MATH 221 NOTES: PART 1

YI SUN

Contents

Introduction

These are notes from the course Math 221: Commutative Algebra taught by Professor Dennis Gaitsgory at Harvard University in Fall 2008.

1. The Tensor Product

1.1. **Existence and Uniqueness for Modules.** We wish to construct the tensor product for modules over an arbitrary ring. In this section, let R be a (non necessarily commutative) ring, M a right R-module, and N a left R-module.

Theorem 1.1. There exists an abelian group $M \underset{R}{\otimes} N$ with an associated map $\phi_{\text{univ}} : M \times N \to M \underset{R}{\otimes} N$ such that for any abelian group A and any map $\phi : M \times N \to A$ of abelian groups, there exists a unique map $\psi : M \underset{R}{\otimes} N \to A$ such that $\phi = \psi \circ \phi_{\text{univ}}$.

The group $M \underset{R}{\otimes} N$ is referred to as the *tensor product* of M and N, and the property is referred to as the *universal property of tensor products.* We call elements in the image of ϕ_{univ} pure tensors and we denote $m \otimes n := \phi_{\text{univ}}(m, n)$. The tensor product also satisfies the following naturality property.

Proposition 1.2. Let $T : M_1 \to M_2$ be a map of right R-modules and N a left R-module. Assume that $M_1 \underset{R}{\otimes} M_2$ and $M_2 \underset{R}{\otimes} N$ exist. Then, there exists a unique map $T \underset{R}{\otimes} N : M_1 \underset{R}{\otimes} N \to M_2 \underset{R}{\otimes} N$ such that $\phi_{2,\text{univ}} = (T \underset{R}{\otimes} N) \circ \phi_{1,\text{univ}}$.

Proof. Apply the universal property of $M_1 \underset{R}{\otimes} N$ to the map $M_1 \times N \to M_2 \underset{R}{\otimes} N$ given by $(m, n) \mapsto \phi_{2,\text{univ}}(T(m), n)$. □

Example. Suppose that $M = R$. Then, for any N, take $R \underset{R}{\otimes} N := N$ and $\phi_{\text{univ}} : R \times N \to N$ given by $(r, n) \mapsto r \cdot n$.

Lemma 1.3. The pair (N, ϕ_{univ}) as defined above satisfies the universal property of the tensor product, meaning that $N = R \underset{R}{\otimes} N$.

Proof. Given $\phi : R \times N \to A$, we can take $\psi(n) = \phi(1, n)$. □

Before we prove Theorem 1.1, we recall some preliminaries about modules.

Definition. Let I be a set, and for each $i \in I$, let M_i be a right R-module. Then, for any right R-module M, their *direct sum* $\bigoplus_{i \in I} M_i$ satisfies the universal property

$$\operatorname{Hom}_R\left(\bigoplus_{i \in I} M_i, M\right) = \prod_{i \in I} \operatorname{Hom}_R(M_i, M).$$

Definition. Let I be a set, and for each $i \in I$, let M_i be a right R-module. Then, for any right R-module M, their *direct product* $\prod_{i \in I} M_i$ satisfies the universal property

$$\operatorname{Hom}_R\left(M, \prod_{i \in I} M_i\right) = \prod_{i \in I} \operatorname{Hom}_R(M, M_i).$$

Recall that the direct sum is realized as the set of assignments $i \mapsto m_i \in M_i$ with $m_i = 0$ for all but finitely many i, and the direct product is realized as the set of all assignments $i \mapsto m_i \in M_i$. Recall also that the direct sum and direct product are isomorphic for finite sets I.

We will now show that the tensor product is nicely behaved under some common operations.

Lemma 1.4. If $M_i \underset{R}{\otimes} N$ exists for all $i \in I$, then $\left(\bigoplus_{i \in I} M_i\right) \underset{R}{\otimes} N$ also exists.

Proof. Let ϕ^i_{univ} be the universal map for each $M_i \underset{R}{\otimes} N$ and let $M = \bigoplus_{i \in I} M_i$. We will claim that

$$\left(\bigoplus_{i \in I} M_i\right) \underset{R}{\otimes} N := \bigoplus_{i \in I} (M_i \underset{R}{\otimes} N)$$

satisfies the universal property with the universal map $\phi_{\text{univ}} : M \times N \to \bigoplus_{i \in I} (M_i \underset{R}{\otimes} N)$ given by

$$\phi_{\text{univ}}(\oplus\, m_i, n) \mapsto \oplus\, \phi^i_{\text{univ}}(m_i, n).$$

We can easily verify that the universal property holds for this map. □

From Lemmas 1.3 and 1.4, then, we see that

$$\left(\bigoplus_{I} R\right) \underset{R}{\otimes} N = \bigoplus_{I} N.$$

We now construct the tensor product for cokernels via the following lemma:

Lemma 1.5. Let $M_1 \xrightarrow{T} M_2 \to M_2 \to M_3 \to 0$ be short exact, and suppose that $M_1 \underset{R}{\otimes} N$ and $M_2 \underset{R}{\otimes} N$ exist. Then, $M_3 \underset{R}{\otimes} N$ also exist and is isomorphic to $\operatorname{coker}(M_1 \underset{R}{\otimes} N \to M_2 \underset{R}{\otimes} N)$.

Proof. Take $\phi_{3,\text{univ}} : M_3 \times N \to \operatorname{coker}(M_1 \underset{R}{\otimes} N \to M_2 \underset{R}{\otimes} N)$ as follows: Given $(m_3, n) \in M_3 \times N$, let m_2 be a preimage of m_3 in M_2. Consider $\phi_{2,\text{univ}}(m_2, n) \in M_2 \underset{R}{\otimes} N$ and project it to $\operatorname{coker}(M_1 \underset{R}{\otimes} N \to M_2 \underset{R}{\otimes} N)$.

We first claim that $\phi_{3,\text{univ}}$ is well-defined. It suffices to check that $\phi_{2,\text{univ}}(T(m_1), n) \in \operatorname{Im}(T \underset{R}{\otimes} N)$. But indeed $\phi_{2,\text{univ}}(T(m_1), n) = (T \underset{R}{\otimes} N)(\phi_{1,\text{univ}}(m_1, n))$.

