応用線形代数特論

土谷 昭善

イントロダクション

線形代数学，特に行列理論における最初の応用は，連立１次方程式を解くことである．まずはその方法について復習する．

k を $\mathbb{Q}$ (有理数全体の集合)，$\mathbb{R}$（実数全体の集合）または $\mathbb{C}$（複素数全体の集合）とする（より一般に k は体として考えても良い）．k 上の連立１次方程式

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

は，行列を用いて表すと

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

と書ける．この式に対応して，$A\mathbf{x} = \mathbf{b}$ と書くことにする．このときの A をこの連立１次方程式の**係数行列**という．さらに A に $\mathbf{b}$ をくっつけた行列，$(A \mid \mathbf{b})$ を**拡大係数行列**という．連立１次方程式の一般解は拡大係数行列に対して，**ガウスの消去法（掃き出し法）**を行うことで得られるのであった．例を見て確認する．

例 0.1. 連立１次方程式として

$$\begin{pmatrix} 1 & 2 & -2 \\ 1 & -1 & 3 \\ 2 & 3 & -5 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 3 \\ 4 \\ 1 \end{pmatrix}$$

を解く．拡大係数行列は行基本変形によって

$$\left(\begin{array}{ccc|c} 1 & 2 & -2 & 3 \\ 1 & -1 & 3 & 4 \\ 2 & 3 & -5 & 1 \end{array}\right) \to \left(\begin{array}{ccc|c} 1 & 2 & -2 & 3 \\ 0 & -3 & 5 & 1 \\ 0 & 0 & 1 & 2 \end{array}\right)$$

と変形できる．３行目は $z = 2$ を意味しており，これと２行目から $y = 3$ が得られ，最終的に１行目から $x = 1$ が得られる．したがってこの連立方程式の解は

$$(x, y, z) = (1, 3, 2)$$

となる．

このように，連立１次方程式の場合，行基本変形を繰り返し，階段行列に変形することで文字を消去し，変数の少ない方程式を新たに見つけることで，連立方程式を解くことが可能である．特に，この変形はどんな連立１次方程式に対しても有限回の操作で終了する．したがって簡単なプログラミングにより連立１次方程式は計算機を使って必ず解くことが可能である．それでは，もう少し複雑な連立方程式の場合はどうか．例えば，１次とは限らない連立方程式，

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

を考えるを機械的に解くことは可能だろうか．実はこの連立方程式で x と y をうまく消去すれば

$$z^4 - 3z^2 + 2 = (z-1)(z+1)(z^2-2) = 0$$

という新しい式が得られ，解を求めることができる．それではこの式をどうやって見つければいいのだろうか．本講義では，一般の計算処理ソフトウェアにも導入されている**グレブナー基底**を使った一般の多項式の連立方程式を解くアルゴリズムを理解することを目標とする．

1　多項式環とアフィン多様体

本講義で重要である多項式環と基本的な幾何的対象であるアフィン多様体を導入する．まずは単項式の定義から始める．

定義 1.1. $x_1, \ldots, x_n$ の**単項式** (monomial) とは

$$x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdots x_n^{\alpha_n}$$

の形の積のことをいう．ここで指数 $\alpha_1, \ldots, \alpha_n$ は非負整数である．和 $\alpha_1 + \cdots + \alpha_n$ をこの単項式の**全次数** (total degree) という．

単項式を簡略化して次のように表記することができる．$\alpha = (\alpha_1, \ldots, \alpha_n)$ を非負整数の n 個の組として，

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

と書く．$\alpha = (0, \ldots, 0)$ のときは，$x^\alpha = 1$ であることに注意する．$|\alpha| = \alpha_1 + \cdots + \alpha_n$ により，単項式 x^α の全次数を表す．

定義 1.2. 係数を k に持つ $x_1, \ldots, x_n$ の**多項式** (polynomial) f とは，k の元を係数とする単項式の有限個の線型結合のことをいう．多項式 f を次のように表す．

$$f = \sum_\alpha a_\alpha x^\alpha, \quad a_\alpha \in k.$$

ここで，和は有限個の $\alpha = (\alpha_1, \ldots, \alpha_n)$ についてとっている．係数を k に持つ $x_1, \ldots, x_n$ の多項式全体の集合を $k[X] := k[x_1, \ldots, x_n]$ と表す．

変数の個数が少ない多項式を扱うときは，添字を省いて，$x_1, x_2, x_3, \ldots$ の代わりに x, y, z, w を使う．
多項式を扱う際に次の用語を使う．

定義 1.3. $f = \sum_\alpha a_\alpha x^\alpha$ を $k[x_1, \ldots, x_n]$ の多項式とする．

1. a_α を単項式 x^α の**係数** (coefficient) という．
2. $a_\alpha \neq 0$ のとき，$a_\alpha x^\alpha$ を f の**項** (term) という．

3. $f \neq 0$ のとき，係数 a_α がゼロでないような $|\alpha|$ の最大値を f の**全次数** (total degree) といい，$\deg(f)$ で表す．零多項式の全次数は定義しない．

例えば，$k[x,y,z]$ の多項式 $f = 2x^3y^2z + 3y^3z^3 - 3xyz + y^2$ は 4 つ項を持ち，全次数は 6 である．また全次数を持つ項は複数個あることに注意する．

2 つの多項式の積や和はふたたび多項式となる．多項式 $f, g \in k[X]$ に対して，$g = fh$ となるような多項式 $h \in k[X]$ が存在するとき，f は g を**割り切る**といい，$f|g$ と表す．

次に $k[X]$ の数学的構造について調べる．

定義 1.4. 可換環 (commutative ring) とは集合 R で，この上に 2 つの 2 項演算 "$+$" と "$\cdot$" が定義されて，次の条件を満たしているものである．

1. $(a+b)+c = a+(b+c)$ と $(a\cdot b)\cdot c = a\cdot(b\cdot c)$ がすべての $a,b,c \in R$ に対して満たされている（結合性）．
2. $a+b = b+a$ と $a\cdot b = b\cdot a$ がすべての $a,b \in R$ に対して満たされている（可換性）．
3. $a\cdot(b+c) = a\cdot b + a\cdot c$ がすべての $a,b,c \in R$ に対して満たされている（分配性）．
4. R の元 $0,1 \in R$ が存在して，すべての $a \in R$ に対して $a+0 = a\cdot 1 = a$ となる（単位元の存在）．
5. 与えられた元 $a \in R$ に対して，元 $b \in R$ が存在して $a+b = 0$ となる（加法の逆元の存在）．

$k[X]$ は加法と乗法の下で，可換環の構造を持つ．ゆえに，$k[X]$ は**多項式環** (polynomial ring) と呼ばれる．

次にアフィン多様体を定義する．

定義 1.5. 集合

$$k^n = \{(a_1,\dots,a_n) : a_1,\dots,a_n \in k\}$$

を k 上の n 次元**アフィン空間** (affine space) と呼ぶ．$f_1,\dots,f_s$ を $k[X]$ の多項式としたとき，

$$\mathbf{V}(f_1,\dots,f_s) = \{(a_1,\dots,a_n) \in k^n : \text{すべての } 1 \le i \le s \text{ に対して } f_i(a_1,\dots,a_n) = 0\}$$

とおき．$\mathbf{V}(f_1,\dots,f_s)$ を $f_1,\dots,f_s$ により定義される**アフィン多様体** (affine variety) という．また $f_1,\dots,f_s$ を $\mathbf{V}(f_1,\dots,f_s)$ の**定義方程式**という．

つまりアフィン多様体 $\mathbf{V}(f_1,\dots,f_s)$ とは連立方程式

$$f_1(x_1,\dots,x_n) = f_2(x_1,\dots,x_n) = \cdots = f_s(x_1,\dots,x_n) = 0$$

の解全体の集合である．したがって，一般の多項式の連立方程式を解く，と言うことは $\mathbf{V}(f_1,\dots,f_s)$ を具体的に記述するということに他ならない．

例 1.6. 平面 $\mathbb{R}^2$ 内の多様体 $\mathbf{V}(x^2+y^2-1)$ を考える．これは原点を中心とする半径 *1* の円である．他にも円錐曲線（円，楕円，放物線，双曲線）はアフィン多様体である．同様に多項式関数のグラフはアフィン多様体である（ $y = f(x)$ のグラフは $\mathbf{V}(y-f(x))$ である）．

アフィン多様体は空集合になりうることにも触れておかなければならない．たとえば $k = \mathbb{R}$ のとき，$x^2+y^2 = -1$ は実数解を持たないから，明らかに $\mathbf{V}(x^2+y^2+1) = \emptyset$ である（$k = \mathbb{C}$ のときには解がある）．別の例は $\mathbf{V}(xy, xy-1)$ である．与えられた x と y に対して，$xy = 0$ と $xy = 1$ が同時に成り立つことはありえないから，これはどんな体上でも空集合である．

最後に，アフィン多様体の基本性質を記しておく．

補題 1.7. $V, W \subset k^n$ がアフィン多様体ならば，$V \cup W$ と $V \cap W$ もアフィン多様体である．

Proof. $V = \mathbf{V}(f_1, \ldots, f_s)$, $W = \mathbf{V}(g_1, \ldots, g_t)$ であるとする．このとき，

$$V \cap W = \mathbf{V}(f_1, \ldots, f_s, g_1, \ldots, g_t)$$
$$V \cup W = \mathbf{V}(f_i g_j : 1 \leq i \leq s, 1 \leq j \leq t)$$

となることを主張する．1 番目の等号の証明は自明である．実際 $V \cap W$ に属するということは，$f_1, \ldots, f_s$ と $g_1, \ldots, g_t$ の両方が消えること，すなわち $f_1, \ldots, f_s, g_1, \ldots, g_t$ が消えることを意味するからである．[1]

2 番目の等式はもう少し大変である．$(a_1, \ldots, a_n) \in V$ とすると，すべての f_i はこの点で消えるから，すべての $f_i g_j$ もまた点 $(a_1, \ldots, a_n)$ で消える．したがって，$V \subset \mathbf{V}(f_i g_j)$ である．同様に $W \subset \mathbf{V}(f_i g_j)$ が従う．これは $V \cup W \subset \mathbf{V}(f_i g_j)$ を示している．逆の包含関係を示すために，$(a_1, \ldots, a_n) \in \mathbf{V}(f_i g_j)$ を選ぶ．これが V に属していれば証明が終わる．そうでないとすると，ある i_0 に対して $f_{i_0}(a_1, \ldots, a_n) \neq 0$ である．任意の j に対して $f_{i_0} g_j$ は $(a_1, \ldots, a_n)$ で消えているから，g_j はこの点で消えていなければならない．これは $(a_1, \ldots, a_s) \in W$ を示している．以上により $\mathbf{V}(f_i g_j) \subset V \cup W$ が示された． □

演習問題

1. 1 点 $(a_1, \ldots, a_n) \in k^n$ はアフィン多様体であることを示せ．
2. k^n の任意の有限部分集合はアフィン多様体であることを示せ．ヒント：補題 1.7 を用いよ．

2 イデアル

この章では本講義で学ぶ基本的な代数的対象を定義する．

定義 2.1. 部分集合 $I \subset k[X]$ が**イデアル** (ideal) であるとは，次を満たすときをいう．

1. $0 \in I$.
2. $f, g \in I$ ならば $f + g \in I$.
3. $f \in I$ かつ $h \in k[X]$ ならば $hf \in I$.

