12. Nullstellensatz

Hilbert's Nullstellensatz

Radicals and Radical Ideals

Definition: If $I \subset R$ is an ideal, I is called *radical* if, whenever $f^n \in I$, we have $f \in I$.
Alternatively, I is radical if R/I has no nilpotent elements. If I is any ideal, then $\mathrm{rad}(I)$ is the set of elements f such that $f^m \in I$ for some m. Finally, the radical of the zero ideal, which is the set of nilpotent elements in R, is called the *nilradical* of R.

Remark: We've seen at various times in the past that the nilpotent elements of a (commutative) ring form an ideal.

Proposition: If I is a proper ideal of R, then the radical of I is the intersection of all the prime ideals of R containing I.

Proof: It's enough to prove that the nilradical of R/I is the intersection of all prime ideals of R/I. If $P \supset I$ is a prime ideal, and $f^n \in I$ for some n, choose the smallest such n. Then $f^n \in P$ so either $f^{n-1} \in P$ or $f \in P$. By minimality of n, this means that $f \in P$. So the nilradical is contained in every prime ideal.

For the converse, suppose that a is not a nilpotent element of R (and is not a unit in R). Then we will construct a prime ideal P that does not contain a. Let A be the set of powers of a: $A = \{a, a^2, a^3, \ldots\}$ and let S be the set of ideals of R not meeting A. This is a nonempty set, since it contains the zero ideal. If $I_1 \subset I_2 \subset \cdots$ is a chain of ideals in S, then the union of the I_k is again an ideal in S, so chains in S have upper bounds. By Zorn's lemma, S has a maximal element Q. Now suppose that x and y are elements of R and $xy \in P$. Since P is maximal in S, we know that some power of a^r is in $(x) + P$ and some power of a^s is in $(y) + P$. But then a^{r+s} is in $xy + P = P$ since $xy \in P$. This is a contradiction, since P is in S. It follows that one of x or y must have been in P, so P is prime.

Corollary: Prime (and maximal) ideals of R are radical ideals.

Integral Extensions

Definition: Let S be a commutative R algebra.

- An element $a \in S$ is integral over R if it is the root of a monic polynomial in $R[x]$.
- If every element of s is integral over R, then S is called an *integral* extension of R.
- The subset of S consisting of elements integral over R is called the *integral closure* of R in S.
- R is integrally closed in S if it is equal to its integral closure.
- If R is an integral domain, and R is integrally closed in its field of fractions, then R is integrally closed (full stop) or *normal*. The integral closure of R in its field of fractions is called its normalization.

Proposition: The following are equivalent:

- a is integral over R.
- $R[a]$ is a finitely generated R module.
- There is a subring $R \subset T \subset S$ containing a wuch that T is a finitely generated R-module

Proof: If a satisfies the monic polynomial $x^n + r_{n-1}x^{n-1} + \cdots + r_0$, then any element of $R[a]$ can be written as a linear combination of $1, a, a^2, \ldots, a^{n-1}$. So $R[a]$ is finitely generated. The ring $R[a] \subset S$ is a finitely generated R module inside S. Finally, if a belongs to a finitely generated R module T, choose generators for T $t_1, \ldots, t_n$ over R and consider the equations

$$at_i = \sum r_{ij} t_j$$

The element a satisfies the (monic) characteristic polynomial made from the entries r_{ij}, so a is integral over R.

Corollary: The sum and product of integral elements are integral; the integral closure of R in S is a subring of S; and if S is integral over R and T is integral over S then T is integral over R.

Corollary: Let $\tilde{R}$ be the integral closure of R in S. Then $\tilde{R}$ is integrally closed.

Proof: If $x \in S$ is integral over $\tilde{R}$, then since $\tilde{R}$ is integral over R, we have x is integral over R so belongs to $\tilde{R}$.

Proposition: Suppose that S is an R-algebra that is integral over R. Then R is a field if and only if S is a field.

Proof: Suppose first that R is a field. Choose $s \in S$. Then

$$s^n + r_{n-1}s^{n-1} + \cdots + r_0 = 0$$

where we can assume $r_0 \neq 0$. Then

$$s(s^{n-1} + r_{n-1}s^{n-2} + \cdots + r_1) = -r_0.$$

Since $-r_0 \neq 0$, we can divide the polynomial on the right by $-r_0$ to obtain a multiplicative inverse for s.

Now suppose that S is a field. If $r \in R$, then $r \in S$, so $r^{-1} \in S$. We have

$$r^{-m} + r_{m-1}r^{-m-1} + \cdots + r_0 = 0$$

so by clearing demoninators we can write r^{-1} as an element of R.

Noether Normalization

Definition: Elements $x_1, \ldots, x_n$ in a k-algebra S are called algebraically independent if there are no nonzero polynomial relations among them: there are no polynomials p so that $p(x_1, \ldots, x_n) = 0$. In other words, they generate a copy of $k[x_1, \ldots, x_n] \subset S$.

Theorem: (Noether Normalization) Let k be a field and let A be a finitely generated k-algebra. Then there are algebraically independent elements $y_1, \ldots, y_q$ in A such that A is integral over $k[y_1, \ldots, y_q]$.

