非可換環上の signature-based algorithm とその実装

Signature-based algorithm on non-commutative rings and its implementation

金沢大学・大学院自然科学研究科　　向 博生 [*1]
Hiroki Mukai
Graduate School of Science and Technology
Kanazawa University

金沢大学・理工研究域　　小原 功任 [*2]
Katsuyoshi Ohara
Faculty of Mathematics and Physics
Kanazawa University

立教大学・大学院理学研究科　　横山 和弘 [*3]
Kazuhiro Yokoyama
Departement of Mathematics
Rikkyo University

Abstract

Signature-based algorithm is an algorithm for computing Gröbner bases over polynomial ring. In this paper, we give the non-commutative theory of minimal signature and the non-commutative signature-based algorithm on both Weyl algebra and Poincaré-Birkhoff-Witt algebra. We also implement both commutative and non-commutative signature-based algorithm on Risa/Asir a computer algebra system.

1　はじめに

Signature-based algorithm (SBA) は，多項式環上のグレブナー基底を求めるアルゴリズムのひとつであり，2002 年に J.-C. Faugère が導入した F5 アルゴリズムに由来する．近年，Tristan Vaccon と横山和弘は SBA を詳しく解析し，minimal signature の概念を導入し SBA の正当性と停止性を明確に示した．本稿では Vaccon-横山の理論を基礎として，SBA を非可換環 Weyl 代数上のグレブナー基底計算に拡張したことについて述べる．[9] に沿って説明をするが多項式環と Weyl 代数の性質の違いに基づいて主張を一部修正し，必要な証明を行った．われわれの方法を用いて，SBA を Poincaré-Birkhoff-Witt 代数上のグレブナー基底計算にも拡張できる．

[*1] 〒 920-1192 金沢市角間町　E-mail: hmukai8101@stu.kanazawa-u.ac.jp
[*2] 〒 920-1192 金沢市角間町　E-mail: ohara@se.kanazawa-u.ac.jp
[*3] 〒 171-8501 豊島区西池袋　E-mail: kazuhiro@rikkyo.ac.jp

2 Signatureの定義と性質

体 K を係数とし，不定元 $x_1,\dots,x_n,\partial_1,\dots,\partial_n$ に関する Weyl 代数を D で表す．よく知られているように，多項式環 $K[x,\xi]=K[x_1,\dots,x_r,\xi_1,\dots,\xi_r]$ を用いて，$P\in D$ の全表象 $P(x,\xi)\in K[x,\xi]$ を考えることが有用である．多項式環 $K[x,\xi]$ における **全次数項順序** $\prec$ を固定しよう．記号を乱用して，$\mathrm{LM}(P):=\mathrm{LM}(P(x,\xi))$ としておく．いま $P_1,P_2,\dots,P_r\in D$ の生成する D の左イデアル $I=DP_1+\cdots+DP_r$ を考える．簡単のため $\mathrm{LM}(P_1)\preceq\cdots\preceq\mathrm{LM}(P_r)$ としておく．$K[x,\xi]$ における単項式全体の集合を $M=\{x^\alpha\xi^\beta\mid\alpha,\beta\in\mathbb{N}_0^n\}$ とする．ここで $M\ni m(x,\xi)=x^\alpha\xi^\beta$に対して $m=x^\alpha\partial^\beta\in D$ と定める．すなわち，$m(x,\xi)$ を全表象に持つ D の元が m であり，これらの関係には注意してほしい．さらに，これからの説明において $K[x,\xi]$ における可換の積を使う箇所と D における非可換の積を使う箇所が混在しているため間違えないように注意してほしい．

r に対し $D^r=\{(Q_1,\dots,Q_r)\mid Q_1,\dots,Q_r\in D\}$ とするとこれは階数 r の左 D 加群である．$D^r\ni\boldsymbol{Q}=(Q_1,\dots,Q_r)$ の (加群の) 全表象を $\boldsymbol{Q}(x,\xi):=(Q_1(x,\xi),\dots,Q_r(x,\xi))$ と定める．続いて，$\{\boldsymbol{e}_1,\dots,\boldsymbol{e}_r\}$ を D^r の標準基底とする．加群単項式の集合 $\boldsymbol{M}$ を，$m(x,\xi)\boldsymbol{e}_i$ 全体の集合とする．$(m(x,\xi)\in M)$

定義 1 (加群単項式順序)
$\boldsymbol{M}$ 上の順序 $\prec_m$ が以下を満たすときに**加群単項式順序**という．ここで $m_1(x,\xi),m_2(x,\xi),m_3(x,\xi)\in M, i,j\in\{1,\dots,r\}$ とする．

(1) $m_1(x,\xi)\boldsymbol{e}_i\prec_m m_2(x,\xi)\boldsymbol{e}_j\ \Rightarrow\ m_1(x,\xi)m_3(x,\xi)\boldsymbol{e}_i\prec_m m_2(x,\xi)m_3(x,\xi)\boldsymbol{e}_j$
(2) $m_1(x,\xi)\prec m_2(x,\xi)\ \Rightarrow\ m_1(x,\xi)\boldsymbol{e}_i\prec_m m_2(x,\xi)\boldsymbol{e}_i$

この $\prec_m$ により，$\boldsymbol{P}\in D^r$ に対し $\mathrm{LM}(\boldsymbol{P}),\mathrm{LC}(\boldsymbol{P}),\mathrm{LT}(\boldsymbol{P})$ が定義される．

例 1
$\prec_m$ の例として以下がある．

(1) POT: $m_1(x,\xi)\boldsymbol{e}_i\prec_m m_2(x,\xi)\boldsymbol{e}_j\ \Leftrightarrow\ i<j$ or $(i=j$ and $m_1(x,\xi)\prec m_2(x,\xi))$
(2) TOP: $m_1(x,\xi)\boldsymbol{e}_i\prec_m m_2(x,\xi)\boldsymbol{e}_j\ \Leftrightarrow\ m_1(x,\xi)\prec m_2(x,\xi)$ or $(m_1(x,\xi)=m_2(x,\xi)$ and $i<j)$
(3) Schreyer: $m_1(x,\xi)\boldsymbol{e}_i\prec_m m_2(x,\xi)\boldsymbol{e}_j\ \Leftrightarrow\ m_1(x,\xi)\mathrm{LM}(P_i)\prec m_2(x,\xi)\mathrm{LM}(P_j)$ or
$(m_1(x,\xi)\mathrm{LM}(P_i)=m_2(x,\xi)\mathrm{LM}(P_j)$ and $i<j)$

命題 2 (部分加群のグレブナー基底と正規形)
$\boldsymbol{S}$ を D^r の部分左 D 加群とし，$\prec_m$ を一つ固定する．

(1) $\boldsymbol{S}$ の有限部分集合 $\boldsymbol{G}$ で以下を満たすものが存在する．この時に $\boldsymbol{G}$ を (加群の) **グレブナー基底**という．
$\boldsymbol{P}\in\boldsymbol{S}\setminus\{\boldsymbol{0}\}$ に対して，ある $\boldsymbol{g}\in\boldsymbol{G}$ が存在して $\mathrm{LM}(\boldsymbol{g})$ は $\mathrm{LM}(\boldsymbol{P})$ を割る．
(すなわち、$\mathrm{LM}(\boldsymbol{g})=m_1(x,\xi)\boldsymbol{e}_i$, $\mathrm{LM}(\boldsymbol{P})=m_2(x,\xi)\boldsymbol{e}_j$ とすると, $i=j$ かつ $m_1(x,\xi)\mid m_2(x,\xi)$ となる．記号として $\mathrm{LM}(\boldsymbol{g})\mid\mathrm{LM}(\boldsymbol{P})$ で表す.)
(2) $\mathbf{S}$ のグレブナー基底を $\boldsymbol{G}$ とする．$\boldsymbol{P}\in D^r$ に対し以下を満たす $\boldsymbol{P}'$ が唯一定まる．この $\boldsymbol{P}'$ を $\boldsymbol{P}$ の $\boldsymbol{G}$ に関する正規形といい, $\mathrm{NF}_{\boldsymbol{G}}(\boldsymbol{P})$ で表す.

$$\boldsymbol{P}-\boldsymbol{P}'\in\boldsymbol{S}\text{ で, }\boldsymbol{P}'\text{は }\boldsymbol{G}\text{ に関し既約である.}$$

(すなわち, $\boldsymbol{P}'(x,\xi)$ に現れる単項式はいかなる $\mathrm{LM}(\boldsymbol{G})$ の元でも割れない.)

