18.725 SOLUTIONS TO PROBLEM SET 1

Required Problem 1 Do Exercise 1.11 from the notes for Lecture 1. Try to use the Nullstellensatz only when necessary.

Solution:(i) Clearly $\mathbb{I}(\emptyset) = k[x_1, \ldots, x_n]$. The Strong Nullstellensatz implies $\mathbb{I}(\mathbb{A}^n_k) = \mathbb{I}(\mathbb{V}(\{0\})) = \text{rad}\{0\} = \{0\}$. This can also be proved by induction on n. For $n = 0$, it is trivial. Let $n > 0$ and assume the result known for $n-1$. For every $f \in k[x_1, \ldots, x_n] - \{0\}$, expand it as $f = \sum_{i=0}^{d} g_i(x_1, \ldots, x_{n-1})x_n^i$ where $g_d \neq 0$. By the induction hypothesis, there exists $(a_1, \ldots, a_{n-1}) \in \mathbb{A}^{n-1}_k$ such that $g_d(a_1, \ldots, a_{n-1}) \neq 0$. The polynomial $f(a_1, \ldots, a_{n-1}, x_n) = \sum_{i=0}^{d} g_i x_n^i$ has degree d, so at most d roots. Since k is infinite there exists $a_n \in k$ such that $f(a_1, \ldots, a_{n-1}, a_n) \neq 0$, i.e., $f \notin \mathbb{I}(\mathbb{A}^n_k)$.

(ii) For every $f \in \mathbb{I}(W)$, since f vanishes on W it also vanishes on V, i.e., $f \in \mathbb{I}(V)$.

(iii) Denote $V = \cap_\lambda V_\lambda$ and denote $I = \sum_\lambda \mathbb{I}(V_\lambda)$. By Exercise 1.3(iii), $V = \mathbb{V}(I)$. By the Strong Nullstellensatz, $\mathbb{I}(V) = \mathbb{I}(\mathbb{V}(I)) = \text{rad}(I)$.

(iv) By (ii), $\mathbb{I}(V \cup W) \subset \mathbb{I}(V) \cap \mathbb{I}(W)$. By Exercise 1.3(ii), $\mathbb{V}(\mathbb{I}(V) \cap \mathbb{I}(W)) \supset V \cup W$, so that by (ii) again, $\mathbb{I}(V) \cap \mathbb{I}(W) \subset \mathbb{I}(\mathbb{V}(\mathbb{I}(V) \cap \mathbb{I}(W))) \subset \mathbb{I}(V \cup W)$. Thus $\mathbb{I}(V \cup W) = \mathbb{I}(V) \cap \mathbb{I}(W)$.

(v) Clearly $V \subset \mathbb{V}(\mathbb{I}(V))$. For every Zariski closed W containing V, $\mathbb{I}(W) \subset \mathbb{I}(V)$ by (ii), and $\mathbb{V}(\mathbb{I}(V)) \subset \mathbb{V}(\mathbb{I}(W)) = W$ by Exercise 1.3(ii). Thus $\mathbb{V}(\mathbb{I}(W))$ is the smallest Zariski closed set containing V.

Required Problem 2 (a) Prove that $\mathbb{A}^1_k$ with the Zariski topology is not Hausdorff.

Solution: The zero locus of a polynomial function on $\mathbb{A}^1_k$ is all of $\mathbb{A}^1_k$ or a finite set. So the intersection of any 2 nonempty open subsets is the complement of a finite set, and thus nonempty.

(b) Prove that any bijection $F : \mathbb{A}^1_k \to \mathbb{A}^1_k$ is a homeomorphism with respect to the Zariski topology.

Solution: The preimage under F of a finite set is a finite set, and of $\mathbb{A}^1_k$ is $\mathbb{A}^1_k$. Thus F is continuous. Since F^{-1} is a bijection, it is also continuuous and F is a homeomorphism.