We now check the universal property. Take any bilinear map $\phi : M_3 \times N \to A$. Observe that a map $\psi : \operatorname{coker}(M_1 \underset{R}{\otimes} N \to M_2 \underset{R}{\otimes} N) \to A$ is equivalent to a map $\psi_2 : M_2 \underset{R}{\otimes} N \to A$ such that $\psi_2 \circ (T \underset{R}{\otimes} N) = 0$. Now, consider the following diagram:

$$\begin{array}{ccccccc}
M_1 \times N & \xrightarrow{T \times \text{id}} & M_2 \times N & \xrightarrow{\pi \times \text{id}} & M_3 \times N & \xrightarrow{\phi} & A \\
\downarrow{\scriptstyle \phi_{1,\text{univ}}} & & \downarrow{\scriptstyle \phi_{2,\text{univ}}} & & & \nearrow{\scriptstyle \psi_2} & \\
M_1 \underset{R}{\otimes} N & \xrightarrow{T \underset{R}{\otimes} N} & M_2 \underset{R}{\otimes} N & & & &
\end{array}$$

Observe that $\phi \circ (\pi \times \text{id})$ is a bilinear map $M_2 \times N \to A$, so it lifts to a map $\psi_2 : M_2 \underset{R}{\otimes} N \to A$. Now, note that

$$\psi_2 \circ (T \underset{R}{\otimes} N) \circ \phi_{1,\text{univ}} = \psi_2 \circ \phi_{2,\text{univ}} \circ (T \times \text{id}) = \phi \circ (\pi \circ \text{id}) \circ (T \times \text{id}) = 0,$$

which means that $\psi_2 \circ (T \underset{R}{\otimes} N)$ is induced by the zero map $M_1 \times N \to A$, so it must itself be zero. Observe now that the ψ corresponding to this ψ_2 satisfies the desired property. $\square$

Finally, we wish to establish that all modules can be written as cokernels via the following lemma:

Lemma 1.6. Every module is the quotient of some free module.

Proof. For a module M over a ring R, consider the free module $N = \bigoplus_M R$ and the map $N \twoheadrightarrow M$ that sends the m^{th} coordinate r_m to m. This is surjective, giving the desired representation. $\square$

Corollary 1.7. Every module can be written as the cokernel of a map of free modules.

Proof. Given a module M, by Lemma 1.6, choose I giving a surjection $\bigoplus_I R \twoheadrightarrow M$. Let M' be the kernel of the map $\bigoplus_I R \twoheadrightarrow M$, and choose J giving a surjection $\bigoplus_J R \twoheadrightarrow M'$. Then, we have the exact sequence

$$\bigoplus_J R \twoheadrightarrow M' \hookrightarrow \bigoplus_I R \twoheadrightarrow M' \to 0,$$

meaning that M' is the cokernel of the map $\bigoplus_J R \to \bigoplus_I R$. $\square$

We are now ready to put everything together to prove the existence of the tensor product.

Proof of Theorem 1.1. First, by Lemmas 1.3 and 1.4, we know that the tensor product $M \underset{R}{\otimes} N$ exists for M a free module. Now, if M is not a free module, write $M = \operatorname{coker}(\bigoplus_J R \to \bigoplus_I R)$ for some I and J by Corollary 1.7. Because $(\bigoplus_J R) \underset{R}{\otimes} N$ and $(\bigoplus_I R) \underset{R}{\otimes} N$ exist, we have by Lemma 1.5 that $M \underset{R}{\otimes} N$ exists, establishing the theorem. $\square$

Corollary 1.8. If $M_1 \twoheadrightarrow M_2$ is a surjection, then $M_1 \underset{R}{\otimes} N \to M_2 \underset{R}{\otimes} N$ is a surjection.

Proof. Recall that a map $T : A_1 \to A_2$ is a surjection in the categorical sense, if for every object A and map $S : A_2 \to A$, then $S \circ T = 0$ implies that $S = 0$. Now, consider the following diagram:

$$\begin{array}{ccccc} M_1 \times N & \xrightarrow{T \times N} & M_2 \times N & & \\ \downarrow & & \downarrow & \overset{\phi_2}{\searrow} & \\ M_1 \underset{R}{\otimes} N & \xrightarrow{T \underset{R}{\otimes} N} & M_2 \underset{R}{\otimes} N & \xrightarrow[\psi_2]{} & A \end{array}$$

Suppose that $T : M_1 \twoheadrightarrow M_2$ is a surjection, so $T \times N$ is a surjection. Now, take any A and $\psi_2 : M_2 \underset{R}{\otimes} N \to A$. Then, we see that $\psi_2 \circ (T \underset{R}{\otimes} N) = 0 \iff \phi_2 \circ (T \times N) = 0 \iff \phi_2 = 0 \iff \psi_2 = 0$, as needed. □

Having established the existence of the tensor product, we now wish to consider its uniqueness, given by the following lemma.

Lemma 1.9. If $(M \underset{R}{\otimes} N)'$ and $M \underset{R}{\otimes} N$ satisfy the universal property of $M \underset{R}{\otimes} N$, then they are canonically isomorphic.

Proof. Consider the following diagram:

$$\begin{array}{ccc} M \times N & \xrightarrow{\phi'_{\text{univ}}} & (M \underset{R}{\otimes} N)' \\ & \underset{\phi_{\text{univ}}}{\searrow} & \uparrow \downarrow \\ & & M \underset{R}{\otimes} N \end{array}$$

By the universal property, we obtain maps $\psi' : (M \underset{R}{\otimes} N)' \to M \underset{R}{\otimes} N$ and $\psi : M \underset{R}{\otimes} N \to (M \underset{R}{\otimes} N)'$ such that $\psi' \circ \phi'_{\text{univ}} = \phi_{\text{univ}}$ and $\psi \circ \phi_{\text{univ}} = \phi'_{\text{univ}}$. This means that $(\psi' \circ \psi) \circ \phi_{\text{univ}} = \phi_{\text{univ}}$. Observe that $\psi' \circ \psi \circ \phi_{\text{univ}} : M \times N \to M \underset{R}{\otimes} N$ is a bilinear map which factors through the identity map $M \underset{R}{\otimes} N \to M \underset{R}{\otimes} N$. By the universal property, this factorization is unique, so $\psi' \circ \psi = \text{id}$. Similarly, $\psi \circ \psi' = \text{id}$, as desired. □

Note that to compute the tensor product in practice, one should find I, J small so that $M = \text{coker}(\bigoplus_J R \to \bigoplus_I R)$. Now, note that if $\bigoplus_J R \to \bigoplus_I R \to M \to 0$ is exact, then tensoring with the right exact functor $- \underset{R}{\otimes} N$ gives the exact sequence

$$\bigoplus_J N \to \bigoplus_I N \to M \underset{R}{\otimes} N \to 0.$$

We now wish to discuss the relation between the tensor product and various homomorphisms of rings. Given a ring homomorphism $\phi : A \to B$, if M is a B-module, we can view it as an A-module with action induced by ϕ. Note that we can view $B \underset{A}{\otimes} N$ as a B-module via the natural action of B on itself.

Lemma 1.10. If N is an A-module, $B \underset{A}{\otimes} N$ has the structure of B-module such that for every B-module M, we have a natural isomorphism $\text{Hom}_A(N, M) \simeq \text{Hom}_B(B \underset{A}{\otimes} N, M)$.