以下，加群単項式順序 $\prec_m$ を一つ固定する．

定義 3 (syzygy 加群)
D^r の部分左 D 加群 $\mathbf{Syz}$ を以下で定める．

$$\mathbf{Syz} = \{\boldsymbol{Q} = (Q_1, \ldots, Q_r) \in D^r \mid Q_1P_1 + \cdots + Q_rP_r = 0\}$$

続いて，$\boldsymbol{M}$ を次の 2 つの集合に分ける．

$$\mathrm{LM}(\mathbf{Syz}) = \{\mathrm{LM}(\boldsymbol{Q}) \mid \boldsymbol{Q} \in \mathbf{Syz}\}$$
$$\mathrm{NS}(\mathbf{Syz}) = \boldsymbol{M} \setminus \mathrm{LM}(\mathbf{Syz})$$

$\tilde{\boldsymbol{G}}$を $\mathbf{Syz}$ のグレブナー基底とすると，上の定義より

$$\mathrm{NS}(\mathbf{Syz}) = \{m(x,\xi)\boldsymbol{e}_i \in \boldsymbol{M} \mid \mathrm{LM}(\boldsymbol{g}) \nmid m(x,\xi)\boldsymbol{e}_i \text{ for } \forall \boldsymbol{g} \in \tilde{\boldsymbol{G}}\}$$

である．

$P \in I \setminus \{0\}$ は，$P = Q_1P_1 + \cdots + Q_rP_r$ と表すことができる．このとき，$(Q_1, \ldots, Q_r)$ を P の**表現ベクトル**と呼ぶ．表現ベクトルは P に対し一意には定まらない．一方で syzygy 加群を用いることでこの表現ベクトルを $\prec_m$ に関して一番小さいものを定めることができて，こちらは一意に定まる．その最小の表現ベクトルの主単項式が minimal signature である．

補題 4 (最小表現ベクトルの存在と一意性)
$P \in I \setminus \{0\}$ の表現ベクトル $\tilde{\boldsymbol{Q}} = (\tilde{Q}_1, \ldots, \tilde{Q}_r)$ として $\tilde{\boldsymbol{Q}}(x,\xi)$ が $\mathrm{NS}(\mathbf{Syz})$ の項のみからなるものがとれ，P に対し一意に定まる．P の任意の表現ベクトルを $\boldsymbol{Q}$ とすると $\tilde{\boldsymbol{Q}} = \mathrm{NF}_{\tilde{\boldsymbol{G}}}(\boldsymbol{Q})$ かつ $\mathrm{LM}(\tilde{\boldsymbol{Q}}) \preceq_m \mathrm{LM}(\boldsymbol{Q})$ である．

証明 Pの表現ベクトルを一つとり，$\boldsymbol{Q} = (Q_1, \ldots, Q_r)$ とし，これの $\tilde{\boldsymbol{G}}$ に関する正規形を $\tilde{\boldsymbol{Q}} = (\tilde{Q}_1, \ldots, \tilde{Q}_r)$ とする．このとき $\boldsymbol{Q} - \tilde{\boldsymbol{Q}} \in \mathbf{Syz}$ であるので，

$$(Q_1 - \tilde{Q}_1, \ldots, Q_r - \tilde{Q}_r) \cdot (P_1, \ldots, P_r) = \sum_{i=1}^{r} (Q_i - \tilde{Q}_i)P_i = 0$$

となる．これは

$$P = \sum_{i=1}^{r} Q_iP_i = \sum_{i=1}^{r} \tilde{Q}_iP_i$$

を意味する．また，正規形の定義より，$\tilde{\boldsymbol{Q}}(x,\xi)$ は $\mathrm{NS}(\mathbf{Syz})$ の項のみからなる．続いて一意性を示す．補題の条件を満たすような表現ベクトル $\boldsymbol{R} = (R_1, \ldots, R_r)$ をとる．このとき $\tilde{\mathbf{G}}$ 既約である．よって $\boldsymbol{R} - \tilde{\boldsymbol{Q}}$ も $\tilde{\mathbf{G}}$ 既約であり，$P = R_1P_1 + \cdots + R_rP_r = \tilde{Q}_1P_1 + \cdots + \tilde{Q}_rP_r$ より，

$$(\boldsymbol{R} - \tilde{\boldsymbol{Q}}) \cdot (P_1, \ldots, P_r) = 0$$

でもある．したがって，$(\boldsymbol{R} - \tilde{\boldsymbol{Q}})$ は $\tilde{\boldsymbol{G}}$ 既約かつ $\mathbf{Syz}$ の元であるので

$$(\boldsymbol{R} - \tilde{\boldsymbol{Q}}) = 0$$

が示される．最後に，$\tilde{\boldsymbol{G}}$ による正規形は順序を下げるので，$\mathrm{LM}(\tilde{\boldsymbol{Q}}) \preceq_m \mathrm{LM}(\boldsymbol{Q})$ である． ∎

定義 5 (signature)
$P \in I \setminus \{0\}$ に対し，補題 4 の $\tilde{\boldsymbol{Q}}$ を P の**最小表現ベクトル**と呼ぶ．さらに，$\mathrm{LM}(\tilde{\mathbf{Q}})$ を P の **minimal signature** と呼び，$S(P)$ と表す．(以下，単に signature と表記する．$S(0) = \mathbf{0}$ とする．) また，P の最小表現ベクトル $\tilde{\boldsymbol{Q}} = (\tilde{Q}_1, \ldots, \tilde{Q}_r)$ による表現

$$P = \tilde{Q}_1 P_1 + \cdots + \tilde{Q}_r P_r$$

を，P の**標準形**と呼ぶ．I の元の signature になりうる $\boldsymbol{M}$ の元の集合を $\sum$ で表す．すなわち，

$$\sum = \{\boldsymbol{s} \in \boldsymbol{M} \mid \text{ある } P \in I \text{ が存在して } S(P) = \boldsymbol{s} \text{ となる．}\}$$

補題 6 (非混在性)
(1) $\{S(P) \mid P \in I \setminus \{0\}\} = \mathrm{NS}(\mathbf{Syz})$ である．
(2) $P \in I \setminus \{0\}$, $m(x,\xi) \in M$ に対し，$m(x,\xi)S(P) \in \mathrm{NS}(\mathbf{Syz}) \Rightarrow S(mP) = m(x,\xi)S(P)$ である．
(3) $P \in I \setminus \{0\}$, $m(x,\xi) \in M$ に対し，$m(x,\xi)S(P) \notin \mathrm{NS}(\mathbf{Syz}) \Rightarrow S(mP) \prec_m m(x,\xi)S(P)$ である．
((2), (3) において $m(x,\xi)$ と $S(P)$ の間は，$K[x,\xi]$ における可換の積の作用であるが m と P の間は D における非可換の積であることに注意)

証明 (1) signature の定義より，$S(P) \in \mathrm{NS}(\mathbf{Syz})$ である．よって $\{S(P) \mid P \in I \setminus \{0\}\} \subset \mathrm{NS}(\mathbf{Syz})$ である．逆に $m(x,\xi)\boldsymbol{e}_i \in \mathrm{NS}(\mathbf{Syz})$ をとり，$P = mP_i$ とおけば，$S(P) = m(x,\xi)\boldsymbol{e}_i$ である．$(m(x,\xi) \in M)$ よって，$\mathrm{NS}(\mathbf{Syz}) \subset \{S(P) \mid P \in I \setminus \{0\}\}$ である．
(2) P の標準形 $P = \tilde{Q}_1 P_1 + \cdots \tilde{Q}_r P_r$ と最小表現ベクトル $\tilde{\boldsymbol{Q}} = (\tilde{Q}_1, \ldots, \tilde{Q}_r)$ を考える．$S(P) = \mathrm{LM}(\tilde{\boldsymbol{Q}})$ である．このとき $mP = m\tilde{Q}_1 P_1 + \ldots + m\tilde{Q}_r P_r$ と表される．ここで，$m\tilde{\mathbf{Q}} = (m\tilde{Q}_1, \ldots, m\tilde{Q}_r)$ は mP の表現ベクトルである．mP の signature を求めるため $m\tilde{\boldsymbol{Q}}$ の正規形を考える．

$$\mathrm{NF}_{\tilde{\boldsymbol{G}}}(m\tilde{\boldsymbol{Q}}) = \mathrm{NF}_{\tilde{\boldsymbol{G}}}(\mathrm{LM}_{\prec_m}(m\tilde{\boldsymbol{Q}})) + \mathrm{NF}_{\tilde{\boldsymbol{G}}}(m\tilde{\boldsymbol{Q}} - \mathrm{LM}_{\prec_m}(m\tilde{\boldsymbol{Q}}))$$

と分けることができる．仮定より，

$$\mathrm{NF}_{\tilde{\boldsymbol{G}}}(\mathrm{LM}_{\prec_m}(m\tilde{\boldsymbol{Q}})) = \mathrm{NF}_{\tilde{\boldsymbol{G}}}(\mathrm{LM}_{\prec}(m)\mathrm{LM}_{\prec_m}(\tilde{\boldsymbol{Q}})) = \mathrm{NF}_{\tilde{\boldsymbol{G}}}(m(x,\xi)S(P)) = m(x,\xi)S(P)$$

である．一方で，

$$\mathrm{LM}(\mathrm{NF}_{\tilde{\boldsymbol{G}}}(m\tilde{\boldsymbol{Q}}) - \mathrm{LM}_{\prec_m}(m\tilde{\boldsymbol{Q}})) \preceq_m \mathrm{LM}(m\tilde{\boldsymbol{Q}} - \mathrm{LM}_{\prec_m}(m\tilde{\boldsymbol{Q}})) \prec_m \mathrm{LM}(m\tilde{\boldsymbol{Q}}) = m(x,\xi)S(P)$$

が成り立つ．したがって，

$$S(mP) = \mathrm{LM}(\mathrm{NF}_{\tilde{\boldsymbol{G}}}(m\tilde{\boldsymbol{Q}})) = m(x,\xi)S(P)$$

が示される．
(3) (2) の証明と同様に進めるが，$m(x,\xi)S(P) \notin \mathrm{NS}(\mathbf{Syz})$ の場合は，

$$\mathrm{NF}_{\tilde{\boldsymbol{G}}}(\mathrm{LM}(m\tilde{\boldsymbol{Q}})) \prec_m m(x,\xi)S(P)$$
$$\mathrm{LM}(\mathrm{NF}_{\tilde{\boldsymbol{G}}}(m\tilde{\boldsymbol{Q}} - \mathrm{LM}(m\tilde{\boldsymbol{Q}})) \prec_m m(x,\xi)S(P)$$

