代数幾何ゼミ

石井大海

早稲田大学基幹理工学部
数学科四年

2013 年 09 月 02 日

終結式

終結式は今までと装いは異なるが，消去理論で重要な役割を果す．

- 問題：$k[x]$ の二つの多項式が共通因子を持つか判定したい．
  1. 因数分解……計算量が大きい．
  2. 互除法…… k での割り算が必要になる．消去理論では余り嬉しくない．

$\rightsquigarrow$ k の割り算を使わずに共通因子を持つか知りたい！

Lemma 6

$f, g \in k[x], \deg(f) = \ell > 0, \deg(g) = m > 0$
f, g が共通因子を持つ
$\Leftrightarrow$ 次を満たす $A, B \in k[x]$ が存在する：

(i) $A \neq 0, B \neq 0$

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

(iii) $Af + Bg = 0$

Proof.

($\Rightarrow$) $f = f_1 h, g = g_1 h, h \in k[x] \setminus k$ とする．この時 $\deg f_1 \leq \ell - 1, \deg g_1 \leq m - 1$ であり，

$$g_1 f - f_1 g = g_1 f_1 h - f_1 g_1 h = 0$$

よって $A = g_1, B = -f_1$ に取ればよい．

($\Leftarrow$) 題意をみたす A, B が与えられたとする．この時 $Bg = -Af$ である．もし f, g が共通因子を持たないなら，$\tilde{A}f + \tilde{B}g = 1$ を満たす $\tilde{A}, \tilde{B} \in k[x]$ が取れる．この両辺に B を掛ければ，

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

である．$B \neq 0$ であるので，$\deg B \geq \deg f \geq \ell$．しかし $\deg B < \ell$ より矛盾．

∎

終結式 I

- 補題 6 を使えば良いかもしれない．しかし，こんな A, B を見付ける方法はあるか？

$\rightsquigarrow$ 線型代数を使う！

線型方程式系を得たいので,

$$f = a_0 x^{\ell} + \cdots + a_{\ell} \qquad a_0 \neq 0$$
$$g = b_0 x^{m} + \cdots + a_{m} \qquad b_0 \neq 0$$
$$A = c_0 x^{m-1} + \cdots + c_{m-1}$$
$$B = d_0 x^{\ell-1} + \cdots + d_{\ell-1}$$

とおいて，$Af + Bg = 0$ に代入する．各項の係数を比較して次の等式を得る：

終結式 II

$$
\begin{array}{lllll}
a_0c_0 & & +b_0d_0 & & = 0 \\
a_1c_0 & +a_0c_1 & +b_1d_0 & +b_0d_1 & = 0 \\
 & & & & \vdots \\
 & a_\ell c_{m-1} & & +b_m d_{\ell-1} & = 0
\end{array}
\tag{5.1}
$$

$c_i, d_j \in k$ を $(i+j)$-個の未知数と見做して非自明解を持つか見る.
上の係数行列は $(i+j)\times(i+j)$-行列なので行列式を見ればよい！

終結式 III

Def. 7

$$\begin{cases} f = a_0 x^\ell + \cdots + a_\ell & (a_0 \neq 0, a_i \in k) \\ g = b_0 x^m + \cdots + a_m & (b_0 \neq 0, b_j \in k) \end{cases}$$

に対し，x についての f, g の Sylvester 行列 $\mathrm{Syl}(f, g, x)$ とは，

$$\mathrm{Syl}(f, g, x) = \underbrace{\begin{pmatrix} a_0 & & \\ a_1 & \ddots & \\ \vdots & \ddots & a_0 \\ a_\ell & & a_1 \\ & \ddots & \vdots \\ & & a_\ell \end{pmatrix}}_{m\text{-列}} \underbrace{\begin{pmatrix} b_0 & & \\ b_1 & \ddots & \\ \vdots & \ddots & b_0 \\ b_m & & b_1 \\ & \ddots & \vdots \\ & & b_m \end{pmatrix}}_{\ell\text{-列}}$$

f, g の x に関する終結式は $\mathrm{Res}(f, g, x) = \det(\mathrm{Syl}(f, g, x))$

終結式の性質

Sylvester 行列の定義から，次が明らかに成立：

Prop. 8

$f, g \in k[x], \deg f > 0, \deg g > 0$

- $\mathrm{Res}(f, g, x) \in k$ は f, g の係数に関する整数多項式
- f と g が $k[x]$ で共通因子を持つ $\iff \mathrm{Res}(f, g, x) = 0$

Example.

