グレブナー基底と代数多様体

菅崎 賢人

目次

概要

当論文は主に『グレブナ基底と代数多様体入門 上・下』をテキストとして書かれている．具体的には第 1，2，3 章の大部分と第 4，6 章の一部の内容である．

主なテーマはアフィン多様体とイデアルの間の対応関係とそれによる連立方程式の解法である．その過程で最も重要な道具であるグレブナー基底が登場し，その性質や利用方法を探る．

まず第 1 章で，多変数多項式の連立方程式の解空間をその多項式で定義されるアフィン多様体として表記し，その多項式で生成されるイデアルを考える．第 2 章で多項式環（あるいは一般の可換環）のイデアルについての基本的な性質であるヒルベルトの基底定理から本格的な議論を始めて，そのイデアルに対してグレブナー基底という良い性質をもった基底がアルゴリズムによって計算できることを示す．第 3 章において，グレブナー基底を用いて連立方程式を解くための考え方である消去理論を扱う．消去理論は消去定理（変数の消去に関する定理）と拡張定理（解の代入に関する定理）の 2 本の柱からなり，それらの証明や幾何学的な意味を考察する．ここで代数と幾何が結びついてくる．また証明では終結式という線形代数の概念が登場する．第 4 章ではヒルベルトの零点定理を証明し根基イデアルと多様体の対応を見る．さらに，アフィン多様体の　既約分解に関しても触れる．第 5 章では，以上の応用としてグレブナー基底を使った幾何の定理の自動証明について考える．これは図形に関する定理や公式を証明する手順が定式化でき，コンピュータが発見・自動証明できるという事実を説明する．そしてこの方法によるトレミーの定理の証明を試みる．

全体に渡って，イデアルのグレブナー基底を始めとする代数学的概念と多様体などの幾何学的対象とを方程式の零点を考えることによって結びつけ，2 つの領域を相互還元的に考えていく．

1　アフィン多様体とイデアル

1.1　アフィン空間

定義 1-1.　体 k と正の整数 n に対して次の集合を定義する

$$k^n = \{(a_1, \ldots, a_n) \mid a_1, \ldots, a_n \in k\}.$$

これを k 上の n 次元**アフィン空間**という.

当論文では，扱う幾何学的対象はすべてこのアフィン空間内の集合である.

k^1 を特にアフィン直線，k^2 はアフィン平面という．またアフィン空間 k^n 内の直線 $y = x - 1$ も同じくアフィン直線 k である．アフィン空間は k 上 n 次元ベクトル空間の部分集合，すなわち部分空間を平行移動して得られた空間である．アフィン空間でない例は，$\mathbb{C} - \{0\}$ のように k^n の形で書けないものである．アフィン空間から有限個の点を除いた集合は，このようにアフィン空間にはならない.

次に当論文の主役となる集合を定義する.

1.2　アフィン多様体

定義 1-2.　k を体，$f_1, \ldots, f_s$ を $k[x_1, \ldots, x_n]$ に属する多項式とする. このとき

$$\mathbf{V}(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) \in k^n \mid 1 \leq \forall i \leq s \;\; s.t. \;\; f_i(a_1, \ldots, a_n) = 0\} \subset k^n$$

とおくと，これを $f_1, \ldots, f_s$ で定義される**アフィン多様体**という.

このアフィン多様体 $\mathbf{V}(f_1, \ldots, f_s) \subset k^n$ とは，つまり連立方程式 $f_1 = \cdots = f_s = 0$ の解空間を意味する.

例 1-3.　$k = \mathbb{R}$ とする．アフィン多様体はその定義方程式系によって，有限個の点や曲線，曲面，超曲面などといった多様な形状を成す.

(1)　$\mathbf{V}(x^2 + y^2 - 1, y - x) \subset \mathbb{R}^2$ は，$x^2 + y^2 - 1 = y - x = 0$ を計算すると $x = y = \dfrac{\sqrt{2}}{2}$ であるので，$\mathbf{V}\left(x - \dfrac{\sqrt{2}}{2}, y - \dfrac{\sqrt{2}}{2}\right)$ に一致する.

(2)　$y = \dfrac{x^3 - 1}{x}$ のグラフを描くと，y 軸に漸近する 2 本の曲線であることが分かる．分母を払うと $xy - x^3 + 1 = 0$ であるが，$x = 0$ はこれを満たさないので，グラフは $\mathbf{V}(xy - x^3 + 1) \subset \mathbb{R}^2$ と一致する.

(3)　$\mathbf{V}(z - x^2 - y^2) \subset \mathbb{R}^3$ は z 軸周りの回転放物面となる.

(4)　$\mathbf{V}(1) \subset k^n$ や $\mathbf{V}(x^2 + y^2 + 1) \subset \mathbb{R}^2$ のように定義方程式に解が無い多様体は空集合である.

(5)　$\mathbf{V}(0) \subset k^n$ は，$0 = 0$ がすべての点で成り立つので，k^n 全体のことである.

アフィン多様体について，次の簡単な補題が直ちに従う.

補題 1-4.　$V = \mathbf{V}(f_1, \ldots, f_s), W = \mathbf{V}(g_1, \ldots, g_t)$ とする．このとき，$V \cap W$ と $V \cup W$ もまたアフィン多様体であり，次のように表せる

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

例 1-5. $\mathbb{R}^3$ 内で考える．

(1) $V_1 = \mathbf{V}(y - x^2, z - x^3)$ は捩れ 3 次曲線である．これは放物面 $\mathrm{V}(y - x^2)$ と 3 次曲面 $\mathbf{V}(z - x^3)$ の共通部分に等しい．

(2) $V_2 = \mathbf{V}(zx, zy)$ は $zx = zy = 0 \iff z = 0$ または $x = y = 0$ であるので $\mathbf{V}(z) \cup \mathbf{V}(x, y)$ と書ける．

ここでアフィン多様体の次元について考察する．例 1-3. を見れば $\mathbb{R}^2$ 内で方程式が 1 本の場合は曲線，すなわち 1 次元である（1 変数のパラメータで表せる）．2 本の場合は有限個の点つまり 0 次元である．$\mathbb{R}^3$ 内で方程式が 1 本ならば曲面となり 2 次元である．ここからアフィン多様体の次元は，全空間の次元から，互いに包含関係のない解空間を持つ方程式の本数だけ次元が下がっている（方程式の本数 = 多様体の余次元）と推測できる．捩れ 3 次曲線 V_1 の場合は $\mathbb{R}^3$ 内で式が 2 本なので 1 次元である．

ここで問題となるのは，上の例 1-5.(2) の V_2 がこの関係式の例外だということである．V_2 は関係式に従えば 1 次元であるはずだが，先ほどの計算から実際は 2 次元の部分も併せ持っている．この問題の原因は，V_2 が可約つまり異なるアフィン多様体の和集合であることにある．

ここまでの議論から，連立方程式の解について興味深い問題が導かれる．

（A） 連立方程式の解を求める一般的な方法はあるか？ また解が無いのはどのような場合か，つまり対応するアフィン多様体が空となる条件は何か？

（B） アフィン多様体の次元を決定できるか？

（C） 特に有限集合（0 次元空間）となるのはいつか？ 解が有限個ならば個数を評価することはできるか？

当論文では 3 つの問題の中では（A）をメインとして扱う．第 2 章から第 3 章までを使って“グレブナー基底の方法”を証明し，最後に第 4 章で完全な（A）への解答を得る．（B）は射影代数幾何の分野となるので，文量の都合で割愛する．（C）については，解が有限となるかどうかの判定法がグレブナー基底の方法の中から分かる（上巻第 5 章参照）．

1.3 イデアル

ここから先は問題（A）について考えていく．まずはグレブナー基底の概念が必要だが，その準備としてグレブナー基底をもつことになるイデアルについて述べていく．

定義 1-6. I を $k[x_1, \ldots, x_n]$ のイデアルとすると次の集合が定義できる
$$\mathbf{V}(I) = \{(a_1, \ldots, a_n) \in k^n \mid \forall f \in I \ \ s.t. \ \ f(a_1, \ldots, a_n) = 0\,\}.$$

命題 1-7. $\mathbf{V}(I)$ はアフィン多様体であり，$I = \langle f_1, \cdots, f_s \rangle$ と書けるとき，次が成立する
$$\mathbf{V}(I) = \mathbf{V}(f_1, \cdots, f_s).$$

証明　($\subset$) I の任意の元が $\mathbf{V}(I)$ のすべての点で消える（0 になる）とき，$1 \leq i \leq s$ に対して $f_i \in I$ も同じように消えるので，$\mathbf{V}(I) \subset \mathbf{V}(f_1, \cdots, f_s)$.
($\supset$) $(a_1, \cdots, a_n) \in \mathbf{V}(f_1, \cdots, f_s)$ とする．$f \in I$ はある $h_i \in k[x_1, \cdots, x_n]$ に対して，$f = \sum_{i=1}^{s} h_i f_i$ と書ける．
よって $f = \sum_{i=1}^{s} h_i(a_1, \cdots, a_n) f_i(a_1, \cdots, a_n) = \sum_{i=1}^{s} h_i(a_1, \cdots, a_n) \cdot 0 = 0$ となり，$\mathbf{V}(f_1, \cdots, f_s) \subset \mathbf{V}(I)$.　□

よって，解空間 $\mathbf{V}(f_1, \cdots, f_s)$ を求めたいときに代わりに $\mathbf{V}(I)$ を求めても同じことである．こうして連立方程式をイデアル I として捉えることで，I の“より簡潔な基底”を計算して I を単純化していくと，実はそれに伴って解 $\mathbf{V}(I)$ も計算しやすくなるのである．これがイデアルを考えた理由である．ここで言う“より簡潔な基底”が後に定義するグレブナー基底である．
次に特別なイデアルの場合を例示しておく．

例 1-8.　$I = k[x_1, \cdots, x_n]$ である場合，$1 \in I$．$\therefore I = \langle 1 \rangle$．よって命題 1-7. より，$\mathbf{V}(I) = \mathbf{V}(1) = \emptyset$.
逆に，$\mathbf{V}(I) = \emptyset$ と仮定すると $I = k[x_1, \cdots, x_n]$ の場合だけでなく $I \neq k[x_1, \cdots, x_n]$ である場合もある．それは $\mathbf{V}(x^2 + y^2 + 1) \subset \mathbb{R}^2$ のように $\mathbb{R}$ 上に根を持たない多項式を用いて I を生成した場合である．

ここで疑問なのは，k を $\mathbb{R}$ ではなく代数的閉体としたときにもこのようなことが起こり得るのかということである．つまり問題（A）について，代数的閉体上において解が無いのは本当に $I = k[x_1, \cdots, x_n]$ の場合だけなのかを知りたいのである．これに対する答えは第 4 章で示す零点定理にある．
ここで，$\mathbf{V}(I)$ と対になる概念を定義しておく．

定義 1-9.　V を k^n 内のアフィン多様体とすると

$$\mathbf{I}(V) = \{ f \in k[x_1, \cdots, x_n] \,|\, \forall (a_1, \cdots, a_n) \in V \ \ s.t. \ \ f(a_1, \cdots, a_n) = 0 \}.$$

補題 1-10.　この $\mathbf{I}(V)$ は $k[x_1, \cdots, x_n]$ のイデアルである．$\mathbf{I}(V)$ を V のイデアルという．

証明　(1) $0 \in k[x_1, \cdots, x_n]$ は k^n 全体で消えているので，$\forall V \subset k^n$ に対して $0 \in \mathbf{I}(V)$ である．
(2) $f, g \in \mathbf{I}(V)$，$h \in k[x_1, \cdots, x_n]$ とし，V の任意の点を $p = (a_1, \cdots, a_n)$ とする．この点において
$(f + g)(p) = f(p) + g(p) = 0$ であるので，$f + g \in \mathbf{I}(V)$.
(3) $(hf)(p) = h(p) f(p) = h(p) \cdot 0 = 0$ であるので，$hf \in \mathbf{I}(V)$.
よって $\mathbf{I}(V)$ は $k[x_1, \cdots, x_n]$ のイデアルである．　□

例 1-11. (1) $\{(0,0)\} \in k^2$ に対して，$\mathbf{I}(\{(0,0)\}) = \langle x, y \rangle$.
証明　($\supset$) 明らか. ($\subset$) 原点で消える多項式を $f \in k[x, y]$ とする．$f = \sum_{i,j} a_{ij} x^i f^j$ と書けるので，定数項は $a_{00} = f(0,0) = 0$ である．したがって

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

(2) k が標数 0 の体 (すなわち無限体) のとき，$\mathbf{I}(k^n) = \langle 0 \rangle$.
k が正標数の体のときは (有限，無限に関わらず) 上は成り立たない．例えば $k = \mathbb{F}_2$ のとき $x^2 y + x y^2$

$\in \mathbb{F}_2[x,y]$ は ${\mathbb{F}_2}^2$ のすべての元で消えるので，$\mathbf{I}({\mathbb{F}_2}^2) \neq \langle 0 \rangle$ である（ちなみに $\mathbf{I}({\mathbb{F}_2}^2)$=$\langle x^2-x, y^2-y \rangle$）.

(3) $V = \mathbf{V}(y-x^2,\ z-x^3) \subset \mathbb{R}^3$に対して，$\mathbf{I}(V) = \langle y-x^2,\ z-x^3 \rangle$ となる.
証明 $(\supset)\ y-x^2, z-x^3 \in \mathbf{I}(V)$ であるので，$\forall a,b \in k[x_1,\cdots,x_n]\ \ s.t.\ a(y-x^2)+b(z-x^3) \in \mathbf{I}(V)$.
$(\subset)$ 任意の $f \in \mathbb{R}[x,y,z]$ を $f = a(y-x^2)+b(z-x^3)+r$ と書くと，剰余の定理より $r = f(x,x^2,x^3) \in \mathbb{R}[x]$ である．今 $f \in \mathbf{I}(V)$ とすると，V のパラメータ付け (t,t^2,t^3) によって $f(t,t^2,t^3)=0$．つまり $r(t)=0$.
$t \in \mathbb{R}$ は任意なので，$r=0$．$\therefore\ f \in \langle y-x^2,\ z-x^3 \rangle$. □

例 1-11.(3) は $I = \mathbf{I}(\mathbf{V}(I))$ の例になっている．これはどのような I に対しても成立するのであろうか？

補題 1-12. $I = \langle f_1,\cdots,f_s \rangle$ と書けるとき，$I \subset \mathbf{I}(\mathbf{V}(I))$ が成立する．等号は必ずしも成立しない.

証明 $(\subset)\ f \in I$ は f_i たちの $k[x_1,\cdots,x_n]$ 線形和であるが，f_i たちは $\mathbf{V}(I)$ で消えるので，f も消える.
$(\subsetneq$ の例$)\ I = \langle x^2,y^2 \rangle$ のとき $\mathbf{I}(\mathbf{V}(x^2,y^2))$= $\mathbf{I}(\{(0,0)\}) = \langle x,y \rangle \supsetneq \langle x^2,y^2 \rangle$. □

等号成立条件については，これも零点定理で記述される.

命題 1-13. V, W を k^n内のアフィン多様体とすると
(1) $V \subset W \iff \mathbf{I}(V) \supset \mathbf{I}(W)$,
(2) $V = W \iff \mathbf{I}(V) = \mathbf{I}(W)$.

証明 (2) は (1) から従うので，(1) を示す.
$(\Rightarrow)$ V の点が W の点でもあるとすると，W で消える式は V でも消える.
$(\Leftarrow)\ \mathbf{I}(V) \supset \mathbf{I}(W)$ とする．$W = \mathbf{V}(g_1,\cdots,g_t)$ であるとすると，$g_1,\cdots,g_t \in \mathbf{I}(W) \subset \mathbf{I}(V)$ より，g_iたちは V で消える．よって $V \subset W$ となる. □

2 グレブナー基底

2.1 単項式順序

問題（A）を考えるとき，連立方程式の解を求めるための要がグレブナー基底である．この方法は方程式どうしを計算して，先頭の項に着目して次数を下げていくことから始まる．ここで問題となるのが次数の順序付けである．例えば xy^2z^3と x^2y^3z はどちらも全次数が 6 であり，多項式の中でどちらの項を先に書くのかを毎回定義する必要がある．このような項の順序付けには様々な種類があるが，まずは定義から述べる.

定義 2-1. $k[x_1,\cdots,x_n]$ における**単項式順序**とは，$\mathbb{N}^n$の順序付け“$>$”で次を満たすものである.
(1) “$>$”は $\mathbb{N}_0^n$ の全順序である,
(2) $\alpha > \beta$ で $\gamma \in \mathbb{N}_0^n$ とすれば $\alpha+\gamma > \beta+\gamma$ である,
(3) “$>$”は $\mathbb{N}_0^n$ の整列順序である.

つまり $\mathbb{N}_0^n$ のどの元の間にも大小関係があり，和を保存し，どの部分集合にも最小限が定められる順序である．条件 (3) は $\alpha \geq 0$ と同値である．

この単項式順序の種類のうち代表的な 3 つを挙げる．

定義 2-2.　辞書式順序（lex 順序）

$\alpha = (\alpha_1, \cdots, \alpha_n), \beta = (\beta_1, \cdots, \beta_n) \in \mathbb{N}_0^n$ に対して $\alpha >_{lex} \beta$ あるとは，$\alpha - \beta \in \mathbb{N}_0^n$ の 0 でない一番左の成分が正であることである．$\alpha >_{lex} \beta$ のとき $x^\alpha >_{lex} x^\beta$ と書くことにする．ただし $x^{(\alpha_1,\cdots,\alpha_n)} = {x_1}^{\alpha_1} \cdot \cdots \cdot {x_n}^{\alpha_n}$ と表記している．

これは例えば $x_1 > \cdots > x_n$ とするとき，まず x_1 について降べきの順に並べ，同次の項がある場合はその中で x_2 に関してまた降べきの順に並べるという操作を以下同様にして並べるときの順序のことである．lex 順序は単項式順序になっている．

例 2-3.　$f = xy^2z + xz^2 + x^3 + x^2z^2 \in k[x, y, z]$ を $x > y > z$ の lex 順序に関して並べ直す

$(3, 0, 0) >_{lex} (2, 0, 2) >_{lex} (1, 2, 1) >_{lex} (1, 0, 2)$ であるので，$f = x^3 + x^2z^2 + xy^2z + xz^2$.

定義 2-4.　次数付き辞書式順序（grlex 順序）

$\alpha, \beta \in \mathbb{N}_0^n$とする．$\alpha >_{grlex} \beta$であるとは

$$\|\alpha\|_1 > \|\beta\|_1 \quad \text{または，} \quad \|\alpha\|_1 = \|\beta\|_1 \quad \text{であって} \quad \alpha >_{lex} \beta$$

を満たすことである．ここで $\|\alpha\|_1 = \sum_{i=1}^{n} \alpha_i$，つまり x^α の全次数である．

この grlex 順序とは，まず全次数で降べきの順に並べ，その後で同じ全次数の項どうしをそれぞれ lex 順序で並べる (同点決勝を行う) 順序である．

例 2-3. の $f = xy^2z + xz^2 + x^3 + x^2z^2$ は，$x > y > z$ の grlex 順序では

$(2,0,2) >_{grlex} (1, 2, 1) >_{grlex} (3, 0, 0) >_{grlex} (1, 0, 2)$．$\therefore\ f = x^2z^2 + xy^2z + x^3 + xz^2$.

定義 2-5.　次数付き逆辞書式順序（grevlex 順序）

$\alpha, \beta \in \mathbb{N}_0^n$とする．$\alpha >_{grevlex} \beta$であるとは

$\|\alpha\|_1 > \|\beta\|_1$　または　$\|\alpha\|_1 = \|\beta\|_1$　であって　$\alpha - \beta \in \mathbb{N}^n$の 0 でない一番右の成分が負であることを満たすことである．

最初に全次数で並べる点では grlex 順序と同じだが，同点決勝の方法が異なる．後ろの方の変数から順に次数を見ていき，その次数の小さな項から並べるのである．

例 2-3. の $f = xy^2z + xz^2 + x^3 + x^2z^2$ は，$x > y > z$ の grevlex 順序では

$(1, 2, 1) >_{grevlex} (2, 0, 2) >_{grevlex} (3, 0, 0) >_{grevlex} (1, 0, 2) \quad \therefore\ f = xy^2z + x^2z^2 + x^3 + xz^2$.

定義 2-6.　$f \in k[x_1, \cdots, x_n]$ の項のうち，ある順序 “$>$” において最大のものを f の先頭項（Leading term）といい $\mathrm{LT}(f)$ と表す．$\mathrm{LT}(f)$ の k 係数を f の先頭係数といい$\mathrm{LC}(f)$ と書く．$\mathrm{LM}(f) = \dfrac{\mathrm{LT}(f)}{\mathrm{LC}(f)}$と書いたものを f の先頭単項式という．また，$\mathrm{LT}(f)$ の次数を表すベクトルを f の多重次数といい，$\mathrm{multideg}(f)$ と表す．

2.2 ヒルベルトの基底定理

先頭項が定義できたので，多変数多項式の割り算を使ってヒルベルトの基底定理を示すことができる．その前に，その証明にはもう一つ〈LT(I)〉という単項式から生成されるイデアルについて言及する必要がある．

定義 2-7.　単項式イデアル

$k[x_1,\cdots,x_n]$ のイデアル I が**単項式イデアル**であるとは，（必ずしも有限ではない）部分集合 $A\subset\mathbb{N}_0^n$があって I の元がすべて $\sum_{\alpha\in A} h_\alpha x^\alpha$ $(h_\alpha\in k[x_1,\cdots,x_n])$ の形の有限和で書けることをいう（つまり h_α は有限個を除いて 0 である）．

例えば，$\langle x^4,x^3y^2,x^2y^4\rangle\subset k[x,y]$ は単項式イデアルであり，$\langle x+y\rangle\subset k[x,y]$ は単項式イデアルではない．単項式イデアルのより興味深い例は定義 2-10. で与えられる．

次に，この単項式イデアルは，実は有限個の単項式から生成できることが分かる．

命題 2-8.　Dickson の補題

$k[x_1,\cdots,x_n]$ の単項式イデアル $I=\langle x^\alpha\mid\alpha\in A\subset\mathbb{N}_0^n\rangle$ は，有限基底を持つ．つまり $\exists\alpha(i)\in A\quad s.t.$ $I=\langle x^{\alpha(1)},\cdots,x^{\alpha(s)}\rangle$ $(s<\infty)$ と書ける．

証明　変数の数 n に関する数学的帰納法を用いる．

(1) $n=1$ のとき，$I=\langle x^\alpha\mid\alpha\in A\subset\mathbb{N}_0^1\rangle$ とする．ある項順序“$<$”を固定すれば，A には最小元 β がある．よって $x_1^\beta\mid x_1^A$ であり，$I=\langle x_1^\beta\rangle$ と書ける（つまり $k[x_1]$ は PID である）．

