18.725 SOLUTIONS TO PROBLEM SET 3

Required Problem 1: Let V be a quasi-affine algebraic set and let $U \subset V$ be a closed subset. For every quasi-affine algebraic set T and every function $F : T \to U$, prove F is regular iff the induced function $F : T \to V$ is regular (this has already been used implicitly a few times in the course; do not simply quote the result from someplace it was used).

Solution: The simplest solution for this problem solves the next problem as well. The argument is in the following lemmas and proposition.

Lemma 0.1. *For every quasi-affine algebraic subset $T \subset \mathbb{A}^m_k$ and every regular function $g \in \mathcal{O}_T(T)$ which is everywhere nonzero, the function $1/g : T \to \mathbb{A}^1_k$ is also regular.*

Proof. It suffices to prove for every point $p \in T$, $1/g$ is regular at p. Because g is regular at p, there exist polynomials $s, u \in k[y_1, \dots, y_m]$ such that $u(p) \neq 0$ and such that the restriction of g to $T \cap D(u)$ equals the restriction of s/u to $T \cap D(u)$. Because g is nonzero, the restriction of s to $T \cap D(u)$ is nonzero. Therefore p is contained in $T \cap D(su)$, and the restriction of $1/g$ equals $u/s = u^2/su$, i.e., $1/g$ is regular at p. □

Lemma 0.2. *For every inclusion of quasi-affine algebraic subsets $U \subset V \subset \mathbb{A}^n_k$, the inclusion mapping $i : U \to V$ is a regular morphism.*

Proof. It suffices to prove for every regular function $g : V \to \mathbb{A}^1_k$ and every $p \in U$, the function $g \circ i$ is regular at p. Because g is regular at $i(p)$, there exist polynomials $h, s \in k[x_1, \dots, x_n]$ such that $s(p) \neq 0$ and the restriction of g to $V \cap D(s)$ equals h/s. The restriction of $g \circ i$ to $U \cap D(s)$ equals h/s, i.e., $g \circ i$ is regular at p. □

Proposition 0.3. *For every inclusion of quasi-affine algebraic sets $U \subset V \subset \mathbb{A}^n_k$, for every quasi-affine algebraic subset $T \subset \mathbb{A}^m_k$, and for every mapping $F : T \to U$, F is a regular morphism of quasi-affine algebraic sets iff $i \circ F$ is a regular morphism of quasi-affine algebraic sets.*

Proof. By the second lemma i is a regular morphism. If F is a regular morphism, then $i \circ F$ is a regular morphism because the composition of regular morphisms is a regular morphism.

Assume $i \circ F$ is a regular morphism. To prove F is a regular morphism, it suffices to prove for every regular function $g \in \mathcal{O}_U(U)$ and every $p \in T$, $g \circ F$ is regular at p. Because g is regular at $F(p)$, there exist polynomials $h, s \in k[x_1, \dots, x_n]$ such that $s(F(p)) \neq 0$ and such that the restriction of g to $U \cap D(s)$ equals h/s. Since $i \circ F$ is regular, $W := (i \circ F)^{-1}(V \cap D(s))$ is open and $h \circ i \circ F$ and $s \circ i \circ F$ are regular functions on T. By the second lemma, the inclusion $j : W \to T$ is a regular morphism so that $h' := h \circ i \circ F \circ j$ and $s' := s \circ i \circ F \circ j$ are regular functions on W. Since s' is everywhere nonzero, the first lemma implies $1/s'$ is a regular function on W. Therefore the product $h'/s' = h' \cdot (1/s')$ is a regular function on W. The restriction of $g \circ F$ to W equals the regular function h'/s', in particular $g \circ F$ is regular at p. $\square$

Required Problem 2: Let V be a quasi-affine algebraic set and let $U \subset V$ be an open subset. For every quasi-affine algebraic set T and every function $F : T \to U$, prove F is regular iff the induced function $F : T \to V$ is regular (this has already been used implicitly a few times in the course; do not simply quote the result from someplace it was used). **Not to be written up:** Conclude that for every subset $U \subset V$ that is a quasi-affine algebraic set and every $F : T \to U$, F is regular iff the induced function $F : T \to V$ is regular.

Solution: See the solution of the last problem.

Required Problem 3: Let V be a quasi-affine algebraic set. By Problem 2 on Problem Set 2, there exists a product $(V \times V, \pi_1, \pi_2)$ for (V, V) in the category of quasi-affine algebraic sets. Define $\Delta_V : V \to V \times V$ to be the unique morphism such that $\pi_1 \circ \Delta_V = \pi_2 \circ \Delta_V = \mathrm{Id}_V$. Prove the image of Δ_V is a Zariski closed subset of $V \times V$. (**Hint:** First consider the case that $V = \mathbb{A}_k^n$.)

Solution: Let $V \subset \mathbb{A}_k^n$ be a quasi-affine algebraic set. Then $\Delta_V(V) \subset V \times V$ equals the intersection $(V \times V) \cap \Delta_{\mathbb{A}_k^n}(\mathbb{A}_k^n)$ inside $\mathbb{A}_k^n \times \mathbb{A}_k^n$. So to prove $\Delta_V(V) \subset V \times V$ is relatively closed, it suffices to prove that $\Delta_{\mathbb{A}_k^n}(\mathbb{A}_k^n) \subset \mathbb{A}_k^n \times \mathbb{A}_k^n$ is closed.

A product for $(\mathbb{A}_k^n, \mathbb{A}_k^n)$ is $(\mathbb{A}_k^{2n}, \pi_1, \pi_2)$,

$$\pi_1(a_1, \ldots, a_n, a_{n+1}, \ldots, a_{2n}) = (a_1, \ldots, a_n),$$
$$\pi_2(a_1, \ldots, a_n, a_{n+1}, \ldots, a_{2n}) = (a_{n+1}, \ldots, a_{2n})$$

Denote by $z_1, \ldots, z_n, z_{n+1}, \ldots, z_{2n}$ the standard coordinates on $\mathbb{A}_k^{2n}$. Then $\Delta_{\mathbb{A}_k^n}(\mathbb{A}_k^n) \subset \mathbb{A}_k^{2n}$ equals $\mathbb{V}(\langle z_{n+1} - z_1, \ldots, z_{n+i} - z_i, \ldots, z_{2n} - z_n\rangle)$, which is a closed subset.

Required Problem 4: Consider the action of $\mathbb{G}_m$ on $X = \mathbb{A}_k^3$ by $m_X(\lambda, (a_1, a_2, a_3)) = (\lambda^{-1}a_1, a_2, \lambda a_3)$.

(a) Determine the associated grading of $k[X] = k[x_1, x_2, x_3]$, and in particular write a finite set of generators of the k-subalgebra $k[X]_0 \subset k[X]$.

Solution: For every integer d,

$$k[X]_d = \text{span}\left\{x_1^{d_1}x_2^{d_2}x_3^{d_3} | (d_1, d_2, d_3) \in \mathbb{Z}^3, \quad d_3 - d_1 = d\right\}.$$

In particular the k-subalgebra $k[X]_0 \subset k[X]$ is generated by x_2 and x_1x_3. More precisely, $k[X]_0$ is isomorphic to the polynomial algebra $k[y_1, y_2]$ where $y_1 \mapsto x_2$ and $y_2 \mapsto x_1x_3$. For every $d > 0$, $k[X]_d$ is a free $k[X]_0$-module generated by x_3^d. For every $d < 0$, $k[X]_d$ is a free $k[X]_0$-module generated by x_1^d (neither of these modules were asked for).

(b) Find an affine algebraic set Y and a morphism $F : X \to Y$ such that $F^* : k[Y] \to k[X]$ is injective with image $k[X]_0$. Prove that $F(m_X(\lambda, p)) = F(p)$ for every $\lambda \in \mathbb{G}_m$ and every $p \in X$.

