# グレブナ基底と代数多様体入門 (Ideals, Varieties, and Algorithms)

ashiato45 のメモ，著者は D.Cox, J.Little, D.O'Shea

2015 年 4 月 27 日

## 1　幾何，代数，アルゴリズム

## 2　グレブナ基底

### 2.1　はじめに

いままでは 1 変数の多項式を研究してきたか，ここからは多変数を研究することになる．多項式のイデアルに関して，次の問題を話題とする．

- イデアルの記述：イデアル $I \subset k[x_1, \ldots, x_n]$ があったとき，$I = \langle f_1, \ldots, f_n \rangle$ となる $f_1, \ldots, f_n \in k[x_1, \ldots, x_n]$ は存在するか？ それを求める手段はあるか？
- イデアルの所属：$f, f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ があったとき，$f \in \langle f_1, \ldots, f_s \rangle$ の真偽を判定するアルゴリズムはあるか？
- 多様体の点の決定，あるいは求解：$f_1, \ldots, f_s \in k[x]$ について，$f_1(x_1, \ldots, x_n) = f_2(x_1, \ldots, x_n) = \cdots = f_s(x_1, \ldots, x_n) = 0$ の解は何か？ 言い換えるなら，$\mathbf{V}(f_1, \ldots, f_s)$ は何か？
- 陰関数表示：$x_1 = f_1(t_1, \ldots, t_s), \ldots, x_n = f_n(t_1, \ldots, t_s)$ とパラメタ表示された図形について，それを包むアフィン多様体はあるか？ それは何か？[*1]？

多項式のうち特殊なものを考えたとき，これらに対する解答の一部は得られている．

まず，1 変数多項式の場合は「イデアルの記述」と「イデアルの所属」は解決している．「イデアルの記述」は $k[x]$ が PID であることから常に可能で，しかも 1 つの生成元で実現する．しかし，具体的なアルゴリズムは分からない．「イデアルの所属」も可能で，所属するかどうかを調べたい有限生成イデアルを，GCD を考えることにより単項生成にし，所属を調べたい多項式をその GCD で割った余りを調べることにより可能である．余りがなければ GCD の倍元なので，イデアルに所属し，余りがあれば所属しない．

また，多変数でも 1 次式だと分かっていれば，「多様体の点の決定」と「陰関数表示」は線形代数を使うことにより可能である．

- 「多様体の点の決定，あるいは求解」：1 次連立方程式を解けばよいが，これは掃き出し法により常に可能である．解がなかったり，パラメタ付けが得られたりする．
- 「陰関数表示」：パラメタが 1 次式のときに，これがアフィン多様体であることが示せ，さらに陰関数表示を求められる．若干工夫がいる．$k^n$ で考える．

$$x_1 = a_{11}t_1 + \cdots + a_{1N}t_N + c_1 \tag{1}$$

$$\vdots \tag{2}$$

$$x_n = a_{n1}t_1 + \cdots + a_{nN}t_N + c_N \tag{3}$$

[*1] 「アフィン多様体かその部分集合である」とあるが，それはあたりまえで，常に $k^n$ の部分集合である．→うそでした．アフィン空間をアフィン多様体と呼ぶかどうかがよくわからない．

を考える．このパラメタ表示であらわされる点全体を $V \subset k^n$ とする．これは，$k^n$ のアフィン線形空間 (原点がずれててもいい) になっている．パラメタ表示なので，$x_\bullet$ のどれかについて条件はないみたいなのは直接的にはない (結果的にあるかもしれない)．$(x_1, \ldots, x_n) \in V$ となるための条件を調べよう．
全て左辺に以降して，

$$\begin{pmatrix} a_{11} & \cdots & a_{1N} & -1 & \ldots & 0 & c_1 \\ \vdots & & & & & & \vdots \\ a_{n1} & \cdots & a_{nN} & 0 & \ldots & -1 & c_N \end{pmatrix} \begin{pmatrix} t_1 \\ \vdots \\ t_N \\ x_1 \\ \vdots \\ x_n \\ 1 \end{pmatrix} = \mathbb{0}. \tag{4}$$

この係数行列を狭義階段行列まで変形して，$(b_{i,j})_{n,(N+n+1)}$ としておく．すると，ピボットが $n$ 個以下得られる．そのピボットの個数を $M(\leq N)$ とする．そのピボットのうち，$1$ から $N$ 列目にあるもの，すなわち $t_1, \ldots, t_N$ に対応するものを，左にあるものから順に $t_{f(1)}, \ldots, t_{f(M)}$ とする．

この準備のもとで，

$$(x_1,\dots,x_n)\in V \tag{5}$$

$$\iff {}^{\exists}t_1,\dots,t_N\colon \begin{pmatrix} a_{11} & \cdots & a_{1N} & -1 & \dots & 0 & c_1 \\ \vdots & & & & & & \vdots \\ a_{n1} & \cdots & a_{nN} & 0 & \dots & -1 & c_N \end{pmatrix} \begin{pmatrix} t_1 \\ \vdots \\ t_N \\ x_1 \\ \vdots \\ x_n \\ 1 \end{pmatrix} = \mathbb{0} \tag{6}$$

$$\iff {}^{\exists}t_1,\dots,t_N\colon (b_{i,j})_{n,(N+n+1)} \begin{pmatrix} t_1 \\ \vdots \\ t_N \\ x_1 \\ \vdots \\ x_n \\ 1 \end{pmatrix} = \mathbb{0} \tag{7}$$

$$\iff {}^{\exists}t_1,\dots,t_N\colon \begin{cases} b_{11}t_1+\cdots+b_{1N}t_N+b_{1,(N+1)}x_1+\cdots+b_{1,(N+n)}x_n+b_{1,(N+n+1)} & =0 \\ & \vdots \\ b_{n1}t_1+\cdots+b_{nN}t_N+b_{n,(N+1)}x_1+\cdots+b_{n,(N+n)}x_n+b_{n,(N+n+1)} & =0 \end{cases} \tag{8}$$

$$\iff {}^{\exists}t_1,\dots,t_N\colon \tag{9}$$

$$\begin{cases} b_{1,f(1)}t_{f(1)}+\cdots+b_{1,f(M)+1}t_{f(M)+1}+\cdots+b_{1,N}t_N+b_{1,(N+1)}x_1+\cdots+b_{1,(N+n)}x_n+b_{1,(N+n+1)} & =0 \\ b_{2,f(2)}t_{f(2)}+\cdots+b_{2,f(M)+1}t_{f(M)+1}+\cdots+b_{2,N}t_N+b_{2,(N+1)}x_1+\cdots+b_{2,(N+n)}x_n+b_{2,(N+n+1)} & =0 \\ \vdots & \vdots \\ b_{M,f(M)}t_{f(M)}+b_{M,f(M)+1}t_{f(M)+1}+\cdots+b_{M,N}t_N+b_{M,(N+1)}x_1+\cdots+b_{M,(N+n)}x_n+b_{M,(N+n+1)} & =0 \\ b_{(M+1),f(M)+1}t_{f(M)+1}+\cdots+b_{(M+1),N}t_N+b_{(M+1),(N+1)}x_1+\cdots+b_{(M+1),(N+n)}x_n+b_{(M+1),(N+n+1)} & =0 \\ & \vdots \\ b_{n,f(M)+1}t_{f(M)+1}+\cdots+b_{n,N}t_N+b_{n,(N+1)}x_1+\cdots+b_{n,(N+n)}x_n+b_{n,(N+n+1)} & =0 \end{cases} \tag{10}$$

$$\iff {}^{\exists}t_{f(1)},\dots,t_{f(M)},t_{f(M)+1},\dots,t_N\colon \tag{11}$$

$$\begin{cases} b_{1,f(1)}t_{f(1)}+\cdots+b_{1,f(M)+1}t_{f(M)+1}+\cdots+b_{1,N}t_N+b_{1,(N+1)}x_1+\cdots+b_{1,(N+n)}x_n+b_{1,(N+n+1)} & =0 \\ b_{2,f(2)}t_{f(2)}+\cdots+b_{2,f(M)+1}t_{f(M)+1}+\cdots+b_{2,N}t_N+b_{2,(N+1)}x_1+\cdots+b_{2,(N+n)}x_n+b_{2,(N+n+1)} & =0 \\ \vdots & \vdots \\ b_{M,f(M)}t_{f(M)}+b_{M,f(M)+1}t_{f(M)+1}+\cdots+b_{M,N}t_N+b_{M,(N+1)}x_1+\cdots+b_{M,(N+n)}x_n+b_{M,(N+n+1)} & =0 \\ b_{(M+1),f(M)+1}t_{f(M)+1}+\cdots+b_{(M+1),N}t_N+b_{(M+1),(N+1)}x_1+\cdots+b_{(M+1),(N+n)}x_n+b_{(M+1),(N+n+1)} & =0 \\ & \vdots \\ b_{n,f(M)+1}t_{f(M)+1}+\cdots+b_{n,N}t_N+b_{n,(N+1)}x_1+\cdots+b_{n,(N+n)}x_n+b_{n,(N+n+1)} & =0 \end{cases} \tag{12}$$

$t_1$ から $t_{f(M)}$ までのうち，ピボットになってないものを抜いた． (13)

⇒ は，ピボットになっていないものを，その左のピボットに押し付ければ可能．⇐ はあきらか． (14)

$$\iff {}^{\exists}t_{f(1)},\dots,t_{f(M)}\colon \tag{15}$$

$$\begin{cases} b_{1,f(1)}t_{f(1)}+b_{1,(N+1)}x_1+\cdots+b_{1,(N+n)}x_n+b_{1,(N+n+1)} & =0 \\ b_{2,f(2)}t_{f(2)}+b_{2,(N+1)}x_1+\cdots+b_{2,(N+n)}x_n+b_{2,(N+n+1)} & =0 \\ \vdots & \vdots \\ b_{M,f(M)}t_{f(M)}+b_{M,(N+1)}x_1+\cdots+b_{M,(N+n)}x_n+b_{M,(N+n+1)} & =0 \\ b_{(M+1),(N+1)}x_1+\cdots+b_{(M+1),(N+n)}x_n+b_{(M+1),(N+n+1)} & =0 \\ & \vdots \\ b_{n,(N+1)}x_1+\cdots+b_{n,(N+n)}x_n+b_{n,(N+n+1)} & =0 \end{cases} \tag{16}$$

ピボットだけを残した．⇒ は，消したものをピボットの $t_\bullet$ に押し付けて，消すものに $0$ を入れれば可能．⇐ はあきらか． (17)

これで，存在を中に入れられ，$t_\bullet$ が残っている分は，$t_1, \dots, t_N$ のうち 1 個しか残っていないから $x_1, \dots, x_n$ にあわせて決めればいいし，$t_\bullet$ が残っていない分は存在はもう関係ないので単に $x_\bullet$ 同士の関係である．この残った関係が，陰関数表示に他ならない．

(問題 1) (a) $(x^2-3x+2) \div (x-2) = (x-1)\dots 0$．よって，$(x^2-3x+2) \in \langle x-2 \rangle$．

(b) $(x^5-4x+1) \div (x^3-x^2+x) = (x^2+x)\dots(-x^2-4x+1)$．よって，$(x^5-4x+1) \notin \langle x^3-x^2+x \rangle$．

(c) $(x^4-6x^2+12x-8) \div (2x^3-10x^2+16x-4)/2 = x+5 \dots 11x^2-24x+12$．$\frac{11}{2}(2x^3-10x^2+16x-4) - (11x^2-24x+12)x = -31x^2+76x-44$．$(-31x^2+76x-44)+3(11x^2-24x+12) = 2(x^2+2x-4)$．$(11x^2-24x+12)-11(x^2+2x-4) = (-2)(23x-16)$．…飽きた．`code/calcgcd.hs` で計算．$\mathrm{GCD}(x^4-6x^2+12x-8, 2x^3-10x^2+16x-4) = 1$．よって，$x^2-4x+4 \in \langle 1 \rangle = I$．

(d) `code/calcgcd.hs` で計算．$\mathrm{GCD}(x^9-1, x^5+x^3-x^2-1) = x^3-1$．よって，$x^3-1 \in \langle x^3-1 \rangle = I$．

(問題 2) (a)

$$\begin{pmatrix} 2 & -3 & -1 & 9 \\ 1 & -1 & 0 & 1 \\ 3 & 7 & -2 & 17 \end{pmatrix} \to \begin{pmatrix} 1 & -1 & 0 & 1 \\ 2 & -3 & -1 & 9 \\ 3 & 7 & -2 & 17 \end{pmatrix} \tag{18}$$

$$\to \begin{pmatrix} 1 & -1 & 0 & 1 \\ 0 & -1 & -1 & 7 \\ 0 & 10 & -2 & 14 \end{pmatrix} \tag{19}$$

$$\to \begin{pmatrix} 1 & -1 & 0 & 1 \\ 0 & -1 & -1 & 7 \\ 0 & 0 & -12 & 84 \end{pmatrix} \tag{20}$$

$$\to \begin{pmatrix} 1 & -1 & 0 & 1 \\ 0 & -1 & -1 & 7 \\ 0 & 0 & 1 & -7 \end{pmatrix} \tag{21}$$

$$\to \begin{pmatrix} 1 & -1 & 0 & 1 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & -7 \end{pmatrix} \tag{22}$$

$$\to \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & -7 \end{pmatrix} \tag{23}$$

$$\tag{24}$$

よって，このアフィン多様体は 1 点で，$\{(1, 0, -7)\}$．

(b)

$$\begin{pmatrix} 1 & 1 & -1 & -1 & 0 \\ 1 & -1 & 1 & 0 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 1 & -1 & -1 & 0 \\ 0 & -2 & 2 & 1 & 0 \end{pmatrix} \tag{25}$$

$$\to \begin{pmatrix} 1 & 1 & -1 & -1 & 0 \\ 0 & 1 & -1 & -1/2 & 0 \end{pmatrix} \tag{26}$$

$$\to \begin{pmatrix} 1 & 0 & 0 & -1/2 & 0 \\ 0 & 1 & -1 & -1/2 & 0 \end{pmatrix} \tag{27}$$

よって，パラメタ付け

$$x_1 = -\frac{1}{2}x_4, \quad x_2 = x_3 + \frac{1}{2}x_4. \tag{28}$$

(c) $y = x^3, \quad z = x^5$．

(問題 3) (a) 左から，$t, x_1, x_2, x_3,$ 定数 の順で並べる．

$$\begin{pmatrix} 1 & -1 & 0 & 0 & -5 \\ 2 & 0 & -1 & 0 & 1 \\ -1 & 0 & 0 & -1 & 6 \end{pmatrix} \to \begin{pmatrix} 1 & -1 & 0 & 0 & -5 \\ 0 & 2 & -1 & 0 & 11 \\ 0 & -1 & 0 & -1 & 1 \end{pmatrix} \tag{29}$$

ここから $t$ を含まないものを取り出せばよいから (さっき示した．)

$$2x_1 - x_2 = 11, \quad -x_1 - x_3 = 1. \tag{30}$$

(b) 左から，$t, u, x_1, x_2, x_3, x_4,$ 定数．

$$\begin{pmatrix} 2 & -5 & -1 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & -1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 3 & 0 & 0 & 0 & -1 & 0 \end{pmatrix} \to \begin{pmatrix} -1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 2 & -5 & -1 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & -1 & 0 & 0 & 0 \\ 1 & 3 & 0 & 0 & 0 & -1 & 0 \end{pmatrix} \tag{31}$$

$$\to \begin{pmatrix} -1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & -3 & -1 & 0 & 2 & 0 & 0 \\ 0 & 3 & 0 & -1 & 1 & 0 & 0 \\ 0 & 4 & 0 & 0 & 1 & -1 & 0 \end{pmatrix} \tag{32}$$

$$\to \begin{pmatrix} -1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & -3 & -1 & 0 & 2 & 0 & 0 \\ 0 & 3 & 0 & -1 & 1 & 0 & 0 \\ 0 & 1 & -1 & 0 & 3 & -1 & 0 \end{pmatrix} \tag{33}$$

$$\to \begin{pmatrix} -1 & 0 & 1 & 0 & -2 & 1 & 0 \\ 0 & 0 & -4 & 0 & 11 & -3 & 0 \\ 0 & 0 & 3 & -1 & -8 & 3 & 0 \\ 0 & 1 & -1 & 0 & 3 & -1 & 0 \end{pmatrix} \tag{34}$$

$$\tag{35}$$

よって，$t, s$ を含まないところを取り出して，

$$-4x_1 + 11x_3 - 3x_4 = 0, \quad 3x_1 - x_2 - 8x_3 + 3x_4 = 0. \tag{36}$$

(c) $y = x^4$, $z = x^7$.

(問題 4) (a) 略．

(b) 仮に $\langle x_1, \ldots \rangle = \langle f_1, \ldots, f_s \rangle$ となる $f_1, \ldots, f_s \in k[x_1, \ldots]$ が存在したとする (背理法)．

- $f_1, \ldots, f_s$ のうちで，定数項を含むものがあるとき：それを $f_1$ として一般性を失なわない．$f_1 \notin \langle x_1, \ldots \rangle$ である．矛盾．
- $f_1, \ldots, f_s$ が全て 1 次以上であるとき：$f_1, \ldots, f_s$ に含まれる変数ではない新たな変数 $x_N$ を考えると，これは左辺に属するが，右辺に属さない (必ず $x_N$ を含むなら，必ずそれは 2 次以上になってしまう．)

(問題 5) (a) 個数は，$\sum_{i=0}^{m}(m-i+1) = (m+1)^2 - \sum_{i=0}^{m} i = (m+1)^2 - \frac{m(m+1)}{2} = (m+1)(m+1-\frac{m}{2}) = \frac{(m+1)(m+2)}{2}$.

(b) $k$ で線形従属であることを示さないと意味がないのでは？ 線形従属は，$u + v \leq m$ をみたすものたち，つまり，

$$\{[f(t)]^u [g(t)]^v | u + v \leq m\} \tag{37}$$

が $k$ 上 1 次従属であることを示す．この項たちは (a) より $\frac{(m+1)(m+2)}{2}$ 個である．また，この項たちの $k[t]$ としての次数は

$$\deg [f(t)]^u [g(t)]^v = u \deg f(t) + v \deg g(t) \leq n(u+v) \leq nm. \tag{38}$$

よって，$m$ を十分大きくすると，項の個数が $m^2$ オーダーで増えていくので，$nm$ 次以下多項式のなす $k$-線形空間が $n + m + 1$ 次であることから，1 次従属となる．

(c) 線形従属なので，$[f(t)]^u [g(t)]^v$ の，すべては 0 でない 1 次結合で 0 が作れる．その式の $f(t)$ を $x$ に，$g(t)$ を $y$ に置換すると，$x, y$ の多項式を $k$ 係数で結合して 0 となったもの，つまり陰関数表示が得られる．パラメタ付けされた曲線はこの陰関数表示の曲線上にある．

(d) 同様の議論をする．$x^u y^v z^w$ の単項式で，$u+v+w \leq m$ となるものの個数は，

$$\sum_{u=0}^{m}\sum_{v=0}^{m-u}\sum_{w=0}^{m-u-v} = \sum_{u=0}^{m}\sum_{v=0}^{m-u}(m-u-v+1) \tag{39}$$

$$= \sum_{u=0}^{m}((m-u+1)^2 - \sum_{v=0}^{m-u} v) \tag{40}$$

$$= \sum_{u=0}^{m}((m-u+1)^2 - (m-u+1)) \tag{41}$$

$$= \sum_{u=0}^{m}(u^2 - 2(m+1)u + (m+1)^2 + u - (m+1)) \tag{42}$$

$$= \frac{m(m+1)(2m+1)}{6} + (-2m-1)\frac{m(m+1)}{2} + m(m+1)^2 \tag{43}$$

$$= \frac{m(m+1)(m+2)}{3}. \tag{44}$$

これが，

$$\{[f(t,\tau)]^u[g(t,\tau)]^v[h(t,\tau)]^w | u+v+w \leq m\} \tag{45}$$

たちの個数であるが，一方これらの次数は，$f, g, h$ の次数が $n$ 以下だとすると，

$$\deg([f(t,\tau)]^u[g(t,\tau)]^v[h(t,\tau)]^w) = u\deg f + v\deg g + w\deg h \leq (u+v+w)n \leq mn. \tag{46}$$

よって，次数の増え方は 1 次だが，多項式の個数の増え方は 3 次なので，上の多項式たちは十分大きい $m$ で 1 次従属になる．よって，それらの多項式で，まともな線形結合をして 0 になる式を作れるので，$f, g, h$ を $x, y, z$ に置換することにより，アフィン多様体が得られる．

## 2.2 多変数多項式の順序付け

1 変数多項式の割り算のとき，これがうまく行くことは単項式の次数による順序付けが以下の性質を持っていることに依存していた．

- 線形順序：すべての単項式 $x^n, x^m$ について，$x^n > x^m$ か $x^n = x^m$ か $x^n < x^m$ かが成立する．これのおかげで，多項式について最高次というものを考えることができ，次数を落とすという操作が意味を持った．
- 順序をかけ算で保つ：$x^n > x^m$ について，$x^{n+l} > x^{m+l}$ であった．これのおかげで，割る多項式を最高次を割られる多項式に合わせるために何倍かするとき，より低い次数の単項式が突然高い次数を持って次数が下がらないという事態にならなかった．
- 最小がある (整列順序)：$x^{n_1} > x^{n_2} > \ldots$ という列は無限には続かない．これのおかげで，途中経過で無限に低い次数が出続けて多項式の割り算が停止しないということがなかった．

あるいは 1 次多変数のときも，変数に順序をつけていた．これについても「線形順序」「順序に下限がある」は満たしていた (「順序をかけ算で保つ」は使わなかった．1 次の特有の性質．)

多項式はいままで $x^\alpha y^\beta \ldots z^\gamma$ とあらわしてきたが，$n$ 次の単項式は指数に注目して，$\mathbb{Z}^n_{\geq 0}$ と同型がつくので，以降こちらで考える．$\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$ について，単項式のかけ算は $\alpha+\beta$ となるし，全次数は $|\alpha|$ となる．

これに倣って，$k[x_1, \ldots, x_n]$ の単項式，あるいは $\mathbb{Z}^n_{\geq 0}$ の順序 $>$ とは，次の性質を持つものであるとする．

- 線形順序：$f, g \in \mathbb{Z}^n_{\geq 0}$ について，$f > g$ か $f = g$ か $f < g$ である．
- 順序をかけ算で保つ：$\alpha > \beta \implies \alpha+\gamma > \beta+\gamma$．
- 最小がある (整列順序)：$\mathbb{Z}^n_{\geq 0}$ の任意の非空部分集合には，$>$ についての最小元が存在する．

整列順序についての特徴付けを見る．これは，アルゴリズムの停止を証明するときに便利である：集合 $X$ 上の順序 $>$ が整列順序であることと，$X$ の元の無限列 $\alpha_1 > \alpha_2 > \ldots$ が存在しないことは同値である．

証明
対偶を示す．

- 整列順序でない $\implies$ 無限列がある：仮定より，$X$ の空でない集合で，最小元がないもの $A \subset X$ が存在する．$A$ は空でないので，$x_1 \in A$ となる $x_1$ が存在する．$x_1$ は $A$ の最小元ではないので，$x_1 > x_2$ となる $x_2 \in A$ が存在する．これをくりかえして，無限列 $x_1 > x_2 > x_3 > \dots$ を得る．
- 無限列がある $\implies$ 整列順序でない：仮定より，$X$ の無限列 $x_1 > x_2 > \dots$ が存在する．$X$ の部分集合として，$\{x_1, \dots\}$ を考える．任意の $x_i \in \{x_1, \dots\}$ について，$x_i > x_{i+1}$ なので，最小元が存在しない．

(証終)

あとで，「線形順序」「順序をかけ算で保つ」の下で，「整列順序」は任意の $\alpha \in \mathbb{Z}^n_{\geq 0}$ について $\alpha \geq 0$ であることと等価であることを見る．

例えば，$\mathbb{Z}_{\geq 0}$ 上の通常の順序は多項式の順序である．証明は自然数の性質による．

まず簡単な $\mathbb{Z}^n_{\geq 0}$ の単項式順序として，lex[*2]順序 $>_{lex}$ を見る．これは，

$$(\alpha_1, \dots, \alpha_n) > (\beta_1, \dots, \beta_n) \iff (\alpha_1 - \beta_1, \dots, \alpha_n - \beta_n)\text{の0でない最も左の元が正．} \tag{47}$$

とする．これは，左端から比べていって，同じならば次へ，異なるならばその要素の大小で勝敗を決するとも読める．つまり，$(\alpha_1, \dots, \alpha_n)$ と $(\beta_1, \dots, \beta_n)$ との大小は，

- $\alpha_1 > \beta_1$ のとき：$\alpha > \beta$
- $\alpha_1 < \beta_1$ のとき：$\alpha < \beta$
- $\alpha_1 = \beta_1$ のとき：$(\alpha_2, \dots, \alpha_n)$ と $(\beta_2, \dots, \beta_n)$ との大小

ということになる．最悪 $\mathbb{Z}_{\geq 0}$ での比較になるので，そこで決着がつく．

先に，整列順序について便利な補題を示しておく (教科書にはない．)：「整列順序の非増加列は安定する」：$>$ を $X$ 上の整列順序とする．$X$ 上の列 $x_1 \geq x_2 \geq \dots$ について，$N$ が存在して，$x_N = x_{N+1} = \dots$ となる．

証明
仮に $x_n > x_{n+1}$ となる $n$ が無数に存在すると，そこをつなげて狭義減少列が作れてしまうが，これは整列順序であることに矛盾する．よって，$x_n > x_{n+1}$ となる $n$ は有限個しかない．その $n$ のうち最大のものを $N-1$ とすると，$x_N = x_{N+1} = \dots$ である．

(証終)

lex 順序 $>_{lex}$ が確かに単項式の順序であることを示す．

証明

- 線形順序であること：$\alpha = (\alpha_1, \dots, \alpha_n), \beta = (\beta_1, \dots, \beta_n)$ とする．$\alpha > \beta$ でも $\alpha = \beta$ でもないとする．$\alpha > \beta$ ではないので，$(\alpha_1 - \beta_1, \dots, \alpha_n - \beta_n)$ のすべての元が正でなく，0 か負である．よって，$\beta - \alpha = (\beta_1 - \alpha_1, \dots, \beta_n - \alpha_n)$ のすべての元は 0 か正である．すべての元が 0 だとすると，$\alpha = \beta$ となり仮定に反するので，少なくとも 1 つの元が正であり，$\beta < \alpha$ である．
- 順序を保つこと：$\alpha - \beta = (\alpha + \gamma) - (\beta + \gamma)$ から従う．
- 整列順序であること：仮に $\mathbb{Z}^n_{\geq 0}$ の無限列 $x^{(0)} > x^{(1)} > \dots$ が存在したとしよう．$n$ の帰納法で示す (背理法)．
  - $n = 1$ のとき？ ：これは $\mathbb{Z} \geq 0$ の無限狭義減少列の存在を示しているが，自然数の性質より矛盾．
  - $n$ のとき成立 $\implies$ $n+1$ のとき？ ：$x^{(m)}_1 < x^{(m+1)}_1$ となる $m$ が存在すると，そこで $x^{(m)} < x^{(m+1)}$ となり，矛盾するので，常に $x^{(m)}_1 \geq x^{(m+1)}_1$ であり，$m \mapsto x^{(m)}_1$ は単調非増加列である．これは整列順序である $\mathbb{Z}_{\geq 0}$ の単調非増加列なので，ある $N$ 以降安定し，

    $$x^{(N)}_1 = x^{(N+1)}_1 = \dots \tag{48}$$

    となる．しかし，$x^{(N)} > x^{(N+1)} > \dots$ なので，$\pi \colon \mathbb{Z}^{n+1}_{\geq 0} \to \mathbb{Z}^n_{\geq 0}$ を数ベクトルの頭 1 つを切り落す射影と

[*2] lexicographic order．辞書順．

すると，

$$\pi x^{(N)} > \pi x^{(N+1)} > \dots \tag{49}$$

となる．これは，「$n$ のとき成立」から出る矛盾より，矛盾．

よって，帰納的に，すべての $n$ で矛盾が得られる．

(証終)

lex 順序は，変数の順序のつけかたに依存して変わる．2 変数なら $x > y$ ということにするか $y > x$ ということにするかの 2 種類があり，$n$ 変数なら $n!$ 種類ある．

次に，grlex[*3]順序を見る．$\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$ について，$\alpha >_{grlex} \beta$ とは，

- $|\alpha| > |\beta|$ なら，$\alpha >_{grlex} \beta$ である．
- $(|\alpha| = |\beta|$ であり，$)\alpha >_{lex} \beta$ なら，$\alpha > \beta$ である．

となる順序である．

これも，単項式順序になってることを見る．

証明

- 線形順序であること：$\alpha$ と $\beta$ を全次数と $>_{lex}$ で比べた 9 通りについて全て定まることから従う．
- かけ算で保つこと：$\alpha >_{grlex} \beta$ とする．
  - $|\alpha| > |\beta|$ のとき：$|\alpha + \gamma| = |\alpha| + |\gamma| > |\beta| + |\gamma| = |\beta + \gamma|$.
  - $|\alpha| = |\beta|$ のとき：$|\alpha + \gamma| = |\alpha| + |\gamma| = |\beta| + |\gamma| = |\beta + \gamma|$ である．さらに，$\alpha >_{lex} \beta$ となるので，$>_{lex}$ の性質により，$\alpha + \gamma >_{lex} \beta + \gamma$ となる．
- 整列順序であること：$>_{grlex}$ に関する狭義減少列 $x_1 > x_2 > \dots$ があったとする．仮に $|x_n| < |x_{n+1}|$ となる $n$ があったとすると，$x_n <_{grlex} x_{n+1}$ となるので，常に $|x_n| \geq |x_{n+1}|$ である．よって，$|x_1| \geq |x_2| \geq \dots$ であり，これは $\mathbb{Z}_{\geq 0}$ の単調非増加列なので，補題よりある $N$ 以降 $|x_N| = |x_{N+1}| = \dots$ となる．しかし，$x_N >_{grlex} x_{N+1} >_{grlex} \dots$ なので，$x_N >_{lex} x_{N+1} >_{lex} \dots$ となり，lex 順序に関する狭義減少列が得られた．これは矛盾である．

(証終)

次に，grevlex[*4]順序を見る．$\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$ について，$\alpha >_{grevlex} \beta$ とは，

- $|\alpha| > |\beta|$ なら，$\alpha >_{grevlex} \beta$ である．
- $(|\alpha| = |\beta|$ であり，$)$ $(\alpha_1 - \beta_1, \dots, \alpha_n - \beta_n)$ の一番右の 0 でない要素が負であることである．

つまり，まず次数で比較して大きいほうが大きい．次数が同じなら，右から順番に見ていって「小さいほうが」大きい．一見，「grlex 順序の変数を付け替えて逆にすれば grevlex 順序になるのでは？」と思うが，不可能である．$x_1 >_{grevlex} \cdots >_{grevlex} x_n$ と同じになる $>_{grlex}$ を構成しようとしてみる．が，少なくとも $x_1 >_{grlex} \cdots >_{grlex} x_n$ にならなければならない．$x^2yz^2 >_{grlex} xy^3z$．一方，$x^2yz^2 <_{grevlex} xy^3z$ となる．2 変数だと grlex と grevlex の両者は一致してしまう．

grevlex 順序が単項式の順序であることを示そう．最後の比較は，多項式の方向を逆にした lex 順序の反転である．この順序を $>_{lex'}$ としておく．$>_{lex'}$ は単項式順序になっている←なっていない!!!(あとでこれは rinvlex 順序とよぶ．)．つまり，$\alpha >_{lex'} \beta$ とは，$\alpha - \beta$ の一番右側の 0 でない元が負であることである．

