整数係数多項式環$\boldsymbol{Z}[x_1, \cdots, x_n]$のイデアルについて

大塚美紀生

Hilbert Basis Theoremにより，Noether環Rを係数とする多項式環$R[x_1, \cdots, x_n]$のイデアルは有限生成であることが知られているが，係数環Rが体であれば，生成元をGröbner basisと呼ばれる標準基底にとることができる。本稿では，体を有理整数環$\boldsymbol{Z}$にしても，Gröbner basisにあたる標準基底が存在することを証明する。その結果は，有理整数環$\boldsymbol{Z}$を一般のユークリッド整域(Euclidean domain)に置き換えてもそのまま成り立つ。

用語や表記法の説明はあとにまわして，まず定理の主張を記述する。

定理１ $\boldsymbol{Z}[x_1, \cdots, x_n]$のmonomial ideal I[注1]は，

$$I = \langle a_1 x^{\alpha(1)}, a_2 x^{\alpha(2)}, \cdots, a_s x^{\alpha(s)} \rangle \quad (a_i \in \boldsymbol{Z},\ \alpha(i) \in \boldsymbol{Z}^n_{\geq 0}),$$
$$(a_i) \subset (a_1) \subset \boldsymbol{Z} \quad (i = 2, \cdots, s)$$

と表される有限生成イデアルである。

定理２ $\boldsymbol{Z}[x_1, \cdots, x_n]$の任意のイデアル$I$[注1]は有限生成イデアルであり，

$$I = \langle f_1, f_2, \cdots, f_s \rangle,$$
$$\mathrm{LT}(f_i) = a_i x^{\alpha(i)} \ \ (a_i \in \boldsymbol{Z},\ \ \alpha(i) \in \boldsymbol{Z}^n_{\geq 0}),$$
$$(a_i) \subset (a_1) \subset \boldsymbol{Z} \quad (i = 2, \cdots, s)$$

と表すことができる。ここに，$\mathrm{LT}(f)$はfの最高次の項を表す。

定理３ $\boldsymbol{Z}[x_1, \cdots, x_n]$の任意のイデアル$I$は

$$I = \langle f_1, f_2, \cdots, f_s \rangle,$$
$$\mathrm{LT}(f_i) = a_i x^{\alpha(i)} \ \ (a_i \in \boldsymbol{Z},\ \ \alpha(i) \in \boldsymbol{Z}^n_{\geq 0}),$$
$$(a_1) \supset (a_2) \supset \cdots \supset (a_s)$$

と表すことができる。

表記法と準備

環，体，多項式，(体でない)環のイデアルなどの基本的な用語については，代数学の教科書(例えば[1], [3]など)を参照してもらいたい。[2]には，最低限の知識が効率良くまとめられている。以下では，本稿で新たに必要となるものをまとめておく。

n個の0以上の整数の組の集合を$\boldsymbol{Z}^n_{\geq 0}$と表し，

$$x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} = x^\alpha, \quad \alpha = (\alpha_1, \alpha_2, \cdots, \alpha_n) \in \boldsymbol{Z}^n_{\geq 0}$$

と略記する。$\boldsymbol{Z}^n_{\geq 0}$における順序$>$は，本稿では[注2]

$$\alpha = (\alpha_1, \alpha_2, \cdots, \alpha_n) > \beta = (\beta_1, \beta_2, \cdots, \beta_n)$$

であることを，

$$\alpha_1+\alpha_2+\cdots+\alpha_n>\beta_1+\beta_2+\cdots+\beta_n$$

または

$$\alpha_1+\alpha_2+\cdots+\alpha_n=\beta_1+\beta_2+\cdots+\beta_n \text{ のとき}$$
$$\alpha-\beta \text{ の成分の左から初めて } 0 \text{ でないものが正}$$