Solution: Let $Y = \mathbb{A}_k^2$ and let $F = (x_2, x_1x_3)$. Then $F^* : k[y_1, y_2] \to k[x_1, x_2, x_3]$ is $y_1 \mapsto x_2$, $y_2 \mapsto x_1x_3$. By the last part, the image of F^* is $k[X]_0$ and $F^* : k[Y] \to k[X]_0$ is an isomorphim of k-algebras. Because the coordinates of F are $\mathbb{G}_m$-invariant, F is $\mathbb{G}_m$-invariant.

Problem 5: For the morphism F in Problem 4, write down all elements $q \in Y$ such that $F^{-1}(q)$ is not a single orbit of $\mathbb{G}_m$, and for each element q write the decomposition of $F^{-1}(q)$ as a union of $\mathbb{G}_m$-orbits.

Solution: Let $p = (a_1, a_2, a_3) \in X$ be a point such that $a_1, a_3 \neq 0$. Let $p' = (b_1, b_2, b_3) \in X$ be a point such that $F(p') = F(p)$. Then $b_2 = a_2$ and $b_1 b_3 = a_1 a_3$. In particular, $b_1, b_3 \neq 0$. So $\lambda := b_3/a_3$ is nonzero and $b_1 = (a_3/b_3)a_1 = \lambda^{-1}a_1$. So $(b_1, b_2, b_3) = m_X(\lambda, (a_1, a_2, a_3))$. Therefore the fiber of F containing p is a single orbit. So if $q = (c_1, c_2) \in Y$ is a point such that $c_2 \neq 0$, then $F^{-1}(q)$ is a single orbit.

On the other hand, suppose that $c_2 = 0$. Then $F^{-1}(q) = \{(a_1, c_1, 0) | a_1 \in k\} \cup \{(0, c_1, 0)\} \cup \{(0, c_1, a_3) | a_3 \in k\}$ is a union of 3 $\mathbb{G}_m$-orbits.

Problem 6: Let $F : X \to Y$ be a regular morphism of quasi-affine algebraic sets. Let $(X \times Y, \pi_1, \pi_2)$ be a product of (X, Y) in the category of quasi-affine algebraic sets. Define $\Gamma_F : X \to X \times Y$, the *graph morphism of* F, to be the unique morphism such that $\pi_1 \circ \Gamma_F = \mathrm{Id}_X$ and $\pi_2 \circ \Gamma_F = F$. Prove the image of Γ_F is a Zariski closed subset of $X \times Y$. (**Hint**: Can you use Problem 3?)

Solution: Consider the morphism $G = (F \circ \pi_1) \times \pi_2 : X \times Y \to Y \times Y$. The inverse image under G of $\Delta_Y(Y) \subset Y \times Y$ is $\{(p, q) \in X \times Y | F(p) = q\}$, i.e., precisely $\Gamma_F(X)$. By Problem 3, $\Delta_Y \subset Y \times Y$ is closed. Because G is continuous, $\Gamma_F(X) = G^{-1}(\Delta_Y(Y))$ is closed.

Problem 7. A weighted projective space: Consider the action of $\mathbb{G}_m$ on $X = \mathbb{A}^3$ by $m_X(\lambda, (a_0, a_1, a_2)) = (a_0, \lambda a_1, \lambda^2 a_2)$. Define $V = X - \mathbb{V}(x_1, x_2)$, and define $F : V \to \mathbb{P}^3_k$ by $F(a_0, a_1, a_2) = [a_1^2, a_2, a_0 a_1^2, a_0 a_2]$.

(a) Prove that F is a well-defined function on V.

Solution: Define $G : X \to \mathbb{A}^4_k$ by $G(a_0, a_1, a_2) = (a_1^2, a_2, a_0 a_1^2, a_0 a_2)$. Because it is a polynomial mapping, G is a regular morphism. If $p = (a_0, a_1, a_2) \in V$, then either $a_1 \neq 0$ or $a_2 \neq 0$. Therefore either $a_1^2 \neq 0$ or $a_2 \neq 0$. So $G(p) \neq 0$. Therefore there is a well-defined mapping $G|_V : V \to \mathbb{A}^4_k - \{0\}$. By Problem 2, this mapping is a regular morphism. And $\pi : \mathbb{A}^4_k \to \mathbb{P}^3_k$ is a regular morphism. Therefore $F = \pi \circ G|_V : V \to \mathbb{P}^3_k$ is a well-defined regular morphism.

(b) Prove that every nonempty fiber of F is an orbit.

Solution: Let $q = [b_0, b_1, b_2, b_3]$ be an element of $\mathbb{P}^3_k$, and let $p = (a_0, a_1, a_2)$ and $p' = (a_0', a_1', a_2')$ be points in $F^{-1}(q)$. If $b_1 = 0$, then $a_2 = a_2' = 0$. Thus $a_1, a_1' \neq 0$. Define $\lambda = a_1'/a_1$. Then $((a_1')^2, 0, a_0'(a_1')^2, 0) = \lambda^2(a_1^2, 0, a_0 a_1^2, 0)$. In particular, $a_0' = \lambda^2(a_1/a_1')^2 a_0 = a_0$. So $(a_0', a_1', 0) = m_X(\lambda, (a_0, a_1, a_2))$. So if $b_1 = 0$, then $F^{-1}(q)$ is an orbit.

Similarly, if $b_0 = 0$, then $a_1 = a_1' = 0$, thus $a_2, a_2' \neq 0$. Let $\lambda \in k$ be such that $a_2'/a_2 = \lambda^2$. Then $(0, a_2', 0, a_0' a_2') = \lambda^2(0, a_2, 0, a_0 a_2)$; in particular, $a_0' = \lambda^2(a_2/a_2')a_0 = a_0$. So $(a_0', 0, a_2') = m_X(\lambda, (a_0, 0, a_2))$. So if $b_0 = 0$, then $F^{-1}(q)$ is an orbit.

Now assume $b_0, b_1 \neq 0$. Then $a_1, a_1' \neq 0$. Define $\lambda = a_1'/a_1$. Then $((a_1')^2, a_2', a_0'(a_1')^2, a_0' a_2') = \lambda^2(a_1^2, a_2, a_0 a_1^2, a_0 a_2)$. Therefore $a_2' = \lambda^2 a_2$ and $a_0' = \lambda^2(a_1/a_1')^2 a_0 = a_0$. So $(a_0', a_1', a_2') = m_X(\lambda, (a_0, a_1, a_2))$. So $F^{-1}(q)$ is an orbit.

(c) Find the ideal of the Zariski closure of Image(F) and give an element in the Zariski closure of Image(F) that is not in Image(F).

Solution: Let y_0, y_1, y_2, y_3 be the standard homogeneous coordinates on $\mathbb{P}^3_k$. Then the Zariski closure of Image(F) is $V = \mathbb{V}(y_0y_3 - y_1y_2)$. The complement $V -$ Image(F) is $\{[0,0,0,1],[0,0,1,0]\}$.

Problem 8: This problem gives another example of an affine group variety. Let $n \geq 1$ be an integer and choose coordinates on $\mathbb{A}^{n^2}_k$ of the form $x_{i,j}$, $1 \leq i,j \leq n$. Define the determinant polynomial $\det \in k[x_{i,j} | 1 \leq i,j \leq n]$ in the usual way,

$$\det = \sum_{\sigma \in \mathfrak{S}_n} \mathrm{sgn}(\sigma) \prod_{i=1}^{n} x_{i,\sigma(i)},$$

where $\mathrm{sgn} : \mathfrak{S}_n \to \{+1,-1\}$ is the unique nontrivial group homomorphism. Define $\mathbf{GL}_n \subset \mathbb{A}^{n^2}_k$ to be $D(\det)$. Define $m : \mathbf{GL}_n \times \mathbf{GL}_n \to \mathbb{A}^{n^2}_k$ to be $m((a_{i,j}),(b_{i,j})) = (c_{i,j})$, where $c_{i,j} = \sum_{h=1}^{n} a_{i,h}b_{h,j}$. Define $e \in \mathbf{GL}_n$ to be the unique element such that $x_{i,j}(e) = 1$ iff $i = j$ and is 0 otherwise.

(a) Prove the image of m is contained in $\mathbf{GL}_n$.

