Math 552: Homework 2

Sep 9th, 2020

Professor Kevin Tucker

Anish Chedalavada

Exercise 1. *Prove the following:*
a) (Cayley-Hamilton Trick) Suppose that M is a finitely generated module over a commutative ring R. If ϕ is any endomorphism, then ϕ satisfies a monic relation.
b) (Zariski's Lemma) if $R \subseteq S$ is a finite extension of domains, then R is a field iff S is a field.

Proof. a) Suppose M is finitely generated over R. In particular, we have an epimorphism from the free module $\pi : R^m \twoheadrightarrow M$ given by selection of the generators of M. Given an endomorphism $\phi : M \to M$, consider the following diagram:

$$
\begin{array}{ccccccc}
& & R^m & \dashrightarrow{\widetilde{\phi}} & \cdots & \dashrightarrow{\widetilde{\phi}} & R^m \\
& \nearrow{\widetilde{\phi}} & \downarrow{\pi} & & & & \downarrow{\pi} \\
R^m & \xrightarrow{\pi} M \xrightarrow{\phi} & M & \xrightarrow{\phi} & \cdots & \xrightarrow{\phi} & M
\end{array}
$$

We have the lift $\widetilde{\phi}$ via the universal property of projective modules (π is surjective), and as this is a free module homomorphism we may represent it by an $m \times m$ matrix A. By the Cayley-Hamilton theorem, we have that $p(x) = det(xI - A)$ for I the identity matrix is a vanishing polynomial for $\widetilde{\phi}$. In particular, this is a monic polynomial in R. Note that by the diagram above, $\pi \circ \widetilde{\phi} = \phi \circ \pi$, and iterating $\widetilde{\phi}$ as in the diagram above yields $\pi \circ \widetilde{\phi}^n = \phi^n \circ \pi$. Thus, we have that $p(\phi) \circ \pi = \pi \circ p(\widetilde{\phi}) = 0$ by the logic above, and as π is a surjective we have that $p(\phi) \circ \pi = 0 \implies p(\phi) = 0$, yielding the claim.

b) Assume R is a field. Given an arbitrary nonzero element $s \in S$, we have that s satisfies some minimal monic polynomial p over R by finiteness, and thus we have a morphism $R[x]/(p) \hookrightarrow S$ given by $x \mapsto s$ (inclusion as p assumed minimal, i.e. that (p) is the kernel). However, as S is assumed to be a domain we have that (p) must be a prime ideal and thus maximal as $R[x]$ is a PID (R assumed to be a field). Thus, $R[s] \subset S$ is a field, implying that s has a multiplicative inverse in S. As $s \in S$ was arbitrary nonzero, this is true of all $s \in S \setminus \{0\}$ and thus S is a field.

Assume now that S is a field. Suppose R is not a field, i.e. that there exists some proper maximal ideal $(0) \neq \mathfrak{m} \subset R$. Then for any $0 \neq m \in \mathfrak{m}$, we have that $m^{-1} \in S$ satisfies a monic relation in R (by finiteness) given by:

$$m^{-n} + a_{n-1}m^{-(n-1)} + \dots + a_0 = 0$$

Multiplying the entire above equation by m^n yields:

$$1 + a_{n-1}m + \dots + a_0 m^n = 0 \implies 1 = a_{n-1}m + \dots + a_0 m^n \implies 1 \in \mathfrak{m}$$

Yielding a contradiction, as $\mathfrak{m}$ assumed to be a proper maximal ideal. Thus, we cannot select $0 \neq m \in \mathfrak{m}$, implying that $\mathfrak{m}$ must be zero and thus the only maximal ideal in R is (0), implying that R is a field. $\square$

Exercise 2. *Let $k = \overline{k}$ be a field of characteristic not 2. Let V_c be the intersection of the circle $x^2 + y^2 = 1$ in $\mathbb{A}^2$ with the line $x = c$, for $c \in k$.*
a) Find $I(V_c)$.
b) Consider the projection $\mathbb{A}^2 \to \mathbb{A}^1$ sending $(x, y) \mapsto x$, restricted to circle $x^2 + y^2 = 1$. Draw a picture to describe this map, and interpret the variety V_c geometrically in terms of this map.
c) What happens in characteristic 2?