Required Problem 3 Let $V \subset \mathbb{A}^m_k$ and $W \subset \mathbb{A}^n_k$ be affine algebraic sets with $\mathbb{I}(V) = I \subset k[x_1, \ldots, x_m]$ and $\mathbb{I}(W) = J \subset k[y_1, \ldots, y_n]$ respectively. Define $K \subset k[z_1, \ldots, z_m, z_{m+1}, \ldots, z_{m+n}]$ to be the ideal,

$$K = \langle f(z_1, \ldots, z_m) | f(x_1, \ldots, x_m) \in I\rangle + \langle g(z_{m+1}, \ldots, z_{m+n}) | g(y_1, \ldots, y_n) \in J\rangle.$$

(a) Prove the map

$$(\pi_1, \pi_2) : \mathbb{A}^{m+n}_k \to \mathbb{A}^m_k \times \mathbb{A}^n_k,\ (z_1, \ldots, z_m, z_{m+1}, \ldots, z_{m+n}) \mapsto ((z_1, \ldots, z_m), (z_{m+1}, \ldots, z_{m+n})),$$

restricts to a bijection from $\mathbb{V}(K)$ to $V \times W$.

Solution: First of all, $\pi_1^*(\mathbb{I}(V))$ and $\pi_2^*(\mathbb{I}(W))$ are contained in K, thus $\pi_1(\mathbb{V}(K)) \subset V$ and $\pi_2(\mathbb{V}(K)) \subset W$. For every $p = (a_1, \ldots, a_m) \in V$ and $q = (b_1, \ldots, b_n) \in W$, all generators of K are zero on $r = (a_1, \ldots, a_m, b_1, \ldots, b_n)$, i.e., $r \in \mathbb{V}(K)$ is an element such that $(\pi_1, \pi_2)(r) = (p, q)$. Hence (π_1, π_2) is surjective. Finally, $(\pi_1, \pi_2) : \mathbb{A}_k^{m+n} \to \mathbb{A}_k^m \times \mathbb{A}_k^n$ is injective, thus also $(\pi_1, \pi_2) : \mathbb{V}(K) \to V \times W$ is injective.

(b) Prove the projections $\pi_1 : \mathbb{V}(K) \to V$, $\pi_2 : \mathbb{V}(K) \to W$ are regular morphisms.

Solution: The coordinates of π_1 and π_2 are usual coordinates on $\mathbb{A}_k^{m+n}$, which are polynomials.

(c) For every affine algebraic set T prove the following set map is a bijection,

$$(\pi_1^*, \pi_2^*) : \text{Regular morphisms}(T, \mathbb{V}(K)) \to \text{Regular morphisms}(T, V) \times \text{Regular morphisms}(T, W),$$
$$(f : T \to \mathbb{V}(K)) \mapsto ((\pi_1 \circ f : T \to V), (\pi_2 \circ f : T \to W))$$

In other words, the pair of regular morphisms (π_1, π_2) is a product of V and W in the category of affine algebraic sets.

Solution: By the correspondence between polynomial mappings and k-algebra homomorphisms, it suffices to prove for every reduced k-algebra A the following set map is a bijection,

$$\text{Hom}_{k-\text{alg}}(k[z_1, \ldots, z_{m+n}]/K, A) \to \text{Hom}_{k-\text{alg}}(k[V], A) \times \text{Hom}_{k-\text{alg}}(k[W], A).$$

First this is proved injective, then surjective. Let $\phi_1, \phi_2 : k[z_1, \ldots, z_{m+n}]/K \to A$ be k-algebra homomorphisms giving equal k-algebra homomorphisms $\pi_1^*\phi_i : k[V] \to A$ and $\pi_2^*\phi_i : k[W] \to A$. In particular, for every $j = 1, \ldots, m$, $\phi_1(\overline{z_j}) = \phi_2(\overline{z_j})$ since both equal the image in A of $\overline{x_i} \in k[V]$. Similarly, for $j = m+1, \ldots, m+n$, $\phi_1(\overline{z_j}) = \phi_2(\overline{z_j})$. Thus for every polynomial $p \in k[z_1, \ldots, z_{m+n}]$,

$$\phi_1(\overline{p}) = p(\phi_1(z_1), \ldots, \phi_1(z_{m+n})) = p(\phi_2(z_1), \ldots, \phi_2(z_{m+n})) = \phi_2(\overline{p}).$$

So $\phi_1 = \phi_2$, i.e., (π_1^*, π_2^*) is injective.

