PMATH 764: Solutions to Assignment 3

In this assignment, we assume the field k to be infinite.

1. Determine whether or not the following are varieties.

   (a) The *orthogonal group*

   $$O(n,k) = \{A \in M_{n\times n}(k) : AA^T = I_{n\times n}\} \subset M_{n\times n}(k),$$

   when k has $\mathrm{char}(k) \neq 2$.

   Proof. Let $M_{n\times n}(k)$ be the set of $n \times n$ matrices with entries in k. If we identify a matrix $A = (a_{ij})$ with the point $(a_{11}, \ldots, a_{1n}, a_{21}, \ldots, a_{2n}, \ldots, a_{nn}) \in \mathbb{A}^{n^2}(k)$, then $AA^T = I_{n\times n}$ is clearly a set of n^2 polynomial equations in n^2 variables, so that $O(n,k)$ is an algebraic subset of $\mathbb{A}^{n^2}$. Nevertheless, any orthogonal matrix can either have determinant 1 or $-1 \neq 1$. Hence,

   $$O(n,k) = V(AA^T - I, \det A - 1) \cup V(AA^T - I, \det A + 1),$$

   implying that $O(n,k)$ is reducible and therefore *not* a variety. □

   (b) The *special unitary group* of complex 2×2 matrices

   $$SU(2,\mathbb{C}) = \{A \in M_{2\times 2}(\mathbb{C}) : A\bar{A}^T = I_{2\times 2}, \det A = 1\} \subset M_{2\times 2}(\mathbb{C}).$$

   Proof. Note that $SU(2,\mathbb{C})$ consists if 2×2 matrices of the form

   $$A = \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}$$

   with $a, b \in \mathbb{C}$ and $\det(A) = 1$. Hence, $SU(2,\mathbb{C})$ can be thought of as a subset of $\mathbb{C}^4$ as follows:

   $$SU(2,\mathbb{C}) = \{(x,y,z,w) \in \mathbb{C}^4 : z = -\bar{y}, w = \bar{x} \text{ and } x\bar{x} + y\bar{y} = 1\}.$$

   Let us show that $SU(2,\mathbb{C})$ is not algebraic, thus implying it is *not* a variety. Suppose instead that $SU(2,\mathbb{C})$ is algebraic. Then $SU(2,\mathbb{C}) \cap V(y,z)$ is also an algebraic subset of $\mathbb{C}^4$, and in particular a closed subset of $V(y,z) = \mathbb{C}^2$. However,

   $$SU(2,\mathbb{C}) \cap V(y,z) = \{(x,w) : w = \bar{x} \text{ and } xw = 1\} \subset V(y,z),$$

   which can be identified with the unit circle in $\mathbb{C}$. Consequently, $SU(2,\mathbb{C}) \cap V(y,z)$ is an infinite *proper* closed subset of $V(xw-1) \subset V(y,z) = \mathbb{C}^2$, which is impossible since $V(xw-1) \subset \mathbb{C}^2$ is the zero set of the irreducible polynomial $xw - 1$ (see Corollary 1.5.2 in the lecture notes). Therefore, $SU(2,\mathbb{C})$ is not algebraic. □

   (c) $V(xz - y^2, yz - x^3, z^2 - x^2y) \subset \mathbb{C}^3$.

   Proof. Let $X = V(xz - y^2, yz - x^3, z^2 - x^2y)$. Note that if $(x,y,z) \in X$, then $x = y = z = 0$ or $xyz \neq 0$; one can also easily verify that $y^3 = x^4$, $z^3 = x^5$ and $z^4 = y^5$. Let us construct a surjective polynomial map $\varphi : \mathbb{A}^1 \to X \subset \mathbb{C}^3, t \mapsto (p(t), q(t), r(t))$. Since $y^3 = x^4$ and $z^4 = y^5$, a natural choice seems to be $\varphi(t) = (t^3, t^4, t^5)$. We clearly have $\varphi(\mathbb{A}^1) \subseteq X$. Let us show that φ is surjective. We have $(0,0,0) = \varphi(0)$. Let $(x_0, y_0, z_0) \neq (0,0,0)$ be any other point in X. Then, $x_0y_0z_0 \neq 0$, so that $x_0 \neq 0$, and $(x_0, y_0, z_0) = \varphi(y_0/x_0)$ since $y_0^3 = x_0^4$, $z_0^3 = x_0^5$ and $z_0^4 = y_0^5$, proving that φ is surjective. Thus, since $\mathbb{A}^1$ is irreducible, $X = \varphi(\mathbb{A}^1)$ is irreducible. □

