

2章 終結式

定義 2.1

$f(X) = a_0X^m + a_1X^{m-1} + \cdots + a_m$ ($a_0 \neq 0$) $g(X) = b_0X^n + b_1X^{n-1} + \cdots + b_n$ ($b_0 \neq 0$) $\in K[X]$ に対して

$$\begin{pmatrix} a_0 & \cdots & 0 & b_0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & a_0 & 0 & 0 & b_0 \\ a_m & 0 & 0 & b_n & 0 & 0 \\ 0 & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & a_m & 0 & 0 & b_n \end{pmatrix}$$

を $f \times g$ のシルベスター行列と呼び、その行列式を f と g の終結式 (resultant) とよび、 $R(f, g)$ で表す

証明 $f(X)$ と $g(X)$ が共通因子を持つ \Leftrightarrow

$$\exists h(X), t(X) \in K[X]$$

$$\deg h < \deg g$$

$$\deg t < \deg f$$

$$f(X)h(X) = g(X)t(X)$$

$$\Leftrightarrow$$

$$\exists h(X) = C_0X^{n-1} + \cdots + C_{n-1} \neq 0$$

$$t(X) = d_0X^{m-1} + \cdots + d_{m-1} \neq 0$$

$$f(X)h(X) = g(X)t(X)$$

$$\Leftrightarrow$$

$$\exists (C_0, \dots, C_{n-1}, d_0, \dots, d_{m-1}) \neq \vec{0} \text{ 共通因子を } s(X) \text{ とすると}$$

$a_0C_0 = b_0d_0$	X^{m+n-1} の係数
$a_1C_0 + a_0C_1 = b_1d_0$	X^{m+n-2} の係数
$a_2C_0 + a_1C_1 + a_0C_2 = b_2d_0 + b_1d_1 + b_0d_2$	X^{m+n-3} の係数
\vdots	\vdots
$a_mC_{n-1} + a_{m-1}C_{n-1} = b_nd_{m-2} + b_{n-1}d_{m-1}$	X の係数
$a_mC_{n-1} = b_nd_{m-1}$	X^0 の係数

定理 2.2

$$R(f, g) \in \langle f(X), g(X) \rangle$$

実は $R(f, g) = h(X)f(X) + t(X)g(X)$ $h(X), t(X)$ の係数は $a_0, \dots, a_m, b_0, \dots, b_n$ の整式 (整数係数多項式)

証明 $R(f, g) = 0$ なら $h(X) = t(X) = 0$ とおけばよい

$R(f, g) \neq 0$ とする。

$$\begin{pmatrix} a_0 & \cdots & 0 & b_0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & a_0 & 0 & 0 & b_0 \\ a_m & 0 & 0 & b_n & 0 & 0 \\ 0 & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & a_m & 0 & 0 & b_n \end{pmatrix} \begin{pmatrix} C_0 \\ \vdots \\ C_{n-1} \\ d_0 \\ \vdots \\ d_{n-1} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

の解 $(C_0, \dots, C_{n-1}, d_0, \dots, d_{m-1})$ に対し、

$h'(X) = C_0 X^{n-1} + \dots + C_{n-1}, t'(X) = d_0 X^{m-1} + \dots + d_{m-1}$ とおくと

$h'(X)f(X) + t'(X)g(X) = 1$ がなりたつことにほかならない

$R(f, g) \neq 0$ なので、解はただひとつ存在して、それは Clamer の公式によって

$$C_i = \frac{1}{R(f, g)}$$

よって、各 C_j, d_j に $R(f, g)$ をかけたものは、 $a_0, \dots, a_m, b_0, \dots, b_n$ の整式になる

$$\text{よって } \begin{matrix} h(X) = h'(X)R(f, g) \\ t(X) = t'(X)R(f, g) \end{matrix} \text{ とおけばよい}$$

定理 2.3 (拡張定理)

- K : 代数的閉体
- $I \subset K[X_1, \dots, X_n]$: イデアル

$$\mathbf{V}_k(I \cap K[X_1, \dots, X_{n-1}]) \ni (C_1, \dots, C_{n-1}) t_0(C_1, \dots, C_{n-1}) \neq 0 \Rightarrow \exists C_n \in K (C_1, \dots, C_n) \in \mathbf{V}_k(I)$$

例

$$K = \mathbf{C} \quad X = X_1, Y = X_2, Z = X_3$$

$$I = \langle ZX - 1, X - Y \rangle \subset \mathbf{C}[X, Y, Z]$$

$$I \cap \mathbf{C}[Y, Z] = \langle X - Y \rangle$$

$$(C_1, C_2) \in \mathbf{V}_{\mathbf{C}}(I \cup \mathbf{C}[Y, Z]) = \mathbf{V}_{\mathbf{C}}(\langle X - Y \rangle) = \{(c, c) \mid c \in \mathbf{C}\}$$

