2章 終結式

定義 2.1

$f(X) = a_0X^m + a_1X^{m-1} + \cdots + a_m \; a_0 \neq 0 g(X) = b_0X^n + b_1X^{n-1} + \cdots b_n \; (b_0 \neq 0) \in K[X]$ に対して

$$\begin{pmatrix} a_0 & \cdots & 0 & b_0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & a_0 & 0 & 0 & b_0 \\ a_m & 0 & 0 & b_n & 0 & 0 \\ 0 & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & a_m & 0 & 0 & b_n \end{pmatrix}$$

を $f \times g$ のシルベスター行列と呼び、その行列式を f と g の終結式 (resultant) とよび、$R(f,g)$ で表す

証明　$f(X)$ と $g(X)$ が共通因子を持つ $\Leftrightarrow$
$^\exists h(X), t(X) \in K[X]$
$\deg h < \deg g$
$\deg t < \deg f$
$f(X)h(X) = g(X)t(X)$
$\Leftrightarrow$
$^\exists h(X) = C_0X^{n-1} + \cdots + C_{n-1} \neq 0$
$t(X) = d_0X^{m-1} + \cdots + d_{m-1} \neq 0$
$f(X)h(X) = g(X)t(X)$
$\Leftrightarrow$
$^\exists(C_0, \ldots, C_{n-1}, d_0, \ldots, d_{m-1}) \neq \vec{0}$ 共通因子を $s(X)$ とすると

$$\begin{array}{ll} a_0C_0 = b_0d_0 & X^{m+n-1}\text{の係数} \\ a_1C_0 + a_0C_1 = b_1d_0 & X^{m+n-2}\text{の係数} \\ a_2C_0 + a_1C_1 + a_0C_2 = b_2d_0 + b_1d_1 + b_0d_2 & X^{m+n-3}\text{の係数} \\ \vdots & \vdots \\ a_mC_{n-1} + a_{m-1}C_{n-1} = b_nd_{m-2} + b_{n-1}d_{m1} & X\text{ の係数} \\ a_mC_{n-1} = b_nd_{m-1} & X^0\text{の係数} \end{array}$$

定理 2.2

$R(f,g) \in \langle f(X), g(X) \rangle$
実は $R(f,g) = h(X)f(X) + t(X)g(X)$ $h(X), t(X)$ の係数は $a_0, \ldots, a_m, b_0, \ldots, b_n$ の整式 (整数係数多項式)

証明　$R(f,g) = 0$ なら $h(X) = t(X) = 0$ とおけばよい
$R(f,g) \neq 0$ とする。

$$\begin{pmatrix} a_0 & \cdots & 0 & b_0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & a_0 & 0 & 0 & b_0 \\ a_m & 0 & 0 & b_n & 0 & 0 \\ 0 & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & a_m & 0 & 0 & b_n \end{pmatrix} \begin{pmatrix} C_0 \\ \vdots \\ C_{n-1} \\ d_0 \\ \vdots \\ d_{n-1} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

の解 $(C_0, \ldots, C_{n-1}, d_0, \ldots, d_{m-1})$ に対し、
$h'(X) = C_0X^{n-1} + \cdots + C_{n-1}, t'(X) = d_0X^{m-1} + \cdots + d_{m-1}$ とおくと
$h'(X)f(X) + t'(X)g(X) = 1$ がなりたつことにほかならない
$R(f, g) \neq 0$ なので、解はただひとつ存在して、それは Clamer の公式によって
$C_i = \frac{1}{R(f,g)}$
よって、各 C_j, d_j に $R(f, g)$ をかけたものは、$a_0, \ldots, a_m, b_0 \ldots, b_n$ の整式になる

よって $\begin{array}{l} h(X) = h'(X)R(f, g) \\ t(X) = t'(X)R(, f, g) \end{array}$ とおけばよい