用が入る．

命題 5 ([3], Proposition 3.12)
I を G-不変イデアル，$\mathrm{Ass}(I) = \{P_1, \ldots, P_k\}$ とする．このとき，$G \times \mathrm{Ass}(I) \ni (\sigma, P) \mapsto \sigma(P) \in \mathrm{Ass}(I)$ により，G は $\mathrm{Ass}(I)$ に作用する．

証明 補題 4 より $\{Q_1, \ldots, Q_r\}$ が I の最短準素分解であれば，$\{\sigma(Q_1), \ldots, \sigma(Q_r)\}$ $(\sigma \in G)$ も I の最短準素分解となるため，素因子の集合の一意性から $\mathrm{Ass}(I) = \{\sqrt{Q_1}, \ldots, \sqrt{Q_r}\} = \{\sqrt{\sigma(Q_1)}, \ldots, \sqrt{\sigma(Q_r)}\} = \{\sigma(\sqrt{Q_1}), \ldots, \sigma(\sqrt{Q_r})\}$ が成立する．したがって，任意の $\sigma \in G$ と $P \in \mathrm{Ass}(I)$ に対し $\sigma(P) \in \mathrm{Ass}(I)$ が成立する．また，任意の $P \in \mathrm{Ass}(I)$ に対し，$(1)(P) = P$ であり，任意の $\sigma, \tau \in G$ に対し，$\sigma(\tau(P)) = \sigma\tau(P)$ が成り立つため，これは作用である． ∎

例 4
$I = \langle x_1^2x_2, x_2^2x_3, x_3^2x_1\rangle \subset \mathbb{Q}[x_1, x_2, x_3]$，$G = \langle\langle(1\ 2\ 3)\rangle\rangle$ とすると，I は G-不変イデアルであり，$I = \langle x_1^2, x_2\rangle \cap \langle x_2^2, x_3\rangle \cap \langle x_3^2, x_1\rangle \cap \langle x_1^2, x_2^2, x_3^2\rangle$ は I の最短準素分解である．よって，素因子の集合は $\mathrm{Ass}(I) = \{\langle x_1, x_2\rangle, \langle x_2, x_3\rangle, \langle x_3, x_1\rangle, \langle x_1, x_2, x_3\rangle\} = \{P_1, P_2, P_3, P_4\}$ である．ここで $\sigma = (1\ 2\ 3)$ に対し，$\sigma(P_1) = P_2$, $\sigma(P_2) = P_3$, $\sigma(P_3) = P_1$, $\sigma(P_4) = P_4$ が成り立つ．

上記のように素因子の集合には G の作用が自然に入るが，準素分解には同様の作用が入るとは限らない．例えば，$I = \langle(x_1+x_2)^2, (x_1+x_2)x_1x_2\rangle$ は対称イデアルであり，$\mathcal{Q} = \{\langle x_1+x_2\rangle, \langle x_1^2, x_2^2+2x_1x_2\rangle\}$ はそ最短準素分解となるが，$\sigma = (1\,2)$ に対して $\mathcal{Q} = \sigma(\mathcal{Q})$ は成立しない．実際，$\sigma(\mathcal{Q}) = \{\langle x_2+x_1\rangle, \langle x_2^2, x_1^2+2x_2x_1\rangle\}$ であり，$\langle x_2^2, x_1^2+2x_2x_1\rangle \in \sigma(\mathcal{Q})$ は $\mathcal{Q}$ に属さない．準素分解自体に作用が入らない理由としては埋没成分の非一意性がある．すなわち，$\sigma(\mathcal{Q})$ は I の最短準素分解ではあるが，その要素が元の準素分解 $\mathcal{Q}$ の成分になっているとは限らない．そこで準素分解への作用を与えるため，以下のように準素成分全体の集合を考える．

定義 6 ([3], Definition 3.15)
P を I の素因子とする．I の P-準素成分全体の集合を $\mathcal{Q}_P[I]$ で表し，I の P-準素類と呼ぶ．また，I の準素類全体の集合 $\{\mathcal{Q}_P[I] \mid P \in \mathrm{Ass}(I)\}$ を $\mathcal{Q}[I]$ で表し，I の準素類集合と呼ぶ．