Next, let $\phi_V : k[V] \to A$ and $\phi_W : k[W] \to A$ be k-algebra homomorphisms. Define a k-algebra homomorphism $\widetilde{\phi} : k[z_1, \ldots, z_n] \to A$ by,

$$\widetilde{\phi}(z_i) = \begin{cases} \phi_V(\overline{x_i}), & 1 \leq i \leq m, \\ \phi_W(\overline{y_{j-m}}), & m+1 \leq i \leq n \end{cases}$$

For every $f \in I$,

$$\widetilde{\phi}(f(z_1, \ldots, z_m)) = f(\widetilde{\phi}(z_1), \ldots, \widetilde{\phi}(z_m)) =$$
$$f(\phi_V(\overline{x_1}), \ldots, \phi_V(\overline{x_m})) = \phi_V(\overline{f(x_1, \ldots, x_m)}) = \phi_V(0) = 0.$$

Similarly, for every $g \in J$, $\widetilde{\phi}(g(z_{m+1}, \ldots, z_{m+n})) = 0$. Therefore K is contained in the kernel of $\widetilde{\phi}$. So it factors through a k-algebra homomorphism $\phi : k[z_1, \ldots, z_{m+n}]/K \to A$. By construction $\pi_1^*\phi = \phi_V$, $\pi_2^*\phi = \phi_W$. Therefore (π_1^*, π_2^*) is also surjective.

Required Problem 4(a) Prove the induced topology on every subset of a Noetherian topological space is Noetherian.

Solution: Let X be a Noetherian topological space, let $Y \subset X$ be a subset, and let $\mathcal{C}$ be a nonempty collection of closed subset of Y. The collection $\mathcal{D}$ of closures in X of sets in $\mathcal{C}$ contains a minimal closes set V. The intersection $V \cap Y$ is in $\mathcal{C}$. For every $W \subset V \cap Y$ in $\mathcal{C}$, the closure of W in X is in $\mathcal{D}$ and a subset of V, thus equals V. So $W = V \cap Y$, i.e., $V \cap Y$ is a minimal closed set in $\mathcal{C}$.

(b) Prove every Noetherian topological space is quasi-compact. (**Hint:** Given an open covering $\mathcal{U}$ of X by open subsets, consider the collection of closed subsets that are complements of unions of finite subsets.)

Solution: Because X is Noetherian, the collection $\mathcal{C}$ of complements of unions of finite subsets of $\mathcal{U}$ contains a minimal closed set V; say $V = X - (\cup_{i=1}^n U_i)$ for $U_1, \dots, U_n$ in $\mathcal{U}$. Every element of X is contained in some set U in $\mathcal{U}$. Since $V - U = X - (U \cup (\cup_i U_i))$, $V - U \subset V$ is in $\mathcal{C}$ so that $V - U = V$. So every element of X is not in V, i.e. $V = \emptyset$. Therefore $(U_1, \dots, U_n)$ is a finite subcovering of $\mathcal{U}$.

Problem 5 Give an example of a Jacobson ring that is not a finitely-generated algebra over a field. Prove your example is a Jacobson ring.

Solution: The ring of integers $\mathbb{Z}$ is a Jacobson ring: the only prime ideal that is not a maximal ideal is (0), which is the intersection over all primes p of $\cap p\mathbb{Z}$.

Problem 6 Denote $f(X,Y) = C_{2,0,0}X^2 + C_{1,1,0}XY + C_{0,2,0}Y^2 + C_{1,0,1}X + C_{0,1,1}Y + C_{0,0,2}$ for coefficients $C_{i,j,k} \in k$ satisfying $(C_{2,0,0}, C_{1,1,0}, C_{0,2,0}) \neq (0,0,0)$.

