ANALYTIC NULLSTELLENSÄTZE AND THE MODEL THEORY OF VALUED FIELDS

MATTHIAS ASCHENBRENNER AND AHMED SRHIR

Abstract. We present a uniform framework for establishing Nullstellensätze for power series rings using quantifier elimination results for valued fields. As an application we obtain Nullstellensätze for p-adic power series (both formal and convergent) analogous to Rückert's complex and Risler's real Nullstellensatz, as well as a p-adic analytic version of Hilbert's 17th Problem. Analogous statements for restricted power series, both real and p-adic, are also considered.

Introduction

Rückert's Nullstellensatz [57] establishes a one-to-one correspondence between radical ideals in rings of germs of complex analytic functions and the zero sets of these ideals. This fundamental theorem plays a role in complex analytic geometry which is similar to that of Hilbert's Nullstellensatz in classical algebraic geometry. A counterpart of Hilbert's Nullstellensatz for polynomials over real closed fields (instead of algebraically closed fields) is due to Risler [50], who also established a version of Rückert's theorem for germs of real analytic functions [51] as well as an analogue of Hilbert's 17th Problem in this setting. An adaptation of Risler's theorem for formal power series over real closed fields was shown by Merrien [44, 45] (with simplifications in [39]) and used for applications to germs of real C^∞-functions.

It was noted early in the history of model theory that there is a close relationship between Nullstellensatz-type statements and A. Robinson's concept of model completeness: for example, Hilbert's Nullstellensatz is essentially equivalent to the model completeness of the theory of algebraically closed fields, whereas Risler's Nullstellensatz for polynomials corresponds to the model completeness of the theory of real closed fields. (This connection has been formalized in [63].)

A. Robinson [56] established Rückert's Nullstellensatz using non-standard methods, and asked for a model-theoretic proof. This was provided by Weispfenning [62], who also gave a proof of Risler's theorem for real analytic function germs using similar methods. His arguments, which were translated into somewhat more algebraic language by Robbin [53, 54], combine the ubiquitous Weierstrass Preparation Theorem (which permits an induction on the number of indeterminates) with model completeness of algebraically closed fields respectively real closed fields.

In this paper we establish a uniform method for obtaining Nullstellensätze in power series rings by relying on quantifier elimination theorems for certain theories of *valued* fields instead of model completeness for *fields* in order to prove the requisite specialization theorems. The advantage of this approach is that it naturally suggests how to also prove Nullstellensätze and versions of Hilbert's 17th Problem for p-adic power series, which seem to be new. (See [25, Conjectures 4.3, 4.4].)

Date: March 2024.

Nullstellensätze for power series over the p-adics. To formulate these, consider the rational function

$$\gamma_p(x) := \frac{1}{p}\left(\wp(x) - \frac{1}{\wp(x)}\right)^{-1} \in \mathbb{Q}(x)$$

where $\wp(x) := x^p - x$ (the Artin-Schreier operator). One calls $\gamma = \gamma_p$ the *p-adic Kochen operator.* It plays a role in p-adic algebra similar to that of the squaring operator x^2 in the real world. To substantiate this, we remark that γ is *p-integral definite,* that is, $|\gamma(a)|_p \leqslant 1$ for all $a \in \mathbb{Q}_p$. (Here and below $|\cdot|_p$ denotes the p-adic absolute value on $\mathbb{Q}_p$.) As a consequence, setting $F := \mathbb{Q}_p(X)$ where $X = (X_1, \dots, X_m)$ is a tuple of distinct indeterminates, every rational function of the form $\gamma(f)$ where $f \in F$ is p-integral definite, and hence so is every element of

$$\Lambda_F := \left\{ \frac{f}{1-pg} : f, g \in \mathbb{Z}[\gamma(F)] \right\}.$$

Kochen [35] proved that conversely, the subring Λ_F of F contains *every* p-integral definite rational function in F; this may be seen as a p-adic analogue of Hilbert's 17th Problem. Kochen also established a p-adic Nullstellensatz for ideals in $\mathbb{Q}_p[X]$, similar to Risler's Nullstellensatz for ideals in $\mathbb{R}[X]$, the statement of which also involves the ring Λ_F. Our first main theorem is an analogous result for ideals in the ring $\mathbb{Q}_p\{X\}$ of convergent power series over $\mathbb{Q}_p$ in the indeterminates X. In the following, we let A be a subring of $\mathbb{Q}_p[[X]]$ with fraction field $F = \mathrm{Frac}(A)$. Then $1 \neq pg$ for each $g \in \mathbb{Z}[\gamma(F)]$, and so we may define the subring Λ_F of F as above. We also let $\Lambda_F A$ denote the subring of F generated by Λ_F and A. With these notations, here is our p-adic analytic Nullstellensatz:

Theorem A. *Suppose $A = \mathbb{Q}_p\{X\}$, and let $f, g_1, \dots, g_n \in A$. If*

$$g_1(a) = \cdots = g_n(a) = 0 \implies f(a) = 0 \quad \textit{for each } a \in \mathbb{Q}_p^m \textit{ sufficiently close to } 0,$$

then there are $h_1, \dots, h_n \in \Lambda_F A$ and $k \geqslant 1$ such that $f^k = g_1h_1 + \cdots + g_nh_n$.

The converse of the implication in this theorem holds trivially. Next, an analytic version of Kochen's p-adic Hilbert's 17th Problem:

Theorem B. *Suppose $A = \mathbb{Q}_p\{X\}$, and let $f, g \in A$. Then $|f(a)|_p \leqslant |g(a)|_p$ for all $a \in \mathbb{Q}_p^m$ sufficiently close to 0 if and only if $f \in g\Lambda_F$.*

We also have a p-adic version of Merrien's theorem for formal power series, where we now let t be a single indeterminate over $\mathbb{Q}_p$:

Theorem C. *Suppose $A = \mathbb{Q}_p[[X]]$, and let $f, g_1, \dots, g_n \in A$ be such that*

$$g_1(a) = \cdots = g_n(a) = 0 \implies f(a) = 0 \quad \textit{for each } a \in \mathbb{Q}_p[[t]]^m \textit{ with } a(0) = 0.$$

Then there are $h_1, \dots, h_n \in \Lambda_F A$ and $k \geqslant 1$ such that $f^k = g_1h_1 + \cdots + g_nh_n$.

In our arguments we systematically work in the framework of *Weierstrass systems* from [18], which axiomatize the algebraic properties of the ring A needed for the proofs to go through (crucially among them, the Weierstrass Division Property). As a consequence, for example, Theorem C also holds for the subring $A = \mathbb{Q}[[X]]$ of $\mathbb{Q}_p[[X]]$, the ring $A = \mathbb{Q}_p[[X]]^{\mathrm{a}}$ of power series in $\mathbb{Q}_p[[X]]$ which are algebraic over $\mathbb{Q}_p(X)$, or the ring $A = \mathbb{Q}_p[[X]]^{\mathrm{da}}$ of differentially algebraic power series. (These facts can also be deduced from the Artin Approximation Theorem as proved in [18], but this would be overkill.)

Restricted analytic variants. Both Theorems A and B above deal with *germs* of p-adic analytic functions at 0. The subring $\mathbb{Q}_p\langle X\rangle$ of $\mathbb{Q}_p\{X\}$ consisting of those power series which converge for all $a \in \mathbb{Q}_p^m$ with $|a|_p \leqslant 1$ also satisfies a Weierstrass Division Theorem (albeit of a slightly different kind than in $\mathbb{Q}_p\{X\}$). Our method is adaptable to this setting, and so we also obtain versions of Theorems A and B for the ring $A = \mathbb{Q}_p\langle X\rangle$ of *restricted* (sometimes called *strictly convergent*) power series over $\mathbb{Q}_p$, where the condition "for each $a \in \mathbb{Q}_p^m$ sufficiently close to 0" in both cases is replaced by "for each $a \in \mathbb{Q}_p^m$ with $|a|_p \leqslant 1$". These theorems also hold for certain subrings of $\mathbb{Q}_p\langle X\rangle$ such as the ring $\mathbb{Q}_p\langle X\rangle^{\mathrm{a}} := \mathbb{Q}_p[[X]]^{\mathrm{a}} \cap \mathbb{Q}_p\langle X\rangle$. (See Corollaries 7.35 and 7.36 for the precise statements.)

The same methods also yield a restricted analytic Nullstellensatz and Hilbert's 17th Problem for real closed fields $\boldsymbol{k}$ equipped with a complete ultrametric absolute value $|\cdot|$, such as the Levi-Civita field: the completion of the group algebra $\mathbb{R}[t^{\mathbb{Q}}]$ equipped with the ultrametric absolute value satisfying $|at^q| = \mathrm{e}^{-q}$ for $a \in \mathbb{R}^\times$, $q \in \mathbb{Q}$. (Cf. [41, Chapter 1, §7].) Let $\boldsymbol{k}\langle X\rangle$ denote the subring of $\boldsymbol{k}[[X]]$ consisting of those power series which converge for all $a \in \boldsymbol{k}^m$ with $|a| \leqslant 1$.

Theorem D. *Let $f, g_1, \dots, g_n \in \boldsymbol{k}\langle X\rangle$. Then*

(1) $g_1(a) = \cdots = g_n(a) = 0 \Rightarrow f(a) = 0$ *for all $a \in \boldsymbol{k}^m$ with $|a| \leqslant 1$ if and only if there are $k \geqslant 1$ and $b_1, \dots, b_l, h_1, \dots, h_n \in \boldsymbol{k}\langle X\rangle$ such that $f^{2k} + b_1^2 + \cdots + b_l^2 = g_1h_1 + \cdots + g_nh_n$; and*

(2) $f(a) \geqslant 0$ *for all $a \in \boldsymbol{k}^m$ with $|a| \leqslant 1$ if and only if there are $g, h_1, \dots, h_k \in \boldsymbol{k}\langle X\rangle \setminus \{0\}$ such that $g^2 f = h_1^2 + \cdots + h_k^2$.*

(*Similarly with $\boldsymbol{k}\langle X\rangle^{\mathrm{a}} := \boldsymbol{k}[[X]]^{\mathrm{a}} \cap \boldsymbol{k}\langle X\rangle$ in place of $\boldsymbol{k}\langle X\rangle$.*)

A version of part (2) of this theorem for $\boldsymbol{k}[X]$ in place of $\boldsymbol{k}\langle X\rangle$ was shown by Dickmann [19, Theorem 2]. For our final theorem (an analogue of Theorem B for $\boldsymbol{k}\langle X\rangle$) we let H_K be the subring of $K := \mathrm{Frac}(\boldsymbol{k}\langle X\rangle)$ generated by the elements $1/(1+h)$ where h is sum of squares in K; this "real" analogue of the p-adic Kochen ring Λ_F from above was introduced by Schülting [58]. We also let $R := \{a \in \boldsymbol{k} : |a| \leqslant 1\}$ be the valuation ring of $\boldsymbol{k}$, with maximal ideal $\mathfrak{m} := \{a \in \boldsymbol{k} : |a| < 1\}$, and we let $R\langle X\rangle$ be the subring of $\boldsymbol{k}\langle X\rangle$ consisting of all $f \in \boldsymbol{k}\langle X\rangle$ with $|f(a)| \leqslant 1$ for all $a \in R^m$. The ring H_K is a Prüfer domain; hence so is the subring $H_K R\langle X\rangle$ of K generated by H_K and $R\langle X\rangle$. (In particular, $H_K R\langle X\rangle$ is integrally closed.)

Theorem E. *Let $f, g \in \boldsymbol{k}\langle X\rangle$. Then*

$$|f(a)| \leqslant |g(a)| \text{ for all } a \in R^m \iff f \in g\, H_K R\langle X\rangle,$$
$$|f(a)| < |g(a)| \text{ for all } a \in R^m \iff f \in g\, \mathfrak{m} H_K R\langle X\rangle.$$

The theorems above permit various further potential generalizations which we have not attempted here. For example, let E be a finite extension of $\mathbb{Q}_p$. Jarden-Roquette [31] proved a Nullstellensatz for ideals in $E[X]$ and established the p-adic version of Hilbert's 17th Problem for rational functions in $E(X)$. (Here, the definition of the p-adic Kochen operator needs to be suitably modified.) It should be routine to adapt Theorems A, B, C to this setting. Less routine would be an adaptation of our theorems to germs of analytic functions on basic p-adic subsets of analytic varieties, analogous to [31, Theorems 1.2, 7.2]. (See also [49, §7].) It would also be interesting to generalize Theorems D and E in a similar way. (For polynomials this was studied in [30, 40].) It would also be interesting to use Theorem C in a similar way as Merrien used his Nullstellensatz for formal power series over the reals in order to obtain a p-adic analogue of his Nullstellensatz for germs of C^∞-functions; see [25, Conjecture 4.3]. (Here one should employ the concept of *strict differentiability* for multivariate p-adic functions developed in [7, 26, 59], in order to avoid the well-known disadvantages of the usual notion of differentiability over the p-adics caused by the failure of the Mean Value Theorem.)

Organization of the paper. After a first preliminary section, in Section 2 we recall basic facts about Weierstrass systems and establish the setting of infinitesimal Weierstrass structures, which provide a convenient framework to state theorems like the ones discussed earlier in this introduction. As a warm-up, since these cases are conceptually easier than the p-adic version, in Sections 3 and 4 we then revisit Rückert's and Risler's Nullstellensätze using our method. Here, the relevant model-theoretic results are quantifier elimination theorems for the theory ACVF of algebraically closed non-trivially valued fields (A. Robinson) and for the theory RCVF of real closed non-trivially convexly valued fields (Cherlin-Dickmann), respectively. The model-theoretic ingredient for the proofs of Theorems A, B, C is an analogous elimination theorem for the theory $p\,$CVF of *p-adically closed non-trivially p-convexly valued fields.* We discuss this theory and the relevant QE theorem (which is less prominent in the literature than those for ACVF and RCVF: but see [6, 29]) in Section 5, before giving the proofs of our Theorems A, B, C in Section 6. Finally, Section 7 contains the restricted analytic adaptations of these results, including proofs of Theorems D and E.

Related work. The Weierstrass systems used here are close to those of [18, 21]. Cluckers-Lipshitz [13] introduced a very general class of subrings of formal power series rings stable under Weierstrass Division, called "separated Weierstrass systems", which in a sense amalgamates the Weierstrass systems used here and our restricted Weierstrass systems from Definition 7.8. Given a separated Weierstrass system $\mathcal{A}$, this leads to the concept of a "separated analytic $\mathcal{A}$-structure" on a henselian valued field, expanding our Definition 2.13, and in the case of characteristic zero, to a quantifier elimination in a certain multi-sorted language [13, Theorem 6.3.7]. In the algebraically closed case (without assumptions on the characteristic) one also has quantifier elimination in a one-sorted language [13, Theorem 4.5.15]. A one-sorted QE for the valued field $\mathbb{Q}_p$ expanded by primitives for the functions defined by the restricted power series was proved by Denef and van den Dries [17]. Cubides Kovacics and Haskell [14] similarly show that the real closed ordered valued field $\boldsymbol{k}$ from the context of Theorems D and E with a separated analytic $\mathcal{A}$-structure where $\mathcal{A}$ contains the rings $R\langle X\rangle$ of restricted power series, admits quantifier elimination in a natural one-sorted language. Bleybel [8] proves a quantifier elimination theorem for the p-adic analogue of the Levi-Civita field (i.e., the completion of the group algebra $\mathbb{Q}_p[t^{\mathbb{Q}}]$ equipped with the ultrametric absolute value satisfying $|at^q| = \mathrm{e}^{-q}$ for $a \in \mathbb{Q}_p^\times$, $q \in \mathbb{Q}$) in a 3-sorted language which contains function symbols for (among other things) the functions on the valuation ring given by overconvergent p-adic power series. It would be interesting to know whether these QE theorems for valued fields with analytic structure can be used to give alternative proofs of our Theorems A–E. But we think that the advantage of our approach is that it shows that the relevant Nullstellensätze and related results can already be obtained from the classical *algebraic* QE theorems for valued fields (together with easy uses of Weierstrass Division), rather than their more involved *analytic* counterparts.

Notational conventions. Throughout this paper k, l, m, n range over the set $\mathbb{N} = \{0, 1, 2, \dots\}$ of natural numbers, and p is a prime number. In this paper all rings are commutative with 1. Let R be a ring. We let $R^\times$ be the group of units of R, and if R is an integral domain, then we denote the fraction field of R by $\operatorname{Frac}(R)$.

Acknowledgments. We thank the anonymous referees for the careful reading of the paper and for numerous suggestions (for example, to include Section 1.1) which improved the paper.

1. Valuation-Theoretic Preliminaries

In this paper a *valued field* is a field equipped with one of its valuation rings. Let K be a valued field. Unless specified otherwise we let $\mathcal{O}$ be the distinguished valuation ring of K, with maximal ideal $\smallo$. The residue field of K is $\operatorname{res}(K) := \mathcal{O}/\smallo$, with residue morphism $a \mapsto \overline{a} = a + \smallo \colon \mathcal{O} \to \operatorname{res}(K)$. The value group of K is the ordered abelian group $\Gamma = K^\times/\mathcal{O}^\times$, written additively, with ordering $a\mathcal{O}^\times \leqslant b\mathcal{O}^\times$ iff $b/a \in \mathcal{O}$. The map $a \mapsto va = a\mathcal{O}^\times \colon K^\times \to \Gamma$ is a valuation on K. If we need to indicate the dependence on K we attach a subscript K, so $\mathcal{O} = \mathcal{O}_K$, $v = v_K$, etc. If $K \subseteq L$ is an extension of valued fields (that is, $K \subseteq L$ is a field extension and $\mathcal{O} = \mathcal{O}_L \cap K$), then we identify $\operatorname{res}(K)$ with a subfield of $\operatorname{res}(L)$ and Γ with an ordered subgroup of Γ_L in the natural way. For $a, b \in K$ we set

$$a \preceq b :\Leftrightarrow va \geqslant vb, \quad a \prec b :\Leftrightarrow va > vb, \quad a \asymp b :\Leftrightarrow va = vb, \quad a \sim b :\Leftrightarrow a - b \prec a.$$

The binary relation $\preceq$ is an example of a dominance relation on K:

Definition 1.1. A *dominance relation* on an integral domain R is a binary relation $\preceq$ on R such that for all $f, g, h \in R$:

(D1) $1 \not\preceq 0$;
(D2) $f \preceq f$;
(D3) $f \preceq g$ and $g \preceq h \Rightarrow f \preceq h$;
(D4) $f \preceq g$ or $g \preceq f$;
(D5) $f \preceq g \Leftrightarrow fh \preceq gh$, provided $h \neq 0$;
(D6) $f \preceq h$ and $g \preceq h \Rightarrow f + g \preceq h$.

Thus, if $\mathcal{O}$ is a valuation ring of K, we obtain a dominance relation on K via

$$f \preceq g \ :\Longleftrightarrow\ vf \geqslant vg \ \Longleftrightarrow\ f = gh \text{ for some } h \in \mathcal{O}. \tag{1.1}$$

Conversely, if $\preceq$ is a dominance relation on K, then clearly

$$\mathcal{O} := \{f \in K : f \preceq 1\}$$

is a valuation ring of K, and if v denotes the corresponding valuation on K, then the equivalence (1.1) holds, for all $f, g \in K$. We call $\mathcal{O}$ the valuation ring *associated* to the dominance relation $\preceq$. This yields a one-to-one correspondence between dominance relations on K and valuation rings of K.

Let R be an integral domain. The *trivial* dominance relation $\preceq_{\mathrm{t}}$ on R is the one with $r \preceq_{\mathrm{t}} s$ for all $r, s \in R$ with $s \neq 0$. For any dominance relation $\preceq$ on R there is a unique dominance relation $\preceq_F$ on $F = \operatorname{Frac}(R)$ such that $(R, \preceq) \subseteq (F, \preceq_F)$:

$$\frac{r_1}{s} \preceq_F \frac{r_2}{s} \quad \Longleftrightarrow \quad r_1 \preceq r_2 \qquad (r_1, r_2, s \in R,\ s \neq 0).$$

Example. The non-trivial dominance relations on $\mathbb{Z}$ are exactly the p-adic dominance relations $\preceq_p$, given by $a \preceq_p b$ iff for all n: $b \in p^n\mathbb{Z} \Rightarrow a \in p^n\mathbb{Z}$.

1.1. **Model-theoretic treatment of valued fields.** We now briefly explain basic model-theoretic terminology and notation, focussing on valued fields. A concise presentation of all the general model theory needed here is in [3, Appendix B]. A textbook which also pays attention to valued fields is [47]; for more specialized expositions of the model theory of valued fields see [11, 22].

A (one-sorted) language $\mathcal{L}$ is a pair $(\mathcal{L}^{\mathrm{r}}, \mathcal{L}^{\mathrm{f}})$ where $\mathcal{L}^{\mathrm{r}}$, $\mathcal{L}^{\mathrm{f}}$ are disjoint (possibly empty, or infinite) collections of *relation symbols* and *function symbols*, respectively. Each of these symbols has an associated *arity* (a natural number); symbols of arity n are also said to be *n-ary.* A 0-ary function symbol is called a *constant symbol.* It is customary to present a language as a disjoint union $\mathcal{L} = \mathcal{L}^{\mathrm{r}} \cup \mathcal{L}^{\mathrm{f}}$ of its sets of relation and function symbols, while separately specifying the arities of the various symbols. For example, $\mathcal{L}_{\mathrm{R}} = \{0, 1, -, +, \cdot\}$ is the language of rings: here 0, 1 are constant symbols, $-$ is a unary function symbol, and $+$, $\cdot$ are binary function symbols (so $\mathcal{L}_{\mathrm{R}}$ has no relation symbols). Another example, relevant for this paper, is the expansion $\mathcal{L}_{\preceq} = \mathcal{L}_{\mathrm{R}} \cup \{\preceq\}$ of $\mathcal{L}_{\mathrm{R}}$ by a binary relation symbol $\preceq$. Here, $\mathcal{L}$ is an *expansion* of a language $\mathcal{L}_0$, and $\mathcal{L}_0$ a *reduct* of $\mathcal{L}$, if $\mathcal{L}_0^{\mathrm{r}} \subseteq \mathcal{L}^{\mathrm{r}}$ and $\mathcal{L}_0^{\mathrm{f}} \subseteq \mathcal{L}^{\mathrm{f}}$, with unchanged arities for the symbols in $\mathcal{L}_0$.

Let $\mathcal{L}$ be a language. An *$\mathcal{L}$-structure* $\boldsymbol{M}$ consists of its *underlying set* $M \neq \emptyset$ together with *interpretations* of each symbol of $\mathcal{L}$ in $\boldsymbol{M}$: for each m-ary $R \in \mathcal{L}^{\mathrm{r}}$, a relation $R^{\boldsymbol{M}} \subseteq M^m$, and for n-ary $f \in \mathcal{L}^{\mathrm{f}}$, a function $f^{\boldsymbol{M}} \colon M^n \to M$. (So each constant symbol c is interpreted by a function $M^0 \to M$, identified with the unique element $c^{\boldsymbol{M}}$ in its image, M^0 being a singleton.) In practice the superscript $\boldsymbol{M}$ is often suppressed, thus a structure and its universe are denoted by the same letter, and so are the symbols of $\mathcal{L}$ and their interpretations in $\boldsymbol{M}$. *Morphisms, embeddings,* and *substructures* of $\mathcal{L}$-structures are defined in the natural way; e.g., an $\mathcal{L}$-structure $\boldsymbol{M}$ is a substructure of an $\mathcal{L}$-structure $\boldsymbol{N}$ if $M \subseteq N$ and $R^{\boldsymbol{M}} = R^{\boldsymbol{N}} \cap M^m$ and $f^{\boldsymbol{N}}|_{M^n} = f^{\boldsymbol{M}}$ for each m-ary $R \in \mathcal{L}^{\mathrm{r}}$ and n-ary $f \in \mathcal{L}^{\mathrm{f}}$. If $\mathcal{L}_0$ is a reduct of $\mathcal{L}$, then $\boldsymbol{M}|\mathcal{L}_0$ is the *$\mathcal{L}_0$-reduct* of $\boldsymbol{M}$: the $\mathcal{L}_0$-structure with same underlying set M and the same interpretations of the symbols in $\mathcal{L}_0$ as in $\boldsymbol{M}$.

Each ring R can be construed as an $\mathcal{L}_{\mathrm{R}}$-structure by interpreting 0, 1 by the additive and multiplicative identity of R, respectively, $-$ by the function $r \mapsto -r$, and $+$, $\cdot$ by $(r, s) \mapsto r + s$ and $(r, s) \mapsto r \cdot s$, respectively. Morphisms, embeddings, and substructures of $\mathcal{L}_{\mathrm{R}}$-structures then correspond to morphisms, embeddings, and substructures of rings, respectively. (But of course we are, in principle, free to also view R as an $\mathcal{L}_{\mathrm{R}}$-structure in an unnatural way, by choosing the interpretations of the symbols of $\mathcal{L}_{\mathrm{R}}$ any way we like.) In this paper we also always construe each valued field $(K, \mathcal{O})$ as an $\mathcal{L}_{\preceq}$-structure by interpreting $\preceq$ as the dominance relation on K given by (1.1). Then "valued subfield" corresponds to "$\mathcal{L}_{\preceq}$-substructure." (This way of treating valued fields as model theoretic structures is essentially equivalent to that in [47, Chapter 4], which employs valuation divisibilities instead of dominance relations. For other choices see [11, 22].)

The purpose of a language $\mathcal{L}$ is to generate *$\mathcal{L}$-formulas,* which express properties of (finite tuples of) elements of $\mathcal{L}$-structures. They are (well-formed, in a certain precise sense) finite words on an alphabet consisting of $\mathcal{L}^{\mathrm{r}} \cup \mathcal{L}^{\mathrm{f}}$ together with the symbols $\top$, $\bot$, $\neg$, $\vee$, $\wedge$, $=$, $\forall$, $\exists$, to be thought of as *true, false, not, or, and, equals, there exists,* and *for all,* respectively, together with an infinite collection of *variables* (usually written x, y, z, $\dots$), thought of as ranging over the universe of an $\mathcal{L}$-structure (and not over, say, subsets thereof). Variables which do not appear within the scope of a quantifier in an $\mathcal{L}$-formula φ are said to be *free* in φ, and $\mathcal{L}$-formulas without free variables are *$\mathcal{L}$-sentences.* For example, the commutativity of addition in a ring is expressed by the $\mathcal{L}_{\mathrm{R}}$-sentence $\forall x \forall y(x+y=y+x)$. Strictly speaking, this should be $\forall x \forall y = +xy + yx$; but as usual we take the liberty of writing binary symbols, including $=$, in infix rather than prefix notation, and of freely employing parentheses to enhance readability. Below φ, ψ, θ range over $\mathcal{L}$-formulas and σ over $\mathcal{L}$-sentences. We also use common abbreviations like $\forall x$ for $\forall x_1 \cdots \forall x_m$, where $x = (x_1, \dots, x_m)$ is a tuple of distinct variables, and $\varphi \leftrightarrow \psi$ in place of $(\varphi \wedge \psi) \vee (\neg\varphi \wedge \neg\psi)$.

Given x as above, writing $\varphi(x)$ indicates that x contains all free variables in φ. For an $\mathcal{L}$-structure $\boldsymbol{M}$ and $a \in M^m$ one then defines, by induction on the construction of φ, when $\boldsymbol{M}$ *satisfies* $\varphi(a)$—in symbols: $\boldsymbol{M} \models \varphi(a)$—in the natural way. The subset of M^m *defined by* $\varphi(x)$ in $\boldsymbol{M}$ is $\varphi^{\boldsymbol{M}} := \big\{a \in M^m : \boldsymbol{M} \models \varphi(a)\big\}$. (For example, for a valued field K and the $\mathcal{L}_{\preceq}$-formulas $\varphi(x)$, $\psi(x)$, $\theta(x)$, where x is a single variable, given by $x \preceq 1$, $x \preceq 1 \wedge \neg 1 \preceq x$, and $x \preceq 1 \wedge \exists y(x \cdot y = 1 \wedge y \preceq 1)$, respectively, we have $\mathcal{O} = \varphi^K$, $o = \psi^K$, and $\mathcal{O}^\times = \theta^K$.) Note: if y is a variable which neither occurs in x nor free in φ, then the $(m+1)$-tuple (x,y) also contains all free variables in φ, so we could write $\varphi = \varphi(x,y)$ according to our earlier convention; however, for $a \in M^m$, $b \in M$ we have $\boldsymbol{M} \models \varphi(a,b)$ iff $\boldsymbol{M} \models \varphi(a)$, and thus in particular, for a $\mathcal{L}$-sentence σ the status of $\boldsymbol{M} \models \sigma$ does not depend on a. The $\mathcal{L}$-structures $\boldsymbol{M}$, $\boldsymbol{N}$ are said to be *elementarily equivalent* ($\boldsymbol{M} \equiv \boldsymbol{N}$) if for each σ we have $\boldsymbol{M} \models \sigma$ iff $\boldsymbol{N} \models \sigma$.

Let Σ be a set of $\mathcal{L}$-sentences. Then $\boldsymbol{M}$ is a *model* of Σ (in symbols: $\boldsymbol{M} \models \Sigma$) if $\boldsymbol{M} \models \sigma$ for all $\sigma \in \Sigma$. We also write $\Sigma \models \sigma$ if every model of Σ satisfies σ. If Σ contains each σ with $\Sigma \models \sigma$, then Σ is an *$\mathcal{L}$-theory.* Clearly $\Sigma^{\models} := \{\sigma : \Sigma \models \sigma\}$ is the smallest $\mathcal{L}$-theory containing Σ. If Σ has a model, then $\boldsymbol{M} \equiv \boldsymbol{N}$ for all $\boldsymbol{M}, \boldsymbol{N} \models \Sigma$ iff for all σ, either $\Sigma \models \sigma$ or $\Sigma \models \neg\sigma$; in this case, Σ is said to be *complete.* Taking $\mathcal{L} = \mathcal{L}_{\preceq}$ and for Σ the set of $\mathcal{L}_{\preceq}$-sentences which consists of the axioms for fields (which can be formulated in the sublanguage $\mathcal{L}_{\mathrm{R}}$ of $\mathcal{L}_{\preceq}$) together with (universal) $\mathcal{L}_{\preceq}$-sentences formalizing the properties (D1)–(D6), we obtain the $\mathcal{L}_{\preceq}$-theory $\mathrm{VF} := \Sigma^{\models}$ of valued fields. The $\mathcal{L}_{\preceq}$-theory VF is not complete since (for example) it has models of different characteristic.

