LECTURE 2 - THE NULLSTELLENSATZ

PATRICK DYLAN ZWICK

In our last lecture we learned, or reviewed, a number of facts about rings and introduced some basic concepts for dealing with rings. We introduced this idea of associating with any set of zeros in $\mathbb{A}^n$ the ideal of polynomials that vanish at these points. We also learned how, for any ideal $I \subseteq K[X_1, \ldots, X_n]$, we can associate with it a set of points in $\mathbb{A}^n$, namely the set of points upon which every element $F \in I$ vanishes.

Our first big theorem here is Hilbert's Nullstellensatz[1] which gives us our fundamental relation between the zeros of an ideal I, and the ideal I itself.

1. The *STRONG* Nullstellensatz

We'll first prove the *strong* Nullstellensatz, and just state the weak Nullstellensatz. Then, after the incredibly tricky and brilliant proof of the strong Nullstellensatz from the weak, we'll prove, in a less tricky way, the weak Nullstellensatz.

Theorem (The Weak Nullstellensatz) Let K be an algebraically closed field and let $I \subset K[X_1, \ldots, X_n]$ be an ideal satisfying $\mathbf{V}(I) = \emptyset$. Then $I = K[X_1, \ldots, X_n]$.

As I said, we'll delay the proof of this for a little while, but we should pause here to note that it's true if *and only if* K is algebraically closed. If K were not algebraically closed, then we'd have a non-constant polynomial $F \in K[X]$ such that F has no roots in K, and therefore for its corresponding polynomial in $K[X_1, \ldots, X_n]$ we'd have $\mathbf{V}(F) = \emptyset$, while $1 \notin (F)$. For example, in $\mathbb{R}[X]$ we have $V(X^2 + 1) = \emptyset$, while $1 \notin (X^2 + 1)$.

Exercises

1: (Harder) Prove that if K is a field which is not algebraically closed, then each algebraic set in K^n is the zero set of a single

[1] This is Hilbert's zeros theorem. In typical German fashion, it's formed from three simpler words: Null (=Zero), Stellen (=Places), Satz (=Theorem). So, it's Hilbert's "zero places theorem", but isn't Nullstellensatz so much more fun to say? Also, according to Miles Reid, you should stick to the German if you don't want to be considered an ignorant peasant.

polynomial $F \in K[X_1, \ldots, X_n]$. *Hint* - Think about how to do this in the case of $\mathbb{R}$, and then generalize the idea.

From now on we'll assume the field over which we're working, k, is algebraically closed unless we say otherwise. The strong Nullstellensatz is equivalent to the weak Nullstellensatz, although at first blush this is not obvious. We'll prove that the weak implies the strong, and leave it as an exercise to prove the strong implies the weak[2].

Theorem (The Strong Nullstellensatz)[3] Let K be an algebraically closed field. If I is an ideal in $K[X_1, \ldots, X_n]$, then[4]

$$\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$$

Proof - If $I =< F_1, \ldots, F_n >$[5] then given a nonzero polynomial $F \in K[X_1, \ldots, X_n]$ which vanishes at every common zero of the polynomials $F_1, \ldots, F_n$, we must show that there exists an integer $m \geq 1$ and polynomials $A_1, \ldots, A_n$ such that:

$$F^m = \sum_{i=1}^{n} A_i F_i.$$

The proof of this is one of my favorite proofs ever. We introduce a new variable, call it Y, and we consider the ideal:

$$\tilde{I} =< F_1, \ldots, F_n, 1 - YF >\subset K[X_1, \ldots, X_n]$$

where $F, F_1, \ldots, F_n$ are as above. Now, we note that if $F_1 = F_2 = \cdots = F_n = 0$ (thinking of them as functions of $n+1$ variables, where the variable Y does not show up) then by assumption $F = 0$, and so therefore $1 - YF \neq 0$. Now, we drag out the weak Nullstellensatz to conclude:

$$\mathbf{V}(\tilde{I}) = \emptyset \Rightarrow 1 \in < F_1, \ldots, F_n, 1 - YF >.$$

[2] Proving the strong implies the weak is much easier. Perhaps that's why it's called strong. Or maybe it's because you need the weak to prove the strong. The strong rely upon the weak to do their hard work for them. Kind of a Hobbesian thing, maybe.

