Solutions 4

P4.1. Assume that $\mathbb{K}$ is an algebraically closed field. Identify affine space $\mathbb{A}^9(\mathbb{K})$ with the space of (3×3)-matrices $\mathbf{A} = [a_{j,k}]$. Let $\rho \colon \mathbb{A}^9(\mathbb{K}) \dashrightarrow \mathbb{A}^9(\mathbb{K})$ be the rational map defined by

$$\mathbf{A} \mapsto \mathbf{A} \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix} \mathbf{A}^{-1} .$$

i. Find equations for the smallest affine subvariety X containing the image of ρ.
ii. Show that X is the set of all nilpotent (3×3)-matrices.

Solution.

i. For the matrix $\mathbf{A} = \begin{bmatrix} x_1 & x_4 & x_7 \\ x_2 & x_5 & x_8 \\ x_3 & x_6 & x_9 \end{bmatrix}$, the Cramer rule shows that

$$\mathbf{A}^{-1} = \frac{1}{\det(\mathbf{A})} \begin{bmatrix} x_5x_9 - x_6x_8 & x_6x_7 - x_4x_9 & x_4x_8 - x_5x_7 \\ x_3x_8 - x_2x_9 & x_1x_9 - x_3x_7 & x_2x_7 - x_1x_8 \\ x_2x_6 - x_3x_5 & x_3x_4 - x_1x_6 & x_1x_5 - x_2x_4 \end{bmatrix} ,$$

so $\mathbf{A} \mapsto \mathbf{A} \left[\begin{smallmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{smallmatrix}\right] \mathbf{A}^{-1}$ is a rational map.

We apply the rational implicitization theorem in *Macaulay2* [M2]. We create the polynomial ring and the generic matrix $\mathbf{A}$.

```
Macaulay2, version 1.24.11
with packages: ConwayPolynomials, Elimination, IntegralClosure, InverseSystems,
               Isomorphism, LLLBases, MinimalPrimes, OnlineLookup,
               PackageCitations, Polyhedra, PrimaryDecomposition, ReesAlgebra,
               Saturation, TangentCone, Truncations, Varieties

i1 : n = 3;

i2 : S = QQ[z, x_1..x_(n^2), y_1..y_(n^2)];

i3 : A = genericMatrix(S, x_1, n, n)

o3 = | x_1 x_4 x_7 |
     | x_2 x_5 x_8 |
     | x_3 x_6 x_9 |

              3      3
o3 : Matrix S  <-- S
```

We next construct the adjugate of $\mathbf{A}$ and verify that $\mathbf{A}\,\mathrm{adj}(\mathbf{A}) = \det(\mathbf{A})\,\mathbf{I}$.

```
i4 : adj = matrix table(n, n, (j,k) -> (-1)^(j+k) *
         det submatrix(A, delete(k,{0,1,2}), delete(j,{0,1,2})))

o4 = | -x_6x_8+x_5x_9 x_6x_7-x_4x_9  -x_5x_7+x_4x_8 |
     | x_3x_8-x_2x_9  -x_3x_7+x_1x_9 x_2x_7-x_1x_8  |
     | -x_3x_5+x_2x_6 x_3x_4-x_1x_6  -x_2x_4+x_1x_5 |

              3      3
o4 : Matrix S  <-- S
```

```
i5 : assert(A*adj - det(A) * id_(S^3) == 0)
```

We construct the ‘graph’ ideal I for the rational parametrization and compute the elimination ideal J.

```
i6 : N = matrix{{0,1,0},{0,0,1_S},{0,0,0}}

o6 = | 0 1 0 |
     | 0 0 1 |
     | 0 0 0 |

              3      3
o6 : Matrix S  <-- S

i7 : M = A*N*adj;

              3      3
o7 : Matrix S  <-- S

i8 : B = genericMatrix(S, y_1, n, n)

o8 = | y_1 y_4 y_7 |
     | y_2 y_5 y_8 |
     | y_3 y_6 y_9 |

              3      3
o8 : Matrix S  <-- S

i9 : I = minors(1, det(A)*B-M) + ideal(1-det(A)*z);

o9 : Ideal of S

i10 : J = eliminate(I, {z} | toList(x_1 .. x_(n^2)));

o10 : Ideal of S

i11 : netList J_*

      +-----------------------------------------------------------+
o11 = |y  + y  + y                                                |
      | 1    5    9                                               |
      +-----------------------------------------------------------+
      |         2                              2                  |
      |y y  + y  + y y  + y y  + y y  + y                         |
      | 2 4    5    3 7    6 8    5 9    9                        |
      +-----------------------------------------------------------+
      |                                                          3|
      |y y y  - y y y  - y y y  - y y y  - y y y  - 2y y y  - y |
      | 3 5 7    2 6 7    3 4 8    5 6 8    3 7 9     6 8 9    9|
      +-----------------------------------------------------------+
```

