Algebra Detour

We need to develop some algebraic tools in order to finish the proof of the Nullstellensatz. Specifically, we want to show:

Thm: If k is algebraically closed, the maximal ideals of $k[x_1, \dots, x_n]$ are of the form $(x_1 - a_1, \dots, x_n - a_n)$, where $a_i \in k$.

Note that a HW #2 problem says that those ideals are always maximal but we want to show that these are exactly the maximal ideals.

This theorem does not hold over an arbitrary field:

Ex: $(x^2+1) \subseteq \mathbb{R}[x]$ is prime and thus maximal (since $\mathbb{R}[x]$ is a PID).

Rings + Modules

Let R be a ring and M an R-module.

Def: M is a finitely generated R-module if there are $m_1, \dots, m_n \in M$ s.t. for all $m \in M$, there are $a_1, \dots, a_n \in R$ such that $m = \sum a_i m_i$.

Now, suppose S is a ring, $R \subseteq S$ a subring.

We can treat S as an R-module, but in this special case, S is called an R-algebra.

Def: If S is a finitely generated R-module, then S is module-finite (or, simply, finite) over R.

Let $v_1, \ldots, v_n \in S$. We denote the subring generated by $R, v_1, \ldots, v_n$ in S by $R[v_1, \ldots, v_n]$. (Roughly, this is the ring of "polynomials" in $v_1, \ldots, v_n$ with coefficients in R.)

Ex: $\mathbb{Q}[\sqrt{2}] \subseteq \mathbb{R}$ is the set of elements of the form $a + b\sqrt{2}$, where $a, b \in \mathbb{Q}$.

Def: S is ring-finite over R (or, a finitely generated R-algebra) if $S = R[v_1, \ldots, v_n]$ for some $v_1, \ldots, v_n \in S$.

Note: If $S = R[v_1, \ldots, v_n]$, there is a natural surjection

$$R[x_1, \ldots, x_n] \twoheadrightarrow S$$

where $R \xrightarrow{id} R$ and $x_i \mapsto v_i$.

Def: $f \in R[x]$ is monic if it is of the form $x^n + a_{n-1}x^{n-1} + \cdots + a_0$. i.e. the initial coefficient is 1.

Def: $v \in S$ is integral over R if there is a monic polynomial $f \in R[x]$ s.t. $f(v) = 0$. (algebraic, if R and S are fields). S is integral over R if every $v \in S$ is.

Check:

1.) Module- and ring- finiteness are both transitive (integrality is trickier – see HW)
2.) Module-finite $\Rightarrow$ ring-finite

We'll soon show that the set of elements integral over R is a subring (in fact a subalgebra) of S, called the <u>integral closure</u> of R in S. If R is an integral domain, the integral closure of R (without reference to a bigger ring) is the integral closure in its field of fractions.

Ex: 1.) $R[x]$ is ring-finite over R but not module-finite or integral.

2.) $R[x]/(x^2) = R + R\bar{x}$ is module-finite, ring-finite, and integral over R.

3.) $\mathbb{Q}[\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \dots]$ is integral over $\mathbb{Q}$, but not ring- or module-finite.

In fact, module-finiteness is a stronger condition than integrality. We'll prove a slightly weaker assertion:

Prop: $R \subseteq S$, S an integral domain, $v \in S$. TFAE:

1.) v is integral over R.

2.) $R[v]$ is module-finite over R.

3.) There's a subring $R' \subseteq S$ containing $R[v]$ that's module-finite over R.

Pf: $\underline{1.) \Rightarrow 2.)}$ $v^n + a_1 v^{n+1} + \dots + a_n = 0$, $a_i \in R$

$\Rightarrow v^n \in R + Rv + \dots + Rv^{n-1} \Rightarrow$ any power of v is in there

$\Rightarrow R[v]$ is module-finite.

$\underline{2.) \Rightarrow 3.)}$ $R' = R[v]$

$\underline{3.) \Rightarrow 1.)}$ Suppose R' is gen. as an R-module by $w_1, \dots, w_n$.

Then $v w_i = a_{i1} w_1 + \dots + a_{in} w_n$, $a_{ij} \in R$

$$\Rightarrow \begin{pmatrix} a_{11} & a_{12} & \cdots & \vdots \\ \vdots & \ddots & & \vdots \\ \vdots & & \ddots & a_{nn} \end{pmatrix} \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} = \begin{pmatrix} v & & 0 \\ & \ddots & \\ 0 & & v \end{pmatrix} \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix}$$

$\Rightarrow vI - (a_{ij})$ has $\begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix}$ in its kernel, so it has zero determinant

$\Rightarrow v^n +$ lower deg terms $= 0 \Rightarrow v$ is integral over R. $\square$

Cor: The set of elements of S that are integral over R is a subring of S containing R (called the <u>integral</u> <u>closure</u> of R in S).

Pf: a, b integral over R.

$\Rightarrow R[a]$ module-finite over R, and b integral over $R[a]$

$\Rightarrow R[a,b]$ is module-finite over $R[a]$ and thus over R.

If $R' = R[a,b]$ and $v = ab$ or $a \pm b$ and we apply the

Prop, v is integral over R. $\square$

Cor: Suppose S is ring-finite over R. Then

S module-finite over $R \iff S$ integral over R.

Pf: Assume S module-finite over R.

Then if $a \in S$, $R[a] \subseteq S$, so a is integral over R. (3.) $\Rightarrow$ 1.))

Thus, S is integral over R.

Now assume S is integral over R.
If we write $S = R[v_1, \ldots, v_n]$, then $R[v_1]$ is mod-finite over R.

