We’ve recently seen how Gröbner bases in lex order allow us to “eliminate” variables; for example, given two plane curves $f(x,y)$ and $g(x,y)$, we expect their intersection to consist of finitely many points (unless they have a common factor), and to find those points, we find a polynomial in $y$ alone (i.e. eliminate $x$) in the ideal $\langle f, g \rangle$ whose roots are then the $y$-coordinates of the intersection points of $f$ and $g$.

It turns out that, at least in this special case, there was an earlier (19th century) approach to the problem without using Gröbner bases, called resultants. Given two polynomials

\begin{align*}
  f(t) &= a_n t^n + a_{n-1} t^{n-1} + \cdots + a_1 t + a_0, \\
  g(t) &= b_m t^m + b_{m-1} t^{m-1} + \cdots + b_1 t + b_0
\end{align*}

of degrees $n$ and $m$ respectively, we already know how to determine whether $f$ and $g$ have a common factor: we simply preform Euclid’s algorithm on $f$ and $g$ (or, to say the same thing in a rather silly way, we compute a Gröbner basis for the ideal $\langle f, g \rangle$). If the coefficients of $f$ or $g$ were changed, however, we would have to start over with Euclid’s algorithm, i.e. we can’t just preform Euclid’s Algorithm on the general polynomials of degree $n$ and $m$. It might be useful then if it were possible to write down (for fixed $n$ and $m$) a polynomial in the coefficients of $f$ and $g$ which is zero precisely when $f$ and $g$ had a common factor.

In order to do this, we look again at a question we’ve studied before: given polynomials $f(t)$ and $g(t)$ of degrees $n$ and $m$ respectively and another polynomial $h(t)$, what are the solutions to the equation

\[ uf + vg = h \]

for polynomials $u(t)$ and $v(t)$? Let us first assume that $f$ and $g$ have no common factors. Then it is possible to solve the equation

\[ \tilde{u} f + \tilde{v} g = 1 \]

and hence we may solve the equation for any polynomial $h$: certainly $(u_0,v_0) = (h\tilde{u}, h\tilde{v})$ is a solution. To find all the solutions, we just note that any two solutions must differ from one another by a solution $(c(t),d(t))$ to the equation

\[ cf + dg = 0. \]

This equation, however, is much easier to solve: we can rewrite it as $cf = -dg$ and since $f$ and $g$ have no factors in common, this means that the solutions to this equation are $(c,d) = (qg, -qf)$,\footnote{The fact that if $f|dg$ and $f$ and $g$ have no common factors, then $f|d$ of course follows from the uniqueness of the factorization of a polynomial into irreducible polynomials, but we can also show it directly. We know from Euclid’s Algorithm that we can write

\[ \tilde{u} f + \tilde{v} g = 1, \]

so that multiplying both sides by $d$ yields

\[ d\tilde{u} f + d\tilde{v} g = d. \]

The term $d\tilde{u} f$ is clearly divisible $f$ and $d\tilde{v} g$ is divisible by $f$ since $dg$ is. Thus $d$ must be divisible by $f$ as well.}
and that the general solution to the original equation is \( u_q = u_0 + qg \) and \( v_q = v_0 - qf \), i.e.

\[
(u_0 + qg)f + (v_0 - qf)g = h
\]

parametrized by an arbitrary polynomial \( q \).

If we want to find a solution that minimizes the degree of \( v = v_0 - qf \), we simply note that there are unique polynomials \( q \) and \( r \) such that \( v_0 = qf + r \) and \( \deg r < \deg f = n \) by the division algorithm. Thus we see that there is a unique solution to the original equation in which \( \deg v < n \). Similarly, it can be shown that there is a unique solution in which \( \deg u < m \). Moreover, if \( \deg h < n + m \), then these two solutions are the same, since if \( \deg v < n \), then \( \deg vg < n + m \) so \( \deg uf = \deg (h - vg) < n + m \), and \( \deg u < m \) as well.

**Proposition.** Let \( f, g \in k[t] \) be polynomials over a field \( k \) of degrees \( n > 0 \) and \( m > 0 \), respectively. Then for any \( h \in k[t] \) of degree less than \( n + m \), there are unique polynomials \( u, v \in k[t] \) with \( \deg u < m \) and \( \deg v < n \) such that

\[
u f + vg = h
\]

if and only if \( f \) and \( g \) have no common factors.

**Proof.** We’ve just shown that if \( f \) and \( g \) are relatively prime, then the above equation has a unique solution. We are left with the “only if” part: we must show \( f \) and \( g \) do have a common factor, then either the existence or the uniqueness of the solutions must fail.

