代数学 III：グレブナー基底と連立方程式

担当：松井紘樹

目次

0　イントロダクション

連立代数方程式（多項式の連立方程式）

$$\begin{cases} f_1(x_1, x_2, \ldots, x_n) = 0 \\ f_2(x_1, x_2, \ldots, x_n) = 0 \\ \qquad\qquad \vdots \\ f_m(x_1, x_2, \ldots, x_n) = 0 \end{cases}$$

を解くという問題は数学やそれ以外の分野に様々な応用があり，重要な問題である：

- 代数幾何学（連立代数方程式の解のなす図形を調べる分野）
- 数式処理
- 機械学習
- 符号理論
- 統計学

最も簡単な状況は $f_1, f_2, \ldots, f_m$ が全て 1 次式の場合で，その場合は連立一次方程式となるので，掃き出し法という連立方程式を解くアルゴリズム（一定の手続き）が知られている．簡単に言えば，掃き出し法とは方程式の実数倍を足し引きすることで変数を消去し，解きやすい連立方程式に帰着させる方法である．一方で，高次の連立代数方程式については，方程式のある項を消去するためには実数倍を足し引きするだけではダメで，多項式倍を足し引きする必要がある．これによりある項を消去すると方程式の次数が上がったり別の項が新たに現れたりし，一筋縄では行かないことが分かる．それでは，高次の連立代数方程式についてもそれを解くアルゴリズムが存在するだろうか？答えは Yes であり，グレブナー基底というものを使うことで高次の連立代数方程式に対しても変数消去を行い，解くことができる．本講義ではグレブナー基底の基本事項とその応用について解説する．

1　復習

この節ではこれまでに学んだであろう内容について復習する．その内容を直接用いることはほとんどないが，後の内容の理解に繋がるものである．

1.1　集合と論理についての復習

最初に論理と集合について復習する．この講義で必要になる知識は特に高尚なものではなく，ほとんどが高校数学で学んだものである．

集合について

集合とは「**要素**または**元**と呼ばれるものの集まり」である．x が集合 A の元であることを $x \in A$ で，x が A の元でないことを $x \notin A$ で表す．

集合は主に以下の 2 通りの方法で表される：

- **外延的記法** $\cdots$ 集合を全ての元を列挙して表す

$$\{1,2,3,4\},\ \{1,3,5,7,\ldots\},\ \{\ldots,-2,-1,0,1,2,\ldots\}$$

- **内包的記法** $\cdots$ 集合を元の満たす条件を用いて表す

$$\{x \mid x \text{ は整数で } 1 \leq x \leq 4\},\ \{x \mid x \text{ は奇数 }\},\ \{x \mid x \text{ は整数 }\}$$

縦線 $\mid$ の**左側に集合の元を，右側に元の満たす条件**を書く

（元の個数が無限個だと基本的に外延的記法では表せないので内包的記法をよく使う）

以下の集合を表す記号はよく使われる．

記号

(1) $\emptyset$：空集合（一つも元を含まない集合）

(2)
- $\mathbb{N} := \{0,1,2,\ldots\}$：自然数全体の集合（この講義では 0 も自然数に含める）
- $\mathbb{Z} := \{\ldots,-2,-1,0,1,2,\ldots\}$：整数全体の集合
- $\mathbb{R}$：実数全体の集合
- $\mathbb{C}$：複素数全体の集合

(3) 1 以上の整数 n に対して，$\mathbb{N}^n, \mathbb{Z}^n, \mathbb{R}^n, \mathbb{C}^n$ でそれぞれ n 個の自然数，整数，実数，複素数を成分に持つベクトル全体の集合を表す：
- $\mathbb{N}^n := \{(k_1,k_2,\ldots,k_n) \mid k_1,k_2,\ldots,k_n \text{ は自然数 }\}$
- $\mathbb{Z}^n := \{(k_1,k_2,\ldots,k_n) \mid k_1,k_2,\ldots,k_n \text{ は整数 }\}$
- $\mathbb{R}^n := \{(k_1,k_2,\ldots,k_n) \mid k_1,k_2,\ldots,k_n \text{ は実数 }\}$
- $\mathbb{C}^n := \{(k_1,k_2,\ldots,k_n) \mid k_1,k_2,\ldots,k_n \text{ は複素数 }\}$

集合に関する記号を復習する：

- $A \subseteq B$ （A は B の**部分集合**）$\overset{def}{\iff}$ 全ての A の元 a は B の元である
- $A = B$（A と B は**等しい**）$\overset{def}{\iff} A \subseteq B$ かつ $B \subseteq A$

  従って，集合 A と集合 B が等しいことを示したいならば，「全ての A の元が B の元であること」および「全ての B の元が A の元であること」を示せば良い．
- $A \cup B := \{x \mid x \in A \text{ または } x \in B\}$（$A$ と B の**和集合**）
- $A \cap B := \{x \mid x \in A \text{ かつ } x \in B\}$（$A$ と B の**共通集合**）
- $A - B := \{x \mid x \in A \text{ かつ } x \notin B\}$（$A$ と B の**差集合**）

例 1.1 $\mathbb{Z}$ の部分集合 A, B, C を $A = \{n \in \mathbb{Z} \mid n \text{ は } 2 \text{ の倍数 }\}$, $B = \{n \in \mathbb{Z} \mid n \text{ は } 3 \text{ の倍数 }\}$, $C = \{n \in \mathbb{Z} \mid n \text{ は } 6 \text{ の倍数 }\}$ とする． このとき，

$$A \cap B = C$$

が成り立つ．

$(\because)$ 集合の等号の定義から，$A \cap B \subseteq C$ および $C \subseteq A \cap B$ を示せば良い．

$A \cap B \subseteq C$:

$A \cap B$ の任意の元 n を考えると，これは A の元なので 2 の倍数，B の元でもあるので 3 の倍数でもある．従って，n は 2 の倍数かつ 3 の倍数なので 6 の倍数である．つまり，$n \in C$ となる．従って，$A \cap B \subseteq C$ が示された．

$C \subseteq A \cap B$:

C の任意の元 n を考えると，これは 6 の倍数である．6 の倍数は 2 の倍数なので n は A の元であり，6 の倍数は 3 の倍数なので n は B の元でもある．従って，n は A の元かつ B の元なので $n \in A \cap C$．よって，$C \subseteq A \cap B$ が示された．

論理について

真（正しい）か偽（正しくない）のどちらか判断できる文を**命題**と呼ぶ．例えば，「2 は偶数である」という命題は真であり，「3 は偶数である」という命題は偽である．

変数 x を含む文であり，x に値を代入すると命題になるものを**述語**と呼ぶ．例えば，x が自然数のときに「$P(x)$ は偶数である」という文は述語である．この場合，

- $x = 2 \rightsquigarrow P(2)$ は真
- $x = 3 \rightsquigarrow P(3)$ は偽

述語 $P(x)$ 用いた「任意の x に対して $P(x)$ が成り立つ」や「ある x が存在して $P(x)$ が成り立つ」という命題はよく現れる．これらはもう少し身近な言葉を使えば以下のような意味を持つ：

- 「任意の x に対して $P(x)$ が成り立つ」＝「どの x に対しても命題 $P(x)$ が真である」
- 「ある x が存在して $P(x)$ が成り立つ」＝「$P(x)$ が真になるような x がある」

> **例 1.2** (1)「任意の実数 x に対して $x^2 = 3$ が成り立つ」は偽である
> (2)「ある実数 x」に対して $x^2 = 3$ が成り立つ」は真である

述語を含む命題の否定については注意が必要である：

- 「任意の x に対して $P(x)$ が成り立つ」の否定は「ある x が存在して $P(x)$ が成り立たない」
- 「ある x が存在して $P(x)$ が成り立つ」の否定は「任意の x に対して $P(x)$ が成り立たない」

数学は定義，定理，命題，補題の繰り返しで進んでいく．確認の為にこれらの言葉についてまとめておく：

- **定義**：新たな概念や記号を導入すること
- **定理，命題，補題**：これらは命題と同義であるが，重要な順に「定理 $>$ 命題 $>$ 補題」と使い分けられる（明確な基準があるわけではなく，どのように呼ぶかは人による）．特に，補題は定理や命題の証明のための準備のときに使われる．

1.2 1 変数の多項式の復習

- 実数 a と自然数 n を用いて
$$ax^n$$
と表される式を x **の単項式**という．
- いくつかの（有限個の）単項式の和で表される式
$$a_n x^n + \cdots + a_2 x^2 + a_1 x + a_0 \quad (s \in \mathbb{N}, a_0, a_1, \ldots, a_n \in \mathbb{R})$$
を x **の多項式**という[*1]．
多項式は
$$f = \sum_{i \in \mathbb{N}} a_i x^i$$
と表すと便利である．ただし，a_i は実数であり，有限個の i を除いて $a_i = 0$ である（従って，上の $\sum$ は有限個の足し算となる）．
- 多項式
$$f = \sum_{i \in \mathbb{N}} a_i x^i$$
に対して，

[*1] 中学や高校では「多項式は 2 つ以上の単項式の和」と習ったかもしれないが，通常は 1 つの単項式の和（つまり，単項式）も多項式と呼ぶ

- a_i を x^i の**係数**という
- $a_i \neq 0$ のとき，$a_i x^i$ を f の**項**という．

- 二つの多項式 $f = \sum_{i \in \mathbb{N}} a_i x^i$, $g = \sum_{i \in \mathbb{N}} b_i x^i$ の和，差，積をそれぞれ
  - $f + g = \sum_{i \in \mathbb{N}} (a_i + b_i) x^i$
  - $f - g = \sum_{i \in \mathbb{N}} (a_i - b_i) x^i$
  - $fg = \sum_{k \in \mathbb{N}} \left(\sum_{i+j=k} a_i b_j \right) x^k$

  で定義する．和，差は各項ごとに係数の和，差を考えれば良い．積の定義は分かりにくいが，通常の数と同様に分配法則を用いて計算すれば良い．

  例：$f = -3x^3 + 2x^2 + 1$, $g = 6x^2 - 5x + 4$ に対して，
  - $f + g = -3x^3 + 8x^2 - 5x + 5$
  - $f - g = -3x^3 - 4x^2 + 5x - 3$
  - $fg = -18x^5 + 27x^4 - 22x^3 + 14x^2 - 5x + 4$

- 0 でない多項式
$$f = a_n x^n + \cdots + a_2 x^2 + a_1 x + a_0 \quad (a_n \neq 0)$$
に対して，
  - n を f の**次数（degree）**といい，$\deg f$ と表す
  - $a_n x^n$ を f の**先頭項（leading term）**といい，$\mathrm{LT}(f)$ と表す

  例：$f = -3x^3 + 2x^2 + 1$, $g = 6x^2 - 5x + 4$ に対して，
  - $\deg f = 3$, $\deg g = 2$
  - $\mathrm{LT}(f) = -3x^3$, $\mathrm{LT}(g) = 6x^2$

この講義で扱うグレブナー基底は多変数の多項式の割り算を上手く扱うために導入されたものである．ここで，1 変数の多項式の割り算について復習しておく．

命題 1.3 f, g を 1 変数の多項式とし，$g \neq 0$ とする．このとき，
$$f = qg + r \quad (r = 0 \text{ または } \deg r < \deg g)$$
を満たすような多項式 q, r が唯一組存在する．このような q, r をそれぞれ f を g **で割った商**，f を g **で割った余り**という．

証明の代わりに商と余りを求めるアルゴリズム[*2]を紹介する：

[*2] アルゴリズムとは答えを求めるための手続きのことである

割り算アルゴリズム（1 変数）

$q := 0$, $r := f$ からスタートして以下のループを繰り返す．

(i) $r = 0$ または $\deg r < \deg g$ ならば商を q，余りを r として終了．
$\deg r \geq \deg g$ ならば (ii) に進む．

(ii) q, r にそれぞれ

$$q + \frac{\mathsf{LT}(r)}{\mathsf{LT}(g)}, \qquad r - \frac{\mathsf{LT}(r)}{\mathsf{LT}(g)} \cdot g$$

を代入して (i) に戻る．

これを繰り返すと最終的に (i) において商 q，余り r が求まる．

例 1.4 $f = x^3 + 2x^2 - 11x + 7$ を $g = x^2 - 3x + 2$ で割り算する．

- $q = 0$, $r = x^3 + 2x^2 - 11x + 7$ からスタートする．
- $\deg r = 3 \geq 2 = \deg g$ なので，

$$\begin{aligned} q &= 0 + \frac{\mathsf{LT}(r)}{\mathsf{LT}(g)} = \frac{x^3}{x^2} = x \\ r &= (x^3 + 2x^2 - 11x + 7) - \frac{\mathsf{LT}(r)}{\mathsf{LT}(g)} \cdot (x^2 - 3x + 2) \\ &= (x^3 + 2x^2 - 11x + 7) - x(x^2 - 3x + 2) \\ &= 5x^2 - 13x + 7 \end{aligned}$$

とする．

- $\deg r = 2 = \deg g$ なので，

$$\begin{aligned} q &= x + \frac{\mathsf{LT}(r)}{\mathsf{LT}(g)} = x + \frac{5x^2}{x^2} = x + 5 \\ r &= (5x^2 - 13x + 7) - \frac{\mathsf{LT}(r)}{\mathsf{LT}(g)} \cdot (x^2 - 3x + 2) \\ &= (5x^2 - 13x + 7) - 5(x^2 - 3x + 2) \\ &= 2x - 3 \end{aligned}$$

- $\deg r = 1 < 2 = \deg g$ なので，商は $q = x + 5$，余りは $r = 2x - 3$ となる：

$$x^3 + 2x^2 - 11x + 7 = (x + 5)(x^2 - 3x + 2) + 2x - 3$$

以上の計算は高校で習った筆算で以下のように書くことができる：

$$\begin{array}{rr|llll} & & x & +5 & & \\ \hline x^2 - 3x + 2 &) & x^3 & +2x^2 & -11x & +7 \\ & & x^3 & -3x^2 & +2x & \\ \hline & & & 5x^2 & -13x & +7 \\ & & & 5x^2 & -15x & +10 \\ \hline & & & & 2x & -3 \end{array}$$

1.3　連立一次方程式の解法

次に，連立一次方程式

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ \qquad\qquad \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m \end{cases}$$

の解法（掃き出し法）について復習する．

この方程式は以下のようにして解くことができる．

(i) 連立方程式に以下の操作を行う：

- 1 つの方程式を 0 でない実数倍する
- 1 つの方程式の実数倍を別の方程式に加える
- 2 つの方程式を入れ替える

これらの操作は可逆なので，これらの操作を行っても連立方程式の解は変わらない．

(ii) (i) の操作を繰り返して変数を消去していき，

$$\begin{cases} x_1 + c_{11}x_{r+1} + \cdots + c_{1,n-r}x_n = d_1 \\ x_2 + c_{21}x_{r+1} + \cdots + c_{2,n-r}x_n = d_2 \\ \qquad\qquad \vdots \\ x_r + c_{r1}x_{r+1} + \cdots + c_{r,n-r}x_n = d_r \\ 0 = d_{r+1} \end{cases}$$

という形の連立方程式に変形する（つまり，(i) の操作で変数を消去している）．ただし，簡単のために必要ならば変数 $x_1, x_2, \ldots, x_n$ の順番を入れ替えている．

(iii)

- $d_{r+1} \neq 0$ のとき，方程式 $0 = d_{r+1}$ は不成立なのでこの連立方程式は解を持たない．
- $d_{r+1} = 0$ のとき，$x_{r+1} = t_1$, $x_{r+2} = t_2$, …, $x_n = t_{n-r}$ を任意の実数とすると (ii) の式より

$$\begin{aligned} x_1 &= -c_{11}t_1 - \cdots - c_{1,n-r}t_{n-r} + d_1 \\ x_2 &= -c_{21}t_1 - \cdots - c_{2,n-r}t_{n-r} + d_2 \\ &\vdots \\ x_r &= -c_{r1}t_1 - \cdots - c_{r,n-r}t_{n-r} + d_r \end{aligned}$$

となる．従って，この連立方程式の解は

$$\begin{cases} x_1 = -c_{11}t_1 + \cdots - c_{1,n-r}t_{n-r} + d_1 \\ x_2 = -c_{21}t_1 + \cdots - c_{2,n-r}t_{n-r} + d_2 \\ \qquad\qquad \vdots \\ x_r = -c_{r1}t_1 + \cdots - c_{r,n-r}t_{n-r} + d_r \\ x_{r+1} = t_1 \\ x_{r+2} = t_2 \\ \quad \vdots \\ x_n = t_{n-r} \end{cases}$$

ただし，$t_1, t_2, \ldots, t_{n-r}$ は任意の実数.