Assume $R[v_1, \ldots, v_k]$ is mod-finite over R.

v_{k+1} is integral over $R[v_1, \ldots, v_k]$ so $R[v_1, \ldots, v_{k+1}]$ is module-finite over $R[v_1, \ldots, v_k]$, and thus over R.

Done by induction. $\square$

Fields

If $K \subseteq L$ are fields, $K(v_1, \ldots, v_n)$ is the field of fractions/quotient field of $K[v_1, \ldots, v_n]$ (also the smallest field containing $K, v_1, \ldots, v_n$).

Def: L is a <u>finitely generated field extension</u> of K if

$L = K(v_1, \dots, v_n)$ for some $v_1, \dots, v_n \in L$.

L is an <u>algebraic extension</u> of K if all the elements of L are algebraic over K.

<u>Ex:</u> $\mathbb{Q}[\sqrt{5}] \left(= \mathbb{Q}(\sqrt{5})\right)$ is an algebraic extension of $\mathbb{Q}$ (elts of the form $\alpha + \beta\sqrt{5}$, $\alpha, \beta \in \mathbb{Q}$). In fact it's module-finite over $\mathbb{Q}$.

$\mathbb{Q}(\pi)$ is not algebraic$/\mathbb{Q}$.

<u>Check:</u> If $K \subseteq L$ are fields, then the elements of K that are algebraic over K form a subfield.

<u>Claim:</u> Although $k(x)$ is a finitely generated field extension of k, it's not ring-finite over k.

<u>Pf:</u> Suppose $k(x) = k[v_1, \dots, v_n]$.

Then $\exists\ b \in k[x]$ s.t. $bv_i \in k[x]\ \forall\ v_i$ (i.e. clear denominators)

Let $c \in k[x]$ be irreducible s.t. c doesn't divide b.

We can write $\frac{1}{c}$ as a k-linear combination of monomials in the v_i's.

$\Rightarrow \exists\ N > 0$ s.t. $\frac{b^N}{c} \in k[x]$, a contradiction. $\square$

Claim: $k[x]$ is its own integral closure in $k(x)$.

Pf: Let $z \in k(x)$ integral over $k[x]$.

Thus $z^n + a_{n-1}z^{n-1} + \dots + a_0 = 0$, $a_i \in k[x]$.

If we write $z = \frac{f}{g}$, $f, g \in k[x]$ rel. prime, then multiplying through by g^n we get:

$$f^n + \underbrace{a_{n-1}f^{n-1}g + \dots + a_0 g^n}_{\text{divisible by } g} = 0 \Rightarrow g \text{ divides } f^n \text{ so } g \in k. \quad \square$$

Now we need one big theorem before we can finish the proof of the Nullstellensatz:

Thm: Let $K \subset L$ be fields. If L is ring-finite over K, then L is module-finite (and thus algebraic) over K.

Pf: Let $L = K[v_1, \dots, v_n]$. We'll prove by induction on n.

If $n = 1$, consider $K[x] \twoheadrightarrow K[v_1]$
$x \longmapsto v_1$

$K[v_1]$ is a field, so $K[v_1] \cong K[x]/(f)$, $f \neq 0$.

Thus $f(v_1) = 0 \Rightarrow v_1$ is algebraic over $K \Rightarrow K[v_1]$ is module-finite over K.

Now assume the statement holds for extensions gen. by $n-1$ elts.

Then $L = K(v_1)[v_2, \dots, v_n]$ is module-finite over $K(v_1)$

$\Rightarrow L$ algebraic over $K(v_1)$.

Case 1: v_1 algebraic over K. Then $K(v_1)$ is alg. over K.

By transitivity of integrality, L is algebraic and thus module-finite over K, and we're done.

Case 2: v_1 not algebraic over K.

Then $K(x) \cong K(v_1)$ (exercise)

Each v_i satisfies $v_i^{n_i} + a_{i1} v_i^{n_i - 1} + \dots + a_{in} = 0$, $a_{ij} \in K(v_1)$

Choose $a \in K[v_1]$ that is a multiple of all denominators of the a_{ij}. Multiplying by a^{n_i}, we get

$(av_i)^{n_i} + aa_{i1}(av_i)^{n_i - 1} + \dots = 0$, where all coeffs are now in $K[v_1]$.

Thus av_i is integral over $K[v_1]$.

Moreover, for $z \in L$, $\exists N > 0$ s.t. $a^N z \in K[v_1][av_2, av_3, \dots, av_n]$.

Thus, since integral elts form a ring $\Rightarrow a^N z$ is integral over $K[v_1]$.

Set $z = \frac{1}{c} \in K(v_1)$ where $c \in K[v_1]$ is rel. prime to a.

Then $\frac{a^N}{c}$ is integral over $K[v_1]$, some $N > 0$. So $\frac{a^N}{c} \in K[v_1]$, a contradiction by the above claim. $\square$

Now we can complete the proof of the Nullstellensatz:

Theorem: If k is algebraically closed and $m \subseteq k[x_1, \dots, x_n] = R$ is a maximal ideal, then $m = (x_1 - a_1, \dots, x_n - a_n)$, where $a_i \in k$.

Pf: Let $L = R/m$. Then L is a field and $k \subseteq L$.

L is ring-finite over k, so L is algebraic over k.

If $z \in L$, then $f(z) = 0$, some $f \in k[x]$. But k is algebraically closed, so $z \in k$. Thus $L = k$.

Thus, for all x_i, $\exists\ a_i \in k$ s.t. $\bar{x}_i = \bar{a}_i$ in $L \Rightarrow x_i - a_i \in m$.

$\Rightarrow (x_1 - a_1, \dots, x_n - a_n) \subseteq m$, but is maximal, so they're equal. $\square$