WORKSHEET 3.1: THE NULLSTELLENSATZ

Throughout this course, "ring" means *commutative* ring with unity. In this worksheet $\mathbb{K}$ will denote a field. In the previous worksheet you built the order-reversing maps

$$I \longmapsto \mathbb{V}(I) \qquad \text{and} \qquad V \longmapsto \mathbb{I}(V)$$

connecting ideals in $\mathbb{K}[x_1,\dots,x_n]$ with algebraic sets in $\mathbb{K}^n$. Our goal now is to prove that over an algebraically closed field these constructions *almost* recover each other exactly. The only restriction being that since $\mathbb{I}(V)$ is always a radical ideal, these functions are only bijections when restricted to the set of radical ideals in $\mathbb{K}[x_1,\dots,x_n]$. More precisely, our goal is to prove the first two versions of Hilbert's Nullstellensatz under the condition that $\mathbb{K}$ is uncountable (i.e. $\mathbb{C}$). Although our work will also show the second version follows from the first for any algebraically closed field.

Theorem 1 (Hilbert's Nullstellensatz I)**.** *If $\mathbb{K}$ is algebraically closed, then every maximal ideal of $\mathbb{K}[x_1,\dots,x_n]$ is of the form $\langle x_1-a_1,\dots,x_n-a_n\rangle$ for some point $(a_1,\dots,a_n)\in\mathbb{K}^n$.*

Theorem 2 (Hilbert's Nullstellensatz II)**.** *If $\mathbb{K}$ is algebraically closed and $V=\mathbb{V}(\mathscr{S})\subset\mathbb{K}^n$ is an algebraic set, for some subset $\mathscr{S}\subset\mathbb{K}[x_1,\dots,x_n]$, then $\mathbb{I}(V)=\sqrt{\langle\mathscr{S}\rangle}$.*

For a point $p=(a_1,\dots,a_n)\in\mathbb{K}^n$, we will often write $\mathfrak{m}_p$ for the ideal $\langle x_1-a_1,\dots,x_n-a_n\rangle\subset\mathbb{K}[x_1,\dots,x_n]$, which by the previous worksheet is the kernel of the evaluation-at-p map $\mathrm{ev}_p:\mathbb{K}[x_1,\dots,x_n]\to\mathbb{K}$. An alternative statement of Hilbert's Nullstellensatz I is to say there is a bijection between $\mathbb{K}^n$ and maximal ideals in $\mathbb{K}[x_1,\dots,x_n]$ given by $p\mapsto\mathfrak{m}_p$. We say that this statement can fail when $\mathbb{K}$ is not algebraically closed, e.g., $\langle x^2+1\rangle\subset\mathbb{R}[x]$.

Since points are themselves algebraic sets, the second version of Hilbert's Nullstellensatz can be thought of as a generalization of the first. In particular Nullstellensatz II can be thought of as saying that $\mathbb{V}$ and $\mathbb{I}$ are mutual inverses giving bijections

$$\left\{\begin{array}{c}\text{algebraic sets}\\ \text{in } \mathbb{K}^n\end{array}\right\} \underset{\mathbb{V}}{\overset{\mathbb{I}}{\rightleftarrows}} \left\{\begin{array}{c}\text{radical ideals}\\ \text{in } \mathbb{K}[x_1,\dots,x_n]\end{array}\right\}$$

Somewhat amazingly, the entire difficulty of this theorem comes down to only one of the four inclusions needed. In particular, last week we showed that $\mathbb{V}(\mathbb{I}(V))=V$ for any algebraic subset $V\subset\mathbb{K}^n$, regardless of the field. Similarly, we also proved that the inclusion $\sqrt{I}\subseteq\mathbb{I}(\mathbb{V}(I))$ holds over an arbitrary field. Thus, the hard part of the proof of Hilbert's Nullstellensatz II is to show that

$$\mathbb{I}(\mathbb{V}(I))\subseteq\sqrt{I}$$

for every ideal $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$. This can fail over non-algebraically closed fields, as the example $I = \langle x^2 + 1 \rangle \subset \mathbb{R}[x]$ shows.

The strategy of this worksheet is to isolate that difficulty: first review the geometry–algebra dictionary, and then prove the point Hilbert's Nullstellensatz I for uncountable fields using field theory and a clever cardinality argument. We will then deduce what some call the weak Nullstellensatz:

Theorem 3 (Hilbert's Weak Nullstellensatz)**.** *If $\mathbb{K}$ is algebraically closed and $I \subset \mathbb{K}[x_1, \ldots, x_n]$ is an ideal then $\mathbb{V}(I) = \varnothing$ if and only if $I = \langle 1 \rangle$.*

Note the difficult direction of the weak Nullstellensatz is the forward direction, the reverse is immediate. Intuitively this is saying that a system of polynomial equations has no solution over $\mathbb{K}$ if and only if the "obvious" obstruction – namely you can write 1 in terms of your polynomials – occurs. Finally we will use Rabinowitsch's trick to obtain the full statement. Along the way we will also pause to recall some field theory language, since the key obstruction is the difference between algebraic and transcendental field extensions.