Proof. a) In a field of characteristic 2, we have that $\sqrt{(x^2 + y^2 - 1)} = (x^2 + y^2 - 1)$, as there does not exist $p \in k[x, y]$ such that $p^n | x^2 + y^2 - 1$ for $n \neq 1$ (required in a UFD). Thus, $I(x^2 + y^2 = 1) = (x^2 + y^2 - 1)$ by the Nullstellensatz. Thus, we have that $I(\{x^2 + y^2 = 1\} \cap \{x = c\}) = (x^2 + y^2 - 1, x - c) = (y^2 + (c^2 - 1), x - c)$. For $c \neq \pm 1$, we have that $y^2 = c^2 - 1$ has two solutions a_1, a_2 for y in $k[y]$, and we have two irreducible components of $\{x^2 + y^2 = 1\} \cap \{x = c\}$ corresponding to the points (c, a_1), (c, a_2) for the prime ideals $(y - a_1, x - c)$, $(y - a_2, x - c)$ which contain and intersect in our ideal. For $c = \pm 1$ we have that $c^2 - 1 = 0$

and $y^2 = c^2 - 1$ has only one solution with multiplicity at 0; i.e. that $\{x^2 + y^2 = 1\} \cap \{x = c\} = (\pm 1, 0)$ corresponding to $\sqrt{(y^2, x - c)} = (y, x - c)$.

b) Consider the following diagram:
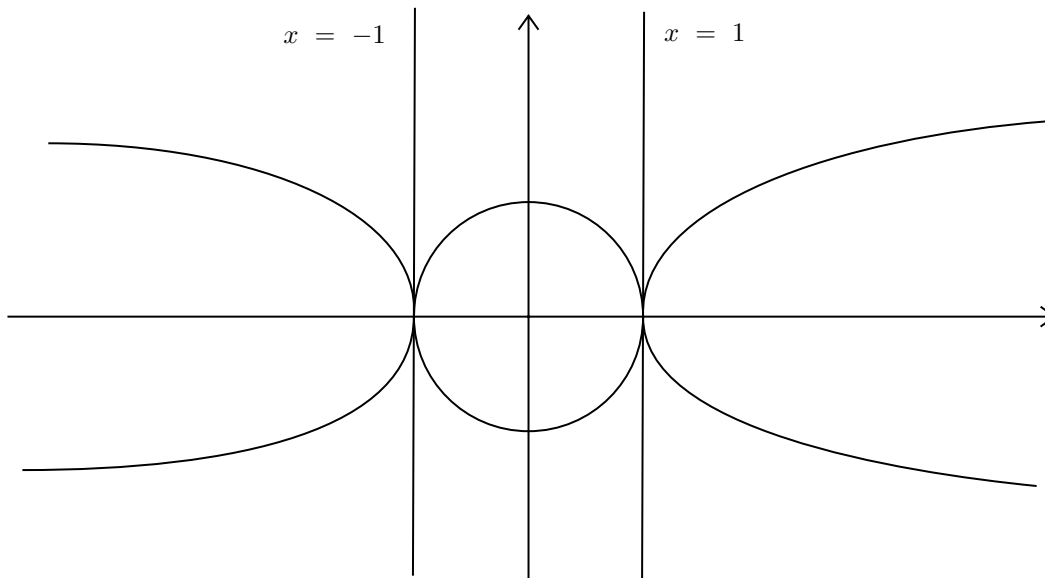
Above is the graph of our algebraic set $x^2 + y^2 = 1$, and at $x = 1, -1$ we have that there is only one solution with a double point singularity, i.e. only one point in the fiber over $x = 0, y = 0$ under the projection.

