UAGS Lecture Notes 2

Wyatt Reeves

1 More on the Zariski Topology

We didn't do problem 2 from problem set 1 during recitation, so here is the solution (at least to the draw a picture part):

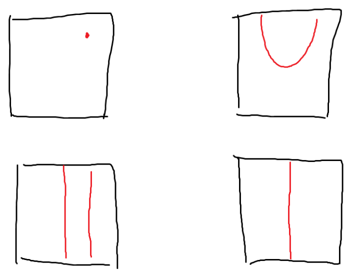

Figure 1: Upper left: $V(x-a, y-b)$, Upper right: $V(x^2-y)$, Lower left: $V(x^2-x)$, Lower right; $V(x^2)$. Here we take the underlying field to be $\mathbb{R}$ for each picture.

Note a couple of things from this. First, note that $V(x^2) = V(x)$, even though $(x^2) \neq (x)$ in $k[x,y]$. Evidently the relationship between ideals and varieties isn't one-to-one. We will revisit this relationship later in the lecture. More qualitatively, note that all of the proper closed subsets in the Zariski topology are "small" or "thin" compared to the kinds of closed subsets that you see in the real-analytic topology. The corresponding statement for open sets is that the open sets in the Zariski topology are all quite large. More precisely, we can say that in general the Zariski topology on $\mathbb{A}^n$ won't be *Hausdorff*.

Definition 1.1. A topological space X is *Hausdorff* if for every pair p, q of distinct points in X, there are non-intersecting open sets U, V such that $p \in U$ and $q \in V$.

Intuitively, the open sets in the Zariski topology are "too big" to not overlap. The open sets of the Zariski topology are at least refined enough that the following holds:

Proposition 1.2. *Every point in $\mathbb{A}^n$ is closed in the Zariski topology.*

Proof. If $p = (p^1 \dots p^n)$ and $k[\mathbb{A}^n] = k[x^1 \dots x^n]$, then $p = V(x^1 - p^1 \dots x^n - p^n)$. □

We can describe the Zariski topology very explicitly in the case of $\mathbb{A}^1$

Proposition 1.3. *The closed sets in the Zariski topology on $\mathbb{A}^1$ are exactly the finite sets.*

Proof. Let $k[\mathbb{A}^1] = k[x]$. Then for any finite collection of points $X = \{p_1 \dots p_n\}$, consider the polynomial

$$f(x) = \prod_{i=1}^{n} (x - p_i).$$

Then $X = V(f)$. Conversely, let I be an ideal in $k[x]$. We know $k[x]$ is a PID, so $I = (f)$ for some polynomial f. Any polynomial has only finitely many roots, so $V(I) = V(f)$ contains only finitely many points. □

We now introduce a property which is a sort of analog of connectedness for spaces with relatively few open sets

Definition 1.4. A topological space X is irreducible if any two non-empty open sets have a nonempty intersection. Equivalently, in terms of closed sets, a topological space is irreducible if and only if the union of any two proper closed sets is again a proper closed set.

Any Hausdorff space with more than one point isn't irreducible, since we can take neighborhoods U, V of any two distinct points that are disjoint. Both U and V are non-empty, but their intersection isn't. In our case, however, we have the following result.

Proposition 1.5. *Let our underlying field k be infinite. Then the Zariski topology on $\mathbb{A}^n$ is irreducible.*

Proof. Suppose I and J are two ideals of $\mathbb{A}^n$ such that $V(I)$ and $V(J)$ are proper closed subsets of $\mathbb{A}^n$. Then we know that I must contain some nonzero polynomial f and J must contain some nonzero polynomial g (otherwise $V(I), V(J)$ wouldn't be proper). We know that $V(I) \cup V(J) = V(IJ)$, and IJ contains the nonzero polynomial fg. Since k is infinite, we know that there is at least one point p of $\mathbb{A}^n$ where fg doesn't vanish, so $p \notin V(IJ)$ and we conclude that $V(I) \cup V(J)$ is again a proper subset of $\mathbb{A}^n$. □

2 Cayley-Hamilton Again

We first prove the following preliminary result:

Lemma 2.1. *Let $f : \mathbb{A}^n \to \mathbb{A}^1$ be a polynomial map. Then f is continuous with respect to the Zariski topologies on $\mathbb{A}^n$ and $\mathbb{A}^1$.*

Proof. We need to show that if K is a closed subset of $\mathbb{A}^1$ then $f^{-1}(K)$ is a closed subset of $\mathbb{A}^n$. By Proposition 1.3, we know that $K = \{a_1 \dots a_n\}$, so $f^{-1}(K) = \bigcup_{i=1}^n f^{-1}(a_i)$. But $f^{-1}(a_i)$ is exactly the set of points $(x^1 \dots x^n) \in \mathbb{A}^n$ such that

$$f(x^1 \dots x^n) = a_i,$$

in other words, $V(f - a_i)$, which is closed. So $f^{-1}(K)$ is a finite union of closed sets, and therefore closed. □

Now we can prove the Cayley-Hamilton theorem over an arbitrary algebraically closed field:

Theorem 2.2 (Cayley-Hamilton)**.** *Let V be a finite-dimensional vector space over an algebraically closed field k. Let $T : V \to V$ be a linear transformation. If p_T is the characteristic polynomial of T, then $p_T(T) = 0$.*