If $A \subseteq M$, we let $\mathcal{L}_A$ be the expansion of $\mathcal{L}$ by a new constant symbol $\underline{a}$ for each $a \in A$, and $\boldsymbol{M}_A$ be the $\mathcal{L}_A$-structure with $\mathcal{L}$-reduct $\boldsymbol{M}$ where each $\underline{a}$ is interpreted by a. We say that $\boldsymbol{M}$ is an *elementary substructure* of $\boldsymbol{N}$, and $\boldsymbol{N}$ an *elementary extension* of $\boldsymbol{M}$, if $M \subseteq N$ and $\boldsymbol{M}_M \equiv \boldsymbol{N}_M$. If every extension of models of Σ is elementary, then Σ is said to be *model complete.* Finally, we say that φ is quantifier-free if $\forall$, $\exists$ do not occur in φ, and Σ is said to admit *quantifier elimination* (QE) if for each $\varphi(x)$, where $x = (x_1, \dots, x_m)$, there is a quantifier-free $\psi(x)$ with $\Sigma \models \forall x(\varphi \leftrightarrow \psi)$. In this case, Σ is also model complete. Moreover, Σ admits QE iff it is *substructure complete*: if $\boldsymbol{M}, \boldsymbol{N} \models \Sigma$ and $\boldsymbol{A}$ is a common substructure of both $\boldsymbol{M}$ and $\boldsymbol{N}$, then $\boldsymbol{M}_A \equiv \boldsymbol{N}_A$. (See, e.g., [3, Corollary B.11.6] or [47, remark after Theorem 3.4.1].)

1.2. **Extension of valuations.** Let A be a local subring of a field K with maximal ideal $\mathfrak{m} = \mathfrak{m}_A$ and residue field $\boldsymbol{k} = A/\mathfrak{m}$. We recall that any maximal element of the class of all local subrings of K lying over A, partially ordered by $B \leqslant B' :\Longleftrightarrow B'$ lies over B, is a valuation ring of K. (Krull; cf., e.g., [3, Proposition 3.1.13].)

In particular, by Zorn, there is always a valuation ring of K lying over A. Under suitable hypotheses on A we can be more precise (see, e.g., [31, Lemma A1]):

Lemma 1.2. *If A is a regular local ring and $K = \operatorname{Frac}(A)$, then there is a valuation ring $\mathcal{O}$ of K lying over A such that the natural inclusion $A \to \mathcal{O}$ induces an isomorphism $\boldsymbol{k} \to \mathcal{O}/\smallo$.*

(Indeed, for each regular system of parameters $x_1, \dots, x_d$ of A there is a unique valuation ring $\mathcal{O}$ as in Lemma 1.2 with $\Gamma = \mathbb{Z}v(x_1) \oplus \cdots \oplus \mathbb{Z}v(x_d)$, ordered lexicographically.)

1.3. **Coarsening and specialization.** Let K be a valued field and Δ be a convex subgroup of $\Gamma = v(K^\times)$. We have the ordered quotient group $\dot{\Gamma} = \Gamma/\Delta$ and the valuation

$$\dot{v} = v_\Delta \colon K^\times \to \dot{\Gamma}, \qquad \dot{v}(a) := v(a) + \Delta \text{ for } a \in K^\times$$

on the field K, the Δ-*coarsening of* v. The valuation ring of $\dot{v}$ is

$$\dot{\mathcal{O}} \ = \ \mathcal{O}_\Delta \ := \ \{a \in K : va \geqslant \delta \text{ for some } \delta \in \Delta\},$$

which has $\mathcal{O}$ as a subring and has maximal ideal

$$\dot{\smallo} \ := \ \{a \in K : va > \Delta\} \subseteq \smallo.$$

The valued field $(K, \dot{\mathcal{O}})$ is called the Δ-*coarsening of* K. Put $\dot{K} := \dot{\mathcal{O}}/\dot{\smallo}$, the residue field of $\dot{\mathcal{O}}$, and $\dot{a} := a + \dot{\smallo} \in \dot{K}$ for $a \in \dot{\mathcal{O}}$. Then for $a \in \dot{\mathcal{O}} \setminus \dot{\smallo}$ the value va depends only on the residue class $\dot{a} \in \dot{K}$. This gives the valuation $v \colon \dot{K}^\times \to \Delta$, $v\dot{a} := va$ with valuation ring $\mathcal{O}_{\dot{K}} = \{\dot{a} : a \in \mathcal{O}\}$, having maximal ideal $\smallo_{\dot{K}} = \{\dot{a} : a \in \smallo\}$. Throughout $\dot{K}$ stands for the valued field $(\dot{K}, \mathcal{O}_{\dot{K}})$, called the Δ-*specialization* of K. The composed map

$$\mathcal{O} \to \mathcal{O}_{\dot{K}} \to \operatorname{res}(\dot{K}) = \mathcal{O}_{\dot{K}}/\smallo_{\dot{K}}$$

has kernel $\smallo$, and thus induces a field isomorphism $\operatorname{res}(K) \xrightarrow{\cong} \operatorname{res}(\dot{K})$, and we identify $\operatorname{res}(K)$ and $\operatorname{res}(\dot{K})$ via this map.

Every subring of K containing $\mathcal{O}$ is a valuation ring of K. In fact, every such subring $\mathcal{O}_1 \supseteq \mathcal{O}$ of K arises as the valuation ring of the Δ_1-coarsening of v for some convex subgroup Δ_1 of Γ, namely $\Delta_1 := v(\mathcal{O}_1 \setminus \{0\})$. The map $\mathcal{O}_1 \mapsto \Delta_1$ is an inclusion-preserving bijection from the set of subrings of K containing $\mathcal{O}$ onto the set of convex subgroups of Γ. (Cf., e.g., [3, Lemmas 3.1.4, 3.1.5].) In particular, the collection of subrings of K containing $\mathcal{O}$ is totally ordered under inclusion, and we have $\mathcal{O}_1 \supset \mathcal{O}$ iff $\Delta_1 \neq \{0\}$. The following is easy to verify:

Lemma 1.3. *Let $\boldsymbol{k} := \operatorname{res}(K)$ and $\mathcal{O}_{\boldsymbol{k}}$ be a valuation ring of $\boldsymbol{k}$. Then $\mathcal{O}_0 := \{a \in \mathcal{O} : \overline{a} \in \mathcal{O}_{\boldsymbol{k}}\}$ is a valuation ring of K. If Δ_0 is the convex subgroup of the value group of $\mathcal{O}_0$ with $\dot{\mathcal{O}}_0 = \mathcal{O}$, then the Δ_0-specialization of $(K, \mathcal{O}_0)$ is $(\boldsymbol{k}, \mathcal{O}_{\boldsymbol{k}})$.*

1.4. **Convexity.** Let K be an ordered field. Recall that a subring of K is convex iff it contains the interval $[0, 1]$, and as a consequence, every convex subring of K is a valuation ring of K. (See, e.g., [3, Lemma 3.5.10].) Let R be a subring of K; then the convex hull

$$A := \big\{a \in K : |a| \leqslant \varepsilon \text{ for some } \varepsilon \in R,\ \varepsilon > 0\big\}$$

of R in K is a subring of K. This is the smallest convex subring of K containing R, with maximal ideal

$$\mathfrak{m} = \big\{a \in K : |a| \leqslant 1/\varepsilon \text{ for all } \varepsilon \in R,\ \varepsilon > 0\big\}.$$

Let $\mathcal{O}_0$ be the convex hull of $\mathbb{Q}$ in K. Then a subring of K is convex iff it contains $\mathcal{O}_0$; in particular, the collection of convex subrings of K is totally ordered under inclusion. We generalize these concepts to an arbitrary valued field. Thus let now K be a valued field with valuation ring $\mathcal{O}$ and associated dominance relation $\preceq$.

Definition 1.4. We say that a subring of K is *convex* (in the valued field K) if it contains $\mathcal{O}$. Clearly $\mathcal{O}$ and K are convex subrings of K; we call these the *trivial* convex subrings of K.

Note that every convex subring of K is a valuation ring of K. In fact, for each convex subgroup Δ of the value group of K, the valuation ring of the Δ-coarsening of K is a convex subring of K, and each convex subring of K arises this way. Thus the set of convex subrings of K is totally ordered under inclusion.

Lemma 1.5. *Let R be a subring of K. Then the subring $A = \mathcal{O}R$ of K generated by $\mathcal{O}$ and R is the smallest convex subring of K which contains R. We have*

$$A = \big\{a \in K : a \preceq \varepsilon \text{ for some } \varepsilon \in R\big\},$$

with maximal ideal

$$\mathfrak{m} = \big\{a \in K : a \prec 1/\varepsilon \text{ for all non-zero } \varepsilon \in R\big\}.$$

Proof. The first statement is easy to verify; for the second statement use that the maximal ideal of the local ring A is given by $\mathfrak{m} = \{a \in A : a = 0 \text{ or } a \notin A^\times\}$. □

Given a subring R of K, we call $A = \mathcal{O}R$ the *convex hull* of R in K, denoted by $\operatorname{conv}_K(R)$, or by $\operatorname{conv}(R)$ if K is clear from the context. (If K comes equipped with a field ordering and $\mathcal{O} = \mathcal{O}_0$ as above, then this agrees with the convex hull of R in the ordered field K.) The map $R \mapsto \operatorname{conv}(R)$ is a closure operator on the collection of subrings of K, that is,

$$R \subseteq \operatorname{conv}(R), \quad R \subseteq S \implies \operatorname{conv}(R) \subseteq \operatorname{conv}(S), \quad \operatorname{conv}(\operatorname{conv}(R)) = \operatorname{conv}(R).$$

Let L be a valued field extension of K and R be a convex subring of K. It is easily seen that $\operatorname{conv}_L(R)$ lies over R. Moreover (cf. [3, remarks after Proposition 3.1.20]):

Lemma 1.6. *If L is algebraic over K, then $\operatorname{conv}_L(R)$ is the unique convex subring of L lying over R.*

We conclude this section with some reminders about $\mathbb{Z}$-groups.

$\mathbb{Z}$-groups. Let Γ be an ordered abelian group, written additively. We let $\Gamma^> := \{\gamma \in \Gamma : \gamma > 0\}$, and similarly with $\geqslant$ instead of $>$. If $\Gamma^>$ has a smallest element, denoted by 1, then we identify $\mathbb{Z}$ with an ordered subgroup of Γ via the embedding $r \mapsto r \cdot 1 \colon \mathbb{Z} \to \Gamma$, making $\mathbb{Z}$ the smallest non-zero convex subgroup of Γ. We recall that Γ is said to be a *$\mathbb{Z}$-group* if $\Gamma^>$ has a smallest element 1 and for each $n \geqslant 1$ and $\gamma \in \Gamma$ there are some $i \in \{0, \dots, n-1\}$ such that $\gamma - i \in n\Gamma$. The ordered abelian group $\mathbb{Z}$ of integers is a $\mathbb{Z}$-group, and every $\mathbb{Z}$-group is elementarily equivalent to $\mathbb{Z}$ in the language $\{0, -, +, \leqslant\}$ of ordered abelian groups. (See, e.g., [47, §4.1].) For future reference here are a few other well-known (and easy to prove) facts :

Lemma 1.7. *Let $\Delta \neq \{0\}$ be a convex subgroup of Γ. Then Γ is a $\mathbb{Z}$-group iff Δ is a $\mathbb{Z}$-group and Γ/Δ is divisible.*

Lemma 1.8. *Let Δ be a subgroup of a $\mathbb{Z}$-group Γ which contains the smallest element of $\Gamma^>$. Then Δ is a $\mathbb{Z}$-group iff Γ/Δ is torsion-free.*

2. Weierstrass Systems and Infinitesimal Analytic Structures

In this section we let $\boldsymbol{k}$ be a field, of arbitrary characteristic unless stated otherwise. We let $(X_m)_{m\geqslant 1}$ be a sequence of distinct indeterminates over $\boldsymbol{k}$. As usual $\boldsymbol{k}[[X_1,\dots,X_m]]$ denotes the ring of formal power series over $\boldsymbol{k}$ in the indeterminates $X_1,\dots,X_m$. In the following we let $X=(X_1,\dots,X_m)$, we let α, β range over $\mathbb{N}^m$, and for $\alpha=(\alpha_1,\dots,\alpha_m)$ put $|\alpha|:=\alpha_1+\cdots+\alpha_m$ and $X^\alpha:=X_1^{\alpha_1}\cdots X_m^{\alpha_m}$. Consider an element

$$f=\sum_\alpha f_\alpha X^\alpha \qquad (f_\alpha\in\boldsymbol{k})$$

of $\boldsymbol{k}[[X]]$. If $f\neq 0$, then the *order* of f is the smallest d such that $f_\alpha\neq 0$ for some α with $|\alpha|=d$. Suppose now $m\geqslant 1$. One says that $f\in\boldsymbol{k}[[X]]$ is *regular of order $d\in\mathbb{N}$ in X_m* if $f(0,X_m)\in\boldsymbol{k}[[X_m]]$ is non-zero of order d. Note that if $f=f_1\cdots f_n$ where $f_1,\dots,f_n\in\boldsymbol{k}[[X]]$, then f is regular in X_m of order d iff f_i is regular in X_m of order d_i for $i=1,\dots,n$, with $d_1+\cdots+d_n=d$.

Let $d\in\mathbb{N}$, $d\geqslant 1$. Then we have a $\boldsymbol{k}$-algebra automorphism τ_d of $\boldsymbol{k}[[X]]$ such that $\tau_d(X_i)=X_i+X_m^{d^{m-i}}$ for $i=1,\dots,m-1$ and $\tau_d(X_m)=X_m$. (See, e.g., [27, I, §4, Satz 3 and the remark following it].) For non-zero $f\in\boldsymbol{k}[[X]]$ there is always some $d\in\mathbb{N}$, $d\geqslant 1$ such that $\tau_d(f)$ is regular in X_m (of some order). In particular, given non-zero $f_1,\dots,f_n\in\boldsymbol{k}[[X]]$, there is some $d\in\mathbb{N}$, $d\geqslant 1$ such that $\tau_d(f_1),\dots,\tau_d(f_n)$ are all regular in X_m.

We also recall that $\boldsymbol{k}[[X]]$ is a complete local noetherian integral domain with maximal ideal generated by $X_1,\dots,X_m$. Thus for $f\in\boldsymbol{k}[[X]]$ we have $f\in\boldsymbol{k}[[X]]^\times$ iff $f(0)\in\boldsymbol{k}^\times$; we say that f is a 1-*unit* if $f(0)=1$.

2.1. Weierstrass systems.

The following definition is a special instance of a concept introduced by Denef-Lipshitz [18]:

Definition 2.1. A *Weierstrass system over $\boldsymbol{k}$* is a family of rings $(W_m)_{m\geqslant 0}$ such that for all m we have, with $X=(X_1,\dots,X_m)$:

- (W1) $\boldsymbol{k}[X]\subseteq W_m\subseteq\boldsymbol{k}[[X]]$;
- (W2) for each permutation σ of $\{1,\dots,m\}$, the $\boldsymbol{k}$-algebra automorphism $f(X)\mapsto f(X_{\sigma(1)},\dots,X_{\sigma(m)})$ of $\boldsymbol{k}[[X]]$ maps W_m onto itself;
- (W3) $W_m\cap\boldsymbol{k}[[X']]=W_{m-1}$ for $X'=(X_1,\dots,X_{m-1})$, $m\geqslant 1$; and
- (W4) if $g\in W_m$ is regular of order d in X_m $(m\geqslant 1)$, then for every $f\in W_m$ there are $q\in W_m$ and a polynomial $r\in W_{m-1}[X_m]$ of degree $<d$ (in X_m) such that $f=qg+r$. (Weierstrass Division.)

(In the case where $\boldsymbol{k}$ has positive characteristic, [18] includes further axioms, but those are not needed for our purposes.)

Examples of Weierstrass systems include

1. the system $\big(\boldsymbol{k}[[X_1,\dots,X_m]]\big)$ consisting of all formal power series rings;
2. the system $\big(\boldsymbol{k}[[X_1,\dots,X_m]]^{\mathrm{a}}\big)$, where $\boldsymbol{k}[[X_1,\dots,X_m]]^{\mathrm{a}}$ is the ring of power series in $\boldsymbol{k}[[X_1,\dots,X_m]]$ which are algebraic over $\boldsymbol{k}[X_1,\dots,X_m]$ (cf. [37]);
3. if $\operatorname{char}\boldsymbol{k}=0$, the system $\big(\boldsymbol{k}[[X_1,\dots,X_m]]^{\mathrm{da}}\big)$, where $\boldsymbol{k}[[X_1,\dots,X_m]]^{\mathrm{da}}$ is the ring of all power series $f\in\boldsymbol{k}[[X]]=\boldsymbol{k}[[X_1,\dots,X_m]]$ which are *differentially algebraic* over $\boldsymbol{k}$, that is, the fraction field of the subring $\boldsymbol{k}\big[\partial^{|\beta|}f/\partial X^\beta\big]$ of $\boldsymbol{k}[[X]]$ generated by the partial derivatives of f has finite transcendence degree over $\boldsymbol{k}$ (see [21, §5]);

(4) assuming that $\boldsymbol{k}$ comes equipped with a complete absolute value, the system $\big(\boldsymbol{k}\{X_1,\dots,X_m\}\big)$, where $\boldsymbol{k}\{X_1,\dots,X_m\}$ consists of all power series in $\boldsymbol{k}[[X_1,\dots,X_m]]$ that converge in some neighborhood of the origin. (See, e.g., [27, Kapitel I, §4].)

In the rest of this section we let $W=(W_m)$ be a Weierstrass system over $\boldsymbol{k}$. Note that the definition of Weierstrass system given above implicitly depends on our fixed choice of the sequence (X_m) of indeterminates. If $Y=(Y_1,\dots,Y_m)$ is an arbitrary tuple of distinct indeterminates, then we let $\boldsymbol{k}\lfloor Y\rfloor := \big\{f\in\boldsymbol{k}[[Y]] : f(X)\in W_m\big\}$. Here as before $X=(X_1,\dots,X_m)$. We also denote by (X) the ideal of $W_m=\boldsymbol{k}\lfloor X\rfloor$ generated by $X_1,\dots,X_m$. In the rest of this subsection we also let $Y=(Y_1,\dots,Y_n)$ be a tuple of distinct indeterminates disjoint from X.

With these conventions, we now list some basic facts about Weierstrass systems which we will be using.

Lemma 2.2. $W_m\cap\boldsymbol{k}[[X]]^\times = W_m^\times$.

Proof. Let $g\in W_m\cap\boldsymbol{k}[[X]]^\times$. Then $X_m g$ is regular of order 1 in X_m, hence (W4) yields $X_m=(X_m g)q+r$ where $q\in W_m$, $r\in W_{m-1}\subseteq\boldsymbol{k}[[X']]$, thus $r=0$ and so $1=gq$. □

By [18, Remarks 1.3(2)] we have:

Lemma 2.3. *Let $f\in\boldsymbol{k}\lfloor X,Y\rfloor$, $g\in(X)^n$. Then $f(X,g(X))\in\boldsymbol{k}\lfloor X\rfloor$.*

Proof. For later use we include the proof. With $g=(g_1,\dots,g_n)$, repeated application of (W4) in $\boldsymbol{k}\lfloor X,Y\rfloor$ yields

$$\begin{aligned} f(X,Y) &= u_n(X,Y)(Y_n-g_n(X))+R_1(X,Y_1,\dots,Y_{n-1})\\ &= u_n(X,Y)(Y_n-g_n(X))+u_{n-1}(X,Y)(Y_{n-1}-g_{n-1}(X))\\ &\qquad + R_2(X,Y_1,\dots,Y_{n-2})\\ &\ \ \vdots\\ &= u_n(X,Y)(Y_n-g_n(X))+\cdots+u_1(X,Y)(Y_1-g_1(X))+R_n(X)\end{aligned}$$

and hence $f(X,g(X))=R_n(X)\in\boldsymbol{k}\lfloor X\rfloor$. □

Corollary 2.4. *For all $f\in\boldsymbol{k}\lfloor Y\rfloor$ and $g\in(X)^n$ we have $f(g(X))\in\boldsymbol{k}\lfloor X\rfloor$.*

Proof. By (W3) we have

$$f' := f(X_1,\dots,X_n)\in\boldsymbol{k}\lfloor X_1,\dots,X_{m+n}\rfloor.$$

Let σ be a permutation of $\{1,\dots,m+n\}$ with $\sigma(i)=m+i$ for $i=1,\dots,n$; then

$$h := f'(X_{\sigma(1)},\dots,X_{\sigma(m+n)})\in\boldsymbol{k}\lfloor X_1,\dots,X_{m+n}\rfloor$$

by (W2). So by Lemma 2.3 applied to h in place of f and $Y=(X_{m+1},\dots,X_{m+n})$ we get $f(g(X))=h(X,g(X))\in\boldsymbol{k}\lfloor X\rfloor$. □

By [18, Remarks 1.3(1),(7),(8)], we have:

Lemma 2.5. *The ring $\boldsymbol{k}\lfloor X\rfloor$ is noetherian regular local; its unique maximal ideal is (X), and its completion is $\boldsymbol{k}[[X]]$.*

Together with [43, Theorem 8.14] this yields:

Corollary 2.6. *The ring $\boldsymbol{k}[[X]]$ is a faithfully flat $\boldsymbol{k}\lfloor X\rfloor$-module.*

The following is [18, Remarks 1.3(4)]:

Lemma 2.7 (Implicit Function Theorem)**.** *Let $f = (f_1, \dots, f_n) \in \boldsymbol{k}\lfloor X, Y\rfloor^n$ be such that*

$$f \equiv 0 \mod (X, Y) \quad \text{and} \quad \det(\partial f_i/\partial Y_j) \not\equiv 0 \mod (X, Y).$$

Then there is some $y = (y_1, \dots, y_n) \in (X)^n$ such that $f(X, y) = 0$.

Using a special case of the previous lemma we obtain:

Lemma 2.8. *The local ring $R = \boldsymbol{k}\lfloor X\rfloor$ is henselian.*

Proof. Let Y be a single indeterminate over R and

$$P(Y) = 1 + Y + b_2 Y^2 + \cdots + b_d Y^d \in R[Y]$$

where $d \geqslant 2$, $b_2, \dots, b_d \in (X)$. It suffices to show that there is some $y \in R$ such that $P(y) = 0$. To see this consider $f(X, Y) := P(Y - 1) \in R[Y] \subseteq \boldsymbol{k}\lfloor X, Y\rfloor$. Then $f \equiv 0 \mod (X, Y)$ and $\partial f/\partial Y \equiv 1 \mod (X, Y)$. Now use Lemma 2.7. □

The local ring $\boldsymbol{k}[[X]]^{\mathrm{a}}$ is the henselization of its local subring $\boldsymbol{k}[X]_{\mathfrak{m}}$ where $\mathfrak{m}$ is the ideal of $\boldsymbol{k}[X]$ generated by $X_1, \dots, X_m$. (See, e.g., [36, Théorème 4].) From this fact in combination with the universal property of henselizations and Lemma 2.8, we obtain $\boldsymbol{k}[[X]]^{\mathrm{a}} \subseteq \boldsymbol{k}\lfloor X\rfloor$. This is not used later, in the contrast to the following, more immediate consequence of Lemma 2.8:

Corollary 2.9. *Let $f \in \boldsymbol{k}\lfloor X\rfloor$, $k \geqslant 1$, and suppose* $\operatorname{char} \boldsymbol{k} = 0$ *or* $\operatorname{char} \boldsymbol{k} = p > 0$ *and $p \nmid k$. Then*

$$f = g^k \text{ for some } g \in \boldsymbol{k}\lfloor X\rfloor^\times \quad \Longleftrightarrow \quad f(0) = a^k \text{ for some } a \in \boldsymbol{k}^\times.$$

In particular, the group of 1*-units of $\boldsymbol{k}\lfloor X\rfloor$ is k-divisible.*

Recall that $\boldsymbol{k}$ is called *euclidean* if $a^2 + b^2 \neq -1$ for all $a, b \in \boldsymbol{k}$, and for all $a \in \boldsymbol{k}$ there is some $b \in \boldsymbol{k}$ with $a = b^2$ or $a = -b^2$. In this case $\boldsymbol{k}$ has a unique ordering making it an ordered field, given by $a \geqslant 0 \Leftrightarrow a = b^2$ for some $b \in \boldsymbol{k}$, and below we then always view $\boldsymbol{k}$ as an ordered field this way. (For example, each real closed field is euclidean, as is the field of real constructible numbers; but neither $\mathbb{Q}$ nor any algebraic number field is euclidean [38, Corollary 5.12].)

Lemma 2.10. *Suppose $\boldsymbol{k}$ is euclidean. Let K be an ordered field and $\sigma\colon \boldsymbol{k}\lfloor X\rfloor \to K$ be a ring morphism, and let $u \in \boldsymbol{k}\lfloor X\rfloor$. Then*

$$u(0) > 0 \quad \Longleftrightarrow \quad u \in \boldsymbol{k}\lfloor X\rfloor^\times \text{ and } \sigma(u) > 0.$$

Proof. Suppose $u(0) > 0$. Then $u \in \boldsymbol{k}\lfloor X\rfloor^\times$, and since $u(0)$ is a square in $\boldsymbol{k}$, u is a square in $\boldsymbol{k}\lfloor X\rfloor$ by Corollary 2.9, so $\sigma(u) > 0$. Conversely, suppose $u \in \boldsymbol{k}\lfloor X\rfloor^\times$ and $\sigma(u) > 0$. Then $u(0) \neq 0$; if $u(0) < 0$ then $\sigma(u) < 0$, by what we just showed applied to $-u$ in place of u, a contradiction. Thus $u(0) > 0$. □

Lemma 2.11 (Weierstrass Preparation)**.** *Suppose $m \geqslant 1$. Let $g \in \boldsymbol{k}\lfloor X\rfloor$ be regular in X_m of order d, and set $X' := (X_1, \dots, X_{m-1})$. Then there are a unit u of $\boldsymbol{k}\lfloor X\rfloor$ and a polynomial*

$$w = X_m^d + w_1 X_m^{d-1} + \cdots + w_d \qquad \text{where } w_1, \dots, w_d \in (X')$$

such that $g = uw$.

This is [18, Remarks 1.3(9)]. Finally, we note:

Lemma 2.12. *Suppose $\boldsymbol{k}$ is perfect. If P is a prime ideal of $\boldsymbol{k}\lfloor X\rfloor$, then the ideal $P\boldsymbol{k}[[X]]$ of $\boldsymbol{k}[[X]]$ generated by P is also prime.*

Proof. By [18, Theorem 2.1] in combination with Lemmas 2.5 and 2.8, $\boldsymbol{k}\lfloor X\rfloor$ is a Weierstrass ring in the sense of Nagata [46, §45], so we can use [46, (45.1)]. □

2.2. **Infinitesimal W-structures.** *In this subsection we let K be a valued field with valuation ring $\mathcal{O}=\mathcal{O}_K$ and maximal ideal $\smallo=\smallo_K$.* The following definition is modeled on [23, axioms C1)–C3) in (2.1)]:

Definition 2.13. An **infinitesimal W-structure** on K is a family $(\phi_m)_{m\geqslant 0}$ of ring morphisms

$$\phi_m\colon W_m\to\{\text{ring of functions } \smallo^m\to\mathcal{O}\}$$

such that:

(A1) $\phi_m(X_i)=i$-th coordinate function on $\smallo^m$, for each $i=1,\dots,m$;
(A2) the map ϕ_{m+1} extends ϕ_m, if we identify in the obvious way functions on $\smallo^m$ with functions on $\smallo^{m+1}$ that do not depend on the last coordinate;
(A3) for all $f\in W_m$, permutations σ of $\{1,\dots,m\}$, and $a=(a_1,\dots,a_m)\in\smallo^m$:

$$\phi_m\big(f(X_{\sigma(1)},\dots,X_{\sigma(m)})\big)(a)=\phi_m(f)\big(a_{\sigma(1)},\dots,a_{\sigma(m)}\big).$$

Note that $\smallo^0=\{\text{pt}\}$ is a singleton, and the map which sends $\alpha\colon\smallo^0\to\mathcal{O}$ to the element $\alpha(\text{pt})$ of $\mathcal{O}$ is an isomorphism from the ring of functions $\smallo^0\to\mathcal{O}$ to the ring $\mathcal{O}$. We identify this ring with $\mathcal{O}$ via the isomorphism $\alpha\mapsto\alpha(\text{pt})$. Then ϕ_0 is a ring embedding $\boldsymbol{k}\to\mathcal{O}$. Hence the valued field K is necessarily of equicharacteristic $\operatorname{char}\boldsymbol{k}$. Moreover, if $f\in\boldsymbol{k}[X]\subseteq W_m$, then $\phi_m(f)\colon\smallo^m\to\mathcal{O}$ is given by $a\mapsto f(a)$.

Lemma 2.14. *For an infinitesimal W-structure (ϕ_m) on K and $f\in\boldsymbol{k}\lfloor X\rfloor$:*

$$\phi_m(f)=\phi_0(f(0))+\phi_m(g)\qquad\textit{where } g\in(X);$$

in particular $\phi_m(f)(\smallo^m)\subseteq\phi_0(f(0))+\smallo$ and $\phi_m(f)(0)=\phi_0(f(0))$.

This follows immediately from (A1), (A2), and the fact that $f-f(0)\in(X)$.

Corollary 2.15. *Suppose $\mathcal{O}=K$, and let $\iota\colon\boldsymbol{k}\to K$ be an embedding. Then there is a unique infinitesimal W-structure (ϕ_m) on K such that $\iota=\phi_0$.*

Proof. We have $\smallo=\{0\}$, therefore the family (ϕ_m), where $\phi_m(f)$ is the function $\{0\}^m\to K$ with value $\iota(f(0))\in K$, for $f\in W_m$, is an infinitesimal W-structure on K with $\iota=\phi_0$. By the previous lemma this is also the only infinitesimal W-structure (ϕ_m) on K with $\iota=\phi_0$. □

Let K_0 be a valued subfield of K, with valuation ring $\mathcal{O}_0$ and maximal ideal $\smallo_0$; so $\mathcal{O}_0=\mathcal{O}\cap K_0$ and $\smallo_0=\smallo\cap K_0$. We say that the infinitesimal W-structure (ϕ_m) on K *restricts* to an infinitesimal W-structure on K_0 if $\phi_m(f)(\smallo_0^m)\subseteq\mathcal{O}_0$ for each m and $f\in W_m$. In this case, the family (ψ_m), where for each m and $f\in W_m$ we let $\psi_m(f)$ be the restriction of $\phi_m(f)\colon\smallo^m\to\mathcal{O}$ to a map $\smallo_0^m\to\mathcal{O}_0$, is an infinitesimal W-structure on K_0. We call (ψ_m) the *restriction* of the W-structure on K to K_0.

