INTRODUCTION TO ALGEBRAIC GEOMETRY, CLASS 2

RAVI VAKIL

Contents

1. A bit more commutative algebra

There was a little more commutative algebra I should have mentioned last time. We won't use it much soon, but I wanted to get it out of the way.

First of all, some of you suggested that I remind you of some facts, so you don't have to recall them quickly in the midst of the lecture.

If R is a ring, then a non-empty subset I is an ideal if it is closed under addition, and if you multiply an element of I by any element of R, you get another element of I. An ideal is prime if $xy \in I$ implies $x \in I$ or $y \in I$. Equivalently, I is prime if R/I is an integral domain, which means that $xy = 0$ (in R/I) means $x = 0$ or $y = 0$ (in R/I). A maximal ideal is a proper ideal maximal with respect to inclusion. Then I is maximal if and only if R/I is a field, so maximal ideals are prime.

Localization. A subset S is multipliciative if $xy \in S$ for all $x, y \in S$. Examples are: (a) $R - \mathfrak{p}$ where $\mathfrak{p}$ is a prime ideal; (b) $\{f, f^2, f^3, \dots,\}$ where $f \in R$. Then you can define a new ring $S^{-1}R$ as follows: elements are of the form (a, b), which you should think of as being a/b, where $b \in S$, and $a \in R$; two elements (a, b) and (c, d) are the same if $s(ad - bc) = 0$ for some element $s \in S$. In the two examples, we write this ring as $R_{\mathfrak{p}}$ and $R_{(f)}$.

(Experts should think about how prime ideals and localization interact.)

Examples of (a) are: $R = \mathbb{Z}$, $\mathfrak{p} = (3)$, so elements of $R_{\mathfrak{p}}$ are fractions with no power of 3 in the denominator. $R = \overline{k}[x]$, $\mathfrak{p} = (x - 1)$, so elements of $R_{\mathfrak{p}}$ are quotients of polynomials with no power of $(x - 1)$ in the denominator. If R is an integral domain, then (0) is a prime ideal, and the localization with respect to this ideal gives you all fractions, e.g. $R = \mathbb{Z}$ you get the rational numbers $\mathbb{Q}$.

Date: September 14, 1999.

Examples of (b) are: $R = \mathbb{Z}$, $f = 3$, so elements of $R_{(f)}$ are fractions with only a power of 3 in the denominator. $R = \overline{k}[x]$, $\mathfrak{p} = (x-1)$, so elements of $R_{(f)}$ are quotients of polynomials with only powers of $(x-1)$ in the denominator.

Warning: Be a little cautious: weird stuff can happen here. For example, if S contains 0, then the localization of S is the zero ring. (That will be an *exericse*.) So in particular, if f is nilpotent (i.e. $f^n = 0$ for some n), then $R_{(f)}$ is the zero-ring.

2. The correspondence between algebraic sets and radical ideals

Let's recap where we are.

An algebraic set in $\mathbb{A}^n(\overline{k})$ is something cut out by polynomials. (We'll see later that we can add "a finite number of" to that sentence.)

From an algebraic set X (or indeed any subset of $\mathbb{A}^n(\overline{k})$) we can cook up an ideal $I(X)$, the ideal of functions vanishing on X. It is a radical ideal.

From any radical ideal I (or indeed any subset of $\overline{k}[x_1, \dots, x_n]$) we can cook up an algebraic set $V(I)$, the "vanishing set" of the ideal.

The Nullstellensatz implies that this gives an equivalence:

$$\text{algebraic sets} \leftrightarrow \text{radical ideals in } \overline{k}[x_1, \dots, x_n].$$

Let's begin to understand this dictionary, by looking in the plane $\mathbb{A}^2$.

0) Ideal corresponding to a point (a, b): $(x-a, y-b)$. (Maximal.)