イデアルは線形代数学でいうベクトル空間の部分空間のようなものである．違うのは，ベクトル空間のスカラー倍が，イデアルでは多項式の積となっていることである．

イデアルの最初の自然な例は，有限個の多項式により生成されるイデアルである．

定義 2.2. $f_1, \ldots, f_s$ を $K[X]$ に含まれる多項式とする．このとき，

$$\langle f_1, \ldots, f_s \rangle = \left\{ \sum_{i=1}^{s} h_i f_i \ : \ h_1, \ldots, h_s \in K[X] \right\}$$

とおく．

重要な事実は，$\langle f_1, \ldots, f_s \rangle$ がイデアルになることである．

補題 2.3. $f_1, \ldots, f_s \in K[X]$ とすると，$\langle f_1, \ldots, f_s \rangle$ は $K[X]$ のイデアルである．$\langle f_1, \ldots, f_s \rangle$ を $f_1, \ldots, f_s \in K[X]$ **により生成されるイデアル**という．

[1]「消える」は vanish の訳で，値がゼロになることを意味する．

Proof. まず $0 = \sum_{i=1}^{s} 0 \cdot f_i$ だから，$0 \in \langle f_1, \ldots, f_s \rangle$ である．次に $f = \sum_{i=1}^{s} p_i f_i$, $g = \sum_{i=1}^{s} q_i f_i$ と仮定し，$h \in K[X]$ とする．このとき等式

$$f + g = \sum_{i=1}^{s} (p_i + q_i) f_i,$$
$$hf = \sum_{i=1}^{s} (hp_i) f_i$$

より，$\langle f_1, \ldots, f_s \rangle$ はイデアルである． □

イデアル $\langle f_1, \ldots, f_s \rangle$ は，多項式の連立方程式を考えるとうまく解釈できる．$f_1, \ldots, f_s \in K[X]$ に対して，連立方程式

$$\begin{aligned} f_1 &= 0, \\ &\vdots \\ f_s &= 0 \end{aligned}$$

を考える．これらの方程式から，代数を用いて別の連立方程式を導くことができる．たとえば，最初の方程式と $h_1 \in K[X]$ の積をとる，2 番目の方程式と $h_2 \in K[X]$ の積をとる，というように順に作った式の和をとると，

$$h_1 f_1 + h_2 f_2 + \cdots + h_s f_s = 0$$

がもとの連立方程式から得られる．この方程式の左辺は，まさにイデアル $\langle f_1, \ldots, f_s \rangle$ の要素になっていることに注意する．したがって，$\langle f_1, \ldots, f_s \rangle$ は連立方程式 $f_1 = f_2 = \cdots = f_s = 0$ から “帰結された多項式” 全体からなる集合と考えることができる．

イデアル I が**有限生成** (finitely generated) であるとは，$I = \langle f_1, \ldots, f_s \rangle$ となる $f_1, \ldots, f_s \in K[X]$ が存在するときをいい，$f_1, \ldots, f_s$ を I の**基底** (basis) または**生成系** (generator) という．後ろの章で，$K[X]$ の**任意の**イデアルは有限生成であるという驚くべき事実を証明する（これはヒルベルトの基底定理として知られている）．

次の命題は，イデアルの果たす別の役割を示唆する．これは多様体がその定義方程式により生成される**イデアル**だけに依存することを示している．

命題 2.4. $f_1, \ldots, f_s$ と $g_1, \ldots, g_t$ が $K[X]$ の同じイデアルの基底である，つまり $\langle f_1, \ldots, f_s \rangle = \langle g_1, \ldots, g_t \rangle$ とする．このとき，$\mathbf{V}(f_1, \ldots, f_s) = \mathbf{V}(g_1, \ldots, g_t)$ である．

Proof. 証明は省略する． □

例として多様体 $\mathbf{V}(2x^2 + 3y^2 - 11, x^2 - y^2 - 3)$ を考える．$\langle 2x^2 + 3y^2 - 11, x^2 - y^2 - 3 \rangle = \langle x^2 - 4, y^2 - 1 \rangle$ となることが容易に示せるので，上の命題より

$$\mathbf{V}(2x^2 + 3y^2 - 11, x^2 - y^2 - 3) = \mathbf{V}(x^2 - 4, y^2 - 1) = \{(\pm 2, \pm 1)\}$$

となる．このようにイデアルの基底を取り換えることにより，多様体を決定しやすくなった．

次に与えられた多様体上で消える多項式**全体**の集合を考える．

定義 2.5. $V \subset k^n$ をアフィン多様体とする．このとき

$$\mathbf{I}(V) = \{f \in K[X] : \text{すべての } (a_1, \ldots, a_n) \in V \text{ に対して } f(a_1, \ldots, a_n) = 0\}$$

とおく．

重要な結果は，$\mathbf{I}(V)$ がイデアルになることである．

補題 2.6. $V \subset k^n$ をアフィン多様体とする．このとき $\mathbf{I}(V) \subset K[X]$ はイデアルである．$\mathbf{I}(V)$ を V **のイデアル**という．

Proof. 零多項式は k^n 全体で消えるから特に V 上消える．したがって $0 \in \mathbf{I}(V)$ は明らかである．次に $f, g \in \mathbf{I}(V)$ と仮定し $h \in K[X]$ とする．

$(a_1, \ldots, a_n)$ を V の任意の点とする．このとき

$$f(a_1, \ldots, a_n) + g(a_1, \ldots, a_n) = 0 + 0 = 0,$$
$$h(a_1, \ldots, a_n) f(a_1, \ldots, a_n) = h(a_1, \ldots, a_n) \cdot 0 = 0$$

となるから，$\mathbf{I}(V)$ はイデアルである． □

例 2.7. 多様体のイデアルの例として，k^2 の原点からなる多様体 $\{(0,0)\}$ を考える．このとき，そのイデアル $\mathbf{I}(\{(0,0\})$ は，原点で消えるすべての多項式からなるが，

$$\mathbf{I}(\{(0,0)\}) = \langle x, y \rangle$$

が成り立つ．$A(x,y)x + B(x,y)y$ の形の多項式は明らかに原点で消えるから，証明の一方向は自明である．もう一方を示すために，$f = \sum_{i,j} a_{ij} x^i y^j$ が原点で消えると仮定する．このとき，$a_{00} = f(0,0) = 0$ であるから，

$$f = a_{00} + \sum_{(i,j) \neq (0,0)} a_{ij} x^i y^j = 0 + \left(\sum_{i>0, j} a_{ij} x^{i-1} y^j \right) x + \left(\sum_{j>0} a_{0j} y^{j-1} \right) y \in \langle x, y \rangle$$

となる．以上により主張が示された．

定義 2.8. イデアル $I \subset k[X]$ が**単項式イデアル** (monomial ideal) であるとは部分集合 $A \subset \mathbb{Z}^n_{\geq 0}$ があって，I が $\sum_{\alpha \in A} h_\alpha x^\alpha (h_\alpha \in k[X])$ の形の有限和で書ける多項式全体からなることをいう．ここで $\mathbb{Z}_{\geq 0}$ は非負整数全体の集合である．このとき，$I = \langle x^\alpha : \alpha \in A \rangle$ と書く．

例 2.9. $\mathbb{Q}[x,y]$ のイデアルとして $I = \langle x+y, x-y \rangle$ を考える．このとき，$((x+y)+(x-y))/2 = x$ と $((x+y)-(x-y))/2 = y$ から $x, y \in I$，特に，$\langle x, y \rangle \subset I$ である．明らかに逆の包含関係が成り立つので，$\langle x, y \rangle = I$ となる．したがって，I は単項式イデアルである．このように，イデアルが単項式でないもので生成されていたとしても，単項式イデアルになることがある．

イデアルに関する代表的問題として，与えられた $f \in k[X]$ がイデアル $I \subset k[X]$ に属するかどうかを決定するアルゴリズムが存在するか？というイデアル所属問題がある．単項式イデアルに関して，この問題は簡単である．

補題 2.10. $I = \langle x^\alpha : \alpha \in A \rangle$ を単項式イデアルとする．このとき，単項式 x^β が I の元であることと，ある $\alpha \in A$ に対して x^β が x^α で割り切れることは同値である．

Proof. もし x^β が適当な $\alpha \in A$ に対して x^α の倍元であるならば，イデアルの定義により $x^\beta \in I$ である．逆に，もし $x^\beta \in I$ であるならば $x^\beta = \sum_{i=1}^s h_i x^{\alpha(i)}$ となる．ここで，$h_i \in k[X]$ かつ $\alpha(i) \in A$ である．もし，各 h_i を項の和に分解すると，

$$x^\beta = \sum_{i=1}^s h_i x^{\alpha(i)} = \sum_{i=1}^s \left(\sum_j c_{i,j} x^{\beta(i,j)} \right) x^{\alpha(i)} = \sum_{i,j} c_{i,j} x^{\beta(i,j)} x^{\alpha(i)}$$

を得る．右辺に現れる単項式の各項は $x^{\alpha(i)}$ のどれかで割り切れる．したがって左辺の単項式 x^β も同じ性質を持つ． □

次に，与えられた多項式 f が単項式イデアルに含まれるどうかの判定法を証明する．

補題 2.11. I を単項式イデアルとし，$f \in k[X]$ とする．このとき，次の 3 つの主張は同値である．

1. $f \in I$,

2. f のすべての項は I に属する．

3. f は I の単項式の k 線形結合である．

Proof. (3) ⇒ (2) ⇒ (1) と (2) ⇒ (3) は明らか．(1) ⇒ (2) は補題 2.10 と同様の方法で証明できる． □

この補題の (3) から，単項式イデアルはその中に含まれる単項式から一意的に決定されることがわかる．したがって次が成り立つ．

系 2.12. 2つの単項式イデアルが同じであることと，そこに含まれる単項式全体が一致することは同値である．

最後に単項式イデアルに対するヒルベルトの基底定理を証明する．

定理 2.13 (ディクソンの補題)**.** $I = \langle x^\alpha : \alpha \in A\rangle$ を単項式イデアルとする．このとき，I は，有限個の $\alpha(1), \ldots, \alpha(s) \in A$ を選んで $I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)}\rangle$ と書き表すことができる．特に，I は有限生成である．

Proof. 変数の個数 n に関する帰納法を使う．$n = 1$ のとき，I は単項式 x_1^α $(\alpha \in A \subset \mathbb{Z}_{\geq 0})$ により生成される．β を A の最小元とする．このとき，$\beta \leq \alpha$ がすべての $\alpha \in A$ に対して成り立つ．よって x_1^β はその他の生成元 x_1^α をすべて割り切る．これより $I = \langle x_1^\beta\rangle$ が従う．

