A NOTE ON HILBERT'S NULLSTELLENSATZ FOR PRINCIPAL IDEALS AND EUCLIDEAN OPEN SUBSETS

SEBASTIAN CASALAINA-MARTIN

ABSTRACT. In this note we review Hilbert's Nullstellensatz for principal ideals over the real numbers, and for open sets in the Euclidean topology. The motivation is an application to a topic in computer science, elicitation complexity in machine learning, that arose in some joint work with Raf Frongillo, Tom Morgan, and Bo Waggoner [CFMW17]. All of the results here are standard, and follow from basic properties of real and complex algebraic geometry found in say [AM69, CLO15, Eis95, BCR98], although perhaps the exact statements proven here may not appear in the references. This note is essentially the content of [CFMW17, Appendix D], with some small additions, and revisions meant to focus the presentation on the algebro-geometric content.

1. INTRODUCTION

Hilbert's Nullstellensatz describes the relationship between the collection of polynomial functions vanishing on an algebraic set, and the collection of polynomials used to define the algebraic set. Typically this is phrased in the language of ideals. For a field K and an ideal $J \subseteq K[x_1, \ldots, x_n]$, we have

$$\sqrt{J} \subseteq I(Z(J)). \tag{1.1}$$

Over an algebraically closed field, Hilbert's Nullstellensatz (see e.g., [AM69, Ex. 7.14, p.85]) states that this containment is an equality.

Theorem 1.1 (Hilbert's Nullstellensatz). *Let $K = \overline{K}$ be an algebraically closed field. For an ideal $J \subseteq \overline{K}[x_1, \ldots, x_n]$, we have*

$$\sqrt{J} = I(Z(J)).$$

It is natural to ask whether a similar result holds when we restrict to Zariski open sets. In other words, we can ask for the relationship between the collection of polynomial functions vanishing on a Zariski open subset of an algebraic set, and the collection of polynomials used to define the algebraic set. The following trivial example shows that the conclusion of the Nullstellensatz can fail:

Example 1.2. Let $J = (x) \subseteq \mathbb{C}[x]$, and let $U = \mathbb{C} - \{0\}$. Then $\sqrt{J} = (x) \subsetneq \mathbb{C}[x] = I(Z(J) \cap U)$.

On the other hand, it is not hard to fix the statement to cover this situation:

Corollary 1.3 (Corollary to Hilbert's Nullstellensatz). *Let $K = \overline{K}$ be an algebraically closed field. Let $J \subsetneq \overline{K}[x_1, \ldots, x_n]$ be a proper ideal, and let $U \subseteq \overline{K}^n$ be an open subset in the Zariski topology. Then $\sqrt{J} = I(Z(J) \cap U)$ if and only if each each irreducible component of $Z(J)$ meets U.*

Over the complex numbers, we can also ask whether a similar result holds when we consider Euclidean open sets.

Corollary 1.4 (Corollary to Hilbert's Nullstellensatz). *Let $K = \mathbb{C}$. Let $J \subsetneq \mathbb{C}[x_1, \ldots, x_n]$ be a proper ideal, and let $U \subseteq \mathbb{C}^n$ be an open subset in the* Euclidean *topology. Then $\sqrt{J} = I(Z(J) \cap U)$ if and only if each each irreducible component of $Z(J)$ in the Zariski topology meets U.*

Date: June 6, 2017.

In another direction, we can consider removing the condition that the field K be algebraically closed. This is already interesting for principal ideals, and the focus of these notes will be on this special case. For principal ideals, Hilbert's Nullstellensatz reads:

$$\sqrt{(f)} = I(Z(f)), \quad (K = \overline{K}); \tag{1.2}$$

in other words $(f) = I(Z(f))$ whenever f is reduced and $K = \overline{K}$ is algebraically closed. Over nonalgebraically closed fields (1.2) clearly fails; i.e., one may have

$$\sqrt{(f)} \subsetneq I(Z(f)).$$

For instance, trivially, one has in $\mathbb{Q}[x]$ that $\sqrt{(x^2+1)} = (x^2+1) \subsetneq \mathbb{Q}[x] = I(\emptyset) = I(Z(x^2+1))$. The following example is a little more interesting:

Example 1.5. Consider $f(x,y) = x^2 + y^2 - x^3 \in \mathbb{R}[x,y]$, and the zero set $Z(f) \subseteq \mathbb{R}^2$. It is a cubic curve with zero set having an isolated point at $(0,0) \in \mathbb{R}^2$. In particular, if we take $U = B_\epsilon(0)$ to be a small ball around $(0,0)$ in $\mathbb{R}^2$, then we have $\sqrt{(x^2+y^2-x^3)} = (x^2+y^2-x^3) \subsetneq (x,y) = I(Z(x^2+y^2-x^3) \cap U)$. On the other hand, it is true that $(x^2+y^2-x^3) = I(Z(x^2+y^2-x^3))$.

For the real numbers, this example motivates a solution. The main result is the following well-known real Nullstellenstatz for principal ideals. See §1.1 for an explanation of the notation.

Theorem 1.6 (Real Principal Nullstellensatz)**.** *Let $\mathbb{K}$ be a real closed field (e.g., $\mathbb{K} = \mathbb{R}$). Suppose that $f(x_1, \ldots, x_n) \in \mathbb{K}[x_1, \ldots, x_n]$ is a nonconstant polynomial, and $U \subseteq \mathbb{K}^n$ is an open subset in the* Euclidean *topology. Suppose that*

$$f(x_1, \ldots, x_n) = f_1(x_1, \ldots, x_n)^{m_1} \cdots f_r(x_1, \ldots, x_n)^{m_r} \tag{1.3}$$

is a factorization into powers of distinct nonconstant irreducible polynomials. The following are equivalent:

(1) $(f) = I(Z(f) \cap U)$.

(2) $m_1 = \cdots = m_r = 1$ *and for each* $i = 1, \ldots, r$ *there is a point* $\alpha^{(i)} \in Z(f_i) \cap U$ *with*

$$(\partial_{x_1} f_i(\alpha^{(i)}), \ldots, \partial_{x_n} f_i(\alpha^{(i)})) \neq 0 \in \mathbb{K}^n.$$

For $\mathbb{K} = \mathbb{R}$*, this is equivalent to having for each* i *that* $Z(f_i) \cap U$ *is a smooth* $(n-1)$*-dimensional submanifold of an open neighborhood of* $\alpha^{(i)}$.

(3) $m_1 = \cdots = m_r = 1$ *and for each* $i = 1, \ldots, r$ *the sign of the polynomial* f_i *changes on an open ball in* U *(i.e., for* $i = 1, \ldots, n$ *there is an open ball* $B_\epsilon^{(i)} \subseteq U$ *and points* $\alpha^{(i)}, \beta^{(i)} \in B_\epsilon^{(i)}$ *such that* $f_i(\alpha^{(i)}) f_i(\beta^{(i)}) < 0$*).*

(4) $m_1 = \cdots = m_r = 1$ *and for each* $i = 1, \ldots, r$ *the semi-algebraic Krull dimension of the topological space* $Z(f_i) \cap U$ *(i.e., the Krull dimension of the ring* $\mathbb{K}[x_1, \ldots, x_n]/I(Z(f_i) \cap U)$*) satisfies*

$$\dim(Z(f_i) \cap U) = n - 1.$$

The case of Theorem 1.6 where $U = \mathbb{K}^n$ and f is irreducible is, for instance, given in [BCR98, Thm. 4.5.1]. These notes essentially expand on that proof to give the more general case above.

Remark 1.7. The case $n = 1$ is elementary and has the following simple interpretation: *we have* $(f(x)) = I(Z(f(x)) \cap U)$ *if and only if all of the roots of* $f(x)$ *in an algebraic closure* $\overline{\mathbb{K}}$ *are distinct, and lie in* $U \subseteq \mathbb{K}$. There are standard techniques to check this condition (e.g., [BCR98, pp.12–14]).