であることにより定める。例えば，

$$(3,\ 2,\ 0)>(3,\ 1,\ 1)>(3,\ 0,\ 2)>(2,\ 3,\ 0)>(3,\ 0,\ 1)>(1,\ 2,\ 0)$$

である。この順序 $>$ で最大の α を最高次といい，$f\in \boldsymbol{Z}[x_1,\ \cdots,\ x_n]$ の最高次 $\alpha=(\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_n)$ を $\mathrm{Deg}\,f$，最高次の項を $\mathrm{LT}(f)$，$\mathrm{LT}(f)$ の係数を $\mathrm{LC}(f)$ で表す。

$$f=7x^3y^2+4x^2y^3+6x^2y^2z-8x^2y-9yz^2$$

であれば，

$$\mathrm{Deg}\,f=(3,\ 2),\quad \mathrm{LT}(f)=7x^3y^2,\quad \mathrm{LC}(f)=7$$

である。

Lemma 1　$\boldsymbol{Z}[x_1,\ \cdots,\ x_n]$ のイデアル I に対して，

$$L=\{\mathrm{LC}(f)\,;f\in I\}$$

は $\boldsymbol{Z}$ のイデアルである。

(証明)　$a,\ b\in L$ とすると，

$$f=ax^{\alpha}+\cdots\quad(\alpha=\mathrm{Deg}\,f),\quad g=bx^{\beta}+\cdots\quad(\beta=\mathrm{Deg}\,g)$$

となる $f,\ g\in I$ が存在する。$\gamma=(\gamma_1,\ \cdots,\ \gamma_n)$ を

$$\gamma_i=\max\{\alpha_i,\ \beta_i\}\quad(i=1,\ \cdots,\ n)$$

により定めると，$x^{\gamma-\alpha}f,\ x^{\gamma-\beta}g\in I$ より

$$x^{\gamma-\alpha}f+x^{\gamma-\beta}g=(a+b)x^{\gamma}+\cdots\in I$$

であるから，

$$a+b\in L$$

$0\in L$ であり，0 でない整数 k に対して

$$kf=kax^{\alpha}+\cdots\in I\quad(\alpha=\mathrm{Deg}\,kf)$$

であるから，

$$ka\in L$$

よって，L は $\boldsymbol{Z}$ のイデアルである。　(証明おわり)

$\boldsymbol{Z}$ は単項イデアル整域であるから，ある整数 a を用いて

$$\{\mathrm{LC}(f)\,;f\in I\}=(a)$$

と表される。なお，本稿では，整数 a で生成される $\boldsymbol{Z}$ のイデアルは (a) と表し，整数 a で生成される $\boldsymbol{Z}[x_1,\ \cdots,\ x_n]$ のイデアルは $\langle a\rangle$ と表すことで混同を避ける。

Lemma 2　$F=(f_1,\ \cdots,\ f_n)$ を $\boldsymbol{Z}[x_1,\ \cdots,\ x_n]$ に属する s 個の多項式の組とするとき，任意の $\boldsymbol{Z}[x_1,\ \cdots,\ x_n]$ の多項式 f に対して，

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

を満たす $\boldsymbol{Z}[x_1,\ \cdots,\ x_n]$ の多項式 $a_i,\ r$ が存在し，$r=0$ であるか，または r の各項はどの $\mathrm{LT}(f_i)$ でもそれ以上割れない(商が 0 になる)[注3] ようにできる。

(証明)　$a_i,\ r$ の存在を示すための手順として，単項式ごとに最高次の項どうしを比べて商と余りを求めていく。

$p=f,\ \ b_1=0,\ \ r=0$ をスタートして，$\mathrm{LT}(p)$ について $>$ の順に

- $\mathrm{LT}(p)$ が $\mathrm{LT}(f_1)$ で割れるとき,[注3]

$$p\longmapsto p-\left[\frac{\mathrm{LC}(p)}{\mathrm{LC}(f_1)}\right]x^{\mathrm{Deg}\,p-\mathrm{Deg}\,f_1}f_1,$$

$$b_1\longmapsto b_1+\left[\frac{\mathrm{LC}(p)}{\mathrm{LC}(f_1)}\right]x^{\mathrm{Deg}\,p-\mathrm{Deg}\,f_1}$$