次に n まで定理が成り立つと仮定する．$R_{n+1} = k[x_1, \ldots, x_n, y]$ とし，単項式を $x^\alpha y^m$ と表し，$I = \langle x^\alpha y^m : (\alpha, m) \in A\rangle$ と書く．$A' = \{\alpha \in \mathbb{Z}_{\geq 0}^n : {}^\exists m, (\alpha, m) \in A\}$ とし，$k[X] = k[x_1, \ldots, x_n]$ のイデアル

$$J := \langle x^\alpha : \alpha \in A'\rangle \subset k[X]$$

を定義する．帰納法の仮定から J は有限個の $\alpha(1), \ldots, \alpha(s) \in A'$ を選んで $J = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)}\rangle$ と書くことができる．各 i に対し，$(\alpha(i), m_i) \in A$ となる m_i がとれるが，M を m_i の最大値とする．次に，$0 \leq k \leq M-1$ に対し，$k[X]$ のイデアル J_k を次のように構成する．

$$J_k := \langle x^\alpha : \alpha \in A_k\rangle \subset k[X],$$

ただし $A_k = \{\alpha \in \mathbb{Z}_{\geq 0}^n : (\alpha, k) \in A\}$．再び帰納法の仮定から有限個の $\alpha_k(1), \ldots, \alpha_k(s_k) \in A_k$ を選んで $J_k = \langle x^{\alpha_k(1)}, \ldots, x^{\alpha_k(s)}\rangle$ と書くことができる．このとき I は次の I に属する単項式

$$x^{\alpha(i)} y^M (1 \leq i \leq s), \quad x^{\alpha_k(i)} y^k (0 \leq k \leq M-1, 1 \leq i \leq s_k)$$

で生成される．実際，I の単項式 $x^\alpha y^m$ があったとき，$m \geq M$ ならば J の構成より，ある $x^{\alpha(i)} y^M$ で割り切れ，$m < M$ ならば J_k の構成より，ある $x^{\alpha_\ell(i)} y^\ell$ $(\ell \leq m)$ で割り切れる．

さらに上の各生成元たちは I に属するから，ある $x^\alpha y^m$ $((\alpha, m) \in A)$ で割り切れる．その生成元をこの $x^\alpha y^m$ に交換しても，生成するイデアルは小さくならないので，やはり I に等しい．したがって，有限個の $(\alpha, m) \in A$ を選んで，I は $x^\alpha y^m$ たちで生成できることがわかった． □

演習問題

1. $\mathbb{Q}[x, y]$ のイデアルの等式 $\langle 2x^2 + 3y^2 - 11, x^2 - y^2 - 3\rangle = \langle x^2 - 4, y^2 - 1\rangle$ を示せ．

2. イデアル $I \subset k[X]$ に対し，$I = k[X]$ であることと $1 \in I$ であることが同値であることを示せ．

3　単項式順序と割り算アルゴリズム

この章では多項式の割り算を考える．まずは $n = 1$，つまり 1 変数の場合の多項式の割り算を思い出す．

例 3.1. x^2+2x+1 を $2x+1$ で割ることを考える．このとき，

$$\begin{array}{r} \frac{1}{2}x\ +\frac{3}{4} \\ 2x+1\overline{)\ x^2+2x+1} \\ \underline{x^2+\frac{1}{2}x\ \ \ \ } \\ \frac{3}{2}x+1 \\ \underline{\frac{3}{2}x+\frac{3}{4}} \\ \frac{1}{4} \end{array}$$

となるから商が $\frac{1}{2}x+\frac{3}{4}$，余りが $\frac{1}{4}$ となる．つまり $x^2+2x+1=(\frac{1}{2}x+\frac{3}{4})(2x+1)+\frac{1}{4}$ と書き表せる．この筆算の最初のステップは元となる多項式 x^2+2x+1 の最高次の項 x^2 を，割る多項式 $2x+1$ に単項式 $\frac{1}{2}x$ を掛けたものを引くことで消し，次数の下がった多項式を得る．得られた次数の下がった多項式に対して同様のステップを繰り返すことで，最終的に残った多項式の次数が割る多項式の次数より小さくなり，ステップは終了する．

この例のように，多項式 $f,g\in k[x]$ に対し，f を g で割るということは，$f=qg+r$ を満たす，“単純な多項式” $q,r\in k[x]$ を見つけることである．より正確に述べると次の命題が成り立つ．

命題 3.2 (割り算アルゴリズム (1 変数))**.** $g\in k[x]$ をゼロでない多項式とする．このとき，任意の $f\in k[x]$ は

$$f=qg+r$$

と書き表せる．ここで，$q,r\in k[x]$ で，$r=0$ または $\deg(r)<\deg(g)$ が成り立つ．さらに q と r は**一意的**に定まる．

Proof. q と r を求めるアルゴリズムの擬似コードを書くだけに止める.（このアルゴリズムが停止することと，得られた結果が命題を満たすことの証明は省略する）．多項式 $f\in k[x]$ に対し，$\mathrm{LT}(f)$ を f の最高次の項とする．

Input : g, f

Output : q,r

$q:=0$; $r:=f$

WHILE $r\neq 0$ AND $\mathrm{LT}(g)$ が $\mathrm{LT}(r)$ を割り切る DO

　　$q:=q+\mathrm{LT}(r)/\mathrm{LT}(g)$

　　$r:=r-(\mathrm{LT}(r)/\mathrm{LT}(g))\,g$

RETURN q,r

□

それでは変数が増えた場合はどうか．多項式 $f\in k[X]$ を $f_1,\dots,f_s\in k[X]$ で割るというのは，$f=q_1f_1+\cdots+q_sf_s+r$ を満たす，”単純な多項式” $q_1,\dots,q_s,r\in k[X]$ を見つけることである．これを 1 変数の場合のアルゴリズムのように，高い次数を打ち消し合うアルゴリズムを作り行いたい．しかし，1 変数の場合と違って，多変数の場合，多項式内に同じ次数の項が存在する場合がある．例えば，x^2+y^2 の x^2 と y^2 はともに次数 2 の項である．この場合，どっちの項を優先して消せばいいのか，という問題が出てくる．多変数の多項式における割り算を定式化するために，まずは単項式全体に順序を付ける．

定義 3.3. Σ を集合とし,「$\leq$」を Σ 上で定義された二項関係とする．つまりある $\Sigma\times\Sigma$ の部分集合 X が存在して，$(a,b)\in X$ ならば $a\leq b$ と書く．このとき，$\leq$ が Σ 上の**半順序** (partial order) であるとは，以下の 3 条件を満たすときをいう．

1. (**反射律**) 任意の $a\in\Sigma$ に対し，$a\leq a$.

2. (**反対称律**) 任意の $a, b \in \Sigma$ に対し，$a \leq b$ かつ $b \leq a$ ならば $a = b$.

3. (**推移律**) 任意の $a, b, c \in \Sigma$ に対し，$a \leq b$ かつ $b \leq c$ ならば $a \leq c$.

$a \leq b$ かつ $a \neq b$ のときは $a < b$ と書く．さらに任意の $a, b \in \Sigma$ に対し，$a \leq b$ または $b \leq a$ を満たすとき，半順序 $\leq$ は**全順序** (total order) と呼ばれる．

例 3.4. Σ を集合 $\{a, b, c\}$ の冪集合とし，$X \subseteq Y$ ならば $X \leq Y$ と書くことにすると，$\leq$ は Σ 上の半順序である．しかし，全順序ではない．実際，$\{a\}$ と $\{b\}$ は比較不可能である．

定義 3.5. $\mathcal{M}_n$ を $k[X]$ の単項式全体の集合とし，$\leq$ を $\mathcal{M}_n$ 上の全順序とする．このとき，$\leq$ が $k[X]$ の**単項式順序** (monomial order) であるとは，次の 2 条件を満たすときをいう．

1. 任意の単項式 $u \in \mathcal{M}_n$ に対し，$1 \leq u$.

2. 任意の $u, v \in \mathcal{M}_n$ に対し，$u \leq v$ ならば，任意の $w \in \mathcal{M}_n$ に対し $uw \leq vw$.

$x^\alpha \leq x^\beta$ のとき，$\alpha \leq \beta$ と書くこともある．

例を挙げる前に，まずは補題を 2 つ紹介する．

補題 3.6. $\leq$ を $K[X]$ 上の単項式順序とする．このとき，任意の $u, v \in \mathcal{M}_n (u \neq v)$ に対し，u が v を割り切るならば $u < v$ である．

Proof. u が v を割り切ると仮定する．このとき，ある $w \in \mathcal{M}_n$ が存在して，$v = wu$ となる．仮定より，$u \neq v$ であるから，$w \neq 1$ である．すると，単項式順序の定義より $1 < w$ となる．したがって，再び単項式順序の定義より $1 \cdot u < w \cdot u = v$ となり，$u < v$ がわかる． □

補題 3.7. $\leq$ を $k[X]$ の単項式順序とする．このとき，$\leq$ に関する単項式の無限減少列

$$u_0 > u_1 > u_2 > \cdots \qquad (u_i \in \mathcal{M}_n)$$

は存在しない．

Proof. 証明略． □

代表的な単項式順序を 3 つ紹介する．以下，$u = x^\alpha, v = x^\beta$ を単項式とする．

例 3.8 (辞書式順序)**.** u, v に対し，$u <_{\mathrm{lex}} v$ をベクトル $\beta - \alpha$ において最も左にある 0 でない成分が正となる，で定義する．例えば，$v = x_1^2 x_2$ と $u = x_1 x_2 x_3$ を考えると $\beta - \alpha = (2, 1, 0) - (1, 1, 1) = (1, 0, -1)$ なので $x_1^2 x_2 >_{\mathrm{lex}} x_1 x_2 x_3$ である．このとき，$<_{\mathrm{lex}}$ は $k[X]$ の単項式順序となる．さらに，$x_1 >_{\mathrm{lex}} x_2 >_{\mathrm{lex}} \cdots >_{\mathrm{lex}} x_n$ が従う．$x_1, x_2, x_3, \ldots$ の代わりにアルファベット $a, b, c, \ldots$ を使い，$a >_{\mathrm{lex}} b >_{\mathrm{lex}} \cdots >_{\mathrm{lex}} z$ のように順序付けられているとすると，辞書の前にある単語の方が “基本的に”大きくなる．例えば，$arrow >_{\mathrm{lex}} arson$ となる．($aa >_{\mathrm{lex}} a$ なので少し例外はある．)

例 3.9 (次数付き辞書式順序)**.** u, v に対し，$u <_{\mathrm{glex}} v$ を $|\alpha| < |\beta|$，または $|\alpha| = |\beta|$ かつベクトル $\beta - \alpha$ において最も左にある 0 でない成分が正となる，で定義する．例えば，$v = x_1^2 x_2$ と $u = x_1 x_2 x_3^2$ を考えると $x_1^2 x_2 <_{\mathrm{glex}} x_1 x_2 x_3^2$ である．(一方で，$x_1^2 x_2 >_{\mathrm{lex}} x_1 x_2 x_3^2$ である．) このとき，$<_{\mathrm{glex}}$ は $k[X]$ の単項式順序となる．

例 3.10 (次数付き逆辞書式順序)**.** u, v に対し，$u <_{\mathrm{rlex}} v$ を $|\alpha| < |\beta|$，または $|\alpha| = |\beta|$ かつベクトル $\beta - \alpha$ において最も右にある 0 でない成分が負となる，で定義する．$v = x_1^2 x_2$ と $u = x_1 x_2 x_3$ を考えると $\beta - \alpha = (2, 1, 0) - (1, 1, 1) = (1, 0, -1)$ なので $x_1^2 x_2 >_{\mathrm{rlex}} x_1 x_2 x_3$ である．このとき，$<_{\mathrm{rlex}}$ は $k[X]$ の単項式順序となる．

