Lecture 10

The Sylvester Resultant

We want to compute intersections of algebraic curves F and G. Let F and G be the vanishing sets of $f(x,y)$ and $g(x,y)$, respectively. Algebraically, we are interested in common zeros of the bivariate polynomials f and g. Let us first ask a simpler question. Do F and G intersect on the line $x = \alpha$. Algebraically, this means to ask whether the univariate polynomials $f(\alpha,y)$ and $g(\alpha,y)$ have a common zero. We address this question first and derive the resultant calculus to solve it. Fortunately, the solution readily extends to the bivariate case.

10.1 Common Zeros of Univariate Polynomials

Let $f(x) \in \mathbb{R}[x]$ and $g(x) \in \mathbb{R}[x]$ be univariate polynomials with real coefficients. We want to determine whether f and g have a common zero. We know already one technique for solving the problem: Compute the gcd of f and g. It comprises exactly the common roots of f and g. The gcd of f and g does not only tell us whether f and g have common roots; it tells us how many common roots there are and it is a compact description of the common roots. In this section, we will see an alternative technique, the resultant calculus. In its basic form, it will only tell us whether f and g have a common root; it will not tell us how many common roots there are nor will it give a description of the common roots. In this sense, resultants are weaker than greatest common divisors. They are stronger in the sense, that they can give us information about common roots of multivariate polynomials.

Assume that f and g have a common factor h. Then $f = (f/h)h$ and $g = (g/h)h$ and hence

$$f \cdot \frac{g}{h} = \frac{f}{h} \cdot h \cdot \frac{g}{h} = \frac{f}{h} g \quad \text{or} \quad f \cdot \frac{g}{h} - \frac{f}{h} \cdot g \equiv 0.$$

In other words, we have nonzero polynomials $s = g/h$ and $t = -f/h$ such that

$$0 \leq \deg s < \deg g \quad \text{and} \quad 0 \leq \deg t < \deg f \quad \text{and} \quad fs + gt \equiv 0. \tag{1}$$

We have thus proved one direction of the following Lemma.

LEMMA 1. *Let $f \in \mathbb{R}[x]$ and $g \in \mathbb{R}[x]$ be univariate polynomials. f and g have a common zero iff there are polynomials s and t satisfying (1).*

Proof. Assume there are s and t satisfying (1). Then $fs = -gt$ and hence any zero of f is also a zero of gt (and at least with the same multiplicity). If f and g would have no common zero, f would have to be a divisor of t. Since t is nonzero and has degree smaller than f, this is impossible. □

How can we find s and t as in (1) or check for their existence? Linear algebra is the answer. Let $n = \deg f$ and $m = \deg g$ and let

$$s = \sum_{0 \le i < m} s_i x^i \quad \text{and} \quad t = \sum_{0 \le i < n} t_i x^i.$$

We do not know the coefficients of s and t yet, but we may introduce names for them.

Exercise 0.1: May we restrict the coefficients of s and t to $\mathbb{R}$ or do we need complex coefficients? ♢

Let $P(x) = f(x)s(x) + g(x)t(x)$. Then

$$P(x) = (f_n s_{m-1} + g_m t_{n-1})x^{m+n-1} + (f_n s_{m-2} + f_{n-1}s_{m-1} + g_m t_{n-m-2} + g_{m-2}t_{n-m-1})x^{m-n-2} + \ldots + (f_0 s_0 + g_0 t_0)x^0.$$

We want $P(x) \equiv 0$. This is equivalent to the following $n+m$ linear equations for the $n+m$ coefficients of s and t.

$$\begin{aligned} f_n s_{m-1} + g_m t_{n-1} &= 0 \\ f_n s_{m-2} + f_{n-1}s_{m-1} + g_m t_{n-m-2} + g_{m-2}t_{n-m-1} &= 0 \\ \vdots &= 0 \\ f_0 s_0 + g_0 t_0 &= 0. \end{aligned}$$