[*3] graded lexicographic

[*4] graded reverse lexicographic

証明

- 線形順序であること：$\alpha > \beta$ でなく $\alpha < \beta$ でもないとする．$\alpha > \beta$ ではないので，

$$\neg((|\alpha| > |\beta|) \vee (|\alpha| \leq |\beta| \to \alpha >_{lex'} \beta)) \tag{50}$$
$$\iff \neg((|\alpha| > |\beta|) \vee (|\alpha| > |\beta| \vee \alpha >_{lex'} \beta)) \tag{51}$$
$$\iff (|\alpha| \leq |\beta|) \wedge (|\alpha| \leq |\beta| \wedge \alpha \leq_{lex'} \beta) \tag{52}$$
$$\iff (|\alpha| \leq |\beta|) \wedge (\alpha \leq_{lex'} \beta) \tag{53}$$

  また，$\alpha < \beta$ ではないので，同様に

$$(|\alpha| \geq |\beta|) \wedge (\alpha \geq_{lex'} \beta). \tag{54}$$

  よって，$\alpha = \beta$ である．
- かけ算で保たれること：あきらか．
- 整列順序であること：減少列 $\alpha_1 >_{grevlex} \alpha_2 >_{grevlex} \dots$ が存在するとする．ある $n$ で $|\alpha_n| < |\alpha_{n+1}|$ であるとすると，$\alpha_n < \alpha_{n+1}$ となってしまい矛盾なので，常に $|\alpha_n| \geq |\alpha_{n+1}|$ となる．これは，$\mathbb{Z}_{\geq 0}$ の非増加列である．よって，ある $N$ 以降で，$|\alpha_N| = |\alpha_{N+1}| = \dots$ となる．$\alpha_N >_{grevlex} \alpha_{N+1} >_{grevlex} \dots$ となっているので，$\alpha_N >_{lex'} \alpha_{N+1} >_{lex'} \dots$ となる．$|\alpha_N| = |\alpha_{N+1}| = \dots$ なので，これら $\alpha_N, \alpha_{N+1}, \dots$ の全次数は一致していなければならず，したがってこのような元は有限個しか存在しない．しかし，$\alpha_N >_{lex'} \alpha_{N+1} >_{lex'} \dots$ は，$\alpha_N, \alpha_{N+1}, \dots$ が全て異なることを要求している．これは，全次数が一定な $\mathbb{Z}^n_{\geq 0}$ の元が無限個存在することを意味するので，矛盾である．

(証終)

これで単項式について順序が入ったので，1 変数多項式の「先頭項」などが拡張できる．$f = \sum_{\alpha \in \mathbb{Z}^n_{\geq 0}} a_\alpha x^\alpha$ について，

- $f$ の多重指数 (multidegree) とは，(次数の拡張)$a_\alpha \neq 0$ なる $\alpha \in \mathbb{Z}^n_{\geq 0}$ のうち，$\alpha$ が，今採用している順序について最高のものの $\alpha$ のことである．これを $\mathrm{multideg}(f)$ と書く．

$$\mathrm{multideg}(f) = \max\left\{\alpha | \alpha \in \mathbb{Z}^n_{\geq 0} \wedge a_\alpha \neq 0\right\} \tag{55}$$

  である．
- $f$ の先頭係数 (leading coefficient) とは，多重指数を持つ項の係数のことで，つまり $a_{\mathrm{multideg}(f)}$ のことである．$\mathrm{LC}(f)$ と書く．
- $f$ の先頭単項式 (leading monomial) とは，多重指数を持つ項の単項式のことで，つまり $x^{\mathrm{multideg}(f)}$ のことである．$\mathrm{LM}(f)$ と書く．
- $f$ の先頭項 (leading term) とは，多重指数を持つ項のことで，$\mathrm{LT}(f)$ と書く．$\mathrm{LT}(f) = \mathrm{LC}(f) \cdot \mathrm{LM}(f)$.

multidegree について，以下の性質が成り立つ．証明は演習．

- $\mathrm{multideg}(fg) = \mathrm{multideg}(f) + \mathrm{multideg}(g)$.
- $f + g \neq 0$ なら，$\mathrm{multideg}(f+g) \leq \max(\mathrm{multideg}(f), \mathrm{multideg}(g))$．さらに，$\mathrm{multideg}(f) \neq \mathrm{multideg}(g)$ ならば，等号が成立する．

(問題 1) (a) $f(x,y,z) = 2x + 3y + z + x^2 - z^2 + x^3$ について．

- lex 順序：$f(x,y,z) = x^3 + x^2 + 2x + 3y - z^2 + z$. $\mathrm{LM}(f) = x^3$. $\mathrm{LT}(f) = x^3$. $\mathrm{multideg}(f) = (3,0,0)$.
- grlex 順序：$f(x,y,z) = x^3 + x^2 - z^2 + 2x + 3y + z$. $\mathrm{LM}(f) = x^3$. $\mathrm{LT}(f) = x^3$. $\mathrm{multideg}(f) = (3,0,0)$.
- grevlex 順序：$f(x,y,z) = x^3 + x^2 - z^2 + 2x + 3y + z$. $\mathrm{LM}(f) = x^3$. $\mathrm{LT}(f) = x^3$. $\mathrm{multideg}(f) = (3,0,0)$.

(b) $f(x,y,z) = 2x^2y^8 - 3x^5yz^4 + xyz^3 - xy^4$ について．

- lex 順序：$f(x,y,z) = -3x^5yz^4 + 2x^2y^8 - xy^4 + xyz^3$. $\mathrm{LM}(f) = x^5yz^4$. $\mathrm{LT}(f) = -3x^5yz^4$. $\mathrm{multideg}(f) = (5,1,4)$.
- grlex 順序：$f(x,y,z) = -3x^5yz^4 + 2x^2y^8 - xy^4 + xyz^3$. $\mathrm{LM}(f) = x^5yz^4$. $\mathrm{LT}(f) = -3x^5yz^4$. $\mathrm{multideg}(f) = (5,1,4)$.

- grevlex 順序：$f(x,y,z) = 2x^2y^8 - 3x^5yz^4 - xy^4 + xyz^3$. $\mathrm{LM}(f) = x^2y^8$. $\mathrm{LT}(f) = 2x^2y^8$. $\mathrm{multideg}(f) = (2,8,0)$.

(問題 2) (a) grlex.
(b) grevlex.
(c) lex.

(問題 3) (a) $f(x,y,z) = 2x + 3y + z + x^2 - z^2 + x^3$ について.
- lex 順序：$f(x,y,z) = -z^2+z+3y+x^3+x^2+2x$. $\mathrm{LM}(f) = z^2$. $\mathrm{LT}(f) = -z^2$. $\mathrm{multideg}(f) = (2,0,0)$.
- grlex 順序：$f(x,y,z) = x^3-z^2+x^2+z+3y+2x$. $\mathrm{LM}(f) = x^3$. $\mathrm{LT}(f) = x^3$. $\mathrm{multideg}(f) = (0,0,3)$.
- grevlex 順序：$f(x,y,z) = x^3-z^2+x^2+2x+3y+z$. $\mathrm{LM}(f) = x^3$. $\mathrm{LT}(f) = x^3$. $\mathrm{multideg}(f) = (0,0,3)$.

(b) $f(x,y,z) = 2x^2y^8 - 3x^5yz^4 + xyz^3 - xy^4$ について.
- lex 順序：$f(x,y,z) = -3x^5yz^4 + xyz^3 + 2x^2y^8 - xy^4$. $\mathrm{LM}(f) = x^5yz^4$. $\mathrm{LT}(f) = -3x^5yz^4$. $\mathrm{multideg}(f) = (4,1,5)$.
- grlex 順序：$f(x,y,z) = -3x^5yz^4 + 2x^2y^8 + xyz^3 - xy^4$. $\mathrm{LM}(f) = x^5yz^4$. $\mathrm{LT}(f) = -3x^5yz^4$. $\mathrm{multideg}(f) = (4,1,5)$.
- grevlex 順序：$2x^2y^8-3x^5yz^4-xy^4+xyz^3$. $\mathrm{LM}(f) = x^2y^8$. $\mathrm{LT}(f) = 2x^2y^8$. $\mathrm{multideg}(f) = (0,8,2)$.

(問題 4) やった.

(問題 5) やった.

(問題 6) $x_1 >_{lex} \cdots >_{lex} x_n$ のとき，$x_n >_{invlex} \cdots >_{invlex} x_1$. 略.

(問題 7) (a) 仮に $\alpha < 0$ となる $\alpha \in \mathbb{Z}^n_{\geq 0}$ が存在したとしよう (背理法). $0 > \alpha$ である. このとき，「かけ算で保つ」より，両辺に $\alpha$ を足して (多項式としてはかけて)，$\alpha > 2\alpha$ である. これを続けると，$0 > \alpha > 2\alpha > 3\alpha > \ldots$ という狭義減少列が得られる. これは，$>$ が単項式順序であり，「整列集合である」ことに反する.

(b) $x^\alpha | x^\beta$ とする. $x^\beta = x^\gamma x^\alpha$ となる $\gamma \in \mathbb{Z}^n_{\geq 0}$ が存在する. よって，$\beta = \gamma + \alpha$ である. $\gamma \geq 0$ が (a) から従う. 単項式順序の「かけ算で保つ」より，両辺に $\alpha$ を足して $\alpha + \gamma \geq \alpha$ を得る. よって，$\beta = \gamma + \alpha \geq \alpha$.

(c)「最小」とは，その元が集合に属し，しかも下限になっていること，つまり任意の集合に属する元は，その下限の元以上になることであった. $\alpha \in \alpha + \mathbb{Z}^n_{\geq 0}$ はあきらかなので，任意の $\beta \in \alpha + \mathbb{Z}^n_{\geq 0}$ について，$\beta \geq \alpha$ を示せばよい. $\beta \in \alpha + \mathbb{Z}^n_{\geq 0}$ なので，$\gamma \in \mathbb{Z}^n_{\geq 0}$ で，$\beta = \alpha + \gamma$ となるものが存在する. (b) より，$\beta \geq \alpha$ である.

(問題 8) 先頭項の大きいものから順に，上から下へ並んでいる.

(問題 9) (a)
- $\Rightarrow$：$\alpha >_{grevlex} \beta$ でかつ，$|\alpha| > |\beta|$ でないとする. $|\alpha| < |\beta|$ だとすると，$\alpha <_{grevlex} \beta$ となり矛盾するので，$\alpha = \beta$ である. あとは $\alpha >_{rinvlex} \beta$ を調べればよい. 今，$|\alpha| = |\beta|$ なので，$\alpha - \beta$ の一番右の 0 でない元が負である. よって，$\beta - \alpha$ の一番右の 0 でない元が正であり，$\beta - \alpha >_{invlex} 0$ である. よって，$\beta >_{invlex} \alpha$ である. よって，$\beta <_{rinvlex} \alpha$ である.
- $\Leftarrow$：$|\alpha| > |\beta|$ のときはあきらかに $\alpha >_{grevlex} \beta$ である. あとは，「$|\alpha| = |\beta|$ で，しかも $\alpha >_{rinvlex} \beta$」のときを調べればよい. $|\alpha| = |\beta|$ なので，$\alpha - \beta$ の一番右の 0 でない元が負であることを言えばよい. $\alpha >_{rinvlex} \beta$ なので，$\alpha <_{invrex} \beta$ である. よって，$\beta - \alpha$ の一番右側の 0 でない元が正である. よって，$\alpha - \beta$ の一番右側の 0 でない元は負である.

(b) 単項式順序でない. $>_{rinvlex}$ を $x$ と書く. $x > x^2 > x^3 > \ldots$ という無限列が得られる. (問題 5 の証明が間違ってた!)

(問題 10) 必ずしも正しくない. lex 順序だと，

$$(2,0) > \cdots > (1,3) > (1,2) > (1,1) > (1,0) > (0,0) \tag{56}$$

となり，$(2,0)$ と $(0,0)$ との間には $(1,0), (1,1), (1,2), \ldots$ が無数に存在する.

一方，grlex 順序ではそのようなことは起こらない. $\alpha > \gamma > \beta$ となる $\gamma$ を考えると，$|\alpha| \geq |\gamma| \geq |\beta|$ となり (たくさんやったので略)，$\gamma$ の全次数は有限個しかありえない. ある全次数を持つ $\mathbb{Z}^n_{\geq 0}$ の元はまた有限個しか存在しないので，$\gamma$ は有限個しかありえない.

(問題 11) (a) $f=\sum_\alpha a_\alpha x^\alpha$ とする．$m=x^\beta$ とする．$mf=\sum_\alpha a_\alpha x^{\alpha+\beta}$ となる．よって，

$$\begin{aligned}\mathrm{multideg}(mf) &= \max\{\alpha+\beta | a_\alpha \neq 0\} && (57)\\ &= \max\{\alpha | a_\alpha \neq 0\}+\beta && (58)\\ &= \mathrm{multideg}(f)+\beta. && (59)\end{aligned}$$

よって，

$$\begin{aligned}\mathrm{LT}(mf) &= a_{\mathrm{multideg}(mf)-\beta}x^{\mathrm{multideg}(mf)} && (60)\\ &= a_{\mathrm{multideg}(f)}x^{\mathrm{multideg}(f)+\beta} && (61)\\ &= ma_{\mathrm{multideg}(f)}x^{\mathrm{multideg}(f)} && (62)\\ &= m\mathrm{LT}(f). && (63)\end{aligned}$$

(b) $f=\sum_\alpha a_\alpha x^\alpha$，$g=\sum_\beta b_\beta x^\beta$ とする．$fg=\sum_\alpha\sum_\beta a_\alpha b_\beta x^{\alpha+\beta}$．

$$\begin{aligned}\mathrm{multideg}(fg) &= \max\{\alpha+\beta | a_\alpha b_\beta \neq 0\} && (64)\\ &= \max\{\alpha+\beta | a_\alpha \neq 0 \wedge b_\beta \neq 0\} && (65)\\ &\overset{\text{かけ算で保つ}}{=} \max\{\alpha+\max\{\beta | b_\beta\neq 0\} | a_\alpha \neq 0\} && (66)\\ &= \max\{\alpha+\mathrm{multideg}(g) | a_\alpha \neq 0\} && (67)\\ &= \max\{\alpha | a_\alpha \neq 0\}+\mathrm{multideg}(g) && (68)\\ &= \mathrm{multideg}(f)+\mathrm{multideg}(g). && (69)\end{aligned}$$

$$\begin{aligned}\mathrm{LC}(fg) &= \sum_{\alpha+\beta=\mathrm{multideg}(fg)} a_\alpha b_\beta && (70)\\ &= \sum_{\alpha+\beta=\mathrm{multideg}(f)+\mathrm{multideg}(g)} a_\alpha b_\beta && (71)\\ &= a_{\mathrm{multideg}(f)}b_{\mathrm{multideg}(g)} && (72)\\ &= \mathrm{LC}(f)\mathrm{LC}(g). && (73)\end{aligned}$$

よって，

$$\begin{aligned}\mathrm{LT}(fg) &= \mathrm{LC}(fg)\mathrm{LM}(fg) && (74)\\ &= \mathrm{LC}(f)\mathrm{LC}(g)x^{\mathrm{multideg}(fg)} && (75)\\ &= \mathrm{LC}(f)\mathrm{LC}(g)x^{\mathrm{multideg}(f)+\mathrm{multideg}(g)} && (76)\\ &= \mathrm{LC}(f)\mathrm{LC}(g)\mathrm{LM}(f)\mathrm{LM}(g) && (77)\\ &= \mathrm{LT}(f)\mathrm{LT}(g). && (78)\end{aligned}$$

(c) $f_1=x$, $f_2=-x$, $g_1=y$, $g_2=y$ とする．このとき，$\sum_{i=1}^2 f_ig_i=xy-xy=0$ となる．よって，このとき，$\mathrm{LM}(\sum_{i=1}^2 f_ig_i)$ が定義されない？

(問題 12) (a) (i) (11-b) でやった．

(ii) $f=\sum_\alpha a_\alpha x^\alpha$，$g=\sum_\alpha b_\alpha x^\alpha$ とする．$\mathrm{multideg}(f)\geq\mathrm{multideg}(g)$ として一般性を失なわない．このとき，$b_\alpha=0 \implies a_\alpha=0$ である．←嘘!! $\mathrm{multideg}(f)\geq\mathrm{multideg}(f+g)$ を示せばよい．まず，

$$\forall N>0\colon a_{\mathrm{multideg}(f)+N}+b_{\mathrm{multideg}(f)+N}=0 \quad (79)$$

を示す．仮に $a_{\mathrm{multideg}(f)+N}+b_{\mathrm{multideg}(f)+N}\neq 0$ となる $N>0$ が存在したとする (背理法)．multideg の性質より，$a_{\mathrm{multideg}(f)+N}=0$ である．よって，$b_{\mathrm{multideg}(f)+N}\neq 0$ である．これは，$\mathrm{multideg}(g)>\mathrm{multideg}(f)$ を意味するが，矛盾である．よって，(79) は成立する．これはつまり，

$$\alpha>\mathrm{multideg}(f) \implies a_\alpha+b_\alpha=0 \quad (80)$$

だが，対偶をとって，

$$a_\alpha + b_\alpha \neq 0 \implies \alpha \leq \mathrm{multideg}(f). \tag{81}$$

よって，$\mathrm{multideg}(f+g) = \max\{\alpha | a_\alpha + b_\alpha \neq 0\} \leq \mathrm{multideg}(f)$.
さらに，$\mathrm{multideg}(f) > \mathrm{multideg}(g)$ を仮定する．$a_{\mathrm{multideg}(f)} + b_{\mathrm{multideg}(f)} \neq 0$ を示す．これが示されれば，

$$\mathrm{multideg}(f) \leq \max\{\alpha | a_\alpha + b_\alpha \neq 0\} = \mathrm{multideg}(f+g) \tag{82}$$

となり，等号が示されるからである．仮に $a_{\mathrm{multideg}(f)} + b_{\mathrm{multideg}(g)} = 0$ となるとする．$a_{\mathrm{multideg}(f)} \neq 0$ なので，$b_{\mathrm{multideg}(f)} \neq 0$ である．これは，$\mathrm{multideg}(f) > \mathrm{multideg}(g)$ に反する．よって，$a_{\mathrm{multideg}(f)} + b_{\mathrm{multideg}(f)} \neq 0$ である．

(b)
- 等しくなる：lex 順序を使う．$f = x^2$，$g = xy$ とする．$\mathrm{multideg}(f+g) = (2,0)$ である．一方，$\mathrm{multideg}(f) = (2,0)$，$\mathrm{multideg}(g) = (1,1)$ であり，$\max(\mathrm{multideg}(f), \mathrm{multideg}(g)) = (2,0)$ であり，等しくなる．
- 等しくならない：lex 順序を使う．$f = x^2+1$，$g = -x^2$ とする．$\mathrm{multideg}(f+g) = \mathrm{multideg}(1) = (0,0)$ である．一方，$\mathrm{multideg}(f) = (2,0)$，$\mathrm{multideg}(g) = (2,0)$ であり，$\max(\mathrm{multideg}(f), \mathrm{multideg}(g)) = (2,0)$ であり，等しくならない．

## 2.3 $k[x_1, \ldots, x_n]$ の割り算アルゴリズム

多変数の割り算アルゴリズムでは，ある多項式を複数の多項式で割るということを考える．ここで，$f$ を $F = (f_1, \ldots, f_s)$(これは多項式の組) で割るとは，

- 

$$f = a_1 f_1 + \cdots + a_s f_s + r \tag{83}$$

- $r$ のすべての単項式は $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)$ のどれでもわりきれない
- $a_i f_i \neq 0 \implies \mathrm{multideg}(a_i f_i) \leq \mathrm{multideg}(f)$

$a_1, \ldots, a_n, r \in k[x_1, \ldots, x_n]$ を求めることとする．このようなものを求める手続があることを示そう．a

**Algorithm 1** $k[x_1, \ldots, x_n]$ の割り算

証明

1: $stock := f$
2: $a_1, \ldots, a_s := 0$
3: $r := 0$
4: **while** $stock \neq 0$ **do**
5: $\quad divisionoccured :=$ `false`
6: $\quad i := 1$
7: $\quad$ /* まず割るだけ割ってみる */
8: $\quad$ **while** $divisionoccured =$ `false` かつ $i \leq s$ **do**
9: $\quad\quad$ **if** $\mathrm{LT}(f_i) | \mathrm{LT}(stock)$ **then**
10: $\quad\quad\quad a_i \Leftarrow a_i + \dfrac{\mathrm{LT}(stock)}{\mathrm{LT}(f_i)}$
11: $\quad\quad\quad stock \Leftarrow stock - \dfrac{\mathrm{LT}(stock)}{\mathrm{LT}(f_i)} f_i$
12: $\quad\quad\quad divisionoccured \Leftarrow$ `true`
13: $\quad\quad$ **end if**
14: $\quad\quad i \Leftarrow i + 1$
15: $\quad$ **end while**
16: $\quad$ /* 割れなければ余りを出す */
17: $\quad$ **if** $divisionoccured =$ `false` **then**
18: $\quad\quad r \Leftarrow r + \mathrm{LT}(stock)$
19: $\quad\quad stock \Leftarrow stock - \mathrm{LT}(stock)$
20: $\quad$ **end if**
21: **end while**

以下のことを示せばよい．

- 和の関係が保たれる：L.3 の時点と L.21 の時点で常に

$$f = a_1 f_1 + \cdots + a_s f_s + stock + r \tag{84}$$

が保たれることを示そう．L.3 ではあきらか．L.4 の時点で，

$$f = a_{1b} f_1 + \cdots + a_{sb} f_s + stock_b + r_b \tag{85}$$

であるとし，L.21 の時点では，$a_{1a}, \ldots, a_{sa}, stock_a, r_a$ となったとする．

  - $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)$ のうちで，$\mathrm{LT}(stock_b)$ を割り切るものがあるとき：そのようなもののうち最小のものを $f_i$ とする．このとき，$j \neq i$ について，

$$a_{ja} = \begin{cases} a_{jb} & j \neq i \\ a_{ib} + \frac{\mathrm{LT}(stock_b)}{\mathrm{LT}(f_i)} & j = i \end{cases} \tag{86}$$

となり，

$$stock_a = stock_b - \frac{\mathrm{LT}(stock_b)}{\mathrm{LT}(f_i)} f_i \tag{87}$$

となり，

$$r_a = r_b \tag{88}$$

となる．たしかに，

$$a_{1a}f_1 + \cdots + a_{sa}f_s + stock_a + r_a = \sum_{j=1}^{s} a_{jb}f_j + \frac{\mathrm{LT}(stock_b)}{\mathrm{LT}(f_i)}f_i + stock_b - \frac{\mathrm{LT}(stock_b)}{\mathrm{LT}(f_i)}f_i + r_b \tag{89}$$

$$= a_{1b}f_1 + \cdots + a_{sb}f_s + stock_b + r_b. \tag{90}$$

– $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)$ のうちで，$\mathrm{LT}(stock_b)$ を割り切るものがないとき：L9-L.13 は実行されず，L.17-L.20 だけが実行される．このとき，

$$a_{ja} = a_{jb} \tag{91}$$

$$stock_a = stock_b - \mathrm{LT}(stock_b) \tag{92}$$

$$r_a = r_b + \mathrm{LT}(stock_b) \tag{93}$$

となる．そして，

$$a_{1a}f_{1a} + \cdots + a_{sa}f_{sa} + stock_a + r_a = a_{1b}f_{1b} + \cdots + a_{sb}f_{sb} + stock_b - \mathrm{LT}(stock_b) + r_b + \mathrm{LT}(stock_b) \tag{94}$$

$$= a_{1b}f_{1b} + \cdots + a_{sb}f_{sb} + stock_b + r_b. \tag{95}$$

どちらにせよ，$a_1f_1 + \cdots + a_sf_s + stock + r$ は実行中保たれることになる．

- アルゴリズムの停止：まず，L.8 から L.15 のループは，高々 $s$ 回で停止する．そこで，L.4 から L.21 のループが有限回で停止することを示す．もしも $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)$ のうち，$\mathrm{LT}(stock)$ を割り切るものがあるならば，L.11 で $stock$ の全次数が真に減少する．詳しく考えると、$\mathrm{LC}(\frac{\mathrm{LT}(stock)}{\mathrm{LT}(f_i)}f_i) = \mathrm{LC}(stock)$ であり、$\deg(\frac{\mathrm{LT}(stock)}{\mathrm{LT}(f_i)}f_i) = \deg(stock)$ となるので、先頭項が消えるからである。もしもそうでなく，$\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)$ はどれも $\mathrm{LT}(stock)$ を割りきらないならば，L.19 で $stock$ の全次数が真に減少する．よって，L.5 から L.20 の間で全次数は真に減少する．もしも L.4-L.21 のループが永遠に止まらないとすると，変化していく $stock$ で列を作ることで，$\mathbb{Z}^n_{\geq 0}$ の単調減少列が得られる．これは，$>$ が単項式順序であり，整列順序であることに矛盾する．よって，L.4-L.21 のループは停止し，アルゴリズムは停止する．
- $r$ が所定の条件を満たす：$r$ が，L.4 と L.20 の時点で，「$r$ のどの項も $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)$ のどれでも割り切れない」という条件を満たしつつけることを示せば十分である．L.4 の時点では $r = 0$ であり，自明．L.4-L.20 で，変化する前の変数は $\bullet_b$，変化したあとの変数を $\bullet_a$ とする．帰納法で，$r_b$ は条件をみたすとし，$r_a$ も条件をみたすことを示せばよい．もしも $\mathrm{LT}(f_{1b}), \ldots, \mathrm{LT}(f_{sb})$ のうち，$\mathrm{LT}(stock_b)$ を割きるものがあれば，$divisionoccured = \texttt{true}$ となり，L.18 は実行されない．よって，$r_a = r_b$ であり，条件をみたす．そこおで，$\mathrm{LT}(f_{1b}), \ldots, \mathrm{LT}(f_{sb})$ のうち，$\mathrm{LT}(stock_b)$ を割りきるものがないとする．すると，L.18 より，

$$r_a = r_b + \mathrm{LT}(stock_b) \tag{96}$$

となるが，$r_b$ は仮定より条件をみたすし，$\mathrm{LT}(stock_b)$ は割りきることに関する仮定より条件をみたす．よって，$r_a$ は条件をみたす．
よって，常に $r$ のすべての項は $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)$ で割りきれないという条件を満たす．
- $a_1, \ldots, a_s$ が所定の条件を満たす：同様に，L.4 と L.21 で条件を満たしつづけることを示す．L.4 では，$\mathrm{multideg}(a_i) = \mathrm{multideg}(0)$ が定義されないので，条件をみたす．そこで，ループ L.4-L.21 での推移を追う．$\mathrm{LT}(f_i)$ が $\mathrm{LT}(stock_b)$ を割りきらないとき，$a_i$ を更新する L.10 が実行されず，他に $a_i$ が更新される機会はないので，$a_{ia} = a_{ib}$ である．$a_{ib}$ は条件をみたすので，$a_{ia}$ も条件をみたす．そこで，$\mathrm{LT}(f_i)$ が $\mathrm{LT}(stock_b)$ を割りきるとする．
  – $a_{ib} = 0$ のときは，$a_{ia} = \frac{\mathrm{LT}(stock_b)}{\mathrm{LT}(f_i)}$ となる．払って，$a_{ia}\mathrm{LT}(f_i) = \mathrm{LT}(stock_b)$ となる．よって，$\mathrm{multideg}(a_{ia}f_i) = \mathrm{multideg}(stock_b)$ となる．$stock$ の初期値が $f$ で，先にみたように $stock$ の multideg は単調に減少するので，$\mathrm{multideg}(stock_b) \leq \mathrm{multideg}(f)$ である．よって，$\mathrm{multideg}(a_{ia}f_i) \leq \mathrm{multideg}(f)$ となる．

– $a_{ib} \neq 0$ のときは，$\mathrm{multideg}(a_{ib}f_i) \leq \mathrm{multideg}(f)$ が満たされている．さらに，L.10 により，

$$a_{ia} = a_{ib} + \frac{\mathrm{LT}(stock_b)}{\mathrm{LT}(f_i)} \tag{97}$$

である．払って，$\mathrm{LT}(f_i)a_{ia} = a_{ib}\mathrm{LT}(f_i) + \mathrm{LT}(stock_b)$ である．よって，

$$\mathrm{multideg}(a_{ia}f_i) \leq \max(\mathrm{multideg}(a_{ib}f_i), \mathrm{LT}(stock_b)) \tag{98}$$

先と同様に，$\mathrm{multideg}(stock_b) \leq \mathrm{multideg}(f)$ である．これと，$\mathrm{multideg}(a_{ib}f_i) \leq \mathrm{multideg}(f)$ をまとめて，

$$\mathrm{multideg}(a_{ia}f_i) \leq \mathrm{multideg}(f) \tag{99}$$

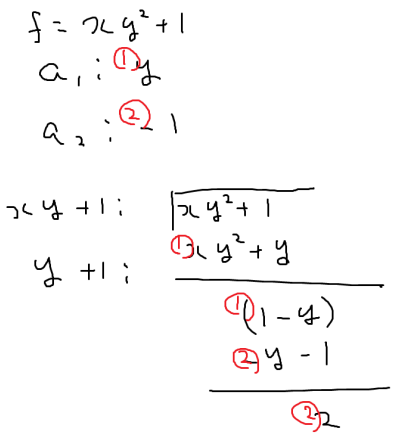
を得る．

(証終)

計算例を示す．

(図 1)`div1.png` 参照．

図 1　`div1.png`

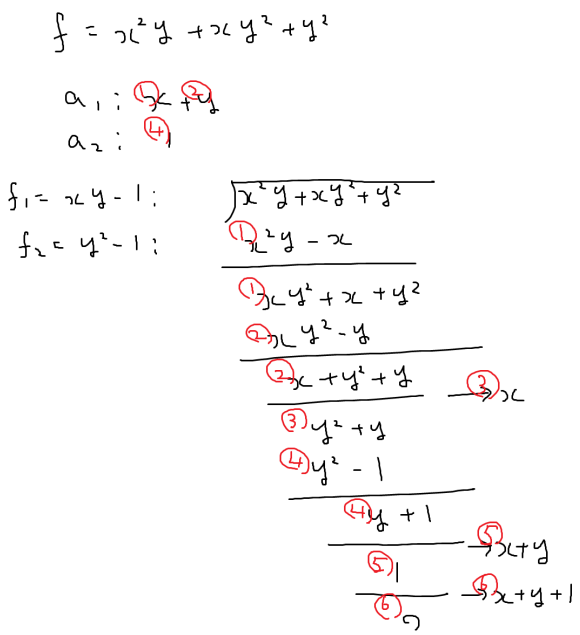



$xy^2 + 1$ を $xy + 1$ と $y + 1$ で割った．

$$xy^2 + 1 = y \cdot (xy + 1) + 1 \cdot (y + 1) + 2. \tag{100}$$

(図 2)`div2.png` 参照．

図 2　div2.png

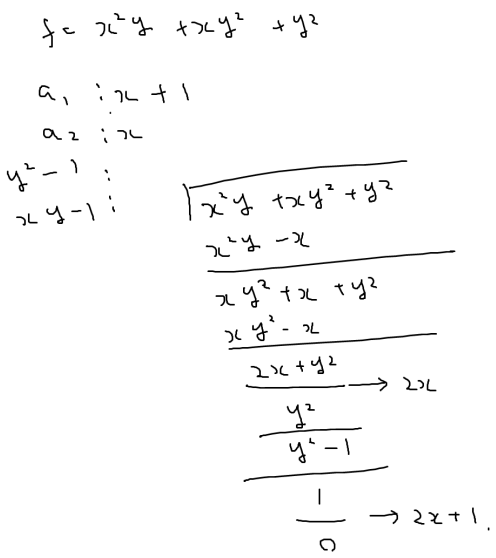



$x^2y + xy^2 + y^2$ を $xy - 1$ と $y^2 - 1$ で割った.

$$x^2y + xy^2 + y^2 = (x + y) \cdot (xy - 1) + 1 \cdot (y^2 - 1) + 0. \tag{101}$$

(図 3)div3.png 参照.