辞書式順序が単項式順序となることの証明を書いておく．(他の順序に関しても，ほぼ同様に証明できる．)

命題 3.11. $\leq_{\mathrm{lex}}$ は単項式順序である．

Proof. 単項式 1 に対応するベクトルは $(0,\ldots,0)$ であるため，任意の $u \in \mathcal{M}_n$ に対し，$1 \leq_{\mathrm{lex}} u$ となることは明らかである．

次に $u, v \in \mathcal{M}_n$ を任意にとり，$u \leq_{\mathrm{lex}} v$ であるとする．このとき，任意の $w = x^\gamma \in \mathcal{M}_n$ に対し，uw と vw を定義に従って比較すると，

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

となるので，$uw \leq_{\mathrm{lex}} vw$ が従う．

以上より $\leq_{\mathrm{lex}}$ は単項式順序である． □

単項式順序に関連していくつか用語を準備する．

定義 3.12. $f = \sum_\alpha a_\alpha x^\alpha \in k[X]$ をゼロでない多項式とし，$<$ を $k[X]$ の単項式順序とする．

1. f の $<$ に関する**多重次数** (multidegree) とは f の中で $<$ に関して最大の項 x^α の指数ベクトル，α のことである．これを $\mathrm{mdeg}(f)$ と書く．
2. f の $<$ に関する**先頭係数** (leading coefficient) とは，$\mathrm{LC}(f) = a_{\mathrm{mdeg}(f)}$ のことである．
3. f の $<$ に関する**先頭単項式** (leading monomial) とは $\mathrm{LM}(f) = x^{\mathrm{mdeg}(f)}$ のことである．
4. f の $<$ に関する**先頭項** (leading term) とは $\mathrm{LT}(f) = \mathrm{LC}(f)\cdot \mathrm{LM(f)}$ のことである．

それでは，多変数の多項式の割り算を定式化する．

定理 3.13 (割り算アルゴリズム (多変数))**.** $k[X]$ の単項式順序 $<$ を 1 つ固定し，$F = (f_1,\ldots,f_s)$ を $k[X]$ の順序付けられた s 個の多項式の組とする．このとき，任意の $f \in k[X]$ は

$$f = q_1 f_1 + \cdots + q_s f_s + r$$

と書ける．ここで，$q_1,\ldots,q_s, r \in k[X]$ で $r = 0$，または $r = \sum_\alpha a_\alpha x^\alpha$ で，どの単項式 $x^\alpha (a_\alpha \neq 0)$ も $\mathrm{LM}(f_1),\ldots,\mathrm{LM}(f_s)$ のいずれでも割り切れない．この r を，f を F で割った**余り** (remainder) と呼ぶ．さらに，もし $q_i f_i \neq 0$ ならば，$\mathrm{LM}(f) \geq \mathrm{LM}(q_i f_i)$ である．

Proof. 1変数の場合と同様に，アルゴリズムの擬似コードを書いて終わりとする．

Input : $f_1, \ldots, f_s,\ f$

Output : $q_1, \ldots, q_s, r$

$q_1 := 0; \ldots; q_s := 0; r := 0$

$p := f$

WHILE $p \neq 0$ DO

  $i := 1$

  divisionoccurred := false

  WHILE $i \leq s$ AND *divisionoccurred* = false DO

    IF $\mathrm{LT}(f_i)$ が $\mathrm{LT}(p)$ を割り切る THEN

      $q_i := q_i + \mathrm{LT}(p)/\mathrm{LT}(f_i)$

      $p := p - (\mathrm{LT}(p)/\mathrm{LT}(f_i))\, f_i$

      divisionoccurred := true

    ELSE

      $i := i + 1$

  IF *divisionoccurred* = false THEN

    $r := r + \mathrm{LT}(p)$

    $p := p - \mathrm{LT}(p)$

RETURN $q_1, \ldots, q_s, r$

□

例 3.14. 割り算アルゴリズムの例として，$f = x^2y + xy^2 + y^2$ を $f_1 = xy - 1$ と $f_2 = y^2 - 1$ で割ろう．ここで単項式順序として $x >_{\mathrm{lex}} y$ となる辞書式順序を考える．このとき，$\mathrm{LT}(f_1) = xy, \mathrm{LT}(f_2) = y^2$ であり，f の中にはこのどちらかで割り切れる項がある．f_1, f_2 と q_1, q_2 を筆算の中で縦に並べて考えると次のようになる．

$$
\begin{array}{rl}
q_1 : & x + y \\
q_2 : & 1
\end{array}
\qquad\qquad
\begin{array}{r}
r \\ \hline
\end{array}
$$

$$
\begin{array}{r|l}
xy - 1 & x^2y + xy^2 + y^2 \\
y^2 - 1 & \underline{x^2y - x} \\
 & \quad xy^2 + x + y^2 \\
 & \quad \underline{xy^2 - y} \\
 & \qquad x + y^2 + y \\
 & \qquad \underline{y^2 - 1} \\
 & \qquad\quad y + 1
\end{array}
\qquad
\begin{array}{rcl}
 & & \\ \hline
 & \longrightarrow & x \\
 & & \\
 & & \\ \hline
 & \longrightarrow & x + y \\
 & \longrightarrow & x + y + 1
\end{array}
$$

この結果より，f は次のように表せる．

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

この余りの項はどれもが $\mathrm{LT}(f_1)$ でも $\mathrm{LT}(f_2)$ でも割り切れない．

このアルゴリズムの残念な点が１つある．それは余りが $f_1, \ldots, f_s$ の順序付けに依存してしまう点である．実際，次の例を見る．

例 3.15. $f_1 = xy - 1, f_2 = y^2 - 1 \in k[x, y]$ とおき，$x >_{\mathrm{lex}} y$ となる辞書式順序を考える．$f = xy^2 - x$ を $F(f_1, f_2)$ で割ると，結果は

$$f = y \cdot (xy - 1) + 0 \cdot (y^2 - 1) + (-x + y)$$

となる．$F = (f_2, f_1)$ に対しては，

$$f = x \cdot (y^2 - 1) + 0 \cdot (xy - 1) + 0$$

となる．したがって，割る多項式の順番によって余りが変わってくる．さらに 2 つ目の割り算の結果から $f \in \langle f_1, f_2 \rangle$ が従うが，1 つ目の割り算の結果からはこのことがわからない．

f の $F = (f_1, \ldots, f_s)$ による割り算を行って，余りが $r = 0$ となったとき，$f \in \langle f_1, \ldots, f_s \rangle$ である．つまり，$r = 0$ は f がイデアルに属するための十分条件である．しかし上の例のように必要条件ではない．イデアル所属問題への応用の点から見てもこの割り算アルゴリズムは不完全である．次の章ではこの問題を改善する．

演習問題

辞書式順序と次数付き辞書式順序で，次の多項式 f の F による割り算を実行し，余りを求めよ．

1. $f = x^2y^2 + xy^2, F = (xy^2 - x, x - y^3)$.
2. $f = xy^2z^2 + xy - yz, F = (x - y^2, y - z^3, z^2 - 1)$.

4　ヒルベルトの基底定理とグレブナー基底

定義 4.1. $I \subset k[X]$ を $\{0\}$ でないイデアルとし，$k[X]$ の単項式順序 $<$ を１つ固定する．

1. $\mathrm{LT}(I)$ をゼロでない元の先頭項全体の集合とする．つまり

   $$\mathrm{LT}(I) = \{\mathrm{LT}(f) : f \in I \setminus \{0\}\}$$

   とする．

2. $\langle \mathrm{LT}(I) \rangle$ で $\mathrm{LT}(I)$ によって生成されるイデアルを表す．これを I の $<$ に関する**先頭項イデアル** (leading term ideal) という．

まずは先頭項イデアルの基本的な性質を挙げる．証明はディクソンの補題などから容易である．

命題 4.2. $I \subset k[X]$ を $\{0\}$ でないイデアルとする．

1. $\langle \mathrm{LT}(I) \rangle$ は単項式イデアルである．
2. $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$ となるように $g_1, \ldots, g_t \in I$ がとれる．

これを用いることですべての多項式イデアルが有限生成であることが証明できる．

定理 4.3 (ヒルベルトの基底定理)**.** すべてのイデアル $I \subset k[X]$ は有限生成である．

Proof. もし $I = \{0\}$ であるならば，生成元の集合を $\{0\}$ ととることができて，有限生成となる．そこで $I \neq \{0\}$ とする．今，$k[X]$ の単項式順序 $<$ を 1 つ固定する．命題 4.2 より $g_1, \ldots, g_t \in I$ を $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$ を満たすようにとることができる．ここで $I = \langle g_1, \ldots, g_t \rangle$ を示す．

$\langle g_1, \ldots, g_t \rangle \subset I$ は明らかである．逆に $f \in I$ を任意の多項式とする．f を $(g_1, \ldots, g_t)$ で割るために，定理 3.13 の割り算アルゴリズムを適用すると，

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

の形が得られる．ここで r のすべての項は $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)$ のいずれでも割り切れない．このとき，$r = 0$ を示す．

$$r = f - q_1 g_1 - \cdots - q_t g_t \in I$$

であることに注意する．もし $r \neq 0$ ならば，

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

であって，補題 2.10 より $\mathrm{LT}(r)$ は $\mathrm{LT}(g_i)$ のいずれかで割り切れなければならない．これは r が余りであることに反しており，$r = 0$ となる．したがって，

$$f = q_1 g_1 + \cdots + q_t g_t + 0 \in \langle g_1, \ldots, g_t \rangle$$

が得られ，$I \subset \langle g_1, \ldots, g_t \rangle$ である．以上より題意が示された． □

ヒルベルトの基底定理の応用を 1 つ紹介する．

定理 4.4 (昇鎖条件 (ACC))**.** $k[X]$ のイデアルの無限昇鎖

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

はある整数 $N \geq 1$ が存在して，

$$I_N = I_{N+1} = I_{N+2} = \cdots$$

となる．

Proof. $I = \bigcup_{i=1}^{\infty} I_i$ とおき，I が $k[X]$ のイデアルとなることを見る．すべての i に対して $0 \in I_i$ であるから $0 \in I$ である．次に，$f, g \in I$ ならば定義により，適当な i と j に対して，$f \in I_i$ かつ $g \in I_j$ である，$k = \max\{i, j\}$ とすると，$f, g \in I_k$ となるので，結局 $f + g \in I_k \subset I$ である．同様に，$f \in I$ かつ $r \in k[X]$ であるならば，適当な i に対し，$f \in I_i$ となり，$r \cdot f \in I_i \subset I$ であるので，I はイデアルとなる．

ヒルベルトの基底定理より $f_1, \ldots, f_s \in I$ が存在して $I = \langle f_1, \ldots, f_s \rangle$ となる．I の定義より各 f_i はどれかの I_j に入る．それを $f_i \in I_{j_i}$ とする．N を j_i のうち最大のものとすると，すべての i に対して $f_i \in I_N$ である．したがって，

$$I = \langle f_1, \ldots, f_s \rangle \subset I_N \subset I_{N+1} \subset \cdots \subset I$$