(a) Prove $\mathbb{V}(f) \subset \mathbb{A}_k^2$ is nonempty.

Solution: It is not hard to prove this directly, but it also follows from the Weak Nullstellensatz: because f is not constant, it it is not invertible and therefore is contained in a maximal ideal, which is $\mathbb{I}(p)$ for some $p \in \mathbb{V}(f)$.

(b) If the following symmetric matrix M is invertible, prove f is irreducible (and thus $\mathbb{V}(f)$ is irreducible).

$$M = \begin{pmatrix} 2C_{2,0,0} & C_{1,1,0} & C_{1,0,1} \\ C_{1,1,0} & 2C_{0,2,0} & C_{0,1,1} \\ C_{1,0,1} & C_{0,1,1} & 2C_{0,0,2} \end{pmatrix}$$

Solution: Assume f is reducible. The matrix M will be proved singular. Because $\text{degree}(f) = 2$, $f = g_1 g_2$ for linear polynomials g_1 and g_2. The rows of the matrix M are the coefficients of X, Y and the constant coefficient in $\partial f/\partial X$, $\partial f/\partial Y$ and $2f - X\partial f/\partial X - Y\partial f/\partial Y$. Expanding this in g_1 and g_2, all three are constant linear combinations of g_1 and g_2; thus the three rows are linearly dependent.

(c) If M has rank at least 2, prove f is not the square of a linear polynomial (and thus $\mathbb{V}(f)$ is not a line).

Solution: Assume $f = g^2$. By the same argument as above, the three rows of M are the coefficients of constant multiples of g so that M has rank at most 1.

Problem 7 With notation from Problem 6 and assuming $\text{char}(k) \neq 2$, prove that $\mathbb{V}(f)$ is a line if M has rank 1, and that $\mathbb{V}(f)$ is reducible if M has rank 2. **Don't write up:** What if $\text{char}(k) = 2$?

Solution: Assume first M has rank 1. Because $(C_{2,0,0}, C_{1,1,0}, C_{0,2,0}) \neq (0,0,0)$, at least one of $\partial f/\partial X$ or $\partial f/\partial Y$ is nonzero; say $\partial f/\partial X \neq 0$. The other 2 rows are multiples of $\partial f/\partial X$, i.e., there exist $a, b \in k$ such that,

$$\begin{aligned} \partial f/\partial Y &= a\partial f/\partial X, \\ 2f - X\partial f/\partial X - Y\partial f/\partial Y &= b\partial f/\partial X \end{aligned}$$

Substituting in,

$$2f = (X + aY + b)\partial f/\partial X.$$

Partial differentiating both sides with respect to X and cancelling,

$$\partial f/\partial X = (X + aY + b)\partial^2 f/\partial X^2.$$

Therefore,

$$2f = (X + aY + b)(\partial^2 f/\partial X^2),$$

and $\mathbb{V}(f) = \mathbb{V}(2f) = \mathbb{V}(X + aY + b)$ is a line.

Next suppose that M has rank 2. Then there exists $(u, v, w) \neq (0, 0, 0)$ and a linear relation,

$$u\partial f/\partial X + v\partial f/\partial Y + w(2f - X\partial f/\partial X - Y\partial f/\partial Y) = 0.$$

If $w = 0$ then, after a linear change of coordinates, the relation gives $\partial f/\partial Y = 0$. Therefore $f = C_{2,0,0}X^2 + C_{1,0,1}X + C_{0,0,2}$, which is the equation of 2 parallel lines. If $w \neq 0$, then after translating to $(u/w, v/w)$, f has no constant or linear terms, i.e., f is the equation of 2 lines intersecting in $(u/w, v/w)$.

Difficult Problem 8 With notation as in Problem 3, prove that K is a radical ideal. **Warning:** You will need to use that k is algebraically closed; for k not a perfect field there are examples where the ideals I and J are radical, but K is not radical.

Solution: First comes a lemma of interest in its own right.