Solution: By standard linear algebra, the polynomial $\det(m((x_{i,j}),(y_{i,j})))$ is the polynomial $\det((x_{i,j}))\cdot\det((y_{i,j}))$. Therefore the pullback of det by m is everywhere nonzero. So the image of m is contained in $\mathbf{GL}_n$.

(b) Prove there exists a regular morphism $i : \mathbf{GL}_n \to \mathbf{GL}_n$ such that for every $A \in \mathbf{GL}_n$, $m(A, i(A)) = e$.

Solution: This is precisely Cramer's rule, or cofactor expansion, from linear algebra: cofactor expansion expresses each entry of the inverse matrix as a ratio whose numerator is a polynomial in the entries, and whose denominator is the determinant.

(c) Prove the regular morphism $\det : \mathbf{GL}_n \to \mathbb{G}_m$ is a group homomorphism.

Solution: This is the same linear algebra fact used in (a).

Problem 9: Assume $\mathrm{char}(k) \neq 2$. A *projective plane conic* is a proper closed subset $C \subset \mathbb{P}^2_k$ of the form $\mathbb{V}(a_{2,0,0}X_0^2 + a_{1,1,0}X_0X_1 + a_{1,0,1}X_0X_2 + a_{0,2,0}X_1^2 + a_{0,1,1}X_1X_2 + a_{0,0,2}X_2^2)$. Determine the analogue of Problem 6 from Problem Set 1 for projective plane conics, and solve the corresponding problem. How does your answer compare to the answer to Problem 6 from Problem Set 1?

Problem 10: Let $d \geq 1$ be an integer and assume that $\mathrm{char}(k)$ does not divide d. Define $\mu_d \subset \mathbb{A}^1_k$ to be $\mathbb{V}(x^d - 1)$.

(a) Prove this is a subgroup of $\mathbb{G}_m$.

Solution: This is a closed subset of $\mathbb{G}_m$. It is necessary to prove that $m^{-1}(\mu_d)$ contains $\mu_d \times \mu_d$, e is in μ_d and $i^{-1}(\mu_d)$ contains μ_d. First of all, $m^*(x^d - 1) = (yz)^d - 1 = (y^d-1)(z^d-1) + (y^d-1) + (z^d-1)$, where y, z are coordinates on the two factors of $\mathbb{G}_m \times \mathbb{G}_m$. Therefore $m^*(x^d-1)$ is zero on $\mu_d \times \mu_d$, i.e., $\mu_d \times \mu_d \subset m^{-1}(\mu_d)$. Secondly $1^d - 1 = 0$, so $1 \in \mu_d$. Finally, $i^*(x^d - 1) = (1/x)^d - 1 = -(x^d-1)/x^d$. So $i^*(x^d - 1)$ is zero on μ_d, i.e., $\mu_d \subset i^{-1}(\mu_d)$.

(b) Let $n \geq 0$ be an integer, and restrict the standard action of $\mathbb{G}_m$ on $\mathbb{A}^n_k - \{0\}$ to an action of μ_d on $\mathbb{A}^n_k - \{0\}$. Prove the Veronese morphism from Problem 9 on

Problem Set 2 is a quotient of this action in the sense that every nonempty fiber is an orbit under μ_n.

Let $F : \mathbb{A}^n_k - \{0\} \to \mathbb{A}^N_k - \{0\}$ be the Veronese morphism. First of all, for every $p = (a_0, \ldots, a_n) \in \mathbb{A}^n_k$, for every $\lambda \in \mu_d$, and for every $\underline{i} = (i_0, \ldots, i_n)$ with $\sum_j i_j = d$, $F^* Z_{\underline{i}}(\lambda \cdot p) = \prod_j (\lambda a_j)^{i_j} = \lambda^d \prod_j a_j^{i_j} = F^* z(p)$. Therefore F is constant on fibers of this action.

Let $p = (a_0, \ldots, a_n)$ and $q = (b_0, \ldots, b_n)$ be elements of $\mathbb{A}^n_k - \{0\}$ such that $F(p) = F(q)$. There exists $0 \leq j \leq n$ such that $a_j \neq 0$. Then $b_j^d = F^* Z_{d\mathbf{e}_j}(q) = F^* Z_{d\mathbf{e}_j}(p) = a_j^d \neq 0$. So $b_j \neq 0$. Define $\lambda = (b_j/a_j)$. Since $b_j^d = a_j^d$, $\lambda^d = 1$, i.e., $\lambda \in \mu_d$. For every $0 \leq i \leq n$,

$$b_i b_j^{d-1} = F^* Z_{\mathbf{e}_i + (d-1)\mathbf{e}_j}(q) = F^* Z_{\mathbf{e}_i + (d-1)\mathbf{e}_j}(p) = a_i a_j^{d-1}.$$

Thus $b_i = (a_j/b_j)^{d-1} a_i = (1/\lambda)^{d-1} a_i$. Because $\lambda^d = 1$, $(1/\lambda)^{d-1} = \lambda$. Therefore $q = m_X(\lambda, p)$ for $\lambda \in \mu_d$, i.e., the fiber of F containing p is an orbit for the action of μ_d.

Difficult Problem 11: Problem 10 from Problem Set 2. (I've decided this is rather difficult after all.) For every pair of integers $n, d \geq 0$, define $N = \binom{n+d}{d}$, and define the *affine Veronese mapping* $F : \mathbb{A}^n_k \to \mathbb{A}^N_k$ as follows. Let $x_1, \ldots, x_n$ be coordinates on $\mathbb{A}^n_k$ and let $z_{i_1,\ldots,i_n}$ be coordinates on $\mathbb{A}^N_k$ where $(i_1, \ldots, i_n)$ runs through all n-tuples of nonnegative integers with $i_1 + \cdots + i_n = d$. Then $F^* z_{i_1,\ldots,i_n} = x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}$. Find an ideal $I \subset k[z_{i_1,\ldots,i_n}]$ such that $\mathbb{V}(I) = \text{Image}(F)$. (**Hint:** The generators of I are homogeneous degree 2 binomials.)

Solution: Denote by $\Sigma_{n,d} \subset (\mathbb{Z}_{\geq 0})^n$ the collection of n-tuples $\underline{i} = (i_1, \ldots, i_n)$ such that $i_1 + \cdots + i_n = d$. Denote by A the polynomial k-algebra with coordinates $z_{\underline{i}}, \underline{i} \in \Sigma_{n,d}$. Denote by $I \subset A$ the homogeneous ideal,

$$I = \langle z_{\underline{i}_1} z_{\underline{i}_2} - z_{\underline{i}_3} z_{\underline{i}_4} | \underline{i}_1, \underline{i}_2, \underline{i}_3, \underline{i}_4 \in \Sigma_{n,d}, \quad \underline{i}_1 + \underline{i}_2 = \underline{i}_3 + \underline{i}_4 \rangle.$$

Clearly $F^* I = 0$, so $\text{Image}(F) \subset \mathbb{V}(I)$. Define $G : \mathbb{A}^n_k \to \mathbb{V}(I)$ to be the induced regular morphism. Proving $\text{Image}(F) = \mathbb{V}(I)$ is tricky. There are other solutions – shorter solutions – than the following.

Order the elements $\underline{i} \in \Sigma_{n,d}$ as follows: $\underline{i} \geq \underline{j}$ if either $\underline{i} = \underline{j}$, or if $i_\alpha > j_\alpha$ for the smallest $1 \leq \alpha \leq n$ such that $i_\alpha \neq j_\alpha$. Denote monomials in A by,

$$z^b = \prod_{\underline{i} \in \Sigma_{n,d}} z_{\underline{i}}^{b(\underline{i})}.$$

Order the monomials as follows: $z^b \geq z^c$ if either $b = c$ or if $b(\underline{i}) > c(\underline{i})$ for the largest $\underline{i} \in \Sigma_{n,d}$ such that $b(\underline{i}) \neq c(\underline{i})$. Denote by $(\mathbf{e}_1, \ldots, \mathbf{e}_n)$ the standard generators for $\mathbb{Z}^n$. For every $\underline{i} \in (\mathbb{Z}_{\geq 0})^n$, for every pair of integers $1 \leq l \leq m \leq n$, denote $\underline{i}(l, m) = \sum_{k=l}^m i_k \mathbf{e}_k$.

