TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 350, Number 1, January 1998, Pages 55–85
S 0002-9947(98)01630-4

RUMELY'S LOCAL GLOBAL PRINCIPLE FOR ALGEBRAIC P$\mathcal{S}$C FIELDS OVER RINGS

MOSHE JARDEN AND AHARON RAZON

To Peter Roquette with gratitude

Abstract. Let $\mathcal{S}$ be a finite set of rational primes. We denote the maximal Galois extension of $\mathbb{Q}$ in which all $p \in \mathcal{S}$ totally decompose by N. We also denote the fixed field in N of e elements $\sigma_1, \ldots, \sigma_e$ in the absolute Galois group $G(\mathbb{Q})$ of $\mathbb{Q}$ by $N(\boldsymbol{\sigma})$. We denote the ring of integers of a given algebraic extension M of $\mathbb{Q}$ by $\mathbb{Z}_M$. We also denote the set of all valuations of M (resp., which lie over S) by $\mathcal{V}_M$ (resp., $\mathcal{S}_M$). If $v \in \mathcal{V}_M$, then $O_{M,v}$ denotes the ring of integers of a Henselization of M with respect to v.

We prove that for almost all $\boldsymbol{\sigma} \in G(\mathbb{Q})^e$, the field $M = N(\boldsymbol{\sigma})$ satisfies the following local global principle: Let V be an affine absolutely irreducible variety defined over M. Suppose that $V(O_{M,v}) \neq \varnothing$ for each $v \in \mathcal{V}_M \backslash \mathcal{S}_M$ and $V_{\mathrm{sim}}(O_{M,v}) \neq \varnothing$ for each $v \in \mathcal{S}_M$. Then $V(O_M) \neq \varnothing$.

We also prove two approximation theorems for M.

Introduction

Hilbert's tenth problem asks for the existence of an algorithm to solve **diophantine equations**, that is, equations with coefficients in $\mathbb{Z}$ whose solutions are sought in $\mathbb{Z}$. The development of recursion theory since 1930 and works of Martin Davis, Hilary Putnam, and Julia Robinson finally led Juri Matijasevich in 1972 to a negative answer to that problem. This invoked Julia Robinson to ask whether Hilbert's tenth problem has a positive solution over the ring $\tilde{\mathbb{Z}}$ of all algebraic integers. Indeed, on page 367 of her joint paper [DMR] with Davis and Matijasevich she guessed that there should be one.

Using capacity theory, Rumely [Ru1] and [Ru2] proved in 1987 a local global principle for $\tilde{\mathbb{Z}}$: If an absolutely irreducible affine variety V over $\tilde{\mathbb{Q}}$ has an integral point over every completion of $\tilde{\mathbb{Q}}$, then V has a point with coordinates in $\tilde{\mathbb{Z}}$. This led Rumely to an algorithm for solving diophantine problems over $\tilde{\mathbb{Z}}$.

Moret-Bailly [MB1], [MB2], [MB3] reproved Rumely's theorem in 1988–89 with methods of algebraic geometry.

Received by the editors June 14, 1994 and, in revised form, August 1, 1995.

1991 *Mathematics Subject Classification.* Primary 11R23.

Key words and phrases. PAC field over rings, P$\mathcal{S}$C fields over rings, local global principle, global fields, absolute Galois group, Haar measure, valuations, Henselian fields, field of totally $\mathcal{S}$-adic numbers.

This research was supported by The Israel Science Foundation administered by The Israel Academy of Sciences and Humanities.

The authors thank Joachim Schmid for useful remarks.

In a conference on model theory in Oberwolfach, 1990, Roquette et al. [Ro2] presented a proof of Rumely's local global principle which uses results from algebraic number theory, the theory of algebraic functions of one variable, but not the theory of analytic functions as in Rumely's original proof.

A predecessor to [Ro2] and indeed an important ingredient in the proof of [Ro2] is the density theorem of Cantor and Roquette [CaR]. The latter theorem generalizes and strengthens a theorem of Skolem from 1934: Let f be a **primitive polynomial** in $\tilde{\mathbb{Z}}[X_1, \ldots, X_n]$ (i.e., the coefficients of f generate $\tilde{\mathbb{Z}}$). Then, there exists $\mathbf{x} \in \tilde{\mathbb{Z}}^n$ such that $f(\mathbf{x})$ is a unit of $\tilde{\mathbb{Z}}$. Cantor and Roquette handled several rational functions simultaneously, and proved, under appropriate conditions, not only the existence of $\mathbf{x}$, but also that the set of such $\mathbf{x}$'s is dense in $\tilde{\mathbb{Z}}^n$, in an appropriate topology.

This density gave the first author enough flexibility to generalize the theorem of Skolem-Cantor-Roquette to rings of integers of other algebraic fields. To explain the latter objects, recall that the absolute Galois group $G(\mathbb{Q})$ of $\mathbb{Q}$ is equipped with a Haar measure. For each $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_e) \in G(\mathbb{Q})^e$ we denote the fixed field of $\sigma_1, \ldots, \sigma_e$ by $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$. Let $\tilde{\mathbb{Z}}(\boldsymbol{\sigma})$ be the ring of integers of $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$. It is known that $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$ is a **PAC** field for almost all $\boldsymbol{\sigma} \in G(\mathbb{Q})^e$. That is, every nonempty absolutely irreducible variety defined over $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$ has a $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$-rational point [Ja1] or [FrJ, Thm. 16.18]. A combination of the technique used to prove the latter theorem with the technique of Cantor-Roquette then proves the density theorem, hence Skolem's theorem, for almost all rings $\tilde{\mathbb{Z}}(\boldsymbol{\sigma})$ [Ja2].

In his closing remarks to the series of talks in Oberwolfach about Rumely's local global principle, Roquette mentioned the manuscript [Ja2], and challenged the first author to generalize Rumely's local global principle from the ring $\tilde{\mathbb{Z}}$ to almost all the rings $\tilde{\mathbb{Z}}(\boldsymbol{\sigma})$.

The keystone to the local global principle is Rumely's existence theorem. Given a smooth irreducible curve Γ over $\tilde{\mathbb{Q}}_p$ and a p-adic open subset U of $\Gamma(\tilde{\mathbb{Q}}_p)$, this principle gives a rational function f on Γ, all of whose zeros belong to U. Moreover, one can control the divisor of poles of f. In an unpublished manuscript [Pop] Pop amended Rumely's existence theorem with a rationality condition. Then Pop took a finite set $\mathcal{S}$ of prime numbers and let $N = \mathbb{Q}_{\mathrm{tot},\mathcal{S}}$ be the maximal Galois extension of $\mathbb{Q}$ in which all $p \in \mathcal{S}$ totally decompose. He proved that N satisfies a local global principle for absolutely irreducible normal varieties (see Remark 8.3(a)). Green, Pop, and Roquette have integrated [Pop] and [Ro2] into [GPR] and proved the local global principle for the ring of integers $\mathbb{Z}_N$ of N. This implies both Rumely's and Pop's earlier results.

The present work is an answer to the challenge of Roquette. It is the third article in a series of three articles of the two authors which were based on the master's thesis of the second author. Indeed, given $\boldsymbol{\sigma} \in G(\mathbb{Q})^e$, we consider the field $N(\boldsymbol{\sigma}) = \tilde{\mathbb{Q}}(\boldsymbol{\sigma}) \cap N$ and denote its ring of integers by $\mathbb{Z}_{N(\boldsymbol{\sigma})}$. In [JR2] we generalize the theorem of Skolem-Cantor-Roquette. In the present work we prove the local global principle and an approximation theorem for almost all rings $\mathbb{Z}_{N(\boldsymbol{\sigma})}$. We then derive an affirmative solution of Hilbert's tenth problem for these rings.

It turns out that the crucial property of almost all fields $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$ which is responsible for the density property and the local global principle of $\mathbb{Z}_{N(\boldsymbol{\sigma})}$ is a certain strengthening of the PAC property, namely "PAC over $\mathbb{Z}$" [JR1, Def. 1.1]. In [JR2] we consider an algebraic extension M_0 of $\mathbb{Q}$ and let $M = M_0 \cap N$. We prove that

if M_0 is PAC over $\mathbb{Z}_M$, then M is "weakly P$\mathcal{S}$C over $\mathbb{Z}_M$" (Data 1.1(n)). Hence, both in [JR2] and in the present work, we take an axiomatic approach and prove all our results for an arbitrary subfield M of N which is weakly P$\mathcal{S}$C over $\mathbb{Z}_M$.

Since "M_0 is PAC over $\mathbb{Z}$" implies "M_0 is PAC over $\mathbb{Z}_M$", all results hold for $M_0 = \tilde{\mathbb{Q}}(\boldsymbol{\sigma})$, excluding a set of $\boldsymbol{\sigma} \in G(\mathbb{Q})^e$ of measure zero. Moreover, $\tilde{\mathbb{Q}}$ is PAC over $\mathbb{Z}$. So, we may take M_0 to be $\tilde{\mathbb{Q}}$. Then $M = N$, and we recover the local global principle [GPR, Main Theorem] of Green, Pop, and Roquette ([GPR] does not include a global approximation theorem.)

Note also, that if S is an empty set, then $N = \tilde{\mathbb{Q}}$ and $M = M_0$. In particular, this proves the local global principle and the approximation theorem for almost all rings $\tilde{\mathbb{Z}}(\boldsymbol{\sigma})$. The approximation theorem in its stronger form is an essential ingredient in a primitive recursive decision procedure for the theory of all elementary statements which are true in almost all rings $\tilde{\mathbb{Z}}(\boldsymbol{\sigma})$ (see the thesis [Raz] of the second author).

The exact formulation of our results appears in Section 1. As is usually the case, we formulate and prove them over a Dedekind domain whose quotient field is a basic global field K.

Acknowledgement. The authors thank Joachim Schmid for useful remarks.

1. Statements of the main results

The objects of our results are defined over global fields rather than over $\mathbb{Q}$. To explain the results in detail, we first set the general framework for the whole work.

Data 1.1. We will use the following data and notation, and will keep the assumptions we make for the rest of this work:

(a) K is a global field.
(b) O is a Dedekind domain with quotient field K.
(c) $\tilde{K}$ is the algebraic closure of K; K_s is the separable closure of K.
(d) $G(K) = \mathcal{G}(K_s/K)$ is the absolute Galois group of K, which we identify with $\mathrm{Aut}(\tilde{K}/K)$.
(e) $\mathcal{V}$ is the set of all valuations of K which correspond to the nonzero prime ideals of O.
(f) For each $v \in \mathcal{V}$, $K_{\mathrm{t}\,v}$ is the maximal Galois extension of K in which v totally splits. If K_v is a Henselian closure of K with respect to v, then $K_{\mathrm{t}\,v} = \bigcap_{\sigma \in G(K)} K_v^\sigma$.
(g) $\mathcal{S}$ is a finite subset of $\mathcal{V}$.
(h) $K_{\mathrm{tot},\mathcal{S}} = \bigcap_{v \in \mathcal{S}} K_{\mathrm{t}\,v}$. This is the maximal Galois extension of K in which each $v \in \mathcal{S}$ totally splits.
(i) $N = K_{\mathrm{tot},\mathcal{S},\mathrm{ins}}$ is the maximal purely inseparable extension of $K_{\mathrm{tot},\mathcal{S}}$. It is a perfect field and a normal algebraic extension of K. If $\mathrm{char}(K) = 0$, then $N = K_{\mathrm{tot},\mathcal{S}}$. If $\mathcal{S} = \emptyset$, then $N = \tilde{K}$.
(j) For each algebraic extension L of K let O_L be the integral closure of O in L. For each subset $\mathcal{R}$ of $\mathcal{V}$, let $\mathcal{R}_L$ be the set of all extensions of the valuations in $\mathcal{R}$ to L. In particular, $O = O_K$ and $\mathcal{V} = \mathcal{V}_K$. If L is a normal extension of K and $\sigma \in \mathrm{Aut}(L/K)$, then σ naturally acts on $\mathcal{V}_L$ by $v^\sigma(a^\sigma) = v(a)$ for $v \in \mathcal{V}_L$ and $a \in L$. If $[L : K] < \infty$, then O_L is a Dedekind domain and $\mathcal{V}_L$ is the set of all valuations of L which correspond to the nonzero prime ideals of O_L. In the general case $O_L = \{x \in L |\ v(x) \geq 0 \text{ for all } v \in \mathcal{V}_L\}$.
(k) $\tilde{O} = O_{\tilde{K}}$ and $\tilde{\mathcal{V}} = \mathcal{V}_{\tilde{K}}$.

(l) For each $w \in \mathcal{V}_N$ choose a Henselian closure N_w of N at w. This choice fixes an extension $\tilde{w}$ of w to $\tilde{K}$ such that N_w is the fixed field in $\tilde{K}$ of the decomposition group $D_N(\tilde{w}) = \{\tau \in G(N) \mid \tilde{w}^\tau = \tilde{w}\}$. For each subextension L of N/K let L_w be the fixed field in L_s of $D_L(\tilde{w}) = \{\tau \in G(L) \mid \tilde{w}^\tau = \tilde{w}\}$. Then L_w is a Henselian closure of L at $w|_L$ which is contained in N_w. Let $O_{L,w}$ be its valuation ring. Note that the residue field of N_w is a finite field; in particular it is not separably closed. Hence, by a theorem of F.K. Schmidt [Ja3, Prop. 14.5], each $\sigma \in \mathrm{Aut}(N/K)$ uniquely extends to an isomorphism of N_w onto N_{w^σ}, which we also denote by σ. It maps L_w (resp., $O_{L,w}$) onto $L^\sigma_{w^\sigma}$ (resp., O_{L^σ,w^σ}).

(m) For an abstract absolutely irreducible variety W defined over a field K and for each extension L of K we let $W(L)$ (resp., $W_{\mathrm{sim}}(L)$) be the set of all L-rational (resp., simple L-rational) points of W. Whenever we say that W is an affine absolutely irreducible variety we also mean that W is embedded in some affine space. Then, if R is a subring of L, an **R-rational point** of W is an L-rational point of W whose coordinates lie in R. We denote the set of all R-rational points of W by $W(R)$. Similar notation is imposed for closed subsets of W.

(n) M is a subextension of N/K. We assume that M is perfect and M is **weakly PSC over O_M**. This means that for each absolutely irreducible polynomial $h \in M[T, X]$ which is monic in X such that the roots of $h(0, X)$ are distinct and in N, and for each $g \in M[T]$ such that $g(0) \neq 0$, there exists $(a, b) \in O_M \times M$ such that $h(a, b) = 0$ and $g(a) \neq 0$ [JR2, Def. 1.3].

(o) $\mathcal{W}_0$ is a finite subset of $\mathcal{V}$ and $\mathcal{W} = \mathcal{W}_{0,N}$. In particular, $w^\sigma \in \mathcal{W}$ for each $w \in \mathcal{W}$ and $\sigma \in \mathrm{Aut}(N/K)$. We assume that $\mathcal{S} \subseteq \mathcal{W}_0$.

(p) Let V be an affine absolutely irreducible variety defined over K. Then $V_{K,\mathcal{S},\mathcal{W}}$ is the set of all points $(\mathbf{z}_w)_{w\in\mathcal{W}} \in \prod_{w\in\mathcal{W}} V_{\mathrm{sim}}(N_w)$ for which

(1) there exists a finite subextension L of M/K such that $\mathbf{z}_{w^\sigma} = \mathbf{z}_w^\sigma$ for each $w \in \mathcal{W}$ and $\sigma \in \mathrm{Aut}(N/L)$.

Each $(\mathbf{z}_w)_{w\in\mathcal{W}}$ that satisfies (1) is said to be **L-rational** (Remark 1.3(d)).

(q) $V_{O,\mathcal{S},\mathcal{W}}$ is the set of all points $(\mathbf{z}_w)_{w\in\mathcal{W}} \in \prod_{w\in\mathcal{W}} V_{\mathrm{sim}}(O_{N,w})$ that satisfy (1).

We will extend these data in the sequel by more data and assumptions, as necessary.

Here is our main theorem.

Theorem 1.2 (Strong approximation theorem). *Let V be an affine absolutely irreducible variety defined over K. Consider $(\mathbf{z}_w)_{w\in\mathcal{W}} \in V_{K,\mathcal{S},\mathcal{W}}$ and a positive integer γ.*

(a) *There exists $\mathbf{z} \in V(M)$ such that $w(\mathbf{z} - \mathbf{z}_w) > \gamma$ for each $w \in \mathcal{W}$.*

(b) *If $V(O_{N,v}) \neq \emptyset$ for each $v \in \mathcal{V}_N \smallsetminus \mathcal{W}$, then there exists $\mathbf{z} \in V(M)$ such that $w(\mathbf{z} - \mathbf{z}_w) > \gamma$ for each $w \in \mathcal{W}$ and $v(\mathbf{z}) \geq 0$ for each $v \in \mathcal{V}_N \smallsetminus \mathcal{W}$.*

(c) *If $V(O_{N,v}) \neq \emptyset$ for each $v \in \mathcal{V}_N \smallsetminus \mathcal{W}$, and $w(\mathbf{z}_w) \geq 0$ for each $w \in \mathcal{W}$, then there exists $\mathbf{z} \in V(O_M)$ such that $w(\mathbf{z} - \mathbf{z}_w) > \gamma$ for each $w \in \mathcal{W}$.*

Part (c) is an interesting special case of Part (b). In §8 we first prove (c), and then conclude (b) and (a).

Remark 1.3. (a) We may replace K in Data 1.1 by any finite subextension L of M/K and extend all the objects that have been defined over K to L. Then the

assumptions made on them remain true and N does not change. It follows that Theorem 1.2 for K implies it also for L. Also, we may start from a variety V which is defined over M and then replace K by a finite subextension of M/K over which V is already defined.

(b) It suffices to prove Theorem 1.2 only for points $(\mathbf{z}_w)_{w\in\mathcal{W}}$ which are K-rational. Indeed, if $(\mathbf{z}_w)_{w\in\mathcal{W}}$ is L-rational for some finite subextension L of M/K, then we may apply the theorem in its restricted form to L instead of to K and approximate $(\mathbf{z}_w)_{w\in\mathcal{W}}$ by a point in $V(M)$ as (a), (b), and (c) of the theorem require.

(c) Let $w \in \mathcal{S}_N$. Since M is perfect, $K_{w,\mathrm{ins}} \subseteq M_w \subseteq N_w \subseteq K_{w,\mathrm{ins}}$. Hence, $M_w = N_w = K_{w,\mathrm{ins}}$. If $w \notin \mathcal{S}_N$, then $M_w = N_w = \tilde{K}$ [JR2, Prop. 1.9].

(d) Suppose that $(\mathbf{z}_w)_{w\in\mathcal{W}} \in V_{K,\mathcal{S},\mathcal{W}}$ is L-rational for some finite subextension L of M/K. Note that $N \cap L_w$ is the decomposition field of w in N/L. That is, $N\cap L_w$ is the fixed field in N of all $\sigma \in \mathrm{Aut}(N/L)$ such that $w^\sigma = w$. Note also that N_w/L_w is a normal extension and that $\mathrm{Aut}(N/N \cap L_w) \cong \mathrm{Aut}(N_w/L_w)$. Hence, if $\sigma \in \mathrm{Aut}(N/N \cap L_w)$, then $\mathbf{z}_w = \mathbf{z}_{w^\sigma} = \mathbf{z}_w^\sigma$. It follows that $\mathbf{z}_w \in V(L_{w,\mathrm{ins}})$.

(e) We use $\mathcal{S}_N \subseteq \mathcal{W}$ (Data 1.1(o)) only to simplify notation. In applications that do not make this assumption we use Lemma 8.1 to restore it. □

The strong approximation theorem yields a weak one, which we prove in §8.

