Algebraic Geometry 1/21/05 (Notes taken by Brian Katz)

Throughout these notes we will let $R = k[x_1, \dots, x_n]$ whenever there is no possibility of confusion about n. Last time we defined the Zariski topology on $\mathbb{A}^n$. Also, for every ideal $\mathfrak{a} \subset R$, we defined the algebraic set, $Z(\mathfrak{a}) = \{p \in \mathbb{A}^n : f(p) = 0 \ \forall f \in \mathfrak{a}\}$. We will spend today's class trying to describe an inverse to the function Z.

Definition 1. *Let $X \subseteq \mathbb{A}^n$, then define $I(X) = \{f \in R : f\mid_X = 0\}$. Note that this function does take algebraic sets to ideals.*

Theorem 0.1. *1) If $X \subseteq Y \subseteq \mathbb{A}^n$, then $I(Y) \subseteq I(X)$.*

2) $I(X) \cap I(Y) = I(X \cup Y)$

3) If $X \subseteq \mathbb{A}^n$ is algebraic, then $X = Z(I(X))$.

Proof. The first two claims are tautological. Note that the converse of the third claim is also trivial. Now suppose that X is an algebraic set, so $X = Z(\mathfrak{a})$ for some ideal $\mathfrak{a} \in R$. Then by definition $Z(I(X)) = \{p \in \mathbb{A}^n : f(p) = 0 \text{ for all } f \text{such that} f\mid_X = 0\}$. Clearly every point in X satisfies this condition, so $X \subseteq Z(I(X))$. To prove the reverse inclusion, we write $Z(I(X)) = Z(I(Z(\mathfrak{a})))$. Furthermore $I(Z(\mathfrak{a})) = \{f : f\mid_{Z(\mathfrak{a})} = 0\}$ and clearly, $\mathfrak{a} \subseteq I(Z(\mathfrak{a}))$, so applying the inclusion-reversing map, Z, to both sides, we see that $Z(I(X)) = Z(I(Z(\mathfrak{a}))) \subseteq Z(\mathfrak{a}) = X$. Combining these inclusions, we have proven the final claim. ☐

Now we have defined two maps, I and Z, as follows:

$$\{algebraic\ sets\ in\ \mathbb{A}^n\} \underset{Z}{\overset{I}{\rightleftharpoons}} \{ideals\ of\ R\}.$$

The previous theorem proves that these two maps, when composed in one direction are inverses. The next logical question is whether they are actually inverses. The answer is no. For example, in $\mathbb{R}[x]$, $Z(x^2)$ is just the point 0, and $I(0) = (x)$. However, you may note that (x) is the radical of (x^2), which we will denote $(x) = \sqrt{(x^2)}$.

Let $\mathfrak{a}$ be an ideal of R. Since R is Noetherian, $\mathfrak{a}$ is finitely generated, so say $\mathfrak{a} = (f_1, \dots, f_s)$. Then

$$I(Z(\mathfrak{a})) = \{f \in R : f\mid_{Z(\mathfrak{a})} = 0\} = \{f \in R : if\ f_1(p) = \cdots = f_s(p) = 0\ then\ f(p) = 0\}.$$

In particular, $a \subseteq I(Z(\mathfrak{a}))$, as we would like.

Theorem 0.2 (Hilbert Nullstellensatz). $I(Z(\mathfrak{a})) = \sqrt{(\mathfrak{a})}$

This is the same as saying: if $f \in k[x_1, \dots, x_n]$ is such that $f_1(p) = \cdots = f_s(p) = 0$ implies $f(p) = 0$, then there exist polynomials $h_i \in R$ and a positive integer l such that $f^l = \sum_{i=1}^{s} h_i f_i$.

