Hilbert's nullstellensatz

This short write-up was written during a graduate course on commutative algebra at NTNU. We used the book by Atiyah and MacDonald, and exercise 7.14 is to prove the strong Hilbert's nullstellensatz. I wanted to thoroughly go through a proof, including lemmas used in the proof to have an almost selfcontained overview of the problem. It turned into this little write-up.

Torgeir Aambø

Contents

1 Preliminaries

All rings mentioned are commutative and have a multiplicative identity, referred to as 1.

We will try not to assume that the reader knows everything, but we will assume general knowledge of algebra and some introductory commutative algebra like definitions of rings, modules, algebras etc.

Teorem 1 (Noether's normalization lemma)**.** *Let k be a field and B a non-trivial finitely generated k-algebra. Then there exists a non-negative integer d and algebraically independent elements $y_1, ..., y_d$, i.e. elements with no relations, in B such that B integral over the polynomial ring $k[y_1, ..., y_d]$.*

Proof. Note that the following proof is heavily based on the proof from Mumford's "The red book".

Since B is finitely generated the proof is done by induction on the number of generators, m.

$m = 0$: In this case $A = k$ and we are done.

Assume $m > 0$ and that the lemma holds for all k-algebras generated by $m-1$ or fewer elements.

Now, let B be generated by $y_1, \dots, y_m$. If there is no relations on the generators, i.e. they are algebraically independent, then

$$B \cong k[y_1, \dots, y_m]$$

and we are done. Hence we assume that f is a relation on the m generators, i.e. a polynomial equation

$$f(y_1, \dots y_m) = 0.$$

Let r be an integer. We are going to determine this later. Set $z_1 = y_1$ and $z_i = y_i - y_1^{r^{i-1}}$ for $2 \leq i \leq m$. Note that the z_i's also are generators of B. Then we can rewrite the relation as

$$f(z_1, z_2 + y_1^r, z_3 + y_1^{r^2}, \dots z_m + y_1^{r^{m-1}}) = 0.$$

For $a \in k$, the highest term of y_1 appearing in $a\prod_1^m (z_i + z_1^{r^{i-1}})^{\alpha_i}$ looks like $a y_1^{\alpha_1 + r\alpha_2 + \dots + r^{m-1}\alpha_m}$. Hence, if r is larger than all of the α_i's appearing in f, then the highest term of y_1 appearing in $f(z_1, z_2 + y_1^r, z_3 + y_1^{r^2}, \dots z_m + y_1^{r^{m-1}})$ also has the same form as the one above, which means that y_1 is integral over $k[y_2, \dots, y_m]$.

Since $y_i = z_i + y_1^{r^{i-1}}$ are also integral over the same ring, the z_i's generate B, and being an integral extension is a transitive property, we get that B is integral over $k[y_2, \dots, y_m]$. Since $k[y_2, \dots, y_m]$ is generated by $m-1$ elements, we can apply the inductive hypothesis, and hence we are done. □

We want to apply Noether's normalization lemma to prove Zariski's lemma. In the proof we present we use a result stating that integral ring extensions preserve Krull dimension. We actually only use the fact that if a ring with Krull dimension zero is an integral ring extension of another ring, then this ring also has Krull dimension zero. The more general statement also is true, but we only prove a more strict statement that we need.

We remind ourself what we mean by Krull dimension.

Definisjon 1 (Krull dimension)**.** *Let A be a ring. The Krull dimension of A is defined as the supremum over the length of all chains of prime ideals in A.*

Proposition 1. *Let S be a ring and T be an integral ring extension of S. Then the Krull dimension of S is lower or equal to the Krull dimension of T.*

Proof. Let $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ be a chain of prime ideals in S. By the Going-up theorem we can extend any chain of length less than n, $\mathfrak{q}_0 \subsetneq \cdots \subsetneq \mathfrak{q}_m$ such that $\mathfrak{q}_i \cap S = \mathfrak{p}_i$, for $i = 1, \ldots, m$, to a chain of prime ideals $\mathfrak{q}_0 \subsetneq \cdots \subsetneq \mathfrak{q}_n$ in T, such that $\mathfrak{q}_i \cap S = \mathfrak{p}_i$ for $i = 1, \ldots, n$. Hence the Krull dimension of an integral ring extension can't get any lower than the Krull dimension of the ring it extends. □

Note that we here used the so called Going-up theorem. This theorem proves exactly what is stated in the proof of the proposition, i.e. that we can extend chains of prime ideals in integral extensions. We will not prove this theorem, but we refer the reader to the proof in Introduction to commutative algebra by Atiyah and MacDonald.

