(c)Karen E. Smith 2018 UM Math Dept
licensed under a Creative Commons
By-NC-SA 4.0 International License.

Math 614: Hilbert's Nullstellensatz

Fix a field K. There are natural order reversing maps of sets:

$$\{\text{Radical Ideals in } K[x_1,\dots,x_n]\} \rightleftarrows \{\text{Algebraic Sets in } K^n\}$$
$$I \longrightarrow \mathbb{V}(I)$$
$$\mathbb{I}(V) \longleftarrow V$$

Hilbert's Nullenstellensatz: If K is algebraically closed, then these maps are mutually inverse.

---

(1) RECALL FROM LAST TIME:
- (a) How is each of these maps is defined?
- (b) Points are special cases of algebraic sets V in K^n. Describe $\mathbb{I}(V)$ in this case, both intrinsically (without giving generators) and explicitly (by describing generators).
- (c) $\langle 0\rangle$ and $\langle 1\rangle$ are special cases of ideals I in $K[x_1,\dots,x_n]$. Describe $\mathbb{V}(I)\subset K^n$ in these cases.
- (d) The ideals $\langle x,y\rangle$ and $\langle x^2+y^2\rangle$ are special cases of ideals I in $\mathbb{R}[x,y]$. Describe $\mathbb{V}(I)\subset\mathbb{R}^2$ in these cases.
- (e) The ideals $\langle 0\rangle$ and $\langle x^p-x, xy^p-x^py\rangle$ are special cases of radical ideals I in $\mathbb{F}_p[x,y]$. Describe $\mathbb{V}(I)\subset\mathbb{F}_p^2$ in these cases.

(2) Consider the map $\overline{\mathbb{F}_{17}}^2 \to \overline{\mathbb{F}_{17}}^3$ sending $(u,v)\mapsto(u^2,uv,v^2)$. Prove that the image is an algebraic set in K^3. Find the corresponding radical ideal in $\overline{\mathbb{F}_{17}}[x,y,z]$. [Hint: Eisenstein's criterion might be useful.]

THE PROOF OF HILBERT'S NULLSTELLENSATZ OVER $\mathbb{C}$.

(3) REDUCTION TO THE CORE DIFFICULTY.
- (a) Last time you showed that the composition of $\mathbb{I}$ and $\mathbb{V}$ in some order is the identity, whether or not $K=\overline{K}$. Which order?
- (b) Also recall your proof that, whether or not $K=\overline{K}$, for any ideal $I\subset K[x_1,\dots,x_n]$, $I\subset\sqrt{I}\subset\mathbb{I}(\mathbb{V}(I))$.
- (c) When $K=\overline{K}$, conclude that to prove the Nullstellensatz, it suffices to show that for all ideals I,
$$\mathbb{I}(\mathbb{V}(I))\subset\sqrt{I}.$$

(4) THE CASE WHERE I IS MAXIMAL. *We need to show that* $\mathbb{I}(\mathbb{V}(m))\subset m$.
- (a) Let $m\in K[x_1,\dots,x_n]$ be a maximal ideal. Show that $K[x_1,\dots,x_n]/m$ has countable dimension over K.
- (b) Let K be an infinite field, and let t be a transcendental element of some extension L. Prove that the elements $\{\frac{1}{t-\lambda}\}_{\lambda\in K}\subset L$ are linearly independent over K.
- (c) Assume K is uncountable. With notation as in (b), show that $[L:K]$ is uncountable.
- (d) Let K be an uncountable field. Let $m\in K[x_1,\dots,x_n]$ be a maximal ideal. Show that $K\hookrightarrow K[x_1,\dots,x_n]/m$ is an algebraic extension.
- (e) Prove that if K is an uncountable algebraically closed field, then every maximal ideal has the form $\langle x_1-a_1,\dots,x_n-a_n\rangle$, where $a_i\in K$.
- (f) Deduce that when $K=\mathbb{C}$, the maps $\mathbb{V}$ and $\mathbb{I}$ define inverse bijections between points $\mathbb{C}^n$ and maximal ideals of $\mathbb{C}[x_1,\dots,x_n]$. (Call this the **Nullstellensatz for Points**.)

(5) THE CASE OF THE UNIT IDEAL. Let K be algebraically closed, and let $I \subset K[x_1, \dots, x_n]$ be an ideal. Assuming the Nullstellensatz for points, show that $\mathbb{V}(I)$ is empty if and only if I is the unit ideal.