2. Show that $X = V(y^2 - x^3) \subset \mathbb{A}^2$ is not isomorphic to $\mathbb{A}^1$.

Proof. We already know that $\Gamma(X) = k[\bar{x}, \bar{y}]$ with the residue classes $\bar{x}$ and $\bar{y}$ satisfying the relation $\bar{y}^2 = \bar{x}^3$. Let us show that $\Gamma(X) \not\simeq k[t] = \Gamma(\mathbb{A}^1)$ as a k-algebra, which will prove that $X \not\simeq \mathbb{A}^1$. Let us do this by showing that $\Gamma(X)$ is not a UFD (whereas $k[t]$ is a UFD). Since $\bar{y}^2 = \bar{x}^3$, if we can show that $\bar{x}$ and $\bar{y}$ are irreducible, then we are done. Let us do it for $\bar{x}$, the proof for $\bar{y}$ being similar. Let us assume instead that $\bar{x}$ can be written as $\bar{x} = ab$ for some $a, b \in \Gamma(X)$. Consider the surjective polynomial map

$$\begin{array}{cccc} \varphi : & \mathbb{A}^1 & \to & X \subset \mathbb{A}^2 \\ & t & \mapsto & (t^2, t^3), \end{array}$$

whose pullback is given by

$$\begin{array}{cccc} \phi^* : & \Gamma(X) & \to & k[t] \\ & \bar{x} & \mapsto & t^2 \\ & \bar{y} & \mapsto & t^3. \end{array}$$

Then, $\varphi^*(a)\varphi^*(b) = \varphi^*(\bar{x}) = t^2$. Since $k[t]$ is a UFD, this means we have three possibilities:

(i) $\varphi^*(a) = \alpha t^2$ and $\varphi^*(b) = 1/\alpha$ for some $\alpha \in k^*$;

(ii) $\varphi^*(a) = \alpha t$ and $\varphi^*(b) = t/\alpha$ for some $\alpha \in k^*$;

(iii) $\varphi^*(a) = \alpha$ and $\varphi^*(b) = t^2/\alpha$ for some $\alpha \in k^*$.

However, the image of φ^* does not contain t, so only (i) or (iii) can occur, say (i). Thus, $\varphi^*(a) = \alpha t^2$. But φ^* is injective since φ is surjective and therefore dominant (see 2.(a)). Hence, $a = \bar{x}/\alpha$ and $b = \alpha$, proving that $\bar{x}$ is irreducible. $\square$

3. Let $X \subset \mathbb{A}^n$ and $Y \subset \mathbb{A}^m$ be two varieties, and $\phi : X \to Y$ be a polynomial map.

   (a) Show that ϕ^* is injective if and only if $\overline{\phi(X)} = Y$.

   Proof. For any $\bar{g} \in \Gamma(Y)$, $\phi^*(\bar{g}) = 0$ if and only if $\overline{g \circ \varphi} = 0$ in $\Gamma(X)$, which occurs if and only if $g(\phi(x)) = 0$ for all $x \in X$. In other words, $\phi^*(\bar{g}) = 0$ if and only if $g \in I(\phi(X))$, implying that the kernel of ϕ^* is $I(\phi(X))$. Nevertheless, ϕ^* is injective if and only if its kernel is $I(Y)$. Consequently, ϕ^* is injective if and only if $I(Y) = I(\phi(X))$, which in turns happens if and only if $Y = V(I(Y)) = V(I(\phi(X))) = \overline{\phi(X)}$. $\square$

   (b) Show that ϕ^* is surjective if and only if ϕ has a polynomial left inverse (that is, a polynomial map $\psi : Y \to \mathbb{A}^n$ such that $\psi \circ \phi = \mathrm{id}_X$).

   Proof. Suppose that ϕ^* is surjective. Then, if $X \subseteq \mathbb{A}^n$ and $x_1, \ldots, x_n$ are ambient coordinates in $\mathbb{A}^n$, we have $\Gamma(X) = k[x_1, \ldots, x_n]/I(X)$ and, for every x_i, there exists $\bar{f}_i \in \Gamma(Y)$ such that $\phi^*(\bar{f}_i) = \bar{x}_i$. Let $\psi : Y \to \mathbb{A}^n$ be the map given by $y \mapsto (f_1(y), \ldots, f_n(y))$. Then, $\bar{f}_i = \psi^*(\bar{x}_i)$ and

   $$(\psi \circ \phi)^*(\bar{x}_i) = \phi^* \circ \psi^*(\bar{x}_i) = \phi^*(\bar{f}_i) = \bar{x}_i,$$

   for every i, implying that $(\psi \circ \phi)^* = \phi^* \circ \psi^*|_{\Gamma(X)} = id_{\Gamma(X)} = (id_X)^*$. Thus, $\psi \circ \phi = id_X$ and ψ is a left inverse of ϕ. $\square$

4. Let k be an algebraically closed field with characteristic $p > 0$. Consider the map $\phi : \mathbb{A}^1 \to \mathbb{A}^1$ defined by $t \mapsto t^p$; this is called the *Frobenius morphism*. Show that ϕ is bijective but not an isomorphism.

