

4 Elimination Theory

Copyright © 2025, Gregory G. Smith
Last updated: 9 February 2025

Elimination theory reduces a system of polynomial equations in many variables to systems in a smaller number of variables. From a geometric perspective, these methods lead to the equations for closures of the image of a rational map.

4.0 Implicitization

How is implicitization related to elimination?

4.0.0 Proposition (Polynomial implicitization). *Let $\mathbb{K}$ be an infinite field and let $X := V(f_1, f_2, \dots, f_r)$ be an affine subvariety in $\mathbb{A}^n$. For any polynomial map $\rho: X \rightarrow \mathbb{A}^m$, consider the ideal*

$$I := \langle y_1 - \rho_1, y_2 - \rho_2, \dots, y_m - \rho_m, f_1, f_2, \dots, f_r \rangle$$

in the polynomial ring $\mathbb{K}[x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_m]$. The Zariski closure of the image $\overline{\rho(X)}$ is $V(I \cap \mathbb{K}[y_1, y_2, \dots, y_m])$.

Proof. Let $Z = V(I) \subseteq \mathbb{A}^{n+m}$ and set $J := I \cap \mathbb{K}[y_1, y_2, \dots, y_m]$. Choose an algebraic closure $\overline{\mathbb{K}}$ of the field $\mathbb{K}$. When $\mathbb{K} = \overline{\mathbb{K}}$, the Closure Theorem 3.2.5 establishes that $V(J)$ is the smallest affine subvariety containing the image $\rho(X) = \pi_2(Z)$ where $\pi_2: \mathbb{A}^{n+m} \rightarrow \mathbb{A}^m$ is defined by $(x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_m) \mapsto (y_1, y_2, \dots, y_m)$. When $\mathbb{K} \neq \overline{\mathbb{K}}$, we cannot apply the closure theorem directly. Since the algorithm that returns the elimination ideal is unaffected by the underlying field, passing to the larger field does not change the ideal J . We prove that $V_{\mathbb{K}}(J)$ is the smallest affine variety in $\mathbb{A}^m(\mathbb{K})$ containing $\rho(X)$.

We first claim that $\rho(X) = \pi_2(Z) \subseteq V_{\mathbb{K}}(J)$. Fix $f \in J$. For each point $a \in \pi_2(X)$, choose a point $b = (b_1, b_2, \dots, b_n, a_1, a_2, \dots, a_m) \in Z$ such that $\pi_2(b) = a$. We have $f(a) = \pi_2^*(f(b)) = 0$. This shows that the polynomial f vanishes at all points in $\pi_2(Z)$.

Let $Y(\mathbb{K}) = V_{\mathbb{K}}(g_1, g_2, \dots, g_s) \subseteq \mathbb{A}^m(\mathbb{K})$ be any affine subvariety such that $\rho(X(\mathbb{K})) \subseteq Y(\mathbb{K})$. We must show $V_{\mathbb{K}}(J) \subseteq Y(\mathbb{K})$. Observe that each g_i vanishes on $Y(\mathbb{K})$, so it also vanishes on the smaller set $\rho(X(\mathbb{K}))$. This shows that each $g_i \circ \rho$ vanishes on $X(\mathbb{K})$. Since $\mathbb{K}$ is infinite, we see that $g_i \circ \rho$ is the zero polynomial and vanishes on $X(\overline{\mathbb{K}})$, so each g_i vanishes on $\rho(X(\overline{\mathbb{K}}))$. We deduce that

$$\rho(X(\overline{\mathbb{K}})) \subseteq Y(\overline{\mathbb{K}}) = V_{\overline{\mathbb{K}}}(g_1, g_2, \dots, g_s) \subseteq \mathbb{A}^m(\overline{\mathbb{K}}).$$

Since the theorem is true over $\overline{\mathbb{K}}$, it follows that $V_{\overline{\mathbb{K}}}(J) \subseteq Y(\overline{\mathbb{K}})$. Concentrating on the points that lie in $\mathbb{A}^m(\mathbb{K})$, we conclude that $V_{\mathbb{K}}(J) \subseteq Y(\mathbb{K})$. $\square$