Definition 0.4. A *segment* is an r-tuple $(\underline{i}_1 \geq \cdots \geq \underline{i}_r)$ of elements of $\Sigma_{n,d}$. A *strict segment* is an r-tuple $(\underline{i}_1 > \cdots > \underline{i}_r)$. For every segment $(\underline{i}_1 \geq \cdots \geq \underline{i}_r)$, the *reduced segment* is the unique strict segment $(\underline{j}_1, \ldots, \underline{j}_s)$ such that $\{\underline{i}_1, \ldots, \underline{i}_r\} = \{\underline{j}_1, \ldots, \underline{j}_2\}$. For every monomial z^b, the *associated segment* is the unique segment $(\underline{i}_1 \geq \cdots \geq \underline{i}_r)$ such that $z^b = z_{\underline{i}_1} \cdot \cdots \cdot z_{\underline{i}_r}$, and the *associated reduced segment* is the reduced segment of the associated segment. A strict segment $\underline{i}_1 > \cdots > \underline{i}_r$ is *minimal form* if either $r = 1$ or if $r \geq 2$, and if there exists a sequence of integers $1 \leq l(1) < \cdots < l(r-1) < m(r-1) \leq \cdots \leq m(1) \leq n$ such that,

(i) $\underline{i}_1 = \underline{i}_r(1, l(1)) + \mathbf{e}_{l(1)} + \underline{i}_1(m(1), n)$,
(ii) for $1 \leq j \leq r$, $\underline{i}_j = \underline{i}_r(1, l(j)) + \mathbf{e}_{l(j)} + \underline{i}_j(m(j), m(j-1))$,
(iii) and $\underline{i}_r = \underline{i}_r(1, m(r-1))$.

A segment, resp. a monomial, is *minimal form* if its reduced segment is minimal form.

Lemma 0.5. *Let* $(\underline{i}_1, \ldots, \underline{i}_r)$ *be a strict segment, and for every* $1 \leq j < k \leq r$, *define* $l(j,k)$ *to be the largest integer such that* $(\underline{i}_j)(1, l(j,k)) = (\underline{i}_k)(1, l(j,k))$, *and define* $m(j,k) > l(j,k)$ *to be the largest integer such that* $\underline{i}_j = (\underline{i}_j)(1, l(j,k)) + (\underline{i}_j)(m(j,k), n)$. *The segment is minimal form iff for every* $1 \leq j < k \leq r$, *both*

(i) $\underline{i}_{j,l(j,k)} = \underline{i}_{k,l(j,k)} + 1$,
(ii) *and* $\underline{i}_k(m(j,k)+1, n) = 0$.

Proof. If the segment is minimal form, it is clear (i) and (ii) hold. On the other hand, suppose (i) and (ii) hold. For each $1 \leq k \leq r-1$, define $l(k) = l(k,r)$ and $m(k) = m(k,r)$. For $1 \leq j < k \leq r-1$, because $\underline{i}_j > \underline{i}_k$, $l(j) < l(k)$. Because $\underline{i}_k(m(j,k)+1, n) = 0$, $m(k) \leq m(j,k) \leq m(j)$. Because the total degree of $\underline{i}_r$ and the total degree of $\underline{i}_{r-1}$ agree, there exists $l(r-1) < \alpha \leq m(r-1)$ such that $\underline{i}_{r,\alpha} \neq 0$. Therefore $1 \leq l(1) < \cdots < l(r-1) < m(r-1) \leq \cdots \leq m(1) \leq n$. The axioms for a minimal form segment follow in a straightforward way from (i) and (ii). $\square$

Proposition 0.6. *For every integer* $r \geq 1$, *for every monomial* $z^b \in A_r$ *there exists a minimal form monomial* $z^c \in A_r$ *such that* $z^b - z^c \in I_r$.

Proof. The proof is by induction on r, and for each r, induction with respect to the ordering on the monomials in A_r. The base case is $r = 1$ which is trivial: every monomial $z^b \in A_1$ is minimal form. By way of induction, assume $r > 1$ and assume the result is known for all smaller values of r. The proof for r is by induction on the monomials in A_r. The smallest monomial is $z^b = z^r_{d\mathbf{e}_n}$. The reduced segment is $(d\mathbf{e}_n)$, which is minimal form, and $z^b - z^b \in I_r$. By way of induction, suppose $z^b > z^r_{d\mathbf{e}_n}$, and suppose the result is known for all smaller monomials in A_r. If z^b is minimal form, then $z^b - z^b \in I_r$, which proves the result for z^b. Therefore assume that z^b is not minimal form. Let $(\mathbf{i}_1, \ldots, \mathbf{i}_s)$ be the reduced segment of z^b. By the lemma there are 2 cases: either there exists $1 \leq j < k \leq r$ such that $\underline{i}_{j,l(j,k)} - \underline{i}_{k,l(j,k)} \geq 2$ or there exists $1 \leq j < k \leq r$ such that $\underline{i}_k(m(j,k)+1, n) \neq 0$ (or both).

In the first case, because $\sum_\alpha \underline{i}_{j,\alpha} = sum_\alpha \underline{i}_{k,\alpha}$, there exists $\alpha > l(j,k)$ such that $\underline{i}_{k,p} > 0$. Define $\underline{i}'_j = \underline{i}_j - \mathbf{e}_{l(j,k)} + \mathbf{e}_\alpha$, $\underline{i}'_k = \underline{i}_k + \mathbf{e}_{l(j,k)} - \mathbf{e}_\alpha$. These are elements of $\Sigma_{n,d}$. Let z^a be the unique monomial such that $z^b = z^a(z_{\underline{i}_j} z_{\underline{i}_k})$, and define $z^{b'} = z^a(z_{\underline{i}'_j} z_{\underline{i}'_k})$. Because $\underline{i}_j > \underline{i}'_j, \underline{i}'_k$, also $z^b > z^{b'}$. Because $\underline{i}_j + \underline{i}_k = \underline{i}'_j + \underline{i}'_k$, $z_{\underline{i}_j} z_{\underline{i}_k} - z_{\underline{i}'_j} z_{\underline{i}'_k} \in I_2$; hence $z^b - z^{b'} \in I_r$. By the induction hypothesis, there exists a minimal form monomial $z^c \in A_r$ such that $z^{b'} - z^c \in I_r$. Therefore $z^b - z^c = (z^b - z^{b'}) + (z^{b'} - z^c)$ is in I_r, which proves the result for z^b.

In the second case, there exists $\alpha > m(j,k)$ such that $\underline{i}_{k,p} > 0$. Define $\underline{i}'_j = \underline{i}_j - \mathbf{e}_{m(j,k)} + \mathbf{e}_\alpha$ and $\underline{i}'_k = \underline{i}_k + \mathbf{e}_{m(j,k)} - \mathbf{e}_\alpha$. These are elements of $\Sigma_{n,d}$. Let

z^a be the unique monomial such that $z^b = z^a(z_{\underline{i}_j} z_{\underline{i}_k})$, and define $z^{b'} = z^a(z_{\underline{i}'_j} z_{\underline{i}'_k})$. Because $\underline{i}_j > \underline{i}'_j, \underline{i}'_k$, also $z^b > z^{b'}$. Because $\underline{i}_j + \underline{i}_k = \underline{i}'_j + \underline{i}'_k$, $z_{\underline{i}_j} z_{\underline{i}_k} - z_{\underline{i}'_j} z_{\underline{i}'_k} \in I_2$; hence $z^b - z^{b'} \in I_r$. By the induction hypothesis, there exists a minimal form monomial $z^c \in A_r$ such that $z^{b'} - z^c \in I_r$. Therefore $z^b - z^c = (z^b - z^{b'}) + (z^{b'} - z^c)$ is in I_r, which proves the result for z^b. So in both cases, the result holds for z^b, i.e., the proposition holds by induction. □