より，$I = I_N = I_{N+1} = I_{N+2} = \cdots$ を得る． □

実は ACC を仮定するとヒルベルトの基底定理が証明できる．つまり，この 2 つは同値な定理である．この性質を持つ環のことを一般に**ネーター環**という．

さて，先頭項イデアルまで話を戻す．命題 4.2 の (2) から「$g_1, \ldots, g_t$ が I の生成系であれば $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)$ は $\mathrm{LT}(I)$ を生成するか」という問いが自然に考えられる．しかし，これは一般には成り立たない．

例 4.5. $f_1 = x^3 - 2xy, f_2 = x^2 y - 2y^2 + x$ とし，$I = \langle f_1, f_2 \rangle \subset k[x, y]$ とおく．$x >_{\mathrm{glex}} y$ を考える．このとき，

$$x \cdot (x^2 y - 2y^2 + x) - y \cdot (x^3 - 2xy) = x^2$$

より，$x^2 \in I$ である．したがって，$x^2 = \mathrm{LT}(x^2) \in \langle \mathrm{LT}(I) \rangle$ を得る．しかし，x^2 は $\mathrm{LT}(f_1) = x^3$ でも $\mathrm{LT}(f_2) = x^2 y$ でも割り切れないから，補題 2.10 から $x^2 \notin \langle \mathrm{LT}(f_1), \mathrm{LT}(f_2) \rangle$ である．

一方で，定理 4.3 の証明から $\langle \mathrm{LT}(I)\rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)\rangle$ であれば，$I = \langle g_1, \ldots, g_t\rangle$ となる，つまり $g_1, \ldots, g_t$ は I の生成系となることがわかる．この特別な生成系に名前をつける．

定義 4.6. $k[X]$ の単項式順序 $<$ を 1 つ固定する．$\{0\}$ でないイデアル $I \subset k[X]$ の有限部分集合 $G = \{g_1, \ldots, g_t\}$ が $<$ に関する**グレブナー基底**[2](Gröbner basis) であるとは，

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

を満たすときにいう．また便宜上 $\langle \emptyset\rangle = \{0\}$ することで，空集合はゼロイデアルのグレブナー基底であると定義する．

定理 4.3 の証明からわかることを述べておく．

命題 4.7. $k[X]$ の単項式順序 $<$ を 1 つ固定する．すべてのイデアル $I \subset k[X]$ は $<$ に関するグレブナー基底を持つ．さらに，I のどんなグレブナー基底も I の生成系となる．

先ほど述べたように，グレブナー基底はイデアルの特別な生成系である．これを用いて不完全であった割り算アルゴリズムを完全なものにし，イデアル所属問題を完全に解決することができる．

命題 4.8 (余りの一意性)**.** $I \subset k[X]$ をイデアルとし，$G = \{g_1, \ldots, g_t\}$ を $k[X]$ のある単項式順序に関する I のグレブナー基底とする．このとき，与えられた $f \in k[X]$ に対して，次の 2 つの条件を満たす多項式 $r \in k[X]$ がただ一つ存在する．

1. r のどの項も $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)$ のどれでも割れない．
2. $f = g + r$ となる $g \in I$ が存在する．

特に，グレブナー基底 G による割り算の余りは，G の元の順番によらない．

Proof. r の存在は $(g_1, \ldots, g_t)$ による割り算を実行すれば良い．一意性を示す．$f = g + r = g' + r'$ が (1) と (2) を満たすとする．このとき，$r - r' = g' - g \in I$ であるので，$r \neq r'$ ならば $\mathrm{LT}(r - r') \in \langle \mathrm{LT}(I)\rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)\rangle$ となる．従って補題 2.10 より，$\mathrm{LT}(r - r')$ は $\mathrm{LT}(g_i)$ のいずれかで割り切れる．しかし，(1) よりこれはあり得ない．したがって $r = r'$ となり一意性は示された． □

注意 4.9. 実は，グレブナー基底による割り算の余りは，グレブナー基底の取り方によらない．したがって，単項式順序を 1 つ固定すると，“イデアル I による f の割り算の余り”を一意に定義することができる．

グレブナー基底により，割り算の余りが一意に定まることがわかったので，これを用いてイデアル所属問題が解決できる．

系 4.10. $I \subset k[X]$ をイデアルとし，$G = \{g_1, \ldots, g_t\}$ を $k[X]$ のある単項式順序に関する I のグレブナー基底とする．このとき，$f \in k[X]$ に対して，$f \in I$ と f を G で割った時の余りがゼロであることは同値である．

Proof. 余りがゼロである時には，$f \in I$ であることはすでに見た．逆に $f \in I$ が与えられた時，$f = f + 0$ は命題 4.8 の 2 つの条件を満たす．これより，0 は f を G で割った余りであることが従う． □

ここまでの議論はイデアルのグレブナー基底 G がすでにわかっているという前提で進んでいる．したがってイデアル I と単項式順序 $<$ が与えられた時，I の $<$ に関するグレブナー基底がいつもでも見つけることができるか，ということが重要な問題となる．次の章で，I の生成系がグレブナー基底となるかどうかの判定法，そしてそれを用いて勝手な生成系からグレブナー基底を見つけるアルゴリズムを紹介する．

[2] グレブナー基底はブッフバーガー（B. Buchberger）の博士論文の中で導入された．その際，彼の指導教員であるグレブナー（W. Gröbner）に敬意を表して，グレブナー基底と名付けた．また同時期に広中平祐によっても同様の概念が定義された．

演習問題

1. $g_1 = xy^2 - xz + y, g_2 = xy - z^2, g_3 = x - yz^4$ とおき，$I = \langle g_1, g_2, g_3 \rangle \subset k[x, y, z]$ とする．$x >_{\text{lex}} y >_{\text{lex}} z$ に対して，$\mathrm{LT}(g) \notin \langle \mathrm{LT}(g_1), \mathrm{LT}(g_2), \mathrm{LT}(g_3) \rangle$ となる $g \in I$ の例を挙げよ．ヒント：先頭項同士を打ち消し合うことで得られる多項式を考えよ．

2. $g_1 = x + z, g_2 = y - z$ とおき，$I = \langle g_1, g_2 \rangle \subset k[x, y]$ とする．このとき，$\{g_1, g_2\}$ は $x >_{\text{lex}} y$ に関する I のグレブナー基底となっている．$f = x^2 + y^2 - 2z^2$ が I に属するかどうか判定せよ．

5　ブッフバーガー判定法とブッフバーガーアルゴリズム

以降，特別な場合を除き，$k[X]$ の単項式順序を一つ固定する．

定義 5.1.　1. 2つの単項式 x^α, x^β に対し，各 i に対して，$\gamma_i = \max(\alpha_i, \beta_i)$ と書き，$\gamma = (\gamma_1, \ldots, \gamma_n)$ とおく．この x^γ を x^α と x^β の**最小公倍元** (least common multiple) と呼び，$x^\gamma = \mathrm{lcm}(x^\alpha, x^\beta)$ と書く．

2. ゼロでない多項式 $f, g \in k[X]$ の S **多項式** (S-polynomial) とは，$x^\gamma = \mathrm{lcm}(\mathrm{LM}(f), \mathrm{LM}(g))$ としたとき，
$$S(f, g) = \frac{x^\gamma}{\mathrm{LT}(f)} \cdot f - \frac{x^\gamma}{\mathrm{LT}(g)} \cdot g$$
で与えられる多項式である．（先頭項を打ち消していることに注意せよ．）定義から $S(f, g) \in \langle f, g \rangle$ がわかる．

例 5.2. $f = x^3y^2 - x^2y^3 + x$ と $g = 3x^4y + y^2$ に対し，$x >_{\text{glex}} y$ の場合を考える．このとき，$\mathrm{LM}(f) = x^3y^2$ と $\mathrm{LM}(g) = x^4$ なので，$\gamma = (4, 2)$ であって，
$$\begin{aligned} S(f, g) &= \frac{x^4y^2}{x^3y^2} \cdot f - \frac{x^4y^2}{3x^4y} \cdot g \\ &= x \cdot f - (1/3) \cdot y \cdot g \\ &= -x^3y^3 + x^2 - (1/3)y^3 \end{aligned}$$
となる．

補題 5.3. $f_1, \ldots, f_s \in k[X]$ がすべて同じ多重次数 $\delta \in \mathbb{Z}^n_{\geq 0}$ をもつとする．このとき，次が成立する．

1. $S(f_i, f_j)$ の多重次数は δ より真に小さい．

2. $f_1 + \cdots + f_s$ の多重次数が δ より真に小さいならば，$f_1 + \cdots + f_s$ は $S(f_i, f_j)$ $(1 \leq i, j \leq s)$ の k 係数の線型結合である．

Proof. $d_i = \mathrm{LC}(f_i)$ とする．すると，$\mathrm{LT}(f_i) = d_i x^\delta$ である．$\mathrm{LM}(f_i) = \mathrm{LM}(f_j)$ から
$$S(f_i, f_j) = \frac{1}{d_i} f_i - \frac{1}{d_j} f_j$$
と変形できる．ここから 1 つ目の主張が容易にわかる．

$f_1 + \cdots + f_s$ の多重次数が δ より真に小さいと仮定する．このとき，仮定より，$d_1 + \cdots + d_s = 0$ であることがわかる．さらに
$$\begin{aligned} \sum_{i=1}^{s-1} d_i S(f_i, f_s) &= d_1 \left(\frac{1}{d_1} f_1 - \frac{1}{d_s} f_s \right) + \cdots + d_{s-1} \left(\frac{1}{d_{s-1}} f_{s-1} - \frac{1}{d_s} f_s \right) \\ &= f_1 + \cdots + f_{s-1} - \frac{1}{d_s}(d_1 + \cdots + d_{s-1}) f_s \end{aligned}$$

が成りたつ．しかし，$d_1+\cdots+d_s=0$ より，$d_1+\cdots+d_{s-1}=-d_s$ であるから，これは

$$\sum_{i=1}^{s-1} d_i S(f_i,f_s) = f_1+\cdots+f_{s-1}+f_s$$

と変形できる．これで 2 つ目の主張が示せた． □

補題 5.4. $f,g\in k[X]$ とし，$\mathrm{LM}(f)=x^\alpha,\mathrm{LM}(g)=x^\beta,x^\gamma=\mathrm{lcm}(x^\alpha,x^\beta)$ とする．x^δ が x^γ で割り切れるとき，

$$S(x^{\delta-\alpha}f,x^{\delta-\beta}g)=x^{\delta-\gamma}S(f,g)$$

である．

Proof. $\mathrm{LM}(x^{\delta-\alpha}f)=x^{\delta-\alpha}\mathrm{LM}(f)=x^\delta$ かつ $\mathrm{LM}(x^{\delta-\beta}g)=x^{\delta-\beta}\mathrm{LM}(g)=x^\delta$ より，

$$\mathrm{lcm}(\mathrm{LM}(x^{\delta-\alpha}f),\mathrm{LM}(x^{\delta-\beta}g))=x^\delta$$