であるため，

$$\mathrm{LM}(NF_{\tilde{\boldsymbol{G}}}(m\tilde{\boldsymbol{Q}})) \prec_m m(x,\xi)S(P)$$

となる．このことから，

$$S(mP) = \mathrm{LM}(NF_{\tilde{\boldsymbol{G}}}(m\tilde{\boldsymbol{Q}})) \prec_m m(x,\xi)S(P)$$

が示される． ∎

補題 7
$\mathrm{NS}(\mathbf{Syz}) = \sum$ である．

証明 signature の定義より，$\sum \subset \mathrm{NS}(\mathbf{Syz})$ は明らか．一方，$\forall \boldsymbol{s} \in \mathrm{NS}(\mathbf{Syz})$ に対し $\boldsymbol{s} = m(x,\xi)\boldsymbol{e}_i$ $(m(x,\xi) \in M)$ とかけ，$P = mP_i$ とおくと補題 6(2) より，

$$S(P) = S(mP_i) = m(x,\xi)S(P_i) = m(x,\xi)\boldsymbol{e}_i = \boldsymbol{s}$$

である．よって，$\mathrm{NS}(\mathbf{Syz}) \subset \sum$ である． ∎

補題 8 (signature の打ち消し，保存)
$P, P' \in I \setminus \{0\}$ とする．

(1) $\mathrm{LM}(P) \succ \mathrm{LM}(P')$ かつ $S(P) = S(P') = \boldsymbol{s}$ のとき，ある $a, b \in K^\times$ が存在して，

$$S(aP + bP') \prec_m S(P) \text{ かつ } \mathrm{LM}(aP + bP') = \mathrm{LM}(P)$$

とできる．

(2) $S(P) \succ_m S(P')$ のとき，任意の $a \in K^\times, b \in K$ に対して，

$$S(aP + bP') = S(P)$$

が成り立つ．

証明 以下 P, P' の表現ベクトルを $\boldsymbol{Q}_1, \boldsymbol{Q}_2$ とする．
(1) $\mathrm{LM}(\mathbf{Q}_1) = S(P) = S(P') = \mathrm{LM}(\mathbf{Q}_2)$ であるので，LT を同じにするように定数倍を行う．すなわち，ある $a, b \in K^\times$ として，$\mathrm{LT}(a\boldsymbol{Q}_1) = \mathrm{LT}(-b\boldsymbol{Q}_2)$ とできる．このとき，$aP + bP'$ の表現ベクトルは $a\mathbf{Q}_1 + b\mathbf{Q}_2$ であり，$a\boldsymbol{Q}_1 + b\boldsymbol{Q}_2$ において $\mathrm{LM}(\boldsymbol{Q}_1)$ の係数は 0 となる，これは

$$S(aP + bP') = \mathrm{LT}(a\boldsymbol{Q}_1 + b\boldsymbol{Q}_2) \prec_m \mathrm{LT}(\boldsymbol{Q}_1) = S(P)$$

を意味する．一方，$\mathrm{LM}(P) \succ \mathrm{LM}(P')$ より $aP + bP'$ では $\mathrm{LM}(P)$ の項が残る．よって $\mathrm{LM}(aP + bP') = \mathrm{LM}(P)$ である．
(2) $S(P) \succ_m S(P')$ より $\mathrm{LM}(\boldsymbol{Q}_1) \succ_m \mathrm{LM}(\boldsymbol{Q}_2)$ である．よって任意の $a \in K^\times, b \in K$ に対して $a\boldsymbol{Q}_1 + b\boldsymbol{Q}_2$ の LM は $\mathrm{LM}(a\boldsymbol{Q}_1)$ である．これは，$S(aP + bP') = S(P)$ を意味する． ∎

補題 9
$m(x,\xi) \in M$, $P \in I \setminus \{0\}$ に対して，$S(mP) = m(x,\xi)S(P)$ であるとする．このとき，$u(x,\xi) \mid m(x,\xi)$ である $u(x,\xi) \in M$ に対して，$S(uP) = u(x,\xi)S(P)$ である．

証明 $S(uP) \neq u(x,\xi)S(P)$ を仮定する．補題 6 より $S(uP) \prec_m u(x,\xi)S(P)$ である．
$w(x,\xi) = \dfrac{m(x,\xi)}{u(x,\xi)}$ とする．(ここで $w(x,\xi)u(x,\xi) = m(x,\xi)$ であるが $wu = m$ となるとは限らないことに注意，前者は $K[x,\xi]$ における可換の積で後者は D における非可換の積である．) このとき，

$$S(mP) = m(x,\xi)S(P) = w(x,\xi)u(x,\xi)S(P) \succ_m w(x,\xi)S(uP) \succeq_m S(wuP) = S(mP)$$

となり矛盾が導かれる．最後の等号 $S(wuP) = S(mP)$ は補題 6(2) の証明の流れと同様に示される．実際，P の最小表現ベクトルを $\tilde{\boldsymbol{Q}} = (\tilde{Q}_1, \ldots, \tilde{Q}_r)$ とすると，$S(P) = \mathrm{LM}(\tilde{\boldsymbol{Q}})$ である．このとき $wuP = wu\tilde{Q}_1P_1 + \ldots + wu\tilde{Q}_rP_r$ と表される．ここで，$wu\tilde{\boldsymbol{Q}} = (wu\tilde{Q}_1, \ldots, wu\tilde{Q}_r)$ は wuP の表現ベクトルである．

$$\mathrm{NF}_{\tilde{\boldsymbol{G}}}(wu\tilde{\boldsymbol{Q}}) = \mathrm{NF}_{\tilde{\boldsymbol{G}}}(\mathrm{LM}_{\prec_m}(wu\tilde{\boldsymbol{Q}})) + \mathrm{NF}_{\tilde{\boldsymbol{G}}}(wu\tilde{\boldsymbol{Q}} - \mathrm{LM}_{\prec_m}(wu\tilde{\boldsymbol{Q}}))$$

と分けることができる．仮定より，$\mathrm{NS}(\mathbf{Syz}) \ni S(mP) = m(x,\xi)S(P)$ ゆえ，

$$\mathrm{NF}_{\tilde{\boldsymbol{G}}}(\mathrm{LM}_{\prec_m}(wu\tilde{\boldsymbol{Q}})) = \mathrm{NF}_{\tilde{\boldsymbol{G}}}(\mathrm{LM}_{\prec}(w)\mathrm{LM}_{\prec}(u)\mathrm{LM}_{\prec_m}(\tilde{\boldsymbol{Q}})) = \mathrm{NF}_{\tilde{\boldsymbol{G}}}(w(x,\xi)u(x,\xi)S(P)) = \mathrm{NF}_{\tilde{\boldsymbol{G}}}(m(x,\xi)S(P)) = m(x,\xi)S(P) = S(mP)$$

である．したがって，

$$S(wuP) = \mathrm{LM}(\mathrm{NF}_{\tilde{\boldsymbol{G}}}(wu\tilde{\boldsymbol{Q}})) = S(mP)$$

が示される． ∎

3 $\mathfrak{S}$-簡約と $\mathfrak{S}$-グレブナー基底

定義 10 ($\mathfrak{S}$-簡約)
$P, R \in I$, $Q \in I \setminus \{0\}$, $\boldsymbol{s} \in \boldsymbol{M}$ とする．P が $\boldsymbol{s}$ と Q により R に **$\mathfrak{S}$-top-簡約**するとは，ある $m(x,\xi) \in M$, $a \in K^\times$ が存在して以下を満たすときにいい，$P \to^{Q}_{\mathfrak{S},\boldsymbol{s}} R$ で表す．(以下，単に $\mathfrak{S}$-簡約と表記する．)

(1) $R = 0$ もしくは $\mathrm{LM}(R) \prec \mathrm{LM}(P)$ かつ $R = P - amQ$
(2) $S(mQ) \prec_m \boldsymbol{s}$

$\boldsymbol{s}$ を明示しない場合，$\boldsymbol{s} = S(P)$ とする．このとき，$S(R) = S(P)$ である．また，Q(もしくは mQ) を **$\mathfrak{S}$-簡約元**という．(m と Q の間は D における非可換の積である．) I の部分集合 H に対して，H の元を $\mathfrak{S}$-簡約元として $\mathfrak{S}$-簡約することを，$P \to^{H}_{\mathfrak{S},\boldsymbol{s}} R$ で表す．

注意 1 (regular 簡約と singular 簡約)
定義 10 における簡約を regular $\mathfrak{S}$-top-簡約と呼ぶ．これと対比して定義 10 において $S(mQ) \preceq_m S(P)$ とした場合を singular $\mathfrak{S}$-top-簡約と呼ぶ．グレブナー基底の理論において，簡約操作により左イデアルの元が 0 になるが，これには singular 簡約が対応する．

定義 11 ($\mathfrak{S}$-既約と $\mathfrak{S}$-可約)
$\boldsymbol{s} \in \boldsymbol{M}$, $P \in I$ に対して P が $\boldsymbol{s}$ に関して **$\mathfrak{S}$-既約**とは，P を $\mathfrak{S}$-簡約する Q が存在しないときにいう．$\boldsymbol{s}$ を明示しない場合，$\boldsymbol{s} = S(P)$ とする．$\mathfrak{S}$-既約でないときに **$\mathfrak{S}$-可約**という．

補題 12 ($\mathfrak{S}$-簡約の有限性)
$P \in I \setminus \{0\}$ に対して，$\mathfrak{S}$-簡約を可能な限り行う．この操作は有限回で停止し，停止したときに得られる元は $\mathfrak{S}$-既約である．