[3] This is, more or less, the proof from "Ideals, Varieties, and Algorithms" by Cox, Little, and O'Shea.

[4] I included this as an exercise in last week's homework. My bad. I've corrected this in the notes that are now online. If you were able to prove it yourself without looking ahead, you're a genius!

[5] We know this can be done using a finite set of polynomials because of the Hilbert Basis Theorem.

Now, this means that

$$1 = \sum_{i=1}^{n} P_i(X_1, \ldots, X_n, Y)F_i + Q(X_1, \ldots, X_n, Y)(1 - YF).$$

If we set $Y = 1/F(X_1, \ldots, X_n)$[6], then our relation implies:

$$1 = \sum_{i=1}^{n} P_i(X_1, \ldots, X_n, 1/F)F_i,$$

and therefore for some $m \in \mathbb{Z}^+$ we have:

$$f^m = \sum_{i=1}^{n} A_i f_i.$$

Was that not the trickiest proof ever?![7]

To finish up our proof we note that it's certainly true that $\sqrt{I} \subset \mathbf{I}(\mathbf{V}(I))$, because $F \in \sqrt{I}$ implies $F^m \in I$, and if F^m vanishes on $\mathbf{V}(I)$, then so does F.

Conversely, using our result we have that if $F \in \mathbf{I}(\mathbf{V}(I))$, then by definition F vanishes on $\mathbf{V}(I)$, and therefore according to our result $F^m \in I$, which means $F \in \sqrt{I}$.

So,

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

Exercise

2: Prove that the strong Nullstellensatz implies the weak. That is to say, if $\sqrt{I} = \mathbf{I}(\mathbf{V}(I))$ then $\mathbf{V}(I) = \emptyset$ implies $I = K[X_1, \ldots, X_n]$.

2. The *weak* Nullstellensatz

Now we must prove the weak Nullstellensatz.[8] Just for clarity, here it is again in a slightly different form:

[6] OK. Technically, we look at the natural ring homomorphism taking $K[X_1, \ldots, X_n, Y]$ to $K(X_1, \ldots, X_n)$ by sending $Y \mapsto 1/F(X_1, \ldots, X_n)$.

[7] This is actually called the "trick of Rabinowitsch".

[8] This will be essentially the proof from Fulton's "Algebraic Curves". This is a very good introductory algebraic geometry book, from a "do it yourself" perspective (most of the book is problems, and you work out most of the results yourself), and you can download it for free from Fulton's website.

Weak Nullstellensatz. If I is a proper ideal in $K[X_1, \ldots, X_n]$, then $V(I) \neq \emptyset$.

We note first that we may assume that I is a maximal ideal, for there is a maximal ideal J containing I, and $\mathbf{V}(J) \subset \mathbf{V}(I)$. So $L = K[X_1, \ldots, X_n]/I$ is a field, and K may be regarded as a subfield of L.

Now, suppose we knew that $K = L$. Then for each i there is an $a_i \in K$ such that the I-residue of X_i is a_i, or $X_i - a_i \in I$. But $(X_1 - a_1, \ldots, X_n - a_n)$ is a maximal ideal, so $I = (X_1 - a_1, \ldots, X_n - a_n)$, and $\mathbf{V}(I) = \{(a_1, \ldots, a_n)\} \neq \emptyset$.[9]

So, we've reduced the Nullstellensatz to the following conjecture:

Conjecture: If an algebraically closed field K is a subfield of a field L, and there is a ring homomorphism from $K[X_1, \ldots, X_n]$ onto L (that is the identity on K), then $K = L$.

This conjecture will follow directly as a special case of Zariski's lemma, which it will take us some work to prove.

To do this we'll first define the algebraic object conspicuously missing from our first lecture. Namely, the module.

