BUT DAT NULLSTELLENSATZ THO

ISHAN LEVY

1. Review and Overview

Here is a review of the notation: $\mathbb{A}^n$ is affine n-space, K is an (algebraically closed unless otherwise specified) field, and if $C \subset K[x_1, \ldots, x_n]$ is an ideal, $\sqrt{C}$ is the radical of C i.e $\{f \in K[x_1, \ldots x_n] | f^n \in C\}$

Hilbert's Nullstellensatz is a way of translating geometry (affine algebraic sets) into algebra (radical ideals of polynomial rings) and vice versa. More specifically, given a $A \subset \mathbb{A}^n$, we can consider $I(A)$ which is the set of polynomials in $K[x_1, \ldots, x_n]$ vanishing on A. Conversely given $C \subset K[x_1, \ldots, x_n]$ we can consider the set of common zeroes of all the elements of C. Are these inverses? The answer is yes if we restrict to algebraic sets and radical ideals. This is the Nullstellensatz.

In particular, maximal ideals correspond to points. This is the Weak Nullstellensatz. We will use this to prove the standard form of it. It can be seen in the case of $K[x]$ easily, as it is a PID so all of the maximal ideals are just irreducibles. K is algebraically closed so indeed we have that the maximal ideals are just $(x - a)$ for $a \in K$, which is what we want, as its zero set is just the point a.

Now before proving anything let's develop some facts about integrality that will be used to prove the main lemma, Noether Normalization, which will be used to deduce Nullstellensatz.

2. Integrality Facts

Definition 2.1. *Let $R \subset S$ be rings, $s \in S$. s is **integral** over R if it is the root of a monic polynomial in $R[x]$. We say S is integral over R if every element of S is.*

Integrality is similar to algebraicity, and reduces to algebraicity in the case that R is a field. It is a good definition because of the following:

Proposition 2.2. *Let $R \subset S$ be rings, $s \in S$. The following are equivalent:*

(1) s is integral over R
(2) There is a subring T, $R \subset T \subset S$ containing s that is f.g (finitely generated) as an R-module.

Proof. (1) $\Rightarrow$ (2) Consider $R[s]$ with the basis $1, s, \ldots s^{k-1}$ where the degree of the monic polynomial for which s vanishes is k.

(2) $\Rightarrow$ (1) Suppose $v_1, \ldots v_k$ generate T as an R-module. Then consider the endomorphism that takes $x \in T$ to sx. In particular, for each v_i, with $a_{ij} \in R$,

$$(1) \qquad sv_i = \sum_1^k a_{ij}v_i \Rightarrow \sum_1^k (\delta_{ij}s - a_{ij})v_i = 0$$

where δ_{ij} is the Kronecker delta. Then by Cramer's Rule s is a root of the characteristic polynomial of the matrix a_{ij} which is monic.

$\square$

Corollary 2.3. *If $R \subset S$ and $s, t \in S$ are integral over R, $s \pm t$ and st are as well. Integrality is also transitive, ie. If T is integral over S and S is integral over R, T is integral over R.*

Proof. If s and t are integral over R, let $v_1, \ldots v_k$ be an R-module generating set of $R[s]$ and let $w_1, \ldots w_l$ be the ones for $R[t]$. Then the products $v_1w_1, \ldots v_1w_l, v_2w_1, \ldots v_kw_l$ generate $R[s, t]$ as an R-module. This proves the first statement. For the second, if $t \in T$ is integral over S, let $a_0, \ldots a_k$ be the coefficients in a monic polynomial in S for which t is a root. Then by the same argument, $R[a_0, \ldots a_k]$ is a f.g R-module, so $R[a_0, \ldots a_k, t]$ is a f.g $R[a_0, \ldots a_k]$-module hence is also f.g as an R-module. $\square$

Great, now that we have the basic facts about integrality, let's prove Noether Normalization!

3. Noether Normalization and Nullstellensatz

Lemma 3.1 (Noether Normalization). *Let $B = K[r_1, \ldots r_m]$ be a f.g K-algebra (ie B is a quotient of a polynomial ring with coefficients in K in finitely many variables). Then there is an injective map from a polynomial ring over K such that B is integral over the image. (This statement doesn't require K algebraically closed)*

Proof. Consider the map $K[x_1, \ldots x_m] \to B$ sending x_i to r_i. If the map is injective, it is an isomorphism so B is trivially integral over the image. If not, let f be a nontrivial element in the kernel, so that $f(r_1, \ldots r_m) = 0$. It would be nice if f were monic in some variable so that we could say that that variable is integral over the rest and induct on m by transitivity of integrality, but this is not necessarily the case (say if the polynomial is x_1x_2). So we will make a change of variables (the "normalization") which will force the polynomial to be monic.

Let d be the degree of f (the degree of a monomial is the sum of the exponents in each variable), and define $a_i = (1 + d)^i$, $X_i = x_i - x_m^{a_i}$ for the change of variables.

Now let g be the polynomial:

$$(2) \qquad\qquad g(X_1, \ldots X_{m-1}, x_m) = f(x_1, \ldots x_m)$$

Why is g (almost) monic in x_m? Well any monomial in f, say $cx_1^{k_1} \ldots x_m^{k_m}$ corresponds to a $c(x_1 + x_m^{a_1})^{k_1} \ldots (x_{m-1} + x_m^{a_{m-1}})^{k_{m-1}} x_m^{k_m}$, so the highest x_m term it contributes contains only the variable x_m. Now by looking at the exponent of the largest monomials in base $d+1$, we see that no two monomials contribute the same highest x_m term so there is no cancelling. Then if the highest degree x_m term in g has coefficient $a \in K$, $\frac{g}{a}$ is a monic polynomial in $K[X_1, \ldots X_{m-1}, x_m]$ so if we set $s_i = r_i - r_m^{a_i}$, $i < m$ then g shows that r_m is integral over $K[s_1, \ldots s_{m-1}]$. Now the defining relation of s_i shows that r_i is integral over $K[s_1, \ldots s_{m-1}, r_m]$, so by transitivity B is integral over $K[s_1, \ldots s_{m-1}]$ so we are done by induction. (The base case is when $m = 0$, which is trivial). $\qquad\square$

We are ready to prove the weak form of the Nullstellensatz. It follows almost immediately from this lemma.