(2) $n\geq 2$ のとき，$n-1$ 変数では補題が正しいと仮定する．x_n を他の変数と区別するために y と置き直し，$\alpha=(\alpha_1,\cdots,\alpha_{n-1})\in\mathbb{N}_0^{n-1}$とおく．今，$I$ を y について射影してできる新たなイデアルを考える．すなわち $\exists m\in\mathbb{N}$ に対し，$x^\alpha y^m\in I$ となるような x^αで生成される $k[x_1,\cdots,x_{n-1}]$ の単項式イデアルを J とする．
帰納法の仮定より J は有限個の単項式で生成される．これを $J=\langle x^{\alpha(1)},\cdots,x^{\alpha(s)}\rangle$ とおく．
J の定義を書き直すと，$1\leq\forall i\leq s$ に対し $\exists m_i\in\mathbb{N}$ で，$x^{\alpha(i)}y^{m_i}\in I$ となる．この m_i のうち最大のものを改めて m とする．次に，$0\leq\forall l\leq m-1$ に対し，$x^\beta y^l\in I$ となるような x^β で生成される $k[x_1,\cdots,x_{n-1}]$ の単項式イデアルを J_l とする．仮定より J_l も有限生成であり，$J_l=\langle x^{\alpha_l(1)},\cdots,x^{\alpha_l(s_l)}\rangle$ とおく．この J_l は，I のちょうど y^l を含む項の“スライス”と考えられる．つまり主張したいのは，I が次の有限個の単項式で生成できることである

$$
\begin{aligned}
&x^{\alpha(1)}y^m,\cdots,x^{\alpha(s)}y^m, && (J\text{ の生成元}\times\ y^m)\\
&x^{\alpha_0(1)},\cdots\cdots,x^{\alpha_0(s_0)}, && (J_0\text{の生成元})\\
&x^{\alpha_1(1)}y,\ \cdots,\ x^{\alpha_1(s_1)}y, && (J_1\text{の生成元}\times\ y)\\
&\cdots\cdots,\\
&x^{\alpha_{m-1}(1)}y^{m-1},\cdots\cdots,x^{\alpha_{m-1}(s_{m-1})}y^{m-1}. && (J_{m-1}\text{の生成元}\times\ y^{m-1})
\end{aligned}
$$

$x^\alpha y^p\in I$ とする．もし $p\geq m$ ならば，$x^\alpha y^p$は $x^{\alpha(i)}y^m$ のどれかで割り切れる．一方 $p\leq m-1$ ならば，$x^\alpha y^p$は $x^{\alpha_p(i)}y^p$ のどれかで割り切れる．よって上の表の有限個の単項式で I は生成できる．

これらの単項式はすべて I の元なので，I の基底は I の元から有限個を選び出して書けることになる．　□

例 2-9.　上の Dickson の補題の証明に当てはめて，$k[x,y]$ の単項式イデアル $I=\langle x^4y^2, x^3y^4, x^2y^5\rangle$ の有限基底を表記してみる．

I の $k[x]$ への射影であるイデアルは，$J=\langle x^2\rangle$ とおける．m_i は各々 $m_1=2, m_3=4, m_3=5$ であり，$m=\max\{m_i\}_{i=1,2,3}=5$ となる．そして $x^jy^l\in I\,(0\leq l\leq m-1=4)$ となるような x^j で生成されるイデアル J_l は，$J_0=J_1=\{0\}, J_2=J_3=\langle x^4\rangle, J_4=\langle x^3\rangle, J=\langle x^2\rangle$ である．よって $x^4y^2, x^4y^3, x^3y^4, x^2y^5\in I$ であり，Dickson の補題より，$I=\langle x^4y^2, x^4y^3, x^3y^4, x^2y^5\rangle$ と書ける．

定義 2-10.　$k[x_1,\cdots,x_n]$ のイデアル I に対し，I の元の先頭項全体を $\mathrm{LT}(I)$，$\mathrm{LT}(I)$ によって生成されるイデアルを $\langle\mathrm{LT}(I)\rangle$ とする．$\langle\mathrm{LT}(I)\rangle$ は単項式イデアルである．

$\langle\mathrm{LT}(I)\rangle$ とはどのようなイデアルなのだろうか．有限生成な $I=\langle f_1,\cdots,f_s\rangle$ が与えられたとき $\langle\mathrm{LT}(I)\rangle=\langle\mathrm{LT}(f_1)$,$\cdots$,$\mathrm{LT}(f_s)\rangle$ と書けるのだろうか？“$\supset$”は明らかであるが，実際“$\supsetneq$”である場合もある．

例 2-11.　$f_1=x^3-2xy, f_2=x^2y-2y^2+x$, $I=\langle f_1,f_2\rangle$ とする．grlex 順序を用いると，項の順序は f_1について $x^3>xy$，f_2について $x^2y>y^2>x$ であるので，$\mathrm{LT}(f_1)=x^3, \mathrm{LT}(f_2)=x^2y$ である．ここで $xf_2-yf_1=x^2$もまた I の元だから，$x^2=\mathrm{LT}(x^2)\in\mathrm{LT}(I)$．しかし，$x^2$ は $\langle\mathrm{LT}(f_1),\mathrm{LT}(f_2)\rangle=\langle x^3,x^2y\rangle$ には含まれない．よって $\langle\mathrm{LT}(I)\rangle\supsetneq\langle\mathrm{LT}(f_1),\mathrm{LT}(f_2)\rangle$ である．

この例のように，一般に $\langle\mathrm{LT}(I)\rangle$ と $\langle\mathrm{LT}(f_1)$,$\cdots$,$\mathrm{LT}(f_s)\rangle$ は異なる．では，多項式 f_1,$\cdots$,f_s が与えられたとき，$\langle\mathrm{LT}(I)\rangle$ はどのように書けるのだろうか？

まず，$\langle\mathrm{LT}(I)\rangle$ は単項式イデアルだったので，Dickson の補題より $\langle\mathrm{LT}(I)\rangle$ は有限生成であることが分かる．ここからようやく次の定理に至る．

定理 2-12.　ヒルベルトの基底定理

$k[x_1,\cdots,x_n]$ のすべてのイデアル I は有限生成である．

証明　Dickson の補題より，$\langle\mathrm{LT}(I)\rangle=\langle\mathrm{LT}(g_1)$,$\cdots$,$\mathrm{LT}(g_t)\rangle$ $(t<\infty)$ となるように $g_1,\cdots,g_t\in I$ をとることができる．あとは $I=\langle g_1,\cdots,g_t\rangle$ であることを示すことができればよい．“$\supset$”は明らかなので，“$\subset$”を示す．

$f\in I$ は，$f=a_1g_1+\cdots+a_tg_t+r$, $a_i,r\in k[x_1,\cdots,x_n]$ と書ける．ここで多変数多項式の割り算アルゴリズムより，ある項順序を固定すると，$r=0$ または，r のすべての項が $\mathrm{LT}(g_1)$,$\cdots$,$\mathrm{LT}(g_t)$ のいずれでも割り切れないような剰余 r をとれる．$r=0$ を示したい．今 $r\in I$ なので

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

となり，$\mathrm{LT}(r)$ は $\mathrm{LT}(g_i)$ のいずれかで割り切れることになる．よって $r=0$ が分かり，$f\in\langle g_1,\cdots,g_t\rangle$．　□

ヒルベルトの基底定理と同値な命題に，イデアルの昇鎖条件 (ACC) がある．これは $k[x_1,\cdots,x_n]$ のイデアルの包含関係における増大列は，必ず有限で止まるという主張である．これを証明するにはは，まず増大列のすべてイデアルの無限和集合を考え，それが再びイデアルとなることを確認する．次に，ヒルベルトの基底定理よりそのイデアルもまた有限基底を持つので，そのイデアルに達したところで列の増大が止まることを最後

に主張する．このイデアルを通常，$k[x_1,\cdots,x_n]$ の極大イデアルという．つまりこれらの命題は $k[x_1,\cdots,x_n]$ が Noether 環であることを主張している．

2.3 グレブナー基底と S 多項式

ヒルベルトの基底定理で登場した有限基底 $g_1,\cdots,g_t$ は，$\langle \mathrm{LT}(I)\rangle = \langle \mathrm{LT}(g_1),\cdots,\mathrm{LT}(g_t)\rangle$ という良い性質をもった基底である．

定義 2-13. ある項順序を固定する．イデアル I の有限部分集合 $G=\{g_1,\cdots,g_t\}$ が

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

を満たすとき，G を**グレブナー基底 (標準基底)** といい，I の基底をなす．

例 2-14. 例 2-11. で，$f_1=x^3-2xy, f_2=x^2y-2y^2+x$, $I=\langle f_1,f_2\rangle$ に対し，grlex 順序で，$xf_2-yf_1=x^2\in\langle \mathrm{LT}(I)\rangle$ だった（定義 2-15(2) の式と比べよう）．しかし $x^2\notin\langle \mathrm{LT}(f_1),\mathrm{LT}(f_2)\rangle=\langle x^3,x^2y\rangle$ であるので，$\langle \mathrm{LT}(f_1),\mathrm{LT}(f_2)\rangle\neq\langle \mathrm{LT}(I)\rangle$ である．すなわち $\{f_1,f_2\}$ は I の grlex 順序でのグレブナー基底ではない．

それでは，$I=\langle f_1,\cdots,f_s\rangle$ のグレブナー基底 $\{g_1,\cdots,g_t\}$ を具体的に求めるにはどうしたらよいのだろうか？ 一般に $\langle \mathrm{LT}(I)\rangle$ は $\langle \mathrm{LT}(f_1),\cdots,\mathrm{LT}(f_s)\rangle$ よりも真に大きい．当然，$\langle \mathrm{LT}(I)\rangle - \langle \mathrm{LT}(f_1),\cdots,\mathrm{LT}(f_s)\rangle$ の元 g をすべて $\langle \mathrm{LT}(f_1),\cdots,\mathrm{LT}(f_s)\rangle$ の生成元として添加していけば，$\langle \mathrm{LT}(I)\rangle$ に至る．つまりこのとき $G=\{f_1,\cdots,f_s,$ すべての g たち $\}$ が I のグレブナー基底となる（これは役割の重複した不要な基底を含むことがある）．

この g を求めよう．$\mathrm{LT}(g)$ はその定義より $\mathrm{LT}(f_1)$,$\cdots$,$\mathrm{LT}(f_s)$ のどれによっても割り切れない．すなわち g は，指定された項順序において $f_1,\cdots,f_s$よりも低次の多項式である．ここで，g は次数が低くてもきちんと I の元である．よって g は $f_1,\cdots,f_s$ の $k[x_1,\cdots,x_n]$-線形和だから，その和の中で $f_1,\cdots,f_s$の先頭項の打ち消し合いが起こることで g は $f_1,\cdots,f_s$ よりも次数が下がっているのである．ここでその打ち消し合いを定式化する．

定義 2-15. **S 多項式**

$k[x_1,\cdots,x_n]\ni f,\ g\neq 0$ とする．

(1) $\mathrm{multideg}(f)=\alpha, \mathrm{multideg}(g)=\beta\in\mathbb{N}_0^n$ とおき，$\gamma_i=\max(\alpha_i,\beta_i)$, $\gamma=(\gamma_1,\cdots,\gamma_n)$ とおく．x^γ を $\mathrm{LM}(f)$ と $\mathrm{LM}(g)$ の最小公倍元といい，$x^\gamma=\mathrm{LCM}(\mathrm{LM}(f),\mathrm{LM}(g))$ と書く．

(2) f,g の **S 多項式**とは，次で与えられる多項式である

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

例 2-16. $f=-x^2y^3+2x^3y^2+x,\ g=3x^4y+y^2\in\mathbb{R}[x,y]$ の S 多項式を求める．

grlex 順序を用いると，$\mathrm{LM}(f)=x^3y^2$, $\mathrm{LM}(g)=x^4y$ であるので

$$\mathrm{multideg}(f)=(3,2),\ \mathrm{multideg}(g)=(4,1)\quad\therefore\ \gamma=(\gamma_1,\gamma_2)=(\max(3,4),\max(2,1))=(4,2)$$

となる．したがって

$$x^\gamma=\mathrm{LCM}(x^3y^2,x^4y)=x^4y^2$$

である．よって

$$\begin{aligned} S(f,g) &= \frac{x^4y^2}{2x^3y^2}\cdot f - \frac{x^4y^2}{3x^4y}\cdot g \\ &= \frac{1}{2}x\cdot f - \frac{1}{3}y\cdot g \\ &= (x^4y^2 - \frac{1}{2}x^3y^3) - (x^4y^2 + \frac{1}{3}y^3) \\ &= -\frac{1}{2}x^3y^3 - \frac{1}{3}y^3 \in I. \end{aligned}$$

このように S 多項式 $S(f,g)$ を用いると，f と g の先頭項が係数ごと打ち消し合い次数を下げることができる．では，定義の前に考えていた g たちは S 多項式のみで書くことができるのだろうか？

補題 2-17. 各 i に対し，$c_i \in k$ で $\mathrm{multideg}(f_i) = \delta \in \mathbb{N}_0^n$であるような多項式の和 $\sum_{i=1}^{s} c_i f_i$ を考える．
もし $\mathrm{multideg}\left(\sum_{i=1}^{s} c_i f_i\right) \lneq \delta$であれば，$c_{jl} \in k$ があって $\sum_{i=1}^{s} c_i f_i$ は $S(f_j, f_l)$ $(1 \leq j, l \leq s)$ の k-線型和である．
さらに，各 j, l に対し $\mathrm{multideg}(S(f_j, f_l)) \lneq \delta$である．

証明 $d_i = \mathrm{LC}(f_i)$ とおくと，$\mathrm{LC}(c_i f_i) = c_i d_i$．そこで $\mathrm{multideg}(f_i) = \delta$, $\mathrm{multideg}\left(\sum_{i=1}^{s} c_i f_i\right) \lneq \delta$とすると
$\sum_{i=1}^{s} c_i d_i = 0 \quad \cdots(1)$ が分かる．

次に $p_i = \dfrac{f_i}{d_i}$とおく．和を次のように変形し差分を作る

$$\begin{aligned} \sum_{i=1}^{s} c_i f_i &= \sum_{i=1}^{s} c_i d_i p_i \\ &= c_1 d_1 (p_1 - p_2) + (c_1 d_1 + c_2 d_2)(p_2 - p_3) + \cdots\cdots + (c_1 d_1 + \cdots + c_{s-1} d_{s-1})(p_{s-1} - p_s) \\ &\quad + (c_1 d_1 + \cdots + c_s d_s) p_s. \quad \cdots(2) \end{aligned}$$

(1) より末項は 0 である．仮定より $\mathrm{LT}(f_i) = d_i x^\delta$ だから，$\mathrm{LCM}(\mathrm{LM}(f_j), \mathrm{LM}(f_l)) = x^\delta$である．よって

$$S(f_j, f_l) = \frac{x^\delta}{\mathrm{LT}(f_j)}\cdot f_j - \frac{x^\delta}{\mathrm{LT}(f_l)}\cdot f_l = p_j - p_l.$$

これを (2) に代入すれば

$$\begin{aligned} \sum_{i=1}^{s} c_i f_i &= c_1 d_1 S(f_1, f_2) + (c_1 d_1 + c_2 d_2) S(f_2, f_3) + \cdots\cdots + (c_1 d_1 + \cdots + c_{s-1} d_{s-1}) S(f_{s-1}, f_s) \\ &= \sum_{j=1}^{s} \left(\left(\sum_{i=1}^{j-1} c_i d_i \right) S(f_{j-1}, f_j) \right) \end{aligned}$$

と書けて，$\sum_{i=1}^{j-1} c_i d_i \in k$ である．

また，$\mathrm{multideg}(p_j) = \delta$ より，$\mathrm{multideg}(S(f_{j-1}, f_j)) = \mathrm{multideg}(p_{j-1} - p_j) \lneq \delta$ が得られる． □

2.4 ブッフベルガーのアルゴリズム

この補題から分かることは，同次の多項式の線形和を計算して次数が下がるとき，先頭項の打ち消しはすべて S 多項式たちの中に入ってしまっているということである．これは，同次とは限らない多項式 $f_1, \cdots, f_s$の線形和を用いてより低次の g を定める場合にも，同じことが言えそうである．つまり，I の基底 $\{f_1, \cdots, f_s\}$ に新たな基底として $g = S(f_i, f_j)$ や $S(f_i, g)$ などすべての S 多項式を付け加えていけば，いずれはグレブナー基底 G に至ると思われる．だから G がグレブナー基底であるための条件は，G の元どうしの S 多項式がすべて G で割り切れることだと考えられる．

定理 2-18.　Buchberger の S ペア判定条件

$k[x_1, \cdots, x_n]$ のイデアル I の基底 $G = \{g_1, \cdots, g_t\}$ がグレブナー基底であることは，次と同値である．
すべての $1 \leq i \neq j \leq t$ に対し，$S(g_i, g_j)$ が G で割り切れる．

証明　$(\Rightarrow)$ は $S(g_i, g_j) \in I$ より明らかなので，$(\Leftarrow)$ を示す．$f \in I, f \neq 0$ とする．$\forall i, j$ に対し $G \mid S(g_i, g_j)$ とする．このとき，$\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \cdots, \mathrm{LT}(g_t) \rangle$ であることを示せばよい．“$\supset$”は明らかなので，
$\mathrm{LT}(f) \in \langle \mathrm{LT}(g_1), \cdots, \mathrm{LT}(g_t) \rangle$ $\cdots (*)$ を示せば十分である．まずは証明の方針を述べる．

$f \in I$ に対し，$h_i \in k[x_1, \cdots, x_n]$ があって，$f = \sum_{i=1}^{t} h_i g_i \cdots (\star)$ と書ける．これに対し，$\mathrm{multideg}(f) \leq \max(\mathrm{multideg}(h_i g_i))$　$\cdots (\star\star)$ が分かる．もし“$\lneq$”が成立するならば，$(\star)$ の和の中で先頭項の打ち消し合いが起こっていることになる．補題 2-17. よりこれは S 多項式を使って書き直すことができる．今，S 多項式は G で割り切れると仮定しているので，S 多項式を項の打ち消し合いがより少ない式（G の元の $k[x_1, \cdots, x_n]$-線型和）で置き換えることができる．これを繰り返していくと，f を打ち消し合いのない線型和で書けて，$(\star\star)$ で等号が成立する．するとある i に対し，$\mathrm{multideg}(f) = \mathrm{multideg}(h_i g_i)$ が成り立つ．このとき $\mathrm{LT}(g_i) \mid \mathrm{LT}(f)$ が従い，$(*)$ が満たされる．

ここから証明の詳細を述べる．$m(i) = \mathrm{multideg}(h_i g_i)$，$\delta = \max\{m(1), \cdots, m(t)\}$ とおく．このとき $(\star\star)$ は $\mathrm{multideg}(f) \leq \delta$となる．さて，$f$ が $(\star)$ の形に書けるような表示の仕方は無数にある．その表示によって，対応する δ も異なる場合が考えられる．そこで，項順序は整列順序だから，そのうちで δ が最小となるような f の表し方 $(\star)$ を選ぶことができる．

一旦この最小の δ が選ばれると，$\mathrm{multideg}(f) = \delta$ となることを示す．これを示せば，$\mathrm{LT}(f)$ が $\mathrm{LT}(g_i)$ のどれかで割り切れるので $(*)$ が従い，証明は完了する．今，$\mathrm{multideg}(f) \lneq \delta$ を仮定し，矛盾を導くことにする．まずは $(\star)$ を，多重次数 δ の項を別にして次のように書く

$$\begin{aligned} f &= \sum_{m(i)=\delta} h_i g_i + \sum_{m(i)<\delta} h_i g_i \\ &= \sum_{m(i)=\delta} \mathrm{LT}(h_i) g_i + \sum_{m(i)=\delta} (h_i - \mathrm{LT}(h_i)) g_i + \sum_{m(i)<\delta} h_i g_i. \end{aligned}$$

仮定の $\mathrm{multideg}(f) \lneq \delta$より，2 行目の最初の和についても，$\mathrm{multideg}\left(\sum_{m(i)=\delta} \mathrm{LT}(h_i) g_i\right) \lneq \delta$となる．

$\mathrm{LT}(h_i) = c_i x^{\alpha(i)}$，$f_i = x^{\alpha(i)} g_i$とおくと，最初の和は $\sum_{m(i)=\delta} c_i f_i$と書ける．よって補題 2-17. よりこの和の中に先頭項の打ち消し合いがあり，$S(x^{\alpha(j)} g_j, x^{\alpha(l)} g_l)$ の k-線形和で書ける．更にこの S 多項式は δ 次未満で

$$S(x^{\alpha(j)}g_j,\, x^{\alpha(l)}g_l) = \frac{x^\delta}{x^{\alpha(j)}\mathrm{LT}(g_j)}x^{\alpha(j)}g_j - \frac{x^\delta}{x^{\alpha(l)}\mathrm{LT}(g_l)}x^{\alpha(l)}g_l \;= x^{\delta-\gamma_{jl}}S(g_j,g_l) \;\cdots(1)$$

と計算できる ($x^{\gamma_{jl}}$ =LCM(LM(g_j), LM(g_l))．したがって，$c_{jl} \in k$ が存在して

$$\sum_{m(i)=\delta} \mathrm{LT}(h_i)g_i = \sum_{j,l} c_{jl}x^{\delta-\gamma_{jl}}S(g_j,g_l)$$

が成り立つ．

次に，仮定 $G \mid S(g_j,g_l)$ より，$S(g_j,g_l) = \sum_{i=1}^{t} a_{i,jl}\, g_i$と書ける．ここで，$a_{i,jl} \in k[x_1,\cdots,x_n]$ である．また割り算なので

$$\mathrm{multideg}(\, a_{i,jl}\, g_i\,) \le \mathrm{multideg}(\, S(g_j,g_l)\,) \;\cdots(2)$$

が $\forall i,j,l$ に対して成り立つ．つまり S 多項式であるのに g_j, g_lの先頭項がすべて打ち消されるわけではない．

この事実を使って，f の表示式に戻って多重次数を評価したい．$S(g_j,g_l)$ の表示に $x^{\delta-\gamma_{jl}}$を掛けて

$$x^{\delta-\gamma_{jl}}S(g_j,g_l) = \sum_{i=1}^{t} b_{i,jl}\, g_i$$

を得る．ここで，$b_{i,jl} = x^{\delta-\gamma_{jl}}a_{i,jl}$ である．このとき，多重次数の評価に戻ると，(1) と (2) より

$$\mathrm{multideg}(b_{i,jl}\, g_i) \le \mathrm{multideg}(\, x^{\delta-\gamma_{jl}}\, S(g_j,g_l)\,) < \delta \;\cdots(3)$$

が導かれる．上の $x^{\delta-\gamma_{jl}}S(g_j,g_l)$ の表示を f の最初の和に代入して

$$\begin{aligned}\sum_{m(i)=\delta} \mathrm{LT}(h_i)g_i &= \sum_{j,l} c_{jl}x^{\delta-\gamma_{jl}}S(g_j,g_l)\\ &= \sum_{j,l} c_{jl}\left(\sum_i b_{i,jl}g_i\right) = \sum_i \tilde{h}_i g_i\end{aligned}$$

を得る．ここで,$\tilde{h}_i \in k[x_1,\cdots,x_n]$ である．これと (3) により，すべての i に対して

$$\mathrm{multideg}(\tilde{h}_i g_i) < \delta$$

が成立する．以上より，g_i の $k[x_1,\cdots,x_n]-$ 線形和としての f の表示を得たことになり，なおかつそのすべての項の多重次数が，δ より真に小さくできることが示された．これはδが最小であるという仮定に反する．したがって，背理法により結論が得られた． □

この S ペア判定条件と先の考察から，グレブナー基底を求める手順が分かる．具体的にグレブナー基底を計算してみよう．

例 2-19. $k[x,y]$ のイデアル I の lex 順序 ($x > y$) におけるグレブナー基底を求める．ここで $I = \langle f_1, f_2\rangle$, $f_1 = x^2y - 1, f_2 = xy^2 - x$ とする．

まず，$\{f_1,f_2\}$ が I のグレブナー基底であるかを判定する．lex 順序により

$$\mathrm{LT}(f_1) = x^2y,\ \mathrm{LT}(f_2) = xy^2,\ x^\gamma = \mathrm{LCM}(x^2y, xy^2) = x^2y^2$$

となり

$$S(f_1,f_2) = \frac{x^2y^2}{x^2y}(x^2y-1) - \frac{x^2y^2}{xy^2}(xy^2-x) = x^2 - y.$$