In fact, both fail. Existence fails because we can not solve the equation \( uf + vg = 1 \), since any common factor of \( f \) and \( g \) must also divide 1. Uniqueness fails even for \( h \) where a solution exists because if \( d \) is a common factor of \( f \) and \( g \), then \( \frac{2}{d}f + \frac{1}{d}g = 0 \) is another solution to \( cf + dg = 0 \) with \( \deg u < m \) and \( \deg v < n \).

Let \( V_k \) be the vector space of polynomials of degree \( k \) or less. Then \( V_k \) has dimension \( k+1 \), since \( 1, t, t^2, \ldots, t^k \) is basis. Multiplication by \( f \) defines a linear transformation from \( V_{m-1} \) to \( V_{n+m-1} \). With respect to these standard bases for \( V_{m-1} \) and \( V_{n+m-1} \), the \((n+m) \times m \) matrix
represents multiplication by \( f \). Similarly, multiplication by \( g \) defines a linear transformation from \( V_{n-1} \) to \( V_{n+m-1} \), represented by the \((n+m) \times n\) matrix

\[
\begin{bmatrix}
  b_0 & 0 & 0 & \ldots & \ldots & \ldots & 0 \\
  b_1 & b_0 & 0 & \ddots & \vdots & \vdots & \vdots \\
  b_2 & b_1 & b_0 & \ddots & 0 & \vdots & \vdots \\
  \vdots & b_2 & b_1 & \ddots & 0 & 0 & \vdots \\
  b_{m-1} & \vdots & b_2 & \ddots & b_0 & 0 & 0 \\
  b_m & b_{m-1} & \vdots & \ddots & b_1 & b_0 & 0 \\
  0 & b_m & b_{m-1} & \ddots & b_2 & b_1 & b_0 \\
  0 & 0 & b_m & \ddots & \vdots & b_2 & b_1 \\
  \vdots & 0 & 0 & \ddots & b_{m-1} & \vdots & b_2 \\
  \vdots & \vdots & 0 & \ddots & b_m & b_{m-1} & \vdots \\
  \vdots & \vdots & \vdots & \ddots & 0 & 0 & b_m \\
  0 & \ldots & \ldots & \ldots & 0 & 0 & b_m \\
\end{bmatrix}
\]

with respect to the standard bases for \( V_{n-1} \) and \( V_{n+m-1} \). Now, let \( V_{m-1} \oplus V_{n-1} \) be the vector space of pairs of polynomials \((u, v)\) where \( \deg u \leq m-1 \) and \( \deg v \leq n-1 \). The vector space \( V_{m-1} \oplus V_{n-1} \) has dimension \( m+n \), since

\[
(1, 0), (t, 0), (t^2, 0), \ldots , (t^{m-1}, 0), (t^m, 0), (0, 1), (0, t), (0, t^2), \ldots , (0, t^{n-1}), (0, t^n)
\]

is a basis; this is essentially the standard basis for \( V_{m-1} \) followed by the standard basis for \( V_{n-1} \). The function \( T(u, v) = uf + vg \) defines a linear transformation from \( V_{m-1} \oplus V_{n-1} \) to \( V_{n+m-1} \) whose matrix with respect to the above basis on \( V_{m-1} \oplus V_{n-1} \) and the standard basis on \( V_{n+m-1} \) is the \((n+m) \times (n+m)\) matrix

\[
\text{Syl}(f, g, t) = \begin{bmatrix}
  a_0 & 0 & \ldots & 0 & 0 & b_0 & 0 & 0 & \ldots & \ldots & \ldots & 0 \\
  a_1 & a_0 & \ddots & \vdots & 0 & \vdots & b_0 & 0 & \ddots & \vdots & \vdots & \vdots \\
  a_2 & a_1 & \ddots & 0 & b_{m-3} & \vdots & b_0 & \ddots & 0 & \vdots & \vdots & \vdots \\
  a_3 & a_2 & \ddots & a_0 & 0 & b_{m-2} & b_{m-3} & \ddots & 0 & 0 & \vdots & \vdots \\
  \vdots & a_3 & \ddots & a_1 & a_0 & b_{m-1} & b_{m-2} & b_{m-3} & \vdots & b_0 & 0 & 0 \\
  a_{n-2} & \vdots & a_2 & a_1 & b_{m-1} & b_{m-2} & b_{m-3} & \vdots & b_0 & 0 & 0 \\
  a_{n-1} & a_{n-2} & \vdots & a_3 & a_2 & 0 & b_m & b_{m-1} & \ddots & b_{m-3} & \vdots & b_0 \\
  a_n & a_{n-1} & \ddots & \vdots & a_3 & \vdots & 0 & b_m & \ddots & b_{m-2} & b_{m-3} & \vdots \\
  0 & a_n & \ddots & a_{n-2} & \vdots & 0 & \vdots & b_{m-1} & b_{m-2} & \ddots & b_{m-3} & b_{m-2} & b_{m-1} \\
  \vdots & 0 & \ddots & a_{n-1} & a_{n-2} & 0 & 0 & \vdots & b_m & b_{m-1} & b_{m-2} & b_{m-1} & b_m \\
  0 & \vdots & \vdots & a_n & a_{n-1} & 0 & 0 & 0 & \ddots & 0 & b_m & b_{m-1} & b_m \\
  0 & 0 & \ldots & \ldots & 0 & a_n & a_{n-1} & 0 & 0 & 0 & \ddots & 0 & b_m & b_{m-1} & b_m \\
\end{bmatrix}
\]
of \( f \) and \( g \) with respect to the variable \( t \). The resultant is a polynomial in the coefficients of \( f \) and \( g \) with integer coefficients.

