# 平成 10 年度卒業論文
# 多項式環上のイデアルの構成要素に関する問題

指導教官:木村俊一 教官

広島大学理学部数学科
学生番号:0771061J
森島 聖

平成 11 年 2 月 10 日

# 序文

この卒業論文は、多項式環上のイデアルの構成要素に関する問題について考察することを目的とする。

4 年セミナーで、1 年を通し、Ideals, Varieties, and Algorithm (David Cox, John Little, Donal O'Shea 著) を、テキストとして読み進めてきた。この論文の内容は、その中で一番興味を抱いた話題についてまとめたものである。

1 章では、多項式環上のイデアルの構成要素に関する問題を提示するにあたっての必要な語句を定義した。この章の内容は、主に 2 年次の代数学の講義の内容とほとんど重複しており、執筆にあたり私自身にとって基礎理論の復習となった。2 章、3 章では、それぞれ 1 変数と多変数の場合にわけて、多項式環上のイデアルの構成要素に関する問題の解法について考察した。本質的には、多変数の場合についてのみ考察すれば、1 変数の場合については考察する必要はないのだが、多変数の場合について考察するにあたっての基礎理論や、1 変数の場合のみの特有の性質などがあったため、各々の場合について考察した。定理等の証明は、出来る限り記述しようとしたが、Gröbner 基底の計算方法の証明については、そこだけで他のかなりの内容を論じなければならず、本題の目的から少しはずれるので、残念ながら割愛した。また、各章の最後に、数学コンピューターソフト *Mathematica* で作成したプログラムを用いて、具体例についての計算を行った。1 年間のコンピューターセミナーでプログラミングにかなりの力を注いだので、それなりのものは作成出来たと思う。(ちなみに、コンピューターセミナーでの研究成果は、広島大学理学部数学科の代数学、整数論講座のホームページ (http://top2.math.sci.hiroshima-u.ac.jp:80/algebra/index-j.html) にリンクしてある。)

最後に、この論文は、多数の方々の助言、御指導のもとで完成することが出来ました。セミナーの指導教官であった木村俊一先生には、3 年次の代数学の講義で、当時、代数学に対して抽象的で難しいというイメージを抱いていた私に、代数学のおもしろさや、奥深さを教えて頂き、さらに、4 年セミナーやコンピューターセミナーで、多大な御指導を頂きました。また、高橋宣能先生には、忙しいながらも、木村先生の出張時にセミナーに参加して頂き、御指導を頂きました。大学院生の田上恵洋さん、百瀬智行さん、奥田俊一朗さん、川上高史さん、4 年生の中川正史君、安本直史君、研究生の Duncan Tebbs さんには、コンピューターセミナーや、4 年セミナーに出席して頂き、様々な助言を頂きました。そして最後に、1 年間私と一緒にセミナーを進めてきた木村省吾さん、森村靖彦君には、助言を頂いたり、様々な面でお世話になり、楽しくセミナーを進めていくことが出来ました。

4 年間で、様々な面においてお世話になった他の諸先生方や、友人達も含めて、この場を借りて感謝の意を表します。

平成 11 年 2 月 10 日　　広島大学理学部数学科　　森島 聖

# 目 次

# Chapter 1

# 準備

この章では、多項式環上のイデアルの構成要素に関する問題を提示するにあたっての、必要な語句を定義し、最後に、多項式環上のイデアルの構成要素に関する問題を提示する。

## 1.1 可換環と体

**Definition 1.1.1** 集合 $R(\neq \emptyset)$ に、二つの演算
加法:$R \times R \ni (x, y) \longrightarrow x + y \in R$
乗法:$R \times R \ni (x, y) \longrightarrow xy \in R$
が、定義されていて

1. $(x + y) + z = z + (y + z) \quad (\forall x, y, z \in R)$
2. $\exists 0 \in R \ s.t. \ x + 0 = 0 + x = x \quad (\forall x \in R)$
   $0$ を**加法単位元**、または**零元**という。
3. $\exists -x \in R \ s.t. \ x + (-x) = (-x) + x = 0 \quad (\forall x \in R)$
   $-x$ を**加法逆元**という。
4. $x + y = y + x \quad (\forall x, y \in R)$
5. $(xy)z = x(yz) \quad (\forall x, y, z \in R)$
6. $\exists 1 \in R \ s.t. \ 1x = x1 = x \quad (\forall x \in R)$
   $1$ を**乗法単位元**という。
7. $x(y + z) = xy + xz \quad (\forall x, y, z \in R)$
   $(x + y)z = xz + yz \quad (\forall x, y, z \in R)$

を満たすときに、$R$を**環**という。

**Lemma 1.1.1** 零元と乗法単位元は、一意である。

(Proof)
0,$0'$ を零元とすると、 $0 = 0 + 0' = 0'$ より、零元は一意である。
1,$1'$ を乗法単位元とすると、 $1 = 1 \cdot 1' = 1'$ より、乗法単位元は一意である。
(証明終わり)

**Lemma 1.1.2** $\forall x \in R$ に対して、$x$ の加法逆元 $-x$ は、一意である。

(Proof)
$y$,$y'$ を $x$ の加法逆元とすると、$y = y + 0 = y + (x + y') = (y + x) + y' = 0 + y' = y'$ より、
$\forall x \in R$ に対して、$x$ の加法逆元は一意である。
(証明終わり)

**Lemma 1.1.3** $\forall x \in R$ に対し

1. $0 \cdot x = x \cdot 0 = 0$
2. $(-1) \cdot x = x \cdot (-1) = -x$

(Proof)

1. $0 \cdot x = (0 + 0) \cdot x = 0 \cdot x + 0 \cdot x$ よって、$0 \cdot x = 0$ である。
   $x \cdot 0$ についても同様に示せる。
2. $0 = 0 \cdot x = \{1 + (-1)\} \cdot x = x + (-1) \cdot x$ よって、$(-1) \cdot x = -x$ である。
   $x \cdot (-1) = -x$ についても同様に示せる。
   (証明終わり)

**Definition 1.1.2** $R$ を環とする。
$\forall x, y \in R$ に対し、$xy = yx$ を満たすとき、$R$ を**可換環**という。

**Definition 1.1.3** $R \neq \{0\}$ を可換環とする。
$\forall x \in R - \{0\}$ に対し、$\exists x^{-1}$ $s.t.$ $x \cdot x^{-1} = x^{-1} \cdot x = 1$ を満たすとき、$R$ を**体**という。

## 1.2 イデアルと生成元

**Definition 1.2.1** $R$ を可換環とする。
$R$ の部分集合 $I$ が

1. $0 \in I$
2. $x, y \in I \Longrightarrow x + y \in I$
3. $x \in I, a \in R \Longrightarrow ax \in I$

を満たすとき、$I$ を $R$ の**イデアル**という。

**Proposition 1.2.1** $R$ を可換環とする。
$x_1, \cdots, x_n \in R$ に対し

$$S =< x_1, \cdots, x_n >= \left\{ \sum_{i=1}^{n} a_i x_i \mid a_1, \cdots, a_n \in R \right\}$$

とおくと、$S$ は、$R$ の、$x_1, \cdots, x_n$ を含む最小のイデアルになる。

(Proof)

1. $0 = 0x_1 + 0x_2 + \cdots + 0x_n$ より、 $0 \in S$ である。
2. $a = a_1x_1 + \cdots + a_nx_n \quad b = b_1x_1 + \cdots + b_nx_n \quad (a, b \in S)$ とおくと
   $a + b = (a_1 + b_1)x_1 + \cdots + (a_n + b_n)x_n \quad a_i + b_i \in R$ より、$a + b \in S$ である。
3. $\alpha \in R$ に対し $\alpha a = \alpha a_1x_1 + \cdots + \alpha a_nx_n \quad \alpha a_i \in R$より、$\alpha a \in S$ である。

以上により、$S$ は $R$ のイデアルである。

次に、$I$ を、$x_1, \cdots, x_n$ を含むイデアルとする。$s \in S$ とすると、$S$ の定義より

$$s = c_1x_1 + \cdots + c_nx_n \quad (c_1, \cdots, c_n \in R)$$

と表せる。一方、$x_1, \cdots, x_n \in I$ より、Definition 1.2.1 の 3 から、$c_1x_1, \cdots, c_nx_n \in I$ になる。よって、Definition 1.2.1 の 2 から、$s = c_1x_1 + \cdots + c_nx_n \in I$ になる。
以上により、$S$ は、$R$ の、$x_1, \cdots, x_n$ を含む最小のイデアルになる。
(証明終わり)

$< x_1, \cdots, x_n >$ を、$x_1, \cdots, x_n$ **で生成されるイデアル** (または、**有限生成イデアル**)、特に、唯一の元 $x$ で生成されるイデアル $< x >$ を、**単項イデアル**という。また、 $x_1, \cdots, x_n$ を、**生成元**という。

**Proposition 1.2.2** $R$ を可換環、$\Lambda$ を添え字の集合、
$\forall \lambda \in \Lambda$ に対して、$x_\lambda \in R$ とする。このとき

$$T =< x_\lambda \ : \ \lambda \in \Lambda >= \left\{ \sum_{\lambda \in \Lambda} a_\lambda x_\lambda \mid a_\lambda \in R\text{で、有限個の } a_\lambda\text{を除いて } a_\lambda = 0 \right\}$$

とおくと、$T$ は、$R$ の、$\{x_\lambda \mid \lambda \in \Lambda\}$ を含む最小のイデアルになる。

(Proof)

1. $0 = \sum_{\lambda \in \Lambda} 0x_\lambda$ より、 $0 \in T$ である。

2. $a = \sum_{\lambda\in\Lambda} a_\lambda x_\lambda \quad b = \sum_{\lambda\in\Lambda} b_\lambda x_\lambda \quad (a, b \in T)$ とおくと
$a_\lambda \in R$ で、有限個の $a_\lambda$ を除いて $a_\lambda = 0$ かつ $b_\lambda \in R$ で、有限個の $b_\lambda$ を除いて $b_\lambda = 0$ より、$a + b = \sum_{\lambda\in\Lambda} (a_\lambda + b_\lambda)x_\lambda$ となり、$a_\lambda + b_\lambda \in R$ で、有限個の $a_\lambda + b_\lambda$ を除いて $a_\lambda + b_\lambda = 0$ より、$a + b \in T$ である。

3. $\alpha \in R$ に対し $\alpha a = \sum_{\lambda\in\Lambda} \alpha a_\lambda x_\lambda \quad \alpha a_\lambda \in R$ で、有限個の $\alpha a_\lambda$ を除いて $\alpha a_\lambda = 0$ より、$\alpha a \in T$ である。

以上により、$T$ は $R$ のイデアルである。

次に、$I$ を、$\{x_\lambda \mid \lambda \in \Lambda\}$ を含むイデアルとする。$t \in T$ とすると、$T$ の定義より

$$t = \sum_{\lambda\in\Lambda} c_\lambda x_\lambda \quad (c_\lambda \in R \text{ で、有限個の } c_\lambda \text{ を除いて } c_\lambda = 0)$$

と表せる。一方、$\forall\lambda \in \Lambda$ に対して、$x_\lambda \in I$ より、Definition 1.2.1 の 3 から、$\forall\lambda \in \Lambda$ に対して、$c_\lambda x_\lambda \in I$ になる。有限個の $c_\lambda x_\lambda$ を除いて $c_\lambda x_\lambda = 0$ より、Definition 1.2.1 の 2 から、$t = \sum_{\lambda\in\Lambda} c_\lambda x_\lambda \in I$ になる。
以上により、$T$ は、$R$ の、$\{x_\lambda \mid \lambda \in \Lambda\}$ を含む最小のイデアルになる。
(証明終わり)

$< x_\lambda : \lambda \in \Lambda >$ を、$\{x_\lambda \mid \lambda \in \Lambda\}$ **で生成されるイデアル**といい、$\{x_\lambda \mid \lambda \in \Lambda\}$ の元を、**生成元**という。また、$\Lambda$ が有限集合のとき、$< x_\lambda : \lambda \in \Lambda >$ は、明らかに有限生成イデアルになる。

**Proposition 1.2.3** $R$ を可換環とする。
任意のイデアル $I \subset R$ は、いくつか (無限個の場合もありうる) の $I$ の元によって生成される。

(Proof)
$I$ そのものを添え字の集合とみて、$\{x \mid x \in I\}$ という集合を考える。これにより生成されるイデアルを、$J =< x : x \in I >$ とする。このとき、$I = J$ を示す。

($\subset$) Proposition 1.2.2 より、$J$ は、$\{x \mid x \in I\}$ を含む最小のイデアルである。また、明らかに $I = \{x \mid x \in I\}$ であるので、$I \subset J$ である。

($\supset$) $y \in J$ とすると

$$y = \sum_{x\in I} a_x x \quad (a_x \in R \text{ で、有限個の } a_x \text{ を除いて } a_x = 0)$$

と表せる。$\forall x \in I$ に対して、$a_x \in R$ より、$a_x x \in I$ であり、有限個の $a_x x$ を除いて $a_x x = 0$ より、$y = \sum_{x\in I} a_x x \in I$ になる。よって、$I \supset J$ である。

