MAS439/MAS6320
CHAPTER 7: PROVING THE NULLSTELLENSATZ

EVGENY SHINDER (PARTLY BASED ON NOTES BY JAMES CRANCH)

In this chapter k is an algebraically closed field, e.g. $k = \mathbb{C}$.

7.1. **Recollection: Nullstellensatz and its Corollaries.** Recall that if $J \subset R$ is an ideal then its radical is $\sqrt{J} = \{r \in R : r^n \in J, \text{ for some } n \geq 1\}$.

The following Theorem was stated (but not proved) in Tom's notes for Semester 1 as Theorem 14.5.

Theorem 7.1 (Hilbert's Nullstellensatz)**.** *Let k be an algebraically closed field, and let J be an ideal in the polynomial algebra $k[x_1, \ldots, x_n]$. Then the ideal of elements of $k[x_1, \ldots, x_n]$ which vanish on the zeroes of J is equal to the radical of J:*

$$I(V(J)) = \sqrt{J}.$$

Corollary 7.2. *The assignments $J \mapsto V(J)$ and $V \mapsto I(V)$ define mutually inverse inclusion-reversing bijections:*

$$V : \{\textit{Radical ideals } J \subset k[x_1, \ldots, x_n]\} \leftrightarrow \{\textit{Algebraic subsets } V \subset \mathbb{A}^n\} : I$$

Proof. It follows easily from definitions that the assignments I, V are inclusion-reversing: $J \subset J' \implies V(J) \supset V(J')$ and $X \subset X' \implies I(X') \supset I(X)$.

If J is a radical ideal, then by the Hilbert Nullstellensatz $I(V(J)) = \sqrt{J} = J$. It remains to show that if X is an algebraic set, then $V(I(X)) = X$. This is surprisingly a very formal, hence simple, step: since X is an algebraic set we have an ideal J such that $X = V(J)$. Now

$$V(I(X)) = V(I(V(J)) = V(\sqrt{J}) = V(J) = X.$$

□

Corollary 7.3. *There is a bijection between the set of points of $\mathbb{A}^n$ and the set of maximal ideals of $k[x_1, \ldots, x_n]$:*

$$k^n \leftrightarrow \mathrm{Specm}(k[x_1, \ldots, x_n])$$
$$a \in k^n \mapsto m_a = (x_1 - a_1, \ldots, x_n - a_n)$$

Proof. Since the bijections I and V of Corollary 7.2 are order reversing, maximal elements among the radical ideals correspond to minimal elements among the algebraic subsets.

We need to be a bit careful here as strictly speaking the only maximal element in the set of radical ideals is the ideal (1) which corresponds to $\emptyset = V(1)$, the empty algebraic set, which is indeed a minimal algebraic subset of $\mathbb{A}^n$.

After dismissing these trivial cases we obtain a bijection between maximal ideals among $J \neq (1)$, that is maximal ideals of $k[x_1, \ldots, x_n]$ and minimal non-empty algebraic subsets of $\mathbb{A}^n$, that is points.

If $a \in \mathbb{A}^n$ is a point, then $I(a) = (x_1 - a_1, \ldots, x_n - a_n)$. Indeed the ideal in the LHS is contained in $I(a)$, and since it is maximal and $I(a) \neq (1)$, the two ideals must be equal. □

Date: March 24, 2017.

We have more general versions of the above corollaries with the k-algebra $R = k[x_1, \dots, x_n]$ replaced by $R = k[X] = k[x_1, \dots, x_n]/I(X)$, the coordinate ring of an algebraic set $X \subset \mathbb{A}^n$.