$f = 2x^2 + 3x + 1, g = 7x^2 + x + 3$ は $\mathbb{Q}[x]$ で共通因子を持つか？

$$\mathrm{Res}(f, g, x) = \begin{vmatrix} 2 & 0 & 7 & 0 \\ 3 & 2 & 1 & 7 \\ 1 & 3 & 3 & 1 \\ 0 & 1 & 0 & 3 \end{vmatrix} = 153 \neq 0$$ より持たない！

消去理論と終結式 I

Example.

$f = xy - 1, g = x^2 + y^2 - 4$ を $(k[y])[x]$ の元と見て終結式を求めてみる：

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

x の現れない式が得られる.

- 一般の $f, g \in k[x]$ についても同様の事が出来る.
- 命題 8 より，$\mathrm{Res}(f, g, x)$ は y についての多項式になる.
- こうして得られる x の消去された式と，消去理論の関係は？

消去理論と終結式 II

Prop. 9

x に関して正次数の $f, g \in k[x, y]$ に対し，

$$Af + Bg = \mathrm{Res}(f, g, x)$$

となるような $A, B \in k[x, y]$ が存在する．更に，A, B の係数は f, g の係数の整多項式となる．

証明．Res を定義した際のと似た議論をする．但し，今回は $\tilde{A}f + \tilde{B}g = 1$ となるような $\tilde{A}, \tilde{B}$ を探すことにする．

消去理論と終結式 III

$\mathrm{Res}(f, g, x) = 0$ ならば $A = B = 0$ とすればよいので,
$\mathrm{Res}(f, g, x) \neq 0$ の時を考える．係数を文字で置いて展開し，係数を比較すると,

$$
\begin{aligned}
a_0 c_0 + b_0 d_0 &= 0 \\
a_1 c_0 + a_0 c_1 + b_1 d_0 + b_0 d_1 &= 0 \\
&\vdots \\
a_\ell c_{m-1} + b_m d_{\ell-1} &= 1
\end{aligned}
$$

となる．係数行列はかわらず，最後の $= 1$ のみが今までのと違う．そこで，Cramer の公式を用いれば,

消去理論と終結式 IV

$$c_i = \frac{1}{\mathrm{Res}(f,g,x)} \begin{vmatrix} a_0 & & 0 & & & b_0 & & \\ \vdots & \ddots & \vdots & \ddots & a_0 & \vdots & \ddots & b_0 \\ a_\ell & & 0 & & \vdots & b_m & & \vdots \\ & \ddots & 1 & \ddots & a_\ell & & \ddots & b_m \end{vmatrix}$$

となる（d_j も同様）．$\tilde{A} = c_0 x^{m-1} + \cdots + c_m \in k[x]$ なので，共通分母 $\mathrm{Res}(f,g,x)$ を括り出せば，

$$\tilde{A} = \frac{1}{\mathrm{Res}(f,g,x)} A$$

となる．$\tilde{B}$ も同様であるので，$\tilde{A}f + \tilde{B}g = 1$ の分母を払えば $Af + Bg = \mathrm{Res}(f,g,x)$ を得る．

∎

消去理論と終結式 V

- GCD と終結式の関係は？
- f, g が共通因子なし $\Leftrightarrow GCD(f,g) = 1 \Leftrightarrow \tilde{A}f + \tilde{B}g = 1$
- 上の命題から $\tilde{A}, \tilde{B}$ は共通分母として $\mathrm{Res}(f,g,x)$ を持つ！

Example.

ふたたび $f = xy - 1, g = x^2 + y^2 - 4$ の場合,
$\mathrm{Res}(f,g,x) = y^4 - 4y^2 + 1 \neq 0$. よって $GCD(f,g) = 1$ であり,

$$-\left(\frac{y}{y^4 - 4y^2 + 1}x + \frac{1}{y^4 - 4y^2 + 1}\right)f + \frac{y^2}{y^4 - 4y^2 + 1}g = 1$$

GCD を使うには体 $k(y)$ で考えなくてはいけない訳だが, ここで分母を払えば,

$$-(yx + 1)f + y^2 g = y^4 - 4y^2 + 1$$

これは命題 9 の例.

消去理論と終結式 VI

- 終結式は「分母なし」版の GCD だと思える！
- f, g の $k[x, y]$-線型結合で書けているので，
  $\mathrm{Res}(f, g, x) \in \langle f, g \rangle \cap k[y]$
- 次回以降は，これを多変数の場合に応用する
- （三つ以上の式の終結式を考える理論もある）

演習問題 I

Exercise 5-8

$f = a_0 x^\ell + \cdots + a_\ell, a_0 \neq 0, \ell > 0$ に対し，f の判別式 $\mathrm{disc}(f)$ を，

$$\mathrm{disc}(f) = \frac{(-1)^{\ell(\ell-1)/2}}{a_0} \mathrm{Res}(f, \tfrac{d}{dx} f, x)$$

により定義する．この時，f が重複因子を持つ $\Leftrightarrow \mathrm{disc}(f) = 0$

Proof.