Lemma 0.1. *If V and W are irreducible, then K is a prime ideal.*

Proof. It suffices to prove for every pair $f', f'' \in k[z_1, \dots, z_{m+n}]$ not in K, $f'f''$ is not in K. Together f' and f'' involves only finitely many monomials, whose $(z_1, \dots, z_m)$-parts map to elements in $k[V]$ spanning a finite dimensional k-vector space, and whose $(z_{m+1}, \dots, z_{m+n})$-parts map to elements in $k[W]$ spanning a finite dimensional k-vector space. Denote by $a_1, \dots, a_r \in k[z_1, \dots, z_m]$ elements mapping to a basis for the finite dimensional k-subspace of $k[V]$, and by $b_1, \dots, b_s \in k[z_{m+1}, \dots, z_{m+n}]$ elements mapping to a basis for the finite dimensional k-subspace of $k[W]$. Modulo K, f' is congruent to $g' = \sum_{i,j} c'_{i,j} a_i b_j$ and f'' is congruent to $g'' = \sum_{i,j} c''_{i,j} a_i b_j$ for elements $c'_{i,j}, c''_{i,j} \in k$. Because f', f'' are not in K, also g', g'' are not in K. To prove $f'f''$ is not in K, it suffices to prove $g'g''$ is not in K.

Because $g' \neq 0$, $\sum_i c'_{i,j_1} a_i \neq 0$ for some j_1; denote this α'_{j_1}. Because $g'' \neq 0$, $\sum_i c''_{i,j_2} a_i \neq 0$ for some j_2; denote this α''_{j_2}. The images $\overline{\alpha'}_{j_1}, \overline{\alpha''}_{j_2} \in k[V]$ are nonzero because $a_1, \dots, a_r$ map to k-linearly independent elements. Because $k[V]$ is an integral domain, $\overline{\alpha'}_{j_1}\overline{\alpha''}_{j_2} \neq 0$, i.e., there exists $p = (p_1, \dots, p_m) \in V$ such that $\overline{\alpha'}_{j_1}(p), \overline{\alpha''}_{j_2}(p) \neq 0$. Denote by $g'(p), g''(p) \in k[W]$ the elements obtained by substituting in $z_i = a_i$ for $i = 1, \dots, m$ and $z_{m+i} = \overline{y_i}$ for $i = 1, \dots, n$. Each is a linear combination of the k-linearly independent elements $\overline{b}_1, \dots, \overline{b}_s$, and the coefficients of $\overline{b}_{j_1}$ in $g'(p)$ and of $\overline{b}_{j_2}$ in $g''(p)$ are nonzero, i.e., $g'(p), g''(p) \neq 0$. Because $k[W]$ is an integral domain, $g'(p)g''(p) \neq 0$, i.e., there exists $q \in W$ such that $g'(p,q)g''(p,q) \neq 0$. By Problem 3, $r = (p, q)$ is in $\mathbb{V}(K)$, therefore $g'g''$ is not in K. □

If either $V = \emptyset$ or $W = \emptyset$, the problem is trivial; hence assume both nonempty. Let $V_1, \dots, V_r$ be the irreducible components of V, and let $W_1, \dots, W_s$ be the irreducible components of W. For each $1 \leq i \leq r$ and $1 \leq j \leq s$, denote by $K_{i,j} \subset k[z_1, \dots, z_{m+n}]$ the ideal determined by $\mathbb{I}(V_i)$ and $\mathbb{I}(W_j)$. Clearly $K \subset \cap_{i,j} K_{i,j}$. The claim is that $K = \cap_{i,j} K_{i,j}$. Let $f \in \cap_{i,j} K_{i,j}$ be any element. Just as in the proof of the lemma, there exist sequences $a_1, \dots, a_r \in \cap_{i,j} K_{i,j}$ and $b_1, \dots, b_s \in \cap_{i,j} K_{i,j}$ mapping to k-linearly independent sets in $k[V]$ and $k[W]$ and such that, modulo K, f is congruent to an element $g = \sum_{v,w} c_{v,w} a_v b_w$. If f is not in K, then $g \neq 0$ so that for some w, $\sum_v c_{v,w} \overline{a_v} \in k[V]$ is nonzero. Therefore there exists $p \in V$ for which this element is nonzero. Thus $g(p) \in k[W]$ is nonzero. Because $g \in \cap_{i,j} K_{i,j}$, $g(p)$ is in $\cap_j \mathbb{I}(W_j) = (0)$. This contradiction proves $f \in K$. So $K = \cap_{i,j} K_{i,j}$. By the lemma, each ideal $K_{i,j}$ is a prime ideal. Therefore K is a radical ideal.