以上により、$I = J$ である。よって、$I =< x \ : \ x \in I >$ と表せるので、$I$ は、$\{x \mid x \in I\}$ によって、生成される。
(証明終わり)

## 1.3 多項式と多項式環

**Definition 1.3.1** 文字 $x_1, \cdots, x_n$ を**変数** (**不定元**)、$\alpha_1, \cdots, \alpha_n$ を非負整数とする。このとき、積 $x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ を、$x_1, \cdots, x_n$ の**単項式**といい、$\alpha_1 + \cdots + \alpha_n$ を**単項式の総次数**という。( 1 変数 $(n = 1)$ の場合は、単に、**単項式の次数**という。)

以後、簡略表記のために、$\alpha = (\alpha_1, \cdots, \alpha_n)$ に対して、$x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ を $x^\alpha$ で表す。また、$x^\alpha$ の総次数を、$|\alpha|$ で表す。

**Definition 1.3.2** $k$を体、$Z_{\geq 0}^n = \{(a_1, \cdots, a_n) \mid a_i \text{ は非負整数 } \}$ とする。

$$f = \sum_\alpha a_\alpha x^\alpha \quad (\alpha \in Z_{\geq 0}^n) \quad (a_\alpha \in k \text{ で、有限個の } a_\alpha \text{ を除いて、} a_\alpha = 0)$$

を、$k$ **の元を係数とする** $n$ **変数** $x_1, \cdots, x_n$ **多項式**という。
さらに、このような任意の多項式全体の集合を $k[x_1, \cdots, x_n]$ と表す。
また、$k$ の元を**定数**という。

**Definition 1.3.3** $f = \sum_\alpha a_\alpha x^\alpha \in k[x_1, \cdots, x_n]$ とする。

1. $a_\alpha$ を、単項式 $x^\alpha$ の**係数**という。
2. $a_\alpha \neq 0$ のとき、$a_\alpha x^\alpha$ を $f$ の**項**という。
3. $a_\alpha \neq 0$ なる任意の $\alpha$ に対し、$|\alpha|$ の最大値を、$f$ の**総次数**といい、$\deg(f)$ と表す。( 1 変数 $(n = 1)$ の場合は、単に、$f$ の**次数**という。)

**Definition 1.3.4** $f = \sum_\alpha a_\alpha x^\alpha, \quad g = \sum_\alpha b_\alpha x^\alpha \in k[x_1, \cdots, x_n]$ に対し
加法: $f + g = \sum_\alpha (a_\alpha + b_\alpha) x^\alpha \in k[x_1, \cdots, x_n]$
乗法: $fg = \sum_\gamma \left( \sum_{\alpha+\beta=\gamma} a_\alpha b_\beta \right) x^\gamma \in k[x_1, \cdots, x_n]$
(但し, $\alpha = (\alpha_1, \cdots, \alpha_n), \quad \beta = (\beta_1, \cdots, \beta_n)$ に対し、$\alpha + \beta := (\alpha_1 + \beta_1, \cdots, \alpha_n + \beta_n)$ )
と定義する。

**Definition 1.3.5** $f, g \in k[x_1, \cdots, x_n]$ に対し、$g = fh$ なる $h \in k[x_1, \cdots, x_n]$ が存在するとき、$f$ は $g$ を**割り切る**という。

**Theorem 1.3.1** $k[x_1, \cdots, x_n]$ は、*Definition 1.3.4* で定義した、加法、乗法に関して可換環になる。
以後、$k[x_1, \cdots, x_n]$ を**多項式環**という。

(Proof)
$f = \sum_{\alpha} a_\alpha x^\alpha, \quad g = \sum_{\alpha} b_\alpha x^\alpha, \quad h = \sum_{\alpha} c_\alpha x^\alpha \in k[x_1, \cdots, x_n]$ とする。

1. $(f+g)+h = \sum_{\alpha}(a_\alpha + b_\alpha)x^\alpha + \sum_{\alpha} c_\alpha x^\alpha = \sum_{\alpha}\{(a_\alpha + b_\alpha) + c_\alpha\}x^\alpha = \sum_{\alpha}\{a_\alpha + b_\alpha + c_\alpha\}x^\alpha$
$= \sum_{\alpha}\{a_\alpha + (b_\alpha + c_\alpha)\}x^\alpha = \sum_{\alpha} a_\alpha x^\alpha + \sum_{\alpha}(b_\alpha + c_\alpha)x^\alpha = f + (g+h)$

2. $0 \in k[x_1, \cdots, x_n]$ が、加法単位元になっている。

3. $f$ に対し、$-f \in k[x_1, \cdots, x_n]$ が、加法逆元になっている。

4. $f + g = \sum_{\alpha}(a_\alpha + b_\alpha)x^\alpha = \sum_{\alpha}(b_\alpha + a_\alpha)x^\alpha = g + f$

5. $(fg)h = \sum_{\gamma}\left(\sum_{\alpha+\beta=\gamma} a_\alpha b_\beta\right)x^\gamma \cdot \sum_{\gamma} c_\gamma x^\gamma = \sum_{r}\left\{\sum_{p+q=r}\left(\sum_{\alpha+\beta=p} a_\alpha b_\beta\right)c_q\right\}x^r$
$= \sum_{r}\left\{\sum_{p+q=r}\left(\sum_{\alpha+\beta=p} a_\alpha b_\beta c_q\right)\right\}x^r = \sum_{r}\left\{\sum_{\alpha+\beta+q=r} a_\alpha b_\beta c_q\right\}x^r$
$= \sum_{r}\left\{\sum_{\alpha+p=r} a_\alpha\left(\sum_{\beta+q=p} b_\beta c_q\right)\right\}x^r = \sum_{\alpha} a_\alpha x^\alpha \cdot \sum_{\alpha}\left(\sum_{\beta+q=\alpha} b_\beta c_q\right)x^\alpha = f(gh)$

6. $1 \in k[x_1, \cdots, x_n]$ が、乗法単位元になっている。

7. $f(g+h) = \sum_{\alpha} a_\alpha x^\alpha \cdot \sum_{\alpha}(b_\alpha + c_\alpha)x^\alpha = \sum_{\gamma}\left\{\sum_{\alpha+\beta=\gamma} a_\alpha(b_\beta + c_\beta)\right\}x^\gamma$
$= \sum_{\gamma}\left(\sum_{\alpha+\beta=\gamma} a_\alpha b_\beta + \sum_{\alpha+\beta=\gamma} a_\alpha c_\beta\right)x^\gamma = \sum_{\gamma}\left(\sum_{\alpha+\beta=\gamma} a_\alpha b_\beta\right)x^\gamma + \sum_{\gamma}\left(\sum_{\alpha+\beta=\gamma} a_\alpha c_\beta\right)x^\gamma$
$= fg + fh$

   $(f+g)h = fh + gh$ も、8. の乗法に関する可換性より、成り立つ。

8. $fg = \sum_{\gamma}\left(\sum_{\alpha+\beta=\gamma} a_\alpha b_\beta\right)x^\gamma = \sum_{\gamma}\left(\sum_{\beta+\alpha=\gamma} b_\beta a_\alpha\right)x^\gamma = gf$

以上により、$k[x_1, \cdots, x_n]$ は、可換環である。
(証明終わり)

## 1.4　多項式環上のイデアルの構成要素に関する問題

多項式環 $k[x_1, \cdots, x_n]$ 上 のイデアル $I \subset k[x_1, \cdots, x_n]$ と、多項式 $f \in k[x_1, \cdots, x_n]$ に対して、$f$ が $I$ の元になっているかどうかという問題を、**多項式環上のイデアルの構成要素に関する問題**とする。3 章で紹介する Hilbert の基底定理によって、任意のイデアル $I$ は、有限生成イデアル (特に、$n = 1$ のときは、単項イデアル) であらわされるので、実際は $f$ が $f_1, \cdots, f_s$ で生成されるイデアル $< f_1, \cdots, f_s >$ の元になっているかどうかの判定法を、2 章では、1 変数多項式環 $k[x]$ について、3 章では、多変数 ($n$ 変数) 多項式環 $k[x_1, \cdots, x_n]$ について論じていく。そして、各章の最後には、数学コンピューターソフト $Mathematica$ でプログラムを組み、具体例について、実際に計算をしていく。

# Chapter 2

# 1 変数多項式環上のイデアルの構成要素に関する問題

この章では、1 変数多項式環 $k[x]$ 上のイデアルの構成要素に関する問題について論じる。

## 2.1 1 変数多項式

**Definition 2.1.1** $f \in k[x]$ に対し

$$f = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_0 \quad (a_m \neq 0 \quad i.e. \quad \deg(f) = m)$$

とする。このとき、$a_m x^m$ を $f$ **の最高次の項**といい、$LT(f)$ と表す。

**Lemma 2.1.1** $f, g \in k[x]$ を零でない多項式とする。このとき

$$\deg(f) \leq \deg(g) \Longleftrightarrow LT(f) \text{ は } LT(g) \text{ を割り切る。}$$

(Proof)
$LT(f) = ax^m, LT(g) = bx^n \quad (a \neq 0, b \neq 0) \quad$ とする。
$(\Longrightarrow) \quad \deg(f) \leq \deg(g)$ より $\quad m \leq n$ である。

$$LT(g) = bx^n = ba^{-1}x^{n-m} \cdot ax^m = ba^{-1}x^{n-m} \cdot LT(f)$$

より、$LT(f)$ は $LT(g)$ を割り切る。

$(\Longleftarrow) \quad LT(f)$ は $LT(g)$ を割り切るので
$\exists cx^l \in k[x] \quad (c \neq 0, l \geq 0) \quad s.t. \quad LT(g) = cx^l \cdot LT(f) = cx^l \cdot ax^m = cax^{l+m}$
よって

$$\deg(g) = \deg(LT(g)) = \deg(cax^{l+m}) = l + m = l + \deg(f)$$

$l \geq 0$ より、$\deg(f) \leq \deg(g)$ である。
(証明終わり)

**Lemma 2.1.2** $f, g \in k[x]$ を零でない多項式とする。このとき

$$\deg(fg) = \deg(f) + \deg(g)$$

(Proof)
$f = \sum_{\alpha} a_\alpha x^\alpha, \quad g = \sum_{\alpha} b_\alpha x^\alpha \quad \deg(f) = m, \quad \deg(g) = n \quad$ とする。
$fg = \sum_{\gamma} c_\gamma x^\gamma \quad (c_\gamma = \sum_{\alpha+\beta=\gamma} a_\alpha b_\beta)$ で、$\deg(fg)$ は定義より、$c_\gamma \neq 0$ なる任意の $\gamma$ の最大値である。$\gamma > m+n$ なる任意の $\gamma$ に対しては、明らかに $c_\gamma = 0$ であり、$\gamma = m+n$ のときは、$c_\gamma = a_m b_n \neq 0$ より、$\deg(fg) = m+n = \deg(f) + \deg(g)$ である。
(証明終わり)

Lemma 2.1.2 は、一般に、多変数多項式環についても成り立つ。

## 2.2 除法定理

**Theorem 2.2.1 (除法定理)** $f, g \in k[x] \quad (g \neq 0)$ に対し

1. $f = qg + r \quad (r = 0 \quad$ または $\quad \deg(r) < \deg(g))$
   を満たす $q, r \in k[x]$ が存在する。( $q$ を**商**、$r$ を**余り**という。)

2. $q, r$ は一意である。

(Proof)

1. $f = 0$ または $\deg(f) < \deg(g)$ のとき、$q = 0,\ r = f$ とすると、1 は成り立つ。
   $\deg(f) \geq \deg(g) \quad (f \neq 0)$ のとき

   $$\begin{cases} f = a_m x^m + a_{m-1} x^{m-1} + \cdots + a_0 \\ g = b_n x^n + b_{n-1} x^{n-1} + \cdots + b_0 \end{cases} \qquad (a_m \neq 0, b_n \neq 0, m \geq n)$$

   とする。$m = 0$ のとき、$f = a_0,\ g = b_0$ より、$q = a_0 b_0^{-1},\ r = 0$ とすると、1 は成り立つ。
   次数が $m(\geq 1)$ より小さい $f$ に対して、1 は成り立つと仮定すると、
   $f_0 = f - a_m b_n^{-1} x^{m-n} g$ は、$\deg(f_0) < m$ より

   $$f_0 = q_0 g + r_0 \quad (r_0 = 0 \quad \text{または} \quad \deg(r_0) < \deg(g))$$

   を満たす $q_0, r_0$ が存在する。

   $$f = f_0 + a_m b_n^{-1} x^{m-n} g = q_0 g + r_0 + a_m b_n^{-1} x^{m-n} g = (q_0 + a_m b_n^{-1} x^{m-n}) g + r_0$$