4.0.1 Example. Let m be a positive integer. The affine cone over the rational normal curve of degree m is the closure of image of the map $\rho: \mathbb{A}^2 \rightarrow \mathbb{A}^{m+1}$ defined by $(x_1, x_2) \mapsto (x_1^m, x_1^{m-1}x_2, x_1^{m-2}x_2^2, \dots, x_2^m)$. Its ideal is generated by the 2-minors of the Hankel $(2 \times m)$ -matrix

$$\begin{matrix} & x_1^{m-1} & x_1^{m-2}x_2 & \dots & x_2^{m-1} \\ x_1 & y_1 & y_2 & \dots & y_m \\ x_2 & y_2 & y_3 & \dots & y_{m+1} \end{matrix}.$$

We use a subscript to keep track of the field, so $V_{\mathbb{K}}(J)$ is the affine subvariety in $\mathbb{A}^m(\mathbb{K})$ and $V_{\overline{\mathbb{K}}}(J)$ is the larger set in $\mathbb{A}^m(\overline{\mathbb{K}})$.

This affine subvariety is a cone because it contains all lines joining the point $(0, 0, \dots, 0)$ with a point on the curve parametrized by $x_2 \mapsto (1, x_2, \dots, x_2^m)$.

For instance, when $m = 3$, the Gröbner basis with respect to the lexicographic order of $\langle y_1 - x_1^3, y_2 - x_1^2 x_2, y_3 - x_1 x_2^2, y_4 - x_2^3 \rangle$ is

$$y_3^2 - y_2 y_4, \quad y_2 y_3 - y_1 y_4, \quad y_2^2 - y_1 y_3, \quad x_2 y_3 - x_1 y_4, \quad x_2 y_2 - x_1 y_3, \\ x_2 y_1 - x_1 y_2, \quad x_2^3 - y_4, \quad x_1 x_2^2 - y_3, \quad x_1^2 x_2 - y_2, \quad x_1^3 - y_1.$$

so closure of the image is cut out by the 2-minors of $\begin{bmatrix} y_1 & y_2 & y_3 \\ y_2 & y_3 & y_4 \end{bmatrix}$. $\diamond$

4.0.2 Remark. The cone over the rational curve of degree 3 in $\mathbb{A}^4$ is $X := V(y_3^2 - y_2 y_4, y_2 y_3 - y_1 y_4, y_2^2 - y_1 y_3)$. All three equations are needed to obtain an irreducible variety. The affine subvariety cut out by any two equations is a union:

$$V(y_2^2 - y_1 y_3, y_2 y_3 - y_1 y_4) = X \cup V(y_1, y_2), \\ V(y_3^2 - y_2 y_4, y_2 y_3 - y_1 y_4) = X \cup V(y_3, y_4), \\ V(y_3^2 - y_2 y_4, y_2^2 - y_1 y_3) = X \cup V(y_2, y_3).$$

This map is named after **Corrado Segre**, an Italian mathematician responsible for important early work in algebraic geometry.

4.0.3 Example. For any positive integers n and m , the **Segre embedding** is the map $\sigma_{n,m}: \mathbb{A}^n \times \mathbb{A}^m \rightarrow \mathbb{A}^{nm}$ defined by

$$(x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_m) \mapsto (x_1 y_1, x_1 y_2, \dots, x_1 y_m, x_2 y_1, x_2 y_2, \dots, x_2 y_m, \dots, x_n y_1, x_n y_2, \dots, x_n y_m).$$

Its ideal is generated by the 2-minors of the generic $(n \times m)$ -matrix

$$\begin{matrix} & y_1 & y_2 & \cdots & y_m \\ x_1 & \begin{bmatrix} z_1 & z_2 & \cdots & z_m \\ z_{m+1} & z_{m+2} & \cdots & z_{2m} \\ \vdots & \vdots & & \vdots \\ z_{(n-1)m+1} & z_{(n-1)m+2} & \cdots & z_{nm} \end{bmatrix} \end{matrix} \quad \diamond$$

When $n = m = 2$, the ideal for the image of the Segre map generated by quadratic polynomial $z_1 z_4 - z_2 z_3$.