Examples. Here are a few examples of infinitesimal W-structures:

(1) Let Γ be an ordered abelian group, written additively, and let t^Γ be a multiplicative copy of Γ, with isomorphism $\gamma \mapsto t^\gamma \colon \Gamma \to t^\Gamma$. Let $\boldsymbol{k}(\!(t^\Gamma)\!)$ be the field of Hahn series with coefficients in $\boldsymbol{k}$ and monomials in t^Γ. Its elements are the formal series

$$f = \sum_{\gamma\in\Gamma} f_\gamma t^\gamma \qquad (f_\gamma \in \boldsymbol{k})$$

whose support $\operatorname{supp} f := \{\gamma \in \Gamma : f_\gamma \neq 0\}$ is a well-ordered subset of Γ, added and multiplied in the natural way. The field $\boldsymbol{k}(\!(t^\Gamma)\!)$ carries a valuation $v\colon \boldsymbol{k}(\!(t^\Gamma)\!)^\times \to \Gamma$ given by

$$f \mapsto v(f) := \min \operatorname{supp} f,$$

which we call the t-adic valuation on $\boldsymbol{k}(\!(t^\Gamma)\!)$. Its valuation ring is

$$\mathcal{O} = \big\{ f \in \boldsymbol{k}(\!(t^\Gamma)\!) : \operatorname{supp} f \geqslant 0 \big\}.$$

The kernel of the surjective ring morphism $f \mapsto f_0 \colon \mathcal{O} \to \boldsymbol{k}$ is the maximal ideal

$$\smallo = \big\{ f \in \boldsymbol{k}(\!(t^\Gamma)\!) : \operatorname{supp} f > 0 \big\}$$

of $\mathcal{O}$, so this morphism induces an isomorphism from the residue field $\mathcal{O}/\smallo$ of $\mathcal{O}$ onto the coefficient field $\boldsymbol{k}$. For $f \in \boldsymbol{k}[[X]]$ and $a \in \smallo^m$, the series $f(a)$ makes sense in $\boldsymbol{k}(\!(t^\Gamma)\!)$. For $f \in W_m$ let $\phi_m(f)$ be the function $a \mapsto f(a) \colon \smallo^m \to \mathcal{O}$. Then the family (ϕ_m) is an infinitesimal W-structure on $\boldsymbol{k}(\!(t^\Gamma)\!)$ where $\phi_0 \colon \boldsymbol{k} \to \mathcal{O}$ is the natural embedding.

(2) Equip the field

$$\boldsymbol{k}(\!(t^*)\!) := \bigcup_{d\geqslant 1} \boldsymbol{k}(\!(t^{1/d})\!)$$

of Puiseux series over $\boldsymbol{k}$ with the t-adic valuation ring

$$\boldsymbol{k}[[t^*]] := \bigcup_{d\geqslant 1} \boldsymbol{k}[[t^{1/d}]],$$

with maximal ideal

$$\bigcup_{d\geqslant 1} t^{1/d}\boldsymbol{k}[[t^{1/d}]].$$

This is a valued subfield of the Hahn field $\boldsymbol{k}(\!(t^{\mathbb{Q}})\!)$. The infinitesimal W-structure on $\boldsymbol{k}(\!(t^{\mathbb{Q}})\!)$ described in (1) restricts to one on $\boldsymbol{k}(\!(t^*)\!)$.

(3) Suppose Γ is archimedean. Then the completion of the $\boldsymbol{k}$-subalgebra $\boldsymbol{k}[t^\Gamma]$ of $\boldsymbol{k}(\!(t^\Gamma)\!)$ under the t-adic valuation is the subfield

$$\operatorname{cl}(\boldsymbol{k}[t^\Gamma]) := \left\{ f \in \boldsymbol{k}(\!(t^\Gamma)\!) : \begin{array}{l} \operatorname{supp} f \text{ is finite or } \operatorname{supp} f = \{\gamma_0, \gamma_1, \dots\} \\ \text{with } \gamma_n \to \infty \text{ as } n \to \infty \end{array} \right\}$$

of $\boldsymbol{k}(\!(t^\Gamma)\!)$. (See [3, Example 3.2.19].) We have $\boldsymbol{k}(\!(t^*)\!) \subseteq \operatorname{cl}(\boldsymbol{k}[t^{\mathbb{Q}}])$. The infinitesimal W-structure on $\boldsymbol{k}(\!(t^{\mathbb{Q}})\!)$ from (1) restricts to one on $\operatorname{cl}(\boldsymbol{k}[t^\Gamma])$.

(4) Suppose $\boldsymbol{k}$ comes equipped with a complete absolute value, and let $K := \boldsymbol{k}\{\{t^*\}\}$ be the subfield of $\boldsymbol{k}(\!(t^*)\!)$ consisting of the convergent Puiseux series over $\boldsymbol{k}$, equipped with the valuation ring $\mathcal{O}_t := \boldsymbol{k}[[t^*]] \cap K$, with maximal ideal $\smallo_t$. Suppose $W = \big(\boldsymbol{k}\{X_1, \dots, X_m\}\big)$ is the Weierstrass system of convergent power series rings. Then for $f \in \boldsymbol{k}\{X_1, \dots, X_m\}$ and $a \in \smallo_t^m$ we have $f(a) \in K$, so the infinitesimal W-structure on $\boldsymbol{k}(\!(t^*)\!)$ from (2) above restricts to an infinitesimal W-structure on K.

In the rest of this subsection we let (ϕ_m) *be an infinitesimal* W*-structure on* K. (The existence of such a (ϕ_m) is a strong assumption on K: see Lemma 2.20 below.) We always identify $\boldsymbol{k}$ with a subfield of $\mathcal{O}$ via the embedding $\phi_0 \colon \boldsymbol{k} \to \mathcal{O}$. Note that then each ϕ_m is a $\boldsymbol{k}$-algebra morphism from $W_m = \boldsymbol{k}\lfloor X \rfloor$ to the $\boldsymbol{k}$-algebra of functions $\smallo^m \to \mathcal{O}$. Thus by Lemma 2.14, for $f \in W_m$ we have $\phi_m(f)(0) = f(0)$. If $Y = (Y_1, \dots, Y_m)$ is an arbitrary tuple of distinct indeterminates, then for $f = f(Y) \in \boldsymbol{k}\lfloor Y \rfloor$ we let $\phi_m(f) := \phi_m(f(X))$. In the next lemma and its corollary $Y = (Y_1, \dots, Y_n)$ is a tuple of distinct indeterminates disjoint from $X = (X_1, \dots, X_m)$.

Lemma 2.16 (Substitution)**.** *Let* $f \in \boldsymbol{k}\lfloor X, Y \rfloor$ *and* $g = (g_1, \dots, g_n) \in \boldsymbol{k}\lfloor X \rfloor^n$ *with* $g(0) = 0$. *Then* $f(X, g(X)) \in \boldsymbol{k}\lfloor X \rfloor$ *and*

$$\phi_m\big(f(X, g(X))\big)(a) = \phi_{m+n}(f)\big(a, \phi_m(g)(a)\big) \qquad \text{for all } a \in \smallo^m.$$

Proof. Lemma 2.3 shows $f(X, g(X)) \in \boldsymbol{k}\lfloor X \rfloor$. As in the proof of that lemma take $u_1, \dots, u_n \in \boldsymbol{k}\lfloor X, Y \rfloor$ and $R \in \boldsymbol{k}\lfloor X \rfloor$ such that

$$f(X, Y) = u_n(X, Y)(Y_n - g_n(X)) + \cdots + u_1(X, Y)(Y_1 - g_1(X)) + R(X).$$

Then $f(X, g(X)) = R(X)$ and so

$$\phi_m\big(f(X, g(X))\big) = \phi_m(R) = \phi_{m+n}(R)$$

by (A2). Let $a \in \smallo^m$ and set $b := \phi_m(g)(a)$; by (A2) we also have $b = \phi_{m+n}(g)(a, b)$ and so using (A1),

$$\phi_{m+n}(f)\big(a, \phi_m(g)(a)\big) = \phi_{m+n}(R)(a, b) = \phi_m\big(f(X, g(X))\big)(a). \qquad \square$$

Corollary 2.17. *Let* $f \in \boldsymbol{k}\lfloor Y \rfloor$ *and* $g = (g_1, \dots, g_n) \in \boldsymbol{k}\lfloor X \rfloor^n$ *with* $g(0) = 0$. *Then*

$$\phi_m\big(f(g(X))\big) = \phi_n(f) \circ \phi_m(g).$$

Proof. Let f', σ, h be as in the proof of Corollary 2.4. Then for $a \in \smallo^m$ we have

$$\begin{aligned} \phi_m\big(f(g(X))\big)(a) &= \phi_m\big(h(X, g(X))\big)(a) \\ &= \phi_{m+n}(h)\big(a, \phi_m(g)(a)\big) \\ &= \phi_{m+n}(f')\big(\phi_m(g)(a), b\big) \quad \text{for some } b \in \smallo^m \\ &= \phi_n(f)\big(\phi_m(g)(a)\big), \end{aligned}$$

where we used Lemma 2.16 for the second, (A3) for the third, and (A2) for the fourth equality. $\square$

Let now $d \in \mathbb{N}$, $d \geqslant 1$. By Corollary 2.4, the $\boldsymbol{k}$-algebra automorphism τ_d of $\boldsymbol{k}[[X]]$ restricts to a $\boldsymbol{k}$-algebra automorphism of $\boldsymbol{k}\lfloor X \rfloor$. Now also consider the automorphism of the $\boldsymbol{k}$-linear space $\smallo^m$, also denoted by τ_d, given by

$$(a_1, \dots, a_m) \mapsto \big(a_1 + a_m^{d^{m-1}}, \dots, a_{m-1} + a_m^d, a_m\big).$$

By (A1) and the previous corollary, we obtain:

Corollary 2.18. *For each* $f \in \boldsymbol{k}\lfloor X \rfloor$ *and* $d \in \mathbb{N}$, $d \geqslant 1$*:* $\phi_m(\tau_d(f)) = \phi_m(f) \circ \tau_d$.

To illustrate Corollary 2.18 we prove that if $\mathcal{O} \neq K$, then each ring morphism ϕ_m is an embedding; more precisely:

Lemma 2.19. *Suppose the valuation of* K *is non-trivial. Then for each non-zero* $f \in \boldsymbol{k}\lfloor X \rfloor$ *and non-empty open* $U \subseteq \smallo^m$ *there is some* $a \in U$ *with* $\phi_m(f)(a) \neq 0$.

Proof. The case $m = 0$ was already observed, so suppose $m \geqslant 1$. Take $\tau = \tau_d$ (where $d \in \mathbb{N}$, $d \geqslant 1$) such that $\tau(f)$ is regular in X_m. Replacing f, U by $\tau(f)$, $\tau^{-1}(U)$ and using Corollary 2.18 we arrange that f is regular in X_m. Lemma 2.11 yields $u \in \boldsymbol{k}\lfloor X\rfloor^\times$ and a monic $w \in \boldsymbol{k}\lfloor X'\rfloor[X_m]$, where $X' = (X_1, \dots, X_{m-1})$, such that $f = uw$. Take $a' \in \smallo^{m-1}$ with $U \cap (\{a'\} \times \smallo) \neq \emptyset$. Since $\smallo$ is infinite, we get an $a_m \in \smallo$ such that $a := (a', a_m) \in U$ and $\phi_m(w)(a) \neq 0$, and then also $\phi_m(f)(a) \neq 0$. □

From now on we often drop ϕ_m from the notation: for $a \in \smallo^m$, $f \in \boldsymbol{k}\lfloor X\rfloor$ we write $f(a)$ instead of $\phi_m(f)(a)$. By (A1) we have $g(\smallo^m) \subseteq \smallo$ for $g \in (X)$ and hence $f(\smallo^m) \subseteq f(0) + \smallo \subseteq \mathcal{O}$ for $f \in \boldsymbol{k}\lfloor X\rfloor$, by Lemma 2.14. Hence given $a \in \smallo^m$, the map $f \mapsto f(a)\colon \boldsymbol{k}\lfloor X\rfloor \to \mathcal{O}$ is a local ring morphism. The presence of an infinitesimal W-structure on a valued field imposes a significant constraint:

Lemma 2.20. *The valued field K is henselian.*

Proof. Let $a_1, \dots, a_m \in \smallo$ and $P(Y) := 1 + Y + a_1Y^2 + \cdots + a_mY^{m+1}$ where Y is a single new indeterminate. It suffices to show that P has a zero in $\mathcal{O}$. Put

$$Q(X, Y) := 1 + Y + X_1Y^2 + \cdots + X_mY^{m+1} \in \boldsymbol{k}\lfloor X\rfloor[Y].$$

Since $\boldsymbol{k}\lfloor X\rfloor$ is henselian (Lemma 2.8), there is some $f \in \boldsymbol{k}\lfloor X\rfloor$ with $Q(X, f(X)) = 0$. Then $P(b) = Q(a, b) = 0$ for $a := (a_1, \dots, a_m)$ and $b := f(a) \in \mathcal{O}$. □

This way we reprove the well-known fact that the valued field $\boldsymbol{k}(\!(t^\Gamma)\!)$ and its valued subfield $\operatorname{cl}(\boldsymbol{k}[t^\Gamma])$ (when Γ is archimedean) are henselian. Similarly, so are the valued fields $\boldsymbol{k}(\!(t^*)\!)$ and $\boldsymbol{k}\{\{t^*\}\}$ (when $\boldsymbol{k}$ is equipped with a complete absolute value).

Lemma 2.21. *Let L be a valued field extension of K equipped with an infinitesimal W-structure which restricts to that of K, and let K_0 be a valued subfield of L containing K which is algebraic over K. Then the infinitesimal W-structure of L restricts to an infinitesimal W-structure on K_0.*

Proof. By induction on n we show: if $f \in \boldsymbol{k}\lfloor X, Y\rfloor$ where $Y = (Y_1, \dots, Y_n)$ is a tuple of distinct indeterminates disjoint from X and $b \in \smallo^m$, $c \in \smallo^n_{K_0}$, then $f(b, c) \preceq 1$. For $n = 0$ this is clear, so suppose $n \geqslant 1$. Let

$$P = Z^d + a_1Z^{d-1} + \cdots + a_d \in K[Z] \qquad (a_1, \dots, a_d \in K)$$

be the minimum polynomial of c_n over K. Then $a := (a_1, \dots, a_d) \in \smallo^d$ since K is henselian and $c_n \prec 1$. (See, e.g., [3, 1.3.12, 3.3.11, 3.3.15].) We have $g(a, c_n) = 0$ where

$$g(U, Y_n) := Y_n^d + U_1Y_n^{d-1} + \cdots + U_d \in \mathbb{Z}[U, Y_n] \subseteq \boldsymbol{k}\lfloor U, Y\rfloor \quad (U = (U_1, \dots, U_d)).$$

Let $Y' = (Y_1, \dots, Y_{n-1})$. Weierstrass Division in $\boldsymbol{k}\lfloor U, X, Y\rfloor$ yields $q \in \boldsymbol{k}\lfloor U, X, Y\rfloor$ and $r \in \boldsymbol{k}\lfloor U, X, Y'\rfloor[Y_n]$ of degree $< d$ with $f = qg + r$. Then $f(b, c) = r(a, b, c) \preceq 1$ by the inductive hypothesis applied to the coefficients of r and (a, b), c' in place of b, c, respectively. □

Let $\boldsymbol{k}^{\mathrm{a}}$ be an algebraic closure of $\boldsymbol{k}$; then $\boldsymbol{k}^{\mathrm{a}}(\!(t^{\mathbb{Q}})\!)$ is algebraically closed. By the previous lemma, the infinitesimal W-structure of $\boldsymbol{k}^{\mathrm{a}}(\!(t^{\mathbb{Q}})\!)$ restricts to an infinitesimal W-structure on the algebraic closure of the field $\boldsymbol{k}(\!(t)\!)$ of Laurent series over $\boldsymbol{k}$ inside $\boldsymbol{k}^{\mathrm{a}}(\!(t^{\mathbb{Q}})\!)$.

2.3. **Infinitesimal W-structures as model-theoretic structures.** Let $\mathcal{L}$ be an expansion of the language $\mathcal{L}_{\preceq} = \{0, 1, -, +, \cdot, \preceq\}$ of rings augmented by a binary relation symbol $\preceq$. (See Section 1.) We then let $\mathcal{L}_W$ be the expansion of $\mathcal{L}$ by a new m-ary function symbol, for each m and $f \in W_m$, also denoted by f. Given an $\mathcal{L}$-theory T containing the $\mathcal{L}_{\preceq}$-theory of valued fields we let T_W be the $\mathcal{L}_W$-theory whose models are the $\mathcal{L}_W$-structures $\boldsymbol{K} = (K; \dots)$ whose $\mathcal{L}$-reduct is a model of T, each $f \in W_m$ is interpreted by a function $f^{\boldsymbol{K}}\colon K^m \to K$ which is identically zero on the complement of $\mathcal{O}^m$ and satisfies $f^{\boldsymbol{K}}(\mathcal{O}^m) \subseteq \mathcal{O}$, and such that the family (ϕ_m) of maps given by $\phi_m(f) = f^{\boldsymbol{K}}|\mathcal{O}^m$ is an infinitesimal W-structure on K. (Note: the underlying valued field of each model of T_W is henselian of equicharacteristic char $\boldsymbol{k}$.)

Example. Let $q \in \mathbb{Q}^{>}$. We then have an automorphism $a(t) \mapsto a(t^q)$ of the valued field $K = \boldsymbol{k}(\!(t^{\mathbb{Q}})\!)$ over $\boldsymbol{k}$ (with inverse $b(t) \mapsto b(t^{1/q})$). For $\mathcal{L} = \mathcal{L}_{\preceq}$, this is also an automorphism of the $\mathcal{L}_W$-structure $\boldsymbol{K} = (K; \dots)$ with $\mathcal{L}$-reduct K described above. This automorphism restricts to an automorphism of the substructure $\big(\boldsymbol{k}(\!(t^*)\!); \dots\big)$ of $\boldsymbol{K}$. Given $a \in \boldsymbol{k}(\!(t^*)\!)$ there is some $d \geqslant 1$ such that $a(t^d) \in \boldsymbol{k}(\!(t)\!)$, and then

$$a \preceq 1 \iff a(t^d) \in \boldsymbol{k}[[t]], \qquad a \prec 1 \iff a(t^d) \in t\boldsymbol{k}[[t]].$$

Suppose $\boldsymbol{k}$ comes equipped with a complete absolute value and W is the Weierstrass system of convergent power series over $\boldsymbol{k}$. Then the automorphism $a(t) \mapsto a(t^q)$ of the $\mathcal{L}_W$-structure $\big(\boldsymbol{k}(\!(t^*)\!); \dots\big)$ further restricts to an automorphism of its substructure $\big(\boldsymbol{k}\{\{t^*\}\}; \dots\big)$.

2.4. **Zero sets and vanishing ideals.** Let (ϕ_m) be an infinitesimal W-structure on a valued field K, and let I be an ideal of $W_m = \boldsymbol{k}\lfloor X \rfloor$. We let

$$\mathrm{Z}_K(I) := \big\{a \in \mathcal{O}^m : f(a) = 0 \text{ for all } f \in I\big\}$$

be the *zero set* of I in K. One verifies easily that if J is another ideal of $\boldsymbol{k}\lfloor X \rfloor$, then $\mathrm{Z}_K(I) \subseteq \mathrm{Z}_K(J)$ if $I \supseteq J$, and

$$\mathrm{Z}_K(IJ) = \mathrm{Z}_K(I \cap J) = \mathrm{Z}_K(I) \cup \mathrm{Z}_K(J), \qquad \mathrm{Z}_K(I + J) = \mathrm{Z}_K(I) \cap \mathrm{Z}_K(J).$$

Let also S be a subset of $\mathcal{O}^m$. We let

$$\mathrm{I}(S) := \big\{f \in \boldsymbol{k}\lfloor X \rfloor : f(a) = 0 \text{ for all } a \in S\big\}.$$

Then $\mathrm{I}(S)$ is an ideal of $\boldsymbol{k}\lfloor X \rfloor$, called the *vanishing ideal* of S. If also $T \subseteq \mathcal{O}^n$, then $\mathrm{I}(S) \subseteq \mathrm{I}(T)$ if $S \supseteq T$, and $\mathrm{I}(S \cup T) = \mathrm{I}(S) \cap \mathrm{I}(T)$. Clearly the ideal $\mathrm{I}(S)$ is radical, so $\mathrm{I}\big(\mathrm{Z}_K(I)\big) \supseteq \sqrt{I}$. Also note $\mathrm{Z}_K(I) = \mathrm{Z}_K(\sqrt{I})$.

2.5. **Germs of analytic functions.** Suppose $\boldsymbol{k}$ is equipped with a complete absolute value. Recall that analytic functions $f\colon U \to \boldsymbol{k}$ and $g\colon V \to \boldsymbol{k}$, where $U, V \subseteq \boldsymbol{k}^m$ are open neighborhoods of 0, are said to have the same *germ* at 0 if there is an open neighborhood W of 0 contained in $U \cap V$ such that $f(a) = g(a)$ for all $a \in W$. The relation of having the same germ at 0 is an equivalence relation on the collection of all analytic functions $f\colon U \to \boldsymbol{k}$ where $U \subseteq \boldsymbol{k}^m$ is an open neighborhood of 0; we denote the equivalence class of f by $[f]$. The equivalence classes of this equivalence relation form a commutative ring such that $[f] + [g] = [f + g]$ and $[f] \cdot [g] = [f \cdot g]$ for all analytic functions $f, g\colon U \to \boldsymbol{k}$ defined on an open neighborhood $U \subseteq \boldsymbol{k}^m$ of 0. The map sending the germ of f to its Taylor series at 0 is a ring isomorphism from this ring onto $\boldsymbol{k}\{X\} = \boldsymbol{k}\{X_1, \dots, X_m\}$, via which we identify these two rings.

3. A Proof of Rückert's Nullstellensatz

In this section $\mathcal{L} = \mathcal{L}_{\preceq}$, and we let ACVF be the $\mathcal{L}$-theory whose models are the algebraically closed non-trivially valued fields. We recall a fundamental theorem of the model theory of algebraically closed valued fields. (See, for example, [3, Theorem 3.6.1] or [47, Theorem 4.4.2] for a proof.)

Theorem 3.1 (A. Robinson [55])**.** ACVF *has* QE.

In particular, the theory ACVF is substructure complete, that is, if $K, L \models$ ACVF and A is a substructure of both K and L, then $K_A \equiv L_A$. (Here K_A is the natural expansion of K to an $\mathcal{L}_A$-structure where $\mathcal{L}_A$ extends the language $\mathcal{L}$ by new constant symbols for the elements of A, and likewise with L_A in place of K_A: see Section 1.1.) Moreover, ACVF is the model completion of the $\mathcal{L}$-theory of pairs $(R, \preceq)$ where R is an integral domain and $\preceq$ is a dominance relation on R [3, Corollary 3.6.4].

In the following we let W be a Weierstrass system over a field $\boldsymbol{k}$. We also let $X = (X_1, \dots, X_m)$ be a tuple of distinct indeterminates and $y = (y_1, \dots, y_n)$ be a tuple of distinct $\mathcal{L}$-variables. Let $K \models \mathrm{ACVF}_W$ and $\mathcal{O} = \mathcal{O}_K$, $\smallo = \smallo_K$. Recall that for $a \in \smallo^m$, the map $f \mapsto f(a)$ is a local ring morphism $\boldsymbol{k}\lfloor X \rfloor \to \mathcal{O}$, and that we view $\boldsymbol{k}$ as a subfield of $\mathcal{O}$. We now use Theorem 3.1 to prove the following specialization property:

Proposition 3.2. *Let $\varphi(y)$ be an $\mathcal{L}$-formula, $f = (f_1, \dots, f_n) \in \boldsymbol{k}\lfloor X \rfloor^n$, $\Omega \models$ ACVF, and $\sigma\colon \boldsymbol{k}\lfloor X \rfloor \to \mathcal{O}_\Omega$ be a local ring morphism such that $\Omega \models \varphi(\sigma(f))$. Then $K \models \varphi(f(a))$ for some $a \in \smallo^m$.*

Proof. We proceed by induction on the length m of X. Note that if we equip $\boldsymbol{k}$ with the trivial dominance relation, then the restriction of σ to an embedding $\boldsymbol{k} \to \Omega$ as well as the natural inclusion $\boldsymbol{k} \to K$ are $\mathcal{L}$-embeddings. Hence the case $m = 0$ follows from substructure completeness of ACVF. Suppose $m \geqslant 1$. By Theorem 3.1 we arrange that φ is quantifier-free, and we may then assume that φ has the form

$$\bigwedge_{i \in I} P_i(y) = 0 \wedge Q(y) \neq 0 \wedge \bigwedge_{j \in J} R_j(y) \mathrel{\square_j} S_j(y)$$

where I, J are finite index sets, $P_i, Q, R_j, S_j \in \mathbb{Z}[Y_1, \dots, Y_n]$, and each $\square_j$ is one of the symbols $\preceq$ or $\prec$. Now note that for each $P \in \mathbb{Z}[Y_1, \dots, Y_n]$ we have $P(f) \in \boldsymbol{k}\lfloor X \rfloor$ as well as $P(\sigma(f)) = \sigma(P(f))$ and $P(f(a)) = P(f)(a)$ for every $a \in \smallo^m$. Hence by suitably modifying φ, f (which may include increasing n) we can arrange that the polynomials P_i, Q, R_j, S_j are just distinct elements of $\{Y_1, \dots, Y_n\}$. For example, for $n = 4$, our formula φ may have the form

$$y_1 = 0 \ \wedge\ y_2 \neq 0 \ \wedge\ y_3 \mathrel{\square} y_4 \quad \text{where } \square \text{ is either } \preceq \text{ or } \prec.$$

(The general case is only notationally more involved.) We may also clearly arrange that the formal power series $f_1, \dots, f_n$ are all non-zero. Take $d \in \mathbb{N}$, $d \geqslant 1$, such that with $\tau := \tau_d$, each $\tau(f_j)$ is regular in X_m. For each $g \in \boldsymbol{k}\lfloor X \rfloor$ and $a \in \smallo^m$ we have $\tau(g)(a) = g(\tau(a))$. (Corollary 2.18.) Hence replacing each f_j by $\tau(f_j)$ and σ by $\sigma \circ \tau^{-1}$ we arrange that f_j is regular in X_m, for $j = 1, \dots, n$. Weierstrass Preparation in $\boldsymbol{k}\lfloor X \rfloor$ (Lemma 2.11) yields a 1-unit $u_j \in \boldsymbol{k}\lfloor X \rfloor$ and a polynomial $w_j \in \boldsymbol{k}\lfloor X' \rfloor[X_m]$, where $X' = (X_1, \dots, X_{m-1})$, such that $f_j = u_j w_j$, for $j = 1, \dots, n$.

We have $\sigma(u_j) \sim 1$ since σ is local. Hence we may replace each f_j by w_j to arrange that $f_j = w_j$ is a polynomial. Take $e \in \mathbb{N}$ and $w_{jk} \in \boldsymbol{k}\lfloor X' \rfloor$ ($j = 1, \dots, n$, $k = 0, \dots, e$) such that

$$w_j = w_{j0} + w_{j1} X_m + \cdots + w_{je} X_m^e,$$

and set $w := (w_{jk})$. Let $u := (u_{jk})$ be a tuple of distinct new variables and v be a new variable; then $\sigma(w_j) = t_j(\sigma(w), \sigma(X_m))$ for the $\mathcal{L}_{\mathrm{R}}$-term

$$t_j(u, v) := u_{j0} + u_{j1} v + \cdots + u_{je} v^e.$$

Consider the existential $\mathcal{L}$-formula

$$\psi(u) := \exists v \big(v \prec 1 \wedge \varphi\big(t_1(u,v), \dots, t_n(u,v)\big)\big).$$

Then

$$\begin{aligned} \Omega \models \varphi(\sigma(f)) \quad &\Longrightarrow \quad \Omega \models \psi(\sigma(w)) \\ &\Longrightarrow \quad K \models \psi(w(b)) \text{ for some } b \in \mathcal{O}^{m-1} \\ &\Longleftrightarrow \quad K \models \varphi(f(a)) \text{ for some } a \in \mathcal{O}^m, \end{aligned}$$

where for the second implication we used the inductive hypothesis applied to ψ, w, and the restriction of σ to $\boldsymbol{k}\lfloor X' \rfloor$ in place of φ, f, σ, respectively. □

The following corollary (not used later) captures the model-theoretic essence of Proposition 3.2:

Corollary 3.3. *Let θ be an existential $\mathcal{L}_W$-sentence. If $K \models \theta$, then $L \models \theta$ for each $L \models \mathrm{ACVF}_W$.*

Proof. Take a tuple $x = (x_1, \dots, x_m)$ of distinct new variables, for some m, and a boolean combination $\psi(x)$ of unnested atomic $\mathcal{L}_W$-formulas with $\models \theta \leftrightarrow \exists x \psi$; here $\exists x$ abbreviates $\exists x_1 \cdots \exists x_m$. (See [3, Lemmas B.4.5 and B.5.5].) Then $\psi(x) = \varphi(x, f(x))$ for some quantifier-free $\mathcal{L}$-formula $\varphi(x,y)$ and $f \in \boldsymbol{k}\lfloor X \rfloor^n$. Now

$$\mathrm{ACVF}_W \models \theta \leftrightarrow \exists x \big((1 \preceq x_1 \vee \cdots \vee 1 \preceq x_m) \wedge \varphi(x, 0) \big) \vee \exists x \big(x_1 \prec 1 \wedge \cdots \wedge x_m \prec 1 \wedge \psi \big),$$

hence the corollary follows from Theorem 3.1 and Proposition 3.2. □

Corollary 3.4. *Let $\varphi(y)$ be an $\mathcal{L}_{\mathrm{R}}$-formula, $f \in \boldsymbol{k}\lfloor X \rfloor^n$, and let $\sigma \colon \boldsymbol{k}\lfloor X \rfloor \to \Omega$ be a ring morphism to an algebraically closed field Ω such that $\Omega \models \varphi(\sigma(f))$. Then $K \models \varphi(f(a))$ for some $a \in \mathcal{O}^m$.*

Proof. Suppose first that $\ker \sigma = (X)$; then $\sigma(g) = \sigma(g(0))$ for every $g \in \boldsymbol{k}\lfloor X \rfloor$, and the corollary follows from substructure completeness of the $\mathcal{L}_{\mathrm{R}}$-theory of algebraically closed fields by taking $a := 0 \in \mathcal{O}^m$. Now suppose $\ker \sigma \neq (X)$. The image A of σ is a local subring of Ω (cf. Lemma 2.5) but not a field. Take a valuation ring of Ω lying over A and equip Ω with the associated dominance relation. Then $\Omega \models \mathrm{ACVF}$ and $\sigma \colon \boldsymbol{k}\lfloor X \rfloor \to \mathcal{O}_\Omega$ is a local ring morphism, so the previous proposition applies. □

Corollary 3.4 now implies a general version of Rückert's Nullstellensatz:

Theorem 3.5 (Rückert's Nullstellensatz)**.** *Let I be an ideal of $\boldsymbol{k}\lfloor X \rfloor$. Then*

$$\mathrm{I}\big(\mathrm{Z}_K(I)\big) = \sqrt{I}.$$

Proof. If we have some $a \in \mathrm{Z}_K(I)$, then the kernel of the ring morphism $f \mapsto f(a)\colon \boldsymbol{k}\lfloor X \rfloor \to K$ is a prime ideal of $\boldsymbol{k}\lfloor X \rfloor$ containing I. Hence we may assume that $I \neq \boldsymbol{k}\lfloor X \rfloor$. Recall: the ring $\boldsymbol{k}\lfloor X \rfloor$ is noetherian (Lemma 2.5). This yields prime ideals $P_1, \dots, P_k$ ($k \geqslant 1$) of $\boldsymbol{k}\lfloor X \rfloor$ such that $\sqrt{I} = P_1 \cap \cdots \cap P_k$. Then

$$\mathrm{I}\big(\mathrm{Z}_K(I)\big) = \mathrm{I}\big(\mathrm{Z}_K(\sqrt{I})\big) = \mathrm{I}\big(\mathrm{Z}_K(P_1)\big) \cap \cdots \cap \mathrm{I}\big(\mathrm{Z}_K(P_k)\big),$$

so it suffices to treat the case where I is prime. So from now on assume I is a prime ideal of $\boldsymbol{k}\lfloor X \rfloor$; we need to show that then $\mathrm{I}\big(\mathrm{Z}_K(I)\big) = I$. Let Ω be an algebraic closure of the fraction field of the integral domain $A := \boldsymbol{k}\lfloor X \rfloor / I$, and let $\sigma\colon \boldsymbol{k}\lfloor X \rfloor \to \Omega$ be the composition of the residue morphism $f \mapsto f+I\colon \boldsymbol{k}\lfloor X \rfloor \to A$ with the natural inclusion $A \subseteq \Omega$. Let $f \in \boldsymbol{k}\lfloor X \rfloor \setminus I$ and let $g_1, \dots, g_n$ generate I. Then $\Omega \models \varphi\big(\sigma(f), \sigma(g_1), \dots, \sigma(g_n)\big)$ where $\varphi(y_0, \dots, y_n)$ is the quantifier-free $\mathcal{L}_{\mathrm{R}}$-formula $y_0 \neq 0 \wedge y_1 = \cdots = y_n = 0$. Corollary 3.4 yields an $a \in \mathcal{O}^m$ with $f(a) \neq 0$ and $g_1(a) = \cdots = g_n(a) = 0$, so $f \notin \mathrm{I}\big(\mathrm{Z}_K(I)\big)$. Thus $\mathrm{I}\big(\mathrm{Z}_K(I)\big) \subseteq I$ as required. $\square$

Let now $\boldsymbol{k}^{\mathrm{a}}$ be an algebraic closure of $\boldsymbol{k}$ and $K = \boldsymbol{k}(\!(t)\!)^{\mathrm{a}}$ be the algebraic closure of $\boldsymbol{k}(\!(t)\!)$ inside $\boldsymbol{k}^{\mathrm{a}}(\!(t^{\mathbb{Q}})\!)$, equipped with the restriction of the dominance relation of $\boldsymbol{k}^{\mathrm{a}}(\!(t^{\mathbb{Q}})\!)$. Expand K to an $\mathcal{L}_W$-structure where W is the Weierstrass system of formal power series over $\boldsymbol{k}$. (See the remarks after Lemma 2.21.) Then $K \models \mathrm{ACVF}_W$, hence by Theorem 3.5 we obtain the “formal” version of Rückert’s Nullstellensatz:

Corollary 3.6. *Let $f, g_1, \dots, g_n \in \boldsymbol{k}[[X]]$ with $f(a) = 0$ for all $a \in \mathcal{O}^m$ such that $g_1(a) = \cdots = g_n(a) = 0$. Then there are $h_1, \dots, h_n \in \boldsymbol{k}[[X]]$ and some $k \geqslant 1$ such that $f^k = g_1h_1 + \cdots + g_nh_n$.*

In the rest of this subsection we assume $\operatorname{char} \boldsymbol{k} = 0$. Then $K = \boldsymbol{k}^{\mathrm{a}}(\!(t^*)\!)$ (see, e.g., [3, Example 3.3.23]). Hence using the automorphisms $a(t) \mapsto a(t^d)$ of the $\mathcal{L}_W$-structure K (where $d \geqslant 1$), from Corollary 3.6 we obtain:

Corollary 3.7. *Let $f, g_1, \dots, g_n \in \boldsymbol{k}[[X]]$ with $f(a) = 0$ for all $a \in t\boldsymbol{k}^{\mathrm{a}}[[t]]^m$ such that $g_1(a) = \cdots = g_n(a) = 0$. Then there are power series $h_1, \dots, h_n \in \boldsymbol{k}[[X]]$ and some $k \geqslant 1$ such that $f^k = g_1h_1 + \cdots + g_nh_n$.*

Proof. Let $a \in \mathcal{O}^m$ be such that $g_1(a) = \cdots = g_n(a) = 0$. Taking $d \geqslant 1$ such that $b := a(t^d)$ lies in $t\boldsymbol{k}^{\mathrm{a}}[[t]]^m$, we then also have $g_1(b) = \cdots = g_n(b) = 0$, so $f(b) = 0$ by the hypothesis of the corollary, thus $f(a) = 0$. Hence the corollary follows from Corollary 3.6. $\square$

For $m = 1$ the previous corollary holds without assuming $\operatorname{char} \boldsymbol{k} = 0$, since $\mathcal{O} \setminus \{0\}$ is an orbit of the group of continuous automorphisms of $\boldsymbol{k}^{\mathrm{a}}(\!(t^{\mathbb{Q}})\!)$ over $\boldsymbol{k}^{\mathrm{a}}$ [34, Theorem 3.4]. But we do not know whether this remains true for $m > 1$. (See [32, 33] for an explicit description of the subfield $\boldsymbol{k}(\!(t)\!)^{\mathrm{a}}$ of $\boldsymbol{k}^{\mathrm{a}}(\!(t^{\mathbb{Q}})\!)$.)

Remark. If in the context of Corollary 3.7 we have $f, g_1, \dots, g_n \in \boldsymbol{k}[[X]]^{\mathrm{a}}$, then we can take $h_1, \dots, h_n \in \boldsymbol{k}[[X]]^{\mathrm{a}}$. This follows either from Theorem 3.5 applied to the Weierstrass system of algebraic formal power series, or the previous corollary and Corollary 2.6. Similarly with $\boldsymbol{k}[[X]]^{\mathrm{a}}$ replaced by $\boldsymbol{k}[[X]]^{\mathrm{da}}$.

Now we also suppose that $\boldsymbol{k}$ is algebraically closed and comes equipped with a complete absolute value. (For example, $\boldsymbol{k} = \mathbb{C}$ or $\boldsymbol{k} = \mathbb{C}_p$ with their usual absolute values.) Then the field $\boldsymbol{k}\{\{t^*\}\}$ of convergent Puiseux series over $\boldsymbol{k}$ is algebraically closed. Arguing as in the proof of Corollary 3.7, with $\boldsymbol{k}\{\{t^*\}\}$ in place of $\boldsymbol{k}(\!(t^*)\!)$

and W = the Weierstrass system of convergent power series over $\boldsymbol{k}$, we obtain the classical version of Rückert's Nullstellensatz for convergent power series:

Corollary 3.8. *Let $f, g_1, \dots, g_n \in \boldsymbol{k}\{X\}$ and suppose that for all $a \in \boldsymbol{k}\{t\}^m$ with $a(0) = 0$ we have $f(a) = 0$ whenever $g_1(a) = \cdots = g_n(a) = 0$. Then there are $h_1, \dots, h_n \in \boldsymbol{k}\{X\}$ and some $k \geqslant 1$ such that $f^k = g_1 h_1 + \cdots + g_n h_n$.*

As usual this yields a version for germs of analytic functions.

Corollary 3.9. *Let $f, g_1, \dots, g_n \colon U \to \boldsymbol{k}$ be analytic functions, where U is an open neighborhood of 0 in $\boldsymbol{k}^m$, such that for all $a \in U$,*

$$g_1(a) = \cdots = g_n(a) = 0 \quad \Longrightarrow \quad f(a) = 0.$$

Then there are analytic functions $h_1, \dots, h_n \colon V \to \boldsymbol{k}$, for some open neighborhood $V \subseteq U$ of 0 in $\boldsymbol{k}^m$, and some $k \geqslant 1$ such that

$$f^k = g_1 h_1 + \cdots + g_n h_n \qquad \text{on } V.$$

Proof. Let $f, g_1, \dots, g_n \in \boldsymbol{k}\{X\}$ also denote the germs of the corresponding analytic functions $U \to \boldsymbol{k}$. Then for all $a \in \boldsymbol{k}\{t\}^m$ with $a(0) = 0$ we have $g_1(a) = \cdots = g_n(a) = 0 \Rightarrow f(a) = 0$. (By the hypothesis and the continuity of each representative of a at 0.) Now Corollary 3.8 yields the existence of $h_1, \dots, h_n$ and k as claimed. □

4. Risler's Nullstellensatz

Let $\mathcal{L} = \mathcal{L}_{\mathrm{OR},\preceq} = \{0, 1, -, +, \cdot, \leqslant, \preceq\}$ be the language $\mathcal{L}_{\mathrm{OR}} = \mathcal{L}_{\mathrm{R}} \cup \{\leqslant\}$ of ordered rings expanded by a new binary relation symbol $\preceq$. Let RCVF be the $\mathcal{L}$-theory whose models are the $\mathcal{L}$-structures $(K, \preceq)$ where K is a real closed ordered field and $\preceq$ is a non-trivial convex dominance relation on K. Here, a dominance relation $\preceq$ on an ordered integral domain R is said to be *convex* if $0 \leqslant r \leqslant s \Rightarrow r \preceq s$, for all $r, s \in R$. The analogue of Theorem 3.1 in this context is the following fact. (For a self-contained proof see [3, Theorem 3.6.6] or [47, Theorem 4.5.1].)

Theorem 4.1 (Cherlin-Dickmann [12])**.** RCVF *has* QE.

Indeed, RCVF is the model completion of the $\mathcal{L}$-theory of ordered integral domains equipped with a convex dominance relation [3, Corollary 3.6.7]. Let W be a Weierstrass system over a euclidean field $\boldsymbol{k}$ and $K \models \mathrm{RCVF}_W$. Also let $X = (X_1, \dots, X_m)$ be a tuple of distinct indeterminates and $y = (y_1, \dots, y_n)$ be a tuple of distinct $\mathcal{L}$-variables. Just like Theorem 3.1 gave rise to Proposition 3.2, Theorem 4.1 implies:

Proposition 4.2. *Let $\varphi(y)$ be an $\mathcal{L}$-formula, $f = (f_1, \dots, f_n) \in \boldsymbol{k}\lfloor X \rfloor^n$, $\Omega \models$ RCVF, and $\sigma \colon \boldsymbol{k}\lfloor X \rfloor \to \mathcal{O}_\Omega$ be a local ring morphism such that $\Omega \models \varphi(\sigma(f))$. Then $K \models \varphi(f(a))$ for some $a \in \smallo^m$.*

Proof. We proceed by induction on m as in the proof of Proposition 3.2. Equipping $\boldsymbol{k}$ with its unique ordering and with the trivial dominance relation, the restriction of σ to an embedding $\boldsymbol{k} \to \Omega$ as well as the natural inclusion $\boldsymbol{k} \to K$ are $\mathcal{L}$-embeddings. Together with substructure completeness of RCVF this takes care of the case $m = 0$. So suppose $m \geqslant 1$. Using Theorem 4.1 we arrange φ to have the form

$$P(y) = 0 \wedge \bigwedge_{i \in I} Q_i(y) > 0 \wedge \bigwedge_{j \in J} R_j(y) \,\square_j\, S_j(y)$$

where I, J are finite index sets, $P, Q_i, R_j, S_j \in \mathbb{Z}[Y_1,\dots,Y_n]$, and each $\square_j$ is $\preceq$ or $\prec$. As in the proof of Proposition 3.2 we also arrange that the P, Q_i, R_j, S_j are distinct elements of $\{Y_1,\dots,Y_n\}$ and $f_1,\dots,f_n$ are all regular in X_m. Take some 1-unit $u_j \in \boldsymbol{k}\lfloor X\rfloor$ and $w_j \in \boldsymbol{k}\lfloor X'\rfloor[X_m]$, where $X' = (X_1,\dots,X_{m-1})$, such that $f_j = u_j w_j$. Then $\sigma(u_j) \sim 1$ since σ is local, hence $\sigma(u_j) > 0$. Thus we may arrange that each $f_j = w_j$ is a polynomial and conclude the argument as in the proof of Proposition 3.2. □

From Proposition 4.2 we obtain the completeness of the existential part of RCVR_W as in the proof of Corollary 3.3:

Corollary 4.3. *For each existential $\mathcal{L}_W$-sentence θ, we either have* $\mathrm{RCVR}_W \models \theta$ *or* $\mathrm{RCVR}_W \models \neg\theta$*.*

Next, an analogue of Corollary 3.4; for this, we first note:

Lemma 4.4. *Let Ω be an ordered field and $\sigma\colon \boldsymbol{k}\lfloor X\rfloor \to \Omega$ be a ring morphism. Equip Ω with the dominance relation associated to the convex hull of $\sigma(\boldsymbol{k})$ in Ω. Then for $g \in \boldsymbol{k}\lfloor X\rfloor$ we have $\sigma\big(g - g(0)\big) \prec 1$.*

Proof. Let $g \in \boldsymbol{k}\lfloor X\rfloor$; replacing g by $g - g(0)$ we arrange $g(0) = 0$. Let $\varepsilon \in \boldsymbol{k}^>$ and consider $u = \varepsilon - g \in \boldsymbol{k}\lfloor X\rfloor$. Then $\sigma(u) > 0$ by Lemma 2.10 and thus $\sigma(g) < \sigma(\varepsilon)$. Similarly one shows $-\sigma(\varepsilon) < \sigma(g)$. Thus $\sigma(g) \prec 1$. □

Corollary 4.5. *Let $\varphi(y)$ be an $\mathcal{L}_{\mathrm{OR}}$-formula, $f \in \boldsymbol{k}\lfloor X\rfloor^n$, and $\sigma\colon \boldsymbol{k}\lfloor X\rfloor \to \Omega$ be a ring morphism to a real closed field Ω such that $\Omega \models \varphi(\sigma(f))$. Then $K \models \varphi(f(a))$ for some $a \in \smallo^m$.*

Proof. Let $\mathcal{O}_\Omega$ be the convex hull of $\sigma(\boldsymbol{k})$ in Ω. By Lemma 4.4, σ is a local ring morphism $\boldsymbol{k}\lfloor X\rfloor \to \mathcal{O}_\Omega$. If $\Omega = \mathcal{O}_\Omega$ then model completeness of the $\mathcal{L}_{\mathrm{OR}}$-theory of real closed ordered fields allows us to replace Ω by a real closed ordered field extension of Ω (such as $\Omega(\!(t^{\mathbb{Q}})\!)$) to arrange $\Omega \neq \mathcal{O}_\Omega$; thus Ω equipped with its dominance relation associated to $\mathcal{O}_\Omega$ is a model of RCVF. Now the corollary follows from Proposition 4.2. □

We now quickly deduce Risler's analytic version of Hilbert's 17th Problem:

Corollary 4.6. *Let $f \in \boldsymbol{k}\lfloor X\rfloor$. Then $f(a) \geqslant 0$ for all $a \in \smallo^m$ iff there are a nonzero $g \in \boldsymbol{k}\lfloor X\rfloor$ and $h_1,\dots,h_k \in \boldsymbol{k}\lfloor X\rfloor$ (for some k) such that $fg^2 = h_1^2 + \cdots + h_k^2$.*

Proof. Suppose there are no such g and h_j. This yields an ordering $\leqslant$ on $F := \mathrm{Frac}(\boldsymbol{k}\lfloor X\rfloor)$ such that $f < 0$. (See, e.g., [9, Corollary 1.1.11].) Let Ω be the real closure of the ordered field $(F, \leqslant)$ and $\sigma\colon \boldsymbol{k}\lfloor X\rfloor \to \Omega$ be the natural inclusion, and apply Corollary 4.5 to the $\mathcal{L}_{\mathrm{OR}}$-formula $y < 0$ (where y is a single variable). This shows the "only if" direction; for "if" use Lemma 2.19. □

Next we give a general version of Risler's real Nullstellensatz analogous to Theorem 3.5. For this, we need to recall some definitions and basic facts from real algebra. Let I be an ideal of a ring R. One says that I is *real* if for every sequence $a_1,\dots,a_k$ of elements of R:

$$a_1^2 + \cdots + a_k^2 \in I \quad \Rightarrow \quad a_1,\dots,a_k \in I.$$

We have (cf. [9, Lemmas 4.1.5, 4.1.6]):

(1) If I is real, then I is radical;

(2) if I is real and R is noetherian, then all minimal prime ideals of R containing I are real; and
(3) if I is a prime ideal and $F := \operatorname{Frac}(R/I)$, then I is real iff F is formally real (that is, there is an ordering on F making F an ordered field).

Next we define

$$\sqrt[r]{I} := \{a \in R : a^{2k} + b_1^2 + \cdots + b_l^2 \in I \text{ for some } k \geqslant 1 \text{ and } b_1, \dots, b_l \in R\}.$$

Then $\sqrt[r]{I}$ is the smallest real ideal of R containing I, called the *real radical* of I. For $R = \boldsymbol{k}\lfloor X \rfloor$, we clearly have $\mathrm{I}(\mathrm{Z}_K(I)) = \mathrm{I}(\mathrm{Z}_K(\sqrt[r]{I}))$.

Theorem 4.7 (Risler's Nullstellensatz)**.** *Let I be an ideal of $\boldsymbol{k}\lfloor X \rfloor$. Then*

$$\mathrm{I}(\mathrm{Z}_K(I)) = \sqrt[r]{I}.$$

Proof. If we have some $a \in \mathrm{Z}_K(I)$, then some real prime ideal of $\boldsymbol{k}\lfloor X \rfloor$ contains I, namely the kernel of the ring morphism $f \mapsto f(a) \colon \boldsymbol{k}\lfloor X \rfloor \to K$. Hence we may assume that some real prime ideal of $\boldsymbol{k}\lfloor X \rfloor$ contains I and thus $\sqrt[r]{I}$. Then there are real prime ideals $P_1, \dots, P_k$ ($k \geqslant 1$) of $\boldsymbol{k}\lfloor X \rfloor$ such that $\sqrt[r]{I} = P_1 \cap \cdots \cap P_k$. We can arrange that I itself is a real prime ideal, and need to show that then $\mathrm{I}(\mathrm{Z}_K(I)) = I$. Equip the fraction field of the integral domain $R := \boldsymbol{k}\lfloor X \rfloor / I$ with some field ordering, let Ω be its real closure, and let $\sigma \colon \boldsymbol{k}\lfloor X \rfloor \to \Omega$ be the composition of $f \mapsto f + I \colon \boldsymbol{k}\lfloor X \rfloor \to R$ with the natural inclusions $R \subseteq \Omega$. Arguing as in the proof of Theorem 3.5, using Corollary 4.5 instead of Corollary 3.4, yields $\mathrm{I}(\mathrm{Z}_K(I)) \subseteq I$. □

If $\boldsymbol{k}$ is real closed, then so is $\boldsymbol{k}(\!(t^*)\!)$; thus the valued field $\boldsymbol{k}(\!(t^*)\!)$ is a model of RCVF. By the previous theorem we hence immediately obtain, in a similar way as Theorem 3.5 implied Corollary 3.7:

Corollary 4.8. *Suppose $\boldsymbol{k}$ is real closed. Let $f, g_1, \dots, g_n \in \boldsymbol{k}[[X]]$ with $f(a) = 0$ for all $a \in t\boldsymbol{k}[[t]]^m$ such that $g_1(a) = \cdots = g_n(a) = 0$. Then there are $k \geqslant 1$ and $b_1, \dots, b_l, h_1, \dots, h_n \in \boldsymbol{k}[[X]]$ such that*

$$f^{2k} + b_1^2 + \cdots + b_l^2 = g_1 h_1 + \cdots + g_n h_n.$$

Remark. If in the context of the previous corollary f and each g_j are in $\boldsymbol{k}_0[[X]]$, where $\boldsymbol{k}_0$ is a euclidean subfield of $\boldsymbol{k}$, then we can take the b_i, h_j in $\boldsymbol{k}_0[[X]]$. To see this apply Theorem 4.7 to the Weierstrass system $(\boldsymbol{k}_0[[X]])$ instead of the Weierstrass system $(\boldsymbol{k}[[X]])$. Similarly with $\boldsymbol{k}_0[[X]]^{\mathrm{a}}$ or $\boldsymbol{k}_0[[X]]^{\mathrm{da}}$ in place of $\boldsymbol{k}_0[[X]]$.

The field $\mathbb{R}\{\{t^*\}\}$ is also real closed; hence we obtain, similarly to Corollary 3.8:

Corollary 4.9. *Let $f, g_1, \dots, g_n \in \mathbb{R}\{X\}$, and suppose that for each $a \in \mathbb{R}\{t\}^m$ with $a(0) = 0$ we have $f(a) = 0$ whenever $g_1(a) = \cdots = g_n(a) = 0$. Then there are $k \geqslant 1$ and $b_1, \dots, b_l, h_1, \dots, h_n \in \mathbb{R}\{X\}$ such that*

$$f^{2k} + b_1^2 + \cdots + b_l^2 = g_1 h_1 + \cdots + g_n h_n.$$

Finally, the previous corollary yields a version for germs of real analytic functions:

Corollary 4.10. *Let $f, g_1, \dots, g_n \colon U \to \mathbb{R}$ be real analytic functions, where U is an open neighborhood of 0 in $\mathbb{R}^m$, such that for all $a \in U$,*

$$g_1(a) = \cdots = g_n(a) \quad \Longrightarrow \quad f(a) = 0.$$

Then there are real analytic functions $b_1, \dots, b_l, h_1, \dots, h_n \colon V \to \mathbb{R}$, for some open neighborhood $V \subseteq U$ of 0 in $\mathbb{R}^m$, and some $k \geqslant 1$ such that

$$f^{2k} + b_1^2 + \cdots + b_l^2 = g_1 h_1 + \cdots + g_n h_n \qquad \text{on } V.$$

Remark. In Corollary 4.10, if the germs of f and of the g_j at 0 are algebraic (over $\mathbb{R}[X]$), then we can choose the b_i, h_j such that their germs at 0 are also algebraic. Similarly with "differentially algebraic" in place of "algebraic". (Cf. the remark following Corollary 4.8.)

5. The Theory $p\,$CVF

Our aim here is to formulate and prove a theorem analogous to Theorem 4.1 in the p-adic context. We first recall the basic algebraic and model-theoretic facts about p-adically closed fields. *Throughout this section K is a field of characteristic zero.*

5.1. **p-valued fields.** Recall that a valuation on K with residue field $\mathbb{F}_p$ such that p is an element of smallest positive valuation is called a *p-valuation* on K. The valuation ring of a p-valuation on K is said to be a *p-valuation ring* of K, and a field of characteristic zero equipped with one of its p-valuation rings is a *p-valued field.* If K is p-valued, then so is each valued subfield of K. We also note:

Lemma 5.1. *Let K be a valued field and $\Delta \neq \{0\}$ be a convex subgroup of its value group. Then K is p-valued iff the Δ-specialization $\dot{K}$ of K is p-valued, and in this case the Δ-coarsening of K is not p-valued.*

Proof. The valued field $\dot{K}$ has value group Δ, and its residue field is isomorphic to $\operatorname{res}(K)$. □

5.2. **p-adically closed fields.** One says that a p-valued field is *p-adically closed* if it has no proper algebraic p-valued field extension. The fundamental result about p-adically closed fields is the following (see [49, Theorem 3.1]):

Theorem 5.2. *A p-valued field is p-adically closed iff it is henselian and its value group is a $\mathbb{Z}$-group.*

Using the Ax-Kochen/Eršov Theorem for unramified henselian valued fields of mixed characteristic (cf., e.g., [22, Theorem 7.1]) this implies:

Corollary 5.3. *Any two p-adically closed valued fields (viewed as $\mathcal{L}_{\preceq}$-structures as usual) are elementarily equivalent.*

We also recall a well-known fact:

Lemma 5.4. *Let $\mathcal{O}$ be a p-valuation ring of K, and set $\varepsilon := 3$ if $p = 2$ and $\varepsilon := 2$ otherwise. Then*

$$\mathcal{O} \ \supseteq \ \mathcal{O}_0 := \big\{a \in K : \text{there is some } b \in K \text{ with } 1 + pa^{\varepsilon} = b^{\varepsilon}\big\},$$

with $\mathcal{O} = \mathcal{O}_0$ if the valued field $(K, \mathcal{O})$ is henselian.

In particular, if $(K, \mathcal{O})$ is p-adically closed, then $\mathcal{O}$ is the unique p-valuation ring of K. Theorem 5.2 in combination with Lemmas 1.7, 5.1, and [3, Lemma 3.4.2] also yields a specialization result for p-adic closedness:

Lemma 5.5. *Let K, Δ be as in Lemma 5.1. Then K is p-adically closed iff the Δ-coarsening of K is henselian with divisible value group and the Δ-specialization $\dot{K}$ of K is p-adically closed.*

In the next lemma and its corollary we let $L \supseteq K$ be an extension of p-valued fields.

Lemma 5.6. *If L is henselian, then*

$$K \text{ is algebraically closed in } L \iff K \text{ is henselian and } \Gamma_L/\Gamma \text{ is torsion-free.}$$

For a proof of this lemma see [49, Lemma 4.2]. Lemma 5.6 in combination with Lemma 1.8 and Theorem 5.2 implies:

Corollary 5.7. *If L is p-adically closed, then the following are equivalent:*

1. *K is p-adically closed;*
2. *K is algebraically closed in L;*
3. *K is henselian and Γ_L/Γ is torsion-free.*

A field which carries at least one p-valuation is said to be *formally p-adic.* Every formally p-adic field has characteristic zero. If K is formally p-adic and satisfies one of the equivalent conditions in the next lemma, then K is called *p-adically closed.*

Lemma 5.8. *For a formally p-adic field K, the following statements are equivalent:*

1. *K has no proper algebraic formally p-adic field extension;*
2. *each p-valuation ring of K makes K a p-adically closed valued field;*
3. *some valuation ring of K makes K a p-adically closed valued field.*

Proof. The implications (1) ⇒ (2) ⇒ (3) are clear. Let $\mathcal{O}$ be a valuation ring of K making K a p-adically closed valued field. Let F be an algebraic field extension of K, and let $\mathcal{O}_F$ be a p-valuation ring of F. Then $\mathcal{O}_F \cap K$ is a p-valuation ring of K, so $\mathcal{O}_F \cap K = \mathcal{O}$ and thus $F = K$ since $(K, \mathcal{O})$ is p-adically closed. □

Below we will have occasion to discuss field equipped with two dependent valuations, one of which is a p-valuation. To facilitate keeping them apart we now generally denote p-valuation rings of K by $\mathcal{O}_p$, with maximal ideal $\smallo_p$, valuation $v_p\colon K^\times \to \Gamma_p$, and associated dominance relation $\preceq_p$. If we want to make the dependence on K explicit, we write $\mathcal{O}_{K,p}$ instead of $\mathcal{O}_p$, etc. (Below, K will often have a unique p-valuation ring, making these notations unambiguous in this case.)

Examples. Let $\boldsymbol{k}$ be a p-adically closed field. Let $v_{\boldsymbol{k}}\colon \boldsymbol{k}^\times \to \Gamma_{\boldsymbol{k}}$ be the p-valuation of $\boldsymbol{k}$, with valuation ring $\mathcal{O}_{\boldsymbol{k}}$ and maximal ideal $\smallo_{\boldsymbol{k}}$. Consider the Hahn field $K = \boldsymbol{k}(\!(t^\Gamma)\!)$ where $\Gamma \neq \{0\}$ is divisible. Then the t-adic valuation $v\colon K^\times \to \Gamma$ of K is not a p-valuation. However, the field K is p-adically closed: Let $\Gamma_p := \Gamma \times \Gamma_{\boldsymbol{k}}$ equipped with the lexicographic ordering, and for $f = \sum_{\gamma \in \Gamma} f_\gamma \gamma \in K^\times$ $(f_\gamma \in \boldsymbol{k})$ set

$$v_p(f) := \big(\delta, v_{\boldsymbol{k}}(f_\delta)\big) \text{ where } \delta = vf;$$

then $v_p\colon K^\times \to \Gamma_p$ is the p-valuation of K. (Cf. Lemma 5.5.) The valuation ring of v_p is $\mathcal{O}_p = \mathcal{O}_{\boldsymbol{k}} + \smallo$, with maximal ideal $\smallo_{\boldsymbol{k}} + \smallo$, where $\smallo$ is the maximal ideal of the valuation ring $\mathcal{O} = \boldsymbol{k} + \smallo$ of v. For $\Gamma = \mathbb{Q}$, the p-valuation on $\boldsymbol{k}(\!(t^{\mathbb{Q}})\!)$ restricts to a p-valuation on its subfield $\boldsymbol{k}(\!(t^*)\!)$, making $\boldsymbol{k}(\!(t^*)\!)$ a p-adically closed valued field. For $\boldsymbol{k} = \mathbb{Q}_p$, the p-valuation on $\mathbb{Q}_p(\!(t^*)\!)$ further restricts to a p-valuation on its subfield $\mathbb{Q}_p\{\{t^*\}\}$, with valuation ring $\mathbb{Z}_p + \smallo_t$ having maximal ideal $p\mathbb{Z}_p + \smallo_t$.

The subgroup $(K^\times)^n = \{a^n : a \in K^\times\}$ of the multiplicative group of a p-adically closed field K consisting of the nth powers of non-zero elements of K plays an important role in the study of K. For $K = \mathbb{Q}_p$ we recall a consequence of compactness of $\mathbb{Z}_p$ and density of $\mathbb{Z}$ in $\mathbb{Z}_p$:

Lemma 5.9. *Let $n \geqslant 1$; then $\big[\mathbb{Q}_p^\times : (\mathbb{Q}_p^\times)^n\big] < \infty$, and each coset of the subgroup $(\mathbb{Q}_p^\times)^n$ of $\mathbb{Q}_p^\times$ has a representative in $\mathbb{Z}$.*

We now let $\mathcal{L}_{\mathrm{Mac}}$ be the expansion of the language $\mathcal{L}_{\mathrm{R}}$ of rings by distinct unary predicate symbols P_n ($n \geqslant 1$), a binary relation symbol $\preceq_p$, and a unary function symbol $^{-1}$. In the following we construe a p-valued field K as an $\mathcal{L}_{\mathrm{Mac}}$-structure by interpreting P_n by the set $(K^\times)^n$, the binary relation symbol $\preceq_p$ by the valuation of K, and $^{-1}$ by the multiplicative inverse function $a \mapsto a^{-1}$ extended to a total function $K \to K$ via $0^{-1} := 0$. Note that the class of p-adically closed valued fields is $\mathcal{L}_{\mathrm{Mac}}$-axiomatizable thanks to Theorem 5.2. We let $p\,\mathrm{CF}$ be the $\mathcal{L}_{\mathrm{Mac}}$-theory of p-adically closed fields.

