Resultant（終結式）

藤原俊朗

2011 年 8 月 26 日

1 Resultant（終結式）

二つの多項式 $f(x)$，$g(x)$ がそれぞれ n 次，m 次で，以下のように与えられているとする．

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \qquad a_n \neq 0, \tag{1}$$

$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0, \qquad b_m \neq 0. \tag{2}$$

このとき，以下のように f の係数を下へ行くにつれて一列ずつずらして m 行，g の係数も同様にずらして n 行並べた $m+n$ 次の正方行列の行列式で Resultant $R(f,g)$ を定義する．

$$R(f,g) = \begin{vmatrix} a_n & a_{n-1} & \dots & \dots & a_0 & & & \\ & a_n & a_{n-1} & \dots & a_1 & a_0 & & \\ & & a_n & \dots & & & & \\ & & & & \vdots & & & \\ & & & a_n & \dots & & a_1 & a_0 \\ b_m & b_{m-1} & \dots & \dots & b_0 & & & \\ & b_m & b_{m-1} & \dots & b_1 & b_0 & & \\ & & b_m & \dots & & & & \\ & & & & \vdots & & & \\ & & & b_m & \dots & & b_1 & b_0 \end{vmatrix}. \tag{3}$$

上で，係数で埋められていないところはゼロとする．

例 1　$f(x) = a_1 x + a_0$，$g(x) = b_2 x^2 + b_1 x + b_0$ のとき，

$$R(f,g) = \begin{vmatrix} a_1 & a_0 & \\ & a_1 & a_0 \\ b_2 & b_1 & b_0 \end{vmatrix}. \tag{4}$$

例 2　$f(x) = a_2 x^2 + a_1 x + a_0$，$g(x) = b_4 x^4 + b_3 x^3 + b_2 x^2 + b_1 x + b_0$ のとき，

$$R(f,g) = \begin{vmatrix} a_2 & a_1 & a_0 & & & \\ & a_2 & a_1 & a_0 & & \\ & & a_2 & a_1 & a_0 & \\ & & & a_2 & a_1 & a_0 \\ b_4 & b_3 & b_2 & b_1 & b_0 & \\ & b_4 & b_3 & b_2 & b_1 & b_0 \end{vmatrix}. \tag{5}$$

定理 1. 方程式 $f(x)=0$ と $g(x)=0$ が共通解を持つための必要十分条件は，$R(f,g)=0$ である．

これを示すために，まずは補題.

補題. 方程式 $f(x)=0$ と $g(x)=0$ が共通解を持つための必要十分条件は，$n-1$ 次以下の多項式 $F(x)$ と $m-1$ 次以下の多項式 $G(x)$ が存在して $fG+gF=0$ が成立する事である．

Proof. 方程式 $f=0$，$g=0$ に共通解があれば，それを解とする多項式 $h(x)$ で両者を割ることができる．すなわち，$f=hF$，$g=-hG$．これからただちに $fG+gF=0$ を得る．

逆に，$fG=-gF$ が成立したとする．このとき，右辺は g で割り切れるから，左辺の fG も g で割り切れなければならない．多項式 g を分解して $g=b_n\prod_k(x-\beta_k)$ としよう．定理の仮定より G は g より次数が小さいので，g の因数 $(x-\beta_k)$ の全てで G を割ることはできず，そのいくつかは f を割り切らねばならない．それらの β_k が f と g の共通解となる． □

この補題をふまえて，定理 1 の証明.

Proof. 上の補題の F と G をそれぞれ

$$F=\alpha_{n-1}x^{n-1}+\cdots+\alpha_1x+\alpha_0, \tag{6}$$
$$G=\beta_{m-1}x^{m-1}+\cdots+\beta_1x+\beta_0 \tag{7}$$

とする．$fG+gF=0$ をこれらで書き下すと，

$$\begin{aligned} fG+gF &= (\beta_{m-1}a_n+\alpha_{n-1}b_m)x^{n+m-1} \\ &\quad +\dots \\ &\quad +\Big((\beta_1a_0+\beta_0a_1)+(\alpha_0b_1+\alpha_1b_0)\Big)x \\ &\quad +\beta_0a_0+\alpha_0b_0 \\ &= 0. \end{aligned}$$

右辺で x の各次の係数がゼロであることを行列で書くと，

$$(\beta_{m-1},\dots,\beta_1,\beta_0,\alpha_{n-1},\dots,\alpha_1,\alpha_0)\begin{pmatrix} a_n & a_{n-1} & \dots & \dots & a_0 & & & \\ & a_n & a_{n-1} & \dots & a_1 & a_0 & & \\ & & a_n & \dots & & & & \\ & & & & \vdots & & & \\ & & & a_n & \dots & & a_1 & a_0 \\ b_m & b_{m-1} & \dots & \dots & b_0 & & & \\ & b_m & b_{m-1} & \dots & b_1 & b_0 & & \\ & & b_m & \dots & & & & \\ & & & & \vdots & & & \\ & & & b_m & \dots & & b_1 & b_0 \end{pmatrix}=0. \tag{8}$$

ベクトル $(\beta_{m-1},\dots,\beta_1,\beta_0,\alpha_{n-1},\dots,\alpha_1,\alpha_0)\neq 0$ が存在するための必要十分条件は，$R=0$ である． □

定理 2. $n-1$ 次以下の多項式 F と $m-1$ 次以下の多項式が存在して，$fG+gF=R$.