Proposition 0.7. *For every integer $r \geq 1$, for every pair of minimal form monomials $z^b, z^c \in A_r$, if $F^* z^b = F^* z^c$, then $z^b = z^c$.*

Proof. The proof is by induction on r. For $r = 1$, the result is trivial. By way of induction, assume $r > 1$ and the result is known for $r - 1$. Let z^b be a minimal form monomial, let $(\underline{i}_1 > \cdots > \underline{i}_s)$ be the reduced segment, and let $z^b = z_{\underline{i}_1}^{e_1} \cdot \cdots \cdot z_{\underline{i}_s}^{e_s}$. Let $F^* z^b = x_1^{f_1} \cdot \cdots \cdot x_n^{f_n}$. Then r divides f_α for $1 \leq \alpha < l(1)$, and $f_{l(1)} \equiv e_1$ modulo r. Thus $l(1)$, $\underline{i}_1(1, l(1))$ and e_1 are uniquely determined by $F^* z^b$. Moreover, $m(1)$ is the least integer such that,

$$e_1 (\sum_{\alpha=1}^{l(1)} \underline{i}_{1,\alpha}) + \sum_{\alpha=m(1)+1}^{n} f_\alpha < d e_1,$$

for every $m(1) < \alpha \leq n$, $e_1 \underline{i}_{1,\alpha} = f_\alpha$, and finally,

$$\underline{i}_{1,m(1)} = d - \left(\sum_{\alpha=1}^{l(1)} \underline{i}_{1,\alpha} \right) - \left(\sum_{\alpha=m(1)+1}^{n} \underline{i}_{1,\alpha} \right).$$

Therefore $\underline{i}_1$ is uniquely determined by $F^* z^b$. Let $z^{b'}$ and $z^{c'}$ be the unique monomials such that $z^b = z^{b'} z_{\underline{i}_1}$, $z^c = z^{c'} z_{\underline{i}_1}$. Then $F^*(z^{b'}) = F^*(z^{c'})$, and $z^{b'}, z^{c'} \in A_{r-1}$ are minimal form monomials. By the induction hypothesis, $z^{b'} = z^{c'}$. Therefore $z^b = z^c$, which proves the proposition by induction. □

Corollary 0.8. *For every integer $r \geq 1$ and every pair of monomials $z^b, z^c \in A_r$ such that $F^* z^b = F^* z^c$, $z^b - z^c \in I_r$. Also $G^* : A/I \to k[x_1, \ldots, x_n]_(d)$ is an isomorphism; in particular I is a prime ideal.*

Proof. By the first proposition, there exist minimal form monomials $z^{b'}, z^{c'} \in A_r$ such that $z^b - z^{b'}, z^c - z^{c'} \in I_r$. Therefore $F^* z^{b'} = F^* z^b$ and $F^* z^{c'} = F^* z^c$. So, by the hypothesis, $F^* z^{b'} = F^* z^{c'}$. By the second proposition, $z^{b'} = z^{c'}$. Therefore $z^b - z^c = (z^b - z^{b'}) + (z^{c'} - z^c) \in I_r$.

By the first proposition, a k-basis for A/I consists of the images of the minimal form monomials, and a k-basis for $k[x_1, \ldots, x_n]_{(d)}$ consists of all monomials of degree divisible by d. The propositions together prove G^* maps the basis for A/I bijectively to the basis for $k[x_1, \ldots, x_n]_{(d)}$. □

It remains to prove $F(\mathbb{A}_k^n) = \mathbb{V}(I)$. Clearly the vertex is in $F(\mathbb{A}_k^n)$. Let $p \in \mathbb{V}(I)$ be an element other than the vertex. Then there exists a monomial z^b such that $z^b(p) \neq 0$. By the second proposition, modulo I, $(z^b)^d$ is congruent to $\prod_{\alpha=1}^n z_{d\mathbf{e}_\alpha}^{f_\alpha}$. So for some α, $z_{d\mathbf{e}_\alpha}(p) \neq 0$. Clearly $F(\mathbb{A}_k^n)$ and $\mathbb{V}(I)$ are $\mathbb{G}_m$-invariant. So, after scaling, assume $z_{d\mathbf{e}_\alpha}(p) = 1$. For every $1 \leq \beta \leq n$, define $a_\beta = z_{(d-1)\mathbf{e}_\alpha + \mathbf{e}_\beta}(p)$. For every $\underline{i} \in \Sigma_{n,d}$, by the corollary,

$$z_{d\mathbf{e}_\alpha}^{d-1} z_{\underline{i}} \equiv \prod_{\beta=1}^{n} (z_{(d-1)\mathbf{e}_\alpha + \mathbf{e}_\beta})^{i_\beta}.$$

Therefore,

$$z_{\underline{i}}(p) = \prod_{\beta=1}^{n} a_\beta^{i_\beta}.$$

In other words, $p = F(a_1, \dots, a_n)$. So $\mathbb{V}(I) = \text{Image}(F)$.

Difficult Problem 12: Problem 11 from Problem Set 2. For every integer $n \geq 2$, define $N = \binom{n}{2}$ and define $F : \mathbb{A}_k^{2n} \to \mathbb{A}_k^N$ as follows. Let $x_{1,1}, \dots, x_{1,n}, x_{2,1}, \dots, x_{2,n}$ be coordinates on $\mathbb{A}_k^{2n}$ and let $z_{i,j}, 1 \leq i < j \leq n$ be coordinates on $\mathbb{A}_k^N$. Then $F^* z_{i,j} = x_{1,i}x_{2,j} - x_{1,j}x_{2,i}$. The image of this morphism is the *affine cone over the Grassmannian* $\boldsymbol{Grass}(2, n)$. Find an ideal $I \subset k[z_{i,j}]$ such that $\mathbb{V}(I) = \text{Image}(F)$. (**Hint:** Interpret elements of $\mathbb{A}_k^{2n}$ as $2 \times n$ matrices; interpret elements of $\mathbb{A}_k^N$ as elements of the exterior square of the n-space, which also give anti-symmetric $n \times n$ matrices, and take Pfaffians of appropriate 4×4-submatrices of this $n \times n$-matrix. The generators are homogeneous degree 2 trinomials.)

Solution: This problem requires a bit of multilinear algebra. It is less confusing if coordinates are suppressed when possible. Therefore denote by V the k-vector space $\mathbb{A}_k^n$. Denote by $\bigwedge^2 V$ the exterior square of V, i.e., there is an alternating, bilinear map $F : V \times V \to \bigwedge^2 V, \quad (v_1, v_2) \mapsto v_1 \wedge v_w$, which is universal with this property. Up to choosing appropriate coordinates, the mapping F above is the universal alternating, bilinear map. Denote by $V^\vee$ the dual vector space to V. There is an alternating, bilinear map $F' : V \times V \to \text{Hom}(V^\vee, V)$ by $F'(v_1, v_2)(\chi) = \chi(v_1)v_2 - \chi(v_2)v_2$ for every $\chi \in V^\vee$. By the universal property, there is a unique linear map $T : \bigwedge^2 V \to \text{Hom}(V^\vee, V)$ such that $T \circ F = F'$. Given $w \in \bigwedge^2 V$, denote by $T_w : V^\vee \to V$ the associated linear map.

Lemma 0.9. *An element $w \in \bigwedge^2 V$ is in $F(V \times V)$ iff T_w has rank ≤ 2.*

Proof. First it is shown that T_w has rank ≤ 2 for every $w \in \bigwedge^2 V$. Let $(v_1, v_2) \in V$. If (v_1, v_2) is not linearly independent, then $F(v_1, v_2) = 0$. Therefore assume (v_1, v_2) is linearly independent. Extend this to an orderd basis $(v_1, v_2, \dots, v_n)$. Let $x_1, \dots, x_n$ be the dual ordered basis for $V^\vee$. Then $T_{v_1 \wedge v_2}(x_1) = v_2$, $T_{v_1 \wedge v_2}(x_2) = -v_1$, and $T_{v_1 \wedge v_w}(x_\alpha) = 0$ for $2 < \alpha \leq n$. Therefore $T_{v_1 \wedge v_2}$ has rank 2.