---

(1) **Warm-Up: Recalling the Correspondence.** Recall the two order-reversing maps

$$I \longmapsto \mathbb{V}(I) \qquad \text{and} \qquad V \longmapsto \mathbb{I}(V).$$

Before we move to proving the main theorems let us warm up with a few examples.

(a) Give the definitions of $\mathbb{V}(I)$ and $\mathbb{I}(V)$.

(b) If $V = \{p\} \subset \mathbb{K}^n$ for $p = (a_1, \ldots, a_n)$, describe $\mathbb{I}(V)$ both intrinsically and by giving generators.

(c) The ideals $\langle 0 \rangle$ and $\langle 1 \rangle$ are the extreme cases. Describe $\mathbb{V}(\langle 0 \rangle)$ and $\mathbb{V}(\langle 1 \rangle)$ as subsets of $\mathbb{K}^n$.

(d) Over $\mathbb{R}$, describe $\mathbb{V}(\langle x, y \rangle)$ and $\mathbb{V}(\langle x^2 + y^2 \rangle) \subseteq \mathbb{R}^2$.

(e) Over $\mathbb{F}_p$, describe $\mathbb{V}(\langle 0 \rangle)$ and $\mathbb{V}(\langle x^p - x, xy^p - x^p y \rangle) \subseteq \mathbb{F}_p^2$.

(2) **A Parameterized Example.** Consider the map

$$\phi : \overline{\mathbb{F}}_{17}^2 \longrightarrow \overline{\mathbb{F}}_{17}^3, \qquad (u, v) \longmapsto (u^2, uv, v^2).$$

(a) Show that every point in the image of ϕ satisfies the equation $xz - y^2 = 0$.

(b) Let $(a, b, c) \in \overline{\mathbb{F}}_{17}^3$ satisfy $ac = b^2$. Show that if $a \neq 0$, then (a, b, c) lies in the image of ϕ. Handle the case $a = 0$ separately.

(c) Deduce that the image of ϕ is equal to $\mathbb{V}(xz - y^2) \subseteq \overline{\mathbb{F}}_{17}^3$.

(d) Show that $xz - y^2$ is irreducible in $\overline{\mathbb{F}}_{17}[x, y, z]$ and conclude that the corresponding radical ideal is $\langle xz - y^2 \rangle$.

(3) **Reduction to the Core Difficulty.** Recall what you proved last time about the interaction of $\mathbb{V}$ and $\mathbb{I}$ over an arbitrary field.

(a) Show that if $V \subseteq \mathbb{K}^n$ is algebraic, then $\mathbb{V}(\mathbb{I}(V)) = V$.

(b) Show that for every ideal $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ one has $I \subseteq \sqrt{I} \subseteq \mathbb{I}(\mathbb{V}(I))$.

(c) Show via an example – other than $\langle x^2 + 1 \rangle \subset \mathbb{R}[x]$ – that the inclusion in 3b can be proper when $\mathbb{K}$ is not algebraically closed

(d) Explain why proving Hilbert's Nullstellensatz II reduces to showing that when $\mathbb{K}$ is algebraically closed, $\mathbb{I}(\mathbb{V}(I)) \subset \sqrt{I}$ for every ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$.

Before the next question, recall some field theory language. If $\mathbb{K}$ is a field and $\mathbb{E}$ is a field containing $\mathbb{K}$, we call $\mathbb{E}/\mathbb{K}$ a *field extension*. In this situation $\mathbb{E}$ is naturally a vector space over $\mathbb{K}$, and we write $[\mathbb{E} : \mathbb{K}] := \dim_{\mathbb{K}} \mathbb{E}$ for its dimension, called the *degree* of the extension. If $[\mathbb{E} : \mathbb{K}]$ is finite we say the extension is *finite*.

Fixing a field extension $\mathbb{E}/\mathbb{K}$, we say an element $\zeta \in \mathbb{E}$ is *algebraic* over $\mathbb{K}$ if there exists a nonzero polynomial $f \in \mathbb{K}[x]$ with $f(\zeta) = 0$; otherwise ζ is *transcendental* over $\mathbb{K}$. The extension $\mathbb{E}/\mathbb{K}$ is called *algebraic* if every element of $\mathbb{E}$ is algebraic over $\mathbb{K}$. Every finite extension is algebraic: if $[\mathbb{E} : \mathbb{K}] = d$, then for any $\zeta \in \mathbb{E}$ the $d + 1$ elements $\zeta^0, \zeta, \ldots, \zeta^d$ are $\mathbb{K}$-linearly dependent, giving a polynomial relation for ζ over $\mathbb{K}$.

