5 *Extension Theory*

Reducing a system of polynomial equations in several variables to systems in a smaller number of variables is the first step in finding solutions. We still need to understand when a solution to the smaller system can be extended to a solution of the larger system.

5.0 Properties of Resultants

How is the resultant of two polynomials related their roots? We seek alternative characterizations for the resultant.

5.0.0 Problem. Find the resultant of the polynomials $f := a_1(x - \alpha)$ and $g := b_2(x - \beta_1)(x - \beta_2)$ where a_1, α, b_2, β_1, and β_2 are in $\mathbb{K}$.

Solution. In terms of the monomial basis, we have $f = a_1 x + (-\alpha\, a_1)$ and $g = b_2 x^2 + \big(-b_2(\beta_1 + \beta_2)\big)x + b_2\,\beta_1\,\beta_2$. It follows that

$$\begin{aligned}\operatorname{Res}(f, g; x) &= \det \begin{bmatrix} a_1 & -a_1\alpha & 0 \\ 0 & a_1 & -a_1\alpha \\ b_2 & -b_2(\beta_1+\beta_2) & b_2\beta_1\beta_2 \end{bmatrix} \\ &= a_1^2\, b_2(\alpha - \beta_1)(\alpha - \beta_2). \end{aligned}$$ □

Before generalizing this problem, we document a simple feature.

5.0.1 Lemma (Homogeneity)**.** *Let $f = a_0 + a_1\,x + a_2\,x^2 + \cdots + a_\ell\,x^\ell$ and let $g = b_0 + b_1\,x + b_2\,x^2 + \cdots + b_m\,x^m$ where $a_\ell \neq 0 \neq b_m$. The resultant* $\operatorname{Res}(f, g; x)$ *is a bihomogeneous polynomial having degree m in the variables $a_0, a_1, \dots, a_\ell$ and degree ℓ in the variables $b_0, b_1, \dots, b_m$.*

Sketch of proof. The Sylvester matrix has m rows with linear entries in $\mathbb{Z}[a_0, a_1, \dots, a_\ell]$ and ℓ rows with linear entries in $\mathbb{Z}[b_0, b_1, \dots, b_m]$. The claim follows by expanding the determinant along its rows. □

The relationship between resultants and roots is beautiful.

5.0.2 Theorem. *For any $f = a_\ell \prod_{j=1}^{\ell}(x - \alpha_j)$ and $g = b_m \prod_{k=1}^{m}(x - \beta_k)$ where a_ℓ, $\alpha_1, \alpha_2, \dots, \alpha_\ell$, b_m, $\beta_1, \beta_2, \dots, \beta_m$ are in $\mathbb{K}$, we have*

$$\operatorname{Res}(f, g; x) = a_\ell^m\, b_m^\ell \prod_{j=1}^{\ell}\prod_{k=1}^{m}(\alpha_j - \beta_k)\,.$$

Proof. Set $R := a_\ell^m\, b_m^\ell \displaystyle\prod_{j=1}^{\ell}\prod_{k=1}^{m}(\alpha_j - \beta_k)$. The proof has three steps.

- We first show that $\operatorname{Res}(f, g; x)$ is divisible by R. The Sylvester matrix has m rows divisible by a_ℓ and ℓ rows divisible by b_m, so $\operatorname{Res}(f, g; x)$ is divisible by $a_\ell^m \, b_m^\ell$. If some root α_i of f equals some root β_j, then f and g have a common factor and $\operatorname{Res}(f, g; x) = 0$. Hence, the difference $\alpha_i - \beta_j$ divides $\operatorname{Res}(f, g; x)$.
- Secondly, we show that the two polynomials $\operatorname{Res}(f, g; x)$ and R coincide up to a constant factor. Consider the following:

$$\begin{aligned} R &= \left(a_\ell \prod_{i=1}^{\ell} (\beta_1 - \alpha_i) \right) \left(a_\ell \prod_{i=1}^{\ell} (\beta_2 - \alpha_i) \right) \cdots \left(a_\ell \prod_{i=1}^{\ell} (\beta_m - \alpha_i) \right) (-1)^{\ell m} \, b_m^\ell \\ &= f(\beta_1) \, f(\beta_2) \cdots f(\beta_m) \, (-1)^{\ell m} \, b_m^\ell \\ &= a_\ell^m \left(b_m \prod_{j=1}^{m} (\alpha_1 - \beta_j) \right) \left(b_m \prod_{j=1}^{m} (\alpha_2 - \beta_j) \right) \cdots \left(b_m \prod_{j=1}^{m} (\alpha_\ell - \beta_j) \right) \\ &= a_\ell^m \, g(\alpha_1) \, g(\alpha_2) \cdots g(\alpha_\ell) \, . \end{aligned}$$

  The first expression shows that R is homogenous of degree m in the variables $a_0, a_1, \ldots, a_\ell$ and the second shows R is homogenous of degree ℓ in the variables $b_0, b_1, \ldots, b_m$. Since $\operatorname{Res}(f, g; x)$ has the same properties and is divisible by R, we conclude that $\operatorname{Res}(f, g; x)$ and R coincide up to a constant factor.
- The trace of the Sylvester matrix is $a_\ell^m \, b_0^\ell$, so this monomial has coefficient 1 in $\operatorname{Res}(f, g; x)$. Since $b_0 = (-1)^m \, b_m \, \beta_1 \, \beta_2 \cdots \beta_m$, the monomial $a_\ell^m \, b_0^\ell$ also has coefficient 1 in

$$R = f(\beta_1) \, f(\beta_1) \cdots f(\beta_m) \, (-1)^{\ell m} \, b_m^\ell \, .$$

  We conclude that $\operatorname{Res}(f, g; x) = R$. □

5.0.3 Corollary. *The polynomial* $\operatorname{Res}(f, g; x)$ *is irreducible.*

Proof. Suppose that there exists non-constant polynomials h_1 and h_2 in $\mathbb{Z}[a_0, a_1, \ldots, a_\ell, b_0, b_1, \ldots, b_m]$ such that $\operatorname{Res}(f, g; x) = h_1 \, h_2$. The coefficients $a_0, a_1, \ldots, a_{\ell-1}$ and $b_0, b_1, \ldots, b_{m-1}$ are scalar multiples of the elementary symmetric functions in the roots $\alpha_1, \alpha_2, \ldots, \alpha_\ell$ and $\beta_1, \beta_2, \ldots, \beta_m$ respectively. It follows that the polynomials h_1 and h_2 are symmetric functions in the α_i and β_j when lifted to the ring $\mathbb{C}[a_\ell, \alpha_1, \alpha_2, \ldots, \alpha_\ell, b_m, \beta_1, \beta_2, \ldots, \beta_m]$. Hence, if just one $\alpha_i - \beta_j$ divides h_1, the product $\prod_i \prod_j (\alpha_i - \beta_j)$ also does. We deduce that $\operatorname{Res}(f, g; x)$ divides $a_\ell^p \, b_m^q \, h_1$ for some nonnegative integers p and q.

However, we claim that the variables a_ℓ and b_m do not divide $\operatorname{Res}(f, g; x)$ in $\mathbb{Z}[a_0, a_1, \ldots, a_\ell, b_0, b_1, \ldots, b_m]$. If a_ℓ were to divide this resultant, then $\operatorname{Res}(f, g; x)$ would vanish when $a_\ell = 0$. We know that $\operatorname{Res}(f, g; x)$ vanishes if and only if the polynomials f and g have a common divisor which may fail to be the case even when $a_\ell = 0$. We conclude that $\operatorname{Res}(f, g; x)$ divides h_1. □

The next three properties are consequences of theorem.