例 5
$I = \langle x_1^3, x_1^2x_2\rangle \subset \mathbb{Q}[x_1, x_2]$ とすると，$I = \langle x_1^3, x_1^2x_2\rangle = \langle x_1^2\rangle \cap \langle x_1^3, x_2\rangle$ は最短準素分解となる．また，素因子の集合は $\mathrm{Ass}(I) = \{\langle x_1\rangle, \langle x_1, x_2\rangle\} = \{P_1, P_2\}$ である．ここで，I の P_1-準素類は $\mathcal{Q}_{P_1}[I] = \{\langle x_1^2\rangle\}$ であり，P_2-準素類 $\mathcal{Q}_{P_2}[I]$ は $\langle x_1^3, x_1x_2, x_2^m\rangle$ $(m \in \mathbb{N})$ などを含む．

孤立素因子の準素類は 1 つの元からなるが，埋没素因子の準素類は無限個の元からなるため元を列挙することは難しい．しかし，最短準素分解を求めるだけであれば，次のように各準素類の代表元を求めるだけでよい．

命題 7 ([2], Proposition 2.9)
$\mathcal{Q}[I] = \{\mathcal{Q}_{P_1}[I], \ldots, \mathcal{Q}_{P_k}[I]\}$ とし，各 i に対し，準素成分 $Q_i \in \mathcal{Q}_{P_i}[I]$ を任意に 1 つ選ぶ．このとき，$\{Q_1, \ldots, Q_k\}$ は I の最短準素分解である．

命題 7 より $P_1,\ldots,P_k$ に対応するように並べた準素類の直積 $\mathcal{Q}_{P_1}[I]\times\cdots\times\mathcal{Q}_{P_k}[I]$ は I の最短準素成分全体の集合と一致する．特に I が対称イデアルのときには，補題 4 と命題 5 より $\sigma(\mathcal{Q}_P[I])=\mathcal{Q}_{\sigma(P)}[I]$ が成り立つため，準素類集合は次のような対称性を持つ．

定理 8 ([3], Theorem 3.18)
I を G-不変イデアルとする．このとき， $G\times\mathcal{Q}[I]\ni(\sigma,\mathcal{Q}_P[I])\mapsto\sigma(\mathcal{Q}_P[I])\in\mathcal{Q}[I]$ により，G は $\mathcal{Q}[I]$ に作用する．

以上の定理を用いて，対称イデアルの準素分解のアルゴリズムの概要を紹介する．定理 8 より，G は $\mathcal{Q}[I]$ に作用するため，$\mathcal{Q}[I]$ の軌道分解 $C_1,\ldots,C_l$ が考えられる．すなわち，各 i に対し，代表元 $\mathcal{Q}_{P_i}[I]\in C_i$ をとると，$C_i=\{\sigma(\mathcal{Q}_{P_i}[I])\mid\sigma\in G\}$ が成り立つ．

例 6
$I=\langle x_1^2x_2,x_2^2x_3,x_3^2x_1\rangle$ を例 4 のイデアルとする．準素類集合は $\mathcal{Q}[I]=\{\mathcal{Q}_{P_1}[I],\mathcal{Q}_{P_2}[I],\mathcal{Q}_{P_3}[I],\mathcal{Q}_{P_4}[I]\}$ であり，軌道分解は $C_1=\{\mathcal{Q}_{P_1}[I],\mathcal{Q}_{P_2}[I],\mathcal{Q}_{P_3}[I]\}$，$C_2=\{\mathcal{Q}_{P_4}[I]\}$ である．

$\mathcal{Q}[I]$ の軌道分解 $C_1,\ldots,C_l$ に対し，l 個の代表元 $\mathcal{Q}_{P_i}[I]\in C_i$ が与えられれば，それらに G を作用させることで，残りのすべての準素類も計算することができる．特に，l 個の準素成分 $Q_i\in\mathcal{Q}_{P_i}[I]$ が計算できれば，G による作用でそこからすべての準素成分が計算できる．よって，次のアルゴリズムを得る．

