Lecture 12. The weak Nullstellensatz

We next turn to one of the most important theorems in this course.

Theorem 4.29. *(Nullstellensatz - weak version) Suppose that k is algebraically closed. Then, the maximal ideals of $k[X_1, \ldots, X_n]$ are exactly the ideals*

$$(X_1 - a_1, X_2 - a_2, \ldots, X_n - a_n), \text{ where } a_i \in k.$$

Furthermore, if $I \subset k[X_1, \ldots, X_n]$ is a proper ideal, then $\mathcal{V}(I) \neq \emptyset$.

Proof. Let I be an ideal of the form $I = (X_1 - a_1, X_2 - a_2, \ldots, X_n - a_n)$ with $a_i \in k$. Consider the homomorphism $\sigma : k[X_1, X_2, \ldots, X_n] \to k$ given by $X_i \mapsto a_i$, that is, evaluation at $(a_1, \ldots, a_n)$. Then $I \subset \ker(\sigma)$. Moreover $\ker(\sigma)$ is a maximal ideal since σ is onto, so that $k[X_1, \ldots, X_n]/\ker(\sigma) \simeq k$. On the other hand, let $f \in \ker(\sigma)$. Choose a monomial order and divide f by $X_1 - a_1, \ldots, X_n - a_n$, whose leading monomials are $X_1, \ldots, X_n$, to write

$$f = h_1(X_1 - a_1) + h_2(X_2 - a_2) + \ldots + h_n(X_n - a_n) + r, \text{ with } r \in k$$

(the remainder contains no monomial divisible by any X_i, so it is a constant). Then $0 = f(a_1, a_2, \ldots, a_n) = r$, hence $f \in I$. Thus, we have $I = \ker(\sigma)$, which is maximal.

Conversely, suppose $\mathfrak{m} \subset k[X_1, \ldots, X_n]$ is a maximal ideal. Then $A = k[X_1, \ldots, X_n]/\mathfrak{m}$ is a field that is a finitely generated k-algebra. By Noether normalisation (Theorem 4.25), we can find $u_1, \ldots, u_d \in A$ which are algebraically independent such that the extension $A \supset k[u_1, \ldots, u_d]$ is integral. But A is a field, therefore $k[u_1, \ldots, u_d]$ is a field by Corollary 4.23(d). Now, $k[u_1, \ldots, u_d]$ is a polynomial ring in d variables, which is not a field if $d \geq 1$ (the variable u_1 has no inverse), hence $d = 0$. In other words, $A \supset k$ is an integral extension. This means that $A \supset k$ is an algebraic extension of fields but k is algebraically closed, hence $A = k$. Thus, if we define a_i to be the image of X_i under the isomorphism $k[X_1, \ldots, X_n]/\mathfrak{m} \simeq k$, we see that $X_i - a_i \in \mathfrak{m}$. Hence,

$$(X_1 - a_1, X_2 - a_2, \ldots, X_n - a_n) \subset \mathfrak{m}$$

but $(X_1 - a_1, X_2 - a_2, \ldots, X_n - a_n)$ is a maximal ideal, hence

$$\mathfrak{m} = (X_1 - a_1, X_2 - a_2, \ldots, X_n - a_n).$$

In particular, if I is a proper ideal, by Proposition 2.4 (!) there exists a maximal ideal containing I, that is, there exist $a_1, a_2, \ldots, a_n$ such that

$$(X_1 - a_1, X_2 - a_2, \ldots, X_n - a_n) \supset I$$

Hence, applying $\mathcal{V}$, we see that $(a_1, a_2, \ldots, a_n) \in \mathcal{V}(I)$. □

▶ So, for k algebraically closed, the points of k^n correspond bijectively to the maximal ideals of $k[X_1, \ldots, X_n]$:

$$a = (a_1, \ldots, a_n) \longmapsto \mathfrak{m}_a = (X_1 - a_1, \ldots, X_n - a_n),$$

the kernel of evaluation at a (different points give different ideals, since $\mathcal{V}(\mathfrak{m}_a) = \{a\}$). Moreover, $I \subset \mathfrak{m}_a$ if and only if every polynomial in I vanishes at a, that is, $a \in \mathcal{V}(I)$: the points of $\mathcal{V}(I)$ are the maximal ideals containing I. In this dictionary, the second statement of the theorem is Proposition 2.4: a proper ideal is contained in a maximal ideal.

