Resultants

Let $f(x), g(x)$ be polynomials of degree n and m respectively with coefficients from a field F. Note that these polynomials have a common factor of degree greater than zero if and only if there is a polynomial of degree less than $m+n$ which is a multiple of each. Another way to state this condition is to observe that this occurs if and only if the the vector space of multiples of $f(x)$ of degree less than $m+n$ has nonzero intersection with the vector space of multiples of $g(x)$ of degree less than $m+n$, or equivalently that the vectors $f(x), xf(x), x^2f(x), \ldots, x^{m-1}f(x)$ and $g(x), xg(x), x^2g(x), \ldots, x^{n-1}g(x)$ are dependent in the vector space of polynomials of degree at most $m+n$. Using the basis of powers of x we have shown the following.

Proposition: Polynomials $f(x) = v_0x^n + \cdots + v_n,\ g(x) = w_0x^m + \cdots + w_m$ in $F[x]$ have a common factor of degree greater than zero if and only if the $m+n$ by $m+n$ matrix

$$\begin{pmatrix}
v_0 & v_1 & v_2 & \cdots & v_n & 0 & 0 & \cdots & 0 & 0 & 0 \\
0 & v_0 & v_1 & v_2 & \cdots & v_n & 0 & 0 & \cdots & 0 & 0 \\
0 & 0 & v_0 & v_1 & v_2 & \cdots & v_n & 0 & 0 & \cdots & 0 \\
 & & & \cdots & & & & & & & \\
0 & 0 & 0 & 0 & 0 & 0 & v_0 & v_1 & v_2 & \cdots & v_n \\
w_0 & w_1 & w_2 & \cdots & w_n & 0 & 0 & \cdots & 0 & 0 & 0 \\
0 & w_0 & w_1 & w_2 & \cdots & w_n & 0 & 0 & \cdots & 0 & 0 \\
0 & 0 & w_0 & w_1 & w_2 & \cdots & w_m & 0 & 0 & \cdots & 0 \\
 & & & \cdots & & & & & & & \\
0 & 0 & 0 & 0 & 0 & 0 & w_0 & w_1 & w_2 & \cdots & w_m
\end{pmatrix}$$

has determinant 0.

Proof: The rows of this matrix are the coordinates of the vectors $x^if(x), x^jg(x)$ in terms of the basis of powers of x. Hence these vectors are dependent if and only if the determinant vanishes.

We define the determinant above to be the resultant of the polynomials, written as $\mathrm{Res}(f, g)$.

Example 1: Let R be the unique factorization domain of polynomials in indeterminates v_0, w_0, t_i, u_j and let

$$f(x) = v_0 \prod_{i=1}^{n} (x - t_i) = v_0x^n + \cdots + v_n,$$

$$g(x) = w_0 \prod_{i=1}^{m} (x - u_j) = w_0 x^m + \cdots + w_m.$$

Let F be the fraction field of R. Then $\mathrm{Res}(f, g)$ is clearly an element of the ring $R = \mathbf{Z}[v_0, w_0, t_1, \ldots, t_n, u_1, \ldots, u_m]$ which is divisible by $v_0^m w_0^n$ and is homogeneous of degree m in $(v_0, \ldots, v_n)$ and of degree n in $(w_0, \ldots, w_m)$ (that is replacing each v_j by λv_j changes the resultant by λ^m, as the definition via the determinant shows).

Lemma: Let $p(x_1, \ldots, x_k, x)$ be a polynomial in indeterminates x_i, x with integral coefficients such that $p(x_i) = 0$. Then

$$p(x_1, \ldots, x_k, x) = (x - x_i) q(x_1, \ldots, x_k, x)$$

for some polynomial $q(x_1, \ldots, x_k, x)$ with integral coefficients.

Proof: Consider p as a polynomial in x with coefficients in the fraction field of the unique factorization domain $\mathbf{Z}[x_1, \ldots, x_k]$. By the division algorithm, if $x = x_i$ is a root, then $(x - x_i)$ divides p in the ring of polynomials with coefficients in the fraction field. By the Gauss lemma, this factorization must have coefficients in the unique factorization domain itself, establishing the lemma.

Applying the lemma to the example above, we conclude that in this case we have that $\mathrm{Res}(f, g)$ is divisible by $v_0^m w_0^n \prod_{i,j} (t_i - u_j)$. Further this product equals $v_0^m \prod_{i=1}^n g(t_i) = (-1)^{nm} w_0^n \prod_{j=1}^m f(u_j)$. Since both $\mathrm{Res}(f, g)$ and the products have the same homogeneity properties, they are constant multiples of each other. The product of the diagonal elements in the matrix is $v_0^m w_m^n$, which must then be a term in the resultant polynomial in w_i, v_j. Since $v_0^m \prod_{i=1}^n g(t_i)$ clearly has $v_0^m w_m^n$ as a summand (stemming from the constant term of the polynomial g) we have the formula

$$\mathrm{Res}(f, g) = v_0^m w_0^n \prod_{i,j} (t_i - u_j)$$

Example 2: Recall that the discriminant $D(f)$ of a polynomial $f(x) = v_0(x - t_1) \cdots (x - t_n)$ is defined to be $v_0^{2n-2} \prod_{i<j} (t_i - t_j)^2$. The previous example (with $g = f'$, noting that $f'(t_i) = \prod_{1=1, i \neq j}^n (t_i - t_j)$) shows that $\mathrm{Res}(f, f') = (-1)^{n(n-1)/2} D(f)$.

Postscript

We will also have use of the Vandermonde determinant:

$$\det \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ x_1 & x_2 & x_3 & \ldots & x_n \\ x_1^2 & x_2^2 & x_3^2 & \ldots & x_n^2 \\ & & \ldots & & \\ x_1^{n-1} & x_2^{n-1} & x_3^{n-1} & \ldots & x_n^{n-1} \end{pmatrix} = \prod_{i>j} (x_i - x_j)$$

which is easily proved by observing that the lemma above implies that the right hand side divides the left, and that the determinant has the term $x_2 x_3^2 x_4^3 \cdots x_n^{n-1}$ as a summand

of highest weight when the x_i are weighted by their indices. The right hand side of the product also contains this term (which is why the product is written with the index $i > j$ in $(x_i - x_j)$), so the two terms are equal by comparing total degrees.