   より、$q = q_0 + a_m b_n^{-1} x^{m-n},\ r = r_0$ とすると、1 は成り立つ。

2. $f = qg + r = q'g + r'$
   $(r = 0 \quad \text{または} \quad \deg(r) < \deg(g)) \quad (r' = 0 \quad \text{または} \quad \deg(r') < \deg(g))$
   とすると
   $(q - q')g = r' - r$ となる。
   $q - q' \neq 0$ と仮定すると、左辺は零でない多項式で次数は $\deg(g)$ 以上になる。一方、右辺は、零多項式か、次数が $\deg(g)$ より小さい多項式になるので、矛盾。
   よって、$q = q',\ r = r'$ になり、$q, r$ は一意である。

(証明終わり)

**Proposition 2.2.1** $k[x]$ 上のすべてのイデアルは、零でない定数倍を除いて、ある $f \in k[x]$ によって一意に $< f >$ と表される。(つまり、単項イデアルになる。)

(Proof)
$I \subset k[x]$ をイデアルとする。
$I = \{0\}$ のとき、$I =< 0 >$ とおけば成り立つ。
$I \neq \{0\}$ のとき、$f$ を $I$ の元の中の零でない多項式で、次数が最小のものとする。
このとき、$< f >= I$ を示す。
$(\supset) \quad \forall af \in < f > \quad (a \in f[x])$ に対し、イデアルの定義より、$af \in I$ である。

$(\subset) \quad g \in I$ とする。除法定理より

$$g = qf + r \quad (r = 0 \quad \text{または} \quad \deg(r) < \deg(f))$$

と表せる。イデアルの定義より、$g, qf \in I$ に対し、$r = g - qf \in I$
$r \neq 0$ ならば、$\deg(r) < \deg(f)$ より、$f$ の次数の最小性に矛盾する。よって、$r = 0$ より、$g = qf \in < f >$ である。

以上により、$< f >= I$ が示された。

次に、$f$ は、零でない定数倍を除いて一意であることを示す。

$f = 0 \iff < f >= \{0\}$ より、$f = 0$ のときは、零でない定数倍を除かなくても一意であるので、$f \neq 0$ とする。
$< f >=< g > \quad (g \neq 0)$ とすると、$f \in < g >$ より、$f = hg \quad (h \in k[x],\ h \neq 0)$ と表せる。
$\deg(f) = \deg(hg) = \deg(h) + \deg(g) \quad$ よって、$\deg(f) \geq \deg(g)$
$f$ と $g$ の立場を入れかえると、同様に $\deg(f) \leq \deg(g)$ となる。よって、$\deg(f) = \deg(g)$ より、$\deg(h) = 0$ となるので、$h$ は零でない定数である。よって、$f$ は零でない定数倍を除いて一意である。
(証明終わり)

## 2.3 最大公約多項式

1 章の最後で、3 章で紹介する Hilbert の基底定理により、多項式環上の任意のイデアルは、いくつかの有限個の生成元 $f_1, \cdots, f_s$ で生成される ($i.e. \quad < f_1, \cdots, f_s >$ となる。) と

いうことを述べた。しかし、前節で述べたように、1 変数多項式環上においては、任意のイデアルは、さらに単項イデアル ($i.e.\quad \exists f \in k[x] \quad s.t. \quad < f >=< f_1, \cdots, f_s >$) になっていることをみた。この節では、最大公約多項式を定義し、$f_1, \cdots, f_s$ の最大公約多項式が $f$ になっていることを証明する。

**Definition 2.3.1** $f, g \in k[x]$ に対し、$h \in k[x]$ が

1. $h$ は、$f, g$ を割り切る。
2. $p \in k[x]$ を、$f, g$ を割り切るとすると、$p$ は $h$ を割り切る。

を満たすとき、$h$ を**最大公約多項式**といい、$h = GCD(f, g)$ と表す。

**Proposition 2.3.1** $f, g \in k[x]$ とする。

1. $GCD(f, g)$ は、零でない定数倍を除いて一意に存在する。
2. $GCD(f, g)$ で生成される単項イデアルは、$< f, g >$ に等しい。

(Proof)
Proposition 2.2.1 より、$k[x]$ のイデアル $< f, g >$ は、ある $h \in k[x]$ に対し、
$< f, g >=< h >$ と表せる。このとき、$h = GCD(f, g)$ を示す。
$f, g \in < h >$ より、$h$ は $f, g$ を割り切る。よって、Definition 2.3.1 の 1 を満たす。
次に、$p \in k[x]$ を、$f, g$ を割り切るとすると

$$f = Cp \quad g = Dp \quad (C, D \in k[x])$$

と表せる。
また、 $h \in < f, g >$ より

$$h = Af + Bg \quad (A, B \in k[x])$$

と表せる。
$h = ACp + BDp = (AC + BD)p$ となるので、$p$ は $h$ を割り切る。
よって、Definition 2.3.1 の 2 を満たす。よって、$h = GCD(f, g)$ となる。
これにより、存在性と 2 が示された。
次に、$h' = GCD(f, g)$ とすると、Definition 2.3.1 の 2 より、$h, h'$ はおのおのを割り切る。
よって、$h'$ は $h$ の零でない定数倍になる。
(証明終わり)

**Lemma 2.3.1** $f \in k[x]$ に対し

$$GCD(f, 0) = GCD(0, f) = f$$

(Proof)
$f$ は、$f$、0 を割り切る。また、$p \in k[x]$ を、$f$、0 を割り切るとすると、$p$ は $f$ を割り切る。よって、$f = GCD(f, 0) = GCD(0, f)$ である。
(証明終わり)

最大公約多項式の概念は、3 つ以上の多項式の場合に拡張出来る。

**Definition 2.3.2** $f_1, \cdots, f_s \in k[x]$ に対し、$h \in k[x]$ が

1. $h$ は、$f_1, \cdots, f_s$ を割り切る。
2. $p \in k[x]$ が、$f_1, \cdots, f_s$ を割り切るとすると、$p$ は $h$ を割り切る。

を満たすとき、$h$ を**最大公約多項式**といい、$h = GCD(f_1, \cdots, f_s)$ と表す。

**Proposition 2.3.2** $f_1, \cdots, f_s \in k[x] \quad (s \geq 2)$ とする。

1. $GCD(f_1, \cdots, f_s)$ は、零でない定数倍を除いて一意に存在する。
2. $GCD(f_1, \cdots, f_s)$ で生成される単項イデアルは、$< f_1, \cdots, f_s >$ に等しい。
3. $s \geq 3$ のとき
   $GCD(f_1, \cdots, f_s) = GCD(f_1, GCD(f_2, \cdots, f_s))$

(Proof)
1,2 は、Proposition 2.3.1 と同様の方法で証明出来る。よって、3 のみを示す。
$h = GCD(f_2, \cdots, f_s)$ とする。

$$f_1 = f_1 + 0 \cdot f_2 + \cdots + 0 \cdot f_s \in < f_1, \cdots, f_s >$$

$< h >=< f_2, \cdots, f_s >$ より、$h \in < f_2, \cdots, f_s >$ なので、
$h = a_2 f_2 + \cdots + a_s f_s \quad (a_2, \cdots, a_s \in k[x])$ と表せる。よって、

$$h = 0 \cdot f_1 + a_2 f_2 + \cdots + a_s f_s \in < f_1, \cdots, f_s >$$

以上により、$< f_1, \cdots, f_s > \supset < f_1, h >$ となる。

逆に、

$$f_1 = f_1 + 0 \cdot h \in < f_1, h >$$

$< h >=< f_2, \cdots, f_s >$ より、$f_i = b_i h \quad (b_i \in k[x] \quad 2 \leq i \leq s)$ と表せる。よって、

$$f_i = 0 \cdot f_1 + b_i h \in < f_1, h >$$

以上により、$< f_1, \cdots, f_s > \subset < f_1, h >$ となる。

よって、$< f_1, \cdots, f_s >=< f_1, h >$ となる。

Proposition 2.3.2 の 2 より、$< GCD(f_1, \cdots, f_s) >=< GCD(f_1, h) >$ となり、
最大公約多項式は、零でない定数倍を除いて一意より、
$GCD(f_1, \cdots, f_s) = GCD(f_1, h) = GCD(f_1, GCD(f_2, \cdots, f_s))$
(証明終わり)

## 2.4 1 変数多項式環上のイデアルの構成要素に関する問題の解法

$f, f_1, \cdots, f_s \in k[x]$ に対し、$f$が $< f_1, \cdots, f_s >$ の元であるか否かを調べたい。$h = GCD(f_1, \cdots, f_s)$ とすると、$< f_1, \cdots, f_s >=< h >$ となるので、この問題は、$f$ が $< h >$ の元であるか否かに帰着される。$h = 0$ ならば、(つまり、$f_1 = \cdots f_s = 0$ のとき ) $< h >$ の元は、0 のみになるので、$h \neq 0$ の場合について考える。除法定理により、$f = qh + r \quad (r = 0$ または $\deg(r) < \deg(h))$ と、一意に表せる。もし、$r = 0$ ならば、$f = qh \in < h >$であり、$r \neq 0$ ならば、$\deg(r) < \deg(h)$ から、$r \notin < h >$ より、$f = qh + r \notin < h >$ である。

論理的には解決出来たが、実際問題として、$h, q, r$ の存在のみを証明して、求め方については論じていなかったので、具体例について計算が出来ない。そこで、除法定理における $q, r$ と、最大公約多項式 $h$ を求める計算方法を紹介する。

**Proposition 2.4.1** $f, g \in k[x] \quad (g \neq 0)$ に対し、除法定理による

$$f = qg + r \quad (r = 0 \quad \text{または} \quad \deg(r) < \deg(g))$$

なる、$q, r \in k[x]$ を求める計算方法がある。

(Proof)
$m, n \in Z_{\geq 0} \quad (n \geq m) \quad q_0 = 0,\ r_0 = f$ とし、$n \geq m + 1$ を満たす $m$ について

$$\begin{cases} q_{m+1} = q_m + \dfrac{LT(r_m)}{LT(g)} \\ r_{m+1} = r_m - \dfrac{LT(r_m)}{LT(g)} g \end{cases}$$

とする。但し、$n$ は、( $r_m = 0$ または $\deg(r_m) < \deg(g)$ ) を初めて満たす $m$ とする。このとき、$q_n, r_n$ が、求める $q, r$ であることを示す。

1. まず、任意の $m$ に対し、$f = q_m g + r_m$ であることを示す。
   $m = 0$ のとき
   $$q_0 g + r_0 = 0 \cdot g + f = f$$
   $m \geq 1$ のとき、$m - 1$ まで成り立つと仮定すると
   $$q_m g + r_m = \left\{ q_{m-1} + \frac{LT(r_{m-1})}{LT(g)} \right\} g + \left\{ r_{m-1} - \frac{LT(r_{m-1})}{LT(g)} g \right\} = q_{m-1} g + r_{m-1} = f$$
   よって、任意の $m$ に対して、$f = q_m g + r_m$ より、$q_n, r_n$ は、$f = q_n g + r_n$ を満たす。
2. $n$ の条件より、$r_n$ は、( $r_n = 0$ または $\deg(r_n) < \deg(g)$ ) を満たすのは当たり前である。

3. 最後に、条件を満たす $n$ が存在することを示す。( つまり、ある $n$ で、$r_n = 0$ または、$\deg(r_n) < \deg(g)$ が成り立ち、有限回の計算で、終わることを示す。 )
( $r_m \neq 0$ かつ $\deg(r_m) \geq \deg(g)$ ) を満たす $m$ に対し

$$r_m = a_i x^i + \cdots + a_0 \quad ( a_i \neq 0 )$$

$$g = b_j x^j + \cdots + b_0 \quad ( b_j \neq 0 )$$

とする。

$$r_{m+1} = r_m - \frac{LT(r_m)}{LT(g)} g = a_i x^i + \cdots + a_0 - \frac{a_i x^i}{b_j x^j}(b_j x^j + \cdots + b_0)$$

$$= a_{i-1} x^{i-1} + \cdots + a_0 - \left( \frac{a_i x^i}{b_j x^j} b_{j-1} x^{j-1} + \cdots + \frac{a_i x^i}{b_j x^j} b_0 \right)$$

$$= a_{i-1} x^{i-1} + \cdots + a_0 - \frac{a_i}{b_j}(b_{j-1} x^{i-1} + \cdots + b_0 x^{i-j})$$

よって、$r_{m+1}$ は、次数が下がるか、0 になる。このことをくり返すことにより、
( $r_n = 0$ または $\deg(r_n) < \deg(g)$ ) を満たす $n$ が存在することが示される。

以上により、$q_n, r_n$ が、求める $q, r$ であることが示された。
(証明終わり)