More generally, elements $\zeta_1, \ldots, \zeta_r \in \mathbb{E}$ are *algebraically independent* over $\mathbb{K}$ if no nonzero polynomial $f \in \mathbb{K}[x_1, \ldots, x_r]$ satisfies $f(\zeta_1, \ldots, \zeta_r) = 0$. In particular, a single element ζ is transcendental over $\mathbb{K}$ exactly when $\{\zeta\}$ is algebraically independent over $\mathbb{K}$. One helpful characterization of transcendental elements can be phrased in terms of our trusty friend evaluation maps.

Lemma 4. *Let $\mathbb{E}/\mathbb{K}$ be a field extension. An element $\zeta \in \mathbb{E}$ is transcendental over $\mathbb{K}$ if and only if the evaluation-at-ζ homomorphism below is injective:*

$$\begin{array}{ccc} \mathbb{K}[x] & \xrightarrow{\text{ev}_\zeta} & \mathbb{E} \\ f & \longmapsto & f(\zeta) \end{array}.$$

A useful consequence of this lemma is that if $\zeta \in \mathbb{E}$ is transcendental over $\mathbb{K}$, then the map ev_ζ identifies $\mathbb{K}[x]$ with the subring $\mathbb{K}[\zeta] \subseteq \mathbb{E}$. Passing to fields of fractions then identifies the rational function field $\mathbb{K}(x)$ with the subfield $\mathbb{K}(\zeta) \subseteq \mathbb{E}$. You will prove the converse in the exercises as well.

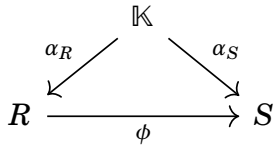
A field $\mathbb{K}$ is *algebraically closed* if every nonconstant polynomial in $\mathbb{K}[x]$ has a root in $\mathbb{K}$. An equivalent formulation is that $\mathbb{K}$ has no nontrivial algebraic extensions. That is, if $\mathbb{E}/\mathbb{K}$ is algebraic, then $\mathbb{E} = \mathbb{K}$. The field $\mathbb{C}$ of complex numbers is the prototypical example.

A $\mathbb{K}$-*algebra* is a ring R equipped with a ring homomorphism $\alpha : \mathbb{K} \to R$. Given such a map, R becomes a $\mathbb{K}$-vector space by defining $\lambda \cdot a := \alpha(\lambda)a$ for $\lambda \in \mathbb{K}$ and $a \in R$. This scalar multiplication is compatible with

the ring multiplication in the sense that

$$\lambda \cdot (ab) = (\lambda \cdot a)b = a(\lambda \cdot b)$$

for all $a, b \in R$ and $\lambda \in \mathbb{K}$. Conversely, any ring R that is simultaneously a $\mathbb{K}$-vector space satisfying the above compatibility condition is a $\mathbb{K}$-algebra; the structure map is $\alpha(\lambda) = \lambda \cdot 1_R$. A *homomorphism of $\mathbb{K}$-algebras* $\phi : R \to S$ is a ring homomorphism that also respects the $\mathbb{K}$-action, i.e. $\phi(\lambda \cdot_R a) = \lambda \cdot_S \phi(a)$ for all $\lambda \in \mathbb{K}$ and $a \in R$. Equivalently, the diagram



commutes, where α_S and α_R are the respective structure maps. In other words, ϕ is a ring homomorphism that is also $\mathbb{K}$-linear. For example, $R = \mathbb{K}[x_1, \ldots, x_n]$ is a $\mathbb{K}$-algebra via the inclusion of constants, and any quotient R/I inherits a $\mathbb{K}$-algebra structure from the surjection $\pi : R \twoheadrightarrow R/I$. If $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ is an ideal, the quotient $\mathbb{K}[x_1, \ldots, x_n]/I$ is a $\mathbb{K}$-algebra. It is a field if and only if I is maximal. In that case, the quotient map π gives a field extension:

$$\mathbb{K} \longrightarrow \mathbb{K}[x_1, \ldots, x_n] \xrightarrow{\pi} \mathbb{K}[x_1, \ldots, x_n]/I$$

gives a field extension of $\mathbb{K}$. Every element of this quotient is a $\mathbb{K}$-linear combination of the images of monomials $x_1^{a_1} \cdots x_n^{a_n}$, so properties of this extension (such as its dimension over $\mathbb{K}$) are controlled by the combinatorics of monomials together with the relations imposed by I.

The problem below uses all of these ideas to prove a beautiful dictionary between algebra and geometry: when $\mathbb{K}$ is both uncountable and algebraically closed (e.g. $\mathbb{K} = \mathbb{C}$), the maximal ideals of $\mathbb{K}[x_1, \ldots, x_n]$ are in natural bijection with the points of $\mathbb{K}^n$.