It is convenient to write this system in matrix form:

$$(s_{m-1}, \ldots, s_0, t_{n-1}, \ldots, t_0)\, Syl(f,g) = 0, \tag{2}$$

where

$$Syl(f,g) = \begin{pmatrix} f_n & & \cdots & & f_0 & & \\ & \ddots & & & & \ddots & \\ & & f_n & \cdots & & & f_0 \\ g_m & & \cdots & g_0 & & & \\ & \ddots & & & \ddots & & \\ & & g_m & \cdots & & & g_0 \end{pmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\end{matrix}}\right\} m \text{ rows} \\ \left.\vphantom{\begin{matrix}a\\a\\a\end{matrix}}\right\} n \text{ rows} \end{matrix}$$

is the Sylvester[1] matrix of f and g. This is a square matrix with $n+m$ rows and columns. The first m rows contain shifted coefficient sequences of f and the second n rows contain contain shifted coefficient sequences of g. More precisely, row i, $1 \le i \le m$, contains the coefficient sequence of fx^{m-i} and row $m+i$, $1 \le i \le n$, contains the coefficient sequence of gx^{n-i}. We have written system (2) with the vector (s,t) on the left so that we can write the coefficient sequences as row vectors.

We know from linear algebra that the system (2) has a nontrivial solution if and only if the determinant of the system is zero. The determinant of the Sylvester matrix will play an important role in the sequel and hence deserves a name. The *resultant* $res(f,g)$ of f and g is defined as the determinant of the Sylvester matrix of f and g, i.e.,

$$res(f,g) := \det Syl(f,g).$$

We now have an elegant condition for f and g having a common zero.

[1] James Joseph Sylvester (September 3, 1814 London – 2013 March 15, 1897 Oxford) was an English mathematician. He made fundamental contributions to matrix theory, invariant theory, number theory, partition theory and combinatorics. He played a leadership role in American mathematics in the later half of the 19th century as a professor at the Johns Hopkins University and as founder of the American Journal of Mathematics. At his death, he was professor at Oxford. (Quote from Wikipedia, January 7, 2010)

THEOREM 2. *Let $f,g \in \mathbb{R}[x]$. Then f and g have a common zero if and only if $res(f,g) = 0$.*

Exercise 0.2: Apply the findings of this section to the following pairs of polynomials:

- $f(x) = x^2 - 5x + 6$ and $g(x) = x^2 - 3x + 2$.
- $f(x) = x^2 - 7x + 12$ and $g(x) = x^2 - x$.

In each case compute the resultant. Also factor the polynomials, in order to determine by other means whether they have a common root. ♢

Exercise 0.3: Prove: f and g have two or more common roots if and only if there are polynomials s and t such that

$$0 \leq \deg s \leq \deg g - 2 \quad \text{and} \quad 0 \leq \deg t \leq \deg f - 2 \quad \text{and} \quad fs + gt \equiv 0.$$

What is the condition for k common roots? ♢

Exercise 0.4: Formulate the condition of the preceding exercise as a linear system for the coefficients of the s and t. How many unknowns are there? How many equations? Formulate a generalization of Theorem 2. ♢

10.2 Common Zeros of Bivariate Polynomials

We now come to the question that really interests us. Given two bivariate polynomials $f \in \mathbb{R}[x,y]$ and $g \in \mathbb{R}[x,y]$ find their common zeros. If the degree of f and g is at most two in one of the variables, say y, a simple method works. We solve the equation $g(x,y) = 0$ for y and then substitute the resulting expression for y into $f(x,y) = 0$. In this way, we have eliminated one of the variables. If the degree in both variables is more than two, this method fails, as we do not how to solve for one of the variables. We will see that the resultant calculus allows us to eliminate a variable without(!!!) first solving one of the equations for this variable.