**Proposition 2.4.2** $f_1, \cdots, f_s \in k[x]$ に対し

$$h = GCD(f_1, \cdots . f_s)$$

を満たす $h$ を求める計算方法がある。

(Proof)
まず、$f$、$g \in k[x]$ に対する $GCD(f, g)$ を求める計算方法があることを示す。
$g = 0$ ならば、$GCD(f, g) = GCD(f, 0) = f$ より、求まるので、$g \neq 0$ とする。除法定理により

$$f = q_1 g + r_1 \quad (r_1 = 0 \text{ または } \deg(r_1) < \deg(g))$$

と表せる。まず、$< f, g > = < f - q_1 g, g >$ を示す。

$$f = 1 \cdot (f - q_1 g) + q_1 \cdot g \in < f - q_1 g, g >$$

$$g = 0 \cdot (f - q_1 g) + 1 \cdot g \in < f - q_1 g, g >$$

以上により、$< f, g > \subset < f - q_1 g, g >$ となる。

$$f - q_1 g = 1 \cdot f - q_1 \cdot g \in < f, g >$$

$$g = 0 \cdot f + 1 \cdot g \in < f, g >$$

以上により、$< f, g > \supset < f - q_1 g, g >$ となる。
よって、$< f, g > = < f - q_1 g, g >$ が示された。このことより

$$GCD(f, g) = GCD(f - q_1 g, g) = GCD(r_1, g) = GCD(g, r_1)$$

$$(r_1 = 0 \quad \text{または} \quad \deg(r_1) < \deg(g))$$

$r_1 = 0$ ならば、$GCD(f, g) = GCD(g, 0) = g$ より、求まる。
$r_1 \neq 0$ とする。同様に除法定理により

$$g = q_2 r_1 + r_2 \quad (r_2 = 0 \quad \text{または} \quad \deg(r_2) < \deg(r_1))$$

同様に

$$GCD(g, r_1) = GCD(r_1, r_2) \quad (r_2 = 0 \quad \text{または} \quad \deg(r_2) < \deg(r_1))$$

同様にくり返していくと、途中で $r_i = 0$ なる $i$ が存在する。もしくは

$$\deg(g) > \deg(r_1) > \deg(r_2) > \deg(r_3) > \cdots\cdots$$

のように次数が下がっていく。もし、$\deg(r_j) = 0$ まで次数が下がったとすると、$r_j$ は定数より、$r_j$ は $r_{j-1}$ を割り切るので $r_{j+1} = 0$ となる。よって、$r_n = 0$ なる $n$ が必ず存在する。よって

$$GCD(f, g) = GCD(g, r_1) = GCD(r_1, r_2) = \cdots = GCD(r_{n-1}, r_n) = GCD(r_{n-1}, 0) = r_{n-1}$$

となり、$GCD(f, g)$ が求まる。

以上により、$GCD(f, g)$ の計算方法がわかった。Proposition 2.3.2 の 3 より、
$h = GCD(f_1, \cdots, f_s)$ は、2 つの多項式の最大公約多項式を求める計算を、有限回 ($s-1$ 回) くり返すことにより、求まる。
(証明終わり)

次に、数学コンピューターソフト $Mathematica$ で、この 2 つの計算方法を利用して組んだプログラムを用いて、具体例を計算してみる。但し、プログラム上では、1 変数多項式 $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \quad (a_n \neq 0)$ を、$\{a_0, a_1, \cdots, a_n\}$ のように、係数のリストで表して処理をする。

以下に、プログラムの紹介をする。

```
In[1]:=ListDiv[f_,g_]:=ListDiv[f,g]=Module[{q,r,deg,coe},
                        q=Table[0,{Max[Length[f]-Length[g]+1,1]}];r=f;
                        While[r=!={0}&&Length[g]<=Length[r],
                        deg=Length[r]-Length[g]; coe=r[[-1]]/g[[-1]];
                        q=ReplacePart[q,coe+q[[deg+1]],deg+1];
                        r=r-Join[Table[0,{deg}],coe*g];
                        While[Length[r]>=1&&r[[-1]]==0,r=Delete[r,-1]]];
                        If[r=={},r={0};{q,r}]
```

ListDiv$[f,g]$ ( 但し、$g \neq 0$) と入力すると、

$$f = qg + r \quad (r = 0 \quad \text{または} \quad \deg(r) < \deg(g))$$

を満たす $\{q, r\}$ を出力する。

```
In[2]:=ListGCD[f_,g_]:=ListGCD[f,g]=Module[{h,s,rem、h1},
                        h=f;s=g;
                        While[s=!={0},rem=ListDiv[h,s][[2]];h=s;s=rem];
                        h/(h[[-1]])]

In[3]:=ListGCDs[f_]:=ListGCDs[f]=Module[{s,h},s=Length[f];h=f[[1]];
                      Do[h=ListGCD[h,f[[i]]],{i,2,s}];h]
```

ListGCDs$[\{f_1, \cdots, f_s\}]$ と入力すると、$GCD(f_1, \cdots, f_s)$ を出力する。

以下に、具体例をあげる。

**Example 1** $Q$ を有理数体とし

$$\begin{cases} f = x^3 + 4x^2 + 3x - 7 \\ f_1 = x^3 - 3x + 2 \\ f_2 = x^4 - 1 \\ f_3 = x^6 - 1 \end{cases} \qquad f, f_1, f_2, f_3 \in Q[x]$$

とする。

```
In[4]:=f={-7,3,4,1};f1={2,-3,0,1};f2={-1,0,0,0,1};f3={-1,0,0,0,0,0,1}
```

$f$ が $< f_1, f_2, f_3 >$ の元であるか否かを調べる。

```
In[5]:=h=ListGCDs[{f1,f2,f3}]
Out[5]={-1,1}
```

$< f_1, f_2, f_3 >=< h >$ より、$f$ が $< h >$ の元であるかどうかを調べる。

```
In[6]:=ListDiv[f,h]
Out[6]={{8,5,1},{1}}
```

余りが $1 \neq 0$ なので、$f \notin < h >$ より、$f \notin < f_1, f_2, f_3 >$である。

**Example 2**

$$\begin{cases} f = x^2 - 4 \\ f_1 = x^3 + x^2 - 4x - 4 \\ f_2 = x^3 - x^2 - 4x + 4 \\ f_3 = x^3 - 2x^2 - x + 2 \end{cases} \qquad f, f_1, f_2, f_3 \in Q[x]$$

とする。

```
In[7]:=f={-4,0,1};f1={-4,-4,1,1};f2={4,-4,-1,1};f3={2,-1,-2,1}
```

$f$ が $< f_1, f_2, f_3 >$ の元であるか否かを調べる。

```
In[8]:=h=ListGCDs[{f1,f2,f3}]
Out[8]={-2,1}
```

$< f_1, f_2, f_3 >=< h >$ より、$f$ が $< h >$ の元であるかどうかを調べる。

```
In[9]:=ListDiv[f,h]
Out[9]={{2,1},{0}}
```

余りが $0$ なので、$f \in < h >$ より、$f \in < f_1, f_2, f_3 >$である。

**Example 3**

$$\begin{cases} f = x^5 - 3x^4 - 1 \\ f_1 = x^4 + x^2 + 1 \\ f_2 = x^4 - x^2 - 2x - 1 \\ f_3 = x^3 - 1 \\ f_4 = x^3 - 3x^2 - 3x - 4 \end{cases} \qquad f, f_1, f_2, f_3, f_4 \in Q[x]$$

とする。

```
In[10]:=f={-1,0,0,0,-3,1};f1={1,0,1,0,1};f2={-1,-2,-1,0,1};f3={-1,0,0,1};
        f4={-4,-3,-3,1}
```

$f$ が $< f_1, f_2, f_3, f_4 >$ の元であるか否かを調べる。

```
In[11]:=h=ListGCDs[{f1,f2,f3,f4}]
Out[11]={1,1,1}
```

$< f_1, f_2, f_3, f_4 >=< h >$ より、$f$ が $< h >$ の元であるかどうかを調べる。

```
In[12]:=ListDiv[f,h]
Out[12]={{1,3,-4,1},{-2,-4}}
```

余りが $-4x - 2 \neq 0$ なので、$f \notin < h >$ より、$f \notin < f_1, f_2, f_3, f_4 >$である。

**Example 4**

$$\begin{cases} f = x^5 - 1 \\ f_1 = x^3 + 2x^2 - x - 2 \\ f_2 = x^3 - 2x^2 - x + 2 \\ f_3 = x^3 - x^2 - 4x + 4 \\ f_4 = x^4 - 1 \end{cases} \qquad f, f_1, f_2, f_3, f_4 \in Q[x]$$

とする。

```
In[13]:=f={-1,0,0,0,0,1};f1={-2,-1,2,1};f2={2,-1,-2,1};f3={4,-4,-1,1};
        f4={-1,0,0,0,1}
```

$f$ が $< f_1, f_2, f_3, f_4 >$ の元であるか否かを調べる。

```
In[14]:=h=ListGCDs[{f1,f2,f3,f4}]
Out[14]={-1,1}
```

$< f_1, f_2, f_3, f_4 >=< h >$ より、$f$ が $< h >$ の元であるかどうかを調べる。

```
In[15]:=ListDiv[f,h]
Out[15]={{1,1,1,1,1},{0}}
```

余りが $0$ なので、$f \in < h >$ より、$f \in < f_1, f_2, f_3, f_4 >$である。

**Example 5**

$$\begin{cases} f = 3x^4 - x^2 - 4 \\ f_1 = x^3 + x^2 + x + 1 \\ f_2 = x^3 - x^2 + x - 1 \\ f_3 = 2x^3 + 3x^2 + 2x + 3 \\ f_4 = x^4 + 2x^2 + 1 \end{cases} \qquad f, f_1, f_2, f_3, f_4 \in Q[x]$$

とする。

```
In[16]:=f={-4,0,-1,0,3};f1={1,1,1,1};f2={-1,1,-1,1};f3={3,2,3,2};
        f4={1,0,2,0,1}
```

$f$ が $< f_1, f_2, f_3, f_4 >$ の元であるか否かを調べる。

```
In[17]:=h=ListGCDs[{f1,f2,f3,f4}]
Out[17]={1,0,1}
```

$< f_1, f_2, f_3, f_4 >=< h >$ より、$f$ が $< h >$ の元であるかどうかを調べる。

```
In[18]:=ListDiv[f,h]
Out[18]={{-4,0,3},{0}}
```

余りが $0$ なので、$f \in < h >$ より、$f \in < f_1, f_2, f_3, f_4 >$である。

# Chapter 3

# 多変数多項式環上のイデアルの構成要素に関する問題

この章では、多変数多項式環 $k[x_1, \cdots, x_n]$ 上のイデアルの構成要素に関する問題について論じる。

## 3.1 単項式順序

この節では、単項式に便宜よく順序づけが出来る単項式順序を紹介する。

**Definition 3.1.1** 集合 $X$ 上の関係 $>$ が、 $X$ の任意の 2 つの元 $\alpha, \beta$ に対し

$$\alpha > \beta \quad \alpha = \beta \quad \beta > \alpha$$

のどれか 1 つだけを必ず満たし、$X$ の任意の元 $\alpha, \beta, \gamma$ に対し

$$\alpha > \beta \quad \beta > \gamma \quad \Longrightarrow \quad \alpha > \gamma$$

を満たすとき、関係 $>$ を、$X$ 上の**全順序** (または**線形順序**) という。

**Definition 3.1.2** 集合 $X$ 上の関係 $>$ に対し、$X$ の空でない任意の部分集合に、$>$ における最小要素が存在するとき、関係 $>$ を、$X$ 上の**整列順序**という。( 但し、一般に関係 $>$ に対し、$\alpha > \beta$ のとき、$\beta$ は $\alpha$ より小さいという。)

**Definition 3.1.3** $Z^n_{\geq 0}$ 上の関係 $>$ が

1. $>$ は、全順序である。
2. $>$ は、整列順序である。
3. $\forall \alpha, \beta, \gamma \in Z^n_{\geq 0}$ に対し、$\alpha > \beta \quad \Longrightarrow \quad \alpha + \gamma > \beta + \gamma$

を満たすとき、$>$ を、$Z^n_{\geq 0}$ 上の**単項式順序**という。

**Lemma 3.1.1** $Z^n_{\geq 0}$ 上の関係 $>$ に対し

$>$ は、整列順序である。　$\Longleftrightarrow$　$Z^n_{\geq 0}$ 上の任意の単調減少要素列は、有限個で終わる。

(Proof)
対偶をとって

$>$ は、整列順序でない。　$\Longleftrightarrow$　無限に続く $Z^n_{\geq 0}$ 上の単調減少要素列が存在する。

を証明する。
($\Longrightarrow$)　$>$ が整列順序でないので、最小要素を持たない $Z^n_{\geq 0}$ の空でない部分集合 $S$ が存在する。
$\alpha(1) \in S$ とする。$\alpha(1)$ は最小要素でないので

$$\exists \alpha(2) \in S \quad s.t. \quad \alpha(1) > \alpha(2)$$

$\alpha(2)$ は最小要素でないので

$$\exists \alpha(3) \in S \quad s.t. \quad \alpha(2) > \alpha(3)$$

同様にくり返すことによって、無限に続く $Z^n_{\geq 0}$ 上の単調減少要素列

$$\alpha(1) > \alpha(2) > \alpha(3) > \alpha(4) > \cdots\cdots$$

が出来る。
($\Longleftarrow$)

$$\alpha(1) > \alpha(2) > \alpha(3) > \alpha(4) > \cdots\cdots$$

を、無限に続く $Z^n_{\geq 0}$ 上の単調減少要素列とする。このとき、集合 $\{\alpha(1), \alpha(2), \alpha(3), \alpha(4), \cdots\cdots\}$ は、最小要素を持たない $Z^n_{\geq 0}$ の空でない部分集合になる。よって、$>$ は、整列順序でない。
(証明終わり)