Theorem 1.4 (Weak approximation theorem). *Let $\mathcal{T}$ be a finite subset of $\mathcal{V}_M$ and let V be an affine absolutely irreducible variety defined over M.*

(a) *If $V_{\mathrm{sim}}(O_{M,v}) \neq \emptyset$ for each $v \in \mathcal{S}_M$ and $V(O_{M,v}) \neq \emptyset$ for each $v \in \mathcal{V}_M \smallsetminus \mathcal{S}_M$, then each point in*

$$\prod_{v\in\mathcal{T}\cap\mathcal{S}_M} V_{\mathrm{sim}}(O_{M,v}) \times \prod_{v\in\mathcal{T}\smallsetminus\mathcal{S}_M} V(O_{M,v})$$

can be approximated by a point in $V(O_M)$.

(b) *If $V_{\mathrm{sim}}(M_v) \neq \emptyset$ for each $v \in \mathcal{S}_M$, then $V_{\mathrm{sim}}(M)$ is dense in*

$$\prod_{v\in\mathcal{T}\cap\mathcal{S}_M} V_{\mathrm{sim}}(M_v) \times \prod_{v\in\mathcal{T}\smallsetminus\mathcal{S}_M} V(M_v).$$

Taking $\mathcal{T}$ in Theorem 1.4 to be nonempty gives a local global principle.

Theorem 1.5 (Local global principle). *Let V be an affine absolutely irreducible variety defined over M. Suppose that $V(O_{M,v}) \neq \emptyset$ for each $v \in \mathcal{V}_M \smallsetminus \mathcal{S}_M$ and $V_{\mathrm{sim}}(O_{M,v}) \neq \emptyset$ for each $v \in \mathcal{S}_M$. Then $V(O_M) \neq \emptyset$.*

Remark 1.6. It is possible to replace M_v in Theorems 1.4 and 1.5 by its completion $\hat{M}_v$

Indeed, $\hat{M}_v/M_v$ is a separable extension [Ja4, Lemma 2.2]. Now, in general, let (L, v) be a Henselian valued field and $(\hat{L}, v)$ its completion. Assume that $\hat{L}/L$ is a separable extension. Let $A \subseteq \mathbb{A}^n$ be a Zariski L-closed set. Then $A(L)$ is v-dense in $A(\hat{L})$.

Indeed, if $\mathbf{x} \in A(\hat{L})$, then $L(\mathbf{x})/L$ is a separable extension. So, $L(\mathbf{x}) = L(\mathbf{t}, y)$, where $\mathbf{t} = (t_1, \dots, t_r)$ is a separating transcendence base for $L(\mathbf{x})/L$ and y is integral over $L[\mathbf{t}]$. Let $f = \mathrm{irr}(y, L(\mathbf{t}))$. Use the Henselianity of L to approximate $(\mathbf{t}, y)$ by an L-rational zero of f. This will give a point of $A(L)$ which is v-close to $\mathbf{x}$. □

Corollary 1.7. *Let V be an affine absolutely irreducible variety defined over M. If $V_{\mathrm{sim}}(O_N)$ is nonempty, then so is $V(O_M)$.*

If $\mathcal{S} = \emptyset$, then $N = \tilde{K}$, $\mathcal{V}_N = \tilde{\mathcal{V}}$, and the assumption that M is weakly P$\mathcal{S}$C over O_M simplifies to the assumption that M is 'PAC over O_M' (see definition after Theorem 1.8). We reformulate Theorem 1.4 for this case.

Theorem 1.8. *Let $\mathcal{T}$ be a finite subset of $\mathcal{V}_M$ and let V be an affine absolutely irreducible variety defined over M.*

(a) *If $V(O_{M,v}) \neq \emptyset$ for each $v \in \mathcal{V}_M$, then $V(O_M)$ is dense in $\prod_{v\in\mathcal{T}} V(O_{M,v})$. In particular, if $V(\tilde{O}) \neq \emptyset$, then $V(O_M) \neq \emptyset$.*
(b) *$V(M)$ is dense in $\prod_{v\in\mathcal{T}} V(M_v)$.*

The only examples we know for fields M which are weakly P$\mathcal{S}$C over O_M arise by [JR2, Lemma 1.4]. To this end consider a field M_0 and a subset R. We say that M_0 is **PAC over** R if it has the following property: For every absolutely irreducible variety V of dimension $r \geq 0$ and for each dominating separable rational map $\varphi\colon V \to \mathbb{A}^r$ over M_0 there exists $\mathbf{a} \in V(M_0)$ such that $\varphi(\mathbf{a}) \in R^r$.

It follows that if $R \subseteq R' \subseteq M_0$ and M_0 is PAC over R, then M_0 is also PAC over R'. Now let M_0 be an algebraic extension of K and let $M = M_0 \cap N$. Lemma 1.4 of [JR2] says that if M_0 is PAC over O_M, then M is weakly P$\mathcal{S}$C over O_M.

In Section 8 we define what it means for M to be "P$\mathcal{S}$C over O_M". We prove that the strong approximation theorem for M implies that M is "P$\mathcal{S}$C over O_M" and note that the latter implies that M is weakly P$\mathcal{S}$C over O_M.

The first example for a perfect field M_0 which is PAC over O_M is $\tilde{K}$. So, we may take $M_0 = \tilde{K}$ and $M = N$ in Theorems 1.2, 1.4, and 1.5. For example, if V is an affine absolutely irreducible variety defined over N and $\mathcal{T}$ is a finite subset of $\mathcal{V}_N$, then each point in $\prod_{v\in\mathcal{T}\cap\mathcal{S}_N} V_{\mathrm{sim}}(O_{N,v}) \times \prod_{v\in\mathcal{T}\smallsetminus\mathcal{S}_N} V(O_{N,v})$ can be approximated by a point in $V(O_N)$. In particular, for $\mathcal{S} = \emptyset$, if an affine absolutely irreducible variety V defined over $\tilde{K}$ has a v-integral $\tilde{K}$-rational point for each $v \in \tilde{\mathcal{V}}$, then $V(\tilde{O}) \neq \emptyset$. In view of Remark 1.6, this is essentially Rumely's local global principle.

More examples for M_0 arise in a probabilistic way. For each $\boldsymbol{\sigma} = (\sigma_1, \dots, \sigma_e) \in G(K)^e$ let $\tilde{K}(\boldsymbol{\sigma})$ be the fixed field in $\tilde{K}$ of the unique extensions of $\sigma_1, \dots, \sigma_e$ to $\tilde{K}$. Let $\tilde{O}(\boldsymbol{\sigma}) = O_{\tilde{K}(\boldsymbol{\sigma})}$ and $N(\boldsymbol{\sigma}) = \tilde{K}(\boldsymbol{\sigma}) \cap N$. By [JR1, Prop. 3.1], for almost all $\boldsymbol{\sigma} \in G(K)^e$, the field $M_0 = \tilde{K}(\boldsymbol{\sigma})$ is PAC over O, hence also over O_M. We may therefore apply Theorems 1.2, 1.4, and 1.5 to these fields.

Corollary 1.9. *In the above notation, for almost all $\boldsymbol{\sigma} \in G(K)^e$, the field $M = \tilde{K}(\boldsymbol{\sigma}) \cap K_{\mathrm{tot},\mathcal{S},\mathrm{ins}}$ satisfies the consequences of Theorems 1.2, 1.4, and 1.5.*

Theorem 1.5 and Corollary 1.9 combine with A. Robinson's local decidability for a solution for Hilbert's tenth problem for $\tilde{O}$ and almost all $\tilde{O}(\boldsymbol{\sigma})$:

Corollary 1.10 (Decidability of Diophantine equations). *Suppose that $\mathcal{S}$ is empty and thus M is PAC over O_M. Let A be a given Zariski closed subset of $\mathbb{A}^n$ over K.*

(a) *If A is absolutely irreducible, then we can decide whether A has an O_M-rational point.*
(b) *For each positive integer e we can compute the Haar measure of all $\boldsymbol{\sigma} \in G(K)^e$ such that A has an $\tilde{O}(\boldsymbol{\sigma})$-rational point.*

In his thesis [Raz], the second author uses Theorem 1.2 to strengthen Corollary 1.10 and prove that the theory of all elementary statements on rings which are

true in $\tilde{O}(\boldsymbol{\sigma})$ for almost all $\boldsymbol{\sigma} \in G(K)^e$ is primitive recursive. He also generalizes Corollary 1.10(b) to elementary formulas.

The assumptions we made in Data 1.1 have some consequences which we formulate as Propositions 1.11 and 1.12. They may be considered as the hypothesis under which the local global principle and the approximation theorem hold.

Proposition 1.11 (Consequences of Assumptions 1.1(a),(b)). *Let L be a finite extension of K.*

(a) *The completion of L under each $v \in \mathcal{V}_L$ is a local field, that is, a finite extension of $\mathbb{Q}_p$ or a finite extension of $\mathbb{F}_p((t))$ for some prime p.*
(b) *For each $a \in L$, $a \neq 0$, there exist only finitely many $v \in \mathcal{V}_L$ such that $v(a) \neq 0$.*
(c) (*Strong approximation*) *Let $\mathcal{W}_1$ be a finite subset of $\mathcal{V}_L$. For each $w \in \mathcal{W}_1$ let $a_w \in L$ and let γ be a positive integer. Then there exists $x \in L$ such that $w(x - a_w) > \gamma$ for each $w \in \mathcal{W}_1$ and $v(x) \geq 0$ for each $v \in \mathcal{V}_L \smallsetminus \mathcal{W}_1$.*
(d) *The class group of O_L is finite.*

Any book on algebraic number theory can be used as a reference to Proposition 1.11.

We use vector notation. Given a valuation v of $\tilde{K}$ and a vector $\mathbf{a} = (a_1, \dots, a_n) \in \tilde{K}^n$ we write $v(\mathbf{a})$ for $\min_{1 \leq i \leq n} v(a_i)$. If $\mathcal{T}$ is a subset of $\mathcal{V}_N$, we let $\tilde{\mathcal{T}} = \mathcal{T}_{\tilde{K}}$ and $V_{\mathcal{T}}(\mathbf{a}) = \min_{v \in \tilde{\mathcal{T}}} v(\mathbf{a})$. We say that an element $a \in \tilde{K}$ is **$\mathcal{T}$-integral** (resp. **$\mathcal{T}$-unit**) if $v(a) \geq 0$ (resp. $v(a) = 0$) for each $v \in \tilde{\mathcal{V}} \smallsetminus \tilde{\mathcal{T}}$.

Proposition 1.12. *Assumption* 1.1(n) *has the following consequences for Data* 1.1.

(a) (*Remark* 1.3(c)) *For each $v \in \mathcal{V}_N$ we have $M_v = N_v$. In particular, M is v-dense in N_v. If $v \notin \mathcal{S}_N$, then $M_v = N_v = \tilde{K}$.*
(b) [JR2, Lemma 1.8] *Let $\mathcal{T}$ be a finite subset of $\mathcal{V}$. For each $x \in N$ and for each positive integer γ there exists a finite subset B of M such that for each $v \in \mathcal{T}$ and each valuation w of N which lies over v there exists $b \in B$ with $w(b - x) > \gamma$.*
(c) [JR2, Thm. 4.3] *Let $\mathcal{T}$ be a K-rational small subset of $\mathcal{V}_N$* (*Definition* 2.8) *which contains $\mathcal{S}_N$. Consider polynomials $f_i \in \tilde{K}[X_1, \dots, X_n]$, $i = 1, \dots, m$, let $\mathbf{a} \in M^n$, and let γ be a positive integer. Suppose that each of the coefficients of the f_i's is a $\mathcal{T}$-unit. Then there exists $\mathbf{x} \in M^n$ such that $V_{\mathcal{T}}(\mathbf{x} - \mathbf{a}) > \gamma$ and $f_i(\mathbf{x})$ is a $\mathcal{T}$-unit, $i = 1, \dots, m$.*
(d) [JR2, Lemma 1.7] *Let F be a regular extension of M of transcendence degree 1 and let Γ be its unique nonsingular projective model. Let t be an element in $F \smallsetminus M$ whose zeros are simple and belong to $\Gamma(N)$. Finally, let A be a finite subset of $M^\times$. Then there exists $\mathfrak{p} \in \Gamma(M)$ such that $t(\mathfrak{p}) \in O_M \smallsetminus A$.*

The main bulk of this work proves Theorem 1.2(c) for curves. Section 8 then proves Theorem 1.2(c) for an arbitrary absolutely irreducible variety and deduces parts (b) and (a) of Theorem 1.2. Section 9 proves Corollary 1.10.

2. Restatement of the approximation theorem for integral points on curves

This section starts the long proof of the strong approximation theorem for integral points on a curve (Theorem 1.2(c) for $\dim(V) = 1$), from which all the other

results follow. We first reformulate the theorem in this case in terms of function fields, state a somewhat stronger result and finally describe the five steps needed to prove the stronger result. To fix notation we add additional data to Data 1.1.

Data 2.1. The following data and notation remain in force until the end of Section 7.

C	is an absolutely irreducible affine curve in $\mathbb{A}^n$ defined over K,
$\mathbf{x} = (x_1, \dots, x_n)$	is a generic point of C over K and over each completion $\hat{K}_v$,
$F_0 = K(\mathbf{x})$	is the function field of C over K,
$F = MF_0 = M(\mathbf{x})$	is the function field of C, considered as a curve over M,
$\mathrm{genus}(F/M)$	is the genus of F/M,
s	$= 2\,\mathrm{genus}(F/M) + 2$ is a useful constant,
Γ	is the unique nonsingular projective model of F/M,
M'	is a field that contains M and is linearly disjoint from F,
$F' = M'F$	is the function field obtained by extension of scalars to M',
$\Gamma(M')$	is the set of all M'-rational points of Γ,
$\Gamma(F'/M')$	is the set of all prime divisors of F'/M',
$\mathrm{Div}(F'/M')$	is the group of divisors of F'/M',
$\mathfrak{p}_1^*, \dots, \mathfrak{p}_e^*$	are the distinct poles of $x_1, \dots, x_n$ in $\Gamma(F/M)$,
$\mathfrak{p}_{i1}^*, \dots, \mathfrak{p}_{i,d_i}^*$	are the distinct prime divisors of $\tilde{K}F/\tilde{K}$ which lie over $\mathfrak{p}_i^*$,
$\mathfrak{d}$	$= \mathfrak{p}_1^* + \cdots + \mathfrak{p}_e^*$,
γ_0	is a positive integer.

Remark 2.2. (a) The existence of Γ uses the hypothesis that M is perfect (or more accurately, that F/M is conservative).

(b) For each divisor $\mathfrak{a}$ of F'/M' we consider the vector space

$$\mathcal{L}_{M'}(\mathfrak{a}) = \{f \in F' |\ (f) + \mathfrak{a} \geq 0\}$$

over M'. It has a finite dimension, which is denoted by $\dim_{M'}(\mathfrak{a})$. The group $\mathrm{Div}(F/M)$ naturally embeds in $\mathrm{Div}(F'/M')$. As M is perfect, a basis of $\mathcal{L}_M(\mathfrak{a})$ is also a basis of $\mathcal{L}_{M'}(\mathfrak{a})$, and $\mathrm{genus}(F/M) = \mathrm{genus}(F'/M')$ [De1, p. 132]. Thus $\dim_M(\mathfrak{a}) = \dim_{M'}(\mathfrak{a})$ and we can drop the reference to the ground field from the dimension of $\mathfrak{a}$. The same rule applies for the degree of $\mathfrak{a}$. Also, each prime divisor of F/M is unramified in $\tilde{K}F$ [De1, p. 113]. In particular $\mathfrak{p}_i^* = \mathfrak{p}_{i1}^* + \cdots + \mathfrak{p}_{i,d_i}^*$, and hence $\deg(\mathfrak{p}_i^*) = d_i$ □

Remark 2.3. We identify each point of $\Gamma(M')$ with a prime divisor $\mathfrak{p}$ of F'/M' of degree 1. If $f \in F'$, then $f(\mathfrak{p})$ is the value of the rational function f of Γ at $\mathfrak{p}$, if we view $\mathfrak{p}$ as a point on the curve, or the value of the place associated with $\mathfrak{p}$ at the element f of F', if we view $\mathfrak{p}$ as a prime divisor of F'/M'. In both cases $f(\mathfrak{p})$ is an element of $M' \cup \{\infty\}$. This element is ∞ exactly when $\mathfrak{p}$ is a pole of f. Thus, if $\mathfrak{p} \in \Gamma(\tilde{K})$ does not belong to $\{\mathfrak{p}_{ij}^* |\ i = 1, \dots, e;\ j = 1, \dots, d_i\}$, then $\mathbf{x}(\mathfrak{p}) = (x_1(\mathfrak{p}), \dots, x_n(\mathfrak{p}))$ is a point in $C(\tilde{K})$.

Now suppose that M' is equipped with a valuation v. The v-adic topology of M' induces a topology on $\Gamma(M')$ whose basis consists of the sets

$$\{\mathfrak{p} \in \Gamma(M') |\ v(f_1(\mathfrak{p})) \geq 0, \dots, v(f_m(\mathfrak{p})) \geq 0\}$$

with $f_1, \dots, f_m \in F'$. Here we make the convention that $v(\infty) = -\infty$. This is actually the weakest topology on $\Gamma(M')$ such that each $f \in F'$ defines a continuous function

$$f\colon \Gamma(M') \to M' \cup \{\infty\}, \qquad \mathfrak{p} \mapsto f(\mathfrak{p}),$$

where the neighborhoods of ∞ are, as usual, the complements of the neighborhoods of 0. □

Suppose now that for each $v \in \mathcal{V}_N$ we are given a point $\mathbf{z}_v \in C(O_{N,v})$ such that $(\mathbf{z}_w)_{w\in\mathcal{W}} \in C_{O,\mathcal{S},\mathcal{W}}$ (Data 1.1(q)). Our goal is to approximate $(\mathbf{z}_w)_{w\in\mathcal{W}}$ by an element of $C(O_M)$. If $v \in \mathcal{W}$, then $\mathbf{z}_v \in C_{\mathrm{sim}}(O_{N,v})$. Hence, there exists a unique $\mathfrak{p}_v \in \Gamma(N_v)$ such that $\mathbf{x}(\mathfrak{p}_v) = \mathbf{z}_v$ [JaR, p. 457, Cor. A3]. If $v \in \mathcal{V}_N \smallsetminus \mathcal{W}$, then $N_v = \tilde{K}$ (Proposition 1.12(a)) and we may choose $\mathfrak{p}_v \in \Gamma(N_v)$ such that $v(\mathbf{x}(\mathfrak{p}_v)) = \mathbf{z}_v$. In all cases, $v(\mathbf{x}(\mathfrak{p}_v)) \geq 0$.

By definition, there exists a finite subextension L of M/K such that $\mathbf{z}_{w^\sigma} = \mathbf{z}_w^\sigma$ for each $w \in \mathcal{W}$ and each $\sigma \in \mathrm{Aut}(N/L)$. By Data 2.1, L_wF_0 is a regular extension of L_w and therefore it is linearly disjoint from N_w over L_w. Hence, each $\sigma \in \mathrm{Aut}(N/L)$ uniquely extends to an isomorphism $\sigma\colon N_wF_0 \to N_{w^\sigma}F_0$ that maps L_w onto L_{w^σ} and fixes each element of F_0 (use Data 1.1(l)). It follows that $\mathbf{x}(\mathfrak{p}_{w^\sigma}) = \mathbf{z}_{w^\sigma} = \mathbf{z}_w^\sigma = \mathbf{x}(\mathfrak{p}_w)^\sigma = \mathbf{x}(\mathfrak{p}_w^\sigma)$. We conclude that $\mathfrak{p}_{w^\sigma} = \mathfrak{p}_w^\sigma$.

