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 3 月 21 日

1　幾何，代数，アルゴリズム

1.1　多項式とアフィン空間

多項式環を定義した．

n 次アフィン空間を k^n で定義した．k^1 をアフィン直線，k^2 をアフィン平面とよぶ．

多項式が作る関数 $k^n \to k$ について，「この多項式は 0 か？」と，「この関数のとる値はつねに 0 か？」という問が湧いてくるが，この 2 つの問題は等価ではない．実際，$\mathbb{F}_2$ 上の多項式 $x(x-1)$ は，0 多項式ではないが関数としては 0 である．有限体だとこういうことがおこるが，無限体であれば多項式として 0 であることと関数として 0 であることは等価である：

命題 1.1.1
k を無限体とする．$f \in k[x_1, \ldots, x_n]$ が $f = 0$ であることと，f から導かれた関数 $f: k^n \to k$ が $f = 0$ であることとは同値である．

証明
多項式として 0 ならば，関数として 0 であることは自明である．関数として 0 であることから多項式として 0 であることを導く．$f \in k[x_1, \ldots, x_n]$ を多項式とする．

- $n = 1$ のとき：$f \in k[x]$ であり，$\widetilde{f}: k \to k$ である．f は n 次式であるとする．もしも f が 1 次以上であれば，f は高々 n 個の根しか持たない．一方，$\widetilde{f}$ が 0 であることと，k が無限体であることから，f は無限個の根を持つことになる．よって，f は 1 次未満，すなわち定数であり，$f = 0$ である．
- $n \geq 2$ のとき：$a_1, \ldots, a_{n-1} \in k^{n-1}$ とする．x_n について整理して，N を x_n についての最高次の次数とする．

$$f = \sum_{i=1}^{N} g_i(x_1, \ldots, x_{n-1}) x^i \tag{1}$$

と書く．f の $x_1, \ldots, x_{n-1}$ に $a_1, \ldots, a_{n-1}$ を代入し，多項式

$$\widetilde{f} = \sum_{i=1}^{N} g_i(a_1, \ldots, a_{n-1}) x^i \tag{2}$$

を得る．$\widetilde{f}$ は 1 変数の多項式であるから，「$n = 1$ のとき」より，

$$^{\forall} i \in \{1, \ldots, N\}: g_i(a_1, \ldots, a_{n-1}) = 0. \tag{3}$$

$a_1, \ldots, a_{n-1}$ は任意だったので，各 $g_i \in k[x_1, \ldots, x_{n-1}]$ は関数として 0 である．帰納法により，$n-1$ のとき成立しているとしてよいから，g_i は多項式として 0 である．よって，f は多項式として 0 である．

(証終)

系として，無限体上で多項式 f, g が多項式として $f = g$ であることと関数として $f = g$ であることが等価であることが得られる．

$\mathbb{C}$ は代数閉体であること，すなわち $\mathbb{C}$ の 1 次以上の多項式は根を 1 つ持つことが知られている．

(問題 1) 加法の単位元は 0，乗法の単位元が 1 であることは総当たりで確かめられる．また，

$$-0 = 0, \quad -1 = 1, 1^{-1}1 \tag{4}$$

が成り立つことも確かめられる．

(問題 2) (a)

$$g(0,0) = 0, \quad g(0,1) = g(1,0) = 0, \quad g(1,1) = 1 + 1 = 0. \tag{5}$$

命題 5 は無限体上の多変数多項式について，それが多変数多項式として 0 であることと関数として 0 であることとが同値であるという主張であったが，$\mathbb{F}_2$ は無限体でないので矛盾しない．

(b) $x(y + z)$．

(c) $x_1(1 - x_1)x_2 \dots x_n$．$x_1$ がどちらでも消えてしまう．

(問題 3) (a) $[a] \in \mathbb{F}_p - \{0\}$ の逆元を求める手続を示そう．$an \equiv 1 \mod p$ となる n を見つけれられればよい．これは，$an + pm = 1$ を満たす n, m を見つけることだが，a は p の倍数ではないので，p が素数であることから a と p とは互いに素である．よって，ユークリッドの互除法により，n と m とを見つけることができる．$[a]^{-1}[n]$ となる．したがって，「理由」は a と p とが互いに素であることである．

(b) $\langle a \rangle$ は $\mathbb{F}_p - \{0\}$ の部分群になるが，ラグランジュの定理により $\mathbb{F}_p - \{0\}$ の部分群は $\{1\}$ か $\mathbb{F}_p - \{0\}$ かである．$\langle a \rangle = \{1\}$ のとき，すなわち $[a] = 1$ のときは明らかに成り立つ．$[a] \neq [1]$ のとき，すなわち $\langle a \rangle = \mathbb{F}_p - \{0\}$ のときは $1, a, a^2, \dots, a^{p-2}$ の $p - 1$ 個が全て異なり，$\mathbb{F}_p - \{0\}$ の元の何らかの順列になっている．したがって，$a^{p-1} = a^n$ となる $0 \leq n \leq p - 2$ となる n があるが，このとき $1 = a^{p-1-n}$ となる．$1 \leq p - n \leq p - 1$ となるが，$1, a, a^2, \dots, a^{p-2}$ の全てが相異なるのだから，$p - 1 - n = p - 1$，すなわち $n = 0$ となるしかない．したがって，$a^{p-1} = 1$ である．

(c) $a = 0$ のときは自明．$a \neq 0$ のときは (b) より $a^{p-1} = 1$ を得て，$a^p = a$ を得る．

(d) $a^p - a$．(c) より従う．

(問題 4) 加法についての F の 1_F の生成する部分群を考えると，$0_F, 1_F, 2 \times 1_F, \dots, (p-1) \times 1_F$ が全て相異なることが (b) と同様にして分かる．$\varphi\colon F \to \mathbb{F}_p$ を，$\varphi(n \times 1_F) = n \times 1_{\mathbb{F}_p}$ と定めると，これは全単射になっている．準同型になっていることが，整数係数に注意すれば示せる．よって，$F \simeq \mathbb{F}_p$ であり，(3-d) から結論が従う．

(問題 5) 略

(問題 6) (1) 先の命題と同様．無限個の根を持つことになってしまうことがポイント．

(2) これも同様．$\mathbb{Z}$ が整域なので，$M + 1$ 個という多すぎる根を持ってしまう．

1.2 アフィン多様体

k を体とし，$f_1, \dots, f_s \in k[x_1, \dots, x_n]$ とする．これらの多項式が定めるアフィン多様体 $\mathbf{V}(f_1, \dots, f_s)$ を

$$\mathbf{V}(f_1, \dots, f_s) = \left\{(x_1, \dots, x_n) \in k^n \middle|^{\forall} i \in \{1, \dots, s\}\colon f_i(x_1, \dots, x_n) = 0\right\} \tag{6}$$

と定める．

アフィン多様体はいろんなところから作られる．ラグランジュの未定乗数法は，$f\colon \mathbb{R}^d \to \mathbb{R}$ の $g\colon \mathbb{R}^d$，$g = 0$ となる制約上での極値を求める技法だった．極値は，$\nabla f = \lambda \nabla g$ をみたすことになる．これに $g = 0$ をつけくわえれば解ける．

アフィン多様体の結びと交わりが，式の組み合わせで書ける：

補題 **1.2.1**

$$A = \mathbf{V}(f_1, \ldots, f_a) \tag{7}$$
$$B = \mathbf{V}(g_1, \ldots, g_b) \tag{8}$$

とする．このとき，

$$A \cap B = \mathbf{V}(\underbrace{f_1, \ldots, f_a, g_1, \ldots, g_b}_{a+b\text{個}}) \tag{9}$$
$$A \cup B = \mathbf{V}(\underbrace{f_1 g_1, \ldots, f_1 g_b, \ldots, f_a g_1, \ldots, f_a g_b}_{ab\text{個}}). \tag{10}$$

証明

- 交わりについて：あきらか．
- 結びについて：
  - $\subset$：$x \in A \cup B$ とする．$x \in A$ であるとして一般性を失わない．このとき，

$$^\forall i \in \{1, \ldots, a\} \colon f_i(x) = 0. \tag{11}$$

    よって，全ての $f_\bullet g_\bullet$ も 0 になる．$x \in \mathbf{V}(f_1 g_1, \ldots, f_a g_b)$ である．
  - $\supset$：$x \notin A \cup B$ とする．$x \notin A$ かつ $x \notin B$ なので，ある $i \in \{1, \ldots, a\}$ が存在して $f_i(x) \neq 0$ となっており，さらにある $j \in \{1, \ldots, b\}$ が存在して $g_j(x) \neq 0$ となっている．このとき，$f_i g_j(x) \neq 0$ であるから，$x \notin \mathbf{V}(f_1 g_1, \ldots, f_a g_b)$ となる．

(証終)

このアフィン多様体について，次の疑問がわいてくる．

存在 いつ $\mathbf{V}(f_1, \ldots, f_n) \neq \emptyset$ となるのか？ 言い換えるなら，$f_1, \ldots, f_n = 0$ はいつ解を持つのか？
有限性 いつ $\mathbf{V}(f_1, \ldots, f_n)$ は有限集合になるのか？ 言いかえるなら，$f_1, \ldots, f_n = 0$ の解はいつ有限個になるのか？それは何か？
次元 $\mathbf{V}(f_1, \ldots, f_n) = 0$ の次元は何か？

(問題 1) (a) $\mathbf{V}(x^2 + 4y^2 - 2x + 16y + 1)$ の形？ $(x-1)^2 + 4(y+2)^2 = -1 + 1 + 16 = 4^2$．よって，$(1, -2)$ 中心の半径 4 の円．
(b) $\mathbf{V}(x^2 - y^2)$ の形？ $\mathbf{V}(x^2 - y^2) = \mathbf{V}((x+y)(x-y)) = \mathbf{V}(x+y) \cup \mathbf{V}(x-y)$．よって，バツ印．
(c) $\mathbf{V}(2x + y - 1, 3x - y + 2)$ の形？ $\mathbf{V}(2x + y - 1, 3x - y + 2) = \mathbf{V}(2x + y - 1) \cap \mathbf{V}(3x - y + 2)$．

(問題 2) $\mathbf{V}(y^2 - x(x-1)(x^2))$ の形？ $y^2 = x(x-1)(x-2)$ を考える．右辺のグラフを考えると，$[0, 1]$ と $[2, \infty)$ で非負なので，ここでのみ y が存在する．よって，$[0, 1]$ で丸っぽいのがあって，2 より右側で $(2, 0)$ を頂点とした放物線みたいになる．

(問題 3) $\mathbf{V}(x^2 + y^2 - 4, xy - 1)$ の形？ $x^2 - 4 + \frac{1}{x^2} = 0$ の解は $\pm\sqrt{2 \pm \sqrt{3}}$ の 4 つ．対称性を考えて，

$$\pm(\sqrt{2+\sqrt{3}}, \sqrt{2-\sqrt{3}}), \pm(\sqrt{2-\sqrt{3}}, \sqrt{2+\sqrt{3}}) \tag{12}$$

の 4 つ．

(問題 4) $\mathbf{V}(xz^2 - xy) = \mathbf{V}(x(z^2 - y)) = \mathbf{V}(x) \cup \mathbf{V}(z^2 - y)$．$\mathbf{V}(x^4 - zx, x^3 - yx) = \mathbf{V}(x^4 - zx) \cap \mathbf{V}(x^3 - yx) = \mathbf{V}(x(x^3 - z)) \cap \mathbf{V}(x(x^2 - y)) = (\mathbf{V}(x) \cup \mathbf{V}(x^3 - z)) \cap (\mathbf{V}(x) \cup \mathbf{V}(x^2 - y)) = \mathbf{V}(x) \cap (\mathbf{V}(x^3 - z) \cup \mathbf{V}(x^2 - y)) = \mathbf{V}(x) \cap \mathbf{V}(y) \cap \mathbf{V}(z)$．$\mathbf{V}(x^2+y^2+z^2-1, x^2+y^2+(z-1)^2-1) = \mathbf{V}(x^2+y^2+z^2-1, x^2+y^2+(z-1)^2-1, z-\frac{1}{2}) = \mathbf{V}(x^2 + y^2 - \frac{3}{4}, z - \frac{1}{2}) = \mathbf{V}(x^2 + y^2 - \frac{3}{4}) \cap \mathbf{V}(z - \frac{1}{2})$．

(問題 5) $\mathbf{V}((x-2)(x^2-y), y(x^2-y), (z+1)(x^2-y)) = \mathbf{V}(x^2 - y) \cup \mathbf{V}(x - 2, y, z + 1)$．

(問題 6) (a) $\{(a_1, \ldots, a_n)\} = \mathbf{V}(x_1 - a_1, \ldots, x_n - a_n)$．

(b) アフィン多様体 2 個の交わりはアフィン多様体なので，繰替えす．

(問題 7) (a) $\{r = \sin(2\theta)\} \subset \mathbf{V}((x^2+y^2)^3 - 4x^2y^2)$？

$$x = r\cos\theta = \sin(2\theta)\cos\theta \tag{13}$$
$$y = r\sin\theta = \sin(2\theta)\sin\theta. \tag{14}$$

$$\begin{aligned}(x^2+y^2)^3 - 4x^2y^2 &= r^6 - 4(r^2\cos^2\theta)(r^2\sin^2\theta) && (15)\\ &= r^4(r^2 - 4\cos^2\theta\sin^2\theta) && (16)\\ &= r^4(r^2 - \sin^2(2\theta)) && (17)\\ &= r^4(\sin^2(2\theta) - \sin^2(2\theta)) && (18)\\ &= 0. && (19)\end{aligned}$$

(b) $\{r = \sin(2\theta)\} \supset \mathbf{V}((x^2+y^2)^3 - 4x^2y^2)$？ $(x,y) \in \mathbf{V}((x^2+y^2)^3 - 4x^2y^2)$ とする．$x = r\cos\theta$, $y = r\sin\theta$ となる r, θ が存在するので，それを選ぶ．多項式に代入すると，

$$\begin{aligned}((r\cos\theta)^2 + (r\sin\theta)^2)^3 - 4(r\cos\theta)^2(r\sin\theta)^2 &= r^6 - 4r^4\cos^2\theta\sin^2\theta && (20)\\ &= r^4(r^2 - (\sin 2\theta)^2) && (21)\\ &= 0 && (22)\end{aligned}$$

とならなければならない．よって，$r = \pm\sin 2\theta$ である．$r = \sin 2\theta$ ならば $(x,y) \in \{r = \sin 2\theta\}$ である．$r = -\sin 2\theta$ ならば，$r = \sin(-2\theta)$ である．

(問題 8) $\mathbb{R}^2 \setminus \{(1,1)\}$ はアフィン多様体でない？ これがアフィン多様体だとし，$f_1, \ldots, f_n \in k[x,y]$ が存在して $\mathbf{V}(f_1, \ldots, f_n) = \mathbb{R}^2 \setminus \{(1,1)\}$ とする．$i \in \{1, \ldots, n\}$ とし，$g_i(t) = f_i(t,t) \in k[t]$ とする．g_i は無数の根を持つので，g_i は関数として 0 であり，$\mathbb{R}$ は無限体なので，$g_i = 0$ しかありえない．よって，$g_i(1,1) = 0$ である．これが全ての i について言えるので，$f_1, \ldots, f_n$ はどれも $(1,1)$ で消える．これは矛盾．

(問題 9) 上半平面はアフィン多様体でない？ 略

(問題 10) $\mathbb{Z}^n \subset \mathbb{C}^n$ はアフィン多様体でない？ 略

(問題 11) (a) $x^n + y^n = 1$ の定めるアフィン多様体 $\subset \mathbb{Q}^2$ を考える．n が奇数なら自明解が 2 つ，偶数なら 4 つ？

- n が奇数：まず $y = 0$ とする．$x^n = 1$ となる．$x = 1$ しかない．$x = 0$ についても同様で，

$$(x,y) = (1,0), (0,1). \tag{23}$$

- n が偶数：まず $y = 0$ とする．$x^n = 1$ となる．$x = \pm 1$ しかない．$x = 0$ についても同様で，$(x,y) = (\pm 1, 0), (0, \pm 1)$．

(b) $F_n = \mathbf{V}(x^n + y^n - 1)$ が $n \geq 3$ について自明でない解を持つことと，フェルマーの最終定理が誤りであることが等価であることを示せ？

$$\begin{aligned}&{}^{\exists}x, y \in \mathbb{Q} \setminus \{0\}\text{: } x^n + y^n = 1 && (24)\\ \iff &{}^{\exists}\frac{x}{z}, \frac{y}{w} \in \mathbb{Q} \setminus \{0\}, \text{既約: } (\frac{x}{z})^n + (\frac{y}{w})^n = 1 && (25)\\ \iff &{}^{\exists}\frac{x}{z}, \frac{y}{w} \in \mathbb{Q} \setminus \{0\}, \text{既約: } (xw)^n + (yz)^n = (zw)^n && (26)\\ & && (27)\end{aligned}$$

とやり，フェルマーのほうの右側を割って 1 にする．

(問題 12) $f(x,y) = x^2 - y^2$ を $g(x) = x^2 + y^2 - 1 = 0$ 上で最大・最小化することを考える．

(問題 13) (a) 略

(b) 角度 3 つで 3 変数っぽい．

(c) 長さ 3 のアームの先端の位置を (x_1, y_1)，長さ 2 のアームは (x_2, y_2)，長さ 1 のアームは (x_3, y_3) とする．このとき，

$$x_1^2 + y_1^2 = 3^2 \tag{28}$$
$$(x_1 - x_2)^2 + (y_1 - y_2)^2 = 2^2 \tag{29}$$
$$(x_2 - x_3)^2 + (y_2 - y_3)^2 = 1^2. \tag{30}$$

(d) 6 変数を 3 式で拘束したので合ってそう．

(問題 14) (a) $p_1 = (x_1, y_1), \ldots, p_3 = (x_3, y_3)$ とする．三角不等式により，$|p_2| = |(p_2 - p_1) + p_1| \leq |p_2 - p_1| + |p_1| = 2 + 3 = 5$．$|p_3| = |(p_3 - p_2) + p_2| \leq |p_3 - p_2| + |p_2| = 1 + 5 = 6$．

(b) 略．1 をうまく回して手の軌道を異なった半径になるようにできる．

(c) 2 から 6 までは先の通り実現できる．0 から 2 までは，長さ 2 の腕を適当に固定して，その先端が原点から 1 になるようにする．これは，長さ 2 の腕を完全に折り畳んで，長さ 3 の腕と重なるようにすることで実現できる．ここを中心に長さ 1 を回すことにより実現される．

(問題 15) (a) 略．

(b) $\mathbb{Z} \subset \mathbb{Q}$ は，$\mathbb{Z} = \bigcup_{i \in \mathbb{Z}} \mathbf{V}(x - i)$ であるが，これはアフィン多様体でない．無限個の根の議論．

(c) $V = \mathbb{R}$ は $\mathbb{R}$ でのアフィン多様体であり，$W = \{0\}$ もまたアフィン多様体だが，$V \setminus W$ はアフィン多様体ではない．これは議論した．

