More facts about the resultant over a UFD

rapha • 17 May 2025

For this post, let A be a unique factorization domain (UFD).

Let f and g be two polynomials in $A[x]$ of degrees n and m respectively. Writing $\mathcal{P}_n$ for the A-module of polynomials in $A[x]$ having degree strictly less than n, we define the linear map

$$S : \mathcal{P}_m \times \mathcal{P}_n \to \mathcal{P}_{n+m}$$

by the equation

$$S(q, p) = qf + pg.$$

For $\mathcal{P}_m \times \mathcal{P}_n$, we may choose the ordered basis

$$(1, 0), (x, 0), \ldots, (x^{m-1}, 0), (0, 1), (0, x), \ldots, (0, x^{n-1})$$

while for $\mathcal{P}_{n+m}$ we may choose

$$1, x, x^2, \ldots, x^{n+m-1}.$$

In these bases, the map S has a matrix representation that is called the *Sylvester matrix* of f and g. Now you can look elsewhere on the Internet to find what this matrix looks like. Here's an example of what it looks like when $f = a_0 + a_1x + a_2x^2 + a_3x^3$ and $g = b_0 + b_1x + b_2x^2$:

$$\begin{pmatrix} a_0 & 0 & b_0 & 0 & 0 \\ a_1 & a_0 & b_1 & b_0 & 0 \\ a_2 & a_1 & b_2 & b_1 & b_0 \\ a_3 & a_2 & 0 & b_2 & b_1 \\ 0 & a_3 & 0 & 0 & b_2 \end{pmatrix}$$

Very nice. Obviously always a square $n + m$ matrix.

Now the **resultant** of f and g, denoted $R(f, g)$, is defined to be the *determinant* of the Sylvester matrix, or equivalently the determinant of the linear map S. For a good guess at where all of this comes from, look at p.24 of Walker's *Algebraic Curves* (1991).

From now on, suppose f and g are non-constant polynomials (in particular they are both non-zero). The proof of the following lemma is simple and uses the fact A is a UFD:

Lemma 1. The polynomials f and g share a non-constant factor if and only if there exists two non-zero polynomials ϕ and ψ, with $\deg \phi < n$ and $\deg \psi < m$, such that $\psi f = \phi g$. ■

Corollary. The polynomials f and g share a non-constant factor if and only if $\ker S \neq 0$.

Proof. Suppose f and g share a non-constant factor. The previous lemma gives us such ϕ and ψ. Now clearly $S(\psi, -\phi) = 0$, hence $(\psi, -\phi) \neq 0$ is in the kernel. Conversely, suppose there exists some non-zero tuple (q, p) in the kernel of S. If we had $p = 0$, then we would have $S(q, p) = qf = 0$, whence $f = 0$ because q is not zero and A is an integral domain. Similarily, it is impossible that q is zero. Therefore both q and p are non-zero polynomials, with $\deg p < n$ and $\deg q < m$. They are in the kernel of S, so $qf + pg = 0$. We win by applying the previous lemma with $\phi = -p$ and $\psi = q$. ■

We will need the following technical result:

Lemma 2. Let M be any square matrix with coefficients lying in an integral domain D. Then $\det M = 0$ if and only if there exists some non-zero vector in the kernel of M. Said differently, an endomorphism on a free D-module has zero determinant if and only if it kills some non-zero vector.[1]

Proof. Suppose we are given a non-zero vector v in the kernel of M. The equation $Mv = 0$ also holds in K, where K is the fraction field of D. Because K is a field, we obtain that the determinant of M over K is zero. This determinant is an algebraic expression in terms of elements of D only, so it is zero in D as well. Conversely, suppose $\det M = 0$. Again, seeing this as a fact in the field K, we know there must exists some non-zero vector v in the kernel of M over K, i.e. the vector v has coefficients in K. This is no problem since we can simply clear the denominators of each component by multiplying by an appropriate element $d \in D$. Then dv is a vector with components in D. Moreover, $Mdv = dMv = 0$ in K, whence $Mdv = 0$ in D. This shows dv is a non-zero element in the kernel of M. ■

By combining everything we have, we obtain this really useful theorem:

Theorem. Two non-constant polynomials f and g with coefficients in a unique factorization domain share a non-constant factor if and only if their resultant is zero.

Proof. The polynomials f and g share such a factor if and only if $\ker S \neq 0$ (by the corollary), if and only if $\det S = 0$ (by the previous lemma). ■

1. Here’s an example where the lemma fails if the ring is not an integral domain: consider the ring of dual numbers $\mathbb{R}[\varepsilon]/(\varepsilon^2)$, and consider the two-by-two diagonal matrix with the infinitesimal ε on the diagonal. Then its determinant is zero, but its kernel is trivial.↩