By remark 1.3(b), we may assume that $L = K$ and conclude that Theorem 1.2(c) for $V = C$ is equivalent to the following theorem:

Theorem 2.4 (Approximation theorem for function fields of one variable). *Suppose that for each $v \in \mathcal{V}_N$ there exists $\mathfrak{p}_v \in \Gamma(N_v)$ such that $v(\mathbf{x}(\mathfrak{p}_v)) \geq 0$. Assume that $\mathfrak{p}_{w^\sigma} = \mathfrak{p}_w^\sigma$ for each $w \in \mathcal{W}$ and $\sigma \in \mathrm{Aut}(N/K)$. Then there exists $\mathfrak{p} \in \Gamma(M)$ such that $v(\mathbf{x}(\mathfrak{p})) \geq 0$ for all $v \in \mathcal{V}_N$ and $w(\mathbf{x}(\mathfrak{p}) - \mathbf{x}(\mathfrak{p}_w)) \geq \gamma_0$ for each $w \in \mathcal{W}$. In particular, $\mathfrak{p} \notin \{\mathfrak{p}_1^*, \dots, \mathfrak{p}_e^*\}$.*

Our method of proof will force us to prove a stronger theorem than Theorem 2.4.

Theorem 2.5. *Suppose that for each $v \in \mathcal{V}_N$ there exists $\mathfrak{p}_v \in \Gamma(N_v)$ such that $v(\mathbf{x}(\mathfrak{p}_v)) \geq 0$. Assume that $\mathfrak{p}_{w^\sigma} = \mathfrak{p}_w^\sigma$ for each $w \in \mathcal{W}$ and each $\sigma \in \mathrm{Aut}(N/K)$. Then there exists a function $f \in F$ with the following properties:*

(1a) *There exists a positive integer k (which can be chosen to be arbitrarily large) such that $(f)_\infty = k\mathfrak{d}$.*
(1b) *Each of the zeros of f is N-rational and* **simple***; that is, $(f)_0 = \sum_{i=1}^m \mathfrak{p}_i$ with distinct $\mathfrak{p}_i \in \Gamma(N)$.*
(1c) *For all $v \in \mathcal{V}_N$ we have $v(\mathbf{x}(\mathfrak{p}_i)) \geq 0$, $i = 1, \dots, m$, and*
(1d) *$w(\mathbf{x}(\mathfrak{p}_i) - \mathbf{x}(\mathfrak{p}_w)) \geq \gamma_0$, $i = 1, \dots, m$, if $w \in \mathcal{W}$.*

Moreover, one of the zeros of f is M-rational.

We note that (1a) is a technical condition which is necessary to carry out the proof of Theorem 2.5.

To prove Theorem 2.5 we fix the data of the assumption of the theorem:

Data and Assumption 2.6. For each $v \in \mathcal{V}_N$ we fix a point $\mathfrak{p}_v$ of $\Gamma(N_v)$ such that $v(\mathbf{x}(\mathfrak{p}_v)) \geq 0$. We assume that $\mathfrak{p}_{w^\sigma} = \mathfrak{p}_w^\sigma$ for each $w \in \mathcal{W}$ and each $\sigma \in \mathrm{Aut}(N/K)$. This data will remain in force until the end of Section 7. □

The function f of Theorem 2.5 will be said to be "$\mathcal{V}_N$-admissible":

Definition 2.7: Admissible functions. Let $v \in \mathcal{V}_N$. A function $f \in NF$ is v-**admissible** if

(2a) there exists a positive integer k such that $(f)_\infty = k\mathfrak{d}$ (we say that f is of **level** k),
(2b) all the zeros of f are simple and belong to $\Gamma(N_v)$,
(2c) $v(\mathbf{x}(\mathfrak{p})) \geq 0$ for each zero $\mathfrak{p} \in \Gamma(N_v)$ of f, and
(2d) if $v \in \mathcal{W}$, then $v(\mathbf{x}(\mathfrak{p}) - \mathbf{x}(\mathfrak{p}_v)) \geq \gamma_0$ for each zero $\mathfrak{p} \in \Gamma(N_v)$ of f.

Let $\mathcal{T}$ be a subset of $\mathcal{V}_N$. We say that f is $\mathcal{T}$-**admissible** if f is v-admissible for each $v \in \mathcal{T}$. In this case we also say that f is **admissible along** $\mathcal{T}$. □

Definition 2.8: Small sets. A subset $\mathcal{T}$ of $\mathcal{V}_N$ is **small** if it satisfies one of the following equivalent conditions:

(3a) $\mathcal{T}|_K$ is a finite set.
(3b) $\mathcal{T}|_L$ is a finite set for each finite subextension L of N/K.
(3c) $\mathcal{T}$ is contained in a set $\mathcal{T}' = \{v \in \mathcal{V}_N \mid \bigvee_{a \in A} v(a) < 0\}$ for some nonempty finite subset A of N.

Thus for each finite subextension L of N/K there is a finite subset $\mathcal{T}_0$ of $\mathcal{T}$ which contains exactly one extension of each element of $\mathcal{T}|_L$. So, $\mathcal{T} \subseteq \{w^\sigma \mid w \in \mathcal{T}_0 \text{ and } \sigma \in G(L)\}$. We say that $\mathcal{T}_0$ **represents** $\mathcal{T}|_L$. If $\mathcal{T} = \{w^\sigma \mid w \in \mathcal{T}_0 \text{ and } \sigma \in G(L)\}$, we say that $\mathcal{T}$ is L-**rational**.

Starting with an arbitrary small set $\mathcal{T}$ as above, we may enlarge A to a finite set which is invariant under $G(K)$. Then $\mathcal{T}'$ becomes K-rational. Thus, each small subset of $\mathcal{V}_N$ is contained in a K-rational small subset of $\mathcal{V}_N$.

Finally, an (L-**rational**) **big subset** of $\mathcal{V}_N$ is the complement of an L-rational small set. □

The proof of Theorem 2.5 constructs f in five steps. In each of them f is admissible along a set $\mathcal{T}$ which is larger than the set of the preceding step. Of course, f is changed from one step to the next. So, in each step we actually construct not only one function, but a family of functions, which are close to each other in the '$\mathcal{T}$-topology'. Our construction follows the construction of Roquette et al. [Ro2] over $\tilde{K}$. We use Proposition 1.12(a) to approximate functions in NF by admissible functions in F.

The headings of the steps below describe the set $\mathcal{T}$ along which f is admissible.

1. A single valuation. To construct a function $f \in NF$ which is v-admissible for a single valuation $v \in \mathcal{V}_N$ we use the Rumely-Jacobi existence theorem for algebraic functions and the theorem about the continuity of the zeros of algebraic functions. The former forces us to assume that the completion of K at $v|_K$ is a local field. The latter holds over N_v. We prove that if f' is v-close enough to f, then it is also v-admissible. Then we use the v-density of M in N to choose $f \in F$.

2. Finitely many valuations. We use the weak approximation theorem.

3. Small sets. An essential tool in this step is Proposition 1.12(b).

4. A big set of valuations. We use here the theory of good reduction.

5. The whole set $\mathcal{V}_N$. In order to combine the big set of valuations with its complement (which is small) we use Proposition 1.12(c).

Finally we use Proposition 1.12(d) in order to choose f with an M-rational zero.

3. Finitely many valuations

The existence of an admissible function at a single valuation is a consequence of the Jacobi-Rumely-Pop existence theorem. We then use the principle of variation of constants (Corollary 3.3) to approximate several functions, each admissible at a single valuation, by a function which is admissible at each of these valuations.

Before we do that, we fix further data and make more assumptions on top of those already made in Data 1.1, Data 2.1, and Data 2.6.

Data and Assumption 3.1. We choose a finite extension K_1 of K which is contained in M and over which Γ is defined. Then $F_1 = K_1(\mathbf{x})$ is the function field of C and of Γ over K_1 and $F = MF_1$. Since M is perfect and $\mathfrak{d}$ is M-rational, we may assume in addition that

(a) $\mathrm{genus}(F_1/K_1) = \mathrm{genus}(F/M)$ (in particular F_1/K_1 is conservative), and
(b) $\mathfrak{d}$ is K_1-rational. □

Let $\sigma \in G(K_1)$. Since $\tilde{K}$ and F_1 are linearly disjoint over K_1, σ extends uniquely to an element of $\mathrm{Aut}(\tilde{K}F/F_1)$, which we also denote by σ. This σ acts on the points $\mathfrak{p} \in \Gamma(\tilde{K})$ such that $f^\sigma(\mathfrak{p}^\sigma) = f(\mathfrak{p})^\sigma$ for each $f \in \tilde{K}F$. Extend the action of σ to the group of divisors of $\tilde{K}F/\tilde{K}$ by linearity. Then $(f)^\sigma = (f^\sigma)$, for each $f \in \tilde{K}F$. Also, Assumption 3.1(b) implies that $\mathfrak{d}^\sigma = \mathfrak{d}$.

Let (M', v) be a valued field which contains K_1 and let $F' = M'F_1$. The following result appears in [Pop, Thm. 1.1] and in [GPR, Cor. 7.2].

Proposition 3.2 (Continuity of zeros of algebraic functions). *Suppose that (M', v) is Henselian. Consider an element $0 \neq f \in F'$, let $(f)_\infty = \mathfrak{a}$, and suppose that $(f)_0 = \sum_{i=1}^m \mathfrak{p}_i$, where $\mathfrak{p}_i$ are distinct prime divisors of F'/M'. Write $f = \sum_{j=1}^d c_j u_j$ with $c_j \in M'$ and $u_1, \dots, u_d$ being a basis for the M'-vector space $\mathcal{L}_{M'}(\mathfrak{a})$. For each $1 \le i \le m$ let $U_i \subseteq \Gamma(M')$ be a v-open neighborhood of $\mathfrak{p}_i$. Then there exists $\gamma > 0$ such that if $c'_1, \dots, c'_d \in M'$ satisfy $v(c'_j - c_j) > \gamma$, $j = 1, \dots, d$, and $f' = \sum_{j=1}^d c'_j u_j$, then $(f')_\infty = \mathfrak{a}$ and $(f')_0 = \sum_{i=1}^m \mathfrak{p}'_i$ with $\mathfrak{p}'_i \in U_i$.*

Corollary 3.3 (Principle of variation of constants). *Let $f \in NF$ be a v-admissible function for a valuation $v \in \mathcal{V}_N$. Set $\mathfrak{a} = (f)_\infty$, let $u_1, \dots, u_d \in NF$ be a basis for $\mathcal{L}_N(\mathfrak{a})$, and write $f = \sum_{j=1}^d c_j u_j$ with $c_j \in N$. Then there exists $\gamma > 0$ such that if $c'_1, \dots, c'_d \in N$ satisfy $v(c'_j - c_j) > \gamma$, $j = 1, \dots, d$, and $f' = \sum_{j=1}^d c'_j u_j$, then f' is v-admissible and $(f')_\infty = \mathfrak{a}$.*

Proof. By assumption, $(f)_0 = \sum_{i=1}^m \mathfrak{p}_i$, with $\mathfrak{p}_i \in \Gamma(N_v)$ distinct and $v(\mathbf{x}(\mathfrak{p}_i)) \ge 0$. Also, $v(\mathbf{x}(\mathfrak{p}_i) - \mathbf{x}(\mathfrak{p}_v)) \ge \gamma_0$ if $v \in \mathcal{W}$, $i = 1, \dots, m$. Apply Proposition 3.2 to the case where $M' = N_v$. Also, choose U_i to be disjoint v-open neighborhoods of $\mathfrak{p}_i$ which are contained in the v-open subset

$$\{\mathfrak{p} \in \Gamma(N_v) |\ v(\mathbf{x}(\mathfrak{p})) \ge 0 \text{ and } v(\mathbf{x}(\mathfrak{p}) - \mathbf{x}(\mathfrak{p}_v)) \ge \gamma_0 \text{ if } v \in \mathcal{W}\}. \qquad \square$$

Proposition 3.4 (Existence theorem for a single valuation). *Let $v \in \mathcal{V}_N$. Then there exists a positive integer k_v such that for each multiple k of k_v there exists a v-admissible function $f \in F$ such that $(f)_\infty = k\mathfrak{d}$.*

Proof. Recall that $\mathfrak{p}_v \in \Gamma(N_v) = \Gamma(M_v)$ (Data 2.6 and Proposition 1.12(a)). Choose a finite subextension L of M/K_1 such that $\mathfrak{p}_v$ is L_v-rational. Let $\hat{L}$ be the completion of L_v.

As L is a global field, $\hat{L}$ is a local field. Since $v(\mathbf{x}(\mathfrak{p}_v)) \geq 0$, the open subset

$$U = \{\mathfrak{p} \in \Gamma(\hat{L}) |\ v(\mathbf{x}(\mathfrak{p})) \geq 0 \text{ and } v(\mathbf{x}(\mathfrak{p}) - \mathbf{x}(\mathfrak{p}_v)) \geq \gamma_0 \text{ if } v \in \mathcal{W}\}$$

of $\Gamma(\hat{L})$ is not empty. Theorem 2.1 of [GPR] improves the Jacobi-Rumely existence theorem and gives a nonconstant function $g \in \hat{L}F_1$ whose pole divisor is a multiple of $\mathfrak{d}$. (Note that by Assumption 3.1(b), $\mathfrak{d}$ is $\hat{L}$-rational.) Moreover, the zeros $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ of g are $\hat{L}$-rational, simple, and belong to U. By [GPR, Remark 2.5], there exists a positive integer k_v such that for each multiple k of k_v the function g can be chosen with $(g)_\infty = k\mathfrak{d}$.[1]

Let $u_1, \ldots, u_d \in LF_1$ be a basis for $\mathcal{L}_L(k\mathfrak{d})$. Assume without loss that $\hat{L}$ is linearly disjoint from LF_1 over L. Since $\hat{L}/L$ is separable (because L is a function field of one varible, hence defectless at v [Ja4, p. 269]), $u_1, \ldots, u_d$ also form a basis for $\mathcal{L}_{\hat{L}}(k\mathfrak{d})$. So, there exist $b_1, \ldots, b_d \in \hat{L}$ such that $g = \sum_{j=1}^d b_j u_j$. Use the density of L in $\hat{L}$ to choose $\mathbf{c} \in L^d \subseteq M^d$ which is v-close to $\mathbf{b}$. Let $f = \sum_{j=1}^d c_j u_j$. Apply Proposition 3.2 to g, f, and $\hat{L}$ instead of to f, f', and M' (choose U_i disjoint and contained in U) and conclude that $(f)_\infty = k\mathfrak{d}$, and each of the zeros of f is simple and belongs to U. In particular, f is v-admissible. □

Lemma 3.5. *Let L be an extension of K_1 which is contained in M, let $v \in \mathcal{V}_N$, and let $\sigma \in \mathrm{Aut}(N/L)$. Suppose that a function $f \in NF$ is v-admissible. Then f^σ is v^σ-admissible. In particular, if $f \in LF_1$, then f is v^σ-admissible.*

Proof. By assumption $(f) = \sum_{j=1}^m \mathfrak{p}_j - k\mathfrak{d}$, where the $\mathfrak{p}_j$ are distinct elements of $\Gamma(N_v)$, k is a positive integer, $v(\mathbf{x}(\mathfrak{p}_j)) \geq 0$ and $v(\mathbf{x}(\mathfrak{p}_j) - \mathbf{x}(\mathfrak{p}_v)) \geq \gamma_0$ if $v \in \mathcal{W}$. Apply σ to get $(f^\sigma) = \sum_{j=1}^m \mathfrak{p}_j^\sigma - k\mathfrak{d}$, $v^\sigma(\mathbf{x}(\mathfrak{p}_j^\sigma)) \geq 0$, and $v^\sigma(\mathbf{x}(\mathfrak{p}_j^\sigma) - \mathbf{x}(\mathfrak{p}_v^\sigma)) \geq \gamma_0$ if $v \in \mathcal{W}$. Also, $\mathfrak{p}_1^\sigma, \ldots, \mathfrak{p}_m^\sigma$ are distinct. So, f^σ is v^σ-admissible. □

Proposition 3.6 (Existence theorem for finitely many valuations). *Let $\mathcal{T}$ be a finite subset of $\mathcal{V}_N$. Then, for each k_0, there exists a $\mathcal{T}$-admissible function $f \in F$ of level $\geq k_0$.*

Proof. Let $\mathcal{T}_0$ be a subset of $\mathcal{T}$ which represents $\mathcal{T}|_M$ (Definition 2.8). For each $v \in \mathcal{T}_0$ let k_v be the positive integer that Proposition 3.4 gives. Choose a common multiple $k \geq k_0$ of the k_v's. For each $v \in \mathcal{T}_0$ take $f_v \in F$ which is v-admissible of level k. Let $u_1, \ldots, u_d$ be a basis for $\mathcal{L}_M(k\mathfrak{d})$ and write $f_v = \sum_{j=1}^d c_{vj} u_j$ with $c_{vj} \in M$.

Apply the weak approximation theorem to $\mathcal{T}_0|_M$ and choose $\mathbf{c} \in M^d$ which is v-close to $\mathbf{c}_v$ for each $v \in \mathcal{T}_0$. By Corollary 3.3, $f = \sum_{j=1}^d c_j u_j$ is v-admissible for each $v \in \mathcal{T}_0$ and $(f)_\infty = k\mathfrak{d}$. By Lemma 3.5, with M replacing L, f is v-admissible for each $v \in \mathcal{T}$. □

[1] The proof of [GPR, Theorem 2.1] uses an embedding φ of Γ into its Jacobian variety J. For $c = \mathrm{genus}(\Gamma)$ and $d = \deg(\mathfrak{d})$, one chooses $\mathfrak{q}_1, \ldots, \mathfrak{q}_c \in U$ and considers the divisor $\mathfrak{b} = c\mathfrak{d} - d\sum_{j=1}^c \mathfrak{q}_j$ of degree 0. Then $\varphi(\mathfrak{b})$ is a point of $J(\hat{L})$. Since $J(\hat{L})$ is v-compact, there exists a positive integer k_v such that for each multiple k of k_v the point $k\varphi(\mathfrak{b})$ is v-close to 0. Thus there exist points $\mathfrak{q}'_j$ in U such that $\varphi(kc\mathfrak{d} - \sum_{j=1}^{kcd} \mathfrak{q}'_j) = 0$ in $J(\hat{L})$. Moreover, it is possible (but not easy) to choose the $\mathfrak{q}'_j$ as distinct. By Abel's theorem, there exists a function $g \in \hat{L}F_1$ such that $(g) = \sum \mathfrak{q}'_j - kc\mathfrak{d}$. This is the desired function.

4. Small sets

We use Proposition 3.6 and the weak approximation theorem to prove an existence and density theorem for admissible functions in F along a given small set. An essential tool in this application is Theorem 1.12(b).

Lemma 4.1. *Let E/L be a function field of one variable and let k be an integer $\geq 2\,\mathrm{genus}(E/L)+1$. Consider distinct prime divisors $\mathfrak{q}_1,\dots,\mathfrak{q}_m$ of E/L with $\deg(\mathfrak{q}_i)=d_i$. Then*

$$\dim(\mathcal{L}_L(k\mathfrak{q}_i)/\mathcal{L}_L((k-1)\mathfrak{q}_i))=d_i,\qquad i=1,\dots,m. \tag{1}$$

Let $y_{i1},\dots,y_{i,d_i}$ be a basis for $\mathcal{L}_L(k\mathfrak{q}_i)$ modulo $\mathcal{L}_L((k-1)\mathfrak{q}_i)$ and let $\mathfrak{a}=\mathfrak{q}_1+\cdots+\mathfrak{q}_m$. Then $(y_{ij})_\infty=k\mathfrak{q}_i$, $i=1,\dots,m$, $j=1,\dots,d_i$ and the y_{ij} together form a basis for $\mathcal{L}_L(k\mathfrak{a})$ modulo $\mathcal{L}_L((k-1)\mathfrak{a})$.

