

包括的 Gröbner 基底系を用いた parametric イデアルの根基計算

東京都立大学大学院 理学研究科 数理科学専攻

22843420

田中一希

2024 年 1 月 10 日

目次

はじめに	2
第 1 章 Gröbner 基底	3
1.1 単項式と Dickson の補題	3
1.2 Gröbner 基底の定義と基本的性質	5
1.3 Buchberger アルゴリズム	6
1.4 簡約 Gröbner 基底とその一意性	10
1.5 消去理論	13
1.6 Gröbner 基底計算の高速化	15
第 2 章 根基イデアルの計算と Gröbner 基底	23
2.1 イデアルの次元	23
2.2 0 次元イデアルの根基イデアルの計算	24
2.3 イデアルの 0 次元化	25
2.4 根基イデアルの計算	30
第 3 章 包括的 Gröbner 基底系	31
3.1 包括的 Gröbner 基底系	31
3.2 鈴木-佐藤アルゴリズム	33
第 4 章 parametric イデアルの根基と CGS	36
4.1 parametric イデアルに対する操作の安定性	36
4.2 parametric イデアルの次元と 0 次元 parametric イデアルの根基	36
4.3 parametric イデアルの 0 次元化と根基の計算	38
今後の課題	41
謝辞	42
付録	43
参考文献	50

はじめに

包括的 Gröbner 基底系 (comprehensive Gröbner system, 以下 CGS) とは, パラメータを係数に含む多項式が生成するイデアル (以下 parametric イデアル) に対して, パラメータの空間を有限個に分割したものとその各分割部において一様に Gröbner 基底を与えるパラメータ付き多項式の有限集合のペアからなる系である. この概念は 1992 年に Weispfenning [22] によって提唱され, 同時にその存在性と計算アルゴリズムが示された. その後, 鈴木-佐藤 [20] によって通常の Gröbner 基底計算アルゴリズムを用いて CGS を計算する鈴木-佐藤アルゴリズム (後述) が与えられ, 計算が高速化されると同時に理論的にも大きなブレイクスルーとなった. さらにその後も鍋島 [13] や Kapur-Sun-Wang [10] など, 鈴木-佐藤アルゴリズムを改良したものが提案されている.

CGS の発展にともない, イデアルに対する操作 (例えば共通部分やイデアル商など) の parametric イデアルへの拡張も研究されている. 横山 [23] は CGS の計算アルゴリズムおよび従来の parameter なしのイデアルに対する根基イデアルの計算アルゴリズムを応用して parametric イデアルに対する根基の計算アルゴリズムを示した.

本研究では, その [23] および [7] をもとに, 0 次元の parametric イデアルに対する根基の計算を実装した. また, 一般次元での根基計算の実装に向けて,

- parametric イデアルの共通部分
- parametric イデアルに対するイデアル商

の計算を実装した. なお, 使用した計算代数システムは Risa/Asir [19] であり, CGS の計算には [14] を用いた.

最後に, 本論文の構成を説明する. 第 1 章で Gröbner 基底の基礎について述べ, 第 2 章で Gröbner 基底を用いた通常のイデアルに対する根基の計算について説明する. そして第 3 章で CGS の定義およびその計算アルゴリズムを説明し, 第 4 章で CGS を用いた parametric イデアルに対する根基の計算について述べる. また, 付録では本研究の主結果である実装を記載している.

第 1 章

Gröbner 基底

本論文では K を体, $\mathbb{Z}_{\geq 0}$ を非負整数全体の集合とする. また, n 個の変数 x_1, \dots, x_n について $X = (x_1, \dots, x_n)$ とし, $a = (a_1, \dots, a_n) \in \mathbb{Z}_{\geq 0}^n$ に対して $x_1^{a_1} \cdots x_n^{a_n}$ を X^a , K 上の n 変数多項式環 $K[x_1, \dots, x_n]$ を $K[X]$ と略記する. この章では Gröbner 基底理論の基礎について述べる.

1.1 単項式と Dickson の補題

定義 1.1. 非負整数の組 $a \in \mathbb{Z}_{\geq 0}^n$ と n 個の変数 X に対して X^a を変数 X の**単項式** (monomial) といい, X の単項式全体の集合を $M(X)$ で表す. また, 多項式 $f = c_{a_1} X^{a_1} + \cdots + c_{a_l} X^{a_l} \in K[X]$ ($a_i \in \mathbb{Z}_{\geq 0}^n$) について, 各 c_{a_i} を X^{a_i} の**係数** (coefficient), 各 $c_{a_i} X^{a_i}$ を f の**項** (term) という.

定義 1.2. $a = (a_1, \dots, a_n) \in \mathbb{Z}_{\geq 0}^n$ に対して,

$$|a| := \sum_{i=1}^n a_i$$

とするとき, この値を単項式 X^a の**全次数** (total degree) といい $\text{tdeg}(X^a)$ で表す. また, 多項式 $f = c_{a_1} X^{a_1} + \cdots + c_{a_l} X^{a_l} \in K[X]$ に対して, f の全次数 $\text{tdeg}(f)$ を

$$\text{tdeg}(f) := \max(|a_1|, \dots, |a_l|)$$

で定める.

定義 1.3. $\mathbb{Z}_{\geq 0}^n$ 上の順序関係 \prec が次を満たすとき, \prec は**単項式順序** (monomial order) であるという.

(i) \prec は全順序かつ整列順序である.

(ii) 任意の $a, b, c \in \mathbb{Z}_{\geq 0}^n$ に対して, $a \prec b \implies a + c \prec b + c$ である.

注意 1.4. 上の単項式順序は, $\mathbb{Z}_{\geq 0}^n$ 上の順序として定義したが, $a \in \mathbb{Z}_{\geq 0}^n$ と $X^a \in M(X)$ を同一視することにより $M(X)$ 上の順序と見なすことができる.

単項式順序となる順序の例をいくつか紹介する. ただし, ここでの $<$ および \leq は通常の整数の大小関係とする.

定義 1.5. 2 つの非負整数の組 $a = (a_1, \dots, a_n), b = (b_1, \dots, b_n) \in \mathbb{Z}_{\geq 0}^n$ に対して, $a \prec_{\text{lex}} b$ であるとは, ある $1 \leq l \leq n$ が存在して,

$$a_i = b_i \ (1 \leq i < l) \quad \text{かつ} \quad a_l < b_l$$

となることである. このようにして定まる $\mathbb{Z}_{\geq 0}^n$ 上の順序 \prec_{lex} を**辞書式順序** (lexicographical order) という.

定義 1.6. 2 つの非負整数の組 $a = (a_1, \dots, a_n), b = (b_1, \dots, b_n) \in \mathbb{Z}_{\geq 0}^n$ に対して, $a \prec_{\text{revlex}} b$ であるとは, ある $1 \leq l \leq n$ が存在して,

$$a_i = b_i \ (l < i \leq n) \quad \text{かつ} \quad a_l < b_l$$

となることである. このようにして定まる $\mathbb{Z}_{\geq 0}^n$ 上の順序 \prec_{revlex} を**逆辞書式順序** (reverse lexicographical order) という.

定義 1.7. 2つの非負整数の組 $a = (a_1, \dots, a_n), b = (b_1, \dots, b_n) \in \mathbb{Z}_{\geq 0}^n$ に対して, $a \prec_{\text{grlex}} b$ であるとは,

$$|a| < |b| \text{ または } |a| = |b| \text{ かつ } a \prec_{\text{lex}} b$$

となることである. このようにして定まる $\mathbb{Z}_{\geq 0}^n$ 上の順序 \prec_{grlex} を**次数付き辞書式順序** (graded lexicographical order) という.

定義 1.8. 2つの非負整数の組 $a = (a_1, \dots, a_n), b = (b_1, \dots, b_n) \in \mathbb{Z}_{\geq 0}^n$ に対して, $a \prec_{\text{grevlex}} b$ であるとは,

$$|a| < |b| \text{ または } |a| = |b| \text{ かつ } a \prec_{\text{revlex}} b$$

となることである. このようにして定まる $\mathbb{Z}_{\geq 0}^n$ 上の順序 \prec_{grevlex} を**次数付き逆辞書式順序** (graded reverse lexicographical order) という.

定義 1.9. X を 2 分割した変数の組 $X_1 = (x_1, \dots, x_m), X_2 = (x_{m+1}, \dots, x_n)$ について, \prec_1, \prec_2 をそれぞれ $M(X_1), M(X_2)$ 上の単項式順序とする. このとき, 2つの非負整数の組 $a = (a_1, \dots, a_n), b = (b_1, \dots, b_n) \in \mathbb{Z}_{\geq 0}^n$ に対して, $a \prec b$ であることを

$$(a_1, \dots, a_m) \prec_1 (b_1, \dots, b_m) \text{ または } ((a_1, \dots, a_m) = (b_1, \dots, b_m) \text{ かつ } (a_{m+1}, \dots, a_n) \prec_2 (b_{m+1}, \dots, b_n))$$

で定める順序 \prec を, $X_1 \gg X_2$ なる**ブロック順序** (block order), あるいは X_1 に関するブロック順序という. 逆に $a \prec b$ であることを

$$(a_{m+1}, \dots, a_n) \prec_2 (b_{m+1}, \dots, b_n) \text{ または } ((a_{m+1}, \dots, a_n) = (b_{m+1}, \dots, b_n) \text{ かつ } (a_1, \dots, a_m) \prec_1 (b_1, \dots, b_m))$$

で定める順序 \prec を, $X_1 \ll X_2$ なる**逆ブロック順序** (inverse block order) という.

定義 1.10. 多項式 $f = c_{a_1} X^{a_1} + \dots + c_{a_l} X^{a_l} \in K[X]$ と $\mathbb{Z}_{\geq 0}^n$ 上の単項式順序 \prec に対して,

$$\text{mdeg}(f) := \max \{a_i \in \mathbb{Z}_{\geq 0}^n \mid c_{a_i} \neq 0\}$$

とする. ただし, ここでの \max は順序 \prec に関する最大元の意味である.

(i) 多項式 f に対して,

$$\text{LC}_{\prec}(f) := c_{\text{mdeg}(f)}$$

を f の**先頭係数** (leading coefficient) という.

(ii) 多項式 f に対して,

$$\text{LM}_{\prec}(f) := X^{\text{mdeg}(f)}$$

を f の**先頭単項式** (leading monomial) という.

(iii) 多項式 f に対して,

$$\text{LT}_{\prec}(f) := \text{LC}_{\prec}(f) \cdot \text{LM}_{\prec}(f)$$

を f の**先頭項** (leading term) という.

以降, どの順序を用いているか特に誤解の恐れがないときは, $\text{LC}_{\prec}(f), \text{LM}_{\prec}(f), \text{LT}_{\prec}(f)$ を単に $\text{LC}(f), \text{LM}(f), \text{LT}(f)$ と表す.

定義 1.11. イデアル $I \subset K[X]$ に対して, ある部分集合 $\mathcal{M} \subset M(X)$ があって

$$I = \langle \mathcal{M} \rangle_{K[X]}$$

となるとき, I を**単項式イデアル** (monomial ideal) という.

定理 1.12 (Dickson の補題). 任意の単項式の集合 $\mathcal{M} \subset M(X)$ に対して, ある有限個の $u_1, \dots, u_l \in \mathcal{M}$ が存在して

$$\langle \mathcal{M} \rangle = \langle u_1, \dots, u_l \rangle$$

が成り立つ. 特に, 単項式イデアルは有限生成である.

証明. [2] 第 2 章 §4 定理 5 を参照. □

1.2 Gröbner 基底の定義と基本的性質

この節では、Gröbner 基底の定義およびその割り算に関する基本的な性質について述べる。

定義 1.13. $\langle 0 \rangle$ でないイデアル $I \subset K[X]$ と単項式順序 \prec に対して、有限集合 $G \subset K[X]$ が I の \prec に関する **Gröbner 基底** (Gröbner basis) であるとは、

$$\langle \text{LT}_{\prec}(I) \rangle = \langle \text{LT}_{\prec}(G) \rangle$$

が成り立つことである。また、有限集合 $G \subset K[X]$ が $\langle G \rangle$ の \prec に関する Gröbner 基底のとき、 G は単に \prec に関する Gröbner 基底であるという。イデアル $\langle 0 \rangle \subset K[X]$ に対しては、その Gröbner 基底を \emptyset で定める。

注意 1.14. 集合 $G \subset K[X]$ がイデアル $I \subset K[X]$ の Gröbner 基底とき、 G は I の生成系である。

命題 1.15. $M(X)$ 上の単項式順序 \prec を 1 つ固定する。多項式 $f \in K[X]$ と s 個の多項式の組 $F = (f_1, \dots, f_s) \in K[X]^s$ に対して、

$$f = q_1 f_1 + \dots + q_s f_s + r$$

を満たすような $q_1, \dots, q_s, r \in K[X]$ が存在し、これらは次を満たす。

- $r = 0$ または、 $r \neq 0$ かつ各 i と任意の $u \in \text{supp}(r)$ に対して $\text{LT}(f_i) \nmid u$ である。
- $q_i f_i \neq 0$ ならば、 $\text{mdeg}(f) \succeq \text{mdeg}(q_i f_i)$ である。

証明. 上記の性質をすべて満たすような $q_1, \dots, q_s, r \in K[X]$ は次のアルゴリズムで構成が可能である。

Algorithm 1.1 Division

Require: $f \in K[X]$, $F = (f_1, \dots, f_s) \in K[X]^s$, 単項式順序 \prec

Ensure: $q_1, \dots, q_s, r \in K[X]$

```

1:  $q_1 \leftarrow 0, \dots, q_s \leftarrow 0, r \leftarrow 0$ 
2:  $p \leftarrow f$ 
3: while  $p \neq 0$  do
4:    $i \leftarrow 1$ 
5:    $\text{divisionoccurred} \leftarrow \text{false}$ 
6:   while  $i \leq s \wedge \text{divisionoccurred} = \text{false}$  do
7:     if  $\text{LT}(f_i) \mid \text{LT}(p)$  then
8:        $q_i \leftarrow q_i + \frac{\text{LT}(p)}{\text{LT}(f_i)}$ 
9:        $p \leftarrow p - \frac{\text{LT}(p)}{\text{LT}(f_i)} \cdot f_i$ 
10:       $\text{divisionoccurred} \leftarrow \text{true}$ 
11:    else
12:       $i \leftarrow i + 1$ 
13:    end if
14:  end while
15:  if  $\text{divisionoccurred} = \text{false}$  then
16:     $r \leftarrow r + \text{LT}(p)$ 
17:     $p \leftarrow p - \text{LT}(p)$ 
18:  end if
19: end while
20: return  $q_1, \dots, q_s, r$ 
```

□

注意 1.16. 命題 1.15 の証明で用いたアルゴリズムを**割り算アルゴリズム** (division algorithm) という.

定義 1.17. 定理 1.15 と同様の記号のもとで, f は F によって r に**簡約** (reduce) されるといい, $f \xrightarrow{F} r$ で表す. また, r を f の F による**余り** (remainder) といい, \overline{f}^F で表す.

命題 1.18. $M(X)$ 上の単項式順序 \prec を 1 つ固定し, $f \in K[X]$ とする. G が \prec に関する Gröbner 基底のとき, G の各元を並べてつくった組 $\mathcal{G} \in G^s$ に対し, f の \mathcal{G} による余り $\overline{f}^{\mathcal{G}}$ は \mathcal{G} の元の並べ方に依らない.

証明. G を並べて作った 2 つの組 $\mathcal{G}_1, \mathcal{G}_2 \in G^s$ に対して $r_1 = \overline{f}^{\mathcal{G}_1}, r_2 = \overline{f}^{\mathcal{G}_2}$ とし, $r_1 - r_2 \neq 0$ と仮定する. まず, $r_1 - r_2 \in \langle G \rangle$ なので, $\text{LT}(r_1 - r_2) \in \langle \text{LT}(\langle G \rangle) \rangle$ である. 一方, $\text{LM}(r_1 - r_2) \in \text{supp}(r_1) \cup \text{supp}(r_2)$ なので, 定理 1.15 から $\text{LT}(r_1 - r_2) \notin \langle \text{LT}(G) \rangle$ である. 以上のことと Gröbner 基底の定義から矛盾が導かれる. □

注意 1.19. この命題により, $G \subset K[X]$ が Gröbner 基底であるときは $\overline{f}^{\mathcal{G}}$ を \overline{f}^G と表記できる.

命題 1.20. 単項式順序 \prec を 1 つ固定する. 多項式 $f \in K[X]$ とイデアル $I \subset K[X]$ の \prec に関する Gröbner 基底 $G \subset K[X]$ について, 次が成り立つ.

$$f \in I \iff \overline{f}^G = 0.$$

証明. (\Leftarrow) これは余りの定義から明らか.

