

## 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  $\text{Rat}(R)$  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  $\overline{\text{Rat}(R)}$  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

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

を  $f$  と  $g$  のシルベスター行列といい，その行列式

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

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

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

であり，同様に  $\text{resul}(a_0, g) = a_m^n$  である．また，共に非零定数の場合は  $\text{resul}(a_0, b_0) = 1$  とし，一方が零多項式の場合は  $\text{resul}(f, 0) = \text{resul}(0, g) = 0$  と定める．

**注意.** 上で定義した  $\text{Syl}(f, g)$  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．

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

## 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.  $\iff \text{resul}(f, g) = 0$ .

**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  $\text{Syl}(f, g)\mathbf{x} = \mathbf{0}$  が非自明解を持つので  $\text{resul}(f, g) = 0$  である.

$(\Leftarrow)$  以下の補題 1 より従う. □

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

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

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

とすると,  $m=3, n=2$  の場合

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

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  $\pm 1$  倍である. また, 各  $A_i, B_j$  はそれぞれ  $\alpha_i, \beta_j$  の 1 次式なので,  $\text{resul}(f, g)$  は  $\alpha_i$  に関して高々  $n$  次で,  $\beta_j$  に関して高々  $m$  次である. 従って,  $\text{resul}(f, g)$  は  $T$  の定数倍であり,  $\alpha_1^n$  の係数を比較して,  $\text{resul}(f, g) = a_m^n b_n^m T$  がわかる.  $\square$

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

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

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)  $\text{resul}(f, f') = 0$ .

**定理 3.**

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

**証明.** 補題 1 より, 一般に

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

が成り立つ. これを  $g = f'$  として適用して

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

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

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

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

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

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

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

**定理 4.**  $f$  を実係数 3 次多項式とする.

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

**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  $\text{disc}(f) > 0$  である.  $f$  が重根を持つとき,  $\text{disc}(f) = 0$  である.  $\alpha_1$  が実数で  $\alpha_2, \alpha_3$  が互いに共役な虚数のとき,

$$\begin{aligned} \text{disc}(f) &= a_3^{2 \cdot 3 - 2} (\alpha_1 - \alpha_2)^2 (\alpha_1 - \alpha_3)^2 (\alpha_2 - \alpha_3)^2 \\ &= a_3^4 ((\alpha_1 - \alpha_2) (\overline{\alpha_1 - \alpha_2}))^2 (2i (\Im \alpha_2))^2 = -4a_3^4 |\alpha_1 - \alpha_2|^2 (\Im \alpha_2)^2 < 0 \end{aligned}$$

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

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

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,

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

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

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

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

**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.

$$g_1 \cdot f + (-f_1) \cdot g = g_1 hf_1 - f_1 hg_1 = 0$$

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,  $\tilde{U}f + \tilde{V}g = 1$  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,  $\mathbf{w}^\top = \begin{bmatrix} u_1 & u_0 & v_2 & v_1 & v_0 \end{bmatrix}$  とすると

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

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

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

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

□

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

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

特に,  $f, g$  の一方が非定数なら,  $U, V \in R[x]$  である.

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

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

とすればよいので,  $f, g$  共に定数でないとし,  $\text{resul}(f, g) \neq 0$  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.  $\tilde{U} = \sum_{i=0}^{n-1} u_i x^i$ ,  $\tilde{V} = \sum_{j=0}^{m-1} v_j x^j$  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  $\text{Syl}(f, g)^\top$  であり, その行列式は  $\text{resul}(f, g) \neq 0$  なのでこれは唯一つの解を持つ. クラームルの公式から, 例えば  $u_1$  は

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

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  $\text{resul}(f, g)$  を払って  $U = \text{resul}(f, g)\tilde{U}$ ,  $V = \text{resul}(f, g)\tilde{V}$  とすれば,  $Uf + Vg = \text{resul}(f, g)$  である. □

## 4 2 変数多項式の終結式と消去法

$k$  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.