We view f and g as polynomials in y with coefficients in $\mathbb{R}[x]$, i.e.,

$$f(x,y) = \sum_{0 \leq i \leq n} f_i(x) y^i \quad \text{and} \quad g(x,y) = \sum_{0 \leq i \leq m} g_i(x) y^i,$$

where $f_i(x), g_j(x) \in \mathbb{R}[x]$. Let us first ask a simpler question.

$$\text{Fix } x = \alpha. \text{ Is there a } \beta \text{ with } f(\alpha,\beta) = g(\alpha,\beta) = 0?$$

We have learned in the preceding section how to answer this question. The substitution $x \mapsto \alpha$ yields univariate polynomials

$$f(\alpha,y) = \sum_{0 \leq i \leq n} f_i(\alpha) y^i \quad \text{and} \quad g(\alpha,y) = \sum_{0 \leq i \leq m} g_i(\alpha) y^i.$$

These polynomials have a common root if their resultant $res(f(\alpha,y),g(\alpha,y))$ is zero. The resultant is[2]

$$\det \begin{pmatrix} f_n(\alpha) & \dots & & f_0(\alpha) & & \\ & \ddots & & & \ddots & \\ & & f_n(\alpha) & \dots & & f_0(\alpha) \\ g_m(\alpha) & & \dots & g_0(\alpha) & & \\ & \ddots & & & \ddots & \\ & & g_m(\alpha) & \dots & & g_0(\alpha) \end{pmatrix} \begin{matrix} \} \, m \text{ rows} \\ \\ \\ \} \, n \text{ rows} \end{matrix} .$$

There is an alternative way to compute this determinant. We leave the entries as polynomials in x, compute the determinant which is then a polynomial in x, and then make the substitution $x \mapsto \alpha$. More precisely, define the Sylvester matrix of f and g with respect to variable y as

$$Syl_y(f,g) = \begin{pmatrix} f_n(x) & \dots & & f_0(x) & & \\ & \ddots & & & \ddots & \\ & & f_n(x) & \dots & & f_0(x) \\ g_m(x) & & \dots & g_0(x) & & \\ & \ddots & & & \ddots & \\ & & g_m(x) & \dots & & g_0(x) \end{pmatrix} \begin{matrix} \} \, m \text{ rows} \\ \\ \\ \} \, n \text{ rows} \end{matrix}$$

and the resultant $res_y(f,g)$ of f and g with respect to variable y as the determinant of this matrix

$$res_y(f,g) = \det Syl_y(f,g).$$

Observe, that $res_y(f,g)$ is a polynomial in x. The following lemma is immediate and captures the two ways of evaluating the determinant:

- substitute α into the f_i and g_j and then evaluate a determinant whose entries are numbers or
- compute a determinant of univariate polynomials and substitute α into the result.

LEMMA 3. *Let $\alpha \in \mathbb{R}$ be such that $f_n(\alpha) \neq 0 \neq g_m(\alpha)$. Then*

$$res(f(\alpha,y),g(\alpha,y)) = res_y(f,g)(\alpha).$$

How about those α, where one of the leading coefficients is zero? Only those α where both leading coefficients are zero, need special treatment, as the main theorem of this section shows. Before stating and proving it, we illustrate the lemma by an example. Consider

$$f(x,y) = y^2 - x^2 \quad \text{and} \quad g(x,y) = y^2 - x.$$

[2]This is only true if $f_n(\alpha) \neq 0$ and $g_n(\alpha) \neq 0$. Otherwise, the degree of $f(\alpha,y)$ is less than n or the degree of $g(\alpha,y)$ is less than m and the Sylvester matrix changes. We will come back to this point below.

Alternatively, we can avoid the complication of vanishing leading coefficients by a *shear* (definition in Webster's dictionary: ((physics) a deformation of an object in which parallel planes remain parallel but are shifted in a direction parallel to themselves; "the shear changed the quadrilateral into a parallelogram")). Define $\bar{f}(x,y) = f(x+ay,y)$ for some nonzero y. A monomial $x^i y^j$ in f becomes $(x+ay)^i y^j = a^i y^{i+j} + y^{i+j-1}(\dots)$. The degree of $\bar{f}$ in y is the total degree of f and the coefficient of $y^{\deg f}$ is constant.