コメント　1 次式 $f_1, f_2, \ldots, f_m$ を

$$\begin{aligned} f_1 &= a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n - b_1 \\ f_2 &= a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n - b_2 \\ &\vdots \\ f_m &= a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n - b_m \end{aligned}$$

と置く．このとき上の (ii) は，ある実数 k_{ij} $(1 \leq i \leq r+1, 1 \leq j \leq n)$ を用いて

$$\begin{aligned} k_{11}f_1 + k_{12}f_2 + \cdots + k_{1m}f_m &= x_1 + c_{11}x_{r+1} + \cdots + c_{1,n-r}x_n - d_1 \\ k_{21}f_1 + k_{22}f_2 + \cdots + k_{2m}f_m &= x_2 + c_{21}x_{r+1} + \cdots + c_{2,n-r}x_n - d_2 \\ &\vdots \\ k_{r1}f_1 + k_{r2}f_2 + \cdots + k_{rm}f_m &= x_r + c_{r1}x_{r+1} + \cdots + c_{r,n-r}x_n - d_r \\ k_{r+1,1}f_1 + k_{r+1,2}f_2 + \cdots + k_{r+1,m}f_m &= -d_{r+1} \end{aligned}$$

と表せることを意味している.

例 1.5　連立方程式

$$\begin{cases} x + 3z = 1 \cdots ① \\ 2x + 3y + 4z = 3 \cdots ② \\ x + 3y + z = 2 \cdots ③ \end{cases}$$

を掃き出し法で解く.

(i) ① の -2 倍を ② に，-1 倍を ③ に加えると

$$\begin{cases} x + 3z = 1 \cdots ①' \\ 3y - 2z = 1 \cdots ②' \\ 3y - 2z = 1 \cdots ③' \end{cases}$$

となる.

②′ の -1 倍を ③′ に加え，②′ を $1/3$ 倍すると

$$\begin{cases} x+3z=1 \\ y-\dfrac{2}{3}z=\dfrac{1}{3} \\ 0=0 \end{cases}$$

となる．

(ii) このとき，元の連立方程式の解と連立方程式

$$\begin{cases} x+3z=1 \\ y-\dfrac{2}{3}z=\dfrac{1}{3} \end{cases}$$

の解は同じである．

(iii) $z=t$ を任意の実数とすれば，$x=-3t+1$, $y=\dfrac{2}{3}t+\dfrac{1}{3}$ となるので，この連立方程式の解は

$$(x,y,z)=(-3t+1,\frac{2}{3}t+\frac{1}{3},t) \quad (t \text{ は任意の実数})$$

となる．

この例において

$$\begin{aligned} f_1&=x+3z-1 \\ f_2&=2x+3y+4z-3 \\ f_3&=x+3y+z-2 \end{aligned}$$

と置くと，(ii) の操作で

$$\begin{aligned} f_1&=x+3z-1 \\ -\frac{2}{3}f_1+\frac{1}{3}f_2&=y-\frac{2}{3}z-\frac{1}{3} \end{aligned}$$

と変数が消去されていることが分かる．

演習問題

問題 1.1 以下の多項式 f を g で割った商と余りを求めよ．

(1) $f=2x^2-3x-4$, $g=x-3$
(2) $f=2x^3+7x^2+5x+6$, $g=x+1$
(3) $f=2x^3+3x^2-11x+3$, $g=x^2+3x-1$
(4) $f=6x^3-11x^2+4x-7$, $g=3x^3-x+4$

問題 1.2　以下の連立一次方程式の解を掃き出し法で求めよ.

(1) $\begin{cases} x+y=2 \\ 2x+5y=7 \end{cases}$　(2) $\begin{cases} 3x+7y+7z=2 \\ x+2y+2z=7 \end{cases}$　(3) $\begin{cases} x+2y=3 \\ 3x-y+z=0 \\ 2x+y+z=0 \end{cases}$　(4) $\begin{cases} x+y-3z=2 \\ x-y+5z=10 \\ 2x+2y-6z=5 \end{cases}$

2　多変数の多項式

2.1　多変数の多項式の基礎

変数が 2 個以上の場合も 1 変数の場合と同様に多項式を定義することができる．

定義 2.1 (多変数の多項式)

(1) 実数 a と自然数 $\alpha_1, \alpha_2, \ldots, \alpha_n$ を用いて

$$ax_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n}$$

と表される式を $x_1, x_2, \ldots, x_n$ **の単項式**という．

簡単のため，自然数のベクトル $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{N}^n$ に対して，

$$x^\alpha := x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n}$$

と書くことにする．このとき α を単項式 ax^α の**指数ベクトル**という．1 変数の場合と同様に，$x_i^0 = 1$ とする．

例：

- $\alpha = (4, 2, 1) \rightsquigarrow x^\alpha = x_1^4x_2^2x_3$
- $\alpha = (0, 1, 2) \rightsquigarrow x^\alpha = x_1^0x_2x_3^2 = x_2x_3^2$

(2) いくつかの（有限個の）単項式の和で表される式を $x_1, x_2, \ldots, x_n$ **の多項式**という．

1 変数の場合と同様に，多項式は

$$f = \sum_{\alpha\in\mathbb{N}^n} a_\alpha x^\alpha$$

と表すことができる．ただし，係数 a_α は実数であり，有限個の α を除いて a_α は 0 である（従って，上の $\sum$ は有限個の足し算となる）．

例：

- $f = x_1^2 + x_2^2x_3 \quad (\alpha = (2,0,0), (0,2,1)$ 以外の α について $a_\alpha = 0)$
- $f = \pi\, x_1x_2^3x_3x_4 + 2x_2x_3^3x_4^2 + \mathrm{e}\, x_3x_4^3$
  $(\alpha = (1,3,1,1), (0,1,3,2), (0,0,1,4)$ 以外の α について $a_\alpha = 0)$

(3) 多項式

$$f = \sum_{\alpha\in\mathbb{N}^n} a_\alpha x^\alpha$$

に対して，

- a_α を x^α **の係数**という
- $a_\alpha \neq 0$ のとき，$a_\alpha x^\alpha$ を f **の項**という．

変数 $x_1, x_2, \ldots, x_n$ の多項式全てを元とする集合を $\mathbb{R}[x_1, x_2, \ldots, x_n]$ と書く．
n が 3 以下の場合，x_1, x_2, x_3 の代わりに使い慣れた記号 x, y, z を用いることにする．

注意　二つの多項式 $f=\sum_{\alpha\in\mathbb{N}^n} a_\alpha x^\alpha$, $g=\sum_{\alpha\in\mathbb{N}^n} b_\alpha x^\alpha$ に対して，

$$f=g \Longleftrightarrow \text{全ての } \alpha\in\mathbb{N} \text{ に対して } a_\alpha=b_\alpha$$

であることに注意しておく．

定義 2.2 (多項式の和，差，積)　二つの多項式 $f=\sum_{\alpha\in\mathbb{N}^n} a_\alpha x^\alpha$, $g=\sum_{\alpha\in\mathbb{N}^n} b_\alpha x^\alpha$ に対して，f と g の和，差，積をそれぞれ

- $f+g=\sum_{\alpha\in\mathbb{N}^n}(a_\alpha+b_\alpha)x^\alpha$
- $f-g=\sum_{\alpha\in\mathbb{N}^n}(a_\alpha-b_\alpha)x^\alpha$
- $fg=\sum_{\gamma\in\mathbb{N}^n}\left(\sum_{\alpha+\beta=\gamma} a_\alpha b_\beta\right)x^\gamma$

と定義する．1 変数の場合と同様に，和，差は各係数の和，差を計算すれば良く，積は分配法則を使って計算すれば良い．

例 2.3　$f=x^2y+y^2z+xz^2$, $g=x^3yz+3xz^2+y^2z$ に対して，

- $f+g=x^3yz+x^2y+4xz^2+2y^2z$
- $f-g=-x^3yz+x^2y-2xz^2$
- $fg=x^5y^2z+x^4yz^3+x^3y^3z^2+3x^3yz^2+x^2y^3z+3x^2z^4+4xy^2z^3+y^4z^2$

多項式の和，差，積は通常の数と同じように以下の自然な性質を満たす．

命題 2.4　多項式 f,g,h に対して以下が成り立つ：

(1) $(f+g)+h=f+(g+h)$
(2) $f+0=0+f$
(3) $f+(-f)=(-f)+f=0$
(4) $f+g=g+f$
(5) $f\cdot 1=1\cdot f=f$
(6) $(fg)h=f(gh)$
(7) $f(g+h)=fg+fh \quad (f+g)h=fh+gh$
(8) $fg=gf$

コメント　性質 (1) ∼ (4) は $\mathbb{R}[x_1, x_2, \ldots, x_n]$ が和に関して**可換群**であることを意味する．さらに，性質 (1) ∼ (8) は $\mathbb{R}[x_1, x_2, \ldots, x_n]$ が和と積に関して**可換環**であることを意味する．

定義 2.5　2 つの 0 でない単項式 $f = ax^\alpha$, $g = bx^\beta$ を考える．

(1) f が g **で割り切れる**とは，$f = qg$ となる単項式 q が存在するときに言う．

これは $\alpha - \beta$ の成分が全て 0 以上であることと同値である．

- x^2y^2z は xy で割り切れる（$(2,2,1) - (1,1,0) = (1,1,1)$ の成分は全て 0 以上）
- x^4yz^2 は $2x^3yz$ で割り切れる（$(4,1,2) - (3,1,1) = (1,0,1)$ の成分は全て 0 以上）

(2) f と g **が互いに素である**とは，f と g を共に割り切る単項式が存在しないときに言う．

これは各 i に対して，「α_i と β_i のいずれかは正ではない」ことと同値である．

- x^3y と z^3 は互いに素（$(3,1,0)$ と $(0,0,3)$ の各成分が共に正になることはない）
- x^2 と y^2z は互いに素（$(2,0,0)$ と $(0,2,1)$ の各成分が共に正になることはない）

2.2　イデアル

$x_1, x_2, \ldots, x_n$ の多項式 $f_1, f_2, \ldots, f_m$ の連立方程式

$$\begin{cases} f_1 = 0 \\ f_2 = 0 \\ \quad \vdots \\ f_m = 0 \end{cases}$$

を考える．$f_1, f_2, \ldots, f_m$ が 1 次式の場合は 1.3 節で見たように $f_1, f_2, \ldots, f_m$ の線形結合（実数倍を足したもの）を用いて変数を消去して解くことができる．しかし，次数が 1 より大きくなると状況は複雑になり，以下の点が問題となる：

(a) 実数倍して足し引きするだけでは変数が消去できない：

例えば $f_1 = x^2y + z, f_2 = xy^2 + yz$ から x^2y および xy^2 を消去するとき，実数倍では不十分であり，多項式倍を考える必要がある．実際，

$$yf_1 - xf_2 = y(x^2y + z) - x(xy^2 + yz) = yz - xyz$$

とすれば x^2y および xy^2 が消去される．

(b) 多項式倍を用いて消去しても別の項にまた現れることがある：

上の例では x^2y および xy^2 が消去されるが，新たに xyz の項が現れてしまっている．

(a) のような状況を扱うために以下の概念を導入する．

定義 2.6 (1) 多項式 $f_1, f_2, \ldots, f_m \in \mathbb{R}[x_1, x_2, \ldots, x_n]$ に対して，

$$q_1 f_1 + q_2 f_2 + \cdots + q_m f_m \quad (q_1, q_2, \ldots, q_m \in \mathbb{R}[x_1, x_2, \ldots, x_n])$$

の形の多項式を $f_1, f_2, \ldots, f_m$ **の多項式線形結合**という．

(2) S を $x_1, x_2, \ldots, x_n$ の多項式の集合とする（つまり，$\mathbb{R}[x_1, x_2, \ldots, x_n]$ の部分集合）．
このとき，S の有限個の元の多項式線型結合すべてを元とするような $\mathbb{R}[x_1, x_2, \ldots, x_n]$ の部分集合を $\langle S \rangle$ と書く：

$$\langle S \rangle := \{q_1 f_1 + q_2 f_2 + \cdots + q_m f_m \mid m \geq 1,\ f_1, f_2, \ldots, f_m \in S,\ q_1, q_2, \ldots, q_m \in \mathbb{R}[x_1, x_2, \ldots, x_n]\}$$

このような形の $\mathbb{R}[x_1, x_2, \ldots, x_n]$ の部分集合を**イデアル**と呼ぶ．

(3) S が有限個の多項式からなる集合 $S = \{f_1, f_2, \ldots, f_m\}$ のとき，$\langle S \rangle$ を

$$\langle f_1, f_2, \ldots, f_m \rangle$$

と書く．このとき，$f_1, f_2, \ldots, f_m$ を**イデアル** $\langle f_1, f_2, \ldots, f_m \rangle$ **の基底**と呼ぶ．
注意深く考えると，

$$\langle f_1, f_2, \ldots, f_m \rangle = \{q_1 f_1 + q_2 f_2 + \cdots + q_m f_m \mid q_1, q_2, \ldots, q_m \in \mathbb{R}[x_1, x_2, \ldots, x_n]\}$$

となることが分かる．つまり，$\langle f_1, f_2, \ldots, f_m \rangle$ は $f_1, f_2, \ldots, f_m$ の全ての多項式線形結合を元として持つ集合である．

例 2.7 $f_1 = x^2 - y^2$, $f_2 = 2x + y^2 + 1$ のとき，

$$\begin{aligned} f_1 + f_2 &= x^2 + 2x + 1 \\ (x+1)f_1 + xyf_2 &= x^3 + 2x^2y + x^2 - xy^3 - xy^2 + xy - y^2 \\ (xy + x + y)f_1 + (x^2 + y)f_2 &= x^3y + 3x^3 + x^2y^2 + x^2y + x^2 - xy^3 - xy^2 + 2xy + y \end{aligned}$$

は f_1 と f_2 の多項式線形結合である．

注意 (1) S の元 f は多項式 1 を用いて $1 \cdot f$ と書けるので，f は $\langle S \rangle$ の元である．
(2) イデアルの基底は一通りとは限らない：

$$\langle x^2 - y^2, 2x + y^2 + 1 \rangle = \langle x^2 - y^2, x^2 + 2x + 1 \rangle$$

命題 2.8 I を $\mathbb{R}[x_1, x_2, \ldots, x_n]$ のイデアルとする．このとき，以下のことが成り立つ：

(i) $0 \in I$
(ii) $f, g \in I$ ならば $f + g \in I$

(iii) $f \in I$, $g \in \mathbb{R}[x_1, x_2, \ldots, x_n]$ ならば $fg \in I$

コメント　実は $\mathbb{R}[x_1, x_2, \ldots, x_n]$ の部分集合 I が命題 2.8 の条件 (i)(ii)(iii) を満たすことと I がイデアルであることは同値であり，(i)(ii)(iii) をイデアルの定義とするのが普通である．

以下の定理はこの講義では表立っては余り現れないが，グレブナー基底の理論の中で重要な役割を果たす．

定理 2.9（ヒルベルトの基底定理）　$\mathbb{R}[x_1, x_2, \ldots, x_n]$ のどのイデアル $I = \langle S \rangle$ も有限個の $f_1, f_2, \ldots, f_m \in S$ を用いて

$$I = \langle f_1, f_2, \ldots, f_m \rangle$$

と書ける（任意のイデアルは基底を持つ）．

コメント　ヒルベルトの基底定理によりイデアルには基底が存在することが分かるが，その基底が具体的にどのようなものかは定理の証明からは全く分からない．それゆえにこの定理は当時「数学ではなく神学である」と言われた．

イデアルの概念は抽象的で分かりにくいが以下の命題がその有用性を表している：

命題 2.10　多項式 $f_1, f_2, \ldots, f_m, g_1, g_2, \ldots, g_t \in \mathbb{R}[x_1, x_2, \ldots, x_n]$ について，$\langle f_1, f_2, \ldots, f_m \rangle = \langle g_1, g_2, \ldots, g_t \rangle$ が成り立つとする．このとき，2 つの連立方程式

$$(1) \begin{cases} f_1 = 0 \\ f_2 = 0 \\ \quad \vdots \\ f_m = 0 \end{cases} \quad \text{と} \quad (2) \begin{cases} g_1 = 0 \\ g_2 = 0 \\ \quad \vdots \\ g_t = 0 \end{cases}$$

の解は等しい．

証明．$\boldsymbol{a} = (a_1, a_2, \ldots, a_n)$ が連立方程式 (1) の解であるとする．つまり，

$$f_1(\boldsymbol{a}) = f_2(\boldsymbol{a}) = \cdots = f_m(\boldsymbol{a} = 0$$

とする．各 g_i は $\langle g_1, g_2, \ldots, g_t \rangle = \langle f_1, f_2, \ldots, f_m \rangle$ の元なので，ある多項式 $q_{i1}, q_{i2}, \ldots, q_{is}$ を用いて

$$g_i = q_{i1} f_1 + q_{i2} f_2 + \cdots + q_{is} f_m$$

と表せる．このとき，$\boldsymbol{a}$ を代入して

$$g_i(\boldsymbol{a}) = q_{i1}(\boldsymbol{a}) f_1(\boldsymbol{a}) + q_{i2}(\boldsymbol{a}) f_2(\boldsymbol{a}) + \cdots + q_{is}(\boldsymbol{a}) f_m(\boldsymbol{a}) = 0$$

となる．従って，

$$g_1(\boldsymbol{a}) = g_2(\boldsymbol{a}) = \cdots = g_t(\boldsymbol{a}) = 0$$

が成り立つので，$\boldsymbol{a}$ は連立方程式 (2) の解となる．

連立方程式 (2) の解が (1) の解となることも同様に証明できる． ■

コメント $\mathbb{R}[x_1, x_2, \ldots, x_n]$ の多項式 $f_1, f_2, \ldots, f_m$ とイデアル I に対して，$f_1, f_2, \ldots, f_m$ が I の元ならば $\langle f_1, f_2, \ldots, f_m \rangle \subseteq I$ が成り立つことが分かる（命題 2.8 より）．