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

係数環を  $R = k[y]$  として定まる終結式  $\text{resul}(f, g) \in k[y]$  を  $\text{resul}_x(f, g)(y)$  と書く. 同様に, シルベスター行列も  $\text{Syl}_x(f, g)(y)$  と書く.

**例 5.**  $f(x, y) = x^2 + y^2 - 1$ ,  $g(x, y) = x^2 + xy + y^2 - 1$  とすると,

$$\text{resul}_x(f, g)(y) = \begin{vmatrix} 1 & 0 & y^2 - 1 & 0 \\ 0 & 1 & 0 & y^2 - 1 \\ 1 & y & y^2 - 1 & 0 \\ 0 & 1 & y & y^2 - 1 \end{vmatrix} = y^4 - y^2 = y^2(y+1)(y-1)$$

である. この根  $y = 0$  を  $f, g$  に代入すると,

$$f(x, 0) = g(x, 0) = x^2 - 1 = (x+1)(x-1)$$

となり,  $f(1, 0) = g(1, 0) = 0$  と  $f(-1, 0) = g(-1, 0) = 0$  がわかる. 残りの根  $y = -1, 1$  も同様に  $f, g$  に代入すると,

$$\begin{cases} f(x, -1) = x^2 \\ g(x, -1) = x^2 - x = x(x-1) \end{cases} \quad \begin{cases} f(x, 1) = x^2 \\ g(x, 1) = x^2 + x = x(x+1) \end{cases}$$

となり,  $f(0, 1) = g(0, 1) = 0$  と  $f(0, -1) = g(0, -1) = 0$  がわかる. つまり,

$$(x, y) = (1, 0), \quad (-1, 0), \quad (0, 1), \quad (0, -1)$$

の 4 点は連立方程式  $f(x, y) = g(x, y) = 0$  の解である. 実はこれが解の全てであることが以下の定理 7 によって保証される.

**定理 7.**  $f(\alpha, \beta) = g(\alpha, \beta) = 0 \implies \text{resul}_x(f, g)(\beta) = 0$

**証明.**  $f, g$  のいずれかが零多項式なら明らかなので, 共に零でないとする. 定理 6 から

$$U(x, y)f(x, y) + V(x, y)g(x, y) = \text{resul}_x(f, g)(y)$$

を満たす  $U(x, y), V(x, y) \in k[x, y]$  が存在するので,  $f(\alpha, \beta) = g(\alpha, \beta) = 0$  ならば  $\text{resul}_x(f, g)(\beta) = 0$  である.  $\square$

**例 6.** 2 変数関数  $f(x, y) = xy(x^2 + y^2 - 4)$  の停留点を全て求めるために、連立方程式  $f_x(x, y) = f_y(x, y) = 0$  を解く.

$$f_x(x, y) = 3yx^2 + y(y^2 - 4), \quad f_y(x, y) = x^3 + (3y^2 - 4)x$$

なので、終結式  $\text{resul}_x(f_x, f_y)$  は第 1 列に関する余因子展開を利用しつつ

$$\begin{aligned} \text{resul}_x(f_x, f_y)(y) &= \begin{vmatrix} 3y & 0 & y(y^2 - 4) & 0 & 0 \\ 0 & 3y & 0 & y(y^2 - 4) & 0 \\ 0 & 0 & 3y & 0 & y(y^2 - 4) \\ 1 & 0 & 3y^2 - 4 & 0 & 0 \\ 0 & 1 & 0 & 3y^2 - 4 & 0 \end{vmatrix} \\ &= \begin{vmatrix} 0 & 0 & -8y(y^2 - 1) & 0 & 0 \\ 0 & 3y & 0 & y(y^2 - 4) & 0 \\ 0 & 0 & 3y & 0 & y(y^2 - 4) \\ 1 & 0 & 3y^2 - 4 & 0 & 0 \\ 0 & 1 & 0 & 3y^2 - 4 & 0 \end{vmatrix} \\ &= - \begin{vmatrix} 0 & -8y(y^2 - 1) & 0 & 0 \\ 3y & 0 & y(y^2 - 4) & 0 \\ 0 & 3y & 0 & y(y^2 - 4) \\ 1 & 0 & 3y^2 - 4 & 0 \end{vmatrix} \\ &= - \begin{vmatrix} 0 & -8y(y^2 - 1) & 0 & 0 \\ 0 & 0 & -8y(y^2 - 1) & 0 \\ 0 & 3y & 0 & y(y^2 - 4) \\ 1 & 0 & 3y^2 - 4 & 0 \end{vmatrix} \\ &= \begin{vmatrix} -8y(y^2 - 1) & 0 & 0 \\ 0 & -8y(y^2 - 1) & 0 \\ 3y & 0 & y(y^2 - 4) \end{vmatrix} = 64y^3(y - 2)(y + 2)(y - 1)^2(y + 1)^2 \end{aligned}$$