証明 $P_1 = P$ とし，$\mathfrak{S}$-簡約の操作で得られる列 $(P_1, P_2, \ldots)$ を考える．このとき，$\mathrm{LM}(P_1) \succ \mathrm{LM}(P_2) \succ \cdots$ の降下列が得られる．$\prec$ は項順序のため，この降下列は有限回で停止する． ∎

補題 13 (既約元の LM 一意性・最小性)
$P, P' \in I \setminus \{0\}$ に対して P, P' は $\mathfrak{S}$-既約であり，$S(P) = S(P')$ とする．このとき $\mathrm{LM}(P) = \mathrm{LM}(P')$ である．さらに，$\boldsymbol{s} \in \mathrm{NS}(\mathbf{Syz})$ に対して，signature が $\boldsymbol{s}$ となる $P \in I$ で $\mathrm{LM}(P)$ が最小になるものは $\mathfrak{S}$-既約であることも分かる．

証明 $P, P' \in I$ として，P, P' は $\mathfrak{S}$-既約であり，$S(P) = S(P')$ とする．$\mathrm{LM}(P) \neq \mathrm{LM}(P')$ として矛盾を導く．必要であれば P と P' を取り替えることで $\mathrm{LM}(P) \succ \mathrm{LM}(P')$ とする．補題 8(1) よりある $a, b \in K^\times$ が存在して

$$S(aP + bP') \prec_m S(P),\ \mathrm{LM}(aP + bP') = \mathrm{LM}(P)$$

とできる．このとき $aP+bP'$ は P の $\mathfrak{S}$-簡約元となるので，P が $\mathfrak{S}$-既約であることに反する．
次に，$\boldsymbol{s} \in \mathrm{NS}(\mathbf{Syz})$ をとる．signature が $\boldsymbol{s}$ になる I の元の LM 全体 $H(\boldsymbol{s})$ を考える．すなわち，

$$H(\boldsymbol{s}) = \{\mathrm{LM}(P) \mid P \in I, S(P) = \boldsymbol{s}\}$$

である．単項式の集合は整列集合であるので，$H(\mathbf{s})$ には最小元が存在する．この最小限を与える $P \in I$ は $\mathfrak{S}$-既約であることを示す．もしそうでないとすると，$\mathfrak{S}$-簡約元が存在する．すなわち，ある $P' \in I$ で $S(P') \prec_m S(P)$ かつ $\mathrm{LM}(P) = \mathrm{LM}(P')$ となるものが存在する．このとき，P' で $\mathfrak{S}$-簡約されたものを $\hat{P}$ とすると，

$$S(\hat{P}) = S(P) = \boldsymbol{s} \text{ かつ } \mathrm{LM}(\hat{P}) \prec \mathrm{LM}(P)$$

となり，P の取り方に反す．∎

補題 14 (既約元の signature 一意性・最小性)
$P, P' \in I \setminus \{0\}$ に対して P, P' は $\mathfrak{S}$-既約であり，$\mathrm{LM}(P) = \mathrm{LM}(P')$ とする．このとき $S(P) = S(P')$ である．これより，$m(x,\xi) \in \mathrm{LM}(I)$ に対して，LM が $m(x,\xi)$ となる $P \in I$ で $S(P)$ が最小になるものは $\mathfrak{S}$-既約であることも分かる．

証明 $P, P' \in I \setminus \{0\}$ に対して P, P'は $\mathfrak{S}$-既約であり，$\mathrm{LM}(P) = \mathrm{LM}(P')$ とする．$S(P) \neq S(P')$ として矛盾を導く．必要であれば P と P' を取り替えることで $S(P) \succ_m S(P')$ とする．このとき，P は P の $\mathfrak{S}$-簡約元となるので P の取り方に反す．
次に，$m(x,\xi) = \mathrm{LM}(P)$ として以下の集合を考える．

$$M(m(x,\xi)) = \{S(P) \mid P \in I, \mathrm{LM}(P) = m(x,\xi)\}$$

$M(m(x,\xi))$ には最小元が存在する．この最小限を与える $P \in I$ は $\mathfrak{S}$-既約であることを示す．もしそうでないとすると，$\mathfrak{S}$-簡約元が存在する．すなわち，ある $P' \in I$ で $S(P') \prec_m S(P)$ かつ $\mathrm{LM}(P) = \mathrm{LM}(P')$ となるものが存在する．これは P の取り方に反す．∎

系 15 (簡約元の既約性)
定義 10 の記号を用いる．$P \in I \setminus \{0\}$ が $\mathfrak{S}$-既約でないとする．このとき，P の $\mathfrak{S}$-簡約元 mQ として，$\mathfrak{S}$-既約なものがとれる．

証明 $\mathrm{LM}(P)$ を LM とする I の元で signature が最小のものは $\mathfrak{S}$-既約である．∎

定義 16 ($\mathfrak{S}$-グレブナー基底)
I の部分集合 G が以下を満たすとき，I の **$\mathfrak{S}$-グレブナー基底**という．
各 $\mathfrak{S}$-既約である $P \in I \setminus \{0\}$ に対して，ある $m(x,\xi) \in M, g \in G$ が存在して次を満たす．

$$\mathrm{LM}(P) = m(x,\xi)\mathrm{LM}(g) \text{ かつ } S(P) = m(x,\xi)S(g)$$

(上の $m(x,\xi)$ はどちらも同じ単項式を指す．結果として $\mathrm{LM}(mg) = m(x,\xi)\mathrm{LM}(g)$, $S(mg) = m(x,\xi)S(g)$ である．)

注意 2
定義 16 の mg は，補題 13 より $\mathfrak{S}$-既約である．さらに，g も $\mathfrak{S}$-既約である．このことから定義 16 の G を $\mathfrak{S}$-既約なものだけからなるとしてよい．これを $\mathfrak{S}$-グレブナー基底の定義にはじめから加えておくこともできる．

補題 13 より，$\mathfrak{S}$-既約な元の LM は signature で一意に定まるので，定義 16 の別の言い方として以下がある．

定義 17 ($\mathfrak{S}$-グレブナー基底その 2)
I の部分集合 G が以下を満たすとき，I の $\mathfrak{S}$-グレブナー基底という．
各 $\boldsymbol{s} \in \mathrm{NS}(\mathbf{Syz})$ に対して，ある $m(x,\xi) \in M$, $g \in G$ が存在して次を満たす．

$$m(x,\xi)S(g) = \boldsymbol{s} \text{ かつ } mg \text{ は } \mathfrak{S}\text{-既約}$$

補題 14 より，各 $m(x,\xi) \in \mathrm{LM}(I)$ に対し LM が $m(x,\xi)$ となる $\mathfrak{S}$-既約な元が存在し，その signature は $m(x,\xi)$ で一意に定まるので，定義 16 の別の言い方として以下がある．

定義 18 ($\mathfrak{S}$-グレブナー基底その 3)
I の部分集合 G が以下を満たすとき，I の $\mathfrak{S}$-グレブナー基底という．
各 $u(x,\xi) \in \mathrm{LM}(I)$ に対して，ある $m(x,\xi) \in M$, $g \in G$ が存在して次を満たす．

$$\mathrm{LM}(mg) = u(x,\xi) \text{ かつ } S(mg) = m(x,\xi)S(g) \text{ かつ } mg \text{ は } \mathfrak{S}\text{-既約}$$

以下の命題は定義 18 より直ちに示される．

命題 19 ($\mathfrak{S}$-グレブナー基底はグレブナー基底である)
I の $\mathfrak{S}$-グレブナー基底は I のグレブナー基底を含む．

補題 20 (singular 簡約による 0 簡約)
G を I の $\mathfrak{S}$-グレブナー基底とする．このとき，$P \in I \setminus \{0\}$ は G による singular 簡約で 0 になる．

証明 $P \in I$ に対して P が $\mathfrak{S}$-既約でなければ，regular 簡約が適用され $\mathfrak{S}$-既約な元に簡約される．このとき，$\mathfrak{S}$-グレブナー基底の定義より，ある $\mathfrak{S}$-既約な mg $(m(x,\xi) \in M, g \in G)$ が存在して $S(mg) = S(p)$ となる．(LM 一意性より $\mathrm{LM}(P) = \mathrm{LM}(mg)$ である．) よって，ある $a \in K^{\times}$ を取れば，$\mathrm{LT}(amg)$ を $\mathrm{LT}(P)$ と一致させることができ，$P' = P - amg$ は

$$S(P') \prec_m S(P) \text{ かつ } \mathrm{LM}(P') \prec_m \mathrm{LM}(P)$$

となる．これは singular 簡約が行われることを意味する．以下，上記の操作を繰り返すことで，

$$P \to P' \to P'' \to \cdots$$

となる signature に関する減少列ができる．これは有限回で止まるので最後は 0 になる． ∎

命題 21 ($\mathfrak{S}$-グレブナー基底の存在)
各 $\boldsymbol{s} \in \mathrm{NS}(\mathbf{Syz})$ に対して signature が $\boldsymbol{s}$ であるような $\mathfrak{S}$-既約な元を一つ取り，それを $P_{\boldsymbol{s}}$ とする．このとき $\{P_{\boldsymbol{s}} \mid \boldsymbol{s} \in \mathrm{NS}(\mathbf{Syz})\}$ は $\mathfrak{S}$-グレブナー基底である．

$\mathfrak{S}$-グレブナー基底の定義では無限集合を許すので以上の命題 21 より $\mathfrak{S}$-グレブナー基底の存在が示された．以下ではさらに有限性を示す．