Next let $w \in \bigwedge^2 V$ be an element such that T_w has rank ≤ 2. Let $(x_1, x_2, \dots, x_n)$ be an ordered basis for $V^\vee$ such that $T_w(x_\alpha) = 0$ for $2 < \alpha \leq n$. Let $(v_1, \dots, v_n)$ be the dual ordered basis for $V^\vee$. Then $(v_\alpha \wedge v_\beta | 1 \leq \alpha < \beta \leq n)$ is a basis for $\bigwedge^2 V$. The coefficient of $v_\alpha \wedge v_\beta$ in w is simply $x_\beta(T_w(x_\alpha)) = -x_\alpha(T_w(x_\beta))$, which is 0 for $\alpha, \beta > 2$. Therefore $w = \lambda v_1 \wedge v_2 = (\lambda v_1) \wedge v_2$ for some $\lambda \in k$, i.e., $w \in F(V \times V)$. $\square$

Let $(\mathbf{e}_1, \dots, \mathbf{e}_n)$ be the standard ordered basis for V and let $(x_1, \dots, x_n)$ be the dual ordered basis for $V^\vee$. For every $w \in \bigwedge^2 V$, T_w is nonzero iff there exists $1 \leq \alpha_1 \leq n$ such that $T_w(x_{\alpha_1}) \neq 0$. And this is true iff there exists $1 \leq \alpha_2 \leq n$ such that $x_{\alpha_2}(T_w(x_{\alpha_1})) \neq 0$. Because of the form of T_w, $y(T_w(x)) = -x(T_w(y))$ for every $x, y \in V^vee$ and $x(T_w(x)) = 0$ for every $x \in V^\vee$ (the first implies the second if $\mathrm{char}(k) \neq 2$). In particular the 2×2 matrix $x_{\alpha_i}(T_w(x_{\alpha_j}))$, $1 \leq i, j \leq 2$ has rank 2. Therefore T_w has rank at least 2 iff there exists $1 \leq \alpha_1 < \alpha_2 \leq n$ such that the 2×2 matrix $x_{\alpha_i}(T_w(x_{\alpha_j}))$ has rank 2.

By a similar argument, T_w has rank > 2 iff there exists $1 \leq \alpha_1 < \alpha_2 < \alpha_3 < \alpha_4 \leq n$ such that the 4×4 matrix $x_{\alpha_i}(T_w(x_{\alpha_j}))$ has rank 4. So T_w has rank ≤ 2 iff for every $1 \leq \alpha_1 < \alpha_2 < \alpha_3 < \alpha_4 \leq n$, the determinant of this 4×4 matrix is 0. Denoting $w = \sum_{\beta_1 < \beta_2} z_{\beta_1,\beta_2} \mathbf{e}_{\beta_1} \wedge \mathbf{e}_{\beta_2}$ (i.e., choosing coordinatex z_{β_1,β_2} on $\bigwedge^2 V$), this 4×4 matrix is,

$$M = \begin{pmatrix} 0 & z_{\alpha_1,\alpha_2} & z_{\alpha_1,\alpha_3} & z_{\alpha_1,\alpha_4} \\ -z_{\alpha_1,\alpha_2} & 0 & z_{\alpha_2,\alpha_3} & z_{\alpha_2,\alpha_4} \\ -z_{\alpha_1,\alpha_3} & -z_{\alpha_2,\alpha_3} & 0 & z_{\alpha_3,\alpha_4} \\ -z_{\alpha_1,\alpha_4} & -z_{\alpha_2,\alpha_4} & -z_{\alpha_3,\alpha_4} & 0 \end{pmatrix}.$$

By a somewhat tedious computation, the determinant is,

$$\det(M) = (Q_{\alpha_1,\alpha_2,\alpha_3,\alpha_4})^2, \ \ Q_{\alpha_1,\alpha_2,\alpha_3,\alpha_4} := z_{\alpha_1,\alpha_2}z_{\alpha_3,\alpha_4} - z_{\alpha_1,\alpha_3}z_{\alpha_2,\alpha_4} + z_{\alpha_1,\alpha_4}z_{\alpha_2,\alpha_3}.$$

Therefore Image(F) is $\mathbb{V}(I)$, where $I = \langle Q_{\alpha_1,\alpha_2,\alpha_3,\alpha_4} | 1 \leq \alpha_1 < \alpha_2 < \alpha_3 < \alpha_4 \leq n \rangle$.

Remark: This does not prove that $\mathbf{I}(\mathrm{Image}(F)) = I$, i.e., that I is a radical ideal. It is not obvious, however it is true that I is a radical ideal.

Very Difficult Problem 13: Problem 14 from Problem Set 2. Prove there exists a quasi-affine algebraic set V such that $\mathcal{O}_V(V)$ is not a finitely-generated k-algebra. The examples I am aware of all have dimension ≥ 4. (**Warning:** This problem would be more appropriate at the end of 18.726. I mention it now because you can understand it, and it is a problem to keep in mind as the semester goes on.)

Solution: At this point, you can verify the following solution works. However, it likely will appear quite arbitrary. Later in the semester, after introducing coherent sheaves, vector bundles and divisors, it will turn out this solution is quite natural.

Assume $\mathrm{char}(k) \neq 2$, and let $i \in k$ be a solution of $x^2 + 1 = 0$. The solution uses Problem 16 and 17 from Problem Set 2 (solved below), which you should read first. Let X, Y, Z be coordinates on $\mathbb{A}^3_k$ and let $\widetilde{C} = \mathbb{V}(Y^2Z - X^2(X - Z)) \subset \mathbb{A}^3_k$. This is an affine cone, so determines a Zariski closed subset $C \subset \mathbb{P}^2_k$, the *nodal plane cubic curve*. Observe that $C \cap D_+(Z) \subset \mathbb{P}^2_k$ considered as an affine algebraic set in $\mathbb{A}^2_k$ is the affine nodal plane cubic from Problem 16 on Problem Set 2. Let $p = (0, 1, 0) \in \widetilde{C}$ and let $(a_0, b_0, 1) \in \widetilde{C}$ be elements such that $(b_0 - ia_0)/(b_0 + ia_0)$ is *not* a root of unity.

Extend the coordinates X, Y, Z to a set of coordinates X, Y, Z, S, T on $\mathbb{A}^5_k$. Denote by $K \subset \mathbb{A}^5_k$ the Zariski closed subset $\mathbb{V}(I)$, where,

$$I = \left\langle \begin{array}{c} Y^2Z - X^2(X - Z), \\ X(X - a_0Z)S - (Y - b_0Z)ZT, \\ X(Y + b_0Z)S - (X^2 + (a_0 - 1)XZ + a_0(a_0 - 1)Z^2)T, \\ (Y^2 - (a_0 - 1)X^2)S - X(Y - b_0Z)T \end{array} \right\rangle$$

Denote by $P \subset K$ the relatively open subset $K - (\mathbb{V}(X, Y, Z) \cup \mathbb{V}(S, T))$. For the quasi-affine algebraic set $P \subset \mathbb{A}^5_k$, $\mathcal{O}_P(P)$ is not a finitely generated k-algebra.

There is a $(3\mathbb{Z})^2$-grading of $k[X, Y, Z, S, T]$ where $\deg(X) = \deg(Y) = \deg(Z) = (3, 0)$ and $\deg(S) = \deg(T) = (3, 3)$. This is really the same as a $\mathbb{Z}^2$-grading;

the reason for the 3 will soon be clear. The ideal I is homogeneous with respect to this grading. So there is an induced $(3\mathbb{Z})^2$-grading of $\mathcal{O}_P(P)$. Consider the subset $S = \{(i,j) \in (3\mathbb{Z})^2 | \mathcal{O}_P(P)_{(i,j)} \neq \{0\}\}$. If $\mathcal{O}_P(P)$ is finitely generated, the generators can be chosen to be homogeneous, and the corresponding degrees of these generators form a finite generating set for the sub-semigroup $S \subset (3\mathbb{Z})^2$. So to prove $\mathcal{O}_P(P)$ is not a finitely generated k-algebra, it suffices to prove S is not a finitely generated semigroup.