Theorem 5.10 (Macintyre)**.** *$p\,\mathrm{CF}$ admits* QE.

We refer to [42] or [49, Theorem 5.6] for proofs of this theorem. For later use we note that the symbols $\preceq_p$ and $^{-1}$ are not actually necessary to achieve QE. For this let $\mathcal{L}^*_{\mathrm{Mac}}$ be the reduct $\mathcal{L}_{\mathrm{R}} \cup \{\mathrm{P}_n : n \geqslant 1\}$ of $\mathcal{L}_{\mathrm{Mac}}$. The following lemma has already been noted, e.g., in [16, Theorem 2.2]. (Note that the proof relies on the specific structure of terms in $\mathcal{L}_{\mathrm{Mac}}$, and would break down, e.g., for the $(\mathcal{L}_{\mathrm{Mac}})_W$-theory $p\,\mathrm{CF}_W$, where W is the Weierstrass system of convergent p-adic power series, and the sublanguage of $(\mathcal{L}_{\mathrm{Mac}})_W$ obtained by removing the symbols $\preceq_p$ and $^{-1}$.)

Lemma 5.11. *Every quantifier-free $\mathcal{L}_{\mathrm{Mac}}$-formula is $p\,\mathrm{CF}$-equivalent to a quantifier-free $\mathcal{L}^*_{\mathrm{Mac}}$-formula.*

Proof. Take representatives $\lambda_1, \dots, \lambda_N \in \mathbb{Z}$ ($N \geqslant 1$) for the cosets of the subgroup $(\mathbb{Q}_p^\times)^n$ of $\mathbb{Q}_p^\times$. Let K be a p-adically closed valued field. Then $\lambda_1, \dots, \lambda_N$ are also representatives for the cosets of the subgroup $(K^\times)^n$ of $K^\times$, by completeness of $p\,\mathrm{CF}$ (Corollary 5.3), hence for $a, b \in K$, $b \neq 0$:

$$a/b \in (K^\times)^n \quad \Longleftrightarrow \quad a\lambda_i, b\lambda_i \in (K^\times)^n \text{ for some } i \in \{1, \dots, N\}.$$

Also, let ε be as in Lemma 5.4; then for $a, b \in K$ of we have

$$a \preceq_p b \quad \Longleftrightarrow \quad b = 0, \text{ or } b \neq 0 \text{ and } \big(1 + p(a/b)^\varepsilon\big) \in (K^\times)^\varepsilon.$$

This easily yields that $p\,\mathrm{CF}$ has closures of $\mathcal{L}^*_{\mathrm{Mac}}$-substructures in the sense of the remarks following [3, B.11.4], so the claim follows from loc. cit. $\square$

Call a field K *p-euclidean* if it is formally p-adic and $\big[K^\times : (K^\times)^n\big] = \big[\mathbb{Q}_p^\times : (\mathbb{Q}_p^\times)^n\big]$ for each $n \geqslant 1$.

Lemma 5.12. *Suppose K is p-euclidean. Then K has a unique expansion to an $\mathcal{L}_{\mathrm{Mac}}$-structure which is a substructure of a model of $p\,\mathrm{CF}$. (In particular, K has a unique p-valuation ring.)*

Proof. Since K is formally p-adic, it has a p-adically closed extension F, and this gives rise to an expansion of K to an $\mathcal{L}_{\mathrm{Mac}}$-substructure of F viewed as an $\mathcal{L}_{\mathrm{Mac}}$-structure. By Lemma 5.9 and $\big[K^\times : (K^\times)^n\big] = \big[\mathbb{Q}_p^\times : (\mathbb{Q}_p^\times)^n\big]$ we have $(F^\times)^n \cap K^\times = (K^\times)^n$ for each $n \geqslant 1$. Let $\mathcal{O}_p$ be the valuation ring of the $\mathcal{L}_{\mathrm{Mac}}$-structure K, and let ε and $\mathcal{O}_0$ be as in Lemma 5.4. Then $\mathcal{O}_0 \subseteq \mathcal{O}_p$ by that lemma, and we claim $\mathcal{O}_p = \mathcal{O}_0$. For this, let $a \in \mathcal{O}_p$; then $1 + pa^\varepsilon \in (F^\times)^\varepsilon \cap K^\times = (K^\times)^\varepsilon$, so we get $a \in \mathcal{O}_0$. $\square$

A field which satisfies the conclusion of the last lemma called *weakly p-euclidean.* We always construe a weakly p-euclidean field as a valued field via its unique p-valuation ring. Every p-adically closed field is p-euclidean; but $\mathbb{Q}$ is not. However:

Lemma 5.13. *The field $\mathbb{Q}$ is weakly p-euclidean.*

Proof. Clearly $\mathbb{Q}$ has only one p-valuation ring, namely

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} : a, b \in \mathbb{Z},\ b \notin p\mathbb{Z} \right\},$$

and thanks to Corollary 5.3 we also have $(\mathbb{Q}_p^\times)^n \cap \mathbb{Q}^\times = (K^\times)^n \cap \mathbb{Q}^\times$ for each $K \models p\,\mathrm{CF}$ and $n \geqslant 1$. □

Question. Are there p-euclidean algebraic number fields?

5.3. **p-convex valuations.** Let $(K, \mathcal{O}_p)$ be a p-valued field. A subring $\mathcal{O}$ of K is said to be *p-convex* if it is convex in $(K, \mathcal{O}_p)$, that is, if $\mathcal{O}_p \subseteq \mathcal{O}$. (See Section 1.4.) Every such p-convex subring of K is a valuation ring of K. If $\preceq$ is the dominance relation on K associated to a p-convex valuation ring of K, then

$$a \preceq_p b \implies a \preceq b, \qquad a \prec b \implies a \prec_p b \qquad \text{for all } a, b \in K.$$

If $K \subseteq L$ is an extension of p-valued fields and $\mathcal{O}_L$ is a p-convex subring of L, then $\mathcal{O}_L \cap K$ is a p-convex subring of K. In the next lemma and its corollary we let $(K, \mathcal{O})$ be an arbitrary valued field with value group Γ and residue field $\boldsymbol{k}$. Note that "$\subset$" means "proper subset".

Lemma 5.14.

K is a p-adically closed field and $\mathcal{O}_p \subset \mathcal{O}$ $\iff$

$(K, \mathcal{O})$ is henselian, Γ is divisible, and $\boldsymbol{k}$ is p-adically closed.

Proof. Suppose the field K is p-adically closed and $\mathcal{O}_p \subset \mathcal{O}$. Let Δ be the convex subgroup of Γ_p such that the Δ-coarsening of $(K, \mathcal{O}_p)$ is $(K, \mathcal{O})$. Then $\Delta \neq \{0\}$, and by Lemma 5.5, $(K, \mathcal{O})$ is henselian, its value group is divisible, and the Δ-specialization of $(K, \mathcal{O}_p)$ is p-adically closed; the underlying field of the latter is $\boldsymbol{k} = \mathcal{O}/\smallo$. Conversely, suppose $(K, \mathcal{O})$ is henselian with divisible value group, and let $\mathcal{O}_{\boldsymbol{k}}$ be a p-valuation ring of $\boldsymbol{k}$ making $\boldsymbol{k}$ a p-adically closed valued field. Take a valuation ring $\mathcal{O}_0$ of K contained in $\mathcal{O}$ and a convex subgroup Δ_0 of the value group of $\mathcal{O}_0$ such that the Δ_0-coarsening of $(K, \mathcal{O}_0)$ is $(K, \dot{\mathcal{O}}_0) = (K, \mathcal{O})$ and the Δ_0-specialization of $(K, \mathcal{O}_0)$ is $(\boldsymbol{k}, \mathcal{O}_{\boldsymbol{k}})$. Note that $\Delta_0 \neq \{0\}$, so $\mathcal{O}_0 \subset \mathcal{O}$. Also, $(K, \dot{\mathcal{O}}_0) = (K, \mathcal{O})$ is henselian, its value group $\Gamma_0/\Delta_0 \cong \Gamma$ is divisible, and the Δ_0-specialization of $(K, \mathcal{O}_0)$ is p-adically closed; hence $(K, \mathcal{O}_0)$ is p-adically closed by Lemma 5.5. □

Corollary 5.15.

K is p-adically closed and $\mathcal{O}$ is a non-trivial p-convex subring of K $\iff$

$(K, \mathcal{O})$ is henselian, $\Gamma \neq \{0\}$ is divisible, and $\boldsymbol{k}$ is p-adically closed.

Example. Let $\Gamma \neq \{0\}$ be a divisible ordered abelian group, written additively, and let $\boldsymbol{k}$ be a p-adically closed field. Then the valuation ring of the t-adic valuation on the Hahn field $K = \boldsymbol{k}(\!(t^\Gamma)\!)$ is a non-trivial p-convex subring of K. Similarly, the t-adic valuation ring $\boldsymbol{k}[[t^*]]$ of field $\boldsymbol{k}(\!(t^*)\!)$ of Puiseux series over $\boldsymbol{k}$ is a non-trivial p-convex subring of $\boldsymbol{k}(\!(t^*)\!)$.

If K is a p-valued field, we define the *p-convex hull* (in K) of a subring R of K to be the convex hull of R in the valued field K.

Lemma 5.16. *Let $(K, \mathcal{O}_p)$ be a p-valued field and let F be a subfield of K, with p-convex hull R in K. Then $R \neq \mathcal{O}_p$, hence if some p-convex subring $\mathcal{O} \neq K$ of K contains F, then R is a non-trivial p-convex subring of K.*

Proof. For the first statement use that $\mathcal{O}_p$ does not contain a subfield of K; the rest follows from this. □

We now let $\mathcal{L} = \mathcal{L}_{\mathrm{Mac},\preceq}$ be the expansion of the language $\mathcal{L}_{\mathrm{Mac}}$ of Macintyre by a single binary relation symbol $\preceq$ (not to be confused with the symbol $\preceq_p$ in $\mathcal{L}$, intended for the dominance relation associated to a p-valuation). Let $p\,\mathrm{CVF}$ be the $\mathcal{L}$-theory expanding $p\,\mathrm{CF}$ by axioms which state that $\preceq$ is interpreted by a dominance relation associated to a non-trivial p-convex valuation ring.

Theorem 5.17. *$p\,\mathrm{CVF}$ has* QE.

This p-adic analogue of Theorem 4.1 is stated without proof in [12, Theorem 5]; see also [6, Corollaire 2.3(1)] and [29, Lemma 2.13]. For the proof, these sources quote the unpublished thesis [15] or the notationally dense and long paper [64] (which also yields a primitive recursive algorithm for QE in $p\,\mathrm{CVF}$). For the convenience of the reader we include a deduction of the important Theorem 5.17 below from standard facts in the literature. We start with a somewhat weaker result:

Proposition 5.18. *$p\,\mathrm{CVF}$ is model complete.*

This follows from the Ax-Kochen/Eršov Theorem for elementary substructures. Here, valued fields are viewed as $\mathcal{L}_{\preceq}$-structures where $\mathcal{L}_{\preceq}$ is the language described in Section 1.1.

Theorem 5.19. *Let $K \subseteq E$ be an extension of henselian valued fields of equicharacteristic zero. Then*

$$K \preceq E \quad \Longleftrightarrow \quad \mathrm{res}(K) \preceq \mathrm{res}(E) \text{ and } \Gamma \preceq \Gamma_E.$$

For a version of this fact in a 3-sorted context, for valued fields equipped with an angular component map, see [22, Corollary 5.23]. One may reduce to this setting by replacing (E, K) by an $\aleph_1$-saturated elementary extension, after which E can be equipped with a cross-section which restricts to a cross-section of K (cf. [3, Lemmas 3.3.39, 3.3.40]).

Proof of Proposition 5.18. Let $K \subseteq E$ be models of $p\,\mathrm{CVF}$. By Corollary 5.15, the valued field E is henselian, $\Gamma_E \neq \{0\}$ is divisible, and $\mathrm{res}(E)$ is p-adically closed; similarly for K, Γ, $\mathrm{res}(K)$ in place of E, Γ_E, $\mathrm{res}(E)$, respectively. We have $\mathrm{res}(K) \preceq \mathrm{res}(E)$ by Theorem 5.10, and also $\Gamma \preceq \Gamma_E$ (see, e.g., [3, Example B.11.12]). Hence K is an elementary $\mathcal{L}_{\preceq}$-substructure of E, by Theorem 5.19. By Corollary 5.7, K is algebraically closed in E, so $(E^\times)^n \cap K = (K^\times)^n$ for each $n \geqslant 1$. Hence also using Lemma 5.4 we obtain that K is also an elementary $\mathcal{L}$-substructure of E. □

By Proposition 5.18 we have

$$\mathbb{Q}_p\{\{t^*\}\} \ \preceq\ \mathbb{Q}_p(\!(t^*)\!) \ \preceq\ \mathrm{cl}(\mathbb{Q}_p[t^{\mathbb{Q}}]) \ \preceq\ \mathbb{Q}_p(\!(t^{\mathbb{Q}})\!)$$

as $\mathcal{L}$-structures. In order to finish the proof of Theorem 5.17, we recall a well-known fact about nth powers in henselian valued fields of equicharacteristic zero:

Lemma 5.20. *Let K be a henselian valued field of equicharacteristic zero, and suppose $n \geqslant 1$. Then*

$$(\mathcal{O}^\times)^n = (K^\times)^n \cap \mathcal{O}^\times = \{a \in \mathcal{O}^\times : \overline{a} \in (\boldsymbol{k}^\times)^n\}.$$

Hence for $a, b \in K^\times$ with $a \sim b$ we have $a \in (K^\times)^n \Leftrightarrow b \in (K^\times)^n$.

Proof of Theorem 5.17. Let $E, F \models p\,\mathrm{CVF}$ and let K be a common substructure of E and of F; we need to show $E_K \equiv F_K$; cf. [3, Corollary B.11.6]. The valuation ring $\mathcal{O}$ of K is p-convex. Note that $\operatorname{res}(K) = \mathcal{O}/\smallo \subseteq \operatorname{res}(E)$ has characteristic zero, thus $\mathcal{O}_p \subset \mathcal{O}$. We reduce to the case $\Gamma \neq \{0\}$. Suppose $\Gamma = \{0\}$. Replacing E, F by elementary extensions we first arrange that E, F are $\aleph_1$-saturated, hence we have cross-sections $s_E \colon \Gamma_E \to E^\times$ of E and $s_F \colon \Gamma_F \to F^\times$ of F. Take any $\alpha \in \Gamma_E^>$ and set $x := s_E(\alpha) \in E^\times$; then x is transcendental over K by [3, Corollary 3.1.8]. Since Γ_E is divisible, we have $x \in (E^\times)^n$ for each $n \geqslant 1$. Similarly we take any $\beta \in \Gamma_F^>$ and set $y := s_F(\beta) \in F^\times$; then y is transcendental over K and $y \in (F^\times)^n$ for each $n \geqslant 1$. The field isomorphism $\sigma \colon K(x) \to K(y)$ over K with $\sigma(x) = y$ is a valued field isomorphism [3, Lemma 3.1.30]. Let $0 \neq f \in K[T]$, where T is a single variable over K, and $n \geqslant 1$. Let $a \in K^\times$, $g \in K[T]$, and m be such that $f = aT^m(1 + gT)$. Then $f(x) \sim ax^m$, hence by Lemma 5.20:

$$f(x) \in (E^\times)^n \iff ax^m \in (E^\times)^n \iff a \in (E^\times)^n.$$

Similarly we obtain $f(y) \in (F^\times)^n \Leftrightarrow a \in (F^\times)^n$. Since K is an $\mathcal{L}_{\mathrm{Mac}}$-substructure of both E and F, this yields $f(x) \in (E^\times)^n \Leftrightarrow f(y) \in (F^\times)^n$. If also $0 \neq g \in K[T]$ and $h := f/g \in K(T)$, then

$$h(x) \in (E^\times)^n \iff (fg^{n-1})(x)/g(x)^n \in (E^\times)^n \iff (fg^{n-1})(x) \in (E^\times)^n,$$

and similarly with F and y in place of E and x, respectively. Hence by the above applied to $fg^{n-1} \in K[T]$ in place of f we obtain $h(x) \in (E^\times)^n \Leftrightarrow h(y) \in (F^\times)^n$. Using Lemma 5.4, this also implies $h(x) \preceq_p 1 \Leftrightarrow h(y) \preceq_p 1$. Hence σ is an isomorphism $K(x) \to K(y)$ between $\mathcal{L}_{\mathrm{Mac}}$-substructures of E and of F, respectively. Now identify $K(x)$ with its image under σ and replace K by $K(x)$ to arrange $\Gamma \neq \{0\}$.

Let L be the algebraic closure of K inside E. Then L is p-adically closed, by Corollary 5.7. Now [49, Theorem 3.10] yields a K-embedding j of the p-valued field L into F, and j is also an embedding of $\mathcal{L}_{\mathrm{Mac}}$-structures. By Lemma 1.6, there is a unique p-convex subring of L lying over $\mathcal{O}$, hence j is also an embedding of $\mathcal{L}$-structures. Identifying L with its image under j we first arrange that L is a common $\mathcal{L}$-substructure of E and F, and replacing K by L we then arrange that $K \models p\,\mathrm{CVF}$. Then $K \preceq E$ and $K \preceq F$ by Proposition 5.18 and thus $E \equiv_K F$. □

Let $\mathcal{L}^* := \mathcal{L}^*_{\mathrm{Mac}} \cup \{\preceq\}$ be the expansion of the language of rings $\mathcal{L}_{\mathrm{R}}$ by the unary relation symbols P_n ($n \geqslant 1$) and the binary relation symbol $\preceq$ (a reduct of $\mathcal{L}$).

Corollary 5.21. *Each $\mathcal{L}$-formula is $p\,\mathrm{CVF}$-equivalent to a quantifier-free $\mathcal{L}^*$-formula.*

This follows from Lemma 5.11 and Theorem 5.17.

Corollary 5.22. *$p\,\mathrm{CVF}$ is complete: $K \equiv \mathbb{Q}_p(\!(t^*)\!)$ for each $K \models p\,\mathrm{CVF}$.*

Proof. Expand the field $\mathbb{Q}$ to an $\mathcal{L}$-structure by interpreting $\preceq_p$ by the p-adic dominance relation on $\mathbb{Q}$, $\preceq$ by the trivial dominance relation on $\mathbb{Q}$, and P_n by $(\mathbb{Q}_p^\times)^n \cap \mathbb{Q}^\times$ ($n \geqslant 1$). Note that $(\mathbb{Q}_p^\times)^n \cap \mathbb{Q} = (K^\times)^n \cap \mathbb{Q}$ for each $K \models p\,\mathrm{CF}$ and $n \geqslant 1$, thanks to Corollary 5.3. This $\mathcal{L}$-structure embeds into each model of $p\,\mathrm{CVF}$ (see Lemma 5.13), so the corollary follows from Theorem 5.17. □

In [5], Bélair gives an explicit axiomatization of the universal part $p\,\mathrm{CF}_\forall$ of the $\mathcal{L}_{\mathrm{Mac}}$-theory $p\,\mathrm{CF}$. We note:

Corollary 5.23. *The $\mathcal{L}$-theory $p\,\mathrm{CVF}_\forall$ is axiomatized by*

$$p\,\mathrm{CF}_\forall \cup \big\{1 \preceq n \cdot 1 : n \geqslant 1\big\} \cup \big\{\forall x \forall y (x \preceq_p y \to x \preceq y)\big\}.$$

Proof. Clearly $p\,\mathrm{CVF}_\forall$ contains the displayed $\mathcal{L}$-theory. Conversely, let K be a model of the latter. Then the valuation ring $\mathcal{O}$ associated to the dominance relation $\preceq$ on K is p-convex, and its residue field has characteristic zero. Take an extension K_1 of the $\mathcal{L}_{\mathrm{Mac}}$-reduct of K to a model of $p\,\mathrm{CF}$, and expand it to an $\mathcal{L}$-structure by interpreting $\preceq$ by the dominance relation associated to the p-convex hull of $\mathcal{O}$ in K_1. Then $K \subseteq K_1$ as $\mathcal{L}$-structures, so replacing K by K_1 we can arrange that $K \models p\,\mathrm{CF}$. If the p-convex subring $\mathcal{O}$ of K is non-trivial, then we are done. Suppose otherwise; then $\mathcal{O} = K$. Then by the example following Corollary 5.15, the valuation ring of the t-adic valuation on the Hahn field $L := K(\!(t^{\mathbb{Q}})\!)$ is a non-trivial p-convex subring of L, and accordingly expanding L to an $\mathcal{L}$-structure yields an extension of K to a model of $p\,\mathrm{CVF}$ as required. □

6. The p-adic Analytic Nullstellensatz

In this section we let K be a field of characteristic zero. We first recall the definition and a few basic facts about the p-adic Kochen operator $\gamma = \gamma_p$, the p-adic Kochen ring Λ_K, and generalize some auxiliary results about p-adic ideals from [60, 61]. In Proposition 6.18 we establish a specialization result analogous to Propositions 3.2 and 4.2, from which a general form of the p-adic analytic version of Hilbert's 17th Problem (Corollary 6.22) and the p-adic analytic Nullstellensatz (Theorem 6.24) follow. Theorems A, B, and C from the introduction are then easy consequences. (See Corollaries 6.25–6.29.)

6.1. The Kochen ring.

We set $K_\infty := K \cup \{\infty\}$ where $\infty \notin K$. For $f \in K$ we put $\wp(f) := f^p - f$ and

$$\gamma(f) := \frac{1}{p}\frac{\wp(f)}{\wp(f)^2 - 1} \in K_\infty \quad \text{where } \gamma(f) := \infty \text{ if } \wp(f) = \pm 1.$$

For the following see [49, Lemma 6.1]:

Lemma 6.1. *Let $\mathcal{O}$ be a valuation ring of K. Then $\mathcal{O}$ is a p-valuation ring of K iff $p \notin \mathcal{O}^\times$ and $\gamma(f) \in \mathcal{O}$ for all $f \in K$.*

By convention, for $R \subseteq K$ we set $\gamma(R) := \big\{\gamma(f) : f \in R\big\} \setminus \{\infty\}$. If K is formally p-adic, then $\gamma(f) \neq \infty$ for each $f \in K$, by the previous lemma, so in this case $\gamma(R)$ indeed agrees with the image of the restriction of the map γ to a map $R \to K_\infty$. For a proof of the following see [49, Theorem 6.4]:

Proposition 6.2. *Let $(K, \mathcal{O})$ be p-valued field and L be a field extension of K. Then there is a p-valuation ring of L lying over $\mathcal{O}$ iff $p \notin \mathcal{O}[\gamma(L)]^\times$.*

Since K is formally p-adic iff there is a p-valuation ring of K which lies over the unique p-valuation ring $\mathbb{Z}_{(p)}$ of the subfield $\mathbb{Q}$ of K, Proposition 6.2 implies:

Corollary 6.3. *K is formally p-adic $\Longleftrightarrow$ $p \notin \mathbb{Z}_{(p)}[\gamma(K)]^\times$.*

The *p-adic Kochen ring* of K is the subring

$$\Lambda_K := \left\{\frac{f}{1 - pg} : f, g \in \mathbb{Z}[\gamma(K)],\ pg \neq 1\right\}$$

of K. It is easy to see that

$$\Lambda_K = \left\{ \frac{f}{1-pg} : f,g \in \mathbb{Z}_{(p)}[\gamma(K)],\ pg \neq 1 \right\}.$$

If K is formally p-adic then by the previous corollary we can omit here the condition "$pg \neq 1$". The next result is shown in [49, Theorem 6.14]:

Theorem 6.4. $\Lambda_K = \bigcap \{\mathcal{O} : \mathcal{O}$ *is a p-valuation ring of* $K\}$.

By Theorem 6.4 and the proof of Lemma 5.12, with $\mathcal{O}_0$ as in Lemma 5.4, we have $\mathcal{O}_0 = \Lambda_K$ whenever K is p-euclidean. Also, K is formally p-adic iff $\Lambda_K \neq K$; moreover:

Corollary 6.5. *K is formally p-adic* $\Longleftrightarrow p \notin \Lambda_K^\times$.

Proof. Suppose K is formally p-adic, and towards a contradiction assume $p \in \Lambda_K^\times$. Take $f,g \in \mathbb{Z}[\gamma(K)]$ with $p^{-1} = f/(1-pg)$; then $p^{-1} = f + g \in \mathbb{Z}[\gamma(K)]$, contradicting Corollary 6.3. □

Theorem 6.4 implies that Λ_K is a Prüfer domain (every localization of Λ_K at a maximal ideal of Λ_K is a valuation ring of K); see [49, Corollary 6.16]. In fact, Λ_K is even a Bézout domain (every finitely generated ideal of Λ_K is principal) with fraction field K; cf. [49, Theorem 6.17]. Hence every subring of K containing Λ_K is also a Bézout domain. In particular, given a subring R of K, the subring

$$\Lambda_K R := \left\{ \frac{f}{1-pg} : f \in R[\gamma(K)],\ g \in \mathbb{Z}[\gamma(K)],\ pg \neq 1 \right\}.$$

of K generated by Λ_K and R is a Bézout domain. (We will not use this fact below.)

6.2. **p-adic ideals and p-adic radical.** *In this subsection we let R be an integral domain with fraction field K.* We say that an ideal I of R is *p-adic* if

$$I = \sqrt{I\,\Lambda_K R} \cap R,$$

that is, if I contains each $r \in R$ such that $r^k \in I\,\Lambda_K R$ for some $k \geqslant 1$. (This notion was introduced in [60] and further studied in [24, 61].) If I is p-adic, then I is radical. The trivial ideals $I = \{0\}$ and $I = R$ of R clearly are p-adic. This notion of p-adic ideal is mainly of interest if K is formally p-adic: otherwise we have $\Lambda_K = K$, hence R has no non-trivial p-adic ideals.

Lemma 6.6. *Let R^* be an integral domain extending R such that R^* is faithfully flat over R, and let I be an ideal of R such that the ideal IR^* of R^* is p-adic. Then I is p-adic.*

Proof. Let $f \in \sqrt{I\,\Lambda_K R} \cap R$. This yields $k \geqslant 1$ with $f^k \in I\,\Lambda_K R$. Now with $K^* := \operatorname{Frac}(R^*)$ we have $\Lambda_K \subseteq \Lambda_{K^*}$, hence $f^k \in I\,\Lambda_{K^*} R^*$. Since IR^* is p-adic we get $f \in IR^*$ and thus $f \in I$ because R^* is faithfully flat over R [43, Theorem 7.5(ii)]. □

Lemma 6.7. *If R is noetherian, then all minimal prime ideals of R containing a given p-adic ideal of R are p-adic.*

This follows from an easy ring-theoretic lemma, applied to $A = R$, $B = \Lambda_K R$:

Lemma 6.8. *Let $A \subseteq B$ be a ring extension where A is noetherian. Let I be an ideal of A such that $I = \sqrt{IB} \cap A$. Then for each minimal prime ideal P of A containing I we also have $P = \sqrt{PB} \cap A$.*

In the next lemma and its corollary we assume that R is local with maximal ideal $\mathfrak{m}$ and residue field $\boldsymbol{k} := R/\mathfrak{m}$ of characteristic zero, and we let $r \mapsto \overline{r}\colon R \to \boldsymbol{k}$ be the residue morphism.

Lemma 6.9. *Let $\alpha \in \gamma(\boldsymbol{k})$; then there is some $a \in \gamma(R) \cap R$ such that $\alpha = \overline{a}$.*

Proof. Take $\beta \in \boldsymbol{k}$ such that $\alpha = \gamma(\beta)$, so

$$\alpha p(\delta^2 - 1) = \delta \qquad \text{where } \delta := \wp(\beta) \in \boldsymbol{k} \setminus \{\pm 1\}.$$

Next let $a, b \in R$ with $\overline{a} = \alpha$, $\overline{b} = \beta$. Then $\overline{d} = \delta$ for $d := \wp(b)$ and so $d \neq \pm 1$, and $ap(d^2 - 1) - d \in \mathfrak{m}$. Now $p(d^2 - 1) \in R^\times$ and thus $a - \gamma(b) = a - \frac{d}{p(d^2-1)} \in \mathfrak{m}$. Hence $\gamma(b) \in R$ and $\alpha = \overline{\gamma(b)}$. □

Corollary 6.10. *Suppose K is formally p-adic. If $\mathfrak{m}$ is p-adic, then $\boldsymbol{k}$ is formally p-adic.*

Proof. Suppose $\boldsymbol{k}$ is not formally p-adic. Corollary 6.5 then yields $\alpha, \beta \in \mathbb{Z}[\gamma(\boldsymbol{k})]$, $p\beta \neq 1$, such that

$$p^{-1} = \frac{\alpha}{1 - p\beta} \quad \text{and hence} \quad 1 - p(\alpha + \beta) = 0.$$

The lemma above yields $a, b \in \mathbb{Z}[\gamma(K)] \cap R$ with $\alpha = \overline{a}$, $\beta = \overline{b}$. We have $1 \neq p(a+b)$ since K is formally p-adic. Thus $1 - p(a + b) \in \mathfrak{m} \cap \Lambda_K^\times$ and so $1 \in \mathfrak{m}\Lambda_K R \cap R$. Hence $\mathfrak{m}$ is not p-adic. □

Next we let P be a prime ideal of R and F be the fraction field of R/P. We let

$$R_P := \big\{ r/s : r, s \in R,\ s \notin P \big\} \subseteq K$$

be the localization of R at P. The residue morphism $R \to R/P$ extends uniquely to a surjective ring morphism $R_P \to F$ with kernel PR_P.