Figure **??** illustrates the vanishing sets of these polynomials. Then

$$Syl_y(f,g) = \begin{pmatrix} 1 & 0 & -x^2 & \\ & 1 & 0 & -x^2 \\ 1 & 0 & -x & \\ & 1 & 0 & -x \end{pmatrix}$$

and hence $res_y(f,g) = x^4 - 2x^3 + x^2 = x^2(x-1)^2$. The specializations for $x \mapsto 0$ and $x \mapsto 2$, respectively, are

$$res(f(0,y),g(0,y)) = \begin{pmatrix} 1 & 0 & 0 & \\ & 1 & 0 & 0 \\ 1 & 0 & 0 & \\ & 1 & 0 & 0 \end{pmatrix} = 0 \quad \text{and} \quad res(f(2,y),g(2,y)) = \begin{pmatrix} 1 & 0 & -4 & \\ & 1 & 0 & -4 \\ 1 & 0 & -2 & \\ & 1 & 0 & -2 \end{pmatrix} = 4.$$

[[*The strengthening that it suffices that one of the leading coefficients is nonzero adds a lot of complication to the proof. Is it worth it?. There is no way to avoid it. We need part c) of the theorem. Assume* (α,β) *is a common zero of* f *and* g*. If* $f_n(\alpha) \neq 0 \neq g_m(\alpha)$*, the Lemma above implies* $r(\alpha) = 0$*. If* $f_n(\alpha) = 0 = g_m(\alpha)$*,* $r(\alpha)$ *is clearly zero. However, if only one of the coefficients is zero, it requires the argument given in the proof of the theorem.*]]

THEOREM 4. *Let* $f(x,y), g(x,y) \in \mathbb{R}[x,y]$ *and let* $r(x) = res_y(f,g) \in \mathbb{R}[x]$ *be the resultant of* f *and* g *with respect to the variable* y*. Then*

(a) f *and* g *have a nontrivial common factor if and only if* r *is identical.y zero.*

(b) If f *and* g *are coprime (do not have a common factor), the following conditions are equivalent:*

- $\alpha \in \mathbb{C}$ *is a root of* r*.*
- $f_n(\alpha) = g_m(\alpha) = 0$ *or there is a* $\beta \in \mathbb{C}$ *with* $f(\alpha,\beta) = 0 = g(\alpha,\beta) = 0$*.*

(c) For all $(\alpha,\beta) \in \mathbb{C} \times \mathbb{C}$*: If* $f(\alpha,\beta) = 0 = g(\alpha,\beta) = 0$ *then* $r(\alpha) = 0$*.*

Proof. Assume first that f and g have a nontrivial common factor, i.e., $f = \tilde{f}h$ and $g = \tilde{g}h$, where $h = h(x,y)$ has degree at least one. Then for every $\alpha \in \mathbb{C}$ there is a $\beta \in \mathbb{C}$ with $h(\alpha,\beta) = 0$. There are only finitely many α's that are a zero of either $f_n(x)$ or $g_m(x)$; in fact there are at most $n+m$ such α's. For any α that is not a zero of $f_n(x)$ or $g_m(x)$, $f(\alpha,y)$ and $g(\alpha,y)$ have degree n and m, respectively, and

$$0 = res(f(\alpha,y),g(\alpha,y)) = res_y(f,g)(\alpha) = r(\alpha),$$

where the first equality follows from Theorem 2 and the second equality follows from Lemma 3. We conclude that $r(x)$ has infinitely many zeros. Thus it is identically zero.

Conversely, assume that r is identically zero and consider any $\alpha \in \mathbb{C}$ that is not a zero of either $f_n(x)$ or $g_m(x)$. Then

$$0 = r(\alpha) = res_y(f,g)(\alpha) = res(f(\alpha,y),g(\alpha,y)),$$

where the first equality holds since r is identically zero, the second equality follows from the definition of r, and the third equality is Lemma 3. Theorem 2 implies the existence of a β with $f(\alpha,\beta) = 0 = g(\alpha,\beta)$. Thus f and g have infinitely many points in common and hence have a common factor. [Strictly speaking,

I should cite Bezout's theorem: Coprime curves $f(x,y)=0$ and $g(x,y)=0$ intersect in at most $\deg f \deg g$ points.]