Proof. For any map $B \underset{A}{\otimes} N \to M$, take the corresponding $\phi : B \times N \to M$ and map it to $\phi' : N \to M$ given by $\phi'(n) = \phi(1, n)$. Map $\psi : N \to M$ to $\psi' : B \underset{A}{\otimes} N \to M$ given by $\psi'(b \otimes n) = b \cdot \psi(n)$. It's easy to check that these maps define the desired isomorphism. □

Lemma 1.11. Let R_1, R_2 be rings, L a right R_1-module, M a (R_1, R_2)-bimodule, and N a left R_2-module. Then, $M \underset{R_2}{\otimes} N$ is a left R_1-module.

Proof. We need to construct a map $R_1 \to \mathrm{End}_{\mathbb{Z}}(M \underset{R_2}{\otimes} N)$. We have a map $R_1 \to \mathrm{End}_{R_2}(M)$ because M is a left R_1-module. The desired action then follows from the functoriality of $- \underset{R_2}{\otimes} N$. □

Note further that $L \underset{R_1}{\otimes} (M \underset{R_2}{\otimes} N) \simeq (L \underset{R_1}{\otimes} M) \underset{R_2}{\otimes} N$. Observe also that we can obtain another proof of Lemma 1.10 by viewing $A \to B$ as a map of right A-modules and using the functoriality of $- \underset{A}{\otimes} N$.

1.2. **Flat Modules.** We now investigate the exactness of the tensor product more closely. Let $M_1 \hookrightarrow M_2$ be an injection of right R-modules.

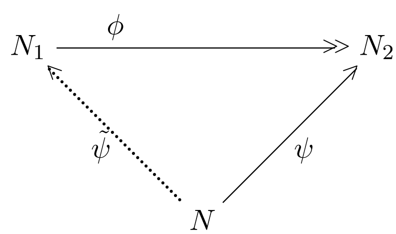
Claim. $M_1 \underset{R}{\otimes} N \to M_2 \underset{R}{\otimes} N$ need not always be injective.

Proof. Take $R = M_1 = M_2 = \mathbb{Z}$ with the map $M_1 \overset{2}{\hookrightarrow} M_2$ given by multiplication. Now let $N = \mathbb{Z}/2\mathbb{Z}$. In this case, we see that $M_1 \underset{R}{\otimes} N = M_2 \underset{R}{\otimes} N = \mathbb{Z}/2\mathbb{Z}$, where the map $M_1 \underset{R}{\otimes} N \to M_2 \underset{R}{\otimes} N$ is given by multiplication by 2. Hence, it is the zero map, which is not injective. □

Definition. A left R-module N is called *flat* if the functor $- \underset{R}{\otimes} N$ is left exact (i.e., it transforms injections to injections).

Example. All free modules are flat because tensor products distribute over direct sums.

1.3. **Projective Modules.** Now, consider the following situation. Let $\phi : N_1 \twoheadrightarrow N_2$ be a surjection of modules and $\psi : N \to N_2$ a map. We wish to determine when there exists a lift $\tilde{\psi} : N \to N_1$ so that $\phi \circ \tilde{\psi} = \psi$.



Observe that such a lift always exists when we are working over a field (i.e., N, N_1, N_2 are vector spaces). However, for $R = \mathbb{Z}$, $N_1 = \mathbb{Z}$, and $N_2 = N = \mathbb{Z}/2\mathbb{Z}$, it does not.

Definition. A module N is called *projective* if, for any surjection $N_1 \twoheadrightarrow N_2$, any map $N \to N_2$ can be lifted to a map $N \to N_1$.

Example. (1) $N = R$ is projective
(2) If $\{N_i\}$ are projective, then so is $\bigoplus_{i \in I} N_i$.

Lemma 1.12. Let P be projective, and let P_1 be a direct summand of P (i.e. we can write $P = P_1 \oplus P_2$). Then, P_1 is projective.

Proof. Take a surjection $N_1 \twoheadrightarrow N_2$ and suppose we have a map $\phi : P_1 \to N_2$. Then, ϕ extends to a map $\tilde{\phi} : P \to N_2$ by sending P_2 to zero. We can then finish the proof by using the lifting property of P. □

Proposition 1.13. Any projective module is a direct summand of a free module.

Proof. Recall that we can take a surjection $\phi : \bigoplus_I R \twoheadrightarrow P$ for some I. Then, lift the identity map $\mathrm{id} : P \to P$ to $\bigoplus_I R$. Thus, ϕ is a surjection with a left inverse, meaning exactly that its image P is a direct summand of $\bigoplus_I R$. □

Corollary 1.14. Any projective module is flat.

Corollary 1.15. Any vector space is free, hence projective and flat.

1.4. **The Commutative Case.** From this point onwards, we take our rings to be commutative. Let R be a commutative ring and recall that every R-module M is equipped with an R-action $\mathrm{act} : R \times M \to M$ such that $\mathrm{act}(r_1, \mathrm{act}(r_2, m)) = \mathrm{act}(r_1 \cdot r_2, m)$. If R is commutative, then every left or right module is automatically a bi-module under the identification $r \cdot m = m \cdot r$. From now on, we will simply refer to such modules as R-modules.

Remark. It is not true that every R-bimodule comes from such a construction. Observe that $R \underset{\mathbb{Z}}{\otimes} R$ is a R-bimodule, but evidently the actions on the left and right are distinct.

Now, let M, N be R-modules; then, $M \underset{R}{\otimes} N$ acquires a priori two R-module structures, as we can either view it as a left R-module or a right R-module.

Lemma 1.16. These two structures coincide.

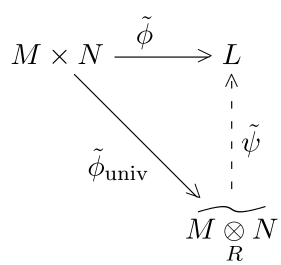
Proof. It suffices to show that the left and right actions of R on $M \underset{R}{\otimes} N$ coincide. This is a consequence of the following equalities: $r \cdot (m \otimes n) = (r \cdot m) \otimes n = (m \cdot r) \otimes n = m \otimes (r \cdot n) = m \otimes (n \cdot r) = (m \otimes n) \cdot r$. □

We now construct the tensor product over a commutative ring in a functorial manner. Given a map $\tilde{\phi} : M \times N \to L$ for R-modules M, N, L, we say that $\tilde{\phi}$ is bilinear if it satisfies the conditions:

$$\tilde{\phi}(m_1 + m_2, n) = \tilde{\phi}(m_1, n) + \tilde{\phi}(m_2, n)$$
$$\tilde{\phi}(m, n_1 + n_2) = \tilde{\phi}(m, n_1) + \tilde{\phi}(m, n_2)$$
$$\tilde{\phi}(rm, n) = r\tilde{\phi}(m, n) = \tilde{\phi}(m, rn).$$

We can now define the tensor product of commutative rings.

