Jber. d. Dt. Math.-Verein. 97 (1995) 43–74
AMS subject classification: 11 G 35, 11 R 58, 14 G 25

On Rumely's Local-Global Principle

B. Green, F. Pop, P. Roquette, Heidelberg

Contents

1 Introduction: Statement of Results

1.1 Algebraic Diophantine Equations

One of the remarkable discoveries in Number Theory in the past decade is *Rumely's Local-Global Principle for algebraic diophantine equations.* The aim of the present paper is to provide a direct and short access to this important theorem, at the same time generalizing it in two ways: first by admitting *archimedean primes,* and secondly including *rationality conditions* at a finite set of primes.[1])

Let K be an algebraic number field of finite degree. Consider finitely many polynomial equations

$$(1) \qquad f_j(x_1, \ldots, x_n) = 0 \qquad (1 \leqslant j \leqslant r)$$

with coefficients in K. We are looking for a solution $\boldsymbol{a} = (a_1, \ldots, a_n)$ whose coordinates a_i are *algebraic integers*, not necessarily contained in K. We speak of *"algebraic diophantine equations"*. A necessary condition for solvability is the *local solvability:* For each prime divisor $\mathfrak{p}$ of K there should be a solution of (1) whose coordinates are $\mathfrak{p}$-*adic algebraic integers* over the completion $K_\mathfrak{p}$.

The Local-Global Principles states this condition is also sufficient, *provided* the ideal generated by the polynomials f_j in the polynomial ring $\tilde{K}[X_1, \ldots, X_n]$ over

[1]) This subject was presented at the Oberwolfach Model Theory meeting, 20. 1.–27. 1. 1990, as part of an organized programme devoted to the elementary theory of the ring of algebraic integers. At that meeting interest was expressed in a published account of the lectures. The present paper is a worked out version of the material we presented there and also contains some unpublished results on the field of totally $\mathfrak{S}$-adic numbers from the manuscript [P].

the algebraic closure $\tilde{K}$, the field of all algebraic numbers, is prime. Equivalently this condition asserts that the affine variety defined by the equations (1) is geometrically integral. We would like to mention that this condition is of *elementary nature,* i.e., it can be expressed as a formula in the elementary language of fields, with the coefficients of the polynomials f_j as parameters.

The Local-Global Principle for Algebraic Diophantine Equations. *Suppose that the affine variety defined by the equations* (1) *is geometrically integral. Then the above necessary condition is also sufficient in the following sense: If for each prime divisor* $\mathfrak{p}$ *of* K *there exists a solution* $a_\mathfrak{p}$ *in* $\mathfrak{p}$*-adic algebraic integers over* $K_\mathfrak{p}$ *then there exists a solution* a *in algebraic integers.*

This result derives its importance from the fact that the *solvability of diophantine algebraic equations over each* $K_\mathfrak{p}$ *is decidable.* This follows from the work of Abraham Robinson [Rob] who has proved that the theory of an algebraically closed valued field is decidable. Applying this to the algebraic closure $\tilde{K}_\mathfrak{p}$ of $K_\mathfrak{p}$ and its canonical valuation, we see that there exists an effective algorithm which enables one to decide whether (1) has solutions in algebraic integers over $K_\mathfrak{p}$. This holds for each prime divisor $\mathfrak{p}$. In fact it is only necessary to check this for finitely many primes $\mathfrak{p}$; these finitely many "critical" primes are effectively computable from the coefficients of the equations (1). The testing of these finitely many critical primes then leads to an *effective algorithm* to decide whether (1) has solutions in algebraic integers – provided the variety defined by (1) is geometrically integral. The solvability of general algebraic diophantine equations, whose variety is not necessarily geometrically integral, can be effectively reduced to the geometrically integral case (over a suitable finite extension of K). This yields:

The solvability of arbitrary algebraic diophantine equations is decidable. So the 10^{th} *problem of Hilbert over the ring* $\tilde{\mathbb{Z}}$ *of algebraic integers has a positive answer.*

This is in contrast to the situation over $\mathbb{Z}$ where it is known that the 10^{th} problem has a negative answer.

A detailed exposition of the above line of arguments, together with historical remarks and precise references, can be found in Rumely's paper [Ru1]. We have mentioned this here only in order to emphasize the importance of the Local-Global Principle within the framework of diophantine geometry. We would also like to draw the reader's attention to the papers by van den Dries [vdD] and by Prestel-Schmidt [Pr-S]. There, the Local-Global Principle is the main ingredient in generalizing the above decidability theorem of Rumely. Namely, it is shown that the whole theory of $\tilde{\mathbb{Z}}$, in the language of rings, is decidable. This is a genuine and non-trivial extension of Rumely's result; there are many statements in the language of rings which cannot be reduced to solving diophantine equations.

We shall now give a reformulation of the Local-Global Principle in terms of "Skolem Problems", at the same time generalizing it in two ways by admitting *archimedean primes*, and including *rationality conditions* at finitely many primes. In this connection we also wish to draw the reader's attention to the papers by Moret-Bailly, [M-B], where Skolem Problems are treated from a more geometric point of view. There, a proof of the Local-Global Principle admitting archimedean primes and including rationality conditions is also given.

1.2 The General Setting

Let K be a global field. A "prime" of K is understood to be an equivalence class of non-trivial absolute values, archimedean or non-archimedean.

Let $\mathfrak{V}$ be a given set of primes $\mathfrak{p}$ of K, with the sole condition that $\mathfrak{V}$ *does not contain all primes of* K. This hypothesis guarantees the validity of the *Strong Approximation Theorem* with respect to $\mathfrak{V}$, i.e., every approximation problem of the form

$$|z - a_\mathfrak{p}|_\mathfrak{p} \leqslant \varepsilon_\mathfrak{p} \qquad (\mathfrak{p} \in \mathfrak{V})$$

can be solved by an element $z \in K$. Here the $a_\mathfrak{p}$ are arbitrarily given elements in the respective completion $K_\mathfrak{p}$, with the only provision that $|a_\mathfrak{p}|_\mathfrak{p} \leqslant 1$ for almost all $\mathfrak{p} \in \mathfrak{V}$ and the approximation bounds $\varepsilon_\mathfrak{p}$ are positive real numbers with $\varepsilon_\mathfrak{p} = 1$ for almost all $\mathfrak{p} \in \mathfrak{V}$.

As a matter of notation, we use $|\cdot|_\mathfrak{p}$ to denote a multiplicative absolute value belonging to the prime $\mathfrak{p}$. Sometimes we shall also use the additive notation $v_\mathfrak{p}(\cdot) = -\log|\cdot|_\mathfrak{p}$. If $\mathfrak{p}$ is non-archimedean then it is customary to normalize $v_\mathfrak{p}$ such that the value group $v_\mathfrak{p}(K_\mathfrak{p}^\times) = \mathbb{Z}$. In most of what we shall say, however, it does not matter how $|\cdot|_\mathfrak{p}$ or $v_\mathfrak{p}$ are normalized among the equivalent valuations.

For a prime $\mathfrak{p} \in \mathfrak{V}$ we denote by $\mathcal{O}_\mathfrak{p}$ the "unit ball" in $K_\mathfrak{p}$, consisting of those $z \in K_\mathfrak{p}$ which satisfy $|z|_\mathfrak{p} \leqslant 1$. Thus if $\mathfrak{p}$ is non-archimedean then $\mathcal{O}_\mathfrak{p}$ is the canonical valuation ring of $K_\mathfrak{p}$. The algebraic closure of $K_\mathfrak{p}$ will be denoted by $\tilde{K}_\mathfrak{p}$, and $\tilde{\mathcal{O}}_\mathfrak{p}$ is the unit ball in $\tilde{K}_\mathfrak{p}$. In the non-archimedean case $\tilde{\mathcal{O}}_\mathfrak{p}$ is the integral closure of $\mathcal{O}_\mathfrak{p}$ in $\tilde{K}_\mathfrak{p}$.

Globally in K, we denote by $\mathcal{O}_\mathfrak{V}$ the set of those elements $a \in K$ which are contained in $\mathcal{O}_\mathfrak{p}$ for all $\mathfrak{p} \in \mathfrak{V}$.[2]) Denoting the set of non-archimedean primes in $\mathfrak{V}$ by $\mathfrak{V}_0$, it follows that the ring of integers $\mathcal{O}_{\mathfrak{V}_0}$ at $\mathfrak{V}_0$ is a *Dedekind ring*, with K as its field of quotients. If L is an algebraic extension of K then let $\mathfrak{W}$ denote the set of all extensions of primes $\mathfrak{p} \in \mathfrak{V}$ to L. We define $\mathcal{O}_\mathfrak{W} \subset L$ with respect to $\mathfrak{W}$ in exactly the same way as we have defined $\mathcal{O}_\mathfrak{V} \subset K$ with respect to $\mathfrak{V}$. If $\mathfrak{V}$ consists of non-archimedean primes only then $\mathcal{O}_\mathfrak{W}$ is the integral closure of $\mathcal{O}_\mathfrak{V}$ in L.

To simplify the language we shall generally speak of $\mathcal{O}_\mathfrak{W}$ *as the integral closure of* $\mathcal{O}_\mathfrak{V}$ *in* L, *even in the presence of archimedean primes.*

The algebraic closure of K is denoted by $\tilde{K}$. The integral closure of $\mathcal{O}_\mathfrak{V}$ in $\tilde{K}$ is denoted by $\tilde{\mathcal{O}}_\mathfrak{V}$.

1.3 Skolem Problems

Let V be a geometrically integral variety defined over K. For any overfield L of K we denote by $V(L)$ the set of L-rational points of V. Let $A \subset L$ be a subset of L and $x = (x_1, \ldots, x_n)$ a finite family of rational functions on V defined over K. We say that a point $P \in V(L)$ is A-rational with respect to x if $x_k(P) \in A\,(1 \leqslant k \leqslant n)$. (Here the condition that each $x_k(P)$ is defined is implicitly assumed). We denote the set of all

---

[2]) Thus in our notation, if $\mathfrak{V} = \{\mathfrak{p}\}$ consists of one prime only, then $\mathcal{O}_{\{\mathfrak{p}\}}$ does *not* coincide with $\mathcal{O}_\mathfrak{p}$ in general. $\mathcal{O}_{\{\mathfrak{p}\}}$ is the unit ball (valuation ring) of $\mathfrak{p}$ in the field K, whereas $\mathcal{O}_\mathfrak{p}$ is the completion of $\mathcal{O}_{\{\mathfrak{p}\}}$ in $K_\mathfrak{p}$. This is, we admit, not a very good notation but for our present purpose we believe it cannot lead to confusion. We shall have no occasion to explicitly study the situation $\mathfrak{V} = \{\mathfrak{p}\}$.

such A-rational points by $V_x(A, L)$. If L is generated by A (as will be the case in our setting below) then we shall simplify the notation and write $V_x(A)$.

The problem of whether $V_x(A) \neq \emptyset$ is called the *Skolem problem* for V over A, with data x. Any point $P \in V_x(A)$ is called a *solution* of that Skolem problem.

Our aim is to investigate Skolem problems over $\tilde{\mathcal{O}}_{\mathfrak{B}} \subset \tilde{K}$.

The relationship between this geometric context of Skolem problems and the solvability of algebraic diophantine equations is transparent: If V is a geometrically integral affine variety defined over an algebraic number field K by equations as in (1), and $x = (x_1, \ldots, x_n)$ is a generic point of V over K, i.e., x can be regarded as a generating system of the function field $K(V) = K(x)$, then the set of all solutions of (1) in $\tilde{\mathbb{Z}}$ coincides with $V_x(\tilde{\mathbb{Z}})$. Thus the problem of solvability of algebraic diophantine equations can be regarded as a Skolem problem.

In the following we prefer to talk about Skolem problems rather than about solvability of algebraic diophantine equations. The above discussion shows that both viewpoints are essentially equivalent.

By what we have said the following theorem is a generalization of the Local-Global Principle for algebraic diophantine equations.

The Local-Global Principle for Skolem Problems. *Let K be a global field, equipped with a set $\mathfrak{B}$ of primes not containing all primes of K. Let V be a geometrically integral variety defined over K, and $x = (x_1, \ldots, x_n)$ a finite family of rational functions on V, defined over K.*

Suppose that locally, for each prime $\mathfrak{p} \in \mathfrak{B}$, the $\mathfrak{p}$-adic Skolem problem for V over $\tilde{\mathcal{O}}_{\mathfrak{p}}$ with data x has a solution, i.e., that $V_x(\tilde{\mathcal{O}}_{\mathfrak{p}}) \neq \emptyset$. The globally, the problem for V over $\tilde{\mathcal{O}}_{\mathfrak{B}}$ with data x has a solution, i.e., $V_x(\tilde{\mathcal{O}}_{\mathfrak{B}}) \neq \emptyset$.

This theorem is not yet in the final form which we will prove in this paper. Namely, we can extend its statement by adding "rationality conditions" at finitely many primes. The situation is as follows.

1.4 Totally $\mathfrak{S}$-adic Field Extensions

Given $\mathfrak{p} \in \mathfrak{B}$, an element $a \in \tilde{K}$ is called *totally $\mathfrak{p}$-adic* over K, if for all K-embeddings $\iota : \tilde{K} \to \tilde{K}_{\mathfrak{p}}$, the image $\iota(a)$ lies in $K_{\mathfrak{p}}$. This is equivalent to saying that the prime $\mathfrak{p}$ splits completely in $K(a)$.

Let $\mathfrak{S} \subset \mathfrak{B}$ be a finite subset of $\mathfrak{B}$. We say that $a \in \tilde{K}$ is *totally $\mathfrak{S}$-adic* over K if a is totally $\mathfrak{p}$-adic for all $\mathfrak{p} \in \mathfrak{S}$. The set of all totally $\mathfrak{S}$-adic elements is a Galois extension K' of K; it can be characterized as the maximal extension in which all primes $\mathfrak{p} \in \mathfrak{S}$ split completely. If $\mathfrak{S}$ is empty then by definition K' is the separable closure, K^s, of K.

If we wish to indicate the defining set $\mathfrak{S}$ then we write $K^{\mathfrak{S}}$ instead of K'. However in most cases it will be clear from the context which set $\mathfrak{S}$ we are referring to; thus we prefer to write K' in order to simplify the notation.

The integral closure of $\mathcal{O}_{\mathfrak{B}}$ in K' will be denoted by $\mathcal{O}'$. If we wish to indicate the defining set $\mathfrak{B}$, we write $\mathcal{O}'_{\mathfrak{B}}$ instead of $\mathcal{O}'$.

We are now able to state the Main Theorem as proved in this paper.

Main Theorem: The Local-Global Principle for Skolem Problems with Rationality Conditions. *Let K be a global field, equipped with a set $\mathfrak{V}$ of primes not containing all primes of K. In addition, let a finite subset $\mathfrak{S} \subset \mathfrak{V}$ be given. Let V be a geometrically integral variety defined over K, and $\boldsymbol{x} = (x_1, \ldots, x_n)$ a finite family of rational functions on V, defined over K.*

Suppose that locally, $V_{\boldsymbol{x}}(\mathcal{O}_\mathfrak{p})$ contains a non-singular point for each prime $\mathfrak{p} \in \mathfrak{S}$, and that $V_{\boldsymbol{x}}(\tilde{\mathcal{O}}_\mathfrak{p})$ is non-empty for $\mathfrak{p} \in \mathfrak{V} \setminus \mathfrak{S}$. Then globally, $V_{\boldsymbol{x}}(\mathcal{O}')$ is non-empty and moreover contains non-singular points of V.