と計算できる. これより,  $\text{resul}_x(f_x, f_y)(y) = 0$  の解  $y = 0, \pm 1, \pm 2$  が得られるので,

- $f_x(x, 0) = 0$  かつ  $f_y(x, 0) = x(x^2 - 4) = 0 \Leftrightarrow x = 0, \pm 2$
- $f_x(x, 1) = 3(x^2 - 1) = 0$  かつ  $f_y(x, 1) = x(x^2 - 1) = 0 \Leftrightarrow x = \pm 1$
- $f_x(x, -1) = -3(x^2 - 1) = 0$  かつ  $f_y(x, -1) = x(x^2 - 1) = 0 \Leftrightarrow x = \pm 1$
- $f_x(x, 2) = 6x^2 = 0$  かつ  $f_y(x, 2) = x(x^2 + 8) = 0 \Leftrightarrow x = 0$
- $f_x(x, -2) = -6x^2 = 0$  かつ  $f_y(x, -2) = x(x^2 + 8) = 0 \Leftrightarrow x = 0$

より,  $f$  の停留点は  $(0, 0)$ ,  $(\pm 2, 0)$ ,  $(1, \pm 1)$ ,  $(-1, \pm 1)$ ,  $(0, \pm 2)$  の 9 点である.



$y$  に関する方程式  $\text{resul}_x(f, g)(y) = 0$  は連立方程式  $f(x, y) = g(x, y) = 0$  から変数  $x$  を消去した方程式である. この  $\text{resul}_x(f, g)(y) = 0$  の解  $y = \beta$  を  $f(x, y) = g(x, y) = 0$  の解  $(x, y) = (\alpha, \beta)$  へと拡張する, というのが 2 変数終結式の使い方である.

ところが,  $\text{resul}_x(f, g)(\beta) = 0$  となる  $\beta$  に対していつでも  $f(\alpha, \beta) = g(\alpha, \beta) = 0$  となる  $\alpha$  が存在するとは限らない. 以下のような例がある.

**例 7.**  $f(x, y) = (y - 1)x^2 + (y^2 - 2y)x + y - 3$ ,  $g(x, y) = (y - 1)x - 1$  に対して

$$\text{resul}_x(f, g)(y) = \begin{vmatrix} y-1 & y^2-2y & y-3 \\ y-1 & -1 & 0 \\ 0 & y-1 & -1 \end{vmatrix} = 2(y-1)^2(y-2)$$

なので,  $\text{resul}_x(f, g)(y) = 0$  の解として  $y = 1, 2$  が得られる. 一方で,

$$f(x, 1) = -x - 2, \quad g(x, 1) = -1$$

なので,  $f(\alpha, 1) = g(\alpha, 1) = 0$  を満たす  $\alpha$  は存在しない.

例 7 のようなことが起こるのは,  $f(x, 1), g(x, 1)$  の  $x$  に関する最高次の係数が 0 となることで,  $\text{Syl}(f(x, 1), g(x, 1))$  の次数が下がり,

$$0 = \text{resul}_x(f, g)(1) \neq \text{resul}(f(x, 1), g(x, 1)) = -1$$

となっていることが原因である. このような問題は, 2 変数多項式の終結式  $\text{resul}_x(f, g)(y)$  に  $y = \beta$  を代入した  $\text{resul}_x(f, g)(\beta)$  と,  $f(x, y), g(x, y)$  に  $y = \beta$  を代入したものの終結式  $\text{resul}(f(x, \beta), g(x, \beta))$  が一致していれば発生しない.