$\mathrm{LT}(S(f_1,f_2)) = x^2$ は $\mathrm{LT}(f_1)$ でも $\mathrm{LT}(f_2)$ で割り切れないので，$S(f_1,f_2)$ は $\{f_1,f_2\}$ で割り切れず，$\{f_1,f_2\}$ は I のグレブナー基底ではない．そこで，$f_3 := x^2 - y \in I$ を基底に加え，今度は $F = \{f_1,f_2,f_3\}$ について判定する．ここで，f の $G = \{g_1,\cdots,g_t\}$ による割り算が定義できるとき，その余りを $\overline{f}^G$と書く．

$$\begin{aligned}&S(f_1,f_2) = f_3 \text{ であるので，} \overline{S(f_1,f_2)}^F = 0,\\ &S(f_3,f_1) = -y^2+1 \quad \therefore \overline{S(f_3,f_1)}^F = -y^2+1 \neq 0.\end{aligned}$$

よって F も I のグレブナー基底ではない．さらに $f_4 := -y^2+1 \in I$ を加えて $F' = \{f_1, f_2, f_3, f_4\}$ とする

$$S(f_2, f_3) = -x^2 + y^3 = -f_3 - yf_4 \quad \therefore \overline{S(f_2, f_3)}^{F'} = 0,$$
$$\overline{S(f_1, f_2)}^{F'} = \overline{S(f_2, f_3)}^{F'} = \overline{S(f_3, f_1)}^{F'} = 0,$$
$$S(f_1, f_4) = x^2 - y = f_3,\ S(f_2, f_4) = 0,\ S(f_3, f_4) = x^2 - y^3 = f_3 + yf_4.$$

したがって，任意の $i, j \in \{1, 2, 3, 4\}$ かつ $i \neq j$ に対し，$\overline{S(f_i, f_j)}^{F'} = 0$ が示され

$$F' = \{x^2y - 1, xy^2 - x, x^2 - y, -y^2 + 1\}$$

を I のグレブナ基底の 1 つとして得られた．この F'は $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(f_1), \cdots, \mathrm{LT}(f_4) \rangle$ を満たす．

このような方法でグレブナー基底は求めることができる．グレブナー基底は基底としては不要なものを含んでいるが，I の元でより低次のものまで一目で分かるようになっている．この例での求め方はすぐに一般化できる．ただしアルゴリズムとして使うためには，有限回の操作で解に辿り着くことが保証されるべきである．

定理 2-20.　Buchberger のアルゴリズム

$k[x_1, \cdots, x_n]$ の 0 でないイデアル $I = \langle f_1, \cdots, f_s \rangle$ のグレブナー基底は，次のアルゴリズムにより有限回のステップで構成することができる．

Input: $F = \{f_1, \cdots, f_s\}$
Output: a Groebner basis $G = (g_1, \cdots, g_t)$ for I, with $F \subset G$
$G := F$
REPEAT
　$G' := G$
　FOR each pair $\{p, q\}$, $p \neq q$ in G' DO
　　$S := \overline{S(p, q)}^{G'}$
　　IF $S \neq 0$ THEN $G := G' \cup \{S\}$
UNTIL $G = G'$

証明　$G = \{g_1, \cdots, g_t\}$ に対し，$\langle G \rangle = \langle g_1, \cdots, g_t \rangle$，$\langle \mathrm{LT}(G) \rangle = \langle \mathrm{LT}(g_1), \cdots, \mathrm{LT}(g_t) \rangle$ と書く．まず，アルゴリズムの各段階において $G \subset I$ であることを示す．最初の段階では $G = F \subset I$ である．G を大きくするときは常に $p, q \in G' := G$ に対し $S = \overline{S(p, q)}^{G'}$ を付け加える．だから，もし $G' \subset I$ ならば $p, q \in I$ であり $S(p, q) \in I$ となる．それを $G' \subset I$ で割るので，$S \in I$ であり，$G := G' \cup \{S\} \subset I$ を得る．したがって帰納的に，各段階で $G \subset I$ が成立し，$F \subset G$ より G は I の基底となる．

アルゴリズムは $G = G'$となったときに停止する．これは，すべての $p, q \in G, p \neq q$ に対して$\overline{S(p, q)}^{G'} = 0$ となることを意味する．よって S ペア判定条件より G は I のグレブナー基底である．

残るはアルゴリズムが停止することの証明である．メインループの各段階において $G' \subset G$ であるので，$\langle \mathrm{LT}(G') \rangle \subset \langle \mathrm{LT}(G) \rangle \cdots (\star)$ である．さらに，$G' \subsetneq G$ であるならば $\langle \mathrm{LT}(G') \rangle \subsetneq \langle \mathrm{LT}(G) \rangle$ である．なぜならば，$S \neq 0$ に対し $G = G' \cup \{S\}$ とするとき，$\mathrm{LT}(S)$ は $\mathrm{LT}(G')$ のどの元でも割り切れないので，だから $\mathrm{LT}(S) \notin \langle \mathrm{LT}(G') \rangle$ であるが，$\mathrm{LT}(S) \in \langle \mathrm{LT}(G) \rangle$ でもあるからである．この対偶を考えると，すなわち $\langle \mathrm{LT}(G') \rangle = \langle \mathrm{LT}(G) \rangle$ ならば $G = G'$である．

($\star$) より，ループを繰り返すことでイデアル $\langle \mathrm{LT}(G')\rangle$ は $k[x_1,\cdots,x_n]$ の増大列をなす．ACC より，有限回このループを繰り返すとこの増大列は安定する．よって，いつかは $\langle \mathrm{LT}(G')\rangle = \langle \mathrm{LT}(G)\rangle$ つまり $G = G'$ となり，アルゴリズムは有限回のステップの後に停止する． □

このアルゴリズムは未発達なバージョンに過ぎず，実際に計算システムで用いられているものには計算を効率的に行うための様々な改良が施されている．簡単な例では，上のアルゴリズムでは同じ組み合わせの S 多項式を何度も計算し，その基底による余りも何度も計算することになるが，割り切れることが前のステップで分かっている S 多項式については計算を省くことができる．あとは，新しく付け加える基底の係数として煩雑な有理数が出てくる場合や計算の途中に出てくる多項式の全次数が極めて大きくなることがよく起こるが，変数変換や変数の順序の入れ替えによって計算量を劇的に減らすことができる場合が多い．

2.5 簡約グレブナー基底

また，定理 2-20. のアルゴリズムでグレブナー基底を計算すると，しばしば多量の不必要な生成元を含むことがある．この不要な生成元を取り除き，グレブナー基底を簡潔に書けるようにする．

補題 2-21. G を多項式イデアル I のグレブナー基底とする．$p \in G$ を $\mathrm{LT}(p) \in \langle \mathrm{LT}(G-\{p\})\rangle$ となる多項式とする．このとき，$G-\{p\}$ もまた I のグレブナー基底である．

証明 グレブナー基底の定義から $\langle \mathrm{LT}(G)\rangle = \langle \mathrm{LT}(I)\rangle$ である．$\mathrm{LT}(p) \in \langle \mathrm{LT}(G-\{p\})\rangle$ であるとすれば $\langle \mathrm{LT}(G-\{p\})\rangle = \langle \mathrm{LT}(I)\rangle$ である．よって，$G-\{p\}$ も I のグレブナー基底である． □

G の元をすべてに対し先頭係数が 1 になるように定数倍して，$\mathrm{LT}(p) \in \mathrm{LT}(G-\{p\})$ となるすべての p を G から除くと，極小グレブナー基底と呼ばれるものに至る．

定義 2-22. イデアル I の**極小グレブナー基底**とは，I のグレブナー基底 G で次の条件を満たすものである
(1) すべての $p \in G$ に対して，$\mathrm{LC}(p) = 1$ である，
(2) すべての $p \in G$ に対して，$\mathrm{LT}(p) \notin \langle \mathrm{LT}(G-\{p\})\rangle$ である．

例 2-23. 例 2-19. のイデアル I の極小グレブナー基底を求める．lex 順序でのグレブナー基底は

$$f_1 = x^2y - 1,\ f_2 = xy^2 - x,\ f_3 = x^2 - y,\ f_4 = -y^2 + 1$$

であった．$\mathrm{LT}(f_1) = x^2y = y \cdot \mathrm{LT}(f_3)$ であるので，f_1を極小グレブナー基底から除くことができる．同様に $\mathrm{LT}(f_2) = xy^2 = -y \cdot \mathrm{LT}(f_4)$ より，f_2 も消去できる．f_3 と f_4 については，互いに互いの先頭項を割り切らない．よって I の極小グレブナー基底は

$$f_3 = x^2 - y,\ f_4' := -f_4 = y^2 - 1.$$

ここで，$f_3' := x^2 + ay^2 - y - a$，$f_4' = y^2 - 1$ $(a \in k)$ もまた I の極小グレブナー基底である．

k を無限体とすると，f_3' のように極小グレブナー基底は無数に作ることができてしまう．しかし，幸いにも

その中から最も良い極小グレブナー基底を 1 つ選び出すことができる．

定義 2-24.　イデアル I の**簡約グレブナー基底**とは，I のグレブナー基底 G で次の条件を満たすものである
(1)　すべての $p \in G$ に対して，$\mathrm{LC}(p) = 1$ である，
(2)　すべての $p \in G$ に対して，p のすべての項が $\langle \mathrm{LT}(G - \{p\}) \rangle$ に含まれない．

例 2-23. について言えば，$a = 0$ である $\{f_3, f_4'\}$ だけが簡約されていることになる．一般に簡約グレブナー基底は次の優れた性質をもつ．

命題 2-25.　$I \neq \{0\}$ を多項式イデアルとする．指定された項順序に関して，I は唯一の簡約グレブナー基底を持つ．

証明　G を I の極小グレブナー基底とする．g のいかなる項も $\langle \mathrm{LT}(G - \{p\}) \rangle$ に含まれないとき，$g \in G$ が G に関して**簡約されている**という．前半の目標は，すべての元が G に関して簡約されているように G を作り直すことである．

$g \in G$ を簡約化したものを g'とし，G において g と g'を置き換えたものを G'とする．これを定式化すると次のように書ける

$$g' = \overline{g}^{G-\{g\}},\ G' = (G - \{g\}) \cup g'.$$

このように表せば，g'はどの項も $\langle \mathrm{LT}(G - \{g\}) \rangle$ に含まれない．$G - \{g\} = G' - \{g'\}$ だから，言い換えると g'のどの項も $\langle \mathrm{LT}(G' - \{g'\}) \rangle$ に含まれない．よって，G'も極小グレブナー基底であるならば，g'は G'に関しても簡約されている．

ここで，G'も極小グレブナー基底であるという仮定が正しいことを示さねばならない．それには $\langle \mathrm{LT}(G') \rangle = \langle \mathrm{LT}(G) \rangle$ を示せばよい．しかし $G - \{g\} = G' - \{g'\}$ だから，$\mathrm{LT}(g') = \mathrm{LT}(g)$ のみを示せば十分である．g と g'を比較すると，$g' = \overline{g}^{G-\{g\}}$ であった．G の極小性より，$\mathrm{LT}(g)$ は $\mathrm{LT}(G - \{g\})$ で割り切れないので，$\mathrm{LT}(g') = \overline{\mathrm{LT}(g)}^{G-\{g\}} = \mathrm{LT}(g)$ である．よって G'はグレブナー基底であり，その極小性も分かる．

この G を G'に置き換える操作をすべての元が簡約されるまで続ける．この操作でグレブナー基底は毎回 1 つずつ置き換えられていくが，先頭項はすべて変わらない (極小性は保たれる)．簡約グレブナー基底の定義はその先頭項によるから，すべての先頭項が変わらなければ，一旦簡約された元は操作を繰り返してもそのまま簡約された元であり続ける．したがってこの操作は高々 $\#\ G$ 回つまり有限回で終わり，簡約グレブナー基底が得られる．

後半は簡約グレブナー基底の一意性を示す．G と $\widetilde{G}$ を I の簡約グレブナー基底とする．G と $\widetilde{G}$ は特に極小グレブナー基底であり，その定義より $\mathrm{LT}(G) = \mathrm{LT}(\widetilde{G})$ と分かる（なぜならば極小グレブナー基底とは，その元がどれか 1 つでも欠けるとグレブナー基底でなくなるものだから，$\mathrm{LT}(G) \neq \mathrm{LT}(\widetilde{G})$ と仮定すると G と $\widetilde{G}$ のいずれかがグレブナー基底でなくなり，矛盾が起こるからである)．よって任意の $g \in G$ に対し $\mathrm{LT}(g) = \mathrm{LT}(\tilde{g})$ なる $\tilde{g}$ が存在する．この各々で $g = \tilde{g}$ が成り立てば，$G = \widetilde{G}$ すなわち題意の一意性が示される．

$g - \tilde{g} \in I$ であるので，$\overline{g - \tilde{g}}^{G} = 0$ である．$\mathrm{LT}(g) = \mathrm{LT}(\tilde{g})$ は分かっており，この両者は $g - \tilde{g}$ の中で打ち消し合う．G と $\widetilde{G}$ が簡約されていたことから，$g - \tilde{g}$ の残りの項はすべて $\mathrm{LT}(G) = \mathrm{LT}(\widetilde{G})$ のどれでも割り切れない（もしくは，割り切れるが $g - \tilde{g}$ である)．割り切れない場合，$\overline{g - \tilde{g}}^{G} = g - \tilde{g}$ が成立するので，結局 $g - \tilde{g} = 0$ が従う．　□

この一意性より，応用としてイデアルの一致アルゴリズムが得られる．2 つの多項式イデアルがいつ等しくなるかを知るためには，項順序を固定して両者の簡約グレブナー基底を計算し，それらがいつ一致するかを見ればよい．

また，1 次の多項式から生成されるイデアルの場合，拡大係数行列に行簡約化のアルゴリズムを使うことで，簡約グレブナー基底は簡単に計算できる．行簡約化もグレブナー基底の簡約化も，どちらも多項式どうしの割り算を行っており，その余りに置き換えているという点では同じある．余りの一意性から，行簡約化によって得られた式も一意であり，簡約グレブナー基底となる．

例 2-26. $I = \langle 3x + 2y - z, 2x - y + 3z \rangle \subset \mathbb{R}[x, y, z]$ とする．

拡大係数行列 $\begin{pmatrix} 3 & 2 & -1 \\ 2 & -1 & 3 \end{pmatrix}$ を行簡約化する

$$\begin{pmatrix} 3 & 2 & -1 \\ 2 & -1 & 3 \end{pmatrix} \rightarrow \underset{\text{(階段形)}}{\begin{pmatrix} 1 & 3 & -4 \\ 0 & 1 & -\frac{11}{7} \end{pmatrix}} \rightarrow \underset{\text{(行簡約形)}}{\begin{pmatrix} 1 & 0 & \frac{5}{7} \\ 0 & 1 & -\frac{11}{7} \end{pmatrix}}.$$

lex 順序 $x > y > z$ を用いる．階段形に対応する $\{x + 3y - 4z,\ y - \frac{11}{7}z\}$ は I の極小グレブナー基底となっている．そして，さらに行簡約形に対応する $\{x + \frac{5}{7},\ y - \frac{11}{7}z\}$ は I の簡約グレブナー基底となっている．

ここまでで任意の多項式イデアル I に対して簡約グレブナー基底が計算できるようになった．I を簡約グレブナー基底で表すと，連立方程式の解 $\mathbf{V}(I)$ の計算がより簡単になる．

3 消去理論

この章で多項式連立方程式を代数的に解く手順とその証明を与える．それは消去定理と拡張定理によって与えられる．消去定理の応用として陰関数表示化の問題を紹介する．また，閉包定理によって拡張定理の幾何学的な解釈を述べ，最後に終結式を使って拡張定理の証明を完成させる．

3.1 消去定理・拡張定理

前章の最後に述べたように，多項式連立方程式を効率よく解くためにグレブナー基底を計算するのだった．グレブナー基底がどのような働きをするのか，まずは実際に具体的な連立方程式の解を求めてみる．

例 3-1.

$$\begin{aligned} x^2 + y + z &= 1, \\ x + y^2 + z &= 1, \qquad \cdots\cdots (1) \\ x + y + z^2 &= 1. \end{aligned}$$

$I = \langle x^2 + y + z - 1\ , x + y^2 + z - 1\ , x + y + z^2 - 1 \rangle \subset \mathbb{C}[x, y, z]$ とおくと，lex 順序に関する I のグレブナー基底は次の 4 本の多項式となる

$$g_1 = x + y + z^2 - 1,$$

$$g_2 = y^2 - y - z^2 + z,$$
$$g_3 = 2yz^2 + z^4 - z^2,$$
$$g_4 = z^6 - 4z^4 + 4z^3 - z^2.$$

これは (1) と同じ解を持つことが分かる．この場合 g_4は z のみを変数に持つので

$$g_4 = z^2(z-1)^2(z^2+2z-1) \quad \therefore\ z = 0, 1, -1 \pm \sqrt{2}.$$

この z の値を $g_2 = 0$ もしくは $g_3 = 0$ に代入すると y の値も決めることができ，さらにそれらを $g_1 = 0$ に代入すれば x の値も決められる．よって (1) の解は次のように分かる

$$(1,0,0),\ (0,1,0),\ (0,0,1),\ (-1+\sqrt{2}, -1+\sqrt{2}, -1+\sqrt{2}),\ (-1-\sqrt{2}, -1-\sqrt{2}, -1-\sqrt{2}).$$

ここで重要だったのは次の 2 つの操作である．

（消去のステップ）もとの連立方程式から z のみを含む方程式を得ることができた．つまり x, y を消去した．

（拡張のステップ）z の値が決まると，これらの解を連立方程式の解にまで拡張することができた．

消去理論とは，この 2 つのステップが非常に一般的にできるということを示す理論である．

ここで注目したいのは，変数の消去が行われた点である．グレブナー基底を計算することにより，順序の大きい変数から次数が下げられるのであった．すると 0 次まで下げることができた変数は，消去されたことになる．また変数を消去された式を観察すると，g_4 は I を用いて，$g_4 \in I \cap \mathbb{C}[z]$ と書ける．

定義 3-2.　与えられたイデアル $I = \langle f_1, \cdots, f_s \rangle \subset k[x_1, \cdots, x_n]$, $l \in \{0, 1, \cdots, n\}$ に対して

$$I_l = I \cap k[x_{l+1}, \cdots, x_n]$$

で定義される $k[x_{l+1}, \cdots, x_n]$ のイデアルを，**l 次の消去イデアル**という．

I_l は連立方程式 $f_1 = \cdots = f_s = 0$ から変数 $x_1, \cdots, x_l$ を消去して得られる式全体であり，イデアルとなる．ここで $I = I_0$ である．また，消去イデアルは項順序に依存せず，変数の順序に依存する．

変数の消去とは消去イデアルの元を求めることを意味する．言い換えると，変数 $x_1, \cdots, x_l$ を消去することが可能であるということは，消去イデアル I_l が 0 でない元をもつことである．ただし消去イデアル $I_l = \{0\}$ である場合もある．それは I のグレブナー基底のすべてに $x_1, \cdots, x_l$のいずれかが含まれる場合である．例えば $I = \langle xy \rangle \subset k[x, y]$ の場合，$I_1 = \{0\}$ である．これは消去ができない例である．

定理 3-3.　**消去定理**

$I \subset k[x_1, \cdots, x_n]$ をイデアルとし，G を I の lex 順序 $x_1 > \cdots > x_n$に関するグレブナー基底であるとする．このとき，$l \in \{0, 1, \cdots, n\}$ に対して

$$G_l = G \cap k[x_{l+1}, \cdots, x_n]$$

は l 次の消去イデアル I_l のグレブナー基底である．

証明　$G_l \subset I_l$ であるので，グレブナー基底の定義より $\langle \mathrm{LT}(I_l) \rangle = \langle \mathrm{LT}(G_l) \rangle$ を示せばよい．“ $\supset$ ”は明らかなので，“ $\subset$ ”を示すために，$f \in I_l$ の先頭項 $\mathrm{LT}(f)$ が適当な $g \in G_l$ をとれば $\mathrm{LT}(g)$ で割り切れることを示す．

$f \in I$ でもあるから，G が I のグレブナー基底であることより，$\mathrm{LT}(f)$ は適当な $g \in G$ をとれば $\mathrm{LT}(g)$ で割り切れる．

この $\mathrm{LT}(g)$ は $f \in I_l = I \cap k[x_{l+1}, \cdots, x_n]$ の先頭項を割り切るので，$\mathrm{LT}(g) \in k[x_{l+1}, \cdots, x_n]$ であると分かる．これと lex 順序 $x_1 > \cdots > x_n$ より $g \in k[x_{l+1}, \cdots, x_n]$ が従い，$g \in G_l$ が示された．　□

ここで例 3-1. に戻る．$I = \langle x^2+y+z-1\ , x+y^2+z-1\ , x+y+z^2-1\rangle$ のグレブナー基底を思い出すと，消去定理により g_1, g_2, g_3, g_4 によって各次の消去イデアルが生成できる

$$I_1 = I \cap \mathbb{C}[y,z] = \langle y^2-y-z^2+z, 2yz^2+z^4-z^2, z^6-4z^4+4z^3-z^2\rangle,$$
$$I_2 = I \cap \mathbb{C}[z] = \langle z^6-4z^4+4z^3-z^2\rangle.$$

つまりグレブナー基底とは可能な消去の仕方の中で最も合理的に消去が行われた式なのである．

次に，拡張のステップについて議論する．$k[x_1, \cdots, x_n]$ のイデアル I について $\mathbf{V}(I)$ の点を記述することが問題である．$l \in \{1, \cdots, n\}$ に対し，消去イデアル I_l をおく．$(x_{l+1}, \cdots, x_n) = (a_{l+1}, \cdots, a_n) \in \mathbf{V}(I_l)$ をもとの方程式系の**部分解**という．$(a_{l+1}, \cdots, a_n)$ を $\mathbf{V}(I)$ の完全な解にまで拡張するために，座標を 1 つずつ付け加えていく．つまり $(a_l, a_{l+1}, \cdots, a_n) \in \mathbf{V}(I_{l-1})$ となるような $x_l = a_l$ を求める．

ここで問題となるのは，この方程式系は共通根を持たないかもしれないということである．つまり，完全な解に拡張できない部分解があるかもしれない．

例 3-4. 次の連立方程式を考える

$$xy = xz = 1.$$

$\mathbb{R}[x,y,z]$ のイデアル $I = \langle xy-1, xz-1\rangle$ をおき，消去定理より消去イデアル $I_1 = I \cap \mathbb{R}[y,z] = \langle y-z\rangle$ が得られる．よって，部分解は $(y,z) = (a,a)$，$a \in \mathbb{R}$ で与えられ，これを拡張すると完全解は $(x,y,z) = (\frac{1}{a}, a, a)$ で与えられる．

ただし，部分解が $(y,z) = (0,0)$ のときは拡張できない．幾何学的にこれを確かめると, 完全解に対応する多様体は平面 $y = z$ 内の双曲線であり，これは直線 $\{\,(x,y,z)\,|\,y = z \wedge x = 0\,\}$ と x 軸に漸近する．つまり $\mathbb{R}^3$ 内で x 軸と交点をもたない．これが部分解 $(y,z) = (0,0)$ のときだけ拡張できない理由である（無限遠点まで含めると $(\infty, 0, 0)$ に拡張できる）．

どの部分解が完全解にまで拡張できるかは，実際に拡張を試みなくてもあらかじめ知ることができる．

定理 3-5. 拡張定理

イデアル $I = \langle f_1, \cdots, f_s\rangle \subset \mathbb{C}[x_1, \cdots, x_n]$ を考え，I_1を I の 1 次の消去イデアルとする．$i \in \{1, \cdots, s\}$ に対して，f_i を次の形に書く

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

ここで，$N_i \geq 0$ とし，$g_i \in \mathbb{C}[x_2, \cdots, x_n]$ は 0 でない多項式である．部分解 $(x_2, \cdots, x_n) = (a_2, \cdots, a_n) \in \mathbf{V}(I_1)$ があると仮定する．このとき，$(a_2, \cdots, a_n) \notin \mathbf{V}(g_1, \cdots, g_s)$ ならば，$a_1 \in \mathbb{C}$ が存在して $(a_1, a_2, \cdots, a_n) \in \mathbf{V}(I)$ である．