次に、単項式順序の例である、辞書式順序を紹介する。

**Definition 3.1.4** $\forall \alpha, \beta \in Z^n_{\geq 0}$ に対し、$\alpha - \beta \in Z^n$ の $0$ でない一番左にくる要素が正の数のとき、$\alpha >_{lex} \beta$ と表し、$>_{lex}$ を、$Z^n_{\geq 0}$ 上の**辞書式順序**という。

**Proposition 3.1.1** $Z^n_{\geq 0}$ 上の辞書式順序は、単項式順序である。

(Proof)

1. $Z_{\geq 0}$ 上の不等号が全順序より、$>_{lex}$ の定義から明らかに、$Z_{\geq 0}^n$ の任意の 2 つの元 $\alpha, \beta$ は

$$\alpha >_{lex} \beta \quad \alpha = \beta \quad \beta >_{lex} \alpha$$

のどれか 1 つだけを必ず満たす。また、$\alpha, \beta, \gamma \in Z_{\geq 0}^n$ に対し、$\alpha >_{lex} \beta \quad \beta >_{lex} \gamma$ と仮定すると、$\alpha >_{lex} \beta$ より、$\alpha - \beta$ の 0 でない一番左の要素 $p$ は、正の数である。( 左から $i$ 番目とする。) また、$\beta >_{lex} \gamma$ より、$\beta - \gamma$ の 0 でない一番左の要素 $q$ は、正の数である。(左から $j$ 番目とする。)

$$\alpha - \gamma = (\alpha - \beta) + (\beta - \gamma)$$

より、$\alpha - \gamma$ の 0 でない一番左の要素は

$$\begin{array}{ll} i = j \text{ のとき} & p + q > 0 \\ i < j \text{ のとき} & p > 0 \\ i > j \text{ のとき} & q > 0 \end{array}$$

より、正の数になる。よって、$\alpha >_{lex} \gamma$ になる。
以上により、$>_{lex}$ は、全順序である。

2. $>_{lex}$ が整列順序でないと仮定する。Lemma 3.1.1 より、無限に続く $Z_{\geq 0}^n$ 上の単調減少要素列

$$\alpha(1) >_{lex} \alpha(2) >_{lex} \alpha(3) >_{lex} \alpha(4) >_{lex} \cdots\cdots$$

が存在する。辞書式順序の定義より

$$\alpha(1), \quad \alpha(2), \quad \alpha(3), \quad \alpha(4), \quad \cdots\cdots$$

の第 1 要素は、単調非増加非負整数列になる。よって、ある自然数 $m_1$ に対して、$\alpha(m_1)$ から先は第 1 要素がすべて同じ値になる。次に、$\alpha(m_1)$ から先の第 2 要素に注目する。先程と同様に

$$\alpha(m_1), \quad \alpha(m_1 + 1), \quad \alpha(m_1 + 2), \quad \alpha(m_1 + 3), \quad \cdots\cdots$$

の第 2 要素は、単調非増加非負整数列になる。よって、ある自然数 $m_2 (\geq m_1)$ に対して、$\alpha(m_2)$ から先は第 2 要素がすべて同じ値になる。このことを第 $n$ 要素までくり返すと、ある自然数 $m_n (\geq \cdots \geq m_2 \geq m_1)$ に対して、$\alpha(m_n)$ から先は第 $n$ 要素がすべて同じ値になる。$\alpha(m_n)$ から先の第 1 要素から第 $n-1$ 要素は、すでに、すべて同じ値になっているので

$$\alpha(m_n) = \alpha(m_n + 1) = \alpha(m_n + 2) = \alpha(m_n + 3) = \cdots\cdots$$

このことは

$$\alpha(m_n) >_{lex} \alpha(m_n + 1) >_{lex} \alpha(m_n + 2) >_{lex} \alpha(m_n + 3) >_{lex} \cdots\cdots$$

に矛盾する。よって、$>_{lex}$ は、整列順序である。

3. $\alpha >_{lex} \beta$ を満たす $\forall \alpha, \beta \in Z^n_{\geq 0}$ に対し、$>_{lex}$ の定義より、$\alpha - \beta$ の 0 でない一番左の要素は正の数である。よって、$\forall \gamma \in Z^n_{\geq 0}$ に対し

$$(\alpha + \gamma) - (\beta + \gamma) = \alpha - \beta$$

より、$\alpha + \gamma >_{lex} \beta + \gamma$ になる。

以上により、$>_{lex}$ は、単項式順序である。
(証明終わり)

**Definition 3.1.5** $f = \sum_{\alpha} a_\alpha x^\alpha \in k[x_1, \cdots, x_n]$ を零でない多項式とし、$>$ を単項式順序とする。このとき

1. $multideg(f) = \max\{\alpha \in Z^n_{\geq 0} \mid a_\alpha \neq 0\}$ を、$f$ の**多重次数**という。
   ( 但し、max は、$>$ による最大要素を意味する。)
2. $LC(f) = a_{multideg(f)}$ を、$f$ の**最高次の係数**という。
3. $LM(f) = x^{multideg(f)}$ を、$f$ の**最高次の単項式**という。
4. $LT(f) = LC(f) \cdot LM(f)$ を、$f$ の**最高次の項**という。

**Lemma 3.1.2** $f \in k[x_1, \cdots, x_n]$ を零でない多項式とし、$>$ を単項式順序とする。

1. $m$ を単項式とすると、$LT(m \cdot f) = m \cdot LT(f)$
2. $g \in k[x_1, \cdots, x_n]$ を零でない多項式とすると、$LT(f \cdot g) = LT(f) \cdot LT(g)$

(Proof)

$$f = a_{\alpha(p)} x^{\alpha(p)} + a_{\alpha(p-1)} x^{\alpha(p-1)} + \cdots + a_{\alpha(1)} x^{\alpha(1)} \qquad (\forall a_{\alpha(i)} \neq 0)$$
$$( \ \alpha(p) > \alpha(p-1) > \cdots > \alpha(1) \ )$$

とする。

1. $m = x^\alpha$ を単項式とする。

   $$m \cdot f = a_{\alpha(p)} x^{\alpha(p)+\alpha} + a_{\alpha(p-1)} x^{\alpha(p-1)+\alpha} + \cdots + a_{\alpha(1)} x^{\alpha(1)+\alpha}$$

   単項式順序の定義より

   $$\alpha(p) + \alpha > \alpha(p-1) + \alpha > \cdots > \alpha(1) + \alpha$$

   よって、$LT(m \cdot f) = a_{\alpha(p)} x^{\alpha(p)+\alpha}$ になる。
   一方、$m \cdot LT(f) = x^\alpha \cdot a_{\alpha(p)} x^{\alpha(p)}$ より、$LT(m \cdot f) = m \cdot LT(f)$ である。

2.

$$g = b_{\beta(q)}x^{\beta(q)} + b_{\beta(q-1)}x^{\beta(q-1)} + \cdots + b_{\beta(1)}x^{\beta(1)} \qquad (\forall b_{\beta(i)} \neq 0)$$
$$(\ \beta(q) > \beta(q-1) > \cdots > \beta(1)\ )$$

とする。

$f \cdot g = \sum_{i=1}^{q}\{(a_{\alpha(p)}x^{\alpha(p)} + a_{\alpha(p-1)}x^{\alpha(p-1)} + \cdots + a_{\alpha(1)}x^{\alpha(1)}) \cdot b_{\beta(i)}x^{\beta(i)}\}$

$= \sum_{i=1}^{q}\{x^{\beta(i)} \cdot (a_{\alpha(p)}b_{\beta(i)}x^{\alpha(p)} + a_{\alpha(p-1)}b_{\beta(i)}x^{\alpha(p-1)} + \cdots + a_{\alpha(1)}b_{\beta(i)}x^{\alpha(1)})\}$

1 より、$\sum$ の中の最高次の項は、$a_{\alpha(p)}b_{\beta(i)}x^{\alpha(p)+\beta(i)}$ になる。単項式順序の定義より

$$\alpha(p) + \beta(q) > \alpha(p) + \beta(q-1) > \cdots > \alpha(p) + \beta(1)$$

よって、$LT(f \cdot g) = a_{\alpha(p)}b_{\beta(q)}x^{\alpha(p)+\beta(q)}$ になる。

一方、$LT(f) \cdot LT(g) = a_{\alpha(p)}x^{\alpha(p)} \cdot b_{\beta(q)}x^{\beta(q)}$ より、$LT(f \cdot g) = LT(f) \cdot LT(g)$ である。

(証明終わり)

**Lemma 3.1.3** $f, g \in k[x_1, \cdots, x_n]$ を零でない多項式とし、$>$ を単項式順序とする。

1. $multideg(fg) = multideg(f) + multideg(g)$
2. $f + g \neq 0$ のとき、$multideg(f+g) \leq \max\{\ multideg(f),\ multideg(g)\ \}$
   (但し、$\beta < \alpha$ とは、$\alpha > \beta$ のこととし、$\leq$ は、$<$ か $=$ のどちらか一方が成り立つことを意味する。)

(Proof)

1. Lemma 3.1.2 の 2 より、明らかである。
2. $multideg(f+g) > \max\{\ multideg(f),\ multideg(g)\ \}$ と仮定する。
   $f = \sum_{\alpha} a_\alpha x^\alpha,\ g = \sum_{\alpha} b_\alpha x^\alpha$ とすると

$$f + g = \sum_{\alpha} c_\alpha x^\alpha \qquad (\ c_\alpha = a_\alpha + b_\alpha\ )$$

   $\beta = \max\{\ multideg(f),\ multideg(g)\ \},\ \gamma = multideg(f+g)$ とすると、
   $\forall \alpha > \beta$ に対し、$a_\alpha = 0$ かつ $b_\alpha = 0$ より $c_\alpha = 0$ となる。仮定より、$\gamma > \beta$ であるから、$c_\gamma = 0$ になる。このことは、$c_\gamma \neq 0$ に矛盾する。
   よって、$multideg(f+g) \leq \max\{\ multideg(f),\ multideg(g)\ \}$ である。

(証明終わり)

以後、単項式順序を固定して論じていく。

## 3.2　多変数多項式の除法定理

**Theorem 3.2.1 (多変数多項式の除法定理)** $f, f_1, \cdots, f_s \in k[x_1, \cdots, x_n]$ （ $\forall f_i \neq 0$ ）に対し

$f = a_1 f_1 + \cdots + a_s f_s + r$　$(r = 0$　または　$\forall LT(f_i)$ は $r$ のすべての項を割り切らない $)$

を満たす $a_1, \cdots, a_s, r \in k[x_1, \cdots, x_n]$ が存在する。( $r$ を**余り**という。)

(Proof)
5 節で、この定理における $a_1, \cdots, a_s, r \in k[x_1, \cdots, x_n]$ を求める計算方法があることを、今まで論じてきたことのみを用いて証明するので、この節では証明を省略する。

以後、この定理を仮定して論じていく。

## 3.3　単項式イデアルと Dickson の補題

**Definition 3.3.1** $I \subset k[x_1, \cdots, x_n]$ をイデアルとする。
$Z^n_{\geq 0}$ の空でない部分集合 $A$ によって

$$I =< x^\alpha : \alpha \in A >$$

と表せるとき、$I$ を**単項式イデアル**という。

**Lemma 3.3.1** $\forall \beta \in Z^n_{\geq 0}$ とする。
単項式イデアル $I =< x^\alpha : \alpha \in A > \subset k[x_1, \cdots, x_n]$ に対し

$$x^\beta \in I \quad \Longleftrightarrow \quad \exists \alpha \in A \quad s.t. \quad x^\alpha \text{ は } x^\beta \text{ を割り切る。}$$

(Proof)
$(\Longleftarrow)$　ある $\alpha \in A$ に対し、$x^\alpha$ は $x^\beta$ を割り切るので

$$x^\beta = x^\gamma \cdot x^\alpha \quad ( \gamma \in Z^n_{\geq 0} )$$

と表せる。$x^\alpha \in I$ より、イデアルの定義から、$x^\beta \in I$ である。

$(\Longrightarrow)$　$x^\beta \in I$ より

$$x^\beta = \sum_{i=1}^{s} h_i x^{\alpha(i)} \quad ( h_i \in k[x_1, \cdots, x_n] \quad \alpha(i) \in A )$$

と表せる。$h_i = \sum_\gamma a_{i\gamma} x^\gamma$ とおくと

$$x^\beta = \left( \sum_\gamma a_{1\gamma} x^\gamma \right) \cdot x^{\alpha(1)} + \cdots + \left( \sum_\gamma a_{s\gamma} x^\gamma \right) \cdot x^{\alpha(s)} = \sum_\gamma a_{1\gamma} x^{\gamma + \alpha(1)} + \cdots + \sum_\gamma a_{s\gamma} x^{\gamma + \alpha(s)}$$

