1　終結式の定義

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

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

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

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

であり，同様に $\mathrm{resul}(a_0,g) = a_m^n$ である．また，共に定数の場合は $\mathrm{resul}(a_0,b_0) = 1$ とし，一方が零多項式の場合は $\mathrm{resul}(f,0) = \mathrm{resul}(0,g) = 0$ 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．

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

次の定理 1 から，f,g は共通根を持ち，f,h は共通根を持たないことがわかる．

2　終結式と共通根

以下，f, g は次のような多項式とする．ただし，$a_m, b_n \neq 0$ とする．

$$f(x) = \sum_{i=0}^{m} a_i x^i = a_m \prod_{i=1}^{m} (x - \alpha_i), \quad g(x) = \sum_{j=0}^{n} b_j x^j = b_n \prod_{j=1}^{n} (x - \beta_j)$$

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

証明. ($\Rightarrow$) $f(\gamma) = g(\gamma) = 0$ とすると，$\gamma^i f(\gamma) = \gamma^j g(\gamma) = 0$ なので以下が成り立つ．

$$\begin{bmatrix} a_3 & a_2 & a_1 & a_0 & 0 \\ 0 & a_3 & a_2 & a_1 & a_0 \\ b_2 & b_1 & b_0 & 0 & 0 \\ 0 & b_2 & b_1 & b_0 & 0 \\ 0 & 0 & b_2 & b_1 & b_0 \end{bmatrix} \begin{bmatrix} \gamma^4 \\ \gamma^3 \\ \gamma^2 \\ \gamma \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad (m = 3, n = 2 \text{ の場合})$$

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

($\Leftarrow$) 以下の補題 1 より従う． □

補題 1. $\mathrm{resul}(f, g) = a_m^n b_n^m \prod_{i=1}^{m} \prod_{j=1}^{n} (\alpha_i - \beta_j)$

証明. 定理 1 の ($\Rightarrow$) から $\alpha_i = \beta_j$ のとき $\mathrm{resul}(f, g) = 0$ なので，因数定理より $T := \prod\prod(\alpha_i - \beta_j)$ は $\mathrm{resul}(f, g)$ を割り切る．そこで，各 α_i, β_j の多項式として $\mathrm{resul}(f, g)$ と T の次数を評価し，係数を比較すればよい．

$$f(x)/a_m = x^m + A_1 x^{m-1} + \cdots + A_m = \prod_{i=1}^{m} (x - \alpha_i),$$
$$g(x)/b_n = x^n + B_1 x^{n-1} + \cdots + B_n = \prod_{j=1}^{n} (x - \beta_j)$$

とすると，$m = 3, n = 2$ の場合

$$\mathrm{resul}(f, g) = a_3^2\ b_2^3 \begin{vmatrix} 1 & A_1 & A_2 & A_3 & 0 \\ 0 & 1 & A_1 & A_2 & A_3 \\ 1 & B_1 & B_2 & 0 & 0 \\ 0 & 1 & B_1 & B_2 & 0 \\ 0 & 0 & 1 & B_1 & B_2 \end{vmatrix}$$

である．各 A_k は $\alpha_1, \dots, \alpha_m$ の，各 B_k は $\beta_1, \dots, \beta_n$ の k 次基本対称式の ± 1 倍である．また，各 A_i, B_j はそれぞれ α_i, β_j の 1 次式なので，$\mathrm{resul}(f,g)$ は α_i に関して高々 n 次で，β_j に関して高々 m 次である．従って，$\mathrm{resul}(f,g)$ は T の定数倍であり，α_1^n の係数を比較して，$\mathrm{resul}(f,g) = a_m^n b_n^m T$ がわかる．□

例 2. $f(x) = ax^2 + bx + c \ (a \neq 0)$ とする．$f'(x) = 2ax + b$ であり，

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

より，$b^2 - 4ac = 0$ のとき f, f' は共通根を持つ．また，このとき f は重根を持つ．

定理 2. 非定数多項式 f に対して，以下は同値.