---

(4) **Hilbert's Nullstellensatz I ($\mathbb{K}$ uncountable).** Let $R := \mathbb{K}[x_1, \ldots, x_n]$ and $\mathfrak{m} \subset R$ be a maximal ideal. Write $L := R/\mathfrak{m}$ for the residue field, which contains $\mathbb{K}$ via the natural quotient map. The goal is to show that if $\mathbb{K}$ is uncountable and algebraically closed, then in fact $L \cong \mathbb{K}$.

(a) Show that the monomials in R form a countable $\mathbb{K}$-basis of R.

(b) Deduce that L has at most countable dimension as a vector space over $\mathbb{K}$.

(c) Let $\mathbb{E}/\mathbb{K}$ be a field extension and let $\zeta \in \mathbb{E}$. Explain why the following are equivalent:

(i) ζ is transcendental over $\mathbb{K}$;

(ii) $\{\zeta\}$ is algebraically independent over $\mathbb{K}$;

(iii) the evaluation map $\mathbb{K}[x] \to \mathbb{E}$ sending $f(x)$ to $f(\zeta)$ is injective.

In particular, if a field extension of $\mathbb{K}$ is not algebraic, then it contains a transcendental element.

(d) Let $\mathbb{K}$ be any infinite field, and let $\zeta \in \mathbb{E}$ be transcendental over $\mathbb{K}$ for some field extension $\mathbb{E}/\mathbb{K}$. Prove that the set of elements in $\mathbb{E}$:

$$\left\{ \frac{1}{\zeta - \lambda} \;\middle|\; \lambda \in \mathbb{K} \right\} \subseteq \mathbb{E}$$

is linearly independent over $\mathbb{K}$. (Hint: Suppose $\sum_{i=1}^{m} \frac{c_i}{\zeta - \lambda_i} = 0$ for distinct $\lambda_1, \ldots, \lambda_m \in \mathbb{K}$ and coefficients $c_1, \ldots, c_m \in \mathbb{K}$. Multiply both sides by $\prod_{j=1}^{m}(\zeta - \lambda_j)$ to obtain $\sum_{i=1}^{m} c_i \prod_{j \neq i}(\zeta - \lambda_j) = 0$. Now define $P(x) = \sum_{i=1}^{m} c_i \prod_{j \neq i}(x - \lambda_j) \in \mathbb{K}[x]$. Then $P(\zeta) = 0$. Since ζ is transcendental over $\mathbb{K}$, conclude that $P(x)$ must be the zero polynomial. Evaluate $P(x)$ at $x = \lambda_k$ for each k to show that $c_k = 0$.)

(e) Now assume that $\mathbb{K}$ is uncountable. Using part 4d, show that if a field extension $\mathbb{E}/\mathbb{K}$ contains a transcendental element, then $[\mathbb{E} : \mathbb{K}]$ is uncountable.

(f) Assume $\mathbb{K}$ is uncountable. Show if $\mathfrak{m} \subseteq R$ is a maximal ideal, then the extension $\mathbb{K} \hookrightarrow R/\mathfrak{m} := L$ is algebraic.

(g) Now assume that $\mathbb{K}$ is both uncountable and algebraically closed. Show that every algebraic extension of $\mathbb{K}$ is trivial, so $L \cong \mathbb{K}$ as $\mathbb{K}$-algebras.

(h) With the notation from part 4g let $\psi : R \to \mathbb{K}$ be the ring map given by the composition

$$R \xrightarrow{\pi} R/\mathfrak{m} = L \xrightarrow{\sim} \mathbb{K}$$

where π is the quotient map and the second map is the identification of L with $\mathbb{K}$ from part 4g. Note $\ker(\psi) = \mathfrak{m}$. Define $a_i := \psi(x_i) \in \mathbb{K}$ for $i = 1, \ldots, n$. Prove that $\mathfrak{m} = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$.

(i) Deduce that when $\mathbb{K}$ is uncountable and algebraically closed, the assignment $p \mapsto \mathfrak{m}_p$ gives a bijection between points of $\mathbb{K}^n$ and maximal ideals of $\mathbb{K}[x_1, \ldots, x_n]$.

We have now proven Hilbert's Nullstellensatz I under the additional assumption that $\mathbb{K}$ is uncountable, using virtually only field theory! Note this applies to $\mathbb{C}$ and $\mathbb{C}_p$ as these are both algebraically closed and uncountable, but does not apply to $\overline{\mathbb{Q}}$ and $\overline{\mathbb{F}_p}$ which while algebraically closed are countable.

In what follows we will *only* assume $\mathbb{K}$ is algebraically closed, and will use Hilbert's Nullstellensatz I to deduce the weak Nullstellensatz. After that we will use what has come to be known as *Rabinowitsch's trick* to upgrade the weak Nullstellensatz to the full statement of Hilbert's Nullstellensatz II.

---

(5) **Weak Nullstellensatz.** Let $\mathbb{K}$ be algebraically closed and let $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ be an ideal.

