平成２５年度　学位論文

グレブナー基底について

兵庫教育大学大学院　学校教育研究科
教育内容・方法開発専攻　認識形成系教育コース
Ｍ１２１５２Ｈ　仲　川　拓　哉

目 次

0章　序

本論文では, グレブナー基底とブッフバーガーアルゴリズムについて述べる.

グレブナー基底の概念は, ブッフバーガー (B. Buchberger) により, 多項式環のイデアルによる剰余類環を計算する問題を研究する過程で発見され, その計算方法であるブッフバーガーアルゴリズムと共に, 彼のインスブルック大学 (オーストリア) での学位論文 (1965年) の中核をなしている.

グレブナー基底とは, 多項式環のイデアルの基底で, "よい条件" をみたすものであり, 多項式がイデアルに属するかどうかの判定問題や連立代数方程式の解法など多方面に応用されている. 例えば, 複素数係数連立代数方程式

$$\begin{cases} f_1(x_1, ..., x_n) = 0 \\ \quad \vdots \\ f_\ell(x_1, ..., x_n) = 0 \end{cases}$$

の解を求める問題は, $f_1, ..., f_\ell$ で生成された $\mathbb{C}[x_1, ..., x_n]$ のイデアル $I = \langle f_1, ..., f_\ell \rangle$ の零点を求める問題と一致し, イデアル I の "よい" 生成系であるグレブナー基底 $g_1, ..., g_m$ を求め, その共通零点を求める問題に帰着する.

筆者は学部の卒業研究の過程で, グレブナー基底を利用して対称式の計算を行った. しかし, グレブナー基底の諸性質について十分に理解していたわけではなく, 計算機を用いて計算するための道具としていたにすぎないことに気付いた. このような理由から, 本大学院において, グレブナー基底の概念とブッフバーガーアルゴリズムについてのより深い理解と知識を得るための研究を行うことにした.

なお, グレブナー基底という名称はブッフバーガーの指導教授 W. Gröbner にちなんで名付けられたようである. また, ほぼ同時期に 広中平祐が代数幾何学の研究からグレブナー基底と同一の概念を発見している.

以下, 論文の構成について述べる.

1章では, 順序と整列順序, 環, 多項式環など, 後章で用いる基本事項について述べる.

2章では, 項順序とモノイデアルを定義し, モノイデアルが有限生成であるというディクソンの補題を示す. また, ディクソンの補題を用いて, 項順序が整列順序であることを導く. これらの結果は3章で有限回の単項簡約で正規化できることの証明やグレブナー基底の存在証明などで用いられる.

§2.1 では, 項のなす集合 $T = T(x_1, ..., x_n)$ 上の項順序と, 指数のなす集合 $\mathbb{Z}_0{}^n$ 上の項順序を定義し, 2つの補題を示す.

§2.2 では, $\mathbb{Z}_0{}^n$ のモノイデアルを定義し, ディクソンの補題を示す. さらに, 項順序が整列順序であることを導く.

3章では, 与えられた項順序のもとに, 先頭項, 先頭単項式, 先頭指数, 単項簡約, 正規形, 正規化などの概念を定義し, すべての多項式が有限回の単項簡約で正規化できることを示す. 次にグレブナー基底を定義し, モノイデアルが有限生成であることを基にグレブナー基底の存在を示す. また, グレブナー基底による正規化が一意に定まることを導く. 最後に, グレブナー基底から極小グレブナー基底が得られること, 極小グレブナー基底から簡約グレブナー基底が得られることを示した後, 簡約グレブナー基底の一意性を証明する.

§3.1 では, 項順序から単項式の大小を定め, 多項式の単項式の中で最大であるものとして先頭単項式を定義する. さらに先頭単項式の倍数を消去する操作である単項簡約を定義し, 項順序が整列順序であることを用いて, すべての多項式が有限回の単項簡約で正規化できることを示す.

§3.2 では, イデアルのグレブナー基底を定義し, イデアルに含まれる多項式の先頭指数からなるモノイデアルが有限生成であることを基にグレブナー基底の存在を示す. これより, 多項式環 $\mathbb{C}[x_1, ..., x_n]$ の任意のイデアルが有限生成であること (ヒルベルトの基底定理) が導かれる. また, グレブナー基底による正規化が一意に定まることを示す.

§3.3 では, 極小グレブナー基底, 簡約グレブナー基底を定義し, グレブナー基底から余分な多項式を取り除いて極小グレブナー基底が得られること, 極小グレブナー基底から正規化により簡約グレブナー基底が得られることを示す. 最後に, 簡約グレブナー基底の一意性を証明する.

4章では, 0 でない2つの多項式に対して S 多項式を定義し, イデアルの有限生成系がグレブナー基底であるかどうか判定するブッフバーガーの判定条件を導く. これより, グレブナー基底を求めるブッフバーガーアルゴリズムが得られる.

§4.1 では, S 多項式を定義し, イデアル I の有限生成系 G がグレブナー基底であるこ

とと「G の任意の 2 元の S 多項式の正規化が 0 となる」こととが同値であるというブッフバーガーの判定条件を導く.

§4.2 では, イデアルの有限生成系にブッフバーガーアルゴリズムを適用することにより, グレブナー基底が得られることを示し, その計算を例示した.

1章　準備

この論文では, 参考文献 [2] にあるような群・環・体についての基本事項は既知とするが, 後章で必要となる順序, 環, 多項式環等についての用語や定理をここに挙げておく. なお, この論文を通して次の記号を用いる.

$\mathbb{Z}$	$=$	$\{0, \pm 1, \pm 2, \pm 3, ...\}$	(整数全体)
$\mathbb{Z}_0$	$=$	$\{0, 1, 2, 3, ...\}$	(非負整数全体)
$\mathbb{Z}_0^n$	$=$	$\underbrace{\mathbb{Z}_0 \times \cdots \times \mathbb{Z}_0}_{n\text{個}} = \{(a_1, ..., a_n) \mid a_1, ..., a_n \in \mathbb{Z}_0\}$	
$\mathbb{C}$	$=$	$\{a + ib \mid a, b$ は実数 $\}$, ただし $i^2 = -1$	(複素数全体)
$\mathbb{C}[x_1, ..., x_n]$	:	$\mathbb{C}$ 上の n 変数 $x_1, ..., x_n$ の多項式環	
$T(x_1, ..., x_n)$	:	n 変数 $x_1, ..., x_n$ の項 $x_1^{i_1} \cdots x_n^{i_n}$ 全体のなす集合	
$\langle g_1, ..., g_m \rangle$	:	多項式 $g_1, ..., g_m$ で生成された $\mathbb{C}[x_1, ..., x_n]$ のイデアル	
$f \mid g$	:	多項式 f が多項式 g を割り切る	
$\forall a \in A$	:	集合 A の任意の元 a に対して	
$A \Rightarrow B$	:	A ならば B である	
$A \Leftrightarrow B$	:	A と B は同値である	
$A \overset{def}{\Longleftrightarrow}$ 条件	:	A を条件で定義する	
$\mathrm{LM}(f)$	:	多項式 $f \neq 0$ の先頭単項式	
$\mathrm{LT}(f)$	:	多項式 $f \neq 0$ の先頭項	
$\mathrm{LC}(f)$	:	多項式 $f \neq 0$ の先頭係数	
$\mathrm{LE}(f)$	:	多項式 $f \neq 0$ の先頭項の指数	
$f \xrightarrow[g]{} h$	:	f に g による単項簡約を行って h を得ること	
$f \xrightarrow[G]{} h$	:	f に G の元による単項簡約を行って h を得ること	
$f \xrightarrow[G]{*} h$	:	f に G の元による単項簡約を有限回行って h を得ること	
$\mathrm{NF}_G(f)$	:	グレブナー基底 G による f の正規化	
$[t_1, t_2]$	:	$t_1, t_2 \in T(x_1, ..., x_n)$ の最小公倍数である $T(x_1, ..., x_n)$ の元	

1.1 整列集合

集合 A の任意の2元 a,b に対して，$a \sim b$ であるか，そうでないか $(a \not\sim b)$，のいずれかが成り立つとき，$\sim$ を A 上の関係という．

定義 1.1 集合 A 上の関係 $\leq$ が次の3条件をみたすとき順序 (関係) であるという．ただし，a,b,c は A の任意の元である．

(1) $a \leq a$

(2) $a \leq b,\ b \leq a \ \Rightarrow\ a = b$

(3) $a \leq b,\ b \leq c \ \Rightarrow\ a \leq c$

- $a \leq b$ を $b \geq a$ と表すこともある．
- $a \leq b$ かつ $a \neq b$ のとき $a < b$，または $a \lneq b$ と表す．

定義 1.2 集合 A 上の順序 $\leq$ が条件「$\forall a,b \in A$ に対して $a \leq b$，または $a \geq b$ のいずれかが成り立つ」をみたすとき全順序 (関係) であるという．

- $\leq$ が集合 A 上の順序であるとき，$(A,\leq)$ を順序集合という．単に A を順序集合ということもある．特に $\leq$ が集合 A 上の全順序であるとき，A を全順序集合という．
- $(A,\leq)$ を順序集合，S をその部分集合とする．次の2条件が成り立つとき，a を S の最小元という．

  (1) $a \in S$

  (2) $a \leq x \ \ (\forall x \in S)$

定義 1.3 全順序集合 A が条件「空でない任意の部分集合に最小元が存在する」をみたすとき整列順序 (関係) であるという．

- 整列順序の定義された集合を整列集合という．

1.2 環

集合 A に加法 $+$, と乗法 $\cdot$ が定義されていて, 次の条件 (1)〜(8) をみたすとき, A を環という. ただし, a, b, c は A の任意の元であり, $0, 1$ は A の特別な元で $0 \neq 1$ である. また, 積 $a \cdot b$ は ab と略記する.

(1) $a+b=b+a$
(2) $(a+b)+c=a+(b+c)$
(3) $a+0=0+a=a$
(4) $a+(-a)=(-a)+a=0$
をみたす $-a$ が存在する.
(5) $ab=ba$
(6) $(ab)c=a(bc)$
(7) $a1=1a=a$
(8) $a(b+c)=ab+ac,\ (a+b)c=ac+bc$

上の条件を満たす A は, 一般に可換環と呼ばれるが, この論文では単に環ということにする. 以下, 環についての基本事項を述べる.

- 環 A において条件「$ab=0$ ならば $a=0$ または $b=0$」が成り立つとき, A を整域という.
- 環 A において条件「$a \neq 0$ のとき $aa^{-1}=a^{-1}a=1$ をみたす $a^{-1} \in A$ が存在する」が成り立つとき, A を体という. a^{-1} を a の逆元という.
- 環 A の空でない部分集合 I で次の条件をみたすものを A のイデアルという.
  - $a, b \in I \ \Rightarrow\ a+b \in I$
  - $a \in A,\ b \in I \ \Rightarrow\ ab \in I$
- 環 A の部分集合 S に対して, S を含む A のイデアルすべての共通部分は A のイデアルとなる. これを S で生成されたイデアルといい, $\langle S \rangle$ と表す. S を $\langle S \rangle$ の生成系, または基底という. $S \neq \emptyset$ のときは

$$\langle S \rangle = \{a_1 s_1 + \cdots + a_r s_r \mid a_i \in A, s_j \in S\}$$

が成り立つ. また, $\langle \emptyset \rangle = 0$ である. ここで 0 は $\{0\}$ と記すべきであるが, 以下, 慣用的に 0 と表すことにする.

- 有限集合 $S=\{s_1, \ldots, s_m\}$ に対して

$$\langle S \rangle = \langle s_1, \ldots, s_m \rangle$$

と表す.

- $I = \langle s_1, ..., s_m \rangle$ と表されるイデアルを有限生成イデアルという. また「I は有限生成である」ともいう.
- すべてのイデアルが有限生成である環 A をネーター環という.
- 環 A がネーター環であることと, 相異なるイデアルからなる無限昇鎖列が存在しないこととは同値である. ただし, 相異なるイデアルからなる無限昇鎖列とは, イデアルの列

$$I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots\cdots \subsetneq I_k \subsetneq I_{k+1} \subsetneq \cdots\cdots$$

のことである.
- A が体であるとき, A のイデアルは A と 0 のみである. 従って体はネーター環である.

1.3 多項式環

A が環であるとき, 次の形の式 $f(x)$ を x を変数とする A 係数多項式という.

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \quad (a_n, ..., a_o \in A)$$

$a_n \neq 0$ のとき $f(x)$ の次数は n であるといい, $\deg f(x) = n$ と表す. x を変数とする A 係数多項式の全体を $A[x]$ と表し, $A[x]$ を A 上の多項式環という. 以下, 多項式環についての基本事項を述べる.