We turn to part b). Assume first that α is a root of r. If $f_n(\alpha)=g_m(\alpha)=0$, we are done. If α is neither a root of $f_n(x)$ nor of $g_m(x)$, we have

$$0=r(\alpha)=res_y(f,g)(\alpha)=res(f(\alpha,y),g(\alpha,y)),$$

where the second equality follows from the definition of r, and the third equality is Lemma 3. We claim that $res(f(\alpha,y),g(\alpha,y))=0$, even if one but not both of the leading coefficients is zero. Assume $g_m(\alpha)\neq 0$, $0=f_n(\alpha)=\ldots=f_{k+1}(\alpha)$ and $f_k(\alpha)=0$; the other case is symmetric. In other words, $\deg(f(\alpha,y))=k$. Then

$$0=r(\alpha)=\det Syl_y(f,g)(\alpha)=\det\begin{pmatrix} f_n(\alpha) & \cdots & & f_0(\alpha) & & \\ & \ddots & & & \ddots & \\ & & f_n(\alpha) & \cdots & & f_0(\alpha) \\ g_m(\alpha) & & \cdots & g_0(\alpha) & & \\ & \ddots & & & \ddots & \\ & & g_m(\alpha) & \cdots & & g_0(\alpha) \end{pmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\end{matrix}}\right\} m \text{ rows} \\ \left.\vphantom{\begin{matrix}a\\a\\a\end{matrix}}\right\} n \text{ rows} \end{matrix}$$

$$=\det\begin{pmatrix} 0 & \cdots & f_k(\alpha) & \cdots & f_0(\alpha) & & \\ & \ddots & & \ddots & & \ddots & \\ & & 0 & \cdots & f_k(\alpha) & \cdots & f_0(\alpha) \\ g_m(\alpha) & & \cdots & g_0(\alpha) & & & \\ & \ddots & & & \ddots & & \\ & & g_m(\alpha) & \cdots & & & g_0(\alpha) \end{pmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\end{matrix}}\right\} m \text{ rows} \\ \left.\vphantom{\begin{matrix}a\\a\\a\end{matrix}}\right\} n-1 \text{ rows} \end{matrix}$$

$$=((-1)^m g_m(\alpha))^{n-k}\det\begin{pmatrix} f_k(\alpha) & \cdots & & f_0(\alpha) & & \\ & \ddots & & & \ddots & \\ & & f_k(\alpha) & \cdots & & f_0(\alpha) \\ g_m(\alpha) & & \cdots & g_0(\alpha) & & \\ & \ddots & & & \ddots & \\ & & g_m(\alpha) & \cdots & & g_0(\alpha) \end{pmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\end{matrix}}\right\} m \text{ rows} \\ \left.\vphantom{\begin{matrix}a\\a\\a\end{matrix}}\right\} k \text{ rows} \end{matrix}$$

$$=((-1)^m g_m(\alpha))^{n-k} res(f(\alpha,y),g(\alpha,y)),$$

where the next to last equality follows from developing the matrix $n-k$ times according to the first column. Each such step eliminates the the first column and the first g-row of the matrix, generates the factor $(-1)^m g_m(\alpha)$, and produces a matrix of the same form but with one less g-row. The last equality is the definition of $res(f(\alpha,y),g(\alpha,y))$. Thus $res(f(\alpha,y),g(\alpha,y))=0$ and hence, by Theorem 2, there is a β with $f(\alpha,\beta)=0=f(\alpha,\beta)=0$.

Assume conversely, that either $f_n(\alpha)=0=g_m(\alpha)$ or there is a $\beta\in\mathbb{C}$ with $f(\alpha,\beta)=0=f(\alpha,\beta)=0$. In the former case, the first column of $Syl_y(f,g)(\alpha)$ is a column of zeros and hence $r(\alpha)=0$. In the latter case, $res(f(\alpha,y),g(\alpha,y))=0$ by Theorem 2. We may assume that either $f_n(\alpha)\neq 0$ or $g_m(\alpha)\neq 0$ as the former case would apply otherwise. The argument in the previous paragraph shows that $r(\alpha)$ is a multiple (with a nonzero factor) of $res(f(\alpha,y),g(\alpha,y))$ and hence $r(\alpha)=0$.

