Resultants

Damien Robert

1 Definition

Let A be a domain, $K = \mathrm{Frac}(A)$.

Lemma 1.1. *If $M : A^n \to A^n$ is a matrix, then M is injective iff $\det M \neq 0$.*
We have $M \operatorname{co} M = \det M$ so $\Im M \supset \det M A^n$.

Definition 1.2. Let f and g be two polynomials in $A[x]$, f of degree ℓ and g of degree m. We define the linear application $\mu : A[x]_{m-1} \oplus A[x]_{l-1} \to A[x]_{l+m-1}$, $(C, D) \mapsto Cf + Dg$. Here $A[x]_n$ denotes the polynomials of degree at most n.
Then the resultant $\mathrm{Res}(f, g)$ is $\mathrm{Res}(f, g) = \det \mu$.

Theorem 1.3. $\mathrm{Res}(f, g) = 0$ *iff μ is not injective iff there exists C, D, $\deg C \leq m-1, \deg D \leq \ell - 1$ such that $Cf + Dg = 0$, iff $\gcd(f, g) \in K[X]$ is non trivial, iff there is a common root in the algebraic closure $\overline{K}$ of K.*

Note: since $\Im \mu \supset \mathrm{Res}(f, g)$, there exists C, D such that $\mathrm{Res}(f, g) = Cf + Dg$.

2 Computing the resultant and properties

Let $\mathrm{Syl}(f, g)$ be the Sylvester matrix; this is the matrix of μ by taking a basis of the form $(x^n, x^{n-1}, \ldots 1)$ to represent $A[x]_n$.
For instance if $f = f_2 x^2 + f_1 x + f_0$, $g = g_3 x^3 + g_2 x^2 + g_1 x + g_0$, then

$$\mathrm{Syl}(f, g) = \begin{pmatrix} f_2 & 0 & 0 & g_3 & 0 \\ f_1 & f_2 & 0 & g_2 & g_3 \\ f_0 & f_1 & f_2 & g_1 & g_2 \\ 0 & f_0 & f_1 & g_0 & g_1 \\ 0 & 0 & f_0 & 0 & g_0 \end{pmatrix}$$

Proposition 2.1.

- $\mathrm{Res}(f, g) = (-1)^{\ell m} \mathrm{Res}(g, f)$
- *If $m \geq \ell$, $\mathrm{Res}(f, g) = f_\ell^{m-d} \mathrm{Res}(f, g \mod f)$ where d is the degree of $g \mod f$.*

- $\mathrm{Res}(f, g_1 g_2) = \mathrm{Res}(f, g_1)\,\mathrm{Res}(f, g_2)$.
- $\mathrm{Res}(x-a, x-b) = a-b$.
- *So if* $f = f_l \prod(x-a_i)$ *and* $g = g_m \prod(x-b_j)$, $\mathrm{Res}(f,g) = f_l^m g_m^l \prod(a_i - b_j) = (-1)^{\ell m} g_m^\ell \prod f(b_j) = f_l^m \prod g(a_i)$.

Corollary 2.2. *If* $P(x) = \prod(x-a_i)$ *is a unitary polynomial with roots* $a_1, \dots, a_n$, *and* Q *is a polynomial, then we can construct the polynomial* P_1 *with roots* $Q(a_1), \dots, Q(a_n)$ *as* $P_1(y) = \mathrm{Res}_x(P(x), y - Q(x))$. *So* P_1 *can be computed over* A *without knowing the roots of* P.

In particular, if $\chi_M(X)$ *is the characteristic polynomial of a matrix* M, $\chi_{Q(M)}(Y) = \mathrm{Res}_X(\chi_M(X), Y - Q(X))$.

Proof. Let $g = y - Q(x)$, then by Proposition 2.1, $\mathrm{Res}_x(P(x), y - Q(x) = \prod g(a_i) = \prod y - Q(a_i)$. □

Remark 2.3. The resultant can also be used to compute the minimal polynomial of $\alpha+\beta$ and of $\alpha\beta$ if we know the minimal polynomial of α and the one of β.

Definition 2.4 (discriminant)**.** Discriminant of a polynomial of degree d: $\mathrm{Disc}(P) = (-1)^{d(d-1)/2}\,\mathrm{Res}(P, P')$.

Lemma 2.5. *If* P *unitary polynomial of degree* d, $\mathrm{Disc}(P) = \prod_{i<j}(a_i - a_j)^2 = (-1)^{d(d-1)/2} \prod_{i\neq j}(a_i - a_j)$.

So $\mathrm{Disc}\, P = 0$ *iff* P *ha a multiple root over* $\overline{K}$ *iff the factorisation of* P *in* $K[X]$ *has multiple factors.*

Example 2.6. $\mathrm{Disc}(aX^2 + bX + c) = b^2 - 4ac$.

3 Using the resultant to find common roots

Let $f = x^3 + 2y^3 - 3$, $g = x^2 + xy + y^3 - 3$. We want to find all the points of intersection over $\mathbb{C}$.

We can see f and g as elements of $\mathbb{C}[y][x]$. Since $\mathbb{C}[y]$ is a domain we can apply the results above.

The resultant, with respect to x, $\mathrm{Res}_x(f,g)$ is then an element of $\mathbb{C}[y]$. Since the resultant R is a linear polynomial combination $R = Cf + Dg$ of f and g, then if (a,b) is a common root of f and g, we have $\mathrm{Res}_x(f,g)(a,b) = \mathrm{Res}_x(f,g)(b) = 0$.

Thus we can search for b such that $\mathrm{Res}_x(f,g)(b) = 0$, and for these b find the correspondings a.

Warning: implicitly when we write $\mathrm{Res}(f,g)$ we should write $\mathrm{Res}_{\ell,m}(f,g)$ since ℓ and m determines the size of the Sylvester matrix. We have $\mathrm{Res}_{x,\ell,m}(f,g)(b) = \mathrm{Res}_{x,\ell,m}(f(x,b), g(x,b))$. So, **if** $f(x,b)$ **is still of degree** ℓ **and** $g(x,b)$ **still of degree** m, we have $\mathrm{Res}_{x,\ell,m}(f(x,b), g(x,b)) = \mathrm{Res}_x(f(x,b), g(x,b))$. By Theorem 1.3, this is zero whenever there is a common root a in $\overline{K}$ of $f(x,b)$ and $g(x,b)$. So in this case we know that the root b of $\mathrm{Res}_x(f,g)$ always correspond to a common root (a,b) of f and g over $\overline{K}$.

But if b is such that $f(x,b)$ and $g(x,b)$ have their leading term becoming zero (meaning that their degrees in x drops), then we always have $\mathrm{Res}_x(f,g)(b) = \mathrm{Res}_{x,\ell,m}(f(b), g(b)) = 0$ even if $\mathrm{Res}_x(f(x,b), g(x,b)) \neq 0$, because we are computing a Sylvester matrix for degrees ℓ and m bigger than the ones of $f(x,b)$ and $g(x,b)$. In this case, this root b of $\mathrm{Res}_x(f,g)$ may not correspond to a common root (a,b) of f and g over $\overline{K}$.

In summary: roots b of $\mathrm{Res}_x(f,g)(y) = 0$ correspond either to common roots (a,b) of f and g or to a drop of degree of $f(x,b)$ and $g(x,b)$ with respect to x.

Example 3.1. Let $f(x,y) = xy - 1, g(x,y) = y^2x$, then the resultant with respec to x is y^2, but $y = 0$ does not corresponds to a common root (x,y) of f and g, instead it corresponds to a drop of degree.