- $A[x]$ は通常の多項式の加法と乗法により環をなす. 特に, A が整域ならば $A[x]$ も整域である.
- 変数 x_1, x_2 に対して, A 上の多項式環 $A[x_1]$ 上の多項式環 $(A[x_1])[x_2]$ が定まる. これを

$$A[x_1, x_2] = (A[x_1])[x_2]$$

とおき, A 上の 2 変数 x_1, x_2 の多項式環という. 同様に, A 上の n 変数多項式環

$$A[x_1, ..., x_n] = (A[x_1, ..., x_{n-1}])[x_n]$$

が定義される.

- 体 F 上の多項式環 $F[x]$ は単項イデアル整域である. すなわち, すべてのイデアルは1元で生成される. 特に $F[x]$ はネーター環である.

定理 1.4 (Hilbert の基底定理, [2, 定理 29.11]) ネーター環上の多項式環はネーター環である. 特に, 体 F 上の n 変数多項式環 $F[x_1, ..., x_n]$ はネーター環である.

- 3章, §3.2 でグレブナー基底を定義し, それより, $\mathbb{C}[x_1, ..., x_n]$ がネーター環であることを導く (系 3.13).

素元分解整域

以下, 整域と素元分解整域についての基本事項を述べる.

- 整域 A の元 u に対して, $uu' = 1$ となる $u' \in A$ が存在するとき, u を可逆元 (または正則元) という.
- 整域 A の元 a, b に対して, $a = ub$ となる可逆元 $u \in A$ が存在するとき a と b は同伴であるという.
- 整域 A の元 a, b に対して, $a = bc$ となる $c \in A$ が存在するとき, b は a を割り切るといい, $b \mid a$ と表す. このとき, a を b の倍数, b を a の約数という.
- 整域 A の可逆元でない元 $p \neq 0$ が条件「$p \mid ab$ $(a, b \in A)$ ならば $p \mid a$ または $p \mid b$」をみたすとき, p を素元という.
- 整域 A の 0 でも可逆元でもない元がすべて素元の積として表されるとき, A を素元分解整域 (または一意分解整域) という.
- 素元分解整域 A においては, 0 でも可逆元でもない元 a はすべて素元の積に同伴を除いて一意的に分解される. すなわち,

$$a = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_\ell$$

と素元の積として2通りに表されたときは, $m = \ell$ であり, 適当に番号を付け替えると p_i と q_i が同伴になるようにできる.

- 素元分解整域とは, 整数環 $\mathbb{Z}$ で素因数分解が成り立つのと類似の性質を持つ整域のことである.

- 整数環 $\mathbb{Z}$ や体 F 上の多項式環 $F[x]$ は素元分解整域である ([2, 例 26.6]). $F[x]$ の素元は既約多項式 (因数分解できない多項式) である.

定理 1.5 ([2, 定理 26.13]) 体 F 上の n 変数多項式環 $F[x_1, ..., x_n]$ は素元分解整域である.

- 定理 1.5 より, n 変数多項式は既約多項式の積として, 定数倍を除いて一意的に表される. 特に, $F[x_1, ..., x_n]$ の 2 つの多項式の最大公約数, 最小公倍数などが定義される.

2章　項順序とモノイデアル

2章では, 項順序とモノイデアルを定義し, モノイデアルが有限生成であるというディクソンの補題を示す. また, ディクソンの補題を用いて, 項順序が整列順序であることを導く. これらの結果は3章でグレブナー基底を考察する際に必要となる.

2.1　項順序

複素数体上の多項式環 $\mathbb{C}[x_1, ..., x_n]$ の多項式 $f(x_1, ..., x_n)$ は

$$f(x_1, ..., x_n) = \sum_{i_1,...,i_n} a_{i_1,...,i_n} {x_1}^{i_1} {x_2}^{i_2} \cdots {x_n}^{i_n} \qquad (a_{i_1,...,i_n} \in \mathbb{C})$$

と表される. ただし, 右辺の和は非負整数の組 $i_1, ..., i_n$ についての和である. ここでいくつかの用語と記号を定義しておく.

- $a_{i_1,...,i_n} \neq 0$ である項 $a_{i_1,...,i_n} {x_1}^{i_1} {x_2}^{i_2} \cdots {x_n}^{i_n}$ を f の単項式という. ただし, 同類項はまとめてあるものとする. 単項式の係数を除いた式 ${x_1}^{i_1} {x_2}^{i_2} \cdots {x_n}^{i_n}$ を項と呼ぶことにする. ただし, $1 = {x_1}^0 {x_2}^0 \cdots {x_n}^0$ も項とみなすことにする. また, $(i_1, ..., i_n)$ を項 ${x_1}^{i_1} {x_2}^{i_2} \cdots {x_n}^{i_n}$ の指数という.

注意：単項式と項の定義は書物により異なる. 上の定義は参考文献 [3] と同じであるが, 例えば, 参考文献 [4] では, 単項式と項の定義が上の定義と逆になっている. しかし, 高等学校教科書の数学I(啓林館, 平成24年度用) などでは「単項式の和として表される式を多項式といい,...」と係数を含めたものを単項式と呼んでいることもあり, この論文では上のように定義することにした.

- 非負整数全体を $\mathbb{Z}_0$ とおき, その n 個の直積集合を $\mathbb{Z}_0^n$ とする.

$$\mathbb{Z}_0 = \{0, 1, 2, 3, ...\}, \qquad \mathbb{Z}_0^n = \underbrace{\mathbb{Z}_0 \times \cdots \times \mathbb{Z}_0}_{n\text{個}} = \{(a_1, ..., a_n) \mid a_1, ..., a_n \in \mathbb{Z}_0\}$$

また, $\mathbb{Z}_0^n$ の2元の和を成分ごとの和として定める.

- 変数 $x_1, ..., x_n$ の項全体を $T(x_1, ..., x_n)$ とおく. $x_1, ..., x_n$ が明白なときは単に T と表す.

$$T = T(x_1, ..., x_n) = \{x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n} \mid (i_1, ..., i_n) \in \mathbb{Z}_0{}^n\}$$

- $T \ni {x_1}^{i_1} {x_2}^{i_2} \cdots {x_n}^{i_n}$ に対して, その指数からなる非負整数の組 $(i_1, ..., i_n) \in \mathbb{Z}_0{}^n$ を対応させる写像は, 明らかに T から $\mathbb{Z}_0{}^n$ への全単射である.

- 以下において, $X = (x_1, ..., x_n)$, $i = (i_1, ..., i_n)$ として

$$X^i = x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$$

と略記することがある.

定義 2.1 T 上の全順序 $\preceq$ で, 次の条件をみたすものを項順序 (term order) という.

(1) $t_1, t_2, t \in T$, $t_1 \preceq t_2$ ならば $tt_1 \preceq tt_2$

(2) 任意の $t \in T$ に対して $1 \preceq t$

注意: 上の定義の条件 (1) において, $t_1 \prec t_2$ ならば $t_1 \neq t_2$ であるから, $tt_1 \neq tt_2$ となるので, $tt_1 \prec tt_2$ が成り立つ.

- 次の条件で定まる T 上の順序 $\preceq$ は項順序である (辞書式順序). ただし, $\prec$ は「$\preceq$ かつ $\neq$」を表す.

$$x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n} \prec x_1^{j_1} x_2^{j_2} \cdots x_n^{j_n} \overset{def}{\iff} \begin{cases} (i_1, ..., i_n) \neq (j_1, ..., j_n), \text{ かつ} \\ i_k \neq j_k \text{ となる最小の } k \text{ について } i_k < j_k \end{cases}$$

- 次の条件で定まる T 上の順序 $\preceq$ は項順序である (全次数順序).

$$x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n} \prec x_1^{j_1} x_2^{j_2} \cdots x_n^{j_n} \overset{def}{\iff} \begin{cases} i_1 + \cdots + i_n < j_1 + \cdots + j_n \text{ であるか,} \\ i_1 + \cdots + i_n = j_1 + \cdots + j_n \text{ かつ} \\ i_1 = j_1, ..., i_k = j_k, \ i_{k+1} < j_{k+1} \end{cases}$$

補題 2.2 $t_1, t_2, t_3, t_4 \in T$ が $t_1 \preceq t_2$, $t_3 \preceq t_4$ をみたせば $t_1 t_3 \preceq t_2 t_4$ が成り立つ. 特に, $t_1 \prec t_2$, または $t_3 \prec t_4$ のときは $t_1 t_3 \prec t_2 t_4$ が成り立つ.

【証明】 定義 2.1 の条件 (1) より

$$t_1 \preceq t_2,\ t_3 \preceq t_4 \implies t_1 t_3 \preceq t_2 t_3,\ t_2 t_3 \preceq t_2 t_4 \implies t_1 t_3 \preceq t_2 t_4$$

が得られる. 特に, $t_1 \prec t_2$, または $t_3 \prec t_4$ のときは $t_1 t_3 \neq t_2 t_4$ となるので, $t_1 t_3 \prec t_2 t_4$ が成り立つ. ∎

定義 2.3 $\mathbb{Z}_0{}^n$ の全順序 $\preceq$ で次の条件をみたすものを $\mathbb{Z}_0{}^n$ 上の項順序という.

(1) $a, b, c \in \mathbb{Z}_0{}^n$, $a \preceq b$ ならば $a + c \preceq b + c$

(2) $0 = (0, \ldots, 0) \preceq a \quad (\forall a \in \mathbb{Z}_0{}^n)$

順序 $\preceq$ が $T = T(x_1, ..., x_n)$ 上の項順序であるとき, $i = (i_1, ..., i_n), j = (j_1, ..., j_n) \in \mathbb{Z}_0{}^n$ に対して

$$i \preceq j \overset{def}{\iff} x_1{}^{i_1} \cdots x_n{}^{i_n} \preceq x_1{}^{j_1} \cdots x_n{}^{j_n}$$

と定めると, $\mathbb{Z}_0{}^n$ 上の項順序となる. 逆に, $\mathbb{Z}_0{}^n$ 上の項順序から $T = T(x_1, ..., x_n)$ 上の項順序が定まる.

- 項順序が整列順序であることを定理 2.11, 系 2.12 で示す.

補題 2.4 $\preceq$ が $\mathbb{Z}_0{}^n$ 上の項順序, $a, b \in \mathbb{Z}_0{}^n$ のとき, $a \preceq a + b$ が成り立つ.

【証明】 定義 2.3 の条件 (2) より, $0 \preceq b$ が成り立つ. これに条件 (1) を用いると $0 + a \preceq b + a$ となるので $a \preceq a + b$ を得る. ∎

- $a, b \in \mathbb{Z}_0{}^n$ が項順序 $\preceq$ について $a \preceq b$ をみたしていても, $b = a + c$ となる $c \in \mathbb{Z}_0{}^n$ が存在するとは限らない. 例えば $\mathbb{Z}_0{}^2$ 上の辞書式順序について $a = (2, 4), b = (3, 1)$ とすると, $a \preceq b$ であるが, $b = a + c$ をみたす $c \in \mathbb{Z}_0{}^n$ は存在しない.

補題 2.5 $\mathbb{Z}_0{}^n$ の項順序 $\preceq$ について次が成り立つ.

$$x_1{}^{i_1} \cdots x_n{}^{i_n} \mid x_1{}^{j_1} \cdots x_n{}^{j_n} \implies (i_1, ..., i_n) \preceq (j_1, ..., j_n)$$

【証明】 仮定より, $x_1{}^{i_1} \cdots x_n{}^{i_n}$ が $x_1{}^{j_1} \cdots x_n{}^{j_n}$ を割り切るので $i_k \leq j_k$ が成り立つ. $r_k = j_k - i_k$ とおけば $(r_1, ..., r_n) \in \mathbb{Z}_0{}^n$ であるから, 補題 2.4 より

$$(i_1, ..., i_n) \preceq (i_1, ..., i_n) + (r_1, ..., r_n) = (j_1, ..., j_n)$$

が得られる. ∎

2.2 モノイデアル

定義 2.6 $\mathbb{Z}_0{}^n$ の部分集合 $L(\neq\emptyset)$ で次の条件をみたすものをモノイデアルという.

$$a\in L,\ \ b\in\mathbb{Z}_0{}^n \implies a+b\in L$$

- モノイデアルは項順序とは独立に定まる概念である.
- p.11 で述べた, T から $\mathbb{Z}_0{}^n$ への全単射により, モノイデアル L に対応する $T=T(x_1,...,x_n)$ の部分集合を T_L とすると, 定義 2.6 の条件は次のようになる.

$$t_L\in T_L,\ \ t\in T \implies t_Lt\in T_L$$

補題 2.7 モノイデアルの和集合はモノイデアルである.