と置き換え，r はそのままにする

- $\mathrm{LT}(p)$ が $\mathrm{LT}(f_1)$ で割れないとき，

$$p\longmapsto p-\mathrm{LT}(p),\ \ r\longmapsto r+\mathrm{LT}(p)$$

と置き換え，b_1 はそのままにする

という作業を続けて[注4]行き，$p=0$ になったときの b_1 を a_1 とする。
a_i まで定まったとき，$p=r=f-a_1f_1-\cdots-a_if_i,\ \ b_{i+1}=0$ として，f_{i+1} について同様に除法を行ない，ついには

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

の形が得られる。以上の操作手順を観察すれば，r の各項は，どの $\mathrm{LT}(f_i)$ でもそれ以上除法の作業はできないことがわかる。　(証明おわり)

$\boldsymbol{Z}[x_1,\ \cdots,\ x_n]$ のイデアル I が **monomial ideal** であるとは，単項式 $a_\alpha x^\alpha$ $(a_\alpha\in\boldsymbol{Z},\ \alpha\in\boldsymbol{Z}^n_{\geq 0})$ で生成されるイデアルのことをいう。monomial ideal を直訳すると「単項イデアル」となるが，単項イデアルは既に principal ideal の訳として定着しているので，本稿では混同を避けるためにそのまま monomial ideal と呼ぶことにする。

一般の可換環 R について，**ascending chain condition** (略して A.C.C.)[注5] とは，R のイデアルの列

$$I_1\subset I_2\subset I_3\subset\cdots$$

が有限で終わることをいう。環 R が A.C.C. を満たすとき，R は Noetherian であるといい，環 R を Noether 環と呼ぶ。

Lemma 3　可換環 R が A.C.C. を満たすための必要十分条件は，R の任意のイデアルが有限生成となることである。

(証明) 必要性を示すために，R に有限生成でないイデアル I があるとする。
I の 0 でない要素 a_1 をとると，有限生成でないから

$$(a_1) \subsetneqq I$$

であり，$a_2 \notin (a_1)$ なる I の要素 a_2 が存在する。以下同様に I の要素 $a_3,\ a_4,\ \cdots$ を定めていくと，イデアルの列

$$(a_1) \subsetneqq (a_1,\ a_2) \subsetneqq (a_1,\ a_2,\ a_3) \subsetneqq \cdots$$

が無限に続くことになり，A.C.C. を満たさない。

十分性を示すために，

$$I_1 \subset I_2 \subset I_3 \subset \cdots$$

を R のイデアルの列とする。

$$I = \bigcup_{n \geqq 1} I_n$$

と定めるとき，$a,\ b \in I$ に対して

$$a \in I_i,\quad b \in I_j$$

となる番号 $i,\ j$ が存在し，$m = \max\{i,\ j\}$ とするとき

$$a,\ b \in I_m$$

であり，I_m はイデアルであるから，

$$a + b \in I_m \subset I$$

R の任意の要素 r に対して，

$$ra \in I_i \subset I$$

よって，I は R のイデアルである。

I も有限生成であるから

$$I = (a_1,\ a_2,\ \cdots,\ a_s)$$

と表され，各 a_k に対して $a_k \in I_{i_k}$ となる番号 i_k が存在する。$n = \max\{i_1,\ i_2,\ \cdots,\ i_s\}$ とするとき

$$(a_1,\ a_2,\ \cdots,\ a_s) \subset I_n \subset I$$

となるから，

$$I_1 \subset I_2 \subset I_3 \subset \cdots \subset I_n = I_{n+1} = I_{n+2} = \cdots$$

が成り立つ。　(証明おわり)