c) If the characteristic of k is 2, then the ideal $I(V_c)$ contains $(x^2 + y^2 + 1, x + c) = (y^2 + c^2 + 1, x + c) = ((y + c + 1)^2, x + c)$, the radical of which is $(y + c + 1, x + c)$, corresponding to the single irreducible component $(c, c + 1)$. Thus, each point in the x-axis has only one point in its fiber under the projection map from the curve. $\qquad\square$

Exercise 3. *Consider the map $\mathbb{A}^1 \to \mathbb{A}^3$ given by $t \mapsto (t, t^2, t^3)$. Show that the image of this map is an affine algebraic set that can be defined by two equations in $k[x, y, z]$.*

Proof. Consider the equations $x^2 - y$, $x^3 - z \in k[x, y, z]$. We have that the vanishing set of these equations is all points (a, b, c) such that $b = a^2$, $c = a^3$; i.e. the points $(a, a^2, a^3) \in \mathbb{A}^3$ for $a \in k$. Thus, we have that the image of the map in the question is exactly an algebraic set, the vanishing of which is given by the equations above. $\qquad\square$

Exercise 4. *Describe the image of the map $f : \mathbb{A}^2 \to \mathbb{A}^2$ given by $f : (x, y) \mapsto (x, xy)$. Is it open, closed, and/or dense?*

Proof. The image of f is given by $\mathbb{A}^2 \setminus \{(0, y) \mid y \neq 0\}$, as for any $(x, y) \in \mathbb{A}^2$ s.t. x is a unit, w.h.t. $f(x, y/x) = (x, y)$. For $x = 0, w.h.t. f(x, y) = (0, 0)$. Consider the map $g_z : \mathbb{A}^1 \to \mathbb{A}^2$ via $g : t \mapsto (t, n)$ (given by the map on coordinate rings given by $k[x, y] \to k[x]$ by $y \mapsto n \in k$); we have that $g_3^{-1}(Im(f)) = \mathbb{A}^2 \setminus \{0\}$ which is open in the Zariski topology, being the complement of the set $\{t = 0\}$, thus $Im(f)$ is not a closed set. We also have the map $h : \mathbb{A}^1 \to \mathbb{A}^2$ by $h : t \mapsto (0, t)$, and $h^{-1}(Im(f)) = \{0\}$, which is closed in the Zariski topology; thus, $Im(f)$ is neither open nor closed in the Zariski topology. Finally, we have that for $g : X \to Y$ a continuous map and $A \subset X$, $\overline{g^{-1}(A)} \subseteq g^{-1}(\overline{A})$. Thus for any $n \neq 0$ in k, w.h.t. $\overline{g_n^{-1}(A)} \subseteq g_n^{-1}(\overline{Im(f)})$, and for $n = 0$ w.h.t. $g^{-1}(Im(f)) = \mathbb{A}^2 \setminus \{0\}$, and thus $\overline{g^{-1}(\mathbb{A}^2)} = \mathbb{A}^2 \subset g^{-1}(\overline{Im(f)})$, implying $\forall\, t \in k$, $(0, t) \in \overline{Im(f)}$, and thus $Im(f) = \mathbb{A}^2$, so the set is dense. $\qquad\square$

Exercise 5. *For the morphisms in 2 b), 3, and 4, describe the induced map of coordinate rings.*

Proof. The morphism in 2 b) is the projection of the curve $C = x^2 + y^2 = 1$ onto the x-axis. We have that the coordinate ring of this curve is given by $k[x,y]/(x^2 + y^2 = 1)$. We have that the projection factors as $C \hookrightarrow \mathbb{A}^2 \twoheadrightarrow \mathbb{A}^1$, inducing a map on coordinate rings by $k[x] \hookrightarrow k[x,y] \twoheadrightarrow k[x,y]?(x^2 + y^2 = 1)$. Thus, the map of coordinate rings is given by $k[x] \to k[x,y]/(x^2 + y^2 = 1)$ via $x \mapsto [x]$.

