多項式方程式系から変数を消去するための系統的な方法。消去理論。
消去定理
拡張定理

1 消去および拡張定理

$$x^2+y+z = 1 \tag{1}$$
$$x+y^2+z = 1 \tag{2}$$
$$x+y+z^2 = 1 \tag{3}$$

$$I=\langle x^2+y+z-1, x+y^2+z-1, x+y+z^2-1\rangle \tag{4}$$

lex 順序に関するグレブナ基底

$$g_1 = x+y+x^2-1 \tag{5}$$
$$g_2 = y^2-y-z^2+z \tag{6}$$
$$g_3 = 2yz^2+z^4-z^2 \tag{7}$$
$$g_4 = z^6-4z^4+4z^3-z^2 \tag{8}$$

$$g_4=z^2(z-1)^2(z^2+2z-1) \tag{9}$$

$$z=0,1,-1\pm\sqrt{2} \tag{10}$$

g_2, g_3 に代入 $\to y$ を決めることが出来る。
g_1 に代入 $\to x$ を決めることが出来る。

$$(1,0,0),(0,1,0),(0,0,1), \tag{11}$$
$$(-1+\sqrt{2},-1+\sqrt{2},-1+\sqrt{2}) \tag{12}$$
$$(-1-\sqrt{2},-1-\sqrt{2},-1-\sqrt{2}) \tag{13}$$

(消去ステップ)
$g_4=0$ は z だけを含む方程式。すなわち連立方程式から x と y を消去した。
(拡張ステップ)
いったん z を決めてしまうと、連立方程式の解にまで拡張することが出来た。
消去理論：消去ステップと拡張ステップが一般的にできる。

定義 1.1. 与えられたイデアル $I = \langle f_1, \ldots, f_s \rangle \subset k[x_1 \ldots, x_n]$ に対して、l 次の消去イデアル I_l とは、

$$I_l = I \cap k[x_{l+1}, \ldots, x_n] \tag{14}$$

で定義される $k[x_{l+1}, \ldots, x_n]$ のイデアルである。
I_l は、連立方程式 $f_1 = \cdots = f_s = 0$ から変数 $x_1, \ldots, x_l$ を消去して得られる式全体からなるイデアルである。

定理 2 (消去定理 (Elimination Theorem)) $I \subset k[x_1, \ldots, x_n]$ をイデアルとし，G を I の lex 順序 $x_1 > x_2 > \cdots > x_n$ に関するグレブナ基底であるとする．このとき，$0 \leq l \leq n$ に対して，集合

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

は l 次の消去イデアル I_l のグレブナ基底である．

証明 l を 0 から n の間で固定する．構成の仕方から，$G_l \subset I_l$ であるので，

グレブナ基底の定義より，

$$\langle \mathrm{LT}(I_l) \rangle = \langle \mathrm{LT}(G_l) \rangle$$

を証明すれば十分である．$\langle \mathrm{LT}(I_l) \rangle$ が $\langle \mathrm{LT}(G_l) \rangle$ を含むことは明らかなので，その逆の $\langle \mathrm{LT}(I_l) \rangle \subset \langle \mathrm{LT}(G_l) \rangle$ を証明するために，$f \in I_l$ の先頭項 $\mathrm{LT}(f)$ は適当な $g \in G_l$ をとれば $\mathrm{LT}(g)$ で割り切れることを示そう．

これを示すために，f は I の元でもあることに注意しよう．したがって，G が I のグレブナ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．$f \in I_l$ であるから，これは $\mathrm{LT}(g)$ が変数 $x_{l+1}, \ldots, x_n$ だけを含むことを意味する．ここで次の重要な事実が観察される．$x_1 > \cdots > x_n$ に関する lex 順序を使っているのだから，$x_1, \ldots, x_l$ を変数に含む単項式は $k[x_{l+1}, \ldots, x_n]$ のすべての単項式よりも上位にある．だから，$\mathrm{LT}(g) \in k[x_{l+1}, \ldots, x_n]$ より $g \in k[x_{l+1}, \ldots, x_n]$ が導かれる．これは $g \in G_l$ を示しており，これで定理の証明ができた． □