(\Rightarrow) $G = \{g_1, \dots, g_s\}$ とおく. f と G に対して division algorithm を適用すると,

$$f = g_1 q_1 + \dots + g_s q_s + r$$

かつ

$$r = 0 \text{ または, } r \neq 0 \text{ ならば任意の } 1 \leq i \leq s \text{ と } u \in \text{supp}(r) \text{ に対して } \text{LT}(g_i) \nmid u$$

なる $q_1, \dots, q_s, r \in K[X]$ がとれる. $r \neq 0$ とすると

$$\text{LT}(r) \in \langle \text{LT}(I) \rangle = \langle \text{LT}(g_1), \dots, \text{LT}(g_s) \rangle$$

となるので矛盾する. □

1.3 Buchberger アルゴリズム

まず, S 多項式の定義を述べる.

定義 1.21. 多項式 $f, g \in K[X] \setminus \{0\}$ に対して, f, g の S 多項式 (S -polynomial) を次で定める.

$$S(f, g) = \frac{\text{lcm}(\text{LM}(f), \text{LM}(g))}{\text{LT}(f)} f - \frac{\text{lcm}(\text{LM}(f), \text{LM}(g))}{\text{LT}(g)} g.$$

補題 1.22. 単項式 $w \in M(X)$ を 1 つ固定する. $\text{LM}(f_i) = w$ なる $f_1, \dots, f_s \in K[X]$ について

$$g = b_1 f_1 + \dots + b_s f_s \text{ かつ } \text{LM}(g) \prec w$$

となる $b_i \in K, g \in K[X]$ をとると, ある $c_{jk} \in K$ が存在して

$$g = \sum_{1 \leq j, k \leq s} c_{jk} S(f_j, f_k)$$

が成り立つ.

証明. 簡単のため, 各 i について

$$c_i = \text{LC}(f_i), \quad g_i = \frac{f_i}{c_i}$$

とおく. このとき,

$$\begin{aligned} S(f_j, f_k) &= \frac{\text{lcm}(\text{LM}(f_j), \text{LM}(f_k))}{\text{LT}(f_j)} f_j - \frac{\text{lcm}(\text{LM}(f_j), \text{LM}(f_k))}{\text{LT}(f_k)} f_k \\ &= g_j - g_k. \end{aligned}$$

これと $\text{LM}(g) \prec w$ より

$$\begin{aligned} g &= \sum_{i=1}^s b_i c_i g_i \\ &= \sum_{i=2}^s (b_1 c_1 + \cdots + b_{i-1} c_{i-1}) (g_{i-1} - g_i) + (b_1 c_1 + \cdots + b_s c_s) g_s \\ &= \sum_{i=2}^s (b_1 c_1 + \cdots + b_{i-1} c_{i-1}) S(g_{i-1}, g_i). \end{aligned}$$

これにより,

$$g = \sum_{1 \leq j, k \leq s} c_{jk} S(f_j, f_k).$$

を満たす $c_{jk} \in K$ が得られる. □

定理 1.23 (Buchberger の判定法). 単項式順序 \prec を 1 つ固定する. イデアル $I \subset K[X]$ と I の生成系 $G = \{g_1, \dots, g_s\}$ について, 次は同値である.

- (i) G は I の \prec に関する Gröbner 基底である.
- (ii) 任意の相異なる i, j に対して, $\overline{S(g_i, g_j)}^G = 0$ が成り立つ.

証明. (1) \Rightarrow (2) を示す. 相異なる i, j に対して S 多項式の定義から

$$S(g_i, g_j) \in \langle g_i, g_j \rangle \subset I$$

となる. これと命題 1.20 から

$$\overline{S(g_i, g_j)}^G = 0.$$

(2) \Rightarrow (1) を示す. $f \in I \setminus \{0\}$ を任意にとり, 表示

$$f = h_1 g_1 + \cdots + h_s g_s \quad (h_i \in K[X])$$

を与える. このとき,

$$\delta(h_1, \dots, h_s) := \max\{\text{LM}(h_i g_i) \mid 1 \leq i \leq s, h_i g_i \neq 0\}$$

とし, さらに

$$\delta_f := \min_{f=h_1 g_1 + \cdots + h_s g_s} \delta(h_1, \dots, h_s)$$

とすると, $\text{LM}(f) \preceq \delta_f$ となる.

このとき, $\text{LM}(f) = \delta_f$ となること示す. そのために, $\text{LM}(f) \prec \delta_f$ なる $f \in I \setminus \{0\}$ が存在すると仮定し, 矛盾を導く. 簡単のため, $c_i = \text{LC}(h_i)$ とする. $\delta(h_1, \dots, h_s) = \delta_f$ なる (h_1, \dots, h_s) に対して

$$\begin{aligned} f &= \sum_{\text{LM}(h_i g_i) = \delta_f} h_i g_i + \sum_{\text{LM}(h_i g_i) \prec \delta_f} h_i g_i \\ &= \sum_{\text{LM}(h_i g_i) = \delta_f} c_i \text{LM}(h_i) g_i + \sum_{\text{LM}(h_i g_i) = \delta_f} (h_i - \text{LT}(h_i)) g_i + \sum_{\text{LM}(h_i g_i) \prec \delta_f} h_i g_i \end{aligned} \quad (1.1)$$

ここで $\text{LM}(f) \prec \delta_f$ なので

$$\text{LM} \left(\sum_{\text{LM}(h_i g_i) = \delta_f} c_i \text{LM}(h_i) g_i \right) \prec \delta_f$$

である。補題 1.22 より、ある $c_{jk} \in K$ が存在して

$$\sum_{\text{LM}(h_i g_i) = \delta_f} c_i \text{LM}(h_i) g_i = \sum_{j,k} c_{jk} S(\text{LM}(h_j) g_j, \text{LM}(h_k) g_k).$$

となる。ここで、

$$b_j = \text{LC}(g_j), \quad u_{jk} = \frac{\delta_f}{\text{lcm}(\text{LM}(g_j), \text{LM}(g_k))}$$

とおくと、 $\delta_f = \text{LM}(h_j g_j) = \text{LM}(h_k g_k)$ なので

$$\begin{aligned} S(\text{LM}(h_j) g_j, \text{LM}(h_k) g_k) &= \frac{\delta_f}{b_j \delta_f} \text{LM}(h_j) g_j - \frac{\delta_f}{b_k \delta_f} \text{LM}(h_k) g_k \\ &= \delta_f \left(\frac{1}{b_j \text{LM}(g_j)} g_j - \frac{1}{b_k \text{LM}(g_k)} g_k \right) \\ &= u_{jk} S(g_j, g_k) \end{aligned}$$

となる。これにより、

$$\sum_{\text{LM}(h_i g_i) = \delta_f} c_i \text{LM}(h_i) g_i = \sum_{j,k} c_{jk} u_{jk} S(g_j, g_k) \quad (1.2)$$

$$\text{LM}(u_{jk} S(g_j, g_k)) = \text{LM}(S(\text{LM}(h_j) g_j, \text{LM}(h_k) g_k)) \prec \delta_f \quad (1.3)$$

が成り立つ。ここで、仮定より、ある $p_{ijk} \in K[X]$ が存在して

$$S(g_j, g_k) = \sum_{i=1}^s p_{ijk} g_i \quad (1.4)$$

$$\text{LM}(p_{ijk} g_i) \prec \text{LM}(S(g_j, g_k)) \prec \delta_f \quad (1.5)$$

となるので、(1.4) を (1.2) に代入して

$$\begin{aligned} \sum_{\text{LM}(h_i g_i) = \delta_f} c_i \text{LM}(h_i) g_i &= \sum_{j,k} c_{jk} u_{jk} \left(\sum_{i=1}^s p_{ijk} g_i \right) \\ &= \sum_{i=1}^s \left(\sum_{j,k} c_{jk} u_{jk} p_{ijk} \right) g_i \end{aligned} \quad (1.6)$$

であり、

$$h'_i = \sum_{j,k} c_{jk} u_{jk} p_{ijk}$$

とすると、(1.3) と (1.5) から $\text{LM}(h'_i g_i) \prec \delta_f$ となる。さらに (1.6) を (1.1) に代入して

$$f = \sum_{i=1}^s h'_i g_i + \sum_{\text{LM}(h_i g_i) = \delta_f} (h_i - \text{LT}(h_i)) g_i + \sum_{\text{LM}(h_i g_i) \prec \delta_f} h_i g_i$$

であり、右辺の各項の先頭単項式は δ_f より小さい。このような表示の存在は δ_f の最小性に矛盾する。以上より、 $\text{LM}(f) = \delta_f$ が示された。このとき、ある i が存在して

$$\text{LM}(f) = \text{LM}(h_i g_i) = \text{LM}(h_i) \text{LM}(g_i), \quad h_i g_i \neq 0$$

となる。よって、

$$\text{LT}(f) \in \langle \text{LT}(g_1), \dots, \text{LT}(g_s) \rangle.$$

となるので、 G は Gröbner 基底である。 □

Buchberger の判定法により, イデアル I の生成系 f_1, \dots, f_s から I の Gröbner 基底を計算するアルゴリズムが得られる. これを **Buchberger アルゴリズム** (Buchberger algorithm) という.

Algorithm 1.2 Buchberger

Require: $F = \{f_1, \dots, f_s\}$, 単項式順序 \prec

Ensure: $I = \langle F \rangle$ の \prec に関する Gröbner 基底 G

```

1:  $G \leftarrow F$ 
2: while  $G \neq G'$  do
3:    $G' \leftarrow G$ 
4:   for all  $\{p, q\} \in G^2 (p \neq q)$  do
5:      $r \leftarrow \overline{S(p, q)}^G$ 
6:     if  $r \neq 0$  then
7:        $G \leftarrow G \cup \{r\}$ 
8:     end if
9:   end for
10: end while
11: return  $G$ 

```

定理 1.24. Buchberger アルゴリズムは有限のステップで終了する.

証明. 背理法で示す. $G = \{g_1, \dots, g_t\}$ として while ループ部分を 1 回処理したとき, その回で停止しないならば, ある相異なる $p, q \in G$ が存在して,

$$\overline{S(p, q)}^G \neq 0$$

となる. ここで $g_{t+1} = \overline{S(p, q)}^G$ とおくと, 余りの定義から

$$\text{LT}(g_{t+1}) \notin \langle \text{LT}(g_1), \dots, \text{LT}(g_t) \rangle$$

となる. よって, Buchberger アルゴリズムが有限のステップで終了しないとすると, 真の増大列

$$\langle \text{LT}(g_1), \dots, \text{LT}(g_s) \rangle \subset \langle \text{LT}(g_1), \dots, \text{LT}(g_{s+1}) \rangle \subset \dots$$

を得る. これは $K[X]$ の Nöther 性に矛盾する. □

例 1.25. 多項式 $f_1 = x^3 - 2xy, f_2 = x^2y - 2y^2 + x$ で生成されるイデアル $I = \langle f_1, f_2 \rangle \subset \mathbb{Q}[x, y]$ に対し, $x \succ_{\text{grlex}} y$ なる次数付き辞書式順序 \prec_{grlex} に関する Gröbner 基底を上記の Buchberger アルゴリズムを用いて計算する.

(i) まず, $G = \{f_1, f_2\}$ とする. このとき,

$$S(f_1, f_2) = yf_1 - xf_2 = -x^2 \xrightarrow{G} x^2$$

となるので, $f_3 = -x^2, G = \{f_1, f_2, f_3\}$ とする.

(ii) 次に

$$S(f_1, f_3) = f_1 + xf_3 = -2xy \xrightarrow{G} -2xy$$

となるので, $f_4 = -2xy, G = \{f_1, f_2, f_3, f_4\}$ とする.

(iii) 次に

$$S(f_2, f_3) = f_2 - yf_3 = -2y^2 + x \xrightarrow{G} -2y^2 + x$$

となるので, $f_5 = -2y^2 + x, G = \{f_1, f_2, f_3, f_4, f_5\}$ とする. (iv) 以降は $1 \leq i, j \leq 5$ に対して,

$$S(f_i, g_j) \xrightarrow{G} 0$$

となるので, Gröbner 基底 $G = \{f_1, f_2, f_3, f_4, f_5\}$ が得られた.

この Gröbner 基底を得るアルゴリズムと命題 1.20 から、多項式 $f \in K[X]$ とイデアルの生成系 $F = \{f_1, \dots, f_s\} \subset K[X]$ に対して $f \in \langle F \rangle$ かどうかを判定する次のアルゴリズムが得られる。

Algorithm 1.3 IdealMembership

Require: $f \in K[X], F = \{f_1, \dots, f_s\} \subset K[X]$

Ensure: $f \in \langle F \rangle$ の真偽

```

1:  $G \leftarrow \text{Buchberger}(F, \prec_{\text{grevlex}})$ 
2:  $r \leftarrow \text{Division}(f, G, \prec_{\text{grevlex}})$ 
3: if  $r = 0$  then
4:   return true
5: else
6:   return false
7: end if

```

1.4 簡約 Gröbner 基底とその一意性

前節までで定義した Gröbner 基底は冗長な元を含むことを許している。この節では、極小な Gröbner 基底および、イデアルに対して一意に定まる簡約 Gröbner 基底について述べる。

補題 1.26. 単項式イデアル $I = \langle \mathcal{M} \rangle$ ($\mathcal{M} \subset M(X)$) を考える。単項式 $u \in M(X)$ に対して、次は同値である。

- (i) $u \in I$ が成り立つ。
- (ii) ある単項式 $v \in \mathcal{M}$ が存在して、 $v \mid u$ が成り立つ。

証明. (ii) \Rightarrow (i) は明らか。

(i) \Rightarrow (ii) を示す。仮定から、ある $v_1, \dots, v_s \in \mathcal{M}$ と $f_1, \dots, f_s \in K[X]$ があって

$$u = \sum_{i=1}^s v_i f_i$$

と表せる。さらに各 i について、 $a_{i1}, \dots, a_{it_i} \in K$, $w_{i1}, \dots, w_{it_i} \in M(X)$ があって

$$f_i = \sum_{j=1}^{t_i} a_{ij} w_{ij}$$

と表せる。これにより、ある i, j があって $u = u_i v_{ij}$ となるので $u_i \mid u$ である。 □

定理 1.27. 単項式イデアル I に対して、その単項式からなる（包含関係に関して）極小な生成系が一意的に存在する。

証明. (存在性) 補題 1.12 より、 I の有限個の生成系 u_1, \dots, u_s が取れる。これらの中で、 $u_i \mid u_j$ なる各ペアについて u_j を除去すれば極小な生成系が得られる。

(一意性) 単項式からなる I の極小な生成系 $\mathcal{U} = \{u_1, \dots, u_s\}, \mathcal{V} = \{v_1, \dots, v_t\}$ をとる。補題 1.26 から、任意の $u_i \in \mathcal{U}$ に対してある j, k が存在して

$$u_i \mid v_j, \quad v_j \mid u_k$$

となる。このとき \mathcal{U} の極小性により $u_i = u_k$ なので、 $u_i = v_j \in \mathcal{V}$ となる。よって $\mathcal{U} \subset \mathcal{V}$ だが、 \mathcal{V} の極小性から $\mathcal{U} = \mathcal{V}$ である。 □

定義 1.28 ([2] §2.4 命題 7). 単項式イデアル I に対し、定理 1.27 の極小な生成系を I の**極小基底** (minimal basis) という。

補題 1.29 ([2] §2.7 補題 3). G をイデアル $I \subset K[X]$ の Gröbner 基底とする.

$g \in G$ が $\text{LT}(g) \in \langle \text{LT}(G \setminus \{g\}) \rangle$ を満たすとき, $G \setminus \{g\}$ は I の Gröbner 基底である.

証明. G は I の Gröbner 基底なので, $\langle \text{LT}(G) \rangle = \langle \text{LT}(I) \rangle$ である. さらに, $\langle \text{LT}(G \setminus \{g\}) \rangle \subset \langle \text{LT}(G) \rangle$ は明らかであり, $\text{LT}(g) \in \langle \text{LT}(G \setminus \{g\}) \rangle$ からその逆も成り立つ. 従って, $\langle \text{LT}(G \setminus \{g\}) \rangle = \langle \text{LT}(I) \rangle$ を得る. \square

この性質から, 次が自然に定義される.

定義 1.30. イデアル $I \subset K[X]$ の Gröbner 基底 G が以下の性質を満たすとき, G は I の **極小 Gröbner 基底** (minimal Gröbner basis) という.

- (1) 任意の $g \in G$ に対し, $\text{LC}(g) = 1$ である.
- (2) 任意の $g \in G$ に対し, $\text{LT}(g) \notin \langle \text{LT}(G \setminus \{g\}) \rangle$ である.

補題 1.26 から Gröbner 基底 G とその元 $g \in G$ について, $\text{LT}(g) \in \langle \text{LT}(G \setminus \{g\}) \rangle$ であることと, ある $g' \in G \setminus \{g\}$ が存在して $\text{LM}(g') \mid \text{LM}(g)$ となることは同値である. これを利用することにより, 次のアルゴリズムが得られる.