アルゴリズム 2 (対称イデアルの準素分解)
入力：I: G-不変イデアル，$G\subset\mathfrak{S}_n$: 部分群
出力：I の最短準素分解

1. $\mathcal{Q}=\{\}$
2. $\mathcal{Q}$ が I の最短準素分解になるまで以下の $(a)-(b)$ を繰り返す
   (a) I の準素成分 Q を 1 つ計算する．その根基 $\sqrt{Q}$ が $\{\sqrt{Q'}\mid Q'\in\mathcal{Q}\}$ に所属している場合には Q を選びなおす．
   (b) $\mathcal{Q}$ に Q を追加する．
3. $\mathcal{Q}$ を返す．

例 7
$I=cyclic(3)=\langle x_1x_2x_3-1,x_1x_2+x_2x_3+x_3x_1,x_1+x_2+x_3\rangle\subset\mathbb{Q}[x_1,x_2,x_3]$ とする．($cyclic(n)$ の定義は *[1]* を参照)．このとき，I は対称イデアルである．I の辞書式順序 $x_1>x_2>x_3$ に関するグレブナー基底 G を計算すると，

$$G=\langle x_3^3-1,x_2^2+x_2x_3+x_3^2,x_1+x_2+x_3\rangle$$

であるため，

$$I\cap\mathbb{Q}[x_3]=\langle x_3^3-1\rangle=\langle x_3-1\rangle\cap\langle x_3^2+x_3+1\rangle.$$

が成り立つ．したがって，I の弱い分解

$$I=(I+\langle x_3-1\rangle)\cap(I+\langle x_3^2+x_3+1\rangle)$$

が得られ，

$$Q_1=(I+\langle x_3-1\rangle)=\langle x_2^2+x_2+1,x_1+x_2+1,x_3-1\rangle$$

は準素イデアルであるから，0 次元イデアル I の準素成分の 1 つである．Q_1 に $\mathfrak{S}_3$ を作用させることで，他の準素成分

$$Q_2 = (1\,2\,3)(Q_1) = \langle x_3^2 + x_3 + 1, x_2 + x_3 + 1, x_1 - 1\rangle$$
$$Q_3 = (1\,3\,2)(Q_1) = \langle x_1^2 + x_1 + 1, x_3 + x_1 + 1, x_2 - 1\rangle$$

を得る．よって，I の最短準素分解

$$I = Q_1 \cap Q_2 \cap Q_3$$

が計算できた．

例 7 ではグレブナー基底を用いて準素成分の 1 つを計算していたが，これ以外にも様々な方法が考えられる．5 節では下山-横山のアルゴリズムを用いて準素成分を計算する．

5　対称イデアルの準素分解の改良

この節では既存の準素分解アルゴリズムの対称イデアルへの特化を考える．ここで考えるものは下山-横山のアルゴリズム (SY-Algorithm) [6] である．まずは下山-横山のアルゴリズムの概略を述べてから，対称イデアルへの特化を考える．

5.1　下山-横山アルゴリズムの概略

下山-横山アルゴリズムは根基の準素分解[1)]を利用することで高速化を図る手法であり，擬準素分解と呼ばれる中間分解を経由して準素分解を計算する．一般的な傾向として，準素成分の重複度（nilpotency の次数）が大きいと計算が複雑になる傾向があるため，I の根基 $\sqrt{I}$ の準素分解を計算することは I の準素分解を計算することよりも容易い．また擬準素分解を計算するためには，セパレータと呼ばれる集合を利用する．ここで，イデアル I はその根基 $\sqrt{I}$ が素イデアルとなるとき，擬準素イデアルと呼ばれる ([6] の Definition 2.3 参照)．

定義 9 ([6], Definition 2.5, Definition 2.8)
I を擬準素ではないイデアルとし，$P_1, \ldots, P_k$ を I の孤立素因子とする．$S_1, \ldots, S_r$ を $K[X]$ の有限部分集合とする．各 S_i は

$$S_i \cap P_i = \emptyset, \quad \text{かつ} \quad S_i \cap P_j \neq \emptyset \quad (i \neq j).$$