Part c) follows immediately from part b). □

Exercise 0.5: Let $f(x,y) = x^2 - y^2$ and $g(x,y) = x^2 - 2xy + y^2$. Compute $r(x) = res_y(f,g)$. Explain, why r is identically zero. ♢

Exercise 0.6: Let $f(x,y) = x^2 - y^2$ and $g(x,y) = x - y^3$. Compute $res_y(f,g)$. Also compute $res_x(f,g)$. What can you say about the points $(\alpha,\beta) \in \mathbb{R}^2$ with $f(x,y) = g(x,y) = 0$?

Answer:

$$res_y(f,g) = \det \begin{pmatrix} -1 & 0 & x^2 & & \\ & -1 & 0 & x^2 & \\ & & -1 & 0 & x^2 \\ -1 & 0 & 0 & x & \\ & -1 & 0 & 0 & x \end{pmatrix} = x^6 - x^2 = x^2(x-1)(x+1)(x^2+1).$$

and

$$res_x(f,g) = \det \begin{pmatrix} 1 & 0 & -y^2 \\ 1 & -y^3 & \\ & 1 & -y^3 \end{pmatrix} = y^6 - y^2 = y^2(y-1)(y+1)(y^2+1).$$

For the real intersections of $f(x,y) = 0$ and $g(x,y) = 0$, we have $\alpha \in \{-1,0,+1\}$ and $\beta \in \{-1,0,+1\}$. ♢

10.3 Real Intersections of Real Algebraic Curves

The results of the preceding section yield a first algorithm for computing the real intersections of real algebraic curves. Let F be the vanishing set of $f(x,y)$ and G be the vanishing set of $g(x,y)$.

(1) If f and g have a common factor[3], factor it out. We assume from now on, that f and g are coprime.

(2) Compute $r(x) = res_y(f,g)$. If r is identically zero, f and g have a common factor. Go back to step (1). Otherwise, determine the real zeros Z_r of r as discussed in Lecture **??**.

(3) Continue with either step (a) or step (b) as preferred.

   (a) For each $\alpha \in Z_r$ determine the common zeros of $f(\alpha,y)$ and $g(\alpha,y)$. This can be done by computing the gcd of $f(\alpha,y)$ and $g(\alpha,y)$ and then isolating the roots of the gcd. The coefficients of $f(\alpha,y)$ and $g(\alpha,y)$ are algebraic numbers and hence this step is computationally hard.

   (b) Compute $s(y) = res_x(f,g)$ and determine the real zeros Z_s of s as discussed in Lecture **??**. For each pair $(\alpha,\beta) \in Z_r \times Z_s$ check whether $f(\alpha,\beta) = 0 = g(\alpha,\beta)$. This step is computationally hard as α and β are algebraic numbers.

10.4 Subresultants of Univariate Polynomials and the Degree of the Common Factor

The resultant of two univariate polynomials decides whether f and g have a common factor. Can we determine the multiplicity of the common factor? The following lemma generalizes Lemma 1 above.

[3] Step 2 will tell us whether this is the case.

LEMMA 5. *Let $f \in \mathbb{R}[x]$ and $g \in \mathbb{R}[x]$, $\deg(f) = n$ and $\deg(g) = m$. The degree of the common factor of f and g is the minimum k such that for all s and t with $deg(s) < m-k$, $deg(t) < n-k$, $t \not\equiv 0$, we have $\deg(fs+gt) \geq k$.*

Proof. Let $h = gcd(f,g)$ and $k_0 = \deg(h)$.

For k with $0 \leq k < k_0$, set $s = g/h$ and $t = -f/h$. Then $t \neq 0$, $\deg s = m - k_0 < m-k$ and $\deg(t) = n - k_0 < n-k$ and $\deg(fs+gt) = \deg(0) = -\infty$.