This immediately implies what we need, i.e. that if a ring with Krull dimension zero is an integral ring extension of another ring, then this ring also has Krull dimension zero.

Corollary 1.1 (Zariski's lemma)**.** *Let k be a field, and K be a field extension that is finitely generated as an algebra over k. Then K is a finite field extension, i.e. a finite dimensional k-vectorspace.*

Proof. By Noether's normalization lemma, K is integral over the ring $k[y_1, \ldots y_d]$, where $y_1, \ldots y_d$ are the elements of K that are algebraically independent over k. Since K is a field, it has Krull dimension 0, and since integral ring extensions preserve Krull dimension, the polynomial ring $k[y_1, \ldots y_d]$ must have Krull dimension zero, i.e. $d = 0$. Hence K is a finitely generated module over k, i.e. a finite dimensional k-vectorspace. □

Now, before we tackle the actual proof of Hilbert's nullstellensatz, we need to chose a formulation. There are many formulations of the theorem, all hopefully equivalent, but we have chosen one of the more standard and iconic ones. The

formulation is based on some language from algebraic geometry, hence we need some definitions.

Definisjon 2 (Radical)**.** *Let A be a ring and $\mathfrak{a}$ an ideal in A. We define the radical of $\mathfrak{a}$ to be the set*

$$\sqrt{\mathfrak{a}} = \{f \in A \mid \exists n \in \mathbb{N} \ s.t. \ f^n \in \mathfrak{a}\}.$$

We say an ideal $\mathfrak{a}$ is a radical ideal if $\mathfrak{a} = \sqrt{\mathfrak{a}}$.

Definisjon 3 (Zero locus)**.** *Let k be an algebraically closed field, A be the polynomial ring $A = k[t_1, \ldots, t_n]$ and let $S \subset A$ be a subset. We define the zero locus of S to be the set*

$$Z(S) = \{x \in k^n \mid f(x) = 0, \ \forall f \in S\}.$$

If a subset $V \subset k^n$ has the form $V = Z(S)$ for some $S \subset A$, then we call V an affine algebraic variety.

Definisjon 4 (Vanishing set)**.** *Let $V \subset k^n$. We define the vanishing set of V to be the set*

$$I(V) = \{f \in A \mid f(x) = 0, \ \forall x \in V\}.$$

2 Hilbert's nullstellensatz

This is by no means the shortest proof of this theorem, nor is it the most elegant. I chose to do it this way because it's more involved and has a couple extra moving parts. It was also a good excuse to look into Jacobson rings.

Teorem 2 (Hilbert's nullstellensatz)**.** *Let k be an algebraically closed field, A be the polynomial ring $A = k[t_1, \ldots, t_n]$ and $\mathfrak{a}$ be an ideal of A. Then*

$$I(Z(\mathfrak{a})) = \sqrt{\mathfrak{a}}$$

We are going to do the proof in three smaller steps.

1. Proving that ideals of the form $\mathfrak{m}_a = (t_1 - a_1, \ldots t_n - a_n)$ where $a \in k^n$ are the only maximal ideals in A. This is known as the weak Hilbert's nullstellensatz.
2. Proving that the radical of an ideal $\mathfrak{b}$ in a finitely generated k-algebra B is equal to the intersection of the maximal ideals in B that contain $\mathfrak{b}$. This shows that all finitely generated algebras over a field is a Jacobson ring.
3. Deduce the result.