Problem 9 Prove $V = \{(t, t^2, t^3) | t \in k\}$ is an affine algebraic subset of $\mathbb{A}^3_k$ and find $\mathbb{I}(V) \subset k[x_1, x_2, x_3]$.

Solution: Clearly $V = \mathbb{V}(\langle x_2 - x_1^2, x_3 - x_1^3 \rangle)$.

Difficult Problem 10 Prove the subset $V = \{(s^3, s^2t, st^2, t^3) | s, t \in k\}$ is an affine algebraic subset of $\mathbb{A}^4_k$ and find $\mathbb{I}(V) \subset k[x_0, x_1, x_2, x_3]$. **Don't write up:** If you do both Problem 9 and Problem 10, compare your answers.

Solution: Consider the ideal $I = \langle x_0x_2 - x_1^2, x_0x_3 - x_1x_2, x_1x_3 - x_2^2 \rangle$. Denote $W = \mathbb{V}(I)$. Clearly $V \subset W$; the claim is $W \subset V$. Let $p = (a_0, \dots, a_3)$ be an element of W. If $a_0 = a_3 = 0$, then $a_1^2 = a_0a_2 = 0$ and $a_2^2 = a_1a_3 = 0$ so that $p = (0, 0, 0, 0)$, which is in V. Therefore assume $a_0 \neq 0$ or $a_3 \neq 0$; without loss of generality $a_0 \neq 0$. Denote by $s \in k$ any cube root of a_0 and denote $t = sa_1/a_0 = a_1/s^2$. Then $a_1 = s^2t$, $a_2 = (a_0a_2)/a_0 = a_1^2/a_0 = s^4t^2/s^3 = st^2$, and $a_3 = (a_0a_3)/a_0 = (a_1a_2)/a_0 = s^3t^3/s^3 = t^3$. So $p = (s^3, s^2t, st^2, t^3)$, which is in V. Therefore $V = \mathbb{V}(I)$.

Every I-congruence class of elements in $k[x_0, x_1, x_2, x_3]$ contains an expression, $f = a(x_0, x_3) + b(x_0, x_3)x_1 + c(x_0, x_3)x_2$, for unique polynomials $a(x_0, x_3), b(x_0, x_3), c(x_0, x_3) \in k[x_0, x_3]$. Consider the k-algebra homomorphism

$$\phi : k[x_0, x_1, x_2, x_3] \to k[s, t],$$
$$x_0 \mapsto s^3, x_1 \mapsto s^2t, x_2 \mapsto st^2, x_3 \mapsto t^3$$

The image $\phi(f)$ is $a(s^3, t^3) + b(s^3, t^3)s^2t + c(s^3, t^3)st^2$. Gathering monomials whose s and t exponent are congruent modulo 3, $\phi(f) = 0$ iff $a(s^3, t^3) = b(s^3, t^3) = c(s^3, t^3) = 0$, i.e., iff $f = 0$. So ϕ determines an injective k-algebra homomorphism $k[x_0, \dots, x_3]/I \to k[s, t]$. Since $k[s, t]$ is an integral domain, also $k[x_0, \dots, x_3]/I$ is an integral domain. Hence I is a prime ideal. By the Strong Nullstellensatz, $\mathbb{I}(V) = \text{rad}(I) = I$.

Problem 11 Assume $\text{char}(k) \neq 2$. Let $g \geq 1$ be an integer, let $a_1, a_2, \dots, a_{2g-1} \in k - \{0, 1\}$ be distinct elements, and denote $f = y^2 - x(x-1)(x-a_1) \dots (x - a_{2g-1}) \in k[x, y]$.