Corollary 7.4. *The assignments $J \mapsto V(J)$ and $V \mapsto I(V)$ define mutually inverse bijections:*

$$V : \{\textit{Radical ideals } J \subset k[X]\} \leftrightarrow \{\textit{Algebraic subsets } V \subset X\} : I$$

Proof. Consider the bijection of Corollary 7.2 applied to the set of radical ideals $J \subset k[x_1, \dots, x_n]$ such that $J \supset I(X)$. Since the $I - V$ bijections are order-reversing we have:

$$J \supset I(X) \iff V(J) \subset V(I(X)) = X,$$

which yields a bijection

$$V : \{\text{Radical ideals } I(X) \subset J \subset k[x_1, \dots, x_n]\} \leftrightarrow \{\text{Algebraic subsets } V \subset X\} : I$$

Now ideals $\overline{J} \subset k[X]$ are in bijection with ideals $I(X) \subset J \subset k[x_1, \dots, x_n]$, and radical ideals correspond to radical ideals (why?). This finishes the proof. □

Corollary 7.5. *There is a bijection between the set of points of X and the set of maximal ideals of $k[X]$:*

$$X \leftrightarrow \mathrm{Specm}(k[X])$$
$$a \in k^n \mapsto m_a = (x_1 - a_1, \dots, x_n - a_n)$$

Proof. This can be deduced either from Corollary 7.3 or from Corollary 7.4. □

7.2. **Proving the Nullstellensatz.** There are many proofs of the Nullstellensatz, and all of them are kind of complicated. Our method of proof will do it in several steps: hopefully these steps may be of independent interest. The proof will use most of the techniques studied so far: quotient rings, localization, integral extensions and Noether Normalization. Before proving the general form of Hilbert Nullstellensatz we establish the bijection between maximal ideals and points of Corollary 7.3.

We start by gaining a little more understanding of finiteness:

Proposition 7.6. *Let $R \subset S$ be an integral extension and assume that R and S are integral domains. Then R is a field if and only if S is a field.*

Note that this gives us (for example) that $\mathbb{Q}$ is not a finitely-generated $\mathbb{Z}$-module, and that $\mathbb{C}(x)$ (the fraction field of $\mathbb{C}[x]$) is not a finitely-generated $\mathbb{C}[x]$-module.

Proof. Will be done in the homework assignment. □

This enables us to prove the following:

Theorem 7.7 (Zariski's Lemma)**.** *Let $k \subset L$ are fields and L is a finitely generated k-algebra, then L is an integral extension of k. Furthermore if k is algebraically closed, then $L = k$.*

Recall that an "integral extension" is a stronger condition than "finitely generated". Zariski's Lemma tells us that for fields the two concepts coincide.

Proof. The Noether Normalization Theorem states that L is an integral extension of some polynomial k-algebra $k[x_1, \dots, x_n]$.

Our aim is to show that $n = 0$. So, in order to get a contradiction, suppose that $n \geq 1$. But then we have that L has is integral over the subring $k[x_1, \dots, x_n]$, and Proposition 7.6 then tells us that $k[x_1, \dots, x_n]$ is a field. That's absurd: for example, x_1 is not invertible.

Assume now that k is algebraically closed. Take any element $x \in L$, it must satisfy a monic equation $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ with coefficients in k. But this polynomial splits as a product of roots (since k is algebraically closed):

$$(x - r_1) \cdots (x - r_n) = 0.$$

However, L is a field, so $x - r_i = 0$ for some i, so $x = r_i$ for some i. Hence any element $x \in L$ is in fact an element of k so that $L = k$. □

We now know enough to classify maximal ideals over polynomial rings over an algebraically closed field.

Theorem 7.8. *Let k be an algebraically closed field. Then the maximal ideals in $k[x_1, \ldots, x_n]$ are exactly the ideals of the form*

$$m_a = (x_1 - a_1, \ldots, x_n - a_n)$$

for elements $a_1, \ldots, a_n \in k$.

Note this says that maximal ideals in $k[x_1, \ldots, x_n]$ correspond to points in k^n. This is same as Corollary 7.3, but note that we do not yet have the Hilbert Nullstellensatz, but are in the process of proving it!