Proof. By the Riemann-Roch theorem (1) (above) and (2) (below) are true:

$$\dim(\mathcal{L}_L(k\mathfrak{a})/\mathcal{L}_L((k-1)\mathfrak{a}))=\deg(\mathfrak{a}). \tag{2}$$

Hence, as $y_{ij}\in\mathcal{L}_L(k\mathfrak{a})$, it suffices to prove that they are linearly independent modulo $\mathcal{L}_L((k-1)\mathfrak{a})$. Indeed, suppose that

$$\sum_{i=1}^{m}\sum_{j=1}^{d_i}a_{ij}y_{ij}\equiv 0 \mod \mathcal{L}_L((k-1)\mathfrak{a}) \tag{3}$$

with $a_{ij}\in L$. Denote the normalized valuation of E/L which corresponds to $\mathfrak{q}_i$ by v_i. Then $v_i(y_{ij})=-k$ and $v_i(y_{i'j})\geq 0$ for $i\neq i'$. It follows from (3) that $v_i(\sum_{j=1}^{d_i}a_{ij}y_{ij})\geq -k+1$. Hence $\sum_{j=1}^{d_i}a_{ij}y_{ij}$ belongs to $\mathcal{L}_L((k-1)\mathfrak{q}_i)$. By the choice of the y_{ij}, this implies that $a_{ij}=0$ for $j=1,\dots,d_i$. This concludes the proof of the lemma. □

We use Lemma 4.1 to construct a basis for $\mathcal{L}_M(k\mathfrak{d})$ modulo $\mathcal{L}_M((k-1)\mathfrak{d})$ which will belong to a finitely generated subgroup of $F^\times$ that does not depend on k. This requires more data.

Data 4.2. Write each $k\geq s=2\,\mathrm{genus}(F/M)+2$ as $k=qs+r$ with $q\geq 0$ and $s\leq r\leq 2s-1$. Let

$$\begin{array}{rcl}
B_{ir} & = & \{u_{ijr}\mid j=1,\dots,d_i\} \text{ be a basis for } \mathcal{L}_M(r\mathfrak{p}_i^*) \text{ modulo } \mathcal{L}_M((r-1)\mathfrak{p}_i^*)\\
 & & \text{(note that } B_{ir} \text{ does not depend on } k),\\
u_{ijk} & = & u_{i1s}^q u_{ijr},\\
B_{ik} & = & \{u_{ijk}\mid j=1,\dots,d_i\},\\
B_k & = & B_{1k}\cup\cdots\cup B_{ek},\\
B_0 & = & \text{basis for } \mathcal{L}_M((s-1)\mathfrak{d}) \text{ which contains } 1,\\
K_2 & = & \text{a finite subextension of } M/K_1 \text{ such that } B_0\cup B_s\cup\cdots\cup B_{2s-1}\subseteq K_2F_1,\\
F_2 & = & K_2F_1,
\end{array}$$
□

Lemma 4.3. *Let $k\geq s$. Then:*

(a) *$(u_{ijk})_\infty=k\mathfrak{p}_i^*$ and B_{ik} is a basis for $\mathcal{L}_M(k\mathfrak{p}_i^*)$ modulo $\mathcal{L}_M((k-1)\mathfrak{p}_i^*)$, $i=1,\dots,e$, $j=1,\dots,d_i$.*
(b) *B_k is a basis of $\mathcal{L}_M(k\mathfrak{d})$ modulo $\mathcal{L}_M((k-1)\mathfrak{d})$.*
(c) *F_2 contains a basis for $\mathcal{L}_M(k\mathfrak{d})$.*

Proof of (a). Let $k = qs + r$ as in Data 4.2. Then $u_{i1s}^q u_{ijr}$, $j = 1, \dots, d_i$, belong to $\mathcal{L}_M(k\mathfrak{p}_i^*)$ and are linearly independent over M modulo $\mathcal{L}_M((k-1)\mathfrak{p}_i^*)$. Conclude from (1) applied to $\mathfrak{p}_i^*$ instead of to $\mathfrak{q}_i$ that these elements form a basis for $\mathcal{L}_M(k\mathfrak{p}_i^*)$ modulo $\mathcal{L}_M((k-1)\mathfrak{p}_i^*)$. □

Proof of (b). Apply Lemma 4.1 to $\mathfrak{d} = \mathfrak{p}_1^* + \cdots + \mathfrak{p}_e^*$ instead of to $\mathfrak{a} = \mathfrak{q}_1 + \cdots + \mathfrak{q}_m$. □

Proof of (c). Combine (a) and (b). □

Notation 4.4. Following Lemma 4.3, for each $k \geq s-1$ let

$$e_k = \dim(\mathcal{L}_M(k\mathfrak{d})).$$

By the Riemann-Roch theorem, $e_k \geq 2$. Then list the elements of $B_0 \cup B_s \cup B_{s+1} \cup B_{s+2} \cup \cdots$ as $u_1, u_2, u_3, \dots$ such that $u_1 = 1$, $B_0 = \{u_1, \dots, u_{e_{s-1}}\}$, and $B_k = \{u_{e_{k-1}+1}, \dots, u_{e_k}\}$ for $k \geq s$. By Data 4.2, all u_i belong to F_2 and $\{u_1, \dots, u_{e_k}\}$ is a basis for $\mathcal{L}_{M'}(k\mathfrak{d})$ for each algebraic extension M' of M, which we fix for the rest of this work. □

Proposition 4.5. *Let $\mathcal{T}$ be a small subset of $\mathcal{V}_N$. Then, for each k_0 there exists a $\mathcal{T}$-admissible function $f \in F$ of level $k \geq k_0$.*

Moreover, write $f = \sum_{i=1}^{e_k} c_i u_i$ with $c_i \in M$. Then there exists $\gamma > 0$ such that if $\mathbf{c}' \in N^{e_k}$ satisfies $V_{\mathcal{T}}(\mathbf{c}' - \mathbf{c}) > \gamma$, then $f' = \sum_{i=1}^{e_k} c_i' u_i$ is also a $\mathcal{T}$-admissible function of level k.

Proof. Let $\mathcal{T}_2$ be a finite subset of $\mathcal{T}$ which represents $\mathcal{T}|_{K_2}$ (Definition 2.8). By Proposition 3.6 there is a $\mathcal{T}_2$-admissible function $g \in F$ of level $k \geq \max\{k_0, s-1\}$. Write $g = \sum_{i=1}^{e_k} a_i u_i$ with $a_i \in M$. By Corollary 3.3 there exists $\varepsilon > 0$ such that for each $w \in \mathcal{T}_2$ if $\mathbf{a}' \in N^{e_k}$ satisfies $w(\mathbf{a}' - \mathbf{a}) > \varepsilon$, then $g' = \sum_{i=1}^{e_k} a_i' u_i$ is w-admissible of level k. □

Let K_2' be a finite normal subextension of N/K_2 which contains $a_1, \dots, a_{e_k}$. Then $A = \{\mathbf{a}^\sigma \mid \sigma \in \mathrm{Aut}(N/K_2)\} = \{\mathbf{a}^\sigma \mid \sigma \in \mathrm{Aut}(K_2'/K_2)\}$ is a finite subset of N. We have not assumed M to be normal over K. Hence, A need not be a subset of M. However, by Proposition 1.12(b), M^{e_k} has a finite subset B with the following property: For each $w \in \mathcal{T}_2$, each $\tau \in \mathrm{Aut}(N/K_2)$, and each $\mathbf{a}' \in A$ there exists $\mathbf{b}_{w^\tau, \mathbf{a}'} \in B$ such that $w^\tau(\mathbf{b}_{w^\tau, \mathbf{a}'} - \mathbf{a}') > \varepsilon$. Choose a finite subextension K_3 of M/K_2 such that $B \subseteq K_3^{e_k}$.

Now let $v \in \mathcal{T}$. Then there exist $\sigma \in \mathrm{Aut}(N/K_2)$ and $w \in \mathcal{T}_2$ such that $v = w^\sigma$. Since $\mathbf{a}' = \mathbf{a}^\sigma$ belongs to A, we have $w^\sigma(\mathbf{b}_{v,\mathbf{a}'} - \mathbf{a}^\sigma) > \varepsilon$. Hence $w(\mathbf{b}_{v,\mathbf{a}'}^{\sigma^{-1}} - \mathbf{a}) > \varepsilon$. Hence, by the first paragraph, $\sum_{i=1}^{e_k} b_{v,\mathbf{a}',i}^{\sigma^{-1}} u_i$ is a w-admissible function of level k. As $u_i \in F_2$ (Notation 4.4), we have $u_i^\sigma = u_i$, $i = 1, \dots, e_k$. Hence, by Lemma 3.5, with K_2 instead of L, $f_v = \sum_{i=1}^{e_k} b_{w,\mathbf{a}',i} u_i$ is a v-admissible function in K_3F_1 of level k.

Choose now a finite subset $\mathcal{T}_3$ of $\mathcal{T}$ which represents $\mathcal{T}|_{K_3}$. By the preceding paragraph, for each $w \in \mathcal{T}_3$ there exists a w-admissible function $f_w = \sum_{i=1}^{e_k} c_{w,i} u_i$ of level k with $c_{w,i} \in K_3$. By Corollary 3.3, there exists $\gamma > 0$ such that if $w \in \mathcal{T}_3$ and $\mathbf{c}' \in N^{e_k}$ satisfy $w(\mathbf{c}' - \mathbf{c}_w) > \gamma$, then $f' = \sum_{i=1}^{e_k} c_i' u_i$ is a w-admissible function of level k.

Use the weak approximation theorem to choose $\mathbf{c} \in K_3^{e_k}$ such that $w(\mathbf{c} - \mathbf{c}_w) > \gamma$ for each $w \in \mathcal{T}_3$. Then $f = \sum_{i=1}^{e_k} c_i u_i$ is w-admissible of level k for each $w \in \mathcal{T}_3$. For each $\sigma \in \mathrm{Aut}(N/K_3)$ we have $f^\sigma = f$. Hence, by Lemma 3.5, f is w^σ-admissible. It follows that f is $\mathcal{T}$-admissible.

Finally suppose that $\mathbf{c}' \in N^{e_k}$ and $v(\mathbf{c}' - \mathbf{c}) > \gamma$ for each $v \in \mathcal{T}$. Write $v = w^\sigma$ with $w \in \mathcal{T}_3$ and $\sigma \in \mathrm{Aut}(N/K_3)$. Then $w((\mathbf{c}')^{\sigma^{-1}} - \mathbf{c}) > \gamma$ and hence $\sum_{i=1}^{e_k} (c_i')^{\sigma^{-1}} u_i$ is w-admissible of level k. We conclude from Lemma 3.5 that $f' = \sum_{i=1}^{e_k} c_i' u_i$ is v-admissible of level k. □

5. Good reduction

Consider a valuation v of $\tilde{K}F$ such that $v|_K \in \mathcal{V} \smallsetminus \mathcal{S}$. Denote the reduction with respect to v of objects associated with F by a bar over these objects. Thus $\bar{F}$ (resp., $\bar{M}$) is the residue field of F (resp., M). By Proposition 1.12(a), $\bar{M}$ is algebraically closed and therefore coincides with the residue field of $\tilde{K}$ at v. It follows that the residue field of $\tilde{K}F$ is $\bar{F}$. We will use these facts only to simplify our notation.

The function field $\tilde{K}F/\tilde{K}$ has **good reduction** at v if the following conditions hold:

(1a) There exists $f \in \tilde{K}F$ which is **v-regular**. That is, $v(f) = 0$, $\bar{f} \in \bar{F}$ is transcendental over $\bar{M}$, and $[\tilde{K}F : \tilde{K}(f)] = [\bar{F} : \bar{M}(\bar{f})]$. Thus $\bar{F}$ is a function field of one variable over $\bar{M}$.

(1b) $\mathrm{genus}(F/M) = \mathrm{genus}(\bar{F}/\bar{M})$.

In this case we also say that v is a **good extension** to $\tilde{K}F$ of $v|_{\tilde{K}}$. Note that if $g \in \tilde{K}F$ and $\bar{g}$ is transcendental over $\bar{M}$, then g is v-regular if and only if $\deg(g)_0 = \deg(\bar{g})_0$ or, equivalently, $\deg(g)_\infty = \deg(\bar{g})_\infty$.

The **support** of a divisor $\mathfrak{a}$ is the set $\mathfrak{p}_1, \dots, \mathfrak{p}_m$ of distinct prime divisors such that $\mathfrak{a} = \sum_{i=1}^m k_i \mathfrak{p}_i$ with nonzero integers k_i.

Corollary 5.2 connects regularity and admissibility of functions. It relies on a sort of reciprocity lemma:

Lemma 5.1 [Ro1, Cor. 3.9]. *Suppose that $\tilde{K}F/\tilde{K}$ has a good reduction at a valuation v. Let $f, g \in \tilde{K}F$ such that f is v-regular and $v(g) = 0$. Then, for each $\mathfrak{p} \in \Gamma(\tilde{K})$,*

$$\mathrm{Supp}(g)_\infty \subseteq \mathrm{Supp}(f)_\infty \text{ and } f(\mathfrak{p}) = 0 \text{ imply } v(g(\mathfrak{p})) \geq 0.$$

We extend each valuation $v \in \mathcal{V}_N \smallsetminus \mathcal{W}$ to the Henselian closure $N_v = \tilde{K}$ (recall that by Data 1.1(o), $\mathcal{S}_N \subseteq \mathcal{W}$). In this way we regard v also as a valuation of $\tilde{K}$.

Corollary 5.2. *Let $v \in \mathcal{V}_N \smallsetminus \mathcal{W}$ be a valuation with a good extension to $\tilde{K}F$. Suppose that $v(x_i) = 0$ if $x_i \neq 0$, for $i = 1, \dots, n$. Let $f \in NF$ be a v-regular function of level k (Definition 2.7). Suppose that each of the zeros of f is simple. Then f is v-admissible.*

Proof. Since $N_v = \tilde{K}$, we have to verify only condition (2c) of Definition 2.7. By assumption $(f)_\infty = k\mathfrak{d}$. Hence, by Data 2.1, $\mathrm{Supp}(f)_\infty = \bigcup_{i=1}^n \mathrm{Supp}(x_i)_\infty$. So, if $\mathfrak{p} \in \Gamma(\tilde{K})$ is a zero of f and $x_i \neq 0$, then $v(x_i) = 0$ and therefore $v(x_i(\mathfrak{p})) \geq 0$ (Lemma 5.1). If $x_i = 0$, then $v(x_i(\mathfrak{p})) = \infty > 0$. We conclude that f is v-admissible. □

In the remainder of this section we explore when functions are regular. This depends on the following extension of the reduction map of elements modulo v to divisors.

Proposition 5.3 [Ro1, p. 247]. *Suppose that $\tilde{K}F/\tilde{K}$ has a good reduction at v. Then there is a natural homomorphism $\mathfrak{a} \mapsto \bar{\mathfrak{a}}$ of $\mathrm{Div}(\tilde{K}F/\tilde{K})$ into $\mathrm{Div}(\bar{F}/\bar{M})$ with the following properties:*

(a) $\deg(\mathfrak{a}) = \deg(\bar{\mathfrak{a}})$.
(b) $\mathfrak{a} \geq 0$ *implies* $\bar{\mathfrak{a}} \geq 0$.
(c) $v(f) = 0$ *implies* $\overline{(f)} = (\bar{f})$.

Lemma 5.4. *Suppose that $\tilde{K}F/\tilde{K}$ has a good reduction at v and let f be an element of $\tilde{K}F$ such that $\bar{f}$ is transcendental over $\bar{M}$. Then $(\bar{f})_0 \leq \overline{(f)_0}$ (resp., $(\bar{f})_\infty \leq \overline{(f)_\infty}$). Equality holds if and only if f is v-regular.*

Proof. By Proposition 5.3(c), $(\bar{f})_0 - (\bar{f})_\infty = (\bar{f}) = \overline{(f)} = \overline{(f)_0} - \overline{(f)_\infty}$. Since $\overline{(f)_\infty} \geq 0$ (Proposition 5.3(b)) and since $(\bar{f})_0$ and $(\bar{f})_\infty$ are relatively prime, $(\bar{f})_0 \leq \overline{(f)_0}$. Similarly, $(\bar{f})_\infty \leq \overline{(f)_\infty}$.

Now, f is v-regular if and only if $\deg(f)_0 = \deg(\bar{f})_0$. Since by Proposition 5.3(a) $\deg(f)_0 = \deg \overline{(f)_0}$, the preceding paragraph implies that the latter condition is equivalent to $(\bar{f})_0 = \overline{(f)_0}$. Similarly, f is v-regular if and only if $(\bar{f})_\infty = \overline{(f)_\infty}$. □

Lemma 5.5. *Suppose that $\tilde{K}F/\tilde{K}$ has a good reduction at v. Let $\mathfrak{a}$ be a positive divisor of $\tilde{K}F/\tilde{K}$. For each i between 1 and m let k_i be a positive integer and let $f_i \in \tilde{K}F$ be a v-regular function such that $(f_i)_\infty = k_i\mathfrak{a}$. Let $k = k_1 + \cdots + k_m$. Then $f = f_1 \cdots f_m$ is also v-regular and $(f)_\infty = k\mathfrak{a}$.*

Proof. By assumption, $(f_i)_0$ is relatively prime to $\mathfrak{a}$. Hence $(f)_\infty = k\mathfrak{a}$.

As f_i is v-regular, $(\bar{f}_i)_\infty = k_i\bar{\mathfrak{a}}$ (Lemma 5.4). Hence, as before, $(\bar{f})_\infty = k\bar{\mathfrak{a}}$. Thus $\bar{f}$ is transcendental over $\bar{M}$ and $(\bar{f})_\infty = \overline{(f)_\infty}$. We conclude from Lemma 5.4 that f is v-regular. □

Lemma 5.6. *Let E/L be a function field of one variable and let k be a positive integer. Consider distinct prime divisors $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ of degree 1. For each i let $y_i \in E$ with $(y_i)_\infty = k\mathfrak{p}_i$ and let $c_i \in L$. Let $\mathfrak{a} = \mathfrak{p}_1 + \cdots + \mathfrak{p}_m$. Let f be an element of E such that*

$$f \equiv \sum_{i=1}^{m} c_i y_i \mod \mathcal{L}_L((k-1)\mathfrak{a}).$$

Then $(f)_\infty = k\mathfrak{a}$ if and only if $c_1, \ldots, c_m \neq 0$.

Proof. Suppose first that $c_i \neq 0$ for $i = 1, \ldots, m$. Let $g = f - \sum_{i=1}^{m} c_i y_i$. For each i denote the normalized valuation of E/L associated with $\mathfrak{p}_i$ by w_i. Then $-k = w_i(y_i) < \min\{w_i(y_j), w_i(g) \mid j \neq i\}$. Hence, $w_i(f) = -k$, and so $(f)_\infty = k\mathfrak{a}$.

To prove the other direction note that if $c_i = 0$, then $(f)_\infty \leq k\mathfrak{a} - \mathfrak{p}_i$. □

The following result is a well known consequence of the Bertini-Noether theorem. For example, it appears in [Ro2] without a proof. So, we give here only a sketch of the proof.

