1 The Nullstellensatz

We start in the middle with the following key result [CR: 5.36], whose statement is fairly easy to understand. From it, we prove Hilbert's Nullstellensatz.

Lemma 1.1 (Zariski)**.** *Let L be a finitely-generated K-algebra. If L is a field then L is a finite algebraic extension of K.*

Consequently, if K is algebraically closed, then $L = K$.

I'm splitting [CR: 5.37] into two easy corollaries of the lemma.

Corollary 1.2. *Let M be a maximal ideal of $K[x_1, \ldots, x_n]$, then the residue field $K[x_1, \ldots, x_n]/M$ is a finite algebraic extension of K.*

If K is algebraically closed then $K[x_1, \ldots, x_n]/M \cong K$. Furthermore, $M = \langle x_1 - p_1, \ldots, x_n - p_n \rangle$ for some $p_i \in K$.

Proof. The residue field is a finitely-generated K-algebra, so by Zariski's lemma, it is a finite algebraic extension of K.

Suppose K is algebraically closed, so the quotient $K[x_1, \ldots, x_n]/M = K$. Let p_i be the image of x_i under the canonical map

$$K[x_1, \ldots, x_n] \xrightarrow{\alpha} K[x_1, \ldots, x_n]/M = K$$

Then $x_i - p_i$ is in the kernel of α, so $\langle x_1 - p_1, \ldots, x_n - p_n \rangle \subseteq M$. But we know $\langle x_1 - p_1, \ldots, x_n - p_n \rangle$ is already a maximal ideal, so these ideals are equal. □

The previous corollary says that, for K algebraically closed, there is a bijection between points of $\mathbb{A}^n_K$ and maximal ideals of $K[x_1, \ldots, x_n]$.

Corollary 1.3 (Weak Nullstellensatz)**.** *Let K be algebraically closed. For any ideal $I \subseteq K[x_1, \ldots, x_n]$, we have $\mathbb{V}(I) \neq \emptyset$.*

Proof. Since $K[x_1, \ldots, x_n]$ is Noetherian, I is contained in some maximal ideal. By the previous corollary, that ideal is $\langle x_1 - p_1, \ldots, x_n - p_n \rangle$ for some $p_i \in K$. This shows that $\bar{p}$ is a point on $\mathbb{V}(I)$. □

Now the culmination, [CR: 5.38], whose proof involves a clever trick (see Problem 6.6)

Theorem 1.4 (Strong Nullstellensatz)**.** *Let K be algebraically closed. For any ideal $I \subseteq K[x_1, \ldots, x_n]$, we have $\mathbb{I}(\mathbb{V}(I)) = \sqrt{I}$.*

Consequently, if I is already radical, then $\mathbb{I}(\mathbb{V}(I)) = I$. We already know that $\mathbb{V}(\mathbb{I}(V)) = V$, for a variety V. Thus we have a bijection between varieties and radical ideals.

2 Modules

In order to prove Zariski's lemma, we need to introduce a new algebraic structure.

Definition 2.1. A module M over a ring R is an abelian group with an R-action (aka R-multiplication). For each $r \in R$ and $m \in M$ there is a unique element $rm = mr$ of M. This R-action satisfies the following properties. For $r, r' \in R$ and $m, m' \in M$,

- $1m = m$
- $r(r'm) = (rr')m$
- $(r + r')m = rm + r'm$
- $r(m + m') = rm + rm'$

There are some basic properties of modules that should be checked: (For example $0_R m = 0_M$, and $(-r)m = -(rm)$, for any $m \in M$ and $r \in R$.) When R is a field, an R-module is simply a vector space over R. Usually we deal with finite-dimensional vector spaces over a field K, but we also treat $K[x]$ as a vector space: one basis is $\left\{x^i : i \in \mathbb{N}_0\right\}$. For modules over a ring things are much more nuanced. Here are the key examples for a ring R.