Remark 1.8. If $f(x_1, \ldots, x_n)$ is given as in (1.3), then $\sqrt{(f)} = (f_1 \cdots f_r)$. Thus Theorem 1.6 also gives conditions for when there is an equality $\sqrt{(f)} = I(Z(f) \cap U)$.

1.1. **Notation and conventions.** Let K be a field. Given an ideal $J \subseteq K[x_1,\dots,x_n]$ we will be interested in both the closed subscheme

$$V(J) \subseteq \mathbb{A}^n_K,$$

as well as the zero set

$$V(J)(\operatorname{Spec} K) \simeq Z_K(J) := \{\alpha \in K^n : f(\alpha) = 0, \text{ for all } f \in J\} \subseteq K^n.$$

If the field is clear from the context, we will write $Z(J) = Z_K(J)$. For a subset $S \subseteq K^n$, we denote the associated ideal by

$$I(S) := \{g(x_1,\dots,x_n) \in K[x_1,\dots,x_n] : g(s) = 0 \text{ for all } s \in S\}.$$

We refer the reader to [BCR98, Def. 1.1.9, Def. 1.2.1] for a review of the definition of a real closed field. In particular, such a field $\mathbb{K}$ is of characteristic 0 and is an ordered field; the Euclidean topology on $\mathbb{K}^n$ then has a basis given by the open balls

$$B_\epsilon(\alpha) := \{\beta \in \mathbb{K}^n : \sum_{i=1}^n (\beta_i - \alpha_i)^2 < \epsilon^2\}$$

for all $\alpha \in \mathbb{K}^n$ and all $\epsilon \in \mathbb{K}$ with $\epsilon > 0$.

1.2. **Acknowledgements.** I would like to thank Jeff Achter for some discussions regarding algebraic sets and perfect fields.

2. Proof of Corollaries 1.3 and 1.4

In this section we give a proof of Corollaries 1.3 and 1.4. This will also provide a proof of Theorem 1.1.

Proof of Corollaries 1.3 and 1.4. Let $K = \overline{K}$ be an algebraically closed field, and let $U \subseteq \overline{K}^n$ be *any* subset. We then have the containments:

$$\sqrt{J} \subseteq I(Z(J)) \subseteq I(Z(J) \cap U). \tag{2.1}$$

Now suppose that $Z(J) = \bigcup_{i=1}^N Z_i$ is a decomposition of $Z(J)$ into irreducible components, and that $Z_1 \cap U = \emptyset$. We have $I(Z(J)) = I(Z_1 \cup \bigcup_{i=2}^N Z_i) = I(Z_1) \cap I(\bigcup_{i=2}^N Z_i)$. We clearly have $I(Z_1) \not\supseteq I(\bigcup_{i=2}^N Z_i)$, since otherwise, $Z_1 = Z(I(Z_1)) \subseteq Z(I(\bigcup_{i=2}^N Z_i)) = \bigcup_{i=2}^N Z_i$, which is ruled out by definition. Thus $I(\bigcup_{i=2}^N Z_i) - I(Z_1) \neq \emptyset$, and if $g \in I(\bigcup_{i=2}^N Z_i) - I(Z_1)$, then $g \in I(Z(J) \cap U)$, but $g \notin \sqrt{J} = I(Z(J))$, since g does not vanish on Z_1.