Remarks. 1) For Skolem problems with rationality conditions the requirement that $V_{\boldsymbol{x}}(\mathcal{O}_\mathfrak{p})$ contains points *which are non-singular* cannot be dropped. For the proof we need the fact that for $\mathfrak{p} \in \mathfrak{S}$, $V_{\boldsymbol{x}}(\mathcal{O}_\mathfrak{p})$ is Zariski dense. In particular this means it contains non-singular points. On the other hand if $V_{\boldsymbol{x}}(\mathcal{O}_\mathfrak{p})$ contains a non-singular point then the density follows by Hensel's Lemma. By Hensel's Lemma it follows that $P_\mathfrak{p}$ is not isolated in $V_{\boldsymbol{x}}(\mathcal{O}_\mathfrak{p})$; in fact, in any $\mathfrak{p}$-adically open neighborhood of $P_\mathfrak{p}$ there exist infinitely many non-singular points which are rational in $K_\mathfrak{p}$ (Appendix, 9.2). As we shall see this will be crucial in our proof. However no non-singularity condition appears at the places $\mathfrak{p} \in \mathfrak{V} \setminus \mathfrak{S}$. This can be explained by the fact that $V_{\boldsymbol{x}}(\tilde{\mathcal{O}}_\mathfrak{p})$ is Zariski dense by the result of Robinson mentioned earlier.

2) The proof of the Main Theorem we give holds under slightly more general hypotheses which could be used to give an axiomatisation of fields endowed with families of places having the Local-Global Principle.

To prove the Local-Global Principle with rationality conditions we first consider the case where V is a normal projective curve over K. This is the part of the proof that requires the most work. After that, a *Bertini* type induction procedure with respect to the dimension of V and considerations of birational nature, lead to the general case. The proof we give for curves rests essentially on the following results:

1) *The Local Existence Theorem* for functions on curves whose zeros are situated near prescribed points on the curve. Using this result we show that if $\mathfrak{S}$ is a finite set of places of K, and for every $\mathfrak{p} \in \mathfrak{S}$ the set $V_{\boldsymbol{x}}(\mathcal{O}_\mathfrak{p})$ contains non-singular points, then for every positive divisor D of the function field of V over K there exist (many) functions $f \in K(V)$ whose pole divisor is a multiple of D and all zeros are distinct and lie in $V_{\boldsymbol{x}}(\mathcal{O}'_\mathfrak{S})$.

2) *The Unit Approximation Lemma for Polynomials over K* from Cantor-Roquette [C–R]. For a given polynomial $p(x)$ this lemma guarantees the existence of an element $c \in K'$ which approximates given $a_\mathfrak{p} \in K$ arbitrarily closely for $\mathfrak{p} \in \mathfrak{S}$ and satisfies the condition that $p(c)$ is a unit at each $\mathfrak{p} \in \mathfrak{V} \setminus \mathfrak{S}$. Using this result together with certain facts from the reduction theory of curves we are able to replace f by another function whose zeros are not only integral points of V with data $\boldsymbol{x}$ semi-locally as in 1), but also globally over $\mathfrak{V}$.

Concerning the structure of the paper we have divided it into two parts. The first part consists of the main body of the paper where the proofs of 1) and the Main Theorem are given. In the course of these proofs certain results from the theory of algebraic varieties and constant reductions are used. For some of these results we

were unable to find suitable adequate references in the literature, and so we have included these in a short appendix in the form we need and with notation that is consistent with the main part of the paper.

2 The Local Existence Theorem

The Existence Theorem refers to a local field $K_\mathfrak{p}$ for a fixed prime $\mathfrak{p}$. In order to simplify our notation we write K instead of $K_\mathfrak{p}$. *Hence in this section, K will denote a locally compact base field and $\mathfrak{p}$ its canonical prime.*

We consider a separably generated function field $F|K$ of one variable with K as its field of constants. The projective normal model, say V, of $F|K$ is a geometrically integral curve over K. There is a natural bijection of $V(K)$ with the set of K-rational places of $F|K$. We shall identify both sets, i.e., we shall not distinguish between K-rational places of $F|K$ and K-rational points on V. *We assume that $V(K)$ is not empty.* $V(K)$ carries naturally a topology, induced by the $\mathfrak{p}$-adic topology of the base field K (see the Appendix, section 6). We speak of the $\mathfrak{p}$-adic topology of $V(K)$.

In this situation we have the following

Theorem 2.1 (Local Existence Theorem.) *Given a $\mathfrak{p}$-adically open set $\mathcal{U} \subset V(K)$ which is non-empty, there exists a function $f \in F$ all of whose zeros are distinct*[3]*, K-rational and contained in $\mathcal{U}$. Moreover, f can be constructed such that its pole divisor is a multiple mD of any prescribed positive divisor D of $F|K$, with m arbitrarily large.*

Over the complex field, this is one of the classical theorems of analytic function theory, due to Jacobi. For the algebraic closure of a non-archimedean local-field this result was first stated and proved by Rumely. Here we shall show that the theorem indeed remains valid rationally over the field K itself; it is not necessary to extend the field of constants. The following proof includes the archimedean case in which $K = \mathbb{R}$ or $K = \mathbb{C}$.

If the function field has genus zero then the theorem is trivial: Choose arbitrary distinct points $Q_1, \ldots, Q_r \in \mathcal{U}$ ($r = m \deg D$); then the divisor $\sum Q_i$ has the same degree as mD and hence there is a function $f \in F$ with zero divisor $\sum Q_i$ and pole divisor mD.

In the following proof we shall assume that $F|K$ is of genus $g > 0$.

If the characteristic of K is 0 then the curve V, being geometrically integral and normal over K, is known to be *smooth*. In characteristic $p > 0$ this is not always the case; the function field $F|K$ is not necessarily conservative. Thus we have to face the situation that V may have singularities. In any case, however, every K-rational point of V is non-singular. In particular the given subset $\mathcal{U} \subset V(K)$ consists of non-singular points only; this will be used in the proof of Theorem 2.1.

Since V is not necessarily smooth, we cannot work with the ordinary jacobian variety but we have to use the *generalized jacobian variety* $\mathcal{J}_V$ in the sense

[3]) As usual, this means that f has no multiple zeros.

of Rosenlicht, which is defined for curves V with singularities. $\mathcal{J}_V$ is a group variety defined over K whose dimension equals the genus g of $F|K$. Let us briefly state its relevant properties which we are going to use.[4])

(J1) For any extension field L of K, the group of L-rational points $\mathcal{J}_V(L)$ is naturally isomorphic to the "generalized divisor class group of degree 0 of V over L". In the present context, it will not be necessary to explain in detail the notion of generalized divisor classes with respect to a possibly singular curve. It will be sufficient to note that for $L=K$, as V is normal over K, *the generalized divisor class group is naturally isomorphic with the ordinary divisor class group $\mathcal{C}\ell(F|K)$ of the function field $F|K$.*[5]) Thus we have a natural isomorphism

$$\mathcal{J}_V(K) = \mathcal{C}\ell_0(F|K) \tag{2}$$

where the index 0 means divisor classes of degree 0. We shall identify both groups whenever convenient and possible.

(J2) Consider the g-fold product $V^g = V\times\cdots\times V$ and the corresponding symmetric product $V^{(g)} = V^g/S_g$, where S_g is the symmetric group of degree g acting naturally on V^g. The variety $V^{(g)}$ parametrizes the positive divisors of degree g on V. Namely, if $A = P_1+\cdots+P_g$ is such a divisor then its corresponding point in $V^{(g)}$ is the image of $(P_1,\ldots,P_g)$ under the projection $\pi: V^g \to V^{(g)}$. In this way, the positive divisors A of degree g of $F|K$ correspond to the K-rational points in $V^{(g)}(K)$. Whenever possible and convenient, we identify such a divisor A with its corresponding point on $V^{(g)}(K)$.

The generalized jacobian $\mathcal{J}_V$ is birationally equivalent to $V^{(g)}$ over K. More precisely, the situation is as follows. Let P_0 be a fixed K-rational point of V. There exists an affine Zariski-open X of $V^{(g)}$ and a smooth morphism $\varphi: X \to \mathcal{J}_V$ defined over K, which establishes a birational equivalence between $V^{(g)}$ and $\mathcal{J}_V$, and which has the following property:

If A is a positive divisor of degree g of $F|K$ which, when considered as a point of $V^{(g)}(K)$, is contained in $X(K)$ then φA is the divisor class of $A - gP_0$, considered as a point of $\mathcal{J}_V(K)$.

We may express this by the formula

$$\varphi A \sim A - gP_0 \quad \text{if} \quad A \in X(K),$$

where $\sim$ means divisor equivalence (modulo principal divisors).

By construction, X and φ depend on the choice of P_0. In the following we assume that P_0 is chosen once for all, if nothing is said to the contrary.

Any non-empty Zariski open subset of X enjoys the same properties as we have announced above for X itself. For technical reasons, it will be convenient to replace X by a suitable Zariski-open subset, as follows. The projection $\pi: V^g \to V^{(g)}$

---

[4]) As a general reference for generalized jacobian varieties we suggest chapter 9 of [B-L-R]. Alternatively, the reader may refer to the treatment in Serre's book [S] but he should be aware that rationality questions, over a fixed field K, are not treated there in the generality which we need here.

[5]) Using the now standard terminology from algebraic geometry the divisors of the function field $F|K$ correspond to the Weil divisors of V.

is of finite degree and separable. Hence there exists a Zariski-open $Y \subset V^{(g)}$ such that π is smooth over Y, which is to say that if $Y' \subset V^g$ denotes the foreimage of Y then π induces a smooth map $Y' \to Y$. Now we replace X by $X \cap Y$ and, hence, we may assume that the projection is smooth over X.

Let X' denote the foreimage of X under π and $\varphi' : X' \xrightarrow{\pi} X \xrightarrow{\varphi} \mathcal{J}_V$ the composite map. By construction, $\varphi' : X' \to \mathcal{J}_V$ is smooth.

(J3) The $\mathfrak{p}$-adic topology of K induces, for every variety over K, a topology in the space of K-rational points of that variety (called the $\mathfrak{p}$-adic topology). In particular $\mathcal{J}_V(K)$ is a topological group, and $\varphi : X(K) \to \mathcal{J}_V(K)$ is a topological homeomorphism of $X(K)$ onto its image, which is a dense subspace of $\mathcal{J}_V(K)$. The map $\varphi' : X'(K) \to \mathcal{J}_V(K)$, being smooth as a geometric map, is a *local homeomorphism.* (This is a consequence of Hensel's Lemma; see the Appendix 9.2.)

In the proof of the Local Existence Theorem we shall need the following

Lemma 2.2 *Let $z \in \mathcal{J}_V(K)$. There exists a sequence of multiples $n_1 z$, $n_2 z$, $n_3 z, \ldots$ of z which converges to 0 in the $\mathfrak{p}$-adic topology of $\mathcal{J}_V(K)$. In other words: Given any neighborhood $\mathcal{W}$ of 0 in $\mathcal{J}_V(K)$ there exist infinitely many $n \in \mathbb{N}$ such that $nz \in \mathcal{W}$.*

If V is smooth then $\mathcal{J}_V$ is the ordinary jacobian variety, hence an abelian variety; this implies that $\mathcal{J}_V(K)$ is *compact* in the $\mathfrak{p}$-adic topology as K is locally compact. In this case the lemma is evident: Because of compactness, the sequence of points z, $2z$, $3z, \ldots$ has an accumulation point in $\mathcal{J}_V(K)$, say a. Consider a subsequence $m_1 z$, $m_2 z$, $m_3 z, \ldots$ which converges to a. Putting $n_k = m_{2k} - m_k$ we conclude that $n_k z$ converges to 0.

If V is not smooth (hence K of positive characteristic) then the above argument has to be modified. To this end we need the following additional properties of the generalized jacobian, concerning base field extensions.

(J4) Let $L|K$ be a finite field extension. We denote by $V_L = V \times_K L$ the corresponding base change. V_L is not necessarily normal over L. Let W be its normalization. The normalization morphism $W \to V_L$ gives rise to a morphism of algebraic groups $\mathcal{J}_{V_L} \to \mathcal{J}_W$ which is defined over L. Hence we have a canonical homomorphism

$$\mathcal{J}_V(L) = \mathcal{J}_{V_L}(L) \to \mathcal{J}_W(L). \tag{4}$$

Combined with the ordinary inclusion $\mathcal{J}_V(K) \hookrightarrow \mathcal{J}_V(L)$ we get a homomorphism

$$\psi_L : \mathcal{J}_V(K) \to \mathcal{J}_W(L). \tag{5}$$

By means of (2) this may be interpreted as a homomorphism of the respective divisor class groups of degree 0:

$$\psi_L : \mathcal{C}\ell_0(F|K) \to \mathcal{C}\ell_0(FL|L). \tag{6}$$

We have: *This homomorphism coincides with the ordinary divisor class map belonging to $FL|L$ as a constant field extension of $F|K$.* In other words: The homomorphism (6) is obtained by regarding each divisor D of $F|K$ as a divisor of $FL|L$ and then factoring by principal divisors.

As a consequence we can state: *The kernel of ψ_L is annihilated by a power p^e of the characteristic exponent p of K.*

This is trivially so if $L|K$ is separable since then $V_L = W$ is normal over L and ψ_L coincides with the inclusion $\mathcal{J}_V(K) \hookrightarrow \mathcal{J}_V(L)$, hence its kernel vanishes. Thus we may assume that $L|K$ is purely inseparable, of degree $[L:K] = p^e$ where $p > 1$ is the characteristic. We interpret the map (5) as the divisor class map (6). Let D be some degree 0 divisor of $F|K$ whose class is in the kernel, in other words: D becomes principal in FL. Let $f_L \in FL$ be a function such that $D = (f_L)$ in $FL|L$. The p^e-th power $f = f_L^{p^e}$ *lies in* F and, hence, $p^e D = (f)$ is a principal divisor in $F|K$. Thus the class of D in $\mathcal{C}\ell_0(F|K)$ is annihilated by p^e.

(J5) Referring to the $\mathfrak{p}$-adic topology, the canonical projection map (4) is a homomorphism of topological groups, and it is an open and closed map. The inclusion map $\mathcal{J}_V(K) \hookrightarrow \mathcal{J}_V(L)$ is a topological immersion. Consequently, the combined map (5) is open and closed onto its image.

Now we can give the proof of Lemma 2.2 *in the case when V is not smooth:*

There exists a purely inseparable finite extension $L|K$ such that the normalization W of V_L is a smooth curve. Then $\mathcal{J}_W$ is the usual jacobian variety of W, hence $\mathcal{J}_W(L)$ is compact. By the argument given above in the compact case, there is a sequence of multiples of $\psi_L(z)$ which converges to 0 in $\mathcal{J}_W(L)$. Hence, given any neighborhood $\mathcal{W}$ of 0 in $\mathcal{J}_V(K)$ we conclude that there are infinitely many $n \in \mathbb{N}$ such that $\psi_L(nz) \in \psi_L(\mathcal{W})$. (Here we have used that ψ_L is open onto its image.) This implies that

$$nz \in \mathcal{W} + \ker(\psi_L).$$

As the kernel is annihilated by some power p^e of the characteristic, we conclude

$$p^e nz \in p^e \mathcal{W}.$$

Here, $p^e \mathcal{W}$ becomes small if $\mathcal{W}$ does. Lemma (2.2) follows.