Algorithm 1.4 MinimalGroebnerBasis

Require: I の Gröbner 基底 $G = \{g_1, \dots, g_s\}$

Ensure: I の極小 Gröbner 基底

```

1:  $F \leftarrow G$ 
2: for  $i = 1, \dots, s$  do
3:    $j \leftarrow 1$ 
4:   while  $j \leq s$  or  $\text{divisible} = \text{true}$  do
5:     if  $i \neq j$  and  $\text{LM}(g_j) \mid \text{LM}(g_i)$  then
6:        $\text{divisible} \leftarrow \text{true}$ 
7:     end if
8:      $j \leftarrow j + 1$ 
9:   end while
10:  if  $\text{divisible} = \text{true}$  then
11:     $F \leftarrow F \setminus \{g_i\}$ 
12:  end if
13: end for
14:  $F' \leftarrow \emptyset$ 
15: for all  $g \in F$  do
16:    $F \leftarrow F \cup \left\{ \frac{g}{\text{LC}(g)} \right\}$ 
17: end for
18: return  $F'$ 

```

例 1.31 (例 1.25 の続き). 多項式 $f_1 = x^3 - 2xy$, $f_2 = x^2y - 2y^2 + x$ で生成されるイデアル $I = \langle f_1, f_2 \rangle \subset \mathbb{Q}[x, y]$ に対して,

$$f_3 = -x^2, f_4 = -2xy, f_5 = -2y^2 + x$$

とすると, I の次数付き辞書式順序 \prec_{grlex} に関する Gröbner 基底は $G = \{f_1, f_2, f_3, f_4, f_5\}$ であった. ここで, $\text{LM}(f_3) \mid \text{LM}(f_1)$, $\text{LM}(f_4) \mid \text{LM}(f_2)$ となるので, f_1, f_2 は G から除去できる. さらに, それぞれ定数倍して

$$\tilde{f}_3 = x^2, \tilde{f}_4 = xy, \tilde{f}_5 = y^2 - \frac{1}{2}$$

とすれば $\{\tilde{f}_3, \tilde{f}_4, \tilde{f}_5\}$ は I の極小 Gröbner 基底となる.

定義 1.32. イデアル $I \subset K[X]$ の Gröbner 基底 G が以下の性質を満たすとき, G は I の **簡約 Gröbner 基底** (reduced Gröbner basis) という.

- (1) 任意の $g \in G$ に対し, $\text{LC}(g) = 1$ である.
- (2) 任意の $g \in G$ に対し, 各 $u \in \text{supp}(g)$ について $u \notin \langle \text{LT}(G \setminus \{g\}) \rangle$ である.

注意 1.33. 簡約 Gröbner 基底は極小 Gröbner 基底の特別なものである.

定理 1.34 ([8] 定理 1.2.5). 任意のイデアル $I \subset K[X]$ に対し, I の簡約 Gröbner 基底は一意的に存在する.

証明. 簡約 Gröbner 基底が存在することを示す. I の極小 Gröbner 基底 $\{g_1, \dots, g_s\}$ をとる. まず, $H_1 = \{g_2, \dots, g_s\}$, $h_1 = \overline{g_1}^{H_1}$ とする. G は極小 Gröbner 基底ゆえ, 任意の $g_i \in H_1$ に対し $\text{LT}(g_i) \nmid \text{LT}(g_1)$ となるので

$$\text{LT}(h_1) = \text{LT}(g_1)$$

となる. よって,

$$\text{LT}(h_1) \notin \langle \text{LT}(H_1) \rangle$$

となるので, $\{h_1\} \cup H_1$ は極小 Gröbner 基底である. さらに, division algorithm の性質から, 任意の $g \in H_1$ と $u \in \text{supp}(h_1)$ に対して $\text{LT}(g) \nmid u$ である. 次に, $H_2 = \{h_1, g_3, \dots, g_s\}$ とし, $h_2 = \overline{g_2}^{H_2}$ とすると, 上と同様の議論により, $\{h_2\} \cup H_2$ は極小 Gröbner であり, 任意の $g \in H_2$ と $u \in \text{supp}(h_2)$ に対して $\text{LT}(g) \nmid u$ である. 同様に H_i と h_i を定義することで, I の簡約 Gröbner 基底 $\{h_1, \dots, h_s\}$ を得る.

次に, 簡約 Gröbner 基底の一意性を示す. I の簡約 Gröbner 基底 $G = \{g_1, \dots, g_s\}$, $\tilde{G} = \{\tilde{g}_1, \dots, \tilde{g}_t\}$ をとる. これらはいずれも単項式イデアル $\langle \text{LT}(I) \rangle$ の極小な生成系なので, 定理 1.27 より $s = t$ であり, \tilde{G} の番号を適当にいかえて

$$\text{LT}(g_i) = \text{LT}(\tilde{g}_i) \quad (1 \leq i \leq s)$$

とできる. あとは各 i に対して $g_i = \tilde{g}_i$ がわかればよいので, $g_i - \tilde{g}_i \neq 0$ として矛盾を導く. $u = \text{LT}(g_i - \tilde{g}_i)$ とする. まず, u の定義から $u \preceq \text{LT}(g_i)$ となるので

$$\text{LT}(g_i) \nmid u$$

である. また, 簡約 Gröbner 基底の定義より, $i \neq j$ のとき

$$\text{LT}(g_j) \nmid u$$

である. ここで, 補題 1.26 を用いると

$$u \notin \langle \text{LT}(I) \rangle$$

となり, $g_i - \tilde{g}_i \in I$ に矛盾する. □

注意 1.35. 定理 1.34 の存在性の証明は極小 Gröbner 基底から簡約 Gröbner を構成するアルゴリズムを示している. 実際にアルゴリズムとして記述すると次のようになる.

Algorithm 1.5 ReducedGroebnerBasis

Require: I の極小 Gröbner 基底 $G = \{g_1, \dots, g_s\}$

Ensure: I の簡約 Gröbner 基底

- 1: $H \leftarrow \emptyset$
 - 2: **for** $i = 1, \dots, s$ **do**
 - 3: $G \leftarrow G \setminus \{g_i\}$
 - 4: $h_i \leftarrow \overline{g_i}^{H \cup G}$
 - 5: $H \leftarrow \{h_i\} \cup H$
 - 6: **end for**
 - 7: **return** H
-

注意 1.36. 以上の Buchberger, MinimalGroebnerBasis, ReducedGroebnerBasis を組み合わせることにより、イデアルと単項式順序からその簡約 Gröbner 基底を得るアルゴリズムが構成できる。このアルゴリズムを ReducedGB で表すことにする。

定理 1.34 から、次が直ちに従う。

系 1.37. イデアル $I, J \subset K[X]$ に対して、 $I = J$ であることと I, J それぞれの簡約 Gröbner 基底が一致することは同値である。

この系により、イデアルの一致を判定するアルゴリズムが得られる。

Algorithm 1.6 IdealMatch

Require: イデアル $I, J \subset K[X]$

Ensure: $I = J$ の真偽

```

1:  $G_1 \leftarrow \text{ReducedGB}(I, \prec_{\text{grevlex}})$ 
2:  $G_2 \leftarrow \text{ReducedGB}(J, \prec_{\text{grevlex}})$ 
3: if  $G_1 = G_2$  then
4:   return true
5: else
6:   return false
7: end if
```

1.5 消去理論

前節までは n 個の変数 $X = (x_1, \dots, x_n)$ を順序対として定義していたが、以降では集合としての表記を許すことにする。例えば、変数の組 X に対して、その一部分からなる m 個の変数の組 $X' = (x_{i_1}, \dots, x_{i_m})$ ($1 \leq i_1 < \dots < i_m \leq n$) を $X' \subset X$ と表し、変数の組 $X = (x_1, \dots, x_m), Y = (y_1, \dots, y_n)$ (任意の i, j に対して $x_i \neq y_j$) に対して、 $X \cup Y = (x_1, \dots, x_m, y_1, \dots, y_n)$ と表す。また、 $P \subset K[X]$ に対して $P_{X'} := P \cap K[X']$ とし、

$$V(P) = \left\{ (a_1, \dots, a_n) \in \overline{K}^n \mid \text{任意の } f \in P \text{ に対して } f(a_1, \dots, a_n) = 0 \right\}$$

と定める。

注意 1.38. 変数の組 X とその一部からなる組 $X' \subset X$ に対して、 $M(X)$ 上の単項式順序 \prec を X' 上に制限した順序を $\prec_{X'}$ と表す。このとき、 $\prec_{X'}$ は $M(X')$ 上の単項式順序でもある。

定義 1.39. イデアル $I \subset K[X]$ と変数の組 $X' \subset X$ に対して、 $K[X']$ のイデアル $I_{X'}$ を I の X' による**消去イデアル** (elimination ideal) という。

定理 1.40 (消去定理). イデアル $I \in K[X]$ と単項式順序 \prec に関する I の Gröbner 基底 G をとる。任意の $g \in G$ に対して

$$\text{LT}(g) \in K[X'] \implies g \in K[X']$$

が成り立つならば、 $G_{X'}$ は $I_{X'}$ の $\prec_{X'}$ に関する Gröbner 基底である。

証明. 多項式 $f \in I_{X'}$ を任意にとる。このとき、 $\text{LT}(f) \in \text{LT}(I) \subset \langle \text{LT}(G) \rangle$ と補題 1.26 から、ある $g \in G$ が存在して

$$\text{LT}(g) \mid \text{LT}(f)$$

となる。ここで、 $\text{LT}(f) \in K[X']$ より $\text{LT}(g) \in K[X']$ であるので

$$g \in K[X']$$

となる。これにより,

$$\langle \text{LT}(I_{X'}) \rangle \subset \langle \text{LT}(G_{X'}) \rangle$$

が示された。逆は明らか。 \square

消去定理により, 次が直ちに得られる。この系は連立方程式を解くうえで重要である。

系 1.41. イデアル $I \in K[X]$ と辞書式順序 \prec_{lex} に関する I の Gröbner 基底 G について, $G_{X'}$ は $I_{X'}$ の \prec_{lex} に関する Gröbner 基底である。

例 1.42. $\mathbb{C}[x, y, z]$ の多項式

$$f_1 = x^2 + y + z - 1, \quad f_2 = x + y^2 + z - 1, \quad f_3 = x + y + z^2 - 1$$

に対して, 連立方程式 $f_1 = f_2 = f_3 = 0$ を解く。

$\mathbb{C}[x, y, z]$ 上の単項式順序を $x \succ y \succ z$ による辞書式順序 \prec_{lex} で定め, $I = \langle f_1, f_2, f_3 \rangle$ とする。このとき,

$$\begin{aligned} g_1 &= x + y + z^2 - 1, \\ g_2 &= y^2 - y - z^2 + z, \\ g_3 &= 2yz^2 + z^4 - z^2, \\ g_4 &= z^6 - 4z^4 + 4z^3 - z^2 \end{aligned}$$

とすると, $G := \{g_1, g_2, g_3, g_4\}$ は I の Gröbner 基底である。よって, 系 1.41 から, $I \cap \mathbb{C}[z]$ の Gröbner 基底は $\{g_4\}$, $I \cap \mathbb{C}[y, z]$ の Gröbner 基底は $\{g_2, g_3, g_4\}$ である。これにより,

$$V(I \cap \mathbb{C}[z]) = V(g_4), \quad V(I \cap \mathbb{C}[y, z]) = V(g_2, g_3, g_4).$$

ここで, $g_4 = z^2(z-1)^2(z^2+2z-1)$ なので,

$$V(I \cap \mathbb{C}[z]) = V(g_4) = 0, 1, -1 \pm \sqrt{2}.$$

よって, これらを g_2, g_3 に代入することで

$$V(I \cap \mathbb{C}[y, z]) = \{(0, 0), (1, 0), (0, 1), (-1 \pm \sqrt{2}, -1 \pm \sqrt{2})\}.$$

同様に, これらを g_1 に代入して

$$V(I) = \{(1, 0, 0), (0, 1, 0), (0, 0, 1), (-1 \pm \sqrt{2}, -1 \pm \sqrt{2}, -1 \pm \sqrt{2})\}.$$

定理 1.43 (拡張定理). イデアル $I = \langle f_1, \dots, f_s \rangle \subset \mathbb{C}[x_1, \dots, x_n]$ を考え, $I_1 = I \cap \mathbb{C}[x_1]$ とする。各 $h_i \in \mathbb{C}[x_2, \dots, x_n]$ を

$$f_i = h_i x_1^{N_1} + (x_1 \text{ の次数が } N_1 \text{ 未満の項})$$

で定める。部分解 $(a_2, \dots, a_n) \in V(I_1)$ に対して,

$$(a_2, \dots, a_n) \notin V(h_1, \dots, h_s)$$

ならば, ある $a_1 \in \mathbb{C}$ が存在して

$$(a_1, a_2, \dots, a_n) \in V(I).$$

例 1.44. $\mathbb{C}[x, y, z]$ の多項式

$$f_1 = xy - 1, \quad f_2 = xz - 1$$

に対して, 連立方程式 $f_1 = f_2 = 0$ を解く。

$S := \mathbb{C}[x, y, z]$ 上の単項式順序を $x \succ y \succ z$ による辞書式順序 \prec_{lex} で定め, $I = \langle f_1, f_2 \rangle$ とする. このとき,

$$g_1 = f_2, \quad g_2 = y - z$$

とすると, $G := \{g_1, g_2\}$ は I の Gröbner 基底である.

消去定理により

$$I_2 := I \cap \mathbb{C}[z] = \langle 0 \rangle, \quad I_1 := I \cap \mathbb{C}[y, z] = \langle g_2 \rangle.$$

よって,

$$V(I_2) = \mathbb{C}, \quad V(I_1) = \{(a, a) \mid a \in \mathbb{C}\}$$

である. ここで $h_1 = y, h_2 = z$ なので, 消去定理から

$(y, z) \neq (0, 0)$ のとき, 解

$$(x, y, z) = \left(\frac{1}{a}, a, a \right) \quad (a \in \mathbb{C})$$

が得られる. また, $(y, z) = (0, 0)$ のときは解は得られない. 以上より

$$V(I) = \left\{ \left(\frac{1}{a}, a, a \right) \mid a \in \mathbb{C} \setminus \{0\} \right\}$$

である.

1.6 Gröbner 基底計算の高速化

この節では, Buchberger アルゴリズムを改良して Gröbner 基底の計算を高速化する方法について述べる.

簡単のため, 以下では $f_i, f_j \in K[X]$ に対して,

$$S_{ij} = S(f_i, f_j), \quad T_{ij} = \text{lcm}(\text{LT}(f_i), \text{LT}(f_j))$$

とする.

1.6.1 不要な多項式ペアの検出

例 1.45. Buchberger アルゴリズムを用いて, $f_1 = x^2 + y^2 - 1, f_2 = x^3 + y^3 - 1$ と辞書式順序について, $I = \langle f_1, f_2 \rangle$ の Gröbner 基底を計算する. ただし, 多項式ペアの選択は normal strategy (後述) を用いる.

1. まず, $D = \{(1, 2)\}, G = \{f_1, f_2\}$ となる.

2. S_{12} について

$$S_{12} = xy^2 - x - y^3 + 1 \xrightarrow{G} xy^2 - x - y^3 + 1 (= f_3)$$

なので, $D = \{(1, 3), (2, 3)\}, G = \{f_1, f_2, f_3\}$ となる.

3. S_{13} について

$$S_{13} = x^2 + xy^3 - x + y^4 - y^2 \xrightarrow{G} xy - x + 2y^4 - 2y^2 - y + 1 (= f_4)$$

なので, $D = \{(2, 3), (1, 4), (2, 4), (3, 4)\}, G = \{f_1, f_2, f_3, f_4\}$ となる.

4. S_{34} について

$$S_{34} = xy - x - 2y^6 + y^3 + y^2 - y + 1 \xrightarrow{G} -2y^5 - 2y^4 + y^3 + 3y^2 (= f_5)$$

なので, $D = \{(2, 3), (1, 4), (2, 4), (1, 5), (2, 5), (3, 5), (4, 5)\}, G = \{f_1, f_2, f_3, f_4, f_5\}$ となる.

5. 残りのペアについては,

$$S_{35} \xrightarrow{G} 0, \quad S_{45} \xrightarrow{G} 0, \quad S_{14} \xrightarrow{G} 0, \quad S_{15} \xrightarrow{G} 0, \quad S_{24} \xrightarrow{G} 0, \quad S_{23} \xrightarrow{G} 0, \quad S_{25} \xrightarrow{G} 0$$

であるので, $G = \{f_1, f_2, f_3, f_4, f_5\}$ は I の Gröbner 基底である.