5.0.4 Corollary. *For all elements λ in $\mathbb{K}$, the resultant*

$$\operatorname{Res}(f,g;x) = R(a_\ell, a_{\ell-1}, \dots, a_0, b_m, b_{m-1}, \dots, b_0)$$

enjoys the following three properties:

- $\operatorname{Res}(f,g;x) = (-1)^{\ell m} \operatorname{Res}(g,f;x)$ (symmetry)
- $\operatorname{Res}(f\,g,h;x) = \operatorname{Res}(f,h;x)\ \operatorname{Res}(g,h;x)$ (multiplicativity)
- $R(\lambda^0 a_\ell, \lambda^1 a_{\ell-1}, \dots, \lambda^\ell a_0, \lambda^0 b_m, \lambda^1 b_{m-1}, \dots, \lambda^m b_0) = \lambda^{\ell m} R(a_\ell, \dots, a_0, b_m, \dots, b_0)$ (quasi-homogeneity)

Sketch of Proof. Over an algebraic closed coefficient field, we have $f = a_k \prod_{i=1}^{k}(x-\alpha_i)$, $g = b_\ell \prod_{i=1}^{\ell}(x-\beta_i)$, and $h = c_m \prod_{i=1}^{m}(x-\gamma_i)$. It follows that

$$\begin{aligned}
\operatorname{Res}(f,h;x) &= a_k^m c_m^k \textstyle\prod_{i,j}(\alpha_i - \gamma_j) \\
\operatorname{Res}(g,h;x) &= b_\ell^m c_m^\ell \textstyle\prod_{i,j}(\beta_i - \gamma_j) \\
\operatorname{Res}(f\,g,h;x) &= (a_k b_\ell)^m c_m^{k+\ell} \textstyle\prod_{i,j}(\alpha_i - \gamma_j) \prod_{i,j}(\beta_i - \gamma_j)\,.
\end{aligned}$$

We also have

$$\begin{aligned}
&R(\lambda^0 a_\ell, \lambda^1 a_{\ell-1}, \dots, \lambda^\ell a_0, \lambda^0 b_m, \lambda^1 b_{m-1}, \dots, \lambda^m b_0) \\
&= a_\ell^m\, b_m^\ell \prod_i \prod_j (\lambda\,\alpha_i - \lambda\,\beta_j) = \lambda^{\ell m}\, a_\ell^m\, b_m^\ell \prod_i \prod_j (\alpha_i - \beta_j)\,. \qquad \square
\end{aligned}$$

5.0.5 Remark. Quasi-homogeneity has a differential form:

$$\begin{aligned}
\sum_{i=1}^{\ell} a_i \frac{\partial R}{\partial a_i} &= mR \\
\sum_{j=1}^{m} b_j \frac{\partial R}{\partial b_j} &= \ell R \\
\sum_{k=1}^{\ell} k a_k \frac{\partial R}{\partial a_k} + \sum_{j=1}^{m} j b_j \frac{\partial R}{\partial b_j} &= \ell\, m\, R\,.
\end{aligned}$$

5.1 Preparations for Extensions

We collect a few lemmata needed to proof an extension theorem. Let

$$f := a_0 + a_1\,x + a_2\,x^2 + \cdots + a_\ell\,x^\ell \quad \text{and} \quad g := b_0 + b_1\,x + b_2\,x^2 + \cdots + b_m\,x^m$$

be polynomials in $\mathbb{K}[x]$ of positive degree where $a_\ell \neq 0$ and $b_m \neq 0$. Without loss of generality, we may assume that $m \geqslant \ell$.