Proof. We first note that the equation $t^p = a$ has a solution for all $a \in \mathbb{A}^1$, since k is algebraically closed, implying that ϕ is surjective. Moreover, if $\phi(t_1) = \phi(t_2)$, then $t_1^p = t_2^p$. But the characteristic of k is p, so $(t_1 - t_1)^p = t_1^p - t_2^p = 0$, implying that $t_1 - t_2 = 0$ since k is a field. Hence, $t_1 = t_2$ and ϕ is a bijection. Nevertheless,

$$\begin{array}{rcl} \phi^* : k[t] & \to & k[t] \\ t & \mapsto & t^p \end{array}$$

is not surjective since t is not in the image of ϕ^*. Consequently, since ϕ^* is not an isomorphism, ϕ cannot be an isomorphism. □

5. Let $X = V(y^2 - x^2(x+1)) \subset \mathbb{A}^2$. Let $z = \bar{y}/\bar{x} \in k(X)$. What are the pole sets of z and z^2? Are z and z^2 in $\Gamma(X)$? Justify your answer.

   Proof. We first note that z may be undefined when $\bar{x} = 0$, which corresponds to the point $(0,0)$ on X. Suppose, on the contrary that, that z is defined at $(0,0)$. There then exist $a, b \in \Gamma(X)$ such that $b(0,0) \neq 0$ and $z = a/b$, or equivalently $a\bar{x} = b\bar{y}$. Lifting to $k[x,y]$, we have

   $$\tilde{a}x = \tilde{b}y + (y^2 - x^2(x+1))h, \tag{*}$$

   for some $\tilde{a}, \tilde{b}, h \in k[x,y]$. Since $\tilde{b}(0,0) = b(0,0) \neq 0$, $\tilde{b}$ has a non-zero constant term, implying that the right-hand of (*) has a linear term in y, whereas every term on the right-hand side of (*) is a multiple of x, a contradiction. The point $(0,0)$ is therefore the (only) pole of z; moreover, since z has a pole, $z \notin \Gamma(X)$. However, $z^2 = \bar{y}^2/\bar{x}^2 = \bar{x}^2(\bar{x}+1)/\bar{x}^2 = \bar{x}+1$ on X, which is defined everywhere, i.e., the pole set of z^2 is empty and $z^2 \in \Gamma(X)$. □

6. *Classification of irreducible conics in* $\mathbb{A}^2$. The zero set of an irreducible polynomial $f \in k[x,y]$ of degree two is called an *irreducible conic* in $\mathbb{A}^2$. You may suppose that the field k is algebraically closed and has $\mathrm{char}(k) = 0$.

   (a) Show that any irreducible conic in $\mathbb{A}^2$ is isomorphic to $V(y - x^2)$ or $V(x^2 + y^2 - 1)$ under an appropriate affine coordinate change.

   Proof. Let us show that the zero set of any irreducible conic in $\mathbb{A}^2$ is isomorphic to $V(y - x^2)$ or $V(x^2 + y^2 - 1)$ under an appropriate affine coordinate change. Consider the irreducible quadratic polynomial

   $$p(x,y) = ax^2 + bxy + cy^2 + dx + ey + f.$$

   Let us first show that, after an appropriate affine transformation, p can be written as $au^2 + Bv^2 + du + Ev + f$. We can clearly only consider the case where $b \neq 0$, otherwise we are done. Let us first assume that $a = c = 0$ so that

   $$p(x,y) = bxy + dx + ey + f = (bx + d)\left(y + \frac{e}{b}\right) + \left(f - \frac{de}{b}\right).$$

   The affine coordinate change $\{bx + d = \alpha(u + iv), y + (e/b) = \alpha(u - iv)\}$, where $\alpha^2 = (de/b - f)$, transforms p into $\alpha^2(u^2 + v^2 - 1)$.
   Let us now assume that $a \neq 0$. Then,

   $$p(x,y) = a\left(x + \frac{by}{2a}\right)^2 + \left(c - \frac{b^2}{2a}\right)y^2 + d\left(x + \frac{by}{2a}\right) + \left(e - \frac{bd}{2a}\right)y + f.$$

   The affine coordinate change $\{x + (by/2a) = u, y = v\}$ then transforms p into a polynomial of the desired form. Finally, if $c \neq 0$, the affine transformation $(x,y) \mapsto (y,x)$ takes us back to the previous case.