2.1 Part 1

Lemma 1. *Let $\mathfrak{m}_a = (t_1 - a_1, \dots t_n - a_n)$ where $a \in k^n$. The ideals of this form are the only maximal ideals in A.*

Proof. Let $a \in k^n$. We define a the evaluation morphism as follows:

$$\begin{aligned} e_a : k[t_1, \dots, t_n] &\longrightarrow k \\ f &\longmapsto f(a). \end{aligned}$$

Note that it is a surjective k-algebra homomorphism and since k is algebraically closed, it has kernel $\mathfrak{m}_a$. Let $\mathfrak{m}$ be a maximal ideal in $k[t_1, \dots, t_n]$. Then $k[t_1, \dots, t_n]/\mathfrak{m}$ is a finitely generated field extension of k. By Zariski's lemma, $k[t_1, \dots, t_n]/\mathfrak{m}$ is in fact a finite field extension, better known as a finite dimensional vector space. Since k is algebraically closed, there is an isomorphism of k-algebras

$$k[t_1, \dots, t_n]/\mathfrak{m} \longrightarrow k.$$

Now, let a_i denote the image of t_i. Then we get that $\mathfrak{m}_a \subseteq \mathfrak{m}$, which implies $\mathfrak{m}_a = \mathfrak{m}$ since $\mathfrak{m}_a$ is a maximal ideal. □

2.2 Part 2

Lemma 2. *Let k be an algebraically closed field, B be a finitely generated k-algebra and $\mathfrak{b}$ be an ideal in B. Then we have*

$$\sqrt{\mathfrak{b}} = \bigcap_{\mathfrak{b} \subseteq \mathfrak{m}} \mathfrak{m}.$$

where $\mathfrak{m}$ are the maximal ideals in B.

Proof. First, we note that the projection $\pi : B \to B/\mathfrak{b}$ induces bijections between the sets

- prime ideals in $B/\mathfrak{b}$ and prime ideals in B that contain $\mathfrak{b}$,
- maximal ideals in $B/\mathfrak{b}$ and maximal ideals in B that contain $\mathfrak{b}$,
- radical ideals in $B/\mathfrak{b}$ and radical ideals in B that contain $\mathfrak{b}$.

Hence we only need to prove the statement for $\mathfrak{b} = (0)$, and since it is clear that $\sqrt{(0)}$ is contained in every maximal ideal because $\sqrt{(0)}$ consists of all nilpotent elements, we only need to show that every element not contained in $\sqrt{(0)}$ is not contained in some maximal ideal.

Let $f \in B$ be non-nilpotent, i.e. $f \in \sqrt{(0)}$. This implies that

$$B_f \cong B[t]/(ft - 1)$$

is a non-trivial k-algebra, hence it has a maximal ideal $\mathfrak{m}$. Consider the morphism $\phi : B \longrightarrow B_f$. This is a morphism of finitely generated k-algebras, and by Zariski's lemma, $k \subseteq B/\phi^{-1}(\mathfrak{m}) \subseteq B_f/\mathfrak{m}$ is a finite extension, and hence $k \subseteq B/\phi^{-1}(\mathfrak{m})$ is an integral extension. Since k is a field, it is a field itself. This gives us that the inverse image of a maximal ideal is again a maximal ideal, i.e. $\phi^{-1}(\mathfrak{m})$ is a maximal ideal of B. But this ideal can't contain f. Hence we have shown that every non-nilpotent element is not contained in all maximal ideals. □

2.3 Part 3

We now deduce the result.

Proof. Let $a \in k^n$. First, note that $a \in Z(\mathfrak{a})$ if and only if $\mathfrak{a} \subseteq \mathfrak{m}_a$. Hence, the maximal ideals containing $\mathfrak{a}$ is just the maximal ideals $\mathfrak{m}_a$ such that $a \in Z(\mathfrak{a})$. In the second step we showed that the radical of an ideal was equal to the intersection of all maximal ideals containing it, hence we have

$$\sqrt{\mathfrak{a}} = \bigcap_{a \in Z(\mathfrak{a})} \mathfrak{m}_a.$$

For the final part, we have for $f \in k[t_1, \ldots, t_n]$ and $a \in k^n$ that $f(x) = 0$ if and only if $f \in \mathfrak{m}_a$. Hence we have for subsets $V \subseteq k^n$ that $I(V) = \bigcap_{a \in V} \mathfrak{m}_a$. And since $a \in Z(\mathfrak{a})$ if and only if $\mathfrak{a} \subseteq \mathfrak{m}_a$ we have finally

$$\begin{aligned} I(Z(\mathfrak{a})) &= \bigcap_{a \in Z(\mathfrak{a})} \mathfrak{m}_a \\ &= \sqrt{\mathfrak{a}}. \end{aligned}$$

And by that, we are done! □