Definition. Let R be a commutative ring. For R-modules M and N, the R-module $\widetilde{M \underset{R}{\otimes} N}$ is a R-module equipped with a bilinear map $\tilde{\phi}_{\mathrm{univ}} : M \times N \to \widetilde{M \underset{R}{\otimes} N}$ satisfying the following universal property: Any bilinear map of R-modules $\tilde{\phi} : M \times N \to L$ factors through a map of R-modules $\tilde{\psi} : \widetilde{M \underset{R}{\otimes} N} \to L$ such that the following diagram commutes:



Theorem 1.17. For any R-modules M and N, the tensor product $\widetilde{M \underset{R}{\otimes} N}$ exists.

Proof. View M as a right R-module and N as a left R-module. Take $\widetilde{M \underset{R}{\otimes} N} := M \underset{R}{\otimes} N$ with $\tilde{\phi}_{\text{univ}} = \phi_{\text{univ}} : M \times N \to M \underset{R}{\otimes} N$. Now, consider any bilinear map $\tilde{\phi} : M \times N \to L$. By the universal property of the $M \underset{R}{\otimes} N$, we have a map of a abelian groups $\psi : M \underset{R}{\otimes} N \to L$ such that $\tilde{\phi} = \psi \circ \tilde{\phi}_{\text{univ}}$. It remains only to check that ψ is actually a map of R-modules, which follows from the fact that $\psi(r \cdot (m \otimes n)) = r \cdot \psi(m \otimes n)$. □

Now, let $M_1, M_2, \ldots, M_n$ be a finite collection of R-modules We want to construct the R-module

$$M_1 \underset{R}{\otimes} M_2 \underset{R}{\otimes} \cdots \underset{R}{\otimes} M_n.$$

Given a map $\phi : M_1 \times M_2 \times \cdots \otimes M_n \to L$, we say that ϕ is multilinear if it is

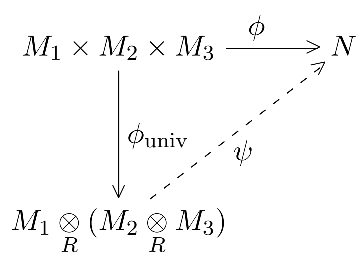
- Additive in each argument
- $\phi(rm_1, m_2, \ldots, m_n) = \phi(m_1, rm_2, \ldots, m_n) = \cdots = \phi(m_1, \ldots, m_{n-1}, rm_n) = r \cdot \phi(m_1, \ldots, m_n)$

Definition. For R-modules $M_1, \ldots, M_n$, the tensor product $M_1 \underset{R}{\otimes} M_2 \underset{R}{\otimes} \cdots \underset{R}{\otimes} M_n$ is a R-module equipped with a multilinear map $\phi_{\text{univ}} : M_1 \times \cdots \times M_n \to M_1 \underset{R}{\otimes} \cdots \underset{R}{\otimes} M_n$ satisfying the following universal property: For any R-module L and any multilinear map $\phi : M_1 \times \cdots \times M_n \to L$, there exists a map $\psi : M_1 \underset{R}{\otimes} \cdots \underset{R}{\otimes} M_n \to L$ of R-modules such that $\psi \circ \phi_{\text{univ}} = \phi$.

We wish to show that this tensor product also exists for all n. Here we will just demonstrate the proof in the case where $n = 3$.

Proposition 1.18. The tensor product $M_1 \underset{R}{\otimes} M_2 \underset{R}{\otimes} M_3$ is given by $M_1 \underset{R}{\otimes} (M_2 \underset{R}{\otimes} M_3)$ with the universal map $\phi_{\text{univ}} : M_1 \times M_2 \times M_3 \to M_1 \underset{R}{\otimes} (M_2 \underset{R}{\otimes} M_3)$ given by $(m_1, m_2, m_3) \mapsto m_1 \otimes (m_2 \otimes m_3)$.

Proof. It suffices to show that for any trilinear $\phi : M_1 \times M_2 \times M_3 \to N$ in the following diagram, we have a factorization ψ.



Taking $\psi = m_1 \otimes (m_2 \otimes m_3) \mapsto \phi(m_1, m_2, m_3)$ finishes the proof. □

Note finally that if R is commutative, we have an isomorphism $M_1 \underset{R}{\otimes} M_2 \simeq M_2 \underset{R}{\otimes} M_1$ given by exchanging the order of factors.

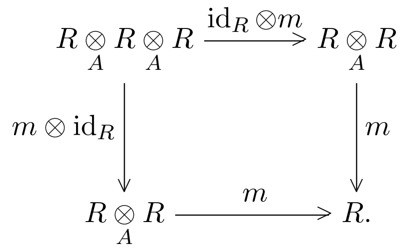
1.5. **For Algebras.** Let A be a commutative ring.

Definition. An A-*module* is a ring R with an additional structure of an A-module such that $(r_1 a) \cdot r_2 = r_1(a \cdot r_2)$.

Claim. For an A-module R, a structure of an A-algebra on R is equivalent to a map of R-modules

$$R \underset{A}{\otimes} R \overset{m}{\twoheadrightarrow} R$$

such that the following diagram commutes

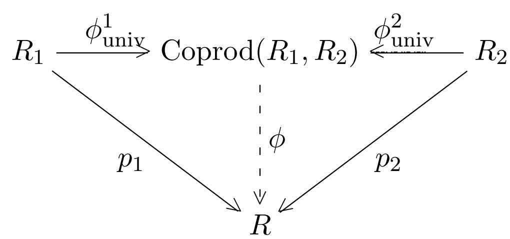


Example. Let $\phi : A \to R$ be a map of rings such that $\phi(A)$ is central. Then, R is naturally an A-algebra under $a \cdot r = \phi(a) \cdot r$.

We now wish to define the notion of the tensor product of A-algebras. This will be the *coproduct* in the category of A-algebras. Let R_1, R_2 be A-algebras.

Definition. In the unital case, the coproduct of R_1 and R_2 is another A-algebra $\mathrm{Coprod}(R_1, R_2)$ equipped with two maps $\phi^1_{\mathrm{univ}} : R_1 \to \mathrm{Coprod}(R_1, R_2)$ and $\phi^2_{\mathrm{univ}} : R_2 \to \mathrm{Coprod}(R_1, R_2)$ such that, for any A-algebra R equipped with maps $p_1 : R_1 \to R$ and $p_2 : R_2 \to R$ whose images commute, we obtain a unique map $\phi : \mathrm{Coprod}(R_1, R_2) \to R$ such that $\phi \circ \phi^1_{\mathrm{univ}} = p_1$ and $\phi \circ \phi^2_{\mathrm{univ}} = p_2$.

In other words, for maps p_1, p_2 with commuting images in the following diagram, there is a unique factoring map ϕ:



Definition. In the non-unital case, we can give $R_1 \underset{A}{\otimes} R_2$ the structure of an A-algebra via

$$(R_1 \underset{A}{\otimes} R_2) \underset{A}{\otimes} (R_1 \underset{A}{\otimes} R_2) \to (R_1 \underset{A}{\otimes} R_1) \underset{A}{\otimes} (R_2 \underset{A}{\otimes} R_2) \to R_1 \underset{A}{\otimes} R_2.$$

In other words, the multiplication is given by $(r_1' \otimes r_2') \cdot (r_1'' \otimes r_2'') = (r_1' \cdot r_1'') \otimes (r_2' \cdot r_2'')$.

