第3章　消去理論
§6　終結式と拡張定理

担当　乳井昌道

§5の終結式を利用して、拡張定理(3章§1定理3)を証明する。

拡張定理の証明のためにやること

(1)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。

(2)どのようにして終結式が部分解の拡張に使われるのか示す。

(3)イデアルが2つの多項式から生成されるに場合において拡張定理を証明する。

(4)任意のイデアルに対する拡張定理を証明する。

§5の終結式を利用して、拡張定理(3章§1定理3)を証明する。

拡張定理の証明のためにやること

(1)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。

(2)どのようにして終結式が部分解の拡張に使われるのか示す。

(3)イデアルが2つの多項式から生成されるに場合において拡張定理を証明する。

(4)任意のイデアルに対する拡張定理を証明する。

多変数の多項式の終結式

$$f = a_0 x_1^l + \cdots + a_l , a_0 \neq 0$$

$$g = b_0 x_1^m + \cdots + b_m , b_0 \neq 0$$

$$\left(a_i , b_i \in k\left[x_2 , \ldots , x_n \right] \right)$$

$$Res\left(f , g , x_1 \right) = \det \begin{pmatrix} a_0 & & & & b_0 & & & \\ a_1 & a_0 & & & b_1 & b_0 & & \\ & a_1 & \ddots & & & b_1 & \ddots & \\ \vdots & & \ddots & a_0 & \vdots & & \ddots & b_0 \\ & \vdots & & a_1 & & \vdots & & b_1 \\ a_l & & & & b_l & & & \\ & a_l & & \vdots & & b_l & & \vdots \\ & & \ddots & & & & \ddots & \\ & & & a_l & & & & b_l \end{pmatrix}$$

命題1

$f,g \in k[x_1,\dots,x_n]$ の x_1 に対する次数が正であると仮定する.
このとき次が成立する.

(ⅰ) $Res(f,g,x_1)$ は, x_1 を消去した1次の消去イデアル
$\langle f,g\rangle \cap k[x_2,\dots,x_n]$ に含まれる.

(ⅱ) $Res(f,g,x_1)=0$ であることと, f と g が $k[x_1,\dots,x_n]$ において
x_1 に関する次数が正の共通因子を持つことは同値である.

証明(命題1(ⅰ))

f , g を x_1 の多項式の形になるように整理して書くと, 係数 a_i , b_i は $k\left[x_2,\ldots,x_n\right]$ に含まれる. 終結式は a_i, b_i の整数係数多項式であるから(§5の命題8), $Res\left(f,g,x_1\right)\in k\left[x_2,\ldots,x_n\right]$ となる.

また, $Af+Bg=Res\left(f,g,x_1\right)$ となる.

A と B は x_1 の多項式で, 係数も a_i, b_i を変数とする整数係数多項式である(§5の命題9).

$k\left[x_2,\ldots,x_n\right]\left[x_1\right]=k\left[x_1,\ldots,x_n\right]$ であり,

上記の方程式から $Res\left(f,g,x_1\right)\in\left\langle f,g\right\rangle$ が導かれる.

証明(命題1(ⅱ))

f と g は$k\left[x_2,\dots,x_n\right]$ に係数を持つ x_1 の多項式で, 係数が属する体は $k\left(x_2,\dots,x_n\right)$ である.
§5の命題8を$f,g\in k\left(x_2,\dots,x_n\right)\left[x_1\right]$ に適用することによって,
$Res\left(f,g,x_1\right)=0$ であることと, f と g は x_1 に関して正の次数を持つ $k\left(x_2,\dots,x_n\right)\left[x_1\right]$ の多項式を共通因子として持つことが同値であることがわかる.
§5の系4を適用すると, これは $k\left[x_1,\dots,x_n\right]$ において x_1 の次数が正である多項式を共通因子として持つことと同値であることがわかる.

系2

$f,g\in C[x]$と仮定する.
このとき $Res(f,g,x)=0$ であることと, f と g が C において
共通根を持つことは同値である.

※複素数体上では, $C[x]$の2つの多項式が共通因子を持つ
ことと, それらが共通根を持つことは同値である.

§5の終結式を利用して、拡張定理(3章§1定理3)を証明する。

拡張定理の証明のためにやること

(1)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。

(2)どのようにして終結式が部分解の拡張に使われるのか示す。

(3)イデアルが2つの多項式から生成されるに場合において拡張定理を証明する。

(4)任意のイデアルに対する拡張定理を証明する。

命題3

$f, g \in C[x_1, \ldots, x_n]$に対して $a_0, b_0 \in C[x_2, \ldots, x_n]$ を

$$f = a_0 x_1^l + \cdots + a_l, a_0 \neq 0$$

$$g = b_0 x_1^m + \cdots + b_m, b_0 \neq 0$$

ととる. もし $Res(f, g, x_1) \in C[x_2, \ldots, x_n]$ が $(c_2, \ldots, c_n) \in C^{n-1}$ 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 $(c_2, \ldots, c_n) \in C^{n-1}$ で消える.