Proposition 5.7. *Let $t_1, \ldots, t_l$ be nonconstant functions of $\tilde{K}F$ and let $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ be distinct primes in $\Gamma(\tilde{K})$. Then there exists a finite subset A of $K^\times$ such that if $v \in \tilde{\mathcal{V}}$ satisfies $v(a) = 0$ for each $a \in A$, then v has a good extension to $\tilde{K}F$, which we also denote by v, such that t_i is v-regular, $i = 1, \ldots, l$, and the reduced primes $\bar{\mathfrak{p}}_1, \ldots, \bar{\mathfrak{p}}_m$ are distinct.*

Proof (Sketch). Let $E = \tilde{K}F$. Choose a separating transcendence element t for $E/\tilde{K}$. Use Section 7 of [De2] to find a finite subset A_0' of $(\tilde{K})^\times$ such that if $v \in \tilde{\mathcal{V}}$ satisfies $v(a) = 0$ for each $a \in A_0'$, then v has a unique good extension to E, which we also denote by v, such that t is v-regular. (Note that the valuations in [De2] are discrete. So, one first has to replace $\tilde{K}$ by a finite extension of K, or argue directly.)

Now choose $f \in E$ such that $f(\mathfrak{p}_1), \dots, f(\mathfrak{p}_m)$ are finite and distinct. Add f to $\{t_1, \dots, t_l\}$, if necessary, to assume that f is one of the t_i's. Also choose an irreducible polynomial $h_i \in \tilde{K}[T_i, T]$ such that $h_i(t_i, t) = 0$, $i = 1, \dots, l$. By Bertini-Noether [FrJ, Prop. 9.29], there exists a finite subset A' of $(\tilde{K})^\times$ which contains A_0' such that if $v \in \tilde{\mathcal{V}}$ satisfies $v(a) = 0$ for each $a \in A'$, then $\bar{h}_i(T_i, T)$ is irreducible of the same degree in T_i and in T as $h(T_i, T)$, $i = 1, \dots, l$, and $\overline{f(\mathfrak{p}_1)}, \dots, \overline{f(\mathfrak{p}_m)}$ are distinct.

It is now convenient to denote $\tilde{K}$ by L. By the choice of A_0', $[\bar{E} : \bar{L}(\bar{t})] = [E : L(t)]$. By the choice of A',

$$[\bar{L}(\bar{t}, \bar{t}_i) : \bar{L}(\bar{t})] = [L(t, t_i) : L(t)] \quad \text{and} \quad [\bar{L}(\bar{t}, \bar{t}_i) : \bar{L}(\bar{t}_i)] = [L(t, t_i) : L(t_i)].$$

Hence, $[\bar{E} : \bar{L}(\bar{t}_i)] = [E : L(t_i)]$. It follows that t_i is regular at v for $i = 1, \dots, l$.

In particular, f is regular at v. Hence $\bar{f}(\bar{\mathfrak{p}}) = \overline{f(\mathfrak{p})}$ for every prime divisor $\mathfrak{p}$ of E/L [Ro1, Prop. 3.8]. It follows from the choice of A' that $\bar{f}(\bar{\mathfrak{p}}_1), \dots, \bar{f}(\bar{\mathfrak{p}}_m)$ are distinct. We conclude that $\bar{\mathfrak{p}}_1, \dots, \bar{\mathfrak{p}}_m$ are distinct.

Finally, replace each $a \in A'$ by the set of all nonzero coefficients of $\mathrm{irr}(a, K)$ and $\mathrm{irr}(a^{-1}, K)$ to obtain the desired set A. □

6. Criteria for regularity

We give here two criteria for regularity of functions of $\tilde{K}F$. The first is formulated in terms of a basis of $\mathcal{L}_{\tilde{K}}(k\mathfrak{p}_{ij}^*)$ modulo $\mathcal{L}_{\tilde{K}}((k-1)\mathfrak{p}_{ij}^*)$ (Data 2.1). Here it is important that $\deg(\mathfrak{p}_{ij}^*) = 1$. The second one, which is built on the first, is formulated in terms of a basis of $\mathcal{L}_M(k\mathfrak{p}_i^*)$ modulo $\mathcal{L}_M((k-1)\mathfrak{p}_i^*)$. In both criteria k has to be large.

Lemma 6.1 (First criterion for regularity). *Let k be an integer $\geq 2\,\mathrm{genus}(F/M) + 1$, and let t_{ij} be an element of $\tilde{K}F$ such that $(t_{ij})_\infty = k\mathfrak{p}_{ij}^*$, $i = 1, \dots, e$, $j = 1, \dots, d_i$. Suppose that $\tilde{K}F/\tilde{K}$ has good reduction at a valuation v such that the reduced primes $\overline{\mathfrak{p}_{ij}^*}$ are distinct and the t_{ij} are v-regular. Let*

$$f = \sum_{i=1}^{e} \sum_{j=1}^{d_i} c_{ij} t_{ij} + g \tag{1}$$

with $c_{ij} \in \tilde{K}$ such that $v(c_{ij}) = 0$ and $g \in \mathcal{L}_{\tilde{K}}((k-1)\mathfrak{d})$ with $v(g) \geq 0$. Then

(a) *$\{t_{ij} \mid i = 1, \dots, e;\ j = 1, \dots, d_i\}$ is a basis for $\mathcal{L}_{\tilde{K}}(k\mathfrak{d})$ modulo $\mathcal{L}_{\tilde{K}}((k-1)\mathfrak{d})$, and*

(b) *f is v-regular of level k.*

Proof of (a). As $\tilde{K}$ is algebraically closed, $\deg(\mathfrak{p}_{ij}^*) = 1$. Hence, t_{ij} form a basis for $\mathcal{L}_{\tilde{K}}(k\mathfrak{p}_{ij}^*)$ modulo $\mathcal{L}_{\tilde{K}}((k-1)\mathfrak{p}_{ij}^*)$. We conclude from Lemma 4.1 that the t_{ij} form a basis for $\mathcal{L}_{\tilde{K}}(k\mathfrak{d})$ modulo $\mathcal{L}_{\tilde{K}}((k-1)\mathfrak{d})$. □

Proof of (b). By Lemma 5.6, $(f)_\infty = k\mathfrak{d}$.

Now reduce (1) modulo v to obtain $\bar{f} = \sum_{i=1}^{e}\sum_{j=1}^{d_i} \bar{c}_{ij}\bar{t}_{ij} + \bar{g}$. By assumption $\mathfrak{a} = (g) + (k-1)\mathfrak{d} \geq 0$. If $v(g) > 0$, then $\bar{g} = 0$. Otherwise, $v(g) = 0$ and $(\bar{g}) + (k-1)\bar{\mathfrak{d}} = \bar{\mathfrak{a}} \geq 0$ (Proposition 5.3). Hence, in both cases $\bar{g} \in \mathcal{L}_{\bar{M}}((k-1)\bar{\mathfrak{d}})$. Since t_{ij} is v-regular, $(\bar{t}_{ij})_\infty = k\overline{\mathfrak{p}_{ij}^*}$ (Lemma 5.4). By assumption, $\bar{c}_{ij} \neq 0$ for all i and j. Hence, we may apply Lemma 5.6 to $\bar{F}/\bar{M}$ instead of to E/L and conclude that $(\bar{f})_\infty = k\bar{\mathfrak{d}} = \overline{(f)_\infty}$. Thus, by Lemma 5.4, f is v-regular of level k. □

Data 6.2. Write each $k \geq s = 2\,\mathrm{genus}(F/M) + 2$ as $k = qs + r$ with $q \geq 0$ and $s \leq r \leq 2s-1$.

(a) Use the Riemann-Roch theorem to choose $t_{ijr} \in \tilde{K}F$ such that $(t_{ijr})_\infty = r\mathfrak{p}_{ij}^*$, $i = 1, \ldots, e$, $j = 1, \ldots, d_i$, $r = s, \ldots, 2s-1$.

(b) Let $t_{ijk} = t_{ijs}^q t_{ijr}$, $i = 1, \ldots, e$, $j = 1, \ldots, d_i$.

(c) By Remark 2.2(b), $\mathfrak{p}_i^* = \mathfrak{p}_{i1}^* + \cdots + \mathfrak{p}_{id_i}^*$. Hence, by Lemma 4.1, $t_{i1r}, \ldots, t_{id_ir}$ form a basis for $\mathcal{L}_{\tilde{K}}(r\mathfrak{p}_i^*)$ modulo $\mathcal{L}_{\tilde{K}}((r-1)\mathfrak{p}_i^*)$. According to Data 4.2, $(u_{ijr})_\infty = r\mathfrak{p}_i^*$ and in particular $u_{ijr} \in \mathcal{L}_{\tilde{K}}(r\mathfrak{p}_i^*)$. Thus there exist unique $b_{ijlr} \in \tilde{K}$ such that

$$u_{ijr} \equiv \sum_{l=1}^{d_i} b_{ijlr} t_{ilr} \mod \mathcal{L}_{\tilde{K}}((r-1)\mathfrak{p}_i^*) \tag{2}$$

By Lemma 5.6, $b_{ijlr} \neq 0$.

(d) Set $\mathbf{Y}_i = (Y_{i1}, \ldots, Y_{i,d_i})$, $i = 1, \ldots, e$, and consider the linear form

$$\lambda_{ilr}(\mathbf{Y}_i) = \sum_{j=1}^{d_i} Y_{ij} b_{ijlr}, \qquad l = 1, \ldots, d_i. \qquad \square$$

Lemma 6.3 (Second criterion for regularity). *Let k be an integer greater than or equal to $s = 2\,\mathrm{genus}(F/M) + 2$ and let $a_{ij}, a_\mu \in \tilde{K}$, $i = 1, \ldots, e$, $j = 1, \ldots, d_i$, $\mu = 1, \ldots, e_{k-1}$. Consider the element*

$$f = \sum_{i=1}^{e}\sum_{j=1}^{d_i} a_{ij} u_{ijk} + \sum_{\mu=1}^{e_{k-1}} a_\mu u_\mu \tag{3}$$

of $\tilde{K}F$. Suppose that $\tilde{K}F$ has a good reduction at v such that the following conditions are satisfied:

(a) *The $\overline{\mathfrak{p}_{ij}^*}$ are distinct,*

(b) *t_{ijr} is v-regular,*

(c) *$v(u_\mu) \geq 0$ (Notation 4.4),*

(d) *$v(b_{ijlr}) = 0$,*

(e) *$v(a_{\mu'}) \geq 0$ and $v(a_{ij}) \geq 0$, and*

(f) *$v(\lambda_{ilr}(\mathbf{a}_i)) = 0$, where $\mathbf{a}_i = (a_{i1}, \ldots, a_{i,d_i})$,*

for $\mu = 1, \ldots, e_{2s-1}$, $\mu' = 1, \ldots, e_{k-1}$, $i = 1, \ldots, e$, $j, l = 1, \ldots, d_i$, and $r = s, \ldots, 2s-1$. Then f is v-regular of level k. □

Proof. Write $k = qs + r$ with $q \geq 0$ and $s \leq r \leq 2s-1$. By (b) and Data 6.2(a), t_{ijs} is v-regular with $(t_{ijs})_\infty = s\mathfrak{p}_{ij}^*$ and t_{ijr} is v-regular with $(t_{ijr})_\infty = r\mathfrak{p}_{ij}^*$. Hence, by Lemma 5.5, $t_{ijk} = t_{ijs}^q t_{ijr}$ is v-regular with $(t_{ijk})_\infty = k\mathfrak{p}_{ij}^*$, for $i = 1, \ldots, e$ and $j = 1, \ldots, d_i$.

By Data 4.2 and by (2)

$$u_{ijk} = u_{i1s}^q u_{ijr} \equiv \big(\sum_{l=1}^{d_i} b_{i1ls} t_{ils}\big)^q \big(\sum_{l=1}^{d_i} b_{ijlr} t_{ilr}\big) \mod \mathcal{L}_{\tilde{K}}((k-1)\mathfrak{p}_i^*). \tag{4}$$

A general term of the expansion of the right hand side of (4) has the form bt, where $b = b_{i,1,l_1,s} \cdots b_{i,1,l_q,s} b_{i,j,l_{q+1},r}$ and $t = t_{i,l_1,s} \cdots t_{i,l_q,s} t_{i,l_{q+1},r}$ and $1 \le l_1, \dots, l_{q+1} \le d_i$. For each l between 1 and d_i denote the normalized valuation of $\tilde{K}F/\tilde{K}$ associated with $\mathfrak{p}_{il}^*$ by w_{il}. Then, $w_{ij}(t_{ijk}) = -k$ and $w_{il}(t_{ijk}) = 0$ if $l \ne j$. Hence,

$$w_{il}(bt) = w_{il}(t_{il_1 s}) + \cdots + w_{il}(t_{il_q s}) + w_{il}(t_{il_{q+1} r}) \ge -(qs + r) = -k$$

and equality holds if and only if $l_1 = \cdots = l_{q+1} = l$. If the condition $l_1 = \cdots = l_{q+1}$ is not satisfied, then $w_{il}(bt) \ge -(k-1)$ for $l = 1, \dots, d_i$. As $\mathfrak{p}_i^* = \mathfrak{p}_{i1}^* + \cdots + \mathfrak{p}_{id_i}^*$, this implies that bt belongs to $\mathcal{L}_{\tilde{K}}((k-1)\mathfrak{p}_i^*)$ and therefore to $\mathcal{L}_{\tilde{K}}((k-1)\mathfrak{d})$. If $l_1 = \cdots = l_{q+1} = l$ for some l between 1 and d_i, then $bt = b_{i1ls}^q b_{ijlr} t_{ilk}$ (Data 6.2(b)). It follows that

$$u_{ijk} \equiv \sum_{l=1}^{d_i} b_{i1ls}^q b_{ijlr} t_{ilk} \mod \mathcal{L}_{\tilde{K}}((k-1)\mathfrak{d}).$$

Hence

$$\begin{aligned} f &\equiv \sum_{i=1}^{e} \sum_{j=1}^{d_i} a_{ij} u_{ijk} \equiv \sum_{i=1}^{e} \sum_{j=1}^{d_i} \sum_{l=1}^{d_i} a_{ij} b_{i1ls}^q b_{ijlr} t_{ilk} \\ &\equiv \sum_{i=1}^{e} \sum_{l=1}^{d_i} b_{i1ls}^q \big(\sum_{j=1}^{d_i} a_{ij} b_{ijlr}\big) t_{ilk} \equiv \sum_{i=1}^{e} \sum_{l=1}^{d_i} b_{i1ls}^q \lambda_{ilr}(\mathbf{a}_i) t_{ilk} \\ &\equiv \sum_{i=1}^{e} \sum_{l=1}^{d_i} c_{il} t_{ilk} \mod \mathcal{L}_{\tilde{K}}((k-1)\mathfrak{d}), \end{aligned} \tag{5}$$

with $c_{il} = b_{i1ls}^q \lambda_{ilr}(\mathbf{a}_i)$. By (d) and (f), $v(c_{il}) = 0$. By (c), $v(u_\mu) \ge 0$, $\mu = 1, \dots, e_{2s-1}$. Hence, by Notation 4.4, $v(u_{ijr}) \ge 0$ for $i = 1, \dots, e$, $j = 1, \dots, d_i$, and $r = s, \dots, 2s-1$. By Data 4.2 and Notation 4.4, for each $\kappa \ge s$ the function u_κ is a product of functions which belong to the set $\{u_{ijs}, \dots, u_{ij,2s-1} |\ i = 1, \dots, e;\ j = 1, \dots, d_i\}$. Hence $v(u_\kappa) \ge 0$. In particular, $v(u_{ijk}) \ge 0$. Hence, by (3) and (e), $v(f) \ge 0$. So, by (5), $g = f - \sum_{i=1}^{e} \sum_{l=1}^{d_i} c_{il} t_{ilk}$ belongs to $\mathcal{L}_{\tilde{K}}((k-1)\mathfrak{d})$ and satisfies $v(g) \ge 0$. We see by Lemma 6.1 that f is v-regular of level k. □

7. Admissible functions along $\mathcal{V}_N$

To create a $\mathcal{V}_N$-admissible function we first use Proposition 5.7 to define a big subset $\mathcal{U}$ of $\mathcal{V}_N$ which takes into account all conditions of Lemma 6.3 which do not concern $\mathbf{a}$. Then, for $\mathcal{T} = \mathcal{V}_N \smallsetminus \mathcal{U}$, we select f of the form (3) of Section 6, so that f is $\mathcal{T}$-admissible. The final step is to use Proposition 1.12(c), Lemma 6.3, and Corollary 5.2 to change the a_{ij}'s so that f also becomes $\mathcal{U}$-admissible (and hence $\mathcal{V}_N$-admissible) and then to use Proposition 1.12(d) to change the a_μ's that in addition f has an M-rational zero.

Data 7.1. We extend each valuation $v \in \mathcal{V}_N \smallsetminus \mathcal{W}$ to a valuation of the Henselian closure $N_v = \tilde{K}$ (Proposition 1.12(a)) with the same name. We use Proposition 5.7 to choose a big subset $\mathcal{U}$ of $\mathcal{V}_N \smallsetminus \mathcal{W}$ (which may be empty if $\mathcal{V}$ is finite) such

that the following statements hold for each $v \in \mathcal{U}$ and for $s = 2\,\mathrm{genus}(F/M) + 2$, $i = 1, \dots, e$, $r = s, \dots, 2s-1$, $j, l = 1, \dots, d_i$, $\mu = 1, \dots, e_{2s-1}$, and $\nu = 1, \dots, n$:

(1a) v has a good extension to $\tilde{K}F$ named v,
(1b) the $\overline{\mathfrak{p}_{ij}^*}$ are distinct,
(1c) t_{ijr} is v-regular,
(1d) $v(u_\mu) \geq 0$ (Notation 4.4),
(1e) $v(b_{ijlr}) = 0$,
(1f) $v(x_\nu) = 0$ if $x_\nu \neq 0$.

Note that $b_{ijlr} \neq 0$ (Data 6.2(c)). So, we may achieve condition (1e). Make $\mathcal{U}$ smaller, if necessary, to assume that $\mathcal{U}$ is K-rational (Definition 2.8). Then, $\mathcal{T} = \mathcal{V}_N \smallsetminus \mathcal{U}$ is a K-rational small subset of $\mathcal{V}_N$ which contains $\mathcal{W}$. □

Notation 7.2. For each positive integer $k \geq s = 2\,\mathrm{genus}(F/M) + 2$ we denote the space $\mathbb{A}^{e_{k-1}} \times \mathbb{A}^{d_1} \times \cdots \times \mathbb{A}^{d_e}$ by A_k. The zero coordinate of a point $\mathbf{a} \in A_k$ is an e_{k-1}-tuple $\mathbf{a}_0 = (a_1, \dots, a_{e_{k-1}})$ and for each $i \geq 1$ the ith coordinate is a d_i-tuple $\mathbf{a}_i = (a_{i1}, \dots, a_{i,d_i})$. □

Proposition 7.3 (Density of admissible functions). *Let $k_0 \geq s = 2\,\mathrm{genus}(F/M) + 2$. Then there exist $k \geq k_0$, a point $\mathbf{c} \in A_k(M)$, and a positive integer γ with the following property: If $\mathbf{a} \in A_k(N)$ satisfies*

(2a) *$V_{\mathcal{T}}(\mathbf{a} - \mathbf{c}) > \gamma$ and*
(2b) *$v(\mathbf{a}) \geq 0$ and $v(\lambda_{ilr}(\mathbf{a}_i)) = 0$ for each $v \in \mathcal{U}$, for $i = 1, \dots, e$, $r = s, \dots, 2s-1$, and $l = 1, \dots, d_i$,*

then the function

$$f = \sum_{i=1}^{e} \sum_{j=1}^{d_i} a_{ij} u_{ijk} + \sum_{\mu=1}^{e_{k-1}} a_\mu u_\mu \tag{3}$$

is $\mathcal{V}_N$-admissible of level k.