証明 $I(C_1, \dots, C_{n-1}) = \{f(C_1, \dots, C_{n-1}, X_n) \in K[X_n] \mid f \in I\}$ とおく

明らかにこれは $K[X_n]$ のイデアル (I がイデアル \Leftrightarrow

1. $I \neq \emptyset$
2. $I \ni p, q \Rightarrow p + q \in I$
3. $I \ni p \Rightarrow \forall h \in K[X_1, \dots, X_n] \quad hp \in I$

)

ケース 1

$I(C_1, \dots, C_{n-1}) = \langle 0 \rangle$ C_n は任意にとれる

ケース 2

$I(C_1, \dots, C_{n-1}) = \langle f(C_1, \dots, C_{n-1}, X_n) \rangle$ $\deg f(C_1, \dots, C_{n-1}, X_n) \geq 1$
 K は代数的閉体なので $\exists C_n \in K \quad f(C_1, \dots, C_{n-1}, C_n) = 0$

ケース 3

$$I(C_1, \dots, C_{n-1}) = \langle f(C_1, \dots, C_{n-1}, X_n) \rangle = \langle 1 \rangle$$

$$f(C_1, \dots, C_{n-1}, X_n) = a \text{ は } 0 \text{ でない定数}$$

$$f = S_0(X_1, \dots, X_{n-1})X_n^M + S_1(X_1, \dots, X_{n-1})X_n^{M-1} + \dots + S_M(X_1, \dots, X_{n-1})$$

とすると

$$S_0(C_1, \dots, C_{n-1}) = 0, \dots, S_{M-1}(C_1, \dots, C_{n-1}) = 0, S_M(C_1, \dots, C_{n-1}) = a \neq 0$$

$$g = t_0(X_1, \dots, X_{n-1})X_n^N + t_1(X_1, \dots, X_{n-1})X_n^{N-1} + \dots + t_N(X_1, \dots, X_{n-1})$$

とする

$$R(g, f, X_n) \in I \cap K[X_1, \dots, X_{n-1}] \quad (\because \text{定理 2.2}) \quad f, g \in I$$

$$\det \begin{pmatrix} t_0 & & s_0 & & \\ & \ddots & & \ddots & \\ & & t_0 & & s_0 \\ t_N & & & S_M & \\ & & & & \vdots \\ & & t_N & & S_m \end{pmatrix} = h(X_1, \dots, X_n)$$

矛盾、よってケース 3 はおこらない

3章 Hilbert の零点定理

定理 3.1 (Hilbert の零点定理 弱系)

K : 代数的閉体

$I \subset K[X_1, \dots, X_n]$: イデアル

$V_K(I) = \emptyset \Rightarrow I \ni 1$ (どんな K に対しても常になりつつ)

Claim 1

$$f'(Y_1, \dots, Y_n, Y_{n+1}) =$$

$$f(Y_1 + a_1 Y_{n+1}, \dots, Y_n + a_n Y_{n+1}, Y_{n+1}) = h(a_1, \dots, a_n) Y_{n+1}^N + t$$

$h(Y_1, \dots, Y_n)$ は 0 でない n 変数多項式 t は Y_{n+1} に関して次数 N 未満の式と表される

Claim 2

$h(1, \dots, a_n) \neq 0$ なる $a_1, \dots, a_n \in K$ が存在する

Claim 3

$I' = \{f(Y_1 + a_1 Y_{n+1}, \dots, Y_n + a_n Y_{n+1}, Y_{n+1}) \mid f \in I\} \subset K[Y_1, \dots, Y_{n+1}]$ とおくと I' はイデアルである

定理 3.2

K を無限体とするとき、

$$f(X_1, \dots, X_n) \in K[X_1, \dots, X_n] \text{ が } \forall c_1, \dots, c_n \in K \ f(c_1, \dots, c_n) = 0 \Rightarrow f(X) = 0$$

注意 1

K が有限体なら成り立たない

注意 2

K が代数的閉体なら K は無限体

定理 3.3 Hilbert の零点定理 (強形)

K : 代数的閉体 とするとき

$$f_1(X_1, \dots, X_n), \dots, f_s(X_1, \dots, X_n), g(X_1, \dots, X_n) \in K[X_1, \dots, X_n] \text{ に対して} \\ g \in \mathbf{I}(\mathbf{V}_K(\{f_1, \dots, f_l\})) \Rightarrow \exists m \in \mathbf{N} \ g^m \in \langle f_1, \dots, f_l \rangle$$

この意味

$$\mathbf{V}_K \text{ は連立方程式 } \begin{cases} f_1 = 0 \\ \vdots \\ f_l = 0 \end{cases} \text{ の } K \text{ における解全体の集合}$$

g が連立方程式のすべての解に対して 0 になるような g を m 乗した g^m がイデアル $\langle f_1, \dots, f_l \rangle$ に属する