▶ In the course of the proof, we saw a proof of the following statement:

Lemma 4.30. *(Zariski's lemma) Suppose that a field K is finitely generated as an algebra over a field k. Then K is finitely generated as a k-module, that is, $K \supset k$ is a finite field extension.*

In other words, for a field extension the two notions of finitely generated coincide. Indeed, the argument above did not use that k is algebraically closed until its last step: for any field k it shows that K is integral over k, hence a finitely generated k-module by Corollary 4.23(a). There are other, direct proofs of Zariski's lemma, which can be used to give a different proof of the Nullstellensatz.

At the end of the proof, I sneakily appealed to Proposition 2.4 whose proof uses Zorn's lemma to show that every proper ideal is contained in a maximal ideal. Most books on commutative algebra do this. Of course, it is rather unsatisfactory[7]. Let us remark that Proposition 2.4 was proved for a general commutative ring. The above theorem is concerned with the ring $k[X_1, \ldots, X_n]$ which we know is Noetherian from Theorem 4.1 and so the existence of a maximal ideal containing a proper ideal can be proved directly (just form an ascending chain out of ideals containing I and appeal to the Noetherian property to show that such a chain stabilises). However, this too uses a countable version of the Axiom of Choice since we make infinitely many choices as we form the ascending chain.

For the true constructivists, let us now give a constructive proof following the nice article by Arrondo [8] which avoids any choice.

Theorem 4.31. *(Nullstellensatz without choice) Let k be any field. Any proper ideal $I \subset k[X_1, X_2 \ldots, X_n]$ is contained in a maximal ideal $\mathfrak{m}$.*

We first prove a lemma that we will use for the inductive step of the proof.

Lemma 4.32. *Let $I \subset k[X_1, \ldots, X_n]$ be a proper ideal containing a polynomial g that is monic in X_n, that is,*

$$g = X_n^d + X_n^{d-1} g_{d-1} + \ldots + X_n g_1 + g_0 \text{ with } g_i \in k[X_1, \ldots, X_{n-1}],$$

and let $\mathfrak{m}' \subset k[X_1, \ldots, X_{n-1}]$ be a maximal ideal containing $I' = I \cap k[X_1, \ldots, X_{n-1}]$. Denote by $(\mathfrak{m}')$ the ideal generated by $\mathfrak{m}'$ in $k[X_1, \ldots, X_n]$; it consists of the polynomials in X_n whose coefficients lie in $\mathfrak{m}'$. Then the ideal $I + (\mathfrak{m}') \subset k[X_1, \ldots, X_n]$ is proper.

[7] There are people out there who build machines using polynomial equations.

Proof. Suppose for contradiction there exist $f \in I$ and $f' \in (\mathfrak{m}')$ such that $f + f' = 1$ or equivalently $f - 1 \in (\mathfrak{m}')$. Let us write

$$f = f_e X_n^e + f_{e-1} X_n^{e-1} + \ldots + f_1 X_n + f_0 \text{ with } f_i \in k[X_1, X_2, \ldots, X_{n-1}].$$

Since $f - 1 \in (\mathfrak{m}')$, we have $f_0 - 1, f_1, f_2, \ldots, f_e \in \mathfrak{m}'$. Viewing both f and g as polynomials in X_n with coefficients in $k[X_1, \ldots, X_{n-1}]$, we can consider their **resultant** with respect to the variable X_n. This is the polynomial in $k[X_1, \ldots, X_{n-1}]$ given by the determinant

$$R = \begin{vmatrix} f_0 & f_1 & \ldots & f_e & 0 & 0 & \ldots & 0 \\ 0 & f_0 & \ldots & f_{e-1} & f_e & 0 & \ldots & 0 \\ & & \ddots & & & & & \\ 0 & \ldots & 0 & f_0 & f_1 & \ldots & f_{e-1} & f_e \\ g_0 & g_1 & \ldots & g_{d-1} & 1 & 0 & \ldots & 0 \\ 0 & g_0 & \ldots & g_{d-2} & g_{d-1} & 1 & 0 \ldots & 0 \\ & & \ddots & & & & \ddots & \\ 0 & \ldots & 0 & g_0 & g_1 & \ldots & g_{d-1} & 1 \end{vmatrix} \begin{matrix} \left.\vphantom{\begin{matrix} a \\ a \\ a \\ a \end{matrix}}\right\} d \text{ rows} \\ \left.\vphantom{\begin{matrix} a \\ a \\ a \\ a \end{matrix}}\right\} e \text{ rows} \\ . \end{matrix}$$