命題 22 ($\mathfrak{S}$-グレブナー基底の有限性)
G を $\mathfrak{S}$-グレブナー基底とする．このとき，G の有限部分集合で $\mathfrak{S}$-グレブナー基底となるものが存在する．

証明 以下の写像を考える．

$$V : G \ni g \longmapsto (\mathrm{LM}(g), S(g)) \in M \oplus \mathbf{M}$$

ディクソンの補題により，G の有限集合 H で $V(G)$ で生成されるモノイデアルを生成するものが存在する．このとき，H が $\mathfrak{S}$-グレブナー基底になることを示す．$P \in I\backslash\{0\}$ を $\mathfrak{S}$-既約とする．$\mathfrak{S}$-グレブナー基底の定義より，ある $m(x,\xi) \in M$, $g \in G$ が存在して

$$m(x,\xi)S(g) = S(mg) = S(P) \text{ かつ } m(x,\xi)\mathrm{LM}(g) = \mathrm{LM}(mg) = \mathrm{LM}(P)$$

が成り立つ．一方，H の取り方より，ある $u(x,\xi), v(x,\xi) \in M$, $h \in H$ が存在して

$$\mathrm{LM}(g) = u(x,\xi)\mathrm{LM}(h) \text{ かつ } S(g) = v(x,\xi)S(h)$$

となる．補題 6 より $v(x,\xi)S(h) = S(vh)$ でもある．

1. $u(x,\xi) = v(x,\xi)$ の場合，$m'(x,\xi) = m(x,\xi)u(x,\xi) = m(x,\xi)v(x,\xi)$ とする．このとき，$S(P) \in \mathrm{NS}(\mathbf{Syz})$ なので補題 6(2) から，

$$\mathrm{LM}(P) = m(x,\xi)\mathrm{LM}(g) = m(x,\xi)u(x,\xi)\mathrm{LM}(h) = m'(x,\xi)\mathrm{LM}(h) = \mathrm{LM}(m'h)$$
$$S(P) = m(x,\xi)S(g) = m(x,\xi)v(x,\xi)S(h) = m'(x,\xi)S(h) = S(m'h)$$

   となる．

2. $u(x,\xi) \prec v(x,\xi)$ の場合，このとき，$u(x,\xi)S(h) \prec_m v(x,\xi)S(h)$ である．1 の場合と同様に $m'(x,\xi)$ を定める．
   1 の場合と同様に $\mathrm{LM}(P) = \mathrm{LM}(m'h)$ であり，

$$S(P) = m(x,\xi)S(g) = m(x,\xi)v(x,\xi)S(h) \succ_m m(x,\xi)u(x,\xi)S(h) = m'(x,\xi)S(h) \succeq_m S(m'h)$$

   となる．これは $m'h$ が P の $\mathfrak{S}$-簡約元となるので P の取り方に反す．

3. $u(x,\xi) \succ v(x,\xi)$ の場合，$m'(x,\xi) = m(x,\xi)v(x,\xi)$ とする．
   1 の場合と同様に $S(P) = S(m'h)$ であり，

$$\mathrm{LM}(P) = m(x,\xi)\mathrm{LM}(g) = m(x,\xi)u(x,\xi)\mathrm{LM}(h) \succ m(x,\xi)v(x,\xi)\mathrm{LM}(h) = m'(x,\xi)\mathrm{LM}(h) = \mathrm{LM}(m'h)$$

   であるが，P は $\mathfrak{S}$-既約であるので，その LM が最小値になることに反す．

以上により $u(x,\xi) = v(x,\xi)$ しか起こりえず，H が $\mathfrak{S}$-グレブナー基底である． ∎

定義 23 (原始性)
$P \in I$ は $\mathfrak{S}$-既約であるとする．$m(x,\xi) \in M\backslash\{1\}$, $P' \in I$ で P' は $\mathfrak{S}$-既約であり，さらに $\mathrm{LM}(mP') = \mathrm{LM}(P)$ かつ $m(x,\xi)S(P') = S(mP') = S(P)$ となるものが存在しないとき，P を**原始的**であると呼ぶ．

補題 24 (極小 $\mathfrak{S}$-グレブナー基底)
G を $\mathfrak{S}$-グレブナー基底とする．G の原始的なもののみからなる集合を $\hat{G}$ とする．このとき，$\hat{G}$ は $\mathfrak{S}$-グレブナー基底である．この $\hat{G}$ を**極小 $\mathfrak{S}$-グレブナー基底**と呼ぶ．

証明 G を $\mathfrak{S}$-既約なものからなるとしてよい．G の元 g で原始的でないものがあった場合に，ある $\hat{g} \in G$ で原始的かつ $\mathrm{LM}(m\hat{g}) = \mathrm{LM}(g)$, $m(x,\xi)S(\hat{g}) = S(m\hat{g}) = S(g)$ となるものが存在することを示せばよい．以下では G の元 g が原始的でないとする．このとき，定義 23 より，ある $m(x,\xi) \in M \setminus \{1\}$, $P \in I$ が存在して

$$\mathrm{LM}(mP) = \mathrm{LM}(g) \text{ かつ } m(x,\xi)S(P) = S(mP) = S(g)$$

である．P は $\mathfrak{S}$-既約である．そこで，$\mathfrak{S}$-グレブナー基底の定義より，G の元 g_1 で，ある $m_1(x,\xi) \in M$ が存在して，

$$\mathrm{LM}(m_1 g_1) = \mathrm{LM}(P) \text{ かつ } m_1(x,\xi)S(g_1) = S(m_1 g_1) = S(P)$$

となる．よって，

$$\mathrm{LM}(mm_1 g_1) = m(x,\xi)\mathrm{LM}(m_1 g_1) = m(x,\xi)\mathrm{LM}(P) = \mathrm{LM}(g)$$
$$m(x,\xi)m_1(x,\xi)S(g_1) = m(x,\xi)S(m_1 g_1) = m(x,\xi)S(P) = S(g)$$

である．$S(g_1) \prec_m S(g)$ に注意する．g_1 が原始的でない場合には，この操作を有限回繰り返すことで原始的な $\hat{g} \in G$ が導出され，これが求めるものである． ∎

4　$\mathfrak{S}$-グレブナー基底の構成

Weyl 代数においても，多項式環同様の議論で $\mathfrak{S}$-グレブナー基底を計算するアルゴリズムを構成することができる．以下では簡単のためグレブナー基底の元はすべて monic とする．(LC を 1 とする．)

定義 25 ($\boldsymbol{s}$ 以下 (未満) $\mathfrak{S}$-グレブナー基底)
$\boldsymbol{s} \in \boldsymbol{M}$ とする．I の部分集合 G が以下の条件 1 を満たすとき，I の **$\boldsymbol{s}$ 以下 (未満)$\mathfrak{S}$-グレブナー基底**という．必要に応じて，条件 1 を条件 2 に置き換えることができる．

(条件 1) signature が $\boldsymbol{s}$ 以下 (未満) で，$\mathfrak{S}$-既約であるような $P \in I \setminus \{0\}$ に対して，ある $m(x,\xi) \in M$, $g \in G$ が存在して次を満たす．

$$\mathrm{LM}(P) = m(x,\xi)\mathrm{LM}(g),\quad S(P) = m(x,\xi)S(g)$$

(条件 2) $\boldsymbol{s'} \in \mathrm{NS}(\mathbf{Syz})$ で $\boldsymbol{s'}$ は $\boldsymbol{s}$ 以下 (未満) なものに対してある $m(x,\xi) \in M$, $g \in G$ が存在して次を満たす．

$$S(mg) = m(x,\xi)S(g) = \boldsymbol{s'} \text{ かつ } mg \text{ は } \mathfrak{S}\text{-既約}$$

I の $\boldsymbol{s}$ 以下 (未満)$\mathfrak{S}$-グレブナー基底 G を，$G_{\preceq \boldsymbol{s}}$ $(G_{\prec \boldsymbol{s}})$ と表記する．また，I の $\boldsymbol{s}$ 未満の $\mathfrak{S}$-グレブナー基底が $\boldsymbol{s}$ 以下の $\mathfrak{S}$-グレブナー基底にはならないとき，$\boldsymbol{s}$ を**必要な signature** といい，そうでないときに $\boldsymbol{s}$ を**不要な signature** という．

定義 26 (正則対，S 多項式)
$P_1, P_2 \in I \setminus \{0\}$ とし，それらは monic とする．対 (P_1, P_2) の S 多項式を $\mathrm{Spoly}(P_1, P_2) = m_1 P_1 - m_2 P_2$ とする．すなわち m_1, m_2 の全表象はそれぞれ

$$\frac{\mathrm{LCM}(\mathrm{LM}(P_1), \mathrm{LM}(P_2))}{\mathrm{LM}(P_1)},\quad \frac{\mathrm{LCM}(\mathrm{LM}(P_1), \mathrm{LM}(P_2))}{\mathrm{LM}(P_2)}$$

であるとする．(S 多項式の m_1 と P_1 の間と m_2 と P_2 の間の積は D における非可換の積である．) ここで，$S(m_1 P_1) \neq S(m_2 P_2)$ のとき，(P_1, P_2) を**正則対**といい，$\mathrm{Spoly}(P_1, P_2)$ を**正則な S 多項式**という．$m_1 P_1$ と $m_2 P_2$ のうち，signature の大きいほうを**主成分**と呼ぶ．このとき，$\mathrm{Spoly}(P_1, P_2)$ の signature は主成分の signature に等しい．これを正則対 (P_1, P_2) の signature と呼ぶ．

例えば正則対 (P_1, P_2) の主成分が m_1P_1 である場合，S 多項式の signature $S(m_1P_1)$ は補題 6(2) より $m_1(x,\xi)S(P_1)$ で表される．続いて，以下の命題は定義 25 の条件 2 より直ちに示される．