Buchberger アルゴリズムで S 多項式の余りが 0 になるかを確認する際に、割り算をせずにそれを判別できる場合がある。そのような多項式のペアを除去することにより、割り算の回数を減らすことで高速化が可能になる。まずは、その方法について述べる。

定義 1.46. 整数 k と $i < j$ に対して、条件 F, M, B を次で定める。

$$\begin{aligned} F_k(i, j) &\iff k < i, T_{kj} = T_{ij}. \\ M_k(i, j) &\iff k < j, \text{LT}(f_k) \mid T_{ij} \text{ かつ } T_{kj} \neq T_{ij}. \\ B_k(i, j) &\iff k > j, \text{LT}(f_k) \mid T_{ij} \text{ かつ } T_{ik} \neq T_{ij}, T_{kj} \neq T_{ij}. \end{aligned}$$

これに対し、次が成り立つ。

定理 1.47. $F = \{f_1, \dots, f_s\}$ について、次は同値である。

- (i) F は $\langle F \rangle$ の Gröbner 基底である。
- (ii) $P = \{(i, j) \mid 1 \leq i < j \leq s, \neg(\exists k \text{ s.t. } F_k(i, j) \vee M_k(i, j) \vee B_k(i, j))\}$ の任意の元 (i, j) に対し、 $S_{ij} \xrightarrow{G} 0$ である。

定義 1.48. $f_i, f_j \in K[X]$ に対して、条件 D を次で定める。

$$D(i, j) \iff \gcd(\text{LT}(f_i), \text{LT}(f_j)) = 1$$

定理 1.49. $f_i, f_j \in K[X]$, $G = \{f_i, f_j\}$ に対して、次が成り立つ。

$$D(i, j) \implies S_{ij} \xrightarrow{G} 0.$$

以上の二つの定理をもとに、Buchberger アルゴリズムの改良が考えられる。
まず、その中で用いる Update 関数を考える。

Algorithm 1.7 Update

Require: 添字のペアの集合 D , 多項式のリスト $F = \{f_1, \dots, f_m\}$, m

Ensure: 添字のペアの集合 D

- 1: $D \leftarrow D \setminus \{(i, j) \in D \mid B_{m+1}(i, j)\}$
 - 2: $D_{m+1} \leftarrow \{(i, m+1) \mid i = 1, \dots, m, \neg(\exists k = 1, \dots, i-1 \text{ s.t. } F_k(i, m+1))\}$
 $\cap \{(i, m+1) \mid i = 1, \dots, m, \neg(\exists k = 1, \dots, i-1, i+1, \dots, m \text{ s.t. } M_k(i, m+1))\}$
 $\cap \{(i, m+1) \mid i = 1, \dots, m, \neg D(i, m+1)\}$
-

これを多項式の追加時に利用するようにしたものが次のアルゴリズムである。

Algorithm 1.8 改良された Buchberger アルゴリズム

Require: $F = \{f_1, \dots, f_s\}$, 単項式順序 $<$

Ensure: $\langle F \rangle$ の Gröbner 基底

```
1:  $g_1 \leftarrow F$  の要素,  $F \leftarrow F \setminus \{g_1\}$ ,  $G \leftarrow \{g_1\}$ 
2:  $D \leftarrow \emptyset$ ,  $m \leftarrow 1$ 
3: while  $F \neq \emptyset$  do
4:    $g_{m+1} \leftarrow F$  の要素
5:    $F \leftarrow F \setminus \{g_{m+1}\}$ 
6:    $G \leftarrow G \cup \{g_{m+1}\}$ 
7:    $D \leftarrow \text{Update}(D, m)$ 
8:    $m \leftarrow m + 1$ 
9: end while
10:  $D \leftarrow \{(i, j) \mid 1 \leq i < j \leq s\}$ 
11:  $G \leftarrow F$ 
12: while  $D \neq \emptyset$  do
13:    $(i, j) \leftarrow D$  の要素
14:    $D \leftarrow D \setminus \{(i, j)\}$ 
15:    $r \leftarrow \overline{S_{ij}}^G$ 
16:   if  $r \neq 0$  then
17:      $g_{m+1} \leftarrow r$ 
18:      $G \leftarrow G \cup \{g_{m+1}\}$ 
19:      $D \leftarrow \text{Update}(D, m)$ 
20:      $G \leftarrow G \cup \{r\}$ 
21:   end if
22: end while
23: return  $G$ 
```

例 1.50. 改良された Buchberger アルゴリズムを用いて, 例 1.45 と同様の計算を行う.

1. まず, $D = \{(1, 2)\}$, $G = \{f_1, f_2\}$ となる.

2. S_{12} について

$$S_{12} = xy^2 - x - y^3 + 1 \xrightarrow{G} xy^2 - x - y^3 + 1 (= f_3)$$

なので, $D = \{(1, 3), (2, 3)\}$, $G = \{f_1, f_2, f_3\}$ となる. ここで $(2, 3)$ について $M_1(2, 3)$ なので, Update により $D = \{(1, 3)\}$ となる.

3. S_{13} について

$$S_{13} = x^2 + xy^3 - x + y^4 - y^2 \xrightarrow{G} xy - x + 2y^4 - 2y^2 - y + 1 (= f_4)$$

なので, $D = \{(1, 4), (2, 4), (3, 4)\}$, $G = \{f_1, f_2, f_3, f_4\}$ となる. ここで $(2, 4)$ について $M_1(2, 4)$ なので, Update により $D = \{(1, 4), (3, 4)\}$ となる.

4. S_{34} について

$$S_{34} = xy - x - 2y^6 + y^3 + y^2 - y + 1 \xrightarrow{G} -2y^5 - 2y^4 + y^3 + 3y^2 (= f_5)$$

なので, $D = \{(1, 4), (1, 5), (2, 5), (3, 5), (4, 5)\}$, $G = \{f_1, f_2, f_3, f_4, f_5\}$ となる. ここで $B_5(1, 4), F_3(4, 5), D(1, 5), D(2, 5)$ なので, Update により $D = \{(3, 5)\}$ となる.

5. 残りのペアについては,

$$S_{35} \xrightarrow{G} 0$$

であるので, $G = \{f_1, f_2, f_3, f_4, f_5\}$ は I の Gröbner 基底である.

1.6.2 多項式ペア選択の戦略

次に, S 多項式のペア選択の順番について述べる. Buchberger アルゴリズムの動作は計算する S 多項式の選び方の順番に大きく影響される. ここでは, その主要な戦略である normal strategy と sugar strategy の違いについて述べる.

定義 1.51. 単項式順序に関して T_{ij} が小さい順に (i, j) を選択する方法を **normal strategy** という.

sugar strategy を定義するために, 多項式の **sugar** を定義する.

定義 1.52. 多項式 f に対し, f の sugar $s(f)$ を次で定める.

(1) 入力された多項式のリスト $\{f_1, \dots, f_s\}$ に対して

$$s(f_i) = \text{tdeg}(f_i).$$

(2) 単項式 m と多項式 f に対して,

$$s(mf) = \text{tdeg}(m + s(f)).$$

(3) 多項式 f, g に対して,

$$s(f + g) = \max\{s(f), s(g)\}.$$

定義 1.53. S 多項式の sugar が (通常の整数の順序に関して) 小さいものから選択し, sugar が等しい場合は normal strategy で選択する方法を **sugar strategy** という.

注意 1.54. 多項式のペア選択の順番について, 次のことが知られている.

- normal strategy で多項式ペアの選択をする場合は \prec_{grlex} , \prec_{grevlex} などの次数つき順序のほうが高速である.
- sugar strategy は \prec_{lex} での計算を高速化するのに非常に有用である.

1.6.3 F_4 アルゴリズム

最後に F_4 アルゴリズムについて述べる.

まず, F_4 アルゴリズムの計算のために必要な定義を述べる.

定義 1.55. 相異なる単項式 $u_1, \dots, u_t \in M(S)$ (ただし, $u_1 \prec_{\text{revlex}} \dots \prec_{\text{revlex}} u_t$) と K 上の $s \times t$ 行列 $M = (m_{ij})_{1 \leq i \leq s, 1 \leq j \leq t}$ に対して, N の各列から定まる多項式の集合 $\text{rows}(N)$ を

$$\text{rows}(N) = \left\{ f_i = \sum_{j=1}^t m_{ij} u_j \mid 1 \leq i \leq s \right\}$$

で定義する.

これにより, 次のように F_4 アルゴリズムを表すことができ, 以下が成り立つ.

定理 1.56. 次のアルゴリズムは有限時間で停止し, 入力 $F \subset K[X]$ に対し $\langle F \rangle$ の Gröbner 基底を正しく出力する.

Algorithm 1.9 F_4 アルゴリズム

Require: $F = \{f_1, \dots, f_s\}$, 単項式順序 \prec **Ensure:** $\langle F \rangle$ の Gröbner 基底

```
1:  $G \leftarrow F$ 
2:  $t \leftarrow s$ 
3:  $B \leftarrow \{\{i, j\} \mid 1 \leq i < j \leq s\}$ 
4: while  $B \neq \emptyset$  do
5:    $B' \leftarrow$  空でない  $B$  の部分集合
6:    $B \leftarrow B \setminus B'$ 
7:    $L \leftarrow \left\{ \frac{\text{lcm}(\text{LM}(f_i), \text{LM}(f_j))}{\text{LT}(f_i)} f_i \mid \{i, j\} \in B' \right\}$ 
8:    $M \leftarrow \text{ComputeM}(L, G, \prec)$ 
9:    $N \leftarrow M$  の行簡約階段形
10:   $N^+ \leftarrow \{f \in \text{rows}(N) \mid \text{LM}(f) \notin \langle \text{LM}(\text{rows}(M)) \rangle\}$ 
11:  for  $f \in N^+$  do
12:     $t \leftarrow t + 1$ 
13:     $f_t \leftarrow f$ 
14:     $G \leftarrow G \cup \{f_t\}$ 
15:     $B \cup \{\{i, t\} \mid 1 \leq i < t\}$ 
16:  end for
17: end while
18: return  $G$ 
```

ただし、このアルゴリズムに登場する ComputeM は以下のアルゴリズムで表される。

Algorithm 1.10 ComputeM

Require: $L \subset K[X]$, $G = \{f_1, \dots, f_t\}$, 単項式順序 \prec **Ensure:** 行列 M

```
1:  $H \leftarrow L$ 
2:  $done \leftarrow \text{LM}(H)$ 
3: while  $done \neq \text{supp}(H)$  do
4:    $u \leftarrow \text{supp}(H) \setminus done$  の元で  $\prec$  に関して最大のもの
5:    $done \leftarrow done \cup \{u\}$ 
6:   if  $\text{LM}(f_i) \mid u$  なる  $f_i \in G$  が存在する then
7:      $f \leftarrow \text{LM}(f) \mid u$  なる  $G$  の元
8:      $H \leftarrow H \cup \left\{ \frac{u}{\text{LM}(f)} f \right\}$ 
9:   end if
10: end while
11:  $M \leftarrow H$  の係数からなる行列 (ただし、列は  $\prec$  に関する降順で並べる)
12: return  $M$ 
```

注意 1.57. 上で述べたアルゴリズムにおいて、 B' の取り方はとくに指定されていない。この取り方の戦略の一つとして、 $\text{lcm}(\text{LM}(f_i), \text{LM}(f_j))$ の全次数が極小のもの全てをとる方法がある。これは正規選択戦略と呼ばれる。

例 1.58 ([2] 第 10 章 §3 例 3). F_4 アルゴリズムによる計算の例として、

$$f_1 = x^2 + xy - 1, f_2 = x^2 - z^2, f_3 = xy + 1$$

に対して、 $x \succ y \succ z$ なる次数付き逆辞書式順序 \prec_{grevlex} による $I = \langle f_1, f_2, f_3 \rangle$ の Gröbner 基底を計算する。

まず, $G = \{f_1, f_2, f_3\}, t = 3, B = \{\{1, 2\}, \{1, 3\}, \{2, 3\}\}$ となる.

(i) $B' = \{\{1, 2\}\}$ をとると, $L = \{f_1, f_2\}$ である. この L に対し ComputeM を実行する.

$H = L$ であり,

$$\text{supp}(H) = \{x^2, xy, z^2, 1\}, \text{ done} = \{x^2\}$$

である. いま $\text{LM}(f_3) \mid xy$ なので

$$H = \{f_1, f_2, f_3\}$$

となり, 残りの $z^2, 1 \in \text{supp}(H) \setminus \text{done}$ についてはこれらを割り切る $\text{LM}(f_i)$ ($1 \leq i \leq 3$) は存在しない. よって,

$$M = \begin{pmatrix} 1 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

が出力される. これを行基本変形して,

$$N = \begin{pmatrix} 1 & 0 & 0 & -2 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & -2 \end{pmatrix}.$$

よって,

$$\text{rows}(N) = \{x^2 - 2, xy + 1, z^2 - 2\}.$$

したがって, $f_4 = z^2 - 2$ として,

$$G = \{f_1, f_2, f_3, f_4\}, B = \{\{1, 3\}, \{2, 3\}, \{1, 4\}, \{2, 4\}, \{3, 4\}\}.$$

(ii) $B' = \{\{1, 3\}, \{2, 3\}\}$ をとると, $L = \{yf_1, yf_2, xf_3\}$ である. この L に対し ComputeM を実行する.

$H = L$ であり,

$$\text{supp}(H) = \{x^2y, xy^2, yz^2, x, y\}, \text{ done} = \{x^2y\}$$

である. いま $\text{LM}(f_3) \mid xy^2$ なので

$$H = \{yf_1, yf_2, xf_3, yf_3\}$$

となり, 次に $\text{LM}(f_4) \mid yz^2$ なので

$$H = \{yf_1, yf_2, xf_3, yf_3, yf_4\}$$

となる. 残りの $x, y \in \text{supp}(H) \setminus \text{done}$ についてはこれらを割り切る $\text{LM}(f_i)$ ($1 \leq i \leq 4$) は存在しない. よって,

$$M = \begin{pmatrix} 1 & 1 & 0 & 0 & -1 \\ 1 & 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & -2 \end{pmatrix}$$

が出力される. これを行基本変形して,

$$N = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

よって,

$$\text{rows}(N) = \{x^2y + x, xy^2 + y, yz^2 + x, x + 2y\}.$$

したがって, $f_5 = x + 2y$ として,

$$G = \{f_1, f_2, f_3, f_4, f_5\}, B = \{\{1, 4\}, \{2, 4\}, \{3, 4\}, \{1, 5\}, \{2, 5\}, \{3, 5\}, \{4, 5\}\}.$$

(iii) $B' = \{\{1, 5\}, \{2, 5\}, \{3, 5\}\}$ をとると, $L = \{f_1, f_2, f_3, xf_5, yf_5\}$ である. この L に対し ComputeM を実行する.

$H = L$ であり,

$$\text{supp}(H) = \{x^2, xy, y^2, z^2, 1\}, \text{ done} = \{x^2, xy\}$$

である. いま $\text{LM}(f_4) \mid z^2$ なので

$$H = \{x^2, xy, y^2, z^2, 1, f_4\}$$

となる. 残りの $y^2, 1 \in \text{supp}(H) \setminus \text{done}$ についてはこれらを割り切る $\text{LM}(f_i)$ ($1 \leq i \leq 5$) は存在しない. よって,

$$M = \begin{pmatrix} 1 & 1 & 0 & 0 & -1 \\ 1 & 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 2 & 0 & 0 & 0 \\ 0 & 1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 1 & -2 \end{pmatrix}$$

が出力される. これを行基本変形して,

$$N = \begin{pmatrix} 1 & 0 & 0 & 0 & -2 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & -1/2 \\ 0 & 0 & 0 & 1 & -2 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

よって

$$\text{rows}(N) = \left\{ x^2 - 2, xy + 1, y^2 - \frac{1}{2}, z^2 - 2 \right\}.$$

したがって, $f_6 = y^2 - \frac{1}{2}$ として,

$$G = \{f_1, f_2, f_3, f_4, f_5, f_6\}, B = \{\{1, 4\}, \{2, 4\}, \{3, 4\}, \{4, 5\}, \{1, 6\}, \{2, 6\}, \{3, 6\}, \{4, 6\}, \{5, 6\}\}.$$

(iv) $B' = \{\{4, 5\}, \{3, 6\}, \{5, 6\}\}$ をとると, $L = \{xf_4, z^2f_5, yf_3, xf_6, y^2f_5\}$ である. この L に対し ComputeM を実行する.