Consider $k = k_0$ and arbitrary s and t satisfying the constraints. Then $fs+gt$ is a multiple of h and hence is either identically zero or has degree at least k_0. We show that the former case is impossible. Assume otherwise. Then $0 = fs+gt = h((f/h)s+(g/h)t)$ and hence $(f/h)s+(g/h)t = 0$. Since $g/h \neq 0$ and $t \neq 0$ and since f/h and g/h are relatively prime, this implies that f/h divides t. But $\deg(f/h) = n-k_0$ and $\deg(t) < n-k_0$, a contradiction. □

The contrapositive of the second condition in the lemma above reads: there are polynomials s and t with with $deg(s) < m-k$, $deg(t) < n-k$, $t \neq 0$, and $\deg(fs+gt) < k$. This can again be formulated in the language of linear algebra. We have $m-k$ variables for the coefficients of s (since s has degree at most $m-k-1$) and $n-k$ variables for the coefficients of t (since t has degree at most $n-k+1$). Let $P = fs+gt$; it is a polynomial of degree at most $n+m-k-1$. We want that the coefficients corresponding to x^k to $x^{n+m-k-1}$ are zero. This results in $n+m-k-1-k+1 = n+m-2k$ linear constraints for the $n+m-2k$ coefficients of s and t. The matrix of this system is a truncated Sylvester matrix. We have $m-k$ rows for shifted coefficient sequences of f and $n-k$ rows for shifted coefficient sequences of g and $n+m-2k$ columns. Everything after column $n+m-2k$ of $Syl(f,g)$ is truncated. The determinant of this matrix is called the k-th principal subresultant and is denoted $sres_k(f,g)$. We summarize in

THEOREM 6. *Let $\deg(f) = n$ and $\deg(g) = m$. The degree of the common factor of f and g is the minimum k such that $sres_k(f,g) \neq 0$, where*

$$sres_k(f,g) = \det \begin{pmatrix} f_n & \cdots & & f_0 & & \\ & \ddots & & & \ddots & \\ & f_n & \cdots & & & f_0 \\ & & f_n & \cdots & & f_1 \\ & & & \ddots & \cdots & \vdots \\ & & & & f_n & \cdots & f_k \\ g_m & \cdots & & g_0 & & \\ & \ddots & & & \ddots & \\ & g_m & \cdots & & & g_0 \\ & & g_m & \cdots & & g_1 \\ & & & \ddots & \cdots & \vdots \\ & & & & g_m & \cdots & g_k \end{pmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\\a\\a\end{matrix}}\right\} m-k \text{ rows} \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\\a\\a\end{matrix}}\right\} n-k \text{ rows} \end{matrix}$$

We apply Theorem 6 to $f(x) = x^2 - 5x + 6$ and $g(x) = x^2 - 3x + 2$. We have

$$sres_0(f,g) = res(f,g) = \det \begin{pmatrix} 1 & -5 & 6 & \\ & 1 & -5 & 6 \\ 1 & -3 & 2 & \\ & 1 & -3 & 2 \end{pmatrix} = 0$$

$$sres_1(f,g) = \det \begin{pmatrix} 1 & -5 \\ 1 & -3 \end{pmatrix} \neq 0$$

and hence f and g have a linear factor in common.

Exercise 0.7: What is the degree of the common factor of $f(x) = x^3 - -9x^2 + 21x - 49$ and $x^3 - 2x^2 + 7x$? ♢

10.5 Subresultants of Bivariate Polynomials and Multiple Intersection of Algebraic Curves

We extend the results to bivariate polynomials $f(x,y) \in \mathbb{R}[x,y]$ and $g(x,y) = \mathbb{R}[x,y]$. As in Section 10.2 we view f and g as polynomials in y with coefficients in $\mathbb{R}[x]$. We define the k-th subresultant as above; $sres_{k,y} = sres_{k,y}(f,g)$ is a polynomial in x.

[introduce the concept of a generic x-value: α is generic for f if the degree of f does not drop at α.

For $\alpha \in \mathbb{C}$ with $f_n(\alpha) \neq 0 \neq g_m(\alpha)$, we have two ways of computing $sres_k(f(\alpha,y), g(\alpha,y))$. We either follow the definition or we compute $sres_{k,y} = sres_{k,y}(f,g)$ and then plug α into the resulting polynomial. Both approaches lead to the same value. We obtain:

THEOREM 7. *Let f and g be bivariate polynomials, let $\alpha \in \mathbb{C}$ be generic for f and g. Then the minimal k such that $res_{k,y}(\alpha) \neq 0$ is precisely the degree of the common factor of $f(\alpha,y)$ and $g(\alpha,y)$.*