(d) $V \subset k^n$，$W \subset k^m$ がアフィン多様体であるとき，$V \times W \subset k^{n+m}$ がアフィン多様体？ $V = \mathbf{V}(f_1, \ldots, f_v)$，$W = \mathbf{V}(g_1, \ldots, g_w)$ とする．$((x, y) \in V \times W) \iff (x \in V \wedge y \in W) \iff (f_1(x) = \cdots = f_v(x) = g_1(y) = \cdots = g_w(y) = 0)$．よって，$f_1, \ldots, f_v$ を k^{n+m} に埋め込んだものを $\widetilde{f}_1, \ldots, \widetilde{f}_v$ とし，$g_1, \ldots, f_w$ を k^{n+m} に埋め込んだものを $\widetilde{g}_1, \ldots, \widetilde{g}_w$ とすると，$V \times W = \mathbf{V}(\widetilde{f}_1, \ldots, \widetilde{f}_v, \widetilde{g}_1, \ldots, \widetilde{g}_w)$．

1.3 アフィン多様体のパラメータ付け

アフィン多様体を方程式系とみなしたとき，その解が有限個のこともあれば無限個のこともある．この無限個の解を表示する方法として，パラメータ付けを学ぶ．例えば，1 次式でできたアフィン多様体が無数個の解を持つとき，その方程式系を掃き出すことにより自由変数を用いて一般的に解をあらわすことができる．このようなものを考える．

f が $x_1, \ldots, x_n$ の k 上の有理関数であるとは，f が $k[x_1, \ldots, x_n]$ の商で表されることである．有理関数の相当は分母を払うことにより確かめられる．

有理関数の組 $r_1, \ldots, r_n \in k(t_1, \ldots, t_T)$ がアフィン多様体 $\mathbf{V}(f_1, \ldots, f_m)$ の有理パラメータ表示であるとは，

$$\left\{(x_1, \ldots, x_n) | {}^{\forall} i \in \{i, \ldots, n\} \colon {}^{\exists} t_1, \ldots, t_T \in k \colon x_i = r_i(t_1, \ldots, t_T)\right\} \subset \mathbf{V}(f_1, \ldots, f_m) \tag{31}$$

となり，かつ $\mathbf{V}(f_1, \ldots, f_n)$ が左辺を包むもののうち「最小」であることである．等しくなくてもいいことに注意．有理関数ではなく多項式であるときには多項式表示とよぶ．また，$\mathbf{V}(f_1, \ldots, f_m)$ について，$f_1 = f_2 = \cdots = f_m = 0$ という方程式系はアフィン多様体の陰関数表示とよぶ．

ここで，

- 有理パラメータ表示から陰関数表示は得られるか？
- 陰関数表示から有理パラメータ表示は得られるか？

という問題が湧いてくる．一般に，陰関数表示から有理パラメータ表示を得ることはできず，それができるときには単有理的であるという．有理パラメータ表示から陰関数表示を得ることは常に可能で，それは消去理論で扱う．

有理パラメータ表示から陰関数表示を計算してみる．ある図形が，

$$x = 1 + t, \quad y = 1 + t^2 \tag{32}$$

で与えられているとする．このとき，

$$y = 1 + (x - 1)^2 = x^2 - 2x + 2 \tag{33}$$

となり，先の図形はアフィン多様体であって，$\mathbf{V}(x^2-2x+2-y)$ であることがわかった．

また，$\mathbf{V}(x^2+y^2-1)$ のパラメータ表示を考えてみる．$(-1,0)$ を通る傾き t の直線 $y=t(x+1)$ を考える．この $x^2+y^2=1$ との共有点を考える．$x^2+t^2(x+1)^2=1$ が得られ，$(1+t^2)x^2+2t^2x+(t^2-1)=0$，すなわち

$$x=\frac{-t^2\pm\sqrt{t^4-(1+t^2)(t^2-1)}}{1+t^2}=\frac{-t^2\pm1}{1+t^2}=-1,\ \frac{1-t^2}{1+t^2}. \tag{34}$$

$x=\frac{1-t^2}{1+t^2}$ のとき，

$$y=t(\frac{1-t^2}{1+t^2}+1)=t\frac{2}{1+t^2}=\frac{2t}{1+t^2}. \tag{35}$$

こうして，有理パラメータ表示

$$x=\frac{1-t^2}{1+t^2},\quad y=\frac{2t}{1+t^2} \tag{36}$$

が得られた．この表示は，$x=-1$ を取り得ないことには注意が要る．ぴったり一致しなくても有理パラメータ表示とよぶことは先に注意した．

アフィン多様体 $\mathbf{V}(y-x^2,z-x^3)$ を考える．これをパラメータ表示すると，

$$x=t,\quad y=t^2,\quad z=t^3 \tag{37}$$

となる．これを 3 次ねじれ曲線とよぶ．この接線を求める．各々微分して，

$$x'=1,\quad y'=2t,\quad z'=3t^2 \tag{38}$$

となり，(t_0,t_0^2,t_0^3) での接線として，

$$\begin{pmatrix}x\\y\\z\end{pmatrix}=s\begin{pmatrix}1\\2t\\3t^2\end{pmatrix}+\begin{pmatrix}t_0\\t_0^2\\t_0^3\end{pmatrix} \tag{39}$$

が得られる．これを t,s に関するパラメータで見ると曲面をあらわしており，これをねじれ 3 次曲線の接平面とよぶ．これの陰関数表示はあとで求める．

ベジェ曲線について考える．制御点 $(x_0,y_0),\dots,(x_3,y_3)\in\mathbb{R}^2$ を考え，パラメータ表示

$$x(t)=x_0(1-t)^3+3x_1(1-t)^2t+3x_2(1-t)t^2+x_3t^3, \tag{40}$$
$$y(t)=y_0(1-t)^3+3y_1(1-t)^2t+3y_2(1-t)t^2+y_3t^3. \tag{41}$$

を考える．この始点は (x_0,y_0) であり，終点は (x_3,y_3) となっている．また，微分を考えると，

$$x'(t)=3x_0(1-t)^2(-1)+3x_1(2(1-t)(-1)t+(1-t)^2)+3x_2((-1)t^2+(1-t)2t)+x_3\cdot3t^2, \tag{42}$$
$$y'(t)=3y_0(1-t)^2(-1)+3y_1(2(1-t)(-1)t+(1-t)^2)+3y_2((-1)t^2+(1-t)2t)+y_3\cdot3t^2. \tag{43}$$

よって，

$$x'(0)=-3x_0+3x_1=3(x_1-x_0), \tag{44}$$
$$y'(0)=-3y_0+3y_1=3(y_1-y_0), \tag{45}$$
$$x'(1)=-3x_2+3x_3=3(x_3-x_2), \tag{46}$$
$$y'(1)=-3y_2+3y_3=3(y_3-y_2). \tag{47}$$

よって，はじまりは (x_1,y_1) に向かい，おわりは (x_2,y_2) から向かうことがわかる．

(問題 1)

$$x+2y-2z+w=-1 \tag{48}$$
$$x+y+z-w=2 \tag{49}$$

をパラメータ付けせよ．

$$\begin{pmatrix} 1 & 2 & -2 & 1 & -1 \\ 1 & 1 & 1 & -1 & 2 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & -2 & 1 & -1 \\ 0 & -1 & 3 & -2 & 3 \end{pmatrix} \tag{50}$$

$$\to \begin{pmatrix} 1 & 0 & 4 & -3 & 5 \\ 0 & -1 & 3 & -2 & 3 \end{pmatrix} \tag{51}$$

$$\to \begin{pmatrix} 1 & 0 & 4 & -3 & 5 \\ 0 & 1 & -3 & 2 & -3 \end{pmatrix}. \tag{52}$$

よって，

$$x = -4z + 3w + 5 \tag{53}$$

$$y = 3z - 2w + 3. \tag{54}$$

(問題 2) $y = 2x^2 - 1$ の $[-1, 1]$ がパラメタ付けされている．すなわち，

$$\left\{(x, y) | y = 2x^2 - 1,\ -1 \leq x \leq 1\right\} = \{(x, y) | x = \cos t,\ y = \cos 2t\}. \tag{55}$$

- $\subset$：$(x, y) \in$ (左辺) とする．$y = 2x^2 - 1$，$-1 \leq x \leq 1$．このとき，$\cos t = x$ となる t が存在する．このとき，$y = 2x^2 - 1 = 2\cos^2 t - 1 = \cos 2t$ である．よって，$(x, y) \in$ (右辺) である．
- $\supset$：$(x, y) \in$ (右辺) とする．$x = \cos t$，$y = \cos 2t$ となる $t \in \mathbb{R}$ が存在する．あきらかに $-1 \leq x = \cos t \leq 1$ であり，

$$y = \cos 2t = 2\cos^2 t - 1 = 2x^2 - 1 \tag{56}$$

である．よって，$(x, y) \in$ (左辺) である．

(問題 3)

$$\mathbf{V}(y - f(x)) = \{(x, y) | y - f(x) = 0\} = \{(x, y) | y = f(x)\}. \tag{57}$$

よって，パラメタ付けは $y = f(x)$ である．

(問題 4) パラメタ表示 $x = \frac{t}{1+t}$, $y = 1 - \frac{1}{t^2}$ とする．

(a) 陰関数表示？ 解いて，$x^2 y - 2x + 1 = 0$．

(b) パラメタ表示は，上の陰関数の定めるアフィン多様体のうち，$\{(1, 1)\}$ を除く点を全て走る？

$$\left\{(x, y) | x^2 y - 2x + 1 = 0\right\} \setminus \{(1, 1)\} = \left\{(x, y) | x = \frac{t}{1+t},\ y = 1 - \frac{1}{t^2}\right\} \tag{58}$$

を示せばよい．

- $\subset$：$(x, y) \in$ (左辺) とする．$x^2 y - 2x + 1 = 0$ であり，$(x, y) = (1, 1)$ ではない．$x = 0$ とするとこの式に矛盾するので，$y = \frac{2x-1}{x^2}$ となる．$t = \frac{x}{1-x}$ とする．これは，$x \neq 1$ より可能である．このとき，

$$(t \mapsto 1 - \frac{1}{t^2})(\frac{x}{1-x}) = 1 - \frac{(1-x)^2}{x^2} \tag{59}$$

$$= \frac{2x - 1}{x^2} \tag{60}$$

$$= y. \tag{61}$$

よって，パラメータが構成できた．$(x, y) \in$ (右辺) である．

- $\supset$：あきらか．

(問題 5) $x^2 - y^2 = 1$ について．

(a) $x = \cosh t$, $y = \sinh t$ は $x^2 - y^2 = 1$ 上？ そのうちのどこ？

$$\{(x, y) | x = \cosh t,\ y = \sinh t\} = \left\{(x, y) | x^2 - y^2 = 1,\ x > 0\right\} \tag{62}$$

を示す．

- $\subset$：あきらか．
- $\supset$：$(x,y)\in$(右辺) とする．$x^2-y^2=1$ であり，$x>0$ である．

$$\sinh t = y \tag{63}$$

を解いてみる．$e^t = y\pm\sqrt{y^2+1}$ だが，$e^t>0$ なので $e^t=y+\sqrt{y^2+1}$ になって，$t=\log(y+\sqrt{y^2+1})$ が得られる．これを cosh に入れてみると実際 $\cosh t = x$ となり，(x,y) に対応するパラメタが得られたので，$(x,y)\in$(左辺)．

(b) $x^2-y^2=1$ に，直線の式を入れて様子を見る．直線なので，x に対して y が一意に定まるので，x の解の数だけ数えれば共有点の個数が得られる．

- $y=ax+b$ のとき：判別式として，$D=(2ab)^2-4(1-a^2)(-1-b^2)$ が得られる．よって，$a^2-b^2<1$ のとき 2 個，$a^2-b^2=1$ のとき 1 個，$a^2-b^2>1$ のとき 0 個．
- $x=c$ のとき：y の個数を数える．$c^2>1$ のとき 2 個，$c^2=1$ のとき 1 個，$c^2<1$ のとき 0 個となる．

(c) $y=a(x+1)$ を $(-1,0)$ を通る傾き a の直線とする．これと双曲線との共有点を考えると，

$$(x,y)=(\frac{-1-a^2}{1-a^2},\ \frac{-2a^3}{1-a^2}). \tag{64}$$

(d) $a=\pm1$ では定義されず，これは漸近線と平行である．

(問題 6) (a) 略．

(b) 始点を北極とする．終点を (u,v) とする．

$$(1-t)\begin{pmatrix}0\\0\\1\end{pmatrix}+t\begin{pmatrix}u\\v\\0\end{pmatrix}=\begin{pmatrix}tu\\tv\\1-t\end{pmatrix}. \tag{65}$$

(c) 代入する．

$$(tu)^2+(tv)^2+(1-t)^2=1 \tag{66}$$

を解く．$t^2(u^2+v^2+1)-2t=0$．よって，$t=\frac{2}{u^2+v^2+1}$．よって，球面の平面の点 (u,v) でのパラメータ付けは

$$(x,y,z)=(\frac{2u}{u^2+v^2+1},\ \frac{2v}{u^2+v^2+1},\ \frac{u^2+v^2-1}{u^2+v^2+1}). \tag{67}$$

(問題 7) パラメータとして，$(p_1,\dots,p_{n-1})$ を考える．いま，$(0,\dots,0,1)$ を北極とよぶことにする．北極を始点とし，$(p_1,\dots,p_{n-1},0)$ を終点とする線分を t をパラメータとしてあらわすと，

$$(1-t)\begin{pmatrix}0\\\vdots\\0\\1\end{pmatrix}+t\begin{pmatrix}p_1\\\vdots\\p_{n-1}\\0\end{pmatrix}=\begin{pmatrix}tp_1\\\vdots\\tp_{n-1}\\1-t\end{pmatrix}. \tag{68}$$

これが球面と交わるときを考え，

$$(tp_1)^2+\cdots+(tp_{n-1})^2+(1-t)^2=1. \tag{69}$$

$t^2(p_1^2+\cdots+p_{n-1}^2+1)-2t=0$．よって，

$$t=\frac{2}{p_1^2+\cdots+p_{n-1}^2+1}. \tag{70}$$

よって，$(p_1,\dots,p_{n-1})$ に対応する (パラメータとする) 球面の点は

$$(x_1,\dots,x_n)=(\frac{2p_1}{p_1^2+\cdots+p_{n-1}^2+1},\dots,\frac{2p_{n-1}}{p_1^2+\cdots+p_{n-1}^2+1},\ \frac{p_1^2+\cdots+p_{n-1}^2-1}{p_1^2+\cdots+p_{n-1}^2+1}). \tag{71}$$

(問題 8) $y^2 = cx^2 - x^3$，$c > 0$ を考える．

(a) 略．

(b) $y = mx$, $m^2 \neq c$ とする．共有点を考えると，$m^2x^2 = cx^2 - x^3$ より，$x = c - m^2$ となる．ただ 1 点である．原点での接線 2 本を引くとそんな気がする．

(c) 略．

(d) $y = tx$ と曲線との共有点は $(c - t^2, t(c - t^2))$ となる．これで $t^2 \neq c$ という条件の下でパラメータ付けが得られている．

(問題 9) (a) $y^2(a - x) = x^2(a + x)$．雑なほうだと $x = -a$ という線があらわれてしまう．すごい．どうしてこんなことになったんだ．

(b) $y = mx$ との共有点を考える．$x = a\frac{m^2-1}{m^2+1}$，$y = am\frac{m^2-1}{m^2+1}$ が得られる．

(問題 10) $y^2(a + x) = (a - x)^3$ を考える．$((a, 0), (0, \pm a)$ に点を持ち，$x = -a$ を漸近線とすることはすぐわかる．

(a) $y = m(x - a)$ を考える．($-a$ を根にしたらうまく行かなかった．) $x = a\frac{1-m^2}{1+m^2}$, $y = am\frac{1-m^2}{1+m^2}$．

(b) このような構成の点全体のなす集合は，計算すると $\left\{(x, y)|y = \frac{-\sqrt{a^2-x^2}}{a+x}(x - a),\ -a < x \leq a\right\}$．

$$\left\{(x, y)|y = \frac{-\sqrt{a^2 - x^2}}{a + x}(x - a),\ -a < x \leq a\right\} = \left\{(x, y)|y^2(a + x) = (a - x)^3,\ y \geq 0\right\} \tag{72}$$

を示せばよい．

- $\subset$：$(x, y) \in$ (左辺) とする．

$$y^2(a + x) = (\frac{-\sqrt{a^2 - x^2}}{a + x}(x - a))^2(a + x) \tag{73}$$
$$= \frac{(a^2 - x^2)(x - a)^2}{(a + x)^2}(a + x) \tag{74}$$
$$\overset{\boxed{0<x+a}}{=} (a - x)(x - a)^2 \tag{75}$$
$$= (a - x)^3. \tag{76}$$

よって，$(x, y) \in$ (右辺)．

- $\supset$：$(x, y) \in$ (右辺) とする．$y \geq 0$ である．$y^2(a + x) = (a - x)^3$ を考える．
  - $x = -a$ のとき：(左辺) $= 0$，(右辺) $= (2a)^3 = 8a^3 > 0$．これは矛盾．
  - $x < -a$ のとき：$x + a < 0$ となるので，(左辺) ≤ 0 となる．また，$x < -a$ なので，$-x > a$ であり，$a - x > 2a > 0$ なので，$(a - x)^3 > 0$ である．これは矛盾．
  - $a < x$ のとき：$0 < 2a < x + a$ なので，左辺は ≥ 0 であり，右辺は $a - x < 0$ なので < 0 であり，矛盾．

  よって，$-a < x \leq a$ である．このもとで，式を y について解いて，

$$y = \sqrt{\frac{(a - x)^3}{(a + x)}} \tag{77}$$
$$\overset{\boxed{x\leq a}}{=} (a - x)\sqrt{\frac{a - x}{a + x}} \tag{78}$$
$$= (a - x)\frac{\sqrt{a^2 - x^2}}{a + x} \tag{79}$$
$$= \frac{-\sqrt{a^2 - x^2}}{a + x}(x - a). \tag{80}$$

(c) a のシッソイドと $y = \frac{1}{2}(x + a)$ との共有点を考える．シッソイドは $y^2(a + x) = (a - x)^3$ に入れて，$y^2(2y) = (a - x)^3$．シッソイドは $-a < x \leq a$ でのみ定義されているので，$0 < \frac{1}{2}(x + a)$ であり，$0 < y$ である．よって，$2 = (\frac{a-x}{y})^3$．

(問題 11) $x^2 - y^2z^2 + z^3 = 0$ のパラメータ付け

$$x = t(u^2 - t^2) \tag{81}$$
$$y = u \tag{82}$$
$$z = u^2 - t^2 \tag{83}$$

を求めたい．$y = u$ と fix する．このとき，$x^2 = u^2z^2 - z^3$ が得られる．先の問をもう一度やる．$x = tz$ を考え，$t^2z^2 = u^2z^2 - z^3$ で，$z = u^2 - t^2$．$x = t(u^2 - t^2)$ である．[*1]

(問題 12) $\mathbf{V}(y - x^2, z - x^4)$ を考える．

(a) 略

(b) $x = t$, $y = t^2$, $z = t^4$.