Let us now assume that p has the form

$$p(x, y) = ax^2 + by^2 + cx + dy + e.$$

If $b = 0$, then b can be written as

$$p(x, y) = \left(dy + e - \frac{c^2}{4a}\right) - \left(\alpha x + \frac{c}{2\alpha}\right)^2,$$

where $\alpha^2 - -a$, so that the affine coordinate change $\{dy + e - (c^2/4a) = u, \alpha x + (c/2\alpha) = v\}$ transforms p into $v - u^2$.

Finally, if $b \neq 0$, then

$$p(x, y) = \left(\alpha x + \frac{c}{2\alpha}\right)^2 + \left(\beta y + \frac{d}{2\beta}\right)^2 + \left(e - \frac{1}{4}\left(\frac{c^2}{a} + \frac{d^2}{b}\right)\right),$$

where $\alpha^2 = a, \beta^2 = b$ and $\gamma^2 = ((c^2/a) + (d^2/b))/4 - e$, so that the affine coordinate change $\{\alpha x + (c/2\alpha) = \alpha u, \beta y + (d/2\beta) = \gamma v\}$ takes p to $\gamma^2(u^2 + v^2 - 1)$.

Consequently, since affine transformations are isomorphisms, this shows that $V(p) \simeq V(y - x^2)$ or $V(x^2 + y^2 - 1)$ for any irreducible quadratic polynomial p. $\square$

(b) Prove that although the parabola $V(y - x^2)$ is isomorphic to $\mathbb{A}^1$, the unit circle $V(x^2 + y^2 - 1)$ is not.

Proof. $V(y - x^2)$ is isomorphic to $\mathbb{A}^1$ since

$$\Gamma(V(y - x^2)) = k[\bar{x}] \simeq k[t] = \Gamma(\mathbb{A}^1).$$

However, $x^2 + y^2 - 1 = (x + iy)(x - iy) - 1 = st - 1$ with $s = x + iy$ and $t = x - iy$; the affine transformation $(x, y) \mapsto (x + iy, x - iy)$ therefore maps $V(x^2 + y^2 - 1)$ isomorphically onto $V(st - 1)$. But we saw in class that $V(st - 1) \not\simeq \mathbb{A}^1$. We have nonetheless shown in class that $V(y - x^2)$ and $V(x^2 + y^2 - 1)$ are both birational to $\mathbb{A}^1$. Since isomorphisms are birational equivalences, this means that any irreducible conic in $\mathbb{A}^2$ is birational to $V(y - x^2)$ or $V(x^2 + y^2 - 1)$, and therefore birational to $\mathbb{A}^1$ $\square$

(c) Consider the unit circle $X = V(x^2 + y^2 - 1)$. The *stereographic projection* of X from the north pole $N = (0, 1) \in X$ onto the x-axis maps a point $P \in X$ to the point of intersection P' of the x-axis with the line passing through N and P (see). Verify that the stereographic projection is given by the rational map $\phi : X \to \mathbb{A}^1, (x, y) \mapsto x/(1 - y)$, where the x-axis is identified with $\mathbb{A}^1$ by sending $(x, 0)$ to x. Show that ϕ is a birational equivalence, thus proving that X is a rational curve. Consequently, all irreducible conics in $\mathbb{A}^2$ are rational.

Proof. $V(y - x^2)$ is isomorphic to $\mathbb{A}^1$ since

$$\Gamma(V(y - x^2)) = k[\bar{x}] \simeq k[t] = \Gamma(\mathbb{A}^1).$$

However, $x^2 + y^2 - 1 = (x + iy)(x - iy) - 1 = st - 1$ with $s = x + iy$ and $t = x - iy$; the affine transformation $(x, y) \mapsto (x + iy, x - iy)$ therefore maps $V(x^2 + y^2 - 1)$ isomorphically onto $V(st - 1)$. But we saw in class that $V(st - 1) \not\simeq \mathbb{A}^1$. We have nonetheless shown in class that $V(y - x^2)$ and $V(x^2 + y^2 - 1)$ are both birational to $\mathbb{A}^1$. Since isomorphisms are birational equivalences, this means that any irreducible conic in $\mathbb{A}^2$ is birational to $V(y - x^2)$ or $V(x^2 + y^2 - 1)$, and therefore birational to $\mathbb{A}^1$ $\square$

Note. An affine variety is said to be *rational* if it is birational to $\mathbb{A}^m$ for some $m \geq 1$.