Proof. Rename the function f that Proposition 4.5 supplies as h and rewrite h in the form

$$h = \sum_{i=1}^{e} \sum_{j=1}^{d_i} c_{ij} u_{ijk} + \sum_{\mu=1}^{e_{k-1}} c_\mu u_\mu,$$

with $\mathbf{c} \in A_k(M)$. Retain also the role of k and γ from Proposition 4.5.

Suppose now that $\mathbf{a} \in A_k(N)$ satisfies condition (2) and f is as in (3). By Proposition 4.5, f is $\mathcal{T}$-admissible of level k. By Data 7.1, (2b), and Lemma 6.3, f is v-regular of level k for each $v \in \mathcal{U}$. In particular, each of the zeros of f is N-rational and simple. By Data 7.1, $\tilde{K}F/\tilde{K}$ has a good reduction at each $v \in \mathcal{U}$. Since f is of level k and $v(x_i) = 0$ if $x_i \neq 0$ for $i = 1, \dots, n$, Corollary 5.2 implies that f is v-admissible. Therefore f is $\mathcal{V}_N$-admissible. □

Proposition 7.4 (Existence of admissible functions). *For each k_0 there exists a $\mathcal{V}_N$-admissible function $f \in F$ of level $k \geq k_0$ which has an M-rational zero.*

Proof. Let k_1 be an integer which is greater than k_0 and $2\,\mathrm{genus}(F/M) + 2$. Now let $k \geq k_1$, $\mathbf{c} \in A_k(M)$ and γ be as in Proposition 7.3. Then $e_{k-1} = \dim((k-1)\mathfrak{d}) \geq 2$ (Notation 4.4).

By (1e), the coefficients of the $\lambda_{ilr}(\mathbf{Y}_i)$ (Data 6.2(d)) are $\mathcal{T}$-units. The same holds for the polynomials Y_{ij}. Also, by Data 7.1, $\mathcal{T}$ is a K-rational small subset of

$\mathcal{V}_N$ which contains $\mathcal{S}_N$. Thus we may apply Proposition 1.12(c) to choose for each i between 1 and e a point $\mathbf{a}_i \in M^{d_i}$ such that $V_{\mathcal{T}}(\mathbf{a}_i - \mathbf{c}_i) > \gamma$, and $v(a_{ij}) = 0$ and $v(\lambda_{ilr}(\mathbf{a}_i)) = 0$ for each $v \in \mathcal{U}$ and for $r = s, \dots, 2s-1$, $j, l = 1, \dots, d_i$.

The field $L = K(c_1, \dots, c_{e_{k-1}})$ is a finite subextension of M/K. As $\mathcal{T}$ is K-rational, we may apply the strong approximation theorem to L (Proposition 1.11(c)) and find $\mathbf{c}_0' \in L^{e_{k-1}}$ such that $V_{\mathcal{T}}(\mathbf{c}_0' - \mathbf{c}_0) > \gamma$ and $v(\mathbf{c}_0') \geq 0$ for each $v \in \mathcal{U}$. Choose $0 \neq m \in O$ such that $V_{\mathcal{T}}(m) > \gamma$ (recall that $\mathcal{T}|_K$ is a finite set).

Let $g = \sum_{i=1}^{e} \sum_{j=1}^{d_i} a_{ij} u_{ijk}$ and $f' = g + \sum_{\mu=1}^{e_{k-1}} c_\mu' u_\mu$. Since the u_μ and the u_{ijk} are linearly independent over M, $u_1 = 1$, and $a_{ij} \neq 0$, we have $f' \in F \smallsetminus M$. Let $t = -\frac{1}{m} f'$. By Proposition 7.3, f' is $\mathcal{V}_N$-admissible of level k. In particular, all the zeros of f' (hence, also of t) are simple and in $\Gamma(N)$. By Proposition 1.12(d), there exists $\mathfrak{p} \in \Gamma(M)$ which is a pole of none of the functions $t, g, u_1, \dots, u_{e_{k-1}}$ such that $t(\mathfrak{p}) \in O_M$. Let $a_1 = mt(\mathfrak{p}) + c_1'$, $a_2 = c_2', \dots, a_{e_{k-1}} = c_{e_{k-1}}'$, and $\mathbf{a}_0 = (a_1, \dots, a_{e_{k-1}})$. Then $V_{\mathcal{T}}(\mathbf{a}_0 - \mathbf{c}_0) > \gamma$ and $v(\mathbf{a}_0) \geq 0$ for each $v \in \mathcal{U}$. Since $u_1 = 1$, we have

$$mt + f' = g + (mt + c_1') + c_2' u_2 + \cdots + c_{e_{k-1}}' u_{e_{k-1}} = 0.$$

Hence, $\mathfrak{p}$ is a zero of the function

$$f = mt(\mathfrak{p}) + f' = g + \sum_{\mu=1}^{e_{k-1}} a_\mu u_\mu.$$

Thus $\mathbf{a} = (\mathbf{a}_0, \mathbf{a}_1, \dots, \mathbf{a}_e) \in A_k(M)$ satisfies (2) and f has the form (3). By Proposition 7.3, f is $\mathcal{V}_N$-admissible of level k. □

Proposition 7.4 is a reformulation of Theorem 2.5. The latter implies Theorem 2.4, which is a reformulation of Theorem 1.2(c) for curves. We state the latter for the record.

Proposition 7.5 (Approximation theorem for integral points on curves). *Let C be an absolutely irreducible affine curve defined over K. Suppose that $C(O_{N,v}) \neq \emptyset$ for each $v \in \mathcal{V}_N \smallsetminus \mathcal{W}$. Consider $(\mathbf{z}_w)_{w \in \mathcal{W}} \in C_{O,\mathcal{S},\mathcal{W}}$ and a positive integer γ. Then there exists $\mathbf{z} \in C(O_M)$ such that $w(\mathbf{z} - \mathbf{z}_w) > \gamma$ for each $w \in \mathcal{W}$.*

8. The approximation theorems and the local global principle for arbitrary affine varieties

In this section we use the approximation theorem for integral points on curves to prove the approximation theorem for integral points on arbitrary varieties. We then prove all other theorems of Section 1.

Lemma 8.1. *Let V be an absolutely irreducible variety defined over K. Let $\mathcal{R}_1$ be a finite subset of $\mathcal{V}_N$ whose elements are mutually nonconjugate over K. For each $v \in \mathcal{R}_1$ let $\mathbf{z}_v \in V(N_v)$. Let $\mathcal{R} = \{v^\sigma \mid v \in \mathcal{R}_1,\ \sigma \in \mathrm{Aut}(N/K)\}$. Then we can find a finite extension L of M/K and extend the point $(\mathbf{z}_v)_{v \in \mathcal{R}_1}$ into a point $(\mathbf{z}_w)_{w \in \mathcal{R}}$ such that $\mathbf{z}_w \in V(L_w)$ and $\mathbf{z}_{w^\sigma} = \mathbf{z}_w^\sigma$ for each $w \in \mathcal{R}$ and each $\sigma \in \mathrm{Aut}(N/L)$.*

Proof. We first prove that M/K has a finite subextension L such that $\mathbf{z}_v^\sigma \in V(L_{v^\sigma})$ for each $v \in \mathcal{R}_1$ and each $\sigma \in \mathrm{Aut}(N/K)$. It suffices to do it in the case that $\mathcal{R}_1$ consists of one valuation v.

First choose a finite normal subextension E of N/K such that $\mathbf{z}_v \in V(E_v)$. Let $K' = E \cap K_{\mathrm{ins}}$. Since M is perfect, $K' \subseteq M$. Then E/K' is a finite Galois

extension, and as such it has a primitive element y. Let γ be an integer which is larger than $v(y-y')$ for all conjugates y' of y over K' with $y' \neq y$. By Proposition 1.12(b) applied to all conjugates of y instead of to x, there exists a finite subset B of M with the following property: For each $w \in \mathcal{V}_N$ which lies over $v|_K$ and each conjugate y' of y over K' there exists $b \in B$ such that $w(b-y') > \gamma$. Then $L = K'(B)$ is a finite subextension of M/K.

Consider $\sigma \in \mathrm{Aut}(N/K)$ and let $w = v^\sigma$, $y' = y^\sigma$. Choose $b \in B$ such that $w(b-y') > \gamma$. By Krasner's lemma [Lan, p. 43], $K'_w(y^\sigma) \subseteq K'_w(b) \subseteq LK_w = L_w$. Hence $\mathbf{z}_v^\sigma \in V(K'_w(y^\sigma)) \subseteq V(L_{v^\sigma})$, as asserted.

Now choose a finite subset $\mathcal{R}_2$ of $\mathcal{R}$ that contains $\mathcal{R}_1$ and represents $\mathcal{R}|_L$ (Definition 2.8). For each $w \in \mathcal{R}_2 \smallsetminus \mathcal{R}_1$ there exists a unique $v \in \mathcal{R}_1$ such that $w|_K = v|_K$. Choose $\lambda \in \mathrm{Aut}(N/K)$ such that $w = v^\lambda$ and define $\mathbf{z}_w = \mathbf{z}_v^\lambda$. Then $\mathbf{z}_w \in V(L_w)$.

If $\sigma \in \mathrm{Aut}(N/L)$ satisfies $w^\sigma = w$, then $\sigma \in \mathrm{Aut}(N/N \cap L_w)$. Hence, the unique extension of σ to N_w (Data 1.1(l)) fixes the elements of L_w. In particular $\mathbf{z}_w^\sigma = \mathbf{z}_w$. It follows that if for arbitrary $w \in \mathcal{R}_2$ and $\tau \in \mathrm{Aut}(N/L)$ we define $\mathbf{z}_{w^\tau} = \mathbf{z}_w^\tau$, then $\mathbf{z}_v$ is well defined for each $v \in \mathcal{R}$, it coincides with the original $\mathbf{z}_v$ if $v \in \mathcal{R}_1$, and it satisfies $\mathbf{z}_{v^\sigma} = \mathbf{z}_v^\sigma$ for each $v \in \mathcal{R}$ and $\sigma \in \mathrm{Aut}(N/L)$. □

We return now to the notation of Data 1.1, copy over Theorem 1.2, and prove it.

Theorem 8.2 (Strong approximation theorem). *Let V be an absolutely irreducible affine variety defined over K. Consider $(\mathbf{z}_w)_{w\in\mathcal{W}} \in V_{K,\mathcal{S},\mathcal{W}}$ and a positive integer γ.*

(a) *There exists $\mathbf{z} \in V(M)$ such that $w(\mathbf{z}-\mathbf{z}_w) > \gamma$ for each $w \in \mathcal{W}$.*
(b) *If $V(O_{N,v}) \neq \emptyset$ for each $v \in \mathcal{V}_N \smallsetminus \mathcal{W}$, then there exists $\mathbf{z} \in V(M)$ such that $w(\mathbf{z}-\mathbf{z}_w) > \gamma$ for each $w \in \mathcal{W}$ and $v(\mathbf{z}) \geq 0$ for each $v \in \mathcal{V}_N \smallsetminus \mathcal{W}$.*
(c) *If $V(O_{N,v}) \neq \emptyset$ for each $v \in \mathcal{V}_N \smallsetminus \mathcal{W}$, and $w(\mathbf{z}_w) \geq 0$ for each $w \in \mathcal{W}$, then there exists $\mathbf{z} \in V(O_M)$ such that $w(\mathbf{z}-\mathbf{z}_w) > \gamma$ for each $w \in \mathcal{W}$.*

Proof. By assumption $\mathbf{z}_w \in V_{\mathrm{sim}}(N_w)$. Also, there exists a finite subextension L of M/K such that $\mathbf{z}_w^\sigma = \mathbf{z}_{w^\sigma}$ for each $w \in \mathcal{W}$ and $\sigma \in \mathrm{Aut}(N/L)$. Our goal is to find a point $\mathbf{z} \in V(M)$ such that $w(\mathbf{z}-\mathbf{z}_w) > \gamma$ for each $w \in \mathcal{W}$. □

Proof of (c). Here we assume in addition that $V(O_{N,v}) \neq \emptyset$ for each $v \in \mathcal{V}_N \smallsetminus \mathcal{W}$ and $\mathbf{z}_w \in V_{\mathrm{sim}}(O_{N,w})$ for each $w \in \mathcal{W}$. We have to approximate the points $\mathbf{z}_w$ with $\mathbf{z} \in V(O_M)$.

Choose a point $\mathbf{z}_0 \in V(\tilde{K})$ and recall that $N_v = \tilde{K}$ for each $v \in \mathcal{V}_N \smallsetminus \mathcal{W}$. Let

$$\mathcal{U} = \{v \in \mathcal{V}_N \smallsetminus \mathcal{W} |\ v(\mathbf{z}_0^\sigma) \geq 0 \text{ for each } \sigma \in G(L)\}, \qquad \mathcal{T} = \mathcal{V}_N \smallsetminus \mathcal{U}.$$

Then $\mathcal{T}$ is an L-rational small set which contains $\mathcal{W}$. Choose a finite subset $\mathcal{W}_1$ of $\mathcal{W}$ which represents $\mathcal{W}|_L$ and a finite subset $\mathcal{R}_1$ of $\mathcal{R} = \mathcal{T} \smallsetminus \mathcal{W}$ which represents $\mathcal{R}|_L$ (Definition 2.8). Let $\mathcal{T}_1 = \mathcal{W}_1 \cup \mathcal{R}_1$.

For each $v \in \mathcal{R}_1$ choose $\mathbf{z}_v \in V(O_{N,v})$. Now use Lemma 8.1, for L instead of K, extend L (hence, also $\mathcal{W}_1$, $\mathcal{R}_1$, and $\mathcal{T}_1$), if necessary, and extend the point $(\mathbf{z}_v)_{v\in\mathcal{T}_1}$ to a point $(\mathbf{z}_v)_{v\in\mathcal{T}}$ such that $\mathbf{z}_v \in V(L_v)$ and $\mathbf{z}_{v^\sigma} = \mathbf{z}_v^\sigma$ for all $v \in \mathcal{T}$ and $\sigma \in \mathrm{Aut}(N/L)$. In particular, each $\mathbf{z}_v$ belongs to $V(O_{L,v})$, hence to $V(O_{N,v})$, and is separable over L. Now extend L again to assume that $\mathbf{z}_0$ is separable over L. Finally, if $v \in \mathcal{U}$, then $N_v = \tilde{K}$. So, let $\mathbf{z}_v = \mathbf{z}_0$.

In an appendix to this paper we show that there exists an affine absolutely irreducible curve C which is defined over L, hence also over M, which lies on V and

passes through $\mathbf{z}_0$ and through $\mathbf{z}_v$ for each $v \in \mathcal{T}_1$. Moreover, $\mathbf{z}_v$ is simple on C for each $v \in \mathcal{W}_1$. For an arbitrary $v' \in \mathcal{V}_N$ the point $\mathbf{z}_{v'}$ is conjugate over L to a point $\mathbf{z}_v$ for some $v \in \mathcal{T}_1 \cup \mathcal{U}$. Hence $\mathbf{z}_{v'}$ belongs to $C(O_{N,v'})$ and is simple if $v' \in \mathcal{W}$. So, $(\mathbf{z}_w)_{w\in\mathcal{W}} \in C_{O,\mathcal{S},\mathcal{W}}$.

By Proposition 7.5 and Remark 1.3(a), there exists $\mathbf{z} \in C(O_M)$ such that $w(\mathbf{z} - \mathbf{z}_w) > \gamma$ for each $w \in \mathcal{W}$. This is a point of V we have been looking for. □

Proof of (b). Here we only assume that $V(O_{N,v}) \neq \emptyset$ for each $v \in \mathcal{V}_N \smallsetminus \mathcal{W}$. We have to approximate the points $\mathbf{z}_w$ with a $\mathcal{W}$-integral point $\mathbf{z} \in V(M)$.

Since $(\mathbf{z}_w)_{w\in\mathcal{W}}$ is L-rational, the set $\{w(\mathbf{z}_w) \mid w \in \mathcal{W}\}$ is finite. Hence, $k = \max\{0, -w(\mathbf{z}_w)\}_{w\in\mathcal{W}}$ is a well defined nonnegative integer. By Proposition 1.12(c) applied to X instead of to f_i there exists $a \in M$ such that $w(a) \geq k$ for each $w \in \mathcal{W}$ and $v(a) = 0$ for each $v \in \mathcal{V}_N \smallsetminus \mathcal{W}$.

Consider the automorphism λ of $\mathbb{A}^n$ defined by $\lambda(\mathbf{x}) = a\mathbf{x}$. It maps V onto an absolutely irreducible variety V' which is defined over $K(a)$. For each $v \in \mathcal{V}_N \smallsetminus \mathcal{W}$ we have $V'(O_{N,v}) \neq \emptyset$. If $w \in \mathcal{W}$, then $\mathbf{z}'_w = a\mathbf{z}_w \in V'_{\mathrm{sim}}(O_{N,w})$. Moreover, if $\sigma \in G(L(a))$, then $\mathbf{z}'_{w^\sigma} = (\mathbf{z}'_w)^\sigma$.

Since $\mathcal{W}|_K$ is finite, the set $\{w(a) \mid w \in \mathcal{W}\}$ is bounded. Hence, by (c), there exists $\mathbf{z}' \in V'(O_M)$ such that $w(\mathbf{z}' - \mathbf{z}'_w) > \gamma + w(a)$ for each $w \in \mathcal{W}$. It follows that $\mathbf{z} = a^{-1}\mathbf{z}' \in V(M)$ and $w(\mathbf{z} - \mathbf{z}_w) > \gamma$ for each $w \in \mathcal{W}$. Finally, as a is a $\mathcal{W}$-unit, we have $v(\mathbf{z}) \geq 0$ for each $v \in \mathcal{V}_N \smallsetminus \mathcal{W}$. □

Proof of (a). Choose $\mathbf{z}_0 \in V(\tilde{K})$ and recall that $N_v = \tilde{K}$ for each $v \in \mathcal{V}_N \smallsetminus \mathcal{W}$. Then $\mathcal{U} = \{v \in \mathcal{V}_N \smallsetminus \mathcal{W} \mid v(\mathbf{z}_0^\sigma) \geq 0 \text{ for all } \sigma \in G(K)\}$ is a well defined K-rational big subset of $\mathcal{V}_N$. Hence, $\mathcal{T} = \mathcal{V}_N \smallsetminus \mathcal{U}$ and $\mathcal{R} = \mathcal{T} \smallsetminus \mathcal{W}$ are K-rational small subsets of $\mathcal{V}_N$.

As in the proof of (b), $k = \max\{0, -v(\mathbf{z}_0)\}_{v\in\mathcal{R}}$ is a well defined nonnegative integer. By Proposition 1.11(c), there exists $a \in M$ such that $v(a) \geq k$ for each $v \in \mathcal{R}$ and $v(a) = 0$ for each $v \in \mathcal{V}_N \smallsetminus \mathcal{R}$. Consider the automorphism λ of $\mathbb{A}^n$ defined by $\lambda(\mathbf{x}) = a\mathbf{x}$. It maps V onto an absolutely irreducible variety V' which is defined over $K(a)$. If $w \in \mathcal{W}$, then $\mathbf{z}'_w = a\mathbf{z}_w \in V'_{\mathrm{sim}}(N_w)$. Moreover, if $\sigma \in G(L(a))$, then $\mathbf{z}'_{w^\sigma} = (\mathbf{z}'_w)^\sigma$. If $v \in \mathcal{R}$, then $N_v = \tilde{K}$, and hence $\mathbf{z}'_v = a\mathbf{z}_0 \in V'(N_v)$ and satisfies $v(\mathbf{z}'_v) \geq 0$. Similarly, if $v \in \mathcal{U}$, then $\mathbf{z}'_v = a\mathbf{z}_0 \in V'(N_v)$ and $v(\mathbf{z}'_v) \geq 0$.