(c) $x' = 1$, $y' = 2t$, $z' = 4t^3$．よって，求める曲面は，

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 \\ 2t \\ 4t^3 \end{pmatrix} s + \begin{pmatrix} t \\ t^2 \\ t^4 \end{pmatrix} = \begin{pmatrix} s + t \\ 2ts + t^2 \\ 4t^3 s + t^4 \end{pmatrix}. \tag{84}$$

(問題 13)

$$x = 1 + u - v, \tag{85}$$
$$y = u + 2v, \tag{86}$$
$$z = -1 - u + v \tag{87}$$

の陰関数表示を求める．

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ -1 \end{pmatrix} u + \begin{pmatrix} -1 \\ 2 \\ 1 \end{pmatrix} v \tag{88}$$

となっている．

$$\begin{pmatrix} 1 \\ 1 \\ -1 \end{pmatrix} \times \begin{pmatrix} -1 \\ 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 1+2 \\ 1-1 \\ 1+2 \end{pmatrix} = \begin{pmatrix} 3 \\ 0 \\ 3 \end{pmatrix} = 3 \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}. \tag{89}$$

はじめの式に $(1, 0, 1)^t$ を内積して，

$$x + z = 1 - 1 = 0. \tag{90}$$

(問題 14) (a) あきらか．

(b) $n = 2$ のときは示した (というかあきらか)．n で成立したとし，$n + 1$ での成立を示す．

$$\sum_{i=1}^{n} t_i \begin{pmatrix} x_i \\ y_i \end{pmatrix} = (\sum_{i=1}^{n-1} t_i \begin{pmatrix} x_i \\ y_i \end{pmatrix}) + t_n \begin{pmatrix} x_n \\ y_n \end{pmatrix} \tag{91}$$
$$= (\sum_{j=1}^{n-1} t_j)(\sum_{i=1}^{n-1} \frac{t_i}{\sum_{j=1}^{n-1} t_i} \begin{pmatrix} x_i \\ y_i \end{pmatrix}) + t_n \begin{pmatrix} x_n \\ y_n \end{pmatrix} \tag{92}$$
$$\tag{93}$$

だが，$(\sum_{i=1}^{n-1} \frac{t_i}{\sum_{j=1}^{n-1} t_i} \begin{pmatrix} x_i \\ y_i \end{pmatrix})$ は帰納法の仮定により S に属し，$\sum_{j=1}^{n-1} t_j + t_n = 1$ なので，$n = 2$ の場合を適用して全体が S に属す．

[*1] z について $z^3 - u^2z^2 + x^2$ がモニックなのがよい．

(問題 15) (a) あきらか．

$$\begin{pmatrix} x \\ y \end{pmatrix} = (1-t)^3 \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} + 3(1-t)^2 t \begin{pmatrix} x_1 \\ y_1 \end{pmatrix} + 3(1-t)t^2 \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} + t^3 \begin{pmatrix} x_3 \\ y_3 \end{pmatrix}. \tag{94}$$

(b) 係数の和は，

$$(1-t)^3 + 3(1-t)^2 t + 3(1-t)t^2 + t^3 = \sum_{i=0}^{3} {}_3C_i (1-t)^i t^{3-i} = (1-t+t)^3 = 1. \tag{95}$$

よって，制御多角形が凸ならば，ベジェ曲線はその制御多角形に包まれる．

(問題 16) $0 \leq t \leq 1$ をパラメータとし，パラメータ表示

$$x = \frac{(1-t)^2 x_1 + 2wt(1-t)x_2 + t^2 x_3}{(1-t)^2 + 2wt(1-t) + t^2}, \tag{96}$$

$$y = \frac{(1-t)^2 y_1 + 2wt(1-t)y_2 + t^2 y_3}{(1-t)^2 + 2wt(1-t) + t^2} \tag{97}$$

を考える．

(a) $w \geq 0$ なら分母は消えない？

$$(\text{分母}) = t^2(1-2w+1) + t(-2+2w) + 1 = 2(1-w)t^2 + 2(w-1)t + 1. \tag{98}$$

$$(\text{判別式})/4 = (w-1)^2 - 2(1-w) = w^2 - 1. \tag{99}$$

よって，$w < 1$ のときには分母は消えない．以降，$w \geq 1$ とする．

$$(\text{分母})|_{t=0} = 1 \tag{100}$$

$$(\text{分母})|_{t=1} = 1. \tag{101}$$

また，$1 - w \geq 0$ で，グラフは上に凸なので，やはり $[0,1]$ で根を持たない．

(b)

$$x(0) = x_1 \tag{102}$$

$$y(0) = y_1 \tag{103}$$

$$x(1) = x_3 \tag{104}$$

$$y(1) = y_3. \tag{105}$$

よって，(x_1, y_1) は曲線の始点に，(x_3, y_3) は終点になっている．

(c)

$$f(t) = (1-t)^2 + 2wt(1-t) + t^2, \tag{106}$$

$$g(t) = (1-t)^2 x_1 + 2wt(1-t)x_2 + t^2 x_3, \tag{107}$$

$$h(t) = (1-t)^2 y_1 + 2wt(1-t)y_2 + t^2 y_3 \tag{108}$$

としておく．

$$f'(t) = 2(1-t)(-1) + 2w((1-t) + t(-1)) + 2t \tag{109}$$

$$= 4t - 2 + 2w(1-2t) \tag{110}$$

$$= 2(2t - 1 + w(1-2t)), \tag{111}$$

$$g'(t) = 2(1-t)(-1)x_1 + 2w((1-t) + t(-1))x_2 + 2tx_3 \tag{112}$$

$$= 2(t-1)x_1 + 2w(1-2t)x_2 + 2tx_3, \tag{113}$$

$$h'(t) = 2(t-1)y_1 + 2w(1-2t)y_2 + 2ty_3. \tag{114}$$

よって，

$$x'(t) = (\frac{g}{f})'(t) = \frac{g'f - gf'}{f^2}(t), \tag{115}$$

$$y'(t) = (\frac{h}{f})'(t) = \frac{h'f - hf'}{f^2}(t). \tag{116}$$

よって，

$$x'(0) = \frac{(-2x_1 + 2wx_2)\cdot 1 - x_1 \cdot 2(-1+w)}{1} \tag{117}$$

$$= 2w(x_2 - x_1), \tag{118}$$

$$y'(0) = 2w(y_2 - y_1), \tag{119}$$

$$x'(1) = \frac{(-2wx_2 + 2x_3)\cdot 1 - x_3 \cdot 2(1-w)}{1} \tag{120}$$

$$= 2w(x_3 - x_2), \tag{121}$$

$$y'(1) = 2w(y_3 - y_2). \tag{122}$$

たしかに，始点では (x_1, y_1) から (x_2, y_2) に進みはじめ，終点では (x_2, y_2) から (x_3, y_3) に向かっている．

(d) 係数の総和は確かに 1 であり，三角形は常に凸なので，曲線は制御多角形，すなわち (x_1, y_1), (x_2, y_2), (x_3, y_3) のなす三角形に包まれる．

(e)

$$\begin{pmatrix} x(1/2) \\ y(1/2) \end{pmatrix} = \frac{1}{1+w} \cdot \frac{\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} + \begin{pmatrix} x_3 \\ y_3 \end{pmatrix}}{2} + \frac{w}{1+w} \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} \tag{123}$$

？ すなわち，曲線の真ん中の点は，始点と終点の中点と制御三角形の残りの頂点とを $1 : w$ で分けた点？ x だけ考えれば十分．

$$x(1/2) = \frac{\frac{x_1}{4} + \frac{w}{2}x_2 + \frac{x_3}{4}}{\frac{1}{2} + \frac{w}{2}} \tag{124}$$

$$= \frac{x_1 + 2wx_2 + x_3}{2(1+w)} \tag{125}$$

$$= \frac{1}{1+w}(\frac{x_1}{2} + \frac{x_3}{2}) + \frac{w}{1+w}x_2. \tag{126}$$

後半はあきらか．

(f) 上式と述べたことよりあきらか．

(問題 17) 始点と終点での速度を考え，

$$(x_1, y_1) = (1, 0), \quad (x_2, y_2) = (1, 1), \quad (x_3, y_3) = (0, 1) \tag{127}$$

とすればよいことがわかる．また，真ん中の点で

$$w : 1 = (1 - \frac{1}{\sqrt{2}}) : (\sqrt{2} - 1) \tag{128}$$

すなわち，

$$w = \frac{1 - \frac{1}{\sqrt{2}}}{\sqrt{2} - 1} = \frac{1}{\sqrt{2}} \tag{129}$$

とならなければならない．このとき，

$$x(t) = \frac{(1-t)^2 \cdot 1 + 2\frac{1}{\sqrt{2}} \cdot t(1-t) \cdot 1 + t^2 \cdot 0}{(1-t)^2 + 2\frac{1}{\sqrt{2}} t(1-t) + t^2} \tag{130}$$

$$= \frac{(1-t)^2 + \sqrt{2}t(1-t)}{(1-t)^2 + \sqrt{2}t(1-t) + t^2}, \tag{131}$$

$$y(t) = \frac{(1-t)^2 \cdot 0 + 2\frac{1}{\sqrt{2}} \cdot t(1-t) \cdot 1 + t^2 \cdot 1}{(1-t)^2 + 2\frac{1}{\sqrt{2}} t(1-t) + t^2} \tag{132}$$

$$= \frac{\sqrt{2}t(1-t) + t^2}{(1-t)^2 + \sqrt{2}t(1-t) + t^2}. \tag{133}$$

パラメタ付けされた曲線が円上にあることは計算で得られる．逆に，円弧がパラメタ付けされた曲線上にあることは，任意の x について対応する t があることは分かり，そこから y が t であらわせて，それがパラメタと一致する (略)．

1.4 イデアル

多変数多項式環の部分集合で，(1)0 を含み，(2) 和について閉じ，(3)$k[x_1, \ldots, x_n]$ 倍について閉じるものをイデアルという．$f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$ について，

$$\langle f_1, \ldots, f_m \rangle = \left\{ \sum_{i=1}^{m} c_i f_i | c_i \in k[x_1, \ldots, x_n] \right\} \tag{134}$$

を，$f_1, \ldots, f_m$ で生成されたイデアルとよぶ．というのは，これがイデアルになるからである．0 の所属は全ての係数を 0 にすれば示される．和について閉じることは，係数の和を考えれば従い，$k[x_1, \ldots, x_n]$ 倍について閉じることも同様に係数を見ればわかる．この生成されたイデアルの元は，連立方程式 $f_1 = \cdots = f_m = 0$ が成り立っているとき，その元も 0 となることに注意する．したがって，連立方程式から文字の消去などを足し引きかけ算をして行ったとき，その元はもとの連立方程式の式から生成されたイデアルに所属することになる．

イデアル $I \subset k[x_1, \ldots, x_n]$ について，$I = \langle f_1, \ldots, f_n \rangle$ となる $f_1, \ldots, f_n \in k[x_1, \ldots, x_n]$ が存在するとき，I を有限生成であるという．あとで，任意の多項式環が有限生成であることを見る．またこのとき，$f_1, \ldots, f_n$ を I の基底であるという．

同じアフィン多様体でも表示はいろいろありうるが，アフィン多様体はそれを定義する連立方程式のイデアルによってのみ決定することがわかる：$f_1, \ldots, f_a, g_1, \ldots, g_b \in k[x_1, \ldots, x_n]$ とし，$\langle f_1, \ldots, f_a \rangle = \langle g_1, \ldots, g_b \rangle$ であるとする．このとき，$\mathbf{V}(f_1, \ldots, f_a) = \mathbf{V}(g_1, \ldots, g_b)$ となる．

証明

$\mathbf{V}(f_1, \ldots, f_a) \subset \mathbf{V}(g_1, \ldots, g_b)$ を示せば十分．$x \in \mathbf{V}(f_1, \ldots, f_a)$ とする．x は $f_1, \ldots, f_a$ のどれでも消える．$\langle f_1, \ldots, f_a \rangle = \langle g_1, \ldots, g_b \rangle$ なので，x は $g_1, \ldots, g_b$ はどれも $f_1, \ldots, f_a$ の線形結合で書かれ，よってどの $g_1, \ldots, g_b$ でも消える．よって，$x \in \mathbf{V}(g_1, \ldots, g_b)$ であり，$\mathbf{V}(f_1, \ldots, f_a) \subset \mathbf{V}(g_1, \ldots, g_b)$ である．

(証終)

アフィン多様体は，多項式の組がすべて消える点の集合として定義されたが，ではアフィン多様体上で消える多項式は定義につかった多項式だけなのだろうか？ それらを全てもとめることはできるか？ 例えば，ねじれ 3 次曲線 $\mathbf{V}(y - x^2, z - x^3)$ は，$x^2 = y$ を x^3 に差し込んで，$z - xy$ という，ねじれ 3 次曲線上消える多項式を作ることができる．考えるために，アフィン多様体について，その上で消える多項式全体を考える．すなわち：アフィン多様体 $V \subset k^n$ について，

$$\mathbf{I}(V) = \left\{ f \in k[x_1, \ldots, x_n]; f \text{は} V \text{上消える} \right\} \tag{135}$$

とする．これはイデアルになるので，アフィン多様体 V のイデアルとよぶ．イデアルとなることを示す．

証明
$V \subset k^n$ をアフィン多様体とする．$f, g \in \mathbf{I}(V)$ とし，$c \in k[x_1, \ldots, x_n]$ とする．また，$\mathbb{o} = (a_1, \ldots, a_n) \in V$ とする．$f(\mathbb{o}) = g(\mathbb{o}) = 0$ である．

- 0 の所属：多項式 0 は $\mathbb{o}$ を消すので，$0 \in \mathbf{I}(V)$．
- 和について閉じる：$(f+g)(\mathbb{o}) = f(\mathbb{o}) + g(\mathbb{o}) = 0$．よって，$f + g \in \mathbf{I}(V)$．
- スカラー倍について閉じる：$(cf)(\mathbb{o}) = c(\mathbb{o})f(\mathbb{o}) = c(\mathbb{o}) \cdot 0 = 0$．よって，$cf \in \mathbf{I}(V)$．

(証終)
多様体のイデアルの例として，$\mathbf{I}(\{(0,0)\}) \subset k[x,y]$ を考える．つまり，$(0,0)$ で消える 2 変数多項式全体の生成するイデアルである．これについて，$\mathbf{I}(\{(0,0)\}) = \langle x, y \rangle$ を示そう．

証明

- $\supset$：あきらか．
- $\subset$：$f \in \mathbf{I}(\{(0,0)\})$ とする．$f \in k[x,y]$ なので，

$$f = \sum_{i=0}^{N} \sum_{j=0}^{M} c_{i,j} x^i y^j \tag{136}$$

と書く．$f(0,0) = c_{0,0} = 0$ となる．よって，

$$f = \sum_{i=1}^{N} c_{i,0} x^i + \sum_{j=1}^{M} c_{0,j} y^j + \sum_{i=1}^{N} \sum_{j=1}^{M} c_{i,j} x^i y^j \tag{137}$$

となり，$f \in \langle x, y \rangle$ である．

(証終)
次に，$\mathbf{I}(k^n)$ を考える．$\mathbf{I}(k^n) = \{0\}$ を示す．

証明

- $\supset$：あきらか．
- $\subset$：k^n 全域で消える多項式は無限個の根を持ち，それは多項式 0 にならざるをえない．

(証終)
$V = \mathbf{V}(y - x^2, z - x^3)$ とし，$\mathbf{I}(V) = \langle y - x^2, z - x^3 \rangle$ を示す．

証明

- $\supset$：あきらか．
- $\subset$：一般の単項式 $x^\alpha y^\beta z^\gamma$ について，

$$x^\alpha y^\beta z^\gamma = x^\alpha ((y - x^2) + x^2)^\beta ((z - x^3) + x^3)^\gamma \tag{138}$$

$$\tag{139}$$

であるが，これを展開すれば $x^\alpha y^\beta z^\gamma \in (k[x])\langle y - x^2, z - x^3 \rangle$ がわかる (記法は察せ)．多項式は単項式の線形結合なので，任意の $k[x,y,z]$ の元について，これは $(k[x])\langle y - x^2, z - x^3 \rangle$ に属する．
$f \in \mathbf{I}(V)$ とする．先のことより，

$$f(x,y,z) = (y - x^2) f_1(x) + (z - x^3) f_2(x) + f_3(x) \tag{140}$$

となる $f_1, f_2, f_3 \in k[x]$ が存在する．V は $t \mapsto (t, t^2, t^3)$ というパラメタ付けがあるので，$f \in \mathbf{I}(V)$ より，$t \in k$ について，$f(t, t^2, t^3) = 0$ が成立しなければならない．このとき，

$$f(t, t^2, t^3) = f_3(t) = 0. \tag{141}$$

$t \in k$ は任意だったので，f_3 は無数の根を持つことになり，$f_3 = 0$ である．よって，

$$f(x,y,z) = (y - x^2) f_1(x) + (z - x^3) f_2(x) \tag{142}$$

であり，$f \in (k[x])\langle y-x^2, z-x^3\rangle \subset \langle y-x^2, z-x^3\rangle$.

(証終) この例は 2 つの意味を持つ．まず，f_3 が恒等的に消えるかどうかと，$f \in \langle y-x^2, z-x^3\rangle$ となるかが等価であることが証明から分かり，f が $\langle y-x^2, z-x^3\rangle$ に属するための条件が与えられたことである．これはパラメタ付けに依存した方法だが，一般的な方法を今後扱う．次に，$\mathbf{I}(\mathbf{V}(y-x^2, z-x^3)) = \langle y-x^2, z-x^3\rangle$ となっており，イデアルから多様体を作り，また元のイデアルに戻っていることである．これは一般的には成立しない：$f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ $\langle f_1, \ldots, f_s\rangle \subsetneq \mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$.

証明

- 包含：$f \in \langle f_1, \ldots, f_s\rangle$ とする．$f = c_1 f_1 + \ldots c_s f_s$ となる $c_1, \ldots, c_s \in k[x_1, \ldots, x_n]$ が存在する．$f \in \mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$ とは，f が $\mathbf{V}(f_1, \ldots, f_s)$ 上すべてで消えることを意味する．$x \in \mathbf{V}(f_1, \ldots, f_s)$ とすると，x は $f_1, \ldots, f_s$ のすべてで消えるので，f でも消える．x は任意だったので，f は $\mathbf{V}(f_1, \ldots, f_s)$ の任意の点で消える．よって，$f \in \mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$ となる．
- 不一致：$\mathbf{I}(\mathbf{V}(x^2, y^2))$ が $\langle x^2, y^2\rangle$ より真に広いことを示す．$\mathbf{V}(x^2, y^2)$ は $x^2 = 0$, $y^2 = 0$ の定めるアフィン多様体だが，これは $(x, y) = (0, 0)$ なので，$\mathbf{I}(\mathbf{V}(x^2, y^2)) = \mathbf{I}(\langle(0, 0)\rangle) = \langle x, y\rangle$．$x \in \langle x, y\rangle$ だが，$x \notin \langle x^2, y^2\rangle$ である．

(証終)

イデアルは多様体を定めていたが，多様体のイデアルも多様体を定める．すなわち：アフィン多様体 V, W について，$\mathbf{I}(V) = \mathbf{I}(W) \iff V = W$.