$\mathrm{disc}(f) = 0$ とすると $\mathrm{Res}(f, f', x) = 0$ より，f, f' は共通因子を持つ．そこで $f' = hg, f = hk$ とすると，$h \mid \mathrm{GCD}(f, f')$ より f は少なくとも h^2 を因子に持つことがわかる．逆については $f = h^2 g$ と置けば，f, f' は共通因子 h を持つので $\mathrm{disc}(f) = 0$. ∎

演習問題 II

Exercise 5-9

前問を用いて，$6x^4 - 23x^3 + 32x^2 - 19x + 4$ が $\mathbb{C}$ で重根を持つかどうか判定し，その重根を求めよ．

CoCoA などに計算させれば $\mathrm{disc}(f) = 0$ となるので重複因子をもつ．よって，特に $\mathbb{C}$ では重根を持つ．$\mathrm{GCD}(f, f') = x - 1$ より，f は重根 1 を持つことがわかる．

Exercise 5-10

二次式 $f = ax^2 + bx + c$ の判別式は何か？これと重複因子の関係を論ぜよ．

計算してみると，

$$\mathrm{Res}(f, f', x) = \begin{vmatrix} a & 2a & 0 \\ b & b & 2a \\ c & 0 & b \end{vmatrix} = a(-b^2 + 4ac)$$

演習問題 III

よって，

$$\mathrm{disc}(f) = \frac{(-1)^{2\cdot 1/2}}{a} a(-b^2 + 4ac) = b^2 - 4ac$$

であり，これはいわゆる「判別式」と一致することがわかる．

終結式の計算アルゴリズム I

以下では，計算量が嵩む行列式を計算せずに，直接終結式を計算する方法を模索する．その為に幾つか必要な議論をしておく．

Exercise 5-14

今までは，次数が正の場合の終結式を考えてきた．以下では，定数も含める場合について考察する．

(a) $\deg f = \ell > 0, g = b_0 \in k$ とすると，
$\mathrm{Syl}(f, g, x) = (\delta_{ij} b_0)_{0 \le i,j \le \ell}$ かつ $\mathrm{Res}(f, b_0, x) = b_0^\ell$ を示せ．

(b) 上の場合でも命題 8, 9 は依然として真である事を示せ．

(c) $\deg g = m > 0, f = a_0 \in k$ の場合はどうなるか？

(d) $$\mathrm{Res}(a_0, b_0) = \begin{cases} 0 & (a_0 = 0 \vee b_0 = 0) \\ 1 & (a_0 \neq 0 \wedge b_0 \neq 0) \end{cases}$$
と定める．$f = g = 2$ の場合を考えることで，f, g が定数なら命題 8, 9 は成り立つとは限らないことを示せ．

終結式の計算アルゴリズム II

(a) $Af + Bb_0 = 0, \deg A < 0, \deg B < \ell$ とすると，必然的に $A = 0$ である．そこで $B = d_0 x^{\ell-1} + \cdots + d_{\ell-1}$ とおけば，

$$b_0 d_0 x^{\ell-1} + \cdots + b_0 d_{\ell-1} = 0$$

この係数行列が $\mathrm{Syl}(f, b_0, x)$ であるので，明らか．

(b) 定数 b_0 と多項式が共通因子を持つのは，$b_0 = 0$ の時，その時に限る．よってこれは自明．

(c) 行列式の性質より
$\mathrm{Res}(a_0, g, x) = (-1)^{\deg(g)\cdot\deg(a_0)}\mathrm{Res}(g, a_0, x) = a_0^m$.

終結式の計算アルゴリズム III

(d) $a_0 b_0 \neq 0$ ならば命題 8 は成立しているような気がする（1 だって a_0, b_0 の整数多項式には違いない）．だから
$f = g = 2$ は反例にはならないと思うが，$f = 2, g = 0$ の時は $\mathrm{Res}(2, 0, 0) = 0$ かつ $2, 0$ は共通因子を持たないので，これが反例である．
命題 9 については $f = g = 2$ がしっかり反例になっている．
$f(x) + g(x) = \frac{1}{2}$ となるような，2 を係数にもつ整数多項式は存在しない．