【証明】 $L_i\ (i\in I)$ を $\mathbb{Z}_0{}^n$ のモノイデアルとして, $L=\bigcup_{i\in I}L_i$ がモノイデアルであることを示す. $a\in L, b\in\mathbb{Z}_0{}^n$ とする. ある $i\in I$ に対して $a\in L_i$ であるから, $a+b\in L_i$ が成り立つ. 従って $a+b\in L$ も成り立つ. ゆえに L はモノイデアルである. ∎

命題 2.8 $\mathbb{Z}_0{}^n$ の部分集合 $S(\neq\emptyset)$ に対して

$$\mathrm{Mono}(S)=\{s+a\mid s\in S, a\in\mathbb{Z}_0{}^n\}$$

はモノイデアルである. これを S の生成するモノイデアルという.

【証明】 $b\in\mathrm{Mono}(S), c\in\mathbb{Z}_0{}^n$ とする. 仮定より $b=s+a\ (s\in S, a\in\mathbb{Z}_0{}^n)$ と表される. これより

$$b+c=s+(a+c)\qquad (a+c\in\mathbb{Z}_0{}^n)$$

となるので, $b+c\in\mathrm{Mono}(S)$ が成り立つ. ∎

- 有限集合 $\{a_1,...,a_m\}$ により生成されるモノイデアルを $\mathrm{Mono}(a_1,...,a_m)$ と表す.

- $\mathrm{Mono}(S) = \bigcup_{s \in S} \mathrm{Mono}(s)$ である.

定理 2.9 (ディクソンの補題) $\mathbb{Z}_0{}^n$ のモノイデアルは有限生成である. すなわち, 任意のモノイデアルは適当な有限集合 $\{a_1, ..., a_\ell\}$ により $\mathrm{Mono}(a_1, ..., a_\ell)$ と表される.

【証明】 L を $\mathbb{Z}_0{}^n$ のモノイデアルとして, n に関する帰納法で証明する.

(1) $n = 1$ のとき, L は下に有界, かつ空でない $\mathbb{Z}$ の部分集合であるから, 通常の大小関係での最小元 s を含む. このとき, モノイデアルの定義より $L \supseteq \mathrm{Mono}(s)$ となる. また, $x \in L$ に対して, $s \leq x$ より

$$x = s + (x - s), \qquad x - s \in \mathbb{Z}_0$$

となり, $x \in \mathrm{Mono}(s)$ を得る. 従って $L \subseteq \mathrm{Mono}(s)$ も成り立ち, $L = \mathrm{Mono}(s)$ が得られる. ゆえに, L は有限生成である.

(2) $n = k$ のとき成立すると仮定し, L を $\mathbb{Z}_0{}^{k+1}$ のモノイデアルとする. $\mathbb{Z}_0{}^{k+1} = \mathbb{Z}_0{}^k \times \mathbb{Z}_0$ であるから $\mathbb{Z}_0{}^{k+1}$ の元は

$$(a, i), \qquad a \in \mathbb{Z}_0{}^k, \quad i \in \mathbb{Z}_0$$

と表すことができる. ここで $i \in \mathbb{Z}_0$ に対して

$$L_i = \{a \in \mathbb{Z}_0{}^k \mid (a, i) \in L\}$$

とおく. このとき L がモノイデアルであることから, 任意の $a \in L_i$, $b \in \mathbb{Z}_0{}^k$ に対して, $a \in L_i$ が成り立つことから,

$$a \in L_i \Rightarrow (a, i) \in L \Rightarrow (a, i) + (b, 0) \in L \Rightarrow a + b \in L_i$$

より, $a + b \in L_i$ が成り立つことになる. ゆえに, L_i は $\mathbb{Z}_0{}^k$ のモノイデアルとなり, 帰納法の仮定から有限生成である. 補題 2.7 より

$$\bigcup_{i \in \mathbb{Z}_0} L_i$$

も $\mathbb{Z}_0{}^k$ のモノイデアルとなるが, 帰納法の仮定から有限生成となり

$$\bigcup_{i \in \mathbb{Z}_0} L_i = \mathrm{Mono}(a_1, ..., a_\ell)$$

と表される. 一方, $i,j \in \mathbb{Z}_0$ が $i \leq j$ をみたすとき, 任意の $a \in L_i$ に対して

$$a \in L_i \Rightarrow (a,i) \in L \Rightarrow (a,i)+(0,j-i) \in L \Rightarrow (a,j) \in L \Rightarrow a \in L_j$$

が成り立つので, $L_i \subseteq L_j$ となり

$$L_0 \subseteq L_1 \subseteq L_2 \subseteq \cdots\cdots$$

は昇鎖列である. $a_1,...,a_\ell$ をすべて含むような L_m を一つ選ぶと

$$\cup_{i\in\mathbb{Z}_0} L_i = \mathrm{Mono}(a_1,...,a_\ell)$$

であるから

$$L_0 \subseteq L_1 \subseteq L_2 \subseteq \cdots\cdots \subseteq L_m = L_{m+1} = \cdots\cdots$$

が成り立つ. ここで, $0 \leq i \leq m-1$ の各 i に対して, L_i も有限生成だから

$$L_i = \mathrm{Mono}(b_1^{(i)},...,b_{m_i}^{(i)})$$

と表すことができる. ただし, $L_i = \emptyset$ のときは $m_i = 0$ としておく. このとき L は次の元を含む.

$$(b_1^{(i)},i)...,(b_{m_i}^{(i)},i) \ \ (0 \leq i \leq m-1), \quad (a_1,m)...,(a_\ell,m)$$

これらの元で生成されるモノイデアルを L' とおく. $L = L'$ を示せば証明が完了する. $L \supseteq L'$ は明らかだから, $L \subseteq L'$ を示せばよい. そのために, 任意の $(a,j) \in L$ を選ぶ. $0 \leq j \leq m-1$ のときは

$$a \in L_j = \mathrm{Mono}(b_1^{(j)},...,b_{m_j}^{(j)})$$

であるから

$$a = b_h^{(j)} + a' \qquad (a' \in {\mathbb{Z}_0}^k,\ 1 \leq h \leq m_j)$$

と表されるので,

$$(a,j) = (b_h^{(j)},j) + (a',0) \in L'$$

が成り立つ. $j \geq m$ のときは

$$L_j = L_m = \mathrm{Mono}(a_1, ..., a_\ell)$$

より

$$a = a_h + a' \qquad (a' \in \mathbb{Z}_0{}^k,\ 1 \leq h \leq \ell)$$

と表されるので,

$$(a, j) = (a_h, m) + (a', j - m) \in L'$$

が成り立つ. 以上で $L = L'$ が得られたので, 定理 2.9 が証明された. ∎

系 2.10 $\mathbb{Z}_0{}^n$ のモノイデアルが S で生成されるとき, 有限部分集合 $S_0 \subseteq S$ が存在して, $\mathrm{Mono}(S_0) = \mathrm{Mono}(S)$ をみたす.

【証明】 前述の定理 2.9 より, $\mathrm{Mono}(S)$ は有限生成であるから

$$\mathrm{Mono}(S) = \mathrm{Mono}(a_1, ..., a_\ell) \qquad a_1, ..., a_\ell \in \mathrm{Mono}(S)$$

をみたす $a_1, ..., a_\ell$ が存在する. このとき, 各 a_j は $\mathrm{Mono}(S) = \bigcup_{b \in S} \mathrm{Mono}(b)$ の元であるから

$$a_j = b_j + c_j \qquad b_j \in S,\ c_j \in \mathbb{Z}_0{}^n$$

と表される. これより $\mathrm{Mono}(a_j) \subseteq \mathrm{Mono}(b_j)$ が成り立つので,

$$\mathrm{Mono}(S) = \mathrm{Mono}(a_1, ..., a_\ell) = \bigcup_{i=1}^{\ell} \mathrm{Mono}(a_i) \subseteq \bigcup_{i=1}^{\ell} \mathrm{Mono}(b_i) \subseteq \mathrm{Mono}(S)$$

が得られる. ゆえに $S_0 = \{b_1, ..., b_\ell\}$ とおけば

$$\mathrm{Mono}(S_0) = \bigcup_{i=1}^{\ell} \mathrm{Mono}(b_i) = \mathrm{Mono}(S)$$

が成り立つ. ∎

定理 2.11 $\mathbb{Z}_0{}^n$ 上の項順序は整列順序である.

【証明】 $\mathbb{Z}_0{}^n$ 上の項順序を $\preceq$ とする. $\preceq$ が整列順序であることを示すには, $\mathbb{Z}_0{}^n$ の空でない部分集合 S が最小元をもつことを示せばよい. S で生成され

たモノイデアル $\mathrm{Mono}(S)$ について, 系 2.10 より, S の有限部分集合 S_0 が存在して $\mathrm{Mono}(S_0) = \mathrm{Mono}(S)$ をみたす. S_0 の最小元を s_0 とおく. 任意の $b \in S$ に対して, $S \subseteq \mathrm{Mono}(S_0)$ に注意すれば, ある $s \in S_0$ が存在して,

$$b = s + c \quad (c \in {\mathbb{Z}_0}^n)$$

と表される. $s_0 \preceq s$ であるから, 補題 2.4 より

$$s_0 \preceq s \preceq s + c = b$$

が成り立つ. ゆえに s_0 は S の最小元である. 以上で $\preceq$ が整列順序であることが示された. ∎

$T = T(x_1, ..., x_n)$ 上の項順序は ${\mathbb{Z}_0}^n$ 上の項順序と同一視できることから次の系が成り立つ.

系 2.12 $T = T(x_1, ..., x_n)$ 上の項順序は整列順序である.

3章　グレブナー基底

3章で証明する定理のほとんどすべてが一般の体上の多項式環において成り立つが, この論文では簡単のため, 複素数係数の多項式環 $\mathbb{C}[x_1, ..., x_n]$ において考察する. 以下, この章を通じて, 項のなす集合 $T = T(x_1, ..., x_n)$ 上に一つの項順序 $\preceq$ が与えられているものとする. この項順序のもとに, 先頭項, 先頭単項式, 先頭指数, 単項簡約, 正規形, 正規化などの概念を定義し, すべての多項式が有限回の単項簡約で正規化できることを示す. 次にグレブナー基底を定義し, モノイデアルが有限生成であることを基にグレブナー基底の存在を示す. また, グレブナー基底による正規化が一意に定まることを導く. 最後に, グレブナー基底から極小グレブナー基底が得られること, 極小グレブナー基底から簡約グレブナー基底が得られることを示した後, 簡約グレブナー基底の一意性を証明する.

3.1　単項簡約

まずいくつかの用語と記号を導入する. 簡単のため, $a_{i_1,...,i_n}\, x_1^{i_1} \cdots x_n^{i_n}$ を $a_i X^i$ と略記する.

(1) 係数が 0 でない2つの単項式 $a_i X^i$, $a_j X^j$ に対して

- $X^i \prec X^j$ のとき, $a_i X^i \prec a_j X^j$ と表し, $a_j X^j$ は $a_i X^i$ より大きいという.
- $X^i = X^j$ のとき, $a_i X^i \cong a_j X^j$ と表し, $a_i X^i$ と $a_j X^j$ は同等であるという.

$a_i X^i$ と $a_j X^j$ が同等のとき, 係数を除いた項の部分 X^i と X^j は一致するが, 係数が一致するとは限らない.

(2) 多項式 $f \in \mathbb{C}[x_1, ..., x_n]$ の, 係数が 0 でない単項式の中で, 項順序 $\preceq$ が最大である項からなる単項式を, f の先頭単項式 (leading monomial) といい, $\mathrm{LM}(f)$ と表す. 先

頭単項式は項順序に依存するので, 正確には $\mathrm{LM}_{\prec}(f)$ などと記すべきであるが, この章では項順序 $\preceq$ を一つ固定してあるので, 単に $\mathrm{LM}(f)$ と表すことにする.

(3) $\mathrm{LM}(f) = a_i X^i$ のとき, X^i を先頭項 (leading term) といい, $\mathrm{LT}(f)$ と表す. また, a_i を先頭係数 (leading coefficient) といい, $\mathrm{LC}(f)$ と表す. このとき $\mathrm{LM}(f) = \mathrm{LC}(f)\cdot\mathrm{LT}(f)$ である.

(4) 差 $f - \mathrm{LM}(f)$ を余項といい, $\mathrm{Rem}(f)$ と表す.