First note that R belongs to I. To see this, multiply the second column by X_n, third column by X_n^2 , and so on until the last column which is to be multiplied by X_n^{d+e-1} and add all these to the first column. This doesn't change the determinant. The resulting matrix then is as follows:

$$R = \begin{vmatrix} f & f_1 & \ldots & f_e & 0 & 0 & \ldots & 0 \\ X_n f & f_0 & \ldots & f_{e-1} & f_e & 0 & \ldots & 0 \\ & \ddots & & & & & & \\ X_n^{d-1} f & \ldots & 0 & f_0 & f_1 & \ldots & f_{e-1} & f_e \\ g & g_1 & \ldots & g_{d-1} & 1 & 0 & \ldots & 0 \\ X_n g & g_0 & \ldots & g_{d-2} & g_{d-1} & 1 & 0 \ldots & 0 \\ & & \ddots & & & & \ddots & \\ X_n^{e-1} g & \ldots & 0 & g_0 & g_1 & \ldots & g_{d-1} & 1 \end{vmatrix} \begin{matrix} \left.\vphantom{\begin{matrix} a \\ a \\ a \\ a \end{matrix}}\right\} d \text{ rows} \\ \left.\vphantom{\begin{matrix} a \\ a \\ a \\ a \end{matrix}}\right\} e \text{ rows} \\ . \end{matrix}$$

Now, expanding the determinant along the first column shows that R is a linear combination of f and g with coefficients in $k[X_1, \ldots, X_n]$, so $R \in I$. Thus, $R \in I \cap k[X_1, \ldots, X_{n-1}] = I' \subset \mathfrak{m}'$. On the other hand, in $k[X_1, \ldots, X_{n-1}]/\mathfrak{m}'$, the original matrix representing R becomes a lower triangular matrix with 1 as the diagonal entries: since $f_0 - 1, f_1, \ldots, f_e \in \mathfrak{m}'$, its first d rows become the first d standard basis vectors, and in the remaining rows the entry 1 lies on the diagonal, with only zeros to its right. Hence $R = 1 \in k[X_1, \ldots, X_{n-1}]/\mathfrak{m}'$, that is $R \notin \mathfrak{m}'$, which is a contradiction. □

► For k algebraically closed, Theorem 4.29 gives the lemma a geometric meaning. The maximal ideal $\mathfrak{m}'$ is a point $b \in k^{n-1}$, which lies in $\mathcal{V}(I')$ since $I' \subset \mathfrak{m}'$, and the zeros of $I + (\mathfrak{m}')$ are the points of $\mathcal{V}(I)$ above b for the projection $k^n \to k^{n-1}$ forgetting the last coordinate. So the lemma

says that every point of $\mathcal{V}(I')$ is the image of a point of $\mathcal{V}(I)$. The monic polynomial g is what prevents points of $\mathcal{V}(I)$ from escaping to infinity above b: its restriction $g(b, X_n) = X_n^d + \dots$ still has degree d. Without it the lemma fails: for $I = (XY - 1) \subset k[X, Y]$ we have $I' = 0$, and for $\mathfrak{m}' = (X)$ the ideal $(XY - 1, X)$ contains 1. The change of variables of Lemma 4.26 repairs this, see Figure 4.