従って，$\langle f_1, f_2, \ldots, f_m \rangle = \langle g_1, g_2, \ldots, g_t \rangle$ を示すためには

- $f_1, f_2, \ldots, f_m \in \langle g_1, g_2, \ldots, g_t \rangle$
- $g_1, g_2, \ldots, g_t \in \langle f_1, f_2, \ldots, f_m \rangle$

が成り立つことを示せば良い．

例 2.11 (1) 1 次式 $f_1 = x+3z-1$, $f_2 = 2x+3y+4z-3$, $f_3 = x+3y+z-2$, $g_1 = x+3z-1$, $g_2 = y - \dfrac{2}{3}z - \dfrac{1}{3}$ を考えると，

- $g_1 = f_1,\ g_2 = -\dfrac{2}{3}f_1 + \dfrac{1}{3}f_2 \in \langle f_1, f_2, f_3 \rangle$
- $f_1 = g_1,\ f_2 = 2g_1 + 3g_2,\ f_3 = g_1 + 3g_2 \in \langle g_1, g_2 \rangle$

より

$$\langle f_1, f_2, f_3 \rangle = \langle g_1, g_2 \rangle$$

が成り立つ．従って，連立方程式

$$\begin{cases} x + 3z = 1 \\ 2x + 3y + 4z = 3 \\ x + 3y + z = 2 \end{cases}$$

の解と

$$\begin{cases} x + 3z = 1 \\ 3y - 2z = 1 \end{cases}$$

の解は等しい．この解は 1 節で求めたように

$$(x, y, z) = (-3t + 1, \frac{2}{3}t + \frac{1}{3}, t) \quad (t \text{ は任意の実数})$$

である．

(2) $f_1 = x^2 - y^2$, $f_2 = 2x + y^2 + 1$, $g_1 = x^2 - y^2$, $g_2 = x^2 + 2x + 1$ を考えると，

- $g_1 = f_1,\ g_2 = f_1 + f_2 \in \langle f_1, f_2 \rangle$
- $f_1 = g_2,\ f_2 = -g_1 + g_2 \in \langle g_1, g_2 \rangle$

より

$$\langle f_1, f_2 \rangle = \langle g_1, g_2 \rangle$$

となる．従って，連立方程式

$$(*) \begin{cases} x^2 - y^2 = 0 \\ 2x + y^2 + 1 = 0 \end{cases}$$

の解と

$$\begin{cases} x^2 - y^2 = 0 \cdots ① \\ x^2 + 2x + 1 = 0 \cdots ② \end{cases}$$

の解は等しい．

② より $x = -1$ となる．これを ① に代入して $1 - y^2 = 0$ となるので $y = \pm 1$.

従って，連立方程式 $(*)$ の解は $(x, y) = (-1, \pm 1)$ となる．

このように，連立方程式

$$\begin{cases} f_1 = 0 \\ f_2 = 0 \\ \quad \vdots \\ f_m = 0 \end{cases}$$

を解きたければ，イデアル $\langle f_1, f_2, \ldots, f_m \rangle$ の基底 $g_1, g_2, \ldots, g_t$ でより簡単なものが取れれば良い．この基底をどのように取るかは次節以降で議論していく．

与えられた多項式 f がイデアル $I = \langle S \rangle$ の元になるかどうか（つまり，f が S の元 $f_1, f_2, \ldots, f_m$ の多項式線形結合となるかどうか）を判定できるか？という問題（**イデアル所属問題**）は一般に難しい問題であるが，この講義で扱うグレブナー基底を用いることで $f \in I$ となるかどうかを判定するアルゴリズムを作ることができる．

一方で，f および S の元が全て単項式の場合，イデアル所属問題は簡単に確かめることができる．

命題 2.12 S を $x_1, x_2, \ldots, x_n$ の単項式からなる集合，f を $x_1, x_2, \ldots, x_n$ の単項式とする．このとき，以下が成り立つ：

$$f \in \langle S \rangle \iff f \text{ は } S \text{ のある元で割り切れる}$$

証明.（$\Longleftarrow$）f が S の元 g で割り切れる，つまり，ある単項式 q を用いて $f = qg$ と表せるとする．このとき，f は S の元 g の多項式線形結合なので $f \in \langle S \rangle$ が成り立つ．

（$\Longrightarrow$）$f \in \langle S \rangle$ とすると，ある S の元 $f_1, f_2, \ldots, f_m$ と多項式 $q_1, q_2, \ldots, q_m$ が存在して $f = q_1 f_1 + q_2 f_2 + \cdots + q_m f_m$ と表せる．仮定から S の元 f_i は単項式なので $f_i = a_i x^{\alpha(i)}$ $(a_i \in \mathbb{R}, \alpha(i) \in \mathbb{N}^n)$ と表せる．f が単項式で $f = q_1 f_1 + q_2 f_2 + \cdots + q_m f_m$ となることから，単項式 f は $q_1 f_1, q_2 f_2, \ldots, q_m f_m$ のいずれかの項となる．f が $q_i f_i$ の項であるとき，f は q_i のある項 $b x^\beta$ と

$f_i = a_i x^{\alpha(i)}$ の積となるので f は S の元 f_i で割り切れる． ■

演習問題

問題 2.1 多項式 $f = xy + yz^2 + z$ を $g = x^2 + xy$ について，以下の多項式を求めよ．

$$(1)\ f - g \quad (2)\ xf - yg \quad (3)\ fg$$

問題 2.2 以下の集合の等式を確かめよ．

(1) $\langle x - y, x + y \rangle = \langle x, y \rangle$
(2) $\langle x + xy, y + xy, x^2, y^2 \rangle = \langle x, y \rangle$

ヒント：命題 2.10 の後のコメントにより，「左辺の基底が右辺の元となること」および「右辺の基底が左辺の元となること」を示せば良い．

3　多変数多項式の割り算

1 変数の多項式の割り算を思い出すと，$r = f$ からスタートして r の最高次の項 $\mathsf{LT}(r)$ を

$$r - \frac{\mathsf{LT}(r)}{\mathsf{LT}(g)} \cdot g$$

として消去することを繰り返せば余りを求めることができた．しかし，多変数の場合には同じ次数の項が複数ある（例えば x^2y, xy^2 はどちらも 3 次）のでどちらを消去すればよいか分からない．そこで，単項式に大小を付けて大きい項から順に消去していくことで多変数の場合にも多項式の割り算を考えることができる．

定義 3.1　$\mathbb{N}^n$ の**項順序**とは，各 $\alpha, \beta \in \mathbb{N}^n$ $(\alpha \neq \beta)$ に対して以下の条件を満たす大小関係 $\alpha > \beta$ を与えるもの：

(0) 3 つの $\alpha, \beta, \gamma \in \mathbb{N}^n$ に対して

$$\alpha > \beta,\ \beta > \gamma \Longrightarrow \alpha > \gamma$$

が成り立つ．

(1) 2 つの $\alpha, \beta \in \mathbb{N}^n$ に対して

$$\alpha > \beta,\ \alpha = \beta,\ \beta > \alpha$$

のいずれか一つのみが成り立つ．

(2) 3 つの $\alpha, \beta, \gamma \in \mathbb{N}^n$ に対して

$$\alpha > \beta \Longrightarrow \alpha + \gamma > \beta + \gamma$$

が成り立つ．

(3) 全ての $\mathbf{0} \neq \alpha \in \mathbb{N}^n$ に対して $\alpha \geq \mathbf{0}$ が成り立つ．

項順序を用いて単項式 x^α, x^β の間の大小を

$$x^\alpha > x^\beta \overset{def}{\Longleftrightarrow} \alpha > \beta$$

で定める．このとき，上の条件は

(0) 3 つの単項式 $x^\alpha, x^\beta, x^\gamma$ に対して

$$x^\alpha > x^\beta,\ x^\beta > x^\gamma \Longrightarrow x^\alpha > x^\gamma$$

が成り立つ．

(1) 2 つの単項式 x^α, x^β に対して

$$x^\alpha > x^\beta,\ x^\alpha = x^\beta,\ x^\beta > x^\alpha$$

のいずれか一つのみが成り立つ．

(2) 3 つの単項式 $x^\alpha, x^\beta, x^\gamma$ に対して

$$x^\alpha > x^\beta \Longrightarrow x^\alpha x^\gamma > x^\beta x^\gamma$$

が成り立つ.

(3) 全ての 1 でない単項式 x^α に対して $x^\alpha > 1$ が成り立つ.

と書き換えることができる.

例 3.2 2 つの $\alpha, \beta \in \mathbb{N}^n$ $(\alpha \neq \beta)$ に対して大小関係 $\alpha > \beta$ を

$$\alpha > \beta \overset{def}{\Longleftrightarrow} \alpha - \beta \text{ の一番左の } 0 \text{ でない成分が正}$$

で定義すると，これは項順序となる．これを**辞書式順序**と呼ぶ.

- $(2,3,2) - (2,1,1) = (0,2,1)$ の一番左の 0 でない成分 2 は正なので

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

- $(1,3,4,1) - (1,3,2,1) = (0,0,2,0)$ の一番左の 0 でない成分 2 は正なので

$$(1,3,4,1) > (1,3,2,1)$$

- $(3,2,3,1) - (2,4,4,3) = (1,-2,-1,-2)$ の一番左の 0 でない成分 1 は正なので

$$(3,2,3,1) > (2,4,4,3)$$

辞書式順序に関して

$$(1,0,\ldots,0) > (0,1,0,\ldots,0) > \cdots > (0,0,\ldots,1) > \mathbf{0}$$

が成り立つので,

$$x_1 > x_2 > \cdots > x_n > 1$$

となる.

注意 1 変数の場合，辞書式順序は

$$x^i > x^j \Longleftrightarrow i > j$$

という順序となる．従って，この場合は単項式の次数の大小と一致する.

実は 1 変数の場合の項順序はこの順序のみであることが知られている．1 変数の多項式の割り算の際に項順序について言及する必要がなかったのはこれが理由である.

以下，項順序は辞書式順序のみを考える（他の項順序については演習問題参照）.

多項式 $f = a_m x^{\alpha(m)} + \cdots + a_2 x^{\alpha(2)} + \cdots + a_1 x^{\alpha(1)} \in \mathbb{R}[x_1, x_2, \cdots, x_n]$ は

$$x^{\alpha(m)} > \cdots x^{\alpha(2)} > x^{\alpha(1)}$$

となっているとき，項順序に関して**降べきの順**であるという．1 変数の場合と同様に降べきの順に並べておくと分かりやすい[*3]．降べきの順に並べた場合に一番左に現れる項およびその指数として 1 変数の場合と同様に以下の定義ができる．

定義 3.3 0 でない多項式 $f \in \mathbb{R}[x_1, x_2, \ldots, x_n]$ を降べきの順で

$$f = a_1 x^{\alpha(1)} + a_2 x^{\alpha(2)} + \cdots + a_m x^{\alpha(m)} \quad (a_1 \neq 0)$$

と表したとき，

- $\alpha(1)$ を f **の多重次数（multi-degree）**と呼び，$\mathsf{mdeg}\, f$ と書く．
- $a_1\alpha(1)$ を f **の先頭項（leading term）**と呼び，$\mathsf{LT}(f)$ と書く

定義から，f を降べきの順に並べたときに一番左に来る項が先頭項であり，その指数ベクトルが多重次数である．

例 3.4 (1) 2 変数の多項式 $f = 2x^2y + xy^4 - xy^2 + 3x^2$ の項の指数ベクトルは左から順に $(2,1), (1,4), (1,2), (2,0)$ となっている．辞書式順序で

$$(2,1) > (2,0) > (1,4) > (1,2)$$

となるので，f を降べきの順に並べると

$$f = 2x^2y + 3x^2 + xy^4 - xy^2$$

となる．従って，

- $\mathsf{mdeg}\, f := (2,1)$
- $\mathsf{LT}(f) := 2x^2y$

(2) 3 変数の多項式 $f = 4xy^2z + 7x^2z^2 - 5x^3 + 4z^2$ の項の指数は左から順に $(1,2,1), (2,2,0), (3,0,0), (0,0,2)$ となっている．辞書式順序で

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

となるので，f を降べきの順に並べると

$$f = -5x^3 + 7x^2z^2 + 4xy^2z + 4z^2$$

となる．従って，

[*3] もちろん昇べきの順でもよい

- $\mathsf{mdeg}\, f := (3,0,0)$
- $\mathsf{LT}(f) := -5x^3$

以上の定義の元で，多変数の多項式の割り算は 1 変数の場合と同様に行われる．

命題 3.5 $x_1, x_2, \ldots, x_n$ の 0 でない多項式 $f_1, f_2, \ldots, f_m \in \mathbb{R}[x_1, x_2, \ldots, x_n]$ を考える．このとき，任意の多項式 f はある多項式 $q_1, q_2, \ldots, q_m, r$ を用いて

$$f = q_1 f_1 + q_2 f_2 + \cdots q_m f_m + r$$

と表せる．ただし，$q_1, q_2, \ldots, q_m, r$ は

- $r = 0$ または r のどの項も $\mathsf{LT}(f_1), \mathsf{LT}(f_2), \ldots, \mathsf{LT}(f_m)$ で割り切れない．
- $q_i f_i \neq 0$ ならば $\mathsf{mdeg}(f) \geq \mathsf{mdeg}(q_i f_i)$ となる．

を満たす．

これを満たすような $q_1, q_2, \ldots, q_m$ を f を $f_1, f_2, \ldots, f_m$ **で割った商**，r を f を $f_1, f_2, \ldots, f_m$ **で割った余り**という．

商と余りは以下のアルゴリズムで求めることができる．

割り算アルゴリズム（多変数）

$q_1 = q_2 = \cdots = q_m := 0$, $r := f$ からスタートして以下のループを繰り返す．

(i) $r = 0$ または r のどの項も $\mathsf{LT}(f_1), \mathsf{LT}(f_2), \ldots, \mathsf{LT}(f_m)$ で割り切れないならば $q_1, q_2, \ldots, q_m$ を商，r を余りとして終了．

それ以外の場合は (ii) に進む．

(ii) r のある項 ax^α がいずれかの $\mathsf{LT}(f_i)$ で割り切れるとき，q_i, r にそれぞれ

$$q_i + \frac{ax^\alpha}{\mathsf{LT}(f_i)}, \qquad r - \frac{ax^\alpha}{\mathsf{LT}(f_i)} \cdot f_i$$

を代入して (i) に戻る（q_i 以外の q_j はそのまま）．

これを繰り返すと最終的に (i) において商 $q_1, q_2, \ldots, q_m$，余り r が求まる．

例 3.6 (1) $f = xy^2 + 1$ を $f_1 = xy + 1$, $f_2 = y + 1$ で割り算する．

- $q_1 = q_2 = 0$, $r = f = xy^2 + 1$ からスタートする．

- $r = xy^2 + 1$ の項 xy^2 は $\mathsf{LT}(f_1) = xy$ で割り切れるので

$$q_1 = 0 + \frac{xy^2}{\mathsf{LT}(f_1)} = y$$
$$q_2 = 0$$
$$r = (xy^2 + 1) - \frac{xy^2}{\mathsf{LT}(f_1)} \cdot f_1 = (xy^2 + 1) - y(xy + 1) = -y + 1$$

  と置く.
- $r = -y + 1$ の項 $-y$ は $\mathsf{LT}(f_2) = y$ で割り切れるので

$$q_1 = y$$
$$q_2 = 0 + \frac{-y}{\mathsf{LT}(f_2)} = -1$$
$$r = (-y + 1) - \frac{-y}{\mathsf{LT}(f_2)} \cdot f_2 = (-y + 1) - (-1)(y + 1) = 2$$

  と置く.
- $r = 2$ のどの項も $\mathsf{LT}(f_1) = xy$, $\mathsf{LT}(f_2) = y$ で割り切れないので，商 $q_1 = y$, $q_2 = -1$, 余り $r = 2$ を得る：

$$xy^2 + 1 = y(xy + 1) + (-1)(y + 1) + 2$$

以上の計算は筆算を用いて以下のように表す：

$$\begin{array}{rr|l} & q_1: \quad y & \\ & q_2: \quad -1 & \\ \hline xy+1 & & \\ y+1 \;\big) & xy^2 \quad +1 & \\ & xy^2 \quad +y & \\ \hline & \quad -y \quad +1 & \\ & \quad -y \quad -1 & \\ \hline & \qquad\quad 2 & \end{array}$$

(2) $f = x^2y + xy^2 + y^2$ を $f_1 = xy - 1$, $f_2 = y^2 - 1$ で割り算する.

- $q_1 = q_2 = 0$, $r = f = x^2y + xy^2 + y^2$ からスタートする.
- $r = x^2y + xy^2 + y^2$ の項 x^2y は $\mathsf{LT}(f_1) = xy$ で割り切れるので

$$q_1 = 0 + \frac{x^2y}{\mathsf{LT}(f_1)} = x$$
$$q_2 = 0$$
$$r = (x^2y + xy^2 + y^2) - \frac{x^2y}{\mathsf{LT}(f_1)} \cdot f_1 = (x^2y + xy^2 + y^2) - x(xy - 1) = xy^2 + x + y^2$$

  と置く.