(5) $\mathrm{LM}(f) = a_{i_1,\ldots,i_n}\, x_1^{i_1}\cdots x_n^{i_n}$ であるとき, $(i_1,\ldots,i_n)$ を f の先頭指数 (leading exponent) といい, $\mathrm{LE}(f)$ と表す. また, 部分集合 $S \subseteq \mathbb{C}[x_1,\ldots,x_n]$ に対して,

$$\mathrm{LE}(S) = \{\mathrm{LE}(f) \mid f \in S\}$$

とおく. $\mathrm{LE}(S)$ は ${\mathbb{Z}_0}^n$ の部分集合である.

補題 3.1 0 でない $f, g \in \mathbb{C}[x_1,\ldots,x_n]$ に対して, $\mathrm{LM}(fg) = \mathrm{LM}(f)\,\mathrm{LM}(g)$ が成り立つ.

【証明】 $\mathrm{LM}(f) = a_i X^i$, $\mathrm{LM}(g) = b_j X^j$ とする. このとき

$$f = a_i X^i + \mathrm{Rem}(f), \qquad g = b_j X^j + \mathrm{Rem}(g)$$

より,

$$f\,g = a_i\,b_j\,X^{i+j} + \mathrm{Rem}(f)\,(b_j X^j) + (a_i X^i)\,\mathrm{Rem}(g) + \mathrm{Rem}(f)\,\mathrm{Rem}(g)$$

と表される. $\mathrm{Rem}(f)\,(b_j X^j)$ の単項式は, $\mathrm{Rem}(f)$ の単項式 $a_{i'} X^{i'}$ により

$$a_{i'}\,b_j\,X^{i'+j}$$

として表される. $X^i \succ X^{i'}$ であるから, 項順序の定義 2.1 の後の注意より,

$$X^{i+j} \succ X^{i'+j}$$

が成り立つ. 同様に $(a_i X^i)\,\mathrm{Rem}(g)$ の単項式 $a_i\,b_{j'}\,X^{i+j'}$ についても

$$X^{i+j} \succ X^{i+j'}$$

が成り立つ. また, $\mathrm{Rem}(f)\,\mathrm{Rem}(g)$ の単項式は $\mathrm{Rem}(f)$ の単項式 $a_{i'}\,X^{i'}$ と $\mathrm{Rem}(g)$ の単項式 $b_{j'}\,X^{j'}$ の積

$$a_{i'}\,b_{j'}\,X^{i'+j'}$$

として得られるものの中から同類項をまとめた和であるが, 補題 2.2 より

$$X^{i+j} \succ X^{i'+j'}$$

が成り立つ. 以上から

$$\mathrm{LM}(fg) = a_i\,b_j\,X^{i+j} = \mathrm{LM}(f)\,\mathrm{LM}(g)$$

が得られる. ∎

命題 3.2 $\mathbb{C}[x_1, ..., x_n]$ のイデアル I に対して, $\mathrm{LE}(I)$ は ${\mathbb{Z}_0}^n$ のモノイデアルである.

【証明】 $I \neq \emptyset$ であるから, $\mathrm{LE}(I) \neq \emptyset$ である. 次に, $i \in \mathrm{LE}(I)$, $j \in {\mathbb{Z}_0}^n$ とする. このとき, ある $f \in I$ に対して, $\mathrm{LM}(f) = a_i\,X^i$ となる $(a_i \neq 0)$. 従って

$$f = a_i\,X^i + \mathrm{Rem}(f)$$

と表されるが, I はイデアルだから

$$X^j\,f = a_i\,X^{i+j} + X^j\,\mathrm{Rem}(f) \in I$$

が成り立つ. 補題 3.1 より

$$\mathrm{LM}(X^j\,f) = a_i\,X^{i+j}$$

となるので

$$i + j = \mathrm{LE}(X^j\,f) \in \mathrm{LE}(I)$$

が得られる. ゆえに $\mathrm{LE}(I)$ はモノイデアルである. ∎

定義 3.3 $f, g \in \mathbb{C}[x_1, ..., x_n]$, $g \neq 0$ として, f の単項式の中に, g の先頭単項式 $\mathrm{LM}(g)$ の倍数 $M \neq 0$ があるとする. このとき

$$h = f - \frac{M}{\mathrm{LM}(g)} g$$

とおき, f から h を得る操作を g による単項簡約といい,

$$f \xrightarrow[g]{} h$$

と表す.

G を 0 でない多項式の有限集合とする. 多項式 f に G の元による単項簡約を行って多項式 h が得られることを G による単項簡約といい

$$f \xrightarrow[G]{} h$$

と表す. また, f に G による単項簡約を 0 回以上, 有限回行って h が得られることを

$$f \xrightarrow[G]{*} h$$

と表すことにする.

定義 3.4 $G \subseteq \mathbb{C}[x_1, ..., x_n]$ を 0 でない多項式の有限集合とする. 多項式 f に対して G のどの元による単項簡約も行えないとき, f は G に関して正規形であるという. また, 単項簡約を有限回行って正規形に変形することを正規化という.

- 正規化により得られた多項式を「正規化」ということがある.
- f が G に関して正規形であるとは, f のどの単項式も, G の元の先頭単項式の倍数ではないことである.
- 0 はどのような G に対しても正規形である.

注意: 正規形は必ずしも一意的ではない. 例えば, $\mathbb{C}[x_1, x_2]$ 上の辞書式順序で,

$$G = \{x_1^2,\ x_1^2 + x_2\}$$

により x_1^2 を正規化する方法は2通りあり

$$x_1^2 \underset{x_1^2}{\longrightarrow} 0$$

$$x_1^2 \underset{x_1^2+x_2}{\longrightarrow} -x_2$$

と異なる正規形が得られる.

項順序の拡張 p.18 で, 項順序から誘導される単項式の間の関係 $\prec$ と $\cong$ を定義したが, それを多項式の間の関係に拡張しておく.

(1) 任意の多項式 $f \neq 0$ に対して $0 \prec f$ と定める.

(2) 0 でない2つの多項式 f, g については, それらを係数が 0 でない単項式の和として大きい方から順に表す.

$$f = M_1 + M_2 + \cdots M_r \quad (M_1 \succ M_2 \succ \cdots \succ M_r)$$
$$g = N_1 + N_2 + \cdots + N_s \quad (N_1 \succ N_2 \succ \cdots \succ N_s)$$

ここで簡単のため $r \leq s$ として, 次のように定める.

(i) $M_i \cong N_i$ $(i = 1, ..., t-1)$, かつ $M_t \prec N_t$ となる t $(\leq r)$ が存在するとき $f \prec g$ と定める.

(ii) $M_i \cong N_i$ $(i = 1, ..., t-1)$, かつ $M_t \succ N_t$ となる t $(\leq r)$ が存在するとき $f \succ g$ と定める.

(iii) $M_i \cong N_i$ $(i = 1, ..., r)$, かつ $r = s$ のとき, f と g は同等であるといい $f \cong g$ と表す.

(iv) $M_i \cong N_i$ $(i = 1, ..., r)$, かつ $r < s$ のとき $f \prec g$ と定める.

補題 3.5 単項簡約 $f \underset{G}{\longrightarrow} h$ において, $f \succ h$ が成り立つ.

【証明】 単項簡約 $f \underset{G}{\longrightarrow} h$ が $g \in G$ によるものとする. このとき, f の単項式で g の先頭単項式 $\mathrm{LM}(g)$ の倍数であるもの $M \neq 0$ があり,

$$h = f - \frac{M}{\mathrm{LM}(g)} g$$

と表される. ここで f を単項式の和として

$$f = \sum_{M' \succ M} M' + M + \sum_{M'' \prec M} M''$$

と表すと

$$h = \sum_{M' \succ M} M' - \frac{M}{\mathrm{LM}(g)} \mathrm{Rem}(g) + \sum_{M'' \prec M} M''$$

となる. f と h の単項式は M より大きい部分が一致するので

$$f - \sum_{M' \succ M} M' = M + \sum_{M'' \prec M} M''$$

と

$$h - \sum_{M' \succ M} M' = -\frac{M}{\mathrm{LM}(g)} \mathrm{Rem}(g) + \sum_{M'' \prec M} M''$$

を比べればよい. $f - \sum_{M' \succ M} M'$ の先頭単項式は M であり, $h - \sum_{M' \succ M} M'$ の先頭単項式は存在したとしても M より小さい. ゆえに $f \succ h$ が成り立つ. ∎

定理 3.6 $G \subseteq \mathbb{C}[x_1, ..., x_n]$ を 0 でない多項式の有限集合とする. このとき, 任意の多項式 f は, G による単項簡約を有限回行うことにより正規化できる.

【証明】 G による単項簡約を有限回行っても正規化できない多項式が存在したと仮定し, それら全体のなす集合を S とする. ここで

$$\mathrm{LT}(S) = \{\mathrm{LT}(f) \mid f \in S\}$$

とおく. 系 2.12 より $\mathrm{LT}(S)$ に最小元 t_0 が存在する. $\mathrm{LT}(f) = t_0$ となる $f \in S$ を選ぶ. t_0 を項とする f の単項式を M_0 とする. S の定め方から, G による単項簡約の無限列

$$f \xrightarrow[G]{} f^{(1)} \xrightarrow[G]{} f^{(2)} \xrightarrow[G]{} \cdots\cdots$$

が存在する. 仮にある単項簡約

$$f^{(k)} \xrightarrow[G]{} f^{(k+1)}$$

で M_0 が消去されたとすれば, $t_0 \succ \mathrm{LT}(f^{(k+1)})$ となり, $f^{(k+1)} \notin S$ となるので, $f^{(k+1)}$ は G による有限回の単項簡約で正規化されることになる. このとき, f も G による有限回の単項簡約で正規化されることになるので仮定に反する. 従って, どの単項簡約の無限列においても M_0 は消去されない. すなわち, 単項簡約

はすべて $f - M_0$ に対して行われていることになる. しかし, $t_0 \succ \mathrm{LT}(f - M_0)$ となるので, $f - M_0$ は有限回の単項簡約で正規化できるはずであるから, f も有限回の単項簡約で正規化できることになり, 矛盾が生じる. ∎

3.2 グレブナー基底の定義と存在

定義 3.7 (グレブナー基底) $I \neq 0$ を $\mathbb{C}[x_1, ..., x_n]$ のイデアルとする. 0 でない多項式からなる有限集合 $G = \{g_1, ..., g_m\} \subseteq I$ が次の条件 (*) をみたすとき, I の グレブナー基底という.

(*) 任意の $f \in I - \{0\}$ に対して, ある $g_i \in G$ が存在して, $\mathrm{LT}(g_i) \mid \mathrm{LT}(f)$ となる.

- $\{1\}$ は $\mathbb{C}[x_1, ..., x_n]$ のグレブナー基底である.
- 以下, 「イデアル I の グレブナー基底」というときは, $I \neq 0$ が仮定されているものとする.

注意: イデアル I のグレブナー基底は一意に定まるわけではない. $G = \{g_1, ..., g_m\}$ が I のグレブナー基底であるとき, 任意の $f \in I - \{0\}$ を付け加えた $G' = \{g_1, ..., g_m, f\}$ も I のグレブナー基底である.

定理 3.8 (グレブナー基底の存在) $\mathbb{C}[x_1, ..., x_n]$ のイデアル $I \neq 0$ にはグレブナー基底が存在する.

【証明】 $I \neq 0$ をイデアルとする. 命題 3.2 より, $\mathrm{LE}(I)$ は $\mathbb{Z}_0{}^n$ のモノイデアルである. ディクソンの補題 (定理 2.9) より, $\mathrm{LE}(I)$ は有限生成であるから

$$\mathrm{LE}(I) = \mathrm{Mono}(a_1, ..., a_m)$$

と表される. ここで

$$a_i = \mathrm{LE}(g_i) \qquad (i = 1, 2, ..., m)$$

をみたす 0 でない多項式 $g_i \in I$ 選び

$$G = \{g_1, ..., g_m\}$$

が I のグレブナー基底であることを示す. 任意の $f \in I - \{0\}$ に対して,

$$\mathrm{LE}(f) \in \mathrm{LE}(I) = \mathrm{Mono}(a_1, ..., a_m) = \bigcup_{i=1}^{m} \mathrm{Mono}(a_i)$$

であるから,

$$\mathrm{LE}(f) \in \mathrm{Mono}(a_i)$$

となる a_i が存在する. このとき, ある $j \in \mathbb{Z}_0{}^n$ により

$$\mathrm{LE}(f) = a_i + j$$

と表されるので, $X = (x_1, ..., x_n)$ なる略記で

$$\mathrm{LT}(f) = X^{\mathrm{LE}(f)} = X^{a_i} X^j = \mathrm{LT}(g_i) X^j$$

が成り立つ. $\mathrm{LT}(g_i) \mid \mathrm{LT}(f)$ をみたす $g_i \in G$ の存在が示されたので, G は I のグレブナー基底である. ∎

次に, グレブナー基底の諸性質について述べる.

