INTRODUCTION TO ALGEBRAIC GEOMETRY, CLASS 3

RAVI VAKIL

Contents

(Before class started, I showed that (finite) Chomp is a first-player win, without showing what the winning strategy is.)

If you've seen a lot of this before, try to solve:

"Fun problem" 2. Suppose $f_1(x_1, \dots, x_n) = 0, \dots, f_r(x_1, \dots, x_n) = 0$ is a system of r polynomial equations in n unknowns, with integral coefficients, and suppose this system has a finite number of complex solutions. Show that each solution is algebraic, i.e. if $(x_1, \dots, x_n)$ is a solution, then $x_i \in \overline{\mathbb{Q}}$ for all i.

1. Where we are

We now have seen, in gory detail, the correspondence between *radical ideals* in $\overline{k}[x_1, \dots, x_n]$, and *algebraic subsets* of $\mathbb{A}^n(\overline{k})$. Inclusions are reversed; in particular, maximal proper ideals correspond to minimal non-empty subsets, i.e. points. A key part of this correspondence involves the *Nullstellensatz.*

Explicitly, if X and Y are two algebraic sets corresponding to ideals I_X and I_Y (so $I_X = I(X)$ and $I_Y = I(Y)$, and $V(I_X) = X$, and $V(I_Y) = Y$), then $I(X \cup Y) = I_X \cap I_Y$, and $I(X \cap Y) = \sqrt{(I_X, I_Y)}$. That "root" is necessary.

Some of these links required the following theorem, which I promised you I would prove later:

Theorem. Each algebraic set in $\mathbb{A}^n(\overline{k})$ is cut out by a finite number of equations.

This leads us to our next topic:

Date: September 16, 1999.

2. Noetherian rings and the Hilbert basis theorem

By our equivalence between algebraic sets and radical ideals, this is equivalent to:

Each radical ideal of $\overline{k}[x_1, \dots, x_n]$ is finitely-generated.

This will follow from:

Theorem. Every ideal of $\overline{k}[x_1, \dots, x_n]$ is finitely-generated.

In proving this, we will come across some important ideas.

Definition. A ring is *Noetherian* if every *ascending* chain of ideals eventually stabilizes.

In other words, if you have a chain of ideals

$$I_1 \subset I_2 \subset I_3 \subset \cdots \subset R$$

then for some n_0, for $n \geq n_0$, $I_n = I_{n_0}$.

This is *equivalent* to: every ideal I of R is finitely-generated. (This definition is often much easier to check.) That will be an *exercise*. This involves *Noetherian induction*.

Examples. (a) A field k. There are only two ideals!

(b) The integers $\mathbb{Z}$. The ideals are of the form (0), and (n) $n \in \mathbb{Z}^+$. It is easy to check that every ascending chain of ideals eventually stabilizes, but easier to check the second condition, that every ideal is finitely-generated: they are all generated by one term. (By this argument, all *principal ideal domains* are Noetherian.)

(c) The quotient of a Noetherian ring is also Noetherian, i.e. if R is Noetherian, and I is any ideal, then R/I is Noetherian.

Proof: ideals in R/I correspond precisely to ideals in R containing I.

(d) The localization of a Noetherian ring is Noetherian.

(e) *The Hilbert Basis Theorem.* If R is Noetherian, then $R[x]$ is Noetherian. (Proof: soon.) Hence by induction $\overline{k}[x_1, \dots, x_n]$ is Noetherian. Combining (a)–(d), we see that *all quotients of finitely-generated rings over a field (or the integers) are Noetherian.*

(f) *Fact.* Essentially every ring you come across in geometry is Noetherian. This isn't so true in number theory / algebraic geometry.

(g) *But!:* Not all rings are Noetherian. For example, consider the ring that I'll call $k[x^\epsilon]$, where elements finite sums of the form ax^b where $a \in k$, and b is a non-zero real number. It's clear how to add and multiply them, so they are really a ring. Also for every $\epsilon > 0$, (x^ϵ) is an ideal. Then

$$(x^1) \subset (x^{1/2}) \subset (x^{1/3}) \subset \cdots \subset R$$

is an ascending chain of ideals that doesn't stabilize.

What we'll do next: (1) The proof is short, so we'll prove the Hilbert basis theorem. (2) For fun, we'll see the game of Chomp. (3) Finally, I'll describe a geometric picture that will make you believe it, and that picture will motivate some reasonable definitions.

(1) Proof of the Hilbert basis theorem.

Some of your intuition from the geometric picture and from chomp will give you a proof.

The statement: If R is Noetherian, then the ring of polynomials in one variable in R, $R[x]$, is Noetherian. In other words, every ideal of $R[x]$ is finitely-generated.