- $r = xy^2 - x + y^2$ の項 xy^2 は $\mathsf{LT}(f_1) = xy$ で割り切れるので

$$q_1 = x + \frac{xy^2}{\mathsf{LT}(f_1)} = x + y$$
$$q_2 = 0$$
$$r = (xy^2 - x + y^2) - \frac{xy^2}{\mathsf{LT}(f_1)} \cdot f_1 = (xy^2 + x + y^2) - y(xy - 1) = x + y^2 + y$$

  と置く．
- $r = x + y^2 + y$ の項 y^2 は $\mathsf{LT}(f_2) = y^2$ で割り切れるので

$$q_1 = x + y$$
$$q_2 = 0 + \frac{y^2}{\mathsf{LT}(f_2)} = 1$$
$$r = (x + y^2 + y) - \frac{y^2}{\mathsf{LT}(f_2)} \cdot f_2 = (x + y^2 + y) - (y^2 - 1) = x + y + 1$$

- $r = x+y+1$ のどの項も $\mathsf{LT}(f_1) = xy$, $\mathsf{LT}(f_2) = y^2$ で割り切れないので，商 $q_1 = x+y$, $q_2 = 1$, 余り $r = x + y + 1$ を得る：

$$x^2y + xy^2 + y^2 = (x + y)(xy - 1) + 1 \cdot (y^2 - 1) + x + y + 1$$

以上の計算は筆算を用いて以下のように表す：

$$\begin{array}{rlllll}
 & q_1: & x & +y & & \\
 & q_2: & 1 & & & \\
\hline
\begin{matrix} xy-1 \\ y^2-1 \end{matrix} \Big) & x^2y & +xy^2 & +y^2 & & \\
 & xy^2 & -x & & & \\
\hline
 & & xy^2 & +x & +y^2 & \\
 & & xy^2 & -y & & \\
\hline
 & & & x & +y^2 & +y \\
 & & & & y^2 & -1 \\
\hline
 & & & x & +y & +1
\end{array}$$

注意　例 3.6(2) の例において，

$$x^2y + xy^2 + y^2 = x(xy - 1) + (x + 1) \cdot (y^2 - 1) + 2x + 1$$

と表すこともでき，余りは $2x+1$ となる．従って，1 変数の場合と異なり**多変数の場合は商と余りは一通りに決まらない．**

以下しばしば「f を $f_1, f_2, \ldots, f_m$ で割った余りが 0 である」という表現をするが，これは余りが 0 になるような割り算が存在する．つまり，

- $f = q_1f_1 + q_2f_2 + \cdots + q_mf_m$ かつ
- $q_if_i \neq 0$ ならば $\mathsf{mdeg}(f) \geq \mathsf{mdeg}(q_if_i)$

となるような多項式 $q_1, q_2, \ldots, q_m$ が存在することを言う.

演習問題

問題 3.1 $\alpha, \beta \in \mathbb{N}^n$ $(\alpha \neq \beta)$ に対して $\alpha > \beta$ を以下のように定めると項順序となることを示せ.

(1) $\alpha > \beta \overset{def}{\iff}$
- $\displaystyle\sum_{i=1}^{n} \alpha_i > \sum_{i=1}^{n} \beta_i$, または
- $\displaystyle\sum_{i=1}^{n} \alpha_i = \sum_{i=1}^{n} \beta_i$ かつ $\alpha - \beta$ の一番左の 0 でない成分が正

このように定義される項順序を**次数付き辞書式順序**と呼ぶ.

(2) $\alpha > \beta \overset{def}{\iff} \alpha - \beta$ の一番右の 0 でない成分が負

このように定義される項順序を**逆辞書式順序**と呼ぶ.

(3) $\alpha > \beta \overset{def}{\iff}$
- $\displaystyle\sum_{i=1}^{n} \alpha_i > \sum_{i=1}^{n} \beta_i$, または
- $\displaystyle\sum_{i=1}^{n} \alpha_i = \sum_{i=1}^{n} \beta_i$ かつ $\alpha - \beta$ の一番右の 0 でない成分が負

このように定義される項順序を**次数付き逆辞書式順序**と呼ぶ.

問題 3.2 以下の多項式を降べきの順に並べ替え，多重次数と先頭項をそれぞれ求めよ.

(1) $f = 7xy^2z + 4xz^2y - 5y^4 + 4x^3$
(2) $f = x^2yz^2 - 3x^3z + 2x^2y^2z + y^2z^3 - 3$

問題 3.3 (1) $f = x^3 - x^2y - x^2 - 1$ を $f_1 = x^2 - z$, $f_2 = xy - 1$ で割り算したときの商と余りを求めよ.
(2) $f = xy^2z^2 + xy - yz$ を $f_1 = x - y^2$, $f_2 = y - z^3$, $f_3 = z^2 - 1$ で割り算したときの商と余りを求めよ.

4　グレブナー基底

4.1　グレブナー基底の定義と性質

前節の最後の注意で述べたように多変数の場合は余りが一通りに決まらない．余りが一通りに決まるような多項式の集まりとして，グレブナー基底という概念が導入される．

定義 4.1 (グレブナー基底)　I を $\mathbb{R}[x_1, x_2, \ldots, x_n]$ の $\{0\}$ でないイデアルとする．このとき，0 でない I の元の集合 $G = \{g_1, g_2, \ldots, g_t\}$ が**グレブナー基底**であるとは，

$$\langle \mathsf{LT}(I) \rangle = \langle \mathsf{LT}(G) \rangle$$

が成り立つときに言う．ここで，

$$\mathsf{LT}(I) = \{\mathsf{LT}(f) \mid 0 \neq f \in I\}$$
$$\mathsf{LT}(G) = \{\mathsf{LT}(g_1), \mathsf{LT}(g_2), \ldots, \mathsf{LT}(g_t)\}$$

と置いている．

つまり，G がグレブナー基底であるとは，

> I の全ての 0 でない元 f に対して f の先頭項 $\mathsf{LT}(f)$ が $\mathsf{LT}(g_1), \mathsf{LT}(g_2), \ldots, \mathsf{LT}(g_t)$ のいずれかで割り切れる

を満たすときに言う．

コメント　グレブナー基底の概念は 1960 年代にブッフバーガーと広中平祐により独立に発見された．グレブナーという名前はブッフバーガーの指導教官の名前から取られている．

命題 4.2　I を $\mathbb{R}[x_1, x_2, \ldots, x_n]$ の $\{0\}$ でないイデアルとする．このとき，

(1) I のグレブナー基底は存在する．
(2) I のグレブナー基底は I の基底である．

証明. (1) ヒルベルトの基底定理(定理 2.9)によりイデアル $\langle \mathsf{LT}(I) \rangle$ には基底 $\mathsf{LT}(g_1), \mathsf{LT}(g_2), \ldots, \mathsf{LT}(g_t)$ $(g_1, g_2, \ldots, g_t \in I)$ が存在する．つまり，

$$\langle \mathsf{LT}(I) \rangle = \langle \mathsf{LT}(g_1), \mathsf{LT}(g_2), \ldots, \mathsf{LT}(g_t) \rangle$$

が成り立つので $\{g_1, g_2, \ldots, g_t\}$ は I のグレブナー基底となる．

(2) 主張だけ見ると自明な事しか言っていないように見えるが，以下が示すべきことである：

I の 0 でない元 $g_1, g_2, \ldots, g_t$ が

$$\langle \mathsf{LT}(I) \rangle = \langle \mathsf{LT}(g_1), \mathsf{LT}(g_2), \ldots, \mathsf{LT}(g_t) \rangle$$

を満たすときに $I = \langle g_1, g_2, \ldots, g_t \rangle$ が成り立つ

$g_1, g_2, \ldots, g_t$ は I の元なので $\langle g_1, g_2, \ldots, g_t \rangle \subseteq I$ が成り立つ．従って，逆の包含 $I \subseteq \langle g_1, g_2, \ldots, g_t \rangle$ を示せば良い．f を I の元とし，$f \in \langle g_1, g_2, \ldots, g_t \rangle$ を示す．

f を $g_1, g_2, \ldots, g_t$ で割り算する：

$$f = q_1 g_1 + q_2 g_2 + \cdots + q_t g_t + r$$

$r = 0$ ならば $f = q_1 g_1 + q_2 g_2 + \cdots + q_t g_t \in \langle g_1, g_2, \ldots, g_t \rangle$ となるので OK．$r \neq 0$ と仮定して矛盾を導く．$f, g_1, g_2, \ldots, g_t$ は I の元なので，命題 2.8 よりこれらの多項式線形結合 $r = f - q_1 g_1 - q_2 g_2 - \cdots - q_t g_t$ は I の元となる．よって，

$$\mathsf{LT}(r) \in \langle \mathsf{LT}(I) \rangle = \langle \mathsf{LT}(g_1), \mathsf{LT}(g_2), \ldots, \mathsf{LT}(g_t) \rangle$$

となり，命題 2.12 より $\mathsf{LT}(r)$ は $\mathsf{LT}(g_1), \mathsf{LT}(g_2), \ldots, \mathsf{LT}(g_t)$ のいずれかで割り切れることになる．しかし，余りの定義から r のどの項も $\mathsf{LT}(g_1), \mathsf{LT}(g_2), \ldots, \mathsf{LT}(g_t)$ で割り切れないので，これは矛盾を導く．従って，$r = 0$ となり証明完了． ■

このグレブナー基底の定義は直感的には分かりにくいが，以下がグレブナー基底の重要な性質である．

命題 4.3 I を $\mathbb{R}[x_1, x_2, \ldots, x_n]$ の $\{0\}$ でないイデアル，$G = \{g_1, g_2, \ldots, g_t\}$ を I のグレブナー基底とする．このとき，I の各元 f に対して以下の 2 条件を満たす多項式 r が唯一つ存在する：

- ある多項式 $q_1, q_2, \ldots, q_t$ を用いて

  $$f = q_1 g_1 + q_2 g_2 + \cdots + q_t g_t + r$$

  と表せる．
- r は 0 であるか，または 0 でなく r のどの項も $\mathsf{LT}(g_1), \mathsf{LT}(g_2), \ldots, \mathsf{LT}(g_t)$ のいずれでも割り切れない

つまり，f を $g_1, g_2, \ldots, g_t$ で割った余りが一通りに決まる．

証明. I の元 f の余りが一通りでない，つまり，

$$f = q_1 g_1 + q_2 g_2 + \cdots + q_t g_t + r = q'_1 g_1 + q'_2 g'_2 + \cdots + q'_t g_t + r'$$

かつ $r \neq r'$ と表されたとする．このとき，移項して整理すると，

$$r - r' = (q'_1 - q_1) f_1 + (q'_2 - q_2) f_1 + \cdots + (q'_t - q_t) f_t$$

が成り立つ．$g_1, g_2, \ldots, g_t$ は I の元なので，命題 2.8 より右辺の多項式は I の元である．従って，$r - r' \in I$ となる．このことから

$$\mathsf{LT}(r - r') \in \mathsf{LT}(I) = \langle \mathsf{LT}(g_1), \mathsf{LT}(g_2), \ldots, \mathsf{LT}(g_t) \rangle$$

が成り立つので，命題 2.12 より $\mathsf{LT}(r - r')$ は $\mathsf{LT}(g_1), \mathsf{LT}(g_2), \ldots, \mathsf{LT}(g_t)$ のいずれかで割り切れる．$\mathsf{LT}(r - r')$ は r または r' の項の実数倍なので，r または r' のある項が $\mathsf{LT}(g_1), \mathsf{LT}(g_2), \ldots, \mathsf{LT}(g_t)$ のいずれかで割り切れることになる．これは余りの性質に矛盾するので，$r = r'$ つまり余りが一通りであることが示された． ■

例 4.4 $\{\underset{g_1}{x + y^3 - y}, \underset{g_2}{y^4 - y^2 + 1}\}$ は $\mathbb{R}[x, y]$ のイデアル $I = \langle x^2 + y^2 - 1, xy - 1 \rangle$ のグレブナー基底である（これは次章で確かめる）．実際に多項式を g_1, g_2 で割った余りが 1 通りに決まるかどうかいくつか計算してみる．

$f = xy^4 - xy^2 + y$ を g_1, g_2 で割り算する．

- $f = -g_1 + xg_2 + y^3$

$$\begin{array}{rrrrrrr}
 & q_1: & -1 & & & & \\
 & q_2: & x & & & & \\
\hline
\begin{matrix} x + y^3 - y \\ y^4 - y^2 + 1 \end{matrix} \Big) & xy^4 & -xy^2 & +y & & & \\
 & xy^4 & -xy^2 & +x & & & \\
\hline
 & & & -x & +y & & \\
 & & & -x & -y^3 & +y & \\
\hline
 & & & & y^3 & &
\end{array}$$

- $f = (y^4 - y^2)g_1 + (-y^3 + y)g_2 + y^3$

$$\begin{array}{rrrrrrrrr}
 & q_1: & y^4 & -y^2 & & & & & \\
 & q_2: & -y^3 & +y & & & & & \\
\hline
\begin{matrix} x + y^3 - y \\ y^4 - y^2 + 1 \end{matrix} \Big) & xy^4 & -xy^2 & +y & & & & & \\
 & xy^4 & +y^7 & -y^5 & & & & & \\
\hline
 & & -xy^2 & -y^7 & +y^5 & +y & & & \\
 & & -xy^2 & -y^5 & +y^3 & & & & \\
\hline
 & & & -y^7 & +2y^5 & -y^3 & +y & & \\
 & & & -y^7 & +y^5 & -y^3 & & & \\
\hline
 & & & & y^5 & +y & & & \\
 & & & & y^5 & -y^3 & +y & & \\
\hline
 & & & & & -y^3 & & &
\end{array}$$

いずれの場合も余りは y^3 となる．

4.2　極小グレブナー基底と被約グレブナー基底

$\{g_1, g_2, \ldots, g_t\}$ がグレブナー基底のとき，定義から $\{g_1, g_2, \ldots, g_t\}$ に I の別の元を加えたものも I のグレブナー基底となることが分かる．従って，グレブナー基底には無駄な多項式が含まれている可能性がある．そこで，無駄なものを省いたものとして以下の概念が定義される．

> **定義 4.5**　グレブナー基底 $G = \{g_1, g_2, \ldots, g_t\}$ が以下の条件を満たすとき，極小グレブナー基底と呼ぶ：
>
> (1) 全ての G の元 g_i の先頭項の係数は 1 である．
> (2) 全ての G の元 g_i の先頭項は他のどの g_j $(j \neq i)$ の先頭項でも割り切れない．

グレブナー基底 $G = \{g_1, g_2, \ldots, g_t\}$ が与えられたとき，極小グレブナー基底は以下のように求めることができる：

まず $g_1, g_2, \ldots, g_t$ を先頭項の係数で割ることで (1) を満たすようにする．次に，ある g_i の先頭項が別の $\mathsf{LT}(g_j)$ $(j \neq i)$ の先頭項で割り切れるならば g_i を取り除く．このとき，次の命題より g_i を取り除いても I のグレブナー基底である．これを繰り返していくと最終的に I の極小グレブナー基底を得る．

> **命題 4.6**　$G = \{g_1, g_2, \ldots, g_t\}$ がイデアル I のグレブナー基底のとする．もし g_i の先頭項がある $\mathsf{LT}(g_j)$ $(j \neq i)$ で割り切れるとき，$G - \{g_i\} = \{g_1, \ldots, g_{i-1}, g_{i+1}, \ldots, g_t\}$ も I のグレブナー基底である．

証明．$i = 1$ として示す．つまり，$\mathsf{LT}(g_1)$ がある $\mathsf{LT}(g_j)$ $(j \neq 1)$ で割り切れると仮定して $\langle \mathsf{LT}(I) \rangle = \langle g_2, g_3, \ldots, g_t \rangle$ を示す．

G が I のグレブナー基底なので $\langle \mathsf{LT}(I) \rangle = \langle g_1, g_2, \ldots, g_t \rangle$ が成り立ち，$\langle g_2, g_3, \ldots, g_t \rangle \subseteq \langle \mathsf{LT}(I) \rangle$ である．従って，逆の包含 $\langle \mathsf{LT}(I) \rangle \subseteq \langle g_2, g_3, \ldots, g_t \rangle$ を示せばよい．I の元 f に対して，$\mathsf{LT}(f) \in \langle \mathsf{LT}(I) \rangle = \langle g_1, g_2, \ldots, g_t \rangle$ なので命題 2.12 より $\mathsf{LT}(f)$ はある $\mathsf{LT}(g_i)$ で割り切れる．

- $i = 2, 3, \ldots, n$ のとき $\mathsf{LT}(f) \in \langle g_2, g_3, \ldots, g_t \rangle$ となる．
- $i = 1$ とする．$\mathsf{LT}(f)$ は $\mathsf{LT}(g_1)$ で割り切れ，$\mathsf{LT}(g_1)$ は $\mathsf{LT}(g_j)$ で割り切れるので，$\mathsf{LT}(f)$ は $\mathsf{LT}(g_j)$ で割り切れる．従って，$\mathsf{LT}(f) \in \langle g_2, g_3, \ldots, g_t \rangle$ となる．

以上より，$\langle \mathsf{LT}(I) \rangle \subseteq \langle g_2, g_3, \ldots, g_t \rangle$ が示された．■