Proof. 関数 $f=a_nx^n+\cdots+a_1x+a_0$ に順次 x^{m-1}，x^{m-2}，... x, 1 をかけたものと，$g=b_mx^m+\cdots+b_1x+b_0$ に順次 x^{n-1}，x^{n-2}，... x, 1 をかけたものを順に並べて，行列の形に書くと，

$$\begin{pmatrix} x^{m-1}f \\ x^{m-2}f \\ \vdots \\ xf \\ f \\ x^{n-1}g \\ x^{n-2}g \\ \vdots \\ x^g \\ g \end{pmatrix} = \begin{pmatrix} a_n & a_{n-1} & \dots & \dots & a_0 & & & \\ & a_n & a_{n-1} & \dots & a_1 & a_0 & & \\ & & a_n & \dots & & & & \\ & & & & \vdots & & & \\ & & & a_n & \dots & & a_1 & a_0 \\ b_m & b_{m-1} & \dots & \dots & b_0 & & & \\ & b_m & b_{m-1} & \dots & b_1 & b_0 & & \\ & & b_m & \dots & & & & \\ & & & & \vdots & & & \\ & & & b_m & \dots & & b_1 & b_0 \end{pmatrix} \begin{pmatrix} x^{m+n-1} \\ x^{m+n-2} \\ \vdots \\ \vdots \\ \\ \\ x^3 \\ x^2 \\ x \\ 1 \end{pmatrix}$$

を得る．右辺の左側の行列を M とし，その余行列を A とすると，${}^tAM=R$. 従って，

$${}^tA \begin{pmatrix} x^{m-1}f \\ x^{m-2}f \\ \vdots \\ xf \\ f \\ x^{n-1}g \\ x^{n-2}g \\ \vdots \\ x^g \\ g \end{pmatrix} = R \begin{pmatrix} x^{m+n-1} \\ x^{m+n-2} \\ \vdots \\ \vdots \\ \\ \\ x^3 \\ x^2 \\ x \\ 1 \end{pmatrix} \tag{9}$$

${}^tA$ の一番下の行を $(\beta_{m-1},\dots,\beta_1,\beta_0,\alpha_{n-1},\dots,\alpha_1,\alpha_0)$ と書くと，上の式は

$$\left(\beta_{m-1}x^{m-1}+\cdots+\beta_1x+\beta_0\right)f+\left(\alpha_{n-1}x^{n-1}+\cdots+\alpha_1x+\alpha_0\right)g=R.$$

□

2 Resultant は Eliminant

二変数以上の場合，Resultant は連立方程式から変数を消去するために用いることができる．今，二変数 x,y の多項式 $f(x,y)$，$g(x,y)$ が与えられたとき，たとえば x を変数，y を定数とみなして Resultant を計算する事が出来る．これを，変数を明記して，

$$\text{Resultant}(f,g,x)=R(y) \tag{10}$$

と書く．上記の定理によれば

$$f(x,y)G(x,y)+g(x,y)F(x,y)=R(y) \tag{11}$$

とする多項式 F と G が存在する．F，G が x の多項式であることは上で証明した．F，G，R が y の多項式でもあるのは，a_i，b_j が y の多項式であり，したがって ${}^tA$ の各要素が y の多項式であることからわかる．

式 (11) によれば，連立方程式 $f(x,y)=0$，$g(x,y)=0$ の解 (x,y) は $R(y)=0$ を満たさなければならない．こうして，連立方程式から x を消去することができた．このように変数の消去に使えることから Resultant を Eliminant とも言う [2].

3　コメント

以下の文献，および，それに記されている文献が参考になるだろう．ここに書かれていることは，全て文献 [1] で学んだことである．

ただし，文献 [1] での Resultant の定義とここでの定義では，符号が異なっている場合がある．ここでは式 (3) に書いたように，係数 a_k, b_k を降順に並べた行列の行列式として定義した．これは，Mathematica の Resultant の定義と一致する．文献 [1] では，逆に係数を昇順に並べたものの行列式として Resultant を定義している．

参考文献

[1] Robert J. Walker *Algebraic curves*, Springer-Verlag New York, 1978

[2] Wolram MathWorld の Resultant の項：http://mathworld.wolfram.com/Resultant.html

[3] Wolram MathWorld の Sylvester Matrix の項：http://mathworld.wolfram.com/SylvesterMatrix.html
Resultant はシルベスター行列の行列式として定義される．