(a) Show that if I is proper, then I is contained in some maximal ideal $\mathfrak{m}$. (Hint: Use Zorn's Lemma.)

(b) Assuming Hilbert's Nullstellensatz I, show that if I is proper then $\mathbb{V}(I) \neq \varnothing$. (Hint: $\mathbb{V}(\mathfrak{m}) \subset \mathbb{V}(I)$.)

(c) Conclude that $\mathbb{V}(I) = \varnothing$ if and only if $I = \langle 1 \rangle$.

(6) **Hilbert's Nullstellensatz II. (Rabinowitsch's Trick)** Let $\mathbb{K}$ be algebraically closed and $R := \mathbb{K}[x_1, \ldots, x_n]$. Let $I = \langle f_1, \ldots, f_t \rangle \subset R$ be an ideal. Choose any element $g \in \mathbb{I}(\mathbb{V}(I))$, we will show that some power of g lies in I. Note if $g = 0$ there is nothing to prove as $0 \in I$. Thus, we assume g is non-zero.

(a) In the larger polynomial ring $R[z]$, define $J := \langle f_1, \ldots, f_t, 1 - gz \rangle$. Show that $\mathbb{V}(J) = \varnothing$ without appealing to the weak Nullstellensatz. (Hint: If $(a_1, \ldots, a_{n+1}) \in \mathbb{V}(J)$ then what do we know about $g(a_1, \ldots, a_n)$ since $g \in \mathbb{I}(\mathbb{V}(I))$.)

(b) Use Question 5 to conclude that $J = \langle 1 \rangle \subset R[z]$. Deduce there exist polynomials $h_1, \ldots, h_t, h_{t+1} \in R[z]$ such that the following relation holds.

$$1 = h_1 f_1 + \cdots + h_t f_t + h_{t+1}(1 - gz) \in R[z].$$

(c) Consider the ring $R[1/g]$ consisting of expressions of the form p/g^k where $p \in R$ and $k \geq 0$, in other words, we enlarge R by formally allowing division by powers of g. Consider the map of $\mathbb{K}$-algebras:

$$\begin{aligned} R[z] &\xrightarrow{\psi} R\left[\tfrac{1}{g}\right] \\ z &\longmapsto \tfrac{1}{g} \end{aligned}$$

Explain why ψ is a well-defined $\mathbb{K}$-algebra homomorphism. (Hint: What does it take to define a $\mathbb{K}$-algebra map out of a polynomial ring $R[z]$?)

(d) Prove that $\psi(1 - gz) = 0$ and deduce that $1 = \psi(h_1) f_1 + \cdots + \psi(h_t) f_t$ in $R[1/g]$.

(e) Explain why there exists $k \in \mathbb{N}$ such that $g^k \psi(h_i) \in R$ for every $i = 1, \ldots, t$. Multiply the equation in part 6d by g^k to conclude that $g^k \in I$. (Hint: Each $\psi(h_i)$ is an element of $R[1/g]$, so it can be written as p_i/g^{k_i} for some $p_i \in R$ and $k_i \geq 0$.)

(f) Conclude that $g \in \sqrt{I}$, and hence $\mathbb{I}(\mathbb{V}(I)) \subseteq \sqrt{I}$.

(g) Combine this with Question 3 to finish the proof of Hilbert's Nullstellensatz II assuming Hilbert's Nullstellensatz I. (The latter we have proven over every uncountable algebraically closed field, in particular over $\mathbb{C}$.)

You have now proved Hilbert's Nullstellensatz for every *uncountable* algebraically closed field, including $\mathbb{C}$. The only remaining gap in the proof over an arbitrary algebraically closed field is the point case: one still needs to show that every maximal ideal is of the form $\mathfrak{m}_p$ without assuming uncountability. We will return to that later, after developing more tools.

For the remainder of the worksheet, assume Hilbert's Nullstellensatz I and II over all algebraically closed fields and use them freely. The point now is to unpack what the theorem says about coordinate rings, closed subsets, irreducibility, and functoriality. In particular, we would like a version of the Nullstellensatz that describes algebraic subsets not of just $\mathbb{K}^n$, but of any algebraic set $V \subset \mathbb{K}^n$. Towards this we will define

and study relative versions of the $\mathbb{I}$ and $\mathbb{V}$ operators. In particular, for an algebraic subset $W \subset V$ and an ideal $J \subset \mathbb{K}[V]$ define

$$\mathbb{I}_V(W) := \{\phi \in \mathbb{K}[V] \mid \phi(p) = 0 \text{ for all } p \in W\}. \qquad \text{and} \qquad \mathbb{V}_V(J) := \{p \in V \mid \phi(p) = 0 \text{ for all } \phi \in J\}.$$

Using these we how to prove the following relative version of the Nullstellensatz connecting algebraic subsets of V and radical ideals in $\mathbb{K}[V]$.