After these preliminaries we are now able to give the

Proof of the Local Existence Theorem. Consider the given subset $\mathcal{U} \subset V(K)$ which by hypothesis is $\mathfrak{p}$-adically open and non-empty. After shrinking $\mathcal{U}$ if necessary we may suppose that $\mathcal{U}$ does not contain the point P_0 which has been chosen in (J2) above, in the course of a description of the generalized jacobian $\mathcal{J}_V$. Moreover, given the positive divisor D as announced in the theorem, we may suppose that $\mathcal{U}$ does not contain any point in the support of D.

Our aim is to find an integer $m > 0$ and distinct points $Q_1, \ldots, Q_r$ in $\mathcal{U}$ such that

$$(7) \qquad mD \sim Q_1 + \cdots + Q_r,$$

where, as above, $\sim$ means divisor equivalence in $F|K$. This relation expresses the fact that there is a function $f \in F$ with mD as its pole divisor and $Q_1 + \cdots + Q_r$ as its zero divisor, as required in the theorem.

Let $d > 0$ be the degree of D. The number r of the points Q_i to be found is necessarily equal to md. Fo technical reasons we let $m = ng$ be a multiple of the

genus g; then $r = ngd$ is a multiple of g too. Accordingly we use another numbering, collecting successively g points of the Q's to form positive divisor of degree g:

$$A_\nu = Q_{\nu 1} + \cdots + Q_{\nu g},$$

and we write (7) in the form

$$(8) \qquad ngD \sim \sum_{1 \leqslant \nu \leqslant nd} A_\nu,$$

Equivalently,

$$(9) \qquad n(gD - gdP_0) \sim \sum_{1 \leqslant \nu \leqslant nd} (A_\nu - gP_0).$$

This is a relation in $\mathscr{C}\ell_0(F|K) = \mathscr{J}_V(K)$.

Let us put

$$\boldsymbol{Q}_\nu = (Q_{\nu 1}, \ldots, Q_{\nu g}) \in V^g(K),$$

so that $A_\nu = \pi(\boldsymbol{Q}_\nu)$ is the image of $\boldsymbol{Q}_\nu$ under the projection $\pi : V^g \to V^{(g)}$. One of the requirements is that all the $Q_{\nu i}$ should be contained in $\mathscr{U}$, i.e., $\boldsymbol{Q}_\nu \in \mathscr{U}^g$. Furthermore we now require that each $\boldsymbol{Q}_\nu$ should be in $X'(K)$, the space which has been defined in (J2) above in the course of a description of the generalized jacobian. If $\boldsymbol{Q}_\nu \in X'(K)$ then $\varphi'(\boldsymbol{Q}_\nu)$ is defined and

$$\varphi'(\boldsymbol{Q}_\nu) \sim A_\nu - gP_0.$$

Hence the relation (9) may be expressed in the form

$$(10) \qquad nz = \sum_{1 \leqslant \nu \leqslant nd} \varphi'(\boldsymbol{Q}_\nu),$$

where for brevity we have written z for the class of the divisor $gD - gdP_0$.

Now the situation is as follows: z is a given point in $\mathscr{J}_V(K)$, and $d > 0$ a positive number. Our aim is to find a natural number $n > 0$ and nd points $\boldsymbol{Q}_\nu \in \mathscr{U}^g \cap X'(K)$ such that (10) holds. In addition, it is required that all the points $Q_{\nu i} \in \mathscr{U}$ which appear as components of the $\boldsymbol{Q}_\nu$ are mutually distinct.

We observe first that $\mathscr{U}^g \cap X'(K)$ is not empty: namely, since $\mathscr{U}$ is $\mathfrak{p}$-adically open in $V(K)$ and consists of non-singular points only, the same holds for $\mathscr{U}^g$ in $V^g(K)$. It follows from Hensel's Lemma that $\mathscr{U}^g$ is Zariski dense in $V^g(K)$, hence indeed $\mathscr{U}^g \cap X'(K)$ is open and non-empty.

As explained in (J3) the map $\varphi' : X'(K) \to \mathscr{J}_V(K)$ is a local homeomorphism. We now choose a non-empty $\mathfrak{p}$-adically open subset

$$\mathscr{U}' \subset \mathscr{U}^g \cap X'(K)$$

such that φ', restricted to $\mathscr{U}'$, is a homeomorphism. We put

$$\mathscr{W} = \varphi'(\mathscr{U}').$$

We shall proceed in two steps. In Step 1 we shall show that for suitable n we can find points x_ν such that

$$(11) \qquad nz = \sum_{1 \leqslant \nu \leqslant nd} x_\nu \quad \text{with} \quad x_\nu \in \mathcal{W}.$$

Writing $x_\nu = \varphi'(Q_\nu)$ with $Q_\nu \in \mathcal{U}'$ we see that this satisfies (10). Thereafter in Step 2 we shall show that by modifying the x_ν slightly within $\mathcal{W}$, we can also satisfy the additional requirement that all the points $Q_{\nu i}$ which appear as components of the Q_ν are distinct.

Step 1: We choose any point $x \in \mathcal{W}$. Then $\mathcal{W} - x$ is a neighborhood of 0 in $\mathcal{J}_V(K)$. Now we apply Lemma 2.2 to the point $z - dx \in \mathcal{J}_V(K)$. We find a natural number n such that $n(z - dx) \in \mathcal{W} - x$, which is to say that there exists $x_1 \in \mathcal{W}$ such that $nz - ndx = x_1 - x$, or,

$$nz = x_1 + (nd - 1)x.$$

Putting $x_\nu = x$ for $\nu = 2, \ldots, nd$ we see that the relation (11) is satisfied. We also note that according to Lemma 2.2 we can choose n to be arbitrarily large. In particular, we can and will assume that $nd \geqslant 3$; this means that on the right hand side of (11) there appear at least three summands. This will be essential in the argument for the second step.

Step 2: Write $x_\nu = \varphi'(Q_\nu)$ with $Q_\nu = (Q_{\nu 1}, \ldots, Q_{\nu g}) \in \mathcal{U}'$. The additional condition requires that for every pair $\mu \neq \nu$, all the components of

$$(Q_\mu, Q_\nu) = (Q_{\mu 1}, \ldots, Q_{\mu g}, Q_{\nu 1}, \ldots, Q_{\nu g}) \in V^{2g}(K)$$

are mutually distinct.

In $V^{2g} = V^g \times V^g = V \times \cdots \times V$ we consider the subvariety Δ consisting of those points $(P_1, \ldots, P_{2g})$ for which at least two components coincide: $P_i = P_j$ for some $i \neq j$ (the "full generalized diagonal"). Δ is of dimension less than $2g$, hence its complement $V^{2g} \setminus \Delta$ is non-empty and Zariski open. Our additional requirement can now be expressed in the form

$$(Q_\mu, Q_\nu) \notin \Delta(K) \quad \text{if} \quad \mu \neq \nu.$$

Now, $\mathcal{U}' \times \mathcal{U}'$ is $\mathfrak{p}$-adically open and non-empty, and it consists of non-singular points only, hence it is Zariski-dense (by Hensel's Lemma again). It follows that the intersection of $\mathcal{U}' \times \mathcal{U}'$ with $V^{2g}(K) \setminus \Delta(K)$ is $\mathfrak{p}$-adically open and dense in $\mathcal{U}' \times \mathcal{U}'$. In other words: if we put

$$\Delta_{\mathcal{U}'} = \Delta(K) \cap (\mathcal{U}' \times \mathcal{U}')$$

then its complement is $\mathfrak{p}$-adically open and dense in $\mathcal{U}' \times \mathcal{U}'$.

Applying the homeomorphism $\varphi' \times \varphi' : \mathcal{U}' \times \mathcal{U}' \to \mathcal{W} \times \mathcal{W}$, we obtain a subset $\Delta_{\mathcal{W}}$ of $\mathcal{W} \times \mathcal{W}$ whose complement is $\mathfrak{p}$-adically open and dense. Now our additional requirement can be expressed as follows:

$$(x_\mu, x_\nu) \notin \Delta_{\mathcal{W}} \quad \text{if} \quad \mu \neq \nu.$$

This condition can be satisfied, as a consequence of the following group theoretical lemma which we prefer to state separately.

Lemma 2.3 *Let G be a topological group whose group operation is written additively, and let $x_1, \ldots, x_k$ be elements in G. For each v, Let $\mathcal{W}_v$ be a neighborhood of x_v and, for each $\mu \neq v$, let $\Delta_{\mu v}$ be a subset of $\mathcal{W}_\mu \times \mathcal{W}_v$ whose complement is open and dense in $\mathcal{W}_\mu \times \mathcal{W}_v$. Then if $k \geqslant 3$, there are elements $y_v \in \mathcal{W}_v$ such that*

$$x_1 + \cdots + x_k = y_1 + \cdots + y_k, \tag{12}$$

and moreover

$$(y_\mu, y_v) \notin \Delta_{\mu v} \quad \text{if} \quad \mu \neq v \tag{13}$$

In other words: By a small perturbation $x_v \mapsto y_v$ the $y_1, \ldots, y_k$ can be made to satisfy the additional condition (13) *without changing the sum* (12).

Proof. If $(x_\mu, x_v) \in \Delta_{\mu, v}$ then (x_μ, x_v) is called a "failure", namely a failure to satisfy condition (13). We assume that $x_1, \ldots, x_k$ has at least one failure; we are going construct $y_1, \ldots, y_k$ with less failures, but with the same sum (12).

If (x_μ, x_v) is not a failure then we choose neighborhoods $\mathcal{U}_\mu \subset \mathcal{W}_\mu$ of x_μ, and $\mathcal{U}_v \subset \mathcal{W}_v$ of x_v such that

$$(\mathcal{U}_\mu \times \mathcal{U}_v) \cap \Delta_{\mu v} = \emptyset$$

(this is possible since the complement of $\Delta_{\mu v}$ is open). After replacing $\mathcal{W}_\mu$ by $\mathcal{U}_\mu$ and $\mathcal{W}_v$ by $\mathcal{U}_v$ we then may suppose that $\Delta_{\mu v} = \emptyset$. This guarantees that for arbitrary choices of $y_1 \in \mathcal{W}_1, \ldots, y_k \in \mathcal{W}_k$ no new failures will appear: if (x_v, x_μ) is not a failure then (y_μ, y_v) is not a failure either.

Let, say, (x_2, x_3) be a failure and recall that $k \geqslant 3$. We put $y_i = x_i$ for $i > 3$. Now the equation (12) reads

$$x_1 + x_2 + x_3 = y_1 + y_2 + y_3, \tag{14}$$

While the x_i are to be regarded as fixed, this defines y_1 as a continuous function of $(y_2, y_3) \in G \times G$, say $y_1 = h(y_2, y_3)$. After shrinking $\mathcal{W}_2$ and $\mathcal{W}_3$ again if necessary, we may assume that $h(\mathcal{W}_2 \times \mathcal{W}_3) \subset \mathcal{W}_1$. Now, since the complement of $\Delta_{2,3}$ is dense there exists

$$(y_2, y_3) \in \mathcal{W}_2 \times \mathcal{W}_3, \qquad (y_2, y_3) \notin \Delta_{2,3}. \tag{15}$$

Putting $y_1 = h(y_2, y_3)$ we see that (14) and hence (12) holds. As said above, among the y_v there appear no new failures. However, from (15) we see that (y_2, y_3) is not a failure although (x_2, x_3) was one. □

The Local Existence Theorem is proved.

For a non-discrete group G the complement of the diagonal in $G \times G$ is open and dense. Hence the above lemma yields the following corollary which we shall use in the next section. In view of the intended application we shall write the group operation multiplicatively here.

Corollary 2.4 *Let G be a non-discrete topological group, written multiplicatively, and let $x_1, \ldots, x_k \in G$. If $k \geqslant 3$ then there are $y_\nu \in G$, arbitrary close to the x_ν, such that $y_1 y_2 \cdots y_k = x_1 x_2 \cdots x_k$ and, moreover, $y_\mu \neq y_\nu$ if $\mu \neq \nu$.*[6])

Remark 2.5 Concerning the pole divisors mD of the functions f of the Existence Theorem: In the above proof we have seen that m can be chosen of the form $m = ng \geqslant 3$, where n is some number such that (11) can be satisfied. Now it is clear that any multiple kn of n also has this property: We have to repeat the sum on the right hand side of (11) k times in order to obtain a similar relation for kn. This yields:

With a suitable choice of $m \in \mathbb{N}$ the following holds: For every multiple km of m ($k \geqslant 1$) there exists a function in F with pole divisor kmD, having the properties as announced in the Existence Theorem above: the zeros of this function are distinct and contained in $\mathcal{U}$.

Remark 2.6 Suppose that $f \in F$ satisfies the conditions of the theorem, and f has pole divisor mD. Then

$$f \in \mathcal{L}(mD)$$

where $\mathcal{L}(mD)$ denotes the linear space of mD in the sense of Riemann-Roch, consisting of all functions in F whose pole divisor is $\leqslant mD$. $\mathcal{L}(mD)$ is a finite dimensional vector space over K and is thus endowed with the natural $\mathfrak{p}$-adic vector space topology. The theorem on the continuity of the roots (Appendix 7.1) now implies:

Any function $h \in \mathcal{L}(mD)$ which is sufficiently close to f also enjoys the same properties as announced for f in the Existence Theorem, namely: All the zeros of h are rational in K and distinct, and are contained in $\mathcal{U}$; moreover, the pole divisor of h is precisely mD.

More precisely, if $z_1, \ldots, z_n$ is a K-basis of $\mathcal{L}(mD)$ and if $f = \sum c_i z_i$ with $c_i \in K$, then there exists $\varepsilon > 0$ such that the announced properties hold for any function h of the form $h = \sum d_i z_i$ with $d_i \in K$ and $\max |d_i - c_i|_\mathfrak{p} \leqslant \varepsilon$.

We remark that for this conclusion it is necessary that the zeros of f are *distinct*. Otherwise, if there would be multiple zeros, we would still have a statement about continuity of roots, but in general the zeros of h will no longer be rational for the given base field K.

In the sequel we shall use this continuity argument many times.

3 Semi-local Approximation

In this section K denotes a field which is equipped with a finite set $\mathfrak{S}$ of primes $\mathfrak{p}$ of local type. We say that $\mathfrak{p}$ is of local type if the completion $K_\mathfrak{p}$ is locally compact and $K_\mathfrak{p}|K$ is separable. Instead of local compactness it is sufficient to require that the Local Existence Theorem 2.1 holds for $K_\mathfrak{p}$.[7])

---

[6]) For most groups G this statement holds also for $k = 2$; the exceptions are those which contain arbitrary small open subgroups of exponent two.

[7]) In [G-M-P] it is shown that for the Local Existence Theorem to hold, it suffices to suppose that with respect to $\mathfrak{p}$, the value group of K has rational rank 1 and the residue field is algebraic over a finite field.