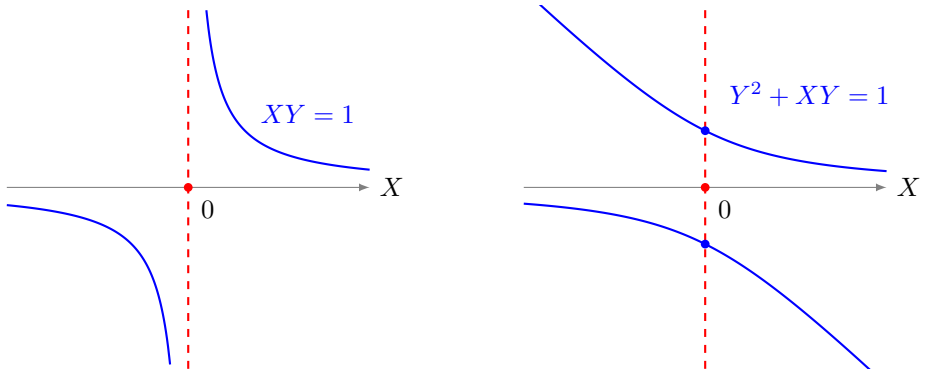


Figure 4: The hyperbola $XY = 1$ has no point above $X = 0$: the ideal $(XY - 1) + (X)$ is not proper. After the change of variables $X \mapsto X + Y$ it becomes $Y^2 + XY = 1$, which is monic in Y and meets every vertical line.

Proof of Theorem 4.31. We argue by induction on n. For $n = 1$, recall that $k[X]$ is a PID, so $I = (f)$ for some f, which is either 0 or non-constant since I is proper. If $f = 0$ then $I \subset (X)$, and if f is non-constant then any irreducible factor p of f generates a maximal ideal (p) containing (f).

Suppose $n > 1$. If $I = (0)$, then I is contained in the maximal ideal $(X_1, \dots, X_n)$, so assume $I \neq (0)$ and let $g \in I$ be non-zero; it is non-constant since I is proper. By Lemma 4.26, there is a change of variables $X_i \mapsto X_i + \phi_i(X_n)$, $i < n$, after which g becomes monic in X_n up to a non-zero constant factor. This change of variables is an automorphism of $k[X_1, \dots, X_n]$, so it preserves inclusions and maximality of ideals, and we may assume that I contains a polynomial g monic in X_n, as in Lemma 4.32. Now, consider $I' = I \cap k[X_1, \dots, X_{n-1}]$. Since I is proper, $1 \notin I$, hence I' is also proper. By the induction hypothesis, there exists a maximal ideal $\mathfrak{m}'$ containing I'. Let k' be the field $k' = k[X_1, \dots, X_{n-1}]/\mathfrak{m}'$. Reducing coefficients modulo $\mathfrak{m}'$ gives a surjective homomorphism $k[X_1, \dots, X_n] = k[X_1, \dots, X_{n-1}][X_n] \to k'[X_n]$ with kernel $(\mathfrak{m}')$, hence an isomorphism $k[X_1, \dots, X_n]/(\mathfrak{m}') \simeq k'[X_n]$. Composing its inverse with the quotient map, we obtain a surjective homomorphism $\pi : k'[X_n] \to k[X_1, X_2, \dots, X_n]/(I + (\mathfrak{m}'))$ and an isomorphism of rings

$$k'[X_n]/\mathrm{Ker}(\pi) \simeq k[X_1, X_2, \dots, X_n]/(I + (\mathfrak{m}')).$$

Now, by Lemma 4.32, $I + (\mathfrak{m}')$ is a proper ideal, hence $\mathrm{Ker}(\pi)$ is a proper ideal of $k'[X_n]$. By the case $n = 1$ applied to the field k', there is a maximal ideal $\mathfrak{n}$ of $k'[X_n]$ containing $\mathrm{Ker}(\pi)$. Since the ideals of a quotient ring R/J are the ideals of R containing J, with inclusions preserved, $\mathfrak{n}/\mathrm{Ker}(\pi)$ is a maximal ideal of $k'[X_n]/\mathrm{Ker}(\pi)$; the above isomorphism carries it to a maximal

ideal of $k[X_1, \ldots, X_n]/(I + (\mathfrak{m}'))$, that is, to $\mathfrak{m}/(I + (\mathfrak{m}'))$ for a maximal ideal $\mathfrak{m}$ of $k[X_1, \ldots, X_n]$ containing $I + (\mathfrak{m}')$, hence also containing I. Concretely, $\mathfrak{m}$ consists of the polynomials whose reduction modulo $\mathfrak{m}'$ lies in $\mathfrak{n}$. □

There you go; a proof without the Axiom of Choice. From now on, as long as we work with polynomial rings with field coefficients and their quotients, you can rest assured that every proper ideal has a maximal ideal containing it.