Lecture 13. The strong Nullstellensatz

Theorem 4.33. *(Nullstellensatz - strong version) Suppose that k is algebraically closed and let $I \subset k[X_1, \ldots, X_n]$ be an ideal. Then*

$$\mathcal{I}(\mathcal{V}(I)) = \sqrt{I}.$$

Proof. The inclusion $\sqrt{I} \subset \mathcal{I}(\mathcal{V}(I))$ is easy: if $f \in \sqrt{I}$, then $f^\ell \in I$ for some $\ell \geq 1$, so f^ℓ, and hence f, vanishes at every point of $\mathcal{V}(I)$.

Conversely, write $I = (f_1, \ldots, f_s)$, using the Hilbert basis theorem, and let $f \in \mathcal{I}(\mathcal{V}(I))$. Explicitly, this means that if $(a_1, \ldots, a_n) \in k^n$ satisfies $f_i(a_1, \ldots, a_n) = 0$ for all i, then $f(a_1, \ldots, a_n) = 0$. We may assume $f \neq 0$, and we need to show that there exist $\ell > 0$ and $h_1, \ldots, h_s \in k[X_1, \ldots, X_n]$ such that

$$f^\ell = \sum_{i=1}^{s} h_i f_i.$$

For this, we use the Rabinowitsch trick: consider the polynomial ring $k[X_1, \ldots, X_n, Y]$ in one more variable and the ideal $\tilde{I} = (f_1, \ldots, f_s, 1 - Yf) \subset k[X_1, \ldots, X_n, Y]$. We claim that $\tilde{I} = k[X_1, \ldots, X_n, Y]$. Indeed, if $\tilde{I}$ were a proper ideal, then by the weak Nullstellensatz (Theorem 4.29) it would have a zero $(a_1, \ldots, a_n, a_{n+1}) \in k^{n+1}$. Then $f_i(a_1, \ldots, a_n) = 0$ for all i, hence $f(a_1, \ldots, a_n) = 0$, but also

$$1 - f(a_1, \ldots, a_n)a_{n+1} = 0,$$

a contradiction. Hence $1 \in \tilde{I}$, and we can write

$$1 = \sum_{i=1}^{s} g_i f_i + g_0(1 - Yf) \text{ for some } \; g_0, g_1, \ldots, g_s \in k[X_1, \ldots, X_n, Y].$$

Now apply the ring homomorphism $k[X_1, \ldots, X_n, Y] \to k(X_1, \ldots, X_n)$ which sends $X_i \mapsto X_i$ for $1 \leq i \leq n$ and $Y \mapsto \frac{1}{f}$. The last term vanishes, and we get

$$1 = \sum_{i=1}^{s} g_i(X_1, \ldots, X_n, \tfrac{1}{f}) f_i$$

in $k(X_1, \ldots, X_n)$. Multiplying by f^ℓ, where ℓ is the largest power of Y appearing in $g_1, \ldots, g_s$, clears the denominators: $h_i \coloneqq f^\ell g_i(X_1, \ldots, X_n, \frac{1}{f})$ lies in $k[X_1, \ldots, X_n]$, and

$$f^\ell = \sum_{i=1}^{s} h_i f_i.$$

□

▶ The theorem says that the only way a polynomial can vanish on $\mathcal{V}(I)$ without belonging to I is that one of its powers belongs to I. For instance, let $I = (Y - X^2, Y) \subset k[X, Y]$, which describes the intersection of the parabola $Y = X^2$ with the line $Y = 0$, see Figure 5. Then $\mathcal{V}(I) = \{(0, 0)\}$ and $\mathcal{I}(\mathcal{V}(I)) = (X, Y)$, but $X \notin I = (X^2, Y)$: the ideal remembers that the line is tangent to the parabola, as $k[X, Y]/I$ has dimension 2 rather than 1. By contrast, the line $Y = X$ meets the parabola transversally at $(0, 0)$ and $(1, 1)$, and the ideal $(Y - X^2, Y - X) = (X^2 - X, Y - X)$ is radical. The hypothesis that k is algebraically closed cannot be dropped: over $\mathbb{R}$, the ideal $(X^2 + Y^2)$ is prime, hence radical, but its variety is the single point $(0, 0)$, whose ideal is (X, Y).