4.0.4 Example. For any positive integer n and d , set $m := \binom{d+n-1}{d}$. The **Veronese** (or ***d*-uple**) embedding is the map $\nu_d: \mathbb{A}^n \rightarrow \mathbb{A}^m$ defined by $(x_1, x_2, \dots, x_n) \mapsto (x_1^d, x_1^{d-1} x_2, \dots, x_n^d)$. Its ideal is generated by the 2-minors of a catalecticant $(n \times \binom{d+n-2}{d-1})$ -matrix. When (n, d) equals $(3, 2)$ or $(3, 3)$, the matrices are

$$\begin{matrix} x_1 & x_2 & x_3 \\ x_1 & \begin{bmatrix} y_1 & y_2 & y_3 \\ y_2 & y_4 & y_5 \\ y_3 & y_5 & y_6 \end{bmatrix} \end{matrix} \text{ and } \begin{matrix} x_1^2 & x_1 x_2 & x_1 x_3 & x_2^2 & x_2 x_3 & x_3^2 \\ x_1 & \begin{bmatrix} y_1 & y_2 & y_3 & y_4 & y_5 & y_6 \\ y_2 & y_4 & y_5 & y_7 & y_8 & y_9 \\ y_3 & y_5 & y_6 & y_8 & y_9 & y_{10} \end{bmatrix} \end{matrix} \quad \diamond$$

This map is named after **Giuseppe Veronese**, an Italian mathematician who worked on the geometry of multidimensional spaces.

4.1 Toric Ideals

How do we solve the rational implicitization problem?

4.1.0 Theorem (Rational implicitization). *Let $\mathbb{K}$ be an infinite field and let $\rho: \mathbb{A}^n \dashrightarrow \mathbb{A}^m$ be a rational map where $\rho_j = f_j/g_j$ for all $1 \leq j \leq m$. Consider the ideal*

$$I = \langle g_1 y_1 - f_1, g_2 y_2 - f_2, \dots, g_m y_m - f_m, g_1 g_2 \cdots g_m z - 1 \rangle$$

in the ring $\mathbb{K}[z, x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_m]$. The Zariski closure of the image $\rho(\mathbb{A}^n)$ is $V(I \cap \mathbb{K}[y_1, y_2, \dots, y_m])$.

Proof. By setting $g := g_1 g_2 \cdots g_m$, we see that the rational map ρ is well-defined over the open set $U = \{a \in \mathbb{A}^n \mid g(a) \neq 0\}$. Consider

The graph of a rational map may not be an affine subvariety.

the affine subvariety $Y := V(zg - 1) \subset \mathbb{A}^{n+1}$ and the projection map $\pi: \mathbb{A}^{n+1} \rightarrow \mathbb{A}^n$ defined by $(z, x_1, x_2, \dots, x_n) \mapsto (x_1, x_2, \dots, x_n)$. The map π is a birational morphism: the rational map $\psi: \mathbb{A}^n \dashrightarrow Y$ defined by $(x_1, x_2, \dots, x_n) \mapsto (1/g, x_1, x_2, \dots, x_n)$ satisfies both $\pi \circ \psi = \text{id}_U$ and $\psi \circ \pi = \text{id}_Y$. Moreover, the morphism $\phi: Y \rightarrow \mathbb{A}^m$ defined by

$$(z, x_1, x_2, \dots, x_n) \mapsto (f_1 g_2 \cdots g_m z, g_1 f_2 g_3 \cdots g_m z, \dots, g_1 \cdots g_{m-1} f_m z)$$

satisfies $\phi = \rho \circ \pi$. Thus, we have $\phi(Y) = \rho(U)$ and the result follows from the polynomial implicitization theorem. $\square$

4.1.1 Problem. Consider the rational map $\rho: \mathbb{A}^1 \dashrightarrow \mathbb{A}^2$ defined, for all $t \in \mathbb{A}^1$, by $t \mapsto \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$. Find the Zariski closure of its image.