よって、$x^\beta = x^{\gamma+\alpha(i)} = x^\gamma \cdot x^{\alpha(i)}$ を満たす $\gamma, i$ が存在するので、$x^\beta$ を割り切るような $x^\alpha$ が存在する。
(証明終わり)

**Lemma 3.3.2** $I, J \subset k[x_1, \cdots, x_n]$ を単項式イデアルとする。このとき

$$I = J \quad \Longleftrightarrow \quad I \text{ と } J \text{ の単項式の元は、すべて同じである。}$$

(Proof)
($\Longrightarrow$)　明らかである。

($\Longleftarrow$)　$I =< x^\alpha : \alpha \in A >$とおく。
$f = 0$ のとき、明らかに、$f \in I \quad \Longrightarrow \quad f \in J$ である。
$f \neq 0$ のとき、$f = \sum_{i=1}^{s} a_i x^{\beta(i)} \in I \quad (a_i \in k \quad a_i \neq 0)$ とおく。
$f$ は、単項式イデアルの元なので

$$f = \sum_{j=1}^{t} h_j x^{\alpha(j)} \quad (h_i \in k[x_1, \cdots, x_n],\ \alpha(j) \in A)$$

と表せる。Lemma 3.3.1 の証明と同様、右辺を展開すると、任意の $i$ に対し

$$x^{\beta(i)} = x^\gamma \cdot x^{\alpha(j)} \quad (\gamma \in Z^n_{\geq 0})$$

を満たす $\gamma, j$ が存在する。$x^{\alpha(j)} \in I$ より、任意の $i$ に対し、$x^{\beta(i)} \in I$ になる。$I$ と $J$ の単項式の元は、すべて同じなので、$x^{\beta(i)} \in J$ より、$f \in J$ になる。よって、$I \subset J$ である。同様に $I \supset J$ も示せるので、以上により、$I = J$ である。
(証明終わり)

**Theorem 3.3.1 (Dickson の補題)** 単項式イデアル $I =< x^\alpha : \alpha \in A >\subset k[x_1, \cdots, x_n]$ は、有限個の $\alpha(1), \cdots, \alpha(s) \in A$ によって

$$I =< x^{\alpha(1)}, \cdots, x^{\alpha(s)} >$$

と表せる。(つまり、有限生成で表せる。)

(Proof)
$n = 1$ のとき

$$I =< x_1^\alpha : \alpha \in A >\subset k[x_1] \quad (A \subset Z_{\geq 0})$$

$A$ の不等号における最小要素を $\beta$ とする。$\forall \alpha \in A$ に対し、$\beta \leq \alpha$ より、$x_1^\beta$ は $x_1^\alpha$ を割り切る。よって、$I =< x_1^\beta >$ である。

定理が $n-1$ まで成り立つと仮定する。$x_1, \cdots, x_{n-1}, y$ の $n$ 変数で考えると、$k[x_1, \cdots, x_{n-1}, y]$ 上の任意の単項式は

$$x^\alpha y^m \qquad (\ \alpha \in Z^{n-1}_{\geq 0} \quad m \in Z_{\geq 0}\ )$$

と表せる。$I \subset k[x_1, \cdots, x_{n-1}, y]$ を単項式イデアルとする。$J \subset k[x_1, \cdots, x_{n-1}]$ を、$x^\alpha y^m \in I$ を満たすような $m$ が存在する任意の $x^\alpha$ で生成される単項式イデアルとすると、仮定より、有限個の $J$ の生成元 $x^{\alpha(1)}, \cdots, x^{\alpha(s)}$ によって

$$J =< x^{\alpha(1)}, \cdots, x^{\alpha(s)} >$$

と表せる。$J$ の定義より、$1 \leq i \leq s$ の任意の $i$ に対して、$x^{\alpha(i)} y^{m_i} \in I$ を満たす $m_i$ が存在する。ここで

$$m = \max\{\ m_i \mid 1 \leq i \leq s\ \}$$

とする。$0 < l \leq m-1$ の任意の $l$ に対して、$J_l \subset k[x_1, \cdots, x_{n-1}]$ を、$x^\beta y^l \in I$ を満たす任意の $x^\beta$ で生成される単項式イデアルとすると、仮定より、有限個の $J_l$ の生成元 $x^{\alpha_l(1)}, \cdots, x^{\alpha_l(s_l)}$ によって

$$J_l =< x^{\alpha_l(1)}, \cdots, x^{\alpha_l(s_l)} >$$

と表せる。ここで

$$\begin{gathered} x^{\alpha(1)} y^m, \cdots, x^{\alpha(s)} y^m \\ x^{\alpha_0(1)}, \cdots, x^{\alpha_0(s_0)} \\ x^{\alpha_1(1)} y, \cdots, x^{\alpha_1(s_1)} y \\ \vdots \\ x^{\alpha_{m-1}(1)} y^{m-1}, \cdots, x^{\alpha_{m-1}(s_{m-1})} y^{m-1} \end{gathered}$$

で生成される単項式イデアルを $I'$ とする。$\forall x^\alpha y^p \in I$ とすると、$p \geq m$ のとき、$J$ の定義より $x^\alpha y^p$ を割り切るような $x^{\alpha(i)} y^m$ が存在する。$p \leq m-1$ のとき、$J_p$ の定義より $x^\alpha y^p$ を割り切るような $x^{\alpha_p(j)} y^p$ が存在する。よって、Lemma 3.3.1 より、$I$ の単項式の元はすべて $I'$ に含まれる。逆に、$I'$ の生成元は $I$ の元になっているので、$I' \subset I$ より、$I'$ の単項式の元はすべて $I$ に含まれる。$I$ と $I'$ の単項式の元はすべて同じであるので、Lemma 3.3.2 より、$I = I'$ になる。

以上により、単項式イデアル $I =< x^\alpha : \alpha \in A > \subset k[x_1, \cdots, x_n]$ は、
有限個の $x^{\beta(1)}, \cdots, x^{\beta(t)} \in I$ によって

$$I =< x^{\beta(1)}, \cdots, x^{\beta(t)} >$$

と表せることがわかった。また、Lemma 3.3.1 より、$1 \leq i \leq t$ の任意の $i$ に対して、
$x^{\alpha(i)}$ が $x^{\beta(i)}$ を割り切るような $\alpha(i) \in A$ が存在する。このとき、

$$< x^\alpha : \alpha \in A >=< x^{\alpha(1)}, \cdots, x^{\alpha(t)} >$$

であることを示す。

$(\supset)$　明らかである。

$(\subset)$　$< x^\alpha : \alpha \in A >=< x^{\beta(1)}, \cdots, x^{\beta(t)} > \subset < x^{\alpha(1)}, \cdots, x^{\alpha(t)} >$

以上により

$$< x^{\alpha} : \alpha \in A >=< x^{\alpha(1)}, \cdots, x^{\alpha(t)} > \quad (\alpha(i) \in A)$$

である。
(証明終わり)

## 3.4 Hilbert の基底定理と Gröbner 基底

**Definition 3.4.1** $I(\neq \{0\}) \subset k[x_1, \cdots, x_n]$ をイデアルとする。このとき

1. $LT(I) = \{\ LT(f) \mid f \in I - \{0\}\ \}$ とする。
2. $LT(I)$ のすべての元で生成されるイデアルを $< LT(I) >$ と表す。

**Proposition 3.4.1** $I(\neq \{0\}) \subset k[x_1, \cdots, x_n]$ をイデアルとする。このとき

1. $< LT(I) >$ は、単項式イデアルである。
2. $< LT(I) >=< LT(g_1), \cdots, LT(g_s) >$ を満たす $g_1, \cdots, g_s \in I$ が存在する。

(Proof)

1. $< LT(I) >=< LM(g)\ :\ g \in I - \{0\} >$ であることを示す。

   $(\subset)$ $LT(g) \in < LT(I) >$ とする。

   $$LT(g) = LC(g) \cdot LM(g) \in < LM(g)\ :\ g \in I - \{0\} >$$

   $(\supset)$ $LM(f) \in < LM(g)\ :\ g \in I - \{0\} >$ とする。

   $$LM(f) = \frac{1}{LC(f)} \cdot LT(f) \in < LT(I) >$$

   以上により、$< LT(I) >=< LM(g)\ :\ g \in I - \{0\} >$ が成り立つので、$< LT(I) >$ は、単項式イデアルである。

2. $< LT(I) >$ は、単項式イデアルより、Dickson の補題から、

   $$< LT(I) >=< LM(g_1), \cdots, LM(g_s) >$$

   を満たす $g_1, \cdots, g_s \in I$ が存在する。1 の証明と同様の方法で

   $$< LM(g_1), \cdots, LM(g_s) >=< LT(g_1), \cdots, LT(g_s) >$$

   が示せる。よって、$< LT(I) >=< LT(g_1), \cdots, LT(g_s) >$ である。

(証明終わり)

**Theorem 3.4.1 (Hilbert の基底定理)** 任意のイデアル $I \subset k[x_1, \cdots, x_n]$ は、有限個の $g_1, \cdots, g_s \in I$ によって、$I =< g_1, \cdots, g_s >$ と表せる。(つまり、有限生成で表せる。)

(Proof)
$I = \{0\}$ のとき、$I =< 0 >$ である。
$I \neq \{0\}$ のとき、Proposition 3.4.1 の 2 より

$$< LT(I) >=< LT(g_1), \cdots, LT(g_s) >$$

と表せる。このとき、$I =< g_1, \cdots, g_s >$ であることを示す。

$(\supset)$　明らかである。

$(\subset)$　$f \in I$ とする。多変数多項式の除法定理より

$$f = a_1 g_1 + \cdots + a_s g_s + r \quad (a_i, r \in k[x_1, \cdots, x_n])$$
$$(r = 0 \quad \text{または} \quad \forall LT(g_i) \text{ は } r \text{ のすべての項を割り切らない})$$

と表せる。このとき

$$r = f - a_1 g_1 - \cdots - a_s g_s \in I$$

となる。$r \neq 0$ と仮定すると

$$LT(r) \in < LT(I) >=< LT(g_1), \cdots, LT(g_s) >$$

より、$LT(r)$ を割り切る $LT(g_i)$ が存在する。このことは矛盾より、$r = 0$ である。よって、$f = a_1 g_1 + \cdots + a_s g_s \in < g_1, \cdots, g_s >$である。

以上により、$I =< g_1, \cdots, g_s >$ である。
(証明終わり)

**Definition 3.4.2** $I(\neq \{0\}) \subset k[x_1, \cdots, x_n]$ をイデアルとする。$G = \{g_1, \cdots, g_s\} \subset I$ が

$$< LT(g_1), \cdots, LT(g_s) >=< LT(I) >$$

を満たすとき、$G$ を *Gröbner* **基底** (または**標準基底**) という。

Hilbert の基底定理の証明過程により、任意のイデアル $I(\neq \{0\}) \subset k[x_1, \cdots, x_n]$ に対し、Gröbner 基底 $G = \{g_1, \cdots, g_s\}$ が存在し、$I$ の生成元になっていることがわかる。つまり、$I =< g_1, \cdots, g_s >$ と表せる。

**Proposition 3.4.2** $f \in k[x_1, \cdots, x_n]$、$I(\neq \{0\}) \subset k[x_1, \cdots, x_n]$ をイデアル、
$G = \{g_1, \cdots, g_s\} \subset I$ を *Gröbner* 基底とする。このとき、多変数多項式の除法定理により

$$f = a_1 g_1 + \cdots + a_s g_s + r \quad (a_i, r \in k[x_1, \cdots, x_n])$$
$$(r = 0 \quad \text{または} \quad \forall LT(g_i) \text{ は } r \text{ のすべての項を割り切らない})$$

と表したとき、$r$ は一意である。

(Proof)

$$f = g + r = g' + r'$$

$$( \ g = a_1 g_1 + \cdots + a_s g_s \quad g' = b_1 g_1 + \cdots + b_s g_s \quad a_i, b_i \in k[x_1, \cdots, x_n] \ )$$

とする。$g, g' \in I$ より

$$r - r' = g' - g \in I$$

になる。$r \neq r'$ とすると

$$LT(r - r') \in < LT(I) > = < LT(g_1), \cdots, LT(g_s) >$$

より、$LT(r - r')$ を割り切る $LT(g_i)$ が存在する。このことは、$\forall LT(g_i)$ は、$r, r'$ のすべての項を割り切らないことに矛盾する。よって、$r = r'$ である。
(証明終わり)