The polynomials listed in `o11` define the smallest affine variety X containing the image of the rational map ρ.

ii. A (3×3)-matrix $\mathbf{B}$ is nilpotent if and only if its minimal polynomial p equal t^k for some nonnegative integer k. Since each irreducible factor of the characteristic polynomial of $\mathbf{B}$ is also a factor of p, it follows that the characteristic polynomial of $\mathbf{B}$ is t^3. We conclude that the coefficients of the characteristic polynomial of a generic

(3×3)-matrix define the affine variety X. We check that these polynomials generate the ideal J as follows.

```
i12 : J' = ideal substitute(contract(matrix{{z^2,z,1}}, det(z-B)), {z => 0_S});

o12 : Ideal of S

i13 : assert(J' == J)

i14 : netList J'_*

      +--------------------------------------------------+
o14 = |- y  - y  - y                                     |
      |   1    5    9                                    |
      +--------------------------------------------------+
      |- y y  + y y  - y y  - y y  + y y  + y y          |
      |   2 4    1 5    3 7    6 8    1 9    5 9         |
      +--------------------------------------------------+
      |y y y  - y y y  - y y y  + y y y  + y y y  - y y y|
      | 3 5 7    2 6 7    3 4 8    1 6 8    2 4 9    1 5 9|
      +--------------------------------------------------+
```

□

P4.2. For any polynomial $f = a_\ell \, x^\ell + a_{\ell-1} \, x^{\ell-1} + \cdots + a_0 \in \mathbb{C}[x]$ where $a_\ell \neq 0$ and $\ell > 0$, the ***discriminant*** of f is defined to be

$$\operatorname{disc}(f) = \frac{(-1)^{\ell(\ell-1)/2}}{a_\ell} \operatorname{Res}(f, f'; x) \, .$$

i. The polynomial $f \in \mathbb{C}[x]$ is ***separable*** if its has only simple roots. Show that f is separable if and only if f is relatively prime to its derivative f'.

ii. Prove that f has a multiple factor if and only if $\operatorname{disc}(f) = 0$.

iii. Does $6x^4 - 23x^3 + 32x^2 - 19x + 4$ have a multiple root in $\mathbb{C}$?

iv. Compute the discriminant of the quadratic polynomial $f = ax^2 + bx + c$. Explain how your answer relates to the quadratic formula.

Solution.

i. We first show that a complex number a is a simple root of f if and only if a is not a root of its derivative f'. The number a is a root of f if and only if $f = (x - a) \, g$ where g lies in $\mathbb{C}[x]$. For the number a to be a simple root of f, it is necessary and sufficient that $g(a) \neq 0$. Since $f' = g + (x - a) g'$, it follows that $f'(a) = g(a)$.

When the polynomials f and f' are relatively prime, there exists polynomials g and h in $\mathbb{C}[x]$ such that $g \, f + h \, f' = 1$. For any root a of the polynomial f, it follows that $1 = g(a) \, f(a) + h(a) \, f'(a) = h(a) \, f'(a)$. Hence, we have $f'(a) \neq 0$ and a is a simple root of f. Conversely, suppose that f and f' have a common factor g in $\mathbb{C}[x]$ such that $\deg(g) \geqslant 1$. The Fundamental Theorem of Algebra guarantees that g has a complex root $a \in \mathbb{C}$. It follows that a is a common root of f and f' which means that a is not a simple root of f.

ii. From part **i**, we know that f has a multiple root if and only if f and f' have a common factor. The polynomials f and f' have a common factor if and only if $\operatorname{Res}(f, f'; x) = 0$. Since $a_\ell \neq 0$, we see that $\operatorname{disc}(f) = 0$ if and only if $\operatorname{Res}(f, f'; x) = 0$.