Theorem 5 (Hilbert's Nullstellensatz III)**.** *Let $\mathbb{K}$ be an algebraically closed field. If $V \subset \mathbb{K}^n$ is an algebraic subset then the maps $\mathbb{I}_V$ and $\mathbb{V}_V$ induce inverse, inclusion-reversing bijections:*

$$\left\{\begin{array}{c}\textit{algebraic subsets}\\ \textit{in } V\end{array}\right\} \underset{\mathbb{V}_V}{\overset{\mathbb{I}_V}{\rightleftarrows}} \left\{\begin{array}{c}\textit{radical ideals}\\ \textit{in } \mathbb{K}[V]\end{array}\right\}$$

Note that since the coordinate ring of $\mathbb{K}^n$ is canonically isomorphic to $\mathbb{K}[x_1, \ldots, x_n]$ we could view Hilbert's Nullstellensatz II as a special case of this third version. However, the real difficulty in proving the third version boils down to applying the second. As you will see many of the following exercises boil down to the same ideas and arguments we used for $\mathbb{I}$ and $\mathbb{V}$, at times almost verbatim.

---

(7) **Properties of $\mathbb{I}_V$.** Assume $\mathbb{K}$ is algebraically closed, let $V \subseteq \mathbb{K}^n$ be an algebraic set with coordinate ring $\mathbb{K}[V]$. Let $W \subseteq V$ be an algebraic subset and $\rho_W : \mathbb{K}[V] \to \mathbb{K}[W]$ be the restriction homomorphism taking a function $\phi : V \to \mathbb{K}$ and restricting it to W to get a function $\phi|_W : W \to \mathbb{K}$. (If we wanted to feel fancy we could say $\phi|_W$ is the composition of $\phi : V \to \mathbb{K}$ with the inclusion $\iota : W \to V$, but in this setting that is needlessly complex.)

(a) Show that $\mathbb{I}_V(W)$ is an ideal of $\mathbb{K}[V]$, and if $Z \subset W \subset V$ then $\mathbb{I}_V(W) \subset \mathbb{I}_V(W)$.

(b) Since V is an algebraic subset of itself, as a reality check what is $\mathbb{I}_V(V)$?

(c) Prove that ρ_W is a surjective $\mathbb{K}$-algebra homomorphism with kernel $\mathbb{I}_V(W)$.

(d) Prove that ρ_W induces an $\mathbb{K}$-algebra isomorphism $\mathbb{K}[V]/\mathbb{I}_V(W) \cong \mathbb{K}[W]$.

(e) Show that if $W \subset V$ is an algebraic subset then the following diagram commutes:

$$\begin{array}{ccc} \mathbb{K}[x_1, \ldots, x_n] & \xrightarrow{\rho} & \mathbb{K}[V] \\ & \searrow^{\rho'} & \downarrow{\scriptstyle \rho_W} \\ & & \mathbb{K}[W] \end{array}$$

where $\rho' : \mathbb{K}[x_1, \ldots, x_n] \to \mathbb{K}[W]$ is the restriction of functions map defining $\mathbb{K}[W]$. Deduce that $\mathbb{I}_V(W) = \mathbb{I}(W)/\mathbb{I}(V)$.

(f) Conclude that if $W \subset V$ is an algebraic subset then $\mathbb{I}_V(W)$ is a radical ideal of $\mathbb{K}[V]$.

(8) **Properties of $\mathbb{V}_V$.** Let $\mathbb{K}$ be an algebraically closed field, and let $V \subseteq \mathbb{K}^n$ be an algebraic set with coordinate ring $\mathbb{K}[V]$.

(a) Let $J \subset \mathbb{K}[V]$ be an ideal. Show that $\mathbb{V}_V(J)$ is an algebraic subset of V by showing that $\mathbb{V}_V(J) = \mathbb{V}(\rho^{-1}(J)) \subseteq \mathbb{K}^n$. (Hint: Since $\ker(\rho) = \mathbb{I}(V) \subseteq \rho^{-1}(J)$, every point of $\mathbb{V}(\rho^{-1}(J))$ already lies in V.)

(b) Again exploring the extremes what algebraic subsets of V are $\mathbb{V}_V(\langle 1 \rangle)$ and $\mathbb{V}_V(\langle 0 \rangle)$?

(c) Show that if $I \subset J$ are ideals in $\mathbb{K}[V]$ then $\mathbb{V}_V(J) \subset \mathbb{V}_V(I)$.

(9) **Proving Hilbert's Nullstellensatz III.** Assume $\mathbb{K}$ is algebraically closed, let $V \subseteq \mathbb{K}^n$ be an algebraic set with coordinate ring $\mathbb{K}[V]$.