(a) Prove f is an irreducible polynomial. (**Hint:** Eisenstein's criterion.)

Solution: This follows immediately from Eisenstein's criterion for irreducibility.

(b) Prove the ring $k[x, y]/\langle f \rangle$ is not a unique factorization domain.

Solution: By way of contradiction, suppose it is a UFD. The claim is that $\overline{x}$ is a square. Every irreducible factor p of $\overline{x}$ is a factor of $\overline{y}$. Let $\overline{y} = p^e q$ with $q \notin \langle p \rangle$. Then $\overline{y}^2 = p^{2e}q^2$. For every $a \in k - \{0\}$, $a = \overline{x} - (\overline{x} - a)$ and p does not divide a, thus p does not divide $\overline{x} - a$. So p^{2e} divides $\overline{x}$. Because p does not divide q, it does not divide q^2, hence $\overline{x} = p^{2e}r$ with $r \notin \langle p \rangle$. Therefore the irreducible factorization of $\overline{x}$ is $p_1^{2e_1} \cdots p_m^{2e_m}$, i.e., $\overline{x} = u^2$ for $u = p_1^{e_1} \cdots p_m^{e_m}$.

Every element in $k[x,y]$ is congruent modulo $\langle f \rangle$ to $a(x) + b(x)y$ for unique polynomials $a(x), b(x) \in k[x]$; call this the *standard form* of the congruence class. Let $a(x) + b(x)y$ be a standard form such that $u = \overline{a(x) + b(x)y}$. Modulo f,

$$\begin{aligned}(a(x) + b(x)y)^2 &= a(x)^2 + 2a(x)b(x)y + b(x)^2y^2 \\ &\equiv (a(x)^2 + b(x)^2 x(x-1)\cdots(x-a_{2g-1})) + (2a(x)b(x))y,\end{aligned}$$

which is also congruent modulo f to $x + 0y$. Because the standard form of the congruence class is unique, $2a(x)b(x) = 0$ and $(a(x)^2 + b(x)^2x(x-1)\cdots(x-a_{2g-1})) = x$. Because $\text{char}(k) \neq 2$, $a(x)b(x) = 0$, i.e., $a(x) = 0$ or $b(x) = 0$. If $a(x) = 0$, then $x = b(x)^2x(x-1)\cdots(x-a_{2g-1})$. But then, in particular, $x - 1$ divides x which is absurd. If $b(x) = 0$, then $x = a(x)^2$ which is again absurd. This contradiction proves the hypothesis is false, i.e., $k[x,y]/\langle f \rangle$ is not a UFD.

(c) Conclude the affine algebraic set $\mathbb{V}(f) \subset \mathbb{A}_k^2$ is not isomorphic to $\mathbb{A}_k^1$. This affine algebraic set is the affine part of a *genus g hyperelliptic curve*.

Solution: The coordinate ring of $\mathbb{A}_k^1$ is $k[t]$, which is a UFD. Since the coordinate ring of $\mathbb{V}(f)$ is not isomorphic to the coordinate ring of $\mathbb{A}_k^1$, $\mathbb{V}(f)$ is not isomorphic to $\mathbb{A}_k^1$.

Difficult Problem 12 With notation from Problem 11, prove there is no non-constant regular morphism $F : \mathbb{A}_k^1 \to \mathbb{V}(f)$. (**Hint:** If there where such a morphism, what could you say about the irreducible factors of F^*y, F^*x, $F^*(x-1)$, etc.)

Solution: Let $F : \mathbb{A}_k^1 \to \mathbb{V}(f)$ be a regular morphism. The coordinate ring of $\mathbb{A}_k^1$ is $k[t]$, which is a UFD. Because they differ by nonzero constants, the irreducible factors of F^*x, $F^*(x-1)$, etc. are all distinct. But the concatenation of these irreducible factors is the irreducible factorization of F^*y^2, which is a square. Therefore each of F^*x, $F^*(x-1)$, etc. is a square. In particular, $F^*x = u^2$ and $F^*(x-1) = v^2$ for some polynomials $u, v \in k[t]$. But then $1 = F^*x - F^*(x-1) = u^2 - v^2 = (u-v)(u+v)$. So $u - v = a, u + v = a^{-1}$ for some nonzero constant. Solving, $2u = a + a^{-1}$. Thus F^*x is a constant. So also $F^*(x(x-1)\dots(x-a_{2g-1}))$ is a constant. Thus $F^*(y^2)$ is a constant, which implies $F^*(y)$ is a constant. Therefore F is a constant morphism.

