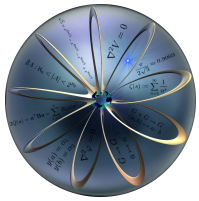

planetmath.org

Math for the people, by the people.

resultant (alternative treatment)

Canonical name	ResultantalternativeTreatment
Date of creation	2013-03-22 12:32:52
Last modified on	2013-03-22 12:32:52
Owner	Mathprof (13753)
Last modified by	Mathprof (13753)
Numerical id	6
Author	Mathprof (13753)
Entry type	Definition
Classification	msc 12E05
Related topic	Discriminant

Summary. The *resultant* of two polynomials is a number, calculated from the coefficients of those polynomials, that vanishes if and only if the two polynomials share a common root. Conversely, the resultant is non-zero if and only if the two polynomials are mutually prime.

Definition. Let $\mathbb{K}$ be a field and let

$$\begin{aligned} p(x) &= a_0 x^n + a_1 x^{n-1} + \ldots + a_n, \\ q(x) &= b_0 x^m + b_1 x^{m-1} + \ldots + b_m \end{aligned}$$

be two polynomials over $\mathbb{K}$ of degree n and m, respectively. We define $\mathrm{Res}[p, q] \in \mathbb{K}$, the resultant of $p(x)$ and $q(x)$, to be the determinant of a $n + m$ square matrix with columns 1 to m formed by shifted sequences consisting of the coefficients of $p(x)$, and columns $m + 1$ to $n + m$ formed by shifted sequences consisting of coefficients of $q(x)$, i.e.

$$\mathrm{Res}[p, q] = \begin{vmatrix} a_0 & 0 & \ldots & 0 & b_0 & 0 & \ldots & 0 \\ a_1 & a_0 & \ldots & 0 & b_1 & b_0 & \ldots & 0 \\ a_2 & a_1 & \ldots & 0 & b_2 & b_1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & a_{n-1} & 0 & 0 & \ldots & b_{m-1} \\ 0 & 0 & \ldots & a_n & 0 & 0 & \ldots & b_m \end{vmatrix}$$

Proposition 1 *The resultant of two polynomials is non-zero if and only if the polynomials are relatively prime.*

Proof. Let $p(x), q(x) \in \mathbb{K}[x]$ be two arbitrary polynomials of degree n and m, respectively. The polynomials are relatively prime if and only if every polynomial — including the unit polynomial 1 — can be formed as a linear combination of $p(x)$ and $q(x)$. Let

$$\begin{aligned} r(x) &= c_0 x^{m-1} + c_1 x^{m-2} + \ldots + c_{m-1}, \\ s(x) &= d_0 x^{n-1} + b_1 x^{n-2} + \ldots + d_{n-1} \end{aligned}$$

be polynomials of degree $m - 1$ and $n - 1$, respectively. The coefficients of the linear combination $r(x)p(x) + s(x)q(x)$ are given by the following matrix–vector multiplication:

$$\begin{bmatrix} a_0 & 0 & \dots & 0 & b_0 & 0 & \dots & 0 \\ a_1 & a_0 & \dots & 0 & b_1 & b_0 & \dots & 0 \\ a_2 & a_1 & \dots & 0 & b_2 & b_1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a_{n-1} & 0 & 0 & \dots & b_{m-1} \\ 0 & 0 & \dots & a_n & 0 & 0 & \dots & b_m \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ \vdots \\ c_{m-1} \\ d_0 \\ d_1 \\ d_2 \\ \vdots \\ d_{n-1} \end{bmatrix}$$

In consequence of the preceding remarks, $p(x)$ and $q(x)$ are relatively prime if and only if the matrix above is non-singular, i.e. the resultant is non-vanishing. Q.E.D.

Alternative Characterization. The following Proposition describes the resultant of two polynomials in terms of the polynomials' roots. Indeed this property uniquely characterizes the resultant, as can be seen by carefully studying the appended proof.

Proposition 2 *Let $p(x), q(x)$ be as above and let $x_1, \dots, x_n$ and $y_1, \dots, y_m$ be their respective roots in the algebraic closure of $\mathbb{K}$. Then,*

$$\text{Res}[p, q] = a_0^m \, b_0^n \prod_{i=1}^{n} \prod_{j=1}^{m} (x_i - y_j)$$

Proof. The multilinearity property of determinants implies that

$$\text{Res}[p, q] = a_0^m \, b_0^n \begin{vmatrix} 1 & 0 & \dots & 0 & 1 & 0 & \dots & 0 \\ A_1 & 1 & \dots & 0 & B_1 & 1 & \dots & 0 \\ A_2 & A_1 & \dots & 0 & B_2 & B_1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & A_{n-1} & 0 & 0 & \dots & B_{m-1} \\ 0 & 0 & \dots & A_n & 0 & 0 & \dots & B_m \end{vmatrix}$$

where

$$A_i = \frac{a_i}{a_0}, \quad i = 1, \ldots n,$$
$$B_j = \frac{b_j}{b_0}, \quad j = 1, \ldots m.$$

It therefore suffices to prove the proposition for monic polynomials. Without loss of generality we can also assume that the roots in question are algebraically independent.

Thus, let $X_1, \ldots, X_n, Y_1, \ldots, Y_m$ be indeterminates and set

$$\begin{aligned} F(X_1, \ldots, X_n, Y_1, \ldots, Y_m) &= \prod_{i=1}^{n} \prod_{j=1}^{m} (X_i - Y_j) \\ P(x) &= (x - X_1) \ldots (x - X_n), \\ Q(x) &= (x - Y_1) \ldots (x - Y_m), \\ G(X_1, \ldots, X_n, Y_1, \ldots, Y_m) &= \mathrm{Res}[P, Q] \end{aligned}$$

Now by Proposition 1, G vanishes if we replace any of the $Y_1, \ldots, Y_m$ by any of $X_1, \ldots, X_n$ and hence F divides G.

Next, consider the main diagonal of the matrix whose determinant gives $\mathrm{Res}[P, Q]$. The first m entries of the diagonal are equal to 1, and the next n entries are equal to $(-1)^m Y_1 \ldots Y_m$. It follows that the expansion of G contains a term of the form $(-1)^{mn} Y_1^n \ldots Y_m^n$. However, the expansion of F contains exactly the same term, and therefore $F = G$. Q.E.D.