2.1. **Modules.**

Let R be a ring. An R-module is a commutative group M together with a scalar multiplicaiton (a mapping from $R \times M$ to M) satisfying:

1. $(a + b)m = am + bm$, for all $a, b \in R$, $m \in M$.
2. $a(m + n) = am + an$, for all $a \in R$, $m, n \in M$.
3. $(ab)m = a(bm)$ for all $a, b \in R$, $m \in M$.
4. $1m = m$ for $m \in M, 1 \in R$.

A subgroup N of an R-module is called a submodule if $an \in N$ for all $a \in R$, $n \in N$. So, a submodule $N \subseteq M$ is itself an R-module.

If S is a set of elements in an R-module M, then the submodule generated by S is defined to be $\{\sum r_i s_i | r_i \in R, s_i \in S|\}$. We denote this module $\sum Rs_i$.

Exercise

3: Verify that the submodule generated by S using the above definition is the smallest submodule of M containing S.

[9] I asked you to prove that points in $\mathbb{A}^n$ and maximal ideals in $K[X_1, \ldots, X_n]$ correspond in the last lecture. Again, my bad.

A module M is said to be *finitely generated* if $M = \sum Rs_i$ for some $s_1, \ldots, s_n \in M$.

2.2. **Finiteness Conditions.** Now, if R is a subring of a ring S, then there are several types of finiteness conditions for S over R, depending on whether we consider S as an R-module, a ring, or (possibly) a field.

- S is said to be *module-finite* over R, if S is finitely generated as an R-module. If R and S are fields, and S is module finite over R, we denote the dimension of S over R by $[S : R]$. You'll get very use to this notation, and this idea, in your second-semester algebra prelim class.
- Let $v_1, \ldots, v_n \in S$. Let $\phi : R[X_1, \ldots, X_n] \to S$ be the ring homomorphism taking X_i to v_i. The image of ϕ is written $R[v_1, \ldots, v_n]$. It is a subring of S containing R and $v_1, \ldots, v_n$, and it's the smallest such ring. Explicitly, $R[v_1, \ldots, v_n] = \{\sum a_{(i)} v_1^{i_1} \cdots v_n^{i_n} | a_{(i)} \in R\}$. The ring S is *ring-finite* over R if $S = R[v_1, \ldots, v_n]$ for some $v_1, \ldots, v_n \in S$. In other words, S can be viewed as a polynomial over R in a finite number of "variables".
- Suppose $R = K$, $S = L$ are fields. If $v_1, \ldots, v_n \in L$, let $K(v_1, \ldots, v_n)$ be the quotient field of $K[v_1, \ldots, v_n]$. We regard $K(v_1, \ldots, v_n)$ as a subfield of L; it is the smallest subfield of L containing K and $v_1, \ldots, v_n$. The field L is said to be a *finitely generated field extension* of K if $L = K(v_1, \ldots, v_n)$ for some $v_1, \ldots, v_n \in L$.

Examples

(1) The field extension $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$ is module-finite, and $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

(2) The ring $\mathbb{Q}[\pi]$ is ring-finite over $\mathbb{Q}$, but not module-finite. This is equivalent to saying π is transcendental, which is pretty hard to prove.

(3) The field extension $\mathbb{Q}(X)$ is a finitely-generated field extension of $\mathbb{Q}$, but is not ring-finite over $\mathbb{Q}$. You'll prove this as an exercise.

Exercises

4: Show that if S is module-finite over R, then S is ring-finite over R.

5: Show that $S = R[X]$ (the ring of polynomials in one variable) is ring-finite over R, but not module-finite.

6: If L is ring-finite over K (K, L fields) then L is a finitely generated field extension of K.

7: Show that $L = K(X)$ (the field of rational functions in one variable) is a finitely generated field extension of K, but L is not ring-finite over K.[10]

8: Let R be a subring of S, S a subring of T.