5.1.0 Problem. Given polynomials q and r in the ring $\mathbb{K}[x]$ such that $g = q\,f + r$ and $0 \neq \deg(r) < \deg(f) = \ell$, demonstrate that

$$\operatorname{Res}(f,g;x) = a_\ell^{m-\deg(r)} \operatorname{Res}(f,r;x)\,.$$

Solution. Set $h := g - (b_m / a_\ell)\, x^{m-\ell} f$. Taking the advantage of the Euclidean Algorithm, it is enough to demonstrate that

$$\operatorname{Res}(f, g; x) = a_\ell^{m-\deg(h)} \operatorname{Res}(f, h; x) .$$

By definition, we have

$$\operatorname{Res}(f,g;x) = \det \begin{bmatrix} a_\ell & a_{\ell-1} & a_{\ell-2} & \dots & a_1 & a_0 & 0 & \dots & 0 \\ 0 & a_\ell & a_{\ell-1} & \dots & a_2 & a_1 & a_0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & a_\ell & a_{\ell-1} & a_{\ell-2} & \dots & a_0 \\ b_m & b_{m-1} & b_{m-2} & \dots & b_1 & b_0 & 0 & \dots & 0 \\ 0 & b_m & b_{m-1} & \dots & b_2 & b_1 & b_0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & b_m & b_{m-1} & b_{m-2} & \dots & b_0 \end{bmatrix} .$$

Multiplying each of the first m rows by $a_\ell^{-1}\, b_m$ and subtracting them from the corresponding row beginning with b_m yields

$$\operatorname{Res}(f,g;x) = \det \begin{bmatrix} a_\ell & a_{\ell-1} & a_{\ell-2} & \dots & 0 \\ 0 & a_\ell & a_{\ell-1} & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & a_0 \\ 0 & b_{m-1} - a_{\ell-1} a_\ell^{-1} b_m & b_{m-2} - a_{\ell-2} a_\ell^{-1} b_m & \dots & 0 \\ 0 & 0 & b_{m-1} - a_{\ell-1} a_\ell^{-1} b_m & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \end{bmatrix} .$$

By expanding along the first $\deg(h)$ columns, we see that

$$\operatorname{Res}(f, g; x) = a_\ell^{m-\deg(h)} \operatorname{Res}(f, h; x) . \qquad \square$$

5.1.1 Lemma. *For any f and g in $\mathbb{K}[x]$ of positive degree, there exists p and q in $\mathbb{K}[x]$ such that $p\,f + q\,g = \operatorname{Res}(f, g; x)$ and the coefficients of p and q are integer polynomials in the coefficients of f and g.*

Proof. The lemma is trivial when $\operatorname{Res}(f, g; x) = 0$ because we may choose $p = q = 0$. Thus, we may assume $\operatorname{Res}(f, g; x) \neq 0$. Since f and g have no common factor, there exists polynomials $\widehat{p}$ and $\widehat{q}$ in $\mathbb{K}[x]$ such that $\widehat{p}\, f + \widehat{q}\, g = 1$. Set

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

Substituting these formula into $\widehat{p}\, f + \widehat{q}\, g = 1$ and comparing coefficients, we obtain the matrix equation

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

Cramer's rule gives a formula for the unique solution:

$$c_{m-1} = \frac{1}{\operatorname{Res}(f,g;x)} \det \begin{bmatrix} 0 & & & & b_m & & \\ 0 & a_\ell & & & \vdots & \ddots & \\ \vdots & \vdots & \ddots & & \vdots & & b_m \\ 0 & a_0 & & a_\ell & b_0 & & \vdots \\ \vdots & & \ddots & \vdots & & \ddots & \vdots \\ 1 & & & a_0 & & & b_0 \end{bmatrix}$$

The coefficient c_{m-1} is polynomial in $\mathbb{Z}[a_0, a_1, \dots, a_\ell, b_0, b_1, \dots, b_m]$ divided by $\operatorname{Res}(f,g;x)$. It follows that

$$\widehat{p} = \frac{p}{\operatorname{Res}(f,g;x)} \qquad \widehat{q} = \frac{q}{\operatorname{Res}(f,g;x)}$$

for some polynomial p and q in $\mathbb{K}[x]$. Multiplying through by $\operatorname{Res}(f,g;x)$, we obtain the equation $p\,f + q\,g = \operatorname{Res}(f,g;x)$. □