Proof. We should show that an ideal of this form is indeed maximal.

So consider the ideal

$$(x_1 - a_1, \ldots, x_n - a_n).$$

By changing coordinates, writing y_i for $x_i - a_i$ we can consider the special case of $(y_1, \ldots, y_n)$ as an ideal in $k[y_1, \ldots, y_n]$. This ideal consists of all polynomials with zero constant term; the quotient is hence evidently k. Since this is a field, the ideal is maximal.

On the other hand, suppose we have a maximal ideal m of $k[x_1, \ldots, x_n]$. Consider the field $L = k[x_1, \ldots, x_n]/m$. This is generated over k by $\overline{x_1}, \ldots, \overline{x_n}$, and so Zariski Lemma (Theorem 7.7) says that L is isomorphic to k as k-algebra:

$$k \subset L \simeq k$$

Now, let a_i be the image of $\overline{x_i}$ under this isomorphism. Now the element $x_i - a_i$ of $k[x_1, \ldots, x_n]$ is sent to 0 in $k[x_1, \ldots, x_n]/m$, and so $x_i - a_i \in m$.

Hence $(x_1 - a_1, \ldots, x_n - a_n) \subset m$. But since the left-hand side is maximal, this must be m. □

Now (at last!) we can do the Nullstellensatz itself.

Proof of Hilbert Nullstellensatz (Theorem 7.1). The inclusion $I(V(J)) \supset J$ is easy: if $h \in J \subset k[x_1, \ldots, x_n]$, then h is tautologically zero on $V(J)$, so $h \in I(V(J))$. Now since $I(V(J))$ is a radical ideal we also have $I(V(J)) \supset \sqrt{J}$. We need to show the opposite inclusion.

Assume that $f \notin \sqrt{J}$. We'll prove that $f(a) \neq 0$ for some $a \in V(J)$.

Lemma 7.9. *Let $J \subset R$ be any ideal. Then the radical of J is the intersection of all prime ideals containing J: $\sqrt{J} = \bigcap_{P \supset J} P$.*

Proof of Lemma. Will be done in the homework assignment. □

We continue proving Hilbert Nullstellensatz. Since $\sqrt{J} = \bigcap_{P \supset J} P$, and $f \notin \sqrt{J}$, we have $f \notin P$ for some prime ideal $P \supset J$. We now find a maximal ideal $m \supset P \supset J$ such that $f \notin m$.

For that consider the quotient R/P, and its localization $U^{-1}(R/P)$ with $U = \{1, \overline{f}, \overline{f}^2, \ldots\}$. Since the result of localization is inverting f, we will write $R/P[\overline{f}^{-1}]$ for $U^{-1}(R/P)$.

We have a composition of homomorphisms

$$R \to R/P \to R/P[\overline{f}^{-1}].$$

of finitely generated k-algebras.

We get maps on the level of Specm (maximal spectrum):

$$\mathrm{Specm}(R/P[\overline{f}^{-1}]) \to \mathrm{Specm}(R/P) \to \mathrm{Specm}(R).$$

From the standard facts on how ideals behave with respect to taking quotients and localization we deduce that these maps are injective (compare to HW 5, Question 1):

$$\mathrm{Specm}(R/P[\overline{f}^{-1}]) \subset \mathrm{Specm}(R/P) \subset \mathrm{Specm}(R)$$

and in fact the image of $\mathrm{Specm}(R/P[\overline{f}^{-1}])$ in $\mathrm{Specm}(R)$ is

$$\{m \subset R : P \subset m, f \notin m\}.$$

We are done: since $\mathrm{Specm}(R/P[\overline{f}^{-1}]) \neq \emptyset$ (every ring has a maximal ideal) we get a maximal ideal $m \supset P \supset J$ in R such that $f \notin m$. By Theorem 7.8 we have $m = m_a$ for some $a \in k^n$, and we see that $a \in V(I)$, but $f(a) \neq 0$. $\square$