図 3　div3.png

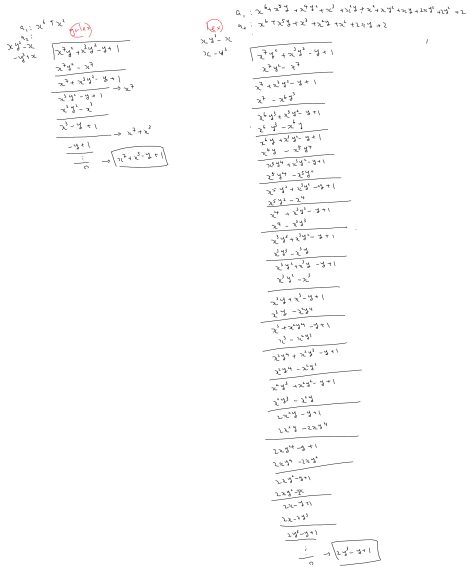


$x - 2y + xy^2 + y^2$ を $y^1 - 1$ と $xy - 1$ で割った．

このように，同じ割り算でも，割る式の順序によって商や余りが異なることがある．このために，イデアルの所属問題の解法で「あまりが 0 ならばよい」という手法は安直には使えない．

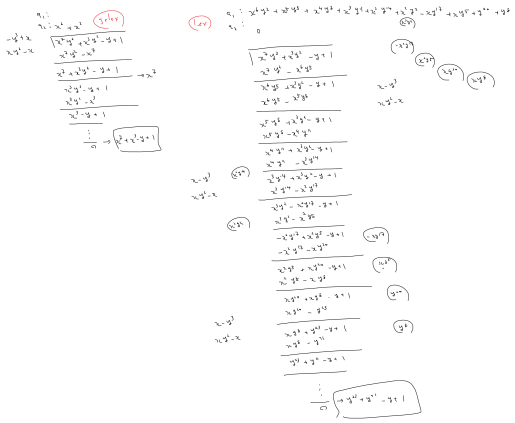
(問題 1)　(a)　(図 4)div3_1a.png 参照．

図 4　div3_1a.png



(b)　(図 5)div3_1b.png 参照．

図 5　div3_1b.png



(問題 2) 何の順序で？

(問題 3) code/ex_2_3_3.hs で計算．出力は以下．

1a,grlex (a) Start: calculates $x^7y^2 + x^3y^2 + (-1)y + 1 \div$

- $xy^2 + (-1)x$,
- $(-1)y^3 + x$,

.

(b) Division: $xy^2 + (-1)x$ divides stock. stock is $x^7 + x^3y^2 + (-1)y + 1$ .

(c) Remainder: $x^7$ moved to remainder.

(d) Division: $xy^2 + (-1)x$ divides stock. stock is $x^3 + (-1)y + 1$ .

(e) Remainder: $x^3$ moved to remainder.

(f) Remainder: $(-1)y$ moved to remainder.

(g) Remainder: 1 moved to remainder.

(h) Completed: quotients are

- $x^6 + x^2$,
- $0$,

. remainder is $x^7 + x^3 + (-1)y + 1$. ■

1a,lex (a) Start: calculates $x^7y^2 + x^3y^2 + (-1)y + 1 \div$

- $xy^2 + (-1)x$,
- $x + (-1)y^3$,

.

(b) Division: $xy^2 + (-1)x$ divides stock. stock is $x^7 + x^3y^2 + (-1)y + 1$ .

(c) Division: $x + (-1)y^3$ divides stock. stock is $x^6y^3 + x^3y^2 + (-1)y + 1$ .

(d) Division: $xy^2 + (-1)x$ divides stock. stock is $x^6y + x^3y^2 + (-1)y + 1$ .

(e) Division: $x + (-1)y^3$ divides stock. stock is $x^5y^4 + x^3y^2 + (-1)y + 1$ .

(f) Division: $xy^2 + (-1)x$ divides stock. stock is $x^5y^2 + x^3y^2 + (-1)y + 1$ .

(g) Division: $xy^2 + (-1)x$ divides stock. stock is $x^5 + x^3y^2 + (-1)y + 1$ .

(h) Division: $x + (-1)y^3$ divides stock. stock is $x^4y^3 + x^3y^2 + (-1)y + 1$ .

(i) Division: $xy^2 + (-1)x$ divides stock. stock is $x^4y + x^3y^2 + (-1)y + 1$ .

(j) Division: $x + (-1)y^3$ divides stock. stock is $x^3y^4 + x^3y^2 + (-1)y + 1$ .

(k) Division: $xy^2 + (-1)x$ divides stock. stock is $2x^3y^2 + (-1)y + 1$ .

(l) Division: $xy^2 + (-1)x$ divides stock. stock is $2x^3 + (-1)y + 1$ .

(m) Division: $x + (-1)y^3$ divides stock. stock is $2x^2y^3 + (-1)y + 1$ .

(n) Division: $xy^2 + (-1)x$ divides stock. stock is $2x^2y + (-1)y + 1$ .

(o) Division: $x + (-1)y^3$ divides stock. stock is $2xy^4 + (-1)y + 1$ .

(p) Division: $xy^2 + (-1)x$ divides stock. stock is $2xy^2 + (-1)y + 1$ .

(q) Division: $xy^2 + (-1)x$ divides stock. stock is $2x + (-1)y + 1$ .

(r) Division: $x + (-1)y^3$ divides stock. stock is $2y^3 + (-1)y + 1$ .

(s) Remainder: $2y^3$ moved to remainder.

(t) Remainder: $(-1)y$ moved to remainder.

(u) Remainder: 1 moved to remainder.

(v) Completed: quotients are

- $x^6 + x^5y + x^4y^2 + x^4 + x^3y + x^2y^2 + 2x^2 + 2xy + 2y^2 + 2$,
- $x^6 + x^5y + x^4 + x^3y + 2x^2 + 2xy + 2$,

. remainder is $2y^3 + (-1)y + 1$. ■

1b,grlex (a) Start: calculates $x^7y^2 + x^3y^2 + (-1)y + 1 \div$

- $(-1)y^3 + x$,
- $xy^2 + (-1)x$,

.

(b) Division: $xy^2 + (-1)x$ divides stock. stock is $x^7 + x^3y^2 + (-1)y + 1$ .

(c) Remainder: $x^7$ moved to remainder.

(d) Division: $xy^2 + (-1)x$ divides stock. stock is $x^3 + (-1)y + 1$ .

(e) Remainder: $x^3$ moved to remainder.

(f) Remainder: $(-1)y$ moved to remainder.

(g) Remainder: 1 moved to remainder.

(h) Completed: quotients are

- 0,
- $x^6 + x^2$,

. remainder is $x^7 + x^3 + (-1)y + 1$. ■

1b,lex (a) Start: calculates $x^7y^2 + x^3y^2 + (-1)y + 1 \div$

- $x + (-1)y^3$,
- $xy^2 + (-1)x$,

.

(b) Division: $x + (-1)y^3$ divides stock. stock is $x^6y^5 + x^3y^2 + (-1)y + 1$ .

(c) Division: $x + (-1)y^3$ divides stock. stock is $x^5y^8 + x^3y^2 + (-1)y + 1$ .

(d) Division: $x + (-1)y^3$ divides stock. stock is $x^4y^{11} + x^3y^2 + (-1)y + 1$ .

(e) Division: $x + (-1)y^3$ divides stock. stock is $x^3y^{14} + x^3y^2 + (-1)y + 1$ .

(f) Division: $x + (-1)y^3$ divides stock. stock is $x^3y^2 + x^2y^{17} + (-1)y + 1$ .

(g) Division: $x + (-1)y^3$ divides stock. stock is $x^2y^{17} + x^2y^5 + (-1)y + 1$ .

(h) Division: $x + (-1)y^3$ divides stock. stock is $x^2y^5 + xy^{20} + (-1)y + 1$ .

(i) Division: $x + (-1)y^3$ divides stock. stock is $xy^{20} + xy^8 + (-1)y + 1$ .

(j) Division: $x + (-1)y^3$ divides stock. stock is $xy^8 + y^{23} + (-1)y + 1$ .

(k) Division: $x + (-1)y^3$ divides stock. stock is $y^{23} + y^{11} + (-1)y + 1$ .

(l) Remainder: $y^{23}$ moved to remainder.

(m) Remainder: $y^{11}$ moved to remainder.

(n) Remainder: $(-1)y$ moved to remainder.

(o) Remainder: 1 moved to remainder.

(p) Completed: quotients are

- $x^6y^2 + x^5y^5 + x^4y^8 + x^3y^{11} + x^2y^{14} + x^2y^2 + xy^{17} + xy^5 + y^{20} + y^8$,
- 0,

. remainder is $y^{23} + y^{11} + (-1)y + 1$. ■

(問題 4) やった．

(問題 5) (a) `ex_2_3_5.hs` で計算．

$$r_1 = x^3 - x^2z + x - z, \tag{102}$$
$$r_2 = x^3 - x^2z. \tag{103}$$

である．はじめに $x^3$ を余りに出すところまではあっているが，残りの $-x^2y - x^2z + x$ はどちらでも割れるので，は割る順序が変わってくる．

(b) $r = r_1 - r_2 = x - z$ である．$r = (-x) \cdot f_2 + 1 \cdot f_1$．

(c) 割り算の定義により，$r_1, r_2$ の項はどれも $f_1, f_2$ のどちらでも割れないことが保証されている．よって，それらの項を足した $r$ も，$f_1, f_2$ のどちらでも割れず，$r \div (f_1, f_2)$ のあまりは $r$ そのものである．

(d)

$$y \cdot f_1 - (xy + 1) \cdot f_2 = 1 - yz. \tag{104}$$

これは $f_1, f_2$ のどちらでも割れず，あきらかに $(f_1, f_2)$ で割ったあまりは 0 でない．

(e) 与えない．上は (d) は，その構成より $\langle f_1, f_2 \rangle$ の元だが，$(f_1, f_2)$，あるいは $(f_2, f_1)$ で割った余りは 0 でない．

(問題 6)

$$g = 3x(2xy^2 - x) - 2y(3x^2y - y - 1) = -3x^2 - 2y^2 - 2y \tag{105}$$

であり，これは $f_1, f_2$ で割ることができないので，余りは 0 でない．

(問題 7)

$$y^2 \cdot f_1 - xy \cdot f_2 = (x^4y^4 - y^2z) - (x^4y^4 - xy) = xy - y^2z = -y^2z + xy \tag{106}$$
$$xy \cdot f_2 - x^2 \cdot f_3, = (x^4y^4 - xy) - (x^4y^4 - 2x^2z) = 2x^2z - xy. \tag{107}$$

次数より，もう割れないことは分かる．

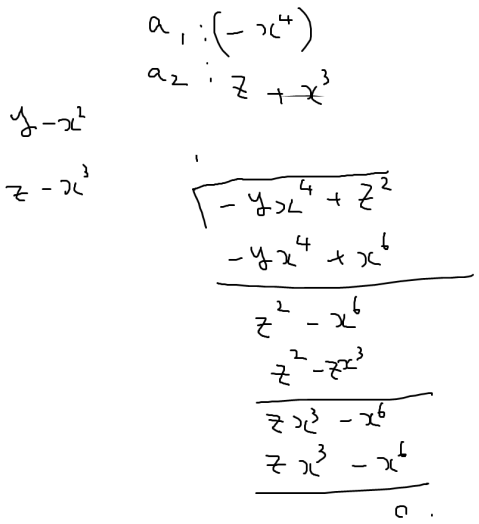
(問題 8) $\mathrm{LT}(g)$ が $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)$ のどれでも割りきれないとき，割り算のあまりは 0 にならないことが保証される．しかし，その $g$ がイデアルに所属することもあるので，余りが 0 かどうかでイデアルの所属を判定することはできない．

(問題 9) (a) $y \geq_{lex} z \geq_{lex} x$ という lex 順序で $f$ を割ることにより余りが $x$ の 1 次以下の式となる．

(b) $x = t, y = t^2, z = t^3$ であった．$z^2 - x^4y = (t^3)^2 - t^4t^2 = 0$．

(c) (図 6)`div3_2_9.png` 参照．

図 6　div3_2_9.png



$$(-x^4)(y-x^2)+(z+x^3)(z-x^3)=-yx^4+z^2=z^2-x^4y. \tag{108}$$

(問題 10) (a) $\{(t,t^m,t^n)\}=\mathbf{V}(y-x^m,z-x^n)$.

(b) $f\in\mathbb{R}^3[x,y,z]$ を $\mathbf{V}(y-x^m,z-x^n)$ を消す多項式とする．$f$ を $y-x^m,z-x^n$ で，$y>_{lex}z>_{lex}x$ という lex 順序で割ることにより，

$$f=h_1\cdot(y-x^m)+h_2\cdot(z-x^n)+h_3 \tag{109}$$

となる $h_1,h_2\in\mathbb{R}^3[x,y,z]$ と $h_3\in\mathbb{R}^3[x]$ が存在することがわかる．$f$ は $\mathbf{V}(y^x-m,z-x^n)=\{(t,t^m,t^n)\}$ を消さなければならないので，任意の $t$ について

$$0=f(t,t^m,t^n)=h_3(t). \tag{110}$$

となる．$t$ は任意であり，無限体上の議論なので，$h_3$ は多項式として 0 である．よって，

$$f=h_1\cdot(y-x^m)+h_2\cdot(z-x^n) \tag{111}$$

であり，$f\in\langle y-x^m,z-x^n\rangle$ となる．よって，$\mathbf{V}(y-x^m,z-x^n)\subset\langle y-x^m,z-x^n\rangle$．逆はあきらか．

(問題 11) (a)

- $\beta\in\Delta_i$ とする．$\beta\in\Delta_i\subset\alpha(1)+\mathbb{Z}^n_{\geq 0}$ となる．よって，$\beta-\alpha(i)\in\mathbb{Z}^n_{\geq 0}$ となり，$x^{\alpha(i)}|x^\beta$ である．次に，$j<i$ とする．$x^{\alpha(j)}|x^\beta$ とする．$\beta-\alpha(j)\in\mathbb{Z}^n_{\geq 0}$ となる．よって，$\beta\in\alpha(j)+\mathbb{Z}^n_{\geq 0}$ となる．よって，対偶を考え，$\beta\in\Delta_i$ から $\beta\notin\alpha(j)+\mathbb{Z}^n_{\geq 0}$ となり，$x^{\alpha(j)}$ は $x^\beta$ を割り切らない．
- $x^{\alpha(i)}$ は $x^\beta$ を割り切り，かつ $j<i$ について $x^{\alpha(j)}$ は $x^\beta$ ど割り切らないとする．$x^{\alpha(i)}$ は $x^\beta$ を割り切るので，$\beta\in\alpha(i)+\mathbb{Z}^n_{\geq 0}$ である．また，$x^{\alpha(j)}$ は $x^\beta$ を割り切らないので，$\beta\notin\alpha(j)+\mathbb{Z}^n_{\geq 0}$ となる．以上をまとめて，$\beta\in(\alpha(i)+\mathbb{Z}^n_{\geq 0})\setminus(\alpha(j)+\mathbb{Z}^n_{\geq 0})\subset\Delta_i$ である．($i=1$ のときは，何も引かないと解釈する．)

(b) 対偶を示す．何か $i$ があって，$x^{\alpha(i)}$ が $x^\gamma$ をわりきるとする．このとき，$\gamma\in\alpha(i)+\mathbb{Z}^n_{\geq 0}$ となり，$\gamma\in\alpha(i)+\mathbb{Z}^n_{\geq 0}$

である．定義より，

$$\Delta_1 = \alpha(1) + \mathbb{Z}^n_{\geq 0} \tag{112}$$
$$\Delta_1 \cup \Delta_2 = \Delta_1 \cup (\alpha(2) + \mathbb{Z}^n_{\geq 0}) \setminus \Delta_1 = (\alpha(1) + \mathbb{Z}^n_{\geq 0}) \cup (\alpha(2) + \mathbb{Z}^n_{\geq 0}) \tag{113}$$
$$\vdots \tag{114}$$
$$\Delta_1 \cup \ldots \cup \Delta_n = (\alpha(1) + \mathbb{Z}^n_{\geq 0}) \cup \ldots \cup (\alpha(n) + \mathbb{Z}^n_{\geq 0}) \tag{115}$$

である．よって，$\gamma \in \Delta_1 \cup \ldots \cup \Delta_n$ となる．よって，$\gamma \notin \overline{\Delta}$ となる．

(c) アルゴリズムより，$a_i$ の項を $cx^\beta$ とする．ある $stock$ があって，$x^\beta = \frac{\mathrm{LT}(stock)}{\mathrm{LT}(f_i)}$ となる．アルゴリズムより，この $stock$ は，$\mathrm{LT}(f_i)$ が $\mathrm{LT}(stock)$ を割りきり，$\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_{i-1})$ が $\mathrm{LT}(stock)$ を割りきらないことが保証されている．よって，$\beta = \mathrm{multideg}(stock) - \alpha(i) = \mathrm{multideg}(stock) - \mathrm{multideg}(f_i) \in \mathbb{Z}^n_{\geq 0}$ である．よって，$\beta + \alpha(i) \in \alpha(i) + \mathbb{Z}^n_{\geq 0}$ である．
次に，$j < i$ とする．$\beta + \alpha(i) \in \alpha(j) + \mathbb{Z}^n_{\geq 0}$ と仮定する．このとき，$\beta = \mathrm{multideg}(stock) - \alpha(i)$ なので，$\mathrm{multideg}(stock) \in \alpha(j) + \mathbb{Z}^n_{\geq 0}$ である．よって，$\alpha(j)$ が $\mathrm{LT}(stock)$ を割り切る．これはすなわち，$\mathrm{LT}(f_j) = x^{\alpha(j)} | \mathrm{LT}(stock)$ となるが，これは $stock$ の条件に矛盾する．よって，$\beta + \alpha(i) \notin \alpha(j) + \mathbb{Z}^n_{\geq 0}$ である．
以上のことより，$\beta + \alpha(i) \in \Delta_i$ となる．
$r$ のすべての項 $cx^\gamma$ は，アルゴリズムより $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)$ のすべてで割り切れないことが保証されているから，$\gamma \in \overline{\Delta}$ である．

(d) 存在はアルゴリズムの存在が示している．一意性を示せばよい．$a_1 f_1 + \cdots + a_s f_s + r = 0$ のときに，$a_1 = a_2 = \cdots = a_s = r = 0$ を示せばよい．仮に $a_i \neq 0$ であるとし，$x^\beta$ を $a_i$ のなかの単項式とする．仮に $a_1 = a_2 = \cdots = a_s = r = 0$ ではないとする．このとき，$a_1 f_1 + \cdots + a_s f_s + r$ の最高次の単項式は，$\mathrm{LM}(a_1)\mathrm{LM}(f_1), \ldots, \mathrm{LM}(a_s)\mathrm{LM}(f_s), \mathrm{LM}(r)$ のいずれかになる．この最高次の単項式を $x^\beta$ としておく．よって，この $a_1 f_1 + \cdots + a_s f_s + r = 0$ という仮定を満足するためには，$x^\beta$ の係数が 0 にならねばならず，よって，$\mathrm{LM}(a_1)\mathrm{LM}(f_1), \ldots, \mathrm{LM}(a_s)\mathrm{LM}(f_s), \mathrm{LM}(r)$ の $k$ 係数 1 次結合が 0 にならなければならない．しかし，$\mathrm{LM}(a_1)\mathrm{LM}(f_1) \in \Delta_1, \ldots, \mathrm{LM}(a_s)\mathrm{LM}(f_s) \in \Delta_s, \mathrm{LM}(r) \in \overline{\Delta}$ となっており，(c) からこれらの集合が互いに素であることがわかっているから，$\mathrm{LM}(a_1)\mathrm{LM}(f_1), \ldots, \mathrm{LM}(a_s)\mathrm{LM}(f_s), \mathrm{LM}(r)$ はそれぞれ異なる単項式であることがわかり，1 次結合を 0 にするには，係数すべてを 0 にするしかない．$\mathrm{LC}(f_1), \ldots, \mathrm{LC}(f_s)$ はどれも 0 ではないので，$\mathrm{LC}(a_1), \ldots, \mathrm{LC}(a_s), \mathrm{LC}(r)$ のすべてが 0 とならなければならない．これは，$a_1, \ldots, a_s, r_0 = 0$ を意味するが，背理法の仮定に矛盾する．

(問題 12) $g_1, g_2$ に対する割り算の適用結果をそれぞれ

$$g_1 = a_1 f_1 + \cdots + a_s f_s + r \tag{116}$$
$$g_2 = b_1 f_1 + \cdots + b_s f_s + r' \tag{117}$$

とする．このとき，

$$c_1 g_1 + c_2 g_2 = (c_1 a_1 + c_2 b_1) f_1 + \cdots + (c_1 a_s + c_2 b_s) f_s + (c_1 r + c_2 r') \tag{118}$$

も，「$(g_1, g_2)$ で割り算した結果」の条件を満たしている．すなわち，$c_1 a_i + c_2 b_i \in \Delta_i$ であり，$c_1 r + c_2 r \in \overline{\Delta}$ となっている．一意性より，実際に $c_1 r + c_2 r'$ が余りとなる．

## 2.4 単項式イデアルとディクソンの補題

イデアルのうち，(係数 1 の) 単項式だけを基底 a として持つものを単項式イデアルという．
$I = \langle x^\alpha | \alpha \in A \rangle$ が単項式イデアルのとき，$x^\beta \in I \iff {}^\exists \alpha \in A \colon x^\alpha | x^\beta$.

証明

- $\Rightarrow$ : $x^\beta = \sum_{i=1}^s h_i x^{\alpha(i)}$ となる $h_i \in k[x_1, \ldots, x_s]$ と $\alpha(i) \in \mathbb{Z}^n_{\geq 0}$ が存在する．右辺は，「単項式はすべて，なんらかの $x^{\alpha(i)}$ で割り切れる」という性質を持つので，これと等しい右辺も同様の性質を持ち，$x^\beta$ もなんらかの $x^{\alpha(i)}$ で割り切れる．

- $\Leftarrow$：自明．

(証終)

$x^\alpha|x^\beta$ は，$\beta \in \alpha + \mathbb{Z}^n_{\geq 0}$ と等価なので，単項式イデアルへある単項式が所属するかどうかは，その単項式イデアルの基底 $\alpha$ について，$\alpha + \mathbb{Z}^n_{\geq 0}$ に属するかということを逐一調べ，1 つでも属する基底があれば属する，ないならば属さないという正確な判定条件が得られる．これを $\mathbb{Z}^n_{\geq 0}$ で図示すると，$\alpha$ から $\infty$ の向きに無限の長方形が作られているように見える．基底が複数個あるなら，これらの和集合として見える．

次は等価である．$I$ は単項式イデアルとする．

(1) $f \in I$．
(2) $f$ の各項は $I$ に属する．
(3) $f$ は $I$ の単項式[*5]の $k$ 係数 1 次結合である．

証明
(3) $\Longrightarrow$ (2) $\Longrightarrow$ (1) は自明．(1) を仮定する．$f \in I$ とすると．

$$f = h_1 x^{\alpha(1)} + \cdots + h_s x^{\alpha(s)} \tag{119}$$

となる $I$ の基底 $\alpha(1), \ldots, \alpha(s)$ と，$k[x_1, \ldots, x_n]$ の元 $h_1, \ldots, h_s$ が存在する．右辺の $h_i x^{\alpha(i)}$ は展開するとすべて $x^{\alpha(i)}$ の倍多項式であり、かつ単項式なので、(3) が満たされる。真面目に書くと、$f = \sum_{i=1}^{s} h_i x^{\alpha(i)}$ となっている。各 $h_\bullet$ について、$h_i = \sum_{j=1}^{N(i)} c_{ij} x^{\beta(i,j)}$ となる $N(i), c_{i\bullet}, \beta(i, \bullet)$ が存在する。すると、$f = \sum_{i=1}^{s} \sum_{j=1}^{N(i)} c_{ij} x^{\beta(i,j)+\alpha(i)}$ となる。これで (3) がみたされていることがわかった。

(証終)

単項式イデアル $I, I'$ があり，$\{I\text{の単項式}\} = \{I'\text{の単項式}\}$ が成立していたとする．このとき，

$$f \in I \overset{\boxed{\text{上の (2)}}}{\Longleftrightarrow} \{f\text{のすべての単項式}\} \subset I \overset{\boxed{\text{単項式の一致}}}{\Longleftrightarrow} \{f\text{のすべての項}\} \subset I' \overset{\boxed{\text{上の (2)}}}{\Longleftrightarrow} f \in I'. \tag{120}$$

となる．よって，$I = I'$ となる．つまり，単項式イデアルは，そこに含まれる単項式で定まり，それのみで定まる．[*6]

ディクソンの補題を示す．$k[x_1, \ldots, x_n]$ で考える．単項式イデアル $I = \langle x^\alpha | \alpha \in A \rangle$ について，$\alpha(1), \ldots, \alpha(s) \in A$ が存在して，$I = \left\langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \right\rangle$ となる．

証明
$n = 1$ のとき，単項式順序の性質より，$\{x^\alpha | \alpha \in A\}$ には最小の元がある．この最小元を $x^{\alpha'}$ とする．今は 1 変数多項式で考えているので，$I = \left\langle x^{\alpha'} \right\rangle$ となる．

以降，$n > 1$ とする．$n - 1$ 以下で成立していると仮定し，$n$ での成立を示す．多項式は $k[x_1, \ldots, x_n]$ で考えるが，$x_n$ のことを $y$ ともよぶことにする．

$$J = \left\langle x^\alpha | x^\alpha y^\beta \in I \right\rangle \subset k[x_1, \ldots, x_{n-1}] \tag{121}$$

とする．すなわち，$I$ の単項式の $k[x_1, \ldots, x_{n-1}]$ への射影のなすイデアルである．$J$ は $k[x_1, \ldots, x_{n-1}]$．なので，帰納法の仮定より，$J = \left\langle x^{\alpha(1)}, \ldots, x^{\alpha(j)} \right\rangle$ となる $\alpha(1), \ldots, \alpha(j) \in \mathbb{Z}^{n-1}_{\geq 0}$ が存在する．$J$ の定義により，$i = 1, \ldots, j$ について，

$$x^{\alpha(i)} y^{\beta(i)} \in I \tag{122}$$

となる $\beta(i) \in \mathbb{Z}_{\geq 0}$ が存在する．このような $\beta(i)$ のうち最小のものを，$\gamma(i)$ とよぶことにする．そして，

$$\gamma = \max(\gamma(1), \ldots, \gamma(j)) \tag{123}$$

---

[*5] 基底ではない!

[*6] 単なるイデアルでは，単項式が同じなのに異なるということがあるか？ $k[x]$ 上で，$\langle 1 \rangle$ と $\langle x \rangle$ は含まれる単項式は同じだが，$\langle 1 \rangle$ のほうが真に広い．← 1 も単項式だし何を言っているのかよくわからない。

とする．このように定義しておくと，$y^\gamma$ 以上を $J$ の元にかけることで，$I$ に属することを保証できるからである．イデアルの図で言うところの、一番上の長方形が表現できたことになる。$x^{\alpha(\bullet)}y^\gamma$ たちは一番上の長方形を表現するのに足る「角」の情報を持っている (あとで示すが)。

$0 \leq \delta < \gamma$ とする．

$$J_\delta = \left\langle x^\alpha | x^\alpha y^\delta \in I \right\rangle \subset k[x_1, \ldots, x_{n-1}] \tag{124}$$

とする．つまり，$y$ の次数が $\delta$ であるような $I$ の単項式の $k[x_1, \ldots, x_{n-1}]$ への射影をなすイデアルである．これは $k[x_1, \ldots, x_{n-1}]$ のイデアルなので，帰納法の仮定より，

$$J_\delta = \left\langle x^{\alpha(\delta;1)}, \ldots, x^{\alpha(\delta;j_\delta)} \right\rangle \tag{125}$$

となる $\alpha(\delta;1), \ldots, \alpha(\delta;j_\delta) \in \mathbb{Z}_{\geq 0}^{n-1}$ が存在する．これで、高さ $\delta$ での必要な「角」の情報が得られたことになる。

これらを集めて，

$$I = \langle x^{\alpha(1)}y^\gamma, \ldots, x^{\alpha(j)}y^\gamma \tag{126}$$

$$x^{\alpha(\gamma-1;1)}, \ldots, x^{\alpha(\gamma-1;j_{\gamma-1})} \tag{127}$$

$$\vdots \tag{128}$$

$$x^{\alpha(0;1)}, \ldots, x^{\alpha(0;j_0)} \rangle \tag{129}$$

となっていることを示そう。$\supset$ は自明なので、$\subset$ を考える。$I$ の単項式が右辺に属することを言えば十分であり、つまり $I$ の単項式が右辺の基底のどれかで割り切れることを言えば十分である。$x^\xi y^\eta \in I$ とし、$x^\xi y^\eta$ が右辺の基底のどれかで割り切れることを示す。

- $\eta \geq \gamma$ のとき: $J$ の定義より、$x^\xi \in J$ である。$J$ に対する考察より、$x^{\alpha(i)} | x^\xi$ となる $i = 1, \ldots, j$ が存在する。さらに、$x^{\alpha(i)}y^\gamma \in I$ となるように $\gamma$ を定義したのだった。$\eta \geq \gamma$ なので、$y^\gamma | y^\eta$ である。よって、$x^{\alpha(i)}y^\gamma | x^\xi y^\eta$ である。$x^{\alpha(i)}y^\gamma$ は基底の 1 つであった。
- $\eta < \gamma$ のとき: $J_\eta$ の定義より、$x^\xi \in J_\eta$ である。$J_\eta$ に対する考察より、$x^{\alpha(\gamma,i)} | x^\xi$ となる $i = 1, \ldots, j_\gamma$ が存在する。よって、$x^{\alpha(\gamma,i)}y^\eta | x^\xi y^\eta$ となる。$x^{\alpha(\gamma,i)}$ は基底の 1 つであった。

よって，$I$ を，$I$ の元の有限生成単項式イデアルとして書くことができた．これで帰納法を終わる．

次に，$I$ の単項式の有限生成である $I$ を，$A$ を多重指数に持つ単項式の有限生成に書き直そう．

$$I = \left\langle x^{\beta(1)}, \ldots, x^{\beta(s)} \right\rangle \tag{130}$$

と，$\beta(1), \ldots, \beta(s) \in \mathbb{Z}_{\geq 0}^n$ が存在して書けることは上の段落で示した．$x^{\beta(\bullet)} \in I = \langle x^\alpha | \alpha \in A \rangle$ となっているので、この節のはじめの「単項式が単項式イデアルに属するとき」の性質より、$x^{\beta(\bullet)}$ は $x^\alpha$ のいずれかで割り切れ、

$$I = \left\langle x^{\alpha(1)+\gamma(1)}, \ldots, x^{\alpha(s)+\gamma(s)} \right\rangle \tag{131}$$

