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

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.

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