証明には終結式が必要なので後回しにする．今は拡張定理の主張する意味を考えていく．

拡張定理が $\mathbb{C}$ 上で考えられている理由は代数学の基本定理による．例えば，$k = \mathbb{R}$ 上で連立方程式 $x^2 = y = z$ を考える．$f_1 = x^2 - y$, $f_2 = x^2 - z$, $I = \langle f_1, f_2\rangle \subset \mathbb{R}[x,y,z]$, $I_1 = I \cap \mathbb{R}[y,z]$ とする．このとき f_1, f_2 は次の形に書ける

$$f_1 = 1 \cdot x^2 + (-y),\ f_2 = 1 \cdot x^2 + (-z).$$

x を消去すると $I_1 = \langle y - z \rangle$ となるので，部分解 $(y, z) = (a, a) \in \mathbf{V}(I_1)$, $a \in \mathbb{R}$ を得る．このとき f_1と f_2 の x に関する先頭係数は $1 \neq 0$ だから，拡張定理によって，部分解 (a, a) は $\mathbb{C}$ 上では拡張できる．しかし $\mathbb{R}$ 上で考えると，$a < 0$ のとき $x^2 = a$ は解を持たない．よって $a \geq 0$ のときにしかこの部分解は拡張できない．つまり，$\mathbb{R}$ 上では拡張定理は成立しない．但し $\mathbb{C}$ 上に限らずとも代数的閉体上ならば，このような解をもたないことは起こらないので，拡張定理は成立する．

では，部分解 $(x_2, \cdots, x_n) = (a_2, \cdots, a_n)$ が拡張可能であるための十分条件 $(a_2, \cdots, a_n) \notin \mathbf{V}(g_1, \cdots, g_s)$ は一体何を意味しているのだろうか．$f_i = 0$ に $(x_2, \cdots, x_n) = (a_2, \cdots, a_n)$ を代入すると，変数が x_1のみの方程式になる．$(a_2, \cdots, a_n) \in \mathbf{V}(g_1, \cdots, g_s)$ であるとは，この代入によってすべての f_i が x_1の最高次の項を消されることを意味する．このときに限って，f_i たちが共通根 $x_1 = a_1$ をもたない可能性があることを拡張定理は示している．これを例 3-4. で確かめると，連立方程式 $xy = xz = 1$ は部分解 $(y, z) = (a, a)$ を持っていた．このうち x の先頭係数 y と z を同時に 0 にする部分解 $(y, z) = (0, 0)$ だけが拡張できない可能性を持つことになるが，$(x, 0, 0)$ という形の解は実際に無いことが簡単に分かる．

ここで，$\mathbf{V}(g_1, \cdots, g_s)$ は I の基底 $\{f_1, \cdots, f_s\}$ のとり方によって変わってくる．もし $\mathbf{V}(g_1, \cdots, g_s)$ が大きいと，拡張定理で判定できないような部分解 $(a_2, \cdots, a_n) \in \mathbf{V}(g_1, \cdots, g_s)$ がより多く出てくるだろう．そうなると計算が面倒になるので，$\mathbf{V}(g_1, \cdots, g_s)$ が最も小さくなるような $\{f_1, \cdots, f_s\}$ のとり方が欲しい．これは射影完備化という方法で，射影代数幾何の道具立てが必要となる（下巻第 8 章参照）．また，アフィン空間に無限遠点の集合を加えた射影空間で考えれば，すべての部分解が拡張可能となることが分かっている（それまで拡張できなかった漸近線上の部分解でも，無限遠点を全体解に含むことで拡張できるようになる）．

また，定理では $x_1 = a_1$が存在するための十分条件を述べているが，変数がいくつ消去された段階においても拡張定理は同様に使うことができる．よって 2 次以上の拡張をする場合は，拡張定理を繰り返し用いればよい．

最後に，始めに部分解を求めるときや拡張するときに代数的解が求められない場合があることを述べる．

例 3-6.　次の連立方程式を考える

$$xy = 4,$$
$$y^2 = x^3 - 1.$$

lex 順序を使うと，グレブナー基底は

$$g_1 = 16x - y^4 - y^2,$$
$$g_2 = y^5 + y^3 - 64$$

で与えられる．$y^5 + y^3 - 64 = 0$ は $y = \pm 1, \pm 2, \pm 4, \cdots, \pm 64$ を満たさないので，g_2 は $\mathbb{Z}$ 上既約であり，すなわち $\mathbb{Q}$ 上既約である．よって $g_2 = 0$ は有理根を持たず，冪根を用いて解けるかもすぐには分からない (楕円曲線 $y^2 = x^3 - 1$ は $(1, 0)$ しか有理点を持たないが，$xy = 4$ がこれを満たさない)．

このような場合には数値的に解を求めるしかない．これにはニュートン − ラフソン法など様々な方法があり，それにより $g_2 = 0$ を解くと

$$y = 2.21363,\ -1.78719 \pm 1.13984i,\ 0.680372 \pm 2.26969i$$

が得られる．これらを $g_1 = 0$ に代入して，数値近似解を決めることができる．部分解を数値的に求めた場合でも拡張定理は使うことができる．また，拡張定理における g_i がすべて 0 に近づくような部分解が得られた

場合は，その付近に拡張が失敗するような部分解があると推測できる．また拡張された解が極端な値をとるときは，その付近で解が発散していると推測できる．

3.2 消去の幾何

前節の定理の幾何学的な解釈を与える．大まかに言うと，変数の消去は多様体をより低次元の部分空間上に射影することに対応している．しかし，拡張定理によれば，変数消去によって得られた部分解は完全解の射影に比べて余分な点を含んでいることがある．これが拡張できない部分解であった．この余分な点を評価するのが閉包定理である．

まず，アフィン多様体の射影を定義する．アフィン多様体 $V = \mathbf{V}(f_1, \cdots, f_s) \subset \mathbb{C}^n$が与えられているとする．変数 $x_1, \cdots, x_l$ を消去するために，**射影写像**

$$\pi_l : \mathbb{C}^n \longrightarrow \mathbb{C}^{n-l}$$

を考える．これは $(a_1, \cdots, a_n)$ を $(a_{l+1}, \cdots, a_n)$ に写す．V の射影 $\pi_l(V)$ と I_l を関係付けていく．

補題 3-7.　上記の記号を使う．$I_l = \langle f_1, \cdots, f_s \rangle \cap \mathbb{C}[x_{l+1}, \cdots, x_n]$ を l 次の消去イデアルとする．このとき，$\mathbb{C}^{n-l}$において

$$\pi_l(V) \subset \mathbf{V}(I_l)$$

が成立する．

証明　$f \in I_l$ とする．$(a_1, \cdots, a_n) \in V = \mathbf{V}(f_1, \cdots, f_s)$ に対し，$f \in \langle f_1, \cdots, f_s \rangle$ であるから $f(a_1, \cdots, a_n) = 0$ である．だが f は $x_1, \cdots, x_l$ に依存しないから

$$f(a_{l+1}, \cdots, a_n) = f(\pi_l(a_1, \cdots, a_n)) = 0$$

と書ける．これは，f が$\pi_l(V)$ のすべての点で消えることを示している．よって$\pi_l(V) \subset \mathbf{V}(f)$　□

この補題により，$\pi_l(V)$ は次のように書ける

$$\pi_l(V) = \left\{ (a_{l+1}, \cdots, a_n) \in \mathbf{V}(I_l) : \begin{array}{l} (a_1, \cdots, a_l, a_{l+1}, \cdots, a_n) \in V \\ \text{となる } a_1, \cdots, a_l \in \mathbb{C} \text{ が存在する} \end{array} \right\}.$$

よって，$\pi_l(V)$ は完全解にまで拡張できる部分解全体にちょうど一致している．

この例として，例 3-4. の多様体 $V = \mathbf{V}(I) \subset \mathbb{C}^3$, $I = \langle xy-1, xz-1 \rangle$ を考える．$S(xy-1, xz-1) = y - z$ だから，消去定理より 1 次の消去イデアルは $I_1 = \langle y - z \rangle$ である．よって部分解 $\mathbf{V}(I_1)$ は $\mathbb{C}^2$ 内の直線 $y = z$ である．一方，射影 $\pi_1 : \mathbb{C}^3 \longrightarrow \mathbb{C}^2$を x 座標を除外する（x 座標に定数を代入する）写像とする．V の点は $(\frac{1}{a}, a, a)$, $a \neq 0$ であるので

$$\pi_1(V) = \{ (a, a) \in \mathbb{C}^2 \,|\, a \neq 0 \}$$

である．ここで,$\pi_1(V)$ はアフィン直線から 1 点 $(0, 0)$ を除いた集合だから，アフィン多様体ではない．このような欠けた点の正体は次の幾何学的拡張定理から直ちに分かる．

定理 3-8.　幾何学的拡張定理

多様体 $V = \mathbf{V}(f_1, \cdots, f_s) \subset \mathbb{C}^n$に対し，$g_i$ を拡張定理で与えた関数とする．I_1を $\langle f_1, \cdots, f_s \rangle$ の 1 次の消去イデアルとする．このとき，$\mathbb{C}^{n-1}$における次の等式が成り立つ

$$\mathbf{V}(I_1) = \pi_1(V) \cup (\mathbf{V}(g_1, \cdots, g_s) \cap \mathbf{V}(I_1)).$$

ここで, $\pi_1 : \mathbb{C}^n \to \mathbb{C}^{n-1}$は, x_1を除いた $n-1$ 変数への射影である.

しかしこの欠けた部分 $\mathbf{V}(g_1, \cdots, g_s)$ の大きさまでは分からないし, ときに不自然に大きくなることもある. 例えば, 連立方程式 $(y-z)x^2 + xy = (y-z)x^2 + xz = 1$ は, $xy = xz = 1$ と同じイデアル I を生成し, 消去イデアルも同じ $I_1 = \langle y - z \rangle$ であることが分かる. このとき, 欠けた部分 $\mathbf{V}(g_1, \cdots, g_s)$ に相当するのは $\mathbf{V}(y-z)$ であり, これは部分解 $\mathbf{V}(I_1)$ と一致してしまう. よってこの場合は拡張定理を使っても効果が無い. また, 定理 3-8. は

$$\mathbf{V}(I_1) = \pi_1(V) \cup (\mathbf{V}(g_1, \cdots, g_s) \cap \mathbf{V}(I_1))$$

となるので, $\pi_1(V)$ の大きさについても何も分からない. だが幸いにも, 次の定理によって $\mathbf{V}(g_1, \cdots, g_s)$ や $\pi_1(V)$ の大きさについて強い主張が得られる.

定理 3-9.　閉包定理

$V = \mathbf{V}(f_1, \cdots, f_s) \subset \mathbb{C}^n$とおき, I_l を $\langle f_1, \cdots, f_s \rangle$ の l 次の消去イデアルとする. このとき次が成り立つ

(i)　$\mathbf{V}(I_l)$ は $\pi_l(V) \subset \mathbb{C}^{n-l}$を含む最小のアフィン多様体である,

(ii)　$V \neq \emptyset$ であるとき, $\mathbf{V}(I_l) - W \subset \pi_l(V)$ となるアフィン多様体 $W \subsetneq \mathbf{V}(I_l)$ がある.

(i) を満たす $\mathbf{V}(I_l)$ を $\pi_l(V)$ のザリスキー閉包という. (i) の証明は第 4 章で行う. (ii) は$\pi_l(V) \subset \mathbf{V}(I_l)$ が $\mathbf{V}(I_l)$ の大部分を覆っているということを意味する. ここでは, $l = 1$ の場合に限り (ii) を証明する.

証明　幾何学的拡張定理による次の結果を用いる

$$\mathbf{V}(I_1) = \pi_1(V) \cup (\mathbf{V}(g_1, \cdots, g_s) \cap \mathbf{V}(I_1)).$$

$W = \mathbf{V}(g_1, \cdots, g_s) \cap \mathbf{V}(I_1)$ とすると, 補題 1-4. より W はアフィン多様体である. 上の分解より, $\mathbf{V}(I_1) - W \subset \pi_1(V) \subset \mathbf{V}(I_l)$ が得られ, $W \neq \mathbf{V}(I_1)$ が示されれば証明は完了する. しかしながら, 閉包定理の直前の例のように $W = \mathbf{V}(I_1)$ となることもある.

この場合には, W が小さくなるように, V を定義する連立方程式を上手く書き換える必要がある. まずは次のように書き換える

$$\text{もし } W = \mathbf{V}(I_1) \text{ ならば } V = \mathbf{V}(f_1, \cdots, f_s, g_1, \cdots, g_s). \quad \cdots(2)$$

まずはこれを示す. 両辺が互いに包含していることを示せばよいが

$$\mathbf{V}(f_1, \cdots, f_s, g_1, \cdots, g_s) \subset \mathbf{V}(f_1, \cdots, f_s) = V$$

は明らかである. 逆方向の包含関係を示すために, $(a_1, \cdots, a_n) \in V$ とする. 各 f_i はこの点で消える. また $(a_2, \cdots, a_n) \in \pi_1(V) \subset \mathbf{V}(I_1) = W \subset \mathbf{V}(g_1, \cdots, g_s)$ であるから, 各 g_i はここで消える. したがって

$$(a_1, \cdots, a_n) \subset \mathbf{V}(f_1, \cdots, f_s, g_1, \cdots, g_s)$$

となり, (2) が証明された.

$I = \langle f_1, \cdots, f_s \rangle$ をもとのイデアルとする. また, $\widetilde{I} = \langle f_1, \cdots, f_s, g_1, \cdots, g_s \rangle$ とする. (2) のように, 仮に I と$\widetilde{I}$は同じ多様体 V を定義するとしても, イデアル自体は異なるかも知れない. よって I_1 と $\widetilde{I}_1$ も異なるかも知れない. しかし, (i) より $\mathbf{V}(I_1)$ と $\mathbf{V}(\widetilde{I}_1)$ は共に $\pi_l(V)$ を含む最小のアフィン多様体であるから $\mathbf{V}(I_1) = \mathbf{V}(\widetilde{I}_1)$ が従う.

次は V をさらに書き換える. $\widetilde{I}$ のより簡潔な基底を求める

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

ここで，$N_i \leq 0$ かつ $g_i \in \mathbb{C}[x_2, \cdots, x_n]$ は 0 でない．今

$$\tilde{f}_1 = f_i - g_i {x_1}^{N_i}$$

とおけば

$$\widetilde{I} = \langle \tilde{f}_1, \cdots, \tilde{f}_s, g_1, \cdots, g_s \rangle$$

と書き換えられる．ここで，$\tilde{f}_i$ は 0 であるか，x_1に関する次数が f_i よりも真に小さいかどちらかである．

さて，幾何学的拡張定理を $V = \mathbf{V}(\tilde{f}_1, \cdots, \tilde{f}_s, g_1, \cdots, g_s)$ に適用する．生成元の先頭項を置き換えたので，次の異なった分解が得られる

$$\mathbf{V}(I_1) = \mathbf{V}(\widetilde{I_1}) = \pi_1(V) \cup \widetilde{W}.$$

ここで，$\widetilde{W}$ は $\tilde{f}_1, \cdots, \tilde{f}_s, g_1, \cdots, g_s$ の x_1 に関する先頭係数が 0 になる部分解よりなる．よって，この $\widetilde{W}$ は $W = \mathbf{V}(I_1)$ に含まれる．

しかし $\widetilde{W} \subsetneq W$ となるとは限らず，相変わらず $\widetilde{W} = \mathbf{V}(I_1)$ となることも起こり得る．そのときは上記のプロセスを繰り返せばよい．繰り返しているうちにどこかで $\mathbf{V}(I_1)$ より真に小さくなれば，証明は完了する．

あとは，常に同じ $\mathbf{V}(I_1)$ が得られる場合を考える．上記のプロセスを繰り返す度に生成元の x_1 の次数は落ちていく，あるいは 0 のままである．最終的にはすべての生成元から x_1 が消去されるので，部分解 $(a_2, \cdots, a_n)$ があるとき，すべての $a_1 \in \mathbb{C}$ に対して $(a_1, a_2, \cdots, a_n) \in V$ となる．したがって，すべての部分解を拡張することができ，$\pi_1(V) = \mathbf{V}(I_1)$ である．つまり $W = \emptyset$ であり，$V \neq \emptyset$ であるとき (ii) が満たされる． □

この閉包定理は拡張定理と同様に，$\mathbb{C}$ 上に限らず任意の代数的閉体 K 上で正しい．

3.3 陰関数表示化

一部の証明は後回しにしているが，ここまででアフィン多様体の点が求められるようになり，その射影と部分解の大きさについて述べることができた．しかし，アフィン多様体の定義方程式は最初から与えられているとは限らないし，パラメータによって表されている場合もある．その場合にはどのように多様体の点を求めればよいのだろうか？

例 3-10. $\mathbb{R}^3$の捩れ 3 次曲線 $C = \mathbf{V}(y - x^2, z - x^3)$ のすべての接線からなる曲面 V を考える（これを C の接曲面という）．V はパラメータ表示によって定義される多様体である．V をグレブナー基底を用いて求めてみる．

$x = t \in \mathbb{R}$ とおくと，C のパラメータ付け $(x, y, z) = (t, t^2, t^3) = \mathbf{r}(t)$ が得られる．よって，C の $\mathbf{r}(t)$ における接線は，$u \in \mathbb{R}$ を用いて，次のようにパラメータ付けされる

$$\mathbf{r}(t) + u\mathbf{r}'(t) = (t, t^2, t^3) + u(t, t^2, t^3) = (t + u, t^2 + 2tu, t^3 + 3t^2u).$$

連立方程式の形で表すと

$$\begin{aligned} x &= t + u, \\ y &= t^2 + 2tu, \qquad \cdots (1) \\ z &= t^3 + 3t^2u \end{aligned}$$

となり，t は C 上の位置を，u は接線上の位置を表すパラメータである．これは次のイデアルを与える

$$I = \langle x - t - u, y - t^2 - 2tu, z - t^3 - 3t^2u \rangle \subset \mathbb{R}[t, u, x, y, z].$$

lex 順序 $t > u > x > y > z$ を使うと，I のグレブナー基底は次のようになる

$$\begin{aligned}
g_1 &= t + u - x,\\
g_2 &= u^2 - x^2 + y,\\
g_3 &= ux^2 - uy - x^3 + \frac{3}{2}xy - \frac{1}{2}z,\\
g_4 &= uxy - uz - x^2y - xz + 2y^2, \qquad \cdots(2)\\
g_5 &= uxz - uy^2 + x^2z + \frac{1}{2}xy^2 - \frac{1}{2}yz,\\
g_6 &= uy^3 - uz^2 - 2x^2yz + \frac{1}{2}xy^3 - xz^2 + \frac{5}{2}y^2z,\\
g_7 &= x^3z - \frac{3}{4}x^2y^2 - \frac{3}{2}xyz + y^3 + \frac{1}{4}z^2.
\end{aligned}$$

このように t と u が順番に消去され，消去定理より $I_2 = I \cap \mathbb{R}[x, y, z] = \langle g_7 \rangle$ である．(1) は $g_7 = 0$ を満たすので，$\mathbf{V}(g_7)$ は V を含む多様体である．しかし $\mathbf{V}(g_7)$ には V の他に余計な点を含んでいる可能性がある．パラメータを消去して得られたアフィン多様体 $\mathbf{V}(g_7)$ は，解空間 V を含む最小の多様体となっているのだろうか？

それを調べるため，一般論に移る．次の多項式パラメータ表示が与えられているとする

$$\begin{aligned}
x_1 &= f_1(t_1, \cdots, t_m),\\
&\vdots \qquad \cdots(3)\\
x_n &= f_n(t_1, \cdots, t_m).
\end{aligned}$$

ここで，$f_1, \cdots, f_n \in k[t_1, \cdots, t_m]$ である．写像 $F = (f_1, \cdots, f_n)$ を

$$F : k^m \longrightarrow k^n, \quad (t_1, \cdots, t_m) \longmapsto (f_1(t_1, \cdots, t_m), \cdots, f_n(t_1, \cdots, t_m))$$

と定める．$F(k^m) \subset k^n$ はアフィン多様体であるとは限らないので，陰関数表示化の目的は $F(k^m)$ を含む最小のアフィン多様体を求めることである．

(3) より，$V = \mathbf{V}(x_1 - f_1, \cdots, x_n - f_n) \subset k^{m+n}$ をおく．V の点は

$$(t_1, \cdots, t_m, f_1(t_1, \cdots, t_m), \cdots, f_n(t_1, \cdots, t_m))$$

と書けるので，V は写像 F のグラフである．この他に

$$\begin{aligned}
p(t_1, \cdots, t_m) &= (t_1, \cdots, t_m, f_1(t_1, \cdots, t_m), \cdots, f_n(t_1, \cdots, t_m)),\\
\pi_m(t_1, \cdots, t_m, x_1, \cdots, x_n) &= (x_1, \cdots, x_n)
\end{aligned}$$

で定義される写像

$$p : k^m \longrightarrow k^{m+n}, \quad \pi_m : k^{m+n} \longrightarrow k^n$$

も得られる．これらの写像は次の図式を与えている

$$\begin{array}{ccccc}
 & & k^{m+n} & & \\
 & p\nearrow & & \searrow\pi_m & \cdots(4)\\
k^m & & \xrightarrow{F} & & k^n
\end{array}$$

つまり $F = \pi_m \circ p$ と書け，$p(k^m) = V$ も分かる．したがって

$$F(k^m) = \pi_m(p(k^m)) = \pi_m(V) \qquad \cdots(5)$$

を得る．パラメータ付けの像はグラフの射影であるということである．

定理 3-11.　多項式陰関数表示化

k を無限体とする．先の議論と同じ集合と写像を用いる．$I = \langle x_1 - f_1, \cdots, x_n - f_n \rangle$ を $k[t_1, \cdots, t_m, x_1, \cdots, x_n]$ のイデアル，$I_m = I \cap k[x_1, \cdots, x_n]$ を m 次の消去イデアルとする．このとき，$\mathbf{V}(I_m)$ は k^n におい

て $F(k^m)$ を含む最小のアフィン多様体である．

証明　$V = \mathbf{V}(I) \subset k^{m+n}$とする．$k = \mathbb{C}$ の場合には，(5) により $F(\mathbb{C}^m) = \pi_m(V)$ を得る．閉包定理により，$\mathbf{V}(I_m)$ が $\pi_m(V)$ を含む最小のアフィン多様体であるので，題意は示された．

次に，k が $\mathbb{C}$ の部分体である場合を考える．$k \subset \mathbb{C}$ であり，この k では $\mathbb{C}$ と同じ演算が定義できるので，k は素体 $\mathbb{Q}$ を含む．よって，k は無限体である．$k \subsetneq \mathbb{C}$ の場合は閉包定理を直接に適用することはできないので，体 k と $\mathbb{C}$ とを行き来しながら証明を進める．k^nにおける多様体であるか $\mathbb{C}^n$における多様体であるかを区別する必要があるので，多様体の記号に添え字として k と $\mathbb{C}$ を付ける．題意は，$\mathbf{V}_k(I_m)$ が $F(k^m)$ を含む最小の多様体となることである．