定理１の証明

n についての数学的帰納法で証明する。

$n=1$ のとき，$\boldsymbol{Z}[x_1]$ の monomial ideal I [注1] の生成元 $ax_1^{\,d}\,(a\in\boldsymbol{Z},\ d\in\boldsymbol{Z}_{\geq 0})$ の中で係数が最小正であるものを $a_1x_1^{\,d_1}$ とする。d_1 次以上の I の生成元 $bx_1^{\,e}$ があれば，

$$b=a_1q+r,\quad 0\leqq r<a_1$$

を満たす整数 $q,\ r$ が存在し，

$$bx_1^{\,e}=qx_1^{\,e-d_1}\cdot a_1x_1^{\,d_1}+rx_1^{\,e}$$

と表されるから，生成元 $bx_1^{\,e}$ を $rx_1^{\,e}$ に取り替えることができる。ここで，$0<r<a_1$ であるとすれば，$a_1x_1^{\,d_1}$ を $rx_1^{\,e}$ に置き換えて以上の作業を行なうと，初めの a_1 より少ない回数でその作業は終わるから，ついには $r=0$ となって，もとから

$$a_1x_1^{\,d_1}\text{ 以外の生成元は }d_1\text{ 次より低次}$$

であるとしてよい。

$k=0,\ 1,\ \cdots,\ d_1-1$ に対して，$J_k=\{b\,;\,bx_1^{\,k}\in I\}$ とおくと，J_k は $\boldsymbol{Z}$のイデアルであるから

$$J_k=\{b\,;\,bx_1^{\,k}\in I\}=(b_k)$$

となる $b_k\in\boldsymbol{Z}$ が存在する。$b_k\neq 0$ のとき，

$$b_k=a_1q_k+r_k,\quad 0\leqq r_k<a_1$$

を満たす整数 $q_k,\ r_k$ が存在し，

$$b_kx_1^{\,k}\cdot x_1^{\,d_1-k}=q_k\cdot a_1x_1^{\,d_1}+r_kx_1^{\,d_1}\in I$$

より $r_kx_1^{\,d_1}\in I$ であり，a_1 の最小性より $r_k=0$ となるから

$$a_1\,|\,b_k$$

よって，$b_k\neq 0$ となる $b_kx_1^{\,k}\,(k=0,\ 1,\ \cdots,\ d_1-1)$ の項を $a_2x_1^{\,d_2},\ \cdots,\ a_sx_1^{\,d_s}$ で表せば，

$$I=\langle a_1x_1^{\,d_1},\ a_2x_1^{\,d_2},\ \cdots,\ a_sx_1^{\,d_s}\rangle,\quad (a_i)\subset(a_1)$$

である。

n のとき定理１が成り立つとして，$\boldsymbol{Z}[x_1,\ \cdots,\ x_n,\ y]$ の monomial ideal I を考える。Lemma 1 より，イデアル

$$L=\{\mathrm{LC}(f)\,;\,f\in I\}=(a_1)\quad(a_1\in\boldsymbol{Z})$$

が定められる。$\mathrm{LC}(f)=a_1$ となる $f\in I$ のうち y の次数が最小のものを f_1 として，

$$\mathrm{LT}(f_1)=a_1x^{\alpha(1)}y^e$$

とおくとき，$ax^\alpha y^e\in I$ となる ax^α で生成される $\boldsymbol{Z}[x_1,\ \cdots,\ x_n]$ の monomial ideal を J_e とする。L の定義より

$$\{\mathrm{LC}(f)\,;\,f\in J_e\}\subset L=(a_1)$$

であるが，$\mathrm{LT}(f_1)=a_1x^{\alpha(1)}y^e\in I$ より

$$a_1\in\{\mathrm{LC}(f)\,;\,f\in J_e\}$$

であるから，

$$(a_1)\subset\{\mathrm{LC}(f)\,;\,f\in J_e\}$$

両方の包含関係が示されたから，

$$\{\mathrm{LC}(f)\,;f\in J_e\}=(a_1)$$

したがって，帰納法の仮定より

$$J_e=\langle a_1x^{\alpha(1)},\ a_2x^{\alpha(2)},\ \cdots,\ a_sx^{\alpha(s)}\rangle,\quad (a_i)\subset(a_1)$$