- An ideal I of R is an R-module using the multiplication in R as the R-action.
- The quotient ring R/I is an R- module, with this R-action:
  For $r \in R$ and $a + I \in R/I$, define $r(a + I) = ra + I$.
- The Cartesian product $R \times R \times \cdots \times R = R^n$ is an abelian group using coordinate wise addition. We make R^n into an R-module by introducing the R-action $r(r_1, r_2, \ldots, r_n) = (rr_1, rr_2, \ldots, rr_n)$. It is called a **free module of rank** n. As with vector spaces, the **standard basis** is $\{e_1, \ldots, e_n\}$ where $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$, with a 1 in the ith coordinate. Every element of R^n can be written in a unique way as a linear combination of basis elements with coefficients from R.
- More generally, the Cartesian product of modules $M_1, \ldots, M_n$ is a module in the same fashion. $r(m_1, m_2, \ldots, m_n) = (rm_1, rm_2, \ldots, rm_n)$.
- The polynomial ring $R[w]$ over R is an R-module. In fact, $R[w]$ is said to be "free" with an infinite basis $1, w, w^2, \ldots$. Every element of $R[w]$ can be written is a unique way as a finite sum of these basis elements.
- If $\varphi : R \longrightarrow S$ is a homomorphism of rings then S is an R-module. The action of an element $r \in R$ on an element $s \in S$ is given by $\varphi(r)s$. In particular, S is a module over any of its subrings.

Example 2.2. $R = K[x, y]$ with $I = \langle x^2, y^2 \rangle$.

I'm going to use w as my parameter for a polynomial ring over the ring R when we consider R modules, because R itself may be a polynomial ring (in x, y, z for example) and I want to be consistent in the use of my parameter for the polynomial ring over R.

Definition 2.3. Let M be an R-module and $\mathcal{A}$ a subset of M. A **linear combination** of the elements of $\mathcal{A}$ is a sum $\sum_{a \in \mathcal{B}} r_a a$ where $\mathcal{B}$ is a *finite* subset of $\mathcal{A}$ and $r_a \in R$. We write $R\mathcal{A}$ for the set of all linear combinations. It is straightforward to check that it is a submodule of M.

An R-module M is **generated** by $a_1, \ldots, a_n$ when any element of m can be written as a linear combination of the a_i with coefficients from R. More generally, M is generated by a set $\mathcal{A} \subseteq M$ when $R\mathcal{A} = M$.

Equivalently, R is generated by $a_1, \ldots, a_n$ iff there is a surjective module homomorphism $R^n \longrightarrow M$ that takes e_i to a_i (here the $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ form the standard basis). Note the difference between this definition and the one for finitely-generated R-algebras: S is generated by $a_1, \ldots, a_n$ *as an algebra* over R when there is a surjective ring homomorphism $R[x_1, \ldots, x_n] \longrightarrow S$ taking x_i to a_i.

Definition 2.4. A function $\varphi : M \longrightarrow N$ is a **homomorphism of R-modules** when $\varphi(m + m') = \varphi(m) + \varphi(m')$ and $\varphi(rm) = r\varphi(m)$ for $m, m' \in M$ and $r \in R$. The first condition says that φ is a homomorphism of abelian groups, and the second that φ respects R-action. We say φ is an isomorphism when it is also a bijection.

3 Rings as modules over a subring

An important consideration for us—in fact the main motivation for introducing modules—is that it is useful to consider whether a ring (think: coordinate ring of a variety) is finitely-generated *as a module* over some subring (think: a subring isomorphic to a polynomial ring).

Example 3.1. Three key examples of rings over $\mathbb{Z}$ that we treat as modules:

- $\mathbb{Z}[\sqrt{2}]$ is free of rank two: each element can be written as a sum $a + b\sqrt{2}$ for $a, b \in \mathbb{Z}$.
- $\mathbb{Z}[\pi]$ is free of infinite (countable) rank. It is isomorphic to the polynomial ring $\mathbb{Z}[w]$
- $\mathbb{Z}[1/2]$ is not free.

Example 3.2. Consider the homomorphism $\mathbb{Z}[w] \longrightarrow \mathbb{Z}[1/2]$ that takes w to $1/2$. I claim the kernel is $2w - 1$, in other words $\mathbb{Z}[w]/\langle 2w - 1\rangle \cong \mathbb{Z}[1/2]$. This may seem obvious, since $\tilde{w}$ is the inverse of 2 in the ring $\mathbb{Z}[w]/\langle 2w - 1\rangle$. Problem 6.2 gives another way to see it.