証明

$\mathbf{I}(V) \subset \mathbf{I}(W) \iff V \supset W$ を示せば，対称性より十分である．

- $\mathbf{I}(V) \subset \mathbf{I}(W) \implies V \supset W$：$x \in W$ とする．x は W を定める多項式で消える．$f_1, \ldots, f_s$ を V を定める多項式とする．$f_1, \ldots, f_s$ が x を消すだろうか？ $\mathbf{I}(V)$ は V を消す多項式全体であり，$f_1, \ldots, f_s$ は V を消すから，$f_1, \ldots, f_s \in \mathbf{I}(V)$ であり，仮定より $f_1, \ldots, f_s \in \mathbf{I}(W)$ である．したがって，$f_1, \ldots, f_s$ は W を消す．$x \in W$ だったので，$f_1, \ldots, f_s$ は x を消す．よって，$W \subset V$.
- $V \supset W \implies \mathbf{I}(V) \subset \mathbf{I}(W)$：$f \in \mathbf{I}(V)$ とする．f は V 上の点を消す．$V \supset W$ なので，f は W を消す．よって，$f \in \mathbf{I}(W)$ である．

(証終)

イデアルについて次の問をあげる．

- イデアルの記述：任意のイデアルは有限生成で，I をイデアルとすれば $I = \langle f_1, \ldots, f_s\rangle$ なる $f_1, \ldots, f_s$ があるか？
- イデアルの所属：$\langle f_1, \ldots, f_s\rangle$ について，$f \in \langle f_1, \ldots, f_s\rangle$ かどうかを判定するアルゴリズムは？ 先にねじれ 3 次曲線については，そのパラメタ付けの特殊性を利用して，$f(t, t^2, t^3)$ が消えるかどうかで判定できるのであった．これが一般化できるか？
- イデアルと多様体のイデアルの関係はどんなだろうか？ (イデアル)⊂(多様体のイデアル) はすでに言ったが，逆はどんなときなのだろうか？

(問題 1) $x^2 + y^2 = 1$ と $xy = 1$ を考える．

(a) $x^4 + x^2y^2 = x^2$ に $xy = 1$ を入れて，$x^4 + 1 = x^2$ となり，$x^4 - x^2 + 1 = 0$ を得る．

$$x^4 - x^2 + 1 = x^2(x^2 + y^2 - 1) - (xy + 1)(xy - 1) \in \langle x^2 + y^2 - 1, xy - 1\rangle. \tag{143}$$

(問題 2) $f_1, \ldots, f_s \in I \iff \langle f_1, \ldots, f_s\rangle \in I$？

- $\supset$：自明．
- $\subset$：$c_1 f_1 + \cdots + c_s f_s \in k[x_1, \ldots, x_n]$ とする．I はスカラー倍で閉じるので，$f_1 \in I$ なので $c_1 f_1 \in I$ である．同様に $c_2 f_2, \ldots, c_s f_s \in I$ である．I は和で閉じるので，$c_1 f_1 + \cdots + c_s f_s \in I$.

(問題 3) (a) $\langle x + y, x - y\rangle = \langle x, y\rangle$？

- $\subset$：自明．
- $\supset$：先の問いより，$x, y \in \langle x+y, x-y\rangle$ を言えば十分．$x = \frac{x+y}{2} + \frac{x-y}{2} \in \langle x+y, x-y\rangle$．$y = \frac{x+y}{2} - \frac{x-y}{2} \in \langle x+y, x-y\rangle$．

(b) $\langle x+xy, y+xy, x^2, y^2\rangle = \langle x, y\rangle$？

- $\subset$：自明．
- $\supset$：$x, y \in \langle x+xy, y+xy, x^2, y^2\rangle$？ $I = \langle x+xy, y+xy, x^2, y^2\rangle$ とする．$x-y = (x+xy)-(y+xy) \in I$ となる．$x^2 - xy = x(x-y) \in I$ となる．$xy = (-1)(x^2-xy)+x^2 \in I$ となる．$x = (x+xy)-xy \in I$．$y = (y+xy) - xy \in I$．

(c) $\langle 2x^2+3y^2-11, x^2-y^2-3\rangle = \langle x^2-4, y^2-1\rangle$？

- $\subset$：基底の所属を言えば十分．$2x^2+3y^2-11 = 2(x^2-4)+3(y^2-1) \in \langle x^2-4, y^2-1\rangle$．$x^2-y^2-3 = (x^2-4)-(y^2-1) \in \langle x^2-4, y^2-1\rangle$．
- $\supset$：基底の所属を言えば十分．$x^2-4 = \frac{1}{5}(2x^2+3y^2-11)+\frac{3}{5}(x^2-y^2-3) \in \langle 2x^2+3y^2-11, x^2-y^2-3\rangle$．$y^2-1 = \frac{1}{5}(2x^2+3y^2-11) - \frac{2}{5}(x^2-y^2-3) \in \langle 2x^2+3y^2-11, x^2-y^2-3\rangle$．

標数 0 でいいんだっけ？

(問題 4) さっきやった．

(問題 5) $\mathbf{V}(x+xy, y+xy, x^2, y^2) = \mathbf{V}(x, y)$？ アフィン多様体はそれに対応するイデアルによって定まるが，先の問いより $\langle x+xy, y+xy, x^2, y^2\rangle = \langle x, y\rangle$ であった．

(問題 6) (a) 仮に $\langle x\rangle$ が k-ベクトル空間が仮に有限次元であるとする．すると，次数が最高のものより大きい多項式を考えれば，それが基底の k 係数線形結合で書けないので矛盾である．

(b) イデアルは $k[x, y]$ 係数なので，

$$0 = \underbrace{(\ y\ )}_{\text{係数}}\underbrace{x}_{\text{基底}} - \underbrace{(\ x\ )}_{\text{係数}}\underbrace{y}_{\text{基底}}. \tag{144}$$

(c) 上と同様に，$f_j f_i - f_i f_j = 0$．

(d)

$$x^2 + xy + y^2 = (x+y)\cdot x + y \cdot y = x \cdot x + (x+y)\cdot y. \tag{145}$$

(e) $\{x\}$ は，この真部分集合は空になるので，極小基底である．$\{x+x^2, x^2\}$ は，この真部分集合は $\{x+x^2\}, \{x^2\}$ である．$\langle x+x^2\rangle$ の元は 0 でなければすべて 2 次以上なので，x は属さず，$k[x]$ の基底にならない．$\langle x^2\rangle$ の元も同様．

線形代数の場合も，基底から 1 個外したらもとのものは書けなくなってしまう．

(問題 7) $\mathbf{I}(\mathbf{V}(x^n, y^m)) = \mathbf{I}(\{0\}) = \langle x, y\rangle$．

(問題 8) (a) $\mathbf{I}(V)$ は根基イデアル？ $f^n \in \mathbf{I}(V)$ とし，n をこのようなもののうち最小のものとする．$n = 1$ を示せばよい．$n > 1$ とする． $V = \mathbf{V}(\langle f_1, \ldots, f_s\rangle)$ とする．$\langle f_1, \ldots, f_s\rangle \subset \mathbf{I}(V)$．$f^n$ は $f_1, \ldots, f_s$ で消える点すべてを消す．n は最小としたので，f^{n-1} には $f_1, \ldots, f_s$ で消える点のうち，消えないものがある．これを $x \in k^N$ とする．$f^{n-1}(x) \neq 0$ である．

$$0 = f^n(x) = \underbrace{f^{n-1}(x)}_{\neq 0} f(x). \tag{146}$$

よって，$f(x) = 0$ である．これは x と n の性質に矛盾する．

(b) $\langle x^2, y^2\rangle$ は根基イデアルでない？ $x^2 \in \langle x^2, y^2\rangle$ だが $x \notin \langle x^2, y^2\rangle$ である．

(問題 9) $V = \mathbf{V}(y-x^2, z-x^3)$ とする．$\mathbf{I}(V) = \langle y-x^2, z-x^3\rangle$ はすでに示した．

(a) $y^2-xz \in \mathbf{I}(V)$？y^2-xz を関数と見て，V を消すことを示せばよい．パラメタ付けより，$V = \langle (t, t^2, t^3) | t \in \mathbb{R}\rangle$ である．$(y^2-xz)(t, t^2, t^3) = (t^2)^2 - t\cdot t^3 = 0$ なので，$y^2 - xz$ を関数と見たとき，これは V を全て消す．

(b) 結合であらわせ？

$$y^2 - xz = (y+x^2)(y-x^2) - x(z-x^3) \in \langle y-x^2, z-x^3\rangle. \tag{147}$$

(問題 10) $\langle x-y\rangle = \mathbf{I}(\mathbf{V}(x-y))$？ $\subset$ は一般に成立する．$\supset$ を示す．$f \in \mathbf{I}(\mathbf{V}(x-y)) \subset k[x,y]$ とする．$k[x,y]$ の単項式は $k[x,y](x-y)+k[x]$ の形に書き直せるので，$k[x,y]$ も $k[x,y](x-y)+k[x]$ の形にでき，

$$f(x,y) = g_1(x,y)(x-y) + g_2(x), \quad g_1 \in k[x,y],\, g_2 \in k[x] \tag{148}$$

とあらわせる．$\mathbf{V}(x-y) = \{(t,t)|t \in k\}$ とパラメタ付けされるので，$f(t,t) = 0$ が恒等的に成立しなければならない．よって，

$$f(t,t) = g_2(t) = 0. \tag{149}$$

g_2 は無限体 k 上で無数の根を持つことになるので，g_2 は多項式として 0 である．よって，$f(x,y) = g_1(x,y)(x-y)$ であり，$f \in \langle x-y\rangle$ である．よって，$\mathbf{I}(\mathbf{V}(x-y)) \subset \langle x-y\rangle$ である．

(問題 11) (t,t^3,t^4) を考える．

(a) V はアフィン多様体？ $V = \left\{(t,t^3,t^4)\right\} = \mathbf{V}(\langle y-x^3, z-x^4\rangle)$ である．

(b) $f \in \mathbf{I}(\mathbf{V}(y-x^3, z-x^4)) \subset k[x,y,z]$ とする．単項式は展開して，$k[x,y,z](y-x^3)+k[x,y,z](z-x^4)+k[x]$ に属する．$k[x,y,z]$ も同様なので，

$$f = g_1(y-x^3) + g_2(z-x^4) + g_3 \tag{150}$$

となる $g_1, g_2 \in k[x,y,z]$, $g_3 \in k[x]$ である．f は $\mathbf{V}(\langle y-x^3, z-x^4\rangle) = \left\{(t,t^3,t^4)\right\}$ を消すので，$f(t,t^3,t^4) = 0$ が恒等的に成り立たなければならず，

$$f(t,t^3,t^4) = g_3(t) = 0 \tag{151}$$

となる．g_3 は無限体 k 上で無限個の根を持つので，g_3 は多項式として 0 である．よって，$f = g_1(y-x^3) + g_3(z-x^4)$ であり，$f \in \langle y-x^3, z-x^4\rangle$ である．$\langle y-x^3, z-x^4\rangle \subset \mathbf{I}(\mathbf{V}(y-x^3, z-x^4))$ は一般に成立するので，

$$\langle y-x^3, z-x^4\rangle = \mathbf{I}(\mathbf{V}(y-x^3, z-x^4)) = \mathbf{I}(V). \tag{152}$$

(問題 12) (t^2,t^3,t^4) を考える．これで定まる点の集合を V とする．

(a) $\mathbf{V}(x^3-y^2, y^4-z^3)$ を考える．$(x,y,z) \in \mathbf{V}(x^3-y^2, y^4-z^3)$ とする．$x^3 = y^2$, $y^4 = z^3$ となる．$t = y^{1/3}$ とすれば (これは一意に定まる)，$x = t^2$, $y = t^3$, $z = t^4$ となり，パラメタ付けがなっている．逆はあきらかなので，$V = \mathbf{V}(x^3-y^2, y^4-z^3)$ である．

(a') $\mathbf{V}(z-x^2, y^2-x^3) = V$ である．t は同様に定めればよい．

(b) $f \in \mathbf{I}(V) \subset k[x,y,z]$ とする．単項式 $x^\alpha y^{2\beta} z^\gamma (\beta \geq 1)$ については，

$$x^\alpha y^{2\beta} z^\gamma = x^\alpha((y^2-x^3)+x^3)^\beta((z-x^2)+x^2)^\gamma \in k[x,y,z](y^2-x^3) + k[x,y,z](z-x^2). \tag{153}$$

単項式 $x^\alpha y^{2\beta+1} z^\gamma (\beta \geq 1)$ については y を 1 個のけて同様に，$k[x,y,z](y^2-x^3) + k[x,y,z](z-x^2)$ となる．よって，

$$f(x,y,z) = k[x,y,z](y^2-x^3) + k[x,y,z](z-x^2) + k[x,z]y + k[x,z] \tag{154}$$

となる．さらに $k[x,z]$ のうち z が含まれているものは $z = (z-x^2) + x^2$ として，

$$f(x,y,z) = k[x,y,z](y^2-x^3) + k[x,y,z](z-x^2) + k[x]y + k[x] \tag{155}$$

とできる．よって，

$$f = g_1(y^2-x^3) + g_2(z-x^2) + h_1 y + h_2 \tag{156}$$

となる $g_1, g_2 \in k[x,y,z]$，$h_1, h_2 \in k[x]$ が存在する．パラメタ表示により，$f(t^2,t^3,t^4) = 0$ なので，

$$0 = f(t^2,t^3,t^4) = h_1(t^2)t^3 + h_2(t^2). \tag{157}$$

よって，$k[t]$ として $h_1(t^2)t^3 + h_2(t^2) = 0$ である．f に今度は $((-t)^2, (-t)^3, (-t)^4) = (t^2, -t^3, t^4)$ を代入すると，

$$0 = f(t^2, -t^3, t^4) = -h_1(t^2)t^3 + h_2(t^2). \tag{158}$$

よって，$k[t]$ として $-h_1(t^2)t^3 + h_2(t^2) = 0$ である．$k[t]$ として

$$h_1(t^2)t^3 + h_2(t^2) = 0 \tag{159}$$
$$-h_1(t^2)t^3 + h_2(t^2) = 0. \tag{160}$$

よって，$h_2(t^2) = 0$ であり，$h_2 = 0$ である．さらに $h_1(t^2)t^3 = 0$ が従い，$h_1 = 0$ である．よって，

$$f = g_1(y^2 - x^3) + g_2(z - x^2). \tag{161}$$

よって，$f \in \langle y^2 - x^3, z - x^2 \rangle$ である．よって，$\mathbf{I}(V) \subset \langle y^2 - x^3, z - x^2 \rangle$ である．逆は示してあるので，$\mathbf{I}(V) = \langle y^2 - x^3, z - x^2 \rangle$ である．

(問題 13) I は $\mathbb{F}_2$ を消す多項式全体のなすイデアルとする．

(a) 基底 $x^2 - x, y^2 - y$ の所属を言えばよい．

$$(x^2 - x)(1,1) = 0, \quad (x^2 - x)(1,0) = 0, \quad (x^2 - x)(0,1) = 0, \quad (x^2 - x)(-,0) = 0. \tag{162}$$

$y^2 - y$ についても同様．よって，$x^2 - x$, $y^2 - y \in I$．

(b) 略．

(c) (x, y) に 4 通り入れる．略．

(d) $f \in I$ とする．(b) より

$$f(x, y) = A(x^2 - x) + B(y^2 - y) + axy + bx + cy + d \tag{163}$$

となる $A, B, a, b, c, d \in \mathbb{F}_2$ と書ける．$f(0,0) = f(1,0) = f(0,1) = f(0,0) = 0$ が $f \in I$ から従うので，(c) より $a = b = c = d = 0$ である．よって，

$$f(x, y) = A(x^2 - x) + B(y^2 - y) \tag{164}$$

である．よって，$f \in \langle x^2 - x, y^2 - y \rangle$ であり，$I \subset \langle x^2 - x, y^2 - y \rangle$．よって，$I = \langle x^2 - x, y^2 - y \rangle$．

(e) $x^2y + y^2x = x^2y + y^2x + 0 \cdot xy = x^2y + y^2x + 2 \cdot xy = y(x^2 + x) + x(y^2 + y)$．

(問題 14) 略．

(問題 15) (a) 略．

(b) $f \in \mathbf{I}(X)$ とする．$(x, y) \neq (1, 1) \in \mathbb{R}^2$ なら $f(x, y) = 0$ となる．$f(t, t) = 0$ が成り立つが，これは無数の根を持つことになり，f は 0 である．よって，$\mathbf{I}(X) = \{0\}$．

(c) 略．

1.5 1 変数多項式

多項式の割り算について研究する．

0 でない 1 変数多項式 $f \in k[x]$ について，その先頭項 $\mathrm{LT}f$ は，その最高次の項である．$f, g \in k[x]$ について，$\deg \mathrm{LT}(f) \leq \deg \mathrm{LT}(g) \iff \mathrm{LT}(f) | \mathrm{LT}(g)$ である．証明はかんたん．

1 変数多項式の割り算を考える．

$$^{\forall} f \in k[x]\colon {}^{\forall} g \in k[x] \setminus \{0\}\colon {}^{\exists!} p, q \in k[x]\colon f = gp + q \text{かつ} (q = 0 \text{または} \deg q < \deg g) \tag{165}$$

が成り立つ．また，このような p, q を求めるアルゴリズムが存在する．

Algorithm 1 1 変数多項式の割り算

証明

1: $q := 0$
2: $r := f$
3: **while** $\deg r \geq \deg g$ **do**
4: $\quad a := \dfrac{\mathrm{LT}r}{\mathrm{LT}g}$
5: $\quad q \Leftarrow q + a$
6: $\quad r \Leftarrow r - ag$
7: **end while**

(0 の次数を $-\infty$ としておけばこれで通る．) まず，これが正しく動作すること，すなわち，この手続が停止することと，望む結果が得られることを示す．

- 手続が停止すること：L.3 から L.7 で，更新される前の q, r をそのまま q, r，更新されたあとの q, r を q', r' とする．L.5 より $q' = q + a$，6 行目より $r' = r - ag$ となる．a の定義より，r の先頭項は消えるので，$\deg r' < \deg r$ である．よって，L.3 から L.7 のループを高々 $\deg f + 1$ 回繰り返せば次数は $\deg f + 1$ だけ減り，3 行目の条件から抜け出すことになる．
- 望む結果が得られること：L.2，L.7 の時点で常に $f = gq + r$ の関係があることを示す．L.2 の時点では自明．L.3 から L.7 の更新前後の q, r を上と同様にする．

$$q' = q + a \tag{166}$$
$$r' = r - ag \tag{167}$$

となる．

$$f = gq + r = g(q' - a) + (r' + ag) = gq' + r' \tag{168}$$

となり，確かに成り立つ．L.3 から L.7 のループから抜けたときには $\deg r < \deg g$ となっているから，このとき q, r は $f = gq + r$ をみたし，かつ $\deg r < \deg g$ となっている．これが望む結果であった．

最後に q, r の一意性を示す．仮に $f = gq' + r'$, $\deg r' < \deg g$ となる q', r' がもう 1 組あったとする．$gq + r = f = gq' + r'$ となり，$g(q - q') + (r - r') = 0$ となる．$g(q - q') = r' - r$ である．$\deg(r' - r) \leq \max(\deg r', \deg r) < \deg g$ であるから，$\deg g(q - q') < \deg g$ である．$g \neq 0$ であったから，$q = q'$ となるしかない．よってさらに $r = r'$ である．一意性が示された．

