ALGEBRAIC GEOMETRY: WEDNESDAY, FEBRUARY 8

1. Hilbert's Nullstellensatz

This is an essential result in commutative algebra that we need to understand the Zariski topology and algebraic varieties in more detail. Maybe you've already seen/proved it.

Theorem 1.1 (Weak Nullstellensatz)**.** *If $k = \overline{k}$, then every maximal ideal m in the ring $R = k[x_1, \ldots, x_n]$ is of the form $m = (x_1 - a_1, \ldots, x_n - a_n)$.*

Proof. Because m is maximal, R/m is a field which is finitely generated as an algebra over k. Because $k = \overline{k}$, this implies $R/m = k$ (using 'Zariski's Lemma': K finitely generated algebra over k is a finite extension of k).

Let a_i be the image of x_i under the map $R \to R/m = k$. Then, $m' = (x_1 - a_1, \ldots, x_n - a_n)$ is contained in m, but m' is maximal, so in fact $m' = m$. □

Corollary 1.2. If f_i is a family of polynomials in R with no common zeros, then the ideal generated by the f_i's is (1).

Proof. Suppose not. Then, the ideal generated by the f_i's lies in some maximal ideal m which must be $m = (x_1 - a_1, \ldots, x_n - a_n)$, so $f_i(a_1, \ldots, a_n) = 0$ for all i, contradicting that they have no common zeros. □

Theorem 1.3 (Strong Nullstellensatz)**.** *If $k = \overline{k}$ and $g, f_1, \ldots, f_m$ are polynomials in R such that g vanishes on the common zeros of f_i, then there exists $n > 0$ such that $g^n \in (f_1, \ldots, f_m)$.*

Proof. Consider the ideal generated by the polynomials $(f_1, \ldots, f_m, x_{n+1}g - 1) \in k[x_1, \ldots, x_n, x_{n+1}]$. These have no common zeros, so by the previous corollary, $(f_1, \ldots, f_m, x_{n+1}g - 1) = (1)$, i.e. there are polynomials p_i such that

$$1 = p_1 f_1 + \cdots + p_m f_m + p_{m+1}(x_{n+1}g - 1)$$

Now plug in $x_{n+1} = 1/g$, which gives:

$$1 = p_1(x_1, \ldots, x_n, 1/g) f_1 + \cdots + p_m(x_1, \ldots, x_n, 1/g) f_m$$

and multiplying both sides by a power of g to clear denominators, we see that $g^n \in (f_1, \ldots, f_m)$. □

2. Correspondence between Z and I

Let $k = \overline{k}$ and $A = k[x_1, \ldots, x_n]$.

Recall the definition of Z ('zeros') from Monday:

Definition 2.1. If $T \subset A$, then $Z(T) = \{p \in \mathbb{A}^n \mid f(p) = 0 \forall f \in T\}$.

A new definition:

Definition 2.2. If $Y \subset \mathbb{A}^n$, define the **ideal** of Y to be $I(Y) = \{f \in A \mid f(p) = 0 \forall p \in Y\}$.

The goal of this section is to prove the following:

Theorem 2.3. *There is an inclusion-reversing bijection between algebraic sets in $\mathbb{A}^n$ and radical ideals in A, given by $Y \mapsto I(Y)$ and $I \mapsto Z(I)$.*

This will be a consequence of the following proposition.

Proposition 2.4. *(1) If $T_1 \subset T_2 \subset A$, then $Z(T_2) \subset Z(T_1)$.*

(2) If $Y_1 \subset Y_2 \subset \mathbb{A}^n$, then $I(Y_2) \subset I(Y_1)$.

(3) If $Y_1, Y_2 \subset \mathbb{A}^n$, then $I(Y_1 \cup Y_2) = I(Y_1) \cap I(Y_2)$.

(4) For any ideal $I \subset A$, $I(Z(I)) = \sqrt{I}$ (the radical of I).

(5) For any $Y \subset \mathbb{A}^n$, $Z(I(Y)) = \overline{Y}$.

Proof. (1) - (3) are clear (if not, try as homework, and come ask me!).

It remains to prove (4) and (5). For (4), write $I = (f_1, \ldots, f_m)$ for some generators f_i, so $Z(I)$ is the common zero locus of the f_i's. If $g \in I(Z(I))$, then g vanishes on the common zero locus of the f_i's, so by the Nullstellensatz, $g^n \in I$ so $g \in \sqrt{I}$. Also, if $g \in \sqrt{I}$, then $g^n \in I$ for some n, so g^n vanishes on the common zero locus of the f_i's and therefore so does g. In particular, $g \in I(Z(I))$. Therefore, $I(Z(I)) = \sqrt{(I)}$.

For (5), Consider $Z(I(Y))$. Because $Y \subset Z(I(Y))$ and $Z(I(Y))$ is closed, $\overline{Y} \subset Z(I(Y))$. Because $\overline{Y}$ is closed, $\overline{Y} = Z(J)$ for some $J \subset A$. Now, $Y \subset \overline{Y}$ implies $I(\overline{Y}) \subset I(Y)$, but $J \subset I(\overline{Y})$, so $J \subset I(Y)$. Therefore, $Z(I(Y)) \subset Z(J) = \overline{Y}$, and hence $Z(I(Y)) = \overline{Y}$. □

Remark 2.5. (4) is false over non-algebraically closed fields! Can you come up with an example?

So, algebraic sets correspond to (radical) ideals in a very nice way. We can therefore use properties of commutative algebra to study them! For example:

Proposition 2.6. *An algebraic set Y is irreducible if and only if $I(Y)$ is a prime ideal.*

Proof. If Y is irreducible, consider $fg \in I(Y)$. To show $I(Y)$ is prime, we must show that either f or g is in $I(Y)$. Because $fg \in I(Y)$, $Y = Z(I(Y)) \subset Z(fg) = Z(f) \cup Z(g)$, so $Y = (Y \cap Z(f)) \cup (Y \cap Z(g))$. Because Y is irreducible, without loss of generality we have $Y \subset Z(f)$, so $f \in I(Y)$.

Now assume that $I(Y)$ is a prime ideal, and suppose that $Y = Z(I(Y)) = Y_1 \cup Y_2$. This implies $I(Y_1) \cap I(Y_2) = I$, and I is prime, so without loss of generality we have $I = I(Y_1)$, so $Y = Y_1$ is irreducible. □

Example 2.7. $\mathbb{A}^n$ is irreducible because $I(\mathbb{A}^n) = (0)$ and (0) is prime.