である．したがって，

$$\begin{aligned}
S(x^{\delta-\alpha}f,x^{\delta-\beta}g) &= \frac{x^\delta}{\mathrm{LT}(x^{\delta-\alpha}f)}\cdot x^{\delta-\alpha}f-\frac{x^\delta}{\mathrm{LT}(x^{\delta-\beta}g)}\cdot x^{\delta-\beta}g\\
&= \frac{x^\delta}{x^{\delta-\alpha}\mathrm{LT}(f)}\cdot x^{\delta-\alpha}f-\frac{x^\delta}{x^{\delta-\beta}\mathrm{LT}(g)}\cdot x^{\delta-\beta}g\\
&= x^{\delta-\gamma}\left(\frac{x^\gamma}{\mathrm{LT}(f)}\cdot f-\frac{x^\gamma}{\mathrm{LT}(g)}\cdot g\right)\\
&= x^{\delta-\gamma}S(f,g).
\end{aligned}$$

□

定理 5.5 (ブッフバーガーの判定条件)**.** I をゼロでない $k[X]$ のイデアルとし，$k[X]$ の単項式順序を一つ固定する．I の生成系 $G=\{g_1,\ldots,g_t\}$ が I のグレブナー基底である必要十分条件は，任意の異なる i,j に対して $S(g_i,g_j)$ を（なんらかの順序が入った）G で割った余りが 0 であることである．

Proof. （十分性）G がグレブナー基底とする．$S(g_i,g_j)\in I$ であるので，系 4.10 から $S(g_i,g_j)$ を G で割った余りは 0 である．

（必要性）任意の $S(g_i,g_j)$ を（なんらかの順序が入った）G で割った余りが 0 であるとする．$0\neq f\in I$ をとると，$f=\sum_i h_ig_i$ $(h_i\in k[X])$ と書けるが，$\mathrm{LM}(f)\le\max_i\{\mathrm{LM}(h_ig_i)\}$ である．もし，等号が成立するならば，ある i に対して，$\mathrm{LM}(f)=\mathrm{LM}(h_ig_i)$ となるので，$\mathrm{LT}(f)\in\langle\mathrm{LT}(g_1),\ldots,\mathrm{LT}(g_t)\rangle$ がいえる．この場合，G がグレブナー基底であることが従う．

等号が成り立たないと仮定する．単項式順序の定義から任意の単項式の集合は極小元を持つことに注意すると，$f=\sum_i h_ig_i$ の書き方は一意的ではないが，そのような書き方のうちから多重次数 $\max_i\{\mathrm{mdeg}(h_ig_i)\}$ が最小となるようにとれる．その最小にとった多重次数を δ とする．このとき，

$$f=\sum_{\mathrm{mdeg}(h_ig_i)=\delta}\mathrm{LT}(h_i)g_i+\sum_{\mathrm{mdeg}(h_ig_i)=\delta}(h_i-\mathrm{LT}(h_i))g_i+\sum_{\mathrm{mdeg}(h_ig_i)<\delta}h_ig_i \tag{1}$$

と変形できる．この，第 2 項，第 3 項の $\sum$ 記号の中に現れる単項式は，すべて多重次数が δ より小さい．さらに $\mathrm{mdeg}(f)<\delta$ より，第 1 項の $\sum$ 記号の項もまた多重次数が δ より真に小さい．この第 1 項に注目すると，これは補題 5.3 の (2) の条件を満たしているので，

$$(\text{第 1 項})=\sum_{i,j}c_{i,j}S(\mathrm{LT}(h_i)g_i,\mathrm{LT}(h_j)g_j)\quad(c_{i,j}\in k)$$

と書くことができる．さらに，$x^{\gamma_{i,j}}=\mathrm{lcm}(\mathrm{LM}(g_i),\mathrm{LM}(g_j))$ とおくことで，補題 5.4 を使い，

$$(\text{第 1 項})=\sum_{i,j}c_{i,j}x^{\delta-\gamma_{i,j}}S(g_i,g_j)$$

となる．仮定から，$S(g_i, g_j)$ を G で割った余りは 0 となるので，$a_{i,j,\ell} \in k[X]$ を用いて

$$(\text{第}1\text{項}) = \sum_{i,j} c_{i,j} x^{\delta-\gamma_{i,j}} \left(\sum_i a_{i,j,\ell} g_\ell \right) = \sum_\ell \left(\sum_{i,j} c_{i,j} x^{\delta-\gamma_{i,j}} a_{i,j,\ell} \right) g_\ell \tag{2}$$

と表せる．ここで割り算アルゴリズムから $\mathrm{mdeg}(a_{i,j,\ell} g_\ell) \leq \mathrm{mdeg}(S(g_i, g_j))$ だから，S 多項式の定義からわかる $\mathrm{mdeg}(S(g_i, g_j)) < \gamma_{i,j}$ と合わせると

$$\mathrm{mdeg}\left(\left(\sum_{i,j} c_{i,j} x^{\delta-\gamma_{i,j}} a_{i,j,\ell} \right) g_\ell \right) \leq \mathrm{mdeg}(x^{\delta-\gamma_{i,j}} S(g_i, g_j)) < \delta$$

したがって，これを元の式 (1) に式 (2) を代入し，g_ℓ の多項式係数の結合 $f = \sum_\ell h'_\ell g_\ell$ として見ると，$\mathrm{mdeg}(h'_\ell g_\ell < \delta$ となり，δ の最小性に矛盾する．以上で証明が完了する． □

この判定を使い，任意の生成系からグレブナー基底を構成することができるアルゴリズムが次の定理である．

定理 5.6 (ブッフバーガーアルゴリズム)**.** $I = \langle f_1, \ldots, f_s \rangle \subset k[X]$ をゼロでないイデアルとする，I のグレブナー基底は，次のアルゴリズムによって，有限回のステップで構成することができる．

Input : $F = (f_1, \ldots, f_s)$
Output : I のグレブナー基底 $G = (g_1, \ldots, g_t)$

$G := F$
REPEAT
　　$G' := G$
　　FOR G' の異なる 2 つの多項式 p, q DO
　　$r := S(p, q)$ を G' で割ったときの余り
　　IF $r \neq 0$ THEN $G := G \cup \{r\}$
UNTIL $G = G'$
RETURN G

Proof. アルゴリズムの最初に $I = \langle G \rangle$ であり，繰り返しの各段階で，G に追加される多項式はその時点での $\langle G \rangle$ の元だから，常に $I = \langle G \rangle$ である．また，アルゴリズムが停止すれば定理 5.5 から G は I のグレブナー基底となる．

あとはアルゴリズムが停止することをいえばよい．繰り返しの段階で G に属さない元 r が追加されたとすると，割り算の性質より，$\mathrm{LT}(r)$ は $\mathrm{LT}(G)$ のどの元でも割り切れない．よって $\langle \mathrm{LT}(G) \rangle \subsetneq \langle \mathrm{LT}(G \cup \{r\}) \rangle$ である．よって，アルゴリズムが動いているうちは，$\langle \mathrm{LT}(G) \rangle$ たちがイデアルの真の上昇列をなすため，ACC よりアルゴリズムは停止する． □

例 5.7. では実際，イデアルのある生成系からグレブナー基底を構成してみよう．$f_1 = x^3 - 2xy, f_2 = x^2 y - 2y^2 + x, I = \langle f_1, f_2 \rangle \subset k[x, y]$ とし，I の次数付き逆辞書式順序 $x >_{\mathrm{rlex}} y$ に関するグレブナー基底を求める．まず $G = (f_1, f_2)$ とし，$S(f_1, f_2) = y \cdot f_1 - x \cdot f_2 = -x^2$ なので，これを G で割ったときの余りは $-x^2$ でこれは 0 ではない．つまり $\{f_1, f_2\}$ は I のグレブナー基底ではない．そこで，この余り $f_3 = -x^2$ を新しい生成元として G に加える．つまり $G = (f_1, f_2, f_3)$ である．すると $S(f_1, f_2)$ を G で割った余りは 0 になる．次に $S(f_1, f_3)$ で同じことを考えると，$S(f_1, f_3) = -2xy$ で，これを G で割っても余りは $-2xy$ で 0 でない．そこで，さらに $f_4 = -2xy$ を G に加えると，$S(f_1, f_3)$ を G で割った余りは 0 となる．次に $S(f_2, f_3)$ を考えると，$S(f_2, f_3) = -2y^2 + x$ で，これを G で割った余りは $-2y^2 + x$ で 0 でない．$f_5 = -2y^2 + x$ と

して G に加えると，$S(f_2, f_3)$ を G で割った余りは 0 となる．特に，どの $S(f_i, f_j)$（$1 \leq i < j \leq 5$）も G で割ったときの余りは 0 である．したがって，

$$\{f_1, f_2, f_3, f_4, f_5\} = \{x^3 - 2xy, x^2y - 2y^2 + x, -x^2, -2xy, -2y^2 + x\}$$

は I の $>_{\mathrm{rlex}}$ に関するグレブナー基底となる．

演習問題

次のイデアル $I \subset k[x, y]$ に対して，I の $x >_{\mathrm{lex}} y$ に関するグレブナー基底を（１つ）求めよ．

1. $I = \langle x + y, x^2 + y^2 \rangle$
2. $I = \langle xy, x^2 + y^2 \rangle$

6　被約グレブナー基底と判定法の改良

ブッフバーガーアルゴリズムを実行すると，多項式がたくさん増えていく．その際，余計な多項式が含まれる場合がある．つまり，取り除いてもグレブナー基底となるような多項式が存在する場合がある．そのため，なるべく余計な多項式を取り除くことを考える．

定義 6.1. 次の２条件を満たすグレブナー基底 G を，**極小グレブナー基底** (minimal Gröbner basis) と呼ぶ：

1. すべての $p \in G$ の先頭係数は 1 である．
2. すべての $p \in G$ に対して，$\mathrm{LT}(p) \notin \langle \mathrm{LT}(G \setminus \{p\}) \rangle$ である．

あるグレブナー基底が (2) の条件を満たさないならば，その p を取り除いても依然としてグレブナー基底である．こうして取り去っていくと，最後には極小グレブナー基底に辿り着くので，極小グレブナー基底は存在する．しかし，一般に極小グレブナー基底は一意ではない．

例 6.2. $f_1 = x^3 - 2xy, f_2 = x^2y - 2y^2 + x, I = \langle f_1, f_2 \rangle \subset k[x, y]$ とし，さらに，$f_3 = -x^2, f_4 = -2xy, f_5 = -2y^2 + x$ とおく．このとき，$\{f_1, f_2, f_3, f_4, f_5\}$ は I の次数付き逆辞書式順序 $x >_{\mathrm{rlex}} y$ に関するグレブナー基底であった．ここから極小グレブナー基底を求める．まずゼロでない定数をかけてもグレブナー基底であることは変わらないので，$f_3' = x^2, f_4' = xy, f_5' = y^2 - \frac{1}{2}x$ として取り替える．今，$\mathrm{LT}(f_1) = x^3 = x \cdot \mathrm{LT}(f_3')$ であるので，f_1 を取り除いてもグレブナー基底であることは変わらない．同様に，$\mathrm{LT}(f_2) = x^2y = y \cdot \mathrm{LT}(f_3')$ より，f_2 も取り除ける．こうして残った $\{f_3', f_4', f_5'\}$ は条件 (1) と (2) を満たすので，これが I の極小グレブナー基底となっている．一方，適当な定数 $a \in k$ を用いて，$\tilde{f}_3 = x^2 + axy$ とおくと，$\{\tilde{f}_3, f_4', f_5'\}$ も I の極小グレブナー基底となることは簡単に確かめられる．つまり，極小グレブナー基底を無限個作ることが可能となる．

