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 \( k[x_1, \ldots, x_n] \) are of the form \( (x_i - a_i, \ldots, x_n - a_n) \), where \( a_i \in k \).

Rings + Modules

S a ring, \( R \subseteq S \) a subring.

We can treat \( S \) as an \( R \)-module.

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

**Def:** \( S \) is **ring-finite** over \( R \) if \( S = R[v_1, \ldots, v_n] \) for some \( v_1, \ldots, v_n \in S \).

In general, \( R[v_1, \ldots, v_n] \subseteq S \) is the subring generated by \( R, v_1, \ldots, v_n \).

**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) Each of these finiteness properties is a transitive relation
2) Module-finite \( \Rightarrow \) ring-finite
**Ex:** $R[x]$ is ring-finite over $R$ but not module-finite or integral.

\[ \frac{R[x]}{(x^2)} = R + R\overline{x} \] is module-finite over $R$.

**Prop:** $\mathcal{S} \subseteq \mathcal{S}$, $\mathcal{S}$ an integral domain, $v \in \mathcal{S}$. TFAE:

1. $v$ is integral over $R$.
2. $R[v]$ is module-finite over $R$.
3. There's a subring $R' \subseteq \mathcal{S}$ containing $R[v]$ that's module-finite over $R$.

**Pf:**

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

   \[ \Rightarrow v^n \in R + Rv + \ldots + Rv^{n-1} \Rightarrow \text{any power of } v \text{ is in there} \]

   \[ \Rightarrow R[v] \text{ is module-finite.} \]

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

3. $\Rightarrow$ 1.) Suppose $R'$ is gen as an $R$-module by $w_1, \ldots, w_n$. Then $v w_i = a_{i1} w_1 + \ldots + a_{in} w_n$, $a_{ij} \in R$.

\[ (a_{i1} \quad \cdots \quad a_{in}) \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} = \begin{pmatrix} v \\ \vdots \\ 0 \end{pmatrix} \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} \]
\[ vI - (a_{ij}) \text{ has } \begin{pmatrix} w_1 & \vdots & w_n \end{pmatrix} \text{ in its kernel, so it has zero determinant} \]
\[ \implies v^n + \text{lower deg terms} = 0 \implies v \text{ is integral over } R. \qed \]

**Cor:** The set of elements of \( S \) that are integral over \( R \) is a subring of \( S \) containing \( R \) (called the integral closure of \( R \) in \( S \)).

**Pf:** \( a, b \) integral over \( R \).
\[ \implies R[a] \text{ module-finite over } R, \text{ and } b \text{ integral over } R[a] \]
\[ \implies R[a, b] \text{ is module-finite over } R[a] \text{ and thus over } R. \]
If \( R' = R[a, b] \) and \( v = a \cdot b \text{ or } a \pm b \) and we apply the Prop, \( v \) is integral over \( R \). \qed

**Cor:** \( S \) ring-finite over \( R \). Then
\[ S \text{ module-finite over } R \iff S \text{ integral over } R. \]

Assume \( S \) module-finite over \( R \).
Then if \( a \in S \), \( R[a] \subseteq S \), so \( a \) is integral over \( R \).

Now assume \( S \) is integral over \( R \).
If we write \( S = R[v_1, \ldots, v_n] \), then \( R[v_i] \) is mod-finite over \( R \).
Assume \( R[x_1, \ldots, v_k] \) 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 \( R \). 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 **finitely generated field extension of \( K \)** if 
\( L = K(v_1, \ldots, v_n) \) for some \( v_1, \ldots, v_n \in L \).

\( L \) is an **algebraic extension of \( K \)** if all the elements of \( L \) are integral over \( K \).

**Ex:** \( \mathbb{Q}[(\sqrt{5})] \) \( (= \mathbb{Q}(\sqrt{5})) \) 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/\( \mathbb{Q} \).

**Check:** If \( K \subseteq L \) are fields, then the elements of \( K \) that are algebraic over \( K \) form a subfield.

**Claim:** Although \( k(x) \) is a finitely generated field extension of \( k \), it's not ring-finite over \( k \).

**Pf:** Suppose \( k(x) = k[v_1, \ldots, v_n] \).
Thus \( \exists b \in k[x] \) 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.

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

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

**Pf:** let \( z \in k(x) \) integral over \( k[x] \).

Then \( z^n + a_{n-1}z^{n-1} + \ldots + a_0 = 0, a_i \in k[x] \).

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

\[ f^n + a_{n-1}f^{n-1}g + \ldots + a_0g^n = 0 \Rightarrow g \text{ divides } f^n \text{ so } g \in k. \]

Thus 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 \( L = K[v_1, ..., v_n] \). We'll prove by induction on \( n \).

If \( n = 1 \), consider \( K[x] \rightarrow K[v_i] \)

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

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

Now assume the statement holds for extensions gen. by \( n-1 \) elts.

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

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

Case 1: \( v_i \) algebraic over \( K \). Then \( K(v_i) \) is alg. over \( K \).

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

Case 2: \( v_i \) not algebraic over \( K \).

Then \( K(x) \rightarrow K(v_i) \) is injective, so it's an isomorphism.

Each \( v_i \) satisfies \( v_i^{n_i} + a_i v_i^{n_i-1} + ... + a_i n = 0 \), \( a_i \in K(v_i) \).

Choose \( a \in K[v_i] \) that is a multiple of all denominators of the \( a_{ij} \).

Multiplying by \( a^{n_i} \), we get
\[(av_i)^n + qa_{i1}(av_i)^n - 1 + \ldots = 0,\] where all coeffs are now in \(k[v_i].\)

Thus, \(av_i\) is integral over \(k[v_i].\)

Moreover, for \(z \in L, \exists N > 0\) s.t. \(a^Nz \in k[v_i][av_2, av_3, \ldots, av_n].\)

Thus, since integral elts form a ring \(\Rightarrow a^Nz\) is integral over \(k[v_i].\)

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

Then \(\frac{a^N}{c}\) is integral over \(k[v_i]\), some \(N > 0.\) So \(\frac{a^N}{c} \in k[v_i],\)
a contradiction by the above claim. \(\square\)

Now we can prove the following, completing our proof of the Nullstellensatz:

**Thm:** If \(k\) is algebraically closed and \(m \subseteq k[x_1, \ldots, x_n]\) a max'l ideal, then \(m = (x_1 - a_1, \ldots, x_n - a_n),\) where \(a_i \in k.\)

**Pf:** Let \(L = \frac{k[x_1, \ldots, x_n]}{m}.\) \(L\) 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 alg. closed
\(\Rightarrow f = (x - a_1) \ldots (x - a_m),\) \(a_i \in k,\) so \(z = a_i \in k,\) so \(L = k.\)
Thus, \( \forall i \in \mathbb{k} \) s.t. \( \overline{x_i} = \overline{a_i} \) in \( L \Rightarrow x_i - a_i \in \mathfrak{m} \)

\[ (x_1 - a_1, \ldots, x_n - a_n) \subseteq \mathfrak{m}, \text{ but is a maximal ideal, so they're equal.} \]