**定理 8.** 次を満たす  $\beta \in \bar{k}$  に対して,  $f(\alpha, \beta) = g(\alpha, \beta) = 0$  を満たす  $\alpha \in \bar{k}$  が存在する.

$$\text{resul}_x(f, g)(\beta) = \text{resul}(f(x, \beta), g(x, \beta)) = 0$$

**証明.** 定理 1 から  $f(x, \beta), g(x, \beta)$  に共通根  $\alpha \in \bar{k}$  が存在し,  $f(\alpha, \beta) = g(\alpha, \beta) = 0$ .  $\square$

実際には,  $f(x, \beta), g(x, \beta)$  の最高次係数が共に 0 でなければ, 2 つの終結式は一致する.

**補題 2.**  $\beta \in \bar{k}$  に対して,  $a_m(\beta) \neq 0$  かつ  $b_n(\beta) \neq 0$  であれば以下が成り立つ.

$$\text{resul}_x(f, g)(\beta) = \text{resul}(f(x, \beta), g(x, \beta))$$

**証明.**  $a_m(\beta) \neq 0$  かつ  $b_n(\beta) \neq 0$  のとき, 2 つのシルベスター行列  $\text{Syl}_x(f, g)(\beta)$  と  $\text{Syl}(f(x, \beta), g(x, \beta))$  は共に  $(m + n)$  次正方行列で各成分が等しい. つまり,  $\text{Syl}_x(f, g)(\beta) = \text{Syl}(f(x, \beta), g(x, \beta))$  でなので, 両者の行列式も当然等しい.  $\square$

例 8. 例 7 の  $\text{resul}_x(f, g)(y) = 0$  の解  $y = 2$  に関しては,  $f(x, 2) = x^2 - 1$ ,  $g(x, 2) = x - 1$  より, いずれも最高次数が下がらず,

$$\text{Syl}_x(f, g)(2) = \text{Syl}(f(x, 2), g(x, 2)) = \begin{bmatrix} 1 & 0 & -1 \\ 1 & -1 & 0 \\ 0 & 1 & -1 \end{bmatrix}$$

である. さらに,  $f(1, 2) = g(1, 2) = 0$  である. 以上から,  $(x, y) = (1, 2)$  が連立方程式  $f(x, y) = g(x, y) = 0$  の解の全てである.

補題 2 と定理 8 から,  $a_m(\beta) \neq 0$  かつ  $b_n(\beta) \neq 0$  なら  $\text{resul}_x(f, g)(y) = 0$  の解  $y = \beta$  を  $f(x, y) = g(x, y) = 0$  の解  $(x, y) = (\alpha, \beta)$  に拡張できるが, この条件は弱められる.

**定理 9 (解の拡張定理).**  $\text{resul}_x(f, g)(\beta) = 0$  のとき,  $a_m(\beta) \neq 0$  または  $b_n(\beta) \neq 0$  なら  $f(\alpha, \beta) = g(\alpha, \beta) = 0$  となる  $\alpha \in \bar{k}$  が存在する.

**証明.**  $b_n(\beta) \neq 0$  のときも同様なので,  $a_m(\beta) \neq 0$  とし,  $k = \deg(g(x, \beta))$  とする.

$k = -\infty$  ( $\Leftrightarrow g(x, \beta) = 0$ ) のとき,  $\text{resul}(f(x, \beta), 0) = 0$  なので, 定理 8 から従う.

$k = 0$  ( $\Leftrightarrow g(x, \beta) = b_0(\beta) \neq 0$ ) とはならない. 実際,  $a_m(\beta) \neq 0$  かつ  $b_n(\beta) = b_0(\beta) \neq 0$  なので補題 2 から  $\text{resul}_x(f, g)(\beta) = \text{resul}(f(x, \beta), g(x, \beta))$  だが, 終結式の定義から  $\text{resul}(f(x, \beta), g(x, \beta)) \text{resul}(f(x, \beta), b_0(\beta)) = a_m(\beta)^n \neq 0$  である.