4 Transcendental, algebraic, integral

Definition 4.1. Let R be a subring of S. Consider the homomorphism $\varphi : R[w] \longrightarrow S$ that takes w to $a \in S$. We write $R[a]$ for the image of φ. We say a is **transcendental** over R when φ is an isomorphism. Otherwise, when the kernel is nontrivial, a is **algebraic** over R. If, additionally, there is a monic polynomial in $\ker(\varphi)$, we say a is **integral** over R.

The ring S is algebraic over R when every element of S is algebraic over R. The ring S is integral over R when every element of S is integral over R.

Example 4.2. Consider $S = K[x, y]/\langle y^3 - 1, xy - x\rangle$ as a $R = K[x]$ module. We show that y is integral over $K[x]$. The homomorphism $R[w] \longrightarrow S$ taking w to y has kernel $\langle w^3 - 1, xw - x\rangle$. Since the monic polynomial $w^3 - 1$ is in the kernel, y is integral over $K[x]$. The fact that there is a non-monic polynomial in the kernel (that is, $xw - x$) doesn't change the determination that y is integral.

Note that when K is a field and S is a K-algebra, an element $a \in S$ that is algebraic over K is also integral over K. For if a is a root of the degree d polynomial $f(w) = f_d w^d + f_{d-1}w^{d-1} + \cdots + f_0$ then it is also a root of the monic polynomial $w_d + \frac{f_{d-1}}{f_d} + \cdots + \frac{f_0}{f_d}$.

The following proposition is not hard to prove.

Proposition 4.3. *Let R be a subring of S and let $a \in S$ be algebraic over R. Then $R[a]$ is a finitely-generated module over R if and only if a is integral over R.*

A more powerful statement is [CR: 5.27], which takes a bit more machinery (and is why modules were introduced).

Proposition 4.4. *Let $R \subseteq S$ be rings with $S = R[a_1, \ldots, a_n]$ (a finitely-generated R-algebra). The following are equivalent.*

(1) S is integral over R.

(2) Each a_i is integral over R.

(3) R is a finitely-generated R-module.

Proof. (1) $\implies$ (2) is immediate. (2) $\implies$ (3) can be proven inductively using the previous proposition. (3) $\implies$ (1) requires a technical tool from linear algebra: the adjugate of a matrix (or Cramer's rule). □

5 Noether Normalization

Now we come to the big theorem [CR: 5.32] that allows us to prove Zariski's lemma!

Definition 5.1. Let $R \subseteq S$ be rings and $a_1, \dots, a_n$ elements of S. We say the a_i are **algebraically independent** when the map $R[x_1, \dots, x_n] \longrightarrow S$ that takes the indeterminate x_i to a_i is injective. Otherwise, the a_i are **algebraically dependent**.

Theorem 5.2 (Noether Normalization)**.** *Let S be a finitely generated K-algebra. There exists an algebraically independent subset $\{a_1, \dots, a_d\}$ of S such that S is integral over $K[a_1, \dots, a_d]$.*

Definition 5.3. A set of algebraically independent elements as in the theorem is called a **Noether basis**.

You might hope that, for a K-algebra S, any two Noether bases would have the same number of elements. You will not be disappointed, but it takes some work. You might ponder why the theorem used a subscript d for the number of elements in a Noether basis.

And now full circle, back to what we wanted to prove.

Corollary 5.4 (Zariski's lemma)**.** *Let L be a finitely-generated K-algebra. If L is a field then L is a finite algebraic extension of K.*

Proof. Suppose L has a Noether basis $a_1, \dots, a_d$ (with $d \in \mathbb{N}$). Since $a_d^{-1} \in L$ and it must be integral over $K[a_1, \dots, a_d]$ there is some polynomial

$$x^n + f_{n-1}(a_1, \dots, a_d)x^{n-1} + \cdots + f_1(a_1, \dots, a_d)x + f_0(a_1, \dots, a_d)$$

that has $1/a_d$ as a root. Substitute $1/a_d$ and multiply by a_d^n. You get a nonzero polynomial in the a_i—that is, an element of $K[a_1, \dots, a_d]$—that is 0. That contradicts the algebraic independence of the a_i. Consequently $d = 0$. □

6 Problems

Problems 6.1. Basic properties of modules [CR: 5.1.7,8,9]

(a) Let $M \subseteq N$ be R modules. Show that the quotient group N/M has a natural R-module structure.