となる $\alpha(\bullet)A$ と、$\gamma(\bullet) \in \mathbb{Z}_{\geq 0}^n$ とが存在する．(この時点ではまだ「$A$ の」指数で書けているかは分からない。$x^{\gamma(\bullet)}$ がかかっている。)$\alpha(1) < \alpha(2) < \ldots$ として一般性を失なわない (何の順序でも良い．)．また，$I$ はどの「1 つの基底を取り除くと $I$ でなくなる」という仮定を置いてよい．なぜなら，もしも取り除いても影響がない基底があるならば，$I = \left\langle x^{\beta(1)}, \ldots, x^{\beta(s)} \right\rangle$ と書いた時点でそのようなものを取り除いても良いからである．$x^{\alpha(1)} \in I$ なので，$x^{\alpha(1)} \in \left\langle x^{\alpha(1)+\gamma(1)}, \ldots, x^{\alpha(s)+\gamma(s)} \right\rangle$．単項式イデアルの性質により，何らかの $i$ について，$\alpha(1) \in \alpha(i) + \gamma(i) + \mathbb{Z}_{\geq 0}^n$ となる．つまり，何らかの $\delta(i) \in \mathbb{Z}_{\geq 0}^n$ が存在して，$\alpha(1) = \alpha(i) + \gamma(i) + \delta(i)$ となる．$i \geq 2$ ならば $\alpha(i) > \alpha(1) = \alpha(i) + \gamma(i) + \delta(i)$ となり，単項式順序の性質より矛盾が導かれる．よって，$i = 1$ となるしかない．このとき，$\alpha(1) = \alpha(1) + \gamma(1) + \delta(1)$ となり，$\gamma(1) = \delta(1) = 0$ となるしかない．よって，$\gamma(1) = 0$ がわかった．$I = \left\langle x^{\alpha(1)}, x^{\alpha(2)+\delta(2)}, \ldots, x^{\alpha(s)} + \gamma(s) \right\rangle$ である．$x^{\alpha(2)} \in I$ なので，$x^{\alpha(2)} \in \left\langle x^{\alpha(1)}, x^{\alpha(2)+\gamma(2)}, \ldots, x^{\alpha(s)+\gamma(s)} \right\rangle$ となる．よって，何らかの $i$ について，$\alpha(2) \in \alpha(i)+\gamma(i)+\mathbb{Z}_{\geq 0}^n$ となる．よって，$\alpha(2) = \alpha(i)+\gamma(i)+\delta(i)$ となる $\delta(i) \in \mathbb{Z}_{\geq 0}^n$ が存在する．$i = 1$ ならば，$\alpha(2) = \alpha(1) + \gamma(1) + \delta(1) = \alpha(1) + \delta(1)$ となる．これは，$x^{\alpha(1)} | x^{\alpha(2)} | x^{\alpha(2)+\gamma(2)}$ を意味

し，$x^{\alpha(2)+\gamma(2)}$ を取り除いても $x^{\alpha(1)}$ の倍数として表現できるために $I$ でありつづけるということになり，「1 つの基底を取り除くと $I$ でなくなる」の仮定に反する．よって，$i \neq 1$ であり，$i \geq 2$ である．$i \geq 3$ であったときには，先と同様に $\alpha(i) > \alpha(2) > \alpha(i) + \gamma(i) + \delta(i)$ という矛盾が生じる．よって，$i = 2$ であり，$\gamma(2) = \delta(2) = 0$ である．以降同様に繰替えし，$\gamma(1) = \gamma(2) = \cdots = \gamma(s)$ を得て，

$$I = \left\langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \right\rangle \tag{132}$$

を得る．

(証終)

このディクソンの補題の応用について述べる．まず，単項式イデアルについては，イデアルの所属問題を完全に解くことができる．すなわち：$I \subset k[x_1, \ldots, x_n]$ を単項式イデアルとし，$f \in k[x_1, \ldots, x_n]$ を一般の多項式とすると，ディクソンの補題により $I = \left\langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \right\rangle$ と書くと，

$$f \in I \iff f\text{を}(x^{\alpha(1)}, \ldots, x^{\alpha(s)})\text{で割ったあまりは}0. \tag{133}$$

証明

$$f \in I \iff f \in \left\langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \right\rangle \tag{134}$$

$$\overset{\boxed{\text{補題}}}{\iff} f\text{は}x^{\alpha(1)}, \ldots, x^{\alpha(s)}\text{の}k[x_1, \ldots, x_n]\text{係数1次結合で書ける} \tag{135}$$

$$\iff f\text{を}(x^{\alpha(1)}, \ldots, x^{\alpha(s)})\text{で割ったあまりは}0. \tag{136}$$

(証終)

また，ディクソンの補題を使って単項式順序であることを確認するのを楽にすることができる．すなわち：$\mathbb{Z}^n_{\geq 0}$ の順序 $>$ が「全順序である」「かけ算で保つ」を満たすとする．このとき，

$$> \text{は整列順序} \iff {}^{\forall}\alpha \in \mathbb{Z}^n_{\geq 0} \colon \alpha \geq 0. \tag{137}$$

証明

- $\Rightarrow$：$\mathbb{Z}^n_{\geq 0}$ の部分集合として $\mathbb{Z}^n_{\geq 0}$ そのものをとる．$>$ は整列順序なので，$\mathbb{Z}^n_{\geq 0}$ に $>$ の最小元が存在する．それを $\alpha$ とよぶ．仮に $\alpha < 0$ であるとする (背理法)．「かけ算を保つ」より，$2\alpha < \alpha$ となり，$\alpha$ より真に小さい元が存在することになるが，これは矛盾である．よって，$\alpha \geq 0$ である．任意の $\beta \in \mathbb{Z}^n_{\geq 0}$ について，$\beta \geq \alpha \geq 0$ なので，示された．
- $\Leftarrow$：$\emptyset \neq A \subset \mathbb{Z}^n_{\geq 0}$ とする．$A$ に最小元があることを示そう．$A$ で生成される単項式イデアル $I$ を考える．ディクソンの補題により，$I = \left\langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \right\rangle$ となる $\alpha(1), \ldots, \alpha(s) \in A$ が存在する．$>$ は「全順序である」から，一般性を失なわず，$\alpha(1) < \cdots < \alpha(s)$ としてよい．$\beta \in A$ とする．$x^\beta \in I = \left\langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \right\rangle$ なので，単項式イデアルの性質より，$x^\beta$ は $x^{\alpha(1)}, \ldots, x^{\alpha(s)}$ のうちで割り切られる．それを $x^{\alpha(j)}$ とする．よって，$\beta = \alpha(j) + \gamma$ となる $\gamma \in \mathbb{Z}^n_{\geq 0}$ が存在する．仮定より，$\gamma \geq 0$ であり，「かけ算で保つ」より，$\alpha(j) + \gamma \geq \alpha(j)$ である．よって，

  $$\beta = \alpha(j) + \gamma \geq \alpha(j) > \text{仮定}\alpha(1) \tag{138}$$

  である．よって，$\alpha(1)$ が $A$ の最小元である．

(証終)

(問題 1) $I$ を，「$f \in I$ ならば $f$ の各単項式も $\in I$ となる」を満たすイデアルとする．$I'$ を，$I$ の単項式すべてが生成するイデアルとする．$I'$ は単項式イデアルである．$I = I'$ を示そう．$I' \subset I$ は自明．$f \in I$ とする．

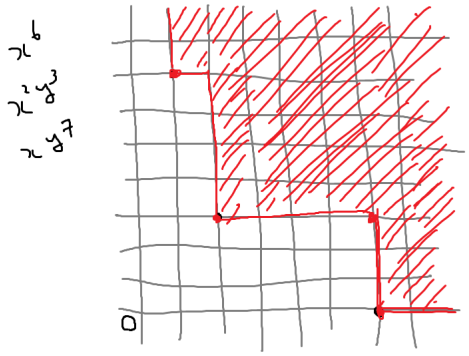
$$f = h_1 x^{\alpha(1)} + \cdots + h_s x^{\alpha(s)} \tag{139}$$

となる $h_1, \ldots, h_s \in k[x_1, \ldots, x_n]$ と $\alpha(1), \ldots, \alpha(s) \in \mathbb{Z}^n_{\geq 0}$ が存在する．$I$ に関する条件より，$x^{\alpha(1)}, \ldots, x^{\alpha(s)} \in I$ であり，$I'$ の構成より $x^{\alpha(1)}, \ldots, x^{\alpha(s)} \in I'$ である．よって，これらの $k[x_1, \ldots, x_s]$ 係数 1 次結合である $f$ も $f \in I'$ となる．$I \subset I'$ である．

(問題 2) やった．

(問題 3) (a) (図 7)ex_2_4_3.png 参照．

図 7　ex_2_4_3.png



(b) $x >_{lex} y$ を採用するなら，$x$ の 1 次項があるので，余りは $y$ の式になる．

(問題 4) (a) まず $I$ の $k[x]$ への射影 $J$ を求めると，これは $J = \langle x^3 \rangle$．$x^3y^b \in I$ となる最小の $b$ は $b = 6$ であり，これ以外に $J$ の生成元がないので，高さ 6 のスライスを考える．

$$J_0 = \langle x^6 \rangle , \tag{140}$$
$$J_1 = \langle x^6 \rangle , \tag{141}$$
$$J_2 = \langle x^6 \rangle , \tag{142}$$
$$J_3 = \langle x^6 \rangle , \tag{143}$$
$$J_4 = \langle x^5 \rangle , \tag{144}$$
$$J_5 = \langle x^5 \rangle . \tag{145}$$
$$\tag{146}$$

よって，

$$I = \langle x^3y^6, x^5y^5, x^5y^4, x^6y^3, x^6y^2, x^6y, x^6 \rangle . \tag{147}$$

(b) 取り除けて，

$$I = \langle x^3y^6, x^5y^4, x^6 \rangle . \tag{148}$$

このうちのどれを除いても真に縮んで，角のものが入らなくなってしまう．

(問題 5) $S$ の最小元を $\alpha$ とし，$\alpha \notin A$ であるとする．$x^\alpha \in I$ ではあるので，単項式イデアルの性質より，$\alpha \in \beta + \mathbb{Z}^n_{\geq 0}$ となる $\beta \in A$ が存在する．$\alpha$ は $A$ の最小元だったので，$\alpha < \beta$ である．よって，$\gamma \in \mathbb{Z}^n_{\geq 0}$ が存在して，$\alpha = \beta + \gamma$ となる．$\alpha < \beta$ に代入して，$\beta + \gamma < \beta$ である．すると，$\beta > \beta + \gamma > \beta + 2\gamma > \beta + 3\gamma + \ldots$ という無限減少列が得られる．これは，$>$ が単項式順序であることに矛盾する．

(問題 6) これが切っ掛けで証明を直した．上のディクソンを参照．「無駄がない」を使った．

(問題 7)「有限個の $a_1, \ldots, a_s \in A$ が存在して〜」は 0 個も許すのかよくわからなくなったが，「$A$ の部分集合で，要素数が有限なものが存在して〜」と解釈すれば OK ということにする．

$$\text{ディクソンの補題} \iff {}^{\forall}A \subset \mathbb{Z}^n_{\geq 0}\colon {}^{\exists}\alpha_1, \ldots, \alpha_s \in A\colon \langle x^{\alpha} | \alpha \in A \rangle = \langle x^{\alpha_1}, \ldots, x^{\alpha_s} \rangle \tag{149}$$

$$\iff {}^{\forall}A \subset \mathbb{Z}^n_{\geq 0}\colon {}^{\exists}\alpha_1, \ldots, \alpha_s \in A\colon \langle x^{\alpha} | \alpha \in A \rangle \subset \langle x^{\alpha_1}, \ldots, x^{\alpha_s} \rangle \tag{150}$$

$$\iff {}^{\forall}A \subset \mathbb{Z}^n_{\geq 0}\colon {}^{\exists}\alpha_1, \ldots, \alpha_s \in A\colon {}^{\forall}\alpha \in A\colon x^{\alpha} \in \langle x^{\alpha_1}, \ldots, x^{\alpha_s} \rangle \tag{151}$$

$$\iff {}^{\forall}A \subset \mathbb{Z}^n_{\geq 0}\colon {}^{\exists}\alpha_1, \ldots, \alpha_s \in A\colon {}^{\forall}\alpha \in A\colon {}^{\exists}i = 1, \ldots, s\colon \alpha \in \alpha_i + \mathbb{Z}^n_{\geq 0} \tag{152}$$

$$\iff {}^{\forall}A \subset \mathbb{Z}^n_{\geq 0}\colon {}^{\exists}\alpha_1, \ldots, \alpha_s \in A\colon {}^{\forall}\alpha \in A\colon {}^{\exists}i = 1, \ldots, s\colon {}^{\exists}\gamma \in \mathbb{Z}^n_{\geq 0}\colon \alpha = \alpha_i + \gamma. \tag{153}$$

---

(問題 8) (a)

```
1: basis := (α(1), ..., α(s))
2: divided := true
3: while divided = true do
4:    divided := false
5:    i := 1
6:    while i ≤ #basis かつ divided = false do
7:       j := 1
8:       while j ≤ #basis かつ divided = false do
9:          if i ≠ j かつ x^{basis[i]} | x^{basis[j]} then
10:            basis から j 番目を除去する.
11:            divided ⇐ true
12:         end if
13:      end while
14:      j ⇐ j + 1
15:   end while
16:   i ⇐ i + 1
17: end while
```

というアルゴリズムにより得られる.

(b) ディクソンの補題と上のアルゴリズムより，$I$ の極小基底 $\alpha_1, \ldots, \alpha_s$ が得られる．$I$ の極小基底 $S$ を考える．$I = \langle x^{\beta} | \beta \in S \rangle$, $S = \{\beta_1, \ldots, \beta_t\}$ となっている． $\alpha_1, \ldots, \alpha_s \in S$ となることを示そう．仮に，$\alpha_i \notin S$ であったとする．しかし，$x^{\alpha_i} \in I = \langle \beta_1, \ldots, \beta_t \rangle$ でなくてはならない．よって，単項式イデアルの性質より何か $j = 1, \ldots, t$ が存在して，$\alpha_i \in \beta_j + \mathbb{Z}^n_{\geq 0}$ とならなければならない．よって，$\alpha_i = \beta_j + \gamma$ となる $\gamma \in \mathbb{Z}^n_{\geq 0}$ が存在する．さらに，$\beta_j \in I$ なので，何か $k = 1, \ldots, s$ が存在して，$\beta_j \in \alpha_k + \mathbb{Z}^n_{\geq 0}$ とならなければならない．よって，$\beta_j = \alpha_k + \delta$ となる $\delta \in \mathbb{Z}^n_{\geq 0}$ となる $\delta$ が存在する．よって，

$$\alpha_i = \beta_j + \gamma = (\alpha_l + \delta) + \gamma = \alpha_l + (\gamma + \delta) \tag{154}$$

となり，$\alpha_i \in \alpha_l + \mathbb{Z}^n_{\geq 0}$ となる．これは，$\{\alpha_1, \ldots, \alpha_s\}$ が極小基底であることに反する．よって，$\{\alpha_1, \ldots, \alpha_s\} \subset \{\beta_1, \ldots, \beta_t\}$ となる．$I$ 極小基底であるためには，少なくとも $\alpha_1, \ldots, \alpha_s$ を含んでいることが必要で，さらにそれで $I$ を生成するので，極小基底は $\alpha_1, \ldots, \alpha_s$ のみで，一意性が示された．

(問題 9) やった．

(問題 10) $x^{\alpha}y^{\beta}$ の多重指数を $(\alpha; \beta)$ と書くことにする．

- 全順序であること：$(\alpha; \beta) >_{mixed} (\gamma; \delta)$ でも $(\alpha; \beta) <_{mixed} (\gamma; \delta)$ でもないと仮定する．$(\alpha; \beta) >_{mixed} (\gamma; \delta)$ ではないので，

$$\neg((\alpha >_{lex} \beta) \vee ((\alpha = \beta) \wedge (\gamma >_{grlex} \delta))) \tag{155}$$

$$\iff (\alpha \leq_{lex} \beta) \wedge ((\alpha \neq \beta) \vee (\gamma \leq_{grlex} \delta)). \tag{156}$$

同様に，$(\alpha; \beta) <_{mixed} (\gamma; \delta)$ なので，$(\alpha \geq_{lex} \beta) \wedge ((\alpha \neq \beta) \vee (\gamma \geq_{grlex} \delta))$．$\alpha \geq_{lex} \beta$ かつ $\alpha \leq_{lex} \beta$ なので，$\alpha = \beta$．さらに，$((\alpha \neq \beta) \vee (\gamma \geq_{grlex} \delta))$ より，$\gamma \geq_{grlex} \delta$．同様に，$\gamma \leq_{grlex} \delta$．よって，$\gamma = \delta$．

- かけ算で保つ：$(\alpha;\beta) > (\gamma;\delta)$ を仮定する．

$$(\alpha >_{lex} \gamma) \vee ((\alpha = \gamma) \wedge (\beta >_{grlex} \delta)). \tag{157}$$

まず，$\alpha >_{lex} \gamma$ が成立しているときを考える．このときは，$\alpha+\epsilon >_{lex} \gamma+\epsilon$ が成立する．よって，$(\alpha+\epsilon;\beta+\zeta) >_{mixed} (\gamma+\epsilon,\delta+\zeta)$．
次に，$(\alpha=\beta)\wedge(\gamma >_{grlex} \delta)$ が成立しているときを考える．このときは，$\alpha+\epsilon=\beta+\epsilon$ が成立する．また，$\gamma+\zeta >_{grlex} \delta+\zeta$ も成り立つ．よって，$(\alpha+\epsilon=\beta+\epsilon)\wedge(\gamma+\zeta>\delta+\zeta)$ も成り立つ．
以上のことより，$(\alpha;\beta)+(\epsilon;\zeta) >_{mixed} (\gamma,\delta)+(\epsilon;\zeta)$ が成立する．

- 整列順序であること：補題より，$(\alpha;\beta) \geq_{mixed} (0;0)$ を示せば十分である．$(\alpha,\beta)=(0;0)$ のときはあきらかに成立する．よって，$(\alpha,\beta)\neq(0;0)$ と仮定してよい．$(\alpha;\beta) >_{mixed} (0;0)$ を示せばよい．$\alpha >_{lex} 0$ のときは成立するので，以降 $\alpha \leq_{lex} 0$ とする．これは，単項式順序の性質より $\alpha=0$ を意味する．このとき，$(\alpha=0)\wedge(\beta >_{grlex} 0)$ を示せばよい．$\alpha=0$ は今成立している．$\beta >_{grlex} 0$ は grlex が単項式順序なので成立する．よって，成立する．

(問題 11) (a) まず、全順序であることを示す。$\alpha >_{\mathfrak{u}} \beta$ でも $\alpha <_{\mathfrak{u}} \beta$ でもないとする。$\alpha >_{\mathfrak{u}} \beta$ ではないので、$\mathfrak{u}\cdot\alpha > \mathfrak{u}\cdot\beta$ ではなく、$\mathfrak{u}\cdot\alpha \leq \mathfrak{u}\cdot\beta$ である。$\alpha <_{\mathfrak{u}} \beta$ でないことから同様に、$\mathfrak{u}\cdot\alpha \geq \mathfrak{u}\cdot\beta$ である。よって、$\mathfrak{u}\cdot\alpha = \mathfrak{u}\cdot\beta$ であり、$\mathfrak{u}\cdot(\alpha-\beta)=0$ である。$\mathfrak{u}$ の成分が線形独立なので、$\alpha=\beta$ である。
次に、かけ算で順序を保つことを示す。$\alpha >_{\mathfrak{u}} \beta$ とする。$\mathfrak{u}\cdot\alpha > \mathfrak{u}\cdot\beta$ となる。自明に、$\mathfrak{u}\cdot\gamma = \mathfrak{u}\cdot\gamma$ が成立する。不等式の両辺にこれを加えても不等式が保たれ、$\mathfrak{u}\cdot(\alpha+\gamma) > \mathfrak{u}\cdot(\beta+\gamma)$ となる。よって、$\alpha+\gamma >_{\mathfrak{u}} \beta+\gamma$ となる。
最後に、整列順序であることを系を用いて示す。任意の $\alpha \in \mathbb{Z}^n_{\geq 0}$ について、$\alpha \geq_{\mathfrak{u}} 0$ であることを示せばよい。$\mathfrak{u}$ の各成分は正であり、$\alpha$ の各成分は非負なので、$\mathfrak{u}\cdot\alpha \geq 0$ である。よって、$\alpha \geq_{\mathfrak{u}} 0$ となる。

(b) $1, \sqrt{2}$ が $\mathbb{Q}$ 上線形独立であることを示せばよい。$\sqrt{2} = \frac{a}{b}\cdot 1$ と、既約な有理数を用いてあらわされたと仮定する。$2b^2 = a^2$ となる。よって、$a^2$ が 2 の倍数である。2 が素数なので、$2|a\cdot a$ であることから、$2|a$ であり、$a$ は 2 の倍数である。よって、$a^2$ は 4 の倍数である。よって、$2|b^2$ である。2 は素数なので、$2|b$ となる。これは、$a, b$ がともに 2 の倍数であることを意味するが、既約という仮定に反する。

(c) $1, \sqrt{2}$ が独立なことは示したので、$\sqrt{3}$ がこの 2 つのなす部分空間に属していないことを示せばよい。$\sqrt{3} = \frac{a}{b} + \frac{c}{d}\sqrt{2}$ となったとする。$a/b, c/d$ は既約としておく。$bd\sqrt{3} = ad + cb\sqrt{2}$ である。二乗して、$3b^2d^2 = a^2d^2 + 2\sqrt{2}abcd + 2b^2c^2$ となる。ここから、

$$\sqrt{2} = \frac{3b^2d^2 - a^2d^2 - 2b^2c^2}{2abcd} \tag{158}$$

がわかるが、これは $\sqrt{2} \in \mathbb{Q}$ を意味し、(b) に矛盾する。

(問題 12) 多分誤植。「$\mathfrak{u}\cdot\alpha >_\sigma \mathfrak{u}\cdot\beta$」→「$\mathfrak{u}\cdot\alpha > \mathfrak{u}\cdot\beta$」だよね。

(a) 略。

(b) $\mathfrak{u} = (1,\ldots,1)$ とすれば、$\mathfrak{u}\cdot\alpha = |\alpha|$ となる。

(c) 問題文が不正確？ $n=1$ のときには切り分けが不必要な場合がある。このとき、$\mathfrak{u}\neq 0$ であるとする。今、$\mathfrak{u}\in\mathbb{Z}_{\geq 0}$ である。$\mathfrak{u}\cdot\alpha = \mathfrak{u}\cdot\beta$ とする。$\mathfrak{u}\cdot(\alpha-\beta)=0$ である。$\mathfrak{u}\neq 0$ で、$n=1$ ゆえ定数なので、割って $\alpha-\beta=0$ を得る。よって、$\alpha=\beta$ が導かれてしまう。
そういうわけで、$n\geq 2$ という仮定をつけたして問題を解く。$\mathfrak{u}\cdot\xi=0$ となる $\xi\in\mathbb{Q}^n\setminus\{0\}$ を考える。$\mathfrak{u}=0$ のときはなんでもよい。$\mathfrak{u}\neq 0$ とする。$\mathfrak{u}=(u_1,\ldots,u_n)$ とする。$u_1>0$ として一般性を失なわない。

$$\mathfrak{u}\cdot\xi = \sum_{i=1}^{n} u_i\xi_i = 0 \tag{159}$$

である。よって、

$$\xi_1 = \frac{-1}{u_1}\sum_{i=2}^{n} u_i\xi_i. \tag{160}$$

そこで、$\xi_2 = \xi_3 = \cdots = \xi_n = 1$ とすると、$\xi_1 < 0$ となる。これで、$\xi$ が条件をみたす。このとき、$\xi$ の分母を払っても $\mathfrak{u} \cdot \xi = 0$ であり続け、$\xi \in \mathbb{Z}^n$ である。さらに、$\beta = (-\xi_1, 0, \ldots, 0), \alpha = (0, \xi_2, \ldots, \xi_n)$ とすると、$\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$ となり、

$$\mathfrak{u} \cdot (\alpha - \beta) = \mathfrak{u} \cdot \xi = 0. \tag{161}$$

しかし、あきらかに $\alpha \neq \beta$ である。

(d)

$$\begin{aligned}
\mathfrak{u} \cdot \alpha &= \sum_{k=1}^{n} u_k \alpha_k && (162)\\
&= \sum_{k=1}^{i} u_k \alpha_k && (163)\\
&= \sum_{k=1}^{i} \alpha_k && (164)\\
&> 0 && (165)\\
&= \sum_{k=1}^{n} u_k \beta_k && (166)\\
&= \mathfrak{u} \cdot \beta. && (167)
\end{aligned}$$

## 2.5 ヒルベルトの基底定理とグレブナ基底

これまで単項式イデアルを考えてきたが、一般の多項式のイデアルについて考えていく。
0 でないイデアル $I \subset k[x_1, \ldots, x_n]$ について、以下を定義する。

- $\mathrm{LT}(I) = \{\mathrm{LT}(f); f \in I\}$ とする。これはただの $k[x_1, \ldots, x_n]$ の集合である。
- $\langle \mathrm{LT}(I) \rangle$ を $\mathrm{LT}(I)$ で生成されたイデアルとする。こちらはイデアルである。まとめて書くと、

$$\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(f); f \in I \rangle \tag{168}$$

であり、$I$ の LT 全体で生成されるイデアルとも呼べる。

$I$ が有限生成であって、$I = \langle f_1, \ldots, f_s \rangle$ のときには、

$$\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(\langle f_1, \ldots, f_s \rangle) \rangle \tag{169}$$

であって、$f_1, \ldots, f_s$ に、「イデアルをとる→ LT をとる→イデアルをとる」というある意味二度イデアルをとる操作をしているが、もっと簡単に「LT をとる→イデアルをとる」とした $\langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s) \rangle$ との関係はどうなっているのだろうか。まずこの操作の順序から、前者のほうがあきらかに広い。すなわち、

$$\langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s) \rangle \subset \langle \mathrm{LT}(\langle f_1, \ldots, f_s \rangle) \rangle . \tag{170}$$

正確に見るなら、$\mathrm{LT}(f_i) \in \mathrm{LT}(\langle f_1, \ldots, f_s \rangle)$ となることから、

$$\{\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)\} \subset \mathrm{LT}(\langle f_1, \ldots, f_s \rangle) \tag{171}$$

となり、両側でイデアルを取ることにより従う。逆が成り立つか、この両者が等しくなるかというと、常にはそうならない。右辺の $\langle \mathrm{LT}(\langle f_1, \ldots, f_s \rangle) \rangle$ のほうが、最後に $f_1, \ldots, f_s$ の先頭項 LT を消してしまうというような小手技が使えるというのがなんとなくの理由になる。例をあげると、$f_1 = y, f_2 = xy + 1$ というのが等号不成立となる。まず、「イデアルをとる→ LT をとる→イデアルをとる」を考えてみると、

$$f_2 - x \cdot f_1 = (xy + 1) - xy = 1 \tag{172}$$

となり、$1 \in \langle f_1, f_2 \rangle$ となるので、$\langle f_1, f_2 \rangle = \langle 1 \rangle$ となり、$\mathrm{LT}(\langle f_1, f_2 \rangle) = \mathrm{LT}(\langle 1 \rangle) = \langle 1 \rangle$ となり、よって $\langle \mathrm{LT}(\langle f_1, f_2 \rangle) \rangle = \langle 1 \rangle$ となる。一方、「LT をとる→イデアルをとる」のほうは、$\mathrm{LT}(\{f_1, f_2\}) = \{y, xy\}$ となり、$\langle \mathrm{LT}(\{f_1, f_2\}) \rangle = \langle y, xy \rangle = \langle y \rangle$ となる。これは $\langle 1 \rangle$ より真に狭い。この例を作るには、イデアルでのたしひきのときにはかならず係数をかけなければならないのだろうかと考えてみたら、もうちょっと簡単になった。$f_1 = x + 1, f_2 = x$ とする。このとき、「イデアルをとる→ LT をとる→イデアルをとる」のほうは、

$$\langle \mathrm{LT}(\langle f_1, f_2 \rangle) \rangle = \langle \mathrm{LT}(\langle x + 1, x \rangle) \rangle = \langle \mathrm{LT}(\langle 1 \rangle) \rangle = \langle \langle 1 \rangle \rangle = \langle 1 \rangle \,. \tag{173}$$

一方、「LT をとる→イデアルをとる」は、

$$\langle \mathrm{LT}(\{f_1, f_2\}) \rangle = \langle \mathrm{LT}(\{x + 1, x\}) \rangle = \langle \{x\} \rangle = \langle x \rangle \,. \tag{174}$$

よって、「イデアルをとる→ LT をとる→イデアルとる」のほうが真に広くなった。先頭項を打ち消せる分前者のほうが広いということがよくわかる。

一般のイデアル $I \subset k[x_1, \ldots, x_s]$ について、あたりまえだが以下のことが言える。定数倍が大丈夫だということの確認である。

1. $\langle \mathrm{LT}(I) \rangle$ は単項式イデアルである。
2. さらに、単項式イデアル $\langle \mathrm{LT}(I) \rangle$ の生成元について、$f_1, \ldots, f_s \in I$ として $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)$ がとれる。

証明

1. イデアルはその元の定数倍をすべて含んでいることに注意すれば、

$$\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(f); f \in I \rangle = \langle \mathrm{LM}(f); f \in I \rangle \tag{175}$$

   であり、確かに単項式イデアルである。
2. 上で、$\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LM}(f); f \in I \rangle$ を示した。$\langle \mathrm{LM}(f); f \in I \rangle$ はディクソンの補題より、$f_1, \ldots, f_s \in I$ があって、

$$\langle \mathrm{LM}(f); f \in I \rangle = \langle \mathrm{LM}(f_1), \ldots, \mathrm{LM}(f_s) \rangle \tag{176}$$

   となる。また定数倍がどうでもいいことに注意すれば、

$$\langle \mathrm{LM}(f_1), \ldots, \mathrm{LM}(f_s) \rangle = \langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s) \rangle \tag{177}$$

   となる。よって、

$$\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s) \rangle \,. \tag{178}$$

(証終)

これでイデアルと先頭項との関係がよくわかり、イデアルと割り算との相性が良くなった。これで、任意の多項式イデアルについて、その生成元から有限個を選んで生成元とできる「ヒルベルトの基底定理」が証明できる。

証明

$I \subset k[x_1, \ldots, x_n]$ をイデアルとする。$I = \{0\}$ のときはあきらかなので、$I \neq \{0\}$ とする。すると、$\mathrm{LT}(I)$ を考えることができ、さらに $\langle \mathrm{LT}(I) \rangle$ を考えることができる。これに先の定理を適用し、

$$\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s) \rangle \tag{179}$$

となる $f_1, \ldots, f_s \in k[x_1, \ldots, x_s]$ が選べる。このとき、実は $I = \langle f_1, \ldots, f_s \rangle$ となることを示そう。$\supset$ はあきらかなので、$I \subset \langle f_1, \ldots, f_s \rangle$ を示す。$f \in I$ とする。$f$ を $(f_1, \ldots, f_s)$ で割り、

$$f = \sum_{i=1}^{s} f_i h_i + r \tag{180}$$

となる $f_1, \ldots, f_s, r \in k[x_1, \ldots, x_m]$ が存在する。さらに、$r$ は余りなので、$r$ のどの項も $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)$ のどれでも割り切れない。$f \in I$ であり、$f_\bullet \in I$ なので、$r \in I$ である。仮に、$r \neq 0$ であるとする。このとき $\mathrm{LT}(r)$ を考えることができ、(ここがポイント！ )$\mathrm{LT}(r) \in \mathrm{LT}(I)$ となり、$\langle \mathrm{LT}(I) \rangle$ は有限生成となるようにしておいたので、

$$\mathrm{LT}(r) \in \langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s) \rangle \tag{181}$$

となる。よって、$\mathrm{LT}(r)$ は $\mathrm{LT}(f_1),\ldots,\mathrm{LT}(f_s)$ のいずれかの倍数とならなければならないが、これは $r$ が余りであることに反する。よって、$r=0$ である。よって、

$$f=\sum_{i=1}^{s}f_ih_i \tag{182}$$

となる。よって、$f\in\langle f_1,\ldots,f_s\rangle$ となる。$f$ は $I$ の任意の元だったので、$I\subset\langle f_1,\ldots,f_s\rangle$ となる。よって、

$$I=\langle f_1,\ldots,f_s\rangle \tag{183}$$

である。

(証終)

この途中で、$I=\langle f_1,\ldots,f_s\rangle$ が $\langle\mathrm{LT}(I)\rangle=\langle\mathrm{LT}(f_1),\ldots,\mathrm{LT}(f_s)\rangle$ となっていた。このようなイデアルの性質に名前をつける:イデアル $I\subset k[x_1,\ldots,x_n]$ について、その有限部分集合 $\{f_1,\ldots,f_s\}\subset I$ が $I$ の Groebner 基底であるとは、

$$\langle\mathrm{LT}(I)\rangle=\langle\mathrm{LT}(f_1),\ldots,\mathrm{LT}(f_s)\rangle \tag{184}$$