$H = L$ であり,

$$\text{supp}(H) = \{xy^2, y^3, xz^2, yz^3, x, y\}, \text{ done} = \{xz^2, xy^2\}$$

である. いま $\text{LM}(f_6) \mid y^3, \text{LM}(f_4) \mid yz^2, \text{LM}(f_5) \mid f_5$ なので

$$H = \{xf_4, z^2f_5, yf_3, xf_6, y^2f_5, yf_6, yf_4, f_5\}$$

となる. 残りの $y \in \text{supp}(H) \setminus \text{done}$ についてはこれらを割り切る $\text{LM}(f_i)$ ($1 \leq i \leq 5$) は存在しない. よって,

$$M = \begin{pmatrix} 0 & 0 & 1 & 0 & -2 & 0 \\ 0 & 0 & 1 & 2 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & -1/2 & 0 \\ 1 & 2 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & -1/2 \\ 0 & 0 & 0 & 1 & 0 & -2 \\ 0 & 0 & 0 & 0 & 1 & 2 \end{pmatrix}$$

が出力される. これを行基本変形して,

$$N = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & -1/2 \\ 0 & 0 & 1 & 0 & -2 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

となる． よって, $N^+ = \emptyset$ なので多項式は追加されず,

$$G = \{f_1, f_2, f_3, f_4, f_5, f_6\}, \quad B = \{\{1, 4\}, \{2, 4\}, \{3, 4\}, \{1, 6\}, \{2, 6\}, \{4, 6\}\}.$$

(v) $B' = B$ をとると, (iv) の場合と同様に多項式は追加されないので

$$G = \{f_1, f_2, f_3, f_4, f_5, f_6\}$$

が I の Gröbner 基底である．

第2章

根基イデアルの計算と Gröbner 基底

イデアルに対して、その根基イデアルは次で定義されるものであった。

定義 2.1. イデアル $I \subset K[X]$ に対して、

$$\sqrt{I} := \{f \in I \mid \exists m \in \mathbb{N} \text{ s.t. } f^m \in I\}$$

で定義される \sqrt{I} を I の**根基イデアル** (radical ideal) という。

この章では、Gröbner 基底を用いて根基イデアル (の生成系) を計算する方法について述べる。

2.1 イデアルの次元

定義 2.2. I を $K[X]$ の固有イデアル, $Y \subset X$ とする. $I_Y = \langle 0 \rangle$ が成り立つとき, Y は I を法とする独立集合 (independent set modulo I) であるという. さらに, Y が I を法とする独立集合の中で (順序関係 \subset について) 極大であるとき, Y は I を法とする**極大独立集合** (maximal independent set modulo I) であるという. また, I の次元 (dimension) $\dim I$ を

$$\dim I = \max\{\#Y \mid Y \subset X : \text{independent modulo } I\}$$

で定義し, $\dim I = 0$ なるイデアル I を **0 次元イデアル** (0-dimensional ideal) という。

独立性に関する特徴付けを示すための, 簡単な補題を述べる。

補題 2.3. $Y \subset X$ とし, 単項式順序 \prec は $Y \ll X \setminus Y$ なるブロック順序とする. このとき, イデアル $I \subset K[X]$ に対して G が I の \prec に関する Gröbner 基底であるならば, G_Y は I_Y の Gröbner 基底である。

証明. $\text{LT}_\prec(g) \in K[Y]$ なる $g \in G$ を任意にとると, \prec の定義から任意の $v \in \text{supp}(g)$ に対して $v \in K[Y]$ となる. よって, 消去定理から主張は従う. \square

命題 2.4 ([1] Lemma 6.47). I を $K[X]$ の固有イデアル, $Y \subset X$ とし, 単項式順序 \prec は $Y \ll X \setminus Y$ なるブロック順序とする. このとき, 次が同値である.

- (i) Y は I を法として独立である.
- (ii) 任意の I の \prec に関する Gröbner 基底 G に対して, $G_Y = \emptyset$ が成り立つ.
- (iii) ある I の \prec に関する Gröbner 基底 G が存在して, $G_Y = \emptyset$ が成り立つ.

証明. (ii) \Rightarrow (iii) は明らか.

(i) \Rightarrow (ii) を示す. I の \prec に関する Gröbner 基底 G を任意にとると, 補題 2.3 から G_Y は I_Y の Gröbner 基底である. ここで (i) より $I_Y = \{0\}$ なので, $G_Y = \emptyset$ となる.

(iii) \Rightarrow (i) を示す. 消去定理と仮定から, $G_Y = \emptyset$ は I_Y の Gröbner 基底であるので,

$$I_Y = \langle \emptyset \rangle = \{0\}.$$

よって, Y は I を法として独立である. \square

例 2.5. 多項式環 $\mathbb{Q}[x, y, z]$ において

$$f_1 = xz + z, f_2 = yz + z$$

としてイデアル $I = \langle f_1, f_2 \rangle$ を考える. このとき, 任意の単項式順序に対して $\text{LT}(f_1) = xz, \text{LT}(f_2) = yz$ なので, $G = \{f_1, f_2\}$ とすると

$$S(f_1, f_2) = yf_1 - xf_2 = yz - xz = f_2 - f_1 \xrightarrow{G} 0$$

となって, G は I の Gröbner 基底である. このとき,

$$G \cap K[x_1] = G \cap K[x_2] = G \cap K[x_3] = G \cap K[x_1, x_2] = \emptyset$$

$$G \cap K[x_1, x_3], G \cap K[x_2, x_3] \neq \emptyset$$

なので,

$$\{x_1\}, \{x_2\}, \{x_3\}, \{x_1, x_2\}$$

は I を法として独立である.

2.2 0 次元イデアルの根基イデアルの計算

この節では K の標数は 0 とする.

定義 2.6. 1 変数多項式 $f \in K[x]$ が重複因子を持たないとき, f を**無平方** (square-free) という. また, f の分解

$$f = f_1^{e_1} \cdots f_s^{e_s} \quad (f_i \in K[x], e_i \in \mathbb{N})$$

について, 各 f_i が無平方かつ各ペア (f_i, f_j) が互いに素であり, さらに $e_1 < \cdots < e_s$ であるとき, この分解を**無平方分解** (square-free decomposition) という.

注意 2.7. 任意の 1 変数多項式に対して, その無平方分解は一意的に存在する.

定義 2.8. 1 変数多項式 $f \in K[x]$ に対し, $e_i \in \mathbb{N}$ と無平方な $f_i \in K[x]$ を用いて

$$f = f_1^{e_1} \cdots f_s^{e_s}$$

と書けるとき, 積 $f_1 \cdots f_s$ を f の**無平方部分** (square-free part) という.

補題 2.9. 1 変数多項式 $f \in K[x]$ が

$$f = f_1^{e_1} \cdots f_s^{e_s} \quad (f_i \in K[x], e_i \in \mathbb{N})$$

と無平方分解できるとき, f' を f の微分とすると

$$\gcd(f, f') = f_1^{e_1-1} \cdots f_s^{e_s-1}$$

が成り立つ.

証明. [24] 補題 4.3.5. を参照. □

この補題により, $f \in K[x]$ に対してその無平方部分を求めるアルゴリズムが得られる.

Algorithm 2.1 SquareFreePart

Require: $f \in K[x]$

Ensure: f の無平方部分

1: $g \leftarrow \gcd(f, f')$

2: **return** $\frac{f}{g}$

定理 2.10 (Seidenberg の補題). 0 次元イデアル $I \subset K[X]$ に対して, 各 $h_i \in K[x_i]$ を

$$\langle h_i \rangle = I \cap K[x_i]$$

なるものとして定める. h_i の無平方部分を g_i とすると

$$\sqrt{I} = I + \langle g_1, \dots, g_n \rangle$$

が成り立つ.

証明. [5] Proposition 4.5.1. を参照. □

この定理により, 0 次元イデアル I の生成系が与えられたとき, その根基 \sqrt{I} の生成系を計算するアルゴリズムが得られる.

Algorithm 2.2 ZeroDimensionalRadical

Require: 0 次元イデアル I の生成系 $\{f_1, \dots, f_s\} \subset K[X]$

Ensure: \sqrt{I} の生成系

- 1: **for** $i = 1, \dots, n$ **do**
 - 2: $\langle h_i \rangle = I \cap K[x_i]$ なる h_i を計算する.
 - 3: $g_i \leftarrow \text{SquareFreePart}(h_i)$
 - 4: **end for**
 - 5: **return** $\{f_1, \dots, f_s, g_1, \dots, g_n\}$
-

2.3 イデアルの 0 次元化

命題 2.11. イデアル $I, J \subset K[X]$ と新しい変数 y に対して,

$$I \cap J = (yI + (1 - y)J)_X$$

が成り立つ.

証明. [5] Lemma 1.8.10. を参照. □

この命題により, イデアルの共通部分を計算する以下のアルゴリズムが与えられる.

Algorithm 2.3 IdealIntersection

Require: $F = \{f_1, \dots, f_s\}, F' = \{f'_1, \dots, f'_t\} \subset K[X]$

Ensure: $\langle F \rangle \cap \langle F' \rangle$ の生成系

- 1: $yF \leftarrow \{yf_1, \dots, yf_s\}$
 - 2: $(1 - y)F' \leftarrow \{(1 - y)f'_1, \dots, (1 - y)f'_t\}$
 - 3: $L \leftarrow yF \cup (1 - y)F'$
 - 4: $G \leftarrow \langle L \rangle_{K[X, y]}$ の $X \gg y$ なる順序に関する Gröbner 基底
 - 5: **return** G_X
-

定義 2.12. イデアル $I \subset K[X]$ と集合 $F \subset K[X]$ に対して,

$$I : F = \{g \in K[X] \mid \forall f \in F, fg \in I\}$$

で定義される $I : F$ を I の F による**イデアル商** (ideal quotient) という. 特に F の元が 1 つ, すなわち $F = \{f\}$ のとき, $I : \{f\}$ を $I : f$ と略記する.

例 2.13. イデアル $\langle xz, yz \rangle \subset \mathbb{Q}[x, y, z]$ に対して,

$$\begin{aligned}\langle xz, yz \rangle : z &= \{g \in \mathbb{Q}[x, y, z] \mid zg \in \langle xz, yz \rangle\} \\ &= \langle x, y \rangle\end{aligned}$$

となる.

命題 2.14. イデアル $I, J \subset K[X]$ と集合 $F, G \subset K[X]$ に対して次が成り立つ.

- (i) $I : F$ は $K[X]$ のイデアル.
- (ii) $I : F = \bigcap_{f \in F} (I : f)$.
- (iii) $I \subset J, F \supset G$ ならば, $I : F \subset J : G$.
- (iv) $I : F = I : \langle F \rangle$.

証明.

(i) まず, $0 \in I : F$ なので $I : F \neq \emptyset$ である. また, $f_1, f_2 \in I : F$ と $h \in K[X]$ を任意にとると, 任意の $g \in F$ に対し,

$$(f_1 - f_2)g = f_1g - f_2g \in I, (f_1h)g = (f_1g)h \in I$$

なので, $I : F$ は $K[X]$ のイデアルである.

(ii) 任意の $g \in K[X]$ に対して,

$$g \in I : F \iff \forall f \in F, fg \in I \iff \forall f \in F, g \in I : f \iff g \in \bigcap_{f \in F} (I : f)$$

となるので, 成立する.

(iii) $g \in I : F$ を任意にとる. 定義より, 任意の $f \in G \subset F$ に対して $fg \in I \subset J$ なので, $g \in J : G$ である.

(iv) $I : F \supset I : \langle F \rangle$ となるのは (iii) より従う. また, $f \in I : F$ を任意にとる. このとき, 任意の $f_1h_1 + \cdots + f_sh_s \in \langle F \rangle$ ($f_i \in F, h_i \in K[X]$) に対して,

$$(f_1h_1 + \cdots + f_sh_s)g = (f_1g)h_1 + \cdots + (f_sg)h_s \in I$$

となるので,

$$f \in I : \langle F \rangle.$$

□

補題 2.15. イデアル $I \subset K[X]$ と多項式 $f \in K[X] \setminus \{0\}$ に対して

$$I : f = \frac{1}{f} \cdot (I \cap \langle f \rangle)$$

が成り立つ.

証明. [5] Lemma 1.8.12 を参照.

□

これにより次のアルゴリズムが得られる.

Algorithm 2.4 IdealQuotient

Require: $F = \{f_1, \dots, f_s\} \subset K[X]$, $f \in K[X]$ **Ensure:** $\langle F \rangle : f$ の生成系

```
1:  $G \leftarrow \text{IdealIntersection}(F, f)$ 
2:  $G' = \emptyset$ 
3: for all  $g \in G$  do
4:    $g' \leftarrow \frac{g}{f}$ 
5:    $G' \leftarrow G' \cup \{g'\}$ 
6: end for
7: return  $G'$ 
```

一般のイデアル商 $I : \{f_1, \dots, f_s\}$ を計算するためには, 命題 2.14(ii) から

$$I : \{f_1, \dots, f_s\} = (I : f_1) \cap \dots \cap (I : f_s)$$

となるので, 各 $I : f_i$ を計算してそれらの共通部分を求めればよい.

定義 2.16. イデアル $I \subset K[X]$ と多項式 $f \in K[X]$ に対して, 集合

$$\bigcup_{k \in \mathbb{N}} I : f^k$$

を I の f による**飽和イデアル** (saturation ideal) といい, $I : f^\infty$ で表す.

注意 2.17. 命題 2.14 (iv) より, イデアルの増大列

$$I : f \subset I : f^2 \subset \dots \subset I : f^k \subset \dots$$

が得られるが, $K[X]$ の Nöther 性から, ある $m \in \mathbb{N}$ があって,

$$I : f^m = I : f^{m+1} = \dots = I : f^\infty$$

が成り立つ.

命題 2.18. イデアル $I \subset K[X]$, 多項式 $f \in K[X]$, $m \in \mathbb{N}$ に対して, 次が同値:

- (i) $I : f^\infty = I : f^m$
- (ii) $I : f^m = I : f^{m+1}$

証明. (i) \Rightarrow (ii) は明らか. また, $I : f^\infty \supset I : f^m$ も明らか.

あとは, (ii) $\Rightarrow I : f^\infty \subset I : f^m$ を示せば良い. $g \in I : f^\infty$ を任意にとると, ある $k \in \mathbb{N}$ が存在して $f^k g \in I$ となる.

よって, $k \leq m$ のときは,

$$f^m g = f^{m-k} \cdot f^k g \in I$$

となり, $k > m$ のときは, (ii) を繰り返し用いることで

$$\begin{aligned} f^k g &= f^{m+1} \cdot f^{k-m-1} g \in I \\ \Rightarrow f^m \cdot f^{k-m-1} g &= f^{m+1} \cdot f^{k-m-2} g \in I \\ &\vdots \\ \Rightarrow f^m \cdot f g &= f^{m+1} \cdot f^0 g \in I \Rightarrow f^m g \in I \end{aligned}$$

となる. □

これにより次のアルゴリズムが得られる.

Algorithm 2.5 IdealSaturation

Require: $F = \{f_1, \dots, f_s\} \subset K[X]$, $f \in K[X]$

Ensure: $\langle F \rangle : f^\infty$ の生成系, $\langle F \rangle : f^m = \langle F \rangle : f^\infty$ なる $m \in \mathbb{N}$

```

1:  $m \leftarrow 0$ 
2:  $idealquotientmatch \leftarrow \mathbf{false}$ 
3:  $G_1 \leftarrow F$  の簡約 Gröbner 基底
4: while  $idealquotientmatch = \mathbf{true}$  do
5:    $F_2 \leftarrow \langle G_1 \rangle : f$  の生成系
6:    $G_2 \leftarrow F_2$  の簡約 Gröbner 基底
7:   if  $G_1 = G_2$  then
8:      $idealquotientmatch \leftarrow \mathbf{true}$ 
9:   else
10:     $G_1 \leftarrow G_2$ 
11:     $m \leftarrow m + 1$ 
12:   end if
13: end while
14: return  $(G_1, m)$ 

```

命題 2.19 ([1] Lemma 6.36). 多項式 $f \in K[X] \setminus \{0\}$ とイデアル $I \subset K[X]$, $J := I + \langle 1 - yf \rangle \subset K[X, y]$ に対して,

$$I : f^\infty = J_X$$

が成り立つ.

証明. (⊂) $g \in I : f^\infty$ を任意にとると, ある $m \in \mathbb{N}$ が存在して $f^m g \in I \subset J$ となる. これと, $1 - yf \in J$ より $y^m f^m \equiv 1 \pmod{J}$ とできることから,

$$g \equiv y^m f^m g \equiv 0 \pmod{J}$$

となる. よって, $g \in J_X$ である.

(⊃) $g \in J_X$ を任意にとると,

$$g = pq + (1 - yf)\tilde{q} \quad (p \in I, q, \tilde{q} \in K[X, y])$$

と表せる. ここで写像

$$\sigma_f : K[X, y] \rightarrow K(X); F(X, y) \mapsto F\left(X, \frac{1}{f}\right)$$

を定義すると,

$$g = \sigma_f(g) = p(X)q\left(X, \frac{1}{f}\right) \in K[X]$$

であるので, $d := \deg_y q$ とすると $f^d g \in I$ となる. □

定義 2.20. イデアル $I \in K[X]$ と集合 $Y \subset X$ に対して, I の Y についての**拡張** (extension) を

$$I^{\text{ext}(Y)} = \langle f \mid f \in I \rangle_{K(Y)[X \setminus Y]}$$

で定める. また, イデアル $J \in K(Y)[X \setminus Y]$ に対して, J の**縮約** (contraction) を

$$J^{\text{cont}} = J \cap K[X]$$

で定める.