を満たすとき，P_i に関する I のセパレータと呼ばれる．セパレータの集合 $\{S_1, \ldots, S_r\}$ は I のセパレータ系と呼ばれる．P_i に関するセパレータ S_i に対し，$s_i = \prod_{s \in S_i} s$ とするとき，$\overline{Q}_i = I : s_i^\infty$ を I の P_i-擬準素成分と呼ぶ．また，あるイデアル $I' \subset K[X]$ が存在して

$$I = \overline{Q}_1 \cap \cdots \cap \overline{Q}_r \cap I'$$

が成り立つ．この分解を I の擬準素分解と呼ぶ．ここで，I' は擬準素分解の残留成分（*remaining component*）[2)] と呼ばれる．

[1)] 根基の準素成分は素イデアルとなるため素分解とも呼ばれる

[2)] 本稿では和訳にあたり残留成分と呼称しているがこれは一般的な呼称とは限らない

I の擬準素成分 $\overline{Q}_i$ に対し，極大独立集合を用いることでその孤立準素成分 Q_i を計算することができる（[6] の Procedure 3.3 を参照）．この Q_i は I の孤立準素成分でもある．したがって，$\overline{Q}_i = Q_i \cap Q_i'$ を満たす Q_i' と残留成分 I' に対し，再帰的にアルゴリズムを適用すれば，I の準素分解を計算することができる．しかし，そのままでは最短準素分解ではなく，冗長な成分を含む可能性がある．元論文 [6] では途中に出てきたイデアルが必要な成分を含むか判定する方法を用いている．本稿では，[4] で提案されている “飽和分離イデアル” (saturated separating ideal) というイデアルを用いることで，冗長な成分を出すことなく最短準素分解を計算する．その意味では本稿で紹介するアルゴリズムは下山-横山アルゴリズムの変種である．

定義 10 ([4], Definition 1)
I と Q を $I \subset Q$ を満たすイデアルとする．イデアル J が $I = Q \cap (I + J)$ を満たすとき，(I, Q) の分離イデアルと呼ばれる．(I, Q) の分離イデアル J が $\sqrt{I : Q} = \sqrt{I + J}$ をみたすとき，J は (I, Q) の飽和分離イデアルと呼ばれる．

次の命題から，(I, Q) の飽和分離イデアル J に対し，$I + J$ の孤立素準素成分はすべて I の準素成分でもあることがいえる．

命題 11 ([4], Theorem 7)
イデアル I と Q，真のイデアル J に対し，$I = Q \cap J$ と $\sqrt{J} = \sqrt{I : Q}$ が成り立っているとする．また，$Q_1, \ldots, Q_r$ を J の孤立準素成分とし，$Q' = Q \cap \bigcap_{i=1}^{r} Q_i$ とする．もし真のイデアル J' が $I = Q' \cap J'$ と $\sqrt{J'} = \sqrt{I : Q'}$ を満たすならば，J' の任意の孤立素因子は J の埋没素因子である．

飽和分離イデアルの存在は次の命題より従う．

命題 12 ([4], Theorem 4)
J を (I, Q) の分離イデアルとする．もし $f \in \sqrt{I : Q}$ であるならば，ある正の整数 m が存在して，$I = Q \cap (I + J + \langle f^m \rangle)$ が成り立つ．