命題 27
$\boldsymbol{s} \in \mathrm{NS}(\mathbf{Syz})$ とし，$G_{\prec \boldsymbol{s}}$ を $\boldsymbol{s}$ 未満 $\mathfrak{S}$-グレブナー基底とする．

(1) ある $m(x,\xi) \in M$, $g \in G_{\prec \mathbf{s}}$ が存在して次を満たすとする．

$$\boldsymbol{s} = m(x,\xi)S(g) \text{ かつ } mg \text{ は } \mathfrak{S}\text{-既約}$$

このとき，$m(x,\xi)S(g) = S(mg)$ で，$G_{\prec \boldsymbol{s}}$ は $\boldsymbol{s}$ 以下 $\mathfrak{S}$-グレブナー基底である．すなわち，$\boldsymbol{s}$ は不要な signature である．

(2) 上記の $m(x,\xi)$, g が存在しないとき，$\boldsymbol{s}$ を signature に持つ $\mathfrak{S}$-既約な元 $g_{\boldsymbol{s}} \in I$ を一つとる．このとき $G_{\prec \boldsymbol{s}}$ に $g_{\boldsymbol{s}}$ を加えた集合は $\boldsymbol{s}$ 以下 $\mathfrak{S}$-グレブナー基底である．すなわち，$\boldsymbol{s}$ は必要な signature である．

命題 27(2) のときに $g_{\boldsymbol{s}}$ を構成する必要があるが，このためには signature が $\boldsymbol{s}$ である S 多項式を構成し (regular) $\mathfrak{S}$-簡約を施すことで得られる．

命題 28
$\boldsymbol{s} = m(x,\xi)\boldsymbol{e}_i \in \mathrm{NS}(\mathbf{Syz})$ とし，$G_{\prec \boldsymbol{s}}$ を $\boldsymbol{s}$ 未満 $\mathfrak{S}$-グレブナー基底とする．

$$S = \{(m(x,\xi), g) \mid m(x,\xi) \in M, g \in G_{\prec \boldsymbol{s}}, m(x,\xi)S(g) = \boldsymbol{s}\}$$

とする．このとき $S \neq \emptyset$ である．さらに S の元 $(m_1(x,\xi), g_1)$ で $\mathrm{LM}(m_1g_1)$ が最小になるものをとる．ここで，以下が成り立つ．

(1) $\mathrm{LM}(m_1g_1) = \mathrm{LM}(m_2g_2)$ となる $m_2(x,\xi) \in M, g_2 \in G_{\prec \boldsymbol{s}}$ で，$m_2(x,\xi)S(g_2) \prec_m \boldsymbol{s}$ となるものが存在しないとき，m_1g_1 は $\mathfrak{S}$-既約である．(すなわち，この場合には m_1g_1 から作られる signature が $\boldsymbol{s}$ の正則な S 多項式は存在しない．) 命題 27(1) より $G_{\prec \boldsymbol{s}}$ は $\boldsymbol{s}$ 以下 $\mathfrak{S}$-グレブナー基底であり，$\boldsymbol{s}$ は不要な signature である．

(2) 上記の $m_2(x,\xi) \in M$, $g_2 \in G_{\prec \boldsymbol{s}}$ で $m_2(x,\xi)S(g_2) \prec_m \boldsymbol{s}$ となるものが存在するとき，$m_1g_1 - m_2g_2$ は g_1, g_2 の正則な S 多項式 $\mathrm{Spoly}(g_1, g_2)$ で，その signature は $\boldsymbol{s}$ である．この場合は $g_{\boldsymbol{s}}$ として $\mathrm{Spoly}(g_1, g_2)$ を可能な限り $\mathfrak{S}$-簡約したものとすれば，$g_{\boldsymbol{s}}$ は signature が $\boldsymbol{s}$ の $\mathfrak{S}$-既約な元であり，命題 27(2) より $G_{\prec \boldsymbol{s}} \cup \{g_{\boldsymbol{s}}\}$ は $\boldsymbol{s}$ 以下 $\mathfrak{S}$-グレブナー基底であり，$\boldsymbol{s}$ は必要な signature である．

証明 ($S \neq \emptyset$ であること) まず，

$$\boldsymbol{s} = m(x,\xi)\boldsymbol{e}_i \in \mathrm{NS}(\mathbf{Syz}) \;\Rightarrow\; \boldsymbol{e}_i \in \mathrm{NS}(\mathbf{Syz})$$

である．(対偶をとれば明らか．) $S(P_i) = \boldsymbol{e}_i$ であり signature が $\boldsymbol{e}_i$の $\mathfrak{S}$-既約な元が存在するので，$\mathfrak{S}$-グレブナー基底の定義より $G_{\prec \boldsymbol{s}}$ の元でその signature が $\boldsymbol{e}_i$ となるものが存在する．その元を $\hat{g}_i$ とすると，

$$S(m\hat{g}_i) = m(x,\xi)S(\hat{g}_i) = m(x,\xi)\boldsymbol{e}_i = \boldsymbol{s}$$

である．したがって $(m(x,\xi), \hat{g}_i) \in S$ である．

(1) m_1g_1が $\mathfrak{S}$-既約ではないと仮定する．
このとき，m_1g_1の $\mathfrak{S}$-簡約元として $\mathfrak{S}$-既約なもの Q がとれる．実際，補題 14 より，

$$M(\mathrm{LM}(m_1g_1)) = \{Q \in I \mid \mathrm{LM}(Q) = \mathrm{LM}(m_1g_1)\}$$

とおけば，$M(\mathrm{LM}(m_1g_1)) \neq \emptyset$ であり，この中で signature が最小のものを Q とすれば Q は $\mathfrak{S}$-既約である．Q は m_1g_1 の $\mathfrak{S}$-簡約元であり $S(Q) \prec_m \boldsymbol{s}$ であるので，$G_{\prec \boldsymbol{s}}$ の定義から，ある $m_2(x,\xi) \in M$, $g_2 \in G_{\prec \boldsymbol{s}}$ で $m_2(x,\xi)S(g_2) = S(Q) \prec_m \boldsymbol{s}$ かつ $\mathrm{LM}(m_2g_2) = \mathrm{LM}(m_1g_1)$ となるものが存在し，これは仮定に矛盾する．

(2) $u_i(x,\xi)$ $(i=1,2) \in M$ をそれぞれ

$$\frac{\mathrm{LCM}(\mathrm{LM}(g_1),\mathrm{LM}(g_2))}{\mathrm{LM}(g_i)}$$

とし，u_i $(i=1,2) \in D$ の全表象をそれぞれ $u_i(x,\xi)$ とする．$u_i(x,\xi) \mid m_i(x,\xi)$ であり，$m_1(x,\xi)\mathrm{LM}(g_1) = m_2(x,\xi)\mathrm{LM}(g_2)$ より，

$$\frac{m_1(x,\xi)}{u_1(x,\xi)} = \frac{m_1(x,\xi)\mathrm{LM}(g_1)}{\mathrm{LCM}(\mathrm{LM}(g_1),\mathrm{LM}(g_2))} = \frac{m_2(x,\xi)\mathrm{LM}(g_2)}{\mathrm{LCM}(\mathrm{LM}(g_1),\mathrm{LM}(g_2))} = \frac{m_2(x,\xi)}{u_2(x,\xi)}$$

である．$v(x,\xi) = \dfrac{m_1(x,\xi)}{u_1(x,\xi)} = \dfrac{m_2(x,\xi)}{u_2(x,\xi)}$ とする．ここで，$\mathrm{LM}(m_1) = \mathrm{LM}(vu_1)$, $\mathrm{LM}(m_2) = \mathrm{LM}(vu_2)$ である．

g_1, g_2 の S 多項式を $\mathrm{Spoly}(g_1,g_2) = u_1g_1 - u_2g_2$ と表記すると，$v\mathrm{Spoly}(g_1,g_2) = vu_1g_1 - vu_2g_2$ となり，$\mathrm{LM}(m_1g_1) = \mathrm{LM}(m_2g_2) = \mathrm{LM}(vu_1g_1) = \mathrm{LM}(vu_2g_2)$ より，

$$\mathrm{LM}(v\mathrm{Spoly}(g_1,g_2)) \prec \mathrm{LM}(m_1g_1)$$

である．また，$S(m_1g_1 - m_2g_2) = S(m_1g_1) = m_1(x,\xi)S(g_1) = \boldsymbol{s}$ であることから，

$$v(x,\xi)u_1(x,\xi)S(g_1) = m_1(x,\xi)S(g_1) \succ_m m_2(x,\xi)S(g_2) = v(x,\xi)u_2(x,\xi)S(g_2)$$

となるため，これと補題 9 から，

$$S(v\mathrm{Spoly}(g_1,g_2)) = S(vu_1g_1 - vu_2g_2) = S(vu_1g_1) = S(m_1g_1) = \boldsymbol{s}$$

である．$S(vu_1g_1) = S(m_1g_1)$ の部分は補題 9 の証明の後半の議論と同様に示される．したがって，

$$S(v\mathrm{Spoly}(g_1,g_2)) = S(m_1g_1 - m_2g_2)$$

となる．ここで，$u_1 = m_1$ であれば，$m_1g_1 - m_2g_2$ は (g_1,g_2) の S 多項式 $\mathrm{Spoly}(g_1,g_2) = u_1g_1 - u_2g_2$ に一致し，その signature は $\boldsymbol{s}$ となる．これを $\mathfrak{S}$-簡約して signature が $\boldsymbol{s}$ の $\mathfrak{S}$-既約な元が構成される．