今，(5) と補題 3-7. により，$F(k^m) = \pi_m(V_k) \subset \mathbf{V}_k(I_m)$ である．ここで $Z_k = \mathbf{V}_k(g_1, \cdots, g_s) \subset k^n$ を $F(k^m)$ を含む任意の多様体とする．このとき $\mathbf{V}_k(I_m) \subset Z_k$ を示せばよい．Z_k 上で g_i は消えるので $F(k^m)$ 上でも g_i は消える．つまり $g_i \circ F$ は k^m全体で消える．$g_i \in k[x_1, \cdots, x_n]$, $F \in k[t_1, \cdots, t_m]^n$であるので $g_i \circ F \in k[t_1, \cdots, t_m]$ が従い，k は無限個の元をもつから，結局 $g_i \circ F$ はすべて零多項式となる．よって $g_i \circ F$ は $\mathbb{C}^m$全体でも消えており，すなわち g_iが $F(\mathbb{C}^m)$ 上で消える．ゆえに $Z_{\mathbb{C}} = \mathbf{V}_{\mathbb{C}}(g_1, \cdots, g_s) \subset \mathbb{C}^n$とおけば，$Z_{\mathbb{C}}$ は $F(\mathbb{C}^m)$ を含む多様体である．証明の前半より，$\mathbb{C}^n$においてはこの定理は正しいので $\mathbf{V}_{\mathbb{C}}(I_m) \subset Z_{\mathbb{C}}$ が成立する．そのうち k^nにある解についても，$\mathbf{V}_k(I_m) = \mathbf{V}_{\mathbb{C}}(I_m) \cap k^n \subset Z_{\mathbb{C}} \cap k^n \subset Z_k$ が成立し，題意を満足する．

最後に k が $\mathbb{C}$ に含まれない無限体である場合を考える．このとき k を含む代数的閉体 K が存在する．K 上でも閉包定理は成立するので，$\mathbb{C}$ の代わりに K を用いると同じ議論に帰着する．以上で定理が証明できた．□

ここで接曲面の例に戻る．定理 3-11. より，$\mathrm{V}_{\mathbb{R}}(g_7)$ は接曲面 V を含む $\mathbb{R}^3$の最小の多様体であることが分かる．

しかし，$V = \mathbf{V}_{\mathbb{R}}(g_7)$ であるかどうかはまだ分からない．これには，部分解 $(x, y, z) \in \mathbf{V}_{\mathbb{R}}(g_7)$ がすべて完全解 $(t, u, x, y, z) \in \mathbf{V}_{\mathbb{R}}(I)$ まで拡張できるかを調べればよい．まずは $\mathbb{C}$ 上で考えて拡張定理を用いる．

I_2 は I_1の 1 次の消去イデアルであり，消去定理により $I_1 = \langle g_2, \cdots, g_7 \rangle$ である．I_1の生成元のうち，g_2 の u に関する先頭係数は $1 \neq 0$ であるので，$(x, y, z) \in \mathbf{V}_{\mathbb{R}}(g_7)$ はすべて $(u, x, y, z) \in \mathbf{V}_{\mathbb{C}}(I_1)$ に拡張できる．そしてこれらはすべて $(t, u, x, y, z) \in \mathbf{V}_{\mathbb{C}}(I)$ にまで拡張できる．g_1におけるtの先頭係数が 1 だからである．したがって，$\mathbf{V}_{\mathbb{C}}(g_7) = V$ であることが分かった．

残るは，この拡張が $\mathbb{R}$ 上でなされているのかという問題である．t と u の定義の仕方を思い出すと，すべての $(t, u) \in \mathbb{R}$ がそれぞれ接曲面 V 上の 1 点 $(x, y, z) \in \mathbb{R}^3$ に対応することが分かる．グレブナー基底を見るとこれを代数的に示すことができる．$g_3 = \cdots = g_6 = 0$ は u の 1 次方程式だから，$(x, y, z) \in \mathbb{R}^3$ のとき $u \in \mathbb{R}$ である．一方 $g_2 = 0$ は 2 次方程式であるが，問題なく $u \in \mathbb{R}$ の存在が示される．なぜならば，曲線 C は放物面 $\mathbf{V}(y - x^2) \subset \mathbb{R}^3$上にあるので，$C$ の接線はこの放物面の凸側にある．よって V の点は $y \leq x^2$を満たすので，$0 = g_2 = u^2 + (y - x^2) \leq u^2$となり，$u \in \mathbb{R}$ が存在する．$g_1 = 0$ は t の 1 次方程式だから，同様にして $t \in \mathbb{R}$ に拡張できる．以上の議論より $V = \mathbf{V}_{\mathbb{R}}(g_7)$ であることが分かる．

一般に，パラメータ表示の像がそのザリスキー閉包を覆い尽くすかどうかを示すことは難しく，与えられた問題ごとに個別に解析するしかない．しかし，今の例のようにグレブナー基底と拡張定理を組み合わせて議論すれば，その様子は解析できるようである．

また，有理パラメータ表示が与えられた場合にも，多項式パラメータ表示の場合のように定理 3-11. とほとんど同様の事実が示される．この場合は，パラメータ表示式の分母にある多項式 h_i を払ってイデアル I を同じように定義する．注意すべき点は，分母 h_i が消える点をパラメータの定義域からあらかじめ除くことである．そして，すべての分母が 0 でないことと同等である方程式 $h_1 \cdot \cdots \cdot h_n y = 1$ を I に添加し新たなイデアル J とする．ここで y は消去すべき新たなパラメータである．この適当な定義域とイデアル J に対し，定理 3-11. と同じ内容が成立する．

3.4 終結式

第 3 章の最後に，積み残していた拡張定理の証明を行う．拡張定理とは与えられた部分解がいつ方程式系の共通解となるかを判定するためのものである．一方，終結式とは与えられた多項式がいつ共通因子を持つかを判定するために生まれた式である．この終結式を上手く用いて拡張定理を示す．

まずは，1 変数の多項式 $f, g \in k[x]$ が共通因子を持つかどうかを知りたいとする．f と g を既約分解すれば共通因子は手に入るが，これは一般に時間のかかる処理である．よりよい方法は，$\mathrm{GCD}(f, g)$ を互除法によって求めることである．しかしこれには体 k における割り算を必要とし，それは消去を行う段階で実は避けたい操作である．そこで，割り算を行わない別のアプローチを探っていく．

補題 3-12. $f, g \in k[x],\ \deg(f) = l > 0,\ \deg(g) = m > 0$ とする．このとき，f と g が共通因子を持つことと次の 3 つの条件を満たす多項式 $A, B \in k[x]$ が存在することとは同値である

(i) $A \neq 0$ かつ $B \neq 0$,

(ii) $\deg(A) \leq m - 1$ かつ $\deg(B) \leq l - 1$,

(iii) $Af + Bg = 0$.

証明 $(\Rightarrow)$ f, g が共通因子 $h \in k[x]$ を持つと仮定する．このとき，$f = hf_1$ と $g = hg_1$ を満たす $f_1, g_1 \in k[x]$ が存在する．ここで $\deg(f_1) \leq l - 1,\ \deg(g_1) \leq m - 1$ である．今

$$f \cdot g_1 = hf_1 g_1 = g \cdot f_1$$

であるので，$A = g_1,\ B = -f_1$ とおくと，A, B は条件 $(i), (ii), (iii)$ を満たす．

$(\Leftarrow)$ ある $A, B \in k[x]$ が条件 $(i), (ii), (iii)$ を満たし，f, g が互いに素であると仮定する．$\mathrm{GCD}(f, g) = 1$ であるので，ある $\widetilde{A}, \widetilde{B} \in k[x]$ が存在して $\widetilde{A}f + \widetilde{B}g = 1$ と書ける．これに B を掛けて (iii) の式を代入すると

$$B = (\widetilde{A}f + \widetilde{B}g)B = \widetilde{A}Bf + \widetilde{B}Bg = \widetilde{A}Bf - \widetilde{B}Af = (\widetilde{A}B - \widetilde{B}A)f$$

となる．$B \neq 0$ より，$\deg(B) \geq \deg(f) = l$ となり，(ii) に矛盾する．よって始めの仮定は誤りで，f, g は共通因子を持つ． □

この判定法は使いにくいので，よりよい条件を導く．まず補題の (ii) を満たす A, B を次のように書く

$$A = a_0 x^{m-1} + \cdots + a_{m-1},$$
$$B = b_0 x^{l-1} + \cdots + b_{l-1}.$$

すると，この $l + m$ 個の係数 $a_i, b_i \in k$ で $Af + Bg = 0$ を満たすものがいつ存在するかを考えればよい．

f, g も次のように書く

$$f = c_0 x^l + \cdots + c_l, \quad c_0 \neq 0,$$

$$g = d_0 x^m + \cdots + d_m, \quad b_0 \neq 0.$$

ここで $c_i, d_i \in k$ である．$Af + Bg = 0$ にこれらを代入し，x の冪の係数を比較すると，次の線形方程式系が得られる

$$\begin{array}{lcll}
a_0c_0 & + & b_0d_0 = 0 & ; x^{l+m1}\text{の係数,} \\
a_0c_1 + a_1c_0 & + & b_0d_1 + b_1d_0 = 0 & ; x^{l+m-2}\text{の係数,} \\
a_0c_2 + a_1c_1 + a_2c_0 & + & b_0d_2 + b_1d_1 + b_2d_0 = 0 & ; x^{l+m-3}\text{の係数,} \\
 & & \vdots & \\
a_{m-2}c_l + a_{m-1}c_{l-1} & + & b_{l-2}d_m + b_{l-1}d_{m-1} = 0 & ; x^1\text{の係数,} \\
a_{m-1}c_l & + & b_{l-1}d_m = 0 & ; x^0\text{の係数.}
\end{array}$$

これを行列の積で書くと

$$\begin{pmatrix}
c_0 & & & & & d_0 & & & \\
c_1 & c_0 & & & & d_1 & d_0 & & \\
c_2 & c_1 & c_0 & & & & d_1 & \ddots & \\
 & c_2 & c_1 & \ddots & & & & \ddots & d_0 \\
\vdots & & c_2 & \ddots & c_0 & \vdots & & & d_1 \\
 & \vdots & & \ddots & c_1 & \vdots & \vdots & & \\
c_{l-1} & & \vdots & & c_2 & & \vdots & & \\
c_l & c_{l-1} & & & & & & & \vdots \\
 & c_l & c_{l-1} & & \vdots & d_m & & & \vdots \\
 & & c_l & \ddots & & & d_m & & \\
 & & & \ddots & c_{l-1} & & & \ddots & \\
 & & & & c_l & & & & d_m
\end{pmatrix}
\begin{pmatrix}
a_0 \\ a_1 \\ a_2 \\ \\ \vdots \\ \\ a_{m-1} \\ b_0 \\ b_1 \\ \\ \vdots \\ \\ b_{l-1}
\end{pmatrix} = O$$

と表される．左辺の $l + m$ 次正方行列が非正則であるとき，またそのときに限って O でない解 $(a_0, \cdots, a_{m-1}, b_0, \cdots, b_{l-1})$ が存在する．この左辺の正方行列

$$\begin{pmatrix}
c_0 & & & d_0 & & O \\
\vdots & \ddots & O & & \ddots & \\
\vdots & & \ddots & \vdots & & d_0 \\
c_l & & & c_0 & & \\
 & \ddots & & \vdots & d_m & \vdots \\
 & O & \ddots & \vdots & & \ddots \\
 & & & c_l & O & d_m
\end{pmatrix} =: \mathrm{Syl}(f, g, x)$$

を f と g の変数 x に関する**シルベスター行列**という．そしてこのシルベスター行列の行列式

$$\mathrm{Res}(f, g, x) := \det\{\mathrm{Syl}(f, g, x)\}$$

を f と g の変数 x に関する**終結式**という．

行列式の定義により

$$\mathrm{Res}(f,g,x) \in \mathbb{Z}[a_i,b_i] \subset k$$

である．以上の議論より次の系が従う．

系 3-13. $f,g \in k[x]$ に対して，$\mathrm{Res}(f,g,x)$ は f と g の係数を変数とする整数係数多項式 (つまり k の元) である. さらに，f と g が $k[x]$ において共通因子を持つことと $\mathrm{Res}(f,g,x)=0$ であることは同値である．

命題 3-13. より，終結式によって変数が消去されていることが分かる． 実は $\mathrm{Res}(f,g,x)$ は $\langle f,g\rangle$ の 1 次の消去イデアルに含まれていることが分かる

命題 3-14. $f,g \in k[x]$ に対して

$$Af+Bg = \mathrm{Res}(f,g,x) \subset \langle f,g\rangle \cap k$$

を満たす $A,B \in k[x]$ が存在する．さらに，A,B の係数は f と g の係数に関する整数係数多項式である．

証明 $\mathrm{Res}(f,g,x)=0$ のときは $A=B=0$ を選べばよく，自明である．

$\mathrm{Res}(f,g,x)\neq 0$ と仮定する．これは f,g が互いに素であることと同値である．つまり，(1) $\widetilde{A}f+\widetilde{B}g=1$ を満たす$\widetilde{A},\widetilde{B} \in k[x]$ が存在する．この両辺に $\mathrm{Res}(f,g,x)$ を掛けると，題意の前半が示される．

ここで $f,g,\widetilde{A},\widetilde{B}$を，上の議論と全く同じように係数 c_i,d_i,a_i,b_iを用いて表記する．(1) を x の冪の係数について整理し，同様にして線形方程式系で表すと

$$\mathrm{Syl}(f,g,x)\begin{pmatrix} a_0 \\ \vdots \\ a_{m-1} \\ b_0 \\ \vdots \\ b_{l-1} \end{pmatrix} = \begin{pmatrix} 0 \\ \\ \vdots \\ \\ 0 \\ 1 \end{pmatrix} \quad \cdots(1)$$

となる．$\mathrm{Res}(f,g,x)\neq 0$ だから，(1) は k で一意解をもち，これはクラメールの公式によって求められる．この公式を見ると，一意解は

$$a_i,b_i = \frac{c_i,d_i\text{の整数係数多項式}}{\mathrm{Res}(f,g,x)}$$

と導かれる．$\widetilde{A}=a_0x^{m-1}+\cdots+a_{m-1}$の共通分母 $\mathrm{Res}(f,g,x)$ を払って

$$A = \mathrm{Res}(f,g,x)\widetilde{A} \in k[x]$$

と書ける．そして A の係数は c_i,d_iの整数係数多項式であることが分かる．B についても A と同様である．□

例 3-15. $f=xy-1$, $g=x^2+y^2-4$ について，$\mathrm{Res}(f,g,x) \in \langle f,g\rangle \cap k[y]$ であることを確かめる

$$\mathrm{Syl}(f,g,x) = \begin{pmatrix} y & 0 & 1 \\ -1 & y & 0 \\ 0 & -1 & y^2-4 \end{pmatrix},$$

$$\mathrm{Res}(f,g,x) = y^2(y^2-4)+1 \neq 0.$$

よって，x のみを変数として扱うと $\mathrm{GCD}(f,g)=1$ であり，$\widetilde{A}f+\widetilde{B}g=1$ を満たす $\widetilde{A},\widetilde{B} \in k(y)[x]$ が存在す

る．クラメールの公式より

$$\widetilde{A} = \frac{\det\begin{pmatrix} 0 & 0 & 1 \\ 0 & y & 0 \\ 1 & -1 & y^2-4 \end{pmatrix}}{\mathrm{Res}(f,g,x)}x + \frac{\det\begin{pmatrix} y & 0 & 1 \\ -1 & 0 & 0 \\ 0 & 1 & y^2-4 \end{pmatrix}}{\mathrm{Res}(f,g,x)} = -\frac{y}{y^4-4y^2+1}x - \frac{1}{y^4-4y^2+1},$$

$$\widetilde{B} = \frac{\det\begin{pmatrix} y & 0 & 0 \\ -1 & y & 0 \\ 0 & -1 & 1 \end{pmatrix}}{\mathrm{Res}(f,g,x)} = \frac{y^2}{y^4-4y^2+1}.$$

これらを代入し分母を払えば

$$-(yx+1)f + y^2 g = y^4 - 4y^2 + 1 \in \langle f, g\rangle \cap k[y] \quad \cdots(2)$$

が得られる．

次に，これまでの終結式の理論を n 変数の多項式の場合にまで適合させる．$f, g \in k[x_1, \cdots, x_n]$ が与えられているとき，x_1について整理し

$$f = a_0 x_1^l + \cdots + a_l, \ \ a_0 \neq 0,$$
$$g = b_0 x_1^m + \cdots + b_m, \ \ b_0 \neq 0$$

と書く．ここで $a_i, b_i \in k[x_2, \cdots, x_n]$ である．f と g の x_1に関する終結式を次で定義する

$$\mathrm{Res}(f,g,x_1) = \det\begin{pmatrix} a_0 & & & & b_0 & & O \\ \vdots & \ddots & O & & & \ddots & \\ \vdots & & \ddots & & \vdots & & b_0 \\ a_l & & & a_0 & & & \\ & \ddots & & \vdots & b_m & & \vdots \\ & O & \ddots & \vdots & & \ddots & \\ & & & a_l & O & & b_m \end{pmatrix}.$$

多変数の多項式の終結式に対しても，1 変数の場合と同じ次の結果が成り立つ．

命題 3-16. $f, g \in k[x_1, \cdots, x_n]$ が x_1を含むとき，次が成立する

(i) $\mathrm{Res}(f,g,x_1) \in \langle f, g\rangle \cap k[x_2, \cdots, x_n]$,

(ii) $\mathrm{Res}(f,g,x_1) = 0$ であることと，f と g が $k[x_1, \cdots, x_n]$ が x_1を含む共通因子をもつことは同値である．

証明 (i) 終結式は a_i, b_iの整数係数多項式であるので，$\mathrm{Res}(f,g,x_1) \in k[x_2, \cdots, x_n]$ となる．また，$Af + Bg = \mathrm{Res}(f,g,x_1)$ を満たし x_1を含む多項式 A, B で，係数が a_i, b_iを変数とする整数係数多項式であるものが存在する．よって，$A, B \in k[x_2, \cdots, x_n][x_1] = k[x_1, \cdots, x_n]$ であるので，$\mathrm{Res}(f,g,x_1) \in \langle f, g\rangle$ が導かれる．
(ii) 系 3-13. より，$\mathrm{Res}(f,g,x_1) = 0$ であることと f と g が x_1を含む $k(x_2, \cdots, x_n)[x_1]$ の多項式を共通因子として持つこととは同値である．その共通因子の分母を払ったものの x_1を含む既約因子 (もとの分母とは異なる

因子) は，$k[x_1, \cdots, x_n]$ で再び f と g の共通因子となる．よって，$\mathrm{Res}(f, g, x_1) = 0$ であることは f と g が x_1 を含む $k[x_1, \cdots, x_n]$ の多項式を共通因子としてもつこととも同値である． □

命題 3-16.(i) より，多変数の場合でも終結式は消去イデアルの元となっている．よって実際に計算するとグレブナー基底に似た形になることはあるが，一致するとは限らない．グレブナー基底に比べ余分な因子や重複を含み次数が高くなることもあり，消去イデアルの基底であるとは限らない．つまり $\mathrm{Res}(f, g, x_1)$ は f と g の共通根の他に余計な根を示すこともあり得る．しかし，変数の消去がスムーズに行えることは終結式の大きな利点である．

一方，代数的閉体上，特に $\mathbb{C}$ 上では $\mathbb{C}[x]$ の 2 本の多項式が共通因子をもつこととそれらが共通根を持つことは同値である．こうして次の系が得られる．

系 3-17. $f, g \in \mathbb{C}[x]$ とする．このとき $\mathrm{Res}(f, g, x) = 0$ であることと f と g が $\mathbb{C}$ において共通根を持つこととは同値である．

この系の応用例として多項式の分離性の判定がある．$\mathrm{Res}(f, g, x_1) = 0$ かどうかを示せば，$f(x)$ と $f'(x)$ が共通因子を持つかどうかが分かり，多項式 $f(x)$ が代数的閉体上で 2 重根を持つかが分かる．

3.5 拡張定理の証明

次の命題は終結式の理論と拡張定理の証明との橋渡しとなる．

命題 3-18. $f, g \in \mathbb{C}[x_1, \cdots, x_n]$ に対して，$a_0, b_0 \in \mathbb{C}[x_2, \cdots, x_n]$ を f, g の x_1に関する先頭係数とする．もし $\mathrm{Res}(f, g, x_1) \in \mathbb{C}[x_2, \cdots, x_n]$ が $(c_2, \cdots, c_n) \in \mathbb{C}^{n-1}$において消えるとすれば次のいずれかが成立する

(i) a_0 または b_0 が $(c_2, \cdots, c_n) \in \mathbb{C}^{n-1}$で消える，

(ii) $c_1 \in \mathbb{C}$ が存在して，f と g は $(c_1, \cdots, c_n) \in \mathbb{C}^n$で消える．

証明 $\mathbf{c} = (c_2, \cdots, c_n)$ とする．$a_0(\mathbf{c})$ と $b_0(\mathbf{c})$ が共に 0 でないとき，$f(x_1, \mathbf{c})$ と $g(x_1, \mathbf{c})$ が共通根 $x_1 = c_1 \in \mathbb{C}$ を持つことを示せば十分である．そのために

$$f(x_1, \mathbf{c}) = a_0(\mathbf{c})x_1^l + \cdots + a_l(\mathbf{c}),\ \ a_0(\mathbf{c}) \neq 0,$$
$$g(x_1, \mathbf{c}) = b_0(\mathbf{c})x_1^m + \cdots + b_m(\mathbf{c}),\ \ b_0(\mathbf{c}) \neq 0$$

と書く．仮定より，$h := \mathrm{Res}(f, g, x_1)$ は $\mathbf{c}$ で消える．よって

$$0 = h(\mathbf{c}) = \det \begin{pmatrix} a_0(\mathbf{c}) & & & & b_0(\mathbf{c}) & & \\ \vdots & \ddots & & & & \ddots & \\ \vdots & & \ddots & & \vdots & & b_0(\mathbf{c}) \\ a_l(\mathbf{c}) & & & a_0(\mathbf{c}) & & & \\ & \ddots & & \vdots & b_m(\mathbf{c}) & & \vdots \\ & & \ddots & \vdots & & \ddots & \\ & & & a_l(\mathbf{c}) & & & b_m(\mathbf{c}) \end{pmatrix} = \mathrm{Res}(f(x_1, \mathbf{c}), g(x_1, \mathbf{c}), x_1)$$

が従う．これと系 3-17. から，$f(x_1, \mathbf{c})$ と $g(x_1, \mathbf{c})$ は共通根 $c_1 \in \mathbb{C}$ をもつ． □

命題 3-19.　2 つの多項式に対する拡張定理

$I = \langle f, g \rangle \subset \mathbb{C}[x_1, \cdots, x_n]$ とし，I_1 を I の 1 次の消去イデアルとする．また，$a_0, b_0 \in \mathbb{C}[x_2, \cdots, x_n]$ を f, g の x_1 に関する先頭係数とする．部分解 $\mathbf{c} = (c_2, \cdots, c_n) \in \mathbf{V}(I_1)$ があって，もし $\mathbf{c} \notin \mathbf{V}(a_0, b_0)$ ならば，$c_1 \in \mathbb{C}$ が存在して $(c_1, \cdots, c_n) \in \mathbf{V}(I)$ となる．

証明　命題 3-16. より，$\mathrm{Res}(f, g, x_1) \in I_1$ であるので，これは $\mathbf{c}$ で消える．a_0 も b_0 も $\mathbf{c}$ において消えないならば，命題 3-18. より，$c_1 \in \mathbb{C}$ が存在して $\mathbf{c}$ は拡張できる．

あとは a_0 と b_0 のどちらか一方が $\mathbf{c}$ において消える場合にも $\mathbf{c}$ が拡張できることを示せばよい．そこで，$a_0(\mathbf{c}) \neq 0$ かつ $b_0(\mathbf{c}) = 0$ であると仮定する．このとき命題 3-18. の証明に登場した

$$\mathrm{Res}(f, g, x_1)(\mathbf{c}) = \mathrm{Res}(f(x_1, \mathbf{c}), g(x_1, \mathbf{c}), x_1)$$

が成り立たないこと $\cdots(*)$ が問題である（理由は後述）．そのため，I の基底を取り換える．$\forall N \in \mathbb{N}$ に対し $\langle f, g \rangle = \langle f, g + x_1^N f \rangle$ が成立する．この N を十分大きくとれば，$g + x_1^N f$ の先頭係数は a_0 となり $\mathbf{c}$ で消えなくなる．よって，$c_1 \in \mathbb{C}$ が存在して $(c_1, \cdots, c_n) \in \mathbf{V}(f, g + x_1^N f) = \mathbf{V}(I)$ とできる． □