As in the introduction $K' = K^{\mathfrak{S}}$, the field of totally $\mathfrak{S}$-adic elements over K; the prolongation of $\mathfrak{S}$ to K' is denoted by $\mathfrak{S}'$ and $\mathcal{O}'_{\mathfrak{S}} \subset K'$ is the integral closure of $\mathcal{O}_{\mathfrak{S}}$ in K'.

We consider the following situation:

$F|K$ a separably generated function field of 1 variable with K as its field of constants,
V the normal projective model of $F|K$, defined over K,
x $= (x_1, \ldots, x_n)$ a finite family of functions in F,
$V_x(\mathcal{O}_{\mathfrak{p}})$ the set of those points $P \in V(K_{\mathfrak{p}})$ for which $x_\nu(P) \in \mathcal{O}_{\mathfrak{p}} (1 \leqslant \nu \leqslant n)$,
$V_x(\mathcal{O}'_{\mathfrak{S}})$ the set of those points $P \in V(K')$ for which $x_\nu(P) \in \mathcal{O}'_{\mathfrak{S}} (1 \leqslant \nu \leqslant n)$.
We remark that as $K'|K$ is separable these points are all non-singular.

The following theorem states a *"semi-local"* Local-Global Principle, with respect to the *finite* set $\mathfrak{S}$.

Theorem 3.1 *Suppose that $V_x(\mathcal{O}_{\mathfrak{p}})$ is non-empty for each prime $\mathfrak{p} \in \mathfrak{S}$. Then $V_x(\mathcal{O}'_{\mathfrak{S}})$ is non-empty.*

In fact, there exists a non-constant function $f \in F$ all of whose zeros are distinct, and contained in $V_x(\mathcal{O}'_{\mathfrak{S}})$. Moreover, f can be constructed such that its pole divisor is a multiple mD of any prescribed K-rational divisor $D > 0$ of $F|K$, and m can be taken arbitrarily large.

Proof. Let $D > 0$ be a K-rational divisor of $F|K$.

For each $\mathfrak{p} \in \mathfrak{S}$ we consider the constant field extension $FK_{\mathfrak{p}}|K_{\mathfrak{p}}$. Note that $V_x(\mathcal{O}_{\mathfrak{p}})$ is *open* in $V(K_{\mathfrak{p}})$ with respect to the $\mathfrak{p}$-adic topology. Hence we can apply the Local Existence Theorem 2.1 to obtain a function $f_{\mathfrak{p}} \in FK_{\mathfrak{p}}$ with pole divisor a multiple of D, such that all zeros of $f_{\mathfrak{p}}$ are distinct, non-singular and contained in $V_x(\mathcal{O}_{\mathfrak{p}})$.

Using Remark 2.5 we can assume that all these finitely many functions $f_{\mathfrak{p}}$ have the same pole divisor mD, with m arbitrarily large. Then

$$f_{\mathfrak{p}} \in \mathcal{L}_{K_{\mathfrak{p}}}(mD),$$

where $\mathcal{L}_{K_{\mathfrak{p}}}(mD)$ denotes the $K_{\mathfrak{p}}$-vector space of mD in $FK_{\mathfrak{p}}$, in the sense of Riemann-Roch. Since $K_{\mathfrak{p}}|K$ is separable we have

$$\mathcal{L}_{K_{\mathfrak{p}}}(mD) = \mathcal{L}_K(mD) \otimes K_{\mathfrak{p}}$$

where $\mathcal{L}_K(mD)$ is the K-vector space for mD within F. Consider the diagonal embedding

$$\mathcal{L}_K(mD) \to \prod_{\mathfrak{p} \in \mathfrak{S}} \mathcal{L}_{K_{\mathfrak{p}}}(mD).$$

For every $\mathfrak{p} \in \mathfrak{S}$ we endow $\mathcal{L}_{K_{\mathfrak{p}}}(mD)$ with the $\mathfrak{p}$-adic vector space topology. Since the places $\mathfrak{p}$ are independent it follows that $\mathcal{L}_K(mD)$ is dense in the product on the right hand side.

Now we use the theorem of the continuity of the roots (see Remark 2.6). If $f \in \mathcal{L}_K(mD)$ approximates $f_{\mathfrak{p}}$ sufficiently and simultaneously for all $\mathfrak{p} \in \mathfrak{S}$, then

firstly, the pole divisor of f is mD, secondly the zeros of f are distinct, $K_\mathfrak{p}$-rational, non-singular and lie in $V_x(\mathcal{O}_\mathfrak{p})$ (since these properties are known for $f_\mathfrak{p}$).

Let P be any zero of f. Then $P \in V(\tilde{K})$. We show that $P \in V(K')$. Consider a K-embedding $\sigma : \tilde{K} \to \tilde{K}_\mathfrak{p}$, and let P^σ be the image of P. Then $f(P^\sigma) = 0$ (since f is defined over K), thus P^σ also is a zero of f. It follows that P^σ is $K_\mathfrak{p}$-rational. This holds for *every* K-embedding $\sigma : \tilde{K} \to \tilde{K}_\mathfrak{p}$; thus P is totally $\mathfrak{p}$-adic. Since $\mathfrak{p} \in \mathfrak{S}$ is arbitrary, it follows that P is totally $\mathfrak{S}$-adic, i.e., $P \in V(K')$.

We now prove that P lies in $V_x(\mathcal{O}'_\mathfrak{S})$. For any x_k and every prime $\mathfrak{p}'$ of K' which is a prolongation of some $\mathfrak{p} \in \mathfrak{S}$ we have to show that $|x_k(P)|_{\mathfrak{p}'} \leqslant 1$. Now, $\mathfrak{p}'$ induces naturally a K-embedding of valued fields:

$$K' \hookrightarrow K_\mathfrak{p}.$$

Accordingly let us identify $K' \subset K_\mathfrak{p}$; then $|x_k(P)|_{\mathfrak{p}'} = |x_k(P)|_\mathfrak{p}$. Since $P \in V_x(\mathcal{O}_\mathfrak{p})$ we have $|x_k(P)|_\mathfrak{p} \leqslant 1$, as contended. □

Definition. *A non-constant function $f \in F$ is called "$\mathfrak{S}$-admissible" if all of its zeros are K'-rational, distinct and contained in $V_x(\mathcal{O}'_\mathfrak{S})$.*

Thus Theorem 3.1 can be expressed by saying that $\mathfrak{S}$-admissible functions exist, and with an arbitrary high multiple mD as pole divisor – provided the hypothesis of the theorem is satisfied, i.e., $V_x(\mathcal{O}_\mathfrak{p})$ is non-empty for all $\mathfrak{p} \in \mathfrak{S}$.

Remark 3.2 Note that using the theorem on the continuity of the roots (see Remark 2.6) it follows that if f is $\mathfrak{S}$-admissible and $g \in \mathcal{L}_K(mD)$ approximates f sufficiently and simultaneously for all $\mathfrak{p} \in \mathfrak{S}$, then g is also an $\mathfrak{S}$-admissible function.

Now let us discuss what happens when the finite set $\mathfrak{S}$ of primes is enlarged. So let $\mathfrak{T}$ be a finite set of primes containing $\mathfrak{S}$. We need the following lemma.

Lemma 3.3 *For each $\mathfrak{p} \in \mathfrak{T} \setminus \mathfrak{S}$ let $L_\mathfrak{p} | K_\mathfrak{p}$ be a finite Galois extension. Then there exists a finite subextension $L|K$ of $K'|K$ such that, for each $\mathfrak{p} \in \mathfrak{T} \setminus \mathfrak{S}$, $L_\mathfrak{p}$ is contained in the completion of L with respect to any prolongation $\mathfrak{p}_L$ of $\mathfrak{p}$.*

Proof. Let $d_\mathfrak{p}$ denote the degree of $L_\mathfrak{p}|K_\mathfrak{p}$. Let d be a common multiple of these finitely many numbers $d_\mathfrak{p}$. We choose $d/d_\mathfrak{p}$ non-conjugate primitive-elements $\vartheta_\mathfrak{p}^{(j)}$ of $L_\mathfrak{p}|K_\mathfrak{p}$ and let

$$f_\mathfrak{p}(X) = \prod_j f_\mathfrak{p}^{(j)}(X) \qquad (\mathfrak{p} \in \mathfrak{T} \setminus \mathfrak{S})$$

be the product of their monic irreducible polynomials. Thus $f_\mathfrak{p}(X)$ is monic of degree d and all its irreducible factors $f_\mathfrak{p}^{(j)}(X)$ generate the same field extension over K, namely $L_\mathfrak{p}$.

Now consider the primes $\mathfrak{p} \in \mathfrak{S}$. We choose d distinct elements $a_1, \ldots, a_d \in K$ and put

$$f_\mathfrak{p}(X) = \prod_{1 \leqslant i \leqslant d} (X - a_i) \qquad (\mathfrak{p} \in \mathfrak{S}).$$

Let $f(X) \in K[X]$ be a monic polynomial of degree d which is a close approximation to $f_\mathfrak{p}(X)$ for each prime $\mathfrak{p}$, those in $\mathfrak{S}$ and those in $\mathfrak{T} \setminus \mathfrak{S}$. Let $\vartheta \in \tilde{K}$ be a root of $f(X)$ and put $L = K(\vartheta)$.

If the approximation is close enough then by Hensel's (or Krasner's) Lemma $f(X)$ has locally the same factorization behavior as the approximated polynomials. Thus $f(X)$ splits completely over $K_\mathfrak{p}$ for $\mathfrak{p} \in \mathfrak{S}$; this implies that $\mathfrak{p}$ splits completely in L and so $L \subset K'$. On the other hand, if $\mathfrak{p} \in \mathfrak{T} \setminus \mathfrak{S}$ then $f(X)$ factors over $K_\mathfrak{p}$ into $d/d_\mathfrak{p}$ irreducible polynomials all of which generate the same field $L_\mathfrak{p}$. Hence for every prolongation $\mathfrak{p}_L$ of $\mathfrak{p}$ to L it follows that the completion concides with the given field $L_\mathfrak{p}$. □

Corollary 3.4 *In the same situation as in Theorem 3.1, consider a finite set $\mathfrak{T}$ of primes of K, containing $\mathfrak{S}$. Suppose that $V_x(\mathcal{O}_\mathfrak{p})$ for $\mathfrak{p} \in \mathfrak{S}$, and $V_x(\tilde{\mathcal{O}}_\mathfrak{p})$ for $\mathfrak{p} \in \mathfrak{T} \setminus \mathfrak{S}$ are non-empty. Then $V_x(\mathcal{O}'_\mathfrak{T})$ is non-empty.*

In fact, there exists a finite extension $L|K$ of K within K' and a non-constant function $f \in FL$ all of whose zeros are distinct, and contained in $V_x(\mathcal{O}'_\mathfrak{T})$. Moreover, f can be constructed such that its pole divisor is a multiple mD of any prescribed K-rational divisor $D > 0$ of $F|K$, and m can be taken arbitrarily large.

Proof. Since $V(K^s_\mathfrak{p})$ is dense in $V(\tilde{K}_\mathfrak{p})$ for every $\mathfrak{p} \in \mathfrak{T}$, and $V_x(\tilde{\mathcal{O}}_\mathfrak{p})$ is nonempty for $\mathfrak{p} \in \mathfrak{T} \setminus \mathfrak{S}$, we can choose a point $P_\mathfrak{p} \in V_x(\tilde{\mathcal{O}}_\mathfrak{p})$ which is K^s-rational. Hence there exists a finite Galois extension $L_\mathfrak{p}$ of $K_\mathfrak{p}$, such that $P_\mathfrak{p}$ is rational in $L_\mathfrak{p}$. Let L be a finite extension of K within K' as in Lemma 3.3. If $\mathfrak{p}_L$ is a prolongation of $\mathfrak{p}$ to L then, by construction, $P_\mathfrak{p}$ is rational in the completion $L_{\mathfrak{p}_L}$.

We see that over L, the hypothesis of Theorem 3.1 holds for the set $\mathfrak{T}_L$. We use Theorem 3.1 for L, $\mathfrak{T}_L$ instead of K, $\mathfrak{S}$ and obtain a function $f \in FL$ which has the required properties. □

Remark 3.5 In the proof of Theorem 3.1 we have only dealt with the case $\mathfrak{S} \neq \emptyset$. For $\mathfrak{S} = \emptyset$, Theorem 3.1 asserts that $V_x(K^s) \neq \emptyset$ and that for a given positive K-rational divisor D, there is a function $f \in FK^s$ with distinct zeros all belonging to $V_x(K^s)$, and pole divisor some multiple of D. This can either be proved directly or deduced using arguments as in 3.4 above.

For normal projective curves, Corollary 3.4 *is identical with our Main Theorem in the case when $\mathfrak{B}$ is finite.* (Take $\mathfrak{T} = \mathfrak{B}$.)

The following sections deal with a refinement of the above approximation procedures in order to be able to deal with the case of an infinite set $\mathfrak{B}$.

4 The Main Theorem for Normal Projective Curves

In this section we are going to prove the Main Theorem for the case of normal projective curves. We begin by recalling those facts from the theory of constant reductions which we are going to need.

Let $F|K$ be a separably generated function field of one variable with exact constant field K. Suppose $\mathfrak{p}$ is a non-archimedean prime of K and $\mathfrak{P}$ an extension to

F. We say that $\mathfrak{P}$ is a constant reduction of $F|K$ (at $\mathfrak{p}$) if the residue fields $F\mathfrak{P}|K\mathfrak{p}$ again form a function field of one variable. A function $f \in F$ is called residually transcendental at $\mathfrak{P}$ if $f\mathfrak{P}$ is not a constant of $F\mathfrak{P}$. We remark that f is residually transcendental if and only if $\mathfrak{P}$ is an extension of the Gauß valuation $|\cdot|_{\mathfrak{p},f}$ on $K(f)$ associated to $\mathfrak{p}$ and f to F. We say that f is regular at $\mathfrak{P}$ if it is residually transcendental and $\deg f = \deg f\mathfrak{P}$. Here the degree is always the degree of the function over the exact constant field. Observe that if f is regular at $\mathfrak{P}$ then $K\mathfrak{p}$ is the exact constant field of $F\mathfrak{P}$ and the valuation $|\cdot|_{\mathfrak{P}}$ associated to $\mathfrak{P}$ is the unique extension of $|\cdot|_{\mathfrak{p},f}$ to F.

(R1) *Let $\mathfrak{P}$ be a constant reduction of $F|K$. Let $f, y \in F$, and assume that f is regular at $\mathfrak{P}$, and that $|y|_{\mathfrak{P}} \leqslant 1$. If $\mathrm{supp}(y)_\infty \subset \mathrm{supp}(f)_\infty$ then we have:*

i) $\mathrm{supp}(y\mathfrak{P})_\infty \subset \mathrm{supp}(f\mathfrak{P})_\infty$.

ii) *$y(Q)$ is integral at $\mathfrak{p}$ for every zero Q of f.*

Remark: We do not assume that Q is of degree one over K, hence $y(Q)$ is an algebraic number contained in the algebraic closure $\tilde{K}$ of K. To say that $y(Q)$ is integral at $\mathfrak{p}$ means that for every extension $\tilde{\mathfrak{p}}$ of $\mathfrak{p}$ to $\tilde{K}$ we have $|y(Q)|_{\tilde{\mathfrak{p}}} \leqslant 1$.