Theorem 3.2 (Weak Nullstellensatz)**.** *The maximal ideals of $K[x_1, \ldots x_m]$ are exactly the ideals of the form $(x_1 - a_1, \ldots x_m - a_m)$ for $a_i \in K$. In particular, if I is a proper ideal of $K[x_1, \ldots x_m]$, it has a zero in $\mathbb{A}^n$.*

Proof. It is obvious that the ideals of the form above are maximal. For the converse, suppose that I is maximal. $K[x_1, \ldots x_m]/I$ is a field K'. By Noether Normalization, K' is integral over $K[x_1, \ldots x_q]$. But q had better be 0 as $\frac{1}{x_1}$ is not integral over $K[x_1, \ldots x_q]$ but K' is a field so would have to contain it. Thus K' is integral $\Rightarrow$ algebraic over K but K is algebraically closed so $K' = K$. Then in the projection map from $K[x_1, \ldots x_m]$ to K' we have that each x_i is sent to some element of K so the kernel, I, is of the form we want.

For the second statement, if an ideal I is proper, it is contained in a maximal ideal M, and so the point M corresponds to is a zero of I. $\qquad\square$

Now we will deduce the stronger form from the weaker.

Theorem 3.3 (Nullstellensatz)**.** *Let C be an ideal of $K[x_1, \ldots x_n]$. Then $\sqrt{C} = I(Z(C))$.*

Proof. Certainly $\sqrt{C} \subset I(Z(C))$ (check this). The hard part is proving the reverse inclusion. Suppose that $g \in I(Z(C))$. We will "localize" away from g and then use the Weak Nullstellensatz to deduce $g \in \sqrt{C}$. By the Hilbert Basis Theorem, $C = (f_1, \ldots f_m)$. Now consider the ideal in $K[x_1, \ldots x_{n+1}]$: $(f_1, \ldots f_m, x_{n+1}g - 1)$ (think of x_{n+1} as "$\frac{1}{g}$"). This has no zeroes in $\mathbb{A}^{n+1}$ as if each f_i is 0, g is too (it's in C), so $x_{n+1}g - 1$ is -1. Then By the Weak Nullstellensatz, $(f_1, \ldots f_m, x_{n+1}g - 1)$ is

not a proper ideal, so there are polynomials $b_i \in K[x_1, \ldots x_m + 1]$ such that:

(3)
$$1 = b_1 f_1 + \ldots b_m f_m + b_{m+1}(x_{n+1}g - 1)$$

Replacing x_{n+1} with $\frac{1}{y}$ in this equation and multiplying through by a large enough power of y to clear denominators yields:

(4)
$$y^k = c_1 f_1 + \ldots c_m f_m + c_{m+1}(g - y)$$

where we have changed b_i to c_i to absorb the new powers of y introduced. Plugging in g, we get

(5)
$$g^k = c_1 f_1 + \ldots c_m f_m$$

which is exactly $g \in \sqrt{C}$. $\qquad\square$

In the proof of Noether Normalization, we have done a particularly strange change of variables in order to force our polynomial to be monic, namely we have sent $x_i \mapsto (x_i + x_n^{a_i})$ where a_i is quite large. However, most of the time it suffices to make a more reasonable change $x_i \mapsto (x_i + \alpha x_n)$ instead. This doesn't always work: for $\mathbb{F}_q$ we can consider $x^q y^q - y^{2q}$, for which no change of variables of the form $y \mapsto y + \alpha x$ will yield a monic polynomial. However, this is the only problem: if we assume our field is infinite, we can do such a change of variables.

To see this, consider the same polynomial $x^q y^q - y^{2q}$. If we do the change of variables $y \mapsto y + \alpha x$ we get $x^q(y + \alpha x)^q - (y^{2q} + \alpha x) = x^q y^q - y^{2q} + (\alpha^q - \alpha^{2q})x^{2q}$. The only way this would not be monic in x is if α is the root of $z^q - z^{2q}$, but this polynomial has finitely many roots, so in an infinite field we can always choose a nice enough α.

In general, we can argue inductively as follows: consider the highest total degree monomials of the form $ax_1^{i_1} \ldots x_n^{i_n}$ and choose one such that the first i so that x_i is in it is the highest (we will continue to refer to this index as i). Now if $i = n$, we are done as the polynomial is already monic in x_n, and if not, we will change the variable $x_i \mapsto x_i + \alpha x_n$. Any other monomials that might cancel this change of variables give a polynomial in 1 variable that α would need to satisfy for this change of variables to be ineffective, so we then use the fact that the field is infinite, and are left with a polynomial which is closer to being monic, and we can induct.

To illustrate this proof of Noether Normalization, we can consider the hyperbola $K[x, y]/(xy - 1)$ and try to project down to $K[x]$. Now this won't give a nice projection onto the x axis as the line $x = 0$ is asymptotic, which corresponds to the fact that y is the inverse of x and hence is not finite over it. We can tilt the y axis by making the change of variables $x \mapsto x + \epsilon y$, which will make the relation $(x + \epsilon y)y$, which is monic in y, and will make y integral by removing the asymptote.