（証明の補足）ここで $(*)$ の理由を述べておく．a_0 も b_0 も $\mathbf{c}$ で消えない場合は $\mathrm{Res}(f, g, x_1)(\mathbf{c})$ と $\mathrm{Res}(f(x_1, \mathbf{c}), g(x_1, \mathbf{c}), x_1)$ は同じ行列の行列式である．けれども b_0 が $\mathbf{c}$ で消える場合はサイズの違う行列になってしまう（後者が 1 行 1 列分小さくなる）．両者をそれぞれ書き下すと

$$\mathrm{Res}(f, g, x_1)(\mathbf{c}) = \det \begin{pmatrix} a_0(\mathbf{c}) & & & & 0 & & \\ \vdots & a_0(\mathbf{c}) & & & b_1(\mathbf{c}) & & \\ \vdots & \vdots & \ddots & & \vdots & & 0 \\ a_l(\mathbf{c}) & \vdots & & a_0(\mathbf{c}) & \vdots & & b_1(\mathbf{c}) \\ & a_l(\mathbf{c}) & & \vdots & b_m(\mathbf{c}) & & \vdots \\ & & \ddots & \vdots & & \ddots & \vdots \\ & & & a_l(\mathbf{c}) & & & b_m(\mathbf{c}) \end{pmatrix},$$

$$\mathrm{Res}(f(x_1,\mathbf{c}),g(x_1,\mathbf{c}),x_1)=\det\begin{pmatrix} a_0(\mathbf{c}) & & & b_1(\mathbf{c}) & & \\ \vdots & \ddots & & \vdots & \ddots & \\ \vdots & & a_0(\mathbf{c}) & \vdots & & b_1(\mathbf{c}) \\ a_l(\mathbf{c}) & & \vdots & b_m(\mathbf{c}) & & \vdots \\ & \ddots & \vdots & & \ddots & \vdots \\ & & a_l(\mathbf{c}) & & & b_m(\mathbf{c}) \end{pmatrix}$$

となり，余因子展開を用いて

$$\mathrm{Res}(f,g,x_1)(\mathbf{c})=a_0(\mathbf{c})\cdot\mathrm{Res}(f(x_1,\mathbf{c}),g(x_1,\mathbf{c}),x_1)\ \cdots(\star)$$

と書ける．つまり両者は $a_0(\mathbf{c})$ 倍だけ違っているため，$(*)$ となる．

このときであっても，$\mathrm{Res}(f,g,x_1)$ が $\mathbf{c}$ で消えると仮定すると，$(\star)$ と $a_0(\mathbf{c})\neq 0$ より $\mathrm{Res}(f(x_1,\mathbf{c}),g(x_1,\mathbf{c}),x_1)=0$ が成立する．すなわち共通根 $c_1\in\mathbb{C}$ が存在する．

最後の証明の前に，3 つ以上の多項式に対する終結式を定義しなければならない．

定義 3-20.　一般終結式

新たな変数 $u_2,\cdots,u_s$を導入し，f_1と $u_2f_2+\cdots+u_sf_s\in\mathbb{C}[u_2,\cdots,u_s,x_1,\cdots,x_s]$ の終結式を考える．$\mathbb{C}[x_2,\cdots,x_s]$ の終結式を得るために，これを $u_2,\cdots,u_s$について冪級数展開する

$$\mathrm{Res}(f_1,u_2f_2+\cdots u_sf_s,x_1)=\sum_{\alpha}h_\alpha(x_2,\cdots,x_s)u^\alpha.$$

ここで，$h_\alpha\in\mathbb{C}[x_2,\cdots,x_s]$ である．この多項式 h_αたちを $f_1,\cdots,f_s$の**一般終結式**という．

例 3-21.

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

とする．u_2,u_3を用いた終結式は

$$\begin{aligned} \mathrm{Res}(f_1,u_2f_2+u_3f_3,x)=&(y^4+2y^2z-2y^2+z^2+y-z)u_2^2\\ &+2(y^2z^2+y^3+z^3-y^2-z^2+yz)u_2u_3\\ &+(z^4+2yz^2+y^2-2z^2-y+z){u_3}^2 \end{aligned}$$

となり，一般終結式は次のようになる

$$\begin{aligned} h_{20}&=y^4+2y^2z-2y^2+z^2+y-z,\\ h_{11}&=2(y^2z^2+y^3+z^3-y^2-z^2+yz),\\ h_{02}&=z^4+2yz^2+y^2-2z^2-y+z. \end{aligned}$$

定理 3-22.　拡張定理

イデアル $I=\langle f_1,\cdots,f_s\rangle\subset\mathbb{C}[x_1,\cdots,x_n]$ を考え，I_1を I の 1 次の消去イデアルとする．$i\in\{1,\cdots,s\}$ に対して，f_i を次の形に書く

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

ここで，$N_i\geq 0$ とし，$g_i\in\mathbb{C}[x_2,\cdots,x_n]$ は 0 でない多項式である．部分解 $(c_2,\cdots,c_n)\in\mathbf{V}(I_1)$ があると仮定する．このとき，$(c_2,\cdots,c_n)\notin\mathbf{V}(g_1,\cdots,g_s)$ ならば $c_1\in\mathbb{C}$ が存在して $(c_1,c_2,\cdots,c_n)\in\mathbf{V}(I)$ である．

証明　$s=2$ の場合は既に示した．$s=1$ も自明である．

以下 $s=3$ の場合に $f_i(x_1,\mathbf{c})$ たちの共通根を求める．ここで $\mathbf{c}=(c_2,\cdots,c_n)$ とする．今，$\mathbf{c}\notin\mathbf{V}(g_1,\cdots,g_s)$ より $g_1(\mathbf{c})\neq 0$ と仮定しても一般性を失わない．

$$h:=\mathrm{Res}(f_1,u_2f_2+\cdots+u_sf_s,x_1)=\sum_\alpha h_\alpha(x_2,\cdots,x_s)u^\alpha.$$

一般終結式 $h_\alpha\in\mathbf{c}[x_2,\cdots,x_n]$ は環 $\mathbb{C}[u_2,\cdots,u_s,x_1,\cdots,x_n]$ 上において $\langle f_1,\cdots,f_s\rangle$ に入ることが証明できる．よって $h_\alpha\in I_1$である．$\mathbf{c}\in\mathbf{V}(I_1)$ ならばすべての α に対し $h_\alpha(\mathbf{c})=0$ である．すなわち $h(\mathbf{c})=0$ である．

あとは終結式について

$$h(\mathbf{c})=\mathrm{Res}(f_1(x_1,\mathbf{c}),u_2f_2(x_1,\mathbf{c})+\cdots+u_sf_s(x_1,\mathbf{c}),x_1)\quad\cdots(*)$$

であることを示せば，終結式が消え，示すべき共通根の存在を証明できる．

$(*)$ が成立するためには，f_1と $u_2f_2+\cdots+u_sf_s$ の x_1 に関する先頭係数が $\mathbf{c}$ で消えなければ十分である（命題 3-18. より）．$g_1(\mathbf{c})\neq 0$ と仮定したので，あとは $u_2f_2+\cdots+u_sf_s$ の方を考えれば良い．

$u_2f_2+\cdots+u_sf_s$の x_1 についての先頭項が消えるとき，命題 3-19. の証明で行ったのと同様に，f_2 の代わりに $f_2+x_1^Nf_1$を用いる．この操作によって I はイデアルとして変化しない．十分に大きい整数 N をとれば $u_2f_2+\cdots+u_sf_s$の先頭項は $\mathbf{c}$ で消えないようにできる．

したがって $(*)$ は成立し，$f_1(x_1,\mathbf{c})$ と $u_2f_2(x_1,\mathbf{c})+\cdots+u_sf_s(x_1,\mathbf{c})$ は x_1を含む共通因子 F を持つ．F は $f_1(x_1,\mathbf{c})$ を割り切るので，$\mathbb{C}[x_1]$ の元である．一方 $u_2f_2(x_1,\mathbf{c})+\cdots+u_sf_s(x_1,\mathbf{c})$ は $\mathbb{C}[x_1,u_2,\cdots,u_s]$ の元である．ここから $F(x_1)$ を括り出せば，$u_2,\cdots,u_s$ の係数を比較することにより，F が $f_2(x_1,\mathbf{c}),\cdots,f_s(x_1,\mathbf{c})$ のそれぞれを割り切ることが分かる．よって F はすべての $f_i(x_1,\mathbf{c})$ の正の次数を持つ共通因子である．$c_1\in\mathbb{C}$ を F の根とすると，c_1 はすべての $f_i(x_1,\mathbf{c})$ の共通根となる．f_2 の代わりに $f_2+x_1^Nf_1$を用いても，c_1 はすべての I の元の共通根となる．　□

以上で拡張定理が証明された．証明をよく見ると，拡張定理は $\mathbb{C}$ を他の代数的閉体に代えても成立する．

4　代数と幾何の対応

4.1　ヒルベルトの零点定理

第 4 章では，第 1 章の例 1-8. からしていた議論を深める．それは多様体とイデアルとの対応関係についてである．

$I=k[x_1,\cdots,x_n]$ のとき，$1\in I$ であるので，$\mathbf{V}(I)=\emptyset$ である．逆に $\mathbf{V}(I)=\emptyset$ としても，このような I は $k[x_1,\cdots,x_n]$ 以外にもあるかもしれない．I が k に根を持たない多項式で生成されていればよいからである．それでは k が代数的閉体であれば，根を持たないイデアルは多項式環全体に一致するのだろうか？

定理 4-1.　弱い零点定理

k を代数的閉体とし，$I\subset k[x_1,\cdots,x_n]$ を $\mathbf{V}(I)=\emptyset$ を満たすイデアルとする．このとき $I=k[x_1,\cdots,x_n]$ である．

証明　$\mathbf{V}(I)=\emptyset$ としたとき，$1\in I$ であることを示す．証明には，変数の個数 n に関する帰納法を用いる．

$n=1$ の場合，$\mathbf{V}(I)=\emptyset$ より，$f\in I$ は 0 でない定数である．このとき $\dfrac{1}{f}\in k$ だから，$1=(\dfrac{1}{f})\cdot f\in I$

となる．つまり $I = k[x]$ である．

次に，$n-1$ 変数の多項式環 $k[x_2, \cdots, x_n]$ に対して，結果が証明されていると仮定する．そして考えるのは，$\mathbf{V}(I) = \emptyset$ を満たすような $k[x_1, \cdots, x_n]$ の任意のイデアル $I = \langle f_1, \cdots, f_s \rangle$ である．f_1 が定数ならば証明は終わるので，以降 f_1 は定数ではないと仮定する．f_1 の全次数を N とすると，$N \geq 1$ である．ここで次のような線型座標変換を施して，f_1 を都合のよい形に書き換える

$$\begin{aligned} x_1 &= \tilde{x}_1, \\ x_2 &= \tilde{x}_2 + a_2\tilde{x}_1, \\ &\vdots \\ x_n &= \tilde{x}_n + a_n\tilde{x}_1. \end{aligned}$$

ここで係数 $a_i \in k$ は後でうまく選ぶことにする．この変換を f_1 に施すと

$$\begin{aligned} f_1(x_1, \cdots, x_n) &= f_1(\tilde{x}_1, \tilde{x}_2 + a_2\tilde{x}_1, \cdots, \tilde{x}_n + a_n\tilde{x}_1) \\ &= c(a_2, \cdots, a_n)\tilde{x}_1^N + (\tilde{x}_1\text{に関して } N \text{ 次未満の式}) \end{aligned}$$

と書ける．f_1 の $\tilde{x}_1$ に関する次数 N は，全次数 N と一致しているので，$c(a_2, \cdots, a_n)$ は消えない（$a_2, \cdots, a_n$ の零関数ではない）．代数的閉体は無限体であるので，$c(a_2, \cdots, a_n) \neq 0$ となるような $a_2, \cdots, a_n$ が存在して，選ぶことができる．

その $a_2, \cdots, a_n$ を選び，上の座標変換により $f \in k[x_1, \cdots, x_n]$ が写された多項式を $\tilde{f} \in k[\tilde{x}_1, \cdots, \tilde{x}_n]$ と表すことにする．この変換は線型性を保つので，集合 $\widetilde{I} = \{\tilde{f} \mid f \in I\}$ は再び $k[\tilde{x}_1, \cdots, \tilde{x}_n]$ のイデアルとなる．ここで，もし変換された方程式が解を持つならば，もとの方程式も解を持つので，$\mathbf{V}(I) = \emptyset$ ならば $\mathbf{V}(\widetilde{I}) = \emptyset$ である．また，この変換によって定数は変化しないので，$1 \in \widetilde{I}$ が得られれば $1 \in I$ も従う．

以上より，$1 \in \widetilde{I}$ を示せば十分である．$f_1 \in I$ は $\tilde{f}_1 \in \widetilde{I}$ に写されるので，次のように書き換えられる

$$\tilde{f}_1(\tilde{x}_1, \cdots, \tilde{x}_n) = c(a_2, \cdots, a_n)\tilde{x}_1^N + (\tilde{x}_1\text{に関して } N \text{ 次未満の式}).$$

ここで $c(a_2, \cdots, a_n) \neq 0$ である．これは，部分解 $(\tilde{x}_2, \cdots, \tilde{x}_n)$ が与えられたときに，$\tilde{x}_1$ に関して拡張できることを意味する．

$$\pi_1 : k^n \longrightarrow k^{n-1}$$

を後ろの $n-1$ 成分への射影とする．$\widetilde{I}_1 = \widetilde{I} \cap k[\tilde{x}_2, \cdots, \tilde{x}_n]$ とする．幾何学的拡張定理により，k^{n-1}での部分解は常に拡張できること，すなわち $\mathbf{V}(\widetilde{I}_1) = \pi_1(\mathbf{V}(\widetilde{I}))$ が分かる．よって，$\mathbf{V}(\widetilde{I}_1) = \pi_1(\mathbf{V}(\widetilde{I})) = \pi_1(\emptyset) = \emptyset$ となる．帰納法の仮定より，$\mathbf{V}(\widetilde{I}_1) = \emptyset$ のとき $\widetilde{I}_1 = k[\tilde{x}_2, \cdots, \tilde{x}_n]$ となる．したがって $1 \in \widetilde{I}_1 \subset \widetilde{I}$となり，証明が完結した． □

弱零点定理により，第 1 章の問題（A）を解くことができる．この問題は多項式連立方程式 $f_1 = \cdots = f_s = 0$ が $\mathbb{C}^n$ に解を持つかというものであった．この連立方程式が解を持たないことは，$\mathbf{V}(f_1, \cdots, f_s) = \emptyset$ つまり $1 \in \langle f_1, \cdots, f_s \rangle$ と同値である．したがって，$\langle f_1, \cdots, f_s \rangle$ の簡約グレブナー基底が $\{1\}$ であるかを調べればよい．逆にこの基底が $\{1\}$ でなければ（0 であるか変数を含むならば）$\mathbb{C}^n$ にこのイデアルの元の共通零点が存在する．

このように，代数的閉体上では多様体とイデアルの間にある程度の対応関係がある．しかしそれは 1 対 1 対応とまではいかない．補題 1-12. で議論したようにどのような体上であっても $\mathbf{V}(x) = \mathbf{V}(x^2) = \{0\}$ である．これは異なるイデアルにそれぞれ同じ多様体が対応している例である．$\langle x, y \rangle$ と $\langle x^m, y^n \rangle$ もそうである．異なるイデアルが同じ多様体を定める理由は，多項式とその冪は同じ集合上で消えるからである．

定理 4-2.　ヒルベルトの零点定理

k を代数的閉体とする．多項式 $f, f_1, \cdots, f_s \in k[x_1, \cdots, x_n]$ が $f \in \mathbf{I}(\mathbf{V}(f_1, \cdots, f_s))$ を満たすとする．このとき，ある整数 $m \in \mathbb{N}_+$ が存在して

$$f^m \in \langle f_1, \cdots, f_s \rangle$$

となる．逆も成立する．

証明　多項式 $f_1, \cdots, f_s$の共通零点で消える多項式 f に対して，$m \in \mathbb{N}_+$と $A_1, \cdots, A_s \in k[x_1, \cdots, x_n]$ で

$$f^m = \sum_{i=1}^{s} A_i f_i \quad \cdots (*)$$

を満たすものが存在することを示す．

そのためにまずイデアル

$$\widetilde{I} = \langle f_1, \cdots, f_s, 1 - yf \rangle \subset k[x_1, \cdots, x_n, y]$$

を考え，これが

$$\mathbf{V}(\widetilde{I}) = \emptyset$$

を満たすことを示す．点 $P = (a_1, \cdots, a_n, a_{n+1}) \in k^{n+1}$をとる．

(1)　$(a_1, \cdots, a_n)$ が $f_1, \cdots, f_s$ の共通零点である場合，仮定より $f(a_1, \cdots, a_n) = 0$ となる．よって，$1 - yf$ の点 P での値は，$1 - a_{n+1} f(a_1, \cdots, a_n) = 1 \neq 0$ となり，$P \notin \mathbf{V}(\widetilde{I})$ となる．

(2)　$(a_1, \cdots, a_n)$ が $f_1, \cdots, f_s$ の共通零点でない場合, ある $i \in \{1, \cdots, s\}$ に対して $f_i(a_1, \cdots, a_n) \neq 0$ である．ここで f_iを y によらないものとすると，$f_i(a_1, \cdots, a_n, a_{n+1}) \neq 0$ となる．よってこの場合も $P \notin \mathbf{V}(\widetilde{I})$ となる．$P \in k^{n+1}$は任意なので，これで $\mathbf{V}(\widetilde{I}) = \emptyset$ が得られた．

したがって弱い零点定理より，$1 \in \widetilde{I}$ が分かる．すなわち

$$1 = \sum_{i=1}^{s} p_i(x_1, \cdots, x_n, y) \cdot f_i + q(x_1, \cdots, x_n, y) \cdot (1 - yf)$$

となるような多項式 $p_i, q \in k[x_1, \cdots, x_n, y]$ が存在する．ここで $y = \dfrac{1}{f} = \dfrac{1}{f(x_1, \cdots, x_n)}$ とおく．すると

$$1 = \sum_{i=1}^{s} p_i(x_1, \cdots, x_n, \frac{1}{f}) f_i$$

が得られる．この両辺に十分高い冪 f^m を掛ければ，$(*)$ を満たす多項式 $A_1, \cdots, A_s$ の存在が言える．逆の手順によって，この逆の成立も分かる．　□

4.2　根基イデアルと多様体の対応

ヒルベルトの零点定理で考えた多様体のイデアル $\mathbf{I}(\mathbf{V}(f_1, \cdots, f_s))$ はどのような集合となるだろうか？ 補題 1-12. より

$$I \subset \mathbf{I}(\mathbf{V}(I))$$

であった．これはヒルベルトの零点定理からもすぐに分かる．

補題 4-3.　V を多様体とすると，$f^m \in \mathbf{I}(V)$ ならば $f \in \mathbf{I}(V)$ である．

証明　$p \in V$ とする．$f^m \in \mathbf{I}(V)$ ならば $(f(p))^m = 0$ である．すなわち $f(p) = 0$ である．$p \in V$ は任意なので $f \in \mathbf{I}(V)$ が成立する．　□

したがって，多様体 V で消える多項式全体によるイデアルは，ある多項式の冪が属せばその多項式自体も属するという性質を持つ．その多項式たちこそが I と $\mathbf{I}(\mathbf{V}(I))$ の差異である．さて，今述べた性質をもつイデアルを改めて定義する．

定義 4-4.　根基イデアル

イデアル I がある $m \in \mathbb{N}_+$に対して $f^m \in I$ ならば $f \in I$ をであるとき，I を**根基イデアル**という．

補題 4-3. を言い換えると，$\mathbf{I}(V)$ は根基イデアルである．I と $\mathbf{I}(\mathbf{V}(I))$ が一致しないのは，I が根基イデアルでないからである．次に，根基イデアルでないイデアル I の根基をとるという操作を導入する．

定義 4-5.　根基

$I \subset k[x_1, \cdots, x_n]$ をイデアルとする．集合

$$\{\, f \mid m \in \mathbb{N}_+ \ \ s.t.\ \ f^m \in I \,\}$$

を I の**根基**といい $\sqrt{I}$ と書く．

まずは根基の性質を考える．$I \subset \sqrt{I}$ は簡単に分かる．実際 $f \in I$ ならば $f^1 \in I$ なので $f \in \sqrt{I}$ である．また，I が根基イデアルであることと $I = \sqrt{I}$ であることは同値である．$\sqrt{\sqrt{I}} = \sqrt{I}$ も簡単である．

例 4-6.　$J = \langle x^2, y^3 \rangle \subset k[x, y]$ の根基の様子を見てみる．

x も y も J には属さないが，$x \in \sqrt{J}$ かつ $y \in \sqrt{J}$ であり，$\sqrt{J} = \langle x, y \rangle$ である．積は

$$(x \cdot y)^2 = x^2 \cdot y^2 \in J$$

より，$x \cdot y \in \sqrt{J}$ である．和は

$$(x + y)^4 = x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4 \in J$$

より，$x + y \in \sqrt{J}$ である．よって$\sqrt{J}$ はイデアルであり，$J \subsetneq \sqrt{J}$ である．

補題 4-7.　I が $k[x_1, \cdots, x_n]$ のイデアルならば，$\sqrt{I}$ も I を含む $k[x_1, \cdots, x_n]$ のイデアルである．すなわち根基イデアルである．

証明　$f, g \in \sqrt{I}$ をとると，正の整数 m, l が存在して $f^m, g^l \in I$ となる．$(f + g)^{m+l-1}$の 2 項展開の各項は因子 $f^i g^j$ を持つ．ここで $i + j = m + l - 1$. $i \geq m$ か $j \geq l$ のいずれかが成立するので，f^i か g^j のいずれかが I に含まれ，$f^i g^l \in I$ となる．したがって $(f + g)^{m+l-1} \in I$ であり，$f + g \in \sqrt{I}$ が得られる．積についても，$f \in \sqrt{I}, h \in k[x_1, \cdots, x_n]$ とすれば $(h \cdot f)^m = h^m \cdot f^m \in I$ である．よって $h \cdot f \in \sqrt{I}$ となる．　□

以上で，零点定理のイデアル論的な定式化を述べることができる．

定理 4-8.　強い零点定理

k を代数的閉体とする．I を $k[x_1, \cdots, x_n]$ のイデアルとすると次が成立する

$$\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}.$$

証明　$(\supset)$ $f \in \sqrt{I}$ とすると，ある正の整数 m に対して $f^m \in I$ であり，f^mは $\mathbf{V}(I)$ で消える．このと

き f も $\mathbf{V}(I)$ で消えるから，$f \in \mathbf{I}(\mathbf{V}(I))$ となる．
$(\subset)$ 逆に $f \in \mathbf{I}(\mathbf{V}(I))$ とすると，f は $\mathbf{V}(I)$ で消える．ヒルベルトの零点定理より，ある正の整数 m が存在して $f^m \in I$ となる．よって $f \in \sqrt{I}$ である． □

零点定理と言えば普通はこの定理 4-8. を指す．零点定理の最も重要な帰結は，幾何と代数の間の対応表を作れることである．その対応表の基盤は次の定理にある．

定理 4-9.　イデアル一多様体対応

k を任意の体とする．

(i) 写像

$$\mathbf{I}：\text{アフィン多様体} \longrightarrow \text{イデアル}$$
$$\mathbf{V}：\text{イデアル} \longrightarrow \text{アフィン多様体}$$