For the morphism in 3, we have that the coordinate ring of the image of $\mathbb{A}^1$ is given by $k[x,y,z]/(x^2 - y, x^3 - z) \cong k[x]$. We have that the functions y, z pull back to the functions x^2, x^3 via this map, and so the map on coordinate rings is explicitly given by the quotient map $k[x,y,z] \to k[x,y,z]/(x-y^2, x-z^3) \cong k[x] = k[\mathbb{A}^1]$.

For the morphism in 4, we have that the function x pulls back along the first coordinate to the function x, and the function y pulls back along (x,xy) to be the function xy. This is clear as $y(a,b) = b$, and so for f the map of 4, $y(f(x,y)) = y(x,xy) = xy$. Thus, the induced map on coordinate rings is given by $k[x,y] \to k[x,y]$ via $x \mapsto x, \ y \mapsto xy$. $\qquad\square$

Exercise 6. *Assume $k = \bar{k}$.*
a) What is the coordinate ring of a point? What is the k-algebra homomorphism corresponding to the inclusion of a point into another affine set?
b) When is the coordinate ring of an affine algebraic set a finite-dimensional k-vector space, and what is the geometric interpretation of the same?

Proof. a) Given a point $(a_1, ..., a_n) \in \mathbb{A}^n$, we have that $(x_1 - a_1, ..., x_n - a_n) \subset I((a_1, ..., a_n)) \subset k[x_1, ..., x_n]$, and as k is algebraically closed we have by the Nullstellensatz that $(x_1 - a, ..., x_n - a_n)$ is maximal: thus, $k[x_1, ..., x_n]/I((x_1 - a_1, ..., x_n - a_n)) \cong k$ is the coordinate ring of a point. The k-algebra homomorphism corresponding to the inclusion of the point into $\mathbb{A}^n$ is given by the quotient homomorphism $k[x_1, ..., x_n] \to k$ via the quotient map.

b) If the coordinate ring R of an affine algebraic set X is a finite dimensional k-vector space then R is Artinian. In particular, R has finitely many prime ideals $\mathfrak{m}_1, ..., \mathfrak{m}_n$ and all the primes are maximal. Thus, $\sqrt{I(X)} \subset k[x_1, ..., x_n]$ is the intersection of finitely many maximal ideals $\mathfrak{m}_i$ (which are the primes containing $I(X)$), and by the Nullstellensatz we have that $X = V(\sqrt{I(X)}) = V(\bigcap_{i=1}^n \mathfrak{m}_i) = \bigcup_{i=1}^n V(\mathfrak{m}_i)$. By the Nullstellensatz again we have that all maximal ideals are of the form $(x_1 - a_1, ..., x_n - a_n)$ corresponding to points $(a_1, ..., a_n) \in \mathbb{A}^n$. Thus, X is the union of finitely many points in $\mathbb{A}^n$. Furthermore, $\sqrt{I(X)} = I(X)$, *again* by the Nullstellensatz, and so $I(X) = \bigcap_{i=1}^n \mathfrak{m}_i$ and so $k[x_1, ..., x_n]/\bigcap_{i=1}^n \mathfrak{m}_i = \prod_{i=1}^n k[x_1, ..., x_n]/\mathfrak{m}_i = \prod_{i=1}^n k$; thus, the dimension of the coordinate ring is the same as the number of maximal ideals, which is the same as the number of points in X. $\qquad\square$

Exercise 7. *Show that any nonempty open subset of an irreducible topological space is dense and irreducible, and that the closure of an subset irreducible in the subspace topology is also irreducible.*

Proof. Given any two distinct proper open sets $U_1, U_2 \subset X$ for X an irreducible topological space, we have that $X \setminus (U_1 \cup U_2) = (X \setminus U_1) \cup (X \setminus U_2) \neq X$ by irreducibility (X not the union of two closed subsets), we thus have that $U_1 \cup U_2 \neq \emptyset$ and so any open set U_1 is dense in X. Now suppose there exist two distinct closed sets $V_1, V_2 \subset U_1$ in the subspace topology s.t. $V_1 \cup V_2 = U_1$. Then there exist $\widetilde{V_1}, \widetilde{V_2} \subset X$ closed subsets such that $\widetilde{V_i} \cup U_1 = V_1$, and $\widetilde{V_1} \cup \widetilde{V_2} \cup (X \setminus U_1) = X$, all of which are distinct, which would contradict the irreducibility of X. Thus, U_1 could not have been reducible.