(a) Use Hilbert's Nullstellensatz in $\mathbb{K}[x_1, \ldots, x_n]$ to prove that $\mathbb{I}_V(\mathbb{V}_V(J)) = \sqrt{J}$ (Hint: First identify $\mathbb{I}_V(\mathbb{V}_V(J))$ with $\mathbb{I}(\mathbb{V}(\rho^{-1}(J)))/\mathbb{I}(V)$, then use $\mathbb{I}(\mathbb{V}(-)) = \sqrt{-}$.)

(b) Show that if $W \subseteq V$ is an algebraic subset, then $\mathbb{V}_V(\mathbb{I}_V(W)) = W$.

(c) Conclude that the assignments $W \longmapsto \mathbb{I}_V(W)$ and $J \mapsto \mathbb{V}_V(J)$ induce inverse, inclusion-reversing bijections between algebraic subsets of V and radical ideals in $\mathbb{K}[V]$.

(d) Prove that under the bijections in the previous parts the maximal ideals of $\mathbb{K}[V]$ correspond to the points of V, thought of as algebraic subsets. Explain why we should think of this as a relative version of Hilbert's Nullstellensatz I.

(10) **Irreducibility and Prime Ideals.** An algebraic set $V \subset \mathbb{K}^n$ is *irreducible* if there do not exist two proper algebraic subsets $W_1, W_2 \subsetneq V$ such that $V = W_1 \cup W_2$. Equivalently, V is not the union of two proper algebraic subsets. An algebraic set that is not irreducible is said to be *reducible*.

(a) Which of the following algebraic sets in $\mathbb{K}^n$ (with $\mathbb{K}$ algebraically closed) do you think are irreducible. Draw pictures when possible.

(i) $V = \mathbb{V}(x^2 - y^2) \subset \mathbb{C}^2$.

(ii) $V = \mathbb{V}(y - x^3) \subset \mathbb{C}^2$.

(iii) $V = \mathbb{V}(xz, yz) \subset \mathbb{C}^3$.

(iv) $V = \mathbb{V}(x^2 + y^2 - 1) \subset \mathbb{C}^2$.

(v) $V = \mathbb{V}(xy - z^2) \subset \mathbb{C}^3$.

(vi) $V = \mathbb{V}(3x^2 - 2xy) \subset \mathbb{C}^2$.

(b) Assume $\mathbb{I}(V)$ is a prime ideal. Show that V is irreducible. (Hint: Suppose for contradiction that $V = W_1 \cup W_2$ with $W_1, W_2 \subsetneq V$. Since $W_i \subsetneq V$, there exist $f_i \in \mathbb{I}(W_i) \setminus \mathbb{I}(V)$. What can you say about the product $f_1 f_2$?)

(c) Show that if $fg \in \mathbb{I}(V)$, then $V \subseteq \mathbb{V}(g) \cup \mathbb{V}(f)$. (Hint: Use that $\mathbb{V}$ is inclusion reversing, together with some facts you proved when checking the Zariski topology is a topology.)

(d) Prove that if V is irreducible then $\mathbb{I}(V)$ is prime. (Hint: Given $fg \in \mathbb{I}(V)$ we must show that $f \in \mathbb{I}(V)$ or $g \in \mathbb{I}(V)$. By 10c if $fg \in \mathbb{I}(V)$ then $V \subset \mathbb{V}(f) \cup \mathbb{V}(g)$ what does V being irreducible imply here?)

(e) Conclude that an algebraic set V is irreducible if and only if $\mathbb{I}(V)$ is prime. State a bijection between irreducible algebraic sets and prime ideals. Why do we not need to say radical?

(11) **Algebraic Sets and Spec.** Continue to assume that $\mathbb{K}$ is an algebraically closed field and that $V \subset \mathbb{K}^n$ is an algebraic subset with coordinate ring $\mathbb{K}[V]$. In this question we will prove an inclusion-reversing bijection between $\mathrm{Spec}(\mathbb{K}[V])$ and the irreducible algebraic subsets of V. Keep the notation from the previous problem, and use the Hilbert's Nullstellensatz III from Questions 7-9.

(12) Show that the correspondence in the previous part induces a homeomorphism between $\mathrm{mSpec}(\mathbb{K}[V])$ (with the subspace Zariski topology inherited from $\mathrm{Spec}(\mathbb{K}[V])$) and V (with its Zariski topology).

(a) If $W_1, W_2 \subseteq V$ are algebraic, show that $\mathbb{I}_V(W_1 \cup W_2) = \mathbb{I}_V(W_1) \cap \mathbb{I}_V(W_2)$. (Note: You proved the same holds of $\mathbb{I}$ when you checked the Zariski topology on algebraic sets is well-defined.)

(b) Let $W \subseteq V$ be an algebraic subset. Show that if $\mathbb{I}_V(W)$ is prime, then W is irreducible.