Proof: The proof is by induction and is (more or less) algorithmic. Start with generators $x_1, \ldots, x_n$ for A. If they are algebraically independent, you're done. Otherwise you have a polynomial relation

$$p(x_1, \ldots, x_n) = 0.$$

This is a sum of monomials $x_1^{a_1} \cdots x_n^{a_n}$. The degree of p is the largest of the sums of these exponents; call that d. Then let α be any integer bigger than d ($d + 1$ works fine).

Introduce new coordinates X_i (for $i = 1, \ldots, n-1$) by:

$$\begin{array}{rcl} x_1 & = & X_1 + x_n^{\alpha} \\ x_2 & = & X_2 + x_n^{\alpha^2} \\ \vdots & = & \vdots \\ x_{n-1} & = & X_{n-1} + x_n^{\alpha^{n-1}} \end{array}$$

If we substitute the new coordinates, we get $p(X_1 + x_m^{\alpha}, \cdots, X_{n-1} + x_n^{\alpha^{n-1}}, x_n) = 0$. But a monomial $x_1^{a_1} \cdots x_n^{a_n}$ will contribute a term

$$x_n^{a_n + a_{n-1}\alpha^{n-1} + a_{n-2}\alpha^{n-2} + \cdots + a_1\alpha}$$

and since we choose α bigger than d we have all $a_i < \alpha$. In other words, all of these exponents of x_n are distinct (they are different in base α).

It follows that the polynomial $p(X_1 + x_m^{\alpha}, \cdots, X_{n-1} + x_n^{\alpha^{n-1}}, x_n)$ has the form

$$p(X_1 + x_m^{\alpha}, \cdots, X_{n-1} + x_n^{\alpha^{n-1}}, x_n) = cx_m^N + \sum H_i(X_1, \dots, X_{n-1}) x_m^i$$

and so x_m is integral over the subring $B = k[X_1, \dots, X_{m-1}]$. But then x_i for $i = 1, \dots, n-1$ are integral over $B[x_m]$ because they satisfy the equations $x_i - X_i - x_n^{\alpha^i}$. Therefore A is integral over B (which has fewer generators). Continue by induction.

Theorem: (the "weak" nullstellensatz) Let k be an algebraically closed field and let $A = k[x_1, \dots, x_n]$. Then the maximal ideals M of A are all of the form

$$M = (x - a_1, \dots, x - a_n)$$

where the $a_i \in k$.

Corollary: The correspondence between ideals and algebraic sets gives a bijection between points and maximal ideals of $\mathbb{A}_k^n$.

Corollary: Let $f_1, \dots, f_k \in A$. Then either the f_i have a common zero, or there are polynomials $g_1, \dots, g_k$ in A such that

$$1 = \sum g_i f_i.$$

Proof: (of the theorem) Clearly an ideal of the form $(x_1 - a_1, \dots, x_n - a_n)$ is maximal, so suppose M is a maximal ideal of A. Let $E = A/M$. Then E is a finitely generated k-algebra, so there are algebraically independent elements $y_1, \dots, y_k$ such that E is integral over $k[y_1, \dots, y_k]$. But E is a field, so $k[y_1, \dots, y_k]$ is a field. But this can only happen if $k = 0$. Then E/k is a finite integral (i.e. algebraic) extension of k, and k is algebraically closed, so $E = k$. This means that each of the generators x_i is congruent mod M to an element of k, or in other words M is of the desired form.

For the corollaries, any proper ideal I of A is contained in a maximal ideal M, so if $X(I)$ contains the point corresponding to M. So the points of $X(I)$ correspond to the maximal ideals containing I.

Finally, if the f_i have no common zero, then they must not generate a proper ideal, so the ideal they generate contains 1.

Theorem: (Nullstellensatz, "strong" form) Let k be an algebraically closed field. Then if $J \subset A$ is any ideal, $I(X(J)) = \mathrm{rad}(J)$. Thus (assuming k is algebraically closed) there are mutually inverse bijections between algebraic sets in $\mathbb{A}_k^n$ and radical ideals in A.

Proof: We know that $\mathrm{rad}(J) \subset I(X(J))$ so we need to prove the opposite. We know that J is finitely generated, say by $f_1, \dots, f_k$. Let g be any polynomial vanishing on $X(J)$. Make a new ring A' by introducing a new variable x_{n+1} and a new ideal $J' \in A'$ by adding the relation $gx_{n+1} - 1$. (Notice that this means that x_{n+1} is $1/g$.) If the elements of J' had a common zero, all of the f_i

would vanish at that point and since $g \in I(X(J))$ so would g. But that doesn't happen, so J' can't be a proper ideal and so we have an equation

$$1 = h_1 f_1 + \cdots + h_k f_k + h_{k+1}(x_{n+1} g - 1)$$

We can divide this equation by a high power of x_{n+1} so that the powers of h_{n+1} in the coefficients h_i are all negative. In other words, writing $y = 1/x_{n+1}$, we get an equation

$$y^N = b_1 f_1 + \cdots + b_k f_k + b_{k+1}(g - y)$$

where the b_i are polynomials in $x_1, \ldots, x_n$ and y. This is an equation in A', where $g = 1/x_{n+1}$, so this means (substituting g for y) that we have an equation showing that g^N is in the ideal generated by the f_i, so $g \in \mathrm{rad}(J)$.

Corollary: If k is not algebraically closed, then we can still conclude that a set of polynomials that generates a proper ideal of $k[x_1, \ldots, x_n]$ must have common zeros in the algebraic closure of k.