Now conversely, suppose that $U \subseteq \overline{K}^n$ is an open subset in the Zariski topology (resp. $U \subseteq \mathbb{C}^n$ is an open subset in the Euclidean topology), and every irreducible component of $Z(J)$ meets U. In light of (2.1), since the radical of an ideal is the intersection of all of the prime ideals containing the ideal, it suffices for us to show that if $\mathfrak{p}$ is a (minimal) prime containing J, then $\mathfrak{p} \supseteq I(Z(J) \cap U)$. For this, it is enough to show that for each prime ideal $\mathfrak{p}$ with $Z(\mathfrak{p})$ meeting U, we have $\mathfrak{p} = I(Z(\mathfrak{p}) \cap U)$. Indeed, if we prove this claim, then we have the following: if $\mathfrak{p} \supseteq J$ is minimal, then $Z(\mathfrak{p}) \subseteq Z(J)$ is an irreducible component of $Z(J)$, and therefore meets U. Thus, since $Z(\mathfrak{p}) \cap U \subseteq Z(J) \cap U$, we would have $\mathfrak{p} = I(Z(\mathfrak{p}) \cap U) \supseteq I(Z(J) \cap U)$.

In other words, we have reduced to the case where $J = \mathfrak{p}$ is a prime ideal. From the containment

$$\mathfrak{p} \subseteq I(Z(\mathfrak{p}) \cap U)$$

and the definition of the Krull dimension, it suffices to show that

$$\dim \overline{K}[x_1,\dots,x_n]/\mathfrak{p} \leq \dim \overline{K}[x_1,\dots,x_n]/I(Z(\mathfrak{p}) \cap U).$$

Now we will simply use that dimension is local; we refer the reader to [Eis95, Ch. 8] for a summary of the properties of dimension that we will be using here. To make the notation easier, let $Z' = \overline{(Z(\mathfrak{p}) \cap U)}^{\text{Zar}} \subseteq \overline{K}^n$ be the closure in the *Zariski* topology. Let $(Z', \mathcal{O}^{alg}_{Z'}) \subseteq (\overline{K}^n, \mathcal{O}^{alg}_{\overline{K}^n})$ (resp. $(Z', \mathcal{O}^{an}_{Z'}) \subseteq (\mathbb{C}^n, \mathcal{O}^{an}_{\mathbb{C}^n})$) be the associated algebraic subscheme (resp. analytic subspace). Next we make the observation that $Z' \cap U = Z(\mathfrak{p}) \cap U$, and that $I(Z') = I(Z(\mathfrak{p}) \cap U)$. From the first equality we have $(Z', \mathcal{O}^{alg}_{Z'})|_U = (Z'|_U, \mathcal{O}^{alg}_{Z'|_U}) = (Z(\mathfrak{p})|_U, \mathcal{O}^{alg}_{Z(\mathfrak{p})|_U})$ (resp. $(Z', \mathcal{O}^{an}_{Z'})|_U = (Z'|_U, \mathcal{O}^{an}_{Z'|_U}) = (Z(\mathfrak{p})|_U, \mathcal{O}^{an}_{Z(\mathfrak{p})|_U})$). Now let $\alpha \in Z(\mathfrak{p}) \cap U \subseteq \overline{K}^n$. In the case where U is a Zariski open set, we have [Eis95, Ax. D.1, p.220]:

$$\dim \overline{K}[x_1, \dots, x_n]/\mathfrak{p} = \dim \mathcal{O}^{alg}_{Z(\mathfrak{p}),\alpha} = \dim \mathcal{O}^{alg}_{Z',\alpha} \leq \dim \overline{K}[x_1, \dots, x_n]/I(Z(\mathfrak{p}) \cap U).$$

Next consider the case $K = \mathbb{C}$, and U is a Euclidean open set. Then we have

$$\begin{aligned} \dim \mathbb{C}[x_1, \dots, x_n]/\mathfrak{p} &= \dim \widehat{\mathcal{O}}^{alg}_{Z(\mathfrak{p}),\alpha} \\ &= \dim \widehat{\mathcal{O}}^{an}_{Z(\mathfrak{p}),\alpha} \\ &= \dim \widehat{\mathcal{O}}^{an}_{Z',\alpha} \\ &= \dim \widehat{\mathcal{O}}^{alg}_{Z',\alpha} \\ &\leq \dim \overline{K}[x_1, \dots, x_n]/I(Z(\mathfrak{p}) \cap U). \end{aligned}$$

