CA LECTURE 6

SCRIBE: ROB BAYER

Some easy facts:

Let $R \leq S \leq T$ be rings:

(1) If S is module-finite / R then S is ring-finite/ R.
(2) If T is ring-finite/S and S is ring-finite/R then T is ring-finite/R (take the union of the generating sets)
(3) If T is module-finite/S and S is module-finite/R then T is module-finite/R (take the pointwise product of the generating sets)

Hilbert's Nullstellensatz: let k be an algberaically closed field and let $R = k[x_1, \dots x_n]$. Here are three versions of the N-Satz:

(1) The maximal ideal of R are precisely the ideals $(x_1 - a_1, \dots x_n - a_n)$ for some point $\vec{a}$ of k^n. Note that this ideal is precisely $\{f \in R : f(\vec{a}) = 0\}$.
(2) If J is an ideal of R, then $I(V(J)) = \sqrt{J}$.
(3) Let $f_1, \dots f_k$ be in R. Then the f's have no common zero iff for some $g_1, \dots g_k \in R$ we have $\sum_i g_i f_i = 1$.

Prove the N-Satz using following technical lemma:

Lemma 1. *Let $A \leq B \leq C$ where A is N'ian, and C is both ring-finite/A and module-finite/B. Then B is ring-finite/A.*

Point: we need some extra conditions to make sure a subextension of a ring-finite extension is ring-finite.

Proof. We will find $\bar{A}$ so that $A \leq \bar{A} \leq B \leq C$, with $\bar{A}$ ring-finite/A and C module-finite/$\bar{A}$. This is sufficient: for by the B-Satz we know that $\bar{A}$ is a N'ian ring, and so since C is fg as a $\bar{A}$-module it is N'ian as a $\bar{A}$-module, hence B is module-finite/$\bar{A}$. So B is ring-finite/$\bar{A}$ which is ring-finite/A, hence B is ring-finite/A.

Let $C = (c_1, \dots c_m)_B = A[d_1, \dots d_n]$. Let $b_1, \dots b_l$ enumerate elements of B such that every d_i and every product $c_j c_k$ is a B-linear combination of the c_s's with coefficients among the b_t's. Now let $\bar{A} = A[b_1, \dots b_l]$. Clearly $\bar{A}$ is ring-finite/A and to finish we claim that $C = (c_1, \dots c_m)_{\bar{A}}$.

Let c be a typical element of C. c can be written as a polynomial in the d_i with coefficients from A, so c is a polynomial in the c_j with coefficients from $\bar{A}$. Now by an easy induction every monomial in the c_j can be written as a linear combination of the c_j with coefficients from $\bar{A}$. □

Before proving the N-Satz we need to see how the finiteness conditions work for field extensions. Recall that if $K \leq L$ are fields then

- Given $a_1, \dots a_t \in L$ the least subfield of L containing $K \cup \{a_1 \dots a_t\}$ is written $K(a_1, \dots a_t)$ and consists of all quotients

$$\frac{f(a_1, \dots a_t)}{g(a_1, \dots a_t)}$$

where $f, g \in K[x_1, \dots x_t]$ and $g(a_1, \dots a_t) \neq 0$.

- $a \in L$ is *algebraic over* K iff there is $f \neq 0$ in $K[x]$ such that $f(a) = 0$. Otherwise a is *transcendental* over K.

Fact 1. *If a is alg/K then $K(a) = K[a]$ and $K(a)$ is a module-finite extension of K (which is just a fancy way of saying it is finite-dimensional when viewed as a VS over K).*

Proof. Let a be algberaic over K and consider the map $\phi : f \mapsto f(a)$ from $K[x]$ to L. Now as usual $im(\phi) \simeq K[x]/ker(\phi)$. $im(\phi)$ is a subring of a field so $im(\phi)$ is an ID, thus $ker(\phi)$ is prime. Since a is algebraic $ker(\phi) \neq 0$ so by general nonsense about PIDs ker(ϕ) is maximal and can be writen as (F_a) for a unique monic polynomial F_a (the "minimal polynomial" of a / K). So $im(\phi)$ is a field.

It is easy to see that $im(\phi) = K[a]$ and since $K[a]$ is a field we have $K[a] = K(a)$. To finish if $deg(F_a) = n$ then every $g \in K[x]$ can be written $g = qF + r$ where $deg(r) < n$, so that $g(a) = r(a) = \sum_{i<n} c_i a^i$ for some $c_i \in K$. It follows that $K(a) = K[a] = (1, a, \dots a^{n-1})_K$ so it is module-finite/ K. □

Cultural note: in fact $\{1, a, \dots a^{n-1}\}$ is linear;y independent so forms a vector space basis for $K(a)$ over K.