Lemma 6.11. *P is p-adic iff the maximal ideal PR_P of R_P is also p-adic.*

Proof. Suppose P is p-adic. Let $f \in R_P$ and $k \geqslant 1$ be such that $f^k \in P\Lambda_K R_P$; we need to show that $f \in PR_P$. Multiplying f by a suitable unit of R_P we arrange $f \in R$. Take $a \in R \setminus P$ such that $af^k \in P\Lambda_K R$. Then $af \in \sqrt{P\Lambda_K R} \cap R = P$, thus $f \in PR_P$ as claimed. Conversely, if PR_P is p-adic, and $f \in R$, $k \geqslant 1$ with $f^k \in P\Lambda_K R$, then $f \in PR_P \cap R = P$, showing that P is p-adic. □

Combining Corollary 6.10 and Lemma 6.11 yields:

Corollary 6.12. *If K is formally p-adic and P is p-adic, then F is formally p-adic.*

Here is a partial converse of the implication in the previous corollary:

Proposition 6.13. *Suppose R is regular and $F = \operatorname{Frac}(R/P)$ is formally p-adic. Then K is formally p-adic and P is p-adic.*

Proof. The local integral domain R_P is regular and its residue field is isomorphic to F. Hence localizing at P we can arrange that R is local with maximal ideal P, by Lemma 6.11. Lemma 1.2 yields a valuation ring $\mathcal{O}$ of K lying over R such that the natural inclusion $R \to \mathcal{O}$ induces an isomorphism $F = R/P \to \boldsymbol{k} = \mathcal{O}/\smallo$; thus $\boldsymbol{k}$ is formally p-adic. Let $\mathcal{O}_{\boldsymbol{k}}$ be a p-valuation ring of $\boldsymbol{k}$ and take a valuation ring $\mathcal{O}_0$ of K with $\mathcal{O}_0 \subseteq \mathcal{O}$ and a convex subgroup Δ_0 of its value group such that the Δ_0-specialization of $(K, \mathcal{O}_0)$ is $(\boldsymbol{k}, \mathcal{O}_{\boldsymbol{k}})$. (See Lemma 1.3.) Then $\mathcal{O}_0$ is a p-valuation ring of K by Lemma 5.1, hence $\Lambda_K \subseteq \mathcal{O}_0 \subseteq \mathcal{O}$ by Theorem 6.4. This yields $P\Lambda_K R \cap R \subseteq P\mathcal{O} \cap R = P$ and thus $\sqrt{P\Lambda_K R} \cap R = P$ as required. □

It would be interesting to weaken the regularity hypothesis in Proposition 6.13. Let now $\sigma\colon R \to L$ be a ring morphism. The previous proposition immediately implies:

Corollary 6.14. *If R is regular and L is formally p-adic, then K is formally p-adic and $\ker\sigma$ is a p-adic prime ideal of R.*

We also note another artifact of the proof of Proposition 6.13.

Lemma 6.15. *Suppose R is regular, and let $f, g \in R$. Then*

$$f \in g\Lambda_K \implies \sigma(f) \in \sigma(g)\Lambda_L.$$

Proof. We may arrange that $L = F = \operatorname{Frac}(R/P)$ and σ is the composition of the residue morphism $R \to R/P$ with the natural inclusion $R/P \to F$. Replacing R, P by R_P, PR_P, respectively, we can also arrange that R is local with maximal ideal P and residue field $L = R/P$, and $\sigma\colon R \to L$ is the residue morphism. Suppose $f \in g\Lambda_K$, and let $\mathcal{O}_L$ be a p-valuation ring of L, with associated dominance relation $\preceq_L$ on L; we need to show $\sigma(f) \preceq_L \sigma(g)$, by Theorem 6.4. Take $\mathcal{O}$ as in the proof of Proposition 6.13 and let $\mathcal{O}_{\boldsymbol{k}}$ be the image of $\mathcal{O}_L$ under the isomorphism $F \to \boldsymbol{k}$. Next take $\mathcal{O}_0$ as in the proof of Proposition 6.13, so $\mathcal{O}_0 = \big\{h \in \mathcal{O} : \sigma(h) \preceq_L 1\big\}$. If $g \in P$, then $f \in P$ since $P\Lambda_K R \cap R = P$, and hence clearly $\sigma(f) \preceq_L \sigma(g)$. Suppose $g \notin P$; then $g \in R^\times$, hence we may replace f, g by $f/g, 1$ to arrange $g = 1$. Then $f \in \Lambda_K$ and so $f \in \mathcal{O}_0$ by Theorem 6.4, thus $\sigma(f) \preceq_L 1$. □

Let I be an ideal of R. We define the *p-radical of I* as

$$\sqrt[p]{I} := \sqrt{I\Lambda_K R} \cap R = \big\{r \in R : r^k \in I\Lambda_K R \text{ for some } k \geqslant 1\big\}.$$

Clearly $\sqrt[p]{I}$ is the smallest p-adic ideal of R containing I. If J is an ideal of R, then $I \subseteq J \Rightarrow \sqrt[p]{I} \subseteq \sqrt[p]{J}$.

6.3. **p-adic ideals under completion.** In this subsection we show a p-adic analogue of [52, Proposition 6.3]. Let W be a Weierstrass system over a formally p-adic field $\boldsymbol{k}$. Let I be an ideal of $R := W_m = \boldsymbol{k}\lfloor X\rfloor$. If the ideal $I\widehat{R}$ of $\widehat{R} := \boldsymbol{k}[[X]]$ generated by I is p-adic, then so is I, by Corollary 2.6 and Lemma 6.6. The converse also holds:

Proposition 6.16. *Suppose I is p-adic; then so is $I\widehat{R}$.*

Proof. We may assume $I \neq R$. Note that since we have a ring morphism $f \mapsto f(0)\colon \widehat{R} \to \boldsymbol{k}$ from the regular local ring $\widehat{R}$ to the formally p-adic field $\boldsymbol{k}$, the field $\widehat{K} := \operatorname{Frac}(\widehat{R})$ is formally p-adic by Corollary 6.14. Let $P_1, \dots, P_k$ ($k \geqslant 1$) be the minimal prime ideals of I. Then $P_1, \dots, P_k$ are p-adic by Lemma 6.7, and $I\widehat{R} = P_1\widehat{R} \cap \dots \cap P_k\widehat{R}$ by [43, Theorem 7.4(ii)]. Hence it is enough to show the proposition in the case where I is prime. In this case, $I\widehat{R}$ is then also prime, by Lemma 2.12. Since we have $I\widehat{R} \cap R = I$ [43, Theorem 7.5(ii)], we may view $F := \operatorname{Frac}(R/I)$ as a subfield of $\widehat{F} := \operatorname{Frac}(\widehat{R}/I\widehat{R})$. Now by Corollary 6.3, F is formally p-adic iff $p^{-1} \notin \mathbb{Z}_{(p)}[\gamma(F)]$, and similarly with $\widehat{F}$ in place of F. By Corollary 6.12, F is formally p-adic, hence so is $\widehat{F}$ by the version of the Artin Approximation Theorem for $R \subseteq \widehat{R}$ from [18, Theorem 1.1]. Thus $I\widehat{R}$ is p-adic by Proposition 6.13. □

Corollary 6.17. $\sqrt[p]{I\widehat{R}} = \sqrt[p]{I}\widehat{R}$.

6.4. **The p-adic analytic Nullstellensatz.** *In this subsection we let $\mathcal{L} = \mathcal{L}_{\text{Mac},\preceq}$. We also let W be a Weierstrass system over a weakly p-euclidean field $\boldsymbol{k}$, and we let $K \models p\,\text{CVF}_W$.* (Note that the infinitesimal W-structure on K is with respect to the distinguished p-convex valuation ring of K, not with respect to the p-valuation ring of K.) We also let $X = (X_1, \dots, X_m)$ be a tuple of distinct indeterminates over $\boldsymbol{k}$ and $y = (y_1, \dots, y_n)$ be a tuple of distinct $\mathcal{L}$-variables.

Proposition 6.18. *For each $\mathcal{L}$-formula $\varphi(y)$ and each $f \in \boldsymbol{k}\lfloor X \rfloor^n$, if $\Omega \models \varphi(\sigma(f))$ for some $\Omega \models p\,\text{CVF}$ and local ring morphism $\sigma\colon \boldsymbol{k}\lfloor X \rfloor \to \mathcal{O}_\Omega$, then $K \models \varphi(f(a))$ for some $a \in \mathcal{O}^m$.*

Proof. The proof is completely analogous to that of Proposition 4.2. Using Corollary 5.21 instead of Theorem 4.1 we first arrange that φ is a quantifier-free $\mathcal{L}^*$-formula. If $k \geqslant 1$ and $\lambda_1, \dots, \lambda_N \in \mathbb{Z}$ ($N \geqslant 1$) are representatives for the cosets $\neq \mathbb{Q}_p^\times$ of the subgroup $(\mathbb{Q}_p^\times)^k$ of $\mathbb{Q}_p^\times$ (Lemma 5.9), then for each single variable v we have

$$p\,\text{CF} \models \neg\,\text{P}_k(v) \leftrightarrow \text{P}_k(\lambda_1 v) \vee \cdots \vee \text{P}_k(\lambda_N v).$$

Hence we can further arrange that φ has the form

$$P(y) = 0 \wedge \bigwedge_{i \in I} \text{P}_{k_i}\big(Q_i(y)\big) \wedge \bigwedge_{j \in J} R_j(y) \,\square_j\, S_j(y)$$

where I, J are finite, $P, Q_i, R_j, S_j \in \mathbb{Z}[Y_1, \dots, Y_n]$, $k_i \geqslant 1$, and each symbol $\square_j$ is $\preceq$ or $\prec$. For each $k \geqslant 1$, every 1-unit of $\boldsymbol{k}\lfloor X \rfloor$ is a kth power of a 1-unit of $\boldsymbol{k}\lfloor X \rfloor$, by Corollary 2.9; using this fact instead of Lemma 2.10 we now finish the argument as in the proof of Proposition 4.2. $\square$

As before, the p-adic version of Corollary 4.3 follows:

Corollary 6.19. *For each existential $\mathcal{L}_W$-sentence θ, we either have $p\,\text{CVF}_W \models \theta$ or $p\,\text{CVF}_W \models \neg\theta$.*

Next an analogue of Lemma 4.4:

Lemma 6.20. *Let Ω be a p-valued field and $\sigma\colon \boldsymbol{k}\lfloor X \rfloor \to \Omega$ be a ring morphism. Let $\preceq$ be the dominance relation on Ω whose valuation ring is the p-convex hull of $\sigma(\boldsymbol{k})$ in Ω. Then for each $g \in \boldsymbol{k}\lfloor X \rfloor$ we have $\sigma\big(g - g(0)\big) \prec 1$.*

Proof. Replacing g by $g - g(0)$ we arrange $g(0) = 0$. Then $1 + pg^2$ is a square in $\boldsymbol{k}\lfloor X \rfloor$, by Corollary 2.9; hence $1 + p\sigma(g)^2$ is a square in Ω, so necessarily $\sigma(g) \preceq_p 1$. Since this also holds for gc^{-1} in place of g, for each $c \in \boldsymbol{k}^\times$, we get $\sigma(g) \preceq_p \sigma(c)$ for all $c \in \boldsymbol{k}^\times$. Thus $\sigma(g) \prec 1$ by Lemma 1.5. $\square$

Corollary 6.21. *Let $\varphi(y)$ be an $\mathcal{L}_{\text{Mac}}$-formula, $f \in \boldsymbol{k}\lfloor X \rfloor^n$, and $\sigma\colon \boldsymbol{k}\lfloor X \rfloor \to \Omega$ be a ring morphism to a p-adically closed field Ω such that $\Omega \models \varphi(\sigma(f))$. Then $K \models \varphi(f(a))$ for some $a \in \mathcal{O}^m$.*

Proof. The p-convex hull of $\sigma(\boldsymbol{k})$ in the p-adically closed field extension $\Omega(\!(t^{\mathbb{Q}})\!)$ of Ω is a non-trivial p-convex subring of K, by Lemma 5.16. Hence using model completeness of the $\mathcal{L}_{\text{Mac}}$-theory $p\,\text{CF}$ we may replace Ω by $\Omega(\!(t^{\mathbb{Q}})\!)$ to arrange that the p-convex hull $\mathcal{O}_\Omega$ of $\sigma(\boldsymbol{k})$ in Ω satisfies $\Omega \neq \mathcal{O}_\Omega$. Then Ω equipped with the dominance relation associated to $\mathcal{O}_\Omega$ is a model of $p\,\text{CVF}$. By Lemma 6.20, σ is a local ring morphism $\boldsymbol{k}\lfloor X \rfloor \to \mathcal{O}_\Omega$. Hence the corollary follows from Proposition 6.18. $\square$

Recall that the ring $\boldsymbol{k}\lfloor X\rfloor$ is regular (Lemma 2.5), hence $F := \operatorname{Frac}(\boldsymbol{k}\lfloor X\rfloor)$ is formally p-adic. We obtain an analytic version of Kochen's p-adic formulation of Hilbert's 17th Problem.

Corollary 6.22.

$$\Lambda_F = \left\{ \frac{f}{g} : f,g \in \boldsymbol{k}\lfloor X\rfloor,\ g \neq 0,\ f(a) \preceq_p g(a) \text{ for all } a \in \mathcal{o}^m \right\}.$$

Proof. Let $f,g \in \boldsymbol{k}\lfloor X\rfloor$, $g \neq 0$, with $f/g \notin \Lambda_F$. By Theorem 6.4 take a p-valuation ring $\mathcal{O}_p$ of F with $f/g \notin \mathcal{O}_p$. Let Ω be a p-adically closed valued field extension of $(F,\mathcal{O}_p)$, with natural inclusion $\sigma\colon \boldsymbol{k}\lfloor X\rfloor \to \Omega$. Then Corollary 6.21 yields some $a \in \mathcal{o}^m$ with $f(a) \not\preceq_p g(a)$. This shows the inclusion $\supseteq$. The reverse inclusion follows from Lemma 6.15. □

Next we prove the p-adic analytic Nullstellensatz. First, a preliminary observation:

Lemma 6.23. *Let I be an ideal of $\boldsymbol{k}\lfloor X\rfloor$. Then $\operatorname{Z}_K(I) = \operatorname{Z}_K(\sqrt[p]{I})$, and if $\operatorname{Z}_K(I) \neq \emptyset$ then some p-adic prime ideal of $\boldsymbol{k}\lfloor X\rfloor$ contains I.*

Proof. For each $a \in \mathcal{o}^m$, the kernel of the ring morphism $f \mapsto f(a)\colon \boldsymbol{k}\lfloor X\rfloor \to K$ is a p-adic prime ideal P_a of $\boldsymbol{k}\lfloor X\rfloor$, by Corollary 6.14. Let $f \in \sqrt[p]{I}$ and $a \in \operatorname{Z}_K(I)$. Then P_a contains I and thus also $\sqrt[p]{I}$; in particular $f \in P_a$ and so $f(a) = 0$. □

Theorem 6.24 (p-adic analytic Nullstellensatz)**.** *Let I be an ideal of $\boldsymbol{k}\lfloor X\rfloor$. Then*

$$\operatorname{I}\big(\operatorname{Z}_K(I)\big) = \sqrt[p]{I}.$$

Proof. If no p-adic prime ideal of $\boldsymbol{k}\lfloor X\rfloor$ contains I, then $\operatorname{Z}_K(I) = \emptyset$ by Lemma 6.23 and thus $\operatorname{I}\big(\operatorname{Z}_K(I)\big) = \boldsymbol{k}\lfloor X\rfloor = \sqrt[p]{I}$ by Lemma 6.7. Hence we can assume that some p-adic prime ideal of $\boldsymbol{k}\lfloor X\rfloor$ contains I. Lemma 6.7 then yields p-adic prime ideals $P_1,\dots,P_k$ ($k \geqslant 1$) of $\boldsymbol{k}\lfloor X\rfloor$ with $\sqrt[p]{I} = P_1 \cap \cdots \cap P_k$. Using Lemma 6.23 we arrange that I itself is a p-adic prime ideal; we need to show that then $\operatorname{I}\big(\operatorname{Z}_K(I)\big) = I$. The fraction field F of $R := \boldsymbol{k}\lfloor X\rfloor/I$ is formally p-adic, by Corollary 6.12. Equip F with some p-valuation, let Ω be a p-adically closed extension of this p-valued field, and let $\sigma\colon \boldsymbol{k}\lfloor X\rfloor \to \Omega$ be the composition of $f \mapsto f+I\colon \boldsymbol{k}\lfloor X\rfloor \to R$ with the natural inclusion $R \subseteq \Omega$. Arguing as in the proof of Theorem 3.5, using Corollary 6.21 instead of Corollary 3.4, then yields $\operatorname{I}\big(\operatorname{Z}_K(I)\big) \subseteq I$. □

Recall that if $\boldsymbol{k}$ is p-adically closed, then the t-adically valued field $\boldsymbol{k}(\!(t^*)\!)$ is a model of $p\,$CVF. Hence in a similar way as Theorem 3.5 implied Corollary 3.7 or Theorem 4.7 implied Corollary 4.8, from Theorem 6.24 we get the Nullstellensatz for formal power series over p-adically closed fields (Theorem C from the introduction):

Corollary 6.25. *Suppose $\boldsymbol{k}$ is p-adically closed, and let $R := \boldsymbol{k}[[X]]$ and $F := \operatorname{Frac}(\boldsymbol{k}[[X]])$. Let $f, g_1,\dots,g_n \in \boldsymbol{k}[[X]]$ be such that for all $a \in t\boldsymbol{k}[[t]]^m$:*

$$g_1(a) = \cdots = g_n(a) = 0 \quad\Longrightarrow\quad f(a) = 0.$$

Then there are $k \geqslant 1$, $g \in \mathbb{Z}[\gamma(F)]$, and $h_1,\dots,h_n \in R[\gamma(F)]$, such that

$$f^k(1-pg) = g_1h_1 + \cdots + g_nh_n.$$

Remarks. Let $\boldsymbol{k}$, R, F be as in the previous corollary.

(1) Let $\boldsymbol{k}_0$ be a weakly p-euclidean subfield of $\boldsymbol{k}$ (such as $\boldsymbol{k}_0 = \mathbb{Q}$). If f and each g_j in Corollary 6.25 are in $\boldsymbol{k}_0[[X]]$, then we can take $g \in \mathbb{Z}[\gamma(F_0)]$ and $h_j \in R_0[\gamma(F_0)]$, where $R_0 := \boldsymbol{k}_0[[X]]$ and $F_0 := \operatorname{Frac}(R_0)$. Similarly with other Weierstrass systems over $\boldsymbol{k}_0$ in place of $\boldsymbol{k}_0[[X]]$, like $\boldsymbol{k}_0[[X]]^{\mathrm{a}}$ or $\boldsymbol{k}_0[[X]]^{\mathrm{da}}$.

(2) With $\operatorname{Hom}_{\boldsymbol{k}}(\boldsymbol{k}[[X]], \boldsymbol{k}[[t]])$ denoting the set of $\boldsymbol{k}$-algebra morphisms $\boldsymbol{k}[[X]] \to \boldsymbol{k}[[t]]$, Corollary 6.25 can also be phrased succinctly as follows: for each ideal I of $\boldsymbol{k}[[X]]$,
$$\sqrt[p]{I} = \bigcap \big\{ \ker\lambda : \lambda \in \operatorname{Hom}_{\boldsymbol{k}}(\boldsymbol{k}[[X]], \boldsymbol{k}[[t]]),\ I \subseteq \ker\lambda \big\}.$$

In the rest of this subsection we let $A := \mathbb{Q}_p\{X\}$, $F := \operatorname{Frac}(\mathbb{Q}_p\{X\})$. Combining Corollaries 6.17 and 6.25 yields:

Corollary 6.26. *Let $g_1, \dots, g_n \in A$ and*
$$Z := \big\{ a \in t\mathbb{Q}_p[[t]]^m : g_1(a) = \cdots = g_n(a) = 0 \big\}.$$
Then the ideal of all $f \in \mathbb{Q}_p[[X]]$ such that $f(a) = 0$ for all $a \in Z$ is generated by power series in $A = \mathbb{Q}_p\{X\}$.

Since the t-adically valued field $\mathbb{Q}_p\{\{t^*\}\}$ is a model of $p\,\mathrm{CVF}$, arguing as in the proof of Corollary 3.7 we also obtain:

Corollary 6.27. *Let $f, g_1, \dots, g_n \in A$, and suppose that for each $a \in \mathbb{Q}_p\{t\}^m$ with $a(0) = 0$ we have*
$$g_1(a) = \cdots = g_n(a) = 0 \quad\Longrightarrow\quad f(a) = 0.$$
Then there are $k \geqslant 1$, $g \in \mathbb{Z}[\gamma(F)]$, $h_1, \dots, h_n \in A[\gamma(F)]$, such that
$$f^k(1 - pg) = g_1h_1 + \cdots + g_nh_n.$$

In the same way that Corollary 3.7 gave rise to Corollary 3.9, the last corollary also yields a version for p-adic analytic functions near 0; this is Theorem A in the introduction:

Corollary 6.28. *Let $f, g_1, \dots, g_n \colon U \to \mathbb{Q}_p$ be analytic functions, where U is an open neighborhood of 0 in $\mathbb{Q}_p^m$, such that for all $a \in U$:*
$$g_1(a) = \cdots = g_n(a) = 0 \quad\Longrightarrow\quad f(a) = 0.$$
Then there are $k \geqslant 1$, $g \in \mathbb{Z}[\gamma(F)]$, $h_1, \dots, h_n \in A[\gamma(F)]$, such that in F, with the germs of $f, g_1, \dots, g_n$ at 0 denoted by the same symbols:
$$f^k(1 - pg) = g_1h_1 + \cdots + g_nh_n. \tag{6.1}$$

Remark. Let $f, g_1, \dots, g_n \colon U \to \mathbb{Q}_p$ be as in Corollary 6.28. If $r, s \colon U \to \mathbb{Q}_p$ are analytic functions and $Z := s^{-1}(0)$, then $\gamma\big(r(a)/s(a)\big) \in \mathbb{Z}_p$ for each $a \in U \setminus Z$, by Lemma 6.1, so we have a continuous function
$$\gamma(r/s) \colon U \setminus Z \to \mathbb{Z}_p \quad \text{with } \gamma(r/s)(a) = \gamma\big(r(a)/s(a)\big) \text{ for } a \in U \setminus Z.$$
Hence if $k \geqslant 1$, $g \in \mathbb{Z}[\gamma(F)]$, and $h_1, \dots, h_n \in A[\gamma(F)]$ are as in the previous corollary, then $g, h_1, \dots, h_n$ give rise to functions $g, h_1, \dots, h_n \colon U \setminus Z \to \mathbb{Q}_p$, where $Z = s^{-1}(0)$ for some analytic $s \colon U \to \mathbb{Q}_p$ with non-zero germ at 0, such that the identity (6.1) above holds in the the ring of continuous functions $U \setminus Z \to \mathbb{Q}_p$.

Finally, we obtain Theorem B, a p-adic analytic version of Hilbert's 17th Problem:

Corollary 6.29. *Let $f, g\colon U \to \mathbb{Q}_p$ be analytic functions, where U is an open neighborhood of 0 in $\mathbb{Q}_p^m$, such that $|f(a)|_p \leqslant |g(a)|_p$ for all $a \in U$. Then, with the germs of f, g at 0 denoted by the same symbols, we have $f \in g\Lambda_F$.*

Proof. If $g = 0$, then also $f = 0$, hence we may assume $g \neq 0$. The hypothesis yields $|f(a)|_p \leqslant |g(a)|_p$ for all $a \in t\mathbb{Q}_p\{t\}^m$ and so $|f(a)|_p \leqslant |g(a)|_p$ for all $a \in \smallo^m$ where $\smallo = \bigcup_{d\geqslant 1} t^{1/d}\mathbb{Q}_p\{\{t^{1/d}\}\}$, the maximal ideal of $\mathbb{Q}_p\{\{t^*\}\}$. Hence $f/g \in \Lambda_F$ by Corollary 6.22. □

In the next section we show how to improve the preceding corollaries 6.28 and 6.29 by replacing $A = \mathbb{Q}_p\{X\}$ above with the ring $\mathbb{Q}_p\langle X\rangle$ of restricted power series.

7. Nullstellensätze for Restricted Power Series

In this section we let $\boldsymbol{k}$ be a field and $|\cdot|\colon \boldsymbol{k} \to \mathbb{R}^{\geqslant}$ be a complete ultrametric absolute value on $\boldsymbol{k}$. We let $R := \{a \in \boldsymbol{k} : |a| \leqslant 1\}$ and $\mathfrak{m} := \{a \in \boldsymbol{k} : |a| < 1\}$ be the valuation ring of $|\cdot|$ and its maximal ideal, respectively. The residue field of R is denoted by $\overline{R} := R/\mathfrak{m}$, with residue morphism $a \mapsto \overline{a}\colon R \to \overline{R}$. Whenever appropriate we view $\boldsymbol{k}$ as an $\mathcal{L}_{\preceq}$-structure by equipping it with the dominance relation $\preceq$ associated to R: $a \preceq b :\Leftrightarrow |a| \leqslant |b|$, for $a, b \in \boldsymbol{k}$.

7.1. **Restricted power series.** The set of all formal power series

$$f = \sum_\alpha f_\alpha X^\alpha \in \boldsymbol{k}[[X]] \quad \text{such that } |f_\alpha| \to 0 \text{ as } |\alpha| \to \infty$$

forms a $\boldsymbol{k}[X]$-subalgebra of $\boldsymbol{k}[[X]] = \boldsymbol{k}[[X_1, \dots, X_m]]$, called the ring of *restricted power series* with coefficients in $\boldsymbol{k}$. Here, as earlier, $\alpha = (\alpha_1, \dots, \alpha_m)$ ranges over all multiindices in $\mathbb{N}^m$, and $|\alpha| = \alpha_1 + \cdots + \alpha_m$. The Gauss norm on $\boldsymbol{k}[X]$ extends to an ultrametric absolute value on the domain $\boldsymbol{k}\langle X\rangle$ by setting

$$|f| := \max_\alpha |f_\alpha| \qquad \text{for } f \neq 0 \text{ as above.}$$

(See [10, §1.5.3, Corollary 2].) The extension of this ultrametric absolute value on $\boldsymbol{k}\langle X\rangle$ to an ultrametric absolute value on $\operatorname{Frac}(\boldsymbol{k}\langle X\rangle)$ is also denoted by $|\cdot|$.

The $f \in \boldsymbol{k}\langle X\rangle$ with $|f| \leqslant 1$ form an $R[X]$-subalgebra $R\langle X\rangle$ of $\boldsymbol{k}\langle X\rangle$, the ring of restricted power series with coefficients in R. This is the completion of its subring $R[X]$ with respect to the $\mathfrak{m}R[X]$-adic topology on $R[X]$. (Cf., e.g., [28, §3].) The natural inclusion $R[X] \to R\langle X\rangle$ induces an embedding $\overline{R}[X] \to R\langle X\rangle/\mathfrak{m}R\langle X\rangle$, via which we identify $\overline{R}[X]$ with a subring of $R\langle X\rangle/\mathfrak{m}R\langle X\rangle$. For each $f \in R\langle X\rangle$ there is some $d \in \mathbb{N}$ such that $|f_\alpha| < 1$ for $|\alpha| > d$; hence $\overline{R}[X] = R\langle X\rangle/\mathfrak{m}R\langle X\rangle$. We denote the image of f under the natural surjection $R\langle X\rangle \to \overline{R}[X]$ by $\overline{f}$.

7.2. **Substitution.** Let $Y = (Y_1, \dots, Y_n)$ be a tuple of distinct indeterminates and $g = (g_1, \dots, g_m) \in R\langle Y\rangle^m$. We set $g^\alpha := g_1^{\alpha_1} \cdots g_m^{\alpha_m} \in R\langle Y\rangle$ for each α. Then for $f \in \boldsymbol{k}\langle X\rangle$ as above we have $f_\alpha g^\alpha \to 0$ as $|\alpha| \to \infty$, hence we may define

$$f(g) = f(g_1, \dots, g_m) := \sum_\alpha f_\alpha g^\alpha \in \boldsymbol{k}\langle Y\rangle. \tag{7.1}$$

The map $f \mapsto f(g)$ is the unique $\boldsymbol{k}$-algebra morphism $\boldsymbol{k}\langle X\rangle \to \boldsymbol{k}\langle Y\rangle$ with $X_i \mapsto g_i$ for $i = 1, \dots, m$; it restricts to an R-algebra morphism $R\langle X\rangle \to R\langle Y\rangle$. In particular, for $a \in R^m$ we have a $\boldsymbol{k}$-algebra morphism $f \mapsto f(a)\colon \boldsymbol{k}\langle X\rangle \to \boldsymbol{k}$, which restricts to an R-algebra morphism $f \mapsto f(a)\colon R\langle X\rangle \to R$. Let $f \in \boldsymbol{k}\langle X\rangle$; then $|f(a)| \leqslant |f|$ for each $a \in R^m$, and moreover:

Lemma 7.1. *Suppose* $\overline{R}$ *is infinite; then* $|f| = \max_{a\in R^m}|f(a)|$.

Proof. This is clear if $f = 0$, so suppose $f \neq 0$. Taking $b \in \boldsymbol{k}$ with $|b| = |f|$ and replacing f by $b^{-1}f$ we arrange $|f| = 1$, so $\overline{f} \in \overline{R}[X]$ is non-zero. Since $\overline{R}$ is infinite, we obtain an $a \in R^m$ such that $\overline{f(a)} = \overline{f}(\overline{a}) \neq 0$, so $|f(a)| = 1 = |f|$. ☐

Hence if $\overline{R}$ is infinite and $f, g \in \boldsymbol{k}\langle X\rangle$ satisfy $|f(a)| \leqslant |g(a)|$ for every $a \in R^m$, then $|f| \leqslant |g|$; similarly with $<$ in place of $\leqslant$.

7.3. **Weierstrass Division in $\boldsymbol{k}\langle X\rangle$.** This works a bit differently than in $\boldsymbol{k}[[X]]$. To explain this, suppose $m \geqslant 1$ and let $X' = (X_1, \dots, X_{m-1})$. Every $f \in R\langle X\rangle$ can be written uniquely in the form

$$f = \sum_{i=0}^{\infty} f_i X_m^i \quad \text{with } f_i(X') \in R\langle X'\rangle \text{ for all } i \in \mathbb{N}, \tag{7.2}$$

where the infinite sum converges with respect to the Gauss norm on $\boldsymbol{k}\langle X\rangle$. An element f of $R\langle X\rangle$, expressed as in (7.2), is called *regular in X_m of degree $d \in \mathbb{N}$* if $c := \overline{f_d} \in \overline{R}^\times$ and $\overline{f_i} = 0$ for all $i > d$, so $c^{-1}\overline{f} \in \overline{R}[X]$ is monic in X_m of degree d. If $f = f_1 \cdots f_n$ where $f_1, \dots, f_n \in R\langle X\rangle$, then f is regular in X_m of degree d iff f_i is regular in X_m of degree d_i for $i = 1, \dots, n$, with $d_1 + \cdots + d_n = d$. Let $d \in \mathbb{N}$, $d \geqslant 1$. The $\boldsymbol{k}$-algebra automorphism τ_d of $\boldsymbol{k}[[X]]$ with $X_i \mapsto X_i + X_m^{d^{m-i}}$ for $1 \leqslant i < m$ and $X_m \mapsto X_m$ then restricts to an R-algebra automorphism of $R\langle X\rangle$.