下記のアルゴリズムは飽和分離イデアルを用いた下山-横山のアルゴリズムの変種の概略である．

アルゴリズム 3 (下山-横山のアルゴリズム（飽和分離イデアル版 ）（SY）)
入力：I: $K[X]$ のイデアル
出力：I の最短準素分解

1. $\mathcal{Q} = \{\}$
2. $P_1, \ldots, P_r \leftarrow I$ の孤立素因子
3. $\{S_1, \ldots, S_r\} \leftarrow I$ のセパレータ系
4. 各 $i = 1, \ldots, r$ に対し，次を計算する．
   (a) $s_i \leftarrow \prod_{s \in S_i} s$
   (b) $\overline{Q}_i \leftarrow I : s_i^{\infty}$
   (c) $Q \leftarrow \overline{Q}_i$ の唯一の孤立素因子
   (d) $J_1 \leftarrow (\overline{Q_i}, Q)$ の飽和分離イデアル
   (e) $I + J_1 \neq K[X]$ ならば $\mathcal{Q} \leftarrow \mathcal{Q} \cup \mathrm{SY}(I + J_1)$
5. $J_2 \leftarrow (I, \bigcap_{i=1}^{r} \overline{Q}_i)$ の飽和分離イデアル
6. $I + J_2 \neq K[X]$ ならば $\mathcal{Q} \leftarrow \mathcal{Q} \cup \mathrm{SY}(I + J_2)$
7. $\mathcal{Q}$ を返す．

5.2 対称イデアルに特化した下山-横山アルゴリズム

ここでは下山-横山アルゴリズムを対称イデアルに特化したアルゴリズムを紹介する．特化に必要な概念は下記の 2 つである．

1. 対称セパレータ系の計算 (命題 13),
2. 対称飽和分離イデアルの計算 (定理 15).

まず，対称セパレータ系について，次の命題からその存在がいえる．

命題 13 ([3], Proposition 4.21)
I を G-不変イデアルで，擬準素イデアルでないものとする．$P_1, \ldots, P_r$ を I の孤立素因子とする．このとき，I のセパレータ系 $\mathcal{S} = \{S_1, \ldots, S_r\}$ で，$G \times \mathcal{S} \ni (\sigma, S) \mapsto \sigma(S) \in \mathcal{S}$ により G が $\mathcal{S}$ に作用するものが存在する．

命題 13 のセパレータ系を G-不変セパレータ系と呼ぶこととする．もし $\sigma(S_i) = S_j$ が成り立つとすると，$\sigma(\overline{Q}_i) = \sigma(I : s_i^\infty) = \sigma(I) : \sigma(s_i)^\infty = I : s_j^\infty = \overline{Q}_j$ となるため，G-不変セパレータ系から作られる擬準素成分の集合 $\{\overline{Q}_1, \ldots, \overline{Q}_r\}$ にも G の作用が入る．そして，次の定理のように，対称イデアルの擬準素成分は 2 つタイプに分けられる．

定理 14 ([3], Theorem 4.22)
$P_1, \ldots, P_r$ を G-不変イデアル I の孤立素因子とし，$\{S_1, \ldots, S_r\}$ を I の G-不変セパレータ系とする．このとき，各 S_i に対応する擬準素成分 $\overline{Q}_i$ は次のどちらか一方を満たす．

1. $\overline{Q}_i$ は G-不変イデアル
2. $\overline{Q}_i$ は G-不変な準素成分を 1 つも含まない

続いて，対称飽和分離イデアルの存在および計算方法について，次の定理 15 で説明する．

定理 15 ([3], Theorem 4.23)
I と Q を G-不変イデアルで，$I \subset Q$ を満たすものとする．また，J を G-不変イデアルであり，(I, Q) の分離イデアルとする．このとき，次の条件をすべて満たすようなある正の整数 l と多項式 $f_1, \ldots, f_l \in K[X]$ が存在する．

1. $I = Q \cap (I + J + \langle f_1, \ldots, f_l \rangle)$
2. $\langle f_1, \ldots, f_l \rangle$ は G-不変イデアル
3. $J + \langle f_1, \ldots, f_l \rangle$ は (I, Q) の飽和分離イデアル

G-不変であり飽和分離でもあるイデアルを G-不変飽和分離イデアルと呼ぶこととする．定理 14 と定理 15 から，対称イデアル I の擬準素分解 $I = \overline{Q}_1 \cap \cdots \cap \overline{Q}_r \cap I'$ を，次の 3 つのタイプの成分からなるように構成できる．

1. 対称な擬準素成分 $\overline{Q_i}$．この場合，対称準素分解のアルゴリズムを $\overline{Q_i}$ に対し再帰的に適用する．
2. 対称ではない擬準素成分 $\overline{Q_i}$．この場合，$\overline{Q_i}$ は対称な準素成分を一切含まないため，通常の準素分解のアルゴリズムを $\overline{Q_i}$ に対し適用する．
3. 対称残留成分 I'．この場合，対称準素分解のアルゴリズムを I' に対し再帰的に適用する．