(1) f は重根を持つ.
(2) f, f' は共通根を持つ.
(3) $\mathrm{resul}(f, f') = 0$.

定理 3.

$$\mathrm{resul}(f, f') = (-1)^{m(m-1)/2} \ a_m^{2m-1} \prod_{1 \le i < j \le m} (\alpha_i - \alpha_j)^2$$

証明. 補題 1 より，一般に

$$\mathrm{resul}(f,g) = a_m^n \ b_n^m \ \prod_{i=1}^m \prod_{j=1}^n (\alpha_i - \beta_j) = a_m^n \ \prod_{i=1}^m \left(b_n \prod_{j=1}^n (\alpha_i - \beta_j) \right) = a_m^n \ \prod_{i=1}^m g(\alpha_i)$$

が成り立つ．これを $g = f'$ として適用して

$$\mathrm{resul}(f, f') = a_m^{m-1} \ \prod_{i=1}^m f'(\alpha_i)$$

を得る．$f'(x) = a_m \displaystyle\sum_{i=1}^m \prod_{\substack{j=1 \\ j \neq i}}^m (x - \alpha_j)$ より $f'(\alpha_i) = a_m \displaystyle\prod_{\substack{j=1 \\ j \neq i}}^m (\alpha_i - \alpha_j)$ から従う．□

定義 (判別式). 2 次以上の多項式 f に対して以下の $\mathrm{disc}(f)$ を f の**判別式**という．

$$\mathrm{disc}(f) = a_m^{2m-2} \prod_{1 \le i < j \le m} (\alpha_i - \alpha_j)^2 = \frac{(-1)^{m(m-1)/2}}{a_m} \mathrm{resul}(f, f')$$

定理 2, 3 より，f が重根を持つことと $\mathrm{disc}(f) = 0$ は同値である．

例 3. $f(x)=x^3+px+q$ とする．$f'(x)=3x^2+p$ より，$\mathrm{disc}(f)$ は以下の通り．

$$\mathrm{disc}(f)=(-1)^3\,\mathrm{resul}(f,f')=-\begin{vmatrix}1&0&p&q&0\\0&1&0&p&q\\3&0&p&0&0\\0&3&0&p&0\\0&0&3&0&p\end{vmatrix}=-(4p^3+27q^2)$$

定理 4. f を実係数 3 次多項式とする．

$$\mathrm{disc}(f)=\begin{cases}>0 & (\,f\text{ は相異なる 3 個の実根を持つ})\\ =0 & (\,f\text{ は重根を持ち，どの根も実数})\\ <0 & (\,f\text{ は 1 個の実根と 2 個の互いに共役な虚根を持つ})\end{cases}$$

証明. f の根 $\alpha_1,\alpha_2,\alpha_3$ が互いに相異なる実数のとき，定義から $\mathrm{disc}(f)>0$ である．f が重根を持つとき，$\mathrm{disc}(f)=0$ である．α_1 が実数で α_2,α_3 が互いに共役な虚数のとき，

$$\begin{aligned}\mathrm{disc}(f)&=a_m^{2m-2}(\alpha_1-\alpha_2)^2(\alpha_1-\alpha_3)^2(\alpha_2-\alpha_3)^2\\&=a_m^{2m-2}\left((\alpha_1-\alpha_2)\left(\overline{\alpha_1-\alpha_2}\right)\right)^2\left(2i\left(\Im\alpha_2\right)\right)^2=-4a_m^{2m-2}\left|\alpha_1-\alpha_2\right|^2\left(\Im\alpha_2\right)^2<0\end{aligned}$$