5.1.2 Proposition. *Let f and g be polynomials in $\mathbb{K}[x_1, x_2, \dots, x_n]$ having positive degree in the variable x_1. The resultant $\operatorname{Res}(f,g;x_1)$ lies in the ideal $\langle f, g\rangle \cap \mathbb{K}[x_2, x_3, \dots, x_n]$. Moreover, we have $\operatorname{Res}(f,g;x_1) = 0$ if and only if the polynomials f and g have a common factor in $\mathbb{K}[x_1, x_2, \dots, x_n]$ which has positive degree in x_1.*

Gröbner bases describe elimination ideals but do not preclude the possibility that they are zero. In contrast, resultants create an element in the elimination ideal.

Proof. Expressing both f and g as polynomials in the variable x_1 whose the coefficients are polynomials in $\mathbb{K}[x_2, x_3, \dots, x_n]$, it follows that $\operatorname{Res}(f,g;x_1)$ lies in $\mathbb{K}[x_2, x_3, \dots, x_n]$. The lemma implies that there exists polynomials p and q in the ring $(\mathbb{K}[x_2, \dots, x_n])[x_1]$ such that $p\,f + q\,g = \operatorname{Res}(f,g;x_1)$. Thus, we have

$$\operatorname{Res}(f,g;x_1) \in \langle f, g\rangle \cap \mathbb{K}[x_2, x_3, \dots, x_n]\,.$$

We know $\operatorname{Res}(f,g;x_1) = 0$ if and only if the polynomials f and g have a common factor in $\mathbb{K}(x_2, x_3, \dots, x_n)[x_1]$ of positive degree in x_1. However, the Gauss Lemma shows that this is equivalent to having a common factor in $\mathbb{K}[x_1, x_2, \dots, x_n]$ of positive degree in x_1. □

5.2 The Extension Theorem

We now use the theory of resultants to prove an extension theorem.

5.2.0 Lemma. *Let f and g be polynomials in $\mathbb{K}[x_1, x_2, \dots, x_n]$ having positive degrees ℓ and m respectively. For any point $\mathbf{c} = (c_2, c_3, \dots, c_n)$ in $\mathbb{A}^{n-1}(\mathbb{K})$ such that $f(x_1, \mathbf{c}) \in \mathbb{K}[x_1]$ has degree ℓ and $g(x_1, \mathbf{c}) \in \mathbb{K}[x_1]$ has degree $k \leqslant m$, the polynomial $h := \operatorname{Res}(f,g;x_1)$ in $\mathbb{K}[x_2, x_3, \dots, x_n]$ satisfies*

$$h(\mathbf{c}) = a_\ell(\mathbf{c})^{m-k} \operatorname{Res}\big(f(x_1,\mathbf{c}), g(x_1,\mathbf{c}); x_1\big)$$

where $a_\ell \in \mathbb{K}[x_2, x_3, \dots, x_n]$ is the leading coefficient of the polynomial f in $(\mathbb{K}[x_2, x_3, \dots, x_n])[x_1]$.

Proof. Substituting $\mathbf{c} = (c_2, c_3, \dots, c_n)$ for the variables $x_2, x_3, \dots, x_n$ in the formula for $h = \operatorname{Res}(f, g; x_1)$ yields

$$h(\mathbf{c}) = \det \begin{bmatrix} a_\ell(\mathbf{c}) & & & b_m(\mathbf{c}) & & \\ \vdots & \ddots & & \vdots & \ddots & \\ \vdots & & a_\ell(\mathbf{c}) & \vdots & & b_m(\mathbf{c}) \\ a_0(\mathbf{c}) & & \vdots & b_0(\mathbf{c}) & & \vdots \\ & \ddots & \vdots & & \ddots & \vdots \\ & & a_0(\mathbf{c}) & & & b_0(\mathbf{c}) \end{bmatrix} .$$