極小グレブナー基底の中で，最も良いもの，つまり，一意に定まるようなものはないか考える．

定義 6.3. 次の２条件を満たすグレブナー基底 G を**被約グレブナー基底** (reduced Gröbner basis) と呼ぶ：

1. すべての $p \in G$ の先頭係数は 1 である．
2. すべての $p \in G$ に対して，p のどの単項式も $\langle \mathrm{LT}(G \setminus \{p\}) \rangle$ に属さない．

定理 6.4. $I \subset k[X]$ をゼロでないイデアルとする．与えられた単項式順序に関して，I は被約グレブナー基底を持ち，被約グレブナー基底は唯一に定まる．

Proof. まずは存在を証明する．極小な I のグレブナー基底 $G = \{g_1, \ldots, g_t\}$ をとる．g_1' を g_1 を $G \setminus \{g_1\}$ で割った余りとし，$G_1 = \{g_1', g_2, \ldots, g_t\}$ とする．極小性より $\mathrm{LT}(g_1) = \mathrm{LT}(g_1')$ である．実際，$\mathrm{LT}(g_1)$ は $\mathrm{LT}(G \setminus \{g_1\})$ のいずれでも割り切れないので，割り算アルゴリズムでは余りに行くからである．よって G_1 は極小グレブナー基底となる．次に g_2' を g_2 を $G_1 \setminus \{g_2\}$ で割った余りとし，$G_2 = \{g_1', g_2', g_3, \ldots, g_t\}$ とすると，G_2 は極小グレブナー基底となる．これを続けていき，g_t' と G_t まで定めると，$\mathrm{LT}(g_i) = \mathrm{LT}(g_i')$ かつ G_i はすべて極小グレブナー基底である．$\mathrm{LT}(G_i) = \mathrm{LT}(G_t)$ と g_i' が余りであることから，G_t は被約グレブナー基底となる．

次に一意性を証明する．G と G' をともに被約グレブナー基底とする．このとき，G と G' は極小グレブナー基底となるので，$\mathrm{LT}(G) = \mathrm{LT}(G')$ である．したがって，$g \in G$ を与えたとき，$\mathrm{LT}(g) = \mathrm{LT}(g')$ となる $g' \in G'$ が存在するが，このとき $g = g'$ を証明すれば一意性が従う．今，$g - g' \in I$ を考える．G がグレブナー基底であるので，$g - g'$ は G で割り切れる．しかし，$\mathrm{LT}(g) = \mathrm{LT}(g')$ であるからこの項は $g - g'$ の中で打ち消しあっている．したがって G と G' が被約グレブナー基底であるので，残っている項は $\mathrm{LT}(G) = \mathrm{LT}(G')$ のどの項でも割り切れない．これは，$g - g'$ の G による割り算の余りが $g - g'$ 自身であることを意味している．つまり $g - g' = 0$ となり証明が完了する． □

例 6.5. 先ほどの例を考える．実は，$\{f_3', f_4', f_5'\}$ は I の被約グレブナー基底である．一方，$\tilde{f}_3$ 単項式 xy が (2) の条件を満たなさいので，$a \neq 0$ であれば，$\{\tilde{f}_3, f_4', f_5'\}$ は I の被約グレブナー基底ではない．

被約グレブナー基底の一意性の応用として 2 つのイデアルが一致するかの判定ができる．

系 6.6. 2 つの $k[X]$ のイデアル I と J が一致する必要十分条件は，I と J がある，特にすべての単項式順序に関する同じ被約グレブナー基底を持つことである．

この系を使って，$k = \mathbb{C}$ のとき，多項式の連立方程式が解を持たないことをグレブナー基底を用いて判定できる．そのために必要な結果の事実だけを紹介する．

定理 6.7 (ヒルベルトの弱零点定理)**.** $k = \mathbb{C}$ とする．(もっと一般に k を代数的閉体としてもよい.) イデアル $I \subset k[X]$ に対し，$\mathbf{V}(I) = \emptyset$ となることと，$I = k[X]$ となることは同値である．

この結果が $k = \mathbb{R}$ で成り立たないことは，$I = \langle x^2 + 1 \rangle$ を考えればわかる．その場合でも，$I = k[X]$ であれば，$\mathbf{V}(I) = \emptyset$ であることは従う．

系 6.8. $k = \mathbb{C}$ とする．イデアル $I \subset k[X]$ に対し，$\mathbf{V}(I) = \emptyset$ となることと，I がある，特にすべての単項式順序に関して $\{1\}$ を被約グレブナー基底に持つことは同値である．

$k = \mathbb{C}$ でなくても，I が $\{1\}$ を被約グレブナー基底に持てば，$\mathbf{V}(I) = \emptyset$ となることは従う．

次にブッフバーガーアルゴリズムの改良を考える．まず，余りがゼロであることの意味についてもっと一般的な見方を与える必要がある．

定義 6.9. 単項式順序を固定し，$G = \{g_1, \ldots, g_t\} \subset k[X]$ とする．与えられた $f \in k[X]$ に対して，f が**標準表現** (standard representation)

$$f = A_1 g_1 + \cdots + A_t g_t, \quad A_i \in k[X]$$

(ただし，$A_i g_i \neq 0$ である限り，いつでも

$$\mathrm{mdeg}(f) \geq \mathrm{mdeg}(A_i g_i)$$

を満たす）を持つとき，f は G を**法としてゼロに簡約される**といい，これを

$$f \to_G 0$$

と書く．

割り算アルゴリズムと余りが一意でなかった例から次のことがわかる．

補題 6.10. $G = (g_1, \ldots, g_t)$ を $k[X]$ の順序集合とし，$f \in k[X]$ を固定する．このとき，f を G で割った余りが 0 であるならば，$f \to_G 0$ である．しかし，この逆は一般に成り立たない．

従って，$f \to_G 0$ は f を G で割った時の余りが 0 となることの一般化となっている．これを使い，ブッフバーガー判定条件を一般化できる．

定理 6.11. イデアル I の基底 $G = \{g_1, \ldots, g_t\}$ がグレブナー基底であることと，$S(g_i, g_j) \to_G 0$ がすべての $i \neq j$ で成り立つことは同値である．

Proof. G がグレブナー基底のとき，$S(g_i, g_j)$ の G による割り算の余りは 0 となり，補題 6.10 より $S(g_i, g_j) \to_G 0$ が従う．逆の証明は，定理 5.5 の証明では，

$$S(g_i, g_j) = \sum_{\ell=1}^{t} A_\ell g_\ell$$

が $A_\ell g_\ell \neq 0$ のとき，

$$\mathrm{mdeg}(A_\ell g_\ell) \leq \mathrm{mdeg}(S(g_i, g_j))$$

を満たすということしか使っていないので，これが $S(g_i, g_j) \to_G 0$ を意味するので，定理が従う． □

この一般化した判定法を使って，アルゴリズムの中で $S(g_i, g_j) \to_G 0$ となる S 多項式は**調べなくてよい**ことが証明できる．しかし，割り算の余りは一意的ではなかったので，$S(g_i, g_j) \to_G 0$ を判定するアルゴリズムは少し工夫が必要なので，今回は，$S(g_i, g_j) \to_G 0$ となる g_i, g_j の十分条件を証明し，アルゴリズムに組み込むことにする．

まず，次の命題は明らかである．

命題 6.12. $f \in k[X]$ を $G = (g_1, \ldots, g_t)$ で割ったときの余りが $r \neq 0$ のとき，$G' = (g_1, \ldots, g_t, r)$ とすると，$f \to_{G'} 0$ である．

この命題から一度チェックした S 多項式は，(必要ならば余りを追加することで）再びチェックする必要はない．これだけでもだいぶ計算を減らすことができる．次の命題も極めて有効である．

命題 6.13. ゼロでない多項式 $f, g \in k[X]$ に対して，f, g の先頭単項式が互いに素，つまり $\mathrm{lcm}(\mathrm{LM}(f), \mathrm{LM}(g)) = \mathrm{LM}(f) \cdot \mathrm{LM}(g)$ となるとき，$S(f, g) \to_{\{f,g\}} 0$ である．

Proof. 適当な定数をかけることで，$\mathrm{LC}(f) = \mathrm{LC}(g) = 1$ としてよい．$f = \mathrm{LM}(f) + p, g = \mathrm{LM}(g) + q$ と書く．このとき，

$$\begin{aligned} S(f, g) &= \mathrm{LM}(g) \cdot f - \mathrm{LM}(f) \cdot g \\ &= (g - q) \cdot f - (f - p) \cdot g \\ &= g \cdot f - q \cdot f - f \cdot g + p \cdot g \\ &= p \cdot g - q \cdot f \end{aligned}$$

と表せる．今，$\mathrm{LT}(pg) = \mathrm{LT}(qf)$ を仮定する．このとき，

$$\mathrm{LM}(p) \cdot \mathrm{LM}(g) = \mathrm{LM}(q) \cdot \mathrm{LM}(f)$$

が従う．よって $\mathrm{LM}(f)$ と $\mathrm{LM}(g)$ は互いに素から $\mathrm{LM}(q)$ は $\mathrm{LM}(g)$ で割り切れる．しかし，$\mathrm{LM}(g) > \mathrm{LM}(q)$ に矛盾する．したがって，$\mathrm{LT}(p \cdot g) \neq \mathrm{LT}(q \cdot f)$ である．これから，

$$\mathrm{mdeg}(S(f, g)) = \mathrm{mdeg}(p \cdot g - q \cdot f) = \max(\mathrm{mdeg}(p \cdot g), \mathrm{mdeg}(q \cdot f))$$

となる．以上より，$S(f, g) \to_{\{f,g\}} 0$ を得る． □

この命題からすぐわかる事実を書いておく．

系 6.14. $I = \langle f_1, \ldots, f_s \rangle \subset k[X]$ をゼロでないイデアルとする．全ての $i \neq j$ に対し，f_i と f_j の先頭単項式が互いに素であれば，$\{f_1, \ldots, f_s\}$ は I のグレブナー基底である．

6.1 演習問題

1. イデアル $I = \langle x+y, x^2+y^2 \rangle$ の $x >_{\text{lex}} y$ に関する被約グレブナー基底を求めよ．
2. イデアル $I = \langle x^2+y+z-1, x+y^2+z-1, x+y+z^2-1 \rangle \subset k[x,y,z]$ に対し，好きな単項式順序を一つ決め，その順序に関する I のグレブナー基底を求めよ．

7 消去定理と拡張定理

この章では，本講義の目的であった多項式の連立方程式 $f_1 = \cdots = f_s = 0$ の解法を考える．1 変数の代数方程式は 5 次以上だと解の公式がないため，一般に多項式の連立方程式は厳密解を求めることができない場合があることに注意する．連立 1 次方程式では，方程式を組み合わせて変数を減らしていき，変数の少ない連立方程式を先に解くことで解を求めていった．これは結局，イデアル $\langle f_1, \ldots, f_s \rangle$ に属する簡単な式を探すことに相当する．この方法を一つ紹介する．非負整数 ℓ に対し，$k[X]_\ell = k[x_{\ell+1}, \ldots, x_\ell]$ とする．ここで $k[X]_0 = k[X]$ である．