以上の議論により，対称イデアル版の下山-横山アルゴリズムを下記に得る．ここで，SY はアルゴリズム 3，SymmetricSY はアルゴリズム 4 を意味している．

アルゴリズム 4 (対称イデアル版 下山-横山のアルゴリズム（SymmetricSY）)
入力：I: G-不変イデアル，$G \subset \mathfrak{S}_n$: 部分群
出力：I の最短準素分解

1. $\mathcal{Q} = \{\}$
2. $P_1, \ldots, P_r \leftarrow I$ の孤立素因子
3. $\{S_1, \ldots, S_r\} \leftarrow I$ の G-不変セパレータ系
4. 各 $i = 1, \ldots, r$ に対し，次を計算する．
   (a) $s_i \leftarrow \prod_{s \in S_i} s$
   (b) $\overline{Q}_i \leftarrow I : s_i^{\infty}$
5. $C_1, \ldots, C_l \leftarrow \{\overline{Q}_1, \ldots, \overline{Q}_r\}$ の G-軌道分解
6. 各 $i = 1, \ldots, l$ に対し，次を計算する．
   (a) もし $|C_i| = 1$ であれば，
      i. $Q \leftarrow \overline{Q_i}$ の孤立準素成分．ただし，$C_i = \{\overline{Q_i}\}$.
      ii. $\mathcal{Q} \leftarrow \mathcal{Q} \cup \{Q\}$
      iii. $J_1 \leftarrow (\overline{Q_i}, Q)$ の G-不変飽和分離イデアル
      iv. もし $I + J_1 \neq K[X]$ であれば $\mathcal{Q} \leftarrow \mathcal{Q} \cup \mathrm{SymmetricSY}(I + J_1)$
   (b) もし $|C_i| > 1$ であれば，
      i. $\overline{Q}_i \in C_i$ を 1 つ選び，$\mathcal{Q}_i \leftarrow \mathrm{SY}(\overline{Q}_i)$
      ii. $\mathcal{Q} \leftarrow \mathcal{Q} \cup \bigcup_{\sigma \in G} \sigma(\mathcal{Q}_i)$
7. $J_2 \leftarrow (I, \bigcap_{i=1}^{r} \overline{Q}_i)$ の G-不変飽和分離イデアル
8. もし $I + J_2 \neq K[X]$ であれば $\mathcal{Q} \leftarrow \mathcal{Q} \cup \mathrm{SymmetricSY}(I + J_2)$
9. $\mathcal{Q}$ を返す．

6 終わりに

本稿では対称性を持つイデアルの準素分解のアルゴリズムについて解説した．対称性を利用することで効率的に準素成分を求めることができ，これまで計算できていなかったイデアルの準素分解が求められることが期待される．

謝　辞

本研究は JSPS 科研費 JP22K13901 の助成を受けたものです．

参 考 文 献

[1] Backelin, J., Fröberg, R. How we prove that there are exactly 924 cyclic 7-roots. In: Proceedings of ISSAC 91, ACM Press, 103-111 (1991)

[2] Ishihara, Y.: Efficient localization at a prime ideal without producing unnecessary primary components, Mathematics in Computer Science, Vol.16, 14 (2022)

[3] Ishihara, Y.: Primary decompositions of symmetric ideals. to appear in Commentarii mathematici Universitatis Sancti Pauli

[4] Kawazoe, T., Noro, M.: Algorithms for computing a primary ideal decomposition without producing intermediate redundant components. J. Symb. Comput. 46(10), 1158-1172 (2011)

[5] Risa/Asir developing team. Risa/Asir. a computer algebra system. http://www.math.kobe-u.ac.jp/Asir.

[6] Shimoyama, T., Yokoyama, K.: Localization and primary decomposition of polynomial ideals. J. Symb. Comput. 22(3), 247-277 (1996)