以下では $u_1 \neq m_1$ が起こりえないことを示す．$u_1 \neq m_1$ と仮定すれば $S(\mathrm{Spoly}(g_1,g_2)) \prec_m \boldsymbol{s}$ であるので，$\mathfrak{S}$-グレブナー基底の定義からある $m_3 \in M$, $g_3 \in G_{\prec \boldsymbol{s}}$ が存在して，

$$m_3(x,\xi)S(g_3) = S(m_3g_3) = S(\mathrm{Spoly}(g_1,g_2)) \prec_m \boldsymbol{s} \text{ かつ } m_3g_3 \text{ は } \mathfrak{S}\text{-既約}$$

である．このとき，補題 13 より $\mathrm{LM}(m_3g_3) \preceq \mathrm{LM}(\mathrm{Spoly}(g_1,g_2))$ となる．ここで $w(x,\xi) = \dfrac{m_1(x,\xi)m_3(x,\xi)}{u_1(x,\xi)} = v(x,\xi)m_3(x,\xi)$ とすると，

$$w(x,\xi)S(g_3) = v(x,\xi)S(m_3g_3) = v(x,\xi)S(\mathrm{Spoly}(g_1,g_2)) = \boldsymbol{s}$$

であり，

$$w(x,\xi)\mathrm{LM}(g_3) = v(x,\xi)\mathrm{LM}(m_3g_3) \preceq v(x,\xi)\mathrm{LM}(\mathrm{Spoly}(g_1,g_2)) \prec \mathrm{LM}(m_1g_1)$$

となる．$(w(x,\xi),g_3) \in S$ であるが $(w(x,\xi),g_3)$ のほうが LM が低いことがわかり $(m_1(x,\xi),g_1)$ の取り方に反す．∎

命題 28 を別の見方をすると以下になる．

命題 29
$\boldsymbol{s} \in \mathrm{NS}(\mathbf{Syz})$ とし，$G_{\prec \boldsymbol{s}}$ を $\boldsymbol{s}$ 未満 $\mathfrak{S}$-グレブナー基底とする．

(1) $G_{\prec \boldsymbol{s}}$ の元の対 (g, g') で，その S 多項式の signature が $\boldsymbol{s}$ になるものが存在したとする．$\boldsymbol{s}$ が必要な signature であるための必要十分条件は，signature が $\boldsymbol{s}$ になる mg $(m(x,\xi) \in M,\, g \in G_{\prec \boldsymbol{s}})$ で LM が最小のものを主成分とする正則対が存在することである．
(2) 上記の対 (g, g') で，その S 多項式の signature が $\boldsymbol{s}$ になるものが存在しないとき，$\boldsymbol{s}$ は不要な signature である．

命題 29 を $\boldsymbol{s}$ 以下 $\mathfrak{S}$-グレブナー基底に置き換えて考える．

命題 30
$\boldsymbol{s} \in \mathrm{NS}(\mathbf{Syz})$ とし，$G_{\preceq \boldsymbol{s}}$ を $\boldsymbol{s}$ 以下 $\mathfrak{S}$-グレブナー基底とする．$G_{\preceq \boldsymbol{s}}$ の元よりなる正則対の集合を SP とし，最小の signature を $\boldsymbol{s'}$ とする．このとき，$G_{\preceq \boldsymbol{s}}$ は $\boldsymbol{s'}$ 未満 $\mathfrak{S}$-グレブナー基底である．

証明 $\hat{\boldsymbol{s}}$ を $G_{\preceq \boldsymbol{s}}$ が $\hat{\boldsymbol{s}}$ 未満の $\mathfrak{S}$-グレブナー基底となるような最大の signature とし，$\hat{\boldsymbol{s}} \prec_m \boldsymbol{s'}$ として矛盾を導く．実際，$G_{\preceq \boldsymbol{s}}$ が $\hat{\boldsymbol{s}}$ 未満の $\mathfrak{S}$-グレブナー基底であるが，signature が $\hat{\boldsymbol{s}}$ の正則対が存在しないので，命題 29 より $G_{\preceq \boldsymbol{s}}$ は $\hat{\boldsymbol{s}}$ 以下 $\mathfrak{S}$-グレブナー基底となり，仮定に反する． ∎

命題 29,30 より $\mathfrak{S}$-グレブナー基底の計算アルゴリズムが得られる．さらに同じアルゴリズムでそのままグレブナー基底を計算することができる．具体的には，signature に関する帰納法で計算する．$\boldsymbol{s}$ 未満 $\mathfrak{S}$-グレブナー基底 $G_{\prec \boldsymbol{s}}$ が与えられたとき，命題 29 の必要十分条件を確認し，必要な signature であれば命題 28(2) のように S 多項式を簡約して得た $g_{\boldsymbol{s}}$ を $G_{\prec \boldsymbol{s}}$ に追加する．不要な signature であれば $G_{\prec \boldsymbol{s}}$ はそのままでよい．これにより $\boldsymbol{s}$ 以下 $\mathfrak{S}$-グレブナー基底 $G_{\preceq \boldsymbol{s}}$ を得る．さらにこれと命題 30 により新たな $\boldsymbol{s'}$未満 $\mathfrak{S}$-グレブナー基底 $G_{\prec \boldsymbol{s'}}$ を得る．この繰り返しで $\mathfrak{S}$-グレブナー基底 G が得られる．以下では signature がいつでも計算できる場合のアルゴリズムの概要を挙げる．

Signature-based algorithm の概要 (Weyl 代数版)，signature がいつでも計算可能な場合

(1) $G = \{P_1, \ldots, P_r\}$ より始める．(最小の signature $\boldsymbol{e}_1$ より開始する．G は $\boldsymbol{e}_1$以下 $\mathfrak{S}$-グレブナー基底である．)
(2) G の元よりなる正則対の集合を SP とし，signature の小さい順に並べる．最小の signature を $\boldsymbol{s}$ とする．(G は $\boldsymbol{s}$ 未満 $\mathfrak{S}$-グレブナー基底である．)
(3) $\boldsymbol{s}$ に対して命題 29(1) の必要十分条件をチェックする．
  (3-1) 正しい場合: 最小の LM になるものを主成分とする S 多項式を作成し，これに $\mathfrak{S}$-簡約を行って $\mathfrak{S}$-既約な元 $g_{\boldsymbol{s}}$ を計算する．これを G に加え，G から signature が $g_{\boldsymbol{s}}$ と同じものを削除する．(G は $\boldsymbol{s}$ 以下 $\mathfrak{S}$-グレブナー基底である．)
  さらに SP より signature が $\boldsymbol{s}$ である正則対をすべて消去し，新たに $g_{\boldsymbol{s}}$ を成分とする正則対を SP に加える．ステップ (2) に戻る．
  (3-2) 正しくない場合: SP より signature が $\boldsymbol{s}$ である正則対をすべて消去し，ステップ (2) に戻る．(G は $\boldsymbol{s}$ 以下 $\mathfrak{S}$-グレブナー基底である．)
(4) G を $\mathfrak{S}$-グレブナー基底として出力する．

G が $\mathfrak{S}$-グレブナー基底となったところで，すべての正則な S 多項式は (3-2) となり，新たな S 多項式の計算は発生しない．

5　予想 signature によるグレブナー基底計算

定義 31 (予想 signature)
$P \in I$ を $S(P)$ が既知の元とする．このとき，$m \in M$ に対して $m(x,\xi)S(P)$ を $S(mP)$ の**予想された signature** と呼び，$\tilde{S}(mP)$ で表す．補題 6 より $S(mP) = \tilde{S}(mP)$ である必要十分条件は，$m(x,\xi)S(P) \in \mathrm{NS}(\mathbf{Syz})$ である．予想された signature に基づいて構成した正則対を**擬正則対**と呼び，これから作られる S 多項式を**擬正則 S 多項式**という．擬正則 S 多項式の signature は (断りのない限り) 予想された signature を考えるものとする．予想された signature と真の signature が異なるとき，予想された signature を**偽の signature** といい，さらに擬正則対を**偽の正則対**，その S 多項式を**偽の S 多項式**という．

通常非可換環においては予想された signature を多項式環のように構成しようとしても，単項式の加群単項式への作用 (単項式と加群単項式の積) が加群単項式とはならない．(非可換の積ではお釣りの項がでて加群の多項式となってしまう．) しかし Weyl 代数に関しては LM に関して可換で計算できるという性質があり，上記の定義のようにして D における積ではなく可換の積によって構成することができる．

Weyl 代数においても，多項式環同様の方法で予想された signature を構成しながら帰納的に $\mathfrak{S}$-グレブナー基底を計算することができる．

命題 32
$\boldsymbol{s} \in \boldsymbol{M}$ とし，$G_{\prec \boldsymbol{s}}$ を $\boldsymbol{s}$ 未満 $\mathfrak{S}$-グレブナー基底とする．$m(x,\xi) \in M$, $g \in G_{\prec \boldsymbol{s}}$ に対して $m(x,\xi)S(g) = \boldsymbol{s}$ であるが $S(mg) \neq m(x,\xi)S(g)$ であれば $\boldsymbol{s} \in \mathrm{LM}(\mathbf{Syz})$ であり，mg は $\boldsymbol{s}$ と $G_{\prec \boldsymbol{s}}$ に関する $\mathfrak{S}$-簡約により 0 となる．特に偽の S 多項式はその signature を $\boldsymbol{s}$ とすると，$\boldsymbol{s}$ と $G_{\prec \boldsymbol{s}}$ に関する $\mathfrak{S}$-簡約により 0 となる．