以下,  $k \geq 1$  とする. このとき,  $\text{resul}_x(f, g)(\beta) = a_m(\beta)^{n-k} \text{resul}(f(x, \beta), g(x, \beta))$  が成り立つ. 実際, 例えば  $m = 4, n = 3, k = 1$  の場合では

$$\begin{aligned} \text{resul}_x(f, g)(\beta) &= \begin{vmatrix} a_4 & a_3 & a_2 & a_1 & a_0 & 0 & 0 \\ 0 & a_4 & a_3 & a_2 & a_1 & a_0 & 0 \\ 0 & 0 & a_4 & a_3 & a_2 & a_1 & a_0 \\ 0 & 0 & b_1 & b_0 & 0 & 0 & 0 \\ 0 & 0 & 0 & b_1 & b_0 & 0 & 0 \\ 0 & 0 & 0 & 0 & b_1 & b_0 & 0 \\ 0 & 0 & 0 & 0 & 0 & b_1 & b_0 \end{vmatrix} \\ &= a_4^2 \begin{vmatrix} a_4 & a_3 & a_2 & a_1 & a_0 \\ b_1 & b_0 & 0 & 0 & 0 \\ 0 & b_1 & b_0 & 0 & 0 \\ 0 & 0 & b_1 & b_0 & 0 \\ 0 & 0 & 0 & b_1 & b_0 \end{vmatrix} = a_4^2 \text{resul}(f(x, \beta), g(x, \beta)) \end{aligned}$$

となる.  $a_m(\beta) \neq 0$  なので, これより  $\text{resul}_x(f, g)(\beta) = \text{resul}(f(x, \beta), g(x, \beta)) = 0$  だから, 定理 8 より従う.  $\square$

**例 9.**  $f(x, y) = (y - 1)x^2 - x + y$ ,  $g(x, y) = yx - 1$  とする.

$$\text{resul}_x(f, g)(y) = y^3 - 1 = (y - 1)(y - \omega)(y - \omega^2) \quad (\omega = \exp(2\pi i/3))$$

である. この根  $y = 1$  を  $f(x, y)$  の  $x$  に関する最高次係数  $a_2(y) = y - 1$  に代入すると  $a_2(1) = 0$  となるが,  $g(x, y)$  の最高次係数  $b_1(y) = y$  に代入しても  $b_1(1) = 1 \neq 0$  なので定理 9 からこの  $y = 1$  を連立方程式  $f(x, y) = g(x, y) = 0$  の解に拡張できる. 実際,

$$f(x, 1) = -x + 1, \quad g(x, 1) = x - 1$$

なので,  $(x, y) = (1, 1)$  が  $f(x, y) = g(x, y) = 0$  の解である.

$$\text{Syl}_x(f, g)(y) = \begin{bmatrix} y - 1 & -1 & y \\ y & -1 & 0 \\ 0 & y & -1 \end{bmatrix}$$

なので,  $y = 1$  を代入して行列式をとれば

$$\det(\text{Syl}_x(f, g)(1)) = \text{resul}_x(f, g)(1) = \begin{vmatrix} 0 & -1 & 1 \\ 1 & -1 & 0 \\ 0 & 1 & -1 \end{vmatrix} = -1 \times \begin{vmatrix} -1 & 1 \\ 1 & -1 \end{vmatrix} = 0$$

となるが, 最後の 2 次の行列式が  $f(x, 1)$  と  $g(x, 1)$  の終結式である.

$$\text{resul}(f(x, 1), g(x, 1)) = \begin{vmatrix} -1 & 1 \\ 1 & -1 \end{vmatrix} = 0$$

なお,  $\text{resul}_x(f, g)(y) = 0$  の残りの解  $y = \omega, \omega^2$  を拡張すれば, 連立方程式  $f(x, y) = g(x, y) = 0$  の残りの解  $(x, y) = (\omega, \omega^2), (\omega^2, \omega)$  が得られる.

## 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).