iii. Given $f = 6x^4 - 23x^3 + 32x^2 - 19x + 4$, we have

$$\operatorname{disc}(f) = \frac{(-1)^{\ell(\ell-1)/2}}{a_\ell} \operatorname{Res}(f, f'; x) = \frac{1}{6} \det \begin{bmatrix} 6 & -23 & 32 & -19 & 4 & 0 & 0 \\ 0 & 6 & -23 & 32 & -19 & 4 & 0 \\ 0 & 0 & 6 & -23 & 32 & -19 & 4 \\ 24 & -69 & 64 & -19 & 0 & 0 & 0 \\ 0 & 24 & -69 & 64 & -19 & 0 & 0 \\ 0 & 0 & 24 & -69 & 64 & -19 & 0 \\ 0 & 0 & 0 & 24 & -69 & 64 & -19 \end{bmatrix}$$

$$= \frac{1}{6} \det \begin{bmatrix} 6 & -23 & 32 & -19 & 4 & 0 & 0 \\ 0 & 6 & -23 & 32 & -19 & 4 & 0 \\ 0 & 0 & 6 & -23 & 32 & -19 & 4 \\ 0 & 23 & -64 & 57 & -16 & 0 & 0 \\ 0 & 0 & 23 & -64 & 57 & -16 & 0 \\ 0 & 0 & 0 & 23 & -64 & 57 & -16 \\ 0 & 0 & 0 & 24 & -69 & 64 & -19 \end{bmatrix} = \det \begin{bmatrix} 6 & -23 & 32 & -19 & 4 & 0 \\ 0 & 6 & -23 & 32 & -19 & 4 \\ 1 & -28 & 71 & -60 & 16 & 0 \\ 0 & 1 & -28 & 71 & -60 & 16 \\ 0 & 0 & 23 & -64 & 57 & -16 \\ 0 & 0 & 1 & -5 & 7 & -3 \end{bmatrix}$$

$$= \det \begin{bmatrix} 145 & -394 & 341 & -92 & 0 \\ 0 & 145 & -394 & 341 & -92 \\ 1 & 0 & -69 & 136 & -68 \\ 0 & 0 & 51 & -104 & 53 \\ 0 & 1 & -5 & 7 & -3 \end{bmatrix} = \det \begin{bmatrix} 8376 & -17045 & 8678 \\ 331 & -674 & 343 \\ 51 & -104 & 53 \end{bmatrix} = 0\,.$$

Hence, f has a multiple root; one verifies that $f = (2x-1)(3x-4)(x-1)^2$.

iv. We have

$$\begin{aligned} \operatorname{disc}(f) &= \frac{(-1)^{\ell(\ell-1)/2}}{a_\ell} \operatorname{Res}(f, f'; x) \\ &= \frac{(-1)}{a} \begin{bmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{bmatrix} = (-1) \begin{bmatrix} 1 & b & c \\ 2 & b & 0 \\ 0 & 2a & b \end{bmatrix} = (-1) \begin{bmatrix} 1 & b & c \\ 0 & -b & -2c \\ 0 & 2a & b \end{bmatrix} \\ &= (-1)\big((-b)(b) - (2a)(-2c)\big) = b^2 - 4ac \end{aligned}$$

Thus, $\operatorname{disc}(f)$ is the polynomial under the square root in the quadratic formula $x = \frac{1}{2a}\big(-b \pm \sqrt{b^2 - 4ac}\big)$. When $\operatorname{disc}(f) = 0$, the double root is $-\frac{b}{2a}$. □

P4.3. Suppose that $f = a_m\, x^m + a_{m-1}\, x^{m-1} + \cdots + a_0$ and $g = b_m\, x^m + b_{m-1}\, x^{m-1} + \cdots + b_0$. Consider the polynomial in two variables

$$\varphi(x, y) = \frac{f(x)g(y) - g(x)f(y)}{x - y} = \sum_{j=0}^{m-1} \sum_{k=0}^{m-1} c_{j,k}\, x^j y^k\,.$$

i. When $m = 2$, show that $\operatorname{Res}(f, g; x) = (-1) \det\big[c_{j,k}\big]$.

ii. For any positive integer m, prove that $\operatorname{Res}(f, g; x) = (-1)^{m(m-1)/2} \det\big[c_{j,k}\big]$.

Solution. **i.** Since

$$\begin{aligned} & f(x)f(y) - g(x)f(y) \\ &= (a_2x^2 + a_1x + a_0)(b_2y^2 + b_1y + b_0) - (b_2x^2 + b_1x + b_0)(a_2y^2 + a_1y + a_0) \\ &= (a_2b_1 - a_1b_2)x^2y + (-a_2b_1 + a_1b_2)xy^2 + (a_2b_0 - a_0b_2)x^2 \\ &\qquad + (-a_2b_0 + a_0b_2)y^2 + (a_1b_0 - a_0b_1)x + (-a_1b_0 + a_0b_1)y \\ &= (x - y)\big((a_2b_1 - a_1b_2)xy + (a_2b_0 - a_0b_2)x + (a_2b_0 - a_0b_2)y + (a_1b_0 - a_0b_1)\big)\,, \end{aligned}$$