If you have an algebraic set, say in $\mathbb{A}^3$, the xy-plane union the z-axis, then this gives you a radical ideal I. We'll work out soon what that radical ideal is. On the geometric side, you have a bunch of points, so on the algebraic side, you have a bunch of maximal ideals. On the algebraic side, how do you see incidence, i.e. how can you tell which points are on the algebraic set? Answer: those maximal ideals containing I.

a) *Caution: this is actually trickier than it looks. It's low-tech, but subtle. It's also very important to understand the guts of the radical ideal / algebraic set "duality", so be sure to think this through.*

Let's understand how to interpret unions of algebraic sets in terms of algebra. The union of two algebraic sets corresponding to radical ideals I_1, I_2 is the radical of the ideal I_1 intersect I_2. Example: the two points (1,0) and (-1,0), give the ideal: elements that are of the form $(y, x+1)$ and $(y, x-1)$.

Do it painfully: If something lies in both ideals, then it has a part that is a multiple of y, plus a polynomial in x, which is divisible by both $(x+1)$ and $(x-1)$.

Notice another way of doing it: $(y^2, (x+1)y, (x-1)y, (x^2-1))$; in general that $\sqrt{I_1 \cap I_2} = \sqrt{I_1 I_2}$.

Exercise. Show that $\sqrt{I_1 \cap I_2} = \sqrt{I_1 I_2}$.

Exercise. If I_1 and I_2 are radical, show that their intersection is also radical.

Example. Find the ideal corresponding to the union of the point (1,1) and the line $y = 2$. Ans: $((y-2)(x-1), (y-2)(y-1))$.

Example. Find the ideal corresponding to the union of the two points (1,0) and (-1,0).

Example. Find the ideal in $\overline{k}[x_1, x_2, x_3]$ corresponding to the union of the z-axis and the xy-plane. (Have them do this.)

Exercise. (In dimension 3.) Find the ideal corresponding to the x_1-axis union the point (1,1,1).

Corollary. A finite union of points is an algebraic set.

b) *This should remind you of high-school algebra, i.e. solving a bunch of equations in a bunch of unknowns, albeit in a more high-powered setting.*

The intersection of two algebraic sets corresponding to radical ideals I_1, I_2 is the radical of the ideal $I_1 + I_2$.

Example. $y = 0$, $y = x^2 - 1$. Ideal is $(y, y - x^2 + 1) = (y, x^2 - 1)$. You can see the two points: $(y, x+1)$ and $(y, x-1)$.

Example. To see that you need take to radical, consider $y = 0$, $y = x^2$. Aside: You want to say that the line intersects the parabola at one point with multiplicity 2. You already see the one point. Can you interpret the 2? This was a scheme-theoretic intersection.

Exercise. Find the intersection of the x-axis and the cubic $y^2 = x^3 + x^2$, using ideals: find the ideal corresponding to those two curves, and compute the intersection. (This isn't actually on the problem set, but resembles some that are.

Summary. We've defined unions and intersections algebraically.

Something else to think about: Maximal ideals correspond to points. What do prime ideals correspond to (that aren't maximal)? Here's where to start: think in the plane $\mathbb{A}^2$. Name some prime ideals, other than those corresponding to points, and the zero-ideal (which might confuse you).

Aside. Affine schemes!

radical ideals $\Leftrightarrow$ algebraic sets (algebraic varieties) (in $\mathbb{A}^n$)

ideals $\Leftrightarrow$ affine schemes! (closed subschemes of $\mathbb{A}^n$)

For example, (x^2, y). (x^2, xy, y^2). We can now define scheme-theoretic unions and intersections, by thinking about ideals. More on this later.

3. More Nullstellensatz

Here's a reminder of the various versions of the Nullstellensatz.

Nullstellensatz Version 1. Suppose $F_1, \ldots, F_m \in \overline{k}[x_1, \ldots, x_n]$. If the ideal $(F_1, \ldots, F_m) \neq (1) = \overline{k}[x_1, \ldots, x_n]$ then the system of equations $F_1 = \cdots = F_m = 0$ has a solution in $\overline{k}$.

We'll prove this soon.

Nullstellensatz Version 2. The maximal ideals of $\overline{k}[x_1, \ldots, x_n]$ are precisely those maximal ideals which come from points, i.e. those ideals of the form $(x_1 - a_1, \ldots, x_n - a_n)$ for some $a_1, \ldots, a_n \in \overline{k}$.