補題 3.9 $G = \{g_1, ..., g_m\}$ が 0 でない多項式からなる有限集合, f が 0 でない多項式, $f \xrightarrow[G]{*} h$ であるとき, 単項式 N_k と $g_{i_k} \in G$ $(1 \leq k \leq \ell)$ が存在して

$$h = f - \sum_{k=1}^{\ell} N_k \, g_{i_k}$$

と表される.

【証明】 仮定より, 適当な $g_{i_k} \in G$ $(1 \leq k \leq \ell)$ が存在して

$$f \xrightarrow[g_{i_1}]{} f^{(1)} \xrightarrow[g_{i_2}]{} f^{(2)} \xrightarrow[g_{i_3}]{} \cdots\cdots\cdots \xrightarrow[g_{i_\ell}]{} f^{(\ell)} = h$$

と表される. また, 単項簡約の定義 (定義 3.3) より, 単項式 N_k $(1 \leq k \leq \ell)$ が存在して

$$\begin{aligned} f^{(1)} &= f - N_1\, g_{i_1} \\ f^{(2)} &= f^{(1)} - N_2\, g_{i_2} = f - (N_1\, g_{i_1} + N_2\, g_{i_2}) \\ &\vdots \qquad\qquad \vdots \\ f^{(\ell)} &= f - (N_1\, g_{i_1} + N_2\, g_{i_2} + \cdots + N_\ell g_{i_\ell}) \end{aligned}$$

が成り立つ. ∎

補題 3.10 $g_1, \ldots, g_m$ を 0 でない多項式, $I = \langle g_1, \ldots, g_m \rangle$, $f \in I - \{0\}$, $f \xrightarrow[G]{*} h$ であるとき, $h \in I$ である.

【証明】 補題 3.9 より, 単項式 N_k と $g_{i_k} \in G$ $(1 \leq k \leq \ell)$ が存在して

$$h = f - \sum_{k=1}^{\ell} N_k\, g_{i_k}$$

と表される. $f \in I$, $g_{i_k} \in I$ $(1 \leq k \leq \ell)$ であるから, $h \in I$ である. ∎

補題 3.11 $G = \{g_1, \ldots, g_m\}$ を イデアル I のグレブナー基底とする. このとき, 任意の $f \in I - \{0\}$ に対して, $f \xrightarrow[G]{*} 0$ が成り立つ.

【証明】 $f \in I - \{0\}$ として, $f \xrightarrow[G]{*} h$ とおく. 補題 3.10 より, $h \in I$ である. ここで, $h \neq 0$ と仮定すると, グレブナー基底の定義 (定義 3.7) より, ある $g_j \in G$ が存在して

$$\mathrm{LT}(g_j) \mid \mathrm{LT}(h)$$

となるが, これは, h が正規形であることに反する. ゆえに $h = 0$ が成り立つ. ∎

定理 3.12 イデアル I のグレブナー基底は I の基底 (生成系) である.

【証明】 $G = \{g_1, \ldots, g_m\}$ をイデアル I のグレブナー基底とする. $I \supseteq \langle g_1, \ldots, g_m \rangle$ は明らかであるから, $I \subseteq \langle g_1, \ldots, g_m \rangle$ を示せばよい. 任意に $f \in I - \{0\}$ を選ぶと, 補題 3.11 より, $f \xrightarrow[G]{*} 0$ が成り立つ. また, 補題 3.9 より, 単

項式 N_k と $g_{i_k} \in G$ $(1 \leq k \leq \ell)$ が存在して

$$0 = f - \sum_{k=1}^{\ell} N_k g_{i_k}$$

が成り立つ. これより,

$$f = \sum_{k=1}^{\ell} N_k g_{i_k} \in \langle g_1, ..., g_m \rangle$$

が得られるので, $I \subseteq \langle g_1, ..., g_m \rangle$ が示された. ∎

任意のイデアル $I \neq 0$ はグレブナー基底をもち, グレブナー基底は I を生成する. グレブナー基底は有限集合であることより, 次の定理が得られる.

系 3.13 (ヒルベルトの基底定理) $\mathbb{C}[x_1, ..., x_n]$ の任意のイデアルは有限生成である.

定理 3.14 (グレブナー基底による正規化の一意性) G がイデアル I のグレブナー基底であるとき, 任意の 0 でない多項式 f の G による正規化は一意的である.

【証明】 f の G による正規化として, 多項式 h_1, h_2 が得られたと仮定する. このとき, 補題 3.9 より, 単項式 N_k, M_k と G の元 g_{i_k}, g_{j_k} が存在して

$$h_1 = f - \sum_{k} N_k g_{i_k}, \qquad h_2 = f - \sum_{k} M_k g_{j_k}$$

が成り立つ. これより

$$h_1 - h_2 = \sum_{k} M_k g_{j_k} - \sum_{k} N_k g_{i_k} \in I$$

が得られる. $h_1 - h_2 \neq 0$ ならば, G がグレブナー基底であることから

$$\mathrm{LT}(g_i) \mid \mathrm{LT}(h_1 - h_2)$$

をみたす $g_i \in G$ が存在することになり, h_1, h_2 が正規形であることに矛盾する. ゆえに $h_1 - h_2 = 0$, すなわち, $h_1 = h_2$ が成り立つ. ∎

- 以下, f のグレブナー基底 G による正規化を $\mathrm{NF}_G(f)$ と表すことにする.

- G がイデアル I のグレブナー基底であるとき, 剰余環 $\mathbb{C}[x_1,...,x_n]/I$ の f の属する剰余類の代表として $\mathrm{NF}_G(f)$ を選ぶことができる.

定理 3.15 G をイデアル I のグレブナー基底とする. このとき, 次の同値が成り立つ.

$$f \in I \iff \mathrm{NF}_G(f) = 0$$

【証明】 $f \in I$ とすると, 補題3.10より, $\mathrm{NF}_G(f) \in I$ となるが, I に含まれる正規形は 0 のみであるから, $\mathrm{NF}_G(f) = 0$ が成り立つ. 逆に, $\mathrm{NF}_G(f) = 0$ と仮定すると, 補題3.9より, 単項式 N_k と $g_{i_k} \in G$ が存在して

$$\mathrm{NF}_G(f) = f - \sum_k N_k\, g_{i_k} = 0$$

となることから,

$$f = \sum_k N_k\, g_{i_k} \in I$$

を得る. ∎

3.3 簡約グレブナー基底

補題 3.16 G をイデアル I のグレブナー基底とする. G の多項式 g, h $(g \neq h)$ が $\mathrm{LT}(g) \mid \mathrm{LT}(h)$ をみたすならば, $G - \{h\}$ も I のグレブナー基底である.

【証明】 任意の $f \in I - \{0\}$ に対して, $g_1 \in G - \{h\}$ で

$$\mathrm{LT}(g_1) \mid \mathrm{LT}(f)$$

となるものが存在することを示せばよい. G は I のグレブナー基底であるから, ある $g_2 \in G$ が存在して

$$\mathrm{LT}(g_2) \mid \mathrm{LT}(f)$$

をみたす. $g_2 \neq h$ ならば $g_2 \in G - \{h\}$ より, $g_1 = g_2$ とすればよい. $g_2 = h$ ならば, $\mathrm{LT}(g) \mid \mathrm{LT}(h)$ より, $\mathrm{LT}(g) \mid \mathrm{LT}(f)$ となるので, $g_1 = g$ とすればよい. ∎

定義 3.17 (極小グレブナー基底) $G = \{g_1, ..., g_m\}$ をイデアル I のグレブナー基底とする. 任意の $1 \leq i \neq j \leq m$ に対して, $\mathrm{LT}(g_i) \nmid \mathrm{LT}(g_j)$ が成り立つとき, G を極小グレブナー基底という.

- 補題 3.16 に従って, グレブナー基底から, 順次, 余分な多項式を取り除くことにより, 極小グレブナー基底が得られる.

補題 3.18 $G = \{g_1, ..., g_m\}$ をイデアル I の極小グレブナー基底とする. このとき, G の各元の先頭項はすべて相異なる.

【証明】 $1 \leq i \neq j \leq m$, かつ $\mathrm{LT}(g_i) = \mathrm{LT}(g_j)$ であるとすれば, $\mathrm{LT}(g_i) \mid \mathrm{LT}(g_j)$ となり, G が極小グレブナー基底であることに反する. ゆえに, G の各元の先頭項はすべて異なる. ∎

定理 3.19 イデアル I の極小グレブナー基底の先頭項からなる集合は極小グレブナー基底の選び方によらず一定である.

【証明】 $G = \{g_1, ..., g_m\}$, $F = \{f_1, ..., f_\ell\}$ をイデアル I の極小グレブナー基底とする. F がグレブナー基底, $g_1 \in I$ であるから, ある $f_j \in F$ が存在して, $\mathrm{LT}(f_j) \mid \mathrm{LT}(g_1)$ となる. 一方, G がグレブナー基底, $f_j \in I$ であるから, ある $g_k \in F$ が存在して, $\mathrm{LT}(g_k) \mid \mathrm{LT}(f_j)$ となる. このとき, $\mathrm{LT}(g_k) \mid \mathrm{LT}(g_1)$ が成り立ち, G は極小グレブナー基底であるから $g_k = g_1$ となる. 従って

$$\mathrm{LT}(f_j) \mid \mathrm{LT}(g_1), \qquad \mathrm{LT}(g_1) \mid \mathrm{LT}(f_j)$$

となるので

$$\mathrm{LT}(g_1) = \mathrm{LT}(f_j)$$

を得る. F の番号を付け替えて

$$\mathrm{LT}(g_1) = \mathrm{LT}(f_1)$$

とする. $m \geq 2$ のときは, F がグレブナー基底, $g_2 \in I$ であるから, ある $f_j \in F$ が存在して, $\mathrm{LT}(f_j) \mid \mathrm{LT}(g_2)$ となる. 上と同様にして

$$\mathrm{LT}(g_2) = \mathrm{LT}(f_j)$$

が得られる. ここで, $\mathrm{LT}(f_1) = \mathrm{LT}(g_1)$, G が極小グレブナー基底であるから $j \geq 2$ である. F の番号を付け替えて

$$\mathrm{LT}(g_2) = \mathrm{LT}(f_2)$$

としてよい. 以下, 同様にすれば, $m = \ell$ であり

$$\mathrm{LT}(g_1) = \mathrm{LT}(f_1),\quad \mathrm{LT}(g_2) = \mathrm{LT}(f_2),\ \ldots\ldots\ldots\ldots,\quad \mathrm{LT}(g_m) = \mathrm{LT}(f_m)$$

が得られる. ∎

- 定理 3.19 より, 極小グレブナー基底の元の個数は一定である.

定義 3.20 (簡約グレブナー基底) イデアル I のグレブナー基底 G が次の 2 条件をみたすとき, I の簡約グレブナー基底であるという.

(1) 任意の $g \in G$ が, $G - \{g\}$ に関して正規形である.

(2) 任意の $g \in G$ に対して $\mathrm{LC}(g) = 1$ である. すなわち, G のどの元の先頭係数も 1 である.

命題 3.21 簡約グレブナー基底は極小グレブナー基底である.

【証明】 $G = \{g_1, \ldots, g_m\}$ をイデアル I の簡約グレブナー基底とする. 今, $i \neq j$, かつ $\mathrm{LT}(g_i) \mid \mathrm{LT}(g_j)$ であると仮定すると, g_j は $G - \{g_j\}$ に関する正規形でないことになり, 矛盾が生じる. よって, $i \neq j$ ならば $\mathrm{LT}(g_i) \nmid \mathrm{LT}(g_j)$ となるので, G は極小グレブナー基底である. ∎

グレブナー基底から次の手順で簡約グレブナー基底が得られる. 特に, 簡約グレブナー基底の存在がわかる.

(1) グレブナー基底から, 補題 3.16 のように, 余分な元を取り除いて, 極小グレブナー基底 G を求める.

(2) 極小グレブナー基底 $G = \{g_1, \ldots, g_m\}$ の元を次のように正規化する.

(i) g_1 を $G - \{g_1\}$ により正規化して g_1^* とする. このとき $\mathrm{LM}(g_1) = \mathrm{LM}(g_1^*)$ である.