we deduce that

$$\begin{aligned}\operatorname{Res}(f,g;x) &= \det\begin{bmatrix} a_2 & a_1 & a_0 & 0 \\ 0 & a_2 & a_1 & a_0 \\ b_2 & b_1 & b_0 & 0 \\ 0 & b_2 & b_1 & b_0 \end{bmatrix} \\ &= a_2^2 b_0^2 - a_1 a_2 b_0 b_1 + a_0 a_2 b_1^2 + a_1^2 b_0 b_2 - 2 a_0 a_2 b_0 b_2 - a_0 a_1 b_1 b_2 + a_0^2 b_2^2 \\ &= (-1)\det\begin{bmatrix} a_1 b_0 - a_0 b_1 & a_2 b_0 - a_0 b_2 \\ a_2 b_0 - a_0 b_2 & a_2 b_1 - a_1 b_2 \end{bmatrix} .\end{aligned}$$

ii. Since

$$\begin{aligned} f(x)\,g(y) - g(x)\,f(y) &= \sum_{j=0}^{m}\sum_{k=0}^{m}(a_j\,b_k - a_k\,b_j)x^j y^k = \sum_{j=0}^{m-1}\sum_{k=j+1}^{m}(a_k\,b_j - a_j\,b_k)(x^k y^j - x^j y^k) \\ &= \sum_{j=0}^{m-1}\sum_{k=j+1}^{m}(a_k\,b_j - a_j\,b_k)x^j y^j (x^{k-j} - y^{k-j}) \\ &= (x-y)\sum_{j=0}^{m-1}\sum_{k=i+1}^{m}(a_k\,b_j - a_j\,b_k)x^j y^j \left(\sum_{i=0}^{k-j-1} x^i y^{k-j-1-i}\right) , \end{aligned}$$

we see that each $c_{j,k}$ is bihomogeneous of degree 1 in the variables a_j and b_k. Hence, the polynomials $R = (-1)^{m(m-1)/2}\det\left[c_{j,k}\right]$ and $\operatorname{Res}(f,g;x)$ are bihomogeneous of degree m in the variables a_j and b_k. The monomial $a_m\,b_0$ appears only in the polynomials $c_{k,m-1-k}$ for $0 \leqslant k \leqslant m-1$. Since the monomial $a_m\,b_0$ appears once in each of the antidiagonal entries of R and the sign of the permutation $\left(m \quad m-1 \quad \cdots \quad 3 \quad 2 \quad 1\right)$ is $(-1)^{m(m-1)/2}$, the coefficient of $a_m^m\,b_0^m$ in both R and $\operatorname{Res}(f,g,x)$ is 1. It remains to show that R vanishes whenever f and g have a common root. Given a common root λ of f and g, we have

$$\begin{aligned} 0 &= \varphi(\lambda, y) \\ &= \begin{bmatrix} 1 & \lambda & \lambda^2 & \cdots & \lambda^{m-1}\end{bmatrix} \begin{bmatrix} c_{0,0} & c_{0,1} & c_{0,2} & \cdots & c_{0,m-1} \\ c_{1,0} & c_{1,1} & c_{1,2} & \cdots & c_{1,m-1} \\ c_{2,0} & c_{2,1} & c_{2,2} & \cdots & c_{2,m-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ c_{m-1,0} & c_{m-1,1} & c_{m-1,2} & \cdots & c_{m-1,m-1} \end{bmatrix} \begin{bmatrix} 1 \\ y \\ y^2 \\ \vdots \\ y^{m-1} \end{bmatrix} \end{aligned}$$

As the vectors of the form $\begin{bmatrix} 1 & y & y^2 & \cdots & y^{m-1}\end{bmatrix}^{\mathsf{T}}$ span $\mathbb{C}^m$, it follows that the vector $\begin{bmatrix} 1 & \lambda & \lambda^2 & \cdots & \lambda^{m-1}\end{bmatrix}^{\mathsf{T}}$ lies in the kernel of the matrix $\left[c_{j,k}\right]^{\mathsf{T}}$, so $\det\left[c_{j,k}\right] = 0$. □

P4.4. A subset U of the polynomial ring $S := \mathbb{K}[x_1, x_2, \dots, x_n]$ is *multiplicatively closed* if any product of elements of U is also in U (including the empty product 1).

i. Let U be a multiplicatively closed subset of S. When an ideal I in S is maximal with respect to inclusion among all ideals not meeting U, show that I is prime.

ii. Let J be any proper ideal in S. Show that the radical ideal $\sqrt{J}$ is the intersection of all prime ideals containing J.