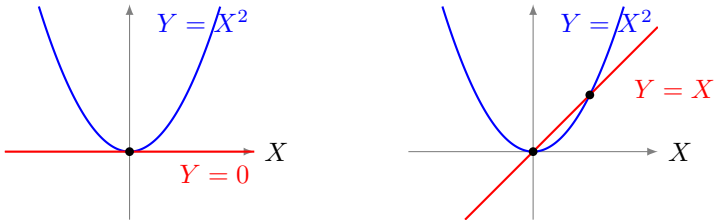


Figure 5: The parabola $Y = X^2$ meets the line $Y = 0$ only at the origin, with multiplicity two: the ideal $(Y - X^2, Y) = (X^2, Y)$ is not radical. It meets the line $Y = X$ transversally at two points, and $(Y - X^2, Y - X) = (X^2 - X, Y - X)$ is radical.

▶ The most important consequence of the Nullstellensatz is that, for k algebraically closed, $\mathcal{I}$ and $\mathcal{V}$ are mutually inverse, inclusion-reversing bijections

$$\{\text{affine varieties in } k^n\} \underset{\mathcal{V}}{\overset{\mathcal{I}}{\rightleftarrows}} \{\text{radical ideals of } k[X_1, \ldots, X_n]\}.$$

Indeed, $\mathcal{V}(\mathcal{I}(V)) = V$ for every affine variety V (an exercise in Lecture 5), $\mathcal{I}(U)$ is a radical ideal for any $U \subset k^n$, and $\mathcal{I}(\mathcal{V}(J)) = J$ for a radical ideal J by the theorem. Points of k^n correspond to maximal ideals, as we saw in Lecture 12, and we will see in the next lecture that irreducible varieties correspond to prime ideals.

Corollary 4.34. *Let k be a field (not necessarily algebraically closed) and $I = (f_1, \ldots, f_s) \subset k[X_1, \ldots, X_n]$. Then $f \in \sqrt{I}$ if and only if 1 belongs to the ideal $\tilde{I} = (f_1, \ldots, f_s, 1 - Yf) \subset k[X_1, \ldots, X_n, Y]$.*

Proof. If $f = 0$ there is nothing to prove. Otherwise, the second half of the proof of Theorem 4.33, from $1 \in \tilde{I}$ on, works over any field and shows that $1 \in \tilde{I}$ implies $f \in \sqrt{I}$. Conversely, suppose $f \in \sqrt{I}$, so that $f^\ell \in I$ for some $\ell > 0$. Since also $1 - Yf \in \tilde{I}$, we can write

$$1 = Y^\ell f^\ell + (1 - Y^\ell f^\ell) = Y^\ell f^\ell + (1 - Yf) \cdot (1 + Yf + \ldots + Y^{\ell-1} f^{\ell-1}) \in \tilde{I}.$$

□

This corollary gives an algorithm for deciding whether $f \in \sqrt{I}$: compute a Gröbner basis of $(f_1, \ldots, f_s, 1 - Yf)$ and check whether it contains a non-zero constant.

◁ Consider the 2-by-2 matrix M with entries X, Y, Z, W. The equation $M^2 = 0$ gives four polynomial equations, which generate the ideal $I = (X^2+YZ, XY+YW, XZ+WZ, W^2+YZ) \subset k[X, Y, Z, W]$. Is I a radical ideal? Show that $\sqrt{I} = (X + W, XW - YZ)$. (Hint: a nilpotent matrix has trace and determinant zero, and the converse holds for 2-by-2 matrices by the Cayley–Hamilton theorem.)

You can also do this in Macaulay2:

```
R = QQ[x,y,z,w];
I = ideal (x^2+y*z,x*y+y*w,x*z+w*z,w^2+y*z);
I == radical I
radical I
```

◁ (Hard) Consider an n-by-n matrix X with entries $X_{i,j}$ for $1 \leq i, j \leq n$ and an n-by-n matrix Y with entries $Y_{i,j}$ for $1 \leq i, j \leq n$. Form the ideal $I \subset \mathbb{C}[X_{i,j}, Y_{i,j}]_{1 \leq i,j \leq n}$ generated by the entries of the matrix $XY - YX$. Is I a radical ideal? It has been known since the 1950s that $\sqrt{I}$ is prime for all n, and whether I itself is prime, that is, radical, was a well-known open question going back to Artin and Hochster (1982). For $n \leq 4$ the answer is yes, by Gröbner basis computations for $n = 3, 4$, and a recent preprint[8] claims a proof for all n. We can check the case $n = 3$ in Macaulay2 as follows:

```
n=3
R = QQ[x_(1,1)..x_(n,n),y_(1,1)..y_(n,n)]
M = matrix table (n, n, (i,j) -> x_(i+1,j+1))
N = matrix table (n, n, (i,j) -> y_(i+1,j+1))
I = minors(1, M*N-N*M)
isPrime I
```

If you want to break your computer, you can set n to a higher value and run the same code.