(a) If $S = \sum Rv_i$, $T = \sum Sw_j$, show that $T = \sum Rv_iw_j$.
(b) If $S = R[v_1, \ldots, v_n]$, $T = S[w_1, \ldots, w_m]$, show that $T = R[v_1, \ldots, v_n, w_1, \ldots, w_m]$.
(c) If R, S, T are fields, and $S = R(v_1, \ldots, v_n)$, and $T = S(w_1, \ldots, w_m)$, show that $T = R(v_1, \ldots, v_n, w_1, \ldots, w_m)$.

So each of the three finiteness conditions is a transitive relation.

9: (Extremely Hard) Prove or disprove that $\mathbb{Q}[e, \pi]$ is not module-finite over $\mathbb{Q}[\pi]$.[11]

2.3. **Integral Elements.** Let R be a subring of a ring S. An element $v \in S$ is said to be *integral* over R if there is a monic polynomial $F = X^n + a_1X^{n-1} + \cdots + a_n \in R[x]$ such that $F(v) = 0$. If R and S are fields, we usually say that v is *algebraic* over R if v is integral over R.

Proposition - Let R be a subring of a domain S, $v \in S$. Then the following are equivalent:

(1) v is integral over R.

(2) $R[v]$ is module-finite over R.

(3) There is a subring R' of S containing $R[v]$ that is module-finite over R.

Proof -

[10] *Hint*: If L were ring-finite over K, a common denominator of ring generators would be an element $b \in K[X]$ such that for all $z \in L, b^nz \in K[X]$ for some n; but let $z = 1/c$, where c doesn't divide b. To prove such a c always exists, modify a very, very, very old proof.

[11] If you prove this, please let me know!

(1) implies (2): : If $v^n + a_1v^{n-1} + \cdots + a_n = 0$, then $v^n \in \sum_{i=0}^{n-1} Rv^i$. It follows that $v^m \in \sum_{i=0}^{n-1} Rv^i$ for all m, so $R[v] = \sum_{i=0}^{n-1} Rv^i$.

(2) implies (3): : This is obvious. We just let $R' = R[v]$.

(3) implies (1): : This is the interesting part of the proof, and involves something called the "determinant trick", which you'll see come up repeatedly in commutative algebra, so it's nice to learn it now. If $R' = \sum_{i=1}^{n} Rw_i$, then $vw_i = \sum_{j=1}^{n} a_{ij}w_j$ for some $a_{ij} \in R$. Then $\sum_{j=1}^{n}(\delta_{ij}v - a_{ij})w_j = 0$ for all i, where $\delta_{ij} = 0$ if $i \neq j$ and $\delta_{ii} = 1$.[12] If we consider these equations in the quotient field of S,[13] we see that $(w_1, \ldots, w_n)$ is a nontrivial solution, so $det(\delta_{ij}v - a_{ij}) = 0$. Since v appears only in the diagonal of the matrix, this determinant has the form $v^n + a_1v^{n-1} + \cdots + a_n, a_i \in R$. So, v is integral over R.

Corollary. The set of elements of S that are integral over R is a subring of S containing R.

Proof. If a, b are integral over R, then b is integral over $R[a] \supseteq R$, so $R[a, b]$ is module-finite over R.[14] And $a \pm b, ab \in R[a, b]$, so they are integral over R by the proposition.

We say that S is *integral* over R if every element of S is integral over R[15]. If R and S are fields, we say S is an *algebraic extension* of R if S is integral over R. The proposition and corollary extend to the case where S is not a domain, with essentially the same proofs, but we won't need that generality.

Problems

10: Let L be a field, K an algebraically closed subfield of L

(a) Show that any element of L that is algebraic over K is itself already in K.

(b) An algebraically closed field has no module-finite field extensions except itself.

[12] This is called the "Kronecker delta function". Its continuous analogue is called the "Dirac delta function", and it's used in physics to describe cool point things like electrons.

[13] This is where we need for S to be a domain.

[14] Problem 9(a).

[15] Pay attention, this will be coming up again in algebraic geometry.

11: Let K be a field, $L = K(X)$ the field of rational functions in one variable over K.