例：
$I = \langle x^2 + y + z - 1, x + y^2 + z - 1, x + y + z^2 - 1 \rangle$。消去定理によって、

$$I_1 = I \cap \mathbb{C}[y, z] \tag{15}$$

$$= \langle y^2 - y - z^2 + z, 2yz^2 + z^4 - z^2, z^6 - 4z^4 + 4z^3 - z^2 \rangle, \tag{16}$$

$$I_2 = I \cap \mathbb{C}[z] \tag{17}$$

$$= \langle z^6 - 4z^4 + 4z^3 - z^2 \rangle \tag{18}$$

もとの方程式から x と y を消して得られる多項式は、g_4 の多項式倍になっているのだから、可能な消去の中からもっとも良い方法で消去を行ったということになる。
拡張ステップ
イデアル $I \subset k[x_1, \ldots, x_n]$ があるとする。これにはアフィン多様体

$$V(I) = \{(a_1, \ldots, a_n) \in k^n : f(a_1, \ldots, a_n) = 0 \text{ for all } f \in I\} \tag{19}$$

が対応している。$V(I)$ の点を記述することが問題。一度に 1 つまで解を拡張して構成する。これは消去イデアル I_l を与える。$(a_{l+1}, \ldots, a_n) \in V(I_l)$ をもとの方程式系の部分解という。$V(I)$ の完全な解に拡張するために、座標を 1 つ余分に付け加える。$(a_l, a_{l+1}, \ldots, a_n)$ が $V(I_{l-1})$ に属するような a_l を求める。具体的には、$I_{l-1} = \langle g_1, \ldots, g_r \rangle$ が $k[x_l, x_{l+1}, \ldots, x_n]$ のイデアルで与えられたとする。このとき、方程式系

$$g_1(x_l, a_{l+1}, \ldots, a_n) = \cdots = g_r(x_l, a_{l+1}, \ldots, a_n) = 0 \tag{20}$$

の解 $x_l = a_l$ を求めたい。a_l は、r 個の多項式の GCD の根になっている。
例

$$xy = 1, \tag{21}$$

$$xz = 1. \tag{22}$$

$I = \langle xy - 1, xz - 1 \rangle$。$I_1 = \langle y - z \rangle$。部分解は、$(y, z) = (a, a)$。完全解は、$(x, y, z) = (1/a, a, a)$。ただし、部分解が $(y, z) = (0, 0)$ のときは拡張できない。部分解が、完全解まで拡張できるかを知りたい。次の定理はいつこれが出来るかを述べている。

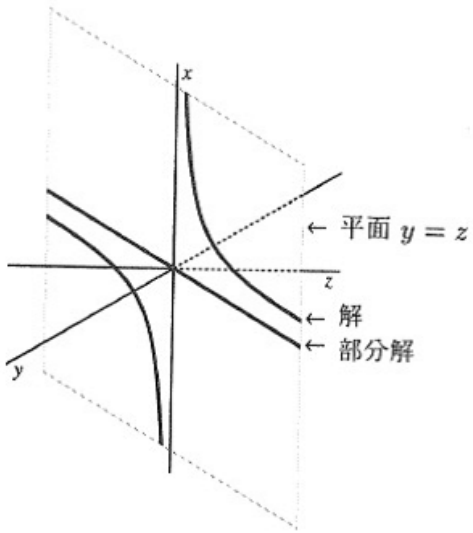

図 1.1 $y = z$ 上の双曲線

定理 3 (拡張定理 (Extension Theorem)) イデアル $I = \langle f_1, \ldots, f_s \rangle \subset \mathbb{C}[x_1, \ldots, x_n]$ を考え，I_1 を I の 1 次の消去イデアルとする．$1 \leq i \leq s$ の各添字 i に対して，f_i を次の形に書く．