2. Finite Generation

2.1. **Finitely Generated Modules.** Let M be a left R-module.

Definition. We say that M is *finitely generated* if there exists a surjection $R^{\oplus n} \twoheadrightarrow M$.

Lemma 2.1. Let $0 \to M_1 \to M_2 \to M_3 \to 0$ be a short exact sequence. If M_1, M_3 are finitely generated, then so is M_2.

Proof. Take surjections $R^{n_1} \twoheadrightarrow M_1$ and $R^{n_3} \twoheadrightarrow M_3$. Because R^{n_3} is free and hence projective, we can lift to a map $R^{n_3} \to M_2$. Now, this map, together with the composition of maps $R^{n_1} \to M_1 \to M_2$, determines a map $R^{n_1} \oplus R^{n_3} \to M_2$. We wish to show that this is surjective. Observe that its image contains the image of M_1 in M_2; further, it projects to all of M_3, so it must be all of M_2, giving the desired surjectivity. ☐

Definition. We say that R is *left Noetherian* if every left ideal $I \subset R$ is finitely generated. We say that M is *left Noetherian* if every submodule of M is finitely generated.

Theorem 2.2. The following conditions are equivalent:

(a) R is left Noetherian.

(b) Any finitely generated R-module is Noetherian.

Proof. (b) $\implies$ (a). This follows because an ideal $I \subset R$ is a submodule of R.
(a) $\implies$ (b). We first claim that it is enough to consider $M = R^n$, since every finitely generated module is a quotient of R^n for some n.

We induct on n. The base case $n = 1$ is provided by (2). Now suppose the claim is shown for $m < n$ and consider some submodule $M \subset R^n$. Then, consider the following diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & R^{n-1} & \longrightarrow & R^n & \longrightarrow & R & \longrightarrow & 0 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 0 & \longrightarrow & M_2 = R^{n-1} \cap M & \longrightarrow & M & \longrightarrow & M_1 & \longrightarrow & 0 \end{array}$$

where $M_1 = M/(M \cap R^{n-1})$. Note that M_2 is finitely generated by the inductive hypothesis, and M_1 is an ideal of R, hence finitely generated. Now by Lemma 2.1, M is finitely generated, finishing the induction. □

Theorem 2.3. The following conditions are equivalent:

(a) M is Noetherian.
(b) For any sequence $M_1 \subset M_2 \subset \cdots$ of submodules of M, there exists an N such that $M_i = M_N$ for all $i > N$.

Proof. (a) $\implies$ (b). Notice that $L = \bigcup_i M_i$ is also a submodule of M. By (a), we may choose a finite set of generators $\{l_i\}$ for L. Since $\bigcup_i M_i = L$, we must have that $l_i \in M_{j_i}$ for some j_i. Letting $j = \max\{j_i\}$, we see that $M_j = L$, so we may take $N = j$ to get the conclusion.
(b) $\implies$ (a). Suppose for contradiction that we had some submodule L of M that was not finitely generated. Now, construct a sequence of elements $\{l_i\}$ of L as follows. Choose l_1 arbitrarily and take $l_{i+1} \in L - \text{span}\{l_1, \ldots, l_i\}$; note that the last set is non-empty by our assumption that L was not finitely generated. Now, take $L_i = \text{span}\{l_1, \ldots, l_i\}$ and notice that we have $L_1 \subset L_2 \subset \cdots$. By condition (b), we may find some N such that $L_i = L_N$ for $i > N$, which is a contradiction, because $l_{N+1} \notin L_N$ by our choice of $\{l_i\}$. Hence L must be finitely generated, so M is Noetherian as desired. □

Example. Any field k is Noetherian.

Lemma 2.4. If we have a surjection $\phi : A \twoheadrightarrow B$, then A Noetherian implies B Noetherian.

Proof. For any ideal $I \subset B$, note that $\phi^{-1}(I) \subset A$ is finitely generated, and the projections of the generators of $\phi^{-1}(I)$ generate I. □

Theorem 2.5 (Hilbert Basis Theorem)**.** If A is Noetherian, then $A[x]$ is Noetherian.

Proof. Take any ideal $I \subset A[x]$. First, let $J \subset A$ be the ideal generated by the highest degree coefficients of elements of I. Let $a_1, \ldots, a_n$ be generators for J (these exist because A is Noetherian). Let $f_1, \ldots, f_n$ be polynomials in $A[x]$ such that a_i is the highest degree coefficient in f_i. Let $d = \max\{\deg(f_1), \ldots, \deg(f_n)\}$. Consider $I \cap (A[x])^{\leq d}$, which is finitely generated as a submodule of A^{d+1}; let $g_1, \ldots, g_m$ be a set of generators.

Now, we claim that $f_1, \ldots, f_n, g_1, \ldots, g_m$ generate I. Suppose otherwise for contradiction. Let $f \in I$ be an element of minimal degree not belonging to the $A[x]$-submodule generated by $f_1, \ldots, f_n, g_1, \ldots, g_m$. First, note that $\deg(f) > d$. Observe now that the leading coefficient a of f belongs to J, so we can write $a = \sum_i c_i a_i$ for some coefficients c_i. Then, consider

$$f - \sum_i c_i f_i x^{\deg(f) - \deg(f_i)},$$

which is an element of degree less than $\deg(f)$ in I which does not belong to the $A[x]$-submodule generated by $f_1, \dots, f_n, g_1, \dots, g_m$. This is a contradiction, completing the proof. $\square$

For the rest of this section, all rings will be Noetherian and commutative. Consider a map $A \to B$ of rings.

Definition. We say that B is *A-finite* or *finite as an A-module* if there exists a surjection $A^n \twoheadrightarrow B$ of A-modules.

Definition. We say that B is *finite over A* or *finite as an A-algebra* if there exists a surjection $A[x_1, \dots, x_n] \twoheadrightarrow B$ of A-algebras.

Lemma 2.6. For maps $A \to B \to C$, if C is finite over B and B is finite over A, then C is finite over A.

Proof. Let the maps be $\phi : A \to B$ and $\psi : B \to C$. Take a (finite) set of generators $\{c_i\}$ for C over B, and a set of generators $\{b_j\}$ for B over A. Then, for any $c \in C$, we can write

$$c = \sum_{i=1}^{n} \psi(b^i) \cdot c_i = \sum_{i=1}^{n} \psi \left(\sum_{j=1}^{m} \phi(a^{ij}) \cdot b_j \right) \cdot c_i = \sum_{i=1}^{n} \sum_{j=1}^{m} \psi(\phi(a^{ij}))\psi(b_j) \cdot c_i,$$

for some $a^{ij} \in A$; hence, $\{\psi(b_j) \cdot c_i\}$ is a finite set of generators for C over A. $\square$

Definition. For $b \in B$, take a homomorphism $\phi : A[x] \to B$ given by $\phi(x) = b$. We say that b is *integral* over A if $\mathrm{Im}(\phi)$ is finite as an A-module.