Solution. The reduced Gröbner basis, with respect to $>_{\text{lex}}$, for the ideal $\langle (1+t^2)y_1 - (1-t^2), (1+t^2)y_2 - 2t, 1 - (1+t^2)z \rangle$ in the polynomial ring $\mathbb{K}[z, t, y_1, y_2]$ is $y_1^2 + y_2^2 - 1, ty_2 + y_1 - 1, ty_1 + t - y_2, 2z - y_1 - 1$, so the closure of the image is the unit circle. $\square$

4.1.2 Definition (Toric ideals). Fix an integer matrix $\mathbf{A} \in \mathbb{Z}^{d \times n}$ with columns $\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_n \in \mathbb{Z}^d$. The affine toric variety $X_{\mathbf{A}}$ associated to the matrix $\mathbf{A}$ is the Zariski closure of the image of the rational map $\rho_{\mathbf{A}}: \mathbb{A}^d \dashrightarrow \mathbb{A}^n$ where $(x_1, x_2, \dots, x_d) \mapsto (x^{\mathbf{a}_1}, x^{\mathbf{a}_2}, \dots, x^{\mathbf{a}_n})$.

4.1.3 Examples. The cone over the rational normal curve of degree m , the Veronese embedding $\nu_2: \mathbb{A}^3 \rightarrow \mathbb{A}^6$, and the Segre embedding $\sigma_{2,2}: \mathbb{A}^2 \times \mathbb{A}^2 \rightarrow \mathbb{A}^4$ correspond to the matrices

$$\begin{bmatrix} m & m-1 & m-2 & \cdots & 1 & 0 \\ 0 & 1 & 2 & \cdots & m-1 & m \end{bmatrix}, \quad \begin{bmatrix} 2 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 2 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 2 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$$

respectively. $\diamond$

4.1.4 Remark. The rational map $\rho_{\mathbf{A}}: \mathbb{A}^d \dashrightarrow \mathbb{A}^n$ corresponds to the ring map $\varphi_{\mathbf{A}}: \mathbb{K}[y_1, y_2, \dots, y_n] \rightarrow \mathbb{K}[x_1^{\pm 1}, x_2^{\pm 1}, \dots, x_d^{\pm 1}]$ defined, for all $1 \leq i \leq n$, by $y_i \mapsto x^{\mathbf{a}_i}$. The **toric ideal** $I_{\mathbf{A}}$ in the polynomial ring $\mathbb{K}[y_1, y_2, \dots, y_n]$ associated to the matrix $\mathbf{A}$ is $\text{Ker } \varphi_{\mathbf{A}}$. The rational implicitization theorem implies that $X_{\mathbf{A}} = V(\text{Ker } \varphi_{\mathbf{A}})$.

4.1.5 Lemma. Let $\mathbf{A}$ be an integer $(d \times n)$ -matrix. The toric ideal $I_{\mathbf{A}}$ in the ring $\mathbb{K}[y_1, y_2, \dots, y_n]$ is spanned as a $\mathbb{K}$ -vector space by the set of binomials

$$\{y^{\mathbf{u}} - y^{\mathbf{v}} \mid \text{for all } \mathbf{u}, \mathbf{v} \in \mathbb{N}^n \text{ satisfying } \mathbf{A}\mathbf{u} = \mathbf{A}\mathbf{v}\}.$$

Proof. A binomial $y^{\mathbf{u}} - y^{\mathbf{v}}$ lies in the ideal $I_{\mathbf{A}}$ if and only if we have $\mathbf{A}\mathbf{u} = \mathbf{A}\mathbf{v}$. Thus, it suffices to show that each polynomial in $I_{\mathbf{A}}$ is a $\mathbb{K}$ -linear combination of these binomials. Fix a monomial order on the polynomial ring $\mathbb{K}[y_1, y_2, \dots, y_n]$. Suppose that f in $I_{\mathbf{A}}$ cannot be written as a $\mathbb{K}$ -linear combination of the binomials. Choose f with this property such that $\text{LT}(f) = y^{\mathbf{u}}$ is minimal with respect to the monomial order. When expanding $f \circ \varphi_{\mathbf{A}} = f(x^{\mathbf{a}_1}, x^{\mathbf{a}_2}, \dots, x^{\mathbf{a}_n})$, we obtain the zero polynomial. The term $x^{\mathbf{A}\mathbf{u}}$ in f must cancel out. Hence, there is some monomial $y^{\mathbf{v}} < y^{\mathbf{u}}$ appearing in f such that