となる。

$ax^\alpha y^{e-1}\in I$ となる ax^α で生成される $\boldsymbol{Z}[x_1,\ \cdots,\ x_n]$ の monomial ideal を J_{e-1}[注6] とすると，帰納法の仮定より

$$\{\mathrm{LC}(f)\,;f\in J_{e-1}\}=(b_1),\quad J_{e-1}=\langle b_1x^{\beta(1)},\ \cdots,\ b_tx^{\beta(t)}\rangle$$

と表され，

$$\{\mathrm{LC}(f)\,;f\in J_{e-1}\}\subset\{\mathrm{LC}(f)\,;f\in I\}=(a_1)$$[注7]

以上の操作を続けると，ついには

$$I=J_ey^e+J_{e-1}y^{e-1}+\cdots+J_1y+J_0$$[注6]

となって，各 k $(k=0,\ 1,\ \cdots,\ e)$ に対して

$$J_k=\langle c_1x^{\gamma(1)},\ \cdots,\ c_ux^{\gamma(u)}\rangle\quad \left(c_i\in\boldsymbol{Z},\ \gamma(i)\in\boldsymbol{Z}^n_{\geq 0}\right)$$

は有限生成[注6]であり，$(c_1)\subset(a_1)$[注7]であるから，$n+1$ のときも定理1は成り立つ。

（証明おわり）

定理2の証明

$$\mathrm{LT}(I)=\langle\mathrm{LT}(f)\,;f\in I\rangle$$

は monomial ideal であるから，定理1より

$$\mathrm{LT}(I)=\langle a_1x^{\alpha(1)},\ a_2x^{\alpha(2)},\ \cdots,\ a_sx^{\alpha(s)}\rangle,\quad (a_i)\subset(a_1)$$

と表される。このとき，

$$\mathrm{LT}(f_i)=a_i\,x^{\alpha(i)}\quad (i=1,\ 2,\ \cdots,\ s)$$

となる $f_i\in I$ が存在し，

$$\langle f_1,\ f_2,\ \cdots,\ f_s\rangle\subset I$$

逆に，任意の $f\in I$ に対して，Lemma 2 より

$$f=b_1f_1+b_2f_2+\cdots+b_sf_s+r\quad (b_i,\ r\in\boldsymbol{Z}[x_1,\ \cdots,\ x_n])$$

と表され，r の各項は $\mathrm{LT}(f_1),\ \cdots,\ \mathrm{LT}(f_s)$ のいずれでもそれ以上割れない（商が0になる）ようにできる。$r=0$ のときは

$$f\in\langle f_1,\ f_2,\ \cdots,\ f_s\rangle$$

である。$r\neq 0$ のときは，イデアルの性質から

$$r=f-b_1f_1-b_2f_2-\cdots-b_sf_s\in I$$

であるから，

$$\mathrm{LT}(r)\in\mathrm{LT}(I)=\langle a_1x^{\alpha(1)},\ a_2x^{\alpha(2)},\ \cdots,\ a_sx^{\alpha(s)}\rangle$$

であるが，線形結合を展開することにより

$$\mathrm{LT}(r)=h_1a_1x^{\alpha(1)}+h_2a_2x^{\alpha(2)}+\cdots+h_sa_sx^{\alpha(s)}\quad (h_i\in\boldsymbol{Z}[x_1,\ \cdots,\ x_n])$$

$$= (c_1a_1 + c_2a_2 + \cdots + c_sa_s)x^{\beta} \quad (c_i \in \boldsymbol{Z},\ \beta = \mathrm{Deg}\ r)$$