Lemma 2.7. The following are equivalent:

(1) b is integral over A.
(2) B satisfies a monic polynomial equation in A. i.e., there exist $a_0, \dots, a_{n-1} \in A$ such that
$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0.$$

Proof. (2) $\implies$ (1): Note that $\mathrm{Im}(\phi)$ is generated by $\{1, b, \dots, b^{n-1}\}$.
(1) $\implies$ (2): Take $M_i = \mathrm{span}\{1, \dots, b^i\}$. We have that $\bigcup_i M_i = \mathrm{Im}(\phi)$; further, M_i will eventually contain all generators of $\mathrm{Im}(\phi)$, so we can find some n with $\mathrm{Im}(\phi) = M_n$; in particular, this means that b^{n+1} is generated by $1, b, \dots, b^n$, finishing the proof. $\square$

Lemma 2.8. Suppose that $b_1, \dots, b_n$ are integral over A and let $\phi_n : A[x_1, \dots, x_n] \to B$ the corresponding map of algebras. Then, $\mathrm{Im}(\phi_n)$ is A-finite.

Proof. Consider the map $\phi_i = \phi_n|_{A[x_1,\dots,x_i]} : A[x_1, \dots, x_i] \to B$. Then, consider the sequence of maps
$$A \to \mathrm{Im}(\phi_1) \to \mathrm{Im}(\phi_2) \to \cdots \to \mathrm{Im}(\phi_{n-1}) \to \mathrm{Im}(\phi_n).$$
Since b_1 is integral over A, we see that $\mathrm{Im}(\phi_1)$ is finite over A. We now claim that $\mathrm{Im}(\phi_i)$ is finite over $\mathrm{Im}(\phi_{i-1})$ for all i. Since b_i is integral over A, we can find some finite set of generators $\{b_{i,t}\}$ for the image of the map $A[x] \to B$ given by $x \mapsto b_i$ (as an A-module); we claim that $\{b_{i,t}\}$ generate $\mathrm{Im}(\phi_i)$ as a $\mathrm{Im}(\phi_{i-1})$-module. Take any $\phi_i(p(x_1, \dots, x_i)) \in \mathrm{Im}(\phi_i)$ and write
$$p(x_1, \dots, x_i) = \sum_j q_j(x_1, \dots, x_{i-1})x_i^j$$
for some $q_j \in k[x_1, \dots, x_{i-1}]$. This means that
$$\phi_i(p(x_1, \dots, x_i)) = \sum_j \phi_{i-1}(q_j(x_1, \dots, x_{i-1}))b_i^j = \sum_j \phi_{i-1}(q_j(x_1, \dots, x_{i-1})) \sum_t c_{i,j,t}b_{i,t}.$$
But $\phi_{i-1}(q_j(x_1, \dots, x_{i-1})), c_{i,j,t} \in \mathrm{Im}(\phi_{i-1})$ (since $c_{i,j,t} \in \phi_{i-1}(A)$), so we've just shown that $b_{i,t}$ generate $\mathrm{Im}(\phi_i)$ as a $\mathrm{Im}(\phi_{i-1})$-module. This means that $\mathrm{Im}(\phi_i)$ is finite over $\mathrm{Im}(\phi_{i-1})$, as desired. Now, apply Lemma 2.6 repeatedly to see that $\mathrm{Im}(\phi_n)$ is finite over A. $\square$

Proposition 2.9. Let b be integral over A and $\phi : A[x] \to B$ the corresponding map. Then, every element $b' \in \mathrm{Im}(\phi)$ is integral over A.

Proof. Let $\phi' : A[x'] \to B$ be given by $x' \mapsto b'$. Because $x' \in \mathrm{Im}(\phi)$, we see that $\mathrm{Im}(\phi') \subset \mathrm{Im}(\phi)$ is finite over A because A is Noetherian. □

Definition. B is *integral* over A if all elements $b \in B$ are integral over A.

2.2. **Finitely Generated Algebras.** Let $A \to B$ be a map of A-algebras.

Definition. We say that B is finitely generated as an A-algebra if there exist finitely many $b_1, \ldots, b_n$ such that

$$\phi_n : A[x_1, \ldots, x_n] \to B$$

is surjective.

Lemma 2.10. If A is Noetherian and B a finitely generated A-algebra, then B is Noetherian.

Proof. Take a surjection $A[x_1, \ldots, x_n] \twoheadrightarrow B$. Note that $A[x_1, \ldots, x_n]$ is Noetherian by the Hilbert Basis Theorem. We've just represented B as a quotient of $A[x_1, \ldots, x_n]$, so B is also Noetherian. □

Lemma 2.11. An A-algebra B is finite as an A-module if and only if it is finitely generated by elements integral over A.

Proof. First suppose that B is finite over A. Then, it's clearly finitely generated as an A-algebra (since it is already finitely generated as an A-module). Now, for any $b \in B$, let $\phi_b : A[x] \to B$ be the evaluation map at b. Then, $\mathrm{Im}(\phi_b) \subset B$ is a sub-module of the finitely generated A-module B; because A is Noetherian, it is finitely generated as well. Thus, b is integral and hence B is integral over A.

Now, suppose that B is integral and finitely generated as an A-algebra. Choose generators $b_1, \ldots, b_k$ for B as an A-algebra, and consider the map $\phi_k : A[x_1, \ldots, x_k] \to B$ given by evaluation at $(b_1, \ldots, b_k)$. Since B is integral, we see that $b_1, \ldots, b_k$ are integral, so, by Lemma 2.8, we find that $B = \mathrm{Im}(\phi_k)$ is finite over A, as desired. □

Corollary 2.12. An A-algebra B is finite as an A-module if and only if it is finitely generated as an A-algebra and integral over A.

3. The Nullstellensatz

Before introducing the Nullstellensatz, we provide some motivation from algebraic geometry. First, what is algebraic geometry?

- Take a field k and $f \in k[x_1, \ldots, x_n]$. If $\underline{c} = (c_1, \ldots, c_n) \in k^n$, we denote the evaluation of f at $\underline{c}$ as a polynomial by $f(\underline{c}) \in k$.
- For α in some index set A, take $f_\alpha \in k[x_1, \ldots, x_n]$. Then, we take the *algebraic subset* of k^n defined by $\{f_\alpha\}$ to be $V(\{f_\alpha\}) = \{\underline{c} \in k^n, f_\alpha(\underline{c}) = 0\}$.