(ii) 以下, $i = 2, 3, .., m$ の順に g_i を $\{g_1^*, ..., g_{i-1}^*, g_{i+1}, ..., g_m\}$ により正規化して g_i^* とする. このとき $\mathrm{LM}(g_i) = \mathrm{LM}(g_i^*)$ である.

(iii) $G^* = \{g_1^*, ..., g_m^*\}$ とおくと, g_i^* は $G^* - \{g_i^*\}$ に関して正規形である. なぜならば, 上の手順からわかるように, g_i^* の単項式は $\mathrm{LM}(g_j^*)$ で割りきれないからである $(j \neq i)$.

(3) $\left\{ \dfrac{1}{\mathrm{LC}(g_1*)} g_1^*, ..., \dfrac{1}{\mathrm{LC}(g_m*)} g_m^* \right\}$ は簡約グレブナー基底である.

定理 3.22 (簡約グレブナー基底の一意性) G, F がイデアル I の簡約グレブナー基底であるならば, 集合として $G = F$ が成り立つ.

【証明】 G, F をイデアル I の簡約グレブナー基底とする. 定理 3.19 より,

$$G = \{g_1, ..., g_m\}, \quad F = \{f_1, ..., f_m\}, \quad \mathrm{LT}(g_i) = \mathrm{LT}(f_i) \quad (i = 1, 2, ..., m)$$

とおくことができる. このとき, $g_i - f_i \in I$ であり, $g_i - f_i$ は $G - \{g_i\}$ に関して正規形である. また, $\mathrm{LC}(g_i) = \mathrm{LC}(f_i) = 1$ より, $g_i - f_i$ の各単項式 M が $M \prec \mathrm{LM}(g_i)$ をみたすことに注意すれば, $g_i - f_i$ は G に関して正規形である. ゆえに, 補題 3.11 より, $g_i - f_i = 0$ となるので, $g_i = f_i$ を得る. i は任意であったから, $G = F$ が成り立つ. ∎

4章　ブッフバーガーアルゴリズム

4章では, S 多項式を定義し, イデアルの生成系がグレブナー基底かどうかを判定するブッフバーガーの判定条件を導く. これより, グレブナー基底を求めるブッフバーガーアルゴリズムが得られる. この章でも多項式はすべて複素数係数とし, $T = T(x_1, ..., x_n)$ 上に一つの項順序が与えられているものとする.

4.1　S多項式

以下, 2つの項 t_1, t_2 の最小公倍数である項を $[t_1, t_2]$ と表すことにする. 例えば

$$t_1 = {x_1}^4 x_2 {x_3}^2, \quad t_2 = {x_1}^2 {x_2}^3 x_3 \implies [t_1, t_2] = {x_1}^4 {x_2}^3 {x_3}^2$$

である.

定義 4.1 (S多項式) 0 でない $f, g \in \mathbb{C}[x_1, ..., x_n]$ に対して

$$S(f, g) = \frac{[\mathrm{LT}(f), \mathrm{LT}(g)]}{\mathrm{LM}(f)} f - \frac{[\mathrm{LT}(f), \mathrm{LT}(g)]}{\mathrm{LM}(g)} g$$

とおき, f, g の S 多項式という.

注意：任意の複素数 $\alpha \neq 0$ に対して $S(f, g) = S(f, \alpha g)$ が成り立つ.

- $T = T(x_1, x_2, x_3)$ の項順序を辞書式順序とする.

  $$f(x_1, x_2, x_3) = 2{x_1}^4 x_2 {x_3}^2 + x_1, \quad g(x_1, x_2, x_3) = {x_1}^2 {x_2}^3 x_3 + x_1 x_2^2$$

  のとき,

  $$\mathrm{LT}(f) = {x_1}^4 x_2 {x_3}^2, \quad \mathrm{LT}(g) = {x_1}^2 {x_2}^3 x_3 \implies [\mathrm{LT}(f), \mathrm{LT}(g)] = {x_1}^4 {x_2}^3 {x_3}^2$$

である. 従って f, g の S 多項式は

$$S(f,g) = \frac{1}{2}{x_2}^2\ f(x_1,x_2,x_3) - {x_1}^2x_3\ g(x_1,x_2,x_3) = \frac{1}{2}x_1{x_2}^2 - {x_1}^3{x_2}^2x_3$$

である.

補題 4.2 $G = \{g_1, ..., g_m\}$ は 0 でない多項式の有限集合, f は 0 でない多項式で $f \xrightarrow[G]{*} 0$ であるとする. このとき, 次をみたす多項式 $h_1, ..., h_m$ が存在する.

$$f = \sum_{i=1}^{m} h_i g_i, \qquad \mathrm{LM}(h_i g_i) \preceq \mathrm{LM}(f) \quad (h_i g_i \neq 0 \text{ のとき})$$

【証明】 補題 3.9 より, 0 でない単項式 N_k と, $g_{i_k} \in G\ (1 \leq k \leq \ell)$ が存在して

$$f = \sum_{k=1}^{\ell} N_k\, g_{i_k}$$

と表される. $\mathrm{LM}(N_1\, g_{i_1})$ は f のある単項式と一致するので

$$\mathrm{LM}(N_1\, g_{i_1}) \preceq \mathrm{LM}(f)$$

が成り立つ. 以下, 帰納的に $\mathrm{LM}(N_r\, g_{i_r})$ が

$$f - \sum_{k=1}^{r-1} N_k\, g_{i_k}$$

のある単項式と一致することから

$$\mathrm{LM}(N_r\, g_{i_r}) \preceq \mathrm{LM}\left(f - \sum_{k=1}^{r-1} N_k\, g_{i_k}\right) \preceq \mathrm{LM}(f)$$

が得られる. 従って

$$f = \sum_{k=1}^{\ell} N_k\, g_{i_k}$$

を整理して

$$f = \sum_{i=1}^{m} h_i g_i$$

と表せば, $h_i g_i \neq 0$ であるすべての $h_i g_i$ に対して

$$\mathrm{LM}(h_i g_i) \preceq \mathrm{LM}(f)$$

が成り立つ. ∎

定理 4.3 イデアル $I \neq 0$ と, 0 でない多項式の有限集合 $G = \{g_1, ..., g_m\} \subseteq I$ について, 次の条件は同値である.

(1) G は I のグレブナー基底である.

(2) 任意の $f \in I - \{0\}$ に対して, 次式をみたす多項式 h_i $(1 \leq i \leq m)$ が存在する.

$$f = \sum_{i=1}^{m} h_i g_i, \qquad \mathrm{LM}(h_i g_i) \preceq \mathrm{LM}(f) \quad (h_i g_i \neq 0 \text{ のとき})$$

【証明】 まず, (1) を仮定する. G が I のグレブナー基底であるから, 任意の $f \in I - \{0\}$ に対して, 補題 3.11 より, $f \xrightarrow[G]{*} 0$ が成り立つ. 従って, 補題 4.2 より,

$$f = \sum_{i=1}^{m} h_i g_i, \qquad \mathrm{LM}(h_i g_i) \preceq \mathrm{LM}(f) \quad (h_i g_i \neq 0 \text{ のとき}) \qquad (\bigstar)$$

をみたす多項式 h_i $(1 \leq i \leq m)$ が存在する. ゆえに (2) が成り立つ.

次に, (2) を仮定すると, 任意の $f \in I - \{0\}$ に対して, 上式 $(\bigstar)$ をみたす多項式 h_i $(1 \leq i \leq m)$ が存在する. このとき

$$\mathrm{LM}(f) = \mathrm{LM}\left(\sum_{i=1}^{m} h_i g_i\right)$$

より, ある i に対して

$$\mathrm{LM}(f) \cong \mathrm{LM}(h_i g_i)$$

が成り立つ. これより

$$\mathrm{LT}(g_i) \mid \mathrm{LT}(f)$$

をみたす $g_i \in G$ が存在するので, G は定義 3.7 の条件をみたす. ゆえに, G は I のグレブナー基底である. ∎

系 4.4 $G = \{g_1, ..., g_m\}$ を 0 でない多項式の集合とする. $u, v \in G$ が $S(u, v) \neq 0$, かつ $S(u, v) \xrightarrow[G]{*} 0$ をみたすならば, 多項式 $h_1, ..., h_m$ が存在して, 次が成り立つ.

$$S(u, v) = \sum_{i=1}^{s} h_i g_i, \qquad \mathrm{LT}(h_i g_i) \prec [\mathrm{LT}(u), \mathrm{LT}(v)] \quad (h_i g_i \neq 0 \text{ のとき})$$

【証明】 仮定より, 補題 4.2 を適用すれば,

$$S(u,v) = \sum_{i=1}^{m} h_i g_i, \qquad \mathrm{LM}(h_i g_i) \preceq \mathrm{LM}(S(u,v)) \quad (h_i g_i \neq 0 \text{ のとき})$$

をみたす多項式 $h_1, ..., h_m$ が存在する. 一方, S 多項式の定め方から

$$\mathrm{LM}(S(u,v)) \cong \mathrm{LT}(S(u,v)) \prec [\mathrm{LT}(u), \mathrm{LT}(v)]$$

が成り立つので

$$\mathrm{LT}(h_i g_i) \prec [\mathrm{LT}(u), \mathrm{LT}(v)] \quad (h_i g_i \neq 0 \text{ のとき})$$

を得る. ∎

ここで, いくつかの記号を導入する. ただし, $G = \{g_1, ..., g_m\}$ は 0 でない多項式の有限集合とする.

- $g_i, g_j \in G$ の先頭項 $\mathrm{LT}(g_i), \mathrm{LT}(g_j)$ の最小公倍数である項を

  $$T_{ij} = [\mathrm{LT}(g_i), \mathrm{LT}(g_j)]$$

  と表すことにする.

- $\mathbb{C}[x_1, ..., x_n]$ の元を成分とする m 次元横ベクトルのなす空間を $\mathbb{C}[x_1, ..., x_n]^m$ とおく.

- $\mathbb{C}[x_1, ..., x_n]^m$ の 2 つのベクトル $a = (a_1, .., a_m)$ と $b = (b_1, ..., b_m)$ の内積 $a \circ b$ を

  $$a \circ b = \sum_{i=1}^{m} a_i b_i$$

  と定める.

- $\mathbb{C}[x_1, ..., x_n]^m \ni e_i = (0, .., 1, ..., 0)$ を第 i 成分のみが 1, 他の成分が 0 のベクトルとして

  $$\begin{aligned} S_{ij} &= \frac{T_{ij}}{\mathrm{LM}(g_i)} e_i - \frac{T_{ij}}{\mathrm{LM}(g_j)} e_j \\ &= \frac{T_{ij}}{\mathrm{LM}(g_i)} (0, \ldots, \overset{i}{\overset{\vee}{1}}, \ldots, 0) - \frac{T_{ij}}{\mathrm{LM}(g_j)} (0, \ldots, \overset{j}{\overset{\vee}{1}}, \ldots, 0) \end{aligned}$$

  とおく.