終結式の計算アルゴリズム IV

Exercise 5-16

$f = a_0 x^\ell + \cdots + a_\ell, g = b_0 x^m + \cdots + b_m, \ell \geq m$

(a) $\tilde{f} = f - \frac{a_0}{b_0} x^{\ell-m} g$ とおく時，$\deg \tilde{f} = \ell - 1$ ならば次が成立：

$$\mathrm{Res}(f, g, x) = (-1)^m b_0 \mathrm{Res}(\tilde{f}, g, x)$$

(b) より一般に $\deg \tilde{f} \leq \ell - 1$ の時次が成立：

$$\mathrm{Res}(f, g, x) = (-1)^{m(\ell - \deg \tilde{f})} b_0^{\ell - \deg \tilde{f}} \mathrm{Res}(\tilde{f}, g, x)$$

(c) 除法アルゴリズムにより $f = qg + r \quad (\deg r < \deg g)$ と書いた時，

$$\mathrm{Res}(f, g, x) = (-1)^{m(\ell - \deg r)} b_0^{\ell - \deg r} \mathrm{Res}(r, g, x)$$

終結式の計算アルゴリズム V

(a) b_i の最初から m 列分を $\frac{a_0}{b_0}$ 倍して a_i の列から引く．一行目で余因子展開すれば望みの結果が得られる．

(b) $(\ell - \deg \tilde{f})$ 回余因子展開をすればいい．

(c) $\deg r = \deg \tilde{f}$ ならば $f = r$ なので良い．そうでない時を考えよう．f の次数に関する帰納法で証明する． $\deg f = 0$ ならOK．$\deg f = n+1$ として，n 次以下で成立するとする．$\tilde{f} = g\tilde{q} + \tilde{r} \quad (\deg \tilde{r} < \deg g)$ とする．この時 $\tilde{f}$ の定義式に代入すれば，

$$f = \left(\frac{a_0}{b_0} x^{\ell - m} + \tilde{q} \right) g + \tilde{r} \quad (\deg \tilde{r} < \deg g)$$

よって，除法原理より $r = \tilde{r}$ である．ここで，もし $\deg \tilde{f} < \deg g$ ならば $r = \tilde{r} = \tilde{f}$ となるので，(b) より成立．$\deg \tilde{f} \geq \deg g$ とする．

終結式の計算アルゴリズム VI

この時，帰納法の仮定より，$\tilde{\ell} = \deg \tilde{f}$ とおけば，

$$\mathrm{Res}(\tilde{f}, g, x) = (-1)^{m(\tilde{\ell}-\deg(r))} b_0^{\tilde{\ell}-\deg(r)} \mathrm{Res}(r, g, x)$$

よって，

$$\begin{aligned}
\mathrm{Res}(f, g, x) &= (-1)^{m(\ell-\tilde{\ell})} b_0^{\ell-\tilde{\ell}} \mathrm{Res}(\tilde{f}, g, x) \\
&= (-1)^{m(\ell-\tilde{\ell})} b_0^{\ell-\tilde{\ell}} (-1)^{m(\tilde{\ell}-\deg(\tilde{r}))} b_0^{\tilde{\ell}-\deg(r)} \mathrm{Res}(r, g, x) \\
&= (-1)^{m(\ell-\deg r)} b_0^{\ell-\deg r} \mathrm{Res}(r, g, x)
\end{aligned}$$

終結式の計算アルゴリズム VII

Exercise 5-17

互除法のアルゴリズムをいじって終結式を得るアルゴリズムを紹介する．互除法では，$f = qg + r, g = q'g + r', \ldots$ などとおいて，

$$\mathrm{GCD}(f, g) = \mathrm{GCD}(g, r) = \mathrm{GCD}(r, r') = \ldots$$

などの関係式を使っていた．今までの結果を用いれば，上の等式の「終結式」版は次のようになる：

$$\begin{aligned}\mathrm{Res}(f, g, x) &= (-1)^{\deg g(\deg f - \deg r)} b_0^{\deg f - \deg r} \mathrm{Res}(r, g, x) \\ &= \cdots \\ &= (-1)^{\deg f \deg g + \deg g \deg r} b_0^{\deg f - \deg r} b_0'^{\deg g - \deg r'} \mathrm{Res}(r, r', x)\end{aligned}$$

これを踏まえれば，次のようなアルゴリズムが考えられる：

終結式の計算アルゴリズム VIII

- 入力：$f, g \in k[x]$
- $h := f, s := g$
- WHILE $deg(s) > 0$ DO
  - $r \longleftarrow \overline{h}^s$
  - $\mathtt{res} \longleftarrow (-1)^{\deg h \deg s} \mathrm{LC}(s)^{\deg h - \deg r} \mathtt{res}$
  - $h \longleftarrow s; s \longleftarrow r$
- IF $h = 0 \vee s = 0$
  - $\mathtt{res} \longleftarrow 0$
- IF $\deg h > 0$
  - $\mathtt{res} \longleftarrow s^{\deg h} \mathtt{res}$
- 出力：res

停止性，妥当性は明らか.