Resultant and discriminant

1 Resultant

Definition

The *resultant* $R(f,g)$ of two polynomials $f(x) = a_0x^n + ... + a_n$ and $g(x) = b_0x^m + ... + b_m$ with $a_0b_0 \neq 0$ is defined as

$$R(f,g) = a_0^m b_0^n \prod_{i,j}(\alpha_i - \beta_j)$$

where the α_i are the roots of $f(x)$ and the β_j those of $g(x)$.

Application

A trivial but useful observation is that if f and g are monic,

$$\prod_{\alpha \text{ root of } f} g(\alpha) = (-1)^{mn} \prod_{\beta \text{ root of } g} f(\beta)$$

(since $f(x) = \prod_\alpha (x-\alpha)$ and $g(x) = \prod_\beta (x-\beta)$ so that both sides are equal to $R(f,g)$).

For example,

$$\prod_{\zeta^n=1} (\zeta^2 - 2) = (\sqrt{2}^n - 1)((-\sqrt{2})^n - 1).$$

Properties

From the definition it is clear that $R(f,g) = 0$ if and only if f and g have a common root.

Since $R(f,g)$ is a symmetric function of the roots of f and g, it can be expressed in terms of the coefficients. The expression is the following determinant

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

of order $m+n$ (with m rows containing coefficients of f and n rows containing coefficients of g).

Proof One has $R(f,g)=0$ if and only if f and g have a common root, that is, if and only if f and g have nontrivial g.c.d., that is, if and only if there are polynomials $r(x)$ and $s(x)$ of degrees not more than $m-1$ and $n-1$, respectively, such that $r(x)f(x)+s(x)g(x)=0$. Considering the $m+n$ coefficients of $r(x)$ and $s(x)$ as unknowns, this equation gives $m+n$ homogeneous equations in $m+n$ unknowns, with nontrivial solution iff the determinant vanishes. But both this determinant and $R(f,g)$ are expressions of degree m in the a_i and n in the b_j. So, this determinant must equal $R(f,g)$ up to a constant, and looking at the coefficient of $a_0^m b_m^n$ shows that the constant is 1. □

If $a_0 b_0 = 0$ we can take this determinant as the definition of $R(f,g)$. Now $R(f,g) = a_0 R(f,\bar{g})$ if $b_0 = 0$, where $\bar{g}(x)$ is the polynomial of degree $m-1$ with $g(x) = \bar{g}(x)$, and similar for $a_0 = 0$. In particular, if $a_0 = b_0 = 0$ then $R(f,g) = 0$. This is natural if one passes to homogeneous polynomials $F(X,Y) = \sum a_i X^{n-i} Y^i$ and $G(X,Y) = \sum b_i X^{n-i} Y^i$. Now $R(f,g) = 0$ expresses that the varieties $V(F)$ and $V(G)$ on the projective line have a common point, and when $a_0 = b_0 = 0$ this common point is $(1,0)$.

Exercise The resultant $R(f(x), g(t-x))$ is a polynomial of degree mn in the variable t, with the mn roots $\alpha_i + \beta_j$.

Exercise The resultant $R(f,g)$ viewed as a polynomial in the coefficients a_i and b_j is homogeneous of degree mn if the variables a_i and b_i are taken to have weight i.

Exercise There exist polynomials $r(x)$ and $s(x)$ of degrees not more than $m-1$ and $n-1$, respectively, and with coefficients that are polynomials with integral coefficients in the a_i and b_j, such that $r(x)f(x)+s(x)g(x) = R(f,g)$.

(Hint: Solve $Ay = b$ with Cramer's rule, where A is the matrix with $\det A = R(f,g)$, and y is the column vector $(x^{n+m-1}, ..., 1)$, and b is the column vector $(x^{m-1}f(x), ..., f(x), x^{n-1}g(x), ..., g(x))$.)

2 Discriminant

The *discriminant* D of a polynomial $f(x)$ as above is defined as

$$D = a_0^{2n-2}(-1)^{n(n-1)/2} \prod_{i \neq j} (\alpha_i - \alpha_j) = a_0^{2n-2} \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

We have $R(f,f') = (-1)^{n(n-1)/2} a_0 D$.

Indeed, from $f(x) = a_0 \prod_i (x-\alpha_i)$ we get $f'(x) = a_0 \sum_j \prod_{i\neq j}(x-\alpha_i)$ so that $f'(\alpha_j) = a_0 \prod_{i\neq j}(\alpha_j - \alpha_i)$ and $R(f,f') = a_0^{n-1} \prod_i f'(\alpha_i) = a_0^{2n-1} \prod_{i\neq j}(\alpha_j - \alpha_i)$.

Example For $f(x) = ax^2+bx+c$ and $f'(x) = 2ax+b$ we find

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

so that $D = b^2 - 4ac$.

Example For $f(x) = x^3 + bx + c$ and $f'(x) = 3x^2 + b$ we find

$$R(f, f') = \begin{vmatrix} 1 & 0 & b & c & 0 \\ 0 & 1 & 0 & b & c \\ 3 & 0 & b & 0 & 0 \\ 0 & 3 & 0 & b & 0 \\ 0 & 0 & 3 & 0 & b \end{vmatrix} = 4b^3 + 27c^2$$

so that $D = -4b^3 - 27c^2$.

3 Intersection multiplicity

Given two curves $f(x, y) = 0$ and $g(x, y) = 0$ without common component, we want to assign intersection multiplicities to their common points in such a way that Bezout's theorem holds. Let f and g have degrees n and m, respectively, and choose coordinates in such a way that these curves do not pass through the origin $(0, 0)$, and such that the origin does not lie on a line joining two intersection points of the curves. Write the equations homogeneously: $F(X, Y, Z) = 0$ and $G(X, Y, Z) = 0$, and consider F and G as polynomials in Z with coefficients in $k[X, Y]$. Our assumptions imply that F and G are polynomials of degrees n and m in Z with coefficients A_i and B_i that are homogeneous polynomials of degree i in X and Y. Now $R(F, G)$ is a homogeneous polynomial of total degree mn in X and Y, call it $R(X, Y)$, and we can define the intersection multiplicity of the curves $F = 0$ and $G = 0$ at $P = (X_0, Y_0, Z_0)$ to be the multiplicity of the root (X_0, Y_0) of $R(X, Y)$. (Remains of course to check that this definition does not depend on the choices made.) With this definition Bezout's theorem becomes the simple statement that the sum of the multiplicities of the roots of a polynomial equals the degree of that polynomial.

Example Consider the two curves $Y = X^3$ and $Y = X^5$. The homogeneous equations are $YZ^2 = X^3$ and $YZ^4 = X^5$, and the common points are the points $(0, 0, 1)$, $(1, 1, 1)$, $(-1, -1, 1)$, $(0, 1, 0)$. The point $(1, 0, 0)$ does not lie on a line joining two common points, so make this the origin by interchanging X and Z. Now our polynomials are $F(X, Y, Z) = Z^3 - X^2Y$ and $G(X, Y, Z) = Z^5 - X^4Y$, and computing a determinant of order 8 we find $R(X, Y) = X^{10}Y^3(Y^2 - X^2)$ with roots $(0, 1)$, $(1, 0)$, $(1, 1)$, $(1, -1)$ of multiplicities 10, 3, 1, 1, so that our two curves have intersection multiplicities 10, 3, 1, 1 at the points $(0, 1, 0)$, $(0, 0, 1)$, $(1, 1, 1)$, $(-1, -1, 1)$.