注意 実は弱形は強形の特殊な場合である。

強形を論理式のみで書くと

$$\forall \bar{c} \in K^n (f_1(\bar{c}) = 0 \wedge \dots \wedge f_s(\bar{c}) = 0 \rightarrow f(\bar{c}) = 0) \rightarrow \exists m \in \mathbf{N} \ f^m \in \langle f_1, \dots, f_s \rangle$$

\Leftrightarrow

$$\neg \forall \bar{c} \in K^n (\neg (f_1(\bar{c}) = 0 \wedge \dots \wedge f_s(\bar{c}) = 0)) \vee \exists m \in \mathbf{N} \ f^m \in \langle f_1, \dots, f_s \rangle$$

$f(\bar{X}) = 1$ に対してももちろんなりたつ、

$$\forall f_1, \dots, f_s \in K[\bar{X}]$$

$$\neg \forall \bar{c} \in K^n (\neg (f_1(\bar{c}) = 0 \wedge \dots \wedge f_s(\bar{c}) = 0)) \vee \exists m \in \mathbf{N} \ 1^m \in \langle f_1, \dots, f_s \rangle$$

4章 連立代数方程式の解の個数

定理 4.1

K : 代数的閉体

$I \subset K[X] = K[X_1, \dots, X_n]$ に対して

$$\mathbf{V}_K(I) \text{ が有限集合 } \Leftrightarrow \forall i = 1, \dots, n \ \exists h_i(X_i) \in K[X_i] \ h_i(X_i) \in I$$

定義 4.1

$I \subset K[\bar{X}]$: イデアル

$f, g \in K[\bar{X}]$ に対して

$f \sim g \stackrel{\text{def}}{\iff} f - g \in I$ で \sim を定義すると \sim は同値関係になる。
 \sim の同値類上に

- $[f]_{\sim} + [g]_{\sim} = [f + g]_{\sim}$
- $[f]_{\sim} \cdot [g]_{\sim} = [fg]_{\sim}$

で $+$ と \cdot を自然に定義すると同値類は可換環になる。これを $K[\bar{X}]$ の I による剰余環とよび、 $K[\bar{X}]$ で表す。

($+$ と \cdot が well-defined になることは示さないといけない。

すなわち、 $f \sim f', g \sim g'$ ならば、 $f + g \sim f' + g', f \cdot g \sim f' \cdot g'$ を示す必要がある。)

定義 4.2

$K[\bar{X}]/I$ は K 上の線形空間で I もその部分空間とみなせる。

$K[\bar{X}]/I$ は線形空間としてのその商空間ともみなせる。

その次元を $\dim K[\bar{X}]/I$ で表す

定理 4.2

K : 代数的閉体

$I \subset K[\bar{X}]$: イデアルに対して

$\mathbf{V}_K(I)$ が有限集合 $\Leftrightarrow \dim K[\bar{X}]/I$ が有限

Claim

$\forall f \in K[\bar{X}] \exists f' \in K[\bar{X}]$ f' に含まれるどの多項式の X_i の次数 $\leq m_i$

定義 4.3 根基イデアル

イデアル $I \subset K[\bar{X}]$ が根基であるとは

$\exists m \in \mathbf{N} f^m \in I \Rightarrow f \in I$

一般のイデアル I に対して I の根基イデアル \sqrt{I} とは

$\sqrt{I} \stackrel{\text{def}}{=} \{f; \exists m \in \mathbf{N} f^m \in I\}$ で定義される

補題 4.1

- (1) \sqrt{I} はイデアル
- (2) I が根基 $\Leftrightarrow I = \sqrt{I}$

定理 4.3

K : 代数的閉体

$I \subset K[\bar{X}]$: イデアル

$$\dim K[\bar{X}]/I < \infty$$

に対して以下がなりたつ。

- (1) $\dim K[\bar{X}]/I \geq |\mathbf{V}_K(I)|$
- (2) $\dim K[\bar{X}]/I = |\mathbf{V}_K(I)| \Leftrightarrow I = \sqrt{I}$

補題 4.2 相異なる $\bar{c}_1, \dots, \bar{c}_l \in K^n$ に対して

$$h_i(\bar{c}_j) = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases} \text{ なる } h_1(\bar{X}), \dots, h_l(\bar{X}) \in K[\bar{X}] \text{ が存在する}$$