Proof: Consider the irreducible equation for y over $K(f)$, of the form

$$\Phi(y, f) = y^s + \sum_i a_i(f) y^i = 0$$

with $a_i(f) \in K(f)$. Since $\mathrm{supp}(y)_\infty \subset \mathrm{supp}(f)_\infty$, the $a_i(f)$ are polynomials in $K[f]$. As $|\cdot|_{\mathfrak{p},f}$ has a unique extension to F (which is $|\cdot|_{\mathfrak{P}}$) and $|y|_{\mathfrak{P}} \leqslant 1$, it follows that y is integral over the valuation ring $\mathcal{O}_{\mathfrak{p},f} \subset K(f)$; hence $|a_i(f)|_{\mathfrak{P}} \leqslant 1$ for each i. This means that the coefficients of the polynomials $a_i(f)$ are integral at $\mathfrak{p}$.

Hence, reducing the above equation modulo $\mathfrak{P}$ we see that $y\mathfrak{P}$ is integral over $K\mathfrak{p}[f\mathfrak{P}]$, and from this that $\mathrm{supp}(y\mathfrak{P})_\infty \subset \mathrm{supp}(f\mathfrak{P})_\infty$.

For assertion ii): Q is not a pole of y, hence $y(Q) \in FQ$ satisfies the $\mathcal{O}_{\mathfrak{p}}$-integral equation $\Phi(y(Q), 0) = 0$, and so is integral at $\mathfrak{p}$.

(R2) *In the situation of* (R1), *if in addition y is $\mathfrak{P}$-regular too, and $\mathrm{supp}(y)_\infty = \mathrm{supp}(f)_\infty$, then the leading coefficient of $a_0(f)$ in the irreducible polynomial of y over $K(f)$ is a unit at $\mathfrak{p}$.*

Proof: The hypothesis is now symmetric in f and y. Hence, considering the irreducible polynomial equation for f over $K(y)$:

$$\Psi(f, y) = f^r + \sum_j b_j(y) f^j = 0,$$

we conclude similarly as above that the $b_j(y) \in K[y]$ are polynomials in y whose coefficients are integral at $\mathfrak{p}$. Now, both polynomials Φ and Ψ differ by a constant factor $\alpha \in K$ only, so $\Phi = \alpha \cdot \Psi$. In fact, α is the coefficient of f^r in Φ and α^{-1} is the

coefficient of y^s in Ψ. Thus both α and α^{-1} are integral at $\mathfrak{p}$, hence α is a unit at $\mathfrak{p}$. As α is the leading coefficient of $a_0(f)$ the results follows.[8])

(R3) *Let $f, y \in F$ be $\mathfrak{P}$-regular functions such that $(f)_\infty = mD$ and $(y)_\infty = nD$ with $(m, n) = 1$. Then there exists a divisor $\bar{D}$ of $F\mathfrak{P}|K\mathfrak{p}$ such that $(f\mathfrak{P})_\infty = m\bar{D}$ and $(y\mathfrak{P})_\infty = n\bar{D}$. In particular, D and $\bar{D}$ have the same degree.*[9])

Proof: We first prove the assertion when $m = n = 1$. Let $\bar{p}(f\mathfrak{P})$ be a monic polynomial over $K\mathfrak{p}$ such that $\bar{p}(f\mathfrak{P})$ and $y\mathfrak{P}$ have no common zeros in $F\mathfrak{P}$. Let $p(f)$ be some monic representative of $\bar{p}(f\mathfrak{P})$ in $K[f]$ and suppose r is its polynomial degree, hence also that of $\bar{p}(f\mathfrak{P})$. Set $u = \dfrac{p(f)}{y^r}$ and observe that

$$\deg u \leqslant r \deg f = r \deg f\mathfrak{P} \leqslant \deg \frac{\bar{p}(f\mathfrak{P})}{y\mathfrak{P}^r} = \deg u\mathfrak{P}.$$

It follows that u is regular at $\mathfrak{P}$ and $(f\mathfrak{P})_\infty = (y\mathfrak{P})_\infty$.

Now suppose that $(f)_\infty = mD$ and $(y)_\infty = nD$ with $(m, n) = 1$. Then $(f^n)_\infty = (y^m)_\infty = mnD$. Hence $n(f\mathfrak{P})_\infty = (f^n\mathfrak{P})_\infty = (y^m\mathfrak{P})_\infty = m(y\mathfrak{P})_\infty$. As $(m, n) = 1$, it follows that $(f\mathfrak{P})_\infty = m\bar{D}$ and $(y\mathfrak{P})_\infty = n\bar{D}$ for some positive divisor $\bar{D}$ of $F\mathfrak{P}|K\mathfrak{p}$. This completes the proof.

(R4) *Given finitely many non-constant functions $f_1, \ldots f_m \in F$ one has: For almost all non-archimedean primes $\mathfrak{p}$ of K there exists a constant reduction $\mathfrak{P}$ of $F|K$ (at $\mathfrak{p}$) such that all f_i are regular at $\mathfrak{P}$.*[10])

Proof: Let $x, y \in F$ be non-constant generators for $F|K$ and $\Phi(X, Y)$ the irreducible polynomial for x, y over K (uniquely determined up to a constant factor). Then for almost all non-achimedean primes $\mathfrak{p}$, reducing coefficientwise yields an irreducible polynomial $\Phi\mathfrak{p}(X, Y)$ of the same degrees in X and Y as Φ. Let $\mathfrak{P}$ denote the associated constant reduction of F. It follows that $\Phi\mathfrak{p}$ is the irreducible polynomial for $x\mathfrak{P}, y\mathfrak{P}$ over K. As the degree is preserved it follows that x, y are $\mathfrak{P}$-regular.

---

[8]) The identity $a_0(0) = \alpha b_0(0)$, obtained from the proof of (R2), can be used to show that there is a unit η at $\mathfrak{p}$ such that

$$\prod_\nu y(Q_\nu) = \eta \prod_\mu f(P_\mu),$$

where the Q_ν range over the zeros of f, each counted with its multiplicity and similarly P_μ ranges over the zeros of y. In particular one deduces, $y(Q_\nu)$ is a unit at $\mathfrak{p}$ for all Q_ν, if and only if $f(P_\mu)$ is a unit at $\mathfrak{p}$ for all P_μ. In [R3] this was called the "Reciprocity Lemma", and the reciprocity factor η was interpreted as a product of local symbols for the poles of f and g. There however, the hypothesis of good reduction is made.

[9]) If $F|K$ admits good reduction at $\mathfrak{p}$ (or, more generally, potentially good reduction) then this is immediate from Deuring's theory of divisor reduction. Our aim here is to prove this without assuming potentially good reduction.

[10]) In the case we are concerned with, where K is a global field, *"almost all"* means *"all but finitely many"*. For arbitrary fields *"almost all"* has to be interpreted as *"all primes of a non-empty Zariski open subset of the space of primes of K"*.

Now consider the $f_i \in F \setminus K$ and let $\Phi_i(X, Y)$ be the irreducible polynomial of x, f_i over K. Again, for almost all primes $\mathfrak{p}$, $\Phi_i(X, Y)$ remains irreducible with the same degrees in X and Y when reduced coefficientwise. We conclude that $\Phi_i \mathfrak{p}(X, Y)$ is the irreducible polynomial for $x\mathfrak{P}, f_i\mathfrak{P}$ over $K\mathfrak{p}$. As the degrees are preserved, we conclude that the f_i are regular at $\mathfrak{p}$.

Following the above preparation we can now prove the Main Theorem for curves.

Theorem 4.1 *Let K be a global field, equipped with a set $\mathfrak{V}$ of primes not containing all primes of K. In addition, let a finite subset $\mathfrak{S} \subset \mathfrak{V}$ be given. Let V be a normal, projective, geometrically integral curve over K with function field $F|K$, and $x = (x_1, \ldots, x_n)$ a finite family of functions from F.*

Suppose that $V_x(\mathcal{O}_\mathfrak{p})$ for $\mathfrak{p} \in \mathfrak{S}$, and $V_x(\tilde{\mathcal{O}}_\mathfrak{p})$ for $\mathfrak{p} \in \mathfrak{V} \setminus \mathfrak{S}$ are non-empty. Then $V_x(\mathcal{O}'_\mathfrak{V})$ is non-empty.

In fact, there exists a finite extension $L|K$ of K within K' and a non-constant function $f \in FL$ all of whose zeros are distinct, and are contained in $V_x(\mathcal{O}'_\mathfrak{V})$.

Proof. We begin with the following preliminary remarks:

The First Enlargement Principle: Let $L|K$ be a finite subextension of $K'|K$ and consider the extensions of $\mathfrak{V}, \mathfrak{S}$ to L. Then the hypotheses of Theorem 4.1 also hold for $L, \mathfrak{V}_L, \mathfrak{S}_L$ instead of $K, \mathfrak{V}, \mathfrak{S}$, with the function field $F|K$, replaced by its constant extension $FL|L$. Moreover, the field L' of totally $\mathfrak{S}_L$-adic elements over L coincides with K'. Consequently, if Theorem 4.1 is known to hold for $L, \mathfrak{V}_L, \mathfrak{S}_L$ then it also holds for $K, \mathfrak{V}, \mathfrak{S}$. *Therefore, in order to prove Theorem* 4.1 *we may replace K by any finite extension L within K' and accordingly $\mathfrak{V}, \mathfrak{S}$ by $\mathfrak{V}_L, \mathfrak{S}_L$. We call this the first enlargement principle and in order to simplify the notation when applying it we will again write $K, \mathfrak{S}$ instead of $L, \mathfrak{S}_L$.*

The Second Enlargement Principle: There is another enlargement principle which allows us to enlarge the set $\mathfrak{S}$. Let $\mathfrak{T} \subset \mathfrak{V}$ be a finite set containing $\mathfrak{S}$. The hypothesis of Theorem 4.1 concerning $\mathfrak{S}$, namely that $V_x(\mathcal{O}_\mathfrak{p}) \neq \emptyset$ for $\mathfrak{p} \in \mathfrak{S}$, may not be satisfied for $\mathfrak{p} \in \mathfrak{T}$. However, Corollary 3.4 shows that there exist points $P \in V_x(\mathcal{O}'_\mathfrak{T})$. Choose any such point P and let L be a finite extension of K within K' such that P is rational over L. Then the values $x_i(P) (1 \leqslant i \leqslant n)$ are L-rational and, at the same time, they are $\mathfrak{p}_L$-integral for every $\mathfrak{p}_L \in \mathfrak{T}_L$. We conclude that the hypothesis of Theorem 4.1 holds for L and $\mathfrak{T}_L$. Now observe that the field of totally $\mathfrak{T}_L$-adic elements over L is contained (by its very definition) in the field K' of totally $\mathfrak{S}$-adic elements over K. Consequently, if Theorem 4.1 is known to hold for $L, \mathfrak{V}_L, \mathfrak{T}_L$ then it also holds for $K, \mathfrak{V}, \mathfrak{S}$. *Therefore, in order to prove Theorem* 4.1 *we may replace $\mathfrak{S}$ by any finite set $\mathfrak{T} \subset \mathfrak{V}$ containing $\mathfrak{S}$, if at the same time K is enlarged suitably within K'. We call this the second enlargement principle.*

The reader should note that if $K, \mathfrak{S}$ is replaced by $L, \mathfrak{T}_L$ then the field $K' = K^\mathfrak{S}$ of totally $\mathfrak{S}$-adic elements over K has to be replaced by the corresponding field $L^{\mathfrak{T}_L}$ of totally $\mathfrak{T}_L$-adic elements. When changing notation and writing again $K, \mathfrak{S}$ instead of $L, \mathfrak{T}_L$ then, consequently, the abbreviated notation K' also changes its meaning, referring now to the new field K (which was formerly L) and the new set $\mathfrak{S}$ (which was formerly $\mathfrak{T}_L$).

The idea of the proof is to enlarge K and $\mathfrak{S}$, as allowed by the enlargement principles, so that the new set $\mathfrak{S}$ will contain all the primes $\mathfrak{p}$ which cause disturbance when going from the semi-local to the global situation.

Applying these principles we observe that from the start we can assume there exists at least one K-rational point on V. Indeed, by Theorem 3.1 it follows that V contains a K'-rational point. Any such K'-rational point of V is already L-rational in a finite subextension field L of K'. By the first enlargement principle we may replace K by L and prove the theorem over L. Changing notation, we again write K instead of L, and so there exists a K-rational point, say P, on V.

For the point P it follows from the Riemann-Roch Theorem that the ring of functions in F having poles only at P is a Dedekind domain with quotient field F. Therefore we can choose a positive integer n_0 sufficiently large such that:

1) there exist non-constant functions $y, y_k \in \mathscr{L}(n_0 P)$ with

$$x_k = \frac{y_k}{y} \qquad (1 \leqslant k \leqslant n).\ ^{11})$$

2) by the Riemann-Roch Theorem there exists $u, t \in F$ with $(u)_\infty = n_0 P$ and $(t)_\infty = (n_0 + 1)P$.

Applying the second enlargement principle we suppose, firstly that $\mathfrak{S}$ contains all archimedean primes of $\mathfrak{B}$. Secondly, in view of (R4) we may assume that for each $\mathfrak{p} \in \mathfrak{B} \setminus \mathfrak{S}$ there is a constant reduction $\mathfrak{P}$ of F prolonging $\mathfrak{p}$ such that all the functions u, t, y, y_k selected in 1) and 2) $(1 \leqslant k \leqslant n)$ are regular at $\mathfrak{P}$. Note that this constant reduction is *uniquely determined* by $\mathfrak{p}$ and these regularity conditions. In the following proof, given any $\mathfrak{p} \in \mathfrak{B} \setminus \mathfrak{S}$, the corresponding symbol $\mathfrak{P}$ will always denote this uniquely determined constant reduction, distinguished by the above conditions.

We remark that by 2) above and (R3) it follows that for each $\mathfrak{p} \in \mathfrak{B} \setminus \mathfrak{S}$ we have $(u\mathfrak{P})_\infty = n_0 \bar{P}$, where $\bar{P}$ is a $K\mathfrak{p}$-rational divisor of $F\mathfrak{P}$ of degree 1.

Now Theorem 3.1 guarantees the existence of a non-constant function $f \in F$ which is $\mathfrak{S}$-admissible, i.e., the zeros of f are distinct, K'-rational and contained in $V_x(\mathcal{O}'_{\mathfrak{S}})$. Moreover, f can be chosen such that

$$(f)_\infty = mn_0 P,$$

a multiple of $n_0 P$. Since f has the same pole divisor as u^m there is a non-zero constant $a \in K$ such that $f = au^m + h$ with $(h)_\infty \leqslant (mn_0 - 1)P$. After multiplying with a^{-1} (which does not change the roots of f and hence does not affect $\mathfrak{S}$-admissibility) we may assume $a = 1$.

We are now going to replace f by a function which is very close to f in the $\mathfrak{S}$-adic topology on $\mathscr{L}(mn_0 P)$, such that all its zeros satisfy the requirements of the theorem. Recall that the property of being $\mathfrak{S}$-admissible is preserved under small perturbations with respect to the $\mathfrak{S}$-topology; see Remark 3.2.