こうして得られた極小グレブナー基底は無駄のないものとなっているが，一通りに決まらない．例えば，例 4.4 で考えたイデアル $I = \langle x^2 + y^2 - 1, xy - 1 \rangle$ に対して，

$$\{x + y^3 - y,\ y^4 - y^2 + 1\} \quad \{x + y^5,\ y^4 - y^2 + 1\}$$

はいずれも I のグレブナー基底となる（これらの元の先頭項が等しいので）．極小グレブナー基底か

らさらに余分な項を省いたものとして以下の概念が定義される．

定義 4.7 グレブナー基底が $G = \{g_1, g_2, \ldots, g_t\}$ が以下の条件を満たすとき，**被約グレブナー基底**と呼ぶ：

(1) 全ての G の元 g_i の先頭項の係数は 1 である．
(2) 全ての G の元 g_i の項は他のどの g_j $(j \neq i)$ の先頭項でも割り切れない．

被約グレブナー基底は一通りに決まる．

定理 4.8 任意の $\mathbb{R}[x_1, x_2, \ldots, x_n]$ の $\{0\}$ でないイデアルは被約グレブナー基底を持ち，さらに被約グレブナー基底は一通りに決まる．

証明. $\{g_1, g_2, \ldots, g_t\}$ を I の極小グレブナー基底とする．このとき以下のようにして被約グレブナー基底を求めることができる．

- g_1 を $g_2, g_3, \ldots, g_t$ で割った余りを g_1' とする：

  $$g_1 = q_2 g_2 + q_3 g_3 + \cdots q_t g_t + g_1'$$

  このとき，余りの定義から $\mathsf{LT}(g_1')$ はどの $\mathsf{LT}(g_2), \mathsf{LT}(g_3), \ldots, \mathsf{LT}(g_t)$ で割り切れない．また，$\mathsf{LT}(g_1)$ は $\mathsf{LT}(q_2 g_2)$, $\mathsf{LT}(q_3 g_3)$, …, $\mathsf{LT}(q_t g_t)$, $\mathsf{LT}(g_1')$ のいずれかと一致するが，G の極小性から $\mathsf{LT}(g_1) = \mathsf{LT}(g_1')$ となる．
  従って，

  $$\langle \mathsf{LT}(I) \rangle = \langle \mathsf{LT}(g_1), \mathsf{LT}(g_2), \ldots, \mathsf{LT}(g_t) \rangle = \langle \mathsf{LT}(g_1'), \mathsf{LT}(g_2), \ldots, \mathsf{LT}(g_t) \rangle$$

  となるので $G' = \{g_1', g_2, \ldots, g_t\}$ も I のグレブナー基底となる．

- g_2 を $g_1', g_3, \ldots, g_t$ で割った余りを g_2' とする：

  $$g_2 = q_1 g_1' + q_3 g_3 + \cdots + q_t g_t + g_2'$$

  このとき，上と同様に $G'' = \{g_1', g_2', g_3, \ldots, g_t\}$ はグレブナー基底であり，$\mathsf{LT}(g_2')$ は $\mathsf{LT}(g_1')$, $\mathsf{LT}(g_3)$, …, $\mathsf{LT}(g_t)$ で割り切れない．

- 以下同様の操作を $g_3, g_4, \ldots, g_t$ に対して行っていけば被約グレブナー基底を得る．

次に，極小グレブナー基底が一通りであることを示す．G と G' が I のグレブナー基底であるとする．$G \neq G'$ であると仮定すると $g \in G$ と $g' \in G'$ で $g \neq g'$ かつ $\mathsf{LT}(g) = \mathsf{LT}(g')$ となるようなものが存在する．このとき，$\mathsf{LT}(g - g')$ は g または g' の先頭項以外の項である．$\mathsf{LT}(g - g')$ は g の先頭項以外の項であるとしても良い．すると，

$$\langle \mathsf{LT}(g - g') \rangle \in \langle \mathsf{LT}(I) \rangle = \langle \mathsf{LT}(G) \rangle$$

となるので命題 2.12 より $\mathsf{LT}(g - g')$ は $\mathsf{LT}(G)$ のいずれかの元で割り切れる．これは G が極小グレブナー基底であることに矛盾する．従って，$G = G'$ が成り立つ． ■

例 4.9 $I = \langle xz - y, x^2 + yz, y^2 + z \rangle$ はグレブナー基底

$$G = \{\underset{g_1}{x^2z - z^5}, \underset{g_2}{x^2 - xz + z^8 - z^4}, \underset{g_3}{xz - y}, \underset{g_4}{xz + z^3}, \underset{g_5}{y - z^8}, \underset{g_6}{z^6 + z}\}$$

を持つ．このとき I の被約グレブナー基底を求める．

$\mathsf{LT}(g_1) = x^2z$, $\mathsf{LT}(g_3) = xz$ は $\mathsf{LT}(g_4) = xz$ で割り切れるので g_1, g_3 を取り除くと

$$G' = \{g_2, g_4, g_5, g_6\}$$

は極小グレブナー基底となる．

ここで，定理 4.8 の証明より，以下のようにして被約グレブナー基底を求めることができる．

- g_2 を g_4, g_5, g_6 で割り算すると余りは $g_2' = x^2 - z^4$ となる：

$$g_2 = (-1)g_4 + 0 \cdot g_5 + z^2 g_6 + (x^2 - z^4)$$

- g_4 を g_2', g_5, g_6 で割り算すると余りは $g_4' = xz + z^3$ となる：

$$g_4 = 0 \cdot g_2' + 0 \cdot g_5 + 0 \cdot g_6 + (xz + z^3)$$

- g_5 を g_2', g_4', g_6 で割り算すると余りは $g_5' = y + z^3$ となる：

$$g_5 = 0 \cdot g_2' + 0 \cdot g_4' + z^2 g_6 + (y + z^3)$$

- g_6 を g_2', g_4', g_5' で割り算すると余りは $g_6' = z^6 + z$ となる：

$$g_6 = 0 \cdot g_2' + 0 \cdot g_4' + 0 \cdot g_5' + (z^6 + z)$$

(g_4, g_6 には $\mathsf{LT}(g_2) = x^2$, $\mathsf{LT}(g_4) = xz$, $\mathsf{LT}(g_5) = y$, $\mathsf{LT}(g_6) = z^6$ で割り切れる項が無いのでこれらは割り算しなくても良い)．

従って，I の被約グレブナー基底は

$$\{x^2 - z^4, xz + z^3, y + z^3, z^6 + z\}$$

となる．

命題 4.2 ではヒルベルトの基底定理を用いてグレブナー基底が存在することを示した．従って，ヒルベルトの基底定理の後の注意で述べたように，I の基底が具体的に与えられていてもどのようなグレブナー基底 $\{g_1, g_2, \ldots, g_t\}$ が取れるかは全く分からない．また，多項式の集合 $\{g_1, g_2, \ldots, g_t\}$ がグレブナー基底であることを確かめようと思ったとき，I の全ての 0 でない元 f に対して，その先頭項 $\mathsf{LT}(f)$ が $\mathsf{LT}(g_1), \mathsf{LT}(g_2), \ldots, \mathsf{LT}(g_t)$ のいずれかで割り切れることを確かめなければならない．しかし，I には無限個の元が含まれるので，それらすべてに対して確かめるのは不可能である．

次節ではグレブナー基底であるかどうかを有限回の計算で確かめることができるブッフバーガーの判定法とそれを用いたグレブナー基底を求めるアルゴリズムを紹介する．

演習問題

問題 4.1 (1) $f_1 = 2xy^2 + 3x + 4y^2$, $f_2 = y^2 - 2y - 2$ とし，$I = \langle f_1, f_2 \rangle$ と置く．このとき，$\mathsf{LT}(f) \notin \langle \mathsf{LT}(f_1), \mathsf{LT}(f_2) \rangle$ となる $f \in I$（つまり，$\mathsf{LT}(f)$ が $\mathsf{LT}(f_1), \mathsf{LT}(f_2)$ のいずれでも割り切れないような $f \in I$）を一つ見つけよ．

(2) $f_1 = x^2 + y^2 + z^2 - 4$, $f_2 = x^2 - 2y^2 - 5$, $f_3 = xz - 1$ とし，$I = \langle f_1, f_2, f_3 \rangle$ と置く．このとき，$\mathsf{LT}(f) \notin \langle \mathsf{LT}(f_1), \mathsf{LT}(f_2), \mathsf{LT}(f_3) \rangle$ となる $f \in I$（つまり，$\mathsf{LT}(f)$ が $\mathsf{LT}(f_1), \mathsf{LT}(f_2), \mathsf{LT}(f_3)$ のいずれでも割り切れないような $f \in I$）を一つ見つけよ．

問題 4.2 (1) $I = \langle x^2 + y^2 - 1, x^3 + y^3 - 1 \rangle$ はグレブナー基底

$$\{x^2+y^2-1,\ x^3+y^3-1,\ xy^2-x-y^3+1,\ xy-x+2y^4-2y^2-y+1,\ -2y^5-2y^4+y^3+3y^2\}$$

を持つ．このとき，I の被約グレブナー基底を求めよ．

(2) $I = \langle x^2 - y^3, xy - z^2 \rangle$ はグレブナー基底

$$\{x^2z^2-y^3z^2,\ x^2+xyz^2-y^3-z^4,\ xyz^2-z^4,\ xy-xz^2+y^4-z^2,\ xz^2-y^5-y^4+z^4,\ y^5-z^4\}$$

を持つ．このとき，I の被約グレブナー基底を求めよ．

5　ブッフバーガーのアルゴリズム

命題 4.3 より，グレブナー基底であるためには余りが一通りに決まらなければならない．そこで，どのようなときに異なる余りが現れるか具体例で見ていく．

$f = x^4 + x^2y - x^2$ を $f_1 = x^3 - 2xy$, $f_2 = x^2y + x - 2y^2$ に対して，

$$f = xf_1 + f_2 + (-x^2 - x + 2y^2) \qquad (*)$$

が成り立つので，f を f_1, f_2 で割った余りは $-x^2 - x + 2y^2$ である．しかし，f_1 と f_2 の間の関係式

$$yf_1 - xf_2 = y(x^3 - 2xy) - x(x^2y + x - 2y^2) = -x^2$$

を用いると

$$f = xf_1+f_2+(-x^2-x+2y^2) = xf_1+f_2+(yf_1 - xf_2)+(-x+2y^2) = (x+y)f_1+(-x+1)f_2+(-x+2y^2)$$

となり，$-x + 2y^2$ も f を f_1, f_2 で割った余りである事がわかる．

この例から，$yf_1 - xf_2 = -x^2$ のように f_1, f_2 の先頭項が打ち消しあうことで低次の項が現れるときに異なる余りがでてくる．そこで，このように先頭項が打ち消し合った多項式として以下の概念を導入する．

定義 5.1　$f, g \in \mathbb{R}[x_1, x_2, \ldots, x_n]$ を 0 でない多項式とし，これらの先頭項をそれぞれ ax^α, bx^β とする．$\gamma := (\max\{\alpha_1, \beta_1\}, \max\{\alpha_2, \beta_2\}, \ldots, \max\{\alpha_n, \beta_n\})$ と置いたとき，f と g の S-多項式 $S(f, g)$ を以下のように定義する：

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

注意　(1) x^γ は $\mathsf{LT}(f)$ および $\mathsf{LT}(g)$ を割り切っている．従って，$\dfrac{x^\gamma}{\mathsf{LT}(f)}$, $\dfrac{x^\gamma}{\mathsf{LT}(g)}$ の部分は多項式となっており，$S(f, g)$ は多項式になっている．

(2) S 多項式 $S(f, g)$ は f と g の先頭項が打ち消し合うような多項式である．

(3) 命題 2.8 より，f, g がイデアル I の元ならば $S(f, g)$ も I の元となる．

例 5.2　(1) $f = x^3 - 2xy$, $g = x^2y + x - 2y^2$ とする．$\mathsf{LT}(f) = x^3$, $\mathsf{LT}(g) = x^2y$ なので，$\gamma = (3, 1)$ であり，f と g の S-多項式は

$$S(f, g) = \frac{x^3y}{x^3} \cdot f - \frac{x^3y}{x^2y} \cdot g = y(x^3 - 2xy) - x(x^2y + x - 2y^2) = -x^2$$

(2) $f = x^3y^2 - x^2y^3 + x$, $g = 3x^4y + y^2$ とする．$\mathsf{LT}(f) = x^3y^2$, $\mathsf{LT}(g) = 3x^4y$ なので，

$\gamma = (4,2)$ であり，f と g の S-多項式は

$$S(f,g) = \frac{x^4y^2}{x^3y^2}\cdot f - \frac{x^4y^2}{3x^4y}\cdot g = x(x^3y^2 - x^2y^3 + x) - \frac{1}{3}y(3x^4y + y^2)$$
$$= -x^3y^3 + x^2 - \frac{1}{3}y^3$$

以下の定理により，与えられた多項式の集合がグレブナー基底であるかどうか有限回の計算で判定することが可能になる．

定理 5.3 （ブッフバーガーの判定法） I を $\mathbb{R}[x_1, x_2, \ldots, x_n]$ のイデアル，$g_1, g_2, \ldots, g_t$ を 0 でない I の元とする．このとき

$\{g_1, g_2, \ldots, g_t\}$ が I のグレブナー基底 $\Longleftrightarrow$ 各 $i < j$ に対して $S(g_i, g_j)$ を $g_1, g_2, \ldots, g_t$ で割った余りが 0

証明. この定理の証明はかなり面倒なので省略する．詳細は [1, 第 2 章 §6 定理 6] を見よ． ■

以下の命題を用いるとグレブナー基底の判定が多少楽になる．

命題 5.4 $f, g \in \mathbb{R}[x_1, x_2, \ldots, x_n]$ を 0 でない多項式とする．もし $\mathsf{LT}(f)$ と $\mathsf{LT}(g)$ が互いに素ならば $S(f,g)$ を f, g で割った余りは 0 になる．

証明. 簡単のため，f と g の先頭項の係数は 1 であるとする．このとき，$\mathsf{LT}(f)$ と $\mathsf{LT}(g)$ が互いに素なので $x^\gamma = \mathsf{LT}(f)\mathsf{LT}(g)$ である．また，f と g を先頭項と低次の項に分けて $f = \mathsf{LT}(f) + p$, $g = \mathsf{LT}(g) + q$ と表す．このとき，

$$\begin{aligned} S(f,g) &= \frac{\mathsf{LT}(f)\mathsf{LT}(g)}{\mathsf{LT}(f)}\cdot f - \frac{\mathsf{LT}(f)\mathsf{LT}(g)}{\mathsf{LT}(g)}\cdot g \\ &= \mathsf{LT}(g)f - \mathsf{LT}(f)g \\ &= (g-q)f - (f-p)g \\ &= (-q)f + pg \end{aligned}$$

となる．従って，$\mathsf{mdeg}((-q)f), \mathsf{mdeg}(pg) \leq \mathsf{mdeg}\, S(f,g)$ であることを示せば $S(f,g)$ を f, g で割った余りが 0 となる．

これが成り立たないと仮定すると，$(-q)f$ と pg の先頭項が打ち消し合う．つまり，$\mathsf{LT}(q)\mathsf{LT}(f) = \mathsf{LT}(qf) = \mathsf{LT}(pg) = \mathsf{LT}(p)\mathsf{LT}(g)$ となるが，これは $\mathsf{LT}(f)$ と $\mathsf{LT}(g)$ が互いに素であることに矛盾する． ■

例 5.5 (1) $g_1 = x + y^3 - y$, $g_2 = y^4 - y^2 + 1$ を考える．このとき，$\mathsf{LT}(g_1) = x$ と $\mathsf{LT}(g_2) = y^4$ は互いに素なので，命題 5.4 より $S(g_1, g_2)$ を g_1, g_2 で割った余りは 0 である．実際，g_1 と

g_2 の S 多項式は

$$S(g_1,g_2)=\frac{xy^4}{\mathsf{LT}(g_1)}\cdot g_1-\frac{xy^4}{\mathsf{LT}(g_2)}\cdot g_2=y^4(x+y^3-y)-x(y^4-y^2+1)$$
$$=xy^2-x+y^7-y^5$$

となり，

$$S(g_1,g_2)=(y^2-1)g_1+(y^3-y)g_2$$

従って，ブッフバーガーの判定法より $\{g_1,g_2\}$ はグレブナー基底である．

(2) $g_1=xy+x-z$, $g_2=xz+y-1$, $g_3=y^2+z^2-1$ を考える．

- g_1 と g_2 の S 多項式は

$$S(g_1,g_2)=\frac{xyz}{\mathsf{LT}(g_1)}\cdot g_1-\frac{xyz}{\mathsf{LT}(g_2)}\cdot g_2=z(xy+x-z)-y(xz+y-1)$$
$$=xz-y^2+y-z^2$$