命題 33
$\boldsymbol{s} \in \boldsymbol{M}$ とし，$G_{\prec \boldsymbol{s}}$ を $\boldsymbol{s}$ 未満 $\mathfrak{S}$-グレブナー基底とする．

(1) $G_{\prec \boldsymbol{s}}$ の元の対 (g, g') で，その擬正則 S 多項式の signature が $\boldsymbol{s}$ になるものが存在したとする．このとき，$\boldsymbol{s}$ が必要な signature であるための必要十分条件は以下の 2 つが成り立つことである．
  (1-1) signature が $\boldsymbol{s}$ になる mg $(m(x,\xi) \in M, g \in G_{\prec \boldsymbol{s}})$ で LM が最小のものを主成分とする擬正則対が存在する．
  (1-2) 擬正則 S 多項式を $\mathfrak{S}$-簡約して 0 にならない．

(2) 上記の対 (g, g') で，擬正則 S 多項式の signature が $\boldsymbol{s}$ になるものが存在しない場合，$\boldsymbol{s}$ は不要な signature である．

証明 (2) は明らか．
(1-2) において，S 多項式が 0 に $\mathfrak{S}$-簡約されることは結果として $\boldsymbol{s} \notin \mathrm{NS}(\mathbf{Syz})$ であることを意味し，簡約されないことは S 多項式の真の signature は $\boldsymbol{s}$ 未満ではないことを意味する．この場合に予想された signature は $\boldsymbol{s}$ であるので，真の signature は $\boldsymbol{s}$ である．
さらに (1-1) が成り立つので，命題 29 より $\boldsymbol{s}$ は必要な siganture であり，S 多項式を $\mathfrak{S}$-簡約することで真の signature が $\boldsymbol{s}$ である $\mathfrak{S}$-既約な元 $g_{\boldsymbol{s}}$ が求められる． ∎
命題 33 を $\boldsymbol{s}$ 以下 $\mathfrak{S}$-グレブナー基底に置き換えて考える．

命題 34
$\boldsymbol{s} \in \boldsymbol{M}$ とし，$G_{\preceq \boldsymbol{s}}$ を $\boldsymbol{s}$ 以下 $\mathfrak{S}$-グレブナー基底とする．$G_{\preceq \boldsymbol{s}}$ の元よりなる擬正則対の集合を SP とし，$\boldsymbol{s}$ より大きい signature の中で最小のものを $\boldsymbol{s}'$ とする．このとき，$G_{\preceq \boldsymbol{s}}$ は $\boldsymbol{s}'$ 未満 $\mathfrak{S}$-グレブナー基底である．

証明 $\hat{\boldsymbol{s}}$ を $G_{\preceq \boldsymbol{s}}$ が $\hat{\boldsymbol{s}}$ 未満の $\mathfrak{S}$-グレブナー基底となるような最大の signature とし，$\hat{\boldsymbol{s}} \prec_m \boldsymbol{s}'$ として矛盾を導く．実際，$G_{\preceq \boldsymbol{s}}$ が $\hat{\boldsymbol{s}}$ 未満の $\mathfrak{S}$-グレブナー基底であるが，signature が $\hat{\boldsymbol{s}}$ の擬正則対が存在しないので，命題 33 より $G_{\preceq \boldsymbol{s}}$ は $\hat{\boldsymbol{s}}$ 以下 $\mathfrak{S}$-グレブナー基底となり，仮定に反する． ∎

注意 3 (syzygy criterion)
命題 33(1) において，予想された signature $\boldsymbol{s}$ が過去に偽 signature と判断されたもの $\boldsymbol{s}'$ で割れた場合，$\boldsymbol{s}$ も偽である．($\boldsymbol{s}' \in \mathrm{LM}(\mathbf{Syz})$ より，$\boldsymbol{s} = m(x,\xi)\boldsymbol{s}'$ であれば $\boldsymbol{s} \in \mathrm{LM}(\mathbf{Syz})$ である．) そこで，これらの偽 signature を保管しておいて $\boldsymbol{s}$ への偽判定への quicktest とすることができる．

Signature-based algorithm の概要 (Weyl 代数版)，signature を並行して計算する場合

(1) $G = \{P_1, \ldots, P_r\}$ より始める．(最小の signature $\boldsymbol{e}_1$ より開始する．G は $\boldsymbol{e}_1$以下 $\mathfrak{S}$-グレブナー基底である．)
(2) G の元よりなる擬正則対の集合を SP とし，signature の小さい順に並べる．最小の signature を $\boldsymbol{s}$ とする．(G は $\boldsymbol{s}$ 未満 $\mathfrak{S}$-グレブナー基底である．)
(3) $\boldsymbol{s}$ に対して命題 33(1) の必要十分条件をチェックする．(注意 3 を quicktest として偽 siganture の判定を行うことができる)
  (3-1) 正しい場合: 最小の LM になるものを主成分とする S 多項式を作成し，これに $\mathfrak{S}$-簡約を行って $\mathfrak{S}$-既約な元 $g_{\boldsymbol{s}}$ を計算する．
    (A) $g_{\boldsymbol{s}} = 0$ のとき，$\boldsymbol{s} \in \mathrm{LM}(\mathbf{Syz})$ である．これは偽であり不要な signature である．
    (B) $g_{\boldsymbol{s}} \neq 0$ のとき，$\boldsymbol{s} \in \mathrm{NS}(\mathbf{Syz})$ であり必要な signature である．$g_{\boldsymbol{s}}$ を G に加える．
    G から signature が $g_{\boldsymbol{s}}$ と同じものがあればそれを削除する．(G は $\boldsymbol{s}$ 以下 $\mathfrak{S}$-グレブナー基底である．) さらに SP より signature が $\boldsymbol{s}$ である擬正則対をすべて消去し，新たに $g_{\boldsymbol{s}}$ を成分とする擬正則対を SP に加える．ステップ (2) に戻る．
  (3-2) 正しくない場合: SP より signature が $\boldsymbol{s}$ である擬正則対をすべて消去し，ステップ (2) に戻る．(G は $\boldsymbol{s}$ 以下 $\mathfrak{S}$-グレブナー基底である．)
(4) G を $\mathfrak{S}$-グレブナー基底として出力する．

G が $\mathfrak{S}$-グレブナー基底となったところで，G を $\mathfrak{S}$-既約な元のみにしておけば，G から擬正則対は発生しない．このアルゴリズムをまとめたものが次のものである．

アルゴリズム 1 (signature-based algorithm (Weyl 代数版))
input: $F = \{P_1, \ldots, P_r\}, \prec_m$
output: F の生成する左イデアルの $\mathfrak{S}$-グレブナー基底 G
$SP \leftarrow \{(P,Q) \mid P, Q \in F\ ; (P,Q)$ は擬正則対 $\}$, $G \leftarrow F$
while $(SP \neq \emptyset)$ do
  $\boldsymbol{s} \leftarrow \min_{\prec_m}\{\tilde{S}(\mathrm{Spoly}(P,Q))\}$ $((P,Q) \in SP)$
  if (quicktest で偽ではない) then
    if $(\tilde{S}(mR) = \boldsymbol{s}$ となる mR $(m(x,\xi) \in M,\ R \in G)$ の中で
      LM 最小のものを主成分とする擬正則対 (P', Q') が存在) then
      $h \leftarrow \mathrm{Spoly}(P', Q')$, $h \longrightarrow^{G}_{\mathfrak{S},\boldsymbol{s}} \tilde{h}$
      if $(\tilde{h} \neq 0)$ then
        $G \leftarrow G \cup \{\tilde{h}\}$
        $SP \leftarrow SP \cup \{(P, \tilde{h}) \mid P \in G\ ; (P, \tilde{h})$ は擬正則対 $\}$

```
            end if
        end if
    end if
    SP ← SP \ {(P, Q) | S̃(Spoly(P, Q)) = s}
end while
return G
```

多項式環における SBA と比較して，$h \leftarrow \mathrm{Spoly}(P', Q')$ と $h \longrightarrow^{G}_{\mathfrak{S},\boldsymbol{s}} \tilde{h}$ の 2 箇所が変更点である．S 多項式を D における積で作成し $\mathfrak{S}$-簡約を D における積で行う．一方で予想された signature は可換の積で構成する．これにより Weyl 代数においても SBA が適用できる．

参 考 文 献

[1] D. Cox, J. Little, D. O'Shea, Ideals, Varieties, and Algorithms, Springer, 2007.

[2] D. Cox, J. Little, D. O'Shea, Using Algebraic Geometry, Springer, 2000.

[3] C. Eder, J. -C. Faugère, A survey on signature-based algorithms for computing Gröbner bases, Journal of Symbolic Computation **80** (2017). 719–784.

[4] J. -C. Faugère, A new efficient algorithm for computing Gröbner bases without reduction to zero (F5), In Proccecings of the 2002 ISSAC, 75–83, ACM, 2002.

[5] 大阿久俊則, D 加群と計算数学, 朝倉書店, 2002.

[6] K. Sakata, Simple Signature-Based Algorithms with Correctness and Termination, Communication of JSSAC **4** (2020). 33–49.

[7] T. Vaccon, K. Yokoyama, A tropical F5 algorithm, In Proccecings of the 2017 ISSAC, 429–436, ACM, 2017.

[8] T. Vaccon, T. Verron, K. Yokoyama, On Affine Tropical F5 Algorithms, In Proccecings of the 2018 ISSAC, 383–390, ACM, 2018.

[9] 横山和弘, Signature-based アルゴリズムの正当性・停止性について, 計算機代数夏の学校 2019 資料, 2019.