Nullstellensatz Version 3 (the "Weak Nullstellensatz"). If I is a proper ideal in $\overline{k}[x_1, ..., x_n]$, then $V(I)$ is nonempty.

(In retrospect, this seems to be the same as version 1!)

Nullstellensatz Version 4. $I(V(I)) = \sqrt{I}$, which implies that: Radical ideals are in 1-1 correspondence with algebraic sets.

Nullstellensatz Version 5. A radical ideal of $\overline{k}[x_1, \ldots, x_n]$ is the intersection of the maximal ideals containing it.

Nullstellensatz Version 6. If F_1, ..., F_r, G are in $\overline{k}[x_1, ..., x_n]$, and G vanishes wherever F_1, ..., F_r vanish, then some power of G lies in the ideal $(F_1, \ldots, F_r)$, i.e. $G^N = A_1F_1 + ... + A_rF_r$ for some $N > 0$ and some A_i in $\overline{k}[x_1, ..., x_n]$. Put differently: if I is a finitely generated ideal of $\overline{k}[x_1, \ldots, x_n]$, and G is 0 on the vanishing set of I ($G \in V(I)$), then $G \in \sqrt{I}$. (We'll later see that all ideals are finitely generated when we talk about Noetherian rings.)

Proof of Nullstellensatz, version 1.

We need a lemma:

Lemma. If a system $F_1 = \cdots = F_m = 0$ with $F_i \in \overline{k}[x_1, \ldots, x_n]$ has a solution in some finitely generated extension field K of $\overline{k}$, then it has a solution in $\overline{k}$.

Proof of Lemma. By structure of finitely-generated extension fields (Shafarevich p. 280), $K = \overline{k}(t_1, \ldots, t_r, \theta) = \overline{k}(\underline{t}, \theta)$ where $t_1, \ldots, t_r$ are algebraically independent over $\overline{k}$ and θ is a root of a polynomial

$$P(\underline{t}, U) = p_0(\underline{t})U^d + \cdots + p_d(\underline{t}) \in \overline{k}(\underline{t})[U],$$

where $P(\underline{t}, U)$ is irreducible over $\overline{k}(\underline{t})$.

Suppose $(\eta_1, \ldots, \eta_n)$ is a solution where $\eta_i \in K$, so $\eta_i = C_i(\underline{t}, \theta)$. Then

$$F_j(C_1(\underline{t}, U), \ldots, C_n(\underline{t}, U)) = P(\underline{t}, U)Q_j(\underline{t}, U)$$

for some polynomial Q_j. Subtitute values $x_i = \alpha_i \in \overline{k}$ for all i, such that $(\alpha_1, \ldots, \alpha_n)$ is not a zero of the denominators of any coefficient of any of the polynomials that have turned up so far, i.e. P, Q_i, $C_i \in \overline{k}(\underline{t})[U]$, nor a zero of the leading coefficient of P. Choose $U = \tau$ to be one of the roots of $P(\alpha_1, \ldots, \alpha_n, \tau) = 0$, and set $C_j(\alpha_1, \ldots, \alpha_n, \tau) = \lambda_j$ for all j. Then $F_j(\lambda_1, \ldots, \lambda_n) = 0$ for all j, so we've found a solution of the system in $\overline{k}$. $\square$

Proof of Nullstellensatz Version 1. If the ideal $(F_1, \ldots, F_m)$ is not the entire ring $\overline{k}[x_1, \ldots, x_n]$ then it is contained in some maximal ideal $\mathfrak{m}$, and $K = \overline{k}[x_1, \ldots, x_n]/\mathfrak{m}$ is a field — and what a nice field it is: writing η_i for the image of x_i in K, then $K = \overline{k}(\eta_1, \ldots, \eta_n)$, and $(\eta_1, \ldots, \eta_n)$ is a solution of the system $F_1 = \cdots = F_m = 0$. By the lemma we get a solution. This proves the Nullstellensatz. $\square$

It's important to see a proof of the Nullstellensatz in order to get a feel for the flavour of the proof, but it isn't necessary to really know it at well at this point, as it differs in flavour from the rest of the course.