By (b), there exists $\mathbf{z}' \in V'(M)$ such that $w(\mathbf{z}' - \mathbf{z}'_w) > \gamma + w(a)$ for each $w \in \mathcal{W}$. Hence $\mathbf{z} = a^{-1}\mathbf{z}'$ belongs to $V(M)$ and satisfies $w(\mathbf{z} - \mathbf{z}_w) > \gamma$ for each $w \in \mathcal{W}$.

This concludes the proof of the theorem. □

Next we show how to deduce the weak approximation theorem from the strong approximation theorem.

Proof of Theorem 1.4(a). There exists a finite subextension K' of M/K over which V is defined and such that the map $\mathrm{res}\colon \mathcal{T} \to \mathcal{T}|_{K'}$ is injective. Assume without loss that $K' = K$. Extend each $v \in \mathcal{T}$ to a valuation of N, if necessary, to assume that $\mathcal{T} \subset \mathcal{V}_N$. Recall that $O_{M,v} = O_{N,v}$ for each $v \in \mathcal{V}_N$ (Proposition 1.12(a)).

For each $v \in \mathcal{T} \cap \mathcal{S}_N$ let $\mathbf{z}_v \in V_{\mathrm{sim}}(O_{N,v})$ and for each $v \in \mathcal{T} \smallsetminus \mathcal{S}_N$ let $\mathbf{z}_v \in V(O_{N,v})$. Also, let γ be a positive integer. We have to find $\mathbf{z} \in V(O_M)$ such that $v(\mathbf{z} - \mathbf{z}_v) > \gamma$ for each $v \in \mathcal{T}$.

Let $\mathcal{T}' = \{v^\sigma \mid v \in \mathcal{T},\ \sigma \in \mathrm{Aut}(N/K)\}$. Then $\mathcal{W} = \mathcal{S}_N \cup \mathcal{T}'$ and $\mathcal{R} = \mathcal{S}_N \smallsetminus \mathcal{T}'$ are K-rational small sets. Choose a finite subset $\mathcal{R}_1$ of $\mathcal{R}$ that represents $\mathcal{R}|_K$. Then $\mathcal{W}_1 = \mathcal{R}_1 \uplus (\mathcal{T} \cap \mathcal{S}_N) \uplus (\mathcal{T} \smallsetminus \mathcal{S}_N)$ represents $\mathcal{W}|_K$.

If $v \in \mathcal{T} \smallsetminus \mathcal{S}_N$, then $N_v = \tilde{K}$ (Proposition 1.12(a)). Since $V_{\mathrm{sim}}(\tilde{K})$ is Zariski open in $V(\tilde{K})$, it is v-dense in $V(\tilde{K})$ [Mum, p. 82]. Hence, we can assume without loss that $\mathbf{z}_v$ is simple. Finally, for each $v \in \mathcal{R}_1$ we choose $\mathbf{z}_v \in V_{\mathrm{sim}}(O_{N,v})$.

By Lemma 8.1, the point $(\mathbf{z}_w)_{w\in\mathcal{W}_1}$ extends to a point $(\mathbf{z}_w)_{w\in\mathcal{W}}$ of $V_{K,\mathcal{S},\mathcal{W}}$. So, Theorem 8.2(c) gives a point $\mathbf{z} \in V(O_M)$ such that $w(\mathbf{z} - \mathbf{z}_w) > \gamma$ for each $w \in \mathcal{W}$ and in particular for each $w \in \mathcal{T}$. □

Proof of Theorem 1.4(b). Replace the use of Theorem 8.2(c) in the proof of (a) by a use of Theorem 8.2(a). □

The assumption we made that M is weakly P$\mathcal{S}$C over O_M is not intrinsic because it involves the field N. We show below that, as a consequence of the strong approximation theorem, M has the more elegant property of being 'P$\mathcal{S}$C over O_M'. The stronger condition implies the weaker one and therefore eventually implies the strong approximation theorem. However, starting from an algebraic extension M_0 of K which is PAC over O (e.g., $\tilde{K}(\boldsymbol{\sigma})$, for almost all $\boldsymbol{\sigma} \in G(K)^e$), all we could prove for $M = M_0 \cap N$ at the beginning of the long proof is that M is weakly P$\mathcal{S}$C over O_M. So, we had to start with the latter condition.

Remark 8.3: P$\mathcal{S}$C fields. (a) A perfect algebraic extension L of K is said to be **P$\mathcal{S}$C** if every absolutely irreducible variety V defined over L has an L-rational point provided it has a simple L_v-rational point for each $v \in S_L$. Theorem 1.4(b) with $\mathcal{T} = \emptyset$ implies that M is P$\mathcal{S}$C. This generalizes a result of [Pop] that N is P$\mathcal{S}$C.

(b) The actual results of our paper depend however on the notion of a PAC field over a ring. Generalizing this concept, consider a perfect algebraic extension L of K. We say that L is **P$\mathcal{S}$C over** O_L if for every absolutely irreducible variety V of dimension r and every dominating separable rational map $\varphi\colon V \to \mathbb{A}^r$ over L there exists $\mathbf{z} \in V(L)$ such that $\varphi(\mathbf{z}) \in O_L^r$ provided that for each $v \in \mathcal{S}_L$ there exists $\mathbf{z}_v \in V_{\mathrm{sim}}(L_v)$ such that $\varphi(\mathbf{z}_v) \in O_{L,v}^r$.

(c) Let U be a nonempty Zariski-open affine subvariety of V over L and let $v \in \mathcal{S}_L$. Then, $O_{L,v}^r$ is v-open in L_v^r and $\varphi\colon V(L_v) \to L_v^r$ is v-continuous. Also, each v-open neighborhood of a point of $V_{\mathrm{sim}}(L_v)$ is Zariski dense in V [GPR, Cor. 9.5]. Hence, if there exists $\mathbf{z}_v \in V_{\mathrm{sim}}(L_v)$ such that $\varphi(\mathbf{z}_v) \in O_{L,v}^r$, then there exists $\mathbf{y}_v \in U_{\mathrm{sim}}(L_v)$ such that $\varphi(\mathbf{y}_v) \in O_{L,v}^r$. It follows that in order for L to be P$\mathcal{S}$C (resp., P$\mathcal{S}$C over O_L) it suffices to consider only affine absolutely irreducible varieties. □

If L is a perfect subextension of N/K which is P$\mathcal{S}$C over O_L, then L is also weakly P$\mathcal{S}$C over O_L. Indeed, in the notation of Data 1.1(n) for L instead of M, we may take V as the affine plane curve $h(T, X) = 0$ (with finitely many points deleted) and φ as the projection on the first coordinate. Note that this observation, as well as the definitions and the comments of Remark 8.3, does not depend on the assumtion that K is a global field. The next result is however a consequence of the strong approximation theorem and therefore relies on the assumption that K is a global field.

Theorem 8.4. *M is* P$\mathcal{S}$C *over O_M.*

Proof. Let V, φ, and $\mathbf{z}_v$ be as in Remark 8.3(b) with M instead of L and with V affine. We have to find $\mathbf{z} \in V(M)$ such that $\varphi(\mathbf{z}) \in O_M^r$.

Assume without loss that V is defined over K. As $\varphi\colon V \to \mathbb{A}^r$ is dominating, we can choose $\mathbf{z}_0 \in V_{\mathrm{sim}}(\tilde{K})$ such that $\varphi(\mathbf{z}_0) \in \tilde{O}^r$. Consider the K-rational big set $\mathcal{U} = \{v \in \mathcal{V}_N \smallsetminus \mathcal{S}_N \mid v(\mathbf{z}_0^\sigma) \geq 0 \text{ for each } \sigma \in \mathrm{Aut}(N/K)\}$ and let $\mathcal{W} = \mathcal{V}_N \smallsetminus \mathcal{U}$. Make $\mathcal{U}$ somewhat smaller, if necessary, to assume that $\mathcal{W} \smallsetminus \mathcal{S}_N$ is nonempty. For each $w \in \mathcal{W} \smallsetminus \mathcal{S}_N$ let $\mathbf{z}_w = \mathbf{z}_0$.

Now let W be the graph of φ. That is, W is the Zariski closure of the set of all points $(\mathbf{z}, \varphi(\mathbf{z}))$ with $\mathbf{z} \in V(\tilde{K})$ at which φ is defined. The Jacobian criteria implies that $(\mathbf{z}_w, \varphi(\mathbf{z}_w)) \in W_{\mathrm{sim}}(N_w)$ for each $w \in \mathcal{W}$. Let γ be a large positive integer. By Lemma 8.1, we can redefine the points $\mathbf{z}_w$ such that $(\mathbf{z}_w, \varphi(\mathbf{z}_w))_{w\in\mathcal{W}} \in W_{K,\mathcal{S},\mathcal{W}}$. Theorem 8.2(b) then supplies $(\mathbf{z}, \mathbf{y}) \in W(M)$ such that $w((\mathbf{z}, \mathbf{y}) - (\mathbf{z}_w, \varphi(\mathbf{z}_w))) > \gamma$ for each $w \in \mathcal{W}$ and $v(\mathbf{z}, \mathbf{y}) \geq 0$ for each $v \in \mathcal{V}_N \smallsetminus \mathcal{W}$. In particular, $\mathbf{z} \in V(M)$. Also, $\mathbf{z}$ is Zariski close to $\mathbf{z}_0$, hence φ is defined at $\mathbf{z}$, and therefore $\mathbf{y} = \varphi(\mathbf{z})$. Finally, $w(\mathbf{y}) \geq 0$ for each $w \in \mathcal{W}$. We conclude that $\varphi(\mathbf{z}) \in O_M^r$, as desired. □

Remark 8.5: Algebraic extensions. Let M_0 be a perfect algebraic extension of K. Let $M = M_0 \cap N$ and suppose that M_0 is PAC over O_M. Consider a subextension M' of N/M and let $M_0' = M_0M'$. Then $M_0' \cap N = M'$, and M_0' is PAC over $O_{M'}$ [JR1, Corollary 2.5]. Hence, the approximation theorems and the local global principle hold also for M'.

Combining the methods of proof of [Ja5, Lemma 7.2] and [JR1, Lemma 2.1], it is possible to prove that if M' is an algebraic extension of M which is unramified over S_M, and in particular if $M' \subseteq N$, then M' is P$\mathcal{S}$C over $O_{M'}$. But we do not elaborate on this. □

9. Decidability

In this section we assume that S is empty, therefore $N = \tilde{K}$, and M is a perfect algebraic extension of K which is PAC over O_M. The local global principle allows us in this case to develop a decision procedure for diophantine problems of M with coefficients in K which is independent of M. Thus, Hilbert's tenth problem with coefficients in K is uniformly solvable for all algebraic extensions M of K which are perfect and which are PAC over O_M.

Our basic auxiliary tool in this procedure is a lemma which uniformizes the decomposition-intersection procedure for Zariski K-closed affine sets [FrJ, Sec. 19.1]. In this lemma K and M do not denote any more the fields which Data 1.1 fixed.

Lemma 9.1 (Uniform decomposition-intersection procedure). *Let K be a field. Let A be a Zariski K-closed subset of $\mathbb{A}^n$. Then there exists a finite normal extension Q of K and for each subfield L of Q such that Q/L is Galois there exists an L-closed subset A_L^* of A which decomposes into a union of absolutely irreducible varieties which are defined over L such that if M is a perfect field which contains K and $Q \cap M = L$, then $A(M) = A_L^*(M)$.*

Moreover, if K has elimination theory in the sense of [FrJ, Def. 17.9]*, then we can effectively construct Q, and for each L as above we can effectively construct A_L^* and decompose it into its absolutely irreducible components over L.*

Proof. We use the notation $E \leq Q$ for two fields E and Q to denote that Q is a Galois extension of E.

Decompose A into its absolutely irreducible components, $A = \bigcup_{i\in I} V_i$, and construct a finite normal extension Q_0 of K over which each V_i is defined. Let $K \subseteq E \le Q_0$. Then $\mathcal{G}(Q_0/E)$ permutes the V_i's. Consider a decomposition

$$\{V_i|\ i \in I\} = \dot{\bigcup_{j\in J_E}} \{V_i|\ i \in I_j\}$$

into $\mathcal{G}(Q_0/E)$-orbits. For each $j \in J_E$, $U_j = \bigcap_{i\in I_j} V_i$ is invariant under $\mathcal{G}(Q_0/E)$ and is therefore an E-closed subset of A. If I_j consists of only one element i, then $U_j = V_i$ is an absolutely irreducible variety which is defined over E. Otherwise, $\dim(V_i) = \dim(V_{i'})$ and $V_i \ne V_{i'}$ for distinct $i, i' \in I_j$. Hence, $\dim(U_j) < \min_{i\in I_j} \dim(V_i) \le \dim(A)$ [FrJ, Lemma 9.19]. Let

$$A_E = \bigcup_{\substack{j\in J_E\\ |I_j|=1}} U_j \qquad \text{and} \qquad B_E = \bigcup_{\substack{j\in J_E\\ |I_j|>1}} U_j.$$

Then A_E is a union of absolutely irreducible varieties which are defined over E, and $\dim(B_E) < \dim(A)$.

Claim: *If M is a perfect field which contains K and $Q_0 \cap M = E$, then $A(M) = A_E(M) \cup B_E(M)$.* Indeed, let $\mathbf{x} \in A(M)$. Then there exist $j \in J_E$ and $i \in I_j$ such that $\mathbf{x} \in V_i(M)$. If $|I_j| = 1$, then $\mathbf{x} \in A_E(M)$. Otherwise, consider $i' \in I_j$. By definition, there exists $\sigma \in \mathcal{G}(Q_0/E)$ such that $V_{i'} = V_i^\sigma$. Since Q_0/E is Galois, σ extends to an element of $\mathcal{G}(Q_0M/M)$. Hence, $\mathbf{x} \in V_{i'}(M)$. It follows that $\mathbf{x} \in U_j(M)$ and therefore $\mathbf{x} \in B_E(M)$, as was to be shown.

If B_E is nonempty, use induction on the dimension to obtain a finite normal extension Q_E of E, and to construct for each $E \subseteq F \le Q_E$ an F-closed subset A'_F such that all absolutely irreducible components of A'_F are defined over F and such that if M is a perfect field which contains E and $Q_E \cap M = F$, then $B_E(M) = A'_F(M)$.

Now let Q be a finite normal extension of K which contains Q_0 and all fields Q_E for which $K \subseteq E \le Q_0$. Consider a field $K \subseteq L \le Q$. Then $E = Q_0 \cap L$ satisfies $K \subseteq E \le Q_0$ and $F = Q_E \cap L$ satisfies $E \subseteq F \le Q_E$. By the above, $A^*_L = A_E \cup A'_F$ is an L-closed subset of A that decomposes into absolutely irreducible varieties each of which is defined over L.

Let M be a perfect field which contains K such that $L = Q \cap M$. Then $L \le Q$. Hence, in the notation of the preceding paragraph, $A(M) = A_E(M) \cup B_E(M) = A_E(M) \cup A'_F(M) = A^*_L(M)$, as desired.

Finally, if K has elimination theory, then Chapter 17 of [FrJ] shows how to make all the above constructions effective. □

We return now to the notation of Data 1.1.

Theorem 9.2 (Decidability of diophantine equations). *Let A be a given Zariski closed subset of $\mathbb{A}^n$ over K.*

(a) *If A is absolutely irreducible, then we can effectively decide whether A has an $\tilde{O}$-rational point, and therefore, by Theorem 1.8(a), also an O_M rational point for each algebraic extension M of K which is perfect and which is PAC over O_M.*

(b) *We can compute a finite normal extension Q of K and the maximal purely inseparable extension K' of K in Q, and for each field $K' \subseteq L \subseteq Q$ we can effectively assign an integer $\nu(L) \in \{0, 1\}$ such that if an algebraic extension*

M of K is perfect and is PAC over O_M and $Q \cap M = L$, then $A(O_M) = \emptyset$ if $\nu(L) = 0$ and $A(O_M) \neq \emptyset$ if $\nu(L) = 1$.

(c) *For each positive integer e we can compute the Haar measure of all $\boldsymbol{\sigma} \in G(K)^e$ such that A has an $\tilde{O}(\boldsymbol{\sigma})$-rational point. This measure is a rational number.*

Proof of (a). By the local global principle, it suffices to check if for each $v \in \tilde{\mathcal{V}}$ there exists $\mathbf{z} \in A(\tilde{K})$ such that $v(\mathbf{z}) \geq 0$. To this end choose $\mathbf{a} \in A(\tilde{K})$, if possible [FrJ, Thm. 8.4]. Let L be a finite extension of K which contains the coordinates of $\mathbf{a}$. Then find a finite set $\mathcal{T}$ of $\mathcal{V}_L$ such that $v(\mathbf{a}) \geq 0$ for all $v \in \mathcal{V}_L \smallsetminus \mathcal{T}$. For each $v \in \mathcal{T}$ use Abraham Robinson's decision procedure ([Rob, p. 54] or Weispfening's procedure [Wei, Cor. 3.3]) for the theory of algebraically closed valued fields to decide whether $A(\tilde{K})$ has a point $\mathbf{a}_v$ such that $\tilde{v}(\mathbf{a}_v) \geq 0$ for some (hence for all) extensions $\tilde{v}$ of v to $\tilde{K}$. If one of these checkups is negative, then $A(\tilde{O})$ is empty, otherwise it is nonempty. □

Proof of (b). Use the notation of Lemma 9.1. Decompose A_L^* into its absolutely irreducible components, $A_L^* = \bigcup W_{L,i}$. Lemma 9.1 says that each of them is defined over L. For each i check, by (a), whether $W_{L,i}(\tilde{O})$ is empty. If this is the case for all i put $\nu(L) = 0$; otherwise let $\nu(L) = 1$.

Now let M be a perfect field which is PAC over O_M, and let $L = Q \cap M$. By Lemma 9.1, $A(M) = A_L^*(M) = \bigcup W_{L,i}(M)$. Hence $A(O_M) = \emptyset$ if and only if $\nu(L) = 0$. □

Proof of (c). Use the notation of (b). For each $\boldsymbol{\sigma}_0 \in \mathcal{G}(Q/K')^e$ let $Q(\boldsymbol{\sigma}_0)$ be the fixed field of $\boldsymbol{\sigma}_0$ in Q. Let k be the number of all $\boldsymbol{\sigma}_0 \in \mathcal{G}(Q/K')^e$ for which $\nu(Q(\boldsymbol{\sigma}_0)) = 1$. For almost all $\boldsymbol{\sigma} \in G(K)^e$, the field $M = \tilde{K}(\boldsymbol{\sigma})$ is perfect and is PAC over O [JR1, Prop. 3.1] and hence also over O_M. Hence, by (b), the desired measure is $k/[Q : K']^e$. □

10. Appendix: Drawing a curve through points of a variety

The reduction of the aproximation theorem for arbitrary affine varieties over K to the same theorem for curves uses an essentially known result from algebraic geometry. We thank Ron Livne for his help in the proof.