注意 2.21. イデアル $I \in K[X]$ と集合 $Y \subset X$ に対して, $I^{\text{ext}(Y)}$ の Gröbner 基底は $Y \ll X \setminus Y$ なるブロック順序に関する I の Gröbner 基底を計算することで求められる. 詳細は補題 3.12 を参照.

命題 2.22. イデアル $I \subset K[X]$ と I を法とする極大独立集合 $Y \subset X$ について次が成り立つ.

(1) $I^{\text{ext}(Y)}$ は 0 次元イデアルである.

(2) $I^{\text{ext}(Y)}$ の Gröbner 基底 $G = \{g_1, \dots, g_s\} \subset K[X]$ について, $h = \text{lcm}(\text{LC}(g_1), \dots, \text{LC}(g_s))$ とするとき,

$$(I^{\text{ext}(Y)})^{\text{cont}} = I : h^\infty$$

が成り立つ.

証明. (1) 空でない $V \subset X \setminus Y$ を任意にとる. このとき, Y の極大性より,

$$(I^{\text{ext}(Y)}) \cap (K(Y))[V] \supset I \cap K[Y \cup V] \supsetneq \{0\}$$

となる. よって, $I^{\text{ext}(Y)}$ を法とする極大独立集合は存在しない. したがって, $\dim(I^{\text{ext}(Y)}) = 0$ である.

(2) まず, $f \in I : h^\infty$ を任意にとると, ある $m \in \mathbb{N}$ があって $fh^m \in I$ となる. ここで定義から $h^m \in K[Y] \setminus \{0\}$ なので

$$f \in \frac{1}{h^m} I \subset I^{\text{ext}(Y)}$$

となる. さらに $f \in K[X]$ なので, $f \in (I^{\text{ext}(Y)})^{\text{cont}}$ となる.

逆に, $f \in (I^{\text{ext}(Y)})^{\text{cont}}$ を任意にとる. division algorithm を用いて f を G で簡約すると, ある $p_i \in K[X], q_i \in K[Y]$ があって

$$f = \frac{p_1}{q_1} g_1 + \dots + \frac{p_s}{q_s} g_s$$

と表せて, さらに各 i に対して $q_i \mid \text{LC}(g_i)$ が成り立つ. よって, 十分大きい $m \in \mathbb{N}$ について $fh^m \in I$ となるので, $f \in I : h^\infty$ となる. \square

Algorithm 2.6 ReductionToZero

Require: $F = \{f_1, \dots, f_s\} \subset K[X]$

Ensure: $Y : \langle F \rangle$ の極大独立集合, $G : \langle F \rangle^{\text{ext}(Y)}$ の Gröbner 基底, $h : (\langle F \rangle^{\text{ext}(Y)})^{\text{cont}} = \langle F \rangle : h$ なる $h \in K[Y]$

1: $Y \leftarrow \langle F \rangle$ の極大独立集合

2: $X' \leftarrow X \setminus Y$

3: $G \leftarrow \langle F \rangle$ の $Y \ll X'$ なる順序に関する Gröbner 基底

4: $h_0 \leftarrow \prod_{g \in G} \text{LC}(g)$

5: $(G_1, m) \leftarrow \text{IdealSaturation}(G, h_0)$

6: $h \leftarrow h_0^m$

7: **return** (Y, G, h)

注意 2.23. 上のアルゴリズムでは $(\langle F \rangle^{\text{ext}(Y)})^{\text{cont}}$ の計算のために

$$h_0 = \prod_{g \in G} \text{LC}(g)$$

で定めた h_0 について $\langle F \rangle : h_0^\infty$ を計算している. これは, 命題 2.22 の証明において h について必要な条件は

- $h \in K[Y] \setminus \{0\}$ である.
- 任意の $g_i \in G$ に対して, $\text{LC}(g_i) \mid h$ が成り立つ.

のみであるため正当化される.

2.4 根基イデアルの計算

補題 2.24 (splitting tool). イデアル $I \subset K[X]$ と $f \in K[X]$ に対して, $I : f = I : f^2$ が成り立つならば

$$I = (I : f) \cap (I + \langle f \rangle)$$

が成り立つ.

証明. (⊂) これは $I \subset I : f$, $I \subset I + \langle f \rangle$ から明らか.

(⊃) 任意の $g \in (I : f) \cap (I + \langle f \rangle)$ に対して, ある $h_1 \in I, h_2 \in K[X]$ が存在して $g = h_1 + fh_2$ となる. このとき, $g \in I : f$ から

$$f^2 h_2 = fh_1 - fg \in I$$

なので, $h_2 \in I : f^2 = I : f$ である. よって,

$$g = h_1 + fh_2 \in I$$

となる. □

この補題と根基イデアルの性質から, $I : h = I : h^\infty$ なる h に対して,

$$\sqrt{I} = \sqrt{I : h} \cap \sqrt{I + \langle h \rangle}$$

であり, $\sqrt{I : h}$ の計算は ZeroDimensionalRadical を用いればよい. これにより, 次のアルゴリズムが得られる.

Algorithm 2.7 Radical

Require: $F = \{f_1, \dots, f_s\} \subset K[X]$

Ensure: $\sqrt{\langle F \rangle}$ の生成系

- 1: $(Y, G, h) \leftarrow \text{ReductionToZero}(F)$
 - 2: $J \leftarrow \text{ZeroDimensionalRadical}(G)$ (ただし, ここでの環は $K(Y)[X \setminus Y]$ として考える.)
 - 3: $\mathcal{G} \leftarrow J$ の Gröbner 基底
 - 4: $p \leftarrow \prod_{g \in \mathcal{G}} \text{LC}(g)$
 - 5: $H \leftarrow \text{IdealSaturation}(\mathcal{G}, p)$
 - 6: **return** $\text{Intersection}(H, \text{Radical}(F \cup \{h\}))$
-

第 3 章

包括的 Gröbner 基底系

以降, 体 K に対して \overline{K} を K の代数閉包とする. また, m 個のパラメータの組 $U = (u_1, \dots, u_m)$ および n 個の変数の組 $X = (x_1, \dots, x_n)$ に対して, 多項式環 $K[u_1, \dots, u_m][x_1, \dots, x_n]$ を $K[U][X]$ で略記する.

3.1 包括的 Gröbner 基底系

まず, 包括的 Gröbner 基底系と包括的 Gröbner 基底の定義を述べるために必要な定義をする.

定義 3.1. 集合 $S \subset \overline{K}^m$ について, ある有限集合 $P, Q \subset K[U]$ が存在して

$$S = V(P) \setminus V(Q)$$

となるとき, S は**構成的** (constructible) であるという.

定義 3.2. $a = (a_1, \dots, a_m) \in \overline{K}^m$ によって定まる自然な環準同型

$$\pi_a : K[U] \rightarrow \overline{K} ; c(U) \mapsto c(a)$$

について, その自然な拡張

$$\pi_a : K[U][X] \rightarrow \overline{K}[X] ; \sum_d c(U)X^d \mapsto \sum_d c(a)X^d$$

を a による**特殊化** (specialization) という.

定義 3.3. イデアル $I \subset K[U][X]$, $S \subset \overline{K}^m$ と単項式順序 \prec を固定する. 有限集合 $G_i \subset K[U][X]$ と $S_i \subset \overline{K}^m$ ($i = 1, \dots, l$) について次が成り立つとき, $\{(S_i, G_i)\}_{i=1, \dots, l}$ は S における I の**包括的 Gröbner 基底系** (comprehensive Gröbner system) という.

(1) 各 S_i は構成的であり,

$$S = \bigcup_{i=1}^l S_i.$$

(2) 任意の $a \in S_i$ に対して, $\pi_a(G_i)$ は $\langle \pi_a(I) \rangle$ の \prec に関する Gröbner 基底である.

(3) 任意の $a \in S_i$ と $g \in G_i$ に対して, $\pi_a(\text{LC}(g)) \neq 0$ が成り立つ.

また, 各 S_i を S の**分割部** (segment) という. 特に $S = \overline{K}^m$ のとき, $\{(S_i, G_i)\}_{i=1, \dots, l}$ は単に I の包括的 Gröbner 基底系という.

以降, 包括的 Gröbner 基底系を CGS と呼ぶ. 構成的な S は $S = V(P) \setminus V(Q)$ なる有限集合のペア $(P, Q) \subset K[U]^2$ と同一視できるので, CGS を次のようにも定義できる.

定義 3.4. 定義 3.3 と同様の仮定のもとで, 有限集合 $G_i \subset K[U][X]$, $P_i, Q_i \subset K[U]$ ($i = 1, \dots, l$) について $\{(V(P_i) \setminus V(Q_i), G_i)\}_{i=1, \dots, l}$ が S における I の CGS であるとき, $\{(P_i, Q_i, G_i)\}_{i=1, \dots, l}$ は S における I の CGS という. 特に $S = \overline{K}^m$ のとき, $\{(S_i, G_i)\}_{i=1, \dots, l}$ は単に I の CGS という.

定義 3.5. S における I の CGS $\{(S_i, G_i)\}_{i=1,\dots,l}$ について, 各 i に対して $G_i \subset I$ となるとき, $\{(S_i, G_i)\}_{i=1,\dots,l}$ は**忠実** (faithful) であるという.

定義 3.6. S における I の CGS $\{(S_i, G_i)\}_{i=1,\dots,l}$ について, 各 i に対して次の (1)(2) が成り立つとき $\{(S_i, G_i)\}_{i=1,\dots,l}$ は**極小** (minimal) であるという.

(1) $\{S_i\}_{i=1,\dots,l}$ は互いに素である.

(2) 任意の $a \in S_i$ に対して, $\pi_a(G_i)$ は $\langle \pi_a(I) \rangle$ の極小 Gröbner 基底である.

さらに, (2) において $\pi_a(G_i)$ が $\langle \pi_a(I) \rangle$ の簡約 Gröbner 基底であるとき, $\{(S_i, G_i)\}_{i=1,\dots,l}$ は**簡約** (reduced) であるという.

例 3.7. パラメータ付き多項式環 $\mathbb{Q}[t][x, y]$ と $x \succ y$ に関する単項式順序 \prec_{lex} を考え,

$$F = \{tx + y^2 - 1, y^3 - 1\}$$

とする. このとき,

$$S_1 = \{0\}, S_2 = \overline{\mathbb{Q}} \setminus \{0\}, G_1 = \{y - 1\}, G_2 = F$$

とおくと, $\{(S_i, G_i)\}_{i=1,2}$ は $\overline{\mathbb{Q}}$ における $\langle F \rangle$ の CGS である.

実際,

$$S_1 = \{0\} \setminus \emptyset = V(t) \setminus V(1), S_2 = \overline{\mathbb{Q}} \setminus \{0\} = V(0) \setminus V(t)$$

なので, S_1, S_2 は構成的であり,

$$\pi_a(\text{LC}(y - 1)) = 1 \ (\forall a \in S_1), \ \pi_a(\text{LC}(tx + y^2 - 1)) = a, \ \pi_a(\text{LC}(y^3 - 1)) = 1 \ (\forall a \in S_2)$$

である. また, 任意の $a \in S_1$ に対して, $\pi_a(G_1) = \{y - 1\}, \pi_a(F) = \{y^2 - 1, y^3 - 1\}$ であり,

$$\langle \text{LT}(y - 1) \rangle = \langle \text{LT}(\langle y^2 - 1, y^3 - 1 \rangle) \rangle$$

なので, $\pi_a(G_1)$ は $\langle \pi_a(F) \rangle$ の Gröbner 基底である. 同様に, 任意の $a \in S_2$ に対して, $\pi_a(G_2) = \pi_a(F) = \{ax + y^2 - 1, y^3 - 1\}$ であり,

$$S(ax + y^2 - 1, y^3 - 1) \xrightarrow{F} 0$$

なので, $\pi_a(G_2)$ は $\langle \pi_a(F) \rangle$ の Gröbner 基底である. 以上により, $\{(S_i, G_i)\}_{i=1,2}$ は $\langle F \rangle$ の CGS である. また,

$$\tilde{G}_2 = \left\{ x + \frac{1}{t}y^2 - \frac{1}{t}, y^3 - 1 \right\}$$

とすると $\{(S_1, G_1), (S_2, \tilde{G}_2)\}$ は $\langle F \rangle$ の reduced CGS である. さらに

$$\tilde{G}_1 = \{-txy + y - 1\} \subset \langle F \rangle$$

とすると $\{(S_1, \tilde{G}_1), (S_2, G_2)\}$ は $\langle F \rangle$ の忠実な CGS である.

定義 3.8. イデアル $I \subset K[U][X]$, 集合 $S \subset \overline{K}^m$ と単項式順序 \prec を固定する. 有限集合 $G \subset K[U][X]$ について, 任意の $a \in S$ に対して $\pi_a(G)$ は $\langle \pi_a(I) \rangle$ の \prec に関する Gröbner 基底であるとき, G は S における I の**包括的 Gröbner 基底** (comprehensive Gröbner basis) という.

特に $S = \overline{K}^m$ のとき, G は単に I の包括的 Gröbner 基底という.

以降, 包括的 Gröbner 基底を CGB と呼ぶ.

定義 3.9. S における I の CGB G について, $G \subset I$ となるとき G は**忠実** (faithful) であるという.

命題 3.10. $\mathcal{G} = \{(S_i, G_i)\}_{i=1,\dots,l}$ を S における I の忠実な CGS とする. このとき,

$$G := \bigcup_{i=1}^l G_i$$

は S における I の忠実な CGB である.

証明. $a \in S$ を任意にとる. このとき, ある $1 \leq i \leq l$ が存在して $a \in S_i$ となる. まず, \mathcal{G} は CGS なので, $\pi_a(G_i)$ は $\langle \pi_a(I) \rangle$ の Gröbner 基底である. また, \mathcal{G} の忠実性から $G \setminus G_i \subset I$ なので,

$$\pi_a(G \setminus G_i) \subset \pi_a(I)$$

である. これにより, $\pi_a(G) \supset \pi_a(G_i)$ は $\langle \pi_a(I) \rangle$ の Gröbner 基底である. □

例 3.11. 上の命題により, 例 3.7 と同様の仮定のもとでは

$$G = G_1 \cup G_2 = \{-txy + y - 1, tx + y^2 - 1, y^3 - 1\}$$

は $\langle F \rangle$ の忠実な CGB である.

3.2 鈴木-佐藤アルゴリズム

まず, 逆ブロック順序に関する性質を述べる.

補題 3.12 ([1] Lemma 8.93). U に関する逆ブロック順序 \prec とその $M(X)$ への制限 \prec_X を考える. 有限集合 $G \subset K[U][X]$ を $\langle G \rangle_{K[U][X]}$ の \prec に関する Gröbner 基底となるようにとると, G は $\langle G \rangle_{K(U)[X]}$ の \prec_X に関する Gröbner 基底である.

証明. $I = \langle G \rangle_{K[U][X]}$, $J = \langle G \rangle_{K(U)[X]}$ とする. まず, 任意の $f \in J$ に対して, ある $g \in G$ が存在して, $\text{LM}_{\prec_X}(g) \mid \text{LM}_{\prec_X}(f)$ となることを示す.

$f \in J$ を任意にとると, ある $q \in K[U]$ が存在して $qf \in I$ となる. ここで, G は I の Gröbner 基底なので, ある $g \in G$ が存在して

$$\text{LT}_{\prec}(g) \mid \text{LT}_{\prec}(qf)$$

よって,

$$\text{LM}_{\prec_X}(g) \mid \text{LM}_{\prec_X}(qf)$$

さらに, $q \in K[U]$ なので,

$$\text{LM}_{\prec_X}(qf) = \text{LM}_{\prec_X}(f)$$

となり示された.

これにより, 任意の $f \in J$ に対して $\text{LT}_{\prec_X}(f) \in \langle \text{LT}_{\prec_X}(G) \rangle_{K(U)[X]}$ となるので

$$\langle \text{LT}_{\prec_X}(G) \rangle_{K(U)[X]} = \langle \text{LT}_{\prec_X}(J) \rangle_{K(U)[X]}$$

が成り立つ. □

次に, Gröbner 基底の安定性について述べる.

定義 3.13. イデアル $I \subset K[U][X]$ を考える. 特殊化 $\pi : K[U][X] \rightarrow \overline{K}[X]$, $M(X)$ 上の順序 \prec について,

$$\langle \text{LT}_{\prec}(\pi(I)) \rangle = \langle \pi(\text{LT}_{\prec}(I)) \rangle$$

が成り立つとき, I は π と \prec に関して**安定** (stable) であるという.

Kalkbrener は [9] で次の重要な Gröbner 基底の安定性の特徴付けを示した.

定理 3.14 ([9] Theorem 3.1). イデアル $I \subset K[U][X]$, $M(X)$ 上の順序 \prec , $a \in \overline{K}^m$ による特殊化 $\pi_a : K[U][X] \rightarrow \overline{K}[X]$ を固定する. I の \prec に関する Gröbner 基底を $G = \{g_1, \dots, g_s\}$ とする. ただし, 各 g_i は

$$\pi_a(g_i) \neq 0 \quad (1 \leq \forall i \leq r), \quad \pi_a(g_i) = 0 \quad (r+1 \leq \forall i \leq s)$$

を満たすように並べる. このとき, 以下が同値である.