となり，$S(g_1,g_2)$ を g_1,g_2,g_3 で割った余りは 0：

$$S(g_1,g_2)=0\cdot g_1+1\cdot g_2+(-1)\cdot g_3$$

- $\mathsf{LT}(g_2)=xz$ と $\mathsf{LT}(g_3)=y^2$ は互いに素なので，命題 5.4 より $S(g_2,g_3)$ を g_1, g_2, g_3 で割った余りは 0 である．実際，g_2 と g_3 の S 多項式は

$$S(g_2,g_3)=\frac{xy^2z}{\mathsf{LT}(g_2)}\cdot g_2-\frac{xy^2z}{\mathsf{LT}(g_3)}\cdot g_3=y^2(xz+y-1)-xz(y^2+z^2-1)$$
$$=-xz^3+xz+y^3-y^2$$

となり，$S(g_2,g_3)$ を g_1, g_2, g_3 で割った余りは 0 である：

$$S(g_2,g_3)=0\cdot g_1+(-z^2+1)\cdot g_2+(y-1)\cdot g_3$$

- g_1 と g_3 の S 多項式は

$$S(g_1,g_3)=\frac{xy^2}{\mathsf{LT}(g_1)}\cdot g_1-\frac{xy^2}{\mathsf{LT}(g_3)}\cdot g_3=y(xy+x-z)-x(y^2+z^2-1)$$
$$=xy-xz^2+x-yz$$

となり，$S(g_1,g_3)$ を g_1,g_2,g_3 で割った余りは 0：

$$S(g_1,g_3)=1\cdot g_1+(-z)\cdot g_2+0\cdot g_3$$

従って，ブッフバーガーの判定法より $\{g_1,g_2,g_3\}$ はグレブナー基底となる．

ブッフバーガーの判定法より，イデアル $I=\langle f_1,f_2,\ldots,f_m\rangle$ に対して，S 多項式 $S(f_i,f_j)$ を $F=\{f_1,f_2,\ldots,f_m\}$ で割った余りを計算し，それが 0 でなければ F に付け加えていく操作を繰り返していけば I のグレブナー基底が求まる．ここでグレブナー基底の定義を思い出すと，付け加え

るべき多項式は先頭項が F の元の先頭項のいずれでも割り切れないようなものであることが分かる．従って，以下のようなアルゴリズムでグレブナー基底を求めることができる．

ブッフバーガーのアルゴリズム．

$\mathbb{R}[x_1, x_2, \ldots, x_n]$ の $\{0\}$ でないイデアル $I = \langle f_1, f_2, \ldots, f_m \rangle$ を考える．このとき，以下のようにして I のグレブナー基底を求めることができる．

$F = \{f_1, f_2, \ldots, f_m\}$ からスタートして以下のループを繰り返す．

(i) F がグレブナー基底ならば終了．

そうでないならば (ii) に進む．

(ii) F の異なる元 f, f' に対してその S 多項式 $S(f, f')$ を F で割った余り r を計算する．

- r が 0 でないならば F を

$$F \cup \{r\}$$

に置き換えて (i) に戻る．

- r が 0 ならばそのまま (i) に戻る．

注意　グレブナー基底の計算量は一般に大きくなるが，以下の点に気をつけると多少計算量を節約できる：

(1) あるループにおいて，$S(f, f')$ を F で割った余り r を計算したとき，それ以降のループでは r を F で割った余りは 0 になるので $S(f, f')$ の余りを改めて計算する必要は無い．

(2) $\mathsf{LT}(f)$ と $\mathsf{LT}(g)$ が互いに素ならば，$S(f, g)$ を f, g で割った余りは 0 になる（命題 5.4 より）ので，この場合は S 多項式 $S(f, g)$ およびそれを F で割った余り F を計算する必要は無い．

例 5.6　(1) $\mathbb{R}[x, y]$ のイデアル $I = \langle x^2 + y^2 - 1, xy - 1 \rangle$ のグレブナー基底をブッフバーガーのアルゴリズムを用いて求める．

$F = \{\underbrace{x^2 + y^2 - 1}_{f_1}, \underbrace{xy - 1}_{f_2}\}$ からスタートする．

- f_1 と f_2 の S 多項式は

$$S(f_1, f_2) = \frac{x^2 y}{\mathsf{LT}(f_1)} \cdot f_1 - \frac{x^2 y}{\mathsf{LT}(f_2)} \cdot f_2 = y(x^2 + y^2 - 1) - x(xy - 1) = x + y^3 - y$$

となり，$S(f_1, f_2)$ を f_1, f_2 で割った余りは $x + y^3 - y$ である：

$$S(f_1, f_2) = 0 \cdot f_1 + 0 \cdot f_2 + (x + y^3 - y)$$

余り $f_3 = x + y^3 - y$ は 0 でないので，F に f_3 を加えて $F = \{f_1, f_2, f_3\}$ とする．

- f_2 と f_3 の S 多項式は

$$S(f_2, f_3) = \frac{xy}{\mathsf{LT}(f_2)} \cdot f_2 - \frac{xy}{\mathsf{LT}(f_3)} \cdot f_3 = (xy - 1) - y(x + y^3 - y) = -y^4 + y^2 - 1$$

となり，$S(f_2, f_3)$ を f_1, f_2, f_3 で割った余りは $-y^4 + y^2 - 1$ である：

$$S(f_2, f_3) = 0 \cdot f_1 + 0 \cdot f_2 + 0 \cdot f_3 + (-y^4 + y^2 - 1)$$

余り $f_4 = -y^4 + y^2 - 1$ は 0 でないので F に f_4 を加えて $F = \{f_1, f_2, f_3, f_4\}$ を考える．

- このとき，
  - $S(f_1, f_3) = -xy^3 + xy + y^2 - 1$ を f_1, f_2, f_3, f_4 で割った余りは 0 である：

    $$S(f_1, f_3) = 0 \cdot f_1 + (-y^2 + 1)f_2 + 0 \cdot f_3 + 0 \cdot f_4$$

  - $\mathsf{LT}(f_1) = x^2$ と $\mathsf{LT}(f_4) = -y^4$ は互いに素なので $S(f_1, f_4)$ を f_1, f_2, f_3, f_4 で割った余りは 0.
  - $S(f_2, f_4) = xy^2 - x - y^3$ を f_1, f_2, f_3, f_4 で割った余りは 0 である：

    $$xy^2 - x - y^3 = 0 \cdot f_1 + yf_2 + (-1)f_3 + 0 \cdot f_4$$

  - $\mathsf{LT}(f_3) = x$ と $\mathsf{LT}(f_4) = -y^4$ は互いに素なので $S(f_3, f_4)$ を f_1, f_2, f_3, f_4 で割った余りは 0.

従って，ブッフバーガーの判定法より $\{f_1, f_2, f_3, f_4\}$ は I のグレブナー基底である．

また，$\mathsf{LT}(f_1) = x^2$, $\mathsf{LT}(f_2) = xy$ は $\mathsf{LT}(f_3) = x$ で割り切れるので，f_1, f_2 を取り除き，適当な実数倍することで I の極小グレブナー基底 $\{x + y^3 - y,\ y^4 - y^2 + 1\}$ を得る．さらに，これは被約グレブナー基底となっている．

(2) $\mathbb{R}[x, y, z]$ のイデアル $I = \langle x^2 - y, x^3 - z \rangle$ のグレブナー基底をブッフバーガーのアルゴリズムを用いて求める．

$F = \{\underset{f_1}{x^2 - y}, \underset{f_2}{x^3 - z}\}$ からスタートする．

- $S(f_1, f_2) = -xy + z$ を f_1, f_2 で割った余りは $-xy + z$ である：

  $$S(f_1, f_2) = 0 \cdot f_1 + 0 \cdot f_2 + (-xy + z)$$

  余り $f_3 = -xy + z$ は 0 でないので F に f_3 を加えて $F = \{f_1, f_2, f_3\}$ とする．

- $S(f_2, f_3) = x^2 z - yz$ を f_1, f_2, f_3 で割った余りは 0 である：

  $$S(f_2, f_3) = zf_1 + 0 \cdot f_2 + 0 \cdot f_3$$

  よって，F はそのまま．

- $S(f_1, f_3) = xz - y^2$ を f_1, f_2, f_3 で割った余りは $f_4 = xz - y^2$ である：

  $$S(f_1, f_3) = 0 \cdot f_1 + 0 \cdot f_2 + 0 \cdot f_3 + (xz - y^2)$$

  余り $f_4 = xz - y^2$ は 0 でないので F に f_4 を加えて $F = \{f_1, f_2, f_3, f_4\}$ とする．

- $S(f_1, f_4) = xy^2 - yz$ を f_1, f_2, f_3, f_4 で割った余りは 0 である：

  $$S(f_1, f_4) = 0 \cdot f_1 + 0 \cdot f_2 + (-y)f_3 + 0 \cdot f_4$$

  よって，F はそのまま．

- $S(f_2, f_4) = x^2y^2 - z^2$ を f_1, f_2, f_3, f_4 で割った余りは 0 である：

$$S(f_2, f_4) = 0 \cdot f_1 + 0 \cdot f_2 + (-xy - z)f_3 + 0 \cdot f_4$$

よって，F はそのまま．

- $S(f_3, f_4) = y^3 - z^2$ を f_1, f_2, f_3, f_4 で割った余りは $y^3 - z^2$ である：

$$S(f_3, f_4) = 0 \cdot f_1 + 0 \cdot f_2 + 0 \cdot f_3 + 0 \cdot f_4 + (y^3 - z^2)$$

余り $f_5 = y^3 - z^2$ は 0 で割り切れないので F に f_5 を加えて $F = \{f_1, f_2, f_3, f_4, f_5\}$ とする．

- さらに，
  - $\mathsf{LT}(f_1) = x^2$ と $\mathsf{LT}(f_5) = -y^3$ は互いに素なので $S(f_1, f_5)$ を f_1, f_2, f_3, f_4, f_5 で割った余りは 0.
  - $\mathsf{LT}(f_2) = x^3$ と $\mathsf{LT}(f_5) = -y^3$ は互いに素なので $S(f_2, f_5)$ を f_1, f_2, f_3, f_4, f_5 で割った余りは 0.
  - $S(f_3, f_5) = xz^2 - y^2z$ を f_1, f_2, f_3, f_4, f_5 で割った余りは 0 である：

$$S(f_3, f_5) = 0 \cdot f_1 + 0 \cdot f_2 + 0 \cdot f_3 + zf_4 + 0 \cdot f_5$$

  - $\mathsf{LT}(f_4) = xz$ と $\mathsf{LT}(f_5) = -y^3$ は互いに素なので $S(f_4, f_5)$ を f_1, f_2, f_3, f_4, f_5 で割った余りは 0.

ブッフバーガーの判定法より $\{f_1, f_2, f_3, f_4, f_5\}$ は I のグレブナー基底である．

$\mathsf{LT}(f_2) = x^3$ は $\mathsf{LT}(f_1) = x^2$ で割り切れるので f_2 を取り除き，適当な実数をすれば極小グレブナー基底 $\{x^2 - y,\ xy - z,\ xz - y^2,\ y^3 - z^2\}$ を得る．さらに，これは被約グレブナー基底となっている．

演習問題

問題 5.1 以下の多項式 f, g の S 多項式 $S(f, g)$ を計算せよ．

(1) $f = 3x^2y - yz,\ g = xy^2z + z^4$
(2) $f = 3x^2yz - y^3z^3,\ g = xy^2 + z^2$

問題 5.2 以下のイデアルの被約グレブナー基底を求めよ．

(1) $\langle xy - 1, xz - 1 \rangle$
(2) $\langle x + y, x^2 + y^2 \rangle$

(3) $\langle x^2y + z, xz + y\rangle$

(4) $\langle x^2 + y + z - 1, x + y^2 + z - 1, x + y + z^2 - 1\rangle$

6　消去定理

6.1　消去定理

前節まででグレブナー基底を具体的に求める方法が分かった．この節では項順序が辞書式順序の場合，グレブナー基底は変数が順番に消去されている形になっている形であることを見る．以下の話は一般の項順序ではダメで，辞書式順序であることを使う．

定義 6.1　$\mathbb{R}[x_1, x_2, \ldots, x_n]$ のイデアル I と $0 \leq l < n$ に対して，

$$I_l := \{f \in I \mid f \text{ は変数 } x_1, x_2, \ldots, x_l \text{ を含まない多項式 }\}$$

と置く．ただし，$I_0 = I$ と約束する．このとき，I_l は $\mathbb{R}[x_{l+1}, x_{l+2}, \ldots, x_n]$ のイデアルとなることに注意しておく．

定理 6.2 (消去定理)　$G = \{g_1, g_2, \ldots, g_t\}$ を $\mathbb{R}[x_1, x_2, \ldots, x_n]$ の $\{0\}$ でないイデアル I のグレブナー基底とし，$0 \leq l < n$ に対して

$$G_l := \{g_i \mid g_i \text{ は変数 } x_1, x_2, \ldots, x_l \text{ を含まない多項式 }\}$$

と置く．ただし，$G_0 = G$ と約束する．このとき，G_l は $\mathbb{R}[x_{l+1}, x_{l+2}, \ldots, x_n]$ のイデアル I_l のグレブナー基底である．

証明. $\langle \mathsf{LT}(I_l) \rangle = \langle \mathsf{LT}(G_l) \rangle$ を示す．$\langle \mathsf{LT}(I_l) \rangle \supseteq \langle \mathsf{LT}(G_l) \rangle$ は明らかなので逆の包含 $\langle \mathsf{LT}(I_l) \rangle \subseteq \langle \mathsf{LT}(G_l) \rangle$ を示せばよい．

f を I_l の元とする．今，G は I のグレブナー基底だったので $\langle \mathsf{LT}(I) \rangle = \langle \mathsf{LT}(G) \rangle$ が成り立っている．従って，$\mathsf{LT}(f)$ は $\langle \mathsf{LT}(G) \rangle$ の元となる．このことから $\mathsf{LT}(f)$ はいずれかの $\mathsf{LT}(g_i)$ で割り切れることになる．$\mathsf{LT}(f)$ には $x_1, x_2, \ldots, x_l$ が含まれないので $\mathsf{LT}(g_i)$ にも $x_1, x_2, \ldots, x_l$ が含まれない．g_i の全ての項は $\mathsf{LT}(g_i)$ 以下であるので，辞書式順序の定義により $x_1, x_2, \ldots, x_l$ を含まない．よって，$g_i \in G_l$ となり $\mathsf{LT}(f) \in \langle \mathsf{LT}(G_l) \rangle$ が示された．以上より，逆の包含 $\langle \mathsf{LT}(I_l) \rangle \subseteq \langle \mathsf{LT}(G_l) \rangle$ が示された．■

消去定理により，イデアル $I = \langle f_1, f_2, \ldots, f_m \rangle$ のグレブナー基底は $f_1, f_2, \ldots, f_m$ から変数を消去したものになっている．

6.2　連立代数方程式への応用

消去定理によりを用いることで連立代数方程式

$$(*)\begin{cases} f_1 = 0 \\ f_2 = 0 \\ \quad \vdots \\ f_m = 0 \end{cases}$$

を以下のようにして解くことができる：

(i) ブッフバーガーアルゴリズムを用いてイデアル $I = \langle f_1, f_2, \ldots, f_m \rangle$ のグレブナー基底 $G = \{g_1, g_2, \ldots, g_t\}$ を求める．このとき，命題 2.10 により $(*)$ の解と

$$(**)\begin{cases} g_1 = 0 \\ g_2 = 0 \\ \quad \vdots \\ g_t = 0 \end{cases}$$

の解は等しいので，$(**)$ を解けば良い．

(ii) 消去定理により，G の中で G_{n-1} に含まれるものは x_n のみを含む多項式である．そこで，これらの 1 変数多項式の解 a_n を求める．G_{n-1} が空集合の場合は a_n はどの実数でも良い．

(iii) 消去定理により，G の中で $G_{n-2} - G_{n-1}$ に含まれるものは x_{n-1}, x_n のみを含む多項式である．(2) で求めた x_n を代入すると，x_{n-1} のみを含む多項式を得る．そこで，これらの 1 変数多項式の解 a_{n-1} を求める．G_{n-2} が空集合の場合は a_{n-1} はどの実数でも良い．

(iv) 消去定理により，G の中で $G_{n-3} - G_{n-2}$ に含まれるものは x_{n-2}, x_{n-1}, x_n のみを含む多項式である．(ii)(iii) で求めた a_{n-1}, a_n を代入すると，x_{n-2} のみを含む多項式を得る．そこで，これらの 1 変数多項式の解 a_{n-2} を求める．G_{n-3} が空集合の場合は a_{n-2} はどの実数でも良い．

(v) 以下この操作を繰り返していく．

> **注意**　上の方法で解いていくと途中で $0 = d$（d は 0 でない数）という方程式が現れることがある．その場合，「解無し」となる．

> **例 6.3**　(1) 連立代数方程式
>
> $$(*)\begin{cases} x^2 + y + z = 1 \\ x + y^2 + z = 1 \\ x + y + z^2 = 1 \end{cases}$$
>
> を解く．
>
> $f_1 = x^2 + y + z - 1$, $f_2 = x + y^2 + z - 1$, $f_3 = x + y + z^2 - 1$ と置いて $I = \langle f_1, f_2, f_3 \rangle$ の

グレブナー基底を計算すると，

$$G = \{\underset{g_1}{x+y+z^2-1},\ \underset{g_2}{y^2-y-z^2+z},\ \underset{g_3}{2yz^2+z^4-z^2},\ \underset{g_4}{z^6-4z^4+4z^3-z^2}\}$$

となる（$G_0 = G$, $G_1 = \{g_2, g_3, g_4\}$, $G_2 = \{g_4\}$ となっている）.

