

# The Sylvester Matrix and Resultants

November 7, 2007

Our goal here is to describe another object we can use for analyzing curves. In particular, resultants will give us another method for implicitizing parametrically defined curves, but will have applications beyond this.

However, in preparation for this, let's consider the problem of deciding when two polynomials share a common nonconstant factor. First, let's make the concept of an irreducible polynomial more concrete:

**Definition 1** *Let  $k$  be a field. A polynomial  $f \in k[x_1, \dots, x_n]$  is irreducible over  $k$  if it is nonconstant and is not the product of two nonconstant polynomials in  $k[x_1, \dots, x_n]$ .*

The following is a simple result of this definition.

**Proposition 1** *Every nonconstant polynomial  $f \in k[x_1, \dots, x_n]$  can be written as a product of polynomials which are irreducible over  $k$ .*

The proof of this is not too difficult. We can show this by induction on the total degree of  $f$ . If  $f$  is irreducible, then we are done. Otherwise, it is the product of two nonconstant polynomials, each of lower total degree than  $f$ . If these polynomials are irreducible, we are done, otherwise repeat this process. Since  $f$  has finite degree, and the total degree of each divisor is strictly less than  $f$ , this process must end in a finite number of steps.

**Proposition 2** *Let  $f \in k[x_1, \dots, x_n]$  be irreducible over  $k$  and suppose that  $f$  divides the product  $gh$ , for  $g, h \in k[x_1, \dots, x_n]$ . Then  $f$  divides either  $g$  or  $h$ .*

The proof of this is quite difficult. However, you can probably convince yourself that this is true by analogy with the integers, and prime numbers being their irreducibles. The idea is similar, but the details of the proof are quite bit more involved.

The following proposition will give us an alternate description of irreducible and reducible polynomials, at least in the one-dimensional case.

**Proposition 3** *Let  $f, g \in k[x]$  be polynomials of degree  $l > 0$  and  $m > 0$ , respectively. Then  $f$  and  $g$  have a common factor if and only if there are polynomials  $A, B \in k[x]$  such that*

- (i)  $A$  and  $B$  are not both zero,
- (ii)  $A$  has degree at most  $m - 1$  and  $B$  has degree at most  $l - 1$ ,
- (iii)  $Af + Bg = 0$ .

The proof of this is not difficult, but a little tricky. You may want to find a proof of this, or you can just convince yourself of this fact by analogy with the integers.

This theorem gives us an answer for when two polynomials share a common factor, though it is usually not that simple to find polynomials  $A$  and  $B$ . But we can use the fact that these will exist to analyze this further.

Assuming that such an  $A$  and  $B$  exist, write them as

$$\begin{aligned} A &= c_0x^{m-1} + \cdots + c_{m-1} \\ B &= d_0x^{l-1} + \cdots + c_{l-1} \end{aligned}$$

Now consider the  $l + m$  coefficients  $c_0, \dots, c_{m-1}, d_0, \dots, d_{l-1}$  as unknown variables. Then we want to find  $c_i, d_j \in k$  such that  $Af + Bg = 0$ , as in the proposition.

Write  $f$  and  $g$  in a similar form, as

$$\begin{aligned} f &= a_0x^l + \cdots + a_l \\ g &= b_0x^m + \cdots + b_m \end{aligned}$$

where  $a_i, b_j \in k$ . Plugging in our expressions for  $A, B, f, g$  into the equation  $Af + Bg = 0$  will give us a pretty huge equation that is identically zero, so we can just consider the coefficient of each monomial  $x^p$  separately. Since the entire equation is zero for any  $x$ , we must have that the coefficient of each  $x^j$  is zero. Therefore, we have the following equations:

$$\begin{array}{rclcl} a_0c_0 & + & b_0d_0 & = & 0 & \text{coefficient of } x^{l+m-1} \\ a_1c_0 + a_0c_1 & + & b_1d_0 + b_0d_1 & = & 0 & \text{coefficient of } x^{l+m-2} \\ & \ddots & & & \vdots & \\ & & a_l c_{m-1} & + & b_m d_{l-1} & = 0 & \text{coefficient of } x^0 \end{array}$$

Now we have a linear system of  $l + m$  equations and  $l + m$  unknowns, so we know there is a nonzero solution if and only if the coefficient matrix has zero determinant. This will lead us to define the following objects:

