Math 505, 2/1

Now (and for the rest of the course) we broaden our focus to commutative rings R, usually however assumed Noetherian. A special case of particular importance for us is the one where $R = K[x_1, \ldots, x_n]$, the polynomial ring in n variables over a field K (usually taken to be algebraically closed for simplicity), or a quotient of this ring. We have seen that every nonzero ideal in a Dedekind domain is uniquely a product of prime ideals; for general commutative rings this is too much to expect, but we can still hope to get a better grasp on prime ideals than on arbitrary ones. We will therefore focus on prime ideals in what follows.

Start with the particular example $R = K[x_1, \ldots, x_n]$ mentioned above, where K is an algebraically closed field. If $n = 1$, we know that the nonzero prime ideals in R are all generated by single linear polynomials $x - a$ for some $a \in K$, and that every such ideal is maximal. It is natural to wonder what happens for larger n. To this end, we define *affine algebraic variety* V in K^n to be the subset S of common zeros of some nonempty collection $\mathcal{S}$ of elements of R. Since the common zeros of the polynomials in $\mathcal{S}$ are the same as those of the ideal I generated by it, we may assume that $\mathcal{S}$ is in fact an ideal I of R; denote the variety of its common zeros by $V(I)$ and call the quotient ring R/I the *coordinate ring* of $V(I)$; we denote this ring by $K[V]$. We will see later that $K[V]$ depends only on V (as the notation indicates) if the ideal iI s suitably restricted; for now we have a map $I \to V(I)$ from ideals of R to subsets of K^n, but this map is clearly not a bijection; even for $n = 1$, the varieties $V(x), V(x^2)$ of the respective principal ideals generated by x, x^2 are both the point $\{0\}$. For $n > 1$, it is not even obvious that $V(I)$ is nonempty if I is proper.

To better understand $V(I)$ we focus on $K[V]$; this is generated as K-algebra (that is, as a ring containing a copy of K which in turn contains its identity element) by finitely many elements $x_1, \ldots, x_n$. I now claim that *given any finitely generated algebra A over K, there are finitely many elements $y_1, \ldots, y_m \in A$ that are algebraically independent over K such that A is a finitely generated integral extension of $B = K[y_1, \ldots, y_m]$*, that is, that every element of A satisfies a monic polynomial equation with coefficients in B. We prove this by induction on n. If the x_i are already algebraically independent then the result is clear; otherwise we have a polynomial p in the x_i with coefficients in K that equals 0 in A. We may regard p as a polynomial in just the last variable x_n (renumbering if necessary) with coefficients polynomials in the other variables x_i. Let d be the maximum degree of all of these coefficients. We now make a change of variable, setting $x_i = y_i + x_n^{(d+1)^i}$ for $i < n$. Writing out p as a polynomial in $y_1, \ldots, y_{n-1}, x_n$ we find that every monomial term of every coefficient of p gives rise to a different power of x_n; the top power of x_n occurring has constant coefficient c and arises from the lexicographically highest term $cx_1^{m_1} \ldots x_{n_1}^{m_{n-1}}$ of any coefficient of p, that is, one first of all with the highest possible power of x_{n-1}, then among these one with the highest possible power of x_{n-2}, and so on; if two coefficients appear with identical powers of the x_i for $i < n$, then the one we want is the one attached to the higher power of x_n. Dividing by c, we get a monic polynomial in x_n with coefficients polynomials in the y_i, so that A is integral over the subalgebra generated by K and the y_i. By induction we realize A in the desired form. Now we pause to note a simple ring-theoretic fact: *given two integral domains $A \subset B$ with B integral over A, then B is a field if and only if A is.* Indeed, if A is a field and $x \in B, x \neq 0$, then we have an equation $x^n = \sum_{i=0}^{n-1} a_i x^i$ with $a_i \in A$; cancelling out a suitable power of x, we may assume that $a_0 \neq 0$, and then a_0 is a multiple of x and so has a multiplicative inverse, whence x does too. Conversely, if B is a field and $x \in A, x \neq 0$, then we have an equation $x^{-n} = \sum_{i=0}^{n-1} a_i x^{i-n}$; multiplying by x^{n-1} we realize x^{-1} as a polynomial in x with coefficients in A, whence it lies in A as desired. Now given a proper quotient R/I of R/I that is a field K', we deduce that K' must be an integral extension of K itself (as opposed to $K[y_1, \dots, y_m]$, which is never a field for $m > 0$), whence if K is algebraically closed , we must have $K' = K$. This forces the generators x_i of R to map to elements a_i of K in the canonical map from R/I to $K' = K$, whence *every maximal ideal of R takes the form $(x_1 - a_1, \dots, x_n - a_n)$, if K is algebraically closed.* Since every proper ideal I of R is in turn contained in a maximal one, we deduce as desired that *$V(I)$ is nonempty for every proper ideal I of $R = K[x_1, \dots, x_n]$.* This is the weak form of a famous result called the Nullstellensatz (zero places theorem); we will prove the strong form and deduce a bijection between suitably restricted ideals I and varieties next time.