となることである。ここでは $I=\langle f_1,\ldots,f_s\rangle$ となっているかどうかは何も言っていないが、先の証明のなかで、$f\in I$ について $(f_1,\ldots,f_s)$ で割った余りを考察することのより、$f\in\langle f_1,\ldots,f_s\rangle$ となることを示していたので OK である。さらに、さきほどのヒルベルトの基底定理で作ったイデアルは $\langle\mathrm{LT}(I)\rangle=\langle\mathrm{LT}(f_1),\ldots,\mathrm{LT}(f_s)\rangle$ を満たしているので、ヒルベルトの基底定理はもっと強めて、「任意のイデアルには Groebner 基底がある」と言える。これのくだけた言い換えとして、「$I$ のどの先頭項も $\mathrm{LT}(f_1),\ldots,\mathrm{LT}(f_s)$ のどれかで割り切れる」とうのがある。両方とも単項式イデアルなので、その特殊性が使えることに注意する。

先程見たように、$x+1,x$ は $\langle x+1,x\rangle$ の grlex 順序での (なんでもいいが)Groebner 基底ではない。$\langle\mathrm{LT}(x+1),\mathrm{LT}(x)\rangle=\langle x\rangle$ であり、$\langle\mathrm{LT}(\langle x+1,x\rangle)\rangle=\langle 1\rangle$ であったからだ。

次の例は、$\langle x+z,y-z\rangle$ である ($z$ が仲間外れ)。これの lex 順序での Groebner 基底として、$x+z,y-z$ が取れることを示す。Groebner 基底の言い換えより、$\langle x+z,y-z\rangle$ のどの先頭項も $\mathrm{LT}(x+z)=x$ あるいは $\mathrm{LT}(y-z)=y$ で割り切れることを示せば必要十分である。仮に $f\in\langle x+z,y-z\rangle\setminus\{0\}$ で、$x$ でも $y$ でも $\mathrm{LT}(f)$ が割り切れないようなものがあるとする。このとき、$\mathrm{LT}(f)\in k[z]$ である。今は lex 順序を採用しているので、$f\in k[z]$ でもあることがわかる。ところで、$f\in\langle x+z,y-z\rangle$ であったから、$\{(-t,t,t)\}$ 上で $f$ は消えなければならない。よって、$\mathbb{R}$ 上で $f$ が消えなければならないが、今は無限体で考えているので、これは $f$ が多項式として 0 であることを意味する (無数に根を持つ)。これは矛盾である。よって、$\langle x+z,y-z\rangle\setminus\{0\}$ のどの先頭項もすべて $x,y$ で割り切れ、$x+z,y-z$ は $\langle x+z,y-z\rangle$ の Groebner 基底である。

$\langle x+z,y-z\rangle$ の Groebner 基底を考えるには、実は

$$\begin{pmatrix}1&0&1\\0&1&-1\end{pmatrix} \tag{185}$$

の階段行列を考えればよい。このことを一般的に示す。

証明

$A=(a_{ij})_{ij}\in M(\mathbb{R},m,n)$ とし、$I\subset k[x_1,\ldots,x_n]$ を $I=\left\langle\sum_{j=1}^{n}a_{ij}x_j;1\leq i\leq m\right\rangle$ とする。$A$ の狭義階段行列を $A'$ としたとき、この各行からなる多項式たち $\left\{\sum_{j=1}^{n}a'_{ij}x_j;1\leq i\leq \mathrm{rank}A\right\}$ が $I$ のある lex 順序についての Groebner 基底であることを示す。

体 $\mathbb{R}$ で考えているから、$A$ を狭義階段行列 $A'$ に変形することができる。$x_{F(1)},\ldots,x_{F(\mathrm{rank}A)}$ がこの狭義階段行列に変形したことで得られたピボットであるとする。そして、$x_{F(1)}>_{lex}x_{F(2)}>_{lex}\cdots>x_{F(\mathrm{rank}A)}>_{lex}\ldots$(残り) という lex 順序を採用する。変形の過程で基本変形をするが、変形しても各行のなすイデアルは変化しないことは確かめられる。よって、

$$I=\left\langle\sum_{j=1}^{n}a'_{ij}x_j;1\leq i\leq\mathrm{rank}A\right\rangle=\left\langle\sum_{j=F(i)}^{F(i+1)-1}a'_{ij}x_j;1\leq i\leq\mathrm{rank}A\right\rangle \tag{186}$$

がわかる (ただし、$F(\mathrm{rank}A+1)=n+1$ とした)。この元の先頭項すべてが

$$\left\{\mathrm{LT}(\sum_{j=1}^{n}a'_{ij}x_j);1\leq i\leq \mathrm{rank}A\right\}=\left\{\mathrm{LT}(\sum_{j=F(i)}^{F(i+1)-1}a'_{ij}x_j);1\leq i\leq \mathrm{rank}A\right\}=\left\{x_{F(i)};1\leq i\leq \mathrm{rank}A\right\} \tag{187}$$

のどれかで割り切れることを示せばよい。しかし、lex 順序をの入れ方から、これはあきらか。

(証終)

ヒルベルトの基底定理を応用する。多項式環の昇鎖条件を考える。$k[x_1,\ldots,x_n]$ のイデアルの昇鎖列

$$I_1\subset I_2\ldots \tag{188}$$

を考える。このとき、ある $N$ があって、$I_N=I_{N+1}=\ldots$ となる。

証明

$I=\bigcup_i I_i$ を考える。これがイデアルであることを示す。

- 和について閉じる:$f,g\in I$ とする。$f\in I$ なので、$a\in\mathbb{N}$ が存在して、$f\in I_a$ となり、同様に $b\in\mathbb{N}$ について $g\in I_b$ となる。$a\leq b$ として一般性を失なわない。このとき、昇鎖であることから、$f,g\in I_b$ となる。よって、$f+g\in I_b$ であり、$f+g\in I$ である。
- 定数倍で閉じる:$f$ を上と同様とする。$cf\in I_a\subset I$ である。

よって、$I$ はイデアルである。

$I\subset k[x_1,\ldots,x_n]$ はイデアルなので、ヒルベルトの基底定理より、

$$I=\langle f_1,\ldots,f_s\rangle \tag{189}$$

となる。$f_1,\ldots,f_s\in I$ なので、$f_i\in I_{F(i)}$ となる $F(i)$ が存在する。そのうち最大のものを $N$ とすると、昇鎖であることより、$f_1,\ldots,f_s\in I_N$ である。よって、$I\subset I_N$ であり、$I=I_N$ である。昇鎖であることより、$I=I_N=I_{N+1}=\ldots$ である。

(証終)

この、昇鎖があるところで一定する条件を昇鎖条件 (Ascending Chain Condition, ACC) という。したがって、$k[x_1,\ldots,x_n]$ のイデアルは ACC を満足する。

いままで、アフィン多様体は有限個の多項式で作るものだったが、イデアルで作ることを考える。イデアル $I$ について、アフィン多様体と同じ記号を使って $\mathbf{V}(I)$ を、

$$\mathbf{V}(I)=\left\{(\xi_1,\ldots,\xi_n);{}^{\forall}f\in k[x_1,\ldots,x_n]\colon f(\xi_1,\ldots,\xi_n)=0\right\} \tag{190}$$

と定義する。実は $\mathbf{V}(I)$ はアフィン多様体で、さらに $\mathbf{V}(f_1,\ldots,f_s)=\mathbf{V}(\langle f_1,\ldots,f_s\rangle)$ となる。

証明

ヒルベルトの基底定理より、$I\subset k[x_1,\ldots,x_n]$ について、$I=\langle f_1,\ldots,f_s\rangle$ となる。よって、$\mathbf{V}(f_1,\ldots,f_s)=\mathbf{V}(\langle f_1,\ldots,f_s\rangle)$ を示せば十分である。

- $\subset$:$x\in\mathbf{V}(f_1,\ldots,f_s)$ とする。$f_\bullet(x)=0$ となる。$(\xi_1,\ldots,\xi_)\in\mathbf{V}(\langle f_1,\ldots,f_s\rangle)$ かどうかを調べたいので、任意に $g\in\langle f_1,\ldots,f_s\rangle$ とする。

  $$g=\sum_{i=1}^{s}f_ih_i \tag{191}$$

  となる $h_\bullet\in k[x_1,\ldots,x_n]$ が存在する。すると、

  $$g(\xi_1,\ldots,\xi_s)=\sum_{i=1}^{s}(f_i\cdot h_i)(\xi_1,\ldots,\xi_s)=0. \tag{192}$$

  よって、$f\in\mathbf{V}(\langle f_1,\ldots,f_s\rangle)$ である。

- $\supset$:$(\xi_1, \ldots, \xi_n) \in \mathbf{V}(\langle f_1, \ldots, f_s \rangle)$ とする。$\mathbf{V}(\langle f_1, \ldots, f_s \rangle)$ の定義より、$f_\bullet(\xi_1, \ldots, \xi_n) = 0$ となる。

(証終) よって、先に示したように、アフィン多様体は、それの作る多項式のなすイデアルによってのみ定まる。

(問題 1)

$$\langle \mathrm{LT}(g_1), \mathrm{LT}(g_2), \mathrm{LT}(g_3) \rangle = \left\langle xy^2, xy, x \right\rangle = \langle x \rangle . \tag{193}$$

一方、

$$g_1 - yg_2 + zg_3 = (xy^2 - xz + y) - y(xy - z^2) + z(x - yz^4) \tag{194}$$

$$= y + yz^2 - yz^5. \tag{195}$$

これはあきらかに $\langle x \rangle$ に属さない。

(問題 2) 問題 5 について $f_1 = x^2y - z, f_2 = xy - 1$ である。(d) より、$1 - yz \in \langle f_1, f_2 \rangle$ であり、$yz = \mathrm{LM}(1 - yz) \in \langle \mathrm{LT}(\langle f_1, f_2 \rangle) \rangle$ となる。一方、$\langle \mathrm{LT}(f_1), \mathrm{LT}(f_2) \rangle = \left\langle x^2y, xy \right\rangle$ であり、$yz$ を含まない。よって、「イデアルをとる→ LT をとる→イデアルをとる」のほうが真に広い。

問題 6 について $f_1 = 2xy^2 - x, f_2 = 3x^2y - y - 1$ である。$-3x^2 - 2y^2 - 2y \in \langle f_1, f_2 \rangle$ であり、$x^2 \in \langle \mathrm{LT}(\langle f_1, f_2 \rangle) \rangle$ である。一方、$\langle \mathrm{LT}(f_1), \mathrm{LT}(f_2) \rangle = \left\langle xy^2, x^2y \right\rangle$ なので、$x^2$ を含まない。よって、真に広い。

問題 7 について $f_1 = x^4y^2 - z, f_2 = x^3y^3 - 1, f_3 = x^2y^4 - 2z$ である。$2x^2z - xy \in \langle f_1, f_2, f_3 \rangle$ であり、$x^2z \in \langle \mathrm{LT}(\langle f_1, f_2, f_3 \rangle) \rangle$ である。一方、$\langle \mathrm{LT}(f_1), \mathrm{LT}(f_2), \mathrm{LT}(f_3) \rangle = \left\langle x^4y^2, x^3y^3, x^2y^4 \right\rangle$ であり、$x^2z$ を含まない。よって、真に広い。

(問題 3) (a) $\langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s) \rangle$ は $\langle \mathrm{LT}(\langle f_1, \ldots, f_s \rangle) \rangle$ より真に小さいので、$\mathrm{LT}(f) \in \langle \mathrm{LT}(\langle f_1, \ldots, f_s \rangle) \rangle \setminus \langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s) \rangle$ となる $f \in k[x_1, \ldots, x_n]$ が存在する。$\mathrm{LT}(f)$ が何か $\mathrm{LT}(f_\bullet)$ で割り切れてしまうと、$\mathrm{LT}(f) \in \langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s) \rangle$ になってしまうので、$\mathrm{LT}(f)$ はどの $\mathrm{LT}(f_\bullet)$ でも割り切れない。$f$ の項のうち、$\mathrm{LT}(f_\bullet)$ のどれかで割りきれるものがあったとする。その次数を $\alpha$ とする。すると、$\alpha \leq \mathrm{multideg}(f)$ であり、かつ $\alpha = \mathrm{multideg}(f_\bullet) + \alpha'$ となる $\alpha' \in \mathbb{Z}^n_{\geq 0}$ が存在する。よって、$\mathrm{multideg}(f) - \mathrm{multideg}(f_\bullet) \in \mathbb{Z}^n_{\geq 0}$ であり、

$$\mathrm{multideg}(f) = (\mathrm{multideg}(f) - \mathrm{multideg}(f_\bullet)) + \mathrm{multideg}(f_\bullet) \tag{196}$$

となり、$\mathrm{LT}(f)$ は $\mathrm{LT}(f_\bullet)$ で割りきれるが、これは矛盾である。よって、$f$ のどの項も $f_bullet$ のどれでも割り切れず、$f$ を $(f_1, \ldots, f_s)$ で割ったあまりは $f$ そのものである。よって、存在する。

(b)「イデアルをとる→ LT をとる→イデアルをとる」と「LT をとる→イデアルをとる」が一致しない場合は、$(f_1, \ldots, f_s)$ で割って余りが 0 とならなかったとしても、イデアルに属するようなものが存在する。

(c) ?

(問題 4) 定数倍を含むのであきらか

(問題 5)

$$\{g_1, \ldots, g_t\} \text{は} I \text{のグレブナ基底} \tag{197}$$

$$\iff \langle \mathrm{LT}(\langle g_1, \ldots, g_t \rangle) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle \tag{198}$$

$$\iff \langle \mathrm{LT}(\langle g_1, \ldots, g_t \rangle) \rangle \subset \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle \tag{199}$$

$$\iff {}^\forall \mathrm{LT}(g) \in \mathrm{LT}(\langle g_1, \ldots, g_t \rangle) \colon \mathrm{LT}(g) \in \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle \tag{200}$$

$$\iff {}^\forall \mathrm{LT}(g) \in \mathrm{LT}(\langle g_1, \ldots, g_t \rangle) \colon \mathrm{LT}(g) \text{は} \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \text{のいずれかで割り切れる} \tag{201}$$

(問題 6) 割り算アルゴリズムのなかで語ることになるが、つまり $stock_b \in I$ として、$stock_a \in I$ が成立することを言えばよい。初期では $stock_b = f$ なのだから、$stock_b \in I$ が成立する。$\mathrm{LT}(stock_b) \in \mathrm{LT}(I) = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$ が成り立つ。よって、$\mathrm{LT}(stock_b)$ は何か $\mathrm{LT}(g_\bullet)$ で割り切れる。$g_\bullet$ を $g_1$ としても一般性は失なわない。

$$stock_a = stock_b - \frac{\mathrm{LT}(stock_b)}{\mathrm{LT}(g_1)} g_1 \tag{202}$$

$g_1 \in I$ であり、$\frac{\mathrm{LT}(stock_b)}{\mathrm{LT}(g_1)} \in k[x_1, \ldots, x_n]$ であり、$stock_b \in i$ なので、$stock_a \in I$ である。あとは書いてあるとおり。

(問題 7)

$$\left\langle \mathrm{LT}(x^4y^2 - z^5), \mathrm{LT}(x^3y^3 - 1), \mathrm{LT}(x^2y^4 - 2z) \right\rangle = \left\langle x^4y^2, x^3y^3, x^2y^4 \right\rangle . \tag{203}$$

一方、

$$y \cdot (x^4y^2 - z^5) - x \cdot (x^3y^3 - 1) = -yz^5 + x \tag{204}$$

となり、この LM は $yz^5$ なので、これは「LT をとる→イデアルをとる」に入らず、「イデアルをとる→ LT をとる→イデアルをとる」は真に広い。よって、Groebner 基底ではない。

(問題 8) Groebner 基底であることを示す。

$$\left\langle \mathrm{LT}(x - z^2), \mathrm{LT}(y - z^3) \right\rangle = \langle x, y \rangle \tag{205}$$

である。$\left\langle \mathrm{LT}(\left\langle x - z^2, y - z^3 \right\rangle) \right\rangle \subset \langle x, y \rangle$ であることを示せばよい。$f \in \mathrm{LT}(\left\langle x - z^2, y - z^3 \right\rangle)$ とする。$f \in \langle x, y \rangle$ を示す。$f = h_1 \cdot (x - z^2) + h_2 \cdot (y - z^3)$ となる $h_1, h_2 \in k[x_1, \ldots, x_n]$ が存在する。仮に $f \notin \langle x, y \rangle$ であるとする。このときは、$f \in k[z]$ とならなければならない。$f = h_1 \cdot (x - z^2) + h_2 \cdot (y - z^3)$ なので、これは $(t^2, t^3, t)$ 上で消え、$f \in k[z]$ だったが、$z = t$ 全体で消える。よって、無限体上では $f$ は多項式として 0 にならなければならない。

(問題 9) やった

(問題 10) 生成元をこの主イデアルに対応するものとすればそうだ？ $I$ の有限部分集合を $f, g_1, \ldots, g_s$ とする。$h \in I = \langle f \rangle$ とし、$\mathrm{LT}(h)$ が $\mathrm{LT}(f), \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s)$ のどれかで割きれればよい。$h \in \langle f \rangle$ なので、$h = fh'$ となり、$\mathrm{LT}(h) = \mathrm{LT}(f)\mathrm{LT}(h')$ となる。よって、$\mathrm{LT}(f)$ で割り切れる。

(問題 11) $f$ に定数項がないときには $f \in \langle x_1, \ldots, x_n \rangle$ となって矛盾である。よって、$f$ には定数項があり、$f$ を $(x_1, \ldots, x_n)$ で割った余り $r$ は定数になる。この $r \in I$ となり、$I = \langle r \rangle = \langle 1 \rangle = k[x_1, \ldots, x_n]$ となる。

(問題 12) 一般のほうを示す。

- 有限生成 $\Rightarrow$ 昇鎖条件: 先と同様。昇鎖 $I_1 \subset I_2 \subset \ldots$ を考える。$I = \bigcup_i I_i$ は先と同様にイデアルとなる。仮定より[*7] $I = \langle f_1, \ldots, f_s \rangle$ となる。$f_1, \ldots, f_s$ の入っている $f_\bullet$ の番号のうち最大のものを $N$ とすると、$I_N = I$ となる。よって、$I_N = I_{N+1} = \ldots$ である。
- 昇鎖条件 $\Rightarrow$ 有限生成: $R$ が有限生成でないとする。$G_0 = \emptyset$ とし、$I_0 = \langle G_0 \rangle = \{0\}$ とする。$G_{n+1}$ を、$G$ に $R \setminus I_n$ の元どれかを付け加えたものとし、$I_{n+1} = \langle G_{n+1} \rangle$ とする。$R \setminus I_n$ は、$R$ が有限生成でなく、$I_n$ が有限生成であることから空でなく、常に元が選択できる。この構成より、$(I_n)_n$ は真の昇鎖となる。これは昇鎖条件に反する。

(問題 13) 仮にこの降鎖が安定しなかったとすると、1 章 4 節の演習問題の「$V \subsetneq W \iff I(V) \supsetneq I(W)$」より、安定しない昇鎖 $I(V_1) \subset I(V_2) \subset \ \ldots$ が得られるが、これは $k[x_1, \ldots, x_n]$ の昇鎖条件に反する。

(問題 14) 昇鎖 $I_n = \langle f_1, \ldots, f_n \rangle$ を考える。昇鎖条件よりこの昇鎖は安定し、ある $N$ について $I_N = I_{N+1} = \ldots$ となる。$m \leq N$ については $f_m \in I_N$ だし、$m > N$ については $f_m \in I_m = I_N$ であるから、$I$ を生成するのに使った元全てが $I_N$ に属している。よって、$I_N = I$ である。

(問題 15) $V_i = \mathbf{V}(f_1, \ldots, f_i)$ とすると、$(V_i)_i$ は降鎖となる。(13) より、この降鎖は安定し、ある $N$ 以降 $V_N = V_{N+1} = \ldots$ となる。$V_N = \mathbf{V}(f_1, f_2, \ldots)$ となることを示す。$\supset$ は自明なので、$\subset$ を示す。$x \in V_N$ とする。$x \in \mathbf{V}(f_1, \ldots)$ を示せばよく、任意の $M$ について $f_M(x) = 0$ を示せばよい。$M \leq N$ については、$x \in V_N \subset V_M$ より $f_M(x) = 0$ である。$M > N$ については、$x \in V_N = V_{N+1} = \cdots = V_M$ なので、$f_M(x) = 0$ である。

(問題 16) $V$ は多様体なので、$V = \mathbf{V}(f_1, \ldots, f_s)$ なる $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ がある。

- $\subset$:$x \in \mathbf{V}(\mathbf{I}(V)) = \mathbf{V}(\mathbf{I}(\mathbf{V}(f_1, \ldots, f_s)))$ とする。$x$ は任意の $\mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$ に属する多項式で消える。$i = 1, \ldots, s$ とする。$f_i \in \mathbf{V}(f_1, \ldots, f_s)$ なので、$f_i \in \mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$ である。よって、$f_i(x) = 0$ である。$i$ は任意だったので、$x$ は $f_1, \ldots, f_s$ の全てで消える。よって、$x \in \mathbf{V}(f_1, \ldots, f_s)$ となる。よって、$\mathbf{V}(\mathbf{I}(V)) \subset V$ である。

[*7] 「すべての」イデアルが有限生成と言っている。

- $\supset$:$x \in \mathbf{V}(f_1, \ldots, f_s)$ とする。$g \in \mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$ とする。$\mathbf{V}(f_1, \ldots, f_s)$ の点全てを消す多項式 $g_1, \ldots, g_t$ と $h_1, \ldots, h_t \in k[x_1, \ldots, x_n]$ が存在して、

$$g = \sum_{i=1}^{t} h_i g_i \tag{206}$$

となる。$x \in \mathbf{V}(f_1, \ldots, f_s)$ となので、$g_1, \ldots, g_t$ がこれを消し、

$$g(x) = \sum_{i=1}^{t} (h_i g_i)(t) = 0 \tag{207}$$

となり、$g$ は $x$ を消す。$g$ は $\mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$ の任意の多項式だったので、$x \in \mathbf{V}(\mathbf{I}(\mathbf{V}(f_1, \ldots, f_s)))$ となる。よって、$V \subset \mathbf{V}(\mathbf{I}(V))$ となる。

(先に示したのは、$\mathbf{I}(\mathbf{V}(f_1, \ldots, f_s)) = \langle f_1, \ldots, f_s \rangle$ は一般には成立しないということである。今回示したのは $\mathbf{V}(\mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))) = \mathbf{V}(f_1, \ldots, f_s)$ である。イデアルが多様体を定めるという感じが出ている。)

(問題 17) (a) $I = \langle x^2 - y, y + x^2 - 4 \rangle = \langle x^2 - y, 2y - 4 \rangle = \langle x^2 - y, x^2 - 2 \rangle$.

(b)

$$\mathbf{V}(I) \overset{\boxed{\text{イデアルが多様体を決める}}}{=} \mathbf{V}(x^2 - y, x^2 - 2) = \left\{(x, y); x^2 = y, x^2 = 2\right\} = \left\{(\pm\sqrt{2}, 2)\right\}. \tag{208}$$

(問題 18) (a)

$$\begin{aligned}
\mathbf{V}(f, g) &= \mathbf{V}(f, g_1 g_2) && (209)\\
&= \{p; f(p) = 0 \wedge ((g_1 g_2)(p) = 0)\} && (210)\\
&= \{p; f(p) = 0 \wedge g_1(p) g_2(p) = 0\} && (211)\\
&= \{p; f(p) = 0 \wedge ((g_1(p) = 0) \vee (g_2(p) = 0))\} && (212)\\
&= \{p; ((f(p) = 0) \wedge (g_1(p) = 0)) \vee ((f(p) = 0) \wedge (g_2(p) = 0))\} && (213)\\
&= \{p; (f(p) = 0) \wedge (g_1(p) = 0)\} \cup \{p; (f(p) = 0) \wedge (g_2(p) = 0)\} && (214)\\
&= \mathbf{V}(f, g_1) \cup \mathbf{V}(f, g_2). && (215)
\end{aligned}$$

(b)

$$\begin{aligned}
\mathbf{V}(y - x^2, xz - y^2) &= \mathbf{V}(\langle y - x^2, xz - y^2 \rangle) && (216)\\
&= \mathbf{V}(\langle y - x^2, xz - x^4 \rangle) && (217)\\
&= \mathbf{V}(y - x^2, xz - x^4). && (218)
\end{aligned}$$

(c) (b) より、

$$\begin{aligned}
\mathbf{V}(y - x^2, xz - y^2) &= \mathbf{V}(y - x^2, xz - {}^4) && (219)\\
&= \mathbf{V}(y - x^2, x(z - x^3)) && (220)\\
&= \mathbf{V}(y - x^2, x) \cup \mathbf{V}(y - x^2, z - x^3). && (221)
\end{aligned}$$

## 2.6 グレブナ基底の性質

これまではヒルベルトの基底定理の応用を見ていて、Groebner 基底はおまけだったが、Groebner 基底の性質を見ていく。まず、Groebner 基底で割り算をすると、その余りが順序によらない。すなわち:$I \subset k[x_1, \ldots, x_n]$ をイデアルとする。$g_1, \ldots, g_s$ が $I$ の Groebner 基底であるとする。このとき、$f \in k[x_1, \ldots, x_n]$ について、$f = \widetilde{f} + r$ となる $\widetilde{f}, r \in k[x_1, \ldots, x_n]$ で、

- $r$ のどの項も $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s)$ で割り切れない
- $\widetilde{f} \in I$ となる

となるものが一意的に存在する。特に、$f$ は $g_1,\dots,g_s$ をどの順序で並べて割っても余りが同じになる。

証明

- 存在:$f$ を $(g_1,\dots,g_s)$ で割れば得られる。
- 一意性: $f=\widetilde{f_1}+r_1=\widetilde{f_2}+r_2$ と 2 つ得られたとする。$\widetilde{f_1}-\widetilde{f_2}=r_2-r_1$ なので、$r_2-r_1\in I$ となる。仮に $r_2-r_1\neq 0$ であるとすると、$\mathrm{LT}(r_2-r_1)$ を考えることができる。Groebner 基底の性質より、

$$\mathrm{LT}(r_2-r_1)\in\mathrm{LT}(I)\subset\langle\mathrm{LT}(I)\rangle=\langle\mathrm{LT}(g_1,\dots,g_s)\rangle\,. \tag{222}$$

  よって、$\mathrm{LT}(r_2-r_1)$ は $\mathrm{LT}(g_1),\dots,\mathrm{LT}(g_s)$ のどれかで割り切れるが、これは $\mathrm{LT}(r_2)$ か $\mathrm{LT}(r_1)$ のどちらかが $\mathrm{LT}(g_1),\dots,\mathrm{LT}(g_s)$ のどれかで割り切れることになる。これは、$r_1,r_2$ に課した条件に反する。よって、$r_2=r_1$ となる。

(証終)

順序によらないので、$r$ を $f$ の $\{g_1,\dots,g_s\}$ での正規形とよぶ。

Groebner 基底がわかっていれば、イデアルへの所属問題が解ける。すなわち:$I\subset k[x_1,\dots,x_n]$ をイデアルとし、$g_1,\dots,g_s$ をこの Groebner 基底とする。このとき、

$$f\in I\iff f\text{は}(g_1,\dots,g_s)\text{で割り切れる}. \tag{223}$$

証明

- $\Rightarrow$:$f=f+0$ なので、$f$ の Groebner 基底 $\{g_1,\dots,g_s\}$ での割り算の余りの一意性より、割り切れる。
- $\Leftarrow$:$f$ は $g_1,\dots,g_s$ の $k[x_1,\dots,x_n]$ の線形結合になる。

(証終)

余りは便利なので、記号を与える。$f$ を $F=(f_1,\dots,f_s)$ で割った余りを

$$\overline{f}^{F} \tag{224}$$

と書く。$F$ が Groebner 基底の列なら、その順序によらないことになる。

ある $I$ の元の組 $\{f_1,\dots,f_s\}$ の Groebner 基底でない、というのは $\langle\mathrm{LT}(\langle f_1,\dots,f_s\rangle)\rangle$ の元であって $\langle\mathrm{LT}(f_1),\dots,\mathrm{LT}(f_s)\rangle$ の元でないものがあるからであり、つまり $f_1,\dots,f_s$ の線形結合でその先頭項が $\mathrm{LT}(f_\bullet)$ の倍数にならないものが作れてしまうからである。もっと考えると、その線形結合でどの先頭項も消えないならば、線形結合全体の先頭項も $f_\bullet$ の先頭項でありつづけることになってしまう。ということで、Groebner 基底でなくなってしまうためには、線形結合で先頭項が消えてしまうことが必要である。そこで、先頭項が消えるという状況を考えてみる。2 つの多項式について、先頭項の消し方で次のようなものを定義する。

$f,g\in k[x_1,\dots,x_n]$ を 0 でない多項式とする。$\mathrm{LM}(f)$ と $\mathrm{LM}(g)$ の最小公倍式 (LCM) を、

$$\mathrm{LCM}(\mathrm{LM}(f),\mathrm{LM}(g))=x^{\mathrm{multideg}(f)\vee\mathrm{multideg}(g)} \tag{225}$$

とする。そして、$f$ と $g$ の S 多項式を、

$$S(f,g)=\frac{x^{\mathrm{LCM}(\mathrm{LM}(f),\mathrm{LM}(g))}}{\mathrm{LT}(f)}f-\frac{x^{\mathrm{LCM}(\mathrm{LM}(f),\mathrm{LM}(g))}}{\mathrm{LT}(g)}g \tag{226}$$

とする。これでどちらの項の先頭項も次数が一致し、しかもモニックになっているので、先頭項が消えることになる。

すべての先頭項が同じ次数の多項式について、その $k$ 係数線形結合の次数が落ちるのなら、その $k$ 係数線形結合が S 多項式の $k$ 係数線形結合で書ける。すなわち: $f_1,\dots,f_s\in k[x_1,\dots,x_n]$ とし、$\mathrm{multideg}(f_\bullet)=\delta$ と、全て等しいとする。さらに、$c_\bullet\in k[x_1,\dots,x_n]$ を係数とした線形結合 $\sum_{i=1}^s c_if_i$ が、$\mathrm{multideg}(\sum_{i=1}^s c_if_i)<\delta$ となるなら (次数が落ちるなら)、$\sum_{i=1}^s c_if_i$ は $S(f_a,f_b)\quad(1\le a,b\le s)$ の $k$ 係数線形結合となる。さらにこのとき、各 $S(f_a,f_b)$ は、$\mathrm{multideg}(S(f_a,f_b))<\delta$ となる。

証明
線形結合 $\sum_{i=1}^{s} c_i f_i$ の次数が落ちているので、

$$\sum_{i=1}^{s} c_i \mathrm{LC}(f_i) = 0 \tag{227}$$

となる。次数の話をしたいのでモニックにしておきたい。$\mathrm{LC}(f_\bullet)p_\bullet = f_\bullet$ と、$p_\bullet$ を定義する。

$$\begin{aligned}
\sum_{i=1}^{s} c_i f_i &= \sum_{i=1}^{s} c_i \mathrm{LC}(f_i) p_i && (228)\\
&= c_1 \mathrm{LC}(f_1) p_1 + \sum_{i=2}^{s} c_i f_i && (229)\\
&= c_1 \mathrm{LC}(f_1)(p_1 - p_2 + p_2) + \sum_{i=2}^{s} c_i f_i && (230)\\
&= c_1 \mathrm{LC}(f_1)(p_1 - p_2) + (c_1 \mathrm{LC}(f_1) + c_2 \mathrm{LC}(f_2)) p_2 + \sum_{i=3}^{s} c_i f_i && (231)\\
&= \dots && (232)\\
&= \sum_{i=1}^{s-1} (\sum_{j=1}^{i} c_j \mathrm{LC}(f_j))(p_i - p_{i+1}) + \sum_{j=1}^{s} c_j \mathrm{LC}(f_j) p_s. && (233)
\end{aligned}$$