Now suppose $Y \subset X$ is irreducible in the subspace topology. Suppose $\overline{Y}$ is reducible, i.e. that there exist closed sets $W_1, W_2 \subset X$ distinct such that $(W_1 \cup W_2) \cap \overline{Y} = \overline{Y}$, then either $Y \subset W_1$ or $Y \subset W_2$ by the irreducibility of Y, implying that either $\overline{Y} \subset W_1$ or $\overline{Y} \subset W_2$ and thus $\overline{Y}$ is irreducible (cannot be the union of two proper closed subsets in the subspace topology. $\qquad\square$

Exercise 8. *Let k be an arbitrary field.*
a) If V and W are affine algebraic sets over k, show that $k[V \times W] = k[V] \otimes_k k[W]$.
b) Suppose that V and W are disjoint algebraic sets in $\mathbb{A}^n$. Show that $k[V \cup W] = k[V] \times k[W]$.

Proof. a) Given two affine algebraic sets $V \subset \mathbb{A}^n$, $W \subset \mathbb{A}^m$, in order to know $k[V \times W] \subset k[x_1, ..., x_n, y_1, ..., y_m]$ (which we'll abbreviate $k[\mathbb{A}^n \times \mathbb{A}^m]$) it suffices to understand the structure as a $k[x_1, ..., x_m, y_1, ..., y_m]$-module, which is the same as a $k[\mathbb{A}^n] \otimes_k k[\mathbb{A}^m]$ module. Now note that we can represent $V \times W \subset \mathbb{A}^n \times \mathbb{A}^m$ as the intersection $V \times \mathbb{A}^n \cap \mathbb{A}^m \times W$. Thus, $I(V \times W)$ is given by ideal generated by $(p_1 \otimes 1, ..., p_n \otimes 1, 1 \otimes q_1, ..., 1 \otimes q_m) \subset k[\mathbb{A}^n \times \mathbb{A}^m]$ for $p_1, ..., p_n$ generating $I(V) \subset k[\mathbb{A}^n]$ and $q_1, ..., q_m$ generating $I(V) \subset k[\mathbb{A}^m]$. We have that that $(p_1 \otimes 1, ..., p_n \otimes 1)$ as a $k[\mathbb{A}^n \times \mathbb{A}^m]$ module is given by $I(V) \otimes_{k[\mathbb{A}^n]} k[\mathbb{A}^n] \otimes_k k[\mathbb{A}^m]$. We have that $k[\mathbb{A}^n] \otimes_k k[\mathbb{A}^m]$ is a free left $k[A^n]$ module and is thus flat, so from the following $k[\mathbb{A}^n]$ resolution,

$$0 \longrightarrow I(V) \longrightarrow k[\mathbb{A}^n] \longrightarrow k[V] \xrightarrow{\pi_V} 0$$

using the functor $- \otimes_{k[A^n]} k[\mathbb{A}^n] \otimes_k k[\mathbb{A}^m] : k[\mathbb{A}^n] - Mod \to k[\mathbb{A}^n] \otimes_k k[\mathbb{A}^m] - Mod$, we have the following diagram:

$$I(V) \otimes_{k[\mathbb{A}^n]} k[\mathbb{A}^n] \otimes_k k[\mathbb{A}^m] \lhook\joinrel\longrightarrow k[\mathbb{A}^n] \otimes_k k[\mathbb{A}^m] \xrightarrow{\pi_V \otimes id} k[V] \otimes_k k[\mathbb{A}^m]$$