## 3.5 多変数多項式環上のイデアルの構成要素に関する問題の解法

$f, f_1, \cdots, f_s \in k[x_1, \cdots, x_n]$ に対し、$f$が $< f_1, \cdots, f_s >$ の元であるか否かを調べたい。$< f_1, \cdots, f_s >= \{0\}$ とすると、$< f_1, \cdots, f_s >$ の元は 0 のみになるので、$< f_1, \cdots, f_s > \neq \{0\}$ の場合について考える。$< f_1, \cdots, f_s >$ の Gröbner 基底を $G = \{g_1, \cdots, g_t\}$ とすると、$< f_1, \cdots, f_s > = < g_1, \cdots, g_t >$ となるので、この問題は、$f$ が $< g_1, \cdots, g_t >$ の元であるか否かに帰着される。多変数多項式の除法定理により、$f = a_1 g_1 + \cdots + a_t g_t + r \quad (r = 0$ または $\forall LT(g_i)$ は $r$ のすべての項を割り切らない ) と表せる。もし、$r = 0$ ならば、$f = a_1 g_1 + \cdots + a_t g_t \in < g_1, \cdots, g_t >$である。$r \neq 0$ ならば、$\{g_1, \cdots, g_t\}$ が Gröbner 基底より、$r$ は一意であるので、$f = b_1 g_1 + \cdots + b_t g_t$ を満たす $b_1, \cdots, b_t$ は存在しない。よって、$f \notin < g_1, \cdots, g_t >$ である。

論理的には解決出来たが、実際問題として、$g_1, \cdots, g_t, a_1, \cdots, a_t, r$ の求め方については論じていなかったので、具体例について計算が出来ない。そこで、多変数多項式の除法定理における $a_1, \cdots, a_t, r$ と、Gröbner 基底 $G = \{g_1, \cdots, g_t\}$ を求める計算方法を紹介する。

**Proposition 3.5.1** $f, f_1, \cdots, f_s \in k[x_1, \cdots, x_n] \quad ( \ \forall f_i \neq 0 \ )$ に対し、多変数多項式の除法定理による

$$f = a_1 f_1 + \cdots + a_s f_s + r \quad (r = 0 \quad \text{または} \quad \forall LT(f_i) \text{ は } r \text{ のすべての項を割り切らない })$$

なる $a_1, \cdots, a_s, r \in k[x_1, \cdots, x_n]$ を求める計算方法がある。

(Proof)
コンピューターの言語をまねたスードコードを用いて表示する。

Input: $f_1, \cdots, f_s, f$
Output: $a_1, \cdots, a_s, r$

$a_1 := 0;\ \cdots;\ a_s := 0;\ r := 0$
$p := f$
WHILE $p \neq 0$ DO
    $i := 1$
    divisionoccurred := false
    WHILE $i \leq s$ AND divisionoccurred := false Do
        IF $LT(f_i)$ divides $LT(p)$ THEN
            $a_i := a_i + LT(p)/LT(f_i)$
            $p := p - (LT(p)/LT(f_i))f_i$
            divisionoccurred := true
        ELSE
            $i := i + 1$
    IF divisionoccurred := false THEN
        $r := r + LT(p)$
        $p := p - LT(p)$

これが、計算方法であることを示す。

この計算方法には、各計算段階において、$LT(p)$ を割り切るような $LT(f_i)$ が存在する場合の段階 (除法段階とする) と、$LT(p)$ を割り切るような $LT(f_i)$ が存在しない場合の段階 (余り段階とする) の 2 通りがある。まず、$a_1, \cdots, a_s, r$、$p$ の初期値を、$a_{1(0)}, \cdots, a_{s(0)}, r_{(0)}, p_{(0)}$ とおき、$m$ 回目の計算段階における $a_1, \cdots, a_s, r$、$p$ の値を、$a_{1(m)}, \cdots, a_{s(m)}, r_{(m)}, p_{(m)}$ とおく。

まず、各計算段階において

$$f = a_1 f_1 + \cdots + a_s f_s + p + r$$

を満たすことを示す。
$m = 0$ のとき

$$a_{1(0)} f_1 + \cdots + a_{s(0)} f_s + p_{(0)} + r_{(0)} = 0 \cdot f_1 + \cdots + 0 \cdot f_s + f + 0 = f$$

$m$ 回目の計算段階に進む前に

$$f = a_{1(m-1)} f_1 + \cdots + a_{s(m-1)} f_s + p_{(m-1)} + r_{(m-1)}$$

が、成り立っていると仮定する。$m$ 回目の計算段階が除法段階のとき、値が変わる変数は、$a_i, p$ で

$$a_{i(m)} f_i + p_{(m)} = \left\{ a_{i(m-1)} + \frac{LT(p_{(m-1)})}{LT(f_i)} \right\} f_i + \left\{ p_{(m-1)} - \frac{LT(p_{(m-1)})}{LT(f_i)} f_i \right\} = a_{i(m-1)} f_i + p_{(m-1)}$$

より

$$f = a_{1(m)}f_1 + \cdots + a_{s(m)}f_s + p_{(m)} + r_{(m)}$$

$m$ 回目の計算段階が余り段階のとき、値が変わる変数は、$p$、$r$ で

$$p_{(m)} + r_{(m)} = \{p_{(m-1)} - LT(p_{(m-1)})\} + \{r_{(m-1)} + LT(p_{(m-1)})\} = p_{(m-1)} + r_{(m-1)}$$

より

$$f = a_{1(m)}f_1 + \cdots + a_{s(m)}f_s + p_{(m)} + r_{(m)}$$

以上により、各計算段階において

$$f = a_1f_1 + \cdots + a_sf_s + p + r$$

を満たす。

次に、$p = 0$ のときに計算が終わるので、出力結果が

$$f = a_1f_1 + \cdots + a_sf_s + r$$

となることは明らかである。

さらに、出力結果が、$r = 0$ または $\forall LT(f_i)$ は $r$ のすべての項を割り切らないという条件を満たすのは、$r$ の初期値 $(r_{(0)} = 0)$ と、余り段階に進む条件 $(LT(p)$ を割り切るような $LT(f_i)$ は存在しない$)$ と、余り段階における計算 $(r_{(m)} = r_{(m-1)} + LT(p_{(m-1)}))$ より、明らかである。

最後に、有限回の計算で $p = 0$ になる。つまり、計算が有限回で終わることを示す。
$m$ 回目の計算段階が除法段階のとき

$$p_{(m)} = p_{(m-1)} - \frac{LT(p_{(m-1)})}{LT(f_i)}f_i$$

$$LT\left(\frac{LT(p_{(m-1)})}{LT(f_i)}f_i\right) = \frac{LT(p_{(m-1)})}{LT(f_i)} \cdot LT(f_i) = LT(p_{(m-1)})$$

より、$multideg(p_{(m)}) < multideg(p_{(m-1)})$ または $p_{(m)} = 0$ になる。
$m$ 回目の計算段階が余り段階のとき

$$p_{(m)} = p_{(m-1)} - LT(p_{(m-1)})$$

より、明らかに $multideg(p_{(m)}) < multideg(p_{(m-1)})$ または $p_{(m)} = 0$ になる。また、単項式順序は整列順序より、以上により、有限回の計算で $p = 0$ になる。
(証明終わり)

一般に、$f_1, \cdots, f_s$ の順番を入れかえて計算すると、計算結果の $a_1, \cdots, a_s$、$r$ の値は、同じであるとは限らない。

**Definition 3.5.1** $f, f_1, \cdots, f_s \in k[x_1, \cdots, x_n]$ （ $\forall f_i \neq 0$ ）とし、
$F = \{f_1, \cdots, f_s\}$ とする。*Proposition 3.5.1* の計算方法を用いて

$f = a_1 f_1 + \cdots + a_s f_s + r$ （$r = 0$ または $\forall LT(f_i)$ は $r$ のすべての項を割り切らない）

と表したときの余り $r$ を、$\overline{f}^F$ と表す。

**Definition 3.5.2** $f, g \in k[x_1, \cdots, x_n]$ を零でない多項式とする。

1. $multideg(f) = \alpha,\ multideg(g) = \beta$ （ $\alpha = (\alpha_1, \cdots, \alpha_n), \beta = (\beta_1, \cdots, \beta_n)$ ）のとき

$$\gamma = (\gamma_1, \cdots, \gamma_n) \quad (\ \gamma_i = \max\{\alpha_i, \beta_i\} \quad (1 \leq \forall i \leq n)\ )$$

に対し、$x^\gamma$ を $LM(f)$ と $LM(g)$ の**最小公倍単項式**といい

$$x^\gamma = LCM(LM(f), LM(g))$$

と表す。

2. $x^\gamma = LCM(LM(f), LM(g))$ のとき

$$S(f, g) = \frac{x^\gamma}{LT(f)} \cdot f - \frac{x^\gamma}{LT(g)} \cdot g$$

を、$f$ と $g$ の $S$ **多項式**という。

**Proposition 3.5.2** イデアル $I =< f_1, \cdots, f_s > (\neq \{0\}) \subset k[x_1, \cdots, x_n]$ の *Gröbner* 基底 $G$ を求める計算方法がある。

(Proof)
スードコードを用いて表示する。

Input: $F = (f_1, \cdots, f_s)$
Output: a Gröbner basis $G = (g_1, \cdots, g_t)$ for $I$, with $F \subset G$

$G := F$
REPEAT
　　$G' := G$
　　FOR each pair $\{p, q\},\ p \neq q$ in $G'$ DO
　　$S := \overline{S(p, q)}^{G'}$
　　IF $S \neq 0$ THEN $G := G \bigcup \{S\}$
UNTIL $G = G'$

これが、計算方法であることの証明は省略する。
(証明終わり)

次に、数学コンピューターソフト $Mathematica$ で、この 2 つの計算方法を利用して組んだプログラムを用いて、具体例を計算してみる。但し、プログラム上では、多変数多項式を、例えば $Q[x,y,z]$ 上の $4xy^2z+4z^2-5x^3+7x^2z^2$ という多項式の場合、

$$\{\{\{0,0,4\}\},\{\{0\},\{0\},\{0,4\}\},\{\{0,0,7\}\},\{\{-5\}\}\}$$

のように、リストの中の 1 番目のかっこは、$x$ の次数について、2 番目のかっこは、$y$ の次数について $\cdots$、という様にして、1 変数多項式の場合のように、係数のリストで表して処理をする。

以下に、プログラムの紹介をする。(但し、単項式順序は、辞書式順序とする。)

```
In[19]:=LT[f_]:=LT[f]=Module[{n,ff,deglist,coe},
                n=Depth[f]-1;ff[i_]:=ff[i]=ff[i-1][[-1]];
                ff[1]:=f;deglist=Table[Length[ff[i]]-1,{i,1,n}];
                coe=Flatten[f][[-1]];{deglist,coe}]

In[20]:=Polymono[f_,m_]:=Polymono[f,m]=
                         Module[{deglist,coe,f1,f2,k,a,zero,f3,co,ze},
                         deglist=m[[1]];coe=m[[2]];k=deglist[[1]]+1;
                         If[Length[f]>=k,If[Length[deglist]==1,
                         If[coe+f[[k]]==0,f1=ReplacePart[f,0,k];
                         While[Length[f1]>=2&&f1[[-1]]==0,f1=Delete[f1,-1]];f1,
                         ReplacePart[f,coe+f[[k]],k]],
                         f2=ReplacePart[f,Polymono[f[[k]],
                         {Delete[deglist,1],coe}],k];
                         While[Length[f2]>=2&&Flatten[f2[[-1]]]=={0},
                         f2=Delete[f2,-1]];f2],a=k-Length[f];zero=0;
                         Do[zero={zero},{Depth[f]-2}];f3=f;
                         Do[f3=Append[f3,zero],{a-1}];co={coe};ze=0;
                         Do[Do[co=Prepend[co,ze],{deglist[[-i]]}];co={co};
                         ze={ze},{i,1,Length[deglist]-1}];
                         If[Depth[co]==2,co=coe,co=FlattenAt[co,{1}]];
                         Append[f3,co]]]

In[21]:=PolyDiv[f_,g_]:=PolyDiv[f,g]=Module[{s,z,a,r,p,i,c,h1,h2,gg},
                        s=Length[g];z=0;Do[z={z},{Depth[f]-1}];a={};
                        Do[a=Append[a,z],{s}];r=z;p=f;
                        While[p=!=z,i=1;c=True;
                        While[i<=s&&c,h1=LT[p][[1]]-LT[g[[i]]][[1]];
```

```
                    If[Select[h1,#1<0&]=={},
                    h2=LT[p][[2]]/(LT[g[[i]]][[2]]);
                    a=ReplacePart[a,Polymono[a[[i]],{h1,h2}],i];gg=g[[i]];
                    While[gg=!=z,
                    p=Polymono[p,{h1+LT[gg][[1]],-h2*LT[gg][[2]]}];
                    gg=Polymono[gg,{LT[gg][[1]],-LT[gg][[2]]}]];
                    c=False,i=i+1]];If[c,r=Polymono[r,LT[p]];
                    p=Polymono[p,{LT[p][[1]],-LT[p][[2]]}]]];{a,r}]
```

PolyDiv$[f,\{f_1,\cdots,f_s\}]$ ( 但し、$\forall f_i \neq 0$) と入力すると、

$f = a_1f_1 + \cdots + a_sf_s + r$ $(r = 0$ または $\forall LT(f_i)$ は $r$ のすべての項を割り切らない )