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

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

証明はセクション 6。

g_i は、f_i を x_1 の多項式と考えた時の先頭係数。$(a_2, \ldots, a_n) \notin V(g_1, \ldots, g_s)$ は、先頭係数が同時にゼロになることはないと言っている。なぜこれらの条件が必要なのか。連立方程式

$$xy = 1, \tag{23}$$

$$xz = 1 \tag{24}$$

は部分解 $(y, z) = (a, a)$ を持つ。拡張できない唯一の解は、$(0, 0)$ であり、先頭係数 y, z がゼロになる部分解。拡張定理は、先頭係数が同時にゼロになるときに限って、拡張ステッ

プがうまくいかない可能性があることを教えている。

先頭項の零点によって定義される多様体 $V(g_1,\ldots,g_s)$ は、I の基底 $\{f_1,\ldots,f_s\}$ の取り方によって変わってくる。$V(g_1,\ldots,g_s)$ がもっとも小さくなるような $(f_1,\ldots,f_s)$ の取り方は、第８章で学ぶ。

変数を複数消去する場合

$$x^2+y^2+z^2 = 1, \tag{25}$$

$$xyz = 1. \tag{26}$$

$I=\langle x^2+y^2+z^2-1, xyz-1\rangle$ に対するグレブナ基底を、lex 順序に関して計算すると

$$g_1 = y^4z^2+y^2z^4-y^2z^2+1, \tag{27}$$

$$g_2 = x+y^3z+yz^3-yz \tag{28}$$

となる。消去定理を使うと、

$$I_1 = I\cap\mathbb{C}[y,z]=\langle g_1\rangle, \tag{29}$$

$$I_2 = I\cap\mathbb{C}[z]=\{0\} \tag{30}$$

を得る。$I_2=\{0\}$ であるから、$V(I_2)=\mathbb{C}$ であり、したがってすべての $c\in\mathbb{C}$ は部分解である。

どの部分解 $c\in\mathbb{C}=V(I_2)$ が $(a,b,c)\in V(I)$ にまで拡張できるか。I_2 から $I_1=\langle g_1\rangle$ に拡張するために拡張定理を適用する。g_1 中の y^4 の係数は z^2 である。したがって、$c\in\mathbb{C}=V(I_2)$ は、$c\neq 0$ である限り (b,c) まで拡張できる。$(y,z)=(b,c)$ を (25,26) へ代入すると、x の二つの方程式が得られる。共通根 a があることは自明でない。x の先頭係数はそれぞれ 1 と yz である。$1\neq 0$ だから拡張定理は常に a が存在することを保証している。したがって、すべての部分解 $c\neq 0$ は $V(I)$ まで拡張されることが示された。

系 4 イデアル $I=\langle f_1,\ldots,f_s\rangle\subset\mathbb{C}[x_1,\ldots,x_n]$ をとり，ある i に対して f_i が次の形をしているとする．

$$f_i = cx_1^N+(x_1\text{ の次数が }<N\text{ である項}).$$

ここで，$c\in\mathbb{C}$ はゼロではなく $N>0$ である．もし，I_1 が I の 1 次の消去イデアルで $(a_2,\ldots,a_n)\in\mathbf{V}(I_1)$ とすると，$a_1\in\mathbb{C}$ が存在して $(a_1,a_2,\ldots,a_n)\in\mathbf{V}(I)$ となる．

証明 これは拡張定理から直ちに従う．すなわち，$g_i = c \neq 0$ であることより $\mathbf{V}(g_1, \ldots, g_s) = \emptyset$ が導かれるので，すべての部分解に対して $(a_2, \ldots, a_n) \notin \mathbf{V}(g_1, \ldots, g_s)$ となる． □

よい解を持たない連立方程式の例。

$$xy = 4, \tag{31}$$

$$y^2 = x^3 - 1 \tag{32}$$

lex 順序を使うと、グレブナ基底は

$$g_1 = 16x - y^2 - y^4 \tag{33}$$

$$g_2 = y^5 + y^3 - 64 \tag{34}$$

$y^5 + y^3 - 64 = 0$ はいかなる有理根も持たない。ニュートン—ラフソン法を用いて数値的に y 求め、それを $g_1 = 0$ に代入して、 x を求める。