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

命題3(証明)

記号(定理4,5の証明でも使う):

$$c=\left(c_2,\ldots,c_n\right)$$

$$f\left(x_1,c\right)=f\left(x_1,c_2,\ldots,c_n\right)$$

$a_0\left(c\right)$ と $b_0\left(c\right)$ がともにゼロでないとき $f\left(x_1,c\right)$ と $g\left(x_1,c\right)$ が共通根を持つことを示せれば十分である.

$$f\left(x_1,c\right)=a_0\left(c\right)x_1^l+\cdots+a_l\left(c\right),a_0\left(c\right)\neq 0$$

$$g\left(x_1,c\right)=b_0\left(c\right)x_1^m+\cdots+b_m\left(c\right),b_0\left(c\right)\neq 0$$

と書く.

命題3(証明)

仮定より, $h = Res\left(f, g, x_1\right)$ は c で消える.
h を与える行列式の点 c における値を求めると

$$0 = h\left(c\right) = \det\begin{pmatrix} a_0\left(c\right) & & & b_0\left(c\right) & & \\ \vdots & \ddots & & \vdots & \ddots & \\ \vdots & & a_0\left(c\right) & \vdots & & b_0\left(c\right) \\ a_l\left(c\right) & & \vdots & b_m\left(c\right) & & \vdots \\ & \ddots & \vdots & & \ddots & \vdots \\ & & a_l\left(c\right) & & & b_m\left(c\right) \end{pmatrix}$$

となる. これより$0 = h\left(c\right) = Res\left(f\left(x_1, c\right), g\left(x_1, c\right), x_1\right)$が従う.
系2から $f\left(x_1, c\right)$ と $g\left(x_1, c\right)$ は共通根を持つ.

§5の終結式を利用して、拡張定理(3章§1定理3)を証明する。

拡張定理の証明のためにやること

(1)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。

(2)どのようにして終結式が部分解の拡張に使われるのか示す。

(3)イデアルが2つの多項式から生成されるに場合において拡張定理を証明する。

(4)任意のイデアルに対する拡張定理を証明する。

定理4(2つの多項式に対する拡張定理)

$I=\langle f,g\rangle\subset C[x_1,\ldots,x_n]$ とし, I_1 を I の1次の消去イデアルとしよう. また, $a_0,b_0\in C[x_2,\ldots,x_n]$ を

$$f=a_0x_1^l+\cdots+a_l,\ a_0\neq 0$$

$$g=b_0x_1^m+\cdots+b_m,\ b_0\neq 0$$

で出てきたものとする.

部分解 $(c_2,\ldots,c_n)\in V(I_1)$ があるとする.

もし, $(c_2,\ldots,c_n)\notin V(a_0,b_0)$ ならば $c_1\in C$ が存在して $(c_1,\ldots,c_n)\in V(I)$ となる.

定理4(証明)

命題1より, $Res\left(f,g,x_1\right)\in I_1$ であり, 終結式は部分解 c において消える. a_0 も b_0 も c において消えないならば, 命題3(ii)より, 拡張した解となる c_1 が存在する.

c に関する仮定で, $a_0\left(c\right)$ あるいは $b_0\left(c\right)$ のいずれかが消えることが許容される. $a_0\left(c\right)\neq 0$ ではあるが $b_0\left(c\right)=0$ であると仮定する. このとき, $g\left(x_1,c\right)$ は変数 x_1 に関する次数が m より真に小さく, $\left(l+m\right)+\left(l+m\right)$ 行列はサイズが大きすぎて, 終結式とならない.

定理4(証明)

$V(f,g)$ はイデアル $\langle f,g\rangle$に依存しているので, $a_0(c)\neq 0$ かつ $b_0(c)=0$ であるときには別の基底をとることができる.
任意の正の整数 N に対して$\langle f,g\rangle=\langle f,g+x_1^N f\rangle$ が成り立つ.
N を大きくとれば, $x_1^N f$ の x_1 に関する次数は g のそれより大きくできる. このとき$g+x_1^N f$ の x_1 に関する最高次係数は a_0 であり, それは c においてゼロではない.
先の議論を f と $g+x_1^N f$ に対して適用することができ, $c_1\in C$ が存在して$(c_1,c)\in V(f,g+x_1^N f)$ となり,$(c_1,c)\in V(f,g)$となる.