$\mathbf{A} \mathbf{u} = \mathbf{A} \mathbf{v}$. The polynomial $f' = f - \mathbf{y}^{\mathbf{u}} + \mathbf{y}^{\mathbf{v}}$ cannot be written as a $\mathbb{K}$ -linear combination of binomials in $I_{\mathbf{A}}$. As $\text{LT}(f') < \text{LT}(f)$, we have a contradiction. $\square$

4.1.6 Remark. Any vector $\mathbf{u}$ in $\mathbb{Z}^n$ can be expressed uniquely in the form $\mathbf{u} = \mathbf{u}^+ - \mathbf{u}^-$ where the vectors $\mathbf{u}^+$ and $\mathbf{u}^-$ are nonnegative and have disjoint support. More precisely, the i th coordinate in $\mathbf{u}^+$ equals u_i if $u_i > 0$ and equals 0 otherwise. Let $\text{Ker } \mathbf{A}$ denote the sublattice of $\mathbb{Z}^n$ consisting of all vectors $\mathbf{u}$ such that $\mathbf{A} \mathbf{u}^+ = \mathbf{A} \mathbf{u}^-$.

4.1.7 Corollary. Let $\mathbf{A}$ be an integer matrix. The toric ideal $I_{\mathbf{A}}$ in the ring $\mathbb{K}[y_1, y_2, \dots, y_n]$ is generated by $\mathbf{y}^{\mathbf{u}^+} - \mathbf{y}^{\mathbf{u}^-}$ where $\mathbf{u} \in \text{Ker } \mathbf{A}$. $\square$

4.1.8 Corollary. Let $\mathbf{A}$ be an integer matrix. For any monomial order $>$ on the polynomial ring $\mathbb{K}[y_1, y_2, \dots, y_n]$, there is a finite set of vectors $\mathcal{G} \subset \text{Ker } \mathbf{A}$ such that the reduced Gröbner basis of the toric ideal $I_{\mathbf{A}}$ with respect to $>$ is equal to $\{\mathbf{y}^{\mathbf{u}^+} - \mathbf{y}^{\mathbf{u}^-} \mid \mathbf{u} \in \mathcal{G}\}$.

Proof. By combining the Hilbert Basis Theorem and Corollary 4.1.7, there is a finite subset of $\text{Ker } \mathbf{A}$ such that the associated binomials generate the toric ideal $I_{\mathbf{A}}$. Apply the Buchberger Algorithm to these binomials to find a Gröbner basis of this ideal. The construction of S-polynomials and the reduction steps preserve the binomial structure. Therefore, any polynomial arising during this process lies in the set $\{\mathbf{y}^{\mathbf{u}^+} - \mathbf{y}^{\mathbf{u}^-} \mid \mathbf{u} \in \text{Ker } \mathbf{A}\}$. $\square$

4.2 Common Roots

When does a system of polynomial equations have solutions? We need a criteria to understand how to solve the extension problem.

To introduce the concept of a resultant, we examine when two polynomials in $\mathbb{K}[x]$ have a common factor.

4.2.0 Lemma. Let f and g be polynomials in $\mathbb{K}[x]$ of positive degrees ℓ and m respectively. The polynomials f and g have a common factor if and only if there exists nonzero polynomials p and q in $\mathbb{K}[x]$ such that $\deg p < m$, $\deg q < \ell$, and $p f + q g = 0$.

Proof. Assume that f and g have a common factor h . Hence, there exists $\hat{f}$ and $\hat{g}$ in $\mathbb{K}[x]$ such that $\deg \hat{f} < \ell$, $f = h \hat{f}$, $\deg \hat{g} < m$, and $g = h \hat{g}$. It follows that $\hat{g} f + (-\hat{f}) g = \hat{g} h \hat{f} - \hat{f} h \hat{g} = 0$.