補題 4.5 $G=\{g_1,...,g_m\}$ は 0 でない多項式の有限集合とする．$\mathbb{C}[x_1,...,x_n]^m$ のベクトル $g=(g_1,...,g_m)$ に対して，次が成り立つ．

$$S_{ij}\circ g = S(g_i,g_j)$$

【証明】 S_{ij} の定め方から

$$\begin{aligned} S_{ij}\circ g &= \left(\frac{T_{ij}}{\mathrm{LM}(g_i)}e_i - \frac{T_{ij}}{\mathrm{LM}(g_j)}e_j\right)\circ(g_1,...,g_m) \\ &= \frac{T_{ij}}{\mathrm{LM}(g_i)}g_i - \frac{T_{ij}}{\mathrm{LM}(g_j)}g_j \\ &= S(g_i,g_j) \end{aligned}$$

が成り立つ． ∎

補題 4.6 $G=\{g_1,...,g_m\}$ は 0 でない多項式の有限集合，$M_1,...,M_m$ は 0 でない単項式で，次の 2 条件をみたすとする．

- 項 $t\in T(x_1,...,x_n)$ が存在して，$t=\mathrm{LT}(M_i)\cdot\mathrm{LT}(g_i)$ が成り立つ $(1\le i\le m)$．
- $\sum_{i=1}^{m} M_i\cdot\mathrm{LM}(g_i)=0$

このとき，単項式 $N_1,...,N_m$ が存在して，次が成り立つ．

(1) $(M_1,...,M_m)=\sum_{i=1}^{m-1} N_i\cdot S_{i,i+1}$

(2) $\mathrm{LT}(N_i)\cdot T_{i,i+1}=t \quad (N_i\neq 0 \text{ のとき})$

【証明】 仮定より，t は $\mathrm{LT}(g_i)$ $(i=1,...,m)$ の公倍数であるから，$T_{i,i+1}$ は t を割り切る．ここで，N_i を次のように定める．

$$N_i=\frac{M_1\cdot\mathrm{LM}(g_1)+\cdots+M_i\cdot\mathrm{LM}(g_i)}{T_{i,i+1}} \qquad (1\le i\le m-1)$$

$M_j\cdot\mathrm{LM}(g_j)$ は単項式で，その項は t であるから，上の N_i の定義式の分子は単項式で，その項は t である．従って，N_i は単項式であり，$N_i\neq 0$ のときは

$\mathrm{LT}(N_i)\cdot T_{i,i+1}=t$ となり, (2) が示された. (1) については

$$\begin{aligned}\sum_{i=1}^{m-1} N_i\cdot S_{i,i+1} &= \sum_{i=1}^{m-1}\frac{M_1\cdot\mathrm{LM}(g_1)+\cdots+M_i\cdot\mathrm{LM}(g_i)}{T_{i,i+1}}\left(\frac{T_{i,i+1}}{\mathrm{LM}(g_i)}\,e_i-\frac{T_{i,i+1}}{\mathrm{LM}(g_{i+1})}\,e_{i+1}\right)\\ &= \sum_{i=1}^{m-1}(M_1\cdot\mathrm{LM}(g_1)+\cdots+M_i\cdot\mathrm{LM}(g_i))\left(\frac{1}{\mathrm{LM}(g_i)}\,e_i-\frac{1}{\mathrm{LM}(g_{i+1})}\,e_{i+1}\right)\\ &= M_1e_1+\\ &\quad\sum_{i=2}^{m-1}\frac{(M_1\cdot\mathrm{LM}(g_1)+\cdots+M_i\cdot\mathrm{LM}(g_i))-(M_1\cdot\mathrm{LM}(g_1)+\cdots+M_{i-1}\cdot\mathrm{LM}(g_{i-1}))}{\mathrm{LM}(g_i)}\,e_i\\ &\qquad+\frac{-(M_1\cdot\mathrm{LM}(g_1)+\cdots+M_{m-1}\cdot\mathrm{LM}(g_{m-1}))}{\mathrm{LM}(g_m)}\,e_m\\ &= M_1e_1+\cdots+M_me_m=(M_1,\ldots,M_m)\end{aligned}$$

より, 成り立つ. ∎

定理 4.7 0 でない多項式の有限集合 $G=\{g_1,\ldots,g_m\}$ とイデアル $I=\langle g_1,\ldots,g_m\rangle$ について, 次の条件は同値である.

(1) G は I のグレブナー基底である.

(2) 任意の $u,v\in G$, $S(u,v)\neq 0$, に対して, 次をみたす多項式 h_i $(1\leq i\leq m)$ が存在する.

$$S(u,v)=\sum_{i=1}^{m}h_ig_i,\qquad \mathrm{LT}(h_ig_i)\prec[\mathrm{LT}(u),\mathrm{LT}(v)]\quad(h_ig_i\neq 0\text{ のとき})$$

【証明】 (1) を仮定すると, 任意の $u,v\in G$, $S(u,v)\neq 0$, に対して, $S(u,v)\in I$ より, 補題 3.11 から, $S(u,v)\xrightarrow[G]{*}0$ となるので, 系 4.4 より (2) が成り立つ.

逆に (2) が成り立つと仮定する. 定理 4.3 の条件 (2) をみたすことを示すことにより, G がグレブナー基底であることを導く. G が I の生成系であることから, 任意の $f\in I-\{0\}$ に対して, 次式をみたす多項式 h_i $(1\leq i\leq m)$ が存在する.

$$f=\sum_{i=1}^{m}h_ig_i \qquad (**)$$

式 $(**)$ をみたす多項式 $\{h_i\}$ を適当に選んで, $h_ig_i\neq 0$ のとき

$$\mathrm{LM}(h_ig_i)\preceq\mathrm{LM}(f)$$

が成り立つようにできればよい. そのために式 $(**)$ をみたす多項式 $\{h_i\}$ をど

のように選んでも

$$\mathrm{LM}(h_i g_i) \succ \mathrm{LM}(f)$$

となる h_i が存在すると仮定して矛盾を導くことにする. ここで

$$\{\mathrm{LT}(h_i g_i) \mid h_i g_i \neq 0\}$$

の最大元を t とおく. $T = T(x_1, ..., x_n)$ は整列集合であるから, 式 $(**)$ をみたす多項式 $\{h_i\}$ のなかで t を最小にするものがある. それを改めて $\{h_i\}$ とする. 集合

$$\{i \mid 1 \leq i \leq m,\ h_i g_i \neq 0,\ \mathrm{LT}(h_i g_i) = t\}$$

は空でない. 適当に番号を付け替えて, 上の集合が $\{1, 2, ..., \ell\}$ であるとする. このとき

$$f = \sum_{i=1}^{m} h_i g_i, \qquad t \succ \mathrm{LT}(f)$$

であるから

$$\sum_{i=1}^{\ell} \mathrm{LM}(h_i g_i) = \sum_{i=1}^{\ell} \mathrm{LM}(h_i)\mathrm{LM}(g_i) = 0$$

が成り立つ.

$$t = \mathrm{LT}(h_i g_i) = \mathrm{LT}(h_i)\mathrm{LT}(g_i) \qquad (1 \leq i \leq \ell)$$

であるから, 補題 4.6 が適用できて

- $(\mathrm{LM}(h_1), ..., \mathrm{LM}(h_\ell)) = \sum_{i=1}^{\ell-1} N_i \cdot S_{i,i+1}$
- $\mathrm{LT}(N_i) \cdot T_{i,i+1} = t \quad (N_i \neq 0 \text{ のとき})$

をみたす単項式 $N_1, ..., N_\ell$ の存在することがわかる. 補題 4.5 より,

$$S_{i,i+1} \circ (g_1, ..., g_\ell) = S(g_i, g_{i+1})$$

となることに注意すると

$$(\mathrm{LM}(h_1), ..., \mathrm{LM}(h_\ell)) \circ (g_1, ..., g_\ell) = \sum_{i=1}^{\ell} \mathrm{LM}(h_i) g_i$$

$$\left(\sum_{i=1}^{\ell-1} N_i \cdot S_{i,i+1} \right) \circ (g_1, ..., g_\ell) = \sum_{i=1}^{\ell-1} N_i \cdot S(g_i, g_{i+1})$$

より

$$\sum_{i=1}^{\ell} \mathrm{LM}(h_i)g_i = \sum_{i=1}^{\ell-1} N_i \cdot S(g_i, g_{i+1})$$

が成り立つ．$S(g_i, g_{i+1})$ に定理の条件 (2) を適用すると

$$S(g_i, g_{i+1}) = \sum_{j=1}^{m} h_{ij}g_j \qquad \mathrm{LT}(h_{ij}g_j) \prec T_{i,i+1} \quad (h_{ij}g_j \neq 0 \text{ のとき})$$

と表されることから

$$\sum_{i=1}^{\ell} \mathrm{LM}(h_i)g_i = \sum_{i=1}^{\ell-1} N_i \cdot S(g_i, g_{i+1}) = \sum_{i=1}^{\ell-1} N_i \cdot \left(\sum_{j=1}^{m} h_{ij}g_j \right) = \sum_{j=1}^{m} \left(\sum_{i=1}^{\ell-1} N_i \cdot h_{ij} \right) g_j$$

が得られる．以上から

$$\begin{aligned}
f &= \sum_{i=1}^{m} h_i g_i = \sum_{i=1}^{\ell} h_i g_i + \sum_{i=\ell+1}^{m} h_i g_i \\
&= \sum_{i=1}^{\ell} \left(h_i - \mathrm{LM}(h_i) + \mathrm{LM}(h_i) \right) g_i + \sum_{i=\ell+1}^{m} h_i g_i \\
&= \sum_{i=1}^{\ell} \left(h_i - \mathrm{LM}(h_i) \right) g_i + \sum_{i=1}^{\ell} \mathrm{LM}(h_i) g_i + \sum_{i=\ell+1}^{m} h_i g_i \\
&= \sum_{i=1}^{\ell} \left(h_i - \mathrm{LM}(h_i) \right) g_i + \sum_{j=1}^{m} \left(\sum_{i=1}^{\ell-1} N_i \cdot h_{ij} \right) g_j + \sum_{i=\ell+1}^{m} h_i g_i \\
&= \sum_{i=1}^{\ell} \left(h_i - \mathrm{LM}(h_i) \right) g_i + \sum_{i=1}^{m} \left(\sum_{j=1}^{\ell-1} N_j \cdot h_{ji} \right) g_i + \sum_{i=\ell+1}^{m} h_i g_i \\
&= \sum_{i=1}^{\ell} \left(h_i - \mathrm{LM}(h_i) + \left(\sum_{j=1}^{\ell-1} N_j \cdot h_{ji} \right) \right) g_i + \sum_{i=\ell+1}^{m} \left(h_i + \left(\sum_{j=1}^{\ell-1} N_j \cdot h_{ji} \right) \right) g_i
\end{aligned}$$

が得られる．これを整理して $f = \sum_{i=1}^{m} h'_i g_i$ とおく．$1 \leq i \leq \ell$ のとき

$$h'_i g_i = \left(h_i - \mathrm{LM}(h_i) + \left(\sum_{j=1}^{\ell-1} N_j \cdot h_{ji} \right) \right) g_i$$

となる．ここで $h_i - \mathrm{LM}(h_i)$ は h_i の先頭項が消去されているので，$h_i - \mathrm{LM}(h_i) \neq 0$ であっても，

$$\mathrm{LT}\left((h_i - \mathrm{LM}(h_i)) g_i \right) \prec t$$

である. また, $N_j \cdot h_{ji} \neq 0$ であっても,

$$\mathrm{LT}(N_j) \cdot T_{j,j+1} = t, \quad \mathrm{LT}(h_{ji}g_j) \prec T_{j,j+1} \quad \Longrightarrow \quad \mathrm{LT}(N_j \cdot h_{ji}g_i) \prec t$$

となるので, $h'_i g_i \neq 0$ であっても

$$\mathrm{LT}(h'_i g_i) \prec t \qquad (1 \leq i \leq \ell)$$

が成り立つ. $\ell + 1 \leq i \leq m$ のときも, 同様にして

$$\mathrm{LT}(h_i g_i) \prec t, \quad \mathrm{LT}(N_j \cdot h_{ji}g_i) \prec t \quad \Longrightarrow \quad \mathrm{LT}(h'_i g_i) \prec t$$

が成り立つ. 従って

$$\max\{\mathrm{LT}(h'_i g_i) \mid h'_i g_i \neq 0\} \prec t$$

となるが, これは t が最小となるように $\{h_i\}$ を選んでいたことに矛盾する. 以上で, 定理 4.3 の条件 (2) をみたす $\{h_i\}$ の存在することが示された. ゆえに G は I のグレブナー基底である. ∎

定理 4.8 (ブッフバーガーの判定条件) 0 でない多項式の有限集合 $G = \{g_1, ..., g_m\}$ とイデアル $I = \langle g_1, ..., g_m \rangle$ について, 次の条件は同値である.

(1) G は I のグレブナー基底である.

(2) 任意の $u, v \in G$ に対して, $S(u,v) \xrightarrow[G]{*} 0$ が成り立つ.

【証明】 まず (1) を仮定する. 任意の $u, v \in G$ に対して, $S(u,v) \in I$ であるから, 補題 3.11 より, $S(u,v) \xrightarrow[G]{*} 0$ が成り立つ. 逆に, (2) を仮定すると, 任意の $u, v \in G$, $S(u,v) \neq 0$, に対して, 系 4.4 より,

$$S(u,v) = \sum_{i=1}^{m} h_i g_i, \qquad \mathrm{LT}(h_i, g_i) \prec [\mathrm{LT}(u), \mathrm{LT}(v)] \quad (h_i g_i \neq 0)$$

をみたす多項式 $h_1, ..., h_m$ が存在する. これより, 定理 4.7 の条件 (2) が成り立ち, G は I のグレブナー基底となる. ∎

4.2 ブッフバーガーアルゴリズム

0 でない多項式からなる有限集合 G に対する次の計算手順 (1)〜(5) をブッフバーガーアルゴリズムという.