先の次数が落ちている条件より、

$$\begin{aligned}
\sum_{i=1}^{s} c_i f_i &= \sum_{i=1}^{s-1} (\sum_{j=1}^{i} c_j \mathrm{LC}(f_j))(p_i - p_{i+1}) && (234)\\
&= \sum_{i=1}^{s-1} (\sum_{j=1}^{i} c_j \mathrm{LC}(f_j)) S(p_i, p_{i+1}). && (235)
\end{aligned}$$

ここで、各 $S(p_i, p_{i+1})$ は実態は $p_i - p_{i+1}$ だったのだから、次数が落ちて $\mathrm{multideg} S(p_i, p_{i+1}) < \delta$ となる。

(証終)

これを使って、あるイデアルの基底が Groebner 基底であるかどうかの判定条件を、S-多項式をつかって作ることができる:「$I \subset k[x_1, \dots, x_n]$ をイデアルとする。$G = \{g_1, \dots, g_s\}$ は $I$ の基底であるとする。このとき、以下は同値である。

(1) $G$ は $I$ の Groebner 基底である。
(2) $G$ で作るどの S-多項式 $S(g_i, g_j)\,(i \neq j)$ も、$G$ の任意の順序で割り切れる。
(3) $G$ で作るどの S-多項式 $S(g_i, g_j)\,(i \neq j)$ も、何か $G$ の適切な順序が存在して、その順序つきの $G$ で割り切れる。

証明

- (2) $\Longrightarrow$ (3):自明。
- (1) $\Longrightarrow$ (2): $S(g_i, g_j)$ は $G$ の $k[x_1, \dots, x_n]$ 線形結合であり、$G$ が Groebner 基底であるから、割り切れる。
- (3) $\Longrightarrow$ (1): Groebner 基底であることを示すには、$\langle \mathrm{LT}\langle G\rangle\rangle \subset \langle \mathrm{LT}(G)\rangle$ であることを示せばよく、生成元の所属を示すために、$\mathrm{LT}(I) = \mathrm{LT}\langle G\rangle \subset \langle \mathrm{LT}(G)\rangle$ であることを示せばよい。$f \in I$ として、$\mathrm{LT}(f) \in \langle \mathrm{LT}(G)\rangle$ を示せばよい。これを示す。
  少し記法を定める。
  - multideg だと長いので、deg と書くことにする。
  - $\delta(h_\bullet)$ で、$\max\{\deg(h_i g_i); i = 1, \dots, s\}$ をあらわすことにする。同じ値に対しても表示によって変わってしまうので、本当は $(h_1, \dots, h_s)$ に対する関数とするのが正当だろうがこのように略記する。
  - $\mathrm{LCM}(\mathrm{LM}(f), \mathrm{LM}(g))$ を、$\mathrm{LCM}(f, g)$ と略記する。これは、入ってきたものに自動的に LM をあてるようにすればいいだけなので、旧来の記法とも矛盾せず、曖昧さはない。

$f \in I = \langle G \rangle$ なので、$f = \sum_{i=1}^{s} h_i g_i$ となる $h_\bullet \in k[x_1, \ldots, x_n]$ が存在する。和で次数が落ちる可能性があるので、$f = \sum_{i=1}^{s} h_i g_i$ より、$\deg(f) \leq \delta(\sum_{i=1}^{s} h_i g_i)$ となっている。いま、$\deg(f) < \delta(\sum_{i=1}^{s} h_i g_i)$ であるとする。このとき、

$$\delta(\sum_{i=1}^{s} h'_i g_i) < \delta(\sum_{i=1}^{s} h_i g_i), \quad f = \sum_{i=1}^{s} h'_i g_i \tag{236}$$

となる $h'_\bullet$ が存在することを示そう。まずは次数を気にせず $h'_\bullet$ を構成する。

$$\sum_{i=1}^{s} h_i g_i \tag{237}$$

$$= \sum_{\deg(h_i g_i) = \delta(\sum h_i g_i)} \mathrm{LT}(h_i) g_i + \sum_{\deg(h_i g_i) = \delta(\sum h_i g_i)} (h_i - \mathrm{LT}(h_i)) g_i + \sum_{\deg(h_i g_i) < \delta(\sum h_i g_i)} h_i g_i \tag{238}$$

と書ける。この第 1 項について、「同次のものを足して次数が落ちて」いるので、定理が使えて、

$$\sum_{\deg(h_i g_i) = \delta(\sum h_i g_i)} \mathrm{LT}(h_i) g_i = \sum_{j,k} c_{j,k} S(\mathrm{LT}(h_j) g_j, \mathrm{LT}(h_k) g_k) \tag{239}$$

となる $c_\bullet \in k$ が存在する。S の中身の特殊性を使って計算してみると、

$$S(\mathrm{LT}(h_j) g_j, \mathrm{LT}(h_k) g_k) = \frac{\mathrm{LCM}(\mathrm{LT}(h_j) g_j, \mathrm{LT}(h_k) g_k)}{\mathrm{LCM}(g_j, g_k)} S(g_j, g_k) \tag{240}$$

である。仮定より、$G$ の適切な順序での割り算を適用して

$$S(g_j, g_k) = \sum_{i=1}^{s} a_{ijk} g_i \tag{241}$$

となる $a_{ijk} \in k[x_1, \ldots, x_n]$ が存在する。まとめると、

$$\sum_{i=1}^{s} h_i g_i = \underbrace{\sum_{j,k} \sum_{i=1}^{s} c_{jk} \frac{\mathrm{LCM}(\mathrm{LT}(h_j) g_j, \mathrm{LT}(h_k) g_k)}{\mathrm{LCM}(g_j, g_k)} a_{ijk} g_i}_{①} + \underbrace{\sum_{\deg(h_i g_i) = \delta(\sum h_i g_i)} (h_i - \mathrm{LT}(h_i)) g_i}_{②} + \underbrace{\sum_{\deg(h_i g_i) < \delta(\sum h_i g_i)} h_i g_i}_{③} \tag{242}$$

となる。この右辺は、$f = \sum_{i=1}^{s} h_i g_i$ の $g_\bullet$ での線形結合の表現になっているので、これにあわせて $h'_\bullet$ を定めればよい。これが次数の条件を満たすことを示す。②, ③ については、$\sum$ の条件よりあきらかなので、① の中身が全て、「次数が $\delta(\sum h_i g_i)$ 未満」を満たせば十分である。$i, j, k$ を固定して考える。

$$\deg(c_{jk} \frac{\mathrm{LCM}(\mathrm{LT}(h_j) g_j, \mathrm{LT}(h_k) g_k)}{\mathrm{LCM}(g_j, g_k)} a_{ijk} g_i) \tag{243}$$

$$\leq \deg(c_{jk} \frac{\mathrm{LCM}(\mathrm{LT}(h_j) g_j, \mathrm{LT}(h_k) g_k)}{\mathrm{LCM}(g_j, g_k)} \sum_{i=1}^{s} a_{ijk} g_i) \tag{244}$$

割り算の性質。(商)×(割る式) の次数は (割られる式) の次数を越えない。アルゴリズム参照。 (245)

$$= \deg(c_{jk} \frac{\mathrm{LCM}(\mathrm{LT}(h_j) g_j, \mathrm{LT}(h_k) g_k)}{\mathrm{LCM}(g_j, g_k)} S(g_j, g_k)) \tag{246}$$

S 多項式を割っていたのだった。 (247)

$$= \deg(c_{jk} S(\mathrm{LT}(h_j) g_j, \mathrm{LT}(h_k) g_k)) \tag{248}$$

$$< \deg(\delta(\sum_{i=1}^{s} h_i g_i)) \tag{249}$$

「同次のものを足して次数が落ちて」の主張。 (250)

よって、条件を満たす $h'_\bullet$ が構成できた。この操作は、$\deg(f) < \delta(\sum_{i=1}^{s} h_i g_i)$ が満たされる限り繰替えせるので、有限回繰替えすことにより、$\deg(f) = \delta(\sum_{i=1}^{s} h_i g_i)$ をみたす $h_\bullet$ が求まる。つまり、$\deg(f) = \deg(h_i g_i)$ となる $i = 1, \ldots, s$ が存在する。よって、$\mathrm{LM}(f) = \mathrm{LM}(h_i g_i) = \mathrm{LM}(h_i)\mathrm{LM}(g_i)$ であり、$\mathrm{LT}(f)$ は $\mathrm{LT}(g_i)$ で割り切れる。よって、$\mathrm{LT}(f) \in \langle \mathrm{LT}G \rangle$ である。

(証終) つまり、ある多項式の組がイデアルの Groebner 基底であるかどうかを見るには、その多項式の組からすべての S 多項式を作って、それを好きな順序の多項式の組で割って、すべて余りが 0 であることを見れば必要十分である。

例として、3 次ねじれ曲線のイデアル $I = \langle y - x^2, z - x^3 \rangle$ の Groebner 基底として、$\{y - x^2, z - x^3\}$ が取れることを示そう。ただし、$y > z > x$ の lex 順序とする。これは、$S(y - x^2, z - x^3)$ が $(y - x^2, z - x^3)$ で割り切れればよい。

$$S(y - x^2, z - x^3) = yx^3 - zx^2 \tag{251}$$

である。これを割ってみると、

$$yx^3 - zx^2 = x^3(y - x^2) + (-x^2)(z - x^3) \tag{252}$$

となり、割り切れたので、Groebner 基底であることがわかった。

(問題 1) (a) $I$ の Groebner 基底 $G$ を作ることができるので、それで $f$ を割ればよい。

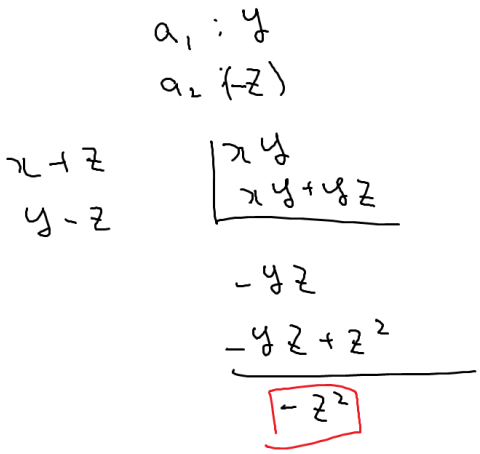
(b) $f = g + r = g' + r'$ と与えられたとする。先の Grobner 基底を考えると、この $g + r = g' + r'$ はすでに $G$ で $I$ の元と正規形とに分けた形になっているので、Groebner 基底の性質より、$r = r'$ となる。

(b') $f = g + r = g' + r'$ と与えられたとする。$(g - g') + (r - r') = 0$ である。$r - r'$ は $r, r'$ の性質より、$\mathrm{LT}(I)$ のどれでも割り切れないので、この 0 の表示はすでに $I$ とその余りとで分けた形になっている。よって、$r - r', g - g'$ となる。

(備考) これで、割り算のあまりが $I$ の基底、あるいはその順序によらずに $I$ だけで決まることがわかった。そういうわけで、採用する順序を変えてもその余りは変化せず、Groebner 基底かどうかを調べるには何か 1 つ基底を選んで調べればよい。他の順序を使ったらあまりが出てしまったということはない。

(問題 2) (a) (図 8)1428152186061.png 参照.

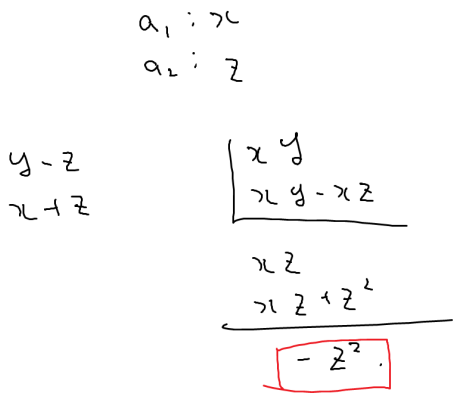
図 8　1428152186061.png




$-z^2$ が余り。商は $(y, -z)$ である。

(b) (図 9)1428152296875.png 参照.

図 9　1428152296875.png




$-z^2$ が余りで先と一致する。しかし、商は $(x, z)$ となり、さっきとは全然違う。

(問題 3) 基底といったら、有限生成なイデアルに対しての有限個の生成元たちのことであったから、$G$ は有限集合である。確認した。$G = \{g_1, \ldots, g_s\}$ とする。$S(g_i, g_j)$ を考える。ただし、$i \neq j$ である。$S(g_i, g_j) \in \langle G \rangle = I$ なので、仮定より $\overline{S(g_i, g_j)}^G = 0$ である。$i, j$ は任意であった。よって、ブッフベルガーの S ペア判定条件より、$G$ は Groebner 基底である。

(問題 4) $G$ での割り算と $G'$ での割り算と $I$ での割り算が一致することを問題 1 で見た。

(問題 5) (a) 先頭を $x^2yz^2$ にあわせる。

$$S(f, g) = \frac{yz}{4}f - xg = (x^2yz^2 - \frac{7}{4}y^3z) - (x^2yz^2 + 3x^2z^4) = -3x^2z^4 - \frac{7}{4}y^3z. \tag{253}$$

(b) 先頭を $x^4yz^2$ にあわせる。

$$S(f, g) = z^2f - \frac{x^3y}{3}g = (x^4yz^2 - z^4) - (x^4yz^2 + \frac{x^3y^2}{3}) = \frac{-1}{3}x^3y^2 - z^4. \tag{254}$$

(c) 先頭を $x^7y^2z$ にあわせる。

$$f - \frac{1}{2}g = (x^7y^2z + 2ixyz) - (x^7y^2z + 2) = 2ixyz - 2. \tag{255}$$

(d) 先頭を $xyz^2$ にあわせる。

$$(z^2)f - (xy)g = (xyz^2 + z^5) - (xyz^2 - 3xyz) = 3xyz + z^5. \tag{256}$$

(問題 6) 異なる。$x > y$ ならば $S(x + y, x) = y$ だが、$y > x$ ならば $S(y + x, x) = x^2$ である。

(問題 7)

$$\deg(S(f, g)) = \deg(\frac{\mathrm{LCM}(f, g)}{\mathrm{LT}(f)}(\mathrm{LT}(f) + (f - \mathrm{LT}(f))) - \frac{\mathrm{LCM}(f, g)}{\mathrm{LT}(g)}(\mathrm{LT}(g) + (g - \mathrm{LT}(g)))) \tag{257}$$

$$= \deg(\frac{\mathrm{LCM}(f, g)}{\mathrm{LT}(f)}(f - \mathrm{LT}(f)) - \frac{\mathrm{LCM}(f, g)}{\mathrm{LT}(g)}(g - \mathrm{LT}(g))) \tag{258}$$

$$= \max\left\{\deg(\frac{\mathrm{LCM}(f, g)}{\mathrm{LT}(f)}(f - \mathrm{LT}(f))), \deg(\frac{\mathrm{LCM}(f, g)}{\mathrm{LT}(g)}(g - \mathrm{LT}(g)))\right\} \tag{259}$$

$$= \max\{\deg(\mathrm{LCM}(f, g)) - \deg(\mathrm{LT}(f)) + \deg(f - \mathrm{LT}(f)), \deg(\mathrm{LCM}(f, g)) - \deg(\mathrm{LT}(g)) + \deg(g - \mathrm{LT}(g))\} \tag{260}$$

$$= \deg(\mathrm{LCM}(f, g)) + \max\{\deg(f - \mathrm{LT}(f)) - \deg(\mathrm{LT}(f)), \deg(g - \mathrm{LT}(g)) - \deg(\mathrm{LT}(g))\} \tag{261}$$

$$< \deg(\mathrm{LCM}(f, g)). \tag{262}$$

(問題 8) $S(-x^2+y, -x^3+z) = xy - z$ である。これを $(-x^2+y, -x^3+z)$ で割ったあまりは $xy-z$ そのものであり、0 でないので S ペア判定法より Groebner 基底でない。

(問題 9) `code/ex_2_3_6.hs` で計算。

(a) Groebner 基底でない。Checking if following bases are Groebner basis. Divisors and bases are

- $x^2 + (-1)y$
- $x^3 + (-1)z$

.

i. $S(x^2 + (-1)y, x^3 + (-1)z) = (-1)xy + z$. Calculation is

A. Start: calculates $(-1)xy + z \div$

- $x^2 + (-1)y$,
- $x^3 + (-1)z$,

.

B. Remainder: $(-1)xy$ moved to remainder.

C. Remainder: $z$ moved to remainder.

D. Completed: quotients are

- 0,
- 0,

. remainder is $(-1)xy + z$. ■

. ■

(b) Groebner 基底である。Checking if following bases are Groebner basis. Divisors and bases are

- $(-1)y + x^2$
- $(-1)z + x^3$

.

i. $S((-1)y + x^2, (-1)z + x^3) = (-1)x^2z + x^3y$. Calculation is

A. Start: calculates $(-1)x^2z + x^3y \div$

- $(-1)y + x^2$,
- $(-1)z + x^3$,

.

B. Division: $(-1)z + x^3$ divides stock. stock is $x^3y + (-1)x^5$ .

C. Division: $(-1)y + x^2$ divides stock. stock is 0 .

D. Completed: quotients are

- $(-1)x^3$,
- $x^2$,

. remainder is 0. ■

. ■

(c) Groebner 基底でない。Checking if following bases are Groebner basis. Divisors and bases are

- $xy^2 + (-1)xz + y$
- $xy + (-1)z^2$
- $x + (-1)yz^4$

.

i. $S(xy^2 + (-1)xz + y, xy + (-1)z^2) = (-1)xz + yz^2 + y$. Calculation is

A. Start: calculates $(-1)xz + yz^2 + y \div$

- $xy^2 + (-1)xz + y$,
- $xy + (-1)z^2$,
- $x + (-1)yz^4$,

.

B. Division: $x + (-1)yz^4$ divides stock. stock is $(-1)yz^5 + yz^2 + y$ .

C. Remainder: $(-1)yz^5$ moved to remainder.

D. Remainder: $yz^2$ moved to remainder.

E. Remainder: $y$ moved to remainder.

F. Completed: quotients are

- 0,
- 0,
- $(-1)z$,

. remainder is $(-1)yz^5 + yz^2 + y$. ■

. ■

ii. $S(xy^2 + (-1)xz + y, x + (-1)yz^4) = (-1)xz + y^3z^4 + y$. Calculation is

A. Start: calculates $(-1)xz + y^3z^4 + y \div$

- $xy^2 + (-1)xz + y$,
- $xy + (-1)z^2$,
- $x + (-1)yz^4$,

.

B. Division: $x + (-1)yz^4$ divides stock. stock is $y^3z^4 + (-1)yz^5 + y$ .

C. Remainder: $y^3z^4$ moved to remainder.

D. Remainder: $(-1)yz^5$ moved to remainder.

E. Remainder: $y$ moved to remainder.

F. Completed: quotients are

- 0,
- 0,
- $(-1)z$,

. remainder is $y^3z^4 + (-1)yz^5 + y$. ■

. ■

iii. $S(xy + (-1)z^2, x + (-1)yz^4) = y^2z^4 + (-1)z^2$. Calculation is

A. Start: calculates $y^2z^4 + (-1)z^2 \div$

- $xy^2 + (-1)xz + y$,
- $xy + (-1)z^2$,
- $x + (-1)yz^4$,

.

B. Remainder: $y^2z^4$ moved to remainder.

C. Remainder: $(-1)z^2$ moved to remainder.

D. Completed: quotients are

- 0,
- 0,
- 0,

. remainder is $y^2z^4 + (-1)z^2$. ■

. ■

(問題 10) この状況では、$\mathrm{LT}(f) = \mathrm{LM}(f), \mathrm{LT}(g) = \mathrm{LM}(g)$ ということになる。あと、$\mathrm{GCD}(\mathrm{LM}(f), \mathrm{LM}(g)) = \mathrm{GCD}(f, g) = f \wedge g$ とかき、$\mathrm{LCM}(\mathrm{LM}(f), \mathrm{LM}(g)) = \mathrm{LCM}(f, g) = f \vee g$ とかくことにする。一般に $\max(a, b) + \min(a, b) = a + b$ が成立することを考えると、$(f \wedge g) + (f \vee g) = \mathrm{LM}(f) + \mathrm{LM}(g)$ となる。さらに、互いに素なので、$f \vee g = 1$ である。

(a)

$$S(f,g) = \frac{f \vee g}{\mathrm{LT}(f)} f - \frac{f \vee g}{\mathrm{LT}(g)} g \tag{263}$$
$$= \frac{f \vee g}{\mathrm{LM}(f)} f - \frac{f \vee g}{\mathrm{LM}(g)} g \tag{264}$$
$$= \frac{\mathrm{LM}(f)\mathrm{LM}(g)/(f \wedge g)}{\mathrm{LM}(f)} f - \frac{\mathrm{LM}(f)\mathrm{LM}(g)/(f \wedge g)}{\mathrm{LM}(g)} g \tag{265}$$
$$= \mathrm{LM}(g) f - \mathrm{LM}(f) g \tag{266}$$
$$= \mathrm{LM}(g)((f - \mathrm{LT}(f)) + \mathrm{LT}(f)) - \mathrm{LM}(f)((g - \mathrm{LT}(g)) + \mathrm{LT}(g)) \tag{267}$$
$$= \mathrm{LM}(g)((f - \mathrm{LM}(f)) + \mathrm{LM}(f)) - \mathrm{LM}(f)((g - \mathrm{LM}(g)) + \mathrm{LM}(g)) \tag{268}$$
$$= \mathrm{LM}(g)(f - \mathrm{LM}(f)) - \mathrm{LM}(f)(g - \mathrm{LM}(g)) \tag{269}$$
$$= \mathrm{LM}(g) f - \mathrm{LM}(f) g \tag{270}$$

あとは余計なのを足せばできる。

(b) 先の展開より、$S(f,g)$ のすべての項が $\mathrm{LM}(g)$ か $\mathrm{LM}(f)$ かの倍元になる。

(問題 11)

$$x^\gamma S(f,g) = \frac{(x^\alpha f) \vee (x^\beta g)}{f \vee g} S(f,g) \tag{271}$$
$$= \frac{(x^\alpha f) \vee (x^\beta g)}{f \vee g} \left(\frac{f \vee g}{\mathrm{LT}(f)} f - \frac{f \vee g}{\mathrm{LT}(g)} g\right) \tag{272}$$
$$= \frac{(x^\alpha f) \vee (x^\beta g)}{\mathrm{LT}(f)} f - \frac{(x^\alpha f) \vee (x^\beta g)}{\mathrm{LT}(g)} g \tag{273}$$
$$= S(x^\alpha f, x^\beta g). \tag{274}$$

(問題 12) (a) $\overline{f}^G = \overline{g}^G \implies f - g \in I$: 問題 1 のように、$I$ で割り算して $f = \widetilde{f} + \overline{f}^G$ と $g = \widetilde{g} + \overline{g}^G$ と書く。$f - g = (\widetilde{f} - \widetilde{g}) + (\overline{f}^G - \overline{g}^G)$ である。

- 上の表示は $f - g$ を $I$ で割った形になっており、$\overline{f}^G = \overline{g}^G$ より、$\overline{f - g}^G = 0$ である。
- $f - g \in I \implies \overline{f}^G = \overline{g}^G$: $f - g \in I$ なので、$I$ でわった余りは 0 であり、$\overline{f}^G - \overline{g}^G = 0$ となる。よって、$\overline{f}^G = \overline{g}^G$ である。

(b) $f = \widetilde{f} + \overline{f}^G$, $g = \widetilde{g} + \overline{g}^G$ としておく。すると、$f + g = (\widetilde{f} + \widetilde{g}) + (\overline{f}^G + \overline{g}^G)$ となり、これはすでに $G$ でわった形なので、$\overline{f + g}^G = \overline{f}^G + \overline{g}^G$ である。

(c) $f, g$ を上と同じに書く。

$$fg = (\widetilde{f}\widetilde{g} + \widetilde{f}\overline{g}^G + \widetilde{g}\overline{f}^G) + \overline{f}^G\overline{g}^G \tag{275}$$

となる。$\overline{f}^G\overline{g}^G$ を $I$ で割って、$\overline{f}^G\overline{g}^G = \widetilde{h} + \overline{\overline{f}^G\overline{g}^G}^G$ を得る。代入し、

$$fg = (\widetilde{f}\widetilde{g} + \widetilde{f}\overline{g}^G + \widetilde{g}\overline{f}^G + \widetilde{h}) + \overline{\overline{f}^G\overline{g}^G}^G \tag{276}$$

を得る。これは $I$ で割った形なので、

$$\overline{fg}^G = \overline{\overline{f}^G\overline{g}^G}^G. \tag{277}$$

## 2.7 ブッフベルガーのアルゴリズム

これまで、任意の $k[x_1, \ldots, x_n]$ のイデアルに Groebner 基底が存在することは示したが、その構成まではわからなかった。そこで、イデアル $I = \langle g_1, \ldots, g_s \rangle$ に対しての Groebner 基底を求める方法を考えてみる。先の章より、S ペア判定法から、どの $g_i, g_j$ についても、$S(g_i, g_j) \in I$ となっていることが必要十分だった。そこで、イデアル $I$ の生成

元 $g_1, \ldots, g_s$ に $S(g_i, g_j)$ をすべてつけ足したらどうかという気分になる。それも Groebner 基底にならなければ、その生成元についてまた S ペアを増やす。実はこれを繰り返すと有限回で Groebner 基底になり、これはアルゴリズムになる。

「$\langle f_1, \ldots, f_s \rangle \subset I$ の Groebner 基底を構成するアルゴリズムが存在する。」

証明
以下のアルゴリズムで構成できることを示す。

**Algorithm 2** Groebner 基底のアルゴリズム

1: $G := \{f_1, \ldots, f_s\}$
2: **repeat**
3: $\quad G' := G$
4: $\quad G \Leftarrow G \cup \left\{ \overline{S(g_1, g_2)}^{G'} ; g_1 \neq g_2 \in G' \text{ かつ } \overline{S(g_1, g_2)}^{G'} \neq 0 \right\}$
5: **until** $G = G'$

これについて、以下を示す必要がある。

- 正しい答えが得られること: このアルゴリズムが停止したとき、

$$\left\{ \overline{S(g_1, g_2)}^{G'} ; g_1 \neq g_2 \in G' \right\} \subset G' \tag{278}$$

となっている。つまり、任意の $g_1 \neq g_2 \in G'$ について、$\overline{S(g_1, g_2)}^{G'} \in G'$ となっている。$\overline{S(g_1, g_2)}^{G'}$ は $G'$ でわった余りなので、これが $G'$ の元であるということは、$\overline{S(g_1, g_2)}^{G'} = 0$ である。よって、停止したとき確かに $G' = G$ は $\langle G' \rangle = \langle G \rangle$ の Groebner 基底になっている。
さらに、$\langle G \rangle = I$ であることを示さなければならない。はじめはあきらかに $I$ の基底になっているので、ループの途中で $I$ をはみ出さなければよいが、L.4 で加えているのは $\overline{S(g_1, g_2)}^{G'}$ である。$S(g_1, g_2) \in \langle G' \rangle = \langle G \rangle = I$ であり、それを $I$ の部分集合である $G'$ で割っているのだから、$\overline{S(g_1, g_2)}^{G'} \in I$ となり、基底として無駄なものを足していることになるので、ずっと $G \subset I$ でありつづける。$G$ は $I$ の生成元である $f_1, \ldots, f_s$ を含んでいるのだから $G \supset I$ であり、常に $G = I$ である。
- 停止すること: 仮に、このアルゴリズムが停止しなかったとし、順次得られる $G$ を $G_\bullet$ とする。停止条件より、真の部分集合の昇鎖

$$G = G_0 \subsetneq G_1 \subsetneq G_2 \subsetneq \ldots \tag{279}$$

が得られる。部分集合の昇鎖であって、イデアルの昇鎖ではないのでこれそのものは問題ではない。さらに、アルゴリズムの L.5 の終了条件より、停止するのは L.4 で追加した (つもりになっていたもの) が前の $G$ に含まれていたときに限るので、$G_i \subsetneq G_{i+1}$ について、$g_1 \neq g_2 \in G_i$ で、$\overline{S(g_1, g_2)}^{G_i} \in G_{i+1} \setminus G_i$ となるものが存在する。 あまりの定義により、$\overline{S(g_1, g_2)}^{G_i}$ のどの項も、$\mathrm{LT}(G_i)$ のどの項でも割りきることができない。したがって特に、$\mathrm{LT}(\overline{S(g_1, g_2)}_i^G)$ のどの項も、$\mathrm{LT}(G_i)$ のどの項でも割り切ることができず、当然 $\overline{S(g_1, g_2)}^{g_i} \in G_{i+1}$ なので、

$$\langle \mathrm{LT}(G_i) \rangle \subsetneq \langle \mathrm{LT}(G_{i+1}) \rangle \tag{280}$$

となる。つまり、先の $G_\bullet$ の昇鎖から、

$$\langle \mathrm{LT}(G) \rangle = \langle \mathrm{LT}(G_0) \rangle \subsetneq \langle \mathrm{LT}(G_1) \rangle \subsetneq \langle \mathrm{LT}(G_2) \rangle \subsetneq \ldots \tag{281}$$

という、$k[x_1, \ldots, x_n]$ の真の昇鎖が得られる。しかしこれは、$k[x_1, \ldots, x_n]$ がネーター環であり、ACC を満たすことに矛盾する。よって、アルゴリズムは停止する。

(証終)

上のアルゴリズムでは $\left\{\overline{S(g_1,g_2)}^{G'}; g_1 \neq g_2 \in G'\right\}$ と書いてしまったが、これは有限の手続で作れることがあきらかなのでこのように書いた。

しかし、これではやたらと無駄な基底が加わってしまっている。そこで、余計なものを除去することを考える。「$G$ がイデアル $I$ の Groebner 基底であり、$p \in G$ が、$\mathrm{LT}(p) \in \langle \mathrm{LT}(G \setminus \{p\})\rangle$ をみたすとする。このとき、$G \setminus \{p\}$ は $I$ の Groebner 基底である。」

証明

仮定より、$\langle \mathrm{LT}(G \setminus \{p\})\rangle = \langle \mathrm{LT}(G)\rangle$ となっている。さらに、$G$ は $I$ の Groebner 基底なので、$\langle \mathrm{LT}(G)\rangle = \langle \mathrm{LT}(I)\rangle$ である。よって、$\langle \mathrm{LT}(G \setminus \{p\})\rangle = \langle \mathrm{LT}(I)\rangle$ となる。

(証終) これで、「$G \setminus \{p\}$ は $I$ の基底になっているのか？」と不安になったが、それが Groebner 基底のあとの定義でやった。復習する。つまり、$G$ が $\langle \mathrm{LT}(G)\rangle = \langle \mathrm{LT}(I)\rangle$ をみたせば、$\langle G\rangle = I$ となるのである。$\langle G\rangle \subset I$ はあきらかなので、逆をしめす。$f \in I$ とする。このとき、$\mathrm{LT}(f) \in \langle \mathrm{LT}(I)\rangle = \langle \mathrm{LT}(G)\rangle$ となる。単項式イデアルの性質より、$f$ の先頭項が $G$ のどれかの先頭項で割り切れることになるので、$f$ は $G$ のどれかで「一回分」割り算がでて、暫定的な余りがでる。この余りは、$f \in I$ であることと $G \subset I$ であることから、やはり $I$ に入る。するとこの余りの先頭項が $\mathrm{LT}(I)$ に入るので、これにあわせてまた $G$ を選んで、と、計算がおわるまで暫定的な余りが $I$ に入り続け、割り切れることになる。復習おわり。

この命題を使って Groebner 基底を削り続けて、削りきれなくなったところがある意味標準形であると考えられるので、次のように定義する。「$G$ がイデアル $I$ の極小 Groebner 基底であるとは、