(6) THE GENERAL CASE. Let K be algebraically closed. We now deduce the full Nullstellensatz from the special cases already proven in (3) - (5).

Let $I = \langle f_1, \dots, f_t \rangle$ be an arbitrary ideal. We want to show $\mathbb{I}(\mathbb{V}(I)) \subset \sqrt{I}$.

(a) Choose $g \in \mathbb{I}(\mathbb{V}(I))$. Prove that $\langle f_1, \dots, f_t, gz-1 \rangle = \langle 1 \rangle$ in the larger polynomial ring $K[x_1, \dots, x_n, z]$.

(b) Prove that we can write $1 = \frac{g_1 f_1 + \cdots + g_t f_t}{g^T}$ (in $K(x_1, \dots, x_n)$) for some $g_1, \dots, g_t \in K[x_1, \dots, x_n]$ and some $T \in \mathbb{N}$. [Hint: Write $1 = h_1 f_1 + \cdots + h_t f_t + h_{t+1}(1 - gz)$ where $h_1, \dots, h_t, h_{t+1} \in K[x_1, \dots, x_n, z]$. Apply an appropriate map $K[x_1, \dots, x_n, z] \to K[x_1, \dots, x_n][\frac{1}{g}]$ sending z to $\frac{1}{g}$.]

(c) Conclude that $g \in \sqrt{I}$. The Nullstellensatz is proved, at least over $\mathbb{C}$!

You've now proved Hilbert's Nullstellensatz for **uncountable** K, including $\mathbb{C}$. You've also reduced the general statement to the following:
If $K = \overline{K}$, then every maximal ideal of $k[x_1, \dots, x_n]$ is of the form m_p for some $p \in K^n$.
WE WILL PROVE THIS LATER, AFTER SOME MORE GENERAL THEORY.

(7) **Assuming Hilbert's Nullstellensatz:** show that if $K = \overline{K}$ and $V \subset K^n$ is any algebraic set, then there are mutually inverse order reversing maps

$$\begin{array}{ccc} \{\text{Reduced Homomorphic } K\text{-algebra images of } K[V]\} & \rightleftarrows & \{\text{Algebraic Subsets of } V\} \\ \operatorname{im}(\pi) & \longrightarrow & \{p \in V \mid f(p) = 0 \ \forall f \in \ker \pi\} \\ (K[V] \xrightarrow[functions]{restrict} K[W]) & \longleftarrow & W \end{array}$$

HINT: Compare also to the set of radical ideals in $K[V]$. Make use of the isomorphism theorems for rings.

---

(8) An algebraic set is **irreducible** if and only if it is not a union of two proper sub-algebraic sets. Prove that an algebraic set V is irreducible if and only if $\mathbb{I}(V)$ is prime. [HINT: $W \subsetneq V$ iff $\exists f \in \mathbb{I}(W) \setminus \mathbb{I}(V)$.]

(9) Fix an algebraic set $V \subset K^n$, where $K = \overline{K}$. Prove that there is a bijection between the non-empty irreducible sub-algebraic sets of V and points of $\operatorname{Spec} k[V]$.

(10) Fix an algebraic set $V \subset K^n$, where $K = \overline{K}$. Recall that there is a topology on V whose closed sets are the sub-algebraic sets. Prove that with this topology, V is homeomorphic to $\operatorname{maxSpec} k[V]$.

(11) Let K be arbitrary, and let $I \subset K[x_1, \dots, x_n]$. Consider the mapping

$$\{\text{Field extensions of } K\} \xrightarrow{\mathcal{V}} \{Sets\}$$
$$L \longrightarrow \mathbb{V}(I) \subset L^n$$

where we view the elements of I as elements also of the overring $L[x_1, \dots, x_n]$.

(a) For the ideal generated by $x^2 + y^2 \in \mathbb{Q}[x, y]$, describe the sets $\mathcal{V}(\mathbb{Q})$, $\mathcal{V}(\mathbb{R})$, $\mathcal{V}(\mathbb{C})$

(b) We can view $\mathcal{V}$ as (part of the information) of a functor. Explain.

(c) Enlarge the source of $\mathcal{V}$ to include all (commutative, unital) K-algebras. Prove that $\mathcal{V}$ defines a representable functor from the category of K-algebras to the category of sets. This is one rather fancy way to define an "affine scheme of finite type over K".