Corollary 4.35. *Let k be algebraically closed and let $I \subset k[X_1, \ldots, X_n]$ be a proper ideal, so that $V = \mathcal{V}(I)$ is non-empty by the weak Nullstellensatz. Then*

$$\dim(V) = \deg HP_I(t),$$

where $\dim(V) \coloneqq \deg HP_{\mathcal{I}(V)}(t)$. In other words, the dimension of V can be computed from any ideal I with $\mathcal{V}(I) = V$.

Proof. Since $I \subset \mathcal{I}(V)$, we have $I_{\leq s} \subset \mathcal{I}(V)_{\leq s}$, hence $HF_{\mathcal{I}(V)}(s) \leq HF_I(s)$ for all s and $\deg HP_{\mathcal{I}(V)}(t) \leq \deg HP_I(t)$. For the other inequality, let $d = \deg HP_I(t)$. By Corollary 4.18, there exist $1 \leq i_1 < i_2 < \ldots < i_d \leq n$ such that $I \cap k[X_{i_1}, X_{i_2}, \ldots, X_{i_d}] = \{0\}$, and by the same corollary it suffices to show that

$$\mathcal{I}(V) \cap k[X_{i_1}, X_{i_2}, \ldots, X_{i_d}] = \{0\}.$$

[8] J. Sempliner, X. Yang, On the normality of the commuting scheme, arXiv:2609.27360 (2026).

Let $f \in \mathcal{I}(V) \cap k[X_{i_1}, X_{i_2}, \ldots, X_{i_d}]$. Since $\mathcal{I}(V) = \sqrt{I}$ by Theorem 4.33, there exists $\ell \geq 1$ such that $f^\ell \in I$. But f^ℓ also lies in $k[X_{i_1}, X_{i_2}, \ldots, X_{i_d}]$, so $f^\ell \in I \cap k[X_{i_1}, X_{i_2}, \ldots, X_{i_d}] = \{0\}$. Thus $f = 0$. □

Corollary 4.36. *Let k be algebraically closed and let $I \subset k[X_1, X_2, \ldots, X_n]$ be a proper ideal. Then $\sqrt{I}$ is the intersection of the maximal ideals containing I:*

$$\sqrt{I} = \bigcap_{\mathfrak{m} \supset I} \mathfrak{m}.$$

Proof. The inclusion $\sqrt{I} \subset \bigcap_{\mathfrak{m} \supset I} \mathfrak{m}$ holds in any ring, since a maximal ideal is prime, so $I \subset \mathfrak{m}$ implies $\sqrt{I} \subset \mathfrak{m}$. Conversely, let $f \in \bigcap_{\mathfrak{m} \supset I} \mathfrak{m}$. By the weak Nullstellensatz (Theorem 4.29), the maximal ideals containing I are the ideals $\mathfrak{m}_a = (X_1 - a_1, \ldots, X_n - a_n)$ with $a = (a_1, \ldots, a_n) \in \mathcal{V}(I)$, and $f \in \mathfrak{m}_a$ means $f(a) = 0$. Therefore f vanishes on $\mathcal{V}(I)$, and by the strong Nullstellensatz $f \in \mathcal{I}(\mathcal{V}(I)) = \sqrt{I}$. □

The last corollary should be contrasted with Proposition 2.7, which says that $\sqrt{I}$ is the intersection of the prime ideals containing I. Firstly, in $k[X_1, \ldots, X_n]$ it suffices to take the maximal ideals containing I. Secondly, we have an explicit description of these maximal ideals, or equivalently of the maximal ideals of the ring $k[X_1, \ldots, X_n]/I$: they are in bijection with the points of $\mathcal{V}(I)$.

A ring R is called a **Jacobson ring** or **Hilbert ring** if every prime ideal of R is an intersection of maximal ideals. Equivalently, for every ideal I of R, the nilradical and the Jacobson radical of R/I coincide. The last corollary says that $k[X_1, \ldots, X_n]$ is a Jacobson ring when k is algebraically closed. A field is obviously a Jacobson ring, and so is $\mathbb{Z}$, but the local ring $k[[X]]$ is not: (0) is a prime ideal, but the only maximal ideal is (X). A generalisation of Hilbert's Nullstellensatz states that any finitely generated algebra over a Jacobson ring is Jacobson; in particular, $k[X_1, \ldots, X_n]$ is a Jacobson ring for every field k.