Let (U,V,S,T) be coordinates on $\mathbb{A}^4_k$. Denote by $L \subset \mathbb{A}^4_k$ the affine algebraic subset,

$$\mathbb{V}(\langle (U^2+V^2)(a_0U+b_0V)S - V(a_0U^2+b_0UV+a_0^2V^2)T\rangle).$$

Denote by $Q \subset L$ the relatively open subset $L - (\mathbb{V}(U,V) \cup \mathbb{V}(S,T))$. There is a regular morphism $F_L : L \to K$ by $(U,V,S,T) \mapsto (V(U^2+V^2), U(U^2+V^2), V^3, S, T)$. This restricts to a regular morphism $F : Q \to P$. There is a "projection" regular morphism $\pi : P \to \mathbb{A}^2_k - \{(0,0)\}$ by $(U,V,S,T) \mapsto (U,V)$. There is a "section" regular morphism $\sigma : \mathbb{A}^2_k - \{(0,0)\} \to P$ by $(U,V) \mapsto (U,V,V(a_0U^2 + b_0UV + a_0^2V^2), (U^2+V^2)(a_0U+b_V))$. This determines a regular morphism $\tau : \mathbb{G}_m \times (\mathbb{A}^2_k - \{(0,0)\}) \to P$ by $\tau(\lambda,(U,V)) = (U,V,\lambda V(a_0U^2+b_0UV+a_0^2V^2), \lambda(U^2+V^2)(a_0U+b_V))$.

Define $g_1 : P \cap D(V(a_0U^2+b_0UV+a_0^2V^2)) \to \mathbb{A}^1_k$ to be the regular function $S/(V(a_0U^2+b_0UV+a_0^2V^2))$, and $g_2 : P \cap D((U^2+V^2)(a_0U+b_V)) \to \mathbb{A}^1_k$ to be the regular function $T/((U^2+V^2)(a_0U+b_V))$. The restriction of g_1 equals the restriction of g_2. By the gluing lemma, there is a regular function g on $P = (P \cap D(V(a_0U^2+b_0UV+a_0^2V^2))) \cup (P \cap D((U^2+V^2)(a_0U+b_V)))$. The regular morphism $\rho : P \to \mathbb{G}_m \times (\mathbb{A}^2_k - \{(0,0)\})$ by $(U,V,S,T) \mapsto (g(U,V,S,T),(U,V))$ is an inverse of τ, i.e., τ is an isomorphism.

There is a $\mathbb{Z}^2$-grading on $k[U,V,S,T]$ by $\deg(U) = \deg(V) = (1,0)$ and $\deg(S) = \deg(T) = (3,3)$. Since the ideal of L is invariant with respect to this grading, there is an induced $\mathbb{Z}^2$-grading of $\mathcal{O}_Q(Q)$. And the k-algebra homomorphism $F^* : \mathcal{O}_P(P) \to \mathcal{O}_Q(Q)$ preserves the grading. By the same argument as in Problem 13 from PS#2, the ring of regular functions on $\mathbb{G}_m \times (\mathbb{A}^2_k - \{0\})$ is $k[U,V][\lambda, 1/\lambda]$. So τ^* is an isomorphism $\mathcal{O}_P(P) \to k[U,V][\lambda,1/\lambda]$. The $\mathbb{Z}^2$-grading on $\mathcal{O}_P(P)$ corresponds to the grading $\deg(U) = \deg(V) = (1,0), \deg(\lambda) = (0,3)$.

For the same reason as in Problem 16 of PS#2, the image of F^* is the subalgebra in $\mathcal{O}_U(U)_{(3)}$ of functions $f(U,V,S,T)$ such that $f(iV,V,S,T) = f(-iV,V,S,T)$. Using the isomorphism τ^*, these are the functions $h(U,V,\lambda)$ such that $h(iV,V,\lambda) = h(-iV,V,(b_0+ia_0)\lambda/(b_0-ia_0))$. Of course for every integer $m<0$ and every integer n, $k[U,V][\lambda,1/\lambda]_{(3m,n)} = \{0\}$. In particular, $(3m,3n) \notin S$ for every $m < 0$.

For $m = 1$ and every integer n, define,

$$C_n = 1/2((b_0+ia_0)^n + (b_0-ia_0)^n),$$

$$D_n = i/2((b_0+ia_0)^n - (b_0-ia_0)^n)$$

Then $h_n(U,V,\lambda) := (C_nV + D_nU)V^2\lambda^n \in k[U,V,\lambda]_{(3,3n)}$ is a nonzero function such that $h_n(iV,V,\lambda) = h_n(-iV,V,(b_0+ia_0)\lambda/(b_0-ia_0))$. More generally, for every $m>0$, $h_{(m,n)}(U,V,\lambda) := (C_nV+D_nU)V^{3m-1}\lambda^n \in k[U,V,\lambda]_{(3m,3n)}$ is a nonzero function such that $h_{(m,n)}(iV,V,\lambda) = h_{(m,n)}(-iV,V,(b_0+ia_0)\lambda/(b_0-ia_0))$. Therefore $(3m,3n) \in S$ for every $m > 0$.

Finally, $k[U,V,\lambda]_{(0,3n)}$ is the k-vector space generated by $h_{(0,n)} = \lambda^n$. For $n=0$, of course $\lambda^0 = 1$ satisfies $h_{(0,0)}(iV,V,\lambda) = h_{(0,0)}(-iV,V,(b_0+ia_0)\lambda/(b_0-ia_0))$. Because of the hypothesis that $(b_0+ia_0)/(b_0-ia_0)$ is *not* a root of unity, for every $n \neq 0$, $\lambda^n \neq (b_0+ia_0)^n\lambda^n/(b_0-ia_0)^n$. Therefore $(0,3n) \in S$ iff $n=0$.

Altogether, this proves $S = \{(0,0)\} \cup \{(3m,3n) | m,n \in \mathbb{Z},\ m>0\}$. So each of the elements $(3,3n) \in S$ is indecomposable, proving S is not a finitely generated semigroup.

Problem 14: Problem 16 from Problem Set 2. Together with the next problem, this problem gives an open subset of an affine algebraic set, itself isomorphic to an affine algebraic set, but not a basic open affine $D(s)$. In both problems, assume $\mathrm{char}(k) \neq 2$ and let i denote a solution of x^2+1 in k. Let $C \subset \mathbb{A}^2_k$ be the *affine nodal plane cubic*, $C = \mathbb{V}(y^2 - x^2(x-1))$ Let $(a_0,b_0) \in C$ and define $F : D(x-a_0) \to \mathbb{A}^3_k$ by $F(a,b) = (a,b,(b+b_0)/(a-a_0))$.

(a) Prove there exists a regular morphism $G : C - \{(a_0,b_0)\} \to \mathbb{A}^3_k$ whose restriction to $D(x-a_0)$ equals F. (**Hint:** Expand the defining equation of C in the coordinates $x-a_0$ and $y-b_0$.)

Solution: Expanding the defining equation, on C,

$$(y+b_0)(y-b_0) = y^2-b_0^2 = (x-a_0)(x+a_0)(x-1)+a_0^2(x-1)-b_0^2 = (x-a_0)((x+a_0)(x-1)+a_0^2).$$

Therefore,

$$(y+b_0)/(x-a_0) = ((x+a_0)(x-1)+a_0^2)/(y-b_0).$$

More precisely, the regular function on $C - D(y-b_0)$ by $(a,b) \mapsto ((a+a_0)(a-1)+a_0^2)/(b-b_0)$ restricts on $C - (D(x-b_0) \cup D(y-b_0))$ to $z \circ F$. Because $(C - D(x-a_0)) \cup (C - D(y-b_0)) = C - \{(a_0,b_0)\}$, by the gluing lemma there is a regular function $g : C - \{(a_0,b_0)\} \to \mathbb{A}^1_k$ whose restriction to $C - D(y-b_0)$ equals $z \circ F$. Define $G(a,b) = (a,b,g(a,b))$.

(b) Prove the image of G is an affine algebraic subset of $\mathbb{A}^3_k$.