Lemma 7.2. *Let $d > 1$ and $f \in R\langle X\rangle$ be such that $\overline{f} \in \overline{R}[X]$ is non-zero of degree $< d$. Then for some $e < d^m$ and some $u \in R^\times$,*

$$\tau_d(f) \equiv uX_m^e + \textit{terms of lower degree in } X_m \mod \mathfrak{m}R\langle X\rangle.$$

(*In particular, $\tau_d(f)$ is regular in X_m of degree $< d^m$.*)

For a proof of this and the following standard facts see, e.g., [10]. Here now is the fundamental property of $R\langle X\rangle$:

Theorem 7.3 (Weierstrass Division Theorem for $R\langle X\rangle$)**.** *Let $g \in R\langle X\rangle$ be regular in X_m of degree d. Then for each $f \in R\langle X\rangle$ there are uniquely determined elements $q \in R\langle X\rangle$ and $r \in R\langle X'\rangle[X_m]$ with $\deg_{X_m} r < d$ such that $f = qg + r$.*

Applying this theorem with $f = X_m^d$, we obtain:

Corollary 7.4 (Weierstrass Preparation Theorem for $R\langle X\rangle$)**.** *Let $g \in R\langle X\rangle$ be regular in X_m of degree d. There are a unique monic polynomial $w \in R\langle X'\rangle[X_m]$ of degree d and a unique $u \in R\langle X\rangle^\times$ such that $g = uw$.*

We remark here that the group of units of $R\langle X\rangle$ is

$$R\langle X\rangle^\times = R^\times\big(1 + \mathfrak{m}R\langle X\rangle\big) = \big\{f \in R\langle X\rangle : \overline{f} \in \overline{R}[X]^\times = \overline{R}^\times\big\},$$

hence $\boldsymbol{k}\langle X\rangle^\times = \boldsymbol{k}^\times\big(1 + \mathfrak{m}R\langle X\rangle\big)$. The elements of the subgroup $1 + \mathfrak{m}R\langle X\rangle$ of $R\langle X\rangle^\times$ are called the 1-*units* of $R\langle X\rangle$. For each 1-unit u of $R\langle X\rangle$ and $a \in R^m$ we have $u(a) \sim 1$ (in the valued field $\boldsymbol{k}$).

A non-zero element $f \in \boldsymbol{k}\langle X\rangle$ is called *regular in X_m of degree $d \in \mathbb{N}$* if there exists some $a \in \boldsymbol{k}$ such that $af \in R\langle X\rangle$ and af is regular in X_m of degree d as defined above. (Note that then necessarily $|a| = |f|^{-1}$.) We denote the unique extension of the R-algebra automorphism τ_d of $R\langle X\rangle$ from Lemma 7.2 to a $\boldsymbol{k}$-algebra automorphism of $\boldsymbol{k}\langle X\rangle$ also by τ_d. By that lemma, for each non-zero $f \in \boldsymbol{k}\langle X\rangle$ there is some $d \in \mathbb{N}$, $d > 1$, such that $\tau_d(f)$ is regular in X_m of degree $< d^m$.

From Theorem 7.3 and Corollary 7.4 we get:

Corollary 7.5. (Weierstrass Division and Preparation for $\boldsymbol{k}\langle X\rangle$.) *Let $g \in \boldsymbol{k}\langle X\rangle$ be regular in X_m of degree d. Then every $f \in \boldsymbol{k}\langle X\rangle$ can be uniquely written as $f = qg + r$ with $q \in \boldsymbol{k}\langle X\rangle$ and $r \in \boldsymbol{k}\langle X'\rangle[X_m]$, $\deg_{X_m} r < d$. In particular, there are a unique monic polynomial $w \in R\langle X'\rangle[X_m]$ of degree d and a unique $u \in \boldsymbol{k}\langle X\rangle^\times$ such that $g = uw$.*

Corollary 7.5 and the remark preceding it imply that $\boldsymbol{k}\langle X\rangle$ is noetherian. (If R is a discrete valuation ring, then $R\langle X\rangle$ is also noetherian.) Euclidean Division in the polynomial ring $\boldsymbol{k}\langle X'\rangle[X_m]$ and the uniqueness part of Weierstrass Division also have another useful consequence:

Corollary 7.6. *Let $w \in R\langle X'\rangle[X_m]$ be monic; then the inclusion $\boldsymbol{k}\langle X'\rangle[X_m] \subseteq \boldsymbol{k}\langle X\rangle$ induces a $\boldsymbol{k}\langle X'\rangle$-algebra isomorphism*

$$\boldsymbol{k}\langle X'\rangle[X_m]/w\boldsymbol{k}\langle X'\rangle[X_m] \xrightarrow{\cong} \boldsymbol{k}\langle X\rangle/w\boldsymbol{k}\langle X\rangle.$$

For future use we note an application of the previous corollary, where we assume $m = 1$ and write $X = X_1$.

Corollary 7.7. *Let $f, g \in \boldsymbol{k}[X]$ with $f \in gR\langle X\rangle$. Then $f \in gR[X](1 + \mathfrak{m}R[X])^{-1}$.*

Proof. This is clear if $g = 0$, so we may assume $g \neq 0$. Weierstrass Preparation then yields $u \in R^\times(1 + \mathfrak{m}R\langle X\rangle)$ and a monic $w \in R[X]$ such that $g = uw$. Then $u \in R[X]$ by Corollary 7.6. Let $h \in R\langle X\rangle$ with $f = gh$. Then Corollary 7.6 also yields $uh \in R[X]$. Thus $h \in R[X](1 + \mathfrak{m}R[X])^{-1}$ as required. □

7.4. **Restricted Weierstrass systems.** We now adapt Definition 2.1 to the setting of restricted power series:

Definition 7.8. A *restricted Weierstrass system over $\boldsymbol{k}$* is a family of rings (W_m) such that for all m we have, with $X = (X_1, \dots, X_m)$:

(RW1) $\boldsymbol{k}[X] \subseteq W_m \subseteq \boldsymbol{k}\langle X\rangle$;
(RW2) for each permutation σ of $\{1, \dots, m\}$, the $\boldsymbol{k}$-algebra automorphism $f(X) \mapsto f(X_{\sigma(1)}, \dots, X_{\sigma(m)})$ of $\boldsymbol{k}\langle X\rangle$ maps W_m onto itself;
(RW3) $W_m \cap \boldsymbol{k}\langle X'\rangle = W_{m-1}$ for $X' = (X_1, \dots, X_{m-1})$, $m \geqslant 1$;
(RW4) if $g \in W_m$ is regular of degree d in X_m ($m \geqslant 1$), then for every $f \in W_m$ there are $q \in W_m$ and $r \in W_{m-1}[X_m]$ of degree $< d$ (in X_m) with $f = qg+r$.

Clearly the system $\big(\boldsymbol{k}\langle X\rangle\big)$ consisting of all restricted power series rings with coefficients in $\boldsymbol{k}$ is a restricted Weierstrass system over $\boldsymbol{k}$. In [2] it is shown that when $\operatorname{char} \boldsymbol{k} = 0$, then the rings $\boldsymbol{k}\langle X\rangle^{\mathrm{a}} := \boldsymbol{k}\langle X\rangle \cap \boldsymbol{k}[[X]]^{\mathrm{a}}$ also form a restricted Weierstrass system over $\boldsymbol{k}$.

In the rest of this section we let $W = (W_m)$ be a restricted Weierstrass system over $\boldsymbol{k}$. For an arbitrary tuple $Y = (Y_1, \dots, Y_m)$ of distinct indeterminates, we let

$$\boldsymbol{k}\lfloor Y\rfloor := \big\{f \in \boldsymbol{k}[[Y]] : f(X) \in W_m\big\} \subseteq \boldsymbol{k}\langle Y\rangle, \qquad R\lfloor Y\rfloor := R\langle Y\rangle \cap \boldsymbol{k}\lfloor Y\rfloor.$$

In the following we let $Y = (Y_1, \dots, Y_n)$ be a tuple of distinct indeterminates disjoint from $X = (X_1, \dots, X_m)$. The elements of the subgroup $1 + \mathfrak{m}R\lfloor X\rfloor$ of $R\lfloor X\rfloor$ are called 1-*units* of $\boldsymbol{k}\lfloor X\rfloor$. We have $W_m \cap \boldsymbol{k}\langle X\rangle^\times = W_m^\times$. (Similar argument as in the proof of Lemma 2.2.) Also using (RW1) this yields $R\lfloor X\rfloor^\times = R^\times(1+\mathfrak{m}R\lfloor X\rfloor)$, so $\boldsymbol{k}\lfloor X\rfloor^\times = \boldsymbol{k}^\times(1+\mathfrak{m}R\lfloor X\rfloor)$.

As in the proof of Lemma 2.3 one shows, using (RW4) instead of (W4):

Lemma 7.9. *Let $f \in \boldsymbol{k}\lfloor X, Y\rfloor$ and $g \in R\lfloor X\rfloor^n$. Then $f(X, g(X)) \in \boldsymbol{k}\lfloor X\rfloor$.*

Using (RW2), (RW3) in place of (W2), (W3), respectively, this yields:

Corollary 7.10. *For all $f \in \boldsymbol{k}\lfloor Y\rfloor$ and $g \in R\lfloor X\rfloor^n$ we have $f(g(X)) \in \boldsymbol{k}\lfloor X\rfloor$.*

In particular, the $\boldsymbol{k}$-algebra automorphism τ_d of $\boldsymbol{k}\langle X\rangle$ maps the subrings $\boldsymbol{k}\lfloor X\rfloor$ and $R\lfloor X\rfloor$ of $\boldsymbol{k}\langle X\rangle$ onto themselves.

Lemma 7.11. *The integral domain $\boldsymbol{k}\lfloor X\rfloor$ is noetherian and factorial. Moreover, suppose R is a DVR; then $R\lfloor X\rfloor$ is also noetherian and factorial, $R\langle X\rangle$ is faithfully flat over $R\lfloor X\rfloor$, and thus $R\lfloor X\rfloor$ is regular.*

Proof. The noetherianity and factoriality statements follow as in [10, §§5.2.5, 5.2.6] using Lemma 7.2 and (RW4). Suppose R is a DVR. Then R is regular, hence so is $R\langle X\rangle$, by [28, Theorem 8.10]. By [28, Theorem 4.9], $R\langle X\rangle$ is faithfully flat over $R\lfloor X\rfloor$; thus $R\lfloor X\rfloor$ is also regular by [28, Theorem 8.7]. □

Remark. The ring $\boldsymbol{k}\langle X\rangle$ is regular; cf., e.g., [10, §7.1.1, Proposition 3]. We will not try to prove here that $\boldsymbol{k}\lfloor X\rfloor$ is regular in general (though this seems plausible). For this it would be enough to see that $\boldsymbol{k}\langle X\rangle$ is faithfully flat over $\boldsymbol{k}\lfloor X\rfloor$; this can probably be shown using Hermann's method in $\boldsymbol{k}\langle X\rangle$ as described in [1].

As usual, (RW4) implies:

Lemma 7.12 (Weierstrass Preparation)**.** *Suppose $m \geqslant 1$. Let $g \in \boldsymbol{k}\lfloor X\rfloor$ be regular in X_m of order d, and set $X' := (X_1, \dots, X_{m-1})$. Then there are a unit u of $\boldsymbol{k}\lfloor X\rfloor$ and a polynomial*

$$w = X_m^d + w_1 X_m^{d-1} + \cdots + w_d \qquad \text{where } w_1, \dots, w_d \in R\lfloor X'\rfloor$$

such that $g = uw$.

Consider now pairs (A, M) where A is a ring and M is a proper ideal of A. Let Y be a single indeterminate over A. A *henselian polynomial* in (A, M) is one of the form $1 + Y + c_2Y^2 + \cdots + c_dY^d$ where $c_2, \dots, c_d \in M$, $d \geqslant 2$. We say that (A, M) is *henselian* if every henselian polynomial in (A, M) has a zero in A. A valued field K is henselian iff the pair $(\mathcal{O}, \smallo)$ is henselian. If A is complete and separated in its M-adic topology (i.e., the natural morphism $A \to \varprojlim A/M^n$ is an isomorphism), then A is henselian with respect to M (Hensel's Lemma). See, e.g., [20, (2.9)] for a proof of this fact; we also recall from [20, (2.10)]:

Lemma 7.13. *Suppose (A, M) is henselian. Then for each $P \in A[Y]$, $z \in A$ and $h \in M$ such that $P(z) = hP'(z)^2$, there is some $y \in A$ such that $P(y) = 0$ and $y \equiv z \bmod P'(z)hA$.*

We now show:

Lemma 7.14. *The pair $\big(R\lfloor X\rfloor, \mathfrak{m}R\lfloor X\rfloor\big)$ is henselian.*

Proof. Let $P(X, Y) \in R\lfloor X\rfloor[Y]$ be henselian in $\big(R\lfloor X\rfloor, \mathfrak{m}R\lfloor X\rfloor\big)$; we need to find a $y \in R\lfloor X\rfloor$ with $P(X, y) = 0$. By our assumption, P is regular in Y of degree 1, so Lemma 7.12 gives a $u \in R\lfloor X, Y\rfloor^\times$ and a monic $w \in R\lfloor X\rfloor[Y]$ of degree 1 with $P = uw$. Now $w = Y - y$ where $y \in R\lfloor X\rfloor$, and y has the required property. □

Corollary 7.15. *Let $f \in \boldsymbol{k}\lfloor X \rfloor$ and $k \geqslant 1$ such that $k \notin \mathfrak{m}$. Then*

$$f = g^k \text{ for some } g \in \boldsymbol{k}\lfloor X \rfloor^\times \quad \Longleftrightarrow \quad f \in (\boldsymbol{k}^\times)^k (1 + \mathfrak{m}R\lfloor X \rfloor).$$

In particular, the group of 1*-units of* $\boldsymbol{k}\lfloor X \rfloor$ *is* k*-divisible.*

Proof. The forward direction is clear, and for the backward direction we may assume $f \in 1 + \mathfrak{m}R\lfloor X \rfloor$, and we need to show that then $f \in (R\lfloor X \rfloor^\times)^k$. To see this consider the polynomial $P = Y^k - f$ and $z = 1$ in Lemma 7.13 applied to the henselian pair $\big(R\lfloor X \rfloor, \mathfrak{m}R\lfloor X \rfloor\big)$. □

7.5. **Zero sets and vanishing ideals.** Let I be an ideal of $\boldsymbol{k}\lfloor X \rfloor$. We then let

$$\mathrm{Z}(I) := \big\{ a \in R^m : f(a) = 0 \text{ for all } f \in I \big\},$$

the zero set of I. If J is another ideal of $\boldsymbol{k}\lfloor X \rfloor$, then $\mathrm{Z}(I) \subseteq \mathrm{Z}(J)$ if $I \supseteq J$, and

$$\mathrm{Z}(IJ) = \mathrm{Z}(I \cap J) = \mathrm{Z}(I) \cup \mathrm{Z}(J), \qquad \mathrm{Z}(I + J) = \mathrm{Z}(I) \cap \mathrm{Z}(J).$$

Let also S be a subset of R^m. The *vanishing ideal* of S is the ideal

$$\mathrm{I}(S) := \big\{ f \in \boldsymbol{k}\lfloor X \rfloor : f(a) = 0 \text{ for all } a \in S \big\}$$

of $\boldsymbol{k}\lfloor X \rfloor$. If also $T \subseteq R^m$, then $\mathrm{I}(S) \subseteq \mathrm{I}(T)$ if $S \supseteq T$, and $\mathrm{I}(S \cup T) = \mathrm{I}(S) \cap \mathrm{I}(T)$. Clearly $\mathrm{I}\big(\mathrm{Z}_K(I)\big) \supseteq \sqrt{I}$ and $\mathrm{Z}_K(I) = \mathrm{Z}_K(\sqrt{I})$. (Since we only need to consider zeros of power series $f \in \boldsymbol{k}\lfloor X \rfloor$ in R^m, and not in the valuation ring of an extension of $\boldsymbol{k}$, we do not require "restricted W-structures" in analogy to Definition 2.13.)

7.6. **The Nullstellensatz for the Tate algebra.** *In this subsection we let $\mathcal{L} = \mathcal{L}_{\preceq}$, and we assume that $\boldsymbol{k}$ is algebraically closed unless noted otherwise.* Thus $\boldsymbol{k}$ (viewed as an $\mathcal{L}$-structure) is a model of ACVF. Let $y = (y_1, \dots, y_n)$ be a tuple of distinct $\mathcal{L}$-variables. Here is an analogue of Proposition 3.2:

Proposition 7.16. *Let $\varphi(y)$ be an $\mathcal{L}$-formula, $f = (f_1, \dots, f_n) \in \boldsymbol{k}\lfloor X \rfloor^n$, $\Omega \models$ ACVF, and $\sigma \colon \boldsymbol{k}\lfloor X \rfloor \to \Omega$ be a ring morphism such that $\sigma(R\lfloor X \rfloor) \preceq 1$, $\sigma(\mathfrak{m}) \prec 1$, and $\Omega \models \varphi(\sigma(f))$. Then $\boldsymbol{k} \models \varphi(f(a))$ for some $a \in R^m$.*

Proof. We proceed by induction on m. The case $m = 0$ follows from model completeness of ACVF since σ restricts to an $\mathcal{L}$-embedding $\boldsymbol{k} \to \Omega$. Suppose $m \geqslant 1$. Using Theorem 3.1, as in the proof of Proposition 3.2 we first arrange that φ is quantifier-free of the form

$$\bigwedge_{i \in I} P_i(y) = 0 \wedge Q(y) \neq 0 \wedge \bigwedge_{j \in J} R_j(y) \,\square_j\, S_j(y)$$

where I, J are finite index sets, $P_i, Q, R_j, S_j \in \mathbb{Z}[Y_1, \dots, Y_n]$, and each $\square_j$ is one of the symbols $\preceq$ or $\prec$. We also arrange that P_i, Q, R_j, S_j are distinct elements of $\{Y_1, \dots, Y_n\}$, and $f_1, \dots, f_n \neq 0$. Take some $d \in \mathbb{N}$, $d > 1$ such that $\tau_d(f_j)$ is regular in X_m, for $j = 1, \dots, n$, and replace f_j by $\tau_d(f_j)$ $(j = 1, \dots, n)$ and σ by $\sigma \circ \tau_d^{-1}$ to further arrange that f_j is regular in X_m, for $j = 1, \dots, n$. As usual let $X' = (X_1, \dots, X_{m-1})$. Lemma 7.12 then yields some 1-unit u_j in $\boldsymbol{k}\lfloor X \rfloor$ as well as a polynomial $w_j \in \boldsymbol{k}\lfloor X' \rfloor[X_m]$ such that $f_j = u_j w_j$, for $j = 1, \dots, n$. In Ω we have $\sigma(u_j) \sim 1$ since $\sigma(\mathfrak{m}R\lfloor X \rfloor) \prec 1$, and in $\boldsymbol{k}$ we have $u_j(a) \sim 1$ for each $a \in R^m$. Hence we may replace each f_j by w_j to arrange that $f_j = w_j$ is a polynomial. Now argue as in the proof of Proposition 3.2 with "$v \prec 1$" in the definition of ψ replaced by "$v \preceq 1$" and K, $\mathcal{O}$ replaced by $\boldsymbol{k}$, R, respectively. □

Corollary 7.17. *Let $\varphi(y)$ be an $\mathcal{L}_{\mathrm{R}}$-formula, $f \in \boldsymbol{k}\lfloor X\rfloor^n$, and $\sigma\colon \boldsymbol{k}\lfloor X\rfloor \to \Omega$ be a ring morphism to an algebraically closed field with $\Omega \models \varphi(\sigma(f))$. Then $\boldsymbol{k} \models \varphi(f(a))$ for some $a \in R^m$.*

Proof. Note that σ restricts to a field embedding $\boldsymbol{k} \to \Omega$; identify $\boldsymbol{k}$ with its image under σ. Let $A := \sigma(R\lfloor X\rfloor)$; then $R \subseteq A$ and $1 \notin \mathfrak{m}A$. Let $M \supseteq \mathfrak{m}A$ be a maximal ideal of A; then the local subring A_M of Ω lies over R. Take a valuation ring of Ω which lies over A_M, and hence over R, and equip Ω with the associated dominance relation. Then $\sigma(R\langle X\rangle) \preceq 1$, $\sigma(\mathfrak{m}) \prec 1$. Model completeness of the $\mathcal{L}_{\mathrm{R}}$-theory of algebraically closed fields allows us to replace Ω by a suitable extension to arrange $\Omega \models \mathrm{ACVF}$. Now use Proposition 7.16. □

Arguing as in the proof of Theorem 3.5, using Corollary 7.17 in place of Corollary 3.4, we obtain the familiar Nullstellensatz for $\boldsymbol{k}\langle X\rangle$. (Cf. [10, §7.1.2, Theorem 3]. This is a special case of a more general Nullstellensatz for power series rings over algebraically closed valued fields from [13, Proposition 5.2.7].)

Corollary 7.18. *Let I be an ideal of $\boldsymbol{k}\lfloor X\rfloor$; then $\mathrm{I}\big(\mathrm{Z}(I)\big) = \sqrt{I}$.*

We also note that Proposition 7.16 easily yields a fact about rational domains (cf. [10, §7.2.3]) which is in analogy to Corollary 6.22 above:

Proposition 7.19. *Let $f, g \in \boldsymbol{k}\lfloor X\rfloor$. Then*

$$|f(a)| \leqslant |g(a)| \text{ for all } a \in R^m \quad\Longleftrightarrow\quad f \in gR\lfloor X\rfloor.$$

Proof. We only need to show "⇒". Thus suppose $|f(a)| \leqslant |g(a)|$ for all $a \in R^m$; then $|f| \leqslant |g|$ by Lemma 7.1. To show $f \in gR\lfloor X\rfloor$ we can assume $g \neq 0$, and it then suffices to show $f \in g\boldsymbol{k}\lfloor X\rfloor$. Suppose otherwise, and let $A := \boldsymbol{k}\lfloor X\rfloor$, $F := \mathrm{Frac}(A)$; then $h := f/g \in F \setminus A$. Now the integral domain A is factorial by Lemma 7.11 and so integrally closed in F (see, e.g., [3, Lemma 1.3.11]). Hence [43, Theorem 10.4] yields a valuation ring $\mathcal{O}_F$ of F containing A but not h. The residue morphism $\pi\colon \mathcal{O}_F \to \boldsymbol{k}_F := \mathcal{O}_F/\mathcal{o}_F$ restricts to a field embedding $\boldsymbol{k} \to \boldsymbol{k}_F$, via which we identify $\boldsymbol{k}$ with a subfield of $\boldsymbol{k}_F$. Let $B := \pi(R\lfloor X\rfloor)$; then $R \subseteq B$ and $1 \notin \mathfrak{m}B$. Let M be a maximal ideal of B containing $\mathfrak{m}B$; then B_M is a local subring of $\boldsymbol{k}_F$ lying over R. Now [3, Proposition 3.1.13] (applied to B_M, $\boldsymbol{k}_F$ in place of A, K) and Lemma 1.3 yield a valuation ring $\mathcal{O}$ of F with $R\lfloor X\rfloor \subseteq \mathcal{O} \subseteq \mathcal{O}_F$ which lies over the valuation ring R of $\boldsymbol{k}$. Let Ω be some algebraically closed field extension of F equipped with the dominance relation associated to a valuation ring of Ω lying over $\mathcal{O}$; then $\Omega \models \mathrm{ACVF}$ and $R\lfloor X\rfloor \preceq 1$, $\mathfrak{m} \prec 1$. Proposition 7.16 now yields some $a \in R^m$ with $|f(a)| > |g(a)|$, a contradiction. □

Remark. The analogue of the previous proposition with $f, g \in \boldsymbol{k}[X]$ was studied in [48]. If the equivalence in Proposition 7.19 holds for all $f, g \in \boldsymbol{k}[X]$, even just when $m = 1$, then $\boldsymbol{k}$ necessarily is algebraically closed. This follows from [48, Theorem 3.1] and Corollary 7.7.

Corollary 7.20. *Let $f, g \in \boldsymbol{k}\lfloor X\rfloor$. Then*

$$|f(a)| < |g(a)| \text{ for all } a \in R^m \quad\Longleftrightarrow\quad f \in g\mathfrak{m}R\lfloor X\rfloor.$$

This follows from the remark after Lemma 7.1 combined with Proposition 7.19. We finish with another application of Proposition 7.16, a generalization of [30, Proposition 5.1]. Here it is convenient to switch from the absolute value $|\cdot|$ of $\boldsymbol{k}$ to the valuation

$$a \mapsto va := -\log|a| \colon \boldsymbol{k}^\times \to \Gamma = v(\boldsymbol{k}^\times) \subseteq \mathbb{R}$$

on $\boldsymbol{k}$. For $a = (a_1, \dots, a_m) \in \boldsymbol{k}^m$ we set $va := \big(v(a_1), \dots, v(a_m)\big) \in \Gamma^m$.

Proposition 7.21. *Let $\varphi(y)$ be an $\mathcal{L}_{\mathrm{R}}$-formula, $f \in \boldsymbol{k}\lfloor X \rfloor^n$, and*

$$S := \big\{a \in R^m : \boldsymbol{k} \models \varphi(f(a))\big\}.$$

Then $vS := \{va : a \in S\} \subseteq \Gamma^m$ is closed.

For the proof, similarly to Section 2.3, we let $\mathcal{L}_W$ be the expansion of $\mathcal{L}$ by a new n-ary function symbol g for each n and $g \in W_n$, and expand $\boldsymbol{k}$ to an $\mathcal{L}_W$-structure by interpreting each such function symbol g by the function $\boldsymbol{k}^n \to \boldsymbol{k}$ which agrees with $a \mapsto g(a)$ on R^n and is identically zero on $\boldsymbol{k}^n \setminus R^n$.

Proof of Proposition 7.21. Let β be an element of the closure of vS. Let $\boldsymbol{k}^*$ be an elementary extension of the $\mathcal{L}_W$-structure $\boldsymbol{k}$, with valuation $v^* \colon (\boldsymbol{k}^*)^\times \to \Gamma^*$, such that Γ^* contains some positive element smaller than every positive element of Γ. This yields a non-zero convex subgroup Δ^* of Γ^* such that $\Gamma \cap \Delta^* = \{0\}$. Now β is contained in the closure of $v^*(S^*)$ where S^* is defined like S with $\boldsymbol{k}$, R replaced by $\boldsymbol{k}^*$ and its valuation ring R^*, respectively. Thus we obtain some $a^* \in S^*$ such that $v^*(a^*) - \beta \in (\Delta^*)^m$. Let Ω be the field $\boldsymbol{k}^*$ equipped with the valuation ring of the Δ^*-coarsening of the valuation of $\boldsymbol{k}^*$. Then $\Omega \models \mathrm{ACVF}$, and the $\mathcal{L}$-reduct of $\boldsymbol{k}$ is a substructure of Ω with $v_\Omega(a^*) = \beta$. Let $\sigma \colon \boldsymbol{k}\lfloor X \rfloor \to \Omega$ be the ring morphism $g \mapsto g^*(a^*)$, where g^* denotes the interpretation of the function symbol g in the $\mathcal{L}_W$-structure $\boldsymbol{k}^*$. Then $\sigma(R\lfloor X \rfloor) \preceq 1$, $\sigma(\mathfrak{m}) \prec 1$. Let $b \in \boldsymbol{k}^m$ with $vb = \beta$. Then the tuple $(X, b, f) \in \boldsymbol{k}\lfloor X \rfloor^{m+m+n}$ satisfies $\sigma(X, b, f) = \big(a^*, b, f^*(a^*)\big)$, and hence $\Omega \models \psi\big(\sigma(X, b, f)\big)$ where $\psi = \psi(w, x, y)$ is the $\mathcal{L}$-formula

$$\varphi(y) \wedge w_1 \asymp x_1 \wedge \cdots \wedge w_m \asymp x_m.$$

Proposition 7.16 now yields $a \in R^m$ with $\boldsymbol{k} \models \psi\big(a, b, f(a)\big)$, so $\beta = va \in vS$. □

7.7. **The real holomorphy ring.** For use in the next subsection we recall the analogue of the Kochen ring in the real setting. *Throughout this section we let K be a field.* A valuation ring of K is said to be *real* if its residue field is formally real. If $\mathcal{O}$ is a real valuation ring of K then some ordering of K makes K an ordered field such that $\mathcal{O}$ is convex. (Baer-Krull [9, Theorem 10.1.10].) Hence every subring of K containing a real valuation ring of K is also a real valuation ring of K. Moreover:

Lemma 7.22. *Let $\mathcal{O}$ be a valuation ring of K and Δ be a convex subgroup of its value group. Then $\mathcal{O}$ is real iff the valuation ring of the Δ-specialization of $(K, \mathcal{O})$ is real.*

Suppose K is formally real (equivalently, has a real valuation ring). Let H_K be the *real holomorphy ring* of K, that is, the intersection of all real valuation rings of K. Schülting [58] showed that H_K is the subring of K generated by the elements $\frac{1}{1+f}$ where f is a sum of squares in K: $f = g_1^2 + \cdots + g_n^2$ ($g_i \in K$); alternatively, H_K consists of all $h \in K$ such that for some n, both $n + h$ and $n - h$ are a sum of squares in K. (Here as everywhere in this paper, n denotes a natural number.) For a subring A of K, the subring $H_K A$ of K generated by H_K and A is the intersection of all real valuation rings of K containing A [4, Lemma 1.12].

Lemma 7.23. *Let $\sigma\colon A \to L$ be a ring morphism to a formally real field where A is a regular integral domain with fraction field K. Let $f, g \in A$. Then*

$$f \in gH_K \implies \sigma(f) \in \sigma(g)H_L.$$

Proof. This is similar to the proof of Lemma 6.15, with A, H_K, H_L in place of R, Λ_K, Λ_L, respectively. Let $P := \ker \sigma$, a real prime ideal of A. As in the proof of that lemma we arrange that A is local with maximal ideal P, $L = A/P$, and $\sigma\colon A \to L$ is the residue morphism. Suppose $f \in gH_K$. Let $\mathcal{O}_L$ be a real valuation ring of L, with associated dominance relation $\preceq_L$ on L; we need to show that $\sigma(f) \preceq_L \sigma(g)$. Take a valuation ring $\mathcal{O}$ of K lying over R such that the natural inclusion $A \to \mathcal{O}$ induces an isomorphism $L = A/P \to \boldsymbol{k} = \mathcal{O}/\smallo$. (Lemma 1.2.) Let $\mathcal{O}_{\boldsymbol{k}}$ be the image of $\mathcal{O}_L$ under the isomorphism $L \to \boldsymbol{k}$. By Lemma 1.3 take a valuation ring $\mathcal{O}_0$ of K with $\mathcal{O}_0 \subseteq \mathcal{O}$ and a convex subgroup Δ_0 of its value group such that the Δ_0-specialization of $(K, \mathcal{O}_0)$ is $(\boldsymbol{k}, \mathcal{O}_{\boldsymbol{k}})$. So $\mathcal{O}_0 = \big\{h \in \mathcal{O} : \sigma(h) \preceq_L 1\big\}$, and $\mathcal{O}_0$ is real by Lemma 7.22, hence $H_K \subseteq \mathcal{O}_0 \subseteq \mathcal{O}$. Arguing as at the end of the proof of Lemma 6.15 with H_K in place of Λ_K, we conclude $\sigma(f) \preceq_L \sigma(g)$ as required. □

7.8. **The Nullstellensatz for real restricted analytic functions.** *In this subsection we assume $\boldsymbol{k}$ to be real closed.* Examples include each Hahn field $\boldsymbol{k} = \mathbb{R}(\!(t^\Gamma)\!)$ where Γ is a divisible ordered subgroup of the ordered additive group of reals, equipped with the absolute value $f \mapsto |f|\colon \boldsymbol{k} \to \mathbb{R}^{\geqslant}$ with $|f| = \mathrm{e}^{-vf}$ for $f \in \boldsymbol{k}^\times$, or the completion $\operatorname{cl}(\mathbb{R}[t^\Gamma])$ of the $\mathbb{R}$-subalgebra $\mathbb{R}[t^\Gamma]$ of $\boldsymbol{k}$, equipped with the restriction of the absolute value of $\boldsymbol{k}$. (See the examples after Corollary 2.15; here $\operatorname{cl}(\mathbb{R}[t^{\mathbb{Q}}])$ is the Levi-Civita field mentioned in the introduction.) Note that since R is henselian, it is a proper convex subring of $\boldsymbol{k}$. (See [3, Corollary 3.3.5 and Lemma 3.5.14].) Thus equipping $\boldsymbol{k}$ with the dominance relation associated to R makes $\boldsymbol{k}$ a model of RCVF. Let $\mathcal{L} = \mathcal{L}_{\mathrm{OR},\preceq}$ and $y = (y_1, \dots, y_n)$ be a tuple of distinct $\mathcal{L}$-variables.