と表される。$r \neq 0$ より少なくとも一つの c_i は 0 でないが，$\mathrm{LT}(r)$ が $\mathrm{LT}(f_i) = a_i x^{\alpha(i)}$ でまだ割ることができるので矛盾する。よって，$r = 0$ となり，

$$I \subset <f_1,\ f_2,\ \cdots,\ f_s>$$

が成り立つ。

以上より，

$$I = <f_1,\ f_2,\ \cdots,\ f_s>,\ \ (a_i) \subset (a_1)$$

である。 (証明おわり)

定理３の証明

定理２により，$\boldsymbol{Z}[x_1,\ \cdots,\ x_n]$ のイデアル I は

$$I = <f_1,\ f_2,\ \cdots,\ f_s>,\ \ \mathrm{LT}(f_i) = a_i x^{\alpha(i)},\ \ (a_i) \subset (a_1)$$

と表される。ここで，

$$I \supsetneqq I_2 = <f_2,\ \cdots,\ f_s>$$

であるとすれば，I_2 に定理２を適用すると，

$$(b_1) = \{\mathrm{LC}(g)\,;g \in I_2\} \subset \{\mathrm{LC}(f)\,;f \in I\} = (a_1)$$

より

$$I_2 = <g_1,\ g_2,\ \cdots,\ g_t>,\ \ \mathrm{LT}(g_i) = b_i x^{\beta(i)},\ \ (b_i) \subset (b_1) \subset (a_1)$$

と表される。$I_2 \supsetneqq I_3 = <g_2,\ \cdots,\ g_t>$ であるとすれば，同様の操作を続けることにより，イデアルの列

$$<f_1> \subset <f_1,\ g_1> \subset \cdots$$

ができる。定理２より，特に $\boldsymbol{Z}[x_1,\ \cdots,\ x_n]$ の任意のイデアルは有限生成であるから，Lemma 3 によりこのイデアルの列は有限で終わる。[注8]

よって，$f_1,\ g_1,\ \cdots$ を順に $h_1,\ h_2,\ \cdots,\ h_u$ と定めると，

$$I = <h_1,\ h_2,\ \cdots,\ h_u>,\ \ \mathrm{LT}(h_i) = c_i\, x^{\gamma(i)}\ (c_i \in \boldsymbol{Z},\ \gamma(i) \in \boldsymbol{Z}^n_{\geq 0}),$$
$$(c_1) \supset (c_2) \supset \cdots \supset (c_u)$$

が成り立つ。 (証明おわり)

注 1　0だけから成る集合 $\{0\}$ もイデアルであるが，$\{0\}$ を考える意味がないときは，いちいち「0でないイデアル」と断らないことにする。

注 2　簡単のため，順序を一つに固定するが，本稿の定理は一般の monomial ordering でも成り立つ。$\boldsymbol{Z}^n_{\geq 0}$ における関係 $>$ が monomial ordering であるとは，

(i)　$>$ は全順序である

(ii)　$\alpha,\ \beta,\ \gamma \in \boldsymbol{Z}^n_{\geq 0}$ について，$\alpha > \beta \Longrightarrow \alpha + \gamma > \beta + \gamma$

(iii)　$>$ の順序において最小のものがある

の 3 条件を満たすときにいう。

注 3　高校数学とは異なって係数が体ではないから，係数についても(整数の)除法を考えなければならない。例えば，x^3y^2 は x^2y で割り切れるが，$5x^3y^2$ は $3x^2y$ では割り切れない。しかし，$5x^3y^2$ を $3x^2y$ を割る作業はまだ続けられて，

$$5x^3y^2 = 3x^2y \cdot xy + 2x^3y^2$$

となるが，$0 \leqq 2 < 3$ よりこれ以上の作業は続けられない。

注 4　例えば，$p = 5x^3y^2 + 4x^2y^2 + 2xy,\ \ f_1 = 3x^2y + 7xy^2,\ \ r = 0$ であるとき，次のような手順で計算している。

$$\mathrm{LT}(p) = 5x^3y^2,\ \ \mathrm{LC}(p) = 5,\ \ \mathrm{Deg}\, p = (3,\ 2)$$
$$\mathrm{LT}(f_1) = 3x^2y,\ \ \mathrm{LC}(f_1) = 3,\ \ \mathrm{Deg}\, f_1 = (2,\ 1)$$