(1) $G$ からどれを外しても Groebner 基底でなくなる: $p \in G \implies \mathrm{LT}(p) \notin \langle \mathrm{LT}(G \setminus \{p\})\rangle$ である。
(2) $G$ のどれもがモニックである

である」と定める。Groebner 基底をモニックにするのは LC で割るだけである。実際に計算するには、1 つ基底をとって、その LT がほかの LT で書けるか、単項式イデアルであることに注目するとほかの LT で割り切れるかを見て、割りきれたらそれを取り除くという操作を基底の個数分繰替えせばよい。極小という名の通り、極小 Groebner 基底は無数に存在する。たとえば $\langle x+z, y+z\rangle = \langle x+2z, y+z\rangle = \langle x+3z, y+z\rangle = \ldots$ はどれも極小 Groebner 基底である。←極小 Groebner 基底には間違いないが、どれもイデアルが違っている！

しかし、極小 Groebner 基底のうち、さらに強い簡約 Groebner 基底を「$G$ がイデアル $I$ の簡約 Groebner 基底であるとは、

(1) $G$ からどれを外しても Groebner 基底でなくなる: $p \in G \implies p$ のどの項も $\langle \mathrm{LT}(G \setminus \{p\})\rangle$ に入らない。(先頭項だけではなく、すべての項になった！ )
(2) $G$ のどれもがモニックである。

証明

$G = \{f_1, \ldots, f_s\}$ を $I$ の極小 Groebner 基底とする。ここから簡約 Groebner 基底を作ることを考える。

**Algorithm 3** 簡約 Groebner 基底を作る

```
1: i = 0
2: G = [f_1, ..., f_s]
3: for i = 1, ..., s do
4:     G[i] ⇐ f_i^{G\{f_i}}
5: end for
```

L.3 に入ったとき $i$ であるとし、このときの $G$ を $G_b$ とする。L.5 に次に到達したとき、$G$ を $G_a$ とする。$G_b$ は 1〜$i-1$ 番目は $G$ について簡約されているとしてよい。停止は自明。

まず、どの時点でも $\mathrm{LT}(G)$ が一定であることを示す。$\mathrm{LT}(G_b) = \mathrm{LT}(G_a)$ を示す。$G_b$ と $G_a$ は $i$ 番目だけ異なるので、$\mathrm{LT}(G_b[i]) = \mathrm{LT}(G_a[i])$ を示せばよい。L.4 より、$\mathrm{LT}(G_b[i]) = \mathrm{LT}(f_i)$ であり、$\mathrm{LT}(G_a[i]) = \mathrm{LT}(\overline{f_i}^{G_b\setminus\{f_i\}})$

なので、$\mathrm{LT}(f_i) = \mathrm{LT}(\overline{f_i}^{G_b\setminus\{f_i\}})$ を示せばよい。$G_b$ は (帰納法の仮定より) 極小 Groebner 基底になっているので、$\mathrm{LT}(f_i) \notin \langle \mathrm{LT}(G_b \setminus \{f_i\})\rangle$ となっている。したがって、$\mathrm{LT}(f_i)$ は $\mathrm{LT}(G_b \setminus \{f_i\})$ のいずれでも割り切れない。ここで割り算のアルゴリズムを思い出すと、初手で割り算が発生せず、割られる式の先頭項が余りに移動するので、$\overline{f_i}^{G_b\setminus\{f_i\}}$ の LT は $\mathrm{LT}(f_i)$ になる[*8]。よって、$\mathrm{LT}(f_i) = \mathrm{LT}(\overline{f_i}^{G_b\setminus\{f_i\}})$ となる。よって、$\mathrm{LT}(G_b) = \mathrm{LT}(G_a)$ である。

次に、どの時点でも $G$ が Groebner 基底であることを示す。L.2 の時点では仮定より Groebner なので、ループ中を考える。$G_b$ は帰納法の仮定より Grobner である。

$$\langle \mathrm{LT}(G_a)\rangle = \langle \mathrm{LT}(G_b)\rangle \overset{\boxed{G_b \text{ は Groebner}}}{=} \langle \mathrm{LT}(\langle G_b\rangle)\rangle = \langle \mathrm{LT}(\langle G_a\rangle)\rangle \tag{282}$$

なので、$G_a$ も Groebner 基底である。

次に、どの時点でも $G$ が極小 Groebner 基底であることを示す。極小 Groebner 基底であることの定義は、「どの基底 $f_i$ についても、$\mathrm{LT}(f_i) \notin \langle G \setminus \{\mathrm{LT}(f_i)\}\rangle$ となる」ことである。しかし、先に「どの時点でも $\mathrm{LT}(G)$ が一定である」ことを示したので、即座に従う。

次に、L.2,L.5 時点で $G[1], \dots, G[i]$ は $G$ について簡約されていることを示す。「$f$ が $G$ について簡約されている」とは、「$f$ のどの項も $\mathrm{LT}(G - \{f\})$ で割り切れない」言い換えるなら、「$\forall x^\alpha$: $f$の項: $x^\alpha \notin \langle \mathrm{LT}(G - \{f\})\rangle$」となることであった。L.2 の時点では $i = 0$ なので自明である。L.5 を考える。帰納法の仮定より、$G_b[1], \dots, G_b[i-1]$ は $G$ について簡約されている。先に、「どの時点でも $\mathrm{LT}(G)$ は一定」であることを示したので、$G_a[1], \dots, G_a[i-1]$ も $G$ について簡約されている。あとは、$G_a[i] = \overline{f_i}^{G-\{f_i\}}$ が $G$ について簡約されていることを示せばよい。しかし、割り算の余りの定義より、$\overline{f_i}^{G-\{f_i\}}$ のすべての項は $G - \{f_i\}$ で一度も割ることができない。

L.5 の時点で「$G[1], \dots, G[i]$ は $G$ について簡約されている」ことを示したので、アルゴリズムが停止したとき、すなわち $i = n$ となったときは $G[1], \dots, G[n]$ は $G$ について簡約されている。よって、$G$ は簡約 Groebner 基底である。前半は示せた。

後半の、簡約 Groebner 基底の一意性を示す。$G, G'$ がイデアル $I$ の簡約 Groebner 基底であるとする。

まず、$\mathrm{LT}(G) = \mathrm{LT}(G')$ であることを示す。$G = \{g_1, \dots, g_s\}$ とし、$G' = \{g'_1, \dots, g'_t\}$ とする。$G, G'$ が Groebner 基底なので、$\langle \mathrm{LT}(g_1), \dots, \mathrm{LT}(g_s)\rangle = \langle \mathrm{LT}(g'_1), \dots, \mathrm{LT}(g'_t)\rangle$ である。$i = 1, \dots, s$ とする。$\mathrm{LT}(g_i) \in \langle \mathrm{LT}(g'_1, \dots, \mathrm{LT}(g'_t))\rangle$ であり、単項式イデアルの性質より、$F(i) \in \{1, \dots, t\}$ が存在して、$\mathrm{LT}(g'_{F(i)})|\mathrm{LT}(g_i)$ となる。さらに同様の考察を $\mathrm{LT}(g'_{F(i)})$ にして、$G(i) \in \{1, \dots, s\}$ が存在して、$\mathrm{LT}(g_{G(i)})|\mathrm{LT}(g'_{F(i)})$ となることがわかる。まとめると、$\mathrm{LT}(g_{G(i)})|\mathrm{LT}(g'_{F(i)})|\mathrm{LT}(g_i)$ となる。仮に $G(i) \neq i$ であるとすると、$\mathrm{LT}(g_{G(i)})|\mathrm{LT}(g_i)$ となり、これは $G$ が極小であることに反する。よって、$G(i) = i$ である。すると、$\mathrm{LT}(g_i)|\mathrm{LT}(g'_{F(i)})|\mathrm{LT}(g_i)$ となるので、$\mathrm{LT}(g'_{F(i)}) = \mathrm{LT}(g_i)$ である。$i \neq j$ なら $G$ の極小性から $\mathrm{LT}(g_i) \neq \mathrm{LT}(g_j)$ であり、よって $\mathrm{LT}(g'_{F(i)}) \neq \mathrm{LT}(g'_{F(j)})$ であり、極小性より再び $F(i) \neq F(j)$ となる。よって、$F$ は単射であり、$\#G \leq \#G'$ となる。同様の考察をすると $\#G' \leq \#G$ となり、$s = \#G = \#G' = t$ となる。$F$ が同じ大きさの有限集合間の単射なので、これは全射でもあり、$F$ が $G$ と $G'$ との間に全単射をつけ、$\mathrm{LT}(g_i) = \mathrm{LT}(g'_{F(i)})$ とする。これで、$\mathrm{LT}(G) = \mathrm{LT}(G')$ が示された。

次に、$G = G'$ を示す。対称性から、$g \in G$ として $g \in G'$ が示せればよい。さきに示したことより、$\mathrm{LT}(G) = \mathrm{LT}(G')$ なので、$\mathrm{LT}(g) = \mathrm{LT}(g')$ となる $g' \in G'$ が存在する。もしも $g = g'$ であれば $g = g' \in G'$ となるので証明がおわる。$g = g'$ を示す。$G, G'$ は $I$ の Groebner 基底なので、$I = \langle G\rangle = \langle G'\rangle$ であり、$\underbrace{g}_{\in G} - \underbrace{g'}_{\in G'} \in I$ なので、$\overline{g - g'}^{G} = \overline{g - g'}^{I} = 0$ となる[*9]。

一方、実は $\overline{g - g'}^{G} = g - g'$ となる。まず、$G$ は簡約 Groebner 基底なので、$g$ の各項は $G - \{g\}$ のいずれでも一度も割れず、$\overline{g - \mathrm{LT}(g)}^{G-\{g\}} = g - \mathrm{LT}(g)$ である。さらに、$g - \mathrm{LT}(g)$ の各項が $g$ で一度も割れないのも明らかなので、$\overline{g - \mathrm{LT}(g)}^{\{g\}} = g - \mathrm{LT}(g)$ でもあり、$\overline{g - \mathrm{LT}(g)}^{I}\overline{g - \mathrm{LT}(g)}^{G} = g - \mathrm{LT}(g)$ となる。同様の考察を $g'$ にもして、

[*8] 余りが $f_i$ になるわけではない。初手では割り算がおこらないかもしれないが、2 手め以降ならわからない。

[*9] イデアルでの割り算は先の演習でやった。

$\overline{g' - \mathrm{LT}(g')}^I = g' - \mathrm{LT}(g')$ となる。先の演習問題から、あまりはたしひきできるので、

$$\overline{g - g'}^I \overset{\boxed{LT(g)=LT(g')}}{=} \overline{(g - \mathrm{LT}(g)) - (g' - \mathrm{LT}(g'))}^I \tag{283}$$
$$= \overline{g - \mathrm{LT}(g)}^I - \overline{g' - \mathrm{LT}(g')}^I \tag{284}$$
$$= (g - \mathrm{LT}(g)) - (g' - \mathrm{LT}(g')) \tag{285}$$
$$\overset{\boxed{LT(g)=LT(g')}}{=} g - g' \tag{286}$$

となる。

以上で、$\overline{g - g'}^I = 0$ と $\overline{g - g'}^I = g - g'$ とを示したので、$g - g' = 0$ となり、$g = g'$ である。よって、$g \in G'$ であり、$G \subset G'$ となる。同様に $G' \subset G$ も成立し、$G = G'$ である。

(証終)

これで、多項式のイデアルから、それを特徴づける一意なデータが引き出せることがわかった。つまり、ある 2 つの有限生成なイデアル $I, J$ があれば、その簡約 Groebner 基底を計算し、あっていれば $I = J$ だし、あっていなければ $I \neq J$ である。

(問題 1) 略

(問題 2) `code/ex_2_3_7.hs` で計算。

(a) lex だと以下の通り。

Calculates groebner basis of
- $x^2y + (-1)$
- $xy^2 + (-1)x$

.
$\overline{S(x^2y + (-1), xy^2 + (-1)x)} = x^2 + (-1)y.$
Not enough. Appends
- $x^2 + (-1)y$

.
$\overline{S(x^2y + (-1), x^2 + (-1)y)} = y^2 + (-1).$
$\overline{S(xy^2 + (-1)x, x^2 + (-1)y)} = y^3 + (-1)y.$
Not enough. Appends
- $y^2 + (-1)$

.
$\overline{S(x^2y + (-1), y^2 + (-1))} = 0.$
$\overline{S(xy^2 + (-1)x, y^2 + (-1))} = 0.$
$\overline{S(x^2 + (-1)y, y^2 + (-1))} = 0.$
Enough for groebner basis. Result is
- $x^2y + (-1)$
- $xy^2 + (-1)x$
- $x^2 + (-1)y$
- $y^2 + (-1)$

. ■ Minimalizes groebner basis
- $x^2y + (-1)$
- $xy^2 + (-1)x$
- $x^2 + (-1)y$
- $y^2 + (-1)$

.
$x^2y + (-1)$ is removed by $x^2 + (-1)y$.
$xy^2 + (-1)x$ is removed by $y^2 + (-1)$.
Minimalized groebner basis is
- $x^2 + (-1)y$
- $y^2 + (-1)$

. ■
Reduce groebner basis
- $x^2 + (-1)y$
- $y^2 + (-1)$

.
Reducing: $\overline{x^2 + (-1)y} = x^2 + (-1)y.$
Reducing: $\overline{y^2 + (-1)} = y^2 + (-1).$
Reduced groebner basis is
- $y^2 + (-1)$
- $x^2 + (-1)y$

. ■

grLex だと、

Calculates groebner basis of
- $x^2y + (-1)$
- $xy^2 + (-1)x$

.
$\overline{S(x^2y + (-1), xy^2 + (-1)x)} = x^2 + (-1)y.$
Not enough. Appends
- $x^2 + (-1)y$

.
$\overline{S(x^2y + (-1), x^2 + (-1)y)} = y^2 + (-1).$
$\overline{S(xy^2 + (-1)x, x^2 + (-1)y)} = y^3 + (-1)y.$
Not enough. Appends
- $y^2 + (-1)$

.
$\overline{S(x^2y+(-1),y^2+(-1))}=0$.
$\overline{S(xy^2+(-1)x,y^2+(-1))}=0$.
$\overline{S(x^2+(-1)y,y^2+(-1))}=0$.
Enough for groebner basis. Result is
- $x^2y+(-1)$
- $xy^2+(-1)x$
- $x^2+(-1)y$
- $y^2+(-1)$

. ■ Minimalizes groebner basis
- $x^2y+(-1)$
- $xy^2+(-1)x$
- $x^2+(-1)y$
- $y^2+(-1)$

.
$x^2y+(-1)$ is removed by $x^2+(-1)y$.
$xy^2+(-1)x$ is removed by $y^2+(-1)$.
Minimalized groebner basis is
- $x^2+(-1)y$
- $y^2+(-1)$

. ■
Reduce groebner basis
- $x^2+(-1)y$
- $y^2+(-1)$

.
Reducing: $\overline{x^2+(-1)y}=x^2+(-1)y$.
Reducing: $\overline{y^2+(-1)}=y^2+(-1)$.
Reduced groebner basis is
- $y^2+(-1)$
- $x^2+(-1)y$

. ■

となる。

(b) lex だと以下の通り。

Calculates groebner basis of
- $x^2+y$
- $x^4+2x^2y+y^2+3y$

.
$\overline{S(x^2+y,x^4+2x^2y+y^2+3y)}=(-3)y$.
Not enough. Appends
- $(-3)y$

.
$\overline{S(x^2+y,(-3)y)}=0$.
$\overline{S(x^4+2x^2y+y^2+3y,(-3)y)}=0$.
Enough for groebner basis. Result is
- $x^2+y$
- $x^4+2x^2y+y^2+3y$
- $(-3)y$

. ■ Minimalizes groebner basis
- $x^2+y$
- $x^4+2x^2y+y^2+3y$
- $(-3)y$

.
$x^4+2x^2y+y^2+3y$ is removed by $x^2+y$.
Minimalized groebner basis is
- $x^2+y$
- $y$

. ■
Reduce groebner basis
- $x^2+y$
- $y$

.
Reducing: $\overline{x^2+y}=x^2$.
Reducing: $\overline{y}=y$.
Reduced groebner basis is
- $y$
- $x^2$

. ■

grlex だと以下の通り。

Calculates groebner basis of
- $x^2+y$
- $x^4+2x^2y+y^2+3y$

.
$\overline{S(x^2+y,x^4+2x^2y+y^2+3y)}=(-3)y$.
Not enough. Appends
- $(-3)y$

.
$\overline{S(x^2+y,(-3)y)}=0$.
$\overline{S(x^4+2x^2y+y^2+3y,(-3)y)}=0$.
Enough for groebner basis. Result is
- $x^2+y$
- $x^4+2x^2y+y^2+3y$
- $(-3)y$

. ■ Minimalizes groebner basis
- $x^2+y$
- $x^4+2x^2y+y^2+3y$
- $(-3)y$

.
$x^4+2x^2y+y^2+3y$ is removed by $x^2+y$.
Minimalized groebner basis is
- $x^2+y$
- $y$

. ■
Reduce groebner basis
- $x^2+y$

- $y$

.
Reducing: $\overline{x^2+y} = x^2$.
Reducing: $\overline{y} = y$.

よって、多様体は $\mathbf{V}(I) = 0$ となる。

(c) lex だと以下のとおり。

Calculates groebner basis of
- $x + (-1)z^4$
- $y + (-1)z^5$

.
$\overline{S(x + (-1)z^4, y + (-1)z^5)} = 0$.
Enough for groebner basis. Result is
- $x + (-1)z^4$
- $y + (-1)z^5$

. ■ Minimalizes groebner basis
- $x + (-1)z^4$
- $y + (-1)z^5$

.
Minimalized groebner basis is
- $x + (-1)z^4$
- $y + (-1)z^5$

. ■
Reduce groebner basis
- $x + (-1)z^4$
- $y + (-1)z^5$

.
Reducing: $\overline{x + (-1)z^4} = x + (-1)z^4$.
Reducing: $\overline{y + (-1)z^5} = y + (-1)z^5$.
Reduced groebner basis is
- $y + (-1)z^5$
- $x + (-1)z^4$

. ■

grlex だと以下のとおり。

Calculates groebner basis of
- $(-1)z^4 + x$
- $(-1)z^5 + y$

.
$\overline{S((-1)z^4 + x, (-1)z^5 + y)} = (-1)xz + y$.
Not enough. Appends
- $(-1)xz + y$

.
$\overline{S((-1)z^4 + x, (-1)xz + y)} = yz^3 + (-1)x^2$.
$\overline{S((-1)z^5 + y, (-1)xz + y)} = 0$.
Not enough. Appends
- $yz^3 + (-1)x^2$

.
$\overline{S((-1)z^4 + x, yz^3 + (-1)x^2)} = 0$.
$\overline{S((-1)z^5 + y, yz^3 + (-1)x^2)} = 0$.
$\overline{S((-1)xz + y, yz^3 + (-1)x^2)} = (-1)y^2z^2 + x^3$.
Not enough. Appends
- $(-1)y^2z^2 + x^3$

.
$\overline{S((-1)z^4 + x, (-1)y^2z^2 + x^3)} = 0$.
$\overline{S((-1)z^5 + y, (-1)y^2z^2 + x^3)} = 0$.
$\overline{S((-1)xz + y, (-1)y^2z^2 + x^3)} = x^4 + (-1)y^3z$.
$\overline{S(yz^3 + (-1)x^2, (-1)y^2z^2 + x^3)} = 0$.
Not enough. Appends
- $x^4 + (-1)y^3z$

.
$\overline{S((-1)z^4 + x, x^4 + (-1)y^3z)} = 0$.
$\overline{S((-1)z^5 + y, x^4 + (-1)y^3z)} = 0$.
$\overline{S((-1)xz + y, x^4 + (-1)y^3z)} = 0$.
$\overline{S(yz^3 + (-1)x^2, x^4 + (-1)y^3z)} = 0$.
$\overline{S((-1)y^2z^2 + x^3, x^4 + (-1)y^3z)} = 0$.
Enough for groebner basis. Result is
- $(-1)z^4 + x$
- $(-1)z^5 + y$
- $(-1)xz + y$
- $yz^3 + (-1)x^2$
- $(-1)y^2z^2 + x^3$
- $x^4 + (-1)y^3z$

. ■ Minimalizes groebner basis
- $(-1)z^4 + x$
- $(-1)z^5 + y$
- $(-1)xz + y$
- $yz^3 + (-1)x^2$
- $(-1)y^2z^2 + x^3$
- $x^4 + (-1)y^3z$

.
$(-1)z^5 + y$ is removed by $(-1)z^4 + x$.
Minimalized groebner basis is
- $z^4 + (-1)x$
- $xz + (-1)y$
- $yz^3 + (-1)x^2$
- $y^2z^2 + (-1)x^3$
- $x^4 + (-1)y^3z$

. ■
Reduce groebner basis
- $z^4 + (-1)x$
- $xz + (-1)y$
- $yz^3 + (-1)x^2$

- $y^2z^2 + (-1)x^3$
- $x^4 + (-1)y^3z$

.

Reducing: $\overline{z^4 + (-1)x} = z^4 + (-1)x$.
Reducing: $\overline{xz + (-1)y} = xz + (-1)y$.
Reducing: $\overline{yz^3 + (-1)x^2} = yz^3 + (-1)x^2$.
Reducing: $\overline{y^2z^2 + (-1)x^3} = y^2z^2 + (-1)x^3$.
Reducing: $\overline{x^4 + (-1)y^3z} = x^4 + (-1)y^3z$.

Reduced groebner basis is

- $x^4 + (-1)y^3z$
- $y^2z^2 + (-1)x^3$
- $yz^3 + (-1)x^2$
- $xz + (-1)y$
- $z^4 + (-1)x$

. ■

(問題 3) 2 でやった。

(問題 4) 途中までは一緒。アルゴリズムが停止しなかったとする (背理法)。すると、終了条件から狭義単調増加な $G$ の列

$$G = G_0 \subsetneq G_1 \subsetneq G_2 \subsetneq \dots \tag{287}$$

が存在する。L.4 で、余りが 0 にならなかったときを追加していることから、$G_{i+1}$ で $G_i$ から追加された元の LT は、$G_i$ のどの LT でも割り切ることができない。よって、

$$\langle \mathrm{LT}(G)\rangle = \langle \mathrm{LT}(G_0)\rangle \subsetneq \langle \mathrm{LT}(G_1)\rangle \subsetneq \langle \mathrm{LT}(G_2)\rangle \subsetneq \dots \tag{288}$$

となっている。ここからがちがう！ $A = \bigcup_{i=0}^{\infty} \mathrm{LT}(G_i)$ を考える。これは $\mathbb{Z}^n_{\geq 0}$ の部分集合なので、演習問題 2-4-7 の、ディクソンの補題の変種より、$\alpha_1, \dots, \alpha_N \in A$ が存在して、

$$^{\forall}\alpha \in A\colon {}^{\exists}i = 1, \dots, N\colon {}^{\exists}\gamma \in \mathbb{Z}^n_{\geq 0}\colon \alpha = \alpha_i + \gamma \tag{289}$$

となる。各 $i$ とそれに付随する $\alpha_i$ について、「$x^{\alpha_i} \notin \left\langle \mathrm{LT}(G_{M(i)-1})\right\rangle$ かつ $x^{\alpha_i} \in \left\langle \mathrm{LT}(G_{M(i)})\right\rangle$」となる $G(i)$ が存在するので、そのようなものを選んでおく。ただし、$\mathrm{LT}(G_{-1}) = \emptyset$ としておく。$M = \max M(1), \dots, M(N)$ とする。$x^\beta \in \langle \mathrm{LT}(G_{M+1})\rangle \setminus \langle \mathrm{LT}(G_M)\rangle$ とする (真の上昇列であることから空でなく、元が選べる)。ディクソンの補題の変種からの帰結 (289) より、

$$\beta = \alpha_i + \gamma \tag{290}$$

となる $i, \alpha_i, \gamma$ が存在する。これは、$x^{\alpha_i} | x^\beta$ を意味するが、$x^{\alpha_i} \in \left\langle \mathrm{LT}(G_{M(i)})\right\rangle$ だったので、$x^\beta \in \left\langle \mathrm{LT}(G_{M(i)})\right\rangle$ となる。しかし、$x^\beta \notin \langle \mathrm{LT}(G_M)\rangle$ と $\beta$ を選んであり、さらに $\left\langle \mathrm{LT}(G_{M(i)})\right\rangle \subset \langle \mathrm{LT}(G_M)\rangle$ なので、$x^\beta \notin \left\langle \mathrm{LT}(G_{M(i)})\right\rangle$ となる。これは矛盾である。

(問題 5)

TODO: 残りをとく

## 2.8 グレブナ基底の最初の応用

グレブナ基底を計算し、それで割り算して余りを見ることでイデアルの所属問題は完全に解くことができる。

次回予告。lex 順序を使って簡約 Groebner 基底を計算することで変数の消去がうまくおこって、多様体の記述 (あるいは連立方程式を解くこと) の問題、陰関数表示の問題はうまく解けそうなことを例を使ってみた。

## 2.9 (選択) ブッフベルガーのアルゴリズムの改良

ブッフベルガーのアルゴリズムの高速化を考える。基本的に、割り算の計算コストが高いので、割り算をしなくてすむときにしないようにすることで高速化する。

まず、「余りが 0 である」ことを一般化して、次のものをいれる。「$G = \{g_1, \dots, g_s\} \subset k[x_1, \dots, x_n]$ と $f \in k[x_1, \dots, x_n]$ について、『$f \to_G 0$』『$f$ は $G$ を法として 0 に簡約される』とは、$a_i g_i \neq 0 \implies \deg(a_i g_i) \leq \deg(f)$ となる $a_\bullet \in k[x_1, \dots, x_n]$ が存在し、

$$f = \sum_{i=1}^{s} a_i f_i \tag{291}$$

となる」ことである。

あたりまえだが、$f$ を $(g_1, \ldots, g_s)$ で割り算して 0 のとき、すなわち $\overline{f}^G = 0$ には $f \to_G 0$ となる。まえの割り算の順序の議論より、割り算して 0 にならなかったからといって $f \to_G 0$ とならないとは言えない。

グレブナ基底と S 多項式の余りとの関係を見たが、これをグレブナ基底と S 多項式の 0 への簡約を見る。「$\{g_1, \ldots, g_s\}$ がグレブナ基底である $\iff$ $i \neq j$ について、$S(g_i, g_j) \to_G 0$」

証明

- $\Rightarrow$: 先の「グレブナ基底と S 多項式の余りとの関係」より、$\overline{S(g_i, g_j)}^G = 0$ となり、あきらかに $S(g_i, g_j) \to_G 0$ である。
- $\Leftarrow$: 復習することになる。$f \in \langle G \rangle$ とする。このとき、$\mathrm{LT}(f) \in \langle \mathrm{LT}(G) \rangle$ となることを示せばよい。$f \in \langle G \rangle$ であるから $f = \sum_{i=1}^s h_i g_i$ となる $h_\bullet \in k[x_1, \ldots, x_n]$ が存在する。和のほうが次数が下がるかもしれないので、$\deg(f) \leq \deg(h_\bullet g_\bullet)$ となる。打ち消しの雰囲気を見るために、$m\colon \{1, \ldots, s\} \to \mathbb{Z}^n_{\geq 0}$ を $m(i) = \deg(h_i g_i)$ と定義する。そして、$m'\colon (g_\bullet$の線形結合の表現$) \to \mathbb{Z}^n_{\geq 0}$ を、

$$m'(\sum_{i=1}^s a_i g_i) = \max\{\deg(a_i g_i); i = 1, \ldots, s\} \tag{292}$$

と定義する。ただし、$\deg(0) = -\infty$ としておき、$-\infty$ は $\mathbb{Z}^n_{\geq 0}$ のどれよりも小さいということにする。そして、$\delta = m'(\sum_{i=1}^s h_i g_i)$ とする。ここで、deg と和の関係 (和を取ったら次数が落ちうる) より、$\delta \geq \deg(f)$ である。$f = \sum_{i=1}^s h_i g_i$ という $f$ の表現のうち、$h_\bullet$ を走らせて $m'$ が最小となるようなものがあるはずなので、$h_\bullet$ をそのように選びなおしておく。

$\delta \geq \deg(f)$ であったが、仮に $\delta > \deg(f)$ であるとする (背理法)。

$$f = \sum_{m(i)=\delta} \mathrm{LT}(h_i) g_i + \sum_{m(i)=\delta} (h_i - \mathrm{LT}(h_i)) g_i + \sum_{m(i)<\delta} h_i g_i \tag{293}$$

$\delta > \deg(f)$ だったので、$\sum_{m(i)=\delta} h_i g_i$ の先頭項が落ちなければならない。

これから $\sum_{m(i)=\delta} h_i g_i$ を別の表現にして、$m'(f) < \delta$ となってしまう (矛盾)$f$ の表現を作ることを目指す。「同次のものを足して次数が落ちた」ので、$S$ 多項式の和で書ける。さらに計算して、

$$\begin{aligned}
\sum_{m(i)=\delta} \mathrm{LT}(h_i) g_i &= \sum_{j,k=1}^s S(\mathrm{LT}(h_j) g_j, \mathrm{LT}(h_k) g_k) && (294)\\
&= \sum_{j,k=1}^s \frac{(\mathrm{LT}(h_j) g_j) \vee (\mathrm{LT}(h_k) g_k)}{\mathrm{LT}(h_j)\mathrm{LT}(g_j)} \mathrm{LT}(h_j) g_j - \frac{(\mathrm{LT}(h_j) g_j) \vee (\mathrm{LT}(h_k) g_k)}{\mathrm{LT}(h_k)\mathrm{LT}(g_k)} \mathrm{LT}(h_k) g_k && (295)\\
&= \sum_{j,k=1}^s \frac{(\mathrm{LT}(h_j) g_j) \vee (\mathrm{LT}(h_k) g_k)}{\mathrm{LT}(g_j)} g_j - \frac{(\mathrm{LT}(h_j) g_j) \vee (\mathrm{LT}(h_k) g_k)}{\mathrm{LT}(g_k)} \mathrm{LT}(h_k) g_k && (296)\\
&= \sum_{j,k=1}^s (\mathrm{LT}(h_j) g_j) \vee (\mathrm{LT}(h_k) g_k) \cdot \frac{1}{g_j \vee g_k} S(g_j, g_k) && (297)
\end{aligned}$$

となる。各 $j, k$ について、今回の仮定 $S(g_j, g_k) \to_G 0$ より、

$$S(g_j, g_k) = \sum_{i=1}^s a_{ijk} g_i, \quad \deg(S(g_j, g_k)) \geq \deg(a_{\bullet jk} g_\bullet) \tag{298}$$

となる $a_\bullet \in k[x_1, \ldots, x_n]$ が存在する。よって、

$$\sum_{m(i)=\delta} \mathrm{LT}(h_i) g_i = \sum_{i,j,k=1}^s \frac{(\mathrm{LT}(h_j) g_j) \vee (\mathrm{LT}(h_k) g_k)}{g_j \vee g_k} a_{ijk} g_i. \tag{299}$$

となる。これで $f$ の新たな表現

$$f = \sum_{m(i)=\delta} \sum_{i,j,k=1}^s \frac{(\mathrm{LT}(h_j) g_j) \vee (\mathrm{LT}(h_k) g_k)}{g_j \vee g_k} a_{ijk} g_i + \sum_{m(i)=\delta} (h_i - \mathrm{LT}(h_i)) g_i + \sum_{m(i)<\delta} h_i g_i \tag{300}$$