---

[11]) Without loss of generality we may assume from the start that the x_k are non zero. Then indeed, the x_k can be represented as quotients of non-constant functions as required here, provided n_0 is sufficiently large. The condition that the y, y_k are non-constant will save us some trivial case distinctions later.

We multiply h with a suitable factor $b \in K$, i.e., we replace $f = u^m + h$ by the function $f' = u^m + bh$. The factor b is chosen very near to 1 in the $\mathfrak{S}$-adic topology, so that f' is close to f. For $\mathfrak{p} \in \mathfrak{V} \setminus \mathfrak{S}$ we require that

$$|b|_{\mathfrak{p}} \leqslant |h^{-1}|_{\mathfrak{p}};$$

this choice of b is possible in view of the Strong Approximation Theorem in K. (Note that $|h|_{\mathfrak{p}} = 1$ for almost all $\mathfrak{p}$, in view of (R4).) Thus we have $|bh|_{\mathfrak{p}} \leqslant 1$ for $\mathfrak{p} \in \mathfrak{V} \setminus \mathfrak{S}$. After writing again h instead of bh and f instead of f' we now have

$$f = u^m + h \quad \text{with} \quad (h)_\infty \leqslant (mn_0 - 1)P,$$

and $\quad |h|_{\mathfrak{p}} \leqslant 1 \quad$ if $\quad \mathfrak{p} \in \mathfrak{V} \setminus \mathfrak{S}$

This then implies: *f is $\mathfrak{P}$-regular for $\mathfrak{p} \in \mathfrak{V} \setminus \mathfrak{S}$.*

Indeed, examining

$$f\mathfrak{P} = u^m \mathfrak{P} + h\mathfrak{P},$$

it follows by (R1) i) that $\operatorname{supp}(h\mathfrak{P})_\infty \subset \operatorname{supp}(u^m\mathfrak{P})_\infty = \bar{P}$. As $\deg h\mathfrak{P} \leqslant \deg h < mn_0$ and $\deg u^m\mathfrak{P} = mn_0$ (since u is regular), we conclude that

$$\deg f\mathfrak{P} = mn_0 = \deg f$$

and so f is regular at $\mathfrak{P}$.

We have constructed an $\mathfrak{S}$-admissible function f with P as its only pole, such that f is $\mathfrak{P}$-regular for all $\mathfrak{p} \in \mathfrak{V} \setminus \mathfrak{S}$.

For the proof of the theorem we are now going to check whether each zero Q of f is constained in $V_x(\mathcal{O}'_{\mathfrak{V}})$. This means that Q should be K'-rational and the algebraic numbers $x_k(Q)$, $(1 \leqslant k \leqslant n)$ integral at every $\mathfrak{p} \in \mathfrak{V}$. Now, for $\mathfrak{p} \in \mathfrak{S}$ this is true since f is $\mathfrak{S}$-admissible. Thus we have to check whether the $x_k(Q)$ are $\mathfrak{S}$-integral.[12]) If not, then we shall try to modify f further such as to achieve this aim.

We begin by reinterpreting our expression for the x_k, $1 \leqslant k \leqslant n$, so as to simplify the argumentation. Recall that as both y and f are regular at each of the $\mathfrak{P}$, by (R1) and (R2) the coefficients of the polynomials $a_i(f)$ in the irreducible equation

$$\Phi(y, f) = y^s + a_{s-1}(f)y^{s-1} + \cdots + a_0(f) = 0$$

are $\mathfrak{S}$-integral and the leading coefficient of $a_0(f)$ is an $\mathfrak{S}$-unit. Setting $z = y^{s-1} + a_{s-1}(f)y^{s-2} + \cdots + a_1(f)$ and substituting in the expressions for the x_k we obtain

$$x_k = \frac{y_k}{y} = \frac{y_k z}{a_0(f)} =: \frac{z_k}{a_0(f)}, \qquad (1 \leqslant k \leqslant n).$$

Now $x_k(Q) = \dfrac{z_k(Q)}{a_0(0)}$, and by (R1) ii) the algebraic numbers $z_k(Q)$, $a_0(0)$ are $\mathfrak{S}$-integral. Therefore it suffices to check whether $a_0(0)$ is an $\mathfrak{S}$-unit, for each

---

[12]) Recall that an algebraic number is said to be $\mathfrak{S}$-integral, respectively an $\mathfrak{S}$-unit, if it is integral, respectively a unit, at each prime $\mathfrak{p} \in \mathfrak{V} \setminus \mathfrak{S}$.

zero Q of f. If this is the case then the proof is finished. If not, then we replace f by the function $f_c = f - c$ for a suitable constant c. First, c has to be chosen close to 0 in the $\mathfrak{S}$-topology, so that f_c remains $\mathfrak{S}$-admissible. Secondly, c should be an $\mathfrak{S}$-integer, so that $f_c = f - c$ remains $\mathfrak{P}$-regular for $\mathfrak{p} \in \mathfrak{B} \setminus \mathfrak{S}$. Finally, c should be chosen in such a way that for each zero Q of f_c, the algebraic number $a_0(f(Q)) = a_0(c)$ is an $\mathfrak{S}$-unit.

In general it is not possible to find such an *algebraic integer* c within the field K. However using the Approximation Lemma 5.2 from [C-R], we know there exists $c \in \tilde{K}$,

- which is arbitrarily close to 0 in the $\mathfrak{S}$-topology,
- such that $a_0(c)$ is an $\mathfrak{S}$-unit,
- such that every prime $\mathfrak{p} \in \mathfrak{S}$ splits completely in the extension field $L = K(c)$; hence $L \subset K'$.

Now $a_0(c)$ is a polynomial in c with $\mathfrak{S}$-integral coefficients, the leading one an $\mathfrak{S}$-unit. As $a_0(c)$ is an $\mathfrak{S}$-unit, it follows that c is $\mathfrak{S}$-integral. After applying the first enlargement principle, identifying K with L, it follows by 3.2 that $f_c = f - c$ is an $\mathfrak{S}$-admissible function, regular at each of the constant reductions $\mathfrak{P}$ for $\mathfrak{p} \in \mathfrak{B} \setminus \mathfrak{S}$. We conclude that if Q is a zero of f_c then $a_0(f(Q)) = a_0(c)$ is an $\mathfrak{S}$-unit and $z_k(Q)$, $1 \leqslant k \leqslant n$, are $\mathfrak{S}$-integral; hence $x_k(Q)$ is $\mathfrak{S}$-integral. As f_c is $\mathfrak{S}$-admissible the algebraic numbers $x_k(Q)$ are also integral for each $\mathfrak{p} \in \mathfrak{S}$.

We have shown that there is a finite extension L of K within K', and an element $c \in L$ such that the function $f_c = f - c$ satisfies all the requirements of the theorem. That is, the zeros of f_c are distinct and contained in $V_x(\mathcal{O}'_{\mathfrak{B}})$. □

5 The General Case: Reduction to Curves

Our proof of the general case has two steps. First we observe that in the statement of the Main Theorem we can suppose that the variety V is affine, smooth, and also that $\boldsymbol{x}$ consists of a system of holomorphic functions on V. The second step involves a Bertini type induction argument on the dimension of the variety which is assumed to satisfy the hypothesis above.

Step 1: *In the context of the Main Theorem let $U \subset V$ be an affine open of V. Then the assertion of the theorem holds for V if and only if it holds for U.*

Proof: Let $F = K(V) = K(U)$ denote the function field of V and U.

Assume the assertion holds for V. Let $\boldsymbol{x}$ be a tuple of K-rational functions on U and suppose that the Skolem problem for U with data $\boldsymbol{x}$ and $\mathfrak{S}$ rationality conditions is locally solvable. We show that it is globally solvable. To do this we first show that there exists a non-zero function $y \in F$ such that its holomorphy domain D_y is contained in U and moreover, setting $\boldsymbol{y} = (y, x_1, \ldots, x_n)$, the Skolem problem for V with data $\boldsymbol{y}$ and $\mathfrak{S}$ rationality conditions is locally solvable. Indeed, let y' be any non-zero function whose holomorphy domain $D_{y'}$ is contained in U. As $V_x(\mathcal{O}_{\mathfrak{p}})$ is Zariski dense for all $\mathfrak{p} \in \mathfrak{S}$ (Appendix 9.5), it follows that for every such $\mathfrak{p}$ there exist some non-singular $P_{\mathfrak{p}} \in V_x(\mathcal{O}_{\mathfrak{p}})$ which also lies in $D_{y'}$, i.e., $y'(P_{\mathfrak{p}}) \neq \infty$. In particular, for the finite set $\mathfrak{S}$ of places $\mathfrak{p}$ there exists a non-zero constant $c_0 \in \mathcal{O}_{\mathfrak{B}}$

such that $|c_0 y'(P_\mathfrak{p})|_\mathfrak{p} \leqslant 1$ for $\mathfrak{p} \in \mathfrak{S}$. Next let $P_0 \in V(\tilde{K})$ be arbitrary such that $y'(P_0) \neq 0$. Then $y'(P_0)$ is a $\mathfrak{p}$-unit for almost all $\mathfrak{p} \in \mathfrak{B}$, hence there exists a non-zero constant $c_1 \in \mathcal{O}_\mathfrak{B}$ such that $|c_1 y'(P_0)|_\mathfrak{p} \leqslant 1$ for all $\mathfrak{p} \in \mathfrak{B}$. Now setting $y = c_0 c_1 y'$ it follows that the Skolem problem for V with data y and $\mathfrak{S}$-rationality conditions is locally solvable. Then by hypothesis it is solvable globally. Let P be a non-singular global solution. Then in particular, P belongs to D_y and so to $U(K')$. Hence the Skolem problem for U with data x and $\mathfrak{S}$ rationality conditions has the global solution P.

Conversely, assume the assertion holds for U. Let x be the data for a Skolem problem with $\mathfrak{S}$ rationality conditions for V which locally has solutions. Then x defines the data for a Skolem problem with $\mathfrak{S}$ rationality conditions for U. The latter Skolem problem also has local solutions, as the $V_x(\tilde{\mathcal{O}}_\mathfrak{p})$ are Zariski dense (Appendix 9.5), hence they meet U. We are now finished, as every global solution of the latter Skolem problem also is a global solution of the former one.

Step 2: *Reduction to Curves.* Suppose that V is affine, smooth, and that x consists of a system of holomorphic functions on V.

By the Noether Normalisation Theorem there exists a system $\boldsymbol{t} = (t_1, \ldots, t_d)$ of algebraically independent elements in $K[V]$ such that $K[V]$ is integral over $K[\boldsymbol{t}]$. We set $K[V] = K[\boldsymbol{T}, \boldsymbol{Z}]/\mathfrak{P}$, where $\boldsymbol{T} = (T_1, \ldots, T_d)$, $\boldsymbol{Z} = (Z_1, \ldots, Z_m)$ and $\mathfrak{P}$ is the relation ideal which is absolutely irreducible. Before going into the details of the proof we remark that using model theory it follows that except for finitely many $a_1 \in K$ one has:

(*) The ideal $\mathfrak{Q} = (\mathfrak{P}, T_1 - a_1)$ generated by $\mathfrak{P}$ and $T_1 - a_1$ in $K[\boldsymbol{T}, \boldsymbol{Z}]$ is an absolutely irreducible ideal.

Let W be the affine variety over K defined by $K[\boldsymbol{T}, \boldsymbol{Z}]/\mathfrak{Q}$. Then W is geometrically integral and setting $\boldsymbol{u} = (T_2, \ldots T_d) \bmod \mathfrak{Q}$ it follows that $K[W] = K[\boldsymbol{T}, \boldsymbol{Z}]/\mathfrak{Q}$ is integral over $K[\boldsymbol{u}]$ and the canonical projection

$$K[V] = K[\boldsymbol{T}, \boldsymbol{Z}]/\mathfrak{P} \to K[\boldsymbol{T}, \boldsymbol{Z}]/\mathfrak{Q} = K[W]$$

gives rise to the following commutative diagram:

$$\begin{array}{ccc} K[V] & \to & K[W] \\ | & & | \\ K[\boldsymbol{t}] & \to & K[\boldsymbol{u}] \end{array}$$

where the bottom row is defined by $\boldsymbol{t} \mapsto (a_1, \boldsymbol{u})$.

Correspondingly one has the following diagram of morphisms of affine varieties defined over K:

$$\begin{array}{ccc} V & \hookleftarrow & W \\ \downarrow{\scriptstyle pr} & & \downarrow \\ \mathbb{A}^d & \hookleftarrow & \mathbb{A}^{d-1} \end{array}$$

where the top row is a K-embedding of W in V and the bottom row, a K-embedding of $\mathbb{A}^{d-1}$ into $\mathbb{A}^d$ with the constant a_1 on the first coordinate.

We now show that for a proper choice of a_1 the subvariety W satisfies the hypothesis of the Main Theorem with respect to the restriction y of x to W. As $\dim W = d-1$ we can conclude the proof of the Main Theorem by induction.

Let $P_k = P(x_k, t)$ be the irreducible polynomial of x_k over $K[t]$. Then P_k is monic in x_k and as $\mathcal{O}_{\mathfrak{B}_0}$ is Dedekind there exists a finite subset $\mathfrak{S}_1$ of $\mathfrak{B}$ containing $\mathfrak{S}$ such that all coefficients of all polynomials P_k are $\mathfrak{S}_1$-integral. As in the case $\dim V = 1$ there exists a finite subextension $L|K$ of K' such that for the prolongation $\mathfrak{T}_1$ of $\mathfrak{S}_1$ to L one has: the set $V_x(\mathcal{O}_{\mathfrak{q}_1})$ contains non-singular points ($\mathfrak{q}_1 \in \mathfrak{T}_1$). Mutatis mutandis, we can suppose that $L = K$ and hence, $\mathfrak{T}_1 = \mathfrak{S}_1$.

By the jacobian criterion it follows that the morphism pr in the diagram above is smooth on an open subset U_t of V which is defined over K. Equivalently, $t_b = t - t(b)$ is a system of local parameters of $b \in U_t$. As $V_x(\mathcal{O}_\mathfrak{p})$ is Zariski dense in $V(K)$ it follows that $V_x(\mathcal{O}_\mathfrak{p}) \cap U_t(K_\mathfrak{p})$ is a ($\mathfrak{p}$-adic open) non empty set. It follows that each $a_\mathfrak{p}$ in this set has a $\mathfrak{p}$-adic neighborhood which is mapped homeomorphically by pr onto a $\mathfrak{p}$-adic neighborhood $\mathcal{U}_\mathfrak{p}$ of $pr(a_\mathfrak{p})$ in $\mathbb{A}^d(K_\mathfrak{p})$. We shall denote by $\mathcal{V}_\mathfrak{p}$ such a neighborhood which is contained in $V_x(\mathcal{O}_\mathfrak{p})$.