**Definition 2** Given polynomials  $f, g \in k[x]$  of positive degree, write them in the form

$$\begin{aligned} f &= a_0x^l + \cdots + a_l, & a_0 \neq 0 \\ g &= b_0x^m + \cdots + b_m, & b_0 \neq 0. \end{aligned}$$

Then the Sylvester matrix of  $f$  and  $g$  with respect to  $x$ , denoted by  $\text{Syl}(f, g, x)$ , is the coefficient matrix of the system of equations given above. Thus  $\text{Syl}(f, g, x)$  is the following  $(l+m) \times (l+m)$  matrix:

$$\text{Syl}(f, g, x) = \begin{pmatrix} a_0 & 0 & \cdots & 0 & b_0 & 0 & \cdots & 0 \\ a_1 & a_0 & \ddots & \vdots & b_1 & b_0 & \ddots & \vdots \\ a_2 & a_1 & \ddots & 0 & b_2 & b_1 & \ddots & 0 \\ \vdots & & \ddots & a_0 & \vdots & & \ddots & b_0 \\ & \vdots & & a_1 & & \vdots & & b_1 \\ a_{l-1} & & & & b_{m-1} & & & \\ a_l & a_{l-1} & & \vdots & b_m & b_{m-1} & & \vdots \\ 0 & a_l & \ddots & & 0 & b_m & \ddots & \\ \vdots & \ddots & \ddots & a_{l-1} & \vdots & \ddots & \ddots & b_{m-1} \\ 0 & \cdots & 0 & a_l & 0 & \cdots & 0 & b_m \end{pmatrix}$$

The resultant of  $f$  and  $g$  with respect to  $x$ , denoted by  $\text{Res}(f, g, x)$ , is the determinant of the Sylvester matrix,

$$\text{Res}(f, g, x) = \det(\text{Syl}(f, g, x)).$$

The following propositions will be discussed a bit further in the exercises.

**Proposition 4** Given  $f, g \in k[x]$  of positive degree, the resultant  $\text{Res}(f, g, x) \in k$  is an integer polynomial in the coefficients of  $f$  and  $g$ . Furthermore,  $f$  and  $g$  have a common factor in  $k[x]$  if and only if  $\text{Res}(f, g, x) = 0$ .

**Proposition 5** Given  $f, g \in k[x]$  of positive degree, there are polynomials  $A, B \in k[x]$  such that

$$Af + Bg = \text{Res}(f, g, x).$$

Furthermore, the coefficients of  $A$  and  $B$  are integer polynomials in the coefficients of  $f$  and  $g$ .

## Exercises

1. Compute the resultant of  $f(x) = x^5 - 3x^4 - 2x^3 + 3x^2 + 7x + 6$  and  $g = x^4 + x^2 + 1$ . Do these polynomials have a common factor in  $\mathbb{Q}[x]$ ?
2. Let  $f, g \in \mathbb{C}[x]$  be polynomials of degree 3. For this case, prove the second part of Proposition 4. That is, prove that the following are equivalent:
  - (i)  $f$  and  $g$  have a common nonconstant factor.
  - (ii)  $\text{Res}(f, g, x) = 0$ .
3. Resultants can give us another method of implicitization, in the following way: Given a rational curve defined parametrically by  $x = \frac{f_1(t)}{g_1(t)}$  and  $y = \frac{f_2(t)}{g_2(t)}$ , we can find an implicit equation by calculating the resultant of the polynomials  $f = f_1(t) - xg_1(t)$  and  $g = f_2(t) - yg_2(t)$ , where  $f$  and  $g$  are polynomials in  $t$  with variables in  $\mathbb{C}[x, y]$ . Use this method to find an implicit equation for the following curves:
  - (i)  $x = t^2, \quad y = t^2(t + 1)$ .
  - (ii)  $x = \frac{t-1}{t^2}, \quad y = t - 1$ .
  - (iii)  $x = \frac{t(t^2+1)}{t^4+1}, \quad y = \frac{t(t^2-1)}{t^4+1}$ .
4. Use the Gröbner basis method to find implicit equations for the parametric curves in the previous problem, and check that they define the same curves.
5. Consider the following polynomials in  $k[x, y]$ :

$$\begin{aligned}f &= x^2y - 3xy^2 + x^2 - 3xy \\g &= x^3y + x^3 - 4y^2 - 3y + 1\end{aligned}$$

- (i) Compute  $\text{Res}(f, g, x)$ .
- (ii) Compute  $\text{Res}(f, g, y)$ .
- (iii) What do your answers from (a) and (b) say about  $f$  and  $g$ ?