□

Remark 2.1. Let $Z = Z(J) \subseteq \overline{K}^n$ be an algebraic subset, let $U \subseteq \overline{K}^n$ be any subset, and let $Z' = \overline{(Z \cap U)}^{\text{Zar}} \subseteq \overline{K}$ be the Zariski closure. In the proof above, we used the equality $Z \cap U = Z' \cap U$. The proof of this assertion is as follows:

$$\begin{array}{cc} Z \cap U \subseteq Z & \qquad Z \cap U \subseteq \overline{(Z \cap U)}^{\text{Zar}} = Z' \\ Z' = \overline{(Z \cap U)}^{\text{Zar}} \subseteq \overline{Z}^{\text{Zar}} = Z & \qquad Z \cap U \subseteq U \\ Z' \cap U \subseteq Z \cap U & \qquad Z \cap U \subseteq Z' \cap U. \end{array}$$

We also used that $I(Z \cap U) = I(Z')$. The proof is as follows. First, from the inclusion $Z \cap U = Z' \cap U \subseteq Z'$, we have $I(Z \cap U) \supseteq I(Z')$. Now suppose that $g \in I(Z \cap U)$. Then since $Z(g)$ is Zariski closed, we have $Z(g) \supseteq \overline{(Z \cap U)}^{\text{Zar}} = Z'$. So $g \in I(Z')$.

Remark 2.2. Let $Z = Z(J) \subseteq \mathbb{C}^n$ be an algebraic subset, and $(Z, \mathcal{O}^{alg}_Z) \subseteq (\mathbb{C}^n, \mathcal{O}^{alg}_{\mathbb{C}^n})$ (resp. $(Z, \mathcal{O}^{an}_Z) \subseteq (\mathbb{C}^n, \mathcal{O}^{an}_{\mathbb{C}^n})$) be the associated algebraic subscheme (resp. analytic subspace). Let $\alpha \in Z$. In the proof above we used that there is an isomorphism $\widehat{\mathcal{O}}^{alg}_{Z,\alpha} \cong \widehat{\mathcal{O}}^{an}_{Z,\alpha}$. The proof is as follows. Up to translation, we may as well assume that $\alpha = 0 \in \mathbb{C}^n$. Suppose that $J = (g_1, \dots, g_r)$. Then we have

$$\widehat{\mathcal{O}}^{alg}_{Z,\alpha} \cong \mathbb{C}[[x_1, \dots, x_n]]/(g_1, \dots, g_r) \cong \widehat{\mathcal{O}}_{\mathbb{C}^n,0}/(g_1, \dots, g_n) \cong \widehat{\mathcal{O}}^{an}_{Z,\alpha}.$$

To obtain the first and last isomorphisms, we localize, and then complete using [AM69, Prop. 10.15].

3. Proof of Theorem 1.6

We now prove Theorem 1.6. The proof is broken into several parts, focusing on various properties of the polynomial $f(x_1, \dots, x_n)$. The case where $f(x_1, \dots, x_n)$ is irreducible is treated first, and finally the general case is obtained from this.

3.1. **The connection with dimension.**

Proposition 3.1. *Let $f(x_1,\dots,x_n) \in K[x_1,\dots,x_n]$ be a nonconstant irreducible polynomial, and let $U \subseteq K^n$ be* any *subset. The following are equivalent:*

(1) $(f) = I(Z(f) \cap U)$.

(2) The semi-algebraic Krull dimension of the topological space $Z(f) \cap U$ (i.e., the Krull dimension of the ring $K[x_1,\dots,x_n]/I(Z(f) \cap U)$) satisfies

$$\dim(Z(f) \cap U) = n-1.$$

Proof. (1) $\implies$ (2). By assumption we have $(f) = I(Z(f) \cap U)$. Now the Krull dimension of $K[x_1,\dots,x_n]$ is n (e.g., [AM69, Exe. 11.7]). Consequently, since f is neither a zero divisor nor a unit, we have that the Krull dimension of $K[x_1,\dots,x_n]/(f)$ is $(n-1)$ (e.g., [AM69, Cor. 11.7]; using that f is irreducible, this is even easier). Note that this direction does not require that f be irreducible.