First, suppose that $g(x_1, \mathbf{c})$ had degree $k = m$. It follows that

$$\begin{aligned} f(x_1, \mathbf{c}) &= a_\ell(\mathbf{c})\, x_1^\ell + a_{\ell-1}(\mathbf{c})\, x_1^{\ell-1} + \cdots + a_0(\mathbf{c}) \\ g(x_1, \mathbf{c}) &= b_m(\mathbf{c}) x_1^m + b_{m-1}(\mathbf{c}) x_1^{m-1} + \cdots + b_0(\mathbf{c}) \end{aligned}$$

where $a_\ell(\mathbf{c}) \neq 0 \neq b_m(\mathbf{c})$. Hence, the determinant is the resultant of $f(x_1, \mathbf{c})$ and $g(x_1, \mathbf{c})$, so that $h(\mathbf{c}) = \operatorname{Res}\big(f(x_1, \mathbf{c}), g(x_1, \mathbf{c}); x_1\big)$. This proves the proposition when $k = m$. When $k < m$, the determinant is no longer the resultant of $f(x_1, \mathbf{c})$ and $g(x_1, \mathbf{c})$; it has the wrong size. In this case, we obtain the desired resultant by repeatedly expanding by minors along the first row. □

5.2.1 Theorem (Extension)**.** *Let $\mathbb{K}$ be an algebraically closed field. For any ideal $I = \langle f_1, f_2 \dots, f_r \rangle$ in $\mathbb{K}[x, y_1 \dots, y_n]$, set $J := I \cap \mathbb{K}[y_1, y_2, \dots, y_n]$. For each index j satisfying $1 \leqslant j \leqslant r$, write f_j in the form*

$$f_j = g_j\, x^{N_j} + (\textit{terms in which } x \textit{ has degree less than } N_j)\,,$$

where $N_j > 0$ and $g_j \in \mathbb{K}[y_1, y_2, \dots, y_n]$ is nonzero.

(Algebraic form) *Consider a point $(c_1, c_2, \dots, c_n)$ in $\mathrm{V}(J) \subseteq \mathbb{A}^n(\mathbb{K})$ to be a partial solution. When $(c_1, c_2 \dots, c_n) \notin \mathrm{V}(g_1, g_2, \dots, g_r)$, there exists an element $c_0 \in \mathbb{K}$ such that $(c_0, c_1, c_2, \dots, c_n) \in \mathrm{V}(I)$.*

(Geometric form) *Let $\pi_2 \colon \mathbb{A}^{n+1}(\mathbb{K}) \to \mathbb{A}^n(\mathbb{K})$ be the projection onto the last n coordinates. For the affine subvariety $X = \mathrm{V}(I)$ in $\mathbb{A}^{n+1}(\mathbb{K})$, we have $\mathrm{V}(J) = \pi_2(X) \cup \big(\mathrm{V}(g_1, g_2 \dots, g_r) \cap \mathrm{V}(J)\big)$.*

Proof of the algebraic form. Consider a point $\mathbf{c} := (c_1, c_2, \dots, c_n)$ in $\mathbb{A}^n(\mathbb{K})$ and the $\mathbb{K}$-algebra homomorphism $\mathbb{K}[x, y_1, y_2, \dots, y_n] \to \mathbb{K}[x]$ defined by $f(x, y_1, y_2, \dots, y_n) \mapsto f(x, \mathbf{c})$. The image of I under this homomorphism is an ideal in $\mathbb{K}[x]$. Since $\mathbb{K}[x]$ is a principal ideal domain, the image of I is generated by one polynomial p. When p has positive degree, there exists an element $c_0 \in \mathbb{K}$ such that $p(c_0) = 0$ because the field $\mathbb{K}$ is algebraically closed. It follows that $f(c_0, \mathbf{c}) = 0$ for all $f \in I$, so the point $(c_0, \mathbf{c}) = (c_0, c_1, c_2, \dots, c_n)$ lies in the affine subvariety $\mathrm{V}(I)$. Observe that this argument also works when p is the zero polynomial.