(a) Show that any element of L that is integral over $K[X]$ is already in $K[X]$.[16]

(b) Show that there is no nonzero element $F \in K[X]$ such that for every $z \in L$, $F^n z$ is integral over $K[X]$ for some $n > 0$.[17]

2.4. **Field Extensions.** Suppose K is a subfield of a field L, and suppose $L = K(v)$ for some $v \in L$. Let $\phi : K[X] \to L$ be the homomorphism taking X to v. Let $ker(\phi) = (F), F \in K[X]$ (since $K[X]$ is a PID). Then $K[X]/(F)$ is isomorphic to $K[v]$, so (F) is prime. Two cases may occur:

Case 1: $F = 0$. Then $K[v]$ is isomorphic to $K[X]$, so $K(v) = L$ is isomorphic to $K(X)$. In this case L is not ring-finite (or module-finite) over K.[18]

Case 2: $F \neq 0$. We may assume F is monic. Then (F) is prime, so F is irreducible and (F) is maximal[19]; therefore $K[v]$ is a field, so $K[v] = K(v)$. And $F(v) = 0$, so v is algebraic over K and $L = K[v]$ is module-finite over K.

Now, to prove the weak Nullstellensatz we must prove that if a field L is a ring-finite extension of an algebraically closed field K, then $L = K$.[20] In view of problem 10 it is enough to show that L is module-finite over K. The following lemma generalizes our discussion above:

Zariski's Lemma - If a field L is ring-finite over a subfield K, then L is module-finite (and hence algebraic) over K.

Proof - Suppose $L = K[v_1, \ldots, v_n]$. The case $n = 1$ was taken care of by our above discussion, so we assume the result for all extensions generated by $n - 1$ elements. Let $K_1 = K(v_1)$. By induction, $L = K_1[v_2, \ldots, v_n]$ is module-finite over K_1. We may assume v_1 is not algebraic over K[21].

[16] *Hint*: If $z^n + a_1 z^{n-1} + \cdots + a_n = 0$, write $z = F/G$, F, G relatively prime. Then $F^n + a_1 F^{n-1} G + \cdots + G^n = 0$, so G divides F. You might also want to use an idea like this in one of your earlier problems, if you're stuck.

[17] *Hint*: See problem 8.

[18] See problem 9.

[19] Every nonzero prime ideal in a PID is maximal.

[20] This is a restatement of our conjecture.

[21] If it were, problem 9(a) would finish the proof.

Each v_i satisfies an equation $v_i^{n_i} + a_{i1}v_i^{n_i-1} + \cdots + a_{in} = 0, a_{ij} \in K_1$. If we take $a \in K[v_1]$ that is a multiple of all the denominators of the a_{ij}, we get equations $(av_i)^{n_i} + aa_{i1}(av_1)^{n_i-1} + \cdots + a^n a_{in} = 0$. It follows from our earlier corollary that for any $z \in L = K[v_1, \ldots, v_n]$, there is an N such that $a^n z$ is integral over $K[v_1]$. In particular, this must hold for $z \in K(v_1)$. But since $K(v_1)$ is isomorphic to the field of rational functions in one variable over K, this is impossible[22]. This proves Zariski's lemma, and as a consequence the weak Nullstellensatz.

Exercise

12: Let K be a field, $F \in K[X]$ an irreducible monic polynomial of degree $n > 0$.

(a) Show that $L = K[X]/(F)$ is a field, and if x is the residue of X in L, then $F(x) = 0$.

(b) Suppose L' is a field extension of K, $y \in L'$ such that $F(y) = 0$. Show that the homomorphism from $K[X]$ to L' that takes X to y induces an isomorphism of L with $K(y)$.

(c) With L', y as in (b), suppose $G \in K[X]$ and $G(y) = 0$. Show that F divides G.

(d) Show that $F = (X - x)F_1, F_1 \in L[X]$.

13: Let K be a field, $F \in K[X]$. Show that there is a field L containing K such that $F = \prod_{i=1}^{n}(X - x_i) \in L[X]$.[23] L is called a *splitting field* of F.[24]

[22] According to problem 11(b).

[23] *Hint*: use problem 12(d) and induction on the degree.

[24] I am the David Foster Wallace of lecture notes.