は，それぞれ包含関係を逆転する．つまりイデアルが $I_1 \subset I_2$ならば $\mathbf{V}(I_1) \supset \mathbf{V}(I_2)$ であり，同様に多様体が $V_1 \subset V_2$ならば $\mathbf{I}(V_1) \supset \mathbf{I}(V_2)$ である．さらに，任意の多様体 V に対して

$$\mathbf{V}(\mathbf{I}(V)) = V$$

が成立し，$\mathbf{I}$ は常に 1 対 1 である．

(ii)　k が代数的閉体のとき，根基イデアルだけを考えれば，写像

$$\mathbf{I}：\text{アフィン多様体} \longrightarrow \text{根基イデアル}$$
$$\mathbf{V}：\text{根基イデアル} \longrightarrow \text{アフィン多様体}$$

はそれぞれ包含関係を逆転する全単射であり，互いに逆写像となる．

証明　(i) 包含関係について，後半は命題1-13. で示したので，ここでは前半を示す．$I_1 \subset I_2 \subset k[x_1, \cdots, x_n]$ とする．それぞれのイデアルの元はその基底の線型和で書けるので，I_1 の生成元は I_2 の生成元でもある．よってある多項式 $g_1, \cdots, g_l \in k[x_1, \cdots, x_n]$ を用いて，$I_2 = I_1 + \langle g_1, \cdots, g_l \rangle$ と書ける．ゆえに，少なくとも I_2 の生成元すべての共通零点全体 $\mathbf{V}(I_2)$ 上では，I_1 の生成元もすべて消えることになり，$\mathbf{V}(I_1) \supset \mathbf{V}(I_2)$ となる．

次に，$\mathbf{V}(\mathbf{I}(V)) = V$ を示す．$V = \mathbf{V}\langle f_1, \cdots, f_s \rangle \subset k^n$とする．$(\supset)$ 任意の $f \in \mathbf{I}(V)$ は V で消えるので．($V \subset \mathbf{V}(f)$ つまり) $V \subset \mathbf{V}(\mathbf{I}(V))$ である．$(\subset)$ $f_1, \cdots, f_s \in \mathbf{I}(V)$ であるので，$\langle f_1, \cdots, f_s \rangle \subset \mathbf{I}(V)$ となる．これに $\mathbf{V}$ を作用させると，包含関係が逆転するので，$\mathbf{V}(\mathbf{I}(V)) \subset V$ となる．以上で示したい等号の成立が分かる．よって $\mathbf{I}$ は左逆写像を持つので，1 対 1 であると分かる．

(ii) $\mathbf{I}(V)$ は根基であるので，$\mathbf{I}$ は多様体の集合から根基イデアルの集合への写像である．$\mathbf{V}(\mathbf{I}(V)) = V$ が得られているので，あとは $\mathbf{I}(\mathbf{V}(I)) = I$ であることを示せばよい．零点定理より $\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$ であるが，I を根基としているので $I = \sqrt{I}$ であり，よって示すべき等式は直ちに得られる．したがって $\mathbf{V}$ と $\mathbf{I}$ は互いに逆写像であり，所与の集合間の全単射を定める． □

この定理の帰結として，多様体に関する問題は，代数的閉体上で考える限りは根基イデアルに関する代数の問題に言い換えられることが分かる．そしてその逆も可能である．この代数と幾何の間を行き来できる特徴は大変に有用である．さらに，多様体どうしの集合論的演算やその他の性質にもイデアルとの整然な対応関係があり，置き換えが可能である（上巻第 4 章の第 3 節から第 6 節を参照）．

ここまでの議論から，イデアルの根基を計算によって求める方法があるのかという疑問が浮かぶ．根基の生成元を求めるアルゴリズムは，近年実用的なものが発見されている．

しかしここでは手の付け易い根基所属問題を解くことに留める．つまり与えられた多項式 f が根基 $\sqrt{I}$ に属するかを判定できるかという問題である．ある正の整数 m に対して $f^m \in I$ かどうかを判定すればいいように思えるが，m の上限が分からない限り，すべての m についてそれを調べることは不可能である．けれども，好運にもヒルベルトの零点定理の証明を用いると，その判定法が与えられる．具体的な m の値は手に入らないが，判定は可能となる．

命題 4-10.　根基所属判定

k を任意の体とし，$I = \langle f_1, \cdots, f_s \rangle \subset k[x_1, \cdots, x_n]$ をイデアルとする．このとき，$f \in \sqrt{I}$ であるための必要十分条件は f が

$$\langle f_1, \cdots, f_s, 1 - yf \rangle = \langle 1 \rangle \subset k[x_1, \cdots, x_n, y]$$

を満たすことである．

証明　$\langle f_1, \cdots, f_s, 1 - yf \rangle = \widetilde{I}$ とおく．

($\Leftarrow$) $1 \in \widetilde{I}$ とすると，ヒルベルトの零点定理の証明にあるように

$$1 = \sum_{s}^{i=1} p_i(x_1, \cdots, x_n, y) \cdot f_i + q(x_1, \cdots, x_n, y) \cdot (1 - yf)$$

となるような多項式 $p_i, q \in k[x_1, \cdots, x_n, y]$ が存在する．$y = \dfrac{1}{f} = \dfrac{1}{f(x_1, \cdots, x_n)}$ とおくと

$$1 = \sum_{s}^{i=1} p_i(x_1, \cdots, x_n, \frac{1}{f}) \cdot f_i$$

が得られる．両辺に十分高い冪 f^m を掛ければ，$f^m \in I$ が分かり，$f \in \sqrt{I}$ が得られる．

($\Rightarrow$) $f \in \sqrt{I}$とする．このときある m に対して $f^m \in I \subset \widetilde{I}$ であり，また $1 - yf \in \widetilde{I}$ でもあるので，結局

$$\begin{aligned} 1 &= y^m f^m + (1 - y^m f^m) \\ &= y^m \cdot f^m + (1 - yf) \cdot (1 + yf + \cdots + y^{m-1} f^{m-1}) \in \widetilde{I} \end{aligned}$$

となる．　□

この方法によれば，イデアル $I + \langle 1 - yf \rangle$ の簡約グレブナー基底を計算して，$I + \langle 1 - yf \rangle = \langle 1 \rangle$ が分かれば $f \in \sqrt{I}$ であり，そうでなければ $f \notin \sqrt{I}$ であると判定できる．

例 4-11.　$k[x, y]$ のイデアル $I = \langle xy^2 + 2y^2, x^4 - 2x^2 + 1 \rangle$ を考える．$f = y - x^2 + 1$ が $\sqrt{I}$ に属するかを判定する．

$k[x, y, z]$ の lex 順序を用いると，イデアル

$$\widetilde{I} = \langle xy^2 + 2y^2, x^4 - 2x^2 + 1, 1 - z(y - x^2 + 1) \rangle \subset k[x, y, z]$$

は簡約グレブナー基底 $\{1\}$ を持つことが分かる．よって判定法より $y - x^2 + 1 \in \sqrt{I}$ が従う．

この f は何乗から I に入るのだろうか？ lex 順序に関する I のグレブナー基底を $G = \{x^4 - 2x^2 + 1, y^2\}$ とする．

$$\begin{aligned} \overline{y - x^2 + 1}^G &= y - x^2 + 1 \notin I, \\ \overline{(y - x^2 + 1)^2}^G &= -2x^2 y + 2y \notin I, \\ \overline{(y - x^2 + 1)^3}^G &= 0 \end{aligned}$$

と計算でき，f は 3 乗から上の冪が I に属することが分かる．

このことを幾何学的に解釈することもできる．I の生成元を因数分解すると

$$xy^2+2y^2=y^2(x+2) \quad と \quad x^4-2x^2+1=(x^2-1)^2$$

である．よって $\mathbf{V}(I)=\{(\pm1,0)\}$ であり，I に属する多項式はこの $\mathbf{V}(I)$ の 2 点それぞれで，少なくとも 2 次の位数で消えている．f も勿論 $(\pm1,0)$ で消えるが，1 次の位数でしか消えていない．だから I の元を得るには，f のより高い冪を考える必要があるのである．

イデアルの根基を計算できる例の 1 つとして，単項イデアル $I=\langle f\rangle$ を考察する．多項式環は UFD であるので，その元 f は一意に既約分解ができる．このとき $\sqrt{I}$ は簡単に書き表せる．

命題 4-12. $f\in k[x_1,\cdots,x_n]$，$I=\langle f\rangle$ とする．$f=f_1^{a_1}f_2^{a_2}\cdots f_r^{a_r}$ を f の異なる既約多項式の積への分解とすると，次のように書ける

$$\sqrt{I}=\sqrt{\langle f\rangle}=\langle f_1f_2\cdots f_r\rangle.$$

証明 $(\supset)$ N を $a_1,\cdots,a_r$の最大値より真に大きい整数とする．このとき

$$(f_1f_2\cdots f_r)^N=f_1^{N-a_1}f_2^{N-a_2}\cdots f_r^{N-a_r}f\in I$$

となり，$f_1f_2\cdots f_r\in\sqrt{I}$であることが分かる．

$(\subset)$ 逆に $g\in\sqrt{I}$ とすると，$g^M\in I$ となるような正の整数 M が存在する．よって $g^M=h\cdot f$ となるような $h\in k[x_1,\cdots,x_n]$ が存在する．ここで，$g=g_1^{b_1}g_2^{g_2}\cdots g_s^{b_s}$ を g の異なる既約な多項式の積への分解とする．このとき $g^M=g_1^{b_1M}g_2^{g_2M}\cdots g_s^{b_sM}$ は，g^Mの異なる既約な多項式の積への分解となる．したがって

$$g_1^{b_1M}g_2^{g_2M}\cdots g_s^{b_sM}=h\cdot f_1^{a_1}f_2^{a_2}\cdots f_r^{a_r}$$

である．一意分解性より，この両辺の既約多項式たちは，定数倍を除いて同じものでなければならない．つまり，各 $f_i\,(1\le i\le r)$ はある g_j の定数倍に一致する．これより g は f の多項式倍であることが分かり，$g\in\langle f_1f_2\cdots f_r\rangle$ が得られる． □

定義 4-13. **簡約化，無平方**

多項式 $f\in k[x_1,\cdots,x_n]$ に対して，f の**簡約化**または**被約化**を，$\langle f_{red}\rangle=\sqrt{\langle f\rangle}$となるような多項式 f_{red}と定義する．$f=f_{red}$を満たすとき f は**簡約**あるいは**被約**である，または**無平方**であるという．

f_{red}は多項式 f の重複した因子をすべて 1 乗に変えたものである．したがって f の既約分解が分かっていれば，f_{red} は得られたのも同然である．また，f_{red}は k の定数倍を除いて一意的に決まる．

f を因数分解しなくても，f から f_{red} を計算するアルゴリズムはあるのだろうか？

命題 4-14. k を素体 $\mathbb{Q}$ を含む体とし，$I=\langle f\rangle\subset k[x_1,\cdots,x_n]$ とする．このとき f の簡約多項式 f_{red}は

$$f_{red}=\frac{f}{\mathrm{GCD}\left(f,\dfrac{\partial f}{\partial x_1},\dfrac{\partial f}{\partial x_2},\cdots,\dfrac{\partial f}{\partial x_n}\right)}$$

で与えられる．

証明 f を命題4-12. のように既約分解 $f=f_1^{a_1}f_2^{a_2}\cdots f_r^{a_r}$ で表すと，$\sqrt{I}=\langle f_1f_2\cdots f_r\rangle$ である．したがっ

て $f_{red} = f_1 f_2 \cdots f_r$ であるので

$$\mathrm{GCD}\left(f, \frac{\partial f}{\partial x_1}, \frac{\partial f}{\partial x_2}, \cdots, \frac{\partial f}{\partial x_n}\right) = f_1^{a_1-1} f_2^{a_2-1} \cdots f_r^{a_r-1}$$

を示せばよい.

まずは f の偏導関数を計算する

$$\frac{\partial f}{\partial x_j} = f_1^{a_1-1} f_2^{a_2-1} \cdots f_r^{a_r-1} \left(a_1 \frac{\partial f_1}{\partial x_j} f_2 \cdots f_r + a_2 f_1 \frac{\partial f_2}{\partial x_f} f_3 \cdots f_r + \cdots\cdots + a_r f_1 \cdots f_{r-1} \frac{\partial f_r}{\partial x_j}\right).$$

これより，$f_1^{a_1-1} f_2^{a_2-1} \cdots f_r^{a_r-1}$ は GCD を割り切ることが分かる．あとは，各 i に対して，$f_i^{a_i}$ で割り切れないような $\dfrac{\partial f}{\partial x_j}$ が存在することを示せばよい.

今，$f = f_i^{a_i} h_i$ と書くことにする．ここで既約性より，h_i は f_i で割り切れない多項式である．また f_i は定数ではないのである変数 x_j を含む．よって f の偏導関数は

$$\frac{\partial f}{\partial x_j} = f_i^{a_i-1} \left(a_i \frac{\partial f_i}{\partial x_j} h_i + f_i \frac{\partial h_i}{\partial x_j}\right)$$

とも書ける．もしこの式が $f_i^{a_i}$ で割り切れるならば，$\dfrac{\partial f_i}{\partial x_j} h_i$ は f_i で割り切れなければならない．f_i は h_i を割り切らないので，f_i は $\dfrac{\partial f_i}{\partial x_j}$ を割り切らなければならない．$\mathbb{Q} \subset k$ だから k は無限体であり，f_i は変数 x_j を含むので，$\dfrac{\partial f_i}{\partial x_j} \neq 0$ である．しかも $\dfrac{\partial f_i}{\partial x_j}$ の全次数は f_i のそれよりも真に小さいので，f_i は $\dfrac{\partial f_i}{\partial x_j}$ を割り切れない．よって，結局 $\dfrac{\partial f}{\partial x_j}$ は $f_i^{a_i}$ では割り切れない．これにより，示したい事実が証明できた． □

体が素体 $\mathbb{Q}$ を含まない場合には，この公式は一般には正しくない．例えば有限体上では，f の次数によってはその偏導関数 $\dfrac{\partial f}{\partial x_j}$ が消えることがあり，そのとき上の公式の分母が 0 となってしまうからである.

最後に，第 3 章でやり残していた定理 3-9. 閉包定理の (i) の証明の準備ができたので，ここで行う.

定理 4-15. k を代数的閉体とする．$V = \mathbf{V}(f_1, \cdots, f_s) \subset k^n$ とする．$\pi_l : k^n \longrightarrow k^{n-l}$ を後ろの $n-l$ 成分への射影とする．I_l を l 次の消去イデアル $I_l = \langle f_1, \cdots, f_s \rangle \cap k[x_{l+1}, \cdots, x_n]$ とすると，$\mathbf{V}(I_l)$ は $\pi_l(V)$ のザリスキー閉包である.

証明 アフィン多様体とは限らない部分集合 $S \subset k^n$ に対し，$\overline{S}$ とは S を含む最小の多様体のことであり，これを S の**ザリスキー閉包**という．これは $\mathbf{V}(\mathbf{I}(S))$ に等しい．$\cdots(\star)$ よって今示すべきことは $\mathbf{V}(I_l) = \mathbf{V}(\mathbf{I}(\pi_l(V)))$ である.

$(\supset)$ 補題 3-7. より，$\pi_l(V) \subset \mathbf{V}(I_l)$ である．$\mathbf{V}(\mathbf{I}(\pi_l(V)))$ は $\pi_l(V)$ のザリスキー閉包であるので $\mathbf{V}(\mathbf{I}(\pi_l(V))) \subset \mathbf{V}(I_l)$ が従う.

$(\subset)$ $f \in \mathbf{I}(\pi_l(V))$ とする．任意の $(a_{l+1}, \cdots, a_n) \in \pi_l(V)$ に対して $f(a_{l+1}, \cdots, a_n) = 0$ である．f を $k[x_1, \cdots, x_n]$ の元と見なすと，任意の $(a_1, \cdots, a_n) \in V$ に対して $f(a_1, \cdots, a_n) = 0$ となる．ヒルベルトの零点定理より，$f^N \in \langle f_1, \cdots, f_s \rangle$ となるような整数 N が存在する．f は $x_1, \cdots, x_l$ に依存しないので，f^N もそうである．したがって $f^N \in \langle f_1, \cdots, f_s \rangle \cap k[x_{l+1}, \cdots, x_n] = I_l$ である．つまり $f \in \sqrt{I_l}$ であり，$\mathbf{I}(\pi_l(V)) \subset \sqrt{I_l}$ となる．以上で $\mathbf{V}(I_l) = \mathbf{V}(\sqrt{I_l}) = \subset \mathbf{V}(\mathbf{I}(\pi_l(V)))$ となり，定理は証明された． □

（証明の補足）$(\star)$ の理由を述べる．$\overline{S} = \mathbf{V}(\mathbf{I}(S))$ であることを示すには，$W \subset k^n$ を S を含む多様体と

したときに $\mathbf{V}(\mathbf{I}(S)) \subset W$ であることを示せばよい．今，$S \subset W$ ならば定理 4-9. より $\mathbf{I}(S) \supset \mathbf{I}(W)$，更に $\mathbf{V}(\mathbf{I}(S)) \subset \mathbf{V}(\mathbf{I}(W)) = W$ である．

4.3 多様体の既約分解

補足として，根基イデアルと共に第 5 章で登場する概念を定義する．第 1 章の第 2 節で多様体どうしの和集合はまた多様体になることを見た．例えば $\mathbf{V}(xz, yz)$ は直線と平面の和集合であった．直線や平面は $\mathbf{V}(xz, yz)$ より単純な集合で，それ以上単純な多様体に分解できないように思える．

定義 4-16.　アフィン多様体 $V \subset k^n$ が**既約**であるとは，V をアフィン多様体 V_1, V_2 を用いて $V = V_1 \cup V_2$ と表したとき，$V_1 = V$ または $V_2 = V$ が成り立つことをいう．

$\mathbf{V}(xz, yz)$ は直線と平面に分解可能であるので可約である．しかし直線や平面が既約であることは，この定義からは自明でない．多様体がいつ既約になるかを判定するには，対応するイデアルを見ればよい．証明は割愛するけれども，実は既約多様体のイデアルは素イデアルとなる．またその逆も成立する．そして素イデアルは根基イデアルになることが簡単に分かるので，代数的閉体上で 2 つの写像 $\mathbf{I}, \mathbf{V}$ は，既約多様体と素イデアルの 1 対 1 対応を誘導する．

可約な多様体に対しては，巨大で複雑であるほど，単純な性質をもつパーツに分析することが重要となる．直観的には，有限次元の任意の多様体は，既約な多様体に分割することができるはずである．つまり多様体の分解が有限回で完了できることである．それはイデアルの ACC に対応している．

命題 4-17.　降鎖条件

k^n の多様体の減少列 $V_1 \supset V_2 \supset \cdots$ は必ず途中で止まる．つまり $\exists N \in \mathbb{N} \quad s.t. \quad V_N = V_{N+1} = \cdots$.

証明　V_i に対応するイデアルをとると，イデアルの昇鎖

$$\mathbf{I}(V_1) \subset \mathbf{I}(V_2) \subset \cdots$$

が得られる．イデアルの ACC ($k[x_1, \cdots, x_n]$ のネーター性) より，$\exists N \in \mathbb{N}_{>0}$ $s.t.$ $\mathbf{I}(V_N) = \mathbf{I}(V_{N+1}) = \cdots$ となる．任意の多様体 V に対して $\mathbf{V}(\mathbf{I}(V)) = V$ であるので，$V_N = V_{N+1} = \cdots$ が得られる．　□

定理 4-18.　$V \subset k^n$ をアフィン多様体とする．V は既約な多様体 V_i の有限和集合

$$V = V_1 \cup \cdots \cup V_m$$

として書き表すことができる．

証明　背理法により示す．示すべき結論を否定すると，V は既約でないので，$V = V_1 \cup V_1'$ で $V \neq V_1, V \neq V_1'$ となるような分解をもつ．さらに V_1 か V_1' のいずれかは既約な多様体の有限和集合として表せない．そうでなければ V 自身が既約な多様体の有限和集合として表せてしまうからである．そこで V_1 がこの性質をもつとする．同様に，$V_1 = V_2 \cup V_2', V_1 \neq V_2, V_1 \neq V_2'$ と分解されて，V_2 が同じ性質をもつと仮定できる．この議論を延々と繰り返すことができ，アフィン多様体の無限列

$$V_1 \subset V_2 \subset \cdots$$

であって

$$V_1 \neq V_2 \neq \cdots$$

を満たすものが得られる．ところがこれは多様体の降鎖条件に反する． □

このように任意の多様体は有限既約分解をもつ．では与えられた多様体の既約分解を求めるにはどのように計算すればよいのだろうか？ 例えば $\mathbf{V}(xz, yz)$ の場合は，生成元の共通因子である z で括り出すことで $\mathbf{V}(x, y) \cup \mathbf{V}(z)$ と分解できる．そこでイデアル商との関連を考える．

定義 4-19.　イデアル商

I, J を $k[x_1, \cdots, x_n]$ のイデアルとする．$I : J$ を

$$\{f \in k[x_1, \cdots, x_n] \mid \forall g \in J \ \ s.t. \ \ fg \in I\}$$

と定義し，I の J による**イデアル商**あるいは**コロンイデアル**という．

$k[x, y, z]$ のイデアル $\langle xz, yz\rangle$ に適用すると

$$\begin{aligned}\langle xz, yz\rangle : \langle z\rangle &= \{f \in k[x, y, z] \mid fz \in \langle xz, yz\rangle\} \\ &= \{f \in k[x, y, z] \mid fz = Axz + Byz\} \\ &= \{f \in k[x, y, z] \mid f = Ax + By\} \\ &= \langle x, y\rangle.\end{aligned}$$

イデアル商 $I : J$ もまた $k[x_1, \cdots, x_n]$ のイデアルであり，I を含む．

また，イデアル商の零点 $\mathbf{V}(I : J)$ は，$\overline{\mathbf{V}(I) - \mathbf{V}(J)}$ を含む．上の包含関係は，I の J による商をとることが I の零点から J の零点を除くことに相当することを意味する．さらに代数的閉体上で I が根基イデアルならば，ここに等号が成立する． このとき

$$\mathbf{V}(I : J) \cup \mathbf{V}(J) = \overline{\mathbf{V}(I) - \mathbf{V}(J)} \cup \mathbf{V}(J) = \mathbf{V}(I) \quad \cdots (\star)$$

というように $\mathbf{V}(I)$ は分解できる．これを有限回繰り返せば，既約分解を得ることは理論上は可能である．

例 4-20.　$I = \langle xz - y^2, x^3 - yz\rangle$ に対し，$V = \mathbf{V}(I)$ の既約分解を求める．

V は図示が可能で，z 軸と 1 本の開いた捩れ 3 次曲線からなることが分かる．よって V は可約であると思われる．z 軸は既約だから，あとは曲線部分 $\overline{V - \mathbf{V}(x, y)}$ を調べればよい．前段落の議論より，イデアル商 $I : \langle x, y\rangle$ を考えることになる．これについて次の等式の成立が簡単に分かる

$$I : \langle x, y\rangle = (I : \langle x\rangle) \cap (I : \langle y\rangle).$$

$I : \langle x\rangle$ の生成元は，$I \cap \langle x\rangle$ の生成元をすべて x で割ったものである．

$z > y > x$ の lex 順序を用いて $I \cap \langle x\rangle$ を計算すると

$$I \cap \langle x\rangle = \langle x^2 z - xy^2, x^4 - xyz, x^3 y - xz^2, x^5 - xy^3\rangle$$

となる．これより

$$I : \langle x\rangle = I + \langle x^2 y - z^2\rangle$$

と計算できる．同様にして

$$I : \langle y\rangle = I + \langle x^2 y - z^2\rangle = I : \langle x\rangle$$

となる．よって

$$I : \langle x, y \rangle = (I : \langle x \rangle) \cap (I : \langle y \rangle) = I + \langle x^2 y - z^2 \rangle$$

である．$W := \mathbf{V}(I + \langle x^2 y - z^2 \rangle)$ は既約であることが分かる．後で $(*)$ で示すように I は根基であるので，$(\star)$ より

$$\overline{V - \mathbf{V}(x, y)} = \mathbf{V}(I : \langle x, y \rangle) = W \subset \mathbb{C}$$