If $f = a_n x^n + \cdots + a_0$ is a polynomial in R (so the a_i's are in R), we say the *initial term* of f is $a_n x^n$, and the *initial co-efficient* of f is a_n.

Proof. Let I be an ideal of $R[x]$; we'll show that it is finitely generated. Choose a sequence $f_1, f_2, \cdots \subset I$ as follows: let f_1 be a non-zero element of least degree in I. For $i \geq 1$, if $(f_1, \ldots, f_i) \neq I$, then choose f_{i+1} to be an element of least degree among those in I but not in $(f_1, \ldots, f_i)$. (If $(f_1, \ldots, f_i) = I$, then we've shown I is finitely generated, so stop choosing elements.)

Let a_j be the initial coefficient of f_j. Since R is Noetherian, the ideal $J = (a_1, a_2, \ldots)$ of the a_i produced is finitely generated. Let m be an integer such that $a_1, \ldots, a_m$ generate J. We claim that $I = (f_1, \ldots, f_m)$.

Otherwise, consider f_{m+1}. $a_{m+1} \in J$, so we can write $a_{m+1} = \sum_{j=1}^m u_j a_j$ for some $u_j \in R$. Define

$$g = \sum_{j=1}^m u_j f_j x^{\deg f_{m+1} - \deg f_j} \in (f_1, \ldots, f_m)$$

and notice that this is of the same degree as f_{m+1}, with the same initial term. The difference $f_{m+1} - g$ is in I but not in $(f_1, \ldots, f_m)$, and has degree strictly less than that of f_{m+1}. But f_{m+1} was something of minimal degree with this property, so we have a contradiction. □

Fact. We won't need this any time soon, but it is worth mentioning. If R is a ring, and M is a module, then M is said to be Noetherian if every ascending chain of submodules of M eventually stabilizes. Then it isn't hard to prove that if R is a Noetherian ring, and M is a finitely-generated R module, then M is a Noetherian module.

(2) The game of Chomp.

Show that infinite chomp is a finite game, and how this follows from the fact that $\overline{k}[x_1, \ldots, x_n]$ is Noetherian.

(3) A geometric picture.

We now know that every ascending chain of ideals of $\overline{k}[x_1, \ldots, x_n]$ must eventually stabilize, so every ascending chain of *radical* ideals of $\overline{k}[x_1, \ldots, x_n]$ must eventually stabilize, so by our identification of radical ideals with algebraic sets, every *descending chain* of algebraic sets in $\mathbb{A}^n$ must eventually stabilize. Let me do an example to convince you that this is reasonable, and then you can tell me why you find it reasonable; these ideas will turn up in the proof of the Hilbert basis theorem.

(Do that, and see what ideas come up.)

This leads us to our next topic.

3. Fundamental definitions: Zariski topology, irreducible, affine variety, dimension, component, etc.

We've now defined our objects of study. We now make some more fundamental definitions; see e.g. Hartshorne I.1.

Definition / way of thinking. The *regular functions* on an algebraic set $X = V(I) \subset \overline{k}[x_1, \ldots, x_n]$ (where I is *radical*) is the ring $\overline{k}[x_1, \ldots, x_n]/I$. Call this the *ring of regular functions*, or the *affine coordinate ring* of X, denoted $A(X)$. (We'll later see how to reconstruct the algebraic set from the ring of regular functions; if you've seen much of this before, then you can think about this.)

Elements of this ring are called *regular functions*.

Example: consider the algebraic set in $\mathbb{A}^2$ defined by the equation $y^2 = x^3 + x$ (which I should draw as a real cubic, with two components). Then the polynomial x is a function on that curve. But the polynomial $y^2 - x^3$ is too, and it's the same function.

Definition. Define the *Zariski topology* on an algebraic set X as follows. Closed sets are defined to be algebraic subsets of X.

This is an extremely unusual topology. But it *is* a topology. I'll check the axioms (which, although usually stated for open sets, I'll state for closed sets). The empty sets is closed. All of X is closed. The finite union of closed sets is closed:

$$V(I_1) \cup \cdots \cup V(I_n) = V(I_1 \cap \cdots \cap I_n).$$

Any intersection of closed sets is closed:

$$\cap_{a \in A} V(I_a) = V((\sum I_a)).$$

As an example, consider the affine line $\mathbb{A}^1$, corresponding to the polynomials in one variable $\overline{k}[x]$. The closed subsets are zero-sets of a single polynomial, so a closed subset is either $\mathbb{A}^1(\overline{k})$, or a finite union of points. The open sets are all huge. In particular, this is not a Hausdorff topology. So be careful; your intuition can lead you astray. The proper way to think of open subsets is to imagine throwing away a union of algebraic sets. For example, if X is a plane union a line...

Definition. A non-empty topological space Y is *irreducible* if it cannot be expressed as the union of $Y_1 \cup Y_2$ of two proper subsets, each closed.