である．f は実係数なので実根は 1 個以上あり，虚根は偶数個で重根ではない．□

例 4 (接点 t 問題)**.** 点 (a,b) から曲線 $y=x^3-3x$ に引ける接線の本数が 3 本になるときの a,b の条件を求めよう．

点 (a,b) を通る直線 $y=m(x-a)+b$ と曲線 $y=x^3-3x$ が接するための必要十分条件は，3 次多項式 $f(x)=x^3-3x-(m(x-a)+b)$ が重根を持つこと，つまり

$$\mathrm{resul}(f,f')=-4m^3+9\left(3a^2-4\right)m^2-54\left(ab+2\right)m+27\left(b-2\right)\left(b+2\right)=0$$

が成り立つことである．そして，このような接線が 3 本存在することは，上の m に関する 3 次方程式が異なる 3 実解を持つことと同値である．つまり，

$$g(m)=-4m^3+9\left(3a^2-4\right)m^2-54\left(ab+2\right)m+27\left(b-2\right)\left(b+2\right)$$

とおいて，$\mathrm{disc}(g)>0$ となる条件を求めればよい．

$$\mathrm{disc}(g)=\frac{-1}{-4}\,\mathrm{resul}(g,g')=314928(a^3-3a-b)(3a+b)^3$$

より，$(a^3-3a-b)(3a+b)>0$ が求める条件である．

3　終結式と共通因子

定理 5. 定数でない多項式 f, g に関して以下は同値である．

(1) f, g は定数でない共通因子を持つ．

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

$$Uf + Vg = 0, \quad \deg U < n,\ \deg V < m$$

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

証明. (1) $\Rightarrow$ (2) h を f, g の共通因子とし，$f = hf_1$, $g = hg_1$ とする．

$$g_1 \cdot f + (-f_1) \cdot g = g_1 h f_1 - f_1 h g = 0$$

より，$U = g_1, V = -f_1$ とすればよい．

(2) $\Rightarrow$ (1) $Uf + Vg = 0$, $\deg U < n$, $\deg V < m$, $V \neq 0$ とする．f, g が共通因子を持たないとすると，$\tilde{U}f + \tilde{V}g = 1$ を満たす多項式 $\tilde{U}, \tilde{V}$ が存在する．$Vg = -Uf$ なので

$$V = V(\tilde{U}f + \tilde{V}g) = \tilde{U}Vf + \tilde{V}Vg = \tilde{U}Vf + \tilde{V}(-Uf) = (\tilde{U}V - \tilde{V}U)f$$

である．$V \neq 0$ なので $\deg V \geq \deg f = n$ より，$\deg V < n$ に矛盾する．

(2) $\Leftrightarrow$ (3) 簡単のため，$m = 3, n = 2$ とする．一般の場合も同様である．

$$U = \sum_{i=0}^{n-1} u_i x^i = u_1 x + u_0, \quad V = \sum_{j=0}^{m-1} v_j x^j = v_2 x^2 + v_1 x + v_0$$

とおき，$\boldsymbol{w}^\top = \begin{bmatrix} u_1 & u_0 & v_2 & v_1 & v_0 \end{bmatrix}$ とすると

$$Uf + Vg = 0 \Leftrightarrow \begin{cases} a_3 u_1 + b_2 v_2 = 0 \\ a_2 u_1 + a_3 u_0 + b_1 v_2 + b_2 v_1 = 0 \\ a_1 u_1 + a_2 u_0 + b_0 v_2 + v_1 v_1 + b_2 v_0 = 0 \\ a_0 u_1 + a_1 u_0 + b_0 v_1 + b_1 v_0 = 0 \\ a_0 u_0 + b_0 v_0 = 0 \end{cases}$$

$$\Leftrightarrow \begin{bmatrix} a_3 & 0 & b_2 & 0 & 0 \\ a_2 & a_3 & b_1 & b_2 & 0 \\ a_1 & a_2 & b_0 & b_1 & b_2 \\ a_0 & a_1 & 0 & b_0 & b_1 \\ 0 & a_0 & 0 & 0 & b_0 \end{bmatrix} \begin{bmatrix} u_1 \\ u_0 \\ v_2 \\ v_1 \\ v_0 \end{bmatrix} = \mathbf{0}_5 \Leftrightarrow \mathrm{Syl}(f, g)^\top\ \boldsymbol{w} = \mathbf{0}_5$$