が成立する．よって

$$V = \mathbf{V}(x, y) \cup W$$

となり，V の既約分解が分かった．

複雑な既約分解になると，既約成分のダブりや別の既約成分に含まれるような成分がしばしば現れる．そうした不要な成分を除外して，簡潔な既約分解を定義する．

定義 4-21.　極小分解

$V \subset k^n$ をアフィン多様体とする．各 V_i が既約であるような分解

$$V = V_1 \cup \cdots \cup V_m$$

が $i \neq j$ に対して $V_i \not\subset V_j$ を満たすとき，**極小分解**あるいは**無駄のない分解**であるという．

定理 4-22.　$V \subset k^n$ をアフィン多様体とする．このとき V は極小分解

$$V = V_1 \cup \cdots \cup V_m$$

をもつ．さらにこの分解は，$V_1, \cdots, V_m$ の順序の入れ換えを除いて一意である．

証明　V は既約分解 $V = V_1 \cup \cdots \cup V_m$ をもつ．ある V_iが $i \neq j$ であるようなある V_j に含まれるならば，V_i を除外して，残りの $j \neq i$ であるような V_j の和集合として V を表せる．m は有限だから，この過程を繰り返せば V の極小分解が得られる．

一意性を示すために，$V = V_1' \cup \cdots \cup V_l'$を V の別の極小分解とする．初めの分解の各 V_i に対して

$$V_i = V_i \cap V = V_i \cap (V_1' \cup \cdots \cup V_l') = (V_i \cap V_1') \cup \cdots \cup (V_i \cap V_l')$$

である．V_i は既約なので，既約多様体の定義よりある j に対して $V_i = V_i \cap V_j'$ となる．つまり $V_i \subset V_j'$ である．同様に，$V_j' \subset V_s$となるような $1 \leq s \leq m$ も存在する．合わせて

$$V_i \subset V_j' \subset V_s$$

となる．極小性より $i = s$ であり，ゆえに $V_i = V_j'$ である．したがって，各 V_i は $V = V_1' \cup \cdots \cup V_l'$ に現れるので，$m \leq l$ を得る．同様に $l \leq m$ も分かり，$m = l$ となる．よって V_i' は V_i の入れ換えであり，一意性が証明された．　□

この一意性は，和が有限でないときには正しくない．例えば平面はその上の点全体の無限和集合であるが，直線全体の無限和集合でもある．そしてその有限性はヒルベルトの基底定理，あるいは多項式環のネーター性の帰結である．

また，根基イデアルと多様体との間の写像の 1 対 1 対応を考えると，この定理は代数的にも述べられる．すなわち，代数的閉体上で，任意の根基イデアルは有限個の素イデアルの無駄のない交わり $I = P_1 \cap \cdots \cap P_r$ として一意的に書ける．ここで $i \neq j$ に対して $P_i \not\subset P_j$ である（任意の体でもこれは成り立つが，その理由は別の考え方による）．

例 4-23.　例 4-20. の $I=\langle xz-y^2, x^3-yz\rangle$ に対し，分解 $V=\mathbf{V}(x,y)\cup W$ は極小分解である．これに対応する I の分解について考える．

今，$I=\langle x,y\rangle\cap(I:x)$ は簡単に分かる．$\langle x,y\rangle$ も I のイデアル商として表すことができるだろうか？ V から W を取り除くことを考えて，$I:(x^2y-z^2)=\langle x,y\rangle$ と計算できる．よって

$$I=(I:(x^2y-z^2))\cap(I:x)$$

となる．$I:(x^2y-z^2)=\langle x,y\rangle$ は素イデアルである．$I:x$ についても，W が既約だから $\mathbf{I}(W)=I:x$ は素イデアルであると分かる．よって，I を商イデアルの形をした素イデアルの交わりとして書くことができた．

$(*)$　例 4-20. で残していた I が根基イデアルである理由を示す．素イデアルはすなわち根基イデアルであったので，I は根基イデアルの交わりである．よって，あとは根基イデアルの交わりが根基イデアルであることを示せばよい．J_1, J_2 を根基イデアルとする．多項式の冪 $f^m\in J_1\cap J_2$ をとると，$f^m\in J_1$かつ $f^m\in J_2$ であるので，$f\in J_1$かつ $f\in J_2$ であり，$f\in J_1\cap J_2$ となる．以上より I は根基イデアルである．

5　幾何の定理の自動証明

最終章は，これまでの応用として自動化された幾何的推論一般について論じる．ユークリッド幾何の一般的な命題を，代数幾何の問題に置き換えて証明するアルゴリズム的手法を与える．このような方法を用いたプログラムによって，実際に新しい定理群が証明された事実がある．これは人間の知能だけに可能な思考領域であると考えられてきたため，近年は人工知能や幾何的造形の両分野の研究者に興味を抱かれている．

この方法の基礎となるアイディアを説明する．まずユークリッド平面に直交座標を導入し，定理で指定される点の座標を与える．幾何の多くの定理における仮定と結論は，与えた座標を変数とする多項式連立方程式で表すことができてしまう．そして仮定の式から結論の式が従うことを，実際に解を求めることなく証明することができる．単純な例で実行してみることにする．

例 5-1.　次の定理の証明を考える．

『平行四辺形の 2 本の対角線はそれぞれの中点で交わる』

平行四辺形の頂点を A,B,C,D とし，対角線 AD と BC の交点を N とする．証明すべき結論は $AN=DN$ である．幾何的には $\triangle ANC\equiv\triangle BND$ を示すことで証明できる．代数幾何でこれを証明するためには，まず直交座標を設定する．ここでは A に原点を AB の向きに水平な軸を据える．$u_1,u_2,u_3\in\mathbb{R}$ を不定元とし，各頂点の座標を $B=(u_1,0), \mathrm{C}=(u_2,u_3)$ とする．　D,N は A,B,C によって決まり，$D=(x_1,x_2), N=(x_3,x_4)$ とおく．このように任意の座標には u_i，その他の座標を x_j と区別する．x_jを u_i の式で表すことが目標となる．それには仮定された幾何的性質を定量すればよい．

(仮定 1) 四角形 $ABDC$ は平方四辺形である．すなわち $AB\parallel CD$ かつ $AC\parallel BD$ である．よって

$$0=\frac{x_2-u_3}{x_1-u_2}\quad\text{かつ}\quad\frac{u_3}{u_2}=\frac{x_2}{x_1-u_1}.$$

これを多項式連立方程式の形に整理して

$$h_1:=x_2-u_3=0,$$
$$h_2:=(x_1-u_1)u_3-x_2u_2=0$$

と書ける．ちなみにこれを解くと $x_1=u_1+u_2, x_2=u_3$ が得られるが，これはベクトル和の平行四辺形則が

プログラムされていれば直接得ることができる．

(仮定 2) 対角線は N で交わる．すなわち N は AD 上かつ BC 上にある．よって

$$\frac{x_4}{x_3}=\frac{x_2}{x_1} \quad \text{かつ} \quad \frac{x_4}{x_3-x_1}=\frac{u_3}{u_2-u_1}.$$

これを整理して

$$h_3 := x_4x_1 - x_3x_2 = 0,$$
$$h_4 := x_4(u_2-u_1) - (x_3-u_1)u_3 = 0$$

と書ける．

一方，証明したい結論は対角線が中点で交わることである．これを定量すると AN = ND かつ BN = NC であるので

$$x_3^2+x_4^2=(x_3-x_1)^2+(x_4-x_2)^2,$$
$$(x_3-u_1)^2+x_4^2=(x_3-u_2)^2+(x_4-u_3)^2$$

である．整理して

$$g_1 := x_1^2 - 2x_1x_3 - 2x_4x_2 + x_2^2 = 0,$$
$$g_2 := 2x_3u_1 - 2x_3u_2 - 2x_4u_3 - u_1^2 + u_2^2 + u_3^2 = 0$$

と書ける．仮定の式 $h_1=h_2=h_3=h_4=0$ の下で結論の式 $g_1=g_2=0$ が成り立つと，定理は翻訳できる．定理は正しいので，勿論これは成り立つ．仮定の式を解くと，実際に $(x_3,x_4)=(\frac{u_1+u_2}{2},\frac{u_3}{2})$ となる．

座標や変数の設定の仕方は自由であり，それにより方程式系も変わる．より複雑な作図の例ではより単純化できるような設定が望まれる．

次に，仮定や結論に現れる幾何的性質で多項式方程式系に翻訳できるものを明らかにする．

(1) $AB \perp CD \iff \overrightarrow{AB}\cdot\overrightarrow{CD}=0.$
(2) C が中心 A, 半径 AB の円周上にある $\iff$ $AB=AC.$
(3) C が AB の中点である $\iff$ A,C,B が同一直線上にあり，かつ $AB=CB.$
(4) $\angle ABC=\angle DEF$(鋭角の場合) $\iff$ 正接が等しい.
(5) BD は$\angle ABC$ を 2 等分する $\iff$ $\angle ABD=\angle CBD.$
(6) AB は $\triangle ACD$ の外接円に接する $\iff$ $\angle ACD=\angle BAD$ (接弦定理).
(7) D は $\triangle ABC$ の外接円の周上にある $\iff$ $\angle BAC=\angle BDC$ など (円周角定理).
(8) 辺の長さの積，比，(分母が 0 でない) 複比に関する等式.
(9) 三角形がある場合は，正弦定理や余弦定理などの関係式.

仮定と結論が多項式方程式系に翻訳可能である幾何の定理を**許容的である**という．許容的な定理の一般形を定める

【仮定】
$$\begin{aligned} &h_1(u_1,\cdots,u_m,x_1,\cdots,x_n)=0,\\ &\qquad\vdots\\ &h_n(u_1,\cdots,u_m,x_1,\cdots,x_n)=0, \end{aligned}$$

$u_1,\cdots,u_m$: 任意座標または独立変数,

$x_1,\cdots,x_n$: 従属変数.

【結論】 $g(u_1,\cdots,u_m,x_1,\cdots,x_n)=0.$

ここで，従属変数 x_i は仮定によって $u_1, \cdots, u_m$ で表せるので，仮定の式の本数は x_i の個数 n 以上でなければならない．また，結論の方程式は複数あっても結局 1 本ずつ扱うことになるので，簡単のため 1 本とする．

結論が仮定から従うか否かを，代数的にどのように導くかを考える．少なくとも，$h_1, \cdots, h_n$ が消えるときに g も消えれば仮定から結論が従うことは分かる．つまり

$$V = \mathbf{V}(h_1, \cdots, h_n) \subset \mathbb{R}^{m+n} \text{に対して } g \in \mathbf{I}(V) \ (\subset \mathbb{R}[u_1, \cdots, u_m, x_1, \cdots, x_n] =: R)$$

となればよい．このとき，結論 g は仮定 $h_1, \cdots, h_n$ から**厳格に従う**という．

しかし，今 $\mathbb{R}$ 上で考えているので，一般に $\mathbf{I}(V)$ を求める方法はない．そこで次の判定法を考える．

命題 5-2. $g \in \sqrt{\langle h_1, \cdots, h_n \rangle}$ ならば，g は $h_1, \cdots, h_n$ から厳格に従う．

証明 $g \in \sqrt{\langle h_1, \cdots, h_n \rangle} \implies \exists s \in \mathbb{N} \quad s.t. \quad g^s \in \langle h_1, \cdots, h_n \rangle$

$\implies \exists A_i \in R \quad s.t. \quad g^s = \sum_{i=1}^{n} A_i h_i.$

このとき $h_1, \cdots, h_n$ が消えれば g^s も消え，g も消える． □

ここで，$\mathbb{R}$ 上では $\sqrt{\langle h_1, \cdots, h_n \rangle} \subsetneq \mathbf{I}(V_{\mathbb{R}})$ であるので，この命題の逆は常には成り立たないことに注意する．

命題 4-10. により

$$g \in \sqrt{\langle h_1, \cdots, h_n \rangle} \iff \widetilde{I} = \langle h_1, \cdots, h_n, 1 - yg \rangle = \langle 1 \rangle$$

であったので，この判定法は有用である．

$\mathbb{C}$ 上で考えると，$g \in \sqrt{\langle h_1, \cdots, h_n \rangle}$の意味は分かりやすい．$\mathbb{C}$ に解をもつことを許すことにより，仮定は多様体 $V_{\mathbb{C}} \subset \mathbb{C}^{m+n}$ を定義する．このとき強い零点定理を用いると

$$g \in \sqrt{\langle h_1, \cdots, h_n \rangle} \subset \mathbb{R}[u_1, \cdots, u_m, x_1, \cdots, x_n]$$
$$\iff g \in \mathbf{I}(V_{\mathbb{C}}) \subset \mathbb{C}[u_1, \cdots, u_m, x_1, \cdots, x_n]$$

であることが証明できる．つまり $g \in \sqrt{\langle h_1, \cdots, h_n \rangle}$は，$g$ は $h_1, \cdots, h_n$から“$\mathbb{C}$ 上で厳格に従う”ことと同値である．$h_1 = \cdots = h_n = 0$ の複素数解（実在しない点の座標や角度や辺の長さ）によって g が消えている場合でも，この条件は満たされてしまうことになる．また，逆に $\mathbb{R}$ 上で正しいが $\mathbb{C}$ 上で正しくないような定理が実際に存在する (B.Sturmfels. Computing final polynomials and final syzygies using Buchberger's Grobner bases method. Results in Mathematics,Vol. 15, pp. 351-360, 1989). グレブナー基底の方法ではそのような定理には通用しない．これがこの方法における限界を示している．

また，厳格に従うという条件ではまだ強すぎる．次がその例である．

例 5-3. 例 5-1. の定理で

$$\widetilde{I} = \langle h_1, h_2, h_3, h_4, 1 - yg_1, 1 - yg_2 \rangle \subset \mathbb{R}[u_1, u_2, u_3, x_1, x_2, x_3, x_4, y]$$

の簡約グレブナー基底を計算すると，驚くべきことに $\{1\}$ にはならない．

$x_1 > x_2 > x_3 > x_4 > u_1 > u_2 > u_3$ の lex 順序における $I = \langle h_1, h_2, h_3, h_4 \rangle$ のグレブナー基底を求めると，次のようになる

$$f_1 = x_1 x_4 + x_4 u_1 - x_4 u_2 - u_1 u_3,$$
$$f_2 = (x_1 - u_1 - u_2) u_3,$$

$$
\begin{aligned}
f_3 &= x_2 - u_3,\\
f_4 &= x_3u_3 + x_4u_1 - x_4u_2 - u_1u_3,\\
f_5 &= (x_4 - \frac{1}{2}u_3)u_1(u_1 - u_2),\\
f_6 &= (x_4 - \frac{1}{2}u_3)u_1u_3.
\end{aligned}
$$

仮定により定義される $\mathbb{R}^7$ の多様体 V とおく．f_2, f_5, f_6 は可約なので，$\mathbf{V}(f_1, \cdots, f_6)$ は可約である．V を既約分解し，整理すると次の極小分解が得られる

$$
\begin{aligned}
V &= V' \cup U_1 \cup U_2 \cup U_3,\\
V' &= \mathbf{V}(x_1 - u_1 - u_2, x_2 - u_3, x_3 - \frac{u_1 + u_2}{2}, x_4 - \frac{u_3}{2}),\\
U_1 &= \mathbf{V}(x_2, x_4, u_3),\\
U_2 &= \mathbf{V}(x_1, x_2, u_1 - u_2, u_3),\\
U_3 &= \mathbf{V}(x_1 - u_2, x_2 - u_3, x_3u_3 - x_4u_2, u_1).
\end{aligned}
$$

U_1 上では $u_3 = 0$ である．u_3 は任意であると仮定していたのでこれは不適切な方程式である．$u_3 = 0$ のときは平行四辺形にならない．$x_2 = x_4 = 0$ のときも同様である．この場合は仮定に反しているため除外されなければならない．U_2, U_3 も点の配置が退化した場合を示している．

また，U_1 上で $x_2 = x_4 = 0$ なので，結論 g_1 は $g_1 = x_1^2 - 2x_1x_3$ となり消えない．U_2, U_3 上でも同じく結論は従わない．一方，V'上では x_i を u_i で表している（u_i は任意のままである）．実際 g_1, g_2 も消えるので V' 上で結論は従う．

V 全体は 4 頂点 A, B, C, D のとりうる配置すべてを表しており，最初からそれらが退化しないための条件も加えておくのが，幾何学的な証明方法である．しかし代数的に解くためには方程式系に翻訳する必要があるので，$u_3 \neq 0$ や不等式を条件として加えるわけにはいかない．よって，このように方程式系の共通零点から退化する点を除く必要がある．

定義 5-4.　$V = \mathbf{V}(h_1, \cdots, h_n)$ の既約成分のうち，すべての u_i が代数的独立（任意）であるような成分全体の和集合を $V' \subset \mathbb{R}^{m+n}$ とする．結論 g が仮定 $h_1, \cdots, h_n$ から**一般に従う**とは

$$
g \in \mathbf{I}(V') \subset \mathbb{R}[u_1, \cdots, u_m, x_1, \cdots, x_n]
$$

となるときをいう．

幾何の定理が正しいということは，その結論が仮定から**一般に従う**ことに他ならない．しかし，V を分解して V' を求めることも $\mathbf{I}(V')$ を求めることも，一般には容易ではない．

そこで，例 5-3. を用いてこの問題を考えてみる．I のグレブナー基底

$$
\begin{aligned}
f_2 &= (x_1 - u_1 - u_2)u_3,\\
f_5 &= (x_4 - \frac{1}{2}u_3)u_1(u_1 - u_2),\\
f_6 &= (x_4 - \frac{1}{2}u_3)u_1u_3
\end{aligned}
$$

に対し，次のように u_i のみの成分を除けばよい

$$
\begin{aligned}
f_2' &:= x_1 - u_1 - u_2,\\
f_5' = f_6' &:= x_4 - \frac{1}{2}u_3.
\end{aligned}
$$

$\{ f_1, f_2', f_3, f_4, f_5' \}$ を I の新たな基底とすれば $\mathbf{I}(V')$ が求まり，非退化な場合のみについて解くことができる．これは u_i を最初から可逆元と見なしたということである．係数体を $\mathbb{R}(u_1, \cdots, u_m)$ とした多項式環で考えるのである．これと命題 5-2. から次の系が分かる．

系 5-5. $H = \langle h_1, \cdots, h_n \rangle$ を $\mathbb{R}(u_1, \cdots, u_m)[x_1, \cdots, x_n]$ のイデアルとする．このとき $g \in \sqrt{H}$ ならば結論 g は仮定 $h_1, \cdots, h_n$ から**一般に従う**．

つまり g かその冪が $H \subset \mathbb{R}(u_1, \cdots, u_m)[x_1, \cdots, x_n]$ に入るかどうかを示せばよい．もしくは $\mathbb{R}(u_1, \cdots, u_m)[x_1, \cdots, x_n, y]$ のイデアルとして $H + \langle 1 - yg \rangle = \langle 1 \rangle$ が成り立てば，定理が証明できることになる．

最後に，この章の総括としてもう一つだけ例を取り上げる．この例は参考文献とは別に，当論文を書くに当たって新しくグレブナー基底の方法を適用したものでる．

例 5-6.　トレミーの定理

円に内接する任意の四角形 $ABCD$ に対して，次の等式が成立する

$$AB \cdot CD + BC \cdot DA = AC \cdot BD.$$

ここでは辺の長さでおく方が簡単であるので，$AB = a, , BC = b, CD = c, DA = d$ とおく．ここで $a, b, c, d \in \mathbb{R}^{\times}$ は既に分かっているものとする．

次に，四角形 $ABCD$ がある円に内接するという条件には，対角の和がπ であることを用いると上手くいく．これは円周角の定理からすぐに分かる．よって四角形 ABCD の 4 角について

$$\angle A + \angle C = \pi,$$
$$\angle B + \angle D = \pi.$$

角度が変数として現れる場合には，できるだけ三角関数に置き換えて翻訳する

$$cos\angle A + cos\angle C = 0,$$
$$cos\angle B + cos\angle D = 0.$$

また，四角形であることから，対角線によって 4 つの三角形 ABD, BCD, ABC, ACD が存在するので余弦定理が選択できる

$$BD^2 = a^2 + d^2 - 2ad\ cos\angle A,$$
$$BD^2 = b^2 + c^2 - 2bc\ cos\angle C,$$
$$AC^2 = a^2 + b^2 - 2ab\ cos\angle B,$$
$$AC^2 = c^2 + d^2 - 2cd\ cos\angle D.$$

ここで，都合良く余弦定理を選択させるためには，定理の結論に含まれる新たな変数 AC, BD を登場させるような立式を優先的に行うように設定する．

未知の変数 $BD = X$, $AC = Y$, $cos\angle A = A$, $cos\angle B = B$, $cos\angle C = C$, $cos\angle D = D$ をおく．単項式順序は $C = D > A = B > X = Y$ の lex 順序とする．

仮定となる $\mathbb{R}[A, B, X, Y]$ の元を考える．簡単のため，あらかじめ C, D を消去すると

$$h_1 := \ \ 2adA + X^2 - a^2 - d^2,$$
$$h_2 := -2bcA + X^2 - b^2 - c^2,$$
$$h_3 := \ \ 2abB + Y^2 - a^2 - b^2,$$
$$h_4 := -2cdB + Y^2 - c^2 - d^2$$

が得られる．

一方，成立を確かめたい結論の式は

$$XY = ac + bd$$

と書ける．簡単のため次の等式を示すことにする

$$X^2Y^2 = (ac + bd)^2.$$

整理して，結論となる $\mathbb{R}[A, B, X, Y]$ の元が以下である

$$g := X^2Y^2 - (ac + bd)^2.$$

系 5-5. より

（ア）　$I = \langle h_1, h_2, h_3, h_4 \rangle$ とおいたときに $g \in \sqrt{I}$,

（イ）　$\widetilde{I} = \langle h_1, h_2, h_3, h_4, 1 - yg \rangle$ とおいたときに $\widetilde{I} = \langle 1 \rangle$

のどちらかを示せば，仮定から結論が**一般に従う**ことになる．

S 多項式を用いて A, B を消去する

$$2abcd \cdot S(h_1, h_2) = (ad + bc)X^2 - (ac + bd)(ab + cd) =: h_5,$$
$$2abcd \cdot S(h_3, h_4) = (ab + cd)Y^2 - (ac + bd)(ad + bc) =: h_6.$$

ここでブッフベルガーのアルゴリズムにより，I のグレブナー基底が $\{h_1, h_2, h_3, h_4, h_5, h_6\}$ であることが分かる．さらに消去定理より，$\{h_5, h_6\}$ は I の消去イデアル $I \cap \mathbb{R}[X, Y]$ のグレブナー基底である．

（ア）　$(ad + bc) \cdot g = (ad + bc)X^2Y^2 - (ac + bd)^2(ad + bc)$

$= Y^2 \cdot h_5 + (ac + bd) \cdot h_6 \in I$

$ad + bc$ は可逆元としてよいので，$g \in I$ であり，$g \in \sqrt{I}$ が示された．

（イ）　$yY^2 \cdot h_5 + y(ac + bd) \cdot h_6 + (ad + bc) \cdot (1 - yg) = ad + bc \in \widetilde{I}$

上と同様にして，$1 \in \widetilde{I}$ すなわち $\widetilde{I} = \langle 1 \rangle$ である．

以上でトレミーの定理が証明された．　□

参考文献

『グレブナ基底と代数多様体入門　上・下』　丸善出版

著者：デビッド・コックス，ドナル・オシー，ジョン・リトル

翻訳：落合 啓之，西山 亨，山本 敦子，示野 信一，室 政和

謝辞

テキストの著者・訳者の皆様にこの理論を学ばせて頂けたことへの感謝，並びにテーマの選考から論文の添削など，完成に至るまで厚くご指導を賜った森田知真先生に厚く御礼を申し上げ，結びの言葉とさせて頂く．