Lemma 10.1. *Let $V \subseteq \mathbb{A}^n$ (resp., $V \subseteq \mathbb{P}^n$) be an affine (resp., projective) absolutely irreducible variety of dimension $r \geq 1$ which is defined over an infinite field L. Let P be a finite subset of $V(L_s)$. Then there exists an absolutely irreducible curve $C \subseteq \mathbb{A}^n$ (resp., $C \subseteq \mathbb{P}^n$) over L which lies on V and passes through each of the points of P. Moreover, if $\mathbf{p} \in P$ is simple on V, then it is also simple on C.*

Proof. The affine case follows from the projective one. So, we assume that V is projective. For $r = 1$ there is nothing to prove. So we assume that $r \geq 2$. Add a point of $V_{\mathrm{sim}}(L_s)$ to P, if necessary, to assume that $P_{\mathrm{sim}} = P \cap V_{\mathrm{sim}}(L_s)$ is nonempty. Add all L-conjugates of points in P, if necessary, to assume that P is invariant under the action of the Galois group $G(L)$.

Consider a positive integer d. Order the set of monomials in $X_0, \ldots, X_n$ of degree d as $m_0, \ldots, m_q$. Let $h(\mathbf{X}) = \sum_{j=0}^{q} a_j m_j(\mathbf{X})$ in $\tilde{L}[X_0, \ldots, X_n]$ be a form of degree d. It defines a hypersurface H in $\mathbb{P}^n$ such that $H(\tilde{L})$ is the set of zeros of h in $\mathbb{P}^n(\tilde{L})$. Identify H with the point $\mathbf{a} = (a_0 : \cdots : a_q)$ of $\mathbb{P}^q$. In this way we identify the set $\mathcal{H} = \mathcal{H}_d$ of all these hypersurfaces with $\mathbb{P}^q$ and equip $\mathcal{H}$ with the Zariski topology of $\mathbb{P}^q$.

Let $\mathcal{P} = \mathcal{P}_d$ be the closed subset of $\mathcal{H}$ consisting of all H which pass through each point of P. It is isomorphic to a linear subspace which is isomorphic to $\mathbb{P}^m$ for some $m \le q$. In particular, $\mathcal{P}$ is absolutely irreducible. Since P is invariant over L and each point in P is separable algebraic, $\mathcal{P}$ is defined over L.

Let $\mathcal{I} = \mathcal{I}_d$ be the set of all $H \in \mathcal{H}$ such that $H \cap V$ is absolutely irreducible. Let $\mathcal{J} = \mathcal{J}_d$ be the set of all $H \in \mathcal{H}$ which do not contain V. For each $\mathbf{p} \in P_{\mathrm{sim}}$ let $\mathcal{E}_{\mathbf{p}} = \mathcal{E}_{\mathbf{p},d}$ be the set of all $H \in \mathcal{J}$ such that $\mathbf{p}$ is simple on $H \cap V$.

We prove that $\mathcal{I}$, $\mathcal{J}$, and $\mathcal{E}_{\mathbf{p}}$ are open in $\mathcal{H}$. We also prove for $d \ge |P|$ that $\mathcal{E}_{\mathbf{p}} \cap \mathcal{P}$ are nonempty. Finally we prove that for infinitely many d's the set $\mathcal{I} \cap \mathcal{P}$ is nonempty. As $\mathcal{P}$ is irreducible, this will imply for some large d that $\mathcal{U} = \mathcal{I} \cap \bigcap_{\mathbf{p} \in P_{\mathrm{sim}}} \mathcal{E}_{\mathbf{p}} \cap \mathcal{P}$ is a nonempty open subset of $\mathcal{P}$. Since L is infinite and $\mathcal{P}$ is linear, there exists $H \in \mathcal{U}(L)$. By the dimension theorem, $H \cap V$ is an absolutely irreducible variety of dimension $r-1$ which is defined over L and goes through each point of P, and $\mathbf{p}$ is simple on $H \cap V$ for each $\mathbf{p} \in P_{\mathrm{sim}}$. Now use induction on r to find the desired curve C.

We have therefore to prove the above claims.

Claim A: *$\mathcal{I}$ and $\mathcal{J}$ are open.* The **Veronese mapping** [Sha, p. 40] (also called the **d-uple embedding** [Har, p. 13]) ν maps each point $\mathbf{x} = (x_0 : \cdots : x_n)$ in $\mathbb{P}^n(\tilde{L})$ to the point $\mathbf{y} = (m_0(\mathbf{x}) : \cdots : m_q(\mathbf{x}))$ of $\mathbb{P}^q(\tilde{L})$. It is an isomorphism of $\mathbb{P}^n$ onto a subvariety of $\mathbb{P}^q$, called the **Veronese variety**, which is defined over the prime field of L. In particular, ν maps V isomorphically to an absolutely irreducible subvariety V^* of $\mathbb{P}^q$. For each hypersurface H of degree d in $\mathbb{P}^n$ which is defined by a form $h(\mathbf{X}) = \sum_{j=0}^q a_j m_j(\mathbf{X})$, the map ν attaches the hyperplane H^* in $\mathbb{P}^q$ which is defined by the linear form $h^*(\mathbf{Y}) = \sum_{j=0}^q a_j Y_j$. The intersection $V \cap H$ is absolutely irreducible if and only if $V^* \cap H^*$ is absolutely irreducible. We identify H^* with the same point $\mathbf{a}$ of $\mathbb{P}^q$ to which we have already identified H. By [HoP, p. 79, Lemma 1], the set of all hyperplanes H^* in $\mathbb{P}^q$ such that $H^* \cap V^*$ is absolutely irreducible is open. Hence, $\mathcal{I}$ is open.

Similarly, the set of all H^* which do not contain V^* is open. Hence, so is $\mathcal{J}$.

Claim B: *For $\mathbf{p} \in P_{\mathrm{sim}}$ the set $\mathcal{E}_{\mathbf{p}}$ is open.* Let $f_1, \ldots, f_k$ be forms in $L[X_0, \ldots, X_n]$ which generate the ideal of all polynomials in $\tilde{L}[X_0, \ldots, X_n]$ that vanish on V. For each form $h \in \tilde{L}[\mathbf{X}]$ of degree d consider the $(k+1) \times (n+1)$ matrix

$$D_h = \begin{pmatrix} \frac{\partial f_i}{\partial p_j} \\ \frac{\partial h}{\partial p_j} \end{pmatrix}$$

with $i = 1, \ldots, k$ and $j = 0, \ldots, n$. Here $\frac{\partial f_i}{\partial p_j} = \frac{\partial f_i}{\partial x_j}(\mathbf{p})$ and $\frac{\partial h}{\partial p_j} = \frac{\partial h}{\partial x_j}(\mathbf{p})$. If the hypersurface H that h defines belongs to $\mathcal{J}$, then each absolutely irreducible component of $H \cap V$ has dimension $r-1$. Hence, $\mathbf{p}$ is simple on $H \cap V$ if and only if D_h has a nonzero subdeterminant of order $n-r+1$. So, $\mathcal{E}_{\mathbf{p}}$ is open.

Claim C: *Suppose that $d \ge |P|$ and let $\mathbf{p} \in P_{\mathrm{sim}}$. Then $\mathcal{E}_{\mathbf{p}} \cap \mathcal{P}$ is nonempty.*

Indeed, let $T_{\mathbf{p}}$ be the tangent space to V at $\mathbf{p}$. Let $\hat{T}_{\mathbf{p}}$ be the dual space consisting of all linear forms $\sum_{i=0}^n \frac{\partial f}{\partial p_i} X_i$ with $f \in \tilde{L}[\mathbf{X}]$ a form which vanishes on V. Then $\dim(T_{\mathbf{p}}) = r$ and $\dim(\hat{T}_{\mathbf{p}}) = n - r < n-1$. On the other hand, the space $\Lambda_{\mathbf{p}}$ of all linear forms in $\mathbf{X}$ which vanish at $\mathbf{p}$ is of dimension $n-1$. Hence $\Lambda_{\mathbf{p}} \not\subseteq \hat{T}_{\mathbf{p}}$. Also, if $\mathbf{q} \ne \mathbf{p}$, then $\Lambda_{\mathbf{p}} \not\subseteq \Lambda_{\mathbf{q}}$. Take $\mathbf{c} \in V(\tilde{L}) \smallsetminus P$. Choose $\lambda(\mathbf{X}) = \sum_{i=0}^n b_i X_i \in \Lambda_{\mathbf{p}} \smallsetminus (\hat{T}_{\mathbf{p}} \cup \Lambda_{\mathbf{c}})$. For each $\mathbf{q} \in P \smallsetminus \{\mathbf{p}\}$ choose $\lambda_{\mathbf{q}}(\mathbf{X}) \in \Lambda_{\mathbf{q}} \smallsetminus (\Lambda_{\mathbf{p}} \cup \Lambda_{\mathbf{c}})$.

Finally choose an extra linear form $\mu(X)$ in $\tilde{L}[\mathbf{X}] \smallsetminus (\Lambda_{\mathbf{p}} \cup \Lambda_{\mathbf{c}})$. Then $h(\mathbf{X}) = \lambda(\mathbf{X}) \prod_{\mathbf{q} \in P \smallsetminus \{\mathbf{p}\}} \lambda_{\mathbf{q}}(\mathbf{X}) \mu(\mathbf{X})^{d-|P|}$ is a form of degree d which vanishes at each point of P but not at $\mathbf{c}$. Moreover, $\frac{\partial h}{\partial p_i} = b_i \prod_{\mathbf{q} \in P \smallsetminus \{\mathbf{p}\}} \lambda_{\mathbf{q}}(\mathbf{p}) \mu(\mathbf{p})^{d-|P|}$ and therefore

$$\sum_{i=0}^{n} \frac{\partial h}{\partial p_i} X_i = \lambda(\mathbf{X}) \prod_{\mathbf{q} \in P \smallsetminus \{\mathbf{p}\}} \lambda_{\mathbf{q}}(\mathbf{p}) \mu(\mathbf{p})^{d-|P|}.$$

As a multiple of $\lambda(X)$ by a constant the latter form does not belong to $\hat{T}_{\mathbf{p}}$. It follows that the rank of D_h is $n - r + 1$. Therefore the hypersurface H that h defines belongs to $\mathcal{E}_{\mathbf{p}} \cap \mathcal{P}$, as claimed.

Claim D: *There exist infinitely many d's for which $\mathcal{I} \cap \mathcal{P}$ is nonempty.* Blow up $\mathbb{P}^n$ at the points of P to obtain a birational morphism $\pi\colon \tilde{\mathbb{P}}^n \to \mathbb{P}^n$ over L with the following properties [Mum, pp. 219–225]:

(1a) $\tilde{\mathbb{P}}^n \subseteq \mathbb{P}^k$ is an absolutely irreducible variety of dimension n defined over L (we have assumed that each point in P is separable over L) for some positive integer k.
(1b) The restriction of π to $\tilde{\mathbb{P}}_n \smallsetminus \pi^{-1}(P)$ is an isomorphism onto $\mathbb{P}^n \smallsetminus P$.
(1c) The Zariski closure of $\pi^{-1}(V \smallsetminus P)$ is an absolutely irreducible subvariety $\tilde{V}$ of $\tilde{\mathbb{P}}^n$ of dimension r and the restriction of π to $\tilde{V}$ is a birational morphism onto V.
(1d) For each $\mathbf{p} \in P$ the fiber $\pi^{-1}(\mathbf{p})$ is of dimension $n-1$.
By (1c), $\tilde{V} \not\subseteq \pi^{-1}(\mathbf{p})$, and hence, by (1d) and the dimension theorem,
(1e) $\dim(\pi^{-1}(\mathbf{p}) \cap \tilde{V}) = r - 1$ for each $\mathbf{p} \in P$.

We have already mentioned that the set of all hyperplanes in $\mathbb{P}^k$ which intersect a given absolutely irreducible variety of dimension m in an absolutely irreducible variety of dimension $m-1$ is Zariski open. Moreover, it is nonempty [HoP, p. 78]. Since L is infinite, $\mathbb{P}^k$ has a hyperplane H' over L such that $H^* = H' \cap \tilde{\mathbb{P}}^n$ is an absolutely irreducible variety of dimension $n-1$, and $H' \cap \tilde{V}$, which is equal to $H^* \cap \tilde{V}$, is an absolutely irreducible variety of dimension $r-1$. Moreover, we can choose H' such that for each $\mathbf{p} \in P$ it does not contain $\pi^{-1}(\mathbf{p}) \cap \tilde{V}$.

It follows that for each $\mathbf{p} \in P$, H^* does not contain $\pi^{-1}(\mathbf{p}) \cap \tilde{V}$. Hence $H = \pi(H^*)$ is an absolutely irreducible subvariety of $\mathbb{P}^n$ of dimension $n-1$ which is defined over L. Let $h(\mathbf{X}) \in L[\mathbf{X}]$ be a form which defines H. Then $H \in \mathcal{H}_d$ with $d = \deg(h)$. Note that $H(\tilde{L})$ is the set of zeros of any power of h. So, we may assume that d is large. In order to complete the proof of the theorem we have to prove that $H \cap V$ is absolutely irreducible and contains P.

Indeed, by the dimension theorem for projective spaces, and since $r - 1 \geq 1$, each of the sets $\pi^{-1}(\mathbf{p}) \cap H^*$ is nonempty. Hence $W = \pi(H^* \cap \tilde{V})$ is an absolutely irreducible subvariety of V of dimension $r-1$ which contains P and is defined over L.

Obviously $W(\tilde{L}) \subseteq H(\tilde{L}) \cap V(\tilde{L})$. Conversely, let $\mathbf{a} \in H(\tilde{L}) \cap V(\tilde{L}) \smallsetminus P$. Then there exist $\mathbf{b} \in H^*(\tilde{L})$ and $\mathbf{c} \in \tilde{V}(\tilde{L})$ such that $\pi(\mathbf{b}) = \mathbf{a} = \pi(\mathbf{c})$. Both $\mathbf{b}$ and $\mathbf{c}$ do not belong to $\pi^{-1}(P)$. Since π is bijective on $\tilde{\mathbb{P}}^n(\tilde{L}) \smallsetminus \pi^{-1}(P)$, we have $\mathbf{b} = \mathbf{c}$. Hence, $\mathbf{a} \in W(\tilde{L})$, and so $W = H \cap V$.

This completes the proof of the last claim. $\square$

References

[CaR] D.C. Cantor and P. Roquette, *On diophantine equations over the ring of all algebraic integers*, Journal of Number Theory **18** (1984), 1–16. MR **85j:**11036

[De1] M. Deuring, *Lectures on the Theory of Algebraic Functions of One Variable*, Lecture Notes in Mathematics, vol. 314, Springer, Berlin, 1973. MR **49:**8790

[De2] M. Deuring, *Reduktion algebraischer Funktionenkörper nach Primdivisoren des Konstantenkörpers*, Mathematische Zeitschrift **47** (1942), 643–654. MR **7:**362c

[DMR] M. Davis, Y. Matijasevič, and J. Robinson, *Hilbert's tenth problem. Diophantine equations: Positive aspects of a negative solution*, Proceedings of Symposia in Pure Mathematics **28** (1976), 323–378. MR **55:**5522

[FrJ] M.D. Fried and M. Jarden, *Field Arithmetic*, Ergebnisse der Mathematik (3), vol. 11, Springer, Heidelberg, 1986. MR **89b:**12010

[GPR] B. Green, F. Pop, and P. Roquette, *On Rumely's local-global principle*, Jahresbericht der Deutsche Mathematickervereinigung **97** (1995), 43–74. CMP 95:15

[Har] R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics, vol. 52, Springer, New York, 1977. MR **57:**3116

[HoP] W.V.D. Hodge and D. Pedoe, *Methods of Algebraic Geometry* II, Cambridge University Press, Cambridge, 1952. MR **13:**972c

[Ja1] M. Jarden, *Elementary statements over large algebraic fields*, Transactions of AMS **164** (1972), 67–91. MR **46:**1795

[Ja2] M. Jarden, *The Skolem problem over the rings of integers of large algebraic fields*, manuscript, Tel Aviv, 1989.

[Ja3] M. Jarden, *Intersection of local algebraic extensions of a Hilbertian field* (A. Barlotti et al., eds.), NATO ASI Series C **333**, Kluwer, Dordrecht, 1991, pp. 343–405. MR **94c:**12003

[Ja4] M. Jarden, *The inverse Galois problem over formal power series fields*, Israel Journal of Mathematics **85** (1994), 263–275. MR **95a:**12009

[Ja5] M. Jarden, *Algebraic realization of p-adically projective groups*, Compositio Mathematica **79** (1991), 21–62. MR **93f:**12007

[JaR] M. Jarden and Peter Roquette, *The Nullstellensatz over p-adically closed fields*, Journal of the Mathematical Society of Japan **32** (1980), 425–460. MR **82g:**14027

[JR1] M. Jarden and A. Razon, *Pseudo algebraically closed fields over rings*, Israel Journal of Mathematics **86** (1994), 25–59. MR **95c:**12006

[JR2] M. Jarden and A. Razon, *Skolem density problems over algebraic PSC fields over rings*, Nieuw Archief Wisskunde **13** (1995), 381–399. CMP 96:09

[Lan] S. Lang, *Algebraic Number Theory*, Addison-Wesley, Reading, MA, 1970. MR **44:**181

[MB1] L. Moret-Bailly, *Points entiers des varietés arithmétiques*, Séminaire de Théorie des Nombres, Paris 1985-86, Progress in Mathematics **71**, Birkhäuser, Boston, 1987, pp. 147–153. MR **91f:**14020

[MB2] L. Moret-Bailly, *Groupes de Picard et problémes de Skolem I*, Annales Scientifiques de l'Ecole Normale Superieure (4) **22** (1989), 161–179. MR **90i:**11065

[MB3] L. Moret-Bailly, *Groupes de Picard et problémes de Skolem II*, Annales Scientifiques de l'Ecole Normale Superieure (4) **22** (1989), 181–194. MR **90i:**11065

[Mum] D. Mumford, *The Red Book of Varieties and Schemes*, Lecture Notes in Mathematics **1358**, Springer, Berlin, 1988. MR **89k:**14001

[Pop] F. Pop, *Fields of totally Σ-adic numbers*, manuscript, Heidelberg, 1992.

[Raz] A. Razon, *Primitive recursive decidability for large rings of algebraic integers*, Ph.D Thesis, Tel Aviv, 1995.

[Ro1] P. Roquette, *Reciprocity in valued function fields*, Journal für die Reine und Angewandte Mathematik **375/376** (1987), 238–258. MR **88f:**11058

[Ro2] P. Roquette, *Rumely's local global principle*, Notes from a meeting in Oberwolfach on model theory, 1990.

[Rob] A. Robinson, *Complete Theories*, North Holland, 1956. MR **17:**817b

[Ru1] R. Rumely, *Arithmetic over the ring of all algebraic integers*, Journal für die Reine und Angewandte Mathematik **368** (1986), 127–133. MR **87i:**11041

[Ru2] R. Rumely, *Capacity Theory on Algebraic Curves*, Lecture Notes in Mathematics, vol. 1378, Springer, Berlin, 1989. MR **91b:**14018

[Sha] I.R. Shafarevich, *Basic Algebraic Geometry*, Grundlehren der mathematischen Wissenschaften **213**, Springer, Berlin, 1977. MR **56:**5538

[Wei] V. Weispfenning, *Quantifier elimination and decision procedures for valued fields*, Models and Sets, Lecture Notes in Mathematics **1103**, Berlin, 1984, pp. 419–472. MR **86m:**03059

School of Mathematical Sciences, Tel Aviv University, Ramat Aviv, Tel Aviv 69978, Israel

E-mail address: jarden@math.tau.ac.il

E-mail address: razon@math.tau.ac.il