(c) Let $W \subseteq V$ be an algebraic subset. Prove that given $f, g \in \mathbb{K}[V]$, if $fg \in \mathbb{I}_V(W)$, then $W \subseteq \mathbb{V}_V(f) \cup \mathbb{V}_V(g)$. (This should feel very familiar to Question 10, except that now we are working with $\mathbb{V}_V$ instead of $\mathbb{V}$.)

(d) Prove that if W is irreducible, then $\mathbb{I}_V(W)$ is a prime ideal of $\mathbb{K}[V]$.

(e) Deduce that the assignment $[P] \mapsto \mathbb{V}_V(P)$ induces an inclusion reversing bijection between $\mathrm{Spec}(\mathbb{K}[V])$ and the set of irreducible algebraic subsets of V.

(f) Show that the correspondence in the previous part induces a homeomorphism between $\mathrm{mSpec}(\mathbb{K}[V])$, with the subspace Zariski topology inherited from $\mathrm{Spec}(\mathbb{K}[V])$, and V with its Zariski topology.

(13) **Functor-of-Points Viewpoint.** Let $\mathbb{K}$ be an arbitrary field, and let $I \subset \mathbb{K}[x_1, \ldots, x_n]$ be an ideal. For a field extension $\mathbb{E}/\mathbb{K}$ define:

$$\mathcal{V}_I(\mathbb{E}) := \left\{(a_1, \ldots, a_n) \in \mathbb{E}^n \;\middle|\; f(a_1, \ldots, a_n) = 0 \text{ for all } f \in I\right\} \subset \mathbb{E}^n$$

where we are viewing the elements of I as elements of $\mathbb{E}[x_1, \ldots, x_n]$ via the natural inclusion, $\mathbb{K}[x_1, \ldots, x_n] \subset \mathbb{E}[x_1, \ldots, x_n]$. Extend $\mathcal{V}_I$ to a function of sets by defining

$$\left\{\begin{matrix}\text{field extensions} \\ \text{of } \mathbb{K}\end{matrix}\right\} \xrightarrow{\quad \mathcal{V}_I \quad} \textbf{Set}$$

$$\mathbb{E} \longmapsto \mathcal{V}_I(\mathbb{E}).$$

(a) For the ideal $I = \langle x^2 + y^2 \rangle \subseteq \mathbb{Q}[x, y]$, describe the sets $\mathcal{V}_I(\mathbb{Q})$, $\mathcal{V}_I(\mathbb{R})$, and $\mathcal{V}_I(\mathbb{C})$.

(b) For the ideal $J = \langle x^2 + 1 \rangle \subseteq \mathbb{Q}[x]$, describe the sets $\mathcal{V}_J(\mathbb{Q})$, $\mathcal{V}_J(\mathbb{R})$, and $\mathcal{V}_J(\mathbb{C})$.

(c) Let $\iota : \mathbb{E} \hookrightarrow \mathbb{F}$ be a $\mathbb{K}$-embedding of field extensions, i.e., a field homomorphism that fixes $\mathbb{K}$ pointwise. Show that ι induces a well-defined map of sets

$$\iota_* : \mathcal{V}_I(\mathbb{E}) \longrightarrow \mathcal{V}_I(\mathbb{F}), \qquad (a_1, \ldots, a_n) \longmapsto (\iota(a_1), \ldots, \iota(a_n)).$$

(Hint: If $f \in \mathbb{K}[x_1, \ldots, x_n]$ and $f(a_1, \ldots, a_n) = 0$, why is $f(\iota(a_1), \ldots, \iota(a_n)) = 0$? Use the fact that ι fixes the coefficients of f.)

(d) Show that $\mathcal{V}_I$ is a *functor* from the category of field extensions of $\mathbb{K}$ (with $\mathbb{K}$-embeddings as morphisms) to the category of sets.

(e) Revisit part 13a; the inclusion $\mathbb{R} \hookrightarrow \mathbb{C}$ gives a map $\mathcal{V}_I(\mathbb{R}) \to \mathcal{V}_I(\mathbb{C})$. Describe this map explicitly. Is it injective? Is it surjective?

(f) Generalize the map $\mathcal{V}_I$ by enlarging the source from the category of field extensions to the category of $\mathbb{K}$-algebra, $\mathcal{V}_I : \mathbb{K} - \mathbf{alg} \to \mathbf{Set}$ Prove that your generalization remains a functor.

The ideas presenedt in Question 13 is one standard description of the affine scheme of finite type cut out by I. If these words do not mean anything to you, imagine a geometric space similar to algebraic set $\mathbb{V}(I)$, but somehow remembering the ideal I itself not just $\sqrt{I}$. This viewpoint is often called the *functor of points* because we think of I as remembering not only its $\mathbb{K}$-valued solutions, but also its solutions in every test $\mathbb{K}$-algebra. That functorial viewpoint is what survives even when $\mathbb{K}$ is not algebraically closed, and it is one of the main bridges from classical algebraic sets to affine schemes. However, much of this jump from algebraic sets to schemes is beyond the scope of this course.