そこで，連立方程式

$$(**)\ \begin{cases} g_1 = x+y+z^2-1 = 0 \\ g_2 = y^2-y-z^2+z = 0 \\ g_3 = 2yz^2+z^4-z^2 = 0 \\ g_4 = z^6-4z^4+4z^3-z^2 = 0 \end{cases}$$

を解く.

- $g_4 = z^2(z-1)^2(z^2+2z-1) = 0$ を解くと，$z = 0, 1, -1\pm\sqrt{2}$ となる.
- $z = 0$ を $g_2 = 0$ に代入すると $y^2 - y = 0$ となるので $y = 0, 1$ を得る.
  $(y, z) = (0, 0)$ を $g_1 = 0$ に代入すると $x = 1$ となる.
  $(y, z) = (0, 1)$ を $g_1 = 0$ に代入すると $x = 0$ となる.
- $z = 1$ を $g_3 = 0$ に代入すると $y = 0$ となる.
  $(y, z) = (0, 1)$ を $g_1 = 0$ に代入すると $x = 0$ となる.
- $z = -1\pm\sqrt{2}$ を $g_3 = 0$ に代入すると $y = -1\pm\sqrt{2}$ となる（複号同順）.
  $(y, z) = (-1\pm\sqrt{2}, -1\pm\sqrt{2})$ を $g_1 = 0$ に代入すると $-1\pm\sqrt{2}$ となる.

以上より，連立代数方程式 $(*)$ の解は

$$(x, y, z) = (1, 0, 0), (0, 1, 0), (0, 0, 1), (-1+\sqrt{2}, -1+\sqrt{2}, -1+\sqrt{2}), (-1-\sqrt{2}, -1-\sqrt{2}, -1-\sqrt{2})$$

となる.

(2) 連立代数方程式

$$(*)\ \begin{cases} xy = 1 \\ xz = 1 \end{cases}$$

を解く.

$f_1 = xy - 1$, $g_2 = xz - 1$ と置いて $I = \langle f_1, f_2\rangle$ のグレブナー基底を計算すると

$$G = \{\underset{g_1}{xz-1},\ \underset{g_2}{y-z}\}$$

を得る（$G_0 = \{g_1, g_2\}$, $G_1 = \{g_2\}$, $G_2 = \emptyset$）.

従って，

$$(**)\ \begin{cases} g_1 = xz-1 = 0 \\ g_2 = y-z = 0 \end{cases}$$

を解けば良い.

- $g_2 = 0$ を解くと $(y, z) = (a, a)$ (a は任意の数) となる.
- $(y, z) = (a, a)$ を $g_1 = 0$ に代入すると $ax - 1 = 0$ となる．これは $a \neq 0$ のとき $x = 1/a$ となり，$a = 0$ のとき解を持たない.

以上より，$(*)$ の解は

$$(x, y, z) = \left(a, a, \frac{1}{a}\right) \quad (a \text{ は } 0 \text{ でない数})$$

注意　ここまででグレブナー基底を用いて連立代数方程式を 1 変数の方程式に帰着させて解くことができると説明した．しかし，1 変数の場合でも多項式の次数が 5 以上の場合には解の公式が存在しないことが知られている（アーベル-ルフィニの定理）ので，手計算で解くことができるとは限らない．

6.3　掃き出し法との関係

掃き出し法とは，連立一次方程式

$$(*)\quad \begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ \qquad\qquad \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m \end{cases}$$

に

- 1 つの方程式を 0 でない実数倍する
- 2 つの方程式を入れ替える
- 1 つの方程式の実数倍を別の方程式に加える

という操作を繰り返し

$$(**)\quad \begin{cases} x_1 + c_{11}x_{r+1} + \cdots + c_{1,n-r}x_n = d_1 \\ x_2 + c_{21}x_{r+1} + \cdots + c_{2,n-r}x_n = d_2 \\ \qquad\qquad \vdots \\ x_r + c_{r1}x_{r+1} + \cdots + c_{r,n-r}x_n = d_r \\ 0 = d_{r+1} \end{cases}$$

の形にして解くというものであった．実は掃き出し法で得られた一次式

$$\begin{cases} g_1 = x_1 + c_{11}x_{r+1} + \cdots + c_{1,n-r}x_n - d_1 \\ g_2 = x_2 + c_{21}x_{r+1} + \cdots + c_{2,n-r}x_n - d_2 \\ \qquad\qquad \vdots \\ g_r = x_r + c_{r1}x_{r+1} + \cdots + c_{r,n-r}x_n - d_r \\ g_{r+1} = -d_{r+1} \end{cases}$$

は元の一次式

$$\begin{cases} f_1 = a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n - b_1 \\ f_2 = a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n - b_2 \\ \qquad\qquad \vdots \\ f_m = a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n - b_m \end{cases}$$

で生成されるイデアル $I = \langle f_1, f_2, \ldots, f_m \rangle$ の極小グレブナー基底となっている．逆に，消去定理（定理 6.2）により $I = \langle f_1, f_2, \ldots, f_m \rangle$ の極小グレブナー基底は (**) の形になっていることも分か

る．従って，本質的には掃き出し法はブッフバーガーのアルゴリズムの特別な場合と思うことができる．

例 6.4　連立一次方程式

$$\begin{cases} x+3z=1 \\ 2x+3y+4z=3 \\ x+3y+z=2 \end{cases}$$

に対して掃き出し法を用いると

$$\begin{cases} x+3z=1 \\ 3y-2z=1 \end{cases}$$

を得る（例 1.5）．このとき，$g_1=x+3z-1$, $g_2=3y-2z-1$ と置くと

$$S(g_1,g_2)=y(x+3z-1)-\frac{1}{3}x(3y-2z-1)=\frac{2}{3}xz+\frac{1}{3}x+3yz-y$$

を g_1, g_2 で割った余りは 0 である：

$$S(g_1,g_2)=\left(\frac{2}{3}z+\frac{1}{3}\right)g_1+\left(z-\frac{1}{3}\right)g_2$$

従って，$\{g_1,g_2\}$ は $\langle x+3z-1, 2x+3y+4z-3, x+3y+z-2\rangle$ のグレブナー基底であり，$\left\{x+3z-1, y-\frac{2}{3}z-\frac{1}{3}\right\}$ は極小グレブナー基底である．

演習問題

問題 6.1　連立代数方程式

$$(*)\quad \begin{cases} xy+z^2=2 \\ x^2-yz=0 \\ xz-y^2=0 \end{cases}$$

を考える．

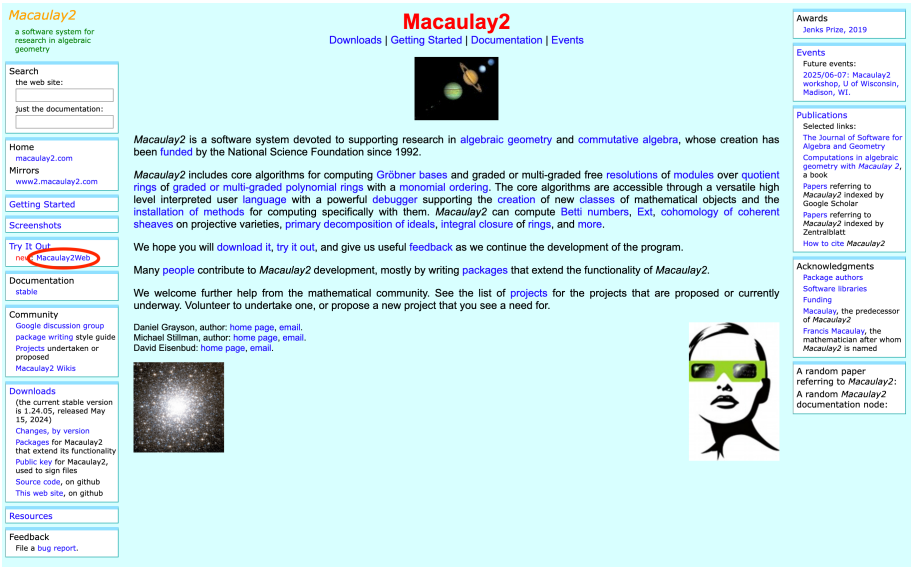
(1) $\langle xy+z^2-2, x^2-yz, xz-y^2\rangle$ の極小グレブナー基底を求めよ．
(2) (1) を用いて $(*)$ の解を求めよ．

7　グレブナー基底の応用

7.1　Macaulay2 を用いたグレブナー基底の計算

ひとまずブッフバーガーのアルゴリズムを用いて理論上グレブナー基底を計算できることになる．しかし，一般にグレブナー基底を求めるための計算量は膨大で手計算では（コンピュータでも！！）難しいことが多い．Macaulay2 という数式処理システムを使うとコンピュータがグレブナー基底を計算してくれる．

- https://macaulay2.com/ にアクセスし，左の真ん中あたりにある Macaulay2Web に飛ぶ：



- 以下のように入力することでイデアルのグレブナー基底が計算できる：

```
i1 : QQ[x,y,z,MonomialOrder=>Lex]

o1 = QQ[x..z]

o1 : PolynomialRing

i2 : I = ideal(x^2+y^2-1, x*y-1)

                   2    2
o2 = ideal (x*y - 1, x  + y  - 1)

o2 : Ideal of QQ[x..z]

i3 : G = gb I;

i4 : gens G

o4 = | y4-y2+1 x+y3-y |

                1      4
o4 : Matrix (QQ[x..z])  <-- (QQ[x..z])

i5 :
```

この入力では以下のような操作をしている：

- i1：使う変数と項順序を指定している．変数をもっとたくさん使いたい場合は x,y,z の部分を x_1,x_2,x_3,x_4,x_5 または x_1..x_5 などにすれば良い．

– i2 : 考えたいイデアルを定義している．ここでは例 5.6(1) のイデアルを入力している．
– i3 : イデアル I のグレブナー基底 G を計算させている．
– i4 : 計算したグレブナー基底 G を表示させている．o4 で I のグレブナー基底が返ってくる．

7.2 地図の塗り分け

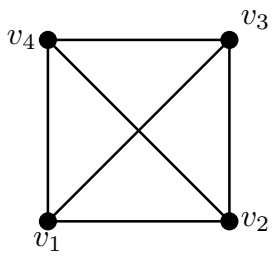
ここでは平面内の地図において，隣り合う領域が異なる色になるように色分けするためには何色必要か？という問題について考える．この問題を数学的に扱いやすくするためにグラフというものを導入する．ここで言うグラフとは，高校数学で扱う関数のグラフとは全く異なるものであることに注意しておく．

定義 7.1 グラフ G とは，**頂点**と呼ばれる有限個の点と，それらを結ぶ**辺**からなる図形である．
グラフの頂点を $v_1, v_2, \ldots, v_n$ と書いたとき，その**辺集合**を

$$E(G) := \{\{v_i, v_j\} \mid v_i \text{ と } v_j \text{ を結ぶ辺がある }\}$$

と表す．

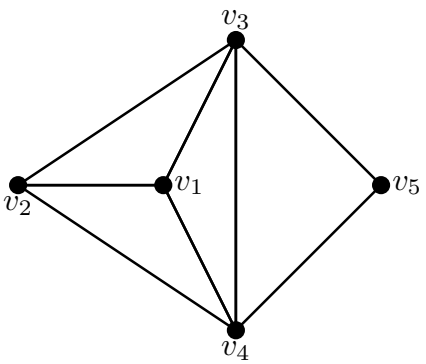
例 7.2 (1) グラフ G を



とすると，その辺集合は

$$E(G) = \{\{v_1, v_2\}, \{v_1, v_3\}, \{v_1, v_4\}, \{v_2, v_3\}, \{v_2, v_4\}, \{v_3, v_4\}\}$$

である．
(2) グラフ G を



とすると，その辺集合は

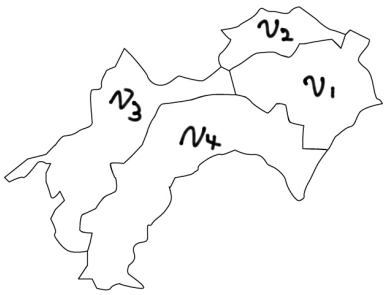
$$E(G) = \{\{v_1, v_2\}, \{v_1, v_3\}, \{v_1, v_4\}, \{v_2, v_3\}, \{v_2, v_4\}, \{v_3, v_4\}, \{v_3, v_5\}, \{v_4, v_5\}\}$$

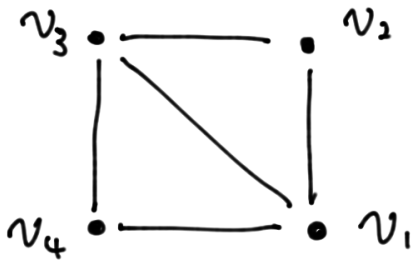
である．

例 7.3 いくつかの領域に分けられた平面上の地図は以下のような頂点と辺を持つグラフだと思うことができる：

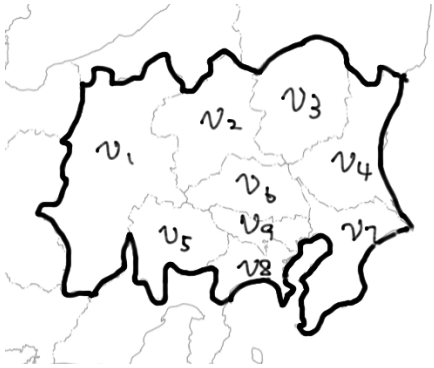
- 頂点：各領域を頂点とする
- 辺：二つの領域が隣り合うときに辺を引く

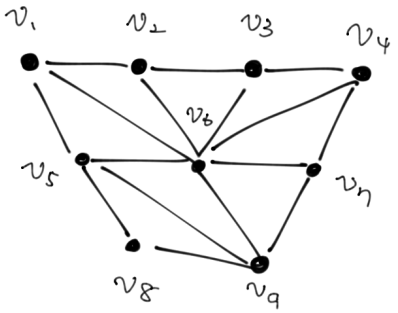
(i) 四国の地図のグラフは以下のようになる．





(ii) 関東近郊の地図のグラフは以下のようになる．



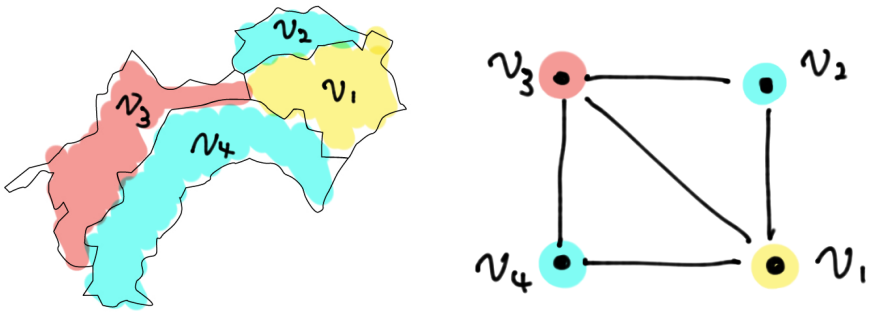


このように平面上の地図をグラフだと思ったとき，隣り合う領域が異なる色になるように色分けするというのは，辺で結ばれた頂点が異なる色になるように各頂点に色を付けることに相当する．そこで，以下のような概念を導入する．

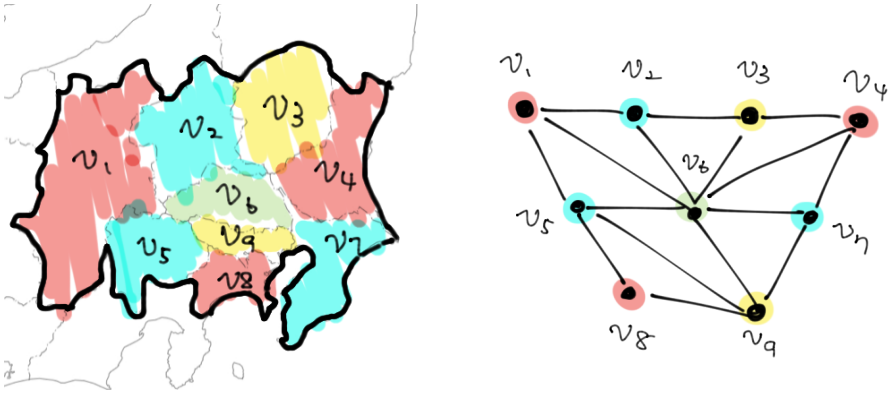
定義 7.4 k を 1 以上の整数とし，G をグラフとする．辺で結ばれた頂点が異なる番号になるように G の各頂点に $1 \sim k$ の番号を振ることができるとき，G は k **彩色可能である**と言う．

ここでは便宜上「$1 \sim k$ の番号を振る」としているが，その代わりに k 色の色を付けると考えてもよい．

例 7.5 (1) 四国の地図は以下のように 3 色で色分けできるので 3 彩色可能である．



(2) 関東近郊の地図は以下のように 4 色で色分けできるので 4 彩色可能である．



また，この地図は 3 色では色分けできないことも容易に分かる．

平面上の地図の色分けについては以下のような有名な事実が知られている．

定理 7.6 (四色定理)　どんな平面上の地図に対応するグラフも 4 彩色可能である．
　つまり，4 色あればどんな平面上の地図も隣接する領域が異なる色になるように色分けすることができる．