Assume that p and q have the desired properties. Suppose that f and g have no common factor, so their greatest common divisor is 1. Hence, there exists a and b in $\mathbb{K}[x]$ such that $a f + b g = 1$. Multiplying this equation by q and using the relation $q g = -p f$, we obtain $q = (a f + b g) q = a q f - b p f = (a q - b p) f$. Since q is nonzero, we deduce that q has degree at least ℓ which contradicts the second condition. Thus, there must be a common factor. $\square$

4.2.1 Remark. This lemma allows one to use linear algebra to determine if f and g have a common factor. The idea is to turn polynomial

equation $pf + qg = 0$ into a system of linear equations. Let

$$\begin{aligned} f &= a_\ell x^\ell + a_{\ell-1} x^{\ell-1} + \cdots + a_0 \\ g &= b_m x^m + b_{m-1} x^{m-1} + \cdots + b_0 \\ p &= c_{m-1} x^{m-1} + c_{m-2} x^{m-2} + \cdots + c_0 \\ q &= d_{\ell-1} x^{\ell-1} + d_{\ell-2} x^{\ell-2} + \cdots + d_0 \end{aligned}$$

where we regard the coefficients as unknowns. Substituting into the equation $pf + qg = 0$ and comparing the coefficients of powers of x , we obtain a homogeneous system of linear equations:

$$\begin{array}{rcl} a_\ell c_{m-1} & + & b_m d_{\ell-1} = 0 \quad \text{coefficient of } x^{\ell+m-1} \\ a_{\ell-1} c_{m-1} + a_\ell c_{m-2} & + & b_{m-1} d_{\ell-1} + b_m d_{\ell-2} = 0 \quad \text{coefficient of } x^{\ell+m-2} \\ \ddots & & \ddots \\ a_0 c_0 & + & b_0 d_0 = 0 \quad \text{coefficient of } x^0 \end{array}$$

$$\Rightarrow \begin{bmatrix} a_\ell & & & & b_m & & & & \\ & \ddots & & & & \ddots & & & \\ & & a_\ell & & & & b_m & & \\ & & & \ddots & & & & \ddots & \\ a_0 & & & & b_0 & & & & \\ & & \ddots & & & \ddots & & & \\ & & & a_0 & & & b_0 & & \end{bmatrix} \begin{bmatrix} c_{m-1} \\ \vdots \\ c_0 \\ d_{\ell-1} \\ \vdots \\ d_0 \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

We know from linear algebra that there is a nonzero solution if and only if the coefficient matrix has zero determinant.

4.2.2 Definition. Given f and g in $\mathbb{K}[x]$ of positive degree, we write $f = a_\ell x^\ell + a_{\ell-1} x^{\ell-1} + \cdots + a_0$ and $g = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_0$ where $a_\ell \neq 0$ and $b_m \neq 0$. The **resultant** of f and g with respect to x is the determinant of the following $((\ell + m) \times (\ell + m))$ -matrix

This matrices are named after **James Sylvester** who did important work on matrix theory.

$$\text{Syl}(f, g; x) := \begin{bmatrix} a_\ell & a_{\ell-1} & a_{\ell-2} & \cdots & a_1 & a_0 & 0 & 0 & \cdots & 0 \\ 0 & a_\ell & a_{\ell-1} & \cdots & a_2 & a_1 & a_0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & a_\ell & a_{\ell-1} & a_{\ell-2} & a_{\ell-3} & \cdots & a_0 \\ b_m & b_{m-1} & b_{m-2} & \cdots & b_1 & b_0 & 0 & 0 & \cdots & 0 \\ 0 & b_m & b_{m-1} & \cdots & b_2 & b_1 & b_0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & b_m & b_{m-1} & b_{m-2} & b_{m-3} & \cdots & b_0 \end{bmatrix} \begin{matrix} 1 \\ 2 \\ \vdots \\ m \\ m+1 \\ m+2 \\ \vdots \\ m+\ell \end{matrix}$$

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

4.2.3 Proposition. For any f and g in $\mathbb{K}[x]$ of positive degree, the resultant $\text{Res}(f, g; x)$ lies in $\mathbb{Z}[a_0, a_1, \dots, a_\ell, b_0, b_1, \dots, b_m]$. The polynomials f and g have a common factor if and only if $\text{Res}(f, g; x) = 0$.