が得られた。これの $m'$ を計算する。まず第 1 の総和を計算する。

$$m'(\text{新しい表現の第1の総和}) = m'(\sum_{m(i)=\delta}\sum_{i,j,k=1}^{s}\frac{(\mathrm{LT}(h_j)g_j)\vee(\mathrm{LT}(h_k)g_k)}{g_j\vee g_k}a_{ijk}g_i) \tag{301}$$

$$\boxed{\text{足し算をしたほうが小さくなる}} \tag{302}$$

$$= \max_{i,j,k}\deg(\frac{(\mathrm{LT}(h_j)g_j)\vee(\mathrm{LT}(h_k)g_k)}{g_j\vee g_k}a_{ijk}g_i) \tag{303}$$

$$\boxed{\text{足し算したほうが小さくなる}} \tag{304}$$

$$= \max_{j,k}\deg(\frac{(\mathrm{LT}(h_j)g_j)\vee(\mathrm{LT}(h_k)g_k)}{g_j\vee g_k}S(g_j,g_k)) \tag{305}$$

$$\boxed{\text{S 多項式の計算}} \tag{306}$$

$$= \max_{j,k}\deg(S(\mathrm{LT}(h_j)g_j,\mathrm{LT}(h_k)g_k) \tag{307}$$

$$\boxed{\text{同次を足したら次数が真に落ちて S 多項式で書ける}} \tag{308}$$

$$< \deg(\sum_{m(i)=\delta}\mathrm{LT}(h_i)g_i) \tag{309}$$

$$= \delta. \tag{310}$$

第 2 の総和、第 3 の総和はそもそも $m'$ は $\delta$ 未満なので、結局

$$m'(\text{新しい表現}) < \delta \tag{311}$$

となる。$\delta = m'(\sum_{i=1}^{s}h_ig_i)$ で、$h_\bullet$ は $m'$ が最小になるように選んでおいたので、$m'(\text{新しい表現}) < \delta$ に矛盾する。よって、$m'(\text{新しい表現}) = \delta$ となる。
ということで、$f = \sum_{i=1}^{s}h_ig_i$ を $m'$ が最小になるように表示すると、

$$\deg(f) \overset{\boxed{\text{さっきの}}}{=} \delta = m'(\sum_{i=1}^{s}h_ig_i) \overset{\boxed{m'\text{ の定義}}}{=} \max_i\deg(h_ig_i) \tag{312}$$

この最大を与える $i$ を $I$ とよぶことにする。このとき、$\mathrm{LT}(g_i)|\mathrm{LT}(f)$ となる。よって、$\mathrm{LT}(f)\in\langle\mathrm{LT}(G)\rangle$ となり、$\mathrm{LT}(\langle G\rangle)\subset\langle\mathrm{LT}(G)\rangle$ となり、よって、$\langle\mathrm{LT}(\langle G\rangle)\rangle\subset\langle\mathrm{LT}(G)\rangle$ となる。よって、$G$ はグレブナ基底である。

(証終)

割り算することなく $S(f,g)\to_G 0$ かどうかを判定する方法の 1 つを見る。「$\mathrm{LM}(f)$ と $\mathrm{LM}(g)$ が互いに素ならば、$S(f,g)\to_G 0$ である。」

証明

$$S(f,g) \overset{\boxed{\text{互いに素}}}{=} \mathrm{LT}(g)f - \mathrm{LT}(f)g \tag{313}$$

$$= \mathrm{LT}(g)(\mathrm{LT}(f)+(f-\mathrm{LT}(f))) - \mathrm{LT}(f)(\mathrm{LT}(g)+(g-\mathrm{LT}(g))) \tag{314}$$

$$= \mathrm{LT}(g)(f-\mathrm{LT}(f)) - \mathrm{LT}(f)(g-\mathrm{LT}(g)). \tag{315}$$

よって、

$$\deg(S(f,g)) \le \max(\mathrm{LT}(g)(f-\mathrm{LT}(f)),\mathrm{LT}(f)(g-\mathrm{LT}(g))) \tag{316}$$

となっている。実際には等号が成立していることを見る。仮に $<$ だとする。このとき、先頭項の打ち消しが起こらなくてはならないから、$\mathrm{LT}(g)\mathrm{LT}(f-\mathrm{LT}(f)) = \mathrm{LT}(f)\mathrm{LT}(g-\mathrm{LT}(g))$ となっている。$\mathrm{LT}(g)$ と $\mathrm{LT}(f)$ は互いに素なので、$\mathrm{LT}(g)|\mathrm{LT}(g-\mathrm{LT}(g))$ とならなければならないが、これは矛盾である。よって、

$$\deg(S(f,g)) = \max(\mathrm{LT}(g)(f-\mathrm{LT}(f)),\mathrm{LT}(f)(g-\mathrm{LT}(g))) \tag{317}$$

となっている。これで、$S(f,g)$ が $f,g$ の線形結合で書けた上に、次数の条件が満たされ、$S(f,g)\to_G 0$ となる。

(証終)

次に、$S$ 多項式の一般化を考える。$F = \{f_1, \ldots, f_s\}$ とする。「$F$ の先頭項のシチギー」あるいは「$\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)$ のシチギー」とは、

$$(h_1, \ldots, h_s) \begin{pmatrix} \mathrm{LT}(f_1) \\ \vdots \\ \mathrm{LT}(f_s) \end{pmatrix} = 0 \tag{318}$$

を満たす多項式の組 $(h_1, \ldots, h_s) \in (k[x_1, \ldots, x_n])^s$ のことである。そして、$S(F) \subset (k[x_1, \ldots, x_n])^s$ を $F$ の先頭項のシチギー全体のなす集合とする。これは $k[x_1, \ldots, x_n]$ の一次方程式の自明でない解集合と考えるとよいかもしれない。

シチギーと S 多項式との関係を見る。$F = \{f_1, \ldots, f_s\}$ について、

$$S_{ij} = \frac{f_i \vee f_j}{\mathrm{LT}(f_i)} \mathbb{e}_i - \frac{f_i \vee f_j}{\mathrm{LT}(f_j)} \mathbb{e}_j \tag{319}$$

と $S_{ij} \in S(F)$ を定義する。そうしておくと、

$$S(f_i, f_j) = S_{ij} \begin{pmatrix} 0 \\ \vdots \\ f_i \\ \vdots \\ f_j \\ \vdots \\ 0 \end{pmatrix} = S_{ij}(f_i \mathbb{e}_i^T + f_j \mathbb{e}_j^T) \tag{320}$$

となっている。

分解の基本になる特殊なシチギーを定義する。あるシチギー $S \in S(F)$ が多重次数 $\alpha$ 次斉次であるとは、

- $S = (c_1 x^{\alpha(1)}, \ldots, c_s x^{\alpha(s)})$
- $c_i \neq 0 \implies \alpha(i) + \deg(f_i) = \alpha$

であることである。雑に言うと、単項式だけでできたシチギー $S$ で、どの第 $i$ 項も $f_i$ の次数を足すと $\alpha$ になるようなものである。一般のシチギーはそもそも単項式ですらない。

$S(F)$ のすべての元 (シチギー) は $S(F)$ の斉次な元の和に一意的に分解できる。

証明

$S \in S(F)$ とする。これを分解する。単位ベクトルで $S = \sum_{i=1}^{s} f_i \mathbb{e}_i$ と書ける。$f_i = \sum_{j=1}^{N(i)} c_{ij} x^{\alpha(i,j)}$ となる $N(i) = 0, 1, \ldots$ と $c_{ij} \in k$ と $\alpha(i,j) \in \mathbb{Z}_{\geq 0}^n$ が一意的に存在する。それで、

$$S = \sum_{i=1}^{s} \mathbb{e}_i \sum_{j=1}^{N(i)} c_{ij} x^{\alpha(i,j)} \tag{321}$$

となる。

一意性は、「$i$ 番目 $\alpha$ 次の係数」というのが一意に定まってしまうので明らか。

(証終)

$F = (f_1, \ldots, f_s)$ として、先の $S_{ij}$ でシチギー全体 $S(F)$ を生成することができる。「$F = (f_1, \ldots, f_s)$ とする。すべてのシチギー $S \in S(F)$ には

$$S = \sum_{i<j} u_{ij} S_{ij} \tag{322}$$

となる $u_{ij} \in k[x_1, ;x_n]$ が存在する。$S_{ij} = \frac{f_i \vee f_j}{\mathrm{LT}(f_i)} \mathbb{e}_i - \frac{f_i \vee f_j}{\mathrm{LT}(f_j)} \mathbb{e}_j$ であった。」

証明
まず $S$ が $\alpha$ 次斉次であるとする。シチギーの定義を考えると、$S$ のうち非 0 な要素が 2 つ以上なければならない。それらが $i$ 番目と $j$ 番目 $(i<j)$ であるとし、$S[i]=c_i x^{\alpha(i)}$, $S[j]=c_j x^{\alpha(j)}$ とする。$S$ は $F$ のシチギーなので、$SF=0$ である。ここで、$S' \in (k[x_1,\dots,x_n])^s$ を、$i$ 番目を 0 にするように

$$S' = S - \underbrace{S_{ij}\frac{\mathrm{LT}(f_i)}{f_i \vee f_j}}_{\text{係数1}} S[i] \tag{323}$$

$$= S - S_{ij}\frac{\mathrm{LT}(f_i)}{f_i \vee f_j} c_i x^{\alpha(i)} \tag{324}$$

$$\tag{325}$$

と定義する。どちらもシチギーであって、$SF=0$ と $S_{ij}F=0$ がなりたつので、線形性より $S'F=0$ となる。よって、$S'$ もシチギーである。このシチギーにも同様の操作を繰り返して、0 にたっする。このとき、$S$ は $S_{ij} \quad (i<j)$ の線形結合でかける。

あとは斉次を $S_{ij}$ で書いたものを足せばよい。

(証終)

ただし、$F$ に対して $S_{ij}$ すべてが必要とは限らないので、余分なものを取り除く方法を考える。

これで、グレブナ基底の判定条件を $\to_G 0$ を使って拡張する。「イデアル $I$ の基底 $G=(g_1,\dots,g_t)$ がグレブナ基底である $\iff$

$$^{\exists} S_1,\dots,S_m \text{は} S(G) \text{の斉次な基底:}\ ^{\forall} i=1,\dots,m\colon S_i G \to_G 0. \tag{326}$$

」

証明

- $\Rightarrow$:$S(G)$ の斉次な基底として $S_{ij}$ 全体をとっておく。すると、$S_{ij}G \to_G 0$ を確かめればよいが、これは $\overline{S(g_i,g_j)}^{G}=0$ を示せばよく、これは先の S 多項式とグレブナ基底の関係である。
- $\Leftarrow$: $f \in I$ とする。$\mathrm{LT}(f) \in \langle \mathrm{LT}(G)\rangle$ を示せばグレブナ基底であることが示せる。$f \in I = \langle G\rangle$ なので、$f=\sum_{i=1}^{t} h_i g_i$ となる $h_\bullet \in k[x_1,\dots,x_n]$ が存在する。$m\colon \{1,\dots,t\} \to \mathbb{Z}^n_{\geq 0}$ を $m(i)=\deg(h_i g_i)$ とする。そして、$m'\colon (g_\bullet\text{の線形結合の表現}) \to \mathbb{Z}^n_{\geq 0}$ を

  $$m'(\sum_{i=1}^{t} a_i g_i) = \max_{i=1,\dots,t} \deg(a_i g_i) \tag{327}$$

  と定義する。そして、$\delta = m'(\sum_{i=1}^{t} h_i g_i)$ とする。$\delta$ が最小になるように $h_\bullet$ 選んでおくことができるので、そうしておく。$f=\sum_{i=1}^{t} h_i g_i$ だったので、$\deg(f) \leq \delta$ である。ここで、仮に $\deg(f)<\delta$ だったとして矛盾を導こう。

  $$f = \sum_{m(i)=\delta} \mathrm{LT}(h_i) g_i + \sum_{m(i)=\delta} (h_i - \mathrm{LT}(h_i)) g_i + \sum_{m(i)<\delta} h_i g_i \tag{328}$$

  と書ける。$\deg(f)<\delta$ と仮定したので、第 1 の総和の $\sum_{m(i)=\delta} \mathrm{LT}(h_i) g_i$ の $m'$ は $\delta$ 未満でなければならない。このためには、この和のなかで先頭項の打ち消しが起こらなければならないので、$\sum_{m(i)=\delta} \mathrm{LT}(h_i)\mathrm{LT}(g_i)=0$ とならなければならない。よって、

  $$S = \sum_{m(i)=\delta} \mathrm{LT}(h_i)\mathbb{e}_i \tag{329}$$

  とすると、これは $S(G)$ に属するシチギーとなる。これは 0 でないところは単項式になっているので、$\delta$ 次斉次のシチギーになっていることがわかる。仮定より、斉次な基底 $S_1,\dots,S_m$ が存在するので、

  $$S = \sum_{j=1}^{m} u_i S_i \tag{330}$$

となる $u_i \in k[x_1, \ldots, x_n]$ が存在する。$S$ が $\delta$ 次斉次であり、$S_j$ らも斉次なので、係数を比較することにより $u_j S_j$ が[*10]$\delta$ 次斉次でないなら、$u_j = 0$ である[*11]。よって、$S = \sum_{u_j \neq 0} u_j S_j$ である。$u_j S_j$ は $G$ の $\delta$ 次斉次なシチギーなので、

$$\deg((u_j S_j)G) < \delta \tag{331}$$

と、真に次数が落ちる。さらに、次数の条件の準備をする。仮定より、$S_j G \to_G 0$ なので、

$$S_j G = \sum_{i=1}^{t} a_{ij} g_i \tag{332}$$

なる $a_{ij} \in k[x_1, \ldots, x_n]$ が存在し、さらに次数の条件

$$\deg(a_{ij} g_i) \leq \deg(S_j G) \tag{333}$$

がかかる。

$$\sum_{m(i)=\delta} \mathrm{LT}(h_i) g_i = SG = (\sum_{j=1}^{m} u_j S_j)G = \sum_{u_j \neq 0} u_j \sum_{i=1}^{t} a_{ij} g_i \tag{334}$$

なので、新たな $f$ の表現

$$f = \sum_{u_j \neq 0} u_j \sum_{i=1}^{t} a_{ij} g_i + \sum_{m(i)=\delta} (h_i - \mathrm{LT}(h_i)) g_i + \sum_{m(i)<\delta} h_i g_i \tag{335}$$

が得られる。これの $m'$ を計算する。まず第 1 の総和について計算する。

$$\begin{aligned}
m'(\text{新しい表現の第1の総和}) &= m'(\sum_{u_j \neq 0} u_j \sum_{i=1}^{t} a_{ij} g_i) && (336)\\
&= \max_{i,j} m(u_j a_{ij} g_i) && (337)\\
&\boxed{m' \text{ の定義}} && (338)\\
&\leq \max_{i,j} m(u_j S_j G) && (339)\\
&\boxed{\text{次数の条件}} && (340)\\
&< \delta && (341)\\
&\boxed{u_j S_j \text{ は } \delta \text{ 次斉次のシチギー}}. && (342)\\
& && (343)
\end{aligned}$$

第 2、第 3 の総和についてはそもそも $m'$ は $\delta$ 未満である。
よって、$m'(\text{新しい表現}) < \delta$ がわかった。これは、はじめに表現を最小に取っておいたことに矛盾する。よって、$\deg(f) = \delta = \max_i \deg(h_i g_i)$ である。最大を与える $i$ を $I$ とすると、$\deg(f) = \deg(h_I g_I)$ となり、$\mathrm{LT}(g_I) | \mathrm{LT}(f)$ となる。よって、$\mathrm{LT}(f) \in \langle \mathrm{LT}(G) \rangle$ となり、$\mathrm{LT}(I) \subset \langle \mathrm{LT}(G) \rangle$ となる。よって、$\langle \mathrm{LT}(I) \rangle \subset \langle \mathrm{LT}(G) \rangle$ となり、$G$ はグレブナ基底である。

(証終)

シチジーの基底から余計なものを取り除く条件を考える。シチジーの基底はペアのシチジーで張れることがさっきわかったので、そのときを考えてみる。「$G = (g_1, \ldots, g_s)$ とする。$\mathcal{S} \subset \{S_{ij}; 1 \leq i < j \leq n\}$ とし、$\mathcal{S}$ が $S(G)$ を張るとする。さらに、相異なる $i, j, k$ について、

[*10] 「$S_j$ が」ではない。
[*11] それならはじめから書かなきゃいいじゃないかという気がするが、基底が来るのが $f$ が来るより先なので仕方無い。

- $\mathrm{LT}(f_k)|(f_i \vee f_j)$
- $S_{ik},\, S_{jk} \in \mathcal{S}$

となっているとする。このとき、$\mathcal{S} - \{S_{ij}\}$ も $S(G)$ の基底になっている。」

証明

$S_{ij}$ が $S_{ik}$ と $S_{jk}$ で書ければよい。$i < j < k$ としておく。

$$S_{ij} = \frac{f_i \vee f_j}{\mathrm{LT}(f_i)}\mathbb{e}_i - \frac{f_i \vee f_j}{\mathrm{LT}(f_j)}\mathbb{e}_j \tag{344}$$

$$= \frac{f_i \vee f_j}{f_i \vee f_k} \cdot \frac{f_i \vee f_k}{\mathrm{LT}(f_i)}\mathbb{e}_i - \frac{f_i \vee f_j}{f_j \vee f_k} \cdot \frac{f_j \vee f_k}{\mathrm{LT}(f_j)}\mathbb{e}_j \tag{345}$$

$$= \frac{f_i \vee f_j}{f_i \vee f_k}\left(\frac{f_i \vee f_k}{\mathrm{LT}(f_i)}\mathbb{e}_i - \frac{f_i \vee f_k}{\mathrm{LT}(f_k)}\mathbb{e}_k + \frac{f_i \vee f_k}{\mathrm{LT}(f_k)}\mathbb{e}_k\right) - \frac{f_i \vee f_j}{f_j \vee f_k}\left(\frac{f_j f_k}{\mathrm{LT}(f_j)}\mathbb{e}_j - \frac{f_j \vee f_k}{\mathrm{LT}(f_k)}\mathbb{e}_k + \frac{f_j \vee f_k}{\mathrm{LT}(f_k)}\mathbb{e}_k\right) \tag{346}$$

$$= \frac{f_i \vee f_j}{f_i \vee f_k}S_{ik} - \frac{f_i \vee f_j}{f_j \vee f_k}S_{jk}. \tag{347}$$

(証終)

アルゴリズム。$[a, b] = (\min(a, b), \max(a, b))$ としておく。

証明

- どの段階でも $B$ に含まれるペアについて、それに対応する $f_\bullet$ が $G$ に含まれること: 初期ではあきらか。$G$ は増えるだけなことに注意。そのため、$B$ が減少することは問題にならない。$B$ が増えるときも、増やした $G$ にあわせている。
- どの段階でも $B$ が次の性質を持つことを示す:

$$\begin{cases} 1 \le i < j \le t \\ \text{かつ} \\ (i, j) \notin B \end{cases} \Longrightarrow \begin{cases} S(f_i, f_j) \to_G 0 \\ \text{または} \\ \mathrm{Criterion}(f_i, f_j, B) \end{cases} \tag{348}$$

いままで同様、メインループ前の変数は $b$ を、後は $a$ をつける。初期では $(i, j) \in B$ がどの $i, j$ についてもみたされ、前件が否定されるので自明に成立する。$B_b$ が条件

$$\begin{cases} 1 \le i_b < j_b \le t_b \\ \text{かつ} \\ (i_b, j_b) \notin B_b \end{cases} \Longrightarrow \begin{cases} S(f_{i_b}, f_{j_b}) \to_{G_b} 0 \\ \text{または} \\ \mathrm{Criterion}(f_{i_b}, f_{j_b}, B_b) \end{cases} \tag{349}$$

を満たしているとし、さらに

$$1 \le i_a < j_a \le t_a \quad \text{かつ} \quad (i_a, j_a) \notin B_a \tag{350}$$

が満たされているとして、

$$S(f_{i_a}, f_{j_a}) \to_{G_a} 0 \quad \text{または} \quad \mathrm{Criterion}(f_{i_a}, f_{j_a}, B_a) \tag{351}$$

を示そう。

(a) $(i_a, j_a) \in B_b$ のとき: $(i_a, j_a) \notin B_a$ でかつ $(i_a, j_a) \in B_b$ となっている。これは、$B$ のプログラム中の遷移を見ると、プログラム中で $(i, j)$ として $(i_a, j_a)$ がえらばれている。この $(i_a, j_a)$ を追跡する。

(A) ①で Yes のとき:

$$B_a = B_b - \{(i_a, j_a)\} \tag{352}$$

$$t_a = t_b \tag{353}$$

$$G_a = G_b \tag{354}$$

である。このときは $\mathrm{LT}(f_{i_a})$ と $\mathrm{LT}(f_{j_a})$ が互いに素である。

このとき、「どの段階でも $B$ に含まれるペアについて、それに対応する $f_\bullet$ が $G$ に含まれる」と $(i_a, j_a) \in B_b$ より、$f_{i_a}, f_{j_a} \in G_b = G_a$ である。よって、先の命題により $S(f_{i_a}, f_{j_a}) \to_{G_a} 0$ である。

(B) ②で Yes のとき:

$$B_a = B_b - \{(i_a, j_a)\} \tag{355}$$
$$t_a = t_b \tag{356}$$
$$G_a = G_b \tag{357}$$

である。

自明に $\mathrm{Criterion}(f_{i_a}, f_{j_a}, B_a)$ が成立する。

(C) ③で Yes のとき:

$$B_a = B_b - \{(i_a, j_a)\} \tag{358}$$
$$t_a = t_b \tag{359}$$
$$G_a = G_b \tag{360}$$

である。このとき、「どの段階でも $B$ に含まれるペアについて、それに対応する $f_\bullet$ が $G$ に含まれる」と $(i_a, j_a) \in B_b$ より、$f_{i_a}, f_{j_a} \in G_b = G_a$ である。よって、

$$\overline{S(f_{i_a}, f_{j_a})}^{G_a} = \overline{S(f_{i_a}, f_{j_a})}^{G_b} = S = 0 \tag{361}$$

となる。よって、$S(f_{i_a}, f_{j_a}) \to_{G_a} 0$ である。

(D) ③で No のとき:

$$t_a = t_b + 1 \tag{362}$$
$$f_{t_a} = S = \overline{S(f_{i_a}, f_{j_a})}^{G_b} \tag{363}$$
$$G_a = G_b + [f_{t_a}] \tag{364}$$
$$B_a = B_b \cup \{(i, t_a); 1 \leq i \leq t_b\} - \{(i_a, j_a)\} \tag{365}$$
$$\tag{366}$$

となっている。このとき、$q_\bullet$ を商として、

$$S(f_{i_a}, f_{j_a}) = \sum_{I=1}^{t_b} q_I f_I + \overline{S(f_{i_a}, f_{j_a})}^{G_b} \tag{367}$$

となっている。さらにすすめると、

$$S(f_{i_a}, f_{j_a}) = \sum_{I=1}^{t_b} q_I f_I + f_{t_a} \tag{368}$$

となっており、$S(f_{i_a}, f_{j_a})$ を $G_a$ で割ったあまりが 0 になることがわかる。よって、$S(f_{i_a}, f_{j_a}) \to_{G_a} 0$ である。

(b) $(i_a, j_a) \notin B_b$ のとき: $(i_a, j_a) \notin B_a$ でかつ $(i_a, j_a) \notin B_b$ となっている。何か $i < j$ なる $(i, j) \in B_b$ がアルゴリズム中で選択されて、

$$B_a = B_b - \{(i, j)\} \tag{369}$$

となっている。$(i, j) \in B_b$ でかつ $(i_a, j_a) \notin B_b$ なので、$(i, j) \neq (i_a, j_a)$ となっている。$(i, j)$ のアルゴリズム中での振舞によって場合分けする。

(A) ①が Yes のとき:

$$B_a = B_b - \{(i, j)\} \tag{370}$$
$$t_a = t_b \tag{371}$$
$$G_a = G_b \tag{372}$$

となる。$1 \leq i_a < j_a \leq t_a = t_b$ となり、かつ $(i_a, j_a) \notin B_b$ なので、$B_b$ の条件が満たされ、

$$S(f_{i_a}, f_{j_a}) \to_{G_b} 0 \quad \text{または} \quad \mathrm{Criterion}(f_{i_a}, f_{j_a}, B_b) \tag{373}$$

$S(f_{i_a}, f_{j_a}) \to_{G_b} 0$ がみたされるなら $G_b = G_a$ より $S(f_{i_a}, f_{j_a}) \to_{G_a} 0$ となり、示される。
$\mathrm{Criterion}(f_{i_a}, f_{j_a}, B_b)$ のときを考える。このとき、

- $[i_a, k] \notin B_b$
- $[j_a, k] \notin B_b$
- $\mathrm{LT}(f_k) | (f_{i_a} \vee f_{j_a})$

のすべてをみたす $k \in \{1, \ldots, t_b\} - \{i_a, j_a\}$ が存在する。$B_a = B_b - \{(i_a, j_a)\}$ なので、$B_a \subset B_b$ なので、$B_b^c \subset B_a^c$ である。$[i_a, k] \in B_b^c \subset B_a^c$ となり、$[i_a, k] \notin B_a$ となる。同様に $[j_a, k] \notin B_a$ となる。また、$t_a = t_b$ なので、$k \in \{1, \ldots, t_a\} - \{i_a, j_a\}$ である。まとめると、$k$ が

- $[i_a, k] \notin B_a$
- $[j_a, k] \notin B_a$
- $\mathrm{LT}(f_k) | (f_{i_a} \vee f_{j_a})$
- $k \in \{1, \ldots, t_a\} - \{i_a, j_a\}$

をみたす。よって、$\mathrm{Criterion}(f_{i_a}, f_{j_a}, B_a)$ が満足される。

(B) ②が Yes のとき:

$$B_a = B_b - \{(i, j)\} \tag{374}$$
$$t_a = t_b \tag{375}$$
$$G_a = G_b \tag{376}$$

なので、「① が Yes のとき」と同様に通る。

(C) ③が Yes のとき: やはり同様。

(D) ③が No のとき: このとき、

$$S = \overline{S(f_i, f_j)}^{G_b} \tag{377}$$
$$t_a = t_b + 1 \tag{378}$$
$$f_{t_a} = S = \overline{S(f_i, f_j)}^{G_b} \tag{379}$$
$$G_a = G_b + [f_{t_a}] \tag{380}$$
$$B_a = (B_b \cup \{(I, t_a); 1 \leq I \leq t_b\}) - \{(i, j)\} \tag{381}$$

となっている。

(i) $j_a = t_a$ のとき: 2 番目の要素を見ると、あきらかに $(i_a, j_a) = (i_a, t_a) \in B_b \cup \{(I, t_a); 1 \leq I \leq t_b\}$ である。また、$(i_a, j_a) = (i_a, t_a) \neq (i, j)$ であることを先に言ったので、

$$(i_a, j_a) \in (B_b \cup \{(I, t_a); 1 \leq I \leq t_b\}) - \{(i, j)\} = B_a \tag{382}$$

である。一方、(b) に入ったときの仮定により、$(i_a, j_a) \notin B_a$ である。これは矛盾であるから、この (a-D-i) という状況は起こらない。

(ii) $j_a < t_a$ のとき: このとき、$B_b$ の条件を満たすので、

$$S(f_{i_a}, f_{j_b}) \to_{G_b} 0 \quad \text{または} \quad \mathrm{Criterion}(f_{i_a}, f_{j_a}, B_b) \tag{383}$$

となる。$S(f_{i_a}, f_{j_a}) \to_{G_b} 0$ を満たすときには、$G_a$ は $G_b$ より広いので $S(f_{i_a}, f_{j_a}) \to_{G_a} 0$ となり、示される。
$\mathrm{Criterion}(f_{i_a}, f_{j_a}, B_b)$ が満たされるときは、

- $[i_a, k] \notin B_b$
- $[j_a, k] \notin B_b$
- $\mathrm{LT}(f_k) | (f_{i_a} \vee f_{j_a})$

のすべてをみたす $k \in \{1,\dots,t_b\} - \{i_a, j_a\}$ が存在する。仮に $[i_a, k] \in B_a$ とする。$i_a$ も $k$ も $\{1,\dots,t_b\}$ の元なので、$\{(I, t_a); 1 \leq I \leq t_b\}$ には属さない。よって、$B_b$ に属する。よって、$[i_a, k] \notin B_a$ がわかった。同様に、$[j_a, k] \notin B_a$ もわかる。引き続き $\mathrm{LT}(f_k)|(f_{i_a} \vee f_{j_a})$ もみたされるので、$\mathrm{Criterion}(f_{i_a} f_{j_a}, B_a)$ も満たされる。

- $B = \emptyset \implies G$はグレブナ基底: $t$ を $G$ の長さとする。

$$\mathcal{I} = \big\{(i,j); 1 \leq i < j \leq t, \quad \mathrm{Criterion}(f_i, f_j, B)\text{は}(i,j)\text{が選択されたとき}false.\big\} \tag{384}$$

とする。このとき、あとで証明する主張がなりたつ: 「$\mathcal{S} = \{S_{ij}; (i,j) \in \mathcal{I}\}$ は『$S_{ij}G = S(f_i, f_j) \to_G 0$ がすべての $S_{ij} \in \mathcal{S}$ について成立する』という性質を持つ $S(G)$ の基底である。」
$\mathcal{S}$ を考えると、これは $S_{ij}$ だけでできた基底なので斉次基底であり、さらに「$S_{ij}G \to_G 0$ がすべての $S_{ij} \in \mathcal{S}$ について成立する」という性質を持つので、先のグレブナ基底の $\to_G 0$ での判定の定理を利用し、$G$ がグレブナ基底であることがわかる。
$B = \emptyset$ はなんだったのかという気がするが、それはこの「主張」を示すのに使う。

- 「主張」の証明:$B \neq \emptyset$ とする。「どの段階でも $B$ が次の性質を持つことを示す」と $B \neq \emptyset$ より、前件が自明に満足されるので、

$$1 \leq i < j \leq t \implies \begin{cases} S(f_i, f_j) \to_G 0 \\ \text{または} \\ \mathrm{Criterion}(f_i, f_j, B) \end{cases} \tag{385}$$

となる。$\mathcal{I}$ の定義より、$(i,j)$ について、$\mathrm{Criterion}(f_i, f_j, B) = false$ がその $B$ において成立するので、「または」の一方が潰され、$S(f_i, f_j) \to_G 0$ が成立する。
あとは、$\mathcal{S}$ が $S(G)$ の基底になることを示す。$list$ を、$B$ から $(i,j)$ のペアを外したときのものを順に入れたものにする。次に、その $list$ を逆順に並べ替える。このはじめの時点では、$S_{ij}$ をすべて含んでいるので、$S(G)$ を張る。この $list$ を先頭から走って、$\mathrm{Criterion}(f_i, f_j, B_{(i,j)\text{が選択されたとき}})$ が $true$ なら除去するという作業をくりかえす。取り除くとき、$\mathrm{Criterion}(f_i, f_j, B_{(i,j)\text{が選択されたとき}})$ が $true$ なので、「何か $k \notin \{i,j\}$ が存在して、これに対して
  - $[i,k] \notin B$
  - $[j,k] \notin B$
  - $\mathrm{LT}(f_k)|(f_i \vee f_j)$ 」となっている。この時点で $[i,k] \notin B$ で $[j,k] \notin B$ なので、$list$ が逆順になっていることから、$[i,k], [j,k] \in list$ となっている。そして、$\mathrm{LT}(f_k)|(f_i \vee f_j)$ となっているので、「シチジーの基底から余計なものを取り除く条件」より、除去したあとでも $S(G)$ を張る。この操作を $list$ を最後まで走ると、$\mathcal{I}$ となる。よって、$\mathcal{I}$ が所与の性質を持つ。
- アルゴリズムの停止: 停止しなかったとしよう。このとき、$B$ は毎回減少するので、停止しないためには永遠に $B$ の追加が行なわれなければならず、これに伴なって $G$ は余りで増やされていく。余りの定義より、$\langle \mathrm{LT}(G) \rangle$ は真に増加し続けることになるが、これは多項式環が ACC を満たすことに矛盾する。

(証終)

# 3 消去理論