Solution. **i.** Suppose that the elements f and g in S are not in the ideal I. The maximality of I implies that both $I + \langle f \rangle$ and $I + \langle g \rangle$ meet the subset U. Hence, there are elements r

and s in S, and elements p and q in I such that $rf + p$ and $sg + q$ belong to U. Assuming that $fg \in I$, we would have $(rf + p)(sg + q) = rs(fg) + (rf)(q) + (sg + q)(p) \in I$. However, this contradicts the hypothesis that $I \cap U = \varnothing$. Therefore, the membership $fg \in I$ implies $f \in I$ or $g \in I$, so the ideal I is prime.

ii. Let $\mathcal{A}$ denote the set of prime ideals in S containing the ideal J. Since prime ideals are radical, we have $J \subseteq \sqrt{J} \subseteq \sqrt{P} = P$ for all $P \in \mathcal{A}$ and $\sqrt{J} \subseteq \bigcap_{P \in \mathcal{A}} P$. For the converse inclusion, consider an element f that does not belong to the radical $\sqrt{J}$. Part **i** implies that the ideal I maximal among all ideals not meeting $U := \{f^m \mid m \geqslant 0\}$ is prime. Therefore, we have $I \in \mathcal{A}$, $f \notin I$, and $f \notin \bigcap_{P \in \mathcal{A}} P$. □

P4.5. **i.** Find the minimal Gröbner basis for
$$\sqrt{\langle x^5 - 2x^4 + 2x^2 - x, x^5 - x^4 - 2x^3 + 2x^2 + x - 1 \rangle} \subset \mathbb{Q}[x] \,.$$

ii. Let $J = \langle xy, (x-y)x \rangle$. Describe $\mathrm{V}(J)$ and show that $\sqrt{J} = \langle x \rangle$.

Solution.

i. The ideal $\langle x^5 - 2x^4 + 2x^2 - x, x^5 - x^4 - 2x^3 + 2x^2 + x - 1 \rangle$ is generated by the greatest common divisor of $x^5 - 2x^4 + 2x^2 - x$ and $x^5 - x^4 - 2x^3 + 2x^2 + x - 1$, because $\mathbb{Q}[x]$ is a principal ideal domain. Since
$$x^5 - 2x^4 + 2x^2 - x = (x^5 - x^4 - 2x^3 + 2x^2 + x - 1) - (x^4 - 2x^3 + 2x - 1)$$
$$x^5 - x^4 - 2x^3 + 2x^2 + x - 1 = (x+1)(x^4 - 2x^3 + 2x - 1)\,,$$
we see that $\langle x^5 - 2x^4 + 2x^2 - x, x^5 - x^4 - 2x^3 + 2x^2 + x - 1 \rangle = \langle x^4 - 2x^3 + 2x - 1 \rangle$. As $x^4 - 2x^3 + 2x - 1 = (x+1)(x^3 - 3x^2 + 3x - 1) = (x+1)(x-1)^3$, we see that
$$\sqrt{\langle x^5 - 2x^4 + 2x^2 - x, x^5 - x^4 - 2x^3 + 2x^2 + x - 1 \rangle} \supseteq \langle (x+1)(x-1) \rangle = \langle x^2 - 1 \rangle \,.$$

When $g \in \sqrt{\langle x^4 - 2x^3 + 2x - 1 \rangle}$, it follows that $g^m \in \langle x^4 - 2x^3 + 2x - 1 \rangle$ for some positive integer m, which means g^m divisible by $x^4 - 2x^3 + 2x - 1$. We deduce that g is divisible by $x^2 - 1$ and $\sqrt{\langle x^4 - 2x^3 + 2x - 1 \rangle} = \langle x^2 - 1 \rangle$. Since $\mathbb{Q}[x]$ has a unique monomial order, the polynomial $x^2 - 1$ is the unique minimal Gröbner basis for the given ideal.

ii. The equation $xy = 0$ implies that $x = 0$ or $y = 0$. When $x = 0$, we have $(x-y)x = 0$ which implies that $\mathrm{V}(x) \subseteq \mathrm{V}(J)$. When $y = 0$, we have $0 = (x-y)x = x^2$ which implies that $x = 0$. Thus, we have $\mathrm{V}(x) = \mathrm{V}(J)$. Since
$$J = \langle xy, x^2 - xy \rangle = \langle x^2, xy \rangle = \langle x \rangle \cap \langle x^2, y \rangle \,,$$
we have $\sqrt{J} = \langle x \rangle \cap \langle x, y \rangle = \langle x \rangle$. □

References

[M2] The *Macaulay2* project authors, *Macaulay2, a software system for research in algebraic geometry*, 2024. available at https://macaulay2.com.