E.g. $\mathbb{A}^1$, point, not plane union line.

Exercise (on next Tues. problem set). Any non-empty open subset of an irreducible space is irreducible and dense.

Warning: At this point in the class, I gave a definition of algebraic variety. That definition was only tentative; the real definition will come up in a class or 2.

Important exercise. Irreducible algebraic subsets of $\mathbb{A}^n(\overline{k})$ correspond (under the bijection radical ideals $\Leftrightarrow$ algebraic sets) to prime ideals.

(You can just look this up in any introductory book on algebraic geometry, but you'll really want to think this through.)

Example: line union a plane. Recall that this has ideal $I = (xz, yz)$. Then R/I isn't prime, which you can see in two ways. Here's the geometric way, it "clearly" isn't irreducible. (We'll find a function f_1 that vanishes on one component but not the other. And we'll find f_2, and we'll see that $f_1 f_2 = 0$ in the ring of regular function.)

Definition. A topological space is *noetherian* if it satisfies the *descending chain condition* for closed subsets: for any sequence $Y_1 \supset Y_2 \supset \dots$ of closed subsets, there is an integer r such that $Y_r = Y_{r+1} = \dots$. Example: as $\overline{k}[x_1, \dots, x_n]$ is noetherian, $\mathbb{A}^n$ is a Noetherian space.

Important exercise. If Y is a Noetherian topological space, it can be expressed as a finite union $Y = Y_1 \cup \dots \cup Y_r$ of irreducible closed subsets Y_i. If we require that Y_i is not contained in any Y_j for any $i \neq j$, then the Y_i are uniquely determined. (Proof: "Noetherian induction.")

These are the *irreducible components* of Y.

So every algebraic set in $\mathbb{A}^n$ can be uniquely expressed as a finite union of irreducible algebraic sets (without redundancies).

Definition. The *dimension* of a topological space is the supremum of all integers n such that there is a chain $\emptyset = Z_0 \subset Z_1 \subset \cdots \subset Z_n$ of distinct irreducible closed subsets of X.

E.g. $\dim \mathbb{A}^1(\overline{k}) = 1$, but it already isn't obvious why $\dim \mathbb{A}^2(\overline{k}) = 2$.

Definition. If $\mathfrak{p}$ is a prime ideal of a ring R, then its *height* is the supremum of all integers n such that there exists a chain $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n = \mathfrak{p}$ of distinct prime ideals. The *Krull dimension* of R is the supremum of the heights of all prime ideals.

Check: If Y is an algebraic set in $\mathbb{A}^n$, then $\dim Y$ is the Krull dimension of its affine coordinate ring $A(Y)$.

Commutative Algebra Fact. If k is a field, and B is an integral domain which is a finitely-generated k-algebra. Then $\dim B = tr.deg_k K(B)$ (where $K(B)$ is the quotient field of B), and for any prime ideal $\mathfrak{p}$ in B,

$$ht\mathfrak{p} + \dim B/\mathfrak{p} = \dim B.$$

Hence (i) $\dim \mathbb{A}^n$ n, as the transcendence degree of $\overline{k}(x_1, \ldots, x_n)$ over $\overline{k}$ is n, and (ii) you should think of the height as codimension.

Example. The *twisted cubic* in $\mathbb{A}^3$. On the problem set, you show that the subset Y of points of the form (t, t^2, t^3) of $\mathbb{A}^3$ is algebraic. It turns out to be irreducible, not surprisingly. So this corresponds to a prime ideal $\mathfrak{p}$. What is its height in $\overline{k}[x_1, x_2, x_3]$?

Exercise. (a) Show that $A(Y)$ is isomorphic to $\overline{k}[x]$, i.e. the ring of polynomials in one variable. Think about what this might mean.

(b) Let Z be the plane curve $xy = 1$. Show that $A(Z)$ is *not* isomorphic to $\overline{k}[t]$.

Exercise. Let Y be the algebraic set in $\mathbb{A}^3$ defined by the two polynomials $x^2 - yz$ and $xz - x$. Show that Y is the union of three irreducible components. Describe them, and find their prime ideals. (Not on problem set.)

Exercise. Show that a $\overline{k}$-algebra B is isomorphic to the affine coordinate ring of some algebraic set in $\mathbb{A}^n(\overline{k})$ for some n if and only if B is a finitely generated k-algebra with no nilpotent elements. (We'll basically prove this next week; not on problem set.)

Next to do: we've described the objects we're interested in, algebraic sets. We'll define morphism. This is even more important than it sounds. For example, we want to say that the line in $\mathbb{A}^2$ and $\mathbb{A}^1$ are really the same thing, and we can't say that unless we know what "same" means.

Then we'll recover affine algebraic sets from their coordinate rings, and we'll define general varieties by gluing together irreducible affine algebraic sets.