(b) Let $\varphi : M \longrightarrow N$ be a homomorphism of R-modules. Show that the kernel and image of φ are R-modules.

(c) Conclude with a First Isomorphism Theorem for R-modules.

Problems 6.2. An algebraic, non-integral extension of $\mathbb{Z}$

Any polynomial in $\mathbb{Z}[w]$ is equivalent modulo $2w - 1$ to a polynomial of the form $a_0 + \sum_{i \in \mathbb{N}} a_i w^i$ where $a_0 \in \mathbb{Z}$, $a_i \in \{0, 1\}$ (and a finite number are nonzero).

(a) Show this representation is also unique.

(b) The image of $a_0 + \sum_{i \in \mathbb{N}} a_i w^i$ is $a_0 + \sum_{i \in \mathbb{N}} a_i 2^{-i}$. Just working with properties of $\mathbb{Z}$ show that this uniquely expresses an element of $\mathbb{Z}[1/2]$.

(c) Prove that $\mathbb{Z}[1/2]$ is not a free $\mathbb{Z}$-module: Prove it is not of rank 1. Prove that no two elements are algebraically independent.

(d) Extend this example to an arbitrary integer m, instead of 2.

Problems 6.3. Transcendental, algebraic, integral over $K[x]$

(a) Create examples analogous to 3.1 over the ring $K[x]$ using x instead of 2.

(b) Create examples analogous to 3.1 over the ring $K[x]$ using $x-1$ instead of 2.

Problems 6.4. More on integral extensions and Proposition 4.4

See [CR: 5.2.6, 5.3.8].

(a) Let $R \subseteq S \subseteq T$ be rings. Suppose that S is generated by $a_1, \ldots, a_m$ *as a module* over R and T is generated by $b_1, \ldots, b_n$ as a module over S. Show that there are mn elements of T that generate T as a module over R.

(b) Now let R be a subring of S. The **integral closure** of R in S is the set T of elements in S that are integral over R. Prove T is actually a ring. Use Prop. 4.4 [CR: 5.27].

Problems 6.5. The holey line

Let $g(x) \in K[x]$. Consider the homomorphism

$$K[x] \longrightarrow \frac{K[x,y]}{1 - yg(x)}$$

(a) Explain why the map is not an isomorphism.

(b) Interpret this as a map of varieties $\mathbb{A}^1 \longleftarrow \mathbb{V}(1 - yg(x))$. What points of $\mathbb{A}^1$ are not in the image?

(c) Under what conditions on g and h is $K[x,y]/\langle 1 - yg(x) \rangle$ isomorphic to $K[x,y]/\langle 1 - yh(x) \rangle$?

(d) Show that $\frac{K[x,y]}{1-yg(x)}$ is integral over $K[\tilde{x} + \tilde{y}]$. Hint: $g(\tilde{x})(\tilde{x} + \tilde{y})$.

Problems 6.6. Some details in the Nullstellensatz

Let $g \in K[x_1, \ldots, x_m]$ and let φ be the composition of the following sequence of homomorphisms (in which the first is the natural embedding),

$$K[x_1, \ldots, x_m] \longrightarrow K[x_1, \ldots, x_m, w] \quad \longrightarrow \frac{K[x_1, \ldots, x_m, w]}{1 - wg(x_1, \ldots, x_m)} \cong K[x_1, \ldots, x_m, \frac{1}{g}]$$

(a) Let I be an ideal in $K[x_1, \ldots, x_m]$. Show that $g^n \in I$ for some $n \in \mathbb{N}$ if and only if $\langle \varphi(I) \rangle = K[x_1, \ldots, x_m, \frac{1}{g}]$.

Problems 6.7. Some details in Noether Normalization

(a) Show that the homomorphism from $K[x_1, \ldots, x_n]$ to itself that takes x_1 to x_1 and, for $i = 2, \ldots, n$ takes x_i to $x_i + f_i(x_1)$ is an isomorphism.

(b) Let $f = x^3 y^2 z^4$ Find a change of variable as in (a) that turns f into a monic polynomial in x.