(2) $\implies$ (1). We have inclusions

$$(f) \subseteq I(Z(f) \cap U) \subseteq K[x_1,\dots,x_n].$$

As above, since f is neither a zero divisor nor a unit, we have that the Krull dimension of the ring $K[x_1,\dots,x_n]/(f)$ is $(n-1)$. By assumption, the Krull dimension of $K[x_1,\dots,x_n]/I(Z(f) \cap U)$ is also $(n-1)$. Now since (f) is prime (finally using that f is irreducible), and has the same Krull dimension as the ideal $I(Z(f) \cap U)$, it follows from the containment above and the definition of Krull dimension that the two ideals are equal. □

3.2. **The connection with smoothness.** We say a zero set $Z(J) \subseteq K^n$ is smooth at a point $\alpha \in Z(J)$ if the associated scheme $V(J) \subseteq \mathbb{A}^n_K$ is smooth at the point $(x_1-\alpha_1,\dots,x_n-\alpha_n) \in V(J)$. We will also simply say that $V(J)$ is smooth at α. If $J = (f)$ is principal and $\alpha \in Z(f)$, then $V(f)$ is smooth at $(x_1-\alpha_1,\dots,x_n-\alpha_n)$ if and only if $(\partial_{x_1} f(\alpha),\dots,\partial_{x_n} f(\alpha)) \neq 0 \in K^n$.

Lemma 3.2. *Suppose K is perfect. Let $f(x_1,\dots,x_n) \in K[x_1,\dots,x_n]$ be a nonconstant polynomial, and let $U \subseteq K^n$ be* any *subset. Then:*

(1) $(f) = I(Z(f) \cap U)$,

implies

(2) There is a point $\alpha^{(0)} \in Z(f) \cap U$ with

$$(\partial_{x_1} f(\alpha^{(0)}),\dots,\partial_{x_n} f(\alpha^{(0)})) \neq 0 \in K^n.$$

In other words, there is a point in U at which $V(f)$ is a smooth scheme.

Proof. Suppose that (2) fails. This means that $\partial_{x_1} f,\dots,\partial_{x_n} f \in I(Z(f) \cap U)$. But since f is nonconstant and K is perfect, either there is an i such that $\partial_{x_i} f$ is nonzero, or $\operatorname{char}(K) = p > 0$ and there exists a polynomial $g \in K[x_1,\dots,x_n]$ such that $f = g^p$ (e.g., [CLO15, Ch. 9 Ex. 10, p.524]). In the first case, since $\partial_{x_i} f$ is nonzero of degree less than the degree of f, it cannot be a multiple of f, and therefore is not in the ideal (f). Thus $(f) \subsetneq I(Z(f) \cap U)$, and (1) fails. In the second case, where $f = g^p$, we have $g \in I(Z(f) \cap U)$, while $g \notin (f)$, again for degree reasons, so that (1) also fails in this case. □

Remark 3.3. I do not know if the hypothesis that K be perfect in Lemma 3.2 is necessary.

The following example shows that the converse to Lemma 3.2 need not hold.

Example 3.4. Let $K = \mathbb{Q}$ and let $f(x_1,x_2) = x_1^3 + x_2^3 - 1$. Then $Z(f) \subseteq \mathbb{Q}^2$ is a finite set of points, and in particular one can show that $(f) \subsetneq I(Z(f))$. On the other hand, at the point say $(1,0) \in Z(f)$, one has $(\partial_{x_1} f(1,0), \partial_{x_2} f(0,1)) = (3,0) \neq 0 \in \mathbb{Q}^2$.