- (1) I は π_a と \prec に関して安定である.
- (2) $\pi_a(\{g_1, \dots, g_r\})$ は $\langle \pi_a(I) \rangle$ の \prec に関する Gröbner 基底である.
- (3) 任意の $g_i \in \{g_{r+1}, \dots, g_s\}$ に対して, $\overline{\pi_a(g)}^{\pi_a(\{g_1, \dots, g_r\})} = 0$.

補題 3.12 と定理 3.14 から次の系がただちに得られる.

系 3.15. U に関する逆ブロック順序 \prec とその $M(X)$ 上への制限 \prec_X を定め, $F \subset K[U, X]$ をとる. また, G を $\langle F \rangle$ の \prec に関する Gröbner 基底とする. このとき, 任意の $a \in V(G \cap K[U]) \setminus V(\text{LC}_{\prec_X}(G \setminus K[U]))$ に対して, $\pi_a(G \setminus K[U])$ は $\langle \pi_a(\langle F \rangle) \rangle$ の \prec_X に関する Gröbner 基底である.

[20] で示された次の鈴木-佐藤アルゴリズムにより, CGS を求めることができる. このアルゴリズムの正当性は系 3.15 から得られる.

Algorithm 3.1 SS-CGS

Require: 有限集合 $F \subset K[U][X]$, U に関する逆ブロック順序 \prec

Ensure: $\langle F \rangle$ の \prec に関する CGS $\mathcal{G} = \{(P, Q, G)\}_i$

- 1: $G_0 \leftarrow \text{GroebnerBasis}(F, \prec)$
 - 2: $\mathcal{G} \leftarrow (\emptyset, G_0 \cap K[U], \{1\})$
 - 3: $\mathcal{H} \leftarrow \text{CGSMain}(F, \prec)$
 - 4: **for** each $(h, G) \in \mathcal{H}$ **do**
 - 5: $\mathcal{G} \leftarrow \mathcal{G} \cup \{(G \cap K[U], \{h\}, G \setminus K[U])\}$
 - 6: **end for**
 - 7: **return** \mathcal{G}
-

Algorithm 3.2 CGSMain

Require: 有限集合 $F \subset K[U][X]$, U に関する逆ブロック順序 \prec

Ensure: 多項式と Gröbner 基底のペア $\mathcal{H} = \{(h, G)\}_i$

- 1: $G \leftarrow \text{GroebnerBasis}(F, \prec)$
 - 2: **if** $G \cap K[U] \neq \emptyset$ **then**
 - 3: $\mathcal{H} \leftarrow \{(1, G)\}$
 - 4: **else**
 - 5: $\{h_1, \dots, h_l\} \leftarrow \{\text{LC}_{\prec_X}(g) \mid g \in G \setminus K[U]\}$
 - 6: $h \leftarrow \text{lcm}(h_1, \dots, h_l)$
 - 7: $\mathcal{H} \leftarrow \{(h, G)\} \cup \text{CGSMain}(G \cup \{h_1\}) \cup \dots \cup \text{CGSMain}(G \cup \{h_l\})$
 - 8: **end if**
 - 9: **return** \mathcal{H}
-

上は $\langle F \rangle$ の \prec に関する CGS を計算するアルゴリズムだが, $S \subset \overline{K}^m$ における CGS を計算するためにはこのアルゴリズムの出力 $\{(P_i, Q_i, G_i)\}_i$ に対して $\{(S \cap V(P_i) \setminus V(Q_i), G_i)\}_i$ を計算すればよい.

例 3.16. 例 3.7 と同様の仮定のもとで, 鈴木-佐藤アルゴリズムを用いて $\langle F \rangle$ の CGS を計算する.

$f_1 = tx + y^2 - 1, f_2 = y^3 - 1$ とする. このとき, $G = \{f_1, f_2\}$ であり,

$$\{\text{LC}_{\prec}(g) \mid g \in G \setminus \mathbb{Q}[U]\} = \{t, 1\}$$

なので, $h = h_1 = t, h_2 = 1$ となる. よって,

$$\mathcal{H} = \{(h, G)\} \cup \text{CGSMain}(G \cup \{h_1\}) \cup \text{CGSMain}(G \cup \{h_2\}).$$

次に $\text{CGSM}_{\text{Main}}(G \cup \{h_1\}), \text{CGSM}_{\text{Main}}(G \cup \{h_2\})$ を計算する. $\text{CGSM}_{\text{Main}}(G \cup \{h_1\}) = \text{CGSM}_{\text{Main}}(\{f_1, f_2, h_1\})$ について, $f_3 = y - 1$ とすると $G = \{f_3, h_1\}$ なので $\mathcal{H} = \{(1, G)\}$ である. 同様に $\text{CGSM}_{\text{Main}}(G \cup \{h_2\}) = \text{CGSM}_{\text{Main}}(\{f_1, f_2, h_2\})$ について, $G = \{1\}$ であり $\mathcal{H} = \{(1, G)\}$ である. 以上より,

$$\mathcal{H} = \{(t, \{f_1, f_2\}), (1, \{f_3, t\}), (1, \{1\})\}$$

であり,

$$\mathcal{G} = \{(\emptyset, \emptyset, \{1\}), (\emptyset, \{t\}, \{f_1, f_2\}), (\{t\}, \{1\}, \{f_3\}), (\{1\}, \{1\}, \emptyset)\}$$

となる. これにより, CGS

$$(V(\emptyset) \setminus V(t), F), (V(t) \setminus V(1), \{y - 1\}))$$

を得る.

第 4 章

parametric イデアルの根基と CGS

この章では係数体 K の標数は 0 とする.

4.1 parametric イデアルに対する操作の安定性

R を環とする. 有限個のイデアル $I_1, \dots, I_l \subset R$ に対して, 新しいイデアル $I \subset R$ を対応させる操作 $\mathcal{F} : (I_1, \dots, I_l) \mapsto I$ を**イデアル操作** (ideal operation) という. 例えばイデアル $I, J \subset R$ に対するイデアルの和 $I + J$ や積 IJ はイデアル操作といえる.

定義 4.1. parametric イデアル $I_1, \dots, I_l \subset K[U][X]$, イデアル操作 \mathcal{F} , 構成的集合 $S \subset \overline{K}^m$ に対して, 構成的集合 $S_1, \dots, S_r \subset \overline{K}^m$ と有限集合 $G_1, \dots, G_r \subset K[U][X]$ からなる組 $(S_i, G_i)_{i=1, \dots, r}$ が次を満たすとき I_1, \dots, I_l の \mathcal{F} に関する**包括的系** (comprehensive system) という.

(i) $\{S_1, \dots, S_r\}$ は S の被覆である, すなわち

$$S = \bigcup_{i=1}^r S_i$$

が成り立つ. (ii) 任意の $a \in S_i$ に対して

$$\pi_a(G_i) = \mathcal{F}(\pi_a(I_1), \dots, \pi_a(I_l))$$

が成り立つ.

4.2 parametric イデアルの次元と 0 次元 parametric イデアルの根基

定義 4.2. parametric イデアル $I \subset K[U][X]$ と構成的集合 $S \subset \overline{K}^m$ に対して, $Y \subset X$ が任意の $a \in S$ に対して $\pi_a(I)$ を法とする極大独立集合であるとき, Y は S における I を法とする**安定な極大独立集合** (stable maximal independent set modulo I) という. また, 任意の $a \in S$ に対して $\dim \pi_a(I)$ が等しい値をとるとき, その値を I の S における**安定な次元** (stable dimension) といい, $\dim I$ で表す. S における安定な次元について $\dim I = 0$ であるとき, I を S における**0 次元イデアル** (0-dimensional ideal) という. \overline{K}^m における 0 次元イデアルを単に 0 次元イデアルという.

安定な極大独立集合の系は次のアルゴリズムで計算できる.

Algorithm 4.1 ParametricMaximalIndependentSet

Require: $F = \{f_1, \dots, f_s\} \in K[U][X]$, 構成的集合 $S \subset \overline{K}^m$

Ensure: 以下からなる系 $\{(S_i, G_i, Y_i)\}_{i=1, \dots, r}$

- 構成的集合 $S_i \subset \overline{K}^m$
- S_i における CGB G_i
- S_i における $\langle G_i \rangle$ を法とする安定な極大独立集合 Y_i

1: $\{(S_i, G_i)\}_{i=1, \dots, r} \leftarrow \text{CGS}(F, S, \prec)$

2: $\mathcal{G} \leftarrow \emptyset$

3: **for** $i = 1, \dots, r$ **do**

4: $Y_i \leftarrow G_i$ の極大独立集合

5: $\mathcal{G} \leftarrow \mathcal{G} \cup (S_i, G_i, Y_i)$

6: **end for**

7: **return** \mathcal{G}

定義 4.3. 1 変数 parametric 多項式 $f, h \in K[U][x]$ と構成的集合 $S \subset \overline{K}^m$ について, 任意の $a \in S$ に対して $\pi_a(h)$ が $\pi_a(f)$ の無平方部分であるとき, h は S における f の**安定な無平方部分** (stable square-free part) であるという.

補題 2.9 を parametric イデアルに対しても用いることにより, 次のアルゴリズムが得られる.

Algorithm 4.2 ParametricSquareFreePart

Require: $f \in K[U][x]$, 構成的集合 $S \subset \overline{K}^m$

Ensure: 以下からなる系 $\{(S_k, h_k)\}_k$

- 構成的集合 $S_k \subset \overline{K}^m$
- S_k における f の安定な無平方部分 h_k

1: $\{(S_i, \{g_i\})\}_{i=1, \dots, r} \leftarrow \text{CGS}(\{f, f'\}, S, \prec)$

2: **return** $\left\{ \left(S_i, \frac{f}{g_i} \right) \right\}_{i=1, \dots, r}$

さらに, 定理 2.10 を用いれば, 次のアルゴリズムが得られる. ただし, \prec_i は $x_i \ll X \setminus \{x_i\}$ なるブロック順序順序である.

Algorithm 4.3 ParametricZeroDimensionalRadical

Require: 0 次元イデアル I の生成系 $F = \{f_1, \dots, f_s\} \subset K[U][X]$, 構成的集合 $S \subset \overline{K}^m$

Ensure: S における \sqrt{I} の包括的系 \mathcal{G}

1: **for** $i = 1, \dots, n$ **do**

2: $\{(S_{ij}, G_{ij})\}_{j=1, \dots, r_i} \leftarrow \text{CGS}(F, S, \prec_i)$

3: $g_{ij} \leftarrow \langle \pi_a(g_{ij}) \rangle = \pi_a(I) \cap K[x_i]$ なる $g_{ij} \in G_{ij} \cap K[x_i]$

4: $\mathcal{G}_i \leftarrow \emptyset$

5: **for** $j = 1, \dots, r_i$ **do**

6: $\mathcal{G}_i \leftarrow \mathcal{G}_i \cup \text{ParametricSquareFreePart}(g_{ij}, S_{ij})$

7: **end for**

8: **end for**

9: $\mathcal{G} \leftarrow \emptyset$

10: **for all** $((S_1, g_1), \dots, (S_n, g_n)) \in \mathcal{G}_1 \times \dots \times \mathcal{G}_n$ **do**

11: $\mathcal{G} \leftarrow \mathcal{G} \cup (S_1 \cap \dots \cap S_n, F \cup \{g_1, \dots, g_n\})$

12: **end for**

13: **return** \mathcal{G}

4.3 parametric イデアルの 0 次元化と根基の計算

この節では、イデアルの 0 次元化の方法を parametric イデアルの 0 次元化へと拡張する。
まず、命題 2.11 から、次のアルゴリズムが得られる。

Algorithm 4.4 ParametricIdealIntersection

Require: $F = \{f_1, \dots, f_s\}, F' = \{f'_1, \dots, f'_t\} \subset K[U][X]$, 構成的集合 $S \subset \overline{K}^m$

Ensure: S における $\langle F \rangle \cap \langle F' \rangle$ の包括的 Gröbner 基底系

- 1: $yF \leftarrow \{yf_1, \dots, yf_s\}$
 - 2: $(1-y)F' \leftarrow \{(1-y)f'_1, \dots, (1-y)f'_t\}$
 - 3: $L \leftarrow yF \cup (1-y)F'$
 - 4: $\{(S_i, G_i)\}_{i=1, \dots, r} \leftarrow \text{CGS}(\langle L \rangle_{K[U][X, y]}, S, \prec)$ /* \prec は $y \gg X$ なるブロック順序とする. */
 - 5: **for** $i = 1, \dots, s$ **do**
 - 6: $G'_i \leftarrow G_i \cap K[U][X]$
 - 7: **end for**
 - 8: **return** $\{(S_i, G'_i)\}_{i=1, \dots, r}$
-

また、IdealQuotient および IdealSaturation を、次のように parametric イデアルに対するアルゴリズムとして拡張できる。

Algorithm 4.5 ParametricIdealQuotient

Require: $F = \{f_1, \dots, f_s\} \subset K[U][X]$, $f \in K[U][X]$, 構成的集合 $S \subset \overline{K}^m$

Ensure: S における $\langle F \rangle : f$ の包括的系

- 1: $S_0 \leftarrow \{a \in S \mid \pi_a(f) = 0\}$
 - 2: $\{(S_i, G_i)\}_{i=1, \dots, r} \leftarrow \text{ParametricIdealIntersection}(F, \{f\}, S)$
 - 3: **for** $i = 1, \dots, r$ **do**
 - 4: $S'_i \leftarrow S_i \setminus S_0$
 - 5: $G'_i \leftarrow \frac{1}{f} \cdot G_i$
 - 6: **end for**
 - 7: **return** $\{(S'_i, G'_i)\}_{i=1, \dots, r}$
-

Algorithm 4.6 ParametricIdealSaturation

Require: $F = \{f_1, \dots, f_s\} \subset K[U][X]$, $f \in K[U][X]$, 構成的集合 $S \subset \overline{K}^m$

Ensure: $\langle F \rangle : f^\infty$ の S における包括的系, $\langle F \rangle : f^m = \langle F \rangle : f^\infty$ なる $m \in \mathbb{N}$

```
1:  $m \leftarrow 0$ 
2:  $\mathcal{G}_1 \leftarrow \text{CGS}(F, S, \prec)$ 
3:  $\text{idealquotientmatch} \leftarrow \text{false}$ 
4: while  $\text{idealquotientmatch} = \text{false}$  do
5:    $\mathcal{G}_2 \leftarrow \emptyset$ 
6:   for all  $(S_i, G_i) \in \mathcal{G}_1$  do
7:      $\mathcal{G}_2 \leftarrow \mathcal{G}_2 \cup \text{ParametricIdealQuotient}(G_i, \{f\}, S_i)$ 
8:   end for
9:   if  $\mathcal{G}_1 = \mathcal{G}_2$  then
10:     $\text{idealquotientmatch} \leftarrow \text{true}$ 
11:   else
12:     $\mathcal{G}_1 \leftarrow \mathcal{G}_2$ 
13:     $m \leftarrow m + 1$ 
14:   end if
15: end while
16: return  $(\mathcal{G}_1, m)$ 
```

以上の ParametricIdealSaturation と ParametricMaximalIndependentSet を用いることで, Parametric イデア
ルに対する 0 次元化のアルゴリズムが得られる.

Algorithm 4.7 ParametricReductionToZero

Require: $F = \{f_1, \dots, f_s\} \subset K[U][X]$, 構成的集合 $S \subset \overline{K}^m$

Ensure: 以下からなる組の系 $(Y_i, S_{ij}, G_{ij}, h_{ij})$

Y_i : $\langle F \rangle$ の極大独立集合,

S_{ij} : 構成的集合,

G_{ij} : $\langle F \rangle^{\text{ext}(Y_i)}$ の S における CGB,

h_{ij} : $(\langle F \rangle^{\text{ext}(Y_i)})^{\text{cont}} = \langle F \rangle : h_{ij}$ なる $h_{ij} \in K[U]$

```
1:  $\mathcal{G} \leftarrow \emptyset$ 
2:  $\{(S_i, G_i, Y_i)\}_{i=1, \dots, r} \leftarrow \text{ParametricMaximalIndependentSet}(S, F)$ 
3: for  $i = 1, \dots, r$  do
4:    $X'_i \leftarrow X \setminus Y_i$ 
5:    $\mathcal{G}_i \leftarrow \text{CGS}(G_i, S_i, \prec)$  /* 変数集合は  $X'_i$  とする */
6:   for all  $(S_{ij}, G_{ij}) \in \mathcal{G}_i$  do
7:      $h_0 \leftarrow \prod_{g \in G_{ij}} \text{LC}_{\prec}(g)$ 
8:      $(\mathcal{G}_{ij}, m_{ij}) \leftarrow \text{ParametricIdealSaturation}(G_{ij}, h_0, S_{ij})$ 
9:      $h_{ij} \leftarrow h_0^{m_{ij}}$ 
10:     $\mathcal{G} \leftarrow \mathcal{G} \cup \{(Y_i, S_{ij}, G_{ij}, h_{ij})\}$ 
11:   end for
12: end for
13: return  $\mathcal{G}$ 
```

そして, Radical と同様に, parametric イデアルに対する根基を計算する次のアルゴリズムが得られる.