ブッフバーガーアルゴリズム

(1) $G_1 = G$, $D_1 = \{(u,v) \mid u,v \in G_1, u \neq v\}$ とおく.

(2) $k = 1$ とする.

(3) D_k から 1 組 (u,v) を選び, $S(u,v)$ の G_k による正規化 r を計算する.

(i) $r = 0$ ならば,

$$G_{k+1} = G_k, \quad D_{k+1} = D_k - \{(u,v)\}$$

とおく.

(ii) $r \neq 0$ ならば,

$$G_{k+1} = G_k \cup \{r\}, \quad D_{k+1} = \big(D_k - \{(u,v)\}\big) \cup \big\{\big(w,r\big) \mid w \in G_k\big\}$$

とおく.

(4) (i) $D_{k+1} = \emptyset$ のとき, 計算を終了する.

(ii) $D_{k+1} \neq \emptyset$ のとき, k を $k+1$ と置き換え, (3) の手順に戻る.

- $I = \langle G_k \rangle$ であることに注意されたい $(k = 1, 2, ...)$.

注意: S 多項式の定義の後 (p.32) で注意したように, α が 0 でない複素数のとき, ブッフバーガーアルゴリズムの手順 (3),(ii) で, r を αr に置き換えても S 多項式の計算に影響しないから, ブッフバーガーアルゴリズムに影響はない (最終的に得られるグレブナー基底の多項式 r が αr に置き換わるのみである).

定理 4.9 ブッフバーガーアルゴリズムは有限回の手順で停止する. 停止時の G_k がイデアル $I = \langle G \rangle$ のグレブナー基底である.

【証明】 まず有限回の手順で停止することを示す. ブッフバーガーアルゴリズムの手順 (3) で計算される $S(u,v)$ の正規化 r が常に 0 であれば, (3),(i) の手順が繰り返されるので, ある時点で $D_k = \emptyset$ となり, 計算が停止する. 0 でない正

規化 r が現れるときは, それらの先頭項を順に $h_1, h_2, ...$ とおき, $\mathbb{C}[x_1, ..., x_n]$ のイデアル J を

$$J = \langle h_1, h_2, ... \rangle$$

とする. 系 3.13 より, J は有限生成であるから

$$J = \langle h_{i_1}, h_{i_2}, ..., h_{i_s} \rangle$$

をみたす $h_{i_1}, h_{i_2}, ..., h_{i_s}$ が存在する. ここで,

$$h_{i_s} = \mathrm{LT}(r), \quad r \neq 0 \text{ は } S(u, v) \text{ の正規化}, \quad (u, v) \in D_k$$

であるとする. このとき, 任意の $(w_1, w_2) \in D_\ell$ $(\ell \geq k+1)$ に対して, G_ℓ による $S(w_1, w_2)$ の正規化 r' が 0 となる. なぜならば

$$r' \neq 0, \quad (w_1, w_2) \in D_\ell \quad (\ell \geq k+1)$$

と仮定すると,

$$\mathrm{LT}(r') \in \langle h_{i_1}, h_{i_2}, ..., h_{i_s} \rangle = \{a_1 h_{i_1} + \cdots + a_s h_{i_s} \mid a_1, ..., a_s \in \mathbb{C}[x_1, ..., x_n]\}$$

となる. 従って, $\mathrm{LT}(r')$ が単項式であることに注意すれば, ある単項式 M とある番号 i_t が存在して

$$\mathrm{LT}(r') = M h_{i_t} \qquad (1 \leq t \leq s)$$

が成り立つ. 一方

$$h_{i_1}, h_{i_2}, ..., h_{i_s} \in G_\ell$$

であるから, r' が G_ℓ による正規形であることに矛盾するからである.

任意の $(w_1, w_2) \in D_\ell$ $(\ell \geq k+1)$ に対して, G_ℓ による $S(w_1, w_2)$ の正規化が 0 となれば, D_ℓ $(\ell \geq k+1)$ の元は (3),(i) の手順で 1 個ずつ消去されるので, ある時点で $\emptyset$ となり, 計算が停止する.

計算停止時の G_k は 0 でない多項式からなる I の有限生成系で, 定理 4.8 の (2) をみたすので, I のグレブナー基底である. ∎

計算例 1 $g_1, g_2 \in \mathbb{C}[x_1, x_2]$ を

$$g_1(x_1, x_2) = x_1^2, \qquad g_2(x_1, x_2) = x_1^2 + x_2$$

と定め,

$$G_1 = \{g_1, g_2\}, \qquad I = \langle G_1 \rangle$$

とおく. $\mathbb{C}[x_1, x_2]$ 上の項順序として辞書式順序を選ぶ. p.21 で注意したように, G_1 による正規化は必ずしも一意的ではない. 従って, 定理 3.14 より, G_1 は I のグレブナー基底でない.

G_1, $D_1 = \{(g_1, g_2)\}$ にブッフバーガーアルゴリズムを適用する.

$$S(g_2, g_1) = x_2$$

は G_1 に関して正規形であるから, $g_3(x_1, x_2) = x_2$ として,

$$G_2 = \{g_1, g_2, g_3\}, \quad D_2 = \{(g_1, g_3), (g_2, g_3)\}$$

とする. このとき

$$S(g_1, g_3) = 0, \quad S(g_2, g_3) = x_2^2 \underset{g_3}{\longrightarrow} 0$$

となるので, G_2 は I のグレブナー基底である.

$\mathrm{LT}(g_1) \mid \mathrm{LT}(g_2)$ となるので, 補題 3.16 より

$$G = G_2 - \{g_2\} = \{g_1, g_3\} = \{x_1^2, x_2\}$$

も I のグレブナー基底である. G は, 定義 3.20 の条件をみたすので, I の簡約グレブナー基底である.

計算例 2 3 変数多項式環 $\mathbb{C}[t, x, y]$ の項順序として辞書式順序 $(t > x > y)$ を選ぶ.

$$g_1(t, x, y) = t^2x + t^2 + x - 1 = (1 + t^2)x - (1 - t^2),$$
$$g_2(t, x, y) = t^2y - 2t + y = (1 + t^2)y - 2t$$

として, $G_1 = \{g_1, g_2\}$, $I = \langle G_1 \rangle$ とおく. このとき

$$[\mathrm{LT}(g_1), \mathrm{LT}(g_2)] = [t^2x, t^2y] = t^2xy$$

であるから,

$$S(g_1, g_2) = yg_1 - xg_2 = t^2y + 2tx - y$$
$$\underset{g_2}{\longrightarrow} 2tx + 2t - 2y$$

と正規化されるので, G_1 は I のグレブナー基底でない.

(1) $G_1 = \{g_1, g_2\}$, $D_1 = \{(g_1, g_2)\}$ にブッフバーガーアルゴリズムを適用する.

(2) $S(g_1, g_2)$ の正規化 $2xt + 2t - 2y$ は 0 でないが, これを $\frac{1}{2}$ 倍したものを

$$g_3(t, x, y) = tx + t - y$$

とおき,

$$G_2 = \{g_1, g_2, g_3\}, \qquad D_2 = \{(g_1, g_3), (g_2, g_3)\}$$

とする.

$$g_1(t, x, y) = t^2x + t^2 + x - 1,$$
$$g_2(t, x, y) = t^2y - 2t + y,$$
$$g_3(t, x, y) = tx + t - y$$

(3) $S(g_1, g_3)$ の正規化を計算する.

$$S(g_1, g_3) = g_1 - tg_3 = ty + x - 1$$

より, $S(g_1, g_3)$ 自身が G_2 に関して正規形である. 従って

$$g_4(t, x, y) = ty + x - 1$$

とおき,

$$G_3 = \{g_1, g_2, g_3, g_4\}, \quad D_3 = \{(g_2, g_3), (g_1, g_4), (g_2, g_4), (g_3, g_4)\}$$

とする.

$$g_1(t,x,y) = t^2x + t^2 + x - 1,$$
$$g_2(t,x,y) = t^2y - 2t + y,$$
$$g_3(t,x,y) = tx + t - y$$
$$g_4(t,x,y) = ty + x - 1$$

(4) $S(g_2, g_3)$ の正規化を計算する.

$$\begin{aligned} S(g_2,g_3) = xg_2 - tyg_3 &= -t^2y - 2tx + ty^2 + xy \\ &\underset{g_2}{\longrightarrow} -2tx + ty^2 - 2t + xy + y \\ &\underset{g_3}{\longrightarrow} ty^2 + xy - y \\ &\underset{g_4}{\longrightarrow} 0 \end{aligned}$$

となるので,

$$G_4 = \{g_1, g_2, g_3, g_4\}, \quad D_4 = \{(g_1, g_4), (g_2, g_4), (g_3, g_4)\}$$

とする.

(5) $S(g_1, g_4)$ の正規化を計算する.

$$\begin{aligned} S(g_1,g_4) = yg_1 - txg_4 &= t^2y - tx^2 + tx + xy - y \\ &\underset{g_2}{\longrightarrow} -tx^2 + tx + 2t + xy - 2y \\ &\underset{g_3}{\longrightarrow} 2tx + 2t - 2y \\ &\underset{g_3}{\longrightarrow} 0 \end{aligned}$$

となるので,

$$G_5 = \{g_1, g_2, g_3, g_4\}, \quad D_5 = \{(g_2, g_4), (g_3, g_4)\}$$

とする.

(6) $S(g_2, g_4)$ の正規化を計算する.

$$\begin{aligned} S(g_2,g_4) = g_2 - tg_4 &= -tx - t + y \\ &\underset{g_3}{\longrightarrow} 0 \end{aligned}$$

となるので,

$$G_6 = \{g_1, g_2, g_3, g_4\}, \quad D_6 = \{(g_3, g_4)\}$$

とする.

(7) $S(g_3, g_4)$ の正規化を計算する.

$$\begin{aligned} S(g_3, g_4) &= yg_3 - xg_4 = ty - x^2 + x - y^2 \\ &\underset{g_4}{\longrightarrow} \quad -x^2 - y^2 + 1 \end{aligned}$$

となるので

$$g_5(t, x, y) = x^2 + y^2 - 1$$

として

$$G_7 = \{g_1, g_2, g_3, g_4, g_5\}, \quad D_7 = \{(g_1, g_5), (g_2, g_5), (g_3, g_5), (g_4, g_5)\}$$

とする.

$$\begin{aligned} g_1(t, x, y) &= t^2x + t^2 + x - 1, \\ g_2(t, x, y) &= t^2y - 2t + y, \\ g_3(t, x, y) &= tx + t - y \\ g_4(t, x, y) &= ty + x - 1 \\ g_5(t, x, y) &= x^2 + y^2 - 1 \end{aligned}$$

(8) $S(g_1, g_5)$ の正規化を計算する.

$$\begin{aligned} S(g_1, g_5) &= xg_1 - t^2g_5 = t^2x - t^2y^2 + t^2 + x^2 - x \\ &\underset{g_1}{\longrightarrow} \quad -t^2y^2 + x^2 - 2x + 1 \\ &\underset{g_2}{\longrightarrow} \quad -2ty + x^2 - 2x + y^2 + 1 \\ &\underset{g_4}{\longrightarrow} \quad x^2 + y^2 - 1 \\ &\underset{g_5}{\longrightarrow} \quad 0 \end{aligned}$$

となる. $S(g_2, g_5)$, $S(g_3, g_5)$, $S(g_4, g_5)$ の正規化も 0 になる (計算略). 従って

$$G_{11} = \{g_1, g_2, g_3, g_4, g_5\}, \quad D_{11} = \emptyset$$

となり, G_{11} は I のグレブナー基底であるが, 補題 3.16 より

$$G = \{g_3, g_4, g_5\}$$

も I のグレブナー基底である. G は, 定義 3.20 の条件をみたすので, I の簡約グレブナー基底である.

(9) 以上で

$$I = \langle\, t^2x + t^2 + x - 1,\ t^2y - 2t + y \,\rangle = \langle g_3, g_4, g_5 \rangle$$
$$g_3(t, x, y) = tx + t - y$$
$$g_4(t, x, y) = ty + x - 1$$
$$g_5(t, x, y) = x^2 + y^2 - 1$$

が示された.

注意 : I に含まれる多項式で, 変数 t を含まないものは $x^2 + y^2 - 1$ の倍数であることが知られている.

参考文献

[1] D.S. Dummit, Abstract Algebra, John Wiley, 2004.

[2] 永尾 汎, 代数学, 朝倉書店, 1983.

[3] 野呂正行・横山和弘, グレブナー基底の計算 基礎編, 東京大学出版会, 2003.

[4] 丸山正樹, グレブナー基底とその応用, 共立出版, 2002.