(証終)

これを使って，多項式の根が有限個であることが示せる：体 k 上の 0 でない多項式 $f \in k[x]$ について，f は高々 $\deg f$ 個の根を持つ．

証明

- $\deg f = 0$ のとき：$f \neq 0$ なので，根は 0 個であり，正しい．
- $\deg f > 0$ のとき：$(\deg f) - 1$ 次の多項式については成立すると仮定し，f で成立することを示す (背理法)．
  f が根を持たないときにはあきらかに成立するので，以降 f は根を持つとする．その根を $a \in k$ とする．$f(a) = 0$ となる．f を $x - a$ で割り，

$$f = (x - a)q + r, \quad \deg r < \deg q \tag{169}$$

となる $q, r \in k[x]$ を得る．1 次式 $x - a$ で割ったので，$\deg r < 1$ であり，多項式 r は 0 を含め定数である．$0 = f(a) = (a - a)q(a) + r(a) = r(a)$ である．よって，r は多項式として 0 である．よって，$f = (x - a)q$ である．今，$x - a$ がモニックなので $\deg f = \deg(x - a) + \deg q$ であり，$\deg q = \deg f - \deg(x - a) = (\deg f) - 1$．帰納法の仮定より，$q$ の根は高々 $(\deg f) - 1$ 個である．$b \neq a$ が f の根であるなら，b は q の根であることを示す．$0 = f(b) = (b - a)q(b)$ であり，$b - a \neq 0$ なので $q(b) = 0$ である．まとめると，f の根は a であるか，高々 $(\deg f) - 1$ 個しかない q の根であるから，f の根は高々 $\deg f$ 個である．

(証終)

これを使って $k[x]$ のイデアルの構造を定めることができる：イデアル $I \subset k[x]$ について，$f \in k[x]$ が存在して，$I = \langle f \rangle$ となる．さらに，このような f は非 0 な定数倍を除いて一意に定まる．

証明

$I = \{0\}$ のときには $I = \langle 0 \rangle$ とすればよい．以降，$I \neq \{0\}$ とする．I のうち，0 でない次数が最小の多項式を f とする．$I = \langle f \rangle$ を示す．$\langle f \rangle \subset I$ は自明なので，$I \subset \langle f \rangle$ を示す．$g \in I$ とする．g を f で割り，

$$g = fq + r, \quad \deg r < \deg f \tag{170}$$

という $q, r \in k[x]$ を得る．$f, g \in I$ なので $r = g - fq \in I$ である．$r \in I$ であり，$\deg r < \deg f$ であり，f は I のなかで 0 でない最小の次数の多項式なので，$r = 0$ である．よって，$g = fq \in I$ である．よって，$I \subset \langle f \rangle$ である．

一意性を示す．$\langle f \rangle = \langle g \rangle$ とする．$f \in \langle g \rangle$ なので，$f = gh$ となる $h \in k[x]$ が存在する．$\deg f = \deg gh \geq \deg g$ となる．対称性より，$\deg g \leq \deg f$ ともなり，$\deg f = \deg g$ となる．よって，$\deg h = 0$ となり，h は 0 でない定数である．

(証終)

整域のすべてのイデアルが単項で生成されるならば，その整域は単項イデアル整域 (PID) という．この定理により，$k[x]$ は PID である．

$\langle f, g \rangle$ を単項イデアルであらわす方法を考える．そのために，最大公約数 GCD を定義する．h が f, g の最大公約数であるとは，

- $h|f$ かつ $h|g$．
- h は上のようなもののうち最大である．すなわち，$h'|f$かつ$h'|g \implies h'|h$．

となることである．一意ではないが，$h = \mathrm{GCD}(f, g)$ とかく．

GCD はある意味で一意で，次のことを示せる．

(1) $\mathrm{GCD}(f, g)$ は定数倍を除いて一意である．
(2) $\langle \mathrm{GCD}(f, g) \rangle = \langle f, g \rangle$．
(3) $\mathrm{GCD}(f, g)$ は存在する．
(4) $\mathrm{GCD}(f, g)$ を求めるアルゴリズムが存在する．

証明

(1) h も $\widetilde{h}$ も $GCD(f, g)$ の条件をみたすとする．$h, \widetilde{h}$ より，$\widetilde{h}|h$ と $h|\widetilde{h}$ をみたす．よって，$\widetilde{h}$ は h の非 0 の定数倍である．

(2) 上の定理より，$k[x]$ は PID なので，$\langle f, g \rangle = \langle h \rangle$ となる $h \neq 0$ が存在する．h が GCD の条件をみたすことを示す．

- わりきる：$f \in \langle h \rangle$ なので，$f = h\widetilde{f}$ となる $\widetilde{f}$ が存在し，$h|f$ である．同様に，$h|g$ である．
- 最大：$h'|f$，$h'|g$ とする．$f = h'h_1$，$g = h'h_2$ となる $h_1, h_2 \in k[x]$ が存在する．$\langle f, g \rangle = \langle h \rangle$ より，$h = h_3 f + h_4 g$ となる $h_3, h_4 \in k[x]$ が存在する．

$$h = h_3 f + h_4 g = h_3(h'h_1) + h_4(h'h_2) = h'(h_3 h_1 + h_4 h_2) \tag{171}$$

となる．よって，$h'|h$ となる．とりあえず h を何かであらわすところから始めなければならない．

(3) (2) が存在証明になっている．もとをたどれば，$k[x]$ が PID であることによる．

Algorithm 2 多項式についての Euclid の互除法

$f, g \in k[x]$ とし，$\mathrm{GCD}(f, g)$ を求める．$\deg f \geq \deg g$ として一般性を失わない．

(4)
1: $p := f$
2: $q := g$
3: **while** $q \neq 0$ **do**
4: $\quad (p, q) \Leftarrow (q, p \bmod q)$
5: **end while**

まず，このアルゴリズムが停止することを示す．L.3 から L.5 の繰り返しで，更新される前の p, q をそのまま p, q，後を p', q' とすると，$\deg q' < \deg q$ であり，q の次数は単調に減少することがわかる．よって，高々 $\deg g + 1$ 回繰替えせば，L.3 の終了条件 $q = 0$ が満たされ，アルゴリズムは停止する．
p, q, p', q' を上と同様とする．q' の定義より，$p = q\widetilde{q} + q'$ となる $\widetilde{q} \in k[x]$ が存在する．これは p を q で割ったときの商であり，割り算のアルゴリズムにより一意に定まる．このとき，

$$\langle p, q \rangle = \langle q\widetilde{q} + q', q \rangle = \langle q', q \rangle = \langle q', p' \rangle \tag{172}$$

となる．
このアルゴリズムで，(p, q) は n 回変化したとし，その各々を (p_i, q_i) とする．$(p_0, q_0) = (f, g)$ であり，$q_n = 0$ である．すると，上のことより

$$\langle f, g \rangle = \langle p_0, q_0 \rangle = \langle p_1, q_1 \rangle = \cdots = \langle p_{n-1}, q_{n-1} \rangle = \langle p_n, q_n \rangle = \langle p_n, 0 \rangle = \langle p_n \rangle. \tag{173}$$

これで，$\langle f, g \rangle$ が，アルゴリズムで求まった p_n の単項イデアルであらわせた．上の定理により，$\mathrm{GCD}(f, g) = p_n$ である．

(証終)

いままでは 2 つの多項式についてのみ GCD を考えてきたが，一般に $n(\geq 2)$ 個に対して考えることができる．g が $f_1, \ldots, f_n$ の最大公約元，GCD であるとは，

- わりきる：g は $f_1, \ldots, f_n$ のすべてを割り切る．
- 最大である：g は「わりきる」をみたすうちで最大である．すなわち，g' が $f_1, \ldots, f_n$ のすべてを割り切るとき，g' は g も割り切ってしまう．

これについて，同様に次がなりたつ．

(1) $\mathrm{GCD}(f_1, \ldots, f_n)$ は定数倍を除いて一意的である．
(2) $\langle f_1, \ldots, f_n \rangle = \langle \mathrm{GCD}(f_1, \ldots, f_n) \rangle$．
(3) $\mathrm{GCD}(f_1, \ldots, f_n)$ は存在する．
(4) $\langle f_1, \ldots, f_n \rangle = \langle f_1, \mathrm{GCD}(f_2, \ldots, f_n) \rangle$．
(5) $\mathrm{GCD}(f_1, \ldots, f_n)$ を求めるアルゴリズムが存在する．

証明

(1) g, g' が $\mathrm{GCD}(f_1, \ldots, f_n)$ であるとする．g は「わりきる」の性質を持つが，これと g' の「最大である」の性質より $g | g'$ となる．同様に $g' | g$ となり，g は g' の定数倍である．
(2) $k[x]$ は PID なので，$\langle f_1, \ldots, f_n \rangle = \langle g \rangle$ となる $g \in k[x]$ が存在する．この g が $\mathrm{GCD}(f_1, \ldots, f_n)$ であることを示す．2 つの性質を持つことを示せばよい．
   - わりきる：$f_1 \in \langle g \rangle$ なので，f_1 は g の倍元であり，$g | f_1$ である．同様に g は $f_1, \ldots, f_n$ をわりきる．
   - 最大である：$\widetilde{g}$ が「わりきる」の性質を持つとする．$\widetilde{g}\widetilde{f}_1 = f_1, \ldots, \widetilde{g}\widetilde{f}_n = f_n$ となる $\widetilde{f}_1, \ldots, \widetilde{f}_n \in k[x]$ が存在する．また，$g \in \langle f_1, \ldots, f_n \rangle$ なので，

$$g = f_1 f_1' + \cdots + f_n f_n' \tag{174}$$

となる $f'_1, \ldots, f'_n \in k[x]$ が存在する．よって，

$$g = f_1 f'_1 + \cdots + f_n f'_n \tag{175}$$
$$= \widetilde{g}\widetilde{f}_1 f'_1 + \cdots + \widetilde{g}\widetilde{f}_n f'_n \tag{176}$$
$$= \widetilde{g}(\widetilde{f}_1 f'_1 + \cdots + \widetilde{f}_n f'_n). \tag{177}$$

よって，$\widetilde{g}$ は g をわりきる．

(3) (2) で，PID から導かれる $\langle f_1, \ldots, f_n \rangle$ の単項の生成元の存在から従う．

(4)

$$\langle f_1, \ldots, f_n \rangle = k[x]f_1 + \langle f_2, \ldots, f_n \rangle \tag{178}$$
$$\overset{\boxed{(2)}}{=} k[x]f_1 + \langle \mathrm{GCD}(f_2, \ldots, f_n) \rangle \tag{179}$$
$$= \langle f_1, \mathrm{GCD}(f_2, \ldots, f_n) \rangle. \tag{180}$$

(5) $n \geq 2$ と仮定し，$f_1, \ldots, f_n$ の最大公約元を求める．

Algorithm 3 一般個数の GCD の計算

```
1: i := 2
2: g := f_1
3: while i ≤ n do
4:     g ⇐ GCD(g, f_i)
5:     i ⇐ i + 1
6: end while
```

アルゴリズムの停止はあきらか．

L.3 から L.6 の繰り返しで更新される前の g を g_0，更新されたあとを g_1 とする．$g_1 = \mathrm{GCD}(g_0, f_i)$ となる．このとき，$\langle g_0, f_i \rangle = \langle g_1 \rangle$ となる．

m 回更新された g を g_n とよぶ．$g_0 = f_1$ であり，ループはちょうど $n-1$ 回実行されるので，これらは g_0 から g_{n-1} まであることがわかる．

$$\langle f_1, f_2, \ldots, f_{n-1}, f_n \rangle = \langle g_0, f_2, \ldots, f_{n-1}, f_n \rangle \tag{181}$$
$$= \langle g_1, f_3, \ldots, f_{n-1}, f_n \rangle \tag{182}$$
$$= \langle g_2, f_4, \ldots, f_{n-1}, f_n \rangle \tag{183}$$
$$= \langle g_{n-2}, f_n \rangle \tag{184}$$
$$= \langle g_{n-1} \rangle. \tag{185}$$

先の証明より，この単項イデアルの生成元 g_{n-1} が $\mathrm{GCD}(f_1, \ldots, f_n)$ であった．

(証終)

これによって，多項式のイデアルを単項イデアルとして具体的にあらわす方法があきらかになった．これを使って，イデアルの所属問題，すなわち「$f_1, \ldots, f_n \in k[x]$ と $f \in k[x]$ について，$f \in \langle f_1, \ldots, f_n \rangle$ か？」を解く手続が得られる．つまり，$f \bmod \mathrm{GCD}(f_1, \ldots, f_n) = 0$ かどうかが所属するかどうかである．

証明

$$f \in \langle f_1, \ldots, f_n \rangle \iff f \in \langle \mathrm{GCD}(f_1, \ldots, f_n) \rangle \tag{186}$$
$$\iff f\text{はGCD}(f_1, \ldots, f_n)\text{の倍元} \tag{187}$$
$$\iff f \bmod \mathrm{GCD}(f_1, \ldots, f_n) = 0. \tag{188}$$

(証終)

(問題 1) f が 1 次式のときは自明である．以降，n 次式のときに成立すると仮定し，$n+1$ 次式で成立することを示す．$\mathbb{C}$ は代数閉体なので f にはすくなくとも 1 つ根がある．それを $a \in \mathbb{C}$ とする．f を $x-a$ で割り，$f = p(x-a)+q$ を得る．ここで，$\deg q < 1$ であり，q は定数である．$0 = f(a) = p(a-a)+q(a) = q(a)$ なので，q は多項式として 0 であり，$f = p(x-a)$ である．$\deg p + \deg(x-a) = \deg f$ であり，$\deg p = \deg f - \deg(x-a) = (n+1)-1 = n$ である．よって，帰納法の仮定より $p = c(x-a_1)\dots(x-a_n)$ となる $c, a_1, \dots, a_n \in \mathbb{C}$ が存在する．よって，$f = c(x-a_1)\dots(x-a_n)(x-a)$ である．

(問題 2)

$$A = \begin{pmatrix} 1 & a_1 & \cdots & a_1^{n-1} \\ 1 & a_2 & \cdots & a_2^{n-1} \\ \vdots & & & \vdots \\ 1 & a_n & \cdots & a_n^{n-1} \end{pmatrix} \in M(k,n) \tag{189}$$

とする．$\det A = 0$ だとする (背理法)．このとき，A の列たちは 1 次従属になるので，

$$c_0 \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} + c_1 \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} + \cdots + c_{n-1} \begin{pmatrix} a_1^{n-1} \\ \vdots \\ a_n^{n-1} \end{pmatrix} = 0 \tag{190}$$

なる，すべては 0 でない $c_1, \dots, c_{n-1} \in k$ が存在する．よって，多項式 f を

$$f(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} \tag{191}$$

と定めると，これは相異なる n 個の解 $a_1, \dots, a_n$ を持つ．

- $c_1 = \cdots = c_{n-1} = 0$ のとき：このときは $c_0 \neq 0$ のはずだが，$c_0 = 0$ が 1 次従属性より従うので矛盾．
- $c_1, \dots, c_{n-1}$ のうち 1 つ以上が 1 のとき：$\deg f \leq n-1$ である．よって，f は高々 $n-1$ 個の解を持つが，これは解 $a_1, \dots, a_n$ を持つことに矛盾する．

いずれにせよ矛盾である．

(問題 3) $f, g \in k[x,y]$ について，$x = fg$ のとき，f か g かは定数になることを示す．仮に f, g が両方とも定数でないとすると，$\deg f, \deg g \geq 1$ となる．k は体で，特に整域なので，$\deg(fg) = \deg f + \deg g \geq 2$ となる．一方，$\deg x = 1$ なので，これは矛盾である．

$\langle x, y \rangle = \langle h \rangle$ となる $h \in k[x,y]$ が存在すると仮定する．$x \in \langle h \rangle$ なので，$x = h\widetilde{h}$ となる $\widetilde{h} \in k[x,y]$ となる．先に示したことにより，h か $\widetilde{h}$ かは定数である．

- h が定数のとき：$h \in \langle x, y \rangle$ となるが，$\deg h \leq 0$ であり，$\langle x, y \rangle$ の元はどれも deg が 1 以上なので，矛盾である．
- $\widetilde{h}$ が定数のとき：$h = x/\widetilde{h}$ となる．よって，$\langle h \rangle = \langle x \rangle$ となり，$\langle x, y \rangle = \langle x \rangle$ となる．$y \in \langle x \rangle$ となので，$y = x\widetilde{h}'$ となる $\widetilde{h}' \in k[x,y]$ が存在する．先に示したことより，x か $\widetilde{h}'$ かは定数になるが，x は定数ではないので $\widetilde{h}'$ が定数である．よって，y は x の定数倍となるが，これは矛盾である．

(問題 4) h は f, g の GCD なので，$\langle f, g \rangle = \langle h \rangle$ である．$h \in \langle f, g \rangle$ なので，$A, B \in k[x]$ が存在して，$Af + Bg = h$ である．

(問題 5) なんか (172) で使ってしまったが示す．$\langle f - qg, g \rangle = \langle f, g \rangle$？

- $\subset$：$f - qg = f + (-q)g \in \langle f, g \rangle$．$g \in \langle f, gg \rangle$．
- $\supset$：$f = 1 \cdot (f - qg) + q \cdot g \in \langle f - qg, g \rangle$．$g \in \langle f - qg, g \rangle$．

(問題 6) やった．

(問題 7) やった．

(問題 8) `code/calcgcd.hs` で計算．

(a) $x^2 + x + 1$．

(b) $x - 1$．

(問題 9) `code/calcgcd.hs` で計算．$\mathrm{GCD}(x^3 + x^2 - 4x - 4, x^3 - x^2 - 4x + 4, x^3 - 2x^2 - x + 2) = x - 2$．$\langle x^3 + x^2 - 4x - 4, x^3 - x^2 - 4x + 4, x^3 - 2x^2 - x + 2 \rangle = \langle x - 2 \rangle$ である．$x^2 - 4 = (x+2)(x-2) \in \langle x - 2 \rangle = \langle x^3 + x^2 - 4x - 4, x^3 - x^2 - 4x + 4, x^3 - 2x^2 - x + 2 \rangle$．

(問題 10) 2 つの多項式の GCD のアルゴリズムの $p_0, \ldots, p_n$，$q_0, \ldots, q_n$ を得る．$p_i = q_i\widetilde{q}_i + q_{i+1}\,(i = 0, \ldots, n-1)$，$p_{i+1} = q_i,\ (i = 0, \ldots, n-1)$，$q_n = 0$，$p_0 = f$，$q_0 = g$ は成立している．ここにあげた式より，$p_0 = f$，$p_1 = g$，$p_i = p_{i+1}\widetilde{q}_i + p_{i+2}\,(p = 0, \ldots, n-2)$ となる．さらに，$p_{n+1} = 0$ としておくことで，これらの式は拡張できる．そこで，

$$\begin{pmatrix} p_{i+2} \\ p_{i+1} \end{pmatrix} = \begin{pmatrix} -\widetilde{q}_i & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} p_{i+1} \\ p_i \end{pmatrix} \quad (i = 0, \ldots, n-1) \tag{192}$$

