1 Summary of steps to prove the Nullstellensatz

Lemma 1.1 (Zariski)**.** *Let L be a finitely-generated K-algebra (think $K(V)$ for V irreducible). If L is a field then L is a finite algebraic extension of K. Consequently, if K is algebraically closed, then $L = K$.*

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 $K[x_1, \ldots, x_n]/M \cong K$. Consequently, $M = \langle x_1 - p_1, \ldots, x_n - p_n \rangle$ for some $p_i \in K$.

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

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

2 Modules

Think of an R-module, for R a ring, as analogous to a vector space. The difference is that R-modules are not necessarily free (isomorphic to R^n). Examples: For I an ideal of R, both I and R/I are R-modules, but generally not free.

Definition 2.1. 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.

Proposition 2.2. *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.

Replacing R with a field K, we can state something similar, but stronger, [CR: 6.13]. Note that if a is algebraic over K, then it is integral over K.

Proposition 2.3. *Let K be a field and let $L = K[a_1, \ldots, a_n]$ (a finitely-generated K-algebra) be a domain. The following are equivalent.*

(1) L is algebraic (i.e. integral) over K.

(2) Each a_i is algebraic (i.e. integral) over K.

(3) L is a finitely-generated vector space over K.

(4) $L = K(a_1, \ldots, a_n)$.

Proof. Proposition 2.2 shows the equivalence of the first 3 items. Assume they are true. To prove (4), one shows inductively that $K[a_1, \ldots, a_t] = K(a_1, \ldots, a_t)$. This is because each a_{t+1} is assumed to be algebraic $K(a_1, \ldots, a_t)$ so there is some irreducible $f(x) \in K(a_1, \ldots, a_t)[x]$ such that $K(a_1, \ldots, a_t)[a_{t+1}] \cong K[a_1, \ldots, a_t][x]/f(x)$, and this is a field.

Conversely, if $L = K(a_1, \ldots, a_t)$ then it is a finitely-generated K-algebra that is also a field. So Zariski's lemma says that L is a finite algebraic extension of K. □

The proof for item (4) uses Zariski's lemma, which should make you cry foul, since we have not yet proven it! But this proposition is not used in proving Zariski's lemma ([CR: 5.36], see the next section). It is used in [CR: Ch. 6]. I list it here to emphasize the relationship with Proposition 2.2.

Corollary 2.4. *Let $K \subseteq L \subseteq M$ be finitely-generated field extensions. If L/K and M/L are both algebraic then so is M/K.*

3 Noether Normalization

Definition 3.1. Let $R \subseteq A$ be rings and $a_1, \ldots, a_n$ elements of A. We say the a_i are **algebraically independent** when the map $R[x_1, \ldots, x_n] \longrightarrow A$ that takes the indeterminate x_i to a_i is injective. Otherwise, the a_i are **algebraically dependent**.

Theorem 3.2 (Noether Normalization)**.** *Let A be a finitely generated K-algebra. There exists an algebraically independent subset $\{a_1, \ldots, a_d\}$ of S such that A is integral over $K[a_1, \ldots, a_d]$.*

Proof. Induction on n, the number of generators for A as a K-algebra. For the induction step, assume that the theorem is true for $k < n$ generators and A has n generators $b_1, \ldots, b_n$. If they are algebraically independent, then there is nothing to prove. Otherwise, they are dependent; suppose that there is polynomial dependence that involves b_1. There is a clever isomorphism from A to itself that turns that algebraic dependence into one that is monic in b_1. Then A is integral over $K[\tilde{b}_2, \dots, \tilde{b}_n]$ for some $\tilde{b}_i$ in A. Applying the induction hypothesis, $K[\tilde{b}_2, \dots, \tilde{b}_n]$ is integral over some subring $K[a_1, \dots, a_d]$ with $a_1, \dots, a_d$ algebraically independent. Now A is integral over $K[a_1, \dots, a_d]$. □

Definition 3.3. A set of algebraically independent elements as in the theorem is called a **Noether basis**.