1°　$5 = 3 \times 1 + 2,\ \ \mathrm{Deg}\, p - \mathrm{Deg}\, f_1 = (1,\ 1)$ であるから，

$$\begin{aligned} p &\longmapsto p - \left[\frac{\mathrm{LC}(p)}{\mathrm{LC}(f_1)}\right] x^{\mathrm{Deg}\, p - \mathrm{Deg}\, f_1} f_1 \\ &= 5x^3y^2 + 4x^2y^2 + 2xy - 1 \cdot xy(3x^2y + 7xy^2) \\ &= 2x^3y^2 - 7x^2y^3 + 4x^2y^2 + 2xy \end{aligned}$$

$$b_1 \longmapsto \left[\frac{\mathrm{LC}(p)}{\mathrm{LC}(f_1)}\right] x^{\mathrm{Deg}\, p - \mathrm{Deg}\, f_1} = xy$$

$$r = 0$$

2°　$\mathrm{LT}(p) = 2x^3y^2$ は $\mathrm{LT}(f_1) = 3x^2y$ で割れないから，

$$p \mapsto p - \mathrm{LT}(p) = -7x^2y^3 + 4x^2y^2 + 2xy$$
$$b_1 = xy$$
$$r \mapsto r + 2x^3y^2 = 2x^3y^2$$

3°　$\mathrm{LT}(p) = -7x^2y^3,\ \ \mathrm{LT}(f_1) = 3x^2y,\ \ -7 = 3 \times (-3) + 2,$
$\mathrm{Deg}\, p - \mathrm{Deg}\, f_1 = (2,\ 3) - (2,\ 1) = (0,\ 2)$ であるから，

$$\begin{aligned} p &\longmapsto p - \left[\frac{\mathrm{LC}(p)}{\mathrm{LC}(f_1)}\right] x^{\mathrm{Deg}\, p - \mathrm{Deg}\, f_1} f_1 \\ &= -7x^2y^3 + 4x^2y^2 + 2xy - (-3y^2)(3x^2y + 7xy^2) \end{aligned}$$

$$= 2x^2y^3 + 4x^2y^2 + 21xy^4 + 2xy$$

$$b_1 \longmapsto b_1 + \left[\frac{\mathrm{LC}(p)}{\mathrm{LC}(f_1)}\right] x^{\mathrm{Deg}\, p - \mathrm{Deg}\, f_1} = xy + (-3y^2) = xy - 3y^2$$

$$r = 2x^3y^2$$

4° $\mathrm{LT}(p) = 2x^2y^3$ は $\mathrm{LT}(f_1) = 3x^2y$ で割れないから，

$$p \mapsto p - \mathrm{LT}(p) = 4x^2y^2 + 21xy^4 + 2xy$$

$$b_1 = xy - 3y^2$$

$$r \mapsto r + 2x^3y^3 = 2x^3y^2 + 2x^2y^3$$

5° $\mathrm{LT}(p) = 4x^2y^2$, $\mathrm{LT}(f_1) = 3x^2y$, $4 = 3 \times 1 + 1$,
$\mathrm{Deg}\, p - \mathrm{Deg}\, f_1 = (2,\ 2) - (2,\ 1) = (0,\ 1)$ であるから，

$$p \longmapsto p - \left[\frac{\mathrm{LC}(p)}{\mathrm{LC}(f_1)}\right] x^{\mathrm{Deg}\, p - \mathrm{Deg}\, f_1} f_1$$