Proof. For any $(n \times n)$ -matrix $\mathbf{A} = [a_{j,k}]$, the standard formula for the determinant is $\det(\mathbf{A}) = \sum_{\sigma \in \mathfrak{S}_n} \text{sgn}(\sigma) a_{1,\sigma(1)} a_{2,\sigma(2)} \cdots a_{n,\sigma(n)}$, which is an integer polynomial in its entries proving the first assertion. The second assertion follows from the preceding remark. $\square$

4.2.4 Example. We have $\text{gcd}(2x^2 + 3x + 1, 7x^2 + x + 3) = 1$ because

$$\begin{aligned}
\text{Res}(2x^2 + 3x + 1, 7x^2 + x + 3; x) &= \det \begin{bmatrix} 2 & 3 & 1 & 0 \\ 0 & 2 & 3 & 1 \\ 7 & 1 & 3 & 0 \\ 0 & 7 & 1 & 3 \end{bmatrix} \\
&= \det \begin{bmatrix} 2 & 3 & 1 & 0 \\ 0 & 2 & 3 & 1 \\ 1 & -8 & 0 & 0 \\ 0 & 1 & -8 & 0 \end{bmatrix} = \det \begin{bmatrix} 2 & 3 & 1 \\ 1 & -8 & 0 \\ 0 & 1 & -8 \end{bmatrix} = \det \begin{bmatrix} 2 & 3 & 1 \\ 1 & -8 & 0 \\ 16 & 25 & 0 \end{bmatrix} \\
&= \det \begin{bmatrix} 1 & -8 \\ 16 & 25 \end{bmatrix} = 25 + 16(8) = 153 \neq 0. \quad \diamond
\end{aligned}$$

4.2.5 Example. Two linear polynomials have a common factor if and only if they span the same 1-dimensional space:

$$\text{Res}(a_1 x + a_0, b_1 x + b_0; x) = \det \begin{bmatrix} a_1 & a_0 \\ b_1 & b_0 \end{bmatrix} = a_1 b_0 - a_0 b_1. \quad \diamond$$

4.2.6 Example. Since

$$\begin{aligned}
\text{Res}(a_2 x^2 + a_1 x + a_0, 2a_2 x + a_1; x) &= \det \begin{bmatrix} a_2 & a_1 & a_0 \\ 2a_2 & a_1 & 0 \\ 0 & 2a_2 & a_1 \end{bmatrix} \\
&= -a_2(a_1^2 - 4a_0 a_2),
\end{aligned}$$

the quadratic polynomial $a_2 x^2 + a_1 x + a_0$ has a double root if and only if we have $a_1^2 - 4a_0 a_2 = 0$. $\diamond$

4.2.7 Example. The cubic $a_3 x^3 + a_2 x^2 + a_1 x + a_0$ has a multiple root if and only we have

$$\begin{aligned}
&\text{Res}(a_3 x^3 + a_2 x^2 + a_1 x + a_0, 3a_3 x^2 + 2a_2 x + a_1; x) \\
&= \det \begin{bmatrix} a_3 & a_2 & a_1 & a_0 & 0 \\ 0 & a_3 & a_2 & a_1 & a_0 \\ 3a_3 & 2a_2 & a_1 & 0 & 0 \\ 0 & 3a_3 & 2a_2 & a_1 & 0 \\ 0 & 0 & 3a_3 & 2a_2 & a_1 \end{bmatrix} \\
&= a_3(27a_0^2 a_3^2 + 4a_0 a_2^3 + 4a_1^3 a_3 - a_1^2 a_2^2 - 18a_0 a_1 a_2 a_3) = 0. \quad \diamond
\end{aligned}$$