Proof. By picking a basis for V, we can identify $\mathrm{End}(V)$ with $\mathrm{Mat}_n(k) \cong \mathbb{A}^{n^2}$, where n is the dimension of V. Having done this, note that the coefficients of p_T are polynomials in the entries of the matrix A representing T, so the statement $p_T(T) = 0$ is equivalent to the statement $p_{ij}(a_{11} \dots a_{nn}) = 0$ for $1 \leq i, j \leq n$, where p_{ij} is a polynomial in the entries of A that equals the i, jth entry of $p_T(T)$. We will now show that these polynomials are all 0. Whenever T is diagonalizable, we know by the argument given last time that $p_T(T) = 0$, so $p_{ij} = 0$ for all i, j. Note that whenever $\mathrm{disc}(p_T) \neq 0$ we know that p_T has no repeated roots, so we know that T is diagonalizable. Therefore on $\mathbb{A}^n \setminus V(\mathrm{disc})$ we know that $p_{ij} = 0$ for all i, j. However, by Proposition 1.5 we know that the Zariski-open subsets of $\mathbb{A}^{n^2}$ are Zariski-dense. Since p_{ij} is a continuous map from $\mathbb{A}^{n^2}$ to $\mathbb{A}^1$ (Lemma 2.1) and since points in $\mathbb{A}^1$ are closed (Proposition 1.2), we must therefore conclude that $p_{i,j} = 0$ on all of $\mathbb{A}^{n^2}$ for all i, j. This shows that $p_T(T) = 0$ for all $T : V \to V$. □

From this a more general result immediately follows:

Corollary 2.3. *Let A be an integral domain and let M be a finitely-generated free A-module and let $T : M \to M$ be an A-linear map. If p_T is the characteristic polynomial of T, then $p_T(T) = 0$.*

Proof. Embed A into the algebraic closure of its fraction field and apply the previous theorem. □

This illustrates a more general phenomenon. If we understand algebra over algebraically closed fields, we can often gain information about more general fields by embedding them into their algebraic closure, doing some computation there, and then extracting back out the original information we wanted to understand. As a result, from here on, unless otherwise stated, **we will always assume our underlying field to be algebraically closed**.

3 Hilbert's Nullstellensatz

We now define an operation that is in some sense "opposite to" V.

Definition 3.1. Given X a subset of $\mathbb{A}^n$, define $\mathcal{I}(X)$ to be the ideal of functions $f \in k[\mathbb{A}^n]$ such that $f(p) = 0$ for all $p \in X$.

Example 3.2. Consider $S = \mathcal{I}(V(x))$. If $f(x, y) \in S$, write $f = f_n(y)x^n + \ldots + f_0(y)$. Then since $f \in S$ we know that $f(0, y) = f_0(y)$ has to vanish for all y, so

$$f = x(f_n(y)x^{n-1} + \ldots + f_1(y)),$$

so $S \subseteq (x)$. Conversely, if $f \in (x)$ then f vanishes on $V(x)$, so $S = (x)$.

clearly $\mathcal{I}$ isn't exactly inverse to V, since $\mathcal{I}(V(x)) = \mathcal{I}(V(x^2)) = (x)$. However, it does seem to be somehow related.

Definition 3.3. Let I be an ideal of a commutative ring A. Then $\sqrt{I}$ is the set of all elements $a \in A$ such that $a^n \in I$.

The following powerful theorem due to David Hilbert makes the relationship between V and $\mathcal{I}$ completely explicit.

Theorem 3.4 (Hilbert)**.** *Let k be algebraically closed and let I be an ideal of $k[\mathbb{A}^n]$. Then $\mathcal{I}(V(I)) = \sqrt{I}$.*

We delay the proof of this theorem until later, when we have more commutative algebra under our belts. We'll go ahead and apply it to get the following result:

Proposition 3.5. *Let $X_1, X_2 \subseteq \mathbb{A}^n$ be disjoint closed subsets. Then there is a polynomial $f \in k[\mathbb{A}^n]$ that vanishes on X_1 but evaluates to 1 on X_2.*

Proof. Let $X_1 = V(I_1)$ and $X_2 = V(I_2)$. Since X_1 and X_2 are disjoint, $X_1 \cap X_2 = V(I_1 + I_2) = \emptyset$. By the Nullstellensatz,

$$\sqrt{I_1 + I_2} = \mathcal{I}(V(I_1 + I_2)) = \mathcal{I}(\emptyset) = k[\mathbb{A}^n].$$

in particular, $1 \in \sqrt{I_1 + I_2}$, so $1^n = 1 \in I_1 + I_2$. We see that there is some $f \in I_1$ and some $g \in I_2$ such that $f = 1 - g$. Since $f \in I_1$ we know that f vanishes on X_1, and since g vanishes on X_2, we know that f evaluates to 1 on X_2, so f is our desired function. $\square$

This gives an analog of algebraic geometry of Urysohn's Lemma for more general topological spaces. Urysohn's Lemma only applies in general to normal spaces, however, which is a category that includes basically none of the spaces we consider. This proposition can be thought of as telling us that our spaces are more separated than they might seem.