Solution: There is an extra hypothesis necessary: $(a_0,b_0) \neq (0,0)$. Consider $V = \mathbb{V}(I) \subset \mathbb{A}^3_k$, where,

$$I = \left\langle \begin{array}{c} y^2 - x^2(x-1), \\ (x-a_0)z - (y+b_0), \\ (y-b_0)z - [(x+a_0)(x-1)+a_0^2] \end{array} \right\rangle$$

It is straightforward that $G^*I = \{0\}$, i.e., $\mathrm{Image}(G) \subset V$. Let $(a,b,c) \in \mathbb{V}(I)$. Then $(a,b) \in C$. Moreover, if $(a,b) = (a_0,b_0)$, then the second last equations in I give,

$$0c - (b_0+b_0) = 0, 0c - [(a_0+a_0)(a_0-1)+a_0^2] = 0,$$

i.e., $2b_0 = 0, a_0(a_0-1) = 0$. By hypothesis $\mathrm{char}(k) \neq 2$, thus $b_0 = 0$. Plugging into the defining equation $a_0 = 0$ or $a_0 = 1$. Because $(a_0,b_0) \neq (0,0)$, $a_0 = 1$. So $2a_0(a_0-1)+a_0^2 = 1 \neq 0$. Therefore $(a,b) \neq (a_0,b_0)$. So the image of $\pi : V \to C$ is $C - \{(a_0,b_0)\}$.

For any other point $(a,b) \in C$, there is a unique solution to the last two equations, namely $c = g(a,b)$. Thus $\mathbb{V}(I) = \mathrm{Image}(G)$.

(c) Prove the projection $\pi : \mathbb{A}^3_k \to \mathbb{A}^2_k$, $\pi(a,b,c) = (a,b)$ restricts on the image of G to an inverse morphism to G. Therefore $C - \{a_0,b_0\}$ is an open subset of C, itself isomorphic to an affine algebraic set.

Solution: Again, there is another hypothesis necessary, $(a_0, b_0) \neq (0, 0)$. This was done in the solution to the last part. Because $\mathbb{V}(I)$ is an affine algebraic set, $C - \{(a_0, b_0)\}$ is isomorphic to an affine algebraic set.

Difficult Problem 15: Problem 17 from Problem Set 2. This problem continues Problem 16; again $\text{char}(k) \neq 2$. Consider the morphism $H : \mathbb{A}^1_k \to C$ by $H(u) = (u^2 + 1, u(u^2 + 1))$. Let t be a coordinate on $\mathbb{A}^1_k$.

(a) Prove $H^* : k[C] \to k[t]$ maps $k[C]$ isomorphically to the subalgebra of functions $f(t) \in k[t]$ such that $f(i) = f(-i)$.

Solution: The image of H is not finite, so the Zariski closure is all of C. Therefore $\ker(H^*) = \mathbb{I}(\text{Image}(H)) = \{0\}$, i.e., H^* is injective. The generators x and y of $k[C]$ map to $t^2 + 1$ and $t(t^2 + 1)$. Every polynomial $f(t) \in k[t]$ has a unique expression as,

$$f(t) = c_0 + c_1 t + c_2(t^2 + 1) + c_3 t(t^2 + 1) + \cdots + c_{2k}(t^2 + 1)^k + c_{2k+1} t(t^2 + 1)^k + \dots$$

Plugging in i and $-i$, $f(i) = f(-i)$ iff $c_1 = 0$. In this case,

$$f = H^*(c_0 + c_2 x + c_3 y + \cdots + c_{2k} x^k + c_{2k+1} x^{k-1} y + \dots).$$

Therefore $f(i) = f(-i)$ iff $f \in \text{Image}(H^*)$.

(b) For (b), (c) and (d), assume $(a_0, b_0) \in C - \{(0, 0)\}$. Prove the ideal of $k[t]$ generated by $H^*(\langle x - a_0, y - b_0\rangle)$ is the principal ideal $\langle a_0 t - b_0\rangle$.

Solution: Denote the ideal by $J \subset k[t]$. Because $(a_0, b_0) \neq (0, 0)$, in particular $a_0 \neq 0$. First of all, $a_0 t - b_0 = H^* y - t H^* x \in J$. Second of all, $a_0^2 H^* x = a_0^2 t^2 + a_0^2 - a_0^3 = a_0^2 t^2 - b_0^2 = (a_0 t + b_0)(a_0 t - b_0) \in \langle a_0 t - b_0\rangle$. Finally, $a_0^2 H^* y = a_0^2(a_0 t - b_0) + t a_0^2 H^* x \in \langle a_0 t - b_0\rangle$.

(c) If there is an element $s \in k[V]$ such that $\mathbb{V}(s) = \{(a_0, b_0)\}$, $H^*(s) = c(a_0 t - b_0)^n$ for some nonzero constant $c \in k$ and integer $n \geq 1$. (**Hint:** Consider the image of s in $k[V][1/xy] \cong k[t][1/(t^2 + 1)]$. Use this to express $H^* s$ as $c(t^2 + 1)^r (a_0 t - b_0)^n$ for some $r \geq 0$, and then use that $s(0, 0) \neq 0$.)

Solution: The ideal in $k[t][1/(t^2+1)]$ generated by I equals the ideal in $k[V][1/xy]$ generated by $\langle x - a_0, y - b_0\rangle$ under the induced isomorphism of k-algebras. So $H^*(s)/1 \in \langle a_0 t - b_0\rangle k[t][1/(t^2+1)]$. Hence there are integer $m, n \geq 0$ and $p(t) \in k[t]$ relatively prime to $(a_0 t - b_0)$ and (t^2+1) such that $(t^2+1)^m H^*(s) = p(t)(a_0 t - b_0)^n$. Because $a_0 \neq 0$, $a_0 - 1 \neq -1$. But $(b_0/a_0)^2 = a_0 - 1$. So $(b_0/a_0)^2 + 1 \neq 0$, i.e., $a_0 t - b_0$ is relatively prime to $t^2 + 1$. Since $k[t]$ is a UFD, $(t^2+1)^m$ divides $p(t)$. Since $p(t)$ is relatively prime to (t^2+1), this implies $m = 0$. Thus $H^*(s) = p(t)(a_0 t - b_0)^n$. If $p(t)$ is not a constant polynomial, it vanishes at some point other than b_0/a_0. The image of this point under H is a point other than (a_0, b_0) at which s vanishes. By hypothesis, s vanishes only at (a_0, b_0). Therefore $p(t) = c$ for some nonzero constant $c \in k$.

(d) Deduce that $(a_0 i - b_0)^n = (-a_0 i - b_0)^n$, because $c(at - b)^n$ is in the image of H^*. Therefore for every $(a_0, b_0) \in C - \{(0, 0)\}$, if $(b_0 - i a_0)/(b_0 + i a_0)$ is not a root of unity, then $C - \{(a_0, b_0)\}$ is of the form $D(s)$ for *no* element $s \in k[V]$ (in fact these are equivalent conditions).

Solution: Continuing as before, $H^*s = c(a_0t - b_0)^n$ for some integer n. For every $f(t) \in \text{Image}(H^*)$, by (a), $f(i) = f(-i)$. Plugging in, this gives,

$$c(ia_0 - b_0)^n = c(-ia_0 - b_0)^n.$$

Because $c \neq 0$, it can be cancelled. Because $(b_0/a_0)^2 + 1 \neq 0$, as discussed above, both sides of the equation are nonzero. So we can divide to get,

$$(b_0 - ia_0)^n/(b_0 + ia_0)^n = 1.$$

So if $(b_0 - ia_0)/(b_0 + ia_0)$ is not a root of unity, then $n = 0$, i.e., $s = c$. So in this case, there is no $s \in k[C]$ such that $\mathbb{V}(s) = \{(a_0, b_0)\}$. As a final point, observe that because $H : \mathbb{A}^1_k \to C$ is surjective, there are plenty of pairs $(a_0, b_0) \in C$ such that $(b_0 - ia_0)/(b_0 + ia_0)$ is not a root of unity.