Algorithm 4.8 ParametricRadical

Require: $F = \{f_1, \dots, f_s\} \subset K[U][X]$, 構成的集合 $S \subset \overline{K}^m$

Ensure: $\sqrt{\langle F \rangle}$ の S における包括的系

```

1:  $\mathcal{G} \leftarrow \emptyset$ ;  $L \leftarrow \emptyset$ 
2:  $\{(Y_i, S_i, G_i, h_i)\}_{i=1, \dots, r} \leftarrow \text{ParametricReductionToZero}(F, S)$ 
3: for  $i = 1, \dots, r$  do
4:    $\{(S_{ij}, G_{ij})\}_{j=1, \dots, s_i} \leftarrow \text{ParametricZeroDimensionalRadical}(G_i, S_i)$  (ただし, 変数集合を  $X \setminus Y_i$  とする. )
5:   for  $j = 1, \dots, s_i$  do
6:      $\{(S_{ijk}, G_{ijk})\}_{k=1, \dots, t_{ij}} \leftarrow \text{CGS}(G_{ij}, S_{ij}, \prec)$  (ただし, 変数集合を  $X \setminus Y_i$  とする. )
7:     for  $k = 1, \dots, t_{ij}$  do
8:        $p_{ijk} \leftarrow \prod_{g \in G_{ijk}} \text{LC}(g)$ 
9:        $\mathcal{G} \leftarrow \mathcal{G} \cup \text{ParametricIdealSaturation}(G_{ijk}, p_{ijk}, S_{ijk})$ 
10:    end for
11:  end for
12:   $\mathcal{G}'_i \leftarrow \text{ParametricRadical}(F \cup \{h_i\}, S_i)$ 
13:  for all  $((S, G), (S', G')) \in \mathcal{G} \times \mathcal{G}'_i$  do
14:     $L \leftarrow L \cup \text{ParametricIdealIntersection}(G, G', S \cap S')$ 
15:  end for
16: end for
17: return  $L$ 

```

今後の課題

本研究では, parametric イdealに対して

- 0次元イdealの根基イdeal
- イdealの共通部分
- イdeal商

の計算を実装した. この先については一般次元の parametric イdealの根基イdeal計算の実現に向けて,

- 飽和イdealの計算
- イdealの0次元化
- 以上を用いた根基イdealの計算

の実装が必要である. この中でも特に問題になるのは飽和イdealの計算だろう. この計算には CGS の一致を判定する部分があり, parameter なしのイdealでは簡約 Gröbner 基底を用いることでイdealの一致を判定できるが, parametric イdealに対しては標準形を与えることが難しいためその判定が困難である. そうした, 判定法の確立および上記の実装を今後の課題としたい.

謝辞

本論文は筆者が東京都立大学大学院理学研究科数理科学専攻博士前期課程に在学中の研究成果をまとめたものである。本研究を3年間熱心に指導していただいたことに加え、進路やその他のことについても親身になって相談にのっていただきました指導教員である横山俊一先生に絶大な感謝の意を申し上げます。そして、ご多忙のところ本論文の副査を快諾してくださった内山成憲先生および内田幸寛先生に感謝の意を申し上げます。また、本研究を進めるにあたり有益な助言を賜りました、東京理科大学理学部第一部応用数学科の鍋島克輔先生と石原侑樹先生、そして九州大学数理学研究院の深作亮也先生に心より感謝申し上げます。最後に、筆者を支えてくださった家族、友人に感謝申し上げます。

付録

コード 4.1 parametric_zradical.rr

```
1
2 /* パッケージの読み込み*/
3
4 load("kcgs2023.rr");
5 load("list_operation.rr");
6
7
8 /*-----*/
9
10 /*comprehensive system の表示*/
11
12 def view(CS){
13     print(" ", 1);
14     N = length(CS);
15     while(CS!=[]){
16         CB=car(CS);
17         CS=cdr(CS);
18         print(CB[0],1);
19         print(CB[1],1);
20         print(CB[2],1);
21         print(" ", 1);
22     }
23     print("No. of segments is");
24     return N;
25 }
26
27
28 /*CGS 計算の呼び出し*/
29
30 def cgs(F, Pars, Vars, Ord){
31     CGS = kcgs1(F, Pars, Vars, Ord);
32     print("");
33     return CGS;
34 }
35
36 def seg_cgs(E, N, F, Pars, Vars, Ord){
37     Result = [];
38     CGS = cgs(F, Pars, Vars, Ord);
39     while(CGS != []){
40         CGB = car(CGS);
41         CGS = cdr(CGS);
```

```

42     NewSeg = seg_intersection(E, N, CGB[0], CGB[1]);
43     Result = cons([NewSeg[0], NewSeg[1], CGB[2]], Result);
44 }
45 return reverse(Result);
46 }
47
48
49 /*-----*/
50
51
52 /* parametric square-free part*/
53
54 def para_sqfr_part(E, N, Poly, Pars, Var){
55     Result = [];
56     DPoly = diff(Poly, Var);
57     CGS = seg_cgs(E, N, [Poly, DPoly], Pars, [Var], 0);
58     while(CGS != []){
59         CGB = car(CGS);
60         CGS = cdr(CGS);
61         SqFr = div(Poly, CGB[2][0]);
62         Result = cons([CGB[0], CGB[1], [SqFr]], Result);
63     }
64     return reverse(Result);
65 }
66
67
68 /* parametric zero-dimensional radical*/
69
70 def para_zradical(E, N, Polys, Pars, Vars){
71     List_AllVar = [];
72     Len = length(Vars);
73     for (I = 1; I <= Len; I++){
74         List_EachVar = [];
75         UniVar = car(Vars);
76         Vars = append(cdr(Vars), [UniVar]);
77         CGS = seg_cgs(E, N, Polys, Pars, Vars, 2);
78         while(CGS != []){
79             CGB = car(CGS);
80             CGS = cdr(CGS);
81             Poly = elimination(CGB[2], Pars, [UniVar]);
82             SegSqfrs = para_sqfr_part(CGB[0], CGB[1], Poly[0], Pars, UniVar);
83             List_EachVar = append(List_EachVar, SegSqfrs);
84         }
85         List_AllVar = append(List_AllVar, [List_EachVar]);
86     }
87     SegNewGens = [[[0],[1],[]]];
88     while(List_AllVar != []){
89         List_EachVar = car(List_AllVar);
90         List_AllVar = cdr(List_AllVar);
91         SegNewGens = parazradical_sub(SegNewGens, List_EachVar);
92     }
93     Result = [];

```

```

94     while(SegNewGens != []){
95         SegNewGen = car(SegNewGens);
96         SegNewGens = cdr(SegNewGens);
97         Gen = append(Polys, SegNewGen[2]);
98         Result = append(Result, [SegNewGen[0], SegNewGen[1], Gen]);
99     }
100     return Result;
101 }
102
103 /* para_zradical 後半部分のsubroutine (各変数での結果を結合する) */
104
105 def parazradical_sub(List_Var1, List_Var2){
106     Result = [];
107     Len1 = length(List_Var1);
108     Len2 = length(List_Var2);
109     for(I = 0; I < Len1; I++){
110         CGB1 = List_Var1[I];
111         E1 = CGB1[0];
112         N1 = CGB1[1];
113         Polys1 = CGB1[2];
114         for(J = 0; J < Len2; J++){
115             CGB2 = List_Var2[J];
116             E2 = CGB2[0];
117             N2 = CGB2[1];
118             Polys2 = CGB2[2];
119             NewSeg = seg_intersection(E1, N1, E2, N2);
120             NewPolys = append(Polys1, Polys2);
121             Result = cons([NewSeg[0], NewSeg[1], NewPolys], Result);
122         }
123     }
124     return reverse(Result);
125 }
126
127
128 /* parametric ideal intersection*/
129
130 def para_intersection(E, N, F1, F2, Pars, Vars){
131     Result = [];
132     Ft = append(map(mult, F1, t), map(mult, F2, 1-t));
133     Varst = cons(t, Vars);
134     CGS = seg_cgs(E, N, Ft, Pars, Varst, 2);
135     while(CGS != []){
136         CGB = car(CGS);
137         CGS = cdr(CGS);
138         GB = elimination(CGB[2], Pars, Vars);
139         if(GB == []){
140             GB = [0];
141         }
142         Result = cons([CGB[0], CGB[1], GB], Result);
143     }
144     return reverse(Result);
145 }

```

```

146
147
148 /* parametric ideal quotient*/
149
150 def para_quotient(E, N, F, Poly, Pars, Vars){
151     Result = [];
152     Coefs = coef_list(Poly, Vars, 0);
153     E0 = nd_gr(Coefs, Pars, 0, 0);
154     if(is_empty(E0, [1], Pars) == 0){
155         Result = cons([E0, [1], [1]], Result);
156     }
157     CGS = para_intersection(E, N, F, [Poly], Pars, Vars);
158     while(CGS != []){
159         CGB = car(CGS);
160         CGS = cdr(CGS);
161         Seg = seg_diff(CGB[0], CGB[1], E0);
162         GB = map(div, CGB[2], Poly);
163         Result = cons([Seg[0], Seg[1], GB], Result);
164     }
165     return reverse(Result);
166 }
167
168
169 /*-----*/
170
171
172 /* subroutine*/
173
174 def elimination(Polys, Pars, Vars){
175     Result = [];
176     ParVars = append(Pars, Vars);
177     while (Polys != []){
178         Poly = car(Polys);
179         Polys = cdr(Polys);
180         if (is_subset(vars(Poly), ParVars)){
181             Result = cons(Poly, Result);
182         }
183     }
184     return reverse(Result);
185 }
186
187 def coef_list(Poly, Vars, Ord){
188     Result = [];
189     dp_ord(Ord);
190     DP = dp_ptod(Poly, Vars);
191     while(DP != 0){
192         Result = cons(dp_hc(DP), Result);
193         DP = DP - dp_hm(DP);
194     }
195     return reverse(Result);
196 }
197

```

```

198
199 /*-----*/
200
201
202 /* segment の共通部分*/
203
204 def seg_intersection(E1, N1, E2, N2){
205     Polys1 = append(E1, E2);
206     NewE = nd_gr(Polys1, vars(Polys1), 0, 0);
207     if (NewE == []){
208         NewE = [0];
209     }
210     Vars = vars(append(N1, N2));
211     NewN = noro_pd.ideal_intersection(N1, N2, Vars, 0);
212     return [NewE, NewN];
213 }
214
215
216 /* (V(E1)-V(N1))-V(E2)の計算 */
217
218 def seg_diff(E1, N1, E2){
219     Vars = vars(append(N1, E2));
220     NewN = noro_pd.ideal_intersection(N1, E2, Vars, 0);
221     return [E1, NewN];
222 }
223
224
225 /* segment が空かどうかの判定*/
226
227 def is_empty(E, N, Pars){
228     while(N != []){
229         Poly = car(N);
230         N = cdr(N);
231         if(noro_pd.radical_membership(Poly, E, Pars) != 0){
232             return 0;
233         }
234     }
235     return 1;
236 }
237
238
239 /*-----*/
240
241
242 /* map 用*/
243
244 def mult(X, Y){
245     return X*Y;
246 }
247
248 def div(F1, F2){
249     return red(F1/F2);

```



```
1
2 def is_in(Elem, List){
3   while(List != []){
4     ListElem = car(List);
5     List = cdr(List);
6     if (Elem == ListElem){
7       return 1;
8     }
9   }
10  return 0;
11 }
12
13
14 def is_subset(List1, List2){
15   while(List1 != []){
16     Elem = car(List1);
17     List1 = cdr(List1);
18     if (is_in(Elem, List2) == 0){
19       return 0;
20     }
21   }
22   return 1;
23 }
24
25
26 def is_coprime(List1, List2){
27   while(List1 != []){
28     Elem = car(List1);
29     List1 = cdr(List1);
30     if (is_in(Elem, List2) == 1){
31       return 0;
32     }
33   }
34   return 1;
35 }
36
37
38 def list_intersection(List1, List2){
39   Result = [];
40   while(List1 != []){
41     Elem = car(List1);
42     List1 = cdr(List1);
43     if (is_in(Elem, List2) == 1){
44       Result = append(Result, [Elem]);
45     }
46   }
47   return Result;
48 }
49
```

```
50
51 def list_union(List1, List2){
52     Result = List1;
53     while(List2 != []){
54         Elem = car(List2);
55         List2 =cdr(List2);
56         if (is_in(Elem, List1) == 0){
57             Result = append(Result, [Elem]);
58         }
59     }
60     return Result;
61 }
62
63
64 def list_difference(List1, List2){
65     Result = [];
66     while(List1 != []){
67         Elem = car(List1);
68         List1 =cdr(List1);
69         if (is_in(Elem, List2) == 0){
70             Result = append(Result, [Elem]);
71         }
72     }
73     return Result;
74 }
```

参考文献

- [1] T.Becker, V.Weispfenning, Gröbner Bases, Graduate Texts in Mathematics 141, Springer-Verlag, 1993.
- [2] D. コックス, J. リトル, D. オシー, グレブナ基底と代数多様体入門 (上・下), 丸善出版, 2023.
- [3] J.C.Faugère, A new efficient algorithm for computing Gröbner bases (F_4), 1999.
- [4] R.Gebauer, M.Möller, On an Installation of Buchberger's Algorithm, 1987.
- [5] G-M.Greuel, G.Pfister, A Singular Introduction to Commutative Algebra, Springer, Heidelberg, 2002.
- [6] 日比孝之 編, グレブナー基底の現在, 数学書房, 2006.
- [7] 石原侑樹, パラメータ付きのイデアル操作の計算について, 京都大学数理解析研究所講究録 第 2255 巻 96-105, 2023.
- [8] JST CREST 日比チーム編, グレブナー道場, 共立出版, 2012.
- [9] M.Kalkbrener, On the Stability of Gröbner Bases under Specialization, Journal of Symbolic Computation Vol.24-1, 51-58, 1997.
- [10] D.Kapur, Y.Sun, D.Wang, A New Algorithm for Computing Comprehensive Gröbner Systems, Proceeding of International Symposium on Symbolic and Algebraic computation 2010, 29-36, 2010.
- [11] 児玉壮, 包括的グレブナー基底系を用いたパラメータ付きイデアルに対する零次元化, 東京都立大学大学院理学研究科数理科学専攻 修士論文, 2022.
- [12] D.Lu, Y.Sun, D.Wang, A Survey on Algorithms for Computing Comprehensive Gröbner Systems and Comprehensive Gröbner Bases, Journal of Systems Science and Complexity Vol.32, 234-255, 2019.
- [13] K.Nabeshima, A Speed-Up of the Algorithm for Computing Comprehensive Gröbner Systems, Proceedings of the International Symposium on Symbolic and Algebraic Computation 2007, 299-306, 2007.
- [14] 鍋島克輔, kcgs2023.rr, <https://www.rs.tus.ac.jp/~nabeshima/software.html>.
- [15] 永井保成, 代数幾何学入門 代数学の基礎を出発点として, 森北出版, 2021.
- [16] 野呂正行, グレブナー基底計算の高速化とその応用, 2010.
<https://www.math.sci.hokudai.ac.jp/sympo/100809/pdf/noro.pdf>
- [17] M.Noro, T.Shimoyama, T.Takeshima: Asir User's Manual, 2019.
<http://www.math.kobe-u.ac.jp/OpenXM/Current/doc/asir2000/html-ja/man/man.html>
- [18] 野呂正行, 横山和弘, グレブナー基底の計算 基礎編 計算代数入門, 東京大学出版, 2003.
- [19] Risa/Asir (Kobe Distribution), <http://www.math.kobe-u.ac.jp/Asir/>.
- [20] A.Suzuki, Y.Sato, A Simple Algorithm to Compute Comprehensive Gröbner Bases, Proceeding of International Symposium on Symbolic and Algebraic Computation 2006, 326-331, 2006.
- [21] W.Vasconcelos, Computational Methods in Commutative Algebra and Algebraic Geometry, Algorithms and Computation in Mathematics Vol.2, Heidelberg, 2004
- [22] V.Weispfenning, Comprehensive Gröbner Bases, Journal of Symbolic Computation Vol.14-1, 1-29, 1992.
- [23] K.Yokoyama, Stability of Parametric Decomposition, Mathematical Software - ICMS 2006. Lecture Notes in Computer Science, vol. 4151, 391-402 Springer, Berlin, Heidelberg, 2006.
- [24] 横山和弘, 多項式と計算機代数 現代基礎数学 17, 朝倉書店, 2022.