What would happen when p is a nonzero constant? By construction, there would exist a polynomial f in the ideal I such that $f(x, \mathbf{c}) = p$ is in $\mathbb{K}^\times$. We claim that this cannot occur. Our partial solution satisfies $\mathbf{c} \notin \mathrm{V}(g_1, g_2, \dots, g_r)$, so we would have $g_j(\mathbf{c}) \neq 0$ for some j. Consider $h := \operatorname{Res}(f_j, f; x)$ in $\mathbb{K}[y_1, y_2, \dots, y_n]$. Lemma 5.2.0 demonstrates that $h(\mathbf{c}) = g_i(\mathbf{c})^{\deg(f)} \operatorname{Res}\big(f_j(x, \mathbf{c}), p; x\big)$ because $f(x, \mathbf{c}) = p$. We would also have $\operatorname{Res}\big(f_i(x, \mathbf{c}), p; x\big) = p^{N_j}$ so $h(\mathbf{c}) = g_j(\mathbf{c})^{\deg(f)} \, p^{N_j} \neq 0$. However, the relations $f_j \in I$ and $f \in I$ imply that $h \in J$, so $h(\mathbf{c}) = 0$ because $\mathbf{c} \in \mathrm{V}(J)$. □

Proof of the geometric form. We have $\mathrm{V}(g_1, g_2, \dots, g_r) \cap \mathrm{V}(J) \subseteq \mathrm{V}(J)$ and we always have $\pi_2(X) \subseteq \mathrm{V}(J)$. On the other hand, the algebraic form shows that $c \notin \mathrm{V}(g_1, g_2, \dots, g_r)$ implies that $c \in \pi_2(X)$. □

The extension theorem tells us that $\pi_2(X)$ fills up the affine subvariety $\mathrm{V}(J)$ except possibly for the part that lies in $\mathrm{V}(g_1, g_2, \dots, g_r)$. In other words, the extension step can fail only when the leading coefficients vanish simultaneously.

5.2.2 Corollary. *Assume that $\mathbb{K}$ is algebraically closed and consider the affine subvariety $X = \mathrm{V}(f_1, f_2, \dots, f_r)$ in $\mathbb{A}^{n+1}(\mathbb{K})$. Suppose that, for some index j, the polynomial f_j has the form*

$$f_j = c\, x^N + \text{terms in which } x \text{ has degree less than } N$$

where $0 \neq c \in \mathbb{K}$ and $N > 0$. We have $\pi_2(X) = \mathrm{V}(I \cap \mathbb{K}[y_1, y_2, \dots, y_n])$ where π_2 is the projection on the last n components. □

5.2.3 Remark. The variety $\mathrm{V}(g_1, g_2, \dots, g_r)$ can be unnaturally large. We claim that

$$\mathrm{V}\big((y-z)x^2 + x\,y - 1, (y-z)x^2 + x\,z - 1\big) = \mathrm{V}(x\,y - 1, x\,z - 1)\,.$$

Indeed, we have

$$\begin{aligned}(y-z)x^2 + x\,y - 1 &= (x+1)(x\,y-1) - x(x\,z-1)\,,\\ (y-z)x^2 + x\,z - 1 &= x(x\,y-1) + (1-x)(x\,z-1)\,,\end{aligned}$$

and

$$\begin{aligned}xy - 1 &= (x^2y - x^2z + x\,z - x)\big((y-z)x^2 + xy - 1\big)\\ &\qquad + (-x^2y + x^2z - x\,y + x + 1)\big((y-z)x^2 + x\,z - 1\big)\\ xz - 1 &= (-x)\big((y-z)x^2 + x\,y - 1\big) + (x+1)\big((y-z)x^2 + x\,z - 1\big)\,.\end{aligned}$$

However, the lex Gröbner basis is simply $\langle y - z, x\,z - 1\rangle$.