i.e. that $k[\mathbb{A}^n \times \mathbb{A}^m]/(p_1 \otimes 1, ..., p_n \otimes 1) \cong k[V] \otimes_k k[\mathbb{A}^m]$. Now we have that $k[V \times W] = k[V] \otimes_k k[\mathbb{A}^m]/([1 \otimes q_1], ..., [1 \otimes q_m])$ for $[1 \otimes q_i] = (\pi_V \otimes id)(1 \otimes q_i)$. We have that $([1 \otimes q_1], ..., [1 \otimes q_m]) \cong k[V] \otimes_k k[\mathbb{A}^m] \otimes_{k[\mathbb{A}^m]} (q_1, ..., q_m)$, again by the same rationale as above: $k[\mathbb{A}^n] \otimes_k k[\mathbb{A}^m] \otimes_{k[\mathbb{A}^m]} (q_1, ..., q_m)$ is a free left $k[\mathbb{A}^n]$ module indexed over a k-basis for $(q_1, ..., q_m)$, and we have the following diagram of $k[\mathbb{A}^n] \otimes k[\mathbb{A}^m]$ modules:

$$
\begin{array}{ccc}
I(V) \otimes_{k[\mathbb{A}^n]} k[\mathbb{A}^n] \otimes_k k[\mathbb{A}^m] \otimes_{k[\mathbb{A}^m]} (q_1, ..., q_m) & \xhookrightarrow{id \otimes \iota} & I(V) \otimes_{k[\mathbb{A}^n]} k[\mathbb{A}^n] \otimes_k k[\mathbb{A}^m] \\
\downarrow & & \downarrow \\
k[\mathbb{A}^n] \otimes_k k[\mathbb{A}^m] \otimes_{k[\mathbb{A}^m]} (q_1, ..., q_m) & \xhookrightarrow{id \otimes \iota} & k[\mathbb{A}^n] \otimes_k k[\mathbb{A}^m] \\
\downarrow{\scriptstyle \pi_V \otimes id} & & \downarrow{\scriptstyle \pi_V \otimes id} \\
k[V] \otimes_k k[\mathbb{A}^m] \otimes_{k[\mathbb{A}^m]} (q_1, ..., q_m) & \xrightarrow{id \otimes \iota} & k[V] \otimes_k k[\mathbb{A}^m]
\end{array}
$$

Where $\iota : k[\mathbb{A}^m] \otimes_{k[\mathbb{A}^m]} (q_1, ..., q_m) \hookrightarrow k[\mathbb{A}^m]$ is the inclusion as an ideal; we see the middle map corresponds exactly to the inclusion of $(1 \otimes q_1, ..., 1 \otimes q_m)$ as an ideal. Note that $k[V] \otimes_k k[\mathbb{A}^m]$ is a free right $k[\mathbb{A}^m]$ module indexed over a k-basis of $k[V]$ and is thus flat, so running the same argument as above with the sequence $0 \to I(W) \to k[\mathbb{A}^m] \to k[W] \to 0$ and the functor $k[V] \otimes_k k[\mathbb{A}^m] \otimes_{k[\mathbb{A}^m]} - : k[\mathbb{A}^n] - Mod \to k[\mathbb{A}^n] \otimes_k k[\mathbb{A}^m] - Mod$ yields that $k[V \times W] = k[V] \otimes_k k[\mathbb{A}^m]/([1 \otimes q_1], ..., [1 \otimes q_m]) = k[V] \otimes_k k[W]$, proving the claim.

b) Assuming k algebraically closed, if V and W are disjoint algebraic sets, we have that $I(V) + I(W) = I(V \cap W) = I(\emptyset) = k[x_1, ..., x_n]$, and we have that $I(V \cup W) = I(V) \cup I(W)$. We have that by Chinese Remainder Theorem (as $I(V), I(W)$ are comaximal), $k[V \cup W] = k[x_1, ..., x_n]/I(V) \cap I(W) = k[x_1, ..., x_n]/I(V) \times k[x_1, ..., x_n]/I(W) = k[V] \times k[W]$. $\qquad \square$