定義

$$I \subset K[\bar{X}]$$

$\dim K[\bar{X}]/I < \infty$ なるイデアル

前に各 X_i に対して 0 でない 1 変数多項式 $h_i(X_i) \in I$ が存在することを示した。

このような多項式で次数が最小のものを I の X_i に関する最小多項式と呼ぶ。

最小多項式は定数倍を除いて一意に定まる。

定理 4.4

$I \in K[\bar{X}]$ を $\dim K[\bar{X}]/I < \infty$ なるイデアルとし、

各 X_i の最小多項式を $h_1(X_1), \dots, h_l(X_l)$ とおく

このとき

$$\sqrt{I} = I + \langle h_1, \dots, h_l \rangle$$

5章 項順序

定義 5.1 順序

集合 S 上の 2 項関係 $>$ は

$$1. a > b, b > c \Rightarrow a > c$$

$$2. a \not> a$$

をみたすとき順序と呼ばれる。

$a \geq b$ を $a > b$ または $a = b$ とすると、 $>$ が順序であることは

$$1'. a \geq b, b \geq c \Rightarrow a \geq c$$

$$2'. a \geq b, b \geq a \Rightarrow a = b$$

が成り立つことにほかならない

\geq が $1', 2'$ を満たすとき、 $a > b$ を $a \geq b$ かつ $a \neq b$ とすると $>$ は $1, 2$ をみたすさらに $>$ が

$$3. \forall a, b \in S (a \neq b) \\ a > b \text{ または } b > a$$

が成り立つとき全順序と呼ばれる。

変数 X_1, \dots, X_n の項とは $X_1^{a_1}, \dots, X_n^{a_n}$ a_i は 0 以上の整数のこと
 $X_1^{a_1} X_2^{a_2} \dots X_n^{a_n}$ と $X_1^{b_1} X_2^{b_2} \dots X_n^{b_n}$ の間に $X_1^{a_1} X_2^{a_2} \dots X_n^{a_n} \geq X_1^{b_1} X_2^{b_2} \dots X_n^{b_n}$
 $\stackrel{\text{def}}{\Leftrightarrow}$

$$a_1 \geq b_1 \wedge a_2 \geq b_2 \wedge \dots \wedge a_n \geq b_n$$

($\Leftrightarrow X_1^{b_1} \dots X_n^{b_n}$ が $X_1^{a_1} \dots X_n^{a_n}$ を割り切る)

で \geq を定めると \geq は順序。 $n \geq 2$ の場合 \geq は全順序にはならない

定義 5.2

集合 S 上の順序 $>$ が

- (1) S の空でない任意の部分集合 A が極小値をもつ
- (2) S の空でない任意の部分集合 A が最小値をもつ
- (3) S の空でない部分集合 A の極小値全体の集合は空でない有限集合になる。

を満たすとき

- (1) well-founded
- (2) well-ordered (整列順序)
- (3) semi-well-ordered

と呼ぶ

定義 5.3

変数 X_1, \dots, X_n の項全体の集合を S とする。

S 上の全順序 $>$ が以下の性質を満たすとき $>$ を項順序と呼ぶ。

1. $X_1^{a_1} \dots X_n^{a_n} > X_1^{b_1} \dots X_n^{b_n} \Rightarrow X_1^{a_1+c_1} \dots X_n^{a_n+c_n} > X_1^{b_1+c_1} \dots X_n^{b_n+c_n}$
 $\forall a_1, \dots, a_n, b_1, \dots, b_n, c_1, \dots, c_n \in \mathbf{N} \cup \{0\}$
2. $X_1^{a_1} \dots X_n^{a_n} \geq 1$

補題 5.1

$>$ を無限集合 S 上の semi-well-order とするとき

S の任意の無限部分集合 A に対し

A の要素からなる単調増加列 $\alpha_1 < \alpha_2 < \dots$ が存在する

定理 5.1

n を固定する

変数 X_1, \dots, X_n の後の間に $X_1^{a_1}, \dots, X_n^{a_n} \leq X_1^{b_1}, \dots, X_n^{b_n}$
 $\stackrel{\text{def}}{\Leftrightarrow}$

$$a_1 \leq b_1, \wedge \dots \wedge a_n \leq b_n$$

で \leq を定義すると \leq は semi-well-order になる

定理 5.2

項順序は well-order になる。

定理 5.3

勝手なイデアル $I \subset K[X_1, \dots, X_n]$ に対して、 $I = \langle f_1, \dots, f_l \rangle$ となる $f_1, \dots, f_l \in K[X_1, \dots, X_n]$ が存在する。

定義 5.5 グレブナー基底

項順序を 1 つ固定する。

イデアル $I \subset K[X_1, \dots, X_n]$ に対して

I のグレブナー基底 $G = \{g, \dots, g_l\}$ とは

$I = \langle g_1, \dots, g_l \rangle$ でかつ任意の $f \in I$ に対して

$\text{LT}(f)$ が $\text{LT}(g_1), \dots, \text{LT}(g_l)$ のいずれかで割り切れるような G