なので，$\mathrm{resul}(f,g)=\det\left(\mathrm{Syl}(f,g)^{\top}\right)$ と合わせて以下を得る．

$$(2) \Leftrightarrow \text{同次形連立 1 次方程式 } \mathrm{Syl}(f,g)^{\top}\,\boldsymbol{x}=\boldsymbol{0} \text{ が非自明解を持つ} \Leftrightarrow (3)$$

$\square$

定理 6. 非零多項式 $f,g\in R[x]$ に対して次を満たす $U,V\in \mathrm{Rat}(R)[x]$ が存在する．

$$Uf+Vg=\mathrm{resul}(f,g)$$

特に，f,g の一方が非定数なら，$U,V\in R[x]$ である．

証明. $\mathrm{resul}(f,g)=0$ なら $U=V=0$ とし，f,g の一方が定数，例えば $f=a_0$ なら

$$\mathrm{resul}(a_0,g)=a_0^n=a_0^{n-1}\cdot f+0\cdot g$$

とすればよいので，f,g 共に定数でないとし，$\mathrm{resul}(f,g)\neq 0$ とする．まず，

$$\tilde{U}f+\tilde{V}g=1$$

を満たす多項式 $\tilde{U},\tilde{V}$ を構成する．$\tilde{U}=\displaystyle\sum_{i=0}^{n-1}u_ix^i$，$\tilde{V}=\displaystyle\sum_{j=0}^{m-1}v_jx^j$ とおくと，

$$\tilde{U}f+\tilde{V}g=1\Leftrightarrow\begin{bmatrix} a_3 & 0 & b_2 & 0 & 0\\ a_2 & a_3 & b_a & b_2 & 0\\ a_1 & a_2 & b_0 & b_1 & b_2\\ a_0 & a_1 & 0 & b_0 & b_1\\ 0 & a_0 & 0 & 0 & b_0\end{bmatrix}\begin{bmatrix} u_1\\ u_0\\ v_2\\ v_1\\ v_0\end{bmatrix}=\begin{bmatrix}0\\0\\0\\0\\1\end{bmatrix}$$

である（$m=3,n=2$ の場合）．この係数行列は $\mathrm{Syl}(f,g)^{\top}$ であり，その行列式は $\mathrm{resul}(f,g)\neq 0$ なのでこれは唯一つの解を持つ．クラーメルの公式から，例えば u_1 は

$$u_1=\frac{1}{\mathrm{resul}(f,g)}\begin{vmatrix} 0 & 0 & b_2 & 0 & 0\\ 0 & a_3 & b_a & b_2 & 0\\ 0 & a_2 & b_0 & b_1 & b_2\\ 0 & a_1 & 0 & b_0 & b_1\\ 1 & a_0 & 0 & 0 & b_0\end{vmatrix}$$

であり，この行列式部分は R の元である．他の u_i,v_j についても同様なので，共通の分母 $\mathrm{resul}(f,g)$ を払って $U=\mathrm{resul}(f,g)\tilde{U}$，$V=\mathrm{resul}(f,g)\tilde{V}$ とすれば，$Uf+Vg=\mathrm{resul}(f,g)$ である．$\square$

4　2変数多項式の終結式

k を体とする．以下 $f, g \in k[x, y] = (k\,[y])\,[x]$ は次のような多項式とする．

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

前節で $R = k[y]$ として定まる終結式 $\mathrm{resul}(f, g) \in k[y]$ を $\mathrm{resul}_x(f, g)$ と書く．

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 Ulgorithms 4th edition*, Springer (2015).

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