Proposition 7.24. *Let $\varphi(y)$ be an $\mathcal{L}$-formula, $f \in \boldsymbol{k}\lfloor X \rfloor^n$, and $\sigma\colon \boldsymbol{k}\lfloor X \rfloor \to \Omega$ be a ring morphism, where $\Omega \models \mathrm{RCVF}$, such that $\sigma(R\lfloor X \rfloor) \preceq 1$, $\sigma(\mathfrak{m}) \prec 1$, and $\Omega \models \varphi(\sigma(f))$. Then $\boldsymbol{k} \models \varphi(f(a))$ for some $a \in R^m$.*

Proof. Induction on m as in the proof of Proposition 7.16. The case $m = 0$ follows from model completeness of RCVF. Suppose $m \geqslant 1$. By Theorem 4.1 we arrange that φ has the form

$$P(y) = 0 \wedge \bigwedge_{i \in I} Q_i(y) > 0 \wedge \bigwedge_{j \in J} R_j(y) \,\square_j\, S_j(y)$$

where I, J are finite, $P, Q_i, R_j, S_j \in \mathbb{Z}[Y_1, \dots, Y_n]$, and each $\square_j$ is $\preceq$ or $\prec$. As in the proof of Proposition 7.16 we also arrange that P, Q_i, R_j, S_j are distinct elements of $\{Y_1, \dots, Y_n\}$ and $f_1, \dots, f_n$ are all regular in X_m. Take a 1-unit $u_j \in R\lfloor X \rfloor$ and some $w_j \in \boldsymbol{k}\lfloor X' \rfloor[X_m]$, where $X' = (X_1, \dots, X_{m-1})$, such that $f_j = u_j w_j$. Then $\sigma(u_j) \sim 1$ since $\sigma(\mathfrak{m}R\lfloor X \rfloor) \prec 1$, hence also $\sigma(u_j) > 0$. Thus we may arrange that each $f_j = w_j$ is a polynomial and argue as in the proof of Proposition 7.16. □

In Lemma 7.25 and its corollary, Ω is an ordered field and $\sigma\colon \boldsymbol{k}\lfloor X \rfloor \to \Omega$ is a ring morphism.

Lemma 7.25. *Equip Ω with the dominance relation associated to the convex hull of $\sigma(R\lfloor X \rfloor)$ in Ω. Then $\sigma(\mathfrak{m}) \prec 1$.*

Proof. Let $a \in \mathfrak{m}$, $a > 0$, and $f \in R\lfloor X \rfloor$. Then $g := 1 - af \in 1 + \mathfrak{m}R\lfloor X \rfloor$ is a square in $R\lfloor X \rfloor$ by Corollary 7.15, thus $\sigma(g) > 0$ and so $\sigma(f) < \sigma(a^{-1})$. Since this holds for all $f \in R\lfloor X \rfloor$, we obtain $1 \prec \sigma(a^{-1})$ and thus $\sigma(a) \prec 1$ as required. □

Corollary 7.26. *Let $\varphi(y)$ be an $\mathcal{L}_{\mathrm{OR}}$-formula, $f \in \boldsymbol{k}\lfloor X \rfloor^n$, and Ω be real closed with $\Omega \models \varphi(\sigma(f))$. Then $\boldsymbol{k} \models \varphi(f(a))$ for some $a \in R^m$.*

Proof. Equip Ω with the dominance relation associated to the convex hull of the subring $\sigma(R\lfloor X \rfloor)$ in Ω. Then $\sigma(\mathfrak{m}) \prec 1$ by the lemma above. Replace Ω by a suitable extension (using model completeness of the $\mathcal{L}_{\mathrm{OR}}$-theory of real closed fields) to arrange $\Omega \models \mathrm{RCVF}$. Now the corollary follows from Proposition 7.24. □

As in the proof of Corollary 4.6 respectively Theorem 4.7, using Corollary 7.26 instead of Corollary 4.5, we now obtain Theorem D from the introduction:

Corollary 7.27 (real restricted analytic Positivstellensatz)**.** *For each $f \in \boldsymbol{k}\lfloor X \rfloor$ we have $f(a) \geqslant 0$ for all $a \in R^m$ iff there are $g \in \boldsymbol{k}\lfloor X \rfloor \setminus \{0\}$ and $h_1, \dots, h_k \in \boldsymbol{k}\lfloor X \rfloor$ such that $fg^2 = h_1^2 + \cdots + h_k^2$.*

Corollary 7.28 (real restricted analytic Nullstellensatz)**.** *Let I be an ideal of $\boldsymbol{k}\lfloor X \rfloor$; then $\mathrm{I}(\mathrm{Z}(I)) = \sqrt[\mathrm{r}]{I}$.*

As in [52, Proposition 6.4], the previous corollary implies a Łojasiewicz Inequality:

Corollary 7.29. *Let $f, g \in \boldsymbol{k}\lfloor X \rfloor$ such that $\mathrm{Z}(f) \supseteq \mathrm{Z}(g)$. Then there are $c \in \mathbb{R}^{\geqslant}$ and $k \geqslant 1$ such that $|f(a)|^k \leqslant c|g(a)|$ for each $a \in R^m$.*

Proof. The previous corollary applied to $I = g\boldsymbol{k}\lfloor X \rfloor$ yields $b_1, \dots, b_l, h \in \boldsymbol{k}\lfloor X \rfloor$ and $k \geqslant 1$ such that $f^{2k} + b_1^2 + \cdots + b_l^2 = gh$. So for each $a \in R^m$ we have $g(a)h(a) \geqslant f^{2k}(a) \geqslant 0$ and thus $c|g(a)| \geqslant |g(a)h(a)| \geqslant |f(a)|^{2k}$ for $c := |h|$. □

To show Theorem E, we restrict to the case $\boldsymbol{k}\lfloor X \rfloor = \boldsymbol{k}\langle X \rangle$. We let $F := \mathrm{Frac}(\boldsymbol{k}\langle X \rangle)$ and consider the real holomorphy ring H_F of F. The value group of $\boldsymbol{k}$ being archimedean, we have $R = H_{\boldsymbol{k}} \subseteq H_F$. We also have $\mathfrak{m}R\langle X \rangle \subseteq H_F$, since for $f \in \mathfrak{m}R\langle X \rangle$, $1 \pm f$ is a square in $R\langle X \rangle$ by Corollary 7.15. Hence $R\langle X \rangle^\times \subseteq H_F^\times$.

Let also $\mathcal{O}_F := \{f \in F : |f| \leqslant 1\}$ be the valuation ring of the Gauss norm on F, with maximal ideal $\mathcal{o}_F = \{f \in F : |f| < 1\}$. The residue field of $\mathcal{O}_F$ is the formally real field $\overline{R}(X)$; hence $H_F \subseteq \mathcal{O}_F$. The following proposition characterizes the elements of the subring $H_F R\langle X \rangle$ of $\mathcal{O}_F$:

Proposition 7.30. *Let $f, g \in \boldsymbol{k}\langle X \rangle$. Then*

$$|f(a)| \leqslant |g(a)| \text{ for all } a \in R^m \quad \Longleftrightarrow \quad f \in gH_F R\langle X \rangle.$$

Proof. Since $\boldsymbol{k}\langle X \rangle$ is regular (see the remark after Lemma 7.11), the backward direction follows from Lemma 7.23 applied to the ring morphisms $h \mapsto h(a) \colon \boldsymbol{k}\langle X \rangle \to \boldsymbol{k}$ ($a \in R^m$), and the fact that $|h(a)| \leqslant 1$ for each $h \in R\langle X \rangle$, $a \in R^m$. For the forward direction we argue as in the proof of Proposition 7.19. Suppose $|f(a)| \leqslant |g(a)|$ for all $a \in R^m$ but $f \notin gH_F R\langle X \rangle$. Then $g \neq 0$. Take a real valuation ring $\mathcal{O}_1$ of F containing $R\langle X \rangle$ but not $h := f/g$. Turn F into an ordered field such that $\mathcal{O}_1$ is convex. Let $\mathcal{O}$ be the convex hull of $R\langle X \rangle$ in F; then $\mathcal{O} \subseteq \mathcal{O}_1$, hence $h \notin \mathcal{O}$. Equip F with the dominance relation associated to $\preceq$, and take $\Omega \models \mathrm{RCVF}$ extending F. Then in Ω we have $R\langle X \rangle \preceq 1$, and $\mathfrak{m} \prec 1$ by Lemma 7.25, so Proposition 7.24 yields an $a \in R^m$ with $|f(a)| > |g(a)|$, a contradiction. □

With Proposition 7.24 in place, we can also use it in the same way as Proposition 7.16 to prove the following real analogue of Proposition 7.21. As in that proposition let $v\colon \boldsymbol{k}^\times \to \Gamma$ be the valuation on $\boldsymbol{k}$ associated to $|\cdot|$.

Proposition 7.31. *Let $\varphi(y)$ be an $\mathcal{L}_{\mathrm{R}}$-formula, $f \in \boldsymbol{k}\lfloor X\rfloor^n$, and*

$$S := \big\{a \in R^m : \boldsymbol{k} \models \varphi(f(a))\big\}.$$

Then $vS := \{va : a \in S\} \subseteq \Gamma^m$ is closed.

See [30, Proposition 5.3] for a weaker result. The preceding proposition now yields a version of Corollary 7.20 in the present setting:

Corollary 7.32. *Let $f, g \in \boldsymbol{k}\langle X\rangle$. Then $|f(a)| < |g(a)|$ for every $a \in R^m$ iff $f \in g\mathfrak{m}H_F R\langle X\rangle$.*

Proof. The backwards direction here is clear from that in Proposition 7.30. For the converse suppose $|f(a)| < |g(a)|$ for all $a \in R^m$. Applying the proposition above to

$$S := \big\{(a, b) \in R^m \times R : f(a) = g(a)b\big\}$$

implies that $\big\{|f(a)/g(a)| : a \in R^m\big\} \subseteq |\boldsymbol{k}|$ is closed. This yields an $\varepsilon \in \mathfrak{m}$ such that $|f(a)| \leqslant |\varepsilon g(a)|$ for all $a \in R$. Then $f \in \varepsilon g H_F R\langle X\rangle$ by Proposition 7.30. ☐

The combination of Proposition 7.30 and Corollary 7.32 now yields Theorem E from the introduction.

7.9. **The Nullstellensatz for p-adic restricted analytic functions.** *In this subsection we assume $\boldsymbol{k} = \mathbb{Q}_p$.* We first note:

Lemma 7.33. *Let Ω be a p-valued field and $\sigma\colon \mathbb{Q}_p\lfloor X\rfloor \to \Omega$ be a ring morphism. Then $\sigma(\mathbb{Z}_p\lfloor X\rfloor) \preceq_p 1$ and $\sigma(p) \prec_p 1$.*

Proof. Note that σ restricts to an embedding of $\mathbb{Q}_p$ into Ω; hence the p-valuation of Ω restricts to the unique p-valuation of $\sigma(\mathbb{Q}_p)$, so $\sigma(p) \prec_p 1$. Now let $g \in \mathbb{Z}_p\lfloor X\rfloor$. Suppose first that p is odd. Then $1 + pg^2$ is a square in $\mathbb{Q}_p\lfloor X\rfloor$, by Corollary 7.15, hence $1 + p\sigma(g)^2$ is a square in Ω, so $\sigma(g) \preceq_p 1$. For $p = 2$ we note that $1 + pg^3$ is a cube in $\mathbb{Q}_p\lfloor X\rfloor$, and as before this yields $\sigma(g) \preceq_p 1$. ☐

We also let $\mathcal{L} = \mathcal{L}_{\mathrm{Mac}}$ and $y = (y_1, \dots, y_n)$ be a tuple of distinct $\mathcal{L}$-variables. We now have a restricted analytic analogue of Proposition 6.18:

Proposition 7.34. *Let $\varphi(y)$ be an $\mathcal{L}$-formula, $f = (f_1, \dots, f_n) \in \mathbb{Q}_p\lfloor X\rfloor^n$, $\Omega \models p\,\mathrm{CF}$, and $\sigma\colon \mathbb{Q}_p\lfloor X\rfloor \to \Omega$ be a ring morphism such that $\Omega \models \varphi(\sigma(f))$. Then $\mathbb{Q}_p \models \varphi(f(a))$ for some $a \in \mathbb{Z}_p^m$.*

Proof. By induction on m in a similar way as in the proof of Proposition 7.16. The case $m = 0$ holds by model completeness of $p\,\mathrm{CF}$. Suppose $m \geqslant 1$. As in the proof of Proposition 6.18, using Theorem 5.10 and the argument to eliminate ${}^{-1}$ in the proof of Lemma 5.11 in place of Corollary 5.21, we arrange that φ has the form

$$P(y) = 0 \wedge \bigwedge_{i \in I} \mathrm{P}_{k_i}\big(Q_i(y)\big) \wedge \bigwedge_{j \in J} R_j(y) \preceq_p S_j(y)$$

where I, J are finite, $P, Q_i, R_j, S_j \in \mathbb{Z}[Y_1, \dots, Y_n]$, $k_i \geqslant 1$. As in the proof of Proposition 7.16 we arrange that P_i, Q, R_j, S_j are distinct elements of $\{Y_1, \dots, Y_n\}$, and $f_1, \dots, f_n$ are regular in X_m. Lemma 7.12 then yields $u_j \in \mathbb{Z}_p\lfloor X\rfloor^\times$ and $w_j \in \mathbb{Q}_p\lfloor X'\rfloor[X_m]$ such that $f_j = u_j w_j$ $(j = 1, \dots, n)$.

Let $k \geqslant 1$ and $\lambda_1, \dots, \lambda_N \in \mathbb{Z}$ ($N \geqslant 1$) be representatives for the cosets of the subgroup $(\mathbb{Q}_p^\times)^k$ of $\mathbb{Q}_p^\times$; then for distinct variables u, w we have

$$p\,\mathrm{CF} \models \mathrm{P}_k(uw) \leftrightarrow \bigvee_{\lambda_i\lambda_j \in (\mathbb{Q}_p^\times)^n} \big(\mathrm{P}_k(\lambda_i u) \wedge \mathrm{P}_k(\lambda_j w)\big).$$

Moreover, $\sigma(u_j) \sim 1$ in Ω, since $\sigma(p\mathbb{Z}_p\langle X\rangle) \prec 1$ (Lemma 7.33), and $u_j(a) \sim 1$ for $a \in \mathbb{Z}_p^m$. Hence we can further arrange that for each $j = 1, \dots, n$, either $f_j \in \mathbb{Z}_p\langle X\rangle^\times$ or $f_j \in \mathbb{Q}_p\lfloor X'\rfloor[X_m]$. Next, let $k \geqslant 1$; if we take $K \in \mathbb{N}$ so large that $1 + p^K\mathbb{Z}_p \subseteq (\mathbb{Q}_p^\times)^k$, and let $\mu_1, \dots, \mu_M \in \mathbb{Z}$ ($M \geqslant 1$) be representatives for all congruence classes modulo p^K of elements of $(\mathbb{Z}_p^\times)^k$, then

$$p\,\mathrm{CF} \models \big(u \asymp_p 1 \wedge \mathrm{P}_k(u)\big) \leftrightarrow \bigvee_i (u - \mu_i) \preceq_p p^K.$$

Using this remark we finally arrange that each f_j is a polynomial in $\mathbb{Q}_p\lfloor X'\rfloor[X_m]$. We now finish the inductive step as in the proof of Proposition 7.16. □

By Lemma 7.11, $\mathbb{Q}_p\lfloor X\rfloor$ is regular, so $F := \mathrm{Frac}(\mathbb{Q}_p\lfloor X\rfloor)$ is formally p-adic, and for each $a \in \mathbb{Z}_p^m$, the kernel of $f \mapsto f(a)\colon \mathbb{Q}_p\lfloor X\rfloor \to \mathbb{Q}_p$ is a p-adic prime ideal of $\mathbb{Q}_p\lfloor X\rfloor$. (Corollary 6.14.) We obtain a restricted analytic version of Corollary 6.22:

Corollary 7.35 (restricted p-adic analytic Hilbert's 17th Problem)**.**

$$\Lambda_F = \left\{ \frac{f}{g} : f, g \in \mathbb{Q}_p\lfloor X\rfloor,\ g \neq 0,\ |f(a)|_p \leqslant |g(a)|_p \text{ for all } a \in \mathbb{Z}_p^m \right\}.$$

This is proved just like Corollary 6.22, using Proposition 7.34 in place of Corollary 6.21. Similarly to Theorem 6.24, using again Proposition 7.34 instead of Corollary 6.21, we also show:

Corollary 7.36 (restricted p-adic analytic Nullstellensatz)**.** *Let I be an ideal of $\mathbb{Q}_p\lfloor X\rfloor$; then $\mathrm{I}\big(\mathrm{Z}(I)\big) = \sqrt[p]{I}$.*

The previous two corollaries apply to $\mathbb{Q}_p\lfloor X\rfloor = \mathbb{Q}_p\langle X\rangle$ and $\mathbb{Q}_p\lfloor X\rfloor = \mathbb{Q}_p\langle X\rangle^{\mathrm{a}}$. For each $f \in \mathbb{Q}_p\{X\}$ there is some $k \geqslant 1$ such that $f(p^k X) \in \mathbb{Q}_p\langle X\rangle$. Hence from the case $\mathbb{Q}_p\lfloor X\rfloor = \mathbb{Q}_p\langle X\rangle$ of Corollaries 7.35 and 7.36 we also deduce once again Theorems A and B from the introduction (but not Theorem C, about $\mathbb{Q}_p[[X]]$, the proof of which seems to crucially require the use of $p\,\mathrm{CVF}$). We finish with an immediate application of Lemma 6.15 and Corollary 7.36: a special case of the p-adic analytic Łojasiewicz Inequality of Denef and van den Dries [17, Theorem 3.37]:

Corollary 7.37. *Let $f, g \in \mathbb{Q}_p\langle X\rangle$ be such that $\mathrm{Z}(f) \supseteq \mathrm{Z}(g)$. Then there is some $k \geqslant 1$ such that $|f(a)|_p^k \leqslant |g(a)|_p$ for all $a \in \mathbb{Z}_p^m$.*

References

1. M. Aschenbrenner, *Ideal membership in polynomial rings over the integers,* J. Amer. Math. Soc. **17** (2004), no. 2, 407–441.
2. ———, *An effective Weierstrass Division Theorem,* manuscript, 2007.
3. M. Aschenbrenner, L. van den Dries, J. van der Hoeven, *Asymptotic Differential Algebra and Model Theory of Transseries,* Annals of Mathematics Studies, vol. 195, Princeton University Press, Princeton, NJ, 2017.
4. E. Becker, *The real holomorphy ring and sums of 2nth powers,* in: J.-L. Colliot-Thélène et al. (eds.), *Géométrie Algébrique Réelle et Formes Quadratiques,* pp. 139–181, Lecture Notes in Mathematics, vol. 959, Springer-Verlag, Berlin-New York, 1982.

5. L. Bélair, *Substructures and uniform elimination for p-adic fields,* Ann. Pure Appl. Logic **39** (1988), no. 1, 1–17.
6. ———, *Anneaux p-adiquement clos et anneaux de fonctions définissables,* J. Symbolic Logic **56** (1991), no. 2, 539–553.
7. W. Bertram, H. Glöckner, K.-H. Neeb, *Differential calculus over general base fields and rings,* Expo. Math. **22** (2004), no. 3, 213–282.
8. A. Bleybel, *p-adically closed fields with nonstandard analytic structure,* J. Symbolic Logic **75** (2010), no. 3, 802–816.
9. J. Bochnak, M. Coste, M.-F. Roy, *Real Algebraic Geometry,* Ergeb. Math. Grenzgeb., vol. 36, Springer-Verlag, Berlin, 1998.
10. S. Bosch, U. Güntzer, R. Remmert, *Non-Archimedean Analysis. A Systematic Approach to Rigid Analytic Geometry*, Grundlehren der Mathematischen Wissenschaften, vol. 261, Springer-Verlag, Berlin, 1984.
11. Z. Chatzidakis, *Introductory notes on the model theory of valued fields,* in: R. Cluckers et al. (eds.), *Motivic Integration and its Interactions with Model Theory and Non-Archimedean Geometry,* I, pp. 35–79, London Math. Soc. Lecture Note Ser., vol. 383, Cambridge Univ. Press, Cambridge, 2011.
12. G. Cherlin, M. A. Dickmann, *Real closed rings.* II. *Model theory,* Ann. Pure Appl. Logic **25** (1983), no. 3, 213–231.
13. R. Cluckers, L. Lipshitz, *Fields with analytic structure,* J. Eur. Math. Soc. (JEMS) **13** (2011), no. 4, 1147–1223.
14. P. Cubides Kovacsics, D. Haskell, *Real closed valued fields with analytic structure,* Proc. Edinb. Math. Soc. (2) **63** (2020), no. 1, 249–261.
15. F. Delon, *Quelques propriétés des corps valués en théorie des modèles,* Thèse d'État, Université Paris VII, Paris, 1982.
16. J. Denef, *The rationality of the Poincaré series associated to the p-adic points on a variety,* Invent. Math. **77** (1984), no. 1, 1–23.
17. J. Denef, L. van den Dries, *p-adic and real subanalytic sets,* Ann. of Math. (2) **128** (1988), no. 1, 79–138.
18. J. Denef, L. Lipshitz, *Ultraproducts and approximation in local rings.* II, Math. Ann. **253** (1980), no. 1, 1–28.
19. M. A. Dickmann, *On polynomials over real closed rings,* in: L. Pacholski et al. (eds.), *Model Theory of Algebra and Arithmetic,* pp. 117–135, Lecture Notes in Mathematics, vol. 834, Springer, Berlin, 1980.
20. L. van den Dries, *A specialization theorem for p-adic power series converging on the closed unit disc,* J. Algebra **73** (1981), no. 2, 613–623.
21. ———, *On the elementary theory of restricted elementary functions,* J. Symbolic Logic **53** (1988), no. 3, 796–808.
22. ———, *Lectures on the model theory of valued fields,* in: D. Macpherson, C. Toffalori (eds.), *Model Theory in Algebra, Analysis and Arithmetic,* pp. 55–157, Lecture Notes in Mathematics, vol. 2111, Springer-Verlag, Heidelberg.
23. L. van den Dries, A. Macintyre, D. Marker, *The elementary theory of restricted analytic fields with exponentiation,* Ann. of Math. (2) **140** (1994), no. 1, 183–205.
24. A. Fekak, A. Srhir, *On the p-adic Nullstellensatz,* Bull. Polish Acad. Sci. Math. **50** (2002), no. 1, 69–76.
25. ———, *On the p-adic algebra and its applications,* Int. Math. Forum **4** (2009), no. 25–28, 1267–1280.
26. H. Glöckner, *Comparison of some notions of C^k-maps in multi-variable non-Archimedian analysis,* Bull. Belg. Math. Soc. Simon Stevin **14** (2007), no. 5, 877–904.
27. H. Grauert, R. Remmert, *Analytische Stellenalgebren,* unter Mitarbeit von O. Riemenschneider, Grundlehren der mathematischen Wissenschaften, vol. 176, Springer-Verlag, Berlin-New York, 1971.
28. S. Greco, P. Salmon, *Topics in $\mathfrak{m}$-adic Topologies,* Ergebnisse der Mathematik und ihrer Grenzgebiete, vol. 58, Springer-Verlag, New York-Berlin, 1971.
29. N. Guzy, *p-convexly valued rings,* J. Pure Appl. Algebra **199** (2005), no. 1–3, 111–131.
30. D. Haskell, Y. Yaffe, *Ganzstellensätze in theories of valued fields,* J. Math. Log. **8** (2008), no. 1, 1–22.

31. M. Jarden, P. Roquette, *The Nullstellensatz over $\mathfrak{p}$-adically closed fields,* J. Math. Soc. Japan **32** (1980), no. 3, 425–460.
32. K. Kedlaya, *The algebraic closure of the power series field in positive characteristic,* Proc. Amer. Math. Soc. **129** (2001), no. 12, 3461–3470.
33. ———, *On the algebraicity of generalized power series,* Beitr. Algebra Geom. **58** (2017), no. 3, 499–527.
34. K. Kedlaya, B. Poonen, *Orbits of automorphism groups of fields,* J. Algebra **293** (2005), no. 1, 167–184.
35. S. Kochen, *Integer valued rational functions over the p-adic numbers: A p-adic analogue of the theory of real fields,* in: W. J. LeVeque, E. G. Straus (eds.), *Proceedings of Symposia in Pure Mathematics,* Vol. XII, pp. 57–73, American Mathematical Society, Providence, R.I., 1969.
36. J.-P. Lafon, *Anneaux henséliens,* Bull. Soc. Math. France **91** (1963), 77–107.
37. ———, *Séries formelles algébriques,* C. R. Acad. Sci. Paris **260** (1965), 3238–3241.
38. T. Y. Lam, *Introduction to Quadratic Forms over Fields,* Graduate Studies in Mathematics, vol. 67, American Mathematical Society, Providence, RI, 2005.
39. G. Lassalle, *Sur le théorème des zéros différentiables,* in: O. Burlet, F. Ronga (eds.), *Singularités d'Applications Différentiables,* pp. 70–97, Lecture Notes in Mathematics, vol. 535, Springer-Verlag, Berlin-New York, 1976.
40. N. Lavi, *Positivstellensatz for semi-algebraic sets in real closed valued fields,* Proc. Amer. Math. Soc. **143** (2015), no. 10, 4479–4484.
41. A. H. Lightstone, A. Robinson, *Nonarchimedean Fields and Asymptotic Expansions,* North-Holland Mathematical Library, vol. 13, North-Holland Publishing Co., Amsterdam-Oxford; American Elsevier Publishing Co., Inc., New York, 1975.
42. A. Macintyre, *On definable subsets of p-adic fields,* J. Symbolic Logic **41** (1976), no. 3, 605–610.
43. H. Matsumura, *Commutative Ring Theory,* 2nd ed., Cambridge Studies in Advanced Mathematics, vol. 8, Cambridge University Press, Cambridge, 1989.
44. J. Merrien, *Idéaux de l'anneau des séries formelles á coefficients réels et variétés associées,* J. Math. Pures Appl. (9) **51** (1972), 169–187.
45. ———, *Un théorème des zéros pour les idéaux de séries formelles à coefficients réels,* C. R. Acad. Sci. Paris Sér. A-B **276** (1973), A1055–A1058.
46. M. Nagata, *Local Rings,* Interscience Tracts in Pure and Applied Mathematics, no. 13, John Wiley & Sons, Inc., New York-London, 1962.
47. A. Prestel, C. Delzell, *Mathematical Logic and Model Theory,* Universitext, Springer, London, 2011.
48. A. Prestel, C. Ripoll, *Integral-valued rational functions on valued fields,* Manuscripta Math. **73** (1991), no. 4, 437–452.
49. A. Prestel, P. Roquette, *Formally p-adic Fields*, Lecture Notes in Mathematics, vol. 1050, Springer-Verlag, Berlin-New York, 1984.
50. J.-J. Risler, *Une caractérisation des idéaux des variétés algebriques réelles,* C. R. Acad. Sci. Paris Sér. A–B **271** (1970), A1171–A1173.
51. ———, *Un théorème des zéros en géométrie analytique réelle,* C. R. Acad. Sci. Paris Sér. A–B **274** (1972), A1488–A1490.
52. ———, *Le théorème des zéros en géométries algébrique et analytique réelles,* Bull. Soc. Math. France **104** (1976), no. 2, 113–127.
53. J. W. Robbin, *Evaluation fields for power series.* I. *The nullstellensatz,* J. Algebra **57** (1979), no. 1, 196–211.
54. ———, *Evaluation fields for power series.* II. *The rellnullstellensatz,* J. Algebra **57** (1979), no. 1, 212–222.
55. A. Robinson, *Complete Theories*, North-Holland Publishing Co., Amsterdam, 1956.
56. ———, *Germs,* in: W. A. J. Luxemburg (ed.), *Applications of Model Theory to Algebra, Analysis, and Probability,* pp. 138–149, Holt, Rinehart and Winston, New York-Montreal, Que.-London, 1969.
57. W. Rückert, *Zum Eliminationsproblem der Potenzreihenideale,* Math. Ann. **107** (1933), 259–281.
58. H.-W. Schülting, *Über die Erzeugendenanzahl invertierbarer Ideale in Prüferringen,* Comm. Algebra **7** (1979), no. 13, 1331–1349.

59. S. de Smedt, *p-adic continuously differentiable functions of several variables,* Collect. Math. **45** (1994), no. 2, 137–152.
60. A. Srhir, *Idéaux p-adiques de p-rang d et le théorème des zéros p-adiques,* C. R. Acad. Sci. Paris Sér. I Math. **333** (2001), no. 7, 605–610.
61. ______, *p-adic ideals of p-rank d and the p-adic Nullstellensatz,* J. Pure Appl. Algebra **180** (2003), no. 3, 299–311.
62. V. Weispfenning, *Two model theoretic proofs of Rückert's Nullstellensatz,* Trans. Amer. Math. Soc. **203** (1975), 331–342.
63. ______, *Nullstellensätze—a model theoretic framework,* Z. Math. Logik Grundlagen Math. **23** (1977), no. 6, 539–545.
64. ______, *Quantifier elimination and decision procedures for valued fields,* in: G. H. Müller, M. M. Richter (eds.), *Models and Sets* (*Aachen, 1983*), pp. 419–472, Lecture Notes in Math., vol. 1103, Springer, Berlin, 1984.

Kurt Gödel Research Center for Mathematical Logic, Universität Wien, 1090 Wien, Austria
Email address: matthias.aschenbrenner@univie.ac.at

Département de Mathématique, Faculté des Sciences, Université Ibn Tofail, Kénitra, Morocco
Email address: ahmedsrhir@hotmail.com