1　1 変数多項式の終結式

多項式の係数はいずれも整域 R の元としておく．こうしておくと多項式の係数を商体 $\mathrm{Rat}(R)$ の元として分数に拡張できる．さらに方程式の解は代数閉包 $\overline{\mathrm{Rat}(R)}$ 上で考えられる．もしかしたら R を UFD くらいに仮定しといた方が安全かもしれない．

定義 (**終結式**)**.** 多項式 $f(x) = \sum_{i=0}^{m} a_m x^i$ と $g(x) = \sum_{j=0}^{n} b_n x^j$ $(a_m, b_n \neq 0)$ に対して

$$\mathrm{Syl}(f,g) := \begin{bmatrix} a_m & a_{m-1} & \cdots & a_1 & a_0 & & & \\ & a_m & a_{m-1} & \cdots & a_1 & a_0 & & \\ & & \ddots & \ddots & & \ddots & \ddots & \\ & & & a_m & a_{m-1} & \cdots & a_1 & a_0 \\ b_n & b_{n-1} & \cdots & b_1 & b_0 & & & \\ & b_n & b_{n-1} & \cdots & b_1 & b_0 & & \\ & & \ddots & \ddots & & \ddots & \ddots & \\ & & & b_n & b_{n-1} & \cdots & b_1 & b_0 \end{bmatrix} \begin{array}{l} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} n \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} m \end{array}$$

を f と g の**シルベスター行列**といい，その行列式

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

を f と g の**終結式 (resultant)** という．なお，零でない定数 $g(x) = b_0 \neq 0$ に対しては

$$\mathrm{Syl}(f,b_0) = \begin{bmatrix} b_0 & & \\ & \ddots & \\ & & b_0 \end{bmatrix}, \quad \mathrm{resul}(f,b_0) = b_0^m$$

と定める．同様に，$\mathrm{resul}(a_0,g) = a_m^n$ とする．さらに，零多項式に対しては $\mathrm{resul}(f,0) = \mathrm{resul}(0,g) = 0$ と定める．

注意. 上で定義した $\mathrm{Syl}(f,g)$ の転置行列をシルベスター行列と呼ぶ流儀もある．

例 1. $f(x) = x^3 + 1,\ g(x) = x^2 + 2x + 1,\ h(x) = x^2 + 1$ とする．

$$\mathrm{resul}(f,g) = \begin{vmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 2 & 1 & 0 & 0 \\ 0 & 1 & 2 & 1 & 0 \\ 0 & 0 & 1 & 2 & 1 \end{vmatrix} = 2, \quad \mathrm{resul}(f,h) = \begin{vmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{vmatrix} = 0$$

終結式に関するいくつかの性質を紹介する．主に線形代数との関わりを紹介したいので，主張や証明が重複することが多々ある．以下，f, g は次のような多項式とする．

$$f(x) = \sum_{i=0}^{m} a_i x^i,\ g(x) = \sum_{j=0}^{n} b_j x^j, \quad a_m, b_n \neq 0$$

定理 1. $\mathrm{resul}(f, g) = 0$ ならば，f と g は共通根を持つ．

証明. $f(\alpha) = g(\alpha) = 0$ とする．

$$\begin{aligned}
\alpha^i f(\alpha) &= a_m \alpha^{m+i} + a_{m-1}\alpha^{m-1+i} + \cdots + a_0 \alpha^i = 0 \quad (i = 0, 1, \ldots, n-1), \\
\alpha^j g(\alpha) &= b_n \alpha^{n+j} + b_{n-1}\alpha^{n-1+j} + \cdots + b_0 \alpha^j = 0 \quad (j = 0, 1, \ldots, m-1)
\end{aligned}$$

が成り立つ．これは行列を使って以下のように書ける．

$$\mathrm{Syl}(f, g) \begin{bmatrix} \alpha^{m+n-1} \\ \alpha^{m+m-2} \\ \vdots \\ \alpha \\ 1 \end{bmatrix} = \mathbf{0}_{m+n}$$

同次形連立 1 次方程式 $\mathrm{Syl}(f, g)\boldsymbol{x} = \mathbf{0}$ が非自明解を持つので $\mathrm{resul}(f, g) = 0$ である． □

定理 2. 定数でない多項式 f, g に関して以下は同値である．

(1) $\mathrm{resul}(f, g) = 0$.

(2) f, g は定数でない共通因子を持つ．

(3) 以下を満たす多項式 A, B （少なくとも一方は非零多項式）が存在する．

$$Af + Bg = 0, \quad \deg A < n,\ \deg B < m$$

証明. □

2　2 変数多項式の終結式

参考文献

[1] 長坂工作・岩根秀直（編),『計算機代数の基礎理論』, 共立出版 (2020).

[2] 三宅敏恒,『線形代数概論』, 培風館 (2023).

[3] 横山和弘,『多項式と計算機代数』, 朝倉書店 (2022).

[4] D. A. Cox, J. Little and D. O'Shea, *Ideals Varieties, and Algorithms 4th edition*, Springer (2015).

[5] S. Lang, *Algebra Revised 3rd edition*, Springer (2004).