となる．よって，

$$\begin{pmatrix} 0 \\ p_n \end{pmatrix} = \begin{pmatrix} p_{n+1} \\ p_n \end{pmatrix} \tag{193}$$

$$= \begin{pmatrix} -\widetilde{q}_{n-1} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} p_n \\ p_{n-1} \end{pmatrix} \tag{194}$$

$$= \begin{pmatrix} -\widetilde{q}_{n-1} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} -\widetilde{q}_{n-2} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} p_{n-1} \\ p_{n-2} \end{pmatrix} \tag{195}$$

$$= \ldots \tag{196}$$

$$= \begin{pmatrix} -\widetilde{q}_{n-1} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} -\widetilde{q}_{n-2} & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} -\widetilde{q}_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} p_1 \\ p_0 \end{pmatrix} \tag{197}$$

$$= \begin{pmatrix} -\widetilde{q}_{n-1} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} -\widetilde{q}_{n-2} & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} -\widetilde{q}_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} g \\ f \end{pmatrix} \tag{198}$$

$$\tag{199}$$

よって，次のアルゴリズムが得られる．

Algorithm 4 GCD の線形結合での表示を得るアルゴリズム

1: $p_0 := f$
2: $q_0 := g$
3: $M_0 = E$
4: $i := 1$
5: **while** $i \leq n$ **do**
6: $\quad (p_i, q_i, \widetilde{q}_{i-1}) := (q_i, p_i \bmod q_i, p_i \div q_i)$
7: $\quad M_i := \begin{pmatrix} -\widetilde{q}_{i-1} & 1 \\ 1 & 0 \end{pmatrix} M_{i-1}$
8: $\quad i \Leftarrow i + 1$
9: **end while**
10: (fの係数) := M_nの$(2,2)$成分
11: (gの係数) := M_nの$(2,1)$成分

とすればよい．$p \div q$ は，本文で言うところの $\mathrm{quotient}(p, q)$．

(問題 11) (a) $f \neq 0$ とする．$\mathbf{V}(f) = \emptyset \iff f$は定数？

- $\Rightarrow$：$\mathbf{V}(f) = \emptyset$ なので，$f(x) = 0$ をみたす x は存在しない，すなわち，f は根を持たない．仮に $\deg f \geq 1$ ならば，$\mathbb{C}$ 上の多項式なので根を持ってしまい，$\deg f \leq 0$ である．f は 0 でないので，f は 0 でない定数である．
- $\Leftarrow$：f は定数でかつ 0 でないので，$\deg f = 0$ である．よって，f は定数である．

(b) $\mathbf{V}(f_1, \ldots, f_n) = \emptyset \iff \mathrm{GCD}(f_1, \ldots, f_n) = 1$？ アフィン多様体はイデアルから定まるので，$\langle f_1, \ldots, f_n \rangle = \langle \mathrm{GCD}(f_1, \ldots, f_n) \rangle$ より，$\mathbf{V}(f_1, \ldots, f_n) = \mathbf{V}(\mathrm{GCD}(f_1, \ldots, f_n))$ である．また，$\mathrm{GCD}(f_1, \ldots, f_n) = 1$ は，GCD は定数倍の (そしてそれのみの) 定数倍を持っていることから，

$\mathrm{GCD}(f_1, \ldots, f_n)$ が定数ということである．よって，

$$\mathbf{V}(f_1, \ldots, f_n) = \emptyset \iff \mathbf{V}(\mathrm{GCD}(f_1, \ldots, f_n)) = \emptyset \tag{200}$$

$$\overset{\boxed{(a)}}{\iff} \mathrm{GCD}(f_1, \ldots, f_n)\text{は定数} \tag{201}$$

$$\overset{\boxed{\text{GCD の不定性}}}{\iff} \mathrm{GCD}(f_1, \ldots, f_n) = 1. \tag{202}$$

(c) $\mathrm{GCD}(f_1, \ldots, f_n)$ を計算して，1(あるいは定数) ならば多様体は空だし，そうでなければ多様体には点がある．

(問題 12) $\mathbf{I}(\mathbf{V}(f_1, \ldots, f_n))$ と $\langle f_1, \ldots, f_n \rangle$ との関係を調べる．今，体は $\mathbb{C}$ で考える．したがって，任意の $f \in \mathbb{C}[x]$ について，

$$f = c(x - a_1)^{r_1} \ldots (x - a_s)^{r_s} \tag{203}$$

と分解される．これは，$\mathbb{C}$ が代数閉体であることから従う．これに対し，

$$f_{red} = c(x - a_1) \ldots (x - a_s) \tag{204}$$

と，冪を取り除いたものを被約部分 (reduced part)，あるいは無平方部分 (square-free part) とよぶ．

(a) $\mathbf{V}(f) = \{a_1, \ldots, a_n\}$？

$$\mathbf{V}(f) = \{x \in \mathbb{C} | f(x) = 0\} = \{a_1, \ldots, a_n\}. \tag{205}$$

(b) $\mathbf{I}(\mathbf{V}(f)) = \langle f_{red} \rangle$？

$$f \in \mathbf{I}(\mathbf{V}(f)) \iff f\text{は}\mathbf{V}(f)\text{全てを消す．} \tag{206}$$

$$\iff f\text{は}\{a_1, \ldots, a_n\}\text{すべてを消す．} \tag{207}$$

$$\iff f_{red} | f \tag{208}$$

$$\iff f \in \langle f_{red} \rangle. \tag{209}$$

(問題 13)

$$f = \sum_{i=0}^{n} a_i x^i, \quad g = \sum_{j=0}^{m} b_j x^j \tag{210}$$

としておく．

- $(af)' = af'$？

$$(af)' = (a \sum_{i=0}^{n} a_i x^i)' \tag{211}$$

$$= (\sum_{i=0}^{n} a a_i x^i)' \tag{212}$$

$$= \sum_{i=1}^{n} i a a_i x^{i-1} \tag{213}$$

$$= a \sum_{i=1}^{n} i a_i x^{i-1} \tag{214}$$

$$= af'. \tag{215}$$

- $(f+g)' = f' + g'$?

$$(f+g)' = (\sum_{i=0}^{n} a_i x^i + \sum_{j=0}^{m} b_j x^j)' \tag{216}$$
$$= (\sum_{k=0}^{n+m} (a_k + b_k) x^k)' \tag{217}$$
$$= \sum_{k=1}^{n+m} k(a_k + b_k) x^{k-1} \tag{218}$$
$$= \sum_{k=1}^{n} k a_k x^{k-1} + \sum_{k=1}^{m} k b_k x^{k-1} \tag{219}$$
$$= f' + g'. \tag{220}$$

- $(fg)' = f'g + fg'$?

$$(fg)' = *(*(\sum_{i=0}^{n} a_i x^i) * (\sum_{j=0}^{m} b_j x^j))' \tag{221}$$
$$= *(\sum_{i=0}^{n}\sum_{j=0}^{m} a_i b_j x^{i+j})' \tag{222}$$
$$= \sum_{i=0}^{n}\sum_{j=0}^{m} a_i b_j (i+j) x^{i+j-1} \tag{223}$$
$$= (\sum_{i=0}^{n}\sum_{j=0}^{m} a_i b_j i x^{i+j-1}) + (\sum_{i=0}^{n}\sum_{j=0}^{m} a_i b_j j x^{i+j-1}) \tag{224}$$
$$= (\sum_{i=0}^{n} i a_i x^{i-1})(\sum_{j=0}^{m} b_j x^j) + (\sum_{i=0}^{n} a_i x^i)(\sum_{j=0}^{m} j b_j x^{j-1}) \tag{225}$$
$$= f'g + fg'. \tag{226}$$

(問題 14) (a)

$$((x-a)^r h)' = r(x-a)^{r-1} h + (x-a)^r h' \tag{227}$$
$$= (x-a)^{r-1}(rh + (x-a)h'). \tag{228}$$

ここで，$(rh + (x-a)h')(a) = 0$ となったとする．このとき，$rh(a) = 0$ であり，$h(a) = 0$ なので，矛盾である．よって，$rh + (x-a)h'$ は a を消さず，これを h_1 とすればよい．

(b) $i = 1, \ldots, l$ とし，根 a_i を考える．f を $(x-a_i)^{r_i}$ と $c(x-a_1)^{r_1} \ldots (x \overset{\text{ナシ}}{\underset{\vee}{-}} a_i)^{r_i} \ldots (x-a_l)^{r_l}$ との積とみなすと，後者は a_i を消さないので，(a) より f の微分は $f' = (x-a_i)^{r_i-1} h_i$ と書け，h_i は a_i を消さない．i は任意だったので，

$$f' = (x-a_1)^{r_1-1} h_1 \tag{229}$$
$$\vdots \tag{230}$$
$$f' = (x-a_l)^{r_l-1} h_l. \tag{231}$$

$(x-a_1), \ldots, (x-a_l)$ はどの 2 つも互いに素なので，$f' = (x-a_1)^{r_1-1} \ldots (x-a_l)^{r_l-1} H$ と書ける．各 i について，

$$(x-a_1)^{r_1-1} \ldots (x-a_l)^{r_l-1} H = (x-a_i)^{r_i-1} h_i \tag{232}$$

となり，

$$(x-a_1)^{r_1-1}\dots\overset{\text{ナシ}}{\overset{\vee}{(x-a_i)^{r_i-1}}}\dots(x-a_l)^{r_l-1}H=h_i \tag{233}$$

となる．右辺は a_i を消さないので左辺も a_i を消さず，よって H は a_i を消さない．i は任意であったから，H は $a_1,\dots,a_l$ を消さない．

(c) GCD を調べたいときはイデアルを調べよう! 一般に，多項式 f,g,h について，$\langle fg,fh\rangle=\langle f\rangle \iff \langle g,h\rangle=\langle 1\rangle$ が成立する．
$h=(x-a_1)^{r_1-1}\dots(x-a_l)^{r_l-1}$ とする．$\langle(x-a_1)\dots(x-a_l),H\rangle=\langle 1\rangle$ が示せれば，上のことより，$\langle f,f'\rangle=\langle h\rangle$ であり，$\mathrm{GCD}(f,f')=h$ が示せる．$\langle(x-a_1)\dots(x-a_l),H\rangle=\langle 1\rangle$ を示そう．これには，$\mathrm{GCD}((x-a_1)\dots(x-a_l),H)=1$ を示せばよい．g が $(x-a_1)\dots(x-a_l)$ と H とを割り切るとする．

$$(x-a_1)\dots(x-a_l)=gg_1,\quad H=gg_2 \tag{234}$$

となる g_1,g_2 が存在する．g がもしも $(x-a_1)$ から $(x-a_l)$ のうち 1 つでも因子を含んでいるならば，g は a_1 から a_l のどれかを消すことになり，H も a_1 から a_l のどれかを消すことになるので，これは H の性質に反する．よって，g は $(x-a_1)$ から $(x-a_l)$ のどれも因子として持たない．よって，g は定数である．まとめると，g が $(x-a_1)\dots(x-a_l)$ と H を割り切るならば，g は定数となる．よって，$\mathrm{GCD}((x-a_1)\dots(x-a_l),H)=1$ である．

(問題 15) (a) 略．GCD はモニックということにしておく．

(b) GCD は `code/calcgcd.hs` で計算．

$$f=x^{11}-x^{10}+2x^8-4x^7+3x^5-3x^4+x^3+3x^2-x-1, \tag{235}$$
$$f'=11x^{10}-10x^9+16x^7-28x^6+15x^4-12x^3+3x^2+6x-1, \tag{236}$$
$$\mathrm{GCD}(f,f')=x^6-x^5+x^3-2x^2+1, \tag{237}$$
$$f/\mathrm{GCD}(f,f')=x^5+x^2-x-1. \tag{238}$$

よって，

$$f_{red}=x^5+x^2-x-1. \tag{239}$$

(問題 16) アフィン多様体はイデアルで定まるので $\mathbf{V}(f_1,\dots,f_s)=\mathbf{V}(\mathrm{GCD}(f_1,\dots,f_s))$ であり，$\mathbf{I}(\mathbf{V}(f_1,\dots,f_s))=\mathbf{I}(\mathbf{V}(\mathrm{GCD}(f_1,\dots,f_s)))$ である．$\mathbf{I}(\mathbf{V}(\mathrm{GCD}(f_1,\dots,f_s)))=\langle\mathrm{GCD}(f_1,\dots,f_s)_{red}\rangle$ であるから，基底は $\mathrm{GCD}(f_1,\dots,f_s)_{red}$ である．

(問題 17) `code/calcgcd.hs` と `code/squarefree.hs` で計算．

$$f=x^5-2x^4+2x^2-x, \tag{240}$$
$$g=x^5-x^4-2x^3+2x^2+x-1 \tag{241}$$

とする．

$$\mathrm{GCD}(f,g)=x^4-2x^3+2x-1. \tag{242}$$

よって，

$$\mathrm{GCD}(f,g)_{red}=x^2-1. \tag{243}$$

よって，基底は x^2-1 である．

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？[*2]？

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．

$$x_1 = a_{11}t_1 + \cdots + a_{1N}t_N + c_1 \tag{244}$$

$$\vdots \tag{245}$$

$$x_n = a_{n1}t_1 + \cdots + a_{nN}t_N + c_N \tag{246}$$

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，

$$\begin{pmatrix} a_{11} & \cdots & a_{1N} & -1 & \ldots & 0 & c_1 \\ \vdots & & & & & & \vdots \\ a_{n1} & \cdots & a_{nN} & 0 & \ldots & -1 & c_N \end{pmatrix} \begin{pmatrix} t_1 \\ \vdots \\ t_N \\ x_1 \\ \vdots \\ x_n \\ 1 \end{pmatrix} = \mathbb{0}. \tag{247}$$

[*2] 「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．

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，

$$(x_1,\dots,x_n)\in V \tag{248}$$

$$\iff {}^{\exists}t_1,\dots,t_N\colon \begin{pmatrix} a_{11} & \cdots & a_{1N} & -1 & \dots & 0 & c_1 \\ \vdots & & & & & & \vdots \\ a_{n1} & \cdots & a_{nN} & 0 & \dots & -1 & c_N \end{pmatrix} \begin{pmatrix} t_1 \\ \vdots \\ t_N \\ x_1 \\ \vdots \\ x_n \\ 1 \end{pmatrix} = \mathbb{0} \tag{249}$$

$$\iff {}^{\exists}t_1,\dots,t_N\colon (b_{i,j})_{n,(N+n+1)} \begin{pmatrix} t_1 \\ \vdots \\ t_N \\ x_1 \\ \vdots \\ x_n \\ 1 \end{pmatrix} = \mathbb{0} \tag{250}$$

$$\iff {}^{\exists}t_1,\dots,t_N\colon \begin{cases} b_{11}t_1+\cdots+b_{1N}t_N+b_{1,(N+1)}x_1+\cdots+b_{1,(N+n)}x_n+b_{1,(N+n+1)} & =0 \\ & \vdots \\ b_{n1}t_1+\cdots+b_{nN}t_N+b_{n,(N+1)}x_1+\cdots+b_{n,(N+n)}x_n+b_{n,(N+n+1)} & =0 \end{cases} \tag{251}$$

$$\iff {}^{\exists}t_1,\dots,t_N\colon \tag{252}$$

$$\begin{cases} b_{1,f(1)}t_{f(1)}+\cdots+b_{1,f(M)+1}t_{f(M)+1}+\cdots+b_{1,N}t_N+b_{1,(N+1)}x_1+\cdots+b_{1,(N+n)}x_n+b_{1,(N+n+1)} & =0 \\ b_{2,f(2)}t_{f(2)}+\cdots+b_{2,f(M)+1}t_{f(M)+1}+\cdots+b_{2,N}t_N+b_{2,(N+1)}x_1+\cdots+b_{2,(N+n)}x_n+b_{2,(N+n+1)} & =0 \\ \vdots & \vdots \\ b_{M,f(M)}t_{f(M)}+b_{M,f(M)+1}t_{f(M)+1}+\cdots+b_{M,N}t_N+b_{M,(N+1)}x_1+\cdots+b_{M,(N+n)}x_n+b_{M,(N+n+1)} & =0 \\ b_{(M+1),f(M)+1}t_{f(M)+1}+\cdots+b_{(M+1),N}t_N+b_{(M+1),(N+1)}x_1+\cdots+b_{(M+1),(N+n)}x_n+b_{(M+1),(N+n+1)} & =0 \\ & \vdots \\ b_{n,f(M)+1}t_{f(M)+1}+\cdots+b_{n,N}t_N+b_{n,(N+1)}x_1+\cdots+b_{n,(N+n)}x_n+b_{n,(N+n+1)} & =0 \end{cases} \tag{253}$$

$$\iff {}^{\exists}t_{f(1)},\dots,t_{f(M)},t_{f(M)+1},\dots,t_N: \tag{254}$$

$$\begin{cases} b_{1,f(1)}t_{f(1)}+\cdots+b_{1,f(M)+1}t_{f(M)+1}+\cdots+b_{1,N}t_N+b_{1,(N+1)}x_1+\cdots+b_{1,(N+n)}x_n+b_{1,(N+n+1)} & =0 \\ b_{2,f(2)}t_{f(2)}+\cdots+b_{2,f(M)+1}t_{f(M)+1}+\cdots+b_{2,N}t_N+b_{2,(N+1)}x_1+\cdots+b_{2,(N+n)}x_n+b_{2,(N+n+1)} & =0 \\ \vdots & \vdots \\ b_{M,f(M)}t_{f(M)}+b_{M,f(M)+1}t_{f(M)+1}+\cdots+b_{M,N}t_N+b_{M,(N+1)}x_1+\cdots+b_{M,(N+n)}x_n+b_{M,(N+n+1)} & =0 \\ b_{(M+1),f(M)+1}t_{f(M)+1}+\cdots+b_{(M+1),N}t_N+b_{(M+1),(N+1)}x_1+\cdots+b_{(M+1),(N+n)}x_n+b_{(M+1),(N+n+1)} & =0 \\ & \vdots \\ b_{n,f(M)+1}t_{f(M)+1}+\cdots+b_{n,N}t_N+b_{n,(N+1)}x_1+\cdots+b_{n,(N+n)}x_n+b_{n,(N+n+1)} & =0 \end{cases} \tag{255}$$

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． (256)

⇒ 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． (257)

$$\iff {}^{\exists}t_{f(1)},\dots,t_{f(M)}: \tag{258}$$

$$\begin{cases} b_{1,f(1)}t_{f(1)}+b_{1,(N+1)}x_1+\cdots+b_{1,(N+n)}x_n+b_{1,(N+n+1)} & =0 \\ b_{2,f(2)}t_{f(2)}+b_{2,(N+1)}x_1+\cdots+b_{2,(N+n)}x_n+b_{2,(N+n+1)} & =0 \\ \vdots & \vdots \\ b_{M,f(M)}t_{f(M)}+b_{M,(N+1)}x_1+\cdots+b_{M,(N+n)}x_n+b_{M,(N+n+1)} & =0 \\ b_{(M+1),(N+1)}x_1+\cdots+b_{(M+1),(N+n)}x_n+b_{(M+1),(N+n+1)} & =0 \\ & \vdots \\ b_{n,(N+1)}x_1+\cdots+b_{n,(N+n)}x_n+b_{n,(N+n+1)} & =0 \end{cases} \tag{259}$$

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． (260)