を、満たす $\{\{a_1,\cdots,a_s\},r\}$ を出力する。

```
In[22]:=S[f_,g_]:=S[f,g]=Module[{mf,mg,s,a,b,z,aa,ff,gg},
                  mf=LT[f][[1]];mg=LT[g][[1]];s=Length[mf];c={};
                  Do[c=Append[c,Max[{mf[[i]],mg[[i]]}]],{i,1,s}];
                  a={c-mf,1/(LT[f][[2]])};b={c-mg,1/(LT[g][[2]])};
                  z=0;Do[z={z},{s}];aa=z;ff=f;While[ff=!=z,
                  aa=Polymono[aa,{a[[1]]+LT[ff][[1]],a[[2]]*LT[ff][[2]]}];
                  ff=Polymono[ff,{LT[ff][[1]],-LT[ff][[2]]}]];gg=g;
                  While[gg=!=z,aa=Polymono[aa,{b[[1]]+LT[gg][[1]],
                  -b[[2]]*LT[gg][[2]]}];
                  gg=Polymono[gg,{LT[gg][[1]],-LT[gg][[2]]}]];aa]

In[23]:=Groeb[F_]:=Groeb[F]=Module[{G,GG,z,s,r},
                   G=F;z=0;Do[z={z},{Depth[F[[1]]]-1}];
                   While[G=!=GG,GG=G;s=Length[G];
                   Do[Do[r=PolyDiv[S[G[[i]],G[[j]]],G][[-1]];
                   If[r=!=z,G=Append[G,r]],{j,i+1,s}],{i,1,s-1}]];G]
```

Groeb$[\{f_1,\cdots,f_s\}]$ と入力すると、$< f_1,\cdots,f_s >$ の Gröbner 基底 $\{g_1,\cdots,g_t\}$ を出力する。

以下に、具体例をあげる。

**Example 6**

$$\begin{cases} f = -4x^2y^2z^2 + y^6 + 3z^5 \\ f_1 = xz - y^2 \\ f_2 = x^3 - z^2 \end{cases} \qquad f, f_1, f_2 \in Q[x,y,z]$$

とする。

```
In[24]:=f={{{0,0,0,0,0,3},{0},{0},{0},{0},{0},{1}},{{0}},{{0},{0},{0,0,-4}}};
       f1={{{0},{0},{-1}},{{0,1}}};f2={{{0,0,-1}},{{0}},{{0}},{{1}}}
```

$f$ が $< f_1, f_2 >$ の元であるか否かを調べる。

```
In[25]:=G=Groeb[{f1,f2}]
Out[25]={{{{0},{0},{-1}},{{0,1}}},{{{0,0,-1}},{{0}},{{0}},{{1}}},
         {{{0,0,0,1}},{{0}},{{0},{0},{-1}}},
         {{{0,0,0,0,1}},{{0},{0},{0},{0},{-1}}},
         {{{0,0,0,0,0,1},{0},{0},{0},{0},{0},{-1}}}}
```

$< f_1, f_2 >=< g : g \in G >$ より、$f$ が $< g : g \in G >$ の元であるかどうかを調べる。

```
In[26]:=PolyDiv[f,G]
Out[26]={{{{{0},{0},{0},{0},{-4}},{{0},{0},{0,-4}}},{{{0}}},{{{0}}},
         {{{0}}},{{{3}}}},{{{0}}}}
```

余りが $0$ なので、$f \in< g : g \in G >$ より、$f \in< f_1, f_2 >$である。

**Example 7**

$$\begin{cases} f = xy^3 - z^2 + y^5 - z^3 \\ f_1 = -x^3 + y \\ f_2 = x^2y - z \end{cases} \qquad f, f_1, f_2 \in Q[x, y, z]$$

とする。

```
In[27]:=f={{{0,0,-1,-1},{0},{0},{0},{0},{1}},{{0},{0},{0},{1}}};
       f1={{{0},{1}},{{0}},{{0}},{{-1}}};f2={{{0,-1}},{{0}},{{0},{1}}}
```

$f$ が $< f_1, f_2 >$ の元であるか否かを調べる。

```
In[28]:=G=Groeb[{f1,f2}]
Out[28]={{{{0},{1}},{{0}},{{0}},{{-1}}},{{{0,-1}},{{0}},{{0},{1}}},
         {{{0},{0},{-1}},{{0,1}}},{{{0,0,-1}},{{0},{0},{0},{1}}},
         {{{0,0,0,1},{0},{0},{0},{0},{-1}}}}
```

$< f_1, f_2 >=< g : g \in G >$ より、$f$ が $< g : g \in G >$ の元であるかどうかを調べる。

```
In[29]:=PolyDiv[f,G]
Out[29]={{{{{0}}},{{{0}}},{{{0}}},{{{1}}},{{{-1}}}},{{{0}}}}
```

余りが $0$ なので、$f \in< g : g \in G >$ より、$f \in< f_1, f_2 >$である。

**Example 8**

$$\begin{cases} f = x^3z - 2y^2 \\ f_1 = xz - y \\ f_2 = xy + 2z^2 \\ f_3 = y - z \end{cases} \qquad f, f_1, f_2, f_3 \in Q[x, y, z]$$

とする。

```
In[30]:=f={{{0},{0},{-2}},{{0}},{{0}},{{0,1}}};f1={{{0},{-1}},{{0,1}}};
        f2={{{0,0,2}},{{0},{1}}};f3={{{0,-1},{1}}}
```

$f$ が $< f_1, f_2, f_3 >$ の元であるか否かを調べる。

```
In[31]:=G=Groeb[{f1,f2,f3}]
Out[31]={{{{0},{-1}},{{0,1}}},{{{0,0,2}},{{0},{1}}},{{{0,-1},{1}}},
        {{{0,0,-1,-2}}},{{{0,1,2}}}}
```

$< f_1, f_2, f_3 >=< g : g \in G >$ より、$f$ が $< g : g \in G >$ の元であるかどうかを調べる。

```
In[32]:=PolyDiv[f,G]
Out[32]={{{{{0,-2}},{{0}},{{1}}},{{{0}},{{1}}},{{{0,-4},{-2}}},{{{0}}},
        {{{-2}}}},{{{0,2}}}}
```

余りが $2z \neq 0$ なので、$f \notin< g : g \in G >$ より、$f \notin< f_1, f_2, f_3 >$である。

**Example 9**

$$\begin{cases} f = 3 + x^2y + y^2 \\ f_1 = x^2 + y \\ f_2 = x^4 + 2x^2y + y^2 + 3 \end{cases} \qquad f, f_1, f_2 \in Q[x, y, z]$$

とする。

```
In[33]:=f={{{3},{0},{1}},{{0}},{{0},{1}}};f1={{{0},{1}},{{0}},{{1}}};
        f2={{{3},{0},{1}},{{0}},{{0},{2}},{{0}},{{1}}}
```

$f$ が $< f_1, f_2 >$ の元であるか否かを調べる。

```
In[34]:=G=Groeb[{f1,f2}]
Out[34]={{{{0},{1}},{{0}},{{1}}},{{{3},{0},{1}},{{0}},{{0},{2}},{{0}},{{1}}},
        {{{-3}}}}
```

$< f_1, f_2 >=< g : g \in G >$ より、$f$ が $< g : g \in G >$ の元であるかどうかを調べる。

```
In[35]:=PolyDiv[f,G]
Out[35]={{{{{0},{1}}},{{{0}}},{{{-1}}}},{{{0}}}}
```

余りが $0$ なので、$f \in< g : g \in G >$ より、$f \in< f_1, f_2 >$である。

**Example 10**

$$\begin{cases} f = x^3y^2 + y + 1 \\ f_1 = x^2y - 1 \\ f_2 = xy^2 - x \end{cases} \qquad f, f_1, f_2 \in Q[x, y, z]$$

とする。

```
In[36]:=f={{{1},{1}},{{0}},{{0}},{{0},{0},{1}}};
        f1={{{-1}},{{0}},{{0},{1}}};f2={{{0}},{{-1},{0},{1}}}
```

$f$ が $< f_1, f_2 >$ の元であるか否かを調べる。

```
In[37]:=G=Groeb[{f1,f2}]
Out[37]={{{{-1}},{{0}},{{0},{1}}},{{{0}},{{-1},{0},{1}}},
        {{{0},{-1}},{{0}},{{1}}},{{{-1},{0},{1}}}}
```

$< f_1, f_2 >=< g : g \in G >$ より、$f$ が $< g : g \in G >$ の元であるかどうかを調べる。

```
In[38]:=PolyDiv[f,G]
Out[38]={{{{{0}},{{0},{1}}},{{{0}}},{{{0}}},{{{0}}}},{{{1},{1}},{{0},{1}}}}
```

余りが $xy + y + 1 \neq 0$ なので、$f \notin< g : g \in G >$ より、$f \notin< f_1, f_2 >$である。

**Example 11**

$$\begin{cases} f = xz^2 - yz \\ f_1 = x - z^4 \\ f_2 = y - z^5 \end{cases} \qquad f, f_1, f_2 \in Q[x, y, z]$$

とする。

```
In[39]:=f={{{0},{0,-1}},{{0,0,1}}};f1={{{0,0,0,0,-1}},{{1}}};
        f2={{{0,0,0,0,0,-1},{1}}}
```

$f$ が $< f_1, f_2 >$ の元であるか否かを調べる。

```
In[40]:=G=Groeb[{f1,f2}]
Out[40]={{{{0,0,0,0,-1}},{{1}}},{{{0,0,0,0,0,-1},{1}}}}
```

$< f_1, f_2 >=< g : g \in G >$ より、$f$ が $< g : g \in G >$ の元であるかどうかを調べる。

```
In[41]:=PolyDiv[f,G]
Out[41]={{{{{0,0,1}}},{{{0,-1}}}},{{{0}}}}
```

余りが $0$ なので、$f \in< g : g \in G >$ より、$f \in< f_1, f_2 >$である。

**Example 12**

$$\begin{cases} f = x^6 - 1 \\ f_1 = y^2zw + 1 \\ f_2 = x^3yzw - yw \\ f_3 = zw - x^3w \\ f_4 = y^4 - 1 \end{cases} \qquad f, f_1, f_2, f_3, f_4 \in Q[x, y, z, w]$$

とする。

```
In[42]:=f={{{{-1}}},{{{0}}},{{{0}}},{{{0}}},{{{0}}},{{{0}}},{{{1}}}};
        f1={{{{1}},{{0}},{{0},{0,1}}}};
        f2={{{{0}},{{0,-1}}},{{{0}}},{{{0}}},{{{0}},{{0},{0,1}}}};
        f3={{{{0},{0,1}}},{{{0}}},{{{0}}},{{{0,-1}}}}
        f4={{{{-1}},{{0}},{{0}},{{0}},{{1}}}}
```

$f$ が $< f_1, f_2, f_3, f_4 >$ の元であるか否かを調べる。

```
In[43]:=G=Groeb[{f1,f2,f3,f4}]
Out[43]={{{{{1}},{{0}},{{0},{0,1}}}},
        {{{{0}},{{0,-1}}},{{{0}}},{{{0}}},{{{0}},{{0},{0,1}}}},
        {{{{0},{0,1}}},{{{0}}},{{{0}}},{{{0,-1}}}},
        {{{{-1}},{{0}},{{0}},{{0}},{{1}}}},
        {{{{0}},{{0}},{{0,1}}},{{{0}}},{{{0}}},{{{1}}}},
        {{{{0},{-1}},{{0}},{{0,-1}}}},{{{{0},{0,1}},{{0}},{{1}}}},
        {{{{0}},{{0,-1},{0},{0,1}}}},{{{{0,-1},{0},{0,1}}}},
        {{{{1},{0},{-1}}}},{{{{1,0,-1}}}}}
```

$< f_1, f_2, f_3, f_4 >=< g : g \in G >$ より、$f$ が $< g : g \in G >$ の元であるかどうかを調べる。

```
In[44]:=PolyDiv[f,G]
Out[44]={{{{{{-1}}}},{{{{0}}}},{{{{0}},{{0}},{{1}}}},{{{{0}}}},
        {{{{0}}},{{{0}}},{{{0}}},{{{1}}}},{{{{0}}}},{{{{0}}}},{{{{0}}}},
        {{{{0}}}},{{{{0}}}},{{{{0}}}}},{{{{0}}}}}
```

余りが $0$ なので、$f \in < g : g \in G >$ より、$f \in < f_1, f_2, f_3, f_4 >$である。

# Bibliography


[1] David Cox, John Little, Donal O'Shea : *Ideals, Varieties, and Algorithm*, Springer-Verag New York, 1996

[2] 上野健爾 : 代数幾何入門, 岩波書店, 1995

[3] 酒井文雄 : 環と体の理論, 共立出版, 1997

[4] 藤崎源二郎 : 体とガロア理論, 岩波書店, 1991

[5] E. アルティン著 寺田文行訳 : ガロア理論入門, 東京書籍, 1974

[6] J. ロットマン著 関口次郎訳 : ガロア理論, シュプリンガー・フェアラーク東京, 1997

[7] 堀田良之 : 代数入門 - 群と加群 - , 裳華房, 1987

[8] 上野健爾, 志賀浩二, 砂田利一 編集 :
数学の楽しみ No.11 「多項式環の視点:グレブナー基底」, 日本評論社, 1999