Theorem 0.3 (Weak Nullstellensatz). *If $k = \overline{k}$, then the maximal ideals of $k[x_1, \dots, x_n]$ are of the form $M = (x_1 - a_1, \dots, x_n - a_n)$ for $a_i \in k$.*

Remark 0.4. *1) An ideal $P \subset R$ is prime if $ab \in P$ and $a \notin P$ implies $b \in P$. Equivalently, P is prime if R/P is an integral domain.*

2) Similarly, an ideal, M, is maximal if there are no proper ideals containing it or if R/M is a field.

3) One might ask if all of the ideals of the form in the theorem are maximal. We can see that

$$k[x_1, \dots, x_n]/(x_1 - a_1, \dots, x_n - a_n) \cong k$$

via the isomorphism of evaluation at the point $(a_1, \dots, a_n)$, and the ideals are maximal by the previous item.

4) The theorem is false if k is not algebraically closed. For example, by definition $\mathbb{C} = \mathbb{R}[x]/(x^2 + 1)$, but $x^2 + 1$ is not of the form described in the theorem.

proof (of Full Null., assuming Weak Null.) Let $\mathfrak{a} = (f_1, \cdots, f_s) \subset k[x_1, \dots, x_n]$, and let f be such that $f_1(p) = \cdots = f_s(p) = 0$ implies that $f(p) = 0$. Consider the following ideal, $J \subset k[x_1, \dots, x_{n+1}]$:

$$J := \mathfrak{a}k[x_1, \dots, x_{n+1}] + (1 - f x_{n+1}).$$

Suppose that J is a proper ideal. Then it is contained in a maximal ideal, which by our assumption is of the form $J \subset M = (x_1 - a_1, \dots, x_{n+1} - a_{n+1})$ for some $a_1, \dots, a_{n+1} \in k$.

Then $f_1(a_1, \dots, a_n) = \cdots = f_s(a_1, \dots, a_n) = 0$, so $f(a_1, \dots, a_n) = 0$. But any polynomial in M is zero at the point $(a_1, \dots, a_{n+1})$, so $0 = 0 + (1 - f(a_1, \dots, a_n)a_{n+1}) = 1 - 0 = 1$, a contradiction. Hence J is not proper. Thus $J = k[x_1, \dots, x_{n+1}]$, so $1 \in J$. Hence

$$1 = \sum_{i=1}^{s} h_i(x_1, \dots, x_{n+1}) f_i(x_1, \dots, x_n) + h_{s+1}(x_1, \dots, x_{n+1})(1 - f(x_1, \dots, x_n)x_{n+1}).$$

Set $x_{n+1} = \frac{1}{f}$ to get the equality

$$1 = \sum_{i=1}^{s} h_i(x_1, \dots, x_n, 1/f) f_i(x_1, \dots, x_n),$$

which in turn implies (by clearing the denominators), that

$$f^l = \sum_{i=1}^{s} \tilde{h}_i(x_1, \dots, x_n) f_i(x_1, \dots, x_n).$$

□

Theorem 0.5. *There is a bijection between algebraic sets in $\mathbb{A}^n$ and radical ideals in R.*

To an algebraic set, X we associate its ideal $I(X)$, and to a radical ideal $\mathfrak{a}$ we associate its zero locus $Z(\mathfrak{a})$. As we have proven above, $Z(I(X)) = X$, and $I(Z(\mathfrak{a})) = \sqrt{\mathfrak{a}} = \mathfrak{a}$.

Example 1. *Let X be the union of a line and a plane in $\mathbb{A}^3$, for example $L : x = y = 0$ and $H : z = 0$. Then $I(X) = I(L \cup H) = I(L) \cap I(H) = (x, y) \cap (z) = (xz, yz)$. This last equality is actually an unpleasant calculation that we will include this once.*

Suppose $ax + by = cz$; we wish to show that z divides both a and b, or at least that it can be manipulated to be in that form. Write $a = zf + a_1(x, y)$ and $b = zg + b_1(x, y)$. Then $z(fx + gy) + (a_1x + b_1y) = cz$. Because the second term contains no z but is divisible by z, it must be zero. Hence we can rewrite our original element as $fxz + gyz$.