$$= 4x^2y^2 + 21xy^4 + 2xy - 1 \cdot y(3x^2y + 7xy^2)$$

$$= x^2y^2 + 21xy^4 - 7xy^3 + 2xy$$

$$b_1 \longmapsto b_1 + y = xy - 3y^2 + y$$

$$r = 2x^3y^2 + 2x^2y^3$$

6° $p = x^2y^2 + 21xy^4 - 7xy^3 + 2xy$ の各項は $\mathrm{LT}(f_1) = 3x^2y$ でもう割れないから，
$b_1 = xy - 3y^2 + y$ のまま

$$(p,\ r) \longmapsto (21xy^4 - 7xy^3 + 2xy,\ \ 2x^3y^2 + 2x^2y^3 + x^2y^2)$$

$$\longmapsto (-7xy^3 + 2xy,\ \ 2x^3y^2 + 2x^2y^3 + x^2y^2 + 21xy^4)$$

$$\longmapsto (2xy,\ \ 2x^3y^2 + 2x^2y^3 + x^2y^2 + 21xy^4 - 7xy^3)$$

$$\longmapsto (0,\ \ 2x^3y^2 + 2x^2y^3 + x^2y^2 + 21xy^4 - 7xy^3 + 2xy)$$

と置き換えられていき，最終的に

$$5x^3y^2 + 4x^2y^2 + 2xy$$

$$= (3x^2y + 7xy^2)(xy - 3y^2 + y) + 2x^3y^2 + 2x^2y^3 + x^2y^2 + 21xy^4 - 7xy^3 + 2xy$$

が得られる。

$n \geqq 2$ であれば，

$$p = 2x^3y^2 + 2x^2y^3 + x^2y^2 + 21xy^4 - 7xy^3 + 2xy$$

と f_2 に対して同様の作業を行ない，以下 f_n まで行なう。

注 5　ascending chain condition は日本語では **昇鎖律** というが，最近ではあまり見聞きしない。本文では，A.C.C. という表現で統一することにした。A.C.C. とは，上に続く任意のイデアルの列が有限個で終わるということであって，環の中にイデアルが有限個しかないという意味ではない。たとえば，有理整数環 $\boldsymbol{Z}$ は，素因数分解できる(有限個の素数の積で表される)ことにより A.C.C. を満たすが，(素数は無数に存在するので) イデアルは無数に存在する。

注 6　$J_k = (0)$ となる場合もあり得る。

注 7　1 変数の場合であれば，次数の最小性より $(b_1) \subsetneqq (a_1)$ が成り立つが，2 変数以上になると $\alpha = (\alpha_1,\ \cdots,\ \alpha_n) > \beta = (\beta_1,\ \cdots,\ \beta_n)$ であっても $x^\beta \,|\, x^\alpha$ とは限らないので，y の次数 e が最小でも $(b_1) = (a_1)$ となり得る。

注 8　$\mathrm{LT}(I) = \langle \mathrm{LT}(f_1),\ \cdots,\ \mathrm{LT}(f_s) \rangle$ という条件を追加して生成元を選んでいくと，有限生成を疑わしく感じるかもしれないが，どのような有限生成であっても A.C.C. を満たすから，イデアルの列

$$\langle f_1 \rangle \subset \langle f_1,\ g_1 \rangle \subset \cdots$$

は有限で終わる。有限生成をわざわざ A.C.C. に言い換えておく理論の存在も，こうした議論に陥る可能性を想定してのことだと思われる。

参考文献

[1] D.Cox and J.Little and D.O'Shea,
Ideals, Varieties, and Algorithms, Third Edition, Springer-Verlag (2007)

[2] 大塚美紀生，整数係数多項式環 $\boldsymbol{Z}[x]$ のイデアルについて，
早稲田数学フォーラム (2008)
(http://homepage2.nifty.com/wasmath/z[x]-ideal.pdf)

[3] J.J.Watkins, *Topics in commutative ring theory*,
Princeton University Press (2007)

2015．1.16
修正　2015．1.20
追加　2015．2．2