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)

$$\begin{pmatrix} 2 & -3 & -1 & 9 \\ 1 & -1 & 0 & 1 \\ 3 & 7 & -2 & 17 \end{pmatrix} \to \begin{pmatrix} 1 & -1 & 0 & 1 \\ 2 & -3 & -1 & 9 \\ 3 & 7 & -2 & 17 \end{pmatrix} \tag{261}$$

$$\to \begin{pmatrix} 1 & -1 & 0 & 1 \\ 0 & -1 & -1 & 7 \\ 0 & 10 & -2 & 14 \end{pmatrix} \tag{262}$$

$$\to \begin{pmatrix} 1 & -1 & 0 & 1 \\ 0 & -1 & -1 & 7 \\ 0 & 0 & -12 & 84 \end{pmatrix} \tag{263}$$

$$\to \begin{pmatrix} 1 & -1 & 0 & 1 \\ 0 & -1 & -1 & 7 \\ 0 & 0 & 1 & -7 \end{pmatrix} \tag{264}$$

$$\to \begin{pmatrix} 1 & -1 & 0 & 1 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & -7 \end{pmatrix} \tag{265}$$

$$\to \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & -7 \end{pmatrix} \tag{266}$$

$$\tag{267}$$

よって，このアフィン多様体は 1 点で，$\{(1, 0, -7)\}$．

(b)

$$\begin{pmatrix} 1 & 1 & -1 & -1 & 0 \\ 1 & -1 & 1 & 0 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 1 & -1 & -1 & 0 \\ 0 & -2 & 2 & 1 & 0 \end{pmatrix} \tag{268}$$

$$\to \begin{pmatrix} 1 & 1 & -1 & -1 & 0 \\ 0 & 1 & -1 & -1/2 & 0 \end{pmatrix} \tag{269}$$

$$\to \begin{pmatrix} 1 & 0 & 0 & -1/2 & 0 \\ 0 & 1 & -1 & -1/2 & 0 \end{pmatrix} \tag{270}$$

よって，パラメタ付け

$$x_1 = -\frac{1}{2}x_4, \quad x_2 = x_3 + \frac{1}{2}x_4. \tag{271}$$

(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．

$$\begin{pmatrix} 1 & -1 & 0 & 0 & -5 \\ 2 & 0 & -1 & 0 & 1 \\ -1 & 0 & 0 & -1 & 6 \end{pmatrix} \to \begin{pmatrix} 1 & -1 & 0 & 0 & -5 \\ 0 & 2 & -1 & 0 & 11 \\ 0 & -1 & 0 & -1 & 1 \end{pmatrix} \tag{272}$$

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．)

$$2x_1 - x_2 = 11, \quad -x_1 - x_3 = 1. \tag{273}$$

(b) 左から，t, u, x_1, x_2, x_3, x_4, 定数．

$$\begin{pmatrix} 2 & -5 & -1 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & -1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 3 & 0 & 0 & 0 & -1 & 0 \end{pmatrix} \to \begin{pmatrix} -1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 2 & -5 & -1 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & -1 & 0 & 0 & 0 \\ 1 & 3 & 0 & 0 & 0 & -1 & 0 \end{pmatrix} \tag{274}$$

$$\to \begin{pmatrix} -1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & -3 & -1 & 0 & 2 & 0 & 0 \\ 0 & 3 & 0 & -1 & 1 & 0 & 0 \\ 0 & 4 & 0 & 0 & 1 & -1 & 0 \end{pmatrix} \tag{275}$$

$$\to \begin{pmatrix} -1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & -3 & -1 & 0 & 2 & 0 & 0 \\ 0 & 3 & 0 & -1 & 1 & 0 & 0 \\ 0 & 1 & -1 & 0 & 3 & -1 & 0 \end{pmatrix} \tag{276}$$

$$\to \begin{pmatrix} -1 & 0 & 1 & 0 & -2 & 1 & 0 \\ 0 & 0 & -4 & 0 & 11 & -3 & 0 \\ 0 & 0 & 3 & -1 & -8 & 3 & 0 \\ 0 & 1 & -1 & 0 & 3 & -1 & 0 \end{pmatrix} \tag{277}$$

$$\tag{278}$$

よって，t, s を含まないところを取り出して，

$$-4x_1 + 11x_3 - 3x_4 = 0, \quad 3x_1 - x_2 - 8x_3 + 3x_4 = 0. \tag{279}$$

(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，

$$\{[f(t)]^u [g(t)]^v | u + v \leq m\} \tag{280}$$

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

$$\deg [f(t)]^u [g(t)]^v = u \deg f(t) + v \deg g(t) \leq n(u+v) \leq nm. \tag{281}$$

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，

$$\sum_{u=0}^{m}\sum_{v=0}^{m-u}\sum_{w=0}^{m-u-v} = \sum_{u=0}^{m}\sum_{v=0}^{m-u}(m-u-v+1) \tag{282}$$

$$= \sum_{u=0}^{m}((m-u+1)^2 - \sum_{v=0}^{m-u} v) \tag{283}$$

$$= \sum_{u=0}^{m}((m-u+1)^2 - (m-u+1)) \tag{284}$$

$$= \sum_{u=0}^{m}(u^2 - 2(m+1)u + (m+1)^2 + u - (m+1)) \tag{285}$$

$$= \frac{m(m+1)(2m+1)}{6} + (-2m-1)\frac{m(m+1)}{2} + m(m+1)^2 \tag{286}$$

$$= \frac{m(m+1)(m+2)}{3}. \tag{287}$$

これが，

$$\{[f(t,\tau)]^u[g(t,\tau)]^v[h(t,\tau)]^w | u+v+w \leq m\} \tag{288}$$

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，

$$\deg([f(t,\tau)]^u[g(t,\tau)]^v[h(t,\tau)]^w) = u\deg f + v\deg g + w\deg h \leq (u+v+w)n \leq mn. \tag{289}$$

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[*3]順序 $>_{lex}$ を見る．これは，

$$(\alpha_1, \dots, \alpha_n) > (\beta_1, \dots, \beta_n) \iff (\alpha_1 - \beta_1, \dots, \alpha_n - \beta_n)\text{の0でない最も左の元が正．} \tag{290}$$

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？ ：$x_1^{(m)} < x_1^{(m+1)}$ 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 $x_1^{(m)} \geq x_1^{(m+1)}$ であり，$m \mapsto x_1^{(m)}$ 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，

    $$x_1^{(N)} = x_1^{(N+1)} = \dots \tag{291}$$

    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

[*3] lexicographic order．辞書順．

すると，

$$\pi x^{(N)} > \pi x^{(N+1)} > \dots \tag{292}$$

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[*4]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：α と β 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[*5]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．

[*4] graded lexicographic
[*5] 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，

$$\neg((|\alpha| > |\beta|) \vee (|\alpha| \leq |\beta| \to \alpha >_{lex'} \beta)) \tag{293}$$
$$\iff \neg((|\alpha| > |\beta|) \vee (|\alpha| > |\beta| \vee \alpha >_{lex'} \beta)) \tag{294}$$
$$\iff (|\alpha| \leq |\beta|) \wedge (|\alpha| \leq |\beta| \wedge \alpha \leq_{lex'} \beta) \tag{295}$$
$$\iff (|\alpha| \leq |\beta|) \wedge (\alpha \leq_{lex'} \beta) \tag{296}$$

  また，$\alpha < \beta$ ではないので，同様に

$$(|\alpha| \geq |\beta|) \wedge (\alpha \geq_{lex'} \beta). \tag{297}$$

  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，α が，今採用している順序について最高のものの α のことである．これを $\mathrm{multideg}(f)$ と書く．

$$\mathrm{multideg}(f) = \max\left\{\alpha | \alpha \in \mathbb{Z}^n_{\geq 0} \wedge a_\alpha \neq 0\right\} \tag{298}$$

  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 α 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 α 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，

$$(2,0) > \cdots > (1,3) > (1,2) > (1,1) > (1,0) > (0,0) \tag{299}$$

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 γ を考えると，$|\alpha| \geq |\gamma| \geq |\beta|$ となり (たくさんやったので略)，γ 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，γ 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，

$$\begin{aligned}
\mathrm{multideg}(mf) &= \max\{\alpha+\beta | a_\alpha \neq 0\} && (300)\\
&= \max\{\alpha | a_\alpha \neq 0\} + \beta && (301)\\
&= \mathrm{multideg}(f) + \beta. && (302)
\end{aligned}$$

よって，

$$\begin{aligned}
\mathrm{LT}(mf) &= a_{\mathrm{multideg}(mf)-\beta} x^{\mathrm{multideg}(mf)} && (303)\\
&= a_{\mathrm{multideg}(f)} x^{\mathrm{multideg}(f)+\beta} && (304)\\
&= m a_{\mathrm{multideg}(f)} x^{\mathrm{multideg}(f)} && (305)\\
&= m\mathrm{LT}(f). && (306)
\end{aligned}$$

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

$$\begin{aligned}
\mathrm{multideg}(fg) &= \max\{\alpha+\beta | a_\alpha b_\beta \neq 0\} && (307)\\
&= \max\{\alpha+\beta | a_\alpha \neq 0 \wedge b_\beta \neq 0\} && (308)\\
&= \max\{\alpha + \max\{\beta | b_\beta \neq 0\} | a_\alpha \neq 0\} && (309)\\
&= \max\{\alpha + \mathrm{multideg}(g) | a_\alpha \neq 0\} && (310)\\
&= \max\{\alpha | a_\alpha \neq 0\} + \mathrm{multideg}(g) && (311)\\
&= \mathrm{multideg}(f) + \mathrm{multideg}(g). && (312)
\end{aligned}$$

$$\begin{aligned}
\mathrm{LC}(fg) &= \sum_{\alpha+\beta=\mathrm{multideg}(fg)} a_\alpha b_\beta && (313)\\
&= \sum_{\alpha+\beta=\mathrm{multideg}(f)+\mathrm{multideg}(g)} a_\alpha b_\beta && (314)\\
&= a_{\mathrm{multideg}(f)} b_{\mathrm{multideg}(g)} && (315)\\
&= \mathrm{LC}(f)\mathrm{LC}(g). && (316)
\end{aligned}$$

よって，

$$\begin{aligned}
\mathrm{LT}(fg) &= \mathrm{LC}(fg)\mathrm{LM}(fg) && (317)\\
&= \mathrm{LC}(f)\mathrm{LC}(g) x^{\mathrm{multideg}(fg)} && (318)\\
&= \mathrm{LC}(f)\mathrm{LC}(g) x^{\mathrm{multideg}(f)+\mathrm{multideg}(g)} && (319)\\
&= \mathrm{LC}(f)\mathrm{LC}(g)\mathrm{LM}(f)\mathrm{LM}(g) && (320)\\
&= \mathrm{LT}(f)\mathrm{LT}(g). && (321)
\end{aligned}$$

(c) $f_1 = x$, $f_2 = -x$, $g_1 = y$, $g_2 = y$ とする．このとき，$\sum_{i=1}^2 f_i g_i = xy - xy = 0$ となる．よって，このとき，$\mathrm{LM}(\sum_{i=1}^2 f_i g_i)$ 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，

$$^\forall N > 0 \colon a_{\mathrm{multideg}(f)+N} + b_{\mathrm{multideg}(f)+N} = 0 \quad (322)$$

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，(322) は成立する．これはつまり，

$$\alpha > \mathrm{multideg}(f) \implies a_\alpha + b_\alpha = 0 \quad (323)$$

だが，対偶をとって，

$$a_\alpha + b_\alpha \neq 0 \implies \alpha \leq \mathrm{multideg}(f). \tag{324}$$

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，

$$\mathrm{multideg}(f) \leq \max\{\alpha | a_\alpha + b_\alpha \neq 0\} = \mathrm{multideg}(f+g) \tag{325}$$

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，

-

$$f = a_1 f_1 + \cdots + a_s f_s + r \tag{326}$$

- 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
- $a_i f_i \implies \mathrm{multideg}(a_i f_i) \leq \mathrm{multideg}(f)$

$a_1, \ldots, a_n, r \in k[x_1, \ldots, x_n]$ 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 5 $k[x_1, \ldots, x_n]$ 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** $\mathrm{LT}(f_i) \leq \mathrm{LT}(stock)$ **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

$$f = a_1 f_1 + \cdots + a_s f_s + stock + r \tag{327}$$

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，

$$f = a_{1b} f_1 + \cdots + a_{sb} f_s + stock_b + r_b \tag{328}$$

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，

$$a_{ja} = \begin{cases} a_{jb} & j \neq i \\ a_{ib} + \frac{\mathrm{LT}(stock_b)}{\mathrm{LT}(f_i)} & j = i \end{cases} \tag{329}$$

となり，

$$stock_a = stock_b - \frac{\mathrm{LT}(stock_b)}{\mathrm{LT}(f_i)} f_i \tag{330}$$

となり，

$$r_a = r_b \tag{331}$$

となる．たしかに，

$$a_{1a}f_1 + \cdots + a_{sa}f_s + stock_a + r_a = \sum_{j=1}^{s} a_{jb}f_j + \frac{\mathrm{LT}(stock_b)}{\mathrm{LT}(f_i)}f_i + stock_b - \frac{\mathrm{LT}(stock_b)}{\mathrm{LT}(f_i)}f_i + r_b \tag{332}$$

$$= a_{1b}f_1 + \cdots + a_{sb}f_s + stock_b + r_b. \tag{333}$$

– $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)$ 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，

$$a_{ja} = a_{jb} \tag{334}$$

$$stock_a = stock_b - \mathrm{LT}(stock_b) \tag{335}$$

$$r_a = r_b + \mathrm{LT}(stock_b) \tag{336}$$

となる．そして，

$$a_{1a}f_{1a} + \cdots + a_{sa}f_{sa} + stock_a + r_a = a_{1b}f_{1b} + \cdots + a_{sb}f_{sb} + stock_b - \mathrm{LT}(stock_b) + r_b + \mathrm{LT}(stock_b) \tag{337}$$

$$= a_{1b}f_{1b} + \cdots + a_{sb}f_{sb} + stock_b + r_b. \tag{338}$$

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．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，

$$r_a = r_b + \mathrm{LT}(stock_b) \tag{339}$$

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，

$$a_{ia} = a_{ib} + \frac{\mathrm{LT}(stock_b)}{\mathrm{LT}(f_i)} \tag{340}$$

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

$$\mathrm{multideg}(a_{ia}f_i) \leq \max(\mathrm{multideg}(a_{ib}), \mathrm{LT}(stock_b)) \tag{341}$$

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，

$$\mathrm{multideg}(a_{ia}f_i) \leq \mathrm{multideg}(f) \tag{342}$$

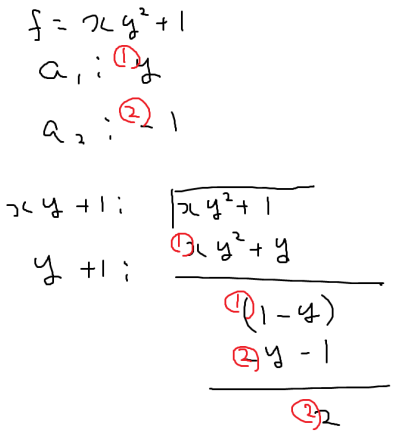
を得る．

(証終)

計算例を示す．

(図 1)div1.png 参照．

図 1　div1.png

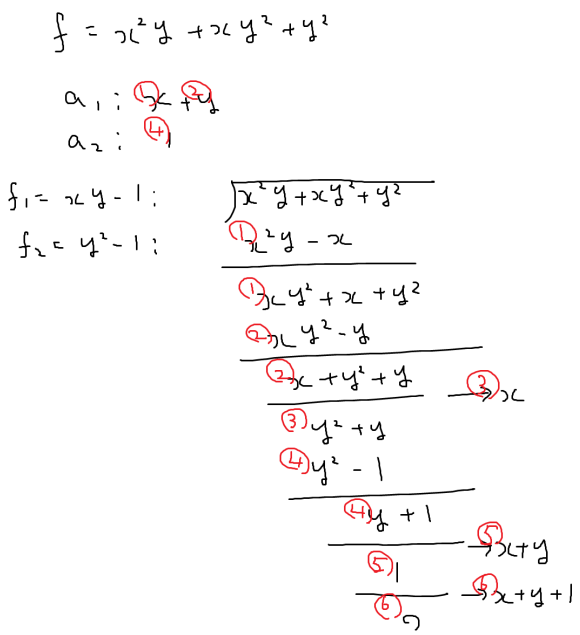


$xy^2 + 1$ を $xy + 1$ と $y + 1$ で割った．

$$xy^2 + 1 = y \cdot (xy + 1) + 1 \cdot (y + 1) + 2. \tag{343}$$

(図 2)div2.png 参照．

図 2　div2.png

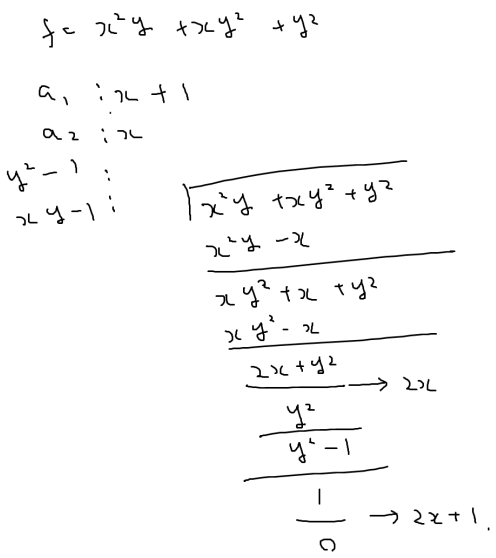


$x^2y + xy^2 + y^2$ を $xy - 1$ と $y^2 - 1$ で割った.

$$x^2y + xy^2 + y^2 = (x + y) \cdot (xy - 1) + 1 \cdot (y^2 - 1) + 0. \tag{344}$$

(図 3)div3.png 参照.