Nevertheless, a converse to Lemma 3.2 does hold over the real and complex numbers (see also Corollaries 1.3 and 1.4). This is essentially because the implicit function theorem asserts that condition (2) implies that the zero set is an $(n-1)$-dimensional manifold in a neighborhood of the given point. In fact, one can also establish the converse over real closed fields:

Lemma 3.5. *Suppose $K = \mathbb{K}$ is real closed or equal to $\mathbb{C}$. Let $f(x_1, \ldots, x_n) \in \mathbb{K}[x_1, \ldots, x_n]$ be a nonconstant irreducible polynomial, and let $U \subseteq \mathbb{K}^n$ be an open subset in the Euclidean topology. Then:*

(1) $(f) = I(Z(f) \cap U)$,

is implied by

(2) There is a point $\alpha^{(0)} \in Z(f) \cap U$ with

$$(\partial_{x_1} f(\alpha^{(0)}), \ldots, \partial_{x_n} f(\alpha^{(0)})) \neq 0 \in \mathbb{K}^n.$$

In other words, there is a point in U at which $V(f)$ is a smooth scheme.

Proof. The case where $K = \mathbb{C}$ is Corollary 1.4. So consider the case $K = \mathbb{K}$ is real closed. Let $\overline{(Z(f) \cap U)}^{\mathrm{Zar}} \subseteq \mathbb{K}^n$ be the closure in the Zariski topology. Now using condition (2), and (iii) $\implies$ (ii) of [BCR98, Prop. 3.3.10], we have that $\dim \mathbb{K}[x_1, \ldots, x_n]/I(\overline{(Z(f) \cap U)}^{\mathrm{Zar}}) = n-1$. (We are applying [BCR98, Prop. 3.3.10] with $V = \overline{(Z(f) \cap U)}^{\mathrm{Zar}}$ and $P_1 = f$.) Now we observe that $I(Z(f) \cap U) = I(\overline{(Z(f) \cap U)}^{\mathrm{Zar}})$ to conclude that $\dim(Z(f) \cap U) = n-1$. Note that so far we did not use that f was irreducible, as this is not required in [BCR98, Prop. 3.3.10]. To conclude (1), we use Proposition 3.1, and the assumption that f is irreducible. □

3.3. **The connection with the sign of the polynomial.** Over the reals, the sign of the polynomial also plays a role. One can in fact make these types of arguments for real closed fields.

Lemma 3.6. *Suppose $K = \mathbb{K}$ is real closed. Let $f(x_1, \ldots, x_n) \in \mathbb{K}[x_1, \ldots, x_n]$ be a nonconstant irreducible polynomial, and let $U \subseteq \mathbb{K}^n$ be an open subset in the* Euclidean *topology. Then the following are equivalent:*

(1) $(f) = I(Z(f) \cap U)$.

(2) The sign of the polynomial f changes on an open ball in U (i.e., there is an open ball $B_\epsilon \subseteq U$ such that $f(\alpha)f(\beta) < 0$ for some $\alpha, \beta \in B_\epsilon$).

Proof. (1) $\implies$ (2). Assuming (1), then from Lemma 3.2, there is a point $\alpha^{(0)} \in Z(f) \cap U$ with $(\partial_{x_1} f(\alpha^{(0)}), \ldots, \partial_{x_n} f(\alpha^{(0)})) \neq 0 \in \mathbb{K}^n$. In other words, there is an i such that $\partial_{x_i} f(\alpha^{(0)}) \neq 0$. Then consider the polynomial in one variable

$$\phi(x_i) := f(\alpha_1^{(0)}, \ldots, x_i, \ldots, \alpha_n^{(0)}).$$

We have $\phi(\alpha_i^{(0)}) = 0$. But since $\phi'(\alpha_i^{(0)}) = \partial_{x_i} f(\alpha_i^{(0)})$ is non-zero, the function $\phi(x_i)$ is monotone in a real interval around $\alpha_i^{(0)}$, and so it changes sign [BCR98, Cor. 1.2.7]. Therefore f changes sign. (Note that we did not use that f was irreducible.)