Problem 13 Let $F : V \to W$ be a regular morphism of affine algebraic sets, and let $F^* : k[W] \to k[V]$ be the induced k-algebra homomorphism on coordinate rings.

(a) Prove $\text{Kernel}(F^*)$ is a radical ideal of $k[W]$.

Solution: The image of F^* is a subalgebra of a reduced ring, and so is itself a reduced ring. Therefore the kernel of F^* is a radical ideal.

(b) Describe the ideal $\mathbb{I}(F(V))$.

Solution: A polynomial function on W is zero on $F(V)$ iff the precomposition with F is zero iff it is in the kernel of F^*. Thus $\mathbb{I}(F(V))$ is $\text{Kernel}(F^*)$.

(c) Give a geometric interpretation to the condition that F^* is injective.

By (b), F^* is injective iff $\mathbb{I}(F(V))$ is the zero ideal iff the Zariski closure $\mathbb{V}(\mathbb{I}(F(V)))$ is all of W. Therefore F^* is injective iff $F(V) \subset W$ is dense in the Zariski topology.

(d) Give an example where F^* is injective, but $F(V) \neq W$.

Solution: Let $V = \mathbb{V}(xy-1) \subset \mathbb{A}^2_k$, let $W = \mathbb{A}^1_k$ and let $F : V \to W$ be $F(x,y) = x$. Then $F^* : k[x] \to k[x,y]/\langle xy-1\rangle = k[x][1/x]$ is injective. But $0 \in W - F(V)$.

Problem 14 Give an example of a homeomorphic regular morphism of affine algebraic sets that is *not* an isomorphism of affine algebraic sets. **Don't write up:** Try to find an example where the coordinate ring of the target is a unique factorization domain.

Solution: A standard example is to take $V = \mathbb{A}^1_k$, $W = \mathbb{V}(x^3 - y^2) \subset \mathbb{A}^2_k$ and $F : V \to W$ is $F(t) = (t^2, t^3)$. It isn't hard to see this is a bijection. Because the Zariski closed subset of V, resp. W, are V itself, resp. W itself, together with all finite subsets, F is a homeomorphism. But it is not an isomorphism, because the map of coordinate rings is not an isomorphism.

A more interesting example is the following, called the *Frobenius morphism* (ubiquitous in positive characteristic algebra). Let k be an algebraically closed field of positive characteristic p. Let $n \geq 1$ and define $F : \mathbb{A}^n_k \to \mathbb{A}^n_k$ by $F(x_1, \dots, x_n) = (x_1^p, \dots, x_n^p)$. This is a bijection because every element of k has a unique p^{th} root. Moreover, for every polynomial $g \in k[x_1, \dots, x_n]$, $g^p = F^*(h)$ for some element $h \in k[x_1, \dots, x_n]$. Therefore $\mathbb{V}(g) = \mathbb{V}(g^p) = F^{-1}(\mathbb{V}(h))$, implying $F(\mathbb{V}(g)) = \mathbb{V}(h)$. So F is a closed, continuous bijection, i.e., F is a homeomorphism. However F is not an isomorphism since there is no $h \in k[x_1, \dots, x_n]$ such that $F^*h = x_1$.

Problem 15 For every choice of $a, b \in k$, find the irreducible components of the affine algebraic set $\mathbb{V}(xy - z, bx + ay - z - ab) \subset \mathbb{A}^3_k$.

Solution: The irreducible components are $\mathbb{V}(x - a, z - ay)$ and $\mathbb{V}(y - b, z - bx)$.