Note that $V(\{f_\alpha\})$ depends only on the ideal I generated by f_α and that I is finitely generated because $k[x_1, \ldots, x_n]$ is Noetherian. We can therefore denote this algebraic subset by $V(I)$. The question we seek to answer in algebraic geometry is:

If we know $V(I)$, can we reconstruct I?

Remark. Not every $X \subset k^n$ arises as $V(I)$ for some I. For instance, take $n = 1$, and X an arbitrary infinite subset of k. Then, $V(I) \neq X$ for any I, because any polynomial has a finite number of roots.

Remark. For I not equal to $k[x_1, \ldots, x_n]$, $V(I)$ can be empty. Take $k = \mathbb{R}$ and $I = (x^2 + 1)$. So we would like k to be algebraically closed.

Remark. If $I \neq J$, we can still have $V(I) = V(J)$. Take k algebraically closed, $I = (x)$, and $J = (x^2)$.

The last remark is a special case of the following theorem, which is the goal of this section.

Theorem 3.1 (Nullstellensatz)**.** *Let k be algebraically closed, I an ideal in $k[x_1, \ldots, x_n]$. Suppose that $f|_{V(I)} = 0$. Then, there exists n such that $f^n \in I$.*

There are several related and weaker versions of this theorem which we will consider before proving it. Recall first the following criterion from ring theory for an ideal to be maximal.

Lemma 3.2. *An ideal $\mathfrak{m} \subset R$ is maximal if and only if $R/\mathfrak{m}$ is a field.*

Lemma 3.3. *The set k^n is in bijection with maps of k-algebras $k[x_1, \ldots, x_n] \to k$.*

Proof. For $\underline{c} \in k^n$, let $\phi_{\underline{c}} : k[x_1, \ldots, x_n] \to k$ be defined by $\phi_{\underline{c}}(x_i) = c_i$. This gives the desired bijection. Note that we obtain in this way a short exact sequence

$$0 \to \mathfrak{m}_{\underline{c}} \to k[x_1, \ldots, x_n] \to k \to 0,$$

where $\ker(\phi_{\underline{c}}) = \mathfrak{m}_{\underline{c}}$ is a maximal ideal. □

The following theorem gives a converse to the construction of Lemma 3.3. We defer the proof.

Theorem 3.4 (Weak Nullstellensatz)**.** *Let k be algebraically closed. Every maximal ideal in $k[x_1, \ldots, x_n]$ is of the form $\mathfrak{m}_{\underline{c}}$ for some $\underline{c} \in k^n$.*

Corollary 3.5. *Let A be a finitely generated k-algebra (where k is algebraically closed). Then, every maximal ideal in A is of the form $\ker \phi$ for $\phi : A \to k$ a map of k-algebras.*

Proof. Take a surjection $\psi : k[x_1, \ldots, x_n] \twoheadrightarrow A$. For any maximal ideal $\mathfrak{m}_a \subset A$, consider the composition $\phi : k[x_1, \ldots, x_n] \to A \to A/\mathfrak{m}_a = K$. Now, take $\ker(\phi) = \psi^{-1}(\mathfrak{m}_a) = \mathfrak{m}$, which is maximal in $k[x_1, \ldots, x_n]$ because A is a finitely generated k-algebra. This means that $\mathrm{Im}(\phi) = k[x_1, \ldots, x_n]/\mathfrak{m} = k$ and hence that $\mathfrak{m}_a = \ker(A \to k)$, as needed. □

Now, let us consider the short exact sequence

$$0 \to I \to k[x_1, \ldots, x_n] \to A \to 0.$$

We then have the following correspondence between maps $A \to k$ and points in the variety $V(I)$.

Lemma 3.6. *The restriction of the bijection $\{k[x_1, \ldots, x_n] \to k\} \simeq k^n$ gives a bijection $\{A \to k\} \simeq V(I) = \{\underline{c} \in k^n \mid f(\underline{c}) = 0 \text{ for all } f \in I\}$.*

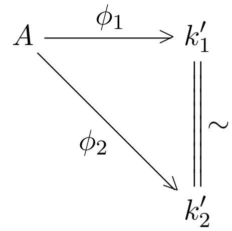
Proof. Take some $\phi : k[x_1, \ldots, x_n] \to k$ that factors through A. Recall that under the identification $\{k[x_1, \ldots, x_n] \to k\} \simeq k^n$, ϕ maps to $\underline{c} = (\phi(x_1), \ldots, \phi(x_n))$. Now, for $f \in I$, notice that $f(\underline{c}) = \phi(f) = 0$, giving one direction. The other direction is similar; any $\underline{c} \in k^n$ with $f(\underline{c}) = 0$ for all $f \in I$ corresponds to the map $\phi : k[x_1, \ldots, x_n] \to k$ such that $\phi(x_i) = c_i$. For any $f \in I$, we see that $\phi(f) = f(\underline{c}) = 0$, so $\phi|_I = 0$, completing the proof. □

Given A, write $\mathrm{Spech}(A) = \{A \to k\}$ for the set of k-algebra maps $A \to k$ and $\mathrm{Specm}(A) = \{\mathfrak{m} \mid \mathfrak{m} \text{ maximal in } A\}$. Note that $\mathrm{Spech}(k[x_1, \ldots, x_n]) \simeq k^n$. Observe that there is a map $\mathrm{Spech}(A) \to \mathrm{Specm}(A)$ given by $\phi \mapsto \ker(\phi)$.

Theorem 3.7 (Maximalidealensatz (MIS))**.** *When k is algebraically closed and A is finitely generated over k, the map $\mathrm{Spech}(A) \to \mathrm{Specm}(A)$ is an isomorphism.*

We defer the proof for now in favor of some remarks. Notice that this fails if $A = k' \supset k$ is an infinite field extension. In particular, for $A = k(x)$, $\mathrm{Spech}(A) = k^*$, while $\mathrm{Specm}(A) = (0)$. For non-algebraically closed fields, we have the following refinement.

Theorem 3.8 (Maximalidealensatz (non-algebraically closed k))**.** There is a bijection between $\mathrm{Specm}(A)$ and maps of k algebras $A \twoheadrightarrow k'$, where k' is an algebraically closed extension of k and we take two maps $\phi_1 : A \to k_1'$ and $\phi_2 : A \to k_2'$ to be equivalent if there exists an isomorphism completing the following diagram:



Theorem 3.9 (Endlich-Ergzeute-Korper-Satz (EEKS))**.** Let $k \subset F$ be a field extension such that F is finitely generated as a k-algebra. Then, F is a finite field extension of k.

Proof. We will first prove the following lemma.

Lemma 3.10. Let A be Noetherian and $A \subset B \subset C$ algebras such that

- C is finitely generated as an A-algebra.
- C is finitely generated as a B-module.

Then, B is finitely generated as an A-algebra.