The determinant of a matrix is non-zero precisely when the corresponding linear transformation is one-to-one (and equivalently, if and only if the linear transformation is onto). Thus, since we know that solutions to \( uf + vg = h \) with \( u \in V_{m-1} \) and \( v \in V_{n-1} \) exist (and are unique) for all \( h \in V_{n+m-1} \) precisely when \( f \) and \( g \) have no common factor, we have the following:

**Theorem.** Suppose that \( f, g \in k[t] \) are polynomials over a field \( k \) of degrees \( n > 0 \) and \( m > 0 \) respectively. Then \( \text{Res}(f, g, t) = 0 \) if and only if \( f \) and \( g \) have a common factor in \( k[t] \).

One thing we need to be careful of is that this theorem only applies when the degrees of \( f \) and \( g \) are actually \( n \) and \( m \). If \( a_n = b_m = 0 \), applying the resultant as if \( f \) and \( g \) had degree \( n \) and \( m \) will always yield zero (Why?) even though \( f \) and \( g \) may not have a common factor.

**Remark.** There’s another way to define the resultant. If we assume that \( f, g \in \mathbb{C}[t] \) are monic polynomials, then by the fundamental theorem of algebra, we can factor them over the complex numbers as

\[
\begin{align*}
  f(t) &= (t - \alpha_1)(t - \alpha_2)(t - \alpha_3) \cdots (t - \alpha_{n-1})(t - \alpha_n), \\
  g(t) &= (t - \beta_1)(t - \beta_2) \cdots (t - \beta_m).
\end{align*}
\]

Then if we form the product

\[
R(f, g, t) = \prod_{j=1}^{n} \prod_{k=1}^{m} (\alpha_j - \beta_k)
\]

then it will certainly have the property that \( R(f, g, t) = 0 \) if and only if \( f \) and \( g \) have a root (or equivalently, a factor) in common. Also, it’s easy to see that permuting the \( \alpha_j \) or permuting the \( \beta_k \) has no effect on this product. It turns out that this means it’s possible to rewrite \( R(f, g, t) \) as a polynomial in the coefficients of \( f \) and \( g \),\(^2\) and in fact \( R(f, g, t) = \text{Res}(f, g, t) \). On the other hand, our original definition of the resultant \( \text{Res}(f, g, t) \) is a polynomial in the coefficients \( a_i, b_j \).

---

\(^2\)The general statements is that a symmetric polynomial in the roots \( \alpha_1, \ldots, \alpha_n \) of a monic polynomial \( f(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_0 \) can be written as a polynomial in the elementary symmetric polynomials

\[
\begin{align*}
  -a_{n-1} &= \sigma_1 = \alpha_1 + \cdots + \alpha_n, \\
  a_{n-2} &= \sigma_2 = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \cdots + \alpha_1\alpha_n + \alpha_2\alpha_3 + \cdots + \alpha_2\alpha_n + \cdots + \alpha_{n-1}\alpha_n, \\
  \vdots \\
  (-1)^r a_{n-r} &= \sigma_r = \sum_{i_1 < i_2 < \cdots < i_r} \alpha_{i_1}\alpha_{i_2}\cdots\alpha_{i_r}, \\
  \vdots \\
  (-1)^n a_0 &= \sigma_n = \alpha_1\alpha_2\cdots\alpha_n,
\end{align*}
\]

and is thus a polynomial in the coefficients of \( f \). See section 7.1 of Cox, Little, and O’Shea for details.