定義 7.1. $k[X]$ のイデアル $I = \langle f_1, \ldots, f_s \rangle$ に対して，ℓ 次**消去イデアル** (elimination ideal) を

$$I_\ell = I \cap k[X]_\ell$$

で定める．つまり，I に属する多項式のうち，最初の ℓ 変数を含まないもの全体のなす集合である．このとき，I_ℓ は $k[X]_\ell$ のイデアルである（証明は省略する）．また，$I_0 = I$ である．

定理 7.2 (消去定理 (Elimination Theorem))**.** $k[X]$ のイデアル I の辞書式順序に関するグレブナー基底を $G = \{g_1, \ldots, g_s\}$ とすると，$0 \le \ell \le n$ に対して，

$$G_\ell = G \cap k[X]_\ell$$

は ℓ 次消去イデアル I_ℓ のグレブナー基底（特に生成系）である．

Proof. ℓ を 0 から n の間で固定する．構成の仕方から，$G_\ell \subset I_\ell$ であるので，グレブナー基底の定義より，

$$\langle \mathrm{LT}(I_\ell) \rangle = \langle \mathrm{LT}(G_\ell) \rangle$$

を証明すればよい．$\supset$ は明らかなので，逆の包含関係を示す．

$f \in I_\ell \subset I$ とする．G が I のグレブナー基底であるので，$\mathrm{LT}(f)$ は適当な $g \in G$ をとれば $\mathrm{LT}(g)$ で割り切れる．$f \in I_\ell$ であるから，これは $\mathrm{LT}(g)$ が変数 $x_{\ell+1}, \ldots, x_n$ だけを含むことを意味する．ここで辞書式順序を用いているので，$x_1, \ldots, x_\ell$ を含む単項式は $k[X]_\ell$ のすべての単項式よりも大きい．したがって $\mathrm{LT}(g) \in k[X]_\ell$ より $g \in k[X]_\ell$ が導かれる．これは $g \in G_\ell$ を示している．よって，$\mathrm{LT}(f)$ は $\mathrm{LT}(G_\ell)$ の単項式のいずれかで割り切れるということになり，$\mathrm{LT}(f) \in \langle \mathrm{LT}(G_\ell) \rangle$ が従い，定理が証明できた． □

注意 7.3. $1 \le \ell \le n$ の中の整数 ℓ を 1 つ固定する．変数 $x_1, \ldots, x_\ell$ を少なくとも 1 つは含む単項式が $k[X]_\ell$ のすべての単項式より大きいとき，単項式順序 $<$ を ℓ **消去タイプ**と呼ぶ．定理 6.2 の証明では辞書式順序のこの性質しか使っていないので，次のように一般化できる：I が $k[X]$ のイデアルで，G が I の ℓ 消去タイプの順序に関するグレブナー基底とする．ことのき，$G \cap k[X]_\ell$ は ℓ 次消去イデアル $I \cap k[X]_\ell$ のグレブナー基底である．辞書式順序は任意の $1 \le \ell \le n$ に対して，ℓ 消去タイプである．

消去定理が何を意味するかというと，イデアルの中で，変数 $x_1, \ldots, x_\ell$ を含まない多項式が存在すれば，それは辞書式順序に関するグレブナー基底の中で見つけることができる（変数の打ち消しが起こる），ということである．これを例で確認してみる．

例 7.4. 連立方程式

$$\begin{aligned} f_1 &= xy + z^2 - 2 = 0 \\ f_2 &= x^2 - yz = 0 \\ f_3 &= xz - y^2 = 0 \end{aligned}$$

を解いてみる．$I = \langle f_1, f_2, f_3 \rangle \subset \mathbb{C}[x, y, z]$ とおくと，I の辞書式順序 $<_{\text{lex}}$ に関するグレブナー基底として，

$$\begin{aligned} g_1 &= z^4 - 3z^2 + 2 = (z-1)(z+1)(z^2-2) \\ g_2 &= yz^2 - y = y(z-1)(z+1) \\ g_3 &= y^3 + z^3 - 2z = y^3 + z(z^2-2) \\ g_4 &= x - y^2 z \end{aligned} \tag{3}$$

がとれる．$\{g_1, g_2, g_3, g_4\}$ は I の生成系なので，$\mathbf{V}(f_1, f_2, f_3) = \mathbf{V}(g_1, g_2, g_3, g_4)$ であった．今，消去定理を使うと，

$$I_1 = I \cap \mathbb{C}[y, z] = \langle g_1, g_2, g_3 \rangle, \quad I_2 = I \cap \mathbb{C}[z] = \langle g_1 \rangle$$

であることがわかる．$g_1 = 0$ より $z = \pm 1, \pm\sqrt{2}$ がわかる．まず，$z = \pm\sqrt{2}$ ならば，$g_2 = 0$ より $y = 0$，さらに $g_4 = 0$ より $x = 0$ となり，解 $(x, y, z) = (0, 0, \pm\sqrt{2})$ を得る．次に，$z = \pm 1$ ならば，$g_3 = 0$ より，$y^3 = \pm 1$ となり，ω を 1 の 3 乗根とすると，$y = \pm\omega$ であり，$g_4 = 0$ より $x = \pm\omega^2$ となるから，解 $(x, y, z) = (\pm\omega^2, \pm\omega, \pm 1)$ を得る．以上より全ての解が求まった．

この例で，$z = \pm 1$ や $(y, z) = (\pm\omega, \pm 1)$ はそれぞれ $\mathbf{V}(I_2) \subset k^1$ や $\mathbf{V}(I_1) \subset k^2$ の点である．つまり，I_2 や I_1 に対応する連立方程式の解である．このような消去イデアルに対応する連立方程式の解を**部分解**と呼ぶ．上の例では，部分解から本来求めたい連立方程式の解に拡張することができた．しかし，一般に，どんな部分解も元の連立方程式の解に拡張できるとは限らない．

例 7.5. 連立方程式

$$\begin{aligned} f_1 &= xy - 1 = 0 \\ f_2 &= xz - 1 = 0 \end{aligned}$$

を考える．$I = \langle f_1, f_2 \rangle \subset k[x, y, z]$ とし，$x >_{\text{lex}} y >_{\text{lex}} z$ を考えると，$\{f_1, f_2, y - z\}$ は I のグレブナー基底となる．よって，消去定理から $y - z$ は I_1 のグレブナー基底となる．したがって，部分解 $(y, z) = (a, a)$ $(a \in \mathbb{C})$ を得る．今，部分解 $(0, 0)$ を考える．元の連立方程式を考えると，$(x, 0, 0)$ が元の連立方程式の解にならないことは明らかである．したがって，この部分解を拡張して，元の連立方程式の解を得ることはできない．

定理 7.6 (拡張定理 (Extension Theorem))**.** イデアル $I = \langle f_1, \ldots, f_s \rangle \subset \mathbb{C}[x_1, \ldots, x_n]$ を考え，I_1 を I の 1 次消去イデアルとする．各 $1 \leq i \leq s$ に対して，f_i を次の形に書く．

$$f_i = c_i(x_2, \ldots, x_n) x_1^{N_i} + (x_1\text{の次数が } N_i \text{ 未満である項}).$$

ここで $N_i \geq 0$ で $c_i \in \mathbb{C}[x_2, \ldots, x_n]$ はゼロでない多項式である．部分解 $(a_2, \ldots, a_n) \in \mathbf{V}(I_1)$ があると仮定する．このとき，$(a_2, \ldots, a_n) \notin \mathbf{V}(c_1, \ldots, c_s)$ ならば，$a_1 \in \mathbb{C}$ が存在して，$(a_1, \ldots, a_n) \in \mathbf{V}(I)$ である．

証明にはもう少し準備が必要なので，主張の紹介だけにとどめておく．

例 7.7. 先の例だと，

$$\begin{aligned} f_1 &= y \cdot x - 1 = 0 \\ f_2 &= z \cdot x - 1 = 0 \end{aligned}$$

なので，$c_1(y,z)=y, c_2(y,z)=z$ となる．このとき部分解 $(0,0)$ を考えると，$(0,0)\in \mathbf{V}(c_1,c_2)$ なので，拡張定理の仮定は成り立たない．実際，拡張ができないことは先ほど見た．一方，$0\neq a\in\mathbb{C}$ に対し，部分解 (a,a) は $\mathbf{V}(c_1,c_2)$ に属さないので，ある $b\in\mathbb{C}$ が存在して，(b,a,a) という元の連立方程式の解に拡張できることが拡張定理からわかる．実際，$(\frac{1}{a},a,a)$ が連立方程式の解である．

グレブナー基底の応用

グレブナー基底の応用として例えば次のようなものがある．

- 数式処理システム
- 整数計画問題
- 学習理論
- ロボット工学
- 代数統計学

このように多種多様な応用先があるが，一つの（最も大きな）問題はグレブナー基底の計算は莫大で，変数が増えるとたちまち計算が終わらなくなることである．そのためにも，グレブナー基底を高速で解くアルゴリズムの開発が求められている．

一方，グレブナー基底は性質が良い分，抽象数学，特に可換環論や代数幾何学において，非常に強力な道具である．例えば，計算機で計算できないような（例えば n 変数など）イデアル I が与えられた時，ある集合がその生成系となることを証明するのにグレブナー基底であることを理論的に証明することがある．これはグレブナー基底かどうかをチェックするテクニックがあるためである．生成系を求めるのは実は難しかったりする．他にも代数多様体の特異点解消のために使われたりする．

Macaulay2

最後に，グレブナー基底を計算できる無料の計算機代数システムとして Macaulay2 を紹介する．Macaulay2 は代数幾何と可換代数の計算のための，フリーのオープンソースな計算機代数システムである．Unix システム，Mac OS X および，Cygwin のもと，Windows でダウンロードし，使用可能である．また，以下のサイトでウェブブラウザからオンラインで使用することも可能である．

`https://www.unimelb-macaulay2.cloud.edu.au/#home`

例えば，イデアル $I=\langle x^2+y, 2xy+y^2\rangle\subset\mathbb{Q}[x,y]$ の $x>_{\text{lex}} y$ に関するグレブナー基底を計算するためには，次のコマンドで計算できる．

```
i1 :  R = QQ[x,y,MonomialOrder=>Lex]
i2 :  I = ideal(x^2 + y,2*x*y + y^2)
i3 :  gens gb I
```

さらに，イデアル I のグレブナー基底による多項式 f の割り算の余りは

```
i4 :  f % I
```

で求まる．単項式順序を変えたければ，例えば次数付き辞書式順序の場合は Lex の部分を GLex などに変えればいい．何も指定しなければ，rlex で計算される．

演習問題

1. 連立方程式

$$\begin{aligned} x^2 + y + z &= 1 \\ x + y^2 + z &= 1 \\ x + y + z^2 &= 1 \end{aligned}$$

をグレブナー基底を用いて解け.

2. 次の連立方程式

$$\begin{aligned} f_1 &= x^2 + 2y^2 - 3 = 0 \\ f_2 &= x^2 + xy + y^2 - 3 = 0 \end{aligned}$$

を考える．$x >_{\text{lex}} y$ と $y >_{\text{lex}} x$ の 2 通りの辞書式順序に関する $I = \langle f_1, f_2 \rangle \subset k[x, y]$ のグレブナー基底を求め，$I \cap k[x]$ と $I \cap k[y]$ の生成系をそれぞれ求めよ．またそれぞれのグレブナー基底から連立方程式を解き，どちらの解も一致することを確かめよ.