(2) $\implies$ (1). [BCR98, Lem. 4.5.2] states the following: *Let $B_\epsilon \subseteq \mathbb{K}^n$ be an open ball (including the case where $B_\epsilon = \mathbb{K}^n$) and let U_1 and U_2 be two disjoint nonempty semi-algebraic open subsets of B_ϵ. Then we have* $\dim(B_\epsilon - (U_1 \cup U_2)) \geq n-1$. Now apply this in our situation, with

$$U_1 = \{\alpha \in B_\epsilon : f(\alpha) > 0\} \text{ and } U_2 = \{\alpha \in B_\epsilon : f(\alpha) < 0\},$$

so that $B_\epsilon - (U_1 \cup U_2) = Z(f) \cap B_\epsilon$. Then

$$n-1 = \dim Z(f) \geq \dim(Z(f) \cap U) \geq \dim(Z(f) \cap B_\epsilon) \geq n-1.$$

As mentioned above, we have that $\dim Z(f) = n - 1$ since f is neither a zero divisor nor a unit. Note that so far we did not use that f was irreducible. To conclude (1), we use Proposition 3.1, and the assumption that f is irreducible. □

3.4. **Proof of Theorem 1.6.**

Proof of Theorem 1.6. We have now proved the theorem under the hypothesis that f is irreducible (Proposition 3.1, Lemma 3.2, Lemma 3.5, Lemma 3.6). We now reduce to this case.

First, it is clear that (2) $\iff$ (3) $\iff$ (4), from the irreducible case. Also, it is clear that if $(f) = I(Z(f) \cap U)$, we must have that $m_1 = m_2 = \cdots = m_r = 1$. Indeed, if say $m_1 > 1$, then $f_1 f_2^{m_2} \cdots f_r^{m_r} \in I(Z(f) \cap U)$, but for degree reasons $f_1 f_2^{m_2} \cdots f_r^{m_r}$ is not a multiple of $f = f_1^{m_1} \cdots f_r^{m_r}$ and thus (1) fails. So from here on, we assume $m_1 = m_2 = \cdots = m_r = 1$.

(1) $\implies$ (2). Suppose that (2) fails. Then there is some i, j so that $\partial_{x_j} f_i \in I(Z(f_i) \cap U)$, and is nonzero. Therefore the product $f_1 \cdots \partial_{x_j} f_i \cdots f_r$ is nonzero and in $I(Z(f) \cap U))$. But for degree reasons, it is not a multiple of $f = f_1 \cdots f_i \cdots f_r$ and thus (1) fails.

(2) $\implies$ (1). This follows from the fact that

$$\begin{aligned} \bigcap (f_i) &= (f_1 \cdots f_r) && (\mathbb{K}[x_1, \ldots, x_n] \text{ is a UFD}) \\ &= (f) \\ &\subseteq I(Z(f) \cap U)) \\ &= I\left(\bigcup (Z(f_i) \cap U) \right) \\ &= \bigcap I(Z(f_i) \cap U), \end{aligned}$$

since, assuming (2) and the special case of the theorem for irreducible polynomials, then for all i, we have $(f_i) = I(Z(f_i) \cap U)$, forcing the containment above to be an inclusion. □

References

[AM69] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[BCR98] Jacek Bochnak, Michel Coste, and Marie-Françoise Roy. *Real algebraic geometry*, volume 36 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1998. Translated from the 1987 French original, Revised by the authors.

[CFMW17] S. Casalaina-Martin, R. Frongillo, T. Morgan, and B. Waggoner. Multi-Observation Elicitation. *ArXiv e-prints*, June 2017.

[CLO15] David A. Cox, John Little, and Donal O'Shea. *Ideals, varieties, and algorithms, An introduction to computational algebraic geometry and commutative algebra*. Undergraduate Texts in Mathematics. Springer, Cham, fourth edition, 2015.

[Eis95] David Eisenbud. *Commutative algebra, with a view toward algebraic geometry*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995.

University of Colorado, Department of Mathematics, Campus Box 395, Boulder, CO 80309, USA
E-mail address: casa@math.colorado.edu