図 3　div3.png

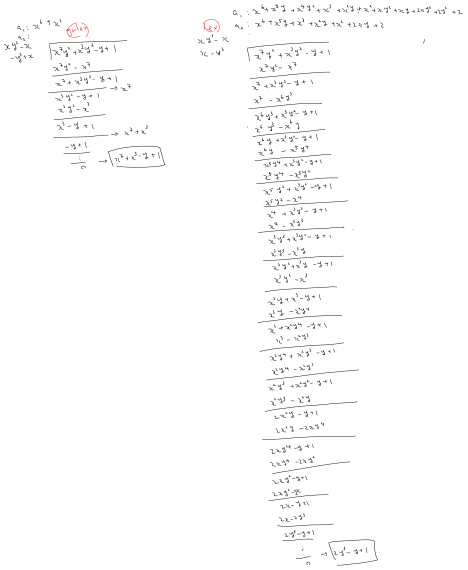


$x - 2y + xy^2 + y^2$ を $y^1 - 1$ と $xy - 1$ で割った．

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．

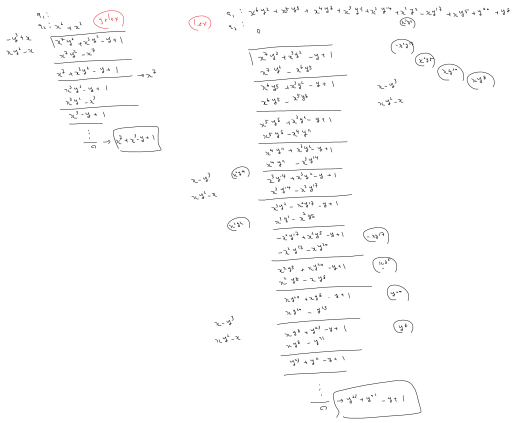
(問題 1)　(a)　(図 4)div3_1a.png 参照．

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．

$$r_1 = x^3 - x^2z + x - z, \tag{345}$$
$$r_2 = x^3 - x^2z. \tag{346}$$

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)

$$y \cdot f_1 - (xy + 1) \cdot f_2 = 1 - yz. \tag{347}$$

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)

$$g = 3x(2xy^2 - x) - 2y(3x^2y - y - 1) = -3x^2 - 2y^2 - 2y \tag{348}$$

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)

$$y^2 \cdot f_1 - xy \cdot f_2 = (x^4y^4 - y^2z) - (x^4y^4 - xy) = xy - y^2z = -y^2z + xy \tag{349}$$
$$xy \cdot f_2 - x^2 \cdot f_3, = (x^4y^4 - xy) - (x^4y^4 - 2x^2z) = 2x^2z - xy. \tag{350}$$

次数より，もう割れないことは分かる．

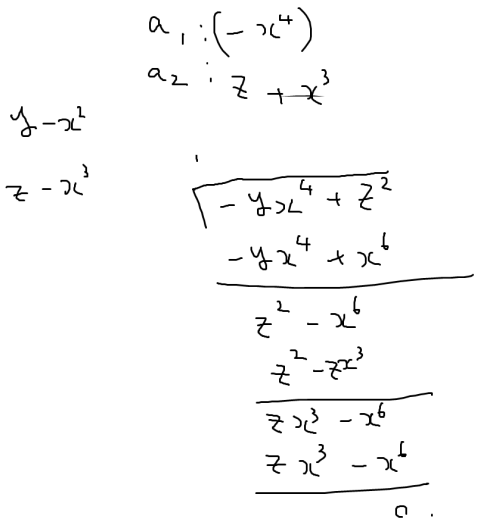
(問題 8) $\mathrm{LT}(g)$ が $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)$ のどれでも割りきれないとき，割り算のあまりは 0 にならないことが保証される．しかし，その g がイデアルに所属することもあるので，余りが 0 かどうかでイデアルの所属を判定することはできない．

(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



$$(-x^4)(y-x^2)+(z+x^3)(z-x^3)=-yx^4+z^2=z^2-x^4y. \tag{351}$$

(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，

$$f=h_1\cdot(y-x^m)+h_2\cdot(z-x^n)+h_3 \tag{352}$$

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

$$0=f(t,t^m,t^n)=h_3(t). \tag{353}$$

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，

$$f=h_1\cdot(y-x^m)+h_2\cdot(z-x^n) \tag{354}$$

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^β を割り切らない．
- $x^{\alpha(i)}$ は x^β を割り切り，かつ $j<i$ について $x^{\alpha(j)}$ は x^β ど割り切らないとする．$x^{\alpha(i)}$ は x^β 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^β 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^γ 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，

$$\Delta_1 = \alpha(1) + \mathbb{Z}^n_{\geq 0} \tag{355}$$
$$\Delta_1 \cup \Delta_2 = \Delta_1 \cup (\alpha(2) + \mathbb{Z}^n_{\geq 0}) \setminus \Delta_1 = (\alpha(1) + \mathbb{Z}^n_{\geq 0}) \cup (\alpha(2) + \mathbb{Z}^n_{\geq 0}) \tag{356}$$
$$\vdots \tag{357}$$
$$\Delta_1 \cup \ldots \cup \Delta_n = (\alpha(1) + \mathbb{Z}^n_{\geq 0}) \cup \ldots \cup (\alpha(n) + \mathbb{Z}^n_{\geq 0}) \tag{358}$$

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^β 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^γ 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^β 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^β 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^β 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

$$g_1 = a_1 f_1 + \cdots + a_s f_s + r \tag{359}$$
$$g_2 = b_1 f_1 + \cdots + b_s f_s + r' \tag{360}$$

とする．このとき，

$$c_1 g_1 + c_2 g_2 = (c_1 a_1 + c_2 b_1) f_1 + \cdots + (c_1 a_s + c_2 b_s) f_s + (c_1 r + c_2 r') \tag{361}$$

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^β 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 α 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，α から ∞ 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[*6]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．

$$f = h_1 x^{\alpha(1)} + \cdots + h_s x^{\alpha(s)} \tag{362}$$

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。

(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，

$$f \in I \iff \{f\text{のすべての項}\} \subset I \iff \{f\text{のすべての項}\} \subset I' \iff f \in I'. \tag{363}$$

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．[*7]

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，$I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$ 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，$I = \langle x^{\alpha'} \rangle$ 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．

$$J = \langle x^\alpha | x^\alpha y^\beta \in I \rangle \subset k[x_1, \ldots, x_{n-1}] \tag{364}$$

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，$J = \langle x^{\alpha(1)}, \ldots, x^{\alpha(j)} \rangle$ 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，

$$x^{\alpha(i)} y^{\beta(i)} \in I \tag{365}$$

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，

$$\gamma = \max(\gamma(1), \ldots, \gamma(j)) \tag{366}$$

とする．このように定義しておくと，

$$J \cdot \langle y^\gamma \rangle = I \cap \{(y\text{の次数}) \geq \gamma\} \tag{367}$$

[*6] 基底ではない!
[*7] 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．

となる． $\gamma \geq \gamma(1), \ldots, \gamma(j)$ なので，y^γ 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．これで，$I \cap \big\{(y\text{の次数}) \geq \gamma\big\}$ は，J が有限生成であることから有限的に書けることになった．y が他の次数のときの I もこのように書いていこう．

$0 \leq \delta < \gamma$ とする．

$$J_\delta = \langle x^\alpha | x^\alpha y^\delta \in I \rangle \subset k[x_1, \ldots, x_{n-1}] \tag{368}$$

とする．つまり，y の次数が δ 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，

$$J_\delta = \langle x^{\alpha(\delta;1)}, \ldots, x^{\alpha(\delta;j_\delta)} \rangle \tag{369}$$

となる $\alpha(\delta;1), \ldots, \alpha(\delta;j_\delta) \in \mathbb{Z}_{\geq 0}^{n-1}$ が存在する．このように定義しておくと，

$$J_\delta \cdot y^\delta = I \cap \big\{(y\text{の次数}) = \delta\big\} \tag{370}$$

となる．以上のことをまとめると，

$$I \cap \big\{(y\text{の次数}) \geq \gamma\big\} = \langle x^{\alpha(1)}, \ldots, x^{\alpha(j)} \rangle \cdot \langle y^\gamma \rangle \tag{371}$$

$$I \cap \big\{(y\text{の次数}) = \gamma - 1\big\} = \langle x^{\alpha(\gamma-1;1)}, \ldots, x^{\alpha(\gamma-1;j_{\gamma-1})} \rangle \tag{372}$$

$$\vdots \tag{373}$$

$$I \cap \big\{(y\text{の次数}) = 0\big\} = \langle x^{\alpha(0;1)}, \ldots, x^{\alpha(0;j_0)} \rangle. \tag{374}$$

である．これらの和集合をとることで，

$$I = \langle x^{\alpha(1)} y^\gamma, \ldots, x^{\alpha(j)} y^\gamma \tag{375}$$

$$x^{\alpha(\gamma-1;1)}, \ldots, x^{\alpha(\gamma-1;j_{\gamma-1})} \tag{376}$$

$$\vdots \tag{377}$$

$$x^{\alpha(0;1)}, \ldots, x^{\alpha(0;j_0)} \rangle \tag{378}$$

であることがわかる．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．

$$I = \langle x^{\beta(1)}, \ldots, x^{\beta(s)} \rangle \tag{379}$$

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．これらの $\beta(i)$ は，$I = \langle x^\alpha | \alpha \in A \rangle$ なので，$x^{\beta(i)}$ は $\langle x^\alpha | \alpha \in A \rangle$ の，1 次結合で書ける．ここで，I は単項式イデアルだったので，特に k 係数の単項式の 1 次結合で書けることが先の補題より分かり，$x^{\beta(i)}$ は単項式だったので，$x^{\beta(i)} = h_i x^{\gamma(i)+\alpha(i)}$ となる $\alpha(i) \in A, \gamma(i) \in \mathbb{Z}_{\geq 0}^n$ が存在することがわかる．よって，

$$I = \langle x^{\alpha(1)+\gamma(1)}, \ldots, x^{\alpha(s)+\gamma(s)} \rangle \tag{380}$$

となる．$\alpha(1) < \alpha(2) < \ldots$ 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，$I = \langle x^{\beta(1)}, \ldots, x^{\beta(s)} \rangle$ 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，$x^{\alpha(1)} \in \langle x^{\alpha(1)+\gamma(1)}, \ldots, x^{\alpha(s)+\gamma(s)} \rangle$．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．$I = \langle x^{\alpha(1)}, x^{\alpha(2)+\delta(2)}, \ldots, x^{\alpha(s)} + \gamma(s) \rangle$ である．$x^{\alpha(2)} \in I$ なので，$x^{\alpha(2)} \in \langle x^{\alpha(1)}, x^{\alpha(2)+\gamma(2)}, \ldots, x^{\alpha(s)+\gamma(s)} \rangle$ となる．

よって，何らかの i について，$\alpha(2) \in \alpha(i)+\gamma(i)+\mathbb{Z}^n_{\geq 0}$ となる．よって，$\alpha(2)=\alpha(i)+\gamma(i)+\delta(i)$ となる $\delta(i) \in \mathbb{Z}^n_{\geq 0}$ 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，

$$I=\langle x^{\alpha(1)},\ldots,x^{\alpha(s)}\rangle \tag{381}$$

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 $I=\langle x^{\alpha(1)},\ldots,x^{\alpha(s)}\rangle$ と書くと，

$$f \in I \iff f\text{を}(x^{\alpha(1)},\ldots,x^{\alpha(s)})\text{で割ったあまりは}0. \tag{382}$$

証明

$$f \in I \iff f \in \langle x^{\alpha(1)},\ldots,x^{\alpha(s)}\rangle \tag{383}$$

$$\overset{\boxed{\text{補題}}}{\iff} f\text{は}x^{\alpha(1)},\ldots,x^{\alpha(s)}\text{の}k\text{係数1次結合で書ける} \tag{384}$$

$$\iff f\text{を}(x^{\alpha(1)},\ldots,x^{\alpha(s)})\text{で割ったあまりは}0. \tag{385}$$

(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，

$$>\text{は整列順序} \iff {}^{\forall}\alpha \in \mathbb{Z}^n_{\geq 0}\colon \alpha \geq 0. \tag{386}$$

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 α 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，α 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，$I=\langle x^{\alpha(1)},\ldots,x^{\alpha(s)}\rangle$ 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．$x^\beta \in I=\langle x^{\alpha(1)},\ldots,x^{\alpha(s)}\rangle$ なので，単項式イデアルの性質より，x^β 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，

$$\beta=\alpha(j)+\gamma \overset{\boxed{\text{仮定!}}}{\leq} \alpha(j) \leq \alpha(1) \tag{387}$$

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．

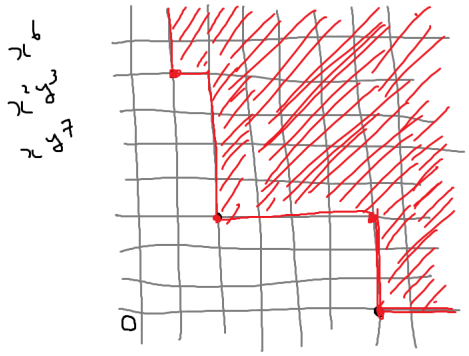
$$f=h_1x^{\alpha(1)}+\cdots+h_sx^{\alpha(s)} \tag{388}$$

となる $h_1, \ldots, h_s \in k[x_1, \ldots, x_n]$ と $\alpha(1), \ldots, \alpha(s) \in \mathbb{Z}_{\geq 0}^n$ 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 $J = \langle x^3 \rangle$．$x^3 y^b \in I$ 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．

$$J_0 = \langle x^6 \rangle, \tag{389}$$
$$J_1 = \langle x^6 \rangle, \tag{390}$$
$$J_2 = \langle x^6 \rangle, \tag{391}$$
$$J_3 = \langle x^6 \rangle, \tag{392}$$
$$J_4 = \langle x^5 \rangle, \tag{393}$$
$$J_5 = \langle x^5 \rangle. \tag{394}$$
$$\tag{395}$$

よって，

$$I = \langle x^3 y^6, x^5 y^5, x^5 y^4, x^6 y^3, x^6 y^2, x^6 y, x^6 \rangle. \tag{396}$$

(b) 取り除けて，

$$I = \langle x^3 y^6, x^5 y^4, x^6 \rangle. \tag{397}$$

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 α 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，$\alpha \in \beta + \mathbb{Z}_{\geq 0}^n$ となる $\beta \in A$ が存在する．α は A の最小元だったので，$\alpha < \beta$ である．よって，$\gamma \in \mathbb{Z}_{\geq 0}^n$ 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．

ディクソンの補題
$$\iff {}^{\forall}A \subset \mathbb{Z}^n_{\geq 0}\colon {}^{\exists}\alpha_1, \ldots, \alpha_s \in A\colon \langle x^{\alpha} | \alpha \in A \rangle = \langle x^{\alpha_1}, \ldots, x^{\alpha_s} \rangle \tag{398}$$
$$\iff {}^{\forall}A \subset \mathbb{Z}^n_{\geq 0}\colon {}^{\exists}\alpha_1, \ldots, \alpha_s \in A\colon \langle x^{\alpha} | \alpha \in A \rangle \subset \langle x^{\alpha_1}, \ldots, x^{\alpha_s} \rangle \tag{399}$$
$$\iff {}^{\forall}A \subset \mathbb{Z}^n_{\geq 0}\colon {}^{\exists}\alpha_1, \ldots, \alpha_s \in A\colon {}^{\forall}\alpha \in A\colon x^{\alpha} \in \langle x^{\alpha_1}, \ldots, x^{\alpha_s} \rangle \tag{400}$$
$$\iff {}^{\forall}A \subset \mathbb{Z}^n_{\geq 0}\colon {}^{\exists}\alpha_1, \ldots, \alpha_s \in A\colon {}^{\forall}\alpha \in A\colon {}^{\exists}i = 1, \ldots, s\colon \alpha \in \alpha_i + \mathbb{Z}^n_{\geq 0} \tag{401}$$
$$\iff {}^{\forall}A \subset \mathbb{Z}^n_{\geq 0}\colon {}^{\exists}\alpha_1, \ldots, \alpha_s \in A\colon {}^{\forall}\alpha \in A\colon {}^{\exists}i = 1, \ldots, s\colon {}^{\exists}\gamma \in \mathbb{Z}^n_{\geq 0}\colon \alpha = \alpha_i + \gamma. \tag{402}$$

(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 δ が存在する．よって，

$$\alpha_i = \beta_j + \gamma = (\alpha_l + \delta) + \gamma = \alpha_l + (\gamma + \delta) \tag{403}$$

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，

$$\neg((\alpha >_{lex} \beta) \vee ((\alpha = \beta) \wedge (\gamma >_{grlex} \delta))) \tag{404}$$
$$\iff (\alpha \leq_{lex} \beta) \wedge ((\alpha \neq \beta) \vee (\gamma \leq_{grlex} \delta)). \tag{405}$$

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．

$$(\alpha >_{lex} \gamma) \vee ((\alpha = \gamma) \wedge (\beta >_{grlex} \delta)). \tag{406}$$

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、α 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、

$$\sqrt{2} = \frac{3b^2d^2 - a^2d^2 - 2b^2c^2}{2abcd} \tag{407}$$

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。

$$\mathfrak{u}\cdot\xi = \sum_{i=1}^{n} u_i\xi_i = 0 \tag{408}$$

である。よって、

$$\xi_1 = \frac{-1}{u_1}\sum_{i=2}^{n} u_i\xi_i. \tag{409}$$

そこで、$\xi_2 = \xi_3 = \cdots = \xi_n = 1$ とすると、$\xi_1 < 0$ となる。これで、ξ が条件をみたす。このとき、ξ 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、

$$\mathfrak{u} \cdot (\alpha - \beta) = \mathfrak{u} \cdot \xi = 0. \tag{410}$$

しかし、あきらかに $\alpha \neq \beta$ である。

(d)

$$\begin{aligned}
\mathfrak{u} \cdot \alpha &= \sum_{k=1}^{n} u_k \alpha_k && (411)\\
&= \sum_{k=1}^{i} u_k \alpha_k && (412)\\
&= \sum_{k=1}^{i} \alpha_k && (413)\\
&> 0 && (414)\\
&= \sum_{k=1}^{n} u_k \beta_k && (415)\\
&= \mathfrak{u} \cdot \beta. && (416)
\end{aligned}$$

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、

$$\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(f); f \in I \rangle \tag{417}$$

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、

$$\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(\langle f_1, \ldots, f_s \rangle) \rangle \tag{418}$$

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、

$$\langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s) \rangle \subset \langle \mathrm{LT}(\langle f_1, \ldots, f_s \rangle) \rangle. \tag{419}$$

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、

$$\{\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)\} \subset \mathrm{LT}(\langle f_1, \ldots, f_s \rangle) \tag{420}$$

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、

$$f_2 - x \cdot f_1 = (xy + 1) - xy = 1 \tag{421}$$

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、

$$\langle \mathrm{LT}(\langle f_1, f_2 \rangle) \rangle = \langle \mathrm{LT}(\langle x + 1, x \rangle) \rangle = \langle \mathrm{LT}(\langle 1 \rangle) \rangle = \langle \langle 1 \rangle \rangle = \langle 1 \rangle. \tag{422}$$

一方、「LT をとる→イデアルをとる」は、

$$\langle \mathrm{LT}(\{f_1, f_2\}) \rangle = \langle \mathrm{LT}(\{x + 1, x\}) \rangle = \langle \{x\} \rangle = \langle x \rangle. \tag{423}$$

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、

$$\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(f); f \in I \rangle = \langle \mathrm{LM}(f); f \in I \rangle \tag{424}$$

   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、

$$\langle \mathrm{LM}(f); f \in I \rangle = \langle \mathrm{LM}(f_1), \ldots, \mathrm{LM}(f_s) \rangle \tag{425}$$

   となる。また定数倍がどうでもいいことに注意すれば、

$$\langle \mathrm{LM}(f_1), \ldots, \mathrm{LM}(f_s) \rangle = \langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s) \rangle \tag{426}$$

   となる。よって、

$$\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s) \rangle. \tag{427}$$

(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、

$$\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s) \rangle \tag{428}$$

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、

$$f = \sum_{i=1}^{s} f_i h_i + r \tag{429}$$

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、

$$\mathrm{LT}(r) \in \langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s) \rangle \tag{430}$$

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、

$$f = \sum_{i=1}^{s} f_i h_i \tag{431}$$

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、

$$I = \langle f_1, \ldots, f_s \rangle \tag{432}$$

である。

(証終)