従って，平面上の地図に対応するグラフについては 3 彩色可能かどうかが問題になる．

ここで，一般のグラフに対して k 彩色可能かどうかを判定する便利な方法を紹介する．
各 $1 \leq i, j \leq n$ と 1 以上の整数 k に対して，以下のような多項式を考える：

- $f_i^k = x_i^k - 1$
- $f_{ij}^k = x_i^{k-1} + x_i^{k-2}x_j + x_i^{k-2}x_j^2 + \cdots + x_i x_j^{k-2} + x_j^{k-1}$

このとき，以下のことが成り立つ．

定理 7.7 ([2, Theorem 2.7.1])　頂点 $v_1, v_2, \ldots, v_n$ を持つグラフ G に対して，G が k 彩色可能であるための必要十分条件は連立方程式

$$\begin{cases} f_i^k = 0 & (1 \leq i \leq n) \\ f_{ij}^k = 0 & (v_i \text{ と } v_j \text{ の間に辺がある}) \end{cases}$$

が複素数の範囲で解を持つことである．

証明. 方程式 $f_i^k = 0$ の解は 1 の k 乗根 $\mathrm{e}^{\frac{2l\pi i}{k}}$ $(l = 1, 2, \ldots, k)$ である．方程式 $f_i^k = 0$ の解が $\mathrm{e}^{\frac{2l\pi i}{k}}$ のとき頂点 i に l を対応させれば各頂点に $1 \sim k$ を対応させることになる．

従って，以下の主張から，これらが $f_{ij}^k = 0$ の解になるという条件が辺で結ばれた頂点には異なる数を対応させることに相当する．

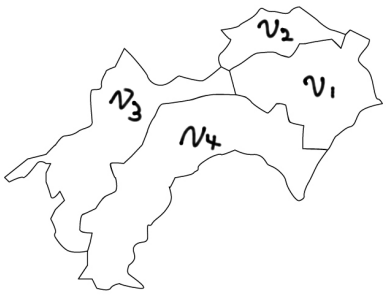
主張 f を 1 変数の n 次多項式とし $f = 0$ が相違なる解を n 個を持つとする．a, b をその二つの解とする．このとき，以下が成り立つ．

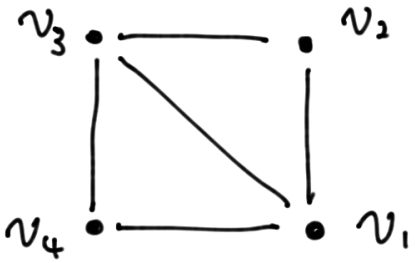
$$(x, y) = (a, b) \text{ が多項式 } \frac{f(x) - f(y)}{x - y} = 0 \text{ の解} \iff a \neq b$$

■

従って，与えられたグラフが k 彩色可能かどうかは前節までのグラブナー基底を用いた方法で判定することができる．

例 7.8 (1) 四国の地図に対応するグラフ G を考える：





このとき，定理 7.7 より

G が 3 彩色可能 $\iff$ 以下の連立方程式が解を持つ

$$\begin{cases} x_1^3 - 1 = 0 \\ x_2^3 - 1 = 0 \\ x_3^3 - 1 = 0 \\ x_4^3 - 1 = 0 \\ x_1^2 + x_1x_2 + x_2^2 = 0 \\ x_1^2 + x_1x_3 + x_3^2 = 0 \\ x_1^2 + x_1x_4 + x_4^2 = 0 \\ x_2^2 + x_2x_3 + x_3^2 = 0 \\ x_3^2 + x_3x_4 + x_4^2 = 0 \end{cases}$$

これらの多項式を基底とするイデアルのグレブナー基底を Macaulay2 で計算すると，

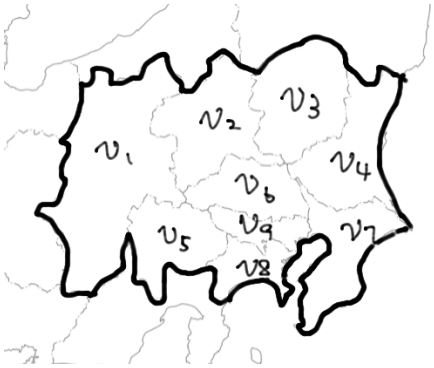
$$g_1 = x_1 + x_3 + x_4, \quad g_2 = x_2 - x_4, \quad g_3 = x_3^2 + x_3x_4 + x_4^2, \quad g_4 = x_4^3 - 1$$

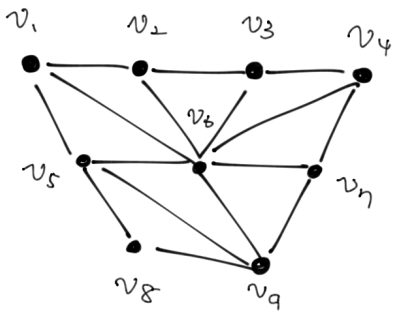
となる．このとき，連立方程式

$$
\begin{aligned}
g_1 &= x_1 + x_3 + x_4 = 0 \\
g_2 &= x_2 - x_4 = 0 \\
g_3 &= x_3^2 + x_3 x_4 + x_4^2 = 0 \\
g_4 &= x_4^3 - 1 = 0
\end{aligned}
$$

は解を持つ（$g_4 = 0$ の解を $g_3 = 0$ に代入して解けば x_3, x_4 が求まり，それを $g_1 = 0, g_2 = 0$ に代入すれば x_1, x_2 が求まる）．従って，四国の地図は 3 彩色可能である．

(2) 関東近郊の地図に対応するグラフ G を考える：





このとき，定理 7.7 より

関東近郊の地図が 3 彩色可能 $\Longleftrightarrow$ 以下の連立方程式が解を持つ

$$
\begin{cases}
x_1^3 - 1 = 0 \\
x_2^3 - 1 = 0 \\
\quad \vdots \\
x_9^3 - 1 = 0 \\
x_1^2 + x_1 x_2 + x_2^2 = 0 \\
x_1^2 + x_1 x_5 + x_5^2 = 0 \\
x_1^2 + x_1 x_6 + x_6^2 = 0 \\
x_2^2 + x_2 x_3 + x_3^2 = 0 \\
x_2^2 + x_2 x_6 + x_6^2 = 0 \\
x_3^2 + x_3 x_4 + x_4^2 = 0 \\
x_3^2 + x_3 x_6 + x_6^2 = 0 \\
x_4^2 + x_4 x_6 + x_6^2 = 0 \\
x_4^2 + x_4 x_7 + x_7^2 = 0 \\
x_5^2 + x_5 x_6 + x_6^2 = 0 \\
x_5^2 + x_5 x_8 + x_8^2 = 0 \\
x_5^2 + x_5 x_9 + x_9^2 = 0 \\
x_6^2 + x_6 x_7 + x_7^2 = 0 \\
x_6^2 + x_6 x_9 + x_9^2 = 0 \\
x_7^2 + x_7 x_9 + x_9^2 = 0 \\
x_8^2 + x_8 x_9 + x_9^2 = 0
\end{cases}
$$

これらの多項式を基底とするイデアルのグレブナー基底を Macaulay2 で計算すると

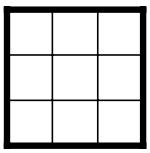
$$g_1 = 1$$

となる．方程式 $g_1 = 0$ は解を持たないので関東近郊の地図は 3 色で塗り分けできないことが分かる．

7.3　数学パズル

魔方陣

3×3 のマス



に以下のルールで数を入れたものを**魔方陣**と呼ぶ[*4]：

- 1 から 9 までの数を一回ずつ使う
- 各行に入る数の和，各列に入る数の和,，対角線上の数の和が全て等しい

例 7.9　例えば以下のものは魔方陣である：

6	1	8
7	5	3
2	9	4

8	1	6
3	5	7
4	9	2

以下，どのような魔方陣があるか考えていく．簡単に分かることとして，1 から 9 までの数の合計は 45 なので，行，列，対角線上の数の合計は $45 \div 3 = 15$ となる．次に，マスに入る数が満たすべき条件を調べていく．以下のように $x_1, x_2, \ldots, x_9$ がマスの中に入っているとする．

x_1	x_2	x_3
x_4	x_5	x_6
x_7	x_8	x_9

このとき，魔方陣のルールから以下のことが成り立っていないといけない：

- 各 $1 \leq i \leq 9$ に対して以下の方程式が成り立つ：

$$f_i = (x_i - 1)(x_i - 2)\cdots(x_i - 9) = 0 \quad \text{(各マスには 1 から 9 までの数が入る)}$$

[*4] 魔法陣ではない

- $i \neq j$ に対して以下の方程式が成り立つ：

$$\frac{f_i - f_j}{x_i - x_j} = 0 \quad (\text{異なるマスには異なる数が入る})$$

（定理 7.7 の証明中の主張を見よ）

- 以下の方程式が成り立つ：

$$\begin{cases} x_1 + x_2 + x_3 = 15 \\ x_4 + x_5 + x_6 = 15 \\ x_7 + x_8 + x_8 = 15 \end{cases} \quad (\text{各行の数の和が } 15)$$

$$\begin{cases} x_1 + x_4 + x_7 = 15 \\ x_2 + x_5 + x_8 = 15 \\ x_3 + x_6 + x_9 = 15 \end{cases} \quad (\text{各列の数の和が } 15)$$

$$\begin{cases} x_1 + x_5 + x_9 = 15 \\ x_3 + x_5 + x_7 = 15 \end{cases} \quad (\text{対角線上の数の和が } 15)$$

従って，この合計 53 個の連立方程式の解を求めれば魔方陣を決定することができる．これらの多項式を基底とするイデアルのグレブナー基底を Macaulay2 で計算すると

$$\begin{aligned} &g_1 = x_1 + x_9 - 10, \quad g_2 = x_2 + x_8 - 10, \quad g_3 = x_3 - x_8 - x_9 + 5, \\ &g_4 = x_4 - x_8 - 2x_9 + 10, \quad g_5 = x_5 - 5, \quad g_6 = x_6 + x_8 + 2x_9 - 20, \\ &g_7 = x_7 + x_8 + x_9 - 15, \quad g_8 = x_8^2 + 2x_8x_9 - 20x_8 + 2x_9^2 - 30x_9 + 115, \\ &g_9 = x_9^4 - 20x_9^3 + 140x_9^2 - 400x_9 + 384 \end{aligned}$$

となる．従って，連立方程式

$$\begin{cases} g_1 = 0 \\ g_2 = 0 \\ g_3 = 0 \\ g_4 = 0 \\ g_5 = 0 \\ g_6 = 0 \\ g_7 = 0 \\ g_8 = 0 \\ g_9 = 0 \end{cases}$$

を解けば良い．x_9 のみの方程式 $g_9 = 0$ の解は $x_9 = 2, 4, 6, 8$ である．これを他の式に代入することで残りの変数の値も求まり，以下のような魔法陣を得る：

- $x_9 = 2$ のとき

8	3	4
1	5	9
6	7	2

8	1	6
3	5	7
4	9	2

- $x_9 = 4$ のとき

6	7	2
1	5	9
8	3	4

6	1	8
7	5	3
2	9	4

- $x_9 = 6$ のとき

4	3	8
9	5	1
2	7	6

4	9	2
3	5	7
8	1	6

- $x_9 = 8$ のとき

2	9	4
7	5	3
6	1	8

2	7	6
9	5	1
4	3	8

従って，3×3 の魔方陣はこれらの 8 種類しかないことが分かる[*5]．

数独

数独（またはナンプレ）とは，以下のようなあらかじめいくつかの数字が入った 4×4 のマス

3			
		2	
	1		**4**

に以下のルールで数字を入れていくパズルである[*6]：

- 入る数字は 1 から 4 までのいずれか
- 各列，各行および太線で囲まれた 2×2 のブロックには 1 から 4 が一つずつ入る

例 7.10

左の数独の問題を解くと右のようになる．

3			
		2	
	1		**4**

3	4	1	2
1	2	4	3
4	3	**2**	1
2	**1**	3	**4**

それでは，数独の問題をグレブナー基底に解いてもらおう．考え方は魔方陣を解いたときと同様

[*5] 4×4 の魔方陣は 880 個あるらしい

[*6] 本来は 9×9 のマスを使うが，話を簡単にするためにこのように小さい場合を考える

で，4×4 のマスに

x_1	x_2	x_3	x_4
x_5	x_6	x_7	x_8
x_9	x_{10}	x_{11}	x_{12}
x_{13}	x_{14}	x_{15}	x_{16}

のように $x_1 \sim x_{16}$ の数が入っているとし，これらが満たすべき方程式をグレブナー基底を用いて解いていく．$x_1 \sim x_{16}$ は数独のルールから以下を満たしていなければならない：

- $1 \leq i \leq 16$ に対して，以下の方程式が成り立つ：

$$f_i = (x_i - 1)(x_i - 2)(x_i - 3)(x_i - 4) = 0 \quad (\text{各マスには } 1, 2, 3, 4 \text{ の数が入る})$$

- $i \neq j$ に対して,，以下の方程式が成り立つ：
  - $1 \leq i, j \leq 4$，$5 \leq i, j \leq 8$，$9 \leq i, j \leq 12$，または $13 \leq i, j \leq 16$ のとき

$$\frac{f_i - f_i}{x_i - x_j} = 0 \quad (\text{各行において異なるマスには異なる数が入る})$$

  - $i, j \in \{1, 5, 9, 13\}$，$i, j \in \{2, 6, 10, 14\}$，$i, j \in \{3, 7, 11, 15\}$，または $i, j \in \{4, 8, 12, 16\}$ のとき

$$\frac{f_i - f_i}{x_i - x_j} = 0 \quad (\text{各列において異なるマスには異なる数が入る})$$

  - $i, j \in \{1, 2, 5, 6\}$，$i, j \in \{3, 4, 7, 8\}$，$i, j \in \{9, 10, 13, 14\}$，または $i, j \in \{11, 12, 15, 16\}$ のとき

$$\frac{f_i - f_i}{x_i - x_j} = 0 \quad (\text{各ブロックにおいて異なるマスには異なる数が入る})$$

  （定理 7.7 の証明中の主張を見よ）
- 初期状態で x_i のマスに a_i が入っているとき，

$$x_i - a_i = 0$$

  例えば，例 7.10 の場合は $x_1 - 3 = 0$, $x_{11} - 2 = 0$, $x_{14} - 1 = 0$, $x_{16} - 4 = 0$.

これらの $88 + \alpha$ 個の連立方程式を解けば数独の答えが分かる．

実際にこれらの多項式を基底とするイデアルのグレブナー基底を Macaulay2 で計算すると

$$\begin{aligned}
&g_1 = x_1 - 3, \quad g_2 = x_2 - 4, \quad g_3 = x_3 - 1, \quad g_4 = x_4 - 2, \\
&g_5 = x_5 - 1, \quad g_6 = x_6 - 2, \quad g_7 = x_7 - 4, \quad g_8 = x_8 - 3, \\
&g_9 = x_9 - 4, \quad g_{10} = x_{10} - 3, \quad g_{11} = x_{11} - 2, \quad g_{12} = x_{12} - 1, \\
&g_{13} = x_{13} - 2, \quad g_{14} = x_{14} - 1, \quad g_{15} = x_{15} - 3, \quad g_{16} = x_{16} - 4
\end{aligned}$$

となる．従って，これらが全て 0 になるものとして $x_1, x_2, \ldots, x_{16}$ が求まる．これを数独のマスに当てはめると

3	4	1	2
1	2	4	3
4	3	**2**	1
2	**1**	3	**4**

となり，これは例 7.10 の答えと一致している．

演習問題

問題 7.1 定理 7.7 の証明中の主張を以下のようにして示せ．

(1) f は相違なる n 個の解を持つので，相違なる複素数 $a_1, a_2, \ldots, a_n$ を用いて $f = (x-a_1)(x-a_2)\cdots(x-a_n)$ と表せる．このとき，$f = 0$ と $f' = 0$ は共通の解を持たないことを示せ．ここで，f' は f の導関数．

(2) 整数 $k \geq 1$ に対して，

$$\frac{x^k - y^k}{x - y}$$

がどのような多項式になるか書け．

(3) $f = c_n x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$ と表す．このとき，多項式

$$g(x,y) = \frac{f(x) - f(y)}{x - y}$$

に対して，$g(x,x) = f'(x)$ となることを確かめよ．

(4) 以上のことを用いて定理 7.7 の証明中の主張を示せ．

問題 7.2 (1) 例 7.2 の二つのグラフが 3 彩色可能であるかどうかグレブナー基底を用いて調べよ．

(2) 中部地方の地図

が 3 色で色分け可能かどうかグレブナー基底を用いて調べよ．

問題 7.3　以下の数独の問題をグレブナー基底を用いて解け.

		2	
	1		
			3
3			

			3
4			
1			
		1	

参考文献

[1] D. コックス, J. リトル, D. オシー著，大杉英史，土谷昭善訳，「グレブナー基底と代数多様体入門 上 原初 4 版」，丸善出版，2023.

[2] W.W. Adams and P. Loustaunau, An introduction to Gröbner bases, *AMS*, 1994.