Lemma 3.4 (Zariski)**.** *Let L be a field that is a finitely-generated K-algebra. Then L is a finite algebraic extension of K.*

Proof. Sketch: Suppose L had a Noether basis consisting of $a \in L$. Then any other element of L would be integral over $K[a]$, in particular a^{-1}. So there would be a polynomial monic $f(x) = x^m + f_{m-1}x^{m-1} + \dots + f_1 x + f_0$ with $f_i \in K$ that has a^{-1} as a root.

$$(a^{-1})^m + f_{m-1}(a^{-1})^{m-1} + \dots + f_1(a^{-1}) + f_0 = 0$$

Multiplying by a^m,

$$1 + f_{m-1}a + \dots + f_1(a^{m-1}) + f_0 a^m = 0$$

This contradicts the assumption that a is transcendental over K. □

4 Transcendence bases and dimension

We want to define dimension for a variety, $D(V)$. Here are the basic things it should satisfy:

(1) The dimension of a point should be 0.

(2) $D(V_1 \cup \dots \cup V_k)$ should be $\max(D(V_i))$.

(3) The dimension of $V \cap \mathbb{V}(f)$ is $D(V) - 1$, provided $f \notin \mathbb{I}(V)$ and $V \cap \mathbb{V}(f) \neq \emptyset$.

Here is our key tool.

Definition 4.1. Let $K \subseteq L$ be fields. A subset $\{a_1, \dots, a_d\}$ of L is a **transcendence basis** of L over K when

(1) $a_1, \dots, a_d$ are algebraically independent, and

(2) L is algebraic (i.e. integral) over $K(a_1, \dots, a_d)$.

For ease of exposition, let's restrict to V an irreducible variety. Some straightforward ideas allow the extension to an arbitrary variety.

We want to show that

(1) A Noether basis of $K[V]$ is also a transcendence basis for $K(V)$.

(2) All transcendence bases have the same number of elements.

(3) The number of elements in a transcendence basis for $K(V)$ satisfies the three properties for dimension.

For Item (1) there are two things to show. First, for $f_1, \ldots, f_d \in K[V]$, they are algebraically independent in $K[V]$ iff they are algebraically independent in $K(V)$. Second: if $K[V]$ is integral over $K[f_1, \ldots, f_d]$ then $K(V)$ is integral (i.e. algebraic) over $K(f_1, \ldots, f_d)$. That is essentially [CR: 6.32] and Exercise 6.5.5.

Item (2) is presented earlier, in [CR: 6.20-22]. The key idea is this: Let $K \subseteq L$ be fields, and let $A = \{a_1, \ldots, a_n\}$ be such that L is algebraic over $K(A)$. For any $b \notin \overline{K}$ there is some a_i such that L is algebraic over $K[A \setminus \{a_i\} \cup \{b\}]$.

Lemma 4.2 (Exchange). *Let $K \subseteq L$ be fields, and let $A = \{a_1, \ldots, a_n\}$ be such that L is algebraic over $K(A)$. Let $B = \{b_1, \ldots, b_m\}$ be a set of algebraically independent elements in L. Then $m < n$ and there is some $A' \subseteq A$ with $|A'| = n - m$ such that L is algebraic over $K[A' \cup B]$.*

Theorem 4.3 ([CR: 6.22]). *Let L be a finitely-generated field extension of K (think $K(V)$). Then L has a transcendence basis, and any two transcendence bases have the same number of elements.*

Definition 4.4. The number of elements in the transcendence basis of L over K is called the **transcendence degree** of L over K. The **dimension** of an irreducible variety V is defined to be transcendence degree of $K(V)/K$.

Corollary 4.5. *Let $K \subseteq L$ be a finitely-generated field extension.*

- *If $a_1, \ldots, a_t$ are algebraically independent then $\{a_1, \ldots, a_t\}$ can be extended to create a transcendence basis of L over K.*
- *If L is algebraic (i.e. integral) over $K(a_1, \ldots, a_t)$ then $\{a_1, \ldots, a_t\}$ contains a transcendence basis.*

Item (3) of our "Want to show" list is proven in [CR: §6.6]