For every $\mathfrak{p} \in \mathfrak{S}_1$ we consider some $a_\mathfrak{p}$, $\mathcal{V}_\mathfrak{p}$ and $\mathcal{U}_\mathfrak{p}$ as above. By the Strong Approximation Theorem for $(K, \mathfrak{B})$ it follows that the set of all points $\boldsymbol{a} \in \mathbb{A}^d(K)$ which lie in all $\mathcal{U}_\mathfrak{p}$ ($\mathfrak{p} \in \mathfrak{S}_1$) and have $\mathfrak{S}_1$-integral coordinates is a Zariski dense subset in $\mathbb{A}^d(K)$. In particular we can choose a point $\boldsymbol{a}$ in this set whose first coordinate a_1 has the property (*) we asked for above. Let y be the restriction of x to W (clearly, y is a system of regular functions on W). For such a point $\boldsymbol{a}$ we note that for every $\mathfrak{p} \in \mathfrak{S}_1$ there exists $b_\mathfrak{p} \in \mathcal{V}_\mathfrak{p}$ such that $pr(b_\mathfrak{p}) = \boldsymbol{a}$. Moreover by the choice of $\boldsymbol{a}$ it follows that $b_\mathfrak{p}$ is a zero of $\mathfrak{Q}$, hence it is a non singular point of W. In particular, $W_y(\mathcal{O}_\mathfrak{p}) \neq \emptyset$ ($\mathfrak{p} \in \mathfrak{S}_1$).

For $\mathfrak{p} \notin \mathfrak{S}_1$ let b be any point of V with $pr(b) = \boldsymbol{a}$. Then $P(x_k(b), \boldsymbol{a}) = 0$ ($1 \leqslant k \leqslant n$). Since P_k is monic in x_k and has $\mathfrak{S}_1$-integral coefficients and $\boldsymbol{a}$ has $\mathfrak{S}_1$-integral coordinates it follows that $x_k(b)$ is $\mathfrak{S}_1$-integral. Hence $W_y(\mathcal{O}_{\mathfrak{p}'}) \neq \emptyset$ for all $\mathfrak{p}'$ not prolonging some $\mathfrak{p} \in \mathfrak{S}_1$.

Therefore, W satisfies the hypothesis of the Main Theorem with respect to the restriction y of x to W. This completes the proof. □

Appendix

In the appendix we have included certain basic facts which were used at several places in the paper. For many of these results we were unable to find suitable adequate references in the literature and so we decided to include this short appendix where they are presented in the form we need and with notation that is consistent with the main part of the paper.

6. Prerequisites concerning Algebraic Varieties

Let V be an absolutely irreducible quasi-projective variety defined over a field K and $\iota : V \hookrightarrow \mathbb{P}^r$ an embedding in some projective space over K. In the text we shall use the word "variety" to mean *"quasi-projective variety"*. A homogeneous function f_d of degree d on V defined over K is the restriction to V via ι of some

homogeneous function of degree d on $\mathbb{P}^r$ which is defined over K. A rational function on V defined over K is by definition the quotient of two homogeneous functions of the same degree on V defined over K. The set of all rational functions on V defined over K is a finitely generated field $K(V)$ over K called the function field of V. Its transcendence degree over K equals $\dim V$.

If $\Omega | K$ is a field extension, then an Ω-rational point of V is defined to be a point P of V such that $\iota(P)$ lies in $\mathbb{P}^r(\Omega)$. One shows that for $P \in V$ to be Ω-rational does not depend on the concrete projective embedding ι used. We shall denote the set of all Ω-rational points by $V(\Omega)$.

Using the language of schemes over K, an absolutely irreducible variety over K is a geometrically integral, separated quasi-projective scheme over K of finite type. For the field extension $\Omega | K$, an Ω-rational point of V corresponds to a homomorphism $\operatorname{Spec} \Omega \to V$ of K-schemes, and the function field $K(V)$ is the local ring of the generic point of V.

With the notations from above let f be a rational function on V defined over K and P a point of V. We say that f is defined at P if there exists a projective embedding ι and a representation $f = f_d/g_d$ of f relative to ι such that g_d does not vanish at P.

The ring of all rational functions on V defined over K which are defined at $P \in V(K)$ is a local subring of $K(V)$ which we denote by $\mathcal{O}_{V,P}$ and call the local ring of P. Its maximal ideal will be denoted by $\mathfrak{m}_{V,P}$.

Let $\mathcal{D}_f$ denote the set of all points at which f is defined. Then f defines a map (which we also denote by f)

$$f : \mathcal{D}_f \to K$$

in a natural way. We endow the set $V(K)$ with the Zariski topology, which has a subbasis the sets $\mathcal{D}_f$ for all rational functions f on V defined over K.

In the scheme language this means that $f \in K(V)$ lies in the image of the canonical ring homomorphism

$$\mathcal{O}_{V,P} \hookrightarrow \mathcal{O}_{V,\eta} = K(V)$$

where η is the generic point of V.

Now suppose that Ω is an algebraically closed overfield of K. We endow $V(\Omega)$ with the Zariski topology as above. Then $V(K)$ embedded canonically in $V(\Omega)$ and equipped with the subspace topology is homeomorphic to $V(K)$ with the Zariski topology.

A subset X of $V(K)$ is called *Zariski dense* if there isn't any non-zero rational function of V vanishing on it. This is equivalent to X being dense in $V(\Omega)$ in the Zariski topology.

Now suppose that K is endowed with a (non-trivial) valuation v. This valuation defines a topology on K, the v-topology in a canonical way.

Further, any finite dimensional K-vector space M can be endowed with a (K, v)-vector space topology in a canonical way. Namely, this is the weakest topology on M such that all K-linear forms $\varphi : M \to (K, v)$ are continuous. This is called the v-topology on M and it has good properties, for example: Any K-multilinear mapping between spaces endowed with the v-topology is continuous.

This topology induces a topology on $\mathbb{P}^r(K)$ (r arbitrary) in a canonical way which we call the v-adic topology on $\mathbb{P}^r(K)$.

More generally, let V be an absolutely irreducible variety over K. Let $\iota: V \hookrightarrow \mathbb{P}^r$ be a projective embedding over K. Then ι induces a canonical bijection of $V(K)$ onto $(\iota(V))(K) = \iota(V) \cap \mathbb{P}^r(K)$. In this way we can endow $V(K)$ with the sub-space topology by ι. One shows that this topology does not depend on the projective embedding ι and we call it the v-adic topology on $V(K)$.

It is clear that a rational function f on V defined over K is continuous in the v-adic topology at all points where it is defined. In fact, the v-adic topology is the weakest topology on $V(K)$ such that all rational functions $f \in K(V)$ are continuous at the points where they are defined. A basis of the v-adic topology is given by all subsets of $V(K)$ of the form

$$\mathcal{U}_x = \{P \in V(K) \mid x_k(P) \in \mathcal{O}_v,\ 1 \leqslant k \leqslant n\}$$

where $x = (x_1, \ldots, x_n)$ runs over all finite systems of rational functions on V. The v-adic opens of the form $\mathcal{U}_x$ are called basic v-adic open subsets of $V(K)$.

From this it follows that the v-adic topology on $V(K)$ is finer then the induced Zariski topology on $V(K)$.

7. Continuity of the Roots of Algebraic Functions

Let (K, v) be an arbitrary valued field and $F|K$ a separably generated function field in 1 variable with constant field K. Let V denote the unique normal projective model of $F|K$. Then the set of all K-rational points $V(K)$ of V is identified in a natural way with the set of all K-rational places of $F|K$. Directly be the defintion of the v-adic topology on $V(K)$ it follows that it is actually the weakest topology on $V(K)$ such that all $f \in F$ define continuous functions

$$f: V(K) \to \mathbb{P}^1(K), \quad P \mapsto f(P).$$

We consider any finite dimensional K-vector subspace M of F as being endowed with the v-topology. Then F itself can be endowed with the strongest topology for which all the inclusions $M \hookrightarrow F$ are continuous. We call this the v-topology of F and we remark the following:

- All inclusions $M \hookrightarrow F$ are immersions in the v-topology.
- F endowed with the v-topology is a topological ring.

Now the main result of this section is:

Theorem 7.1 (Continuity of the Roots) *Let $f \in F$ be a non-zero function. Then we have:*

1) *There exists a v-neighborhood U of f in F such that $(f)_\infty \leqslant (g)_\infty$ for all $g \in U$. In particular, if $g \in U$ and $\deg f = \deg g$ then $(f)_\infty = (g)_\infty$.*

2) *Suppose that K is algebraically closed and let $P_1, \ldots, P_m$ be the distinct zeros of f and $n_k = v_{P_k}(f)$ their multiplicities. Let $\mathcal{U}_k$ be disjoint v-adic neighborhoods of P_k, $(k = 1, \ldots, m)$ in $V(K)$. Then there exists a v-neighborhood U of f in F such that any $g \in U$ has at least n_k zeros in every $\mathcal{U}_k$, if counted with their multiplicities.*

In particular, if $g \in U$ *and* $\deg f = \deg g$ *then* $(f)_\infty = (g)_\infty$ *and* g *has exactly* n_k *zeros in each* $\mathfrak{U}_k$ *if counted with their multiplicities, and these are all the zeros of* g.

Proof. By the definition of the v-topology if suffices to find a v-neighborhood $U = U_M$ of f in every finite dimensional K-vector space $M \subseteq F$ containing f, such that every $g \in U$ has the desired properties. Moreover, since any such M is contained in the linear space of a positive divisor of $F|K$ it suffices to prove the assertion for such spaces. Precisely:

Let A *be a positive divisor of* $F|K$ *and* $\mathscr{L}_K(A)$ *be its linear space over* K. *Then there exists a* v*-neighborhood* $U = U_A$ *of* f *in* $\mathscr{L}_K(A)$ *such that any* $g \in U$ *has the properties* 1) *and* 2) *of the theorem.*

We first remark that our assertions are elementary assertions in the language of valued fields with parameters from K. These parameters come from the definition of V, A, $\mathscr{L}_K(A)$, f and the neighborhoods $\mathfrak{U}_k$ (which we can suppose are basic open sets).

Therefore, to show that our assertions are true, it is sufficient to prove that they are true in a $\varkappa$-saturated extension (K^*, v^*) of (K, v) for some cardinality $\varkappa$. Now suppose that $\varkappa$ is big enough. Then there exist coarsenings v_1 of v^* which are trivial on K. Any such v_1 can be prolonged to a good reduction of $FK^*|K^*$ which is trivial on F. We shall also denote this prolongation by v_1 and let us set $K^* v_1 = K_1$. Now, any non-constant function $h \in F$ is a regular function for v_1 and in particular so is f. Furthermore, since FK^* has good reduction at v_1 it follows that v_1 defines the product topology on $\mathscr{L}_{K^*}(A)$. Therefore,

$$U = f + \{g \in \mathscr{L}_{K^*}(A) \mid v_1(g) > 0\}$$

is a v-neighborhood of f in $\mathscr{L}_{K^*}(A)$ and obviously, $gv_1 = fv_1 = f$ for all $g \in U$.

Next we observe that $(FK^*)v_1$ actually coincides with the constant extension FK_1 of $F|K$. Let

$$\mathrm{Div}\,(FK^*|K^*) \xrightarrow{v_1} \mathrm{Div}\,(FK_1|K_1)$$

be the canonical divisor reduction map, a degree preserving group homomorphism. For the definitions and basic properties of this map, see Deuring [D1] and Roquette [R3]. Taking into account that for any linear space $\mathscr{L}_K(D)$ of any positive divisor D of $F|K$ we have

$$\mathscr{L}_K(D) = (\mathscr{L}_K(D))v_1 \subseteq (\mathscr{L}_{K^*}(A))v_1 = \mathscr{L}_{K_1}(Dv_1)$$

and comparing dimensions we get $\mathscr{L}_{K_1}(Dv_1) = \mathscr{L}_{K_1}(D)$. Therefore, we have a commutative diagram of the form

$$\begin{array}{ccc} \mathrm{Div}\,(F|K) & \xrightarrow{\text{incl}} & \mathrm{Div}\,(FK^*|K^*) \\ \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle v_1} \\ \mathrm{Div}\,(F|K) & \xrightarrow{\text{incl}} & \mathrm{Div}\,(FK_1|K_1) \end{array}$$

Claim: *Let* $\mathfrak{U} = \mathfrak{U}_{f_1,\ldots,f_s}$ *be a basic open subset of* $V(K)$. *Then the preimage of* $\mathfrak{U} \subseteq V(K) \subseteq V(K_1)$ *by the canonical divisor reduction map*

$$\mathrm{Div}\,(FK^*|K^*) \xrightarrow{v_1} \mathrm{Div}\,(FK_1|K_1)$$

is contained in the basic open subset $\mathfrak{U}^*$ defined by $(f_k)_k$ *in* $V(K^*)$.

The proof follows from the following general fact about good reduction:
If w is a good reduction of a function field $E|L$ then for every regular function h and any place $Q \in \mathrm{Div}(E|L)$ it holds: $h(Q)w = hw(Qw)$.
In our situation we have for any $h \in F$ and some P^* which by reduction goes to some $P \in \mathrm{Div}(F|K)$:

$$(h(P^*) - h(P))v_1 = hv_1(P^*v_1) - hv_1(Pv_1) = h(P) - h(P) = 0,$$

ie $h(P^*) - h(P)$ lies in the valuation ideal of v_1 and in particular, also that of v^*. Hence, $v^*(h(P^*)) = v^*(h(P))$ and from this remark our claim follows easily.

We can now complete the proof of the theorem:
With U as above take any $g \in U$. Then, by general constant reduction theory and using $gv_1 = fv_1 = f$ we get:

i) $(g)_\infty v_1 \geqslant (gv_1)_\infty = (f)_\infty$.
ii) $(g)_0 v_1 \geqslant (gv_1)_0 = (f)_0$.

On the other hand, since g lies in $\mathscr{L}_{K^*}(A)$ and A is K-rational it follows that $(g)_\infty$ is K-rational. Hence, by the commutative diagram above we get $(g)_\infty v_1 = (g)_\infty$. Now taking into account i) above the assertion 1) follows. To prove the assertion 2) we remark that by ii) above and the divisor reduction map, the preimage of any $\mathscr{U}_k$ contains at least as many zeros of g as the number of zeros of $gv_1 = f$ in $\mathscr{U}_k$ (counted with their multiplicities, respectively). On the other hand, all these zeros lie in $\mathscr{U}_k^*$, by the claim above. The proof is finished. □

Corollary 7.2 *Let K be a henselian field, $F|K$ a function field and A a positive divisor of $F|K$. Suppose that there exists a function $0 \neq f \in F$ such that $(f)_\infty = A$ and all the zeros P_k of f are K-rational and distinct. Let $\mathscr{U}_k$ be given v-adic open disjoint neighborhood of P_k. Then there exists a neighborhood U of f in $\mathscr{L}_K(A)$ such that all $g \in \mathscr{L}_K(A)$ have the properties:*

1) $(g)_\infty = A$
2) *g has exactly one zeros in each $\mathscr{U}_k$ and these are all the zeros of g.*

Proof. We can suppose that all $\mathscr{U}_k$ are basic open subsets. Let $\tilde{K}$ be the algebraic closure of K and $\tilde{v}$ the unique prolongation of v to $\tilde{K}$. We denote by $\tilde{\mathscr{U}}_k$ the open basic subset of $V(\tilde{K})$ which is defined by the same functions as $\mathscr{U}_k$. Obviously we can suppose that $\tilde{\mathscr{U}}_k$ are pairwise disjoint. By the theorem above we have: If $g \in \mathscr{L}_K(A)$ is sufficiently close to f then $(g)_\infty \geqslant (f)_\infty = A$ and g has at least one $\tilde{K}$-rational zero in every $\tilde{\mathscr{U}}_k$. On the other hand, since g lies in $\mathscr{L}_K(A)$ it follows that $(g)_\infty = A = (f)_\infty$ and therefore, g has exactly one zero in every $\tilde{\mathscr{U}}_k$. Further, we remark that the v-adic basic open sets $\tilde{\mathscr{U}}_k$ are defined over K, hence they are G_K-invariant where G_K denotes the absolute Galois group of K. Since g is defined over K it follows that the zeros of g are G_K-invariant. Since they are also distinct it follows that they are K-rational. □

8. The Higher Dimensional Hensel Lemma

In this section we give the sketch of the proof of the higher dimensional Hensel Lemma we shall use later. Let (K, v) be a valued field. For $\boldsymbol{a} = (a_1, \ldots, a_\varrho)$ in $K^\varrho = K \times \ldots \times K$ we set $v(\boldsymbol{a}) = \min v(a_k)$ $(1 \leqslant k \leqslant \varrho)$ as usual. Now we have the following:

Theorem 8.1 *Let (K, v) be a henselian field. Let $\boldsymbol{f}=(f_1,\ldots,f_\varrho)$ be a system of ϱ polynomials in $\boldsymbol{X}=(X_1,\ldots,X_\varrho)$ variables with v-integral coefficients. Let $J(\boldsymbol{a})$ denote the determinant of the Jacobian matrix $(\partial f_k/\partial X_l(\boldsymbol{a}))$ for an arbitrary $\boldsymbol{a}\in K^\varrho$. Suppose that for some $\boldsymbol{a}$ with v-integral coordinates the following holds:*

$$2v(J(\boldsymbol{a})) < v(\boldsymbol{f}(\boldsymbol{a})).$$

Then there exists a unique $\boldsymbol{b}\in K^\varrho$ with the following properties

1) $\boldsymbol{f}(\boldsymbol{b}) = 0$
2) $v(\boldsymbol{a}-\boldsymbol{b}) > v(J(a))$.