Proof. Let $x_1, \ldots, x_n$ generate C as an A-algebra and $y_1, \ldots, y_m$ generate C as a B-module. This means that we can write $x_i = \sum_j b_{ij} y_j$ for some $b_{ij} \in B$. Further, there are some b_{ijk} such that $y_i y_j = \sum_k b_{ijk} y_k$. Now, let $B_0 \subset B$ be the A-subalgebra in B generated by $\{b_{ij}, b_{ijk}\}$. This is a finitely generated algebra over A and is in particular Noetherian.

We now claim that $y_1, \ldots, y_m$ generate C as a B_0-module. First, note that $x_i = \sum_j b_{ij} y_j$. Further, the x_i generate C as an A-algebra. Thus each monomial of the x_i's is in the linear span of $y_1, \ldots, y_m$ with coefficients b_{ijk} by our definition, giving the claim.

Now, note that B_0 is Noetherian and $B \subset C$, so B is finitely generated as a B_0-module. In particular, it is finitely generated as B_0-algebra, meaning that it is finitely generated as an A-algebra via the chain $A \to B_0 \to B$ of finitely generated algebras. □

We can now proceed to the proof of the theorem. Let $x_1, \ldots, x_n \in F$ be generators of F as a field over k. Let $x_1, \ldots, x_m$ be a maximal subset of algebraically independent elements; i.e., we have a tower of field extensions $k \hookrightarrow k(x_1, \ldots, x_m) \subset F$, where the last extension $k(x_1, \ldots, x_m) \subset F$ is algebraic and hence finite. By Lemma 3.10, we see that $k(x_1, \ldots, x_m)$ is finitely generated as a k-algebra and in particular as an algebra over $k(x_1, \ldots, x_{m-1})$. This is a contradiction, since $K(x)$ is never a finitely generated K-algebra for any field K (here we take $K = k(x_1, \ldots, x_{m-1})$). □

Theorem 3.9 is the key technical assertion that allows us to prove the various formulations of the Nullstellensatz.

Proof of Theorem 3.4. Let $\mathfrak{m}$ be a maximal ideal in $k[x_1, \ldots, x_n]$. Then, we have the projection $k[x_1, \ldots, x_n] \to k[x_1, \ldots, x_n]/\mathfrak{m} = K$ for K a field extension of k. Observe that K is finitely generated as a k-algebra (since the images of $x_1, \ldots, x_n$ are generators), so by Theorem 3.9, it is finitely generated as a k-module. But k was algebraically closed, so it has no non-trivial finite extensions, meaning that $K = k$. Thus we have the exact sequence $0 \to \mathfrak{m} \to k[x_1, \ldots, x_n] \to k \to 0$, as desired. □

Proof of Theorem 3.7. We first claim that it is enough to prove the theorem for A a polynomial algebra. Suppose that the theorem held for polynomial algebras. Then, for a finitely generated A, we'd have a short exact sequence

$$0 \to I \to k[x_1, \ldots, x_n] \to A \to 0.$$

Take $\mathfrak{m} \subset A$ and consider $\mathfrak{m}' = \phi^{-1}(\mathfrak{m})$. Note that $I \subset \mathfrak{m}'$, so there exists $\phi' : k[x_1, \dots, x_n] \to k$ such that $\ker(\phi') = \mathfrak{m}'$. This means that $I \subset \ker(\phi')$ and hence ϕ' factors through A.

Take some maximal ideal $\mathfrak{m} \subset A$, and consider $A/\mathfrak{m} = F$. We want to show that $k \hookrightarrow F$ is an isomorphism. Note that F is a finitely generated k algebra, so F is a finite field extension of k. Since k is algebraically closed, this means that $k = F$. □

Definition. For $I \subset k[x_1, \dots, x_n]$, define its *radical* to be $\text{rad}(I) = \{a \in A \mid a^n \in I \text{ for some } n\}$.

We therefore have the following restatement of the Nullstellensatz (Theorem 3.1).

Theorem 3.11. Let k be algebraically closed. Then, if $f \in k[x_1, \dots, x_n]$ vanishes on $V(I)$, then $f \in \text{rad}(I)$.

Corollary 3.12. If $V(I_1) = V(I_2)$, then $\text{rad}(I_1) = \text{rad}(I_2)$ (for k algebraically closed).

Theorem 3.13. Let A be a finitely generated algebra over an algebraically closed field k. Then, if $f \in A$ is such that f vanishes under every element of $\text{Spech}(A)$, then f is nilpotent.

We will first prove that Theorems 3.11 and 3.13 are equivalent and then prove Theorem 3.13 to establish the full Nullstellensatz.

Proof of equivalence of Theorems 3.11 and 3.13. Take a surjection $k[x_1, \dots, x_n] \twoheadrightarrow A$, giving the short exact sequence

$$0 \to I \to k[x_1, \dots, x_n] \to A \to 0.$$

Now, for $f \in A$, take $\tilde{f} \in k[x_1, \dots, x_n]$ mapping to f. By Lemma 3.6 and Theorem 3.7, f vanishes under each element of $\text{Spech}(A)$ if and only if $\tilde{f}$ vanishes on $V(I)$. The desired equivalence then follows from the fact that $\tilde{f}$ is in $\text{rad}\, I$ if and only if f is nilpotent. □

Proof of Theorem 3.13. Suppose for contradiction that f were not nilpotent. Since f vanishes under all elements of $\text{Spech}(A)$, by Theorem 3.7, we see that $f \in \mathfrak{m}$ for all maximal ideals $\mathfrak{m} \in A$. We first claim that $(tf - 1)$ is a proper ideal in $A[t]$. Suppose otherwise for contradiction; then, we'd have that $1 = p(t) \cdot (tf - 1)$ for some $p(t) = a_0 + a_1 t + \cdots + a_n t^n \in A[t]$, meaning that

$$p(t) \cdot (tf - 1) = f a_n t^{n+1} + (f a_{n-1} - a_n) t^n + \cdots + (f a_0 - a_1) t - a_0 = 1.$$

This implies that $a_0 = -1$, $f a_n = 0$, and $a_{i+1} = f a_i$ for $1 \leq i \leq n$, so we may conclude that $f^{n+1} a_0 = -f^{n+1} = 0$, which is a contradiction because f is not nilpotent.

Now, consider the algebra $B = A[t]/(tf - 1)$; since $A[t]$ is a finitely generated k-algebra, so is B. Now, consider the map $\phi : A \hookrightarrow A[t] \to B$. Take any maximal ideal $\mathfrak{m}' \subset B$. Notice that $\phi(f)$ is invertible in B, so $\phi(f) \notin \mathfrak{m}'$. Thus, we see that $f \notin \phi^{-1}(\mathfrak{m}')$, which is maximal because A is a finitely generated k-algebra. This is a contradiction, so we are done. □

Remark. In the proof of Theorem 3.13, the construction of $B = A[t]/(tf - 1)$ may at first seem like an unmotivated trick. However, it is in fact the *localization* of A at f, forming an instance of a much more general construction.