Proof. We first remark that the assertion of our theorem is true for (K, v) a local field, see Greenberg [Grb]. Therefore, it is true for the algebraic closure of each local field. By the model completeness of the theory of the algebraically closed valued fields, Robinson [Rob], it follows that 8.1 is true for the algebraic closure $(\tilde{K}, \tilde{v})$ of any henselian field (K, v). Now let $\tilde{\boldsymbol{b}}$ be the unique element of $\tilde{K}^\varrho$ satisfying 1) and 2) above. We remark that by property 2) it follows that $v(J(\tilde{\boldsymbol{b}})) = v(J(\boldsymbol{a}))$ and in particular $J(\tilde{\boldsymbol{b}})\neq 0$. Hence $\tilde{\boldsymbol{b}}$ is separable over K, see for instance Lang's Algebra book. Obviously every conjugate of $\tilde{\boldsymbol{b}}$ over K also satisfies 1) and 2). By the uniqueness of $\tilde{\boldsymbol{b}}$ it follows that it is invariant under conjugation. Hence $\tilde{\boldsymbol{b}}$ lies in K^ϱ. □

9. The Algebraic Implicit Function Theorem

Let V be an absolutely irreducible variety defined over K and $a\in V(K)$ a non-singular point. We denote the local ring of a by $\mathcal{O}_{V,a}$ and by $\mathfrak{m}_{V,a}$ the maximal ideal. Note that for *K-rational points $a\in V(K)$* being non-singular is equivalent to the assertion that $\mathcal{O}_{V,a}$ is a regular local ring. The notion of being non-singular is of Zariski local nature and the following assertions on a point $a\in V(K)$ are equivalent, see for instance [M], pp. 233–236:

1) a is a non-singular point of V.
2) Each minimal system of generators of $\mathfrak{m}_a$ consists of exactly $d=\dim V$ elements.
3) Let $U\subset V$ be an affine neighborhood of a defined by $K[U]=K[X_1,\ldots,X_r]/\mathfrak{P}$ with $\mathfrak{P}=(f_1,\ldots,f_s)$ an absolutely irreducible ideal of $K[X_1,\ldots,X_r]$. Then the *Jacobian criterion* holds, i.e., the rank of the matrix $(\partial f_k/\partial X_l(a))$ equals $\varrho=r-\dim V$.

The following fact is well known, see for example [M], p. 240:

9.1 *Let $a\in V(K)$ be a non-singular point of V and $\boldsymbol{t}=(t_1,\ldots,t_d)$ a system of local parameters of $\mathcal{O}_{V,a}$. Then there exists an affine neighborhood U of a which is a complete intersection with respect to $\boldsymbol{t}$, i.e., U is of the form*

$$K[U] = K[T_1,\ldots,T_d, Y_1,\ldots,Y_\varrho]/\mathfrak{P}, \qquad t_k = T_k \bmod \mathfrak{P}\ (1\leqslant k\leqslant d).$$

with $\mathfrak{P}$ generated by exactly ϱ polynomials $\boldsymbol{f}=(f_1,\ldots,f_\varrho)$.

We now prove the following:

Theorem 9.2 (Implicit Function Theorem). *Let (K, v) be a henselian field and V an absolutely irreducible variety defined over K. Let $a\in V(K)$ be a non-singular*

point and $\boldsymbol{t}=(t_1,\ldots,t_d)$ *a system of local parameters at a. Viewing* $\boldsymbol{t}=(t_1,\ldots,t_d)$ *as system of rational functions on V the following assertion holds:*

There exists a v-adic neighborhood of a in $V(K)$ *which is mapped by* $\boldsymbol{t}$ *homeomorphically onto a v-adic neighborhood of the origin in* $\mathbb{A}^d(K)$.

In particular, $V(K)$ *is Zariski dense.*

Proof. We use 9.1 and the notations from there. Over K we identify the affine neighborhood U of a defined at 9.1 with the affine subvariety of $\mathbb{A}^{d+\varrho}$ defined by $\boldsymbol{f}=0$. We write $(\boldsymbol{a}_d, \boldsymbol{a}_\varrho)$ for the current point of $\mathbb{A}^{d+\varrho}$ (with respect to the coordinate functions $(T_1,\ldots,T_d, Y_1,\ldots, Y_\varrho)$ chosen in advance). Making an affine transformation over K (which obviously defines a v-adic homeomorphism of $\mathbb{A}^{d+\varrho}(K)$ onto itself) we can suppose that by this identification a corresponds to the origin of $\mathbb{A}^{d+\varrho}$. Further, after multiplying with properly chosen constants we can suppose that the defining equations $\boldsymbol{f}$ have v-integral coefficients.

Let $J(\boldsymbol{t})$ denote the determinant of the Jacobian matrix $(\partial f_k/\partial Y_l(\boldsymbol{t}))$. Now as $a=(\mathbf{0}_d, \mathbf{0}_\varrho)$ is a non-singular point of U one has $J(\mathbf{0}_d)\neq 0$. Further, as $\boldsymbol{f}(\mathbf{0}_d, \mathbf{0}_\varrho)=0$ it follows by the v-adic continuity of the polynomials that for $\boldsymbol{a}_d$ in a small v-adic neighborhood $\mathcal{U}_0$ of $\mathbf{0}_d$ one has:

$$2v(J(\boldsymbol{a}_d)) = 2v(J(\mathbf{0}_d)) < v(f_k(\boldsymbol{a}_d, \mathbf{0}_\varrho)) \quad (1\leqslant k\leqslant \varrho).$$

By the higher dimensional Hensel Lemma we then have: There exists a unique $\boldsymbol{a}_\varrho$ with the following properties:

$$v(\boldsymbol{a}_\varrho) > v(J(\mathbf{0}_d)) \quad \text{and} \quad \boldsymbol{f}(\boldsymbol{a}_d, \boldsymbol{a}_\varrho)=0.$$

Hence we get: The neighborhood of $a=(\mathbf{0}_d, \mathbf{0}_\varrho)$ in U defined by the conditions $\boldsymbol{a}_d\in\mathcal{U}_0$ and $v(\boldsymbol{a}_\varrho)>v(J(\mathbf{0}_d))$ is mapped homeomorphically by $\boldsymbol{t}$ onto $\mathcal{U}_0$.

Now taking into account that the open immersion $U\subseteq V$ induces a v-adic open immersion $U(K)\subseteq V(K)$ the proof of 9.2 is finished. □

As an application we want to describe the v-adic behaviour of a K-morphism of absolutely irreducible varieties at non-singular points.

First we recall some general facts about smoothness of morphisms. Let V and W be absolutely irreducible varieties over K and $\varphi: V\to W$ a morphism defined over K. Suppose that $\varphi(V)$ is dense in W, i.e., that φ is generically surjective. Let $a\in V(K)$ and $b=\varphi(a)\in W(K)$ be non-singular points. One says that φ is smooth at a if the induced ring homomorphism $\varphi^\#: \mathcal{O}_{W,b}\to\mathcal{O}_{V,a}$ is smooth.

9.3 The following assertions concerning the non-singular points $a\in V(K)$ and $b=\varphi(a)\in W(K)$ are equivalent, see [H], p. 271:

1) φ is smooth at a.
2) The induced canonical mapping $\mathfrak{m}_{W,b}/\mathfrak{m}_{W,b}^2\to\mathfrak{m}_{V,a}/\mathfrak{m}_{V,a}^2$ is injective.

The second condition can be interpreted as follows:

With the above notations φ *is smooth at a if and only if the image* $\varphi^\#\boldsymbol{u}$ *of any system of local parameters* $\boldsymbol{u}$ *at b by* $\varphi^\#$ *can be completed to a system of local parameters of a.*

Further, it is clear from the defintion that any generically surjective morphism $\varphi: V\to W$ is smooth on a Zariski open subset of V.

We now come to the promised description of the K-morphisms at smooth points.

Theorem 9.4 *Let (K, v) be a henselian field, V and W absolutely irreducible varieties defined over K and $\varphi : V \to W$ be a generically surjective morphism defined over K. Suppose that φ is smooth at a K-rational point a of V. Then the following holds:*

1) *There exists a v-adic open neighborhood $\mathfrak{U}_a$ of a in $V(K)$ on which φ is an open map in the v-adic topology.*

2) *If $\dim V = \dim W$ then there exists a v-adic open neighborhood $\mathfrak{U}_a$ of a in $V(K)$ which is mapped homeomorphically onto a v-adic neighborhood $\mathfrak{U}_b$ of $b = \varphi(a)$ in $W(K)$.*

Proof. Let $\varphi^{\#} : \mathcal{O}_{W,b} \to \mathcal{O}_{V,a}$ be the canonical ring homomorphism. Take $\boldsymbol{u}$ an arbitrary system of local parameters of b. By 9.3 the image $\varphi^{\#}(\boldsymbol{u})$ of $\boldsymbol{u}$ by $\varphi^{\#}$ can be completed to a system of local parameters

$$\boldsymbol{t} = (\varphi^{\#}(\boldsymbol{u}), t_1)$$

of a. Let U_a and U_b be affine neighborhoods of a, respectively $b = \varphi(a)$, as at 9.1 such that $\varphi(U_a) \subseteq U_b$ and $\boldsymbol{t}$ is defined on U_a, respectively $\boldsymbol{u}$ is defined on U_b. Now we have a commutative diagram of the form:

$$\begin{array}{ccc} U_a & \xrightarrow{\varphi} & U_b \\ \downarrow{\scriptstyle \phi_t} & & \downarrow{\scriptstyle \phi_u} \\ \mathbb{A}^{\dim V} & \xrightarrow{pr} & \mathbb{A}^{\dim W} \end{array}$$

where ϕ_t is the projection defined by the ring homomorphism $K[\boldsymbol{t}] \hookrightarrow K[U_a]$, ϕ_u is correspondingly defined and pr is the projection obtained from $K[\boldsymbol{u}] \to K[\boldsymbol{t}]$ defined by $\boldsymbol{u} \mapsto \varphi^{\#}(\boldsymbol{u})$. Finally, we remark that by 9.2 ϕ_t and ϕ_u are locally homeomorphisms.

To 1) This is clear, because pr is v-adic open and $\dim V \geqslant \dim W$.

To 2) This is clear, because pr is a v-adic homeomorphism as $\dim V = \dim W$.

The proof of 9.4 is finished. □

Corollary 9.5 *Let K be a henselian field.*

1) *Let $V|K$ be an absolutely irreducible variety and a be a non-singular K-rational point of V. Then any v-adic neighborhood $\mathfrak{U}_a$ of a is Zariski dense in V.*

2) *Let $V|K$ and $W|K$ be absolutely irreducible varieties and $\varphi : V \to W$ a rational morphism defined over K which is generically surjective. Suppose that V has a non-singular K-rational point and $\dim V = \dim W$. Then $V(K)$ and $W(K)$ are Zariski dense in V, respectively W, and on a Zariski open subset of $V(K)$ the map φ is a v-adic local homeomorphism.*

Proof. To 1) Let a be a non-singular point of V and $\boldsymbol{t}$ a system of local parameters of a. Replacing V by an open affine containing a, without loss of generality we can suppose that V is affine and that the projection

$$pr_a : V \to \mathbb{A}^d \quad b \mapsto \boldsymbol{t}(b)$$

is regular at a. Further apply the above theorem.

To 2) By 1) it follows that $V(K)$ and $W(K)$ are Zariski dense. Further the map φ is smooth on a Zariski open subset of V. Therefore, φ is smooth on a Zariski open subset of $V(K)$. On the other hand, by the theorem above φ is a v-adic local homeomorphism at every smooth point. □

References

[B-L-R] Bosch, S.; Lütkebohmert, W.; Raynaud, M.: Néron Models. Mathematische Ergebnisse **21**, Springer Verlag (1990)

[C-R] Cantor, D.; Roquette, P.: On diophantine equations over the ring of all algebraic integers. J. Number Theory **18** (1984) 1–26

[C-K] Chang, C. C.; Keisler, H. J.: Model Theory. Amsterdam-London 1973

[C-S] Cornell, G.; Silverman, J.: Arithmetic Geometry. Springer Verlag 1986

[VdD] Van Den Dries, L.: Elimination theory for the ring of algebraic integers. J. Reine angew. Math. **388** (1988) 189–205

[VdD-McT] Van Den Dries, L.; Macintyre, A.: The logic of Rumely's local-global principle. J. reine angew. Math. **407** (1990) 33–56

[D1] Deuring, M.: Reduktion algebraischer Funktionenkörper nach Primdivisoren des Konstantenkörpers. Math. Z **47** (1942) 643–654

[D2] Deuring, M.: Die Zetafunktion einer algebraischen Kurve vom Geschlecht 1. Nachr. Akad. Wiss. Göttingen Math.-Phys.-Chem. Kl. (1955) 13–42

[E] Eichler, M.: Introduction to algebraic numbers and functions. Academic press, New York and London (1966)

[G-J] Geyer, W.-D.; Jarden, M.: On stable fields in positive characteristic. Geom. Dedic. **29** (1989) 335–376

[G-M-P] Green, B. W.; Matignon, M.; Pop, F.: On the Local Skolem Property. J. reine angew. Math. **458** (1995) 183–199

[G-M-P2] Green, B. W.; Matignon, M.; Pop, F.: On valued function fields II, Regular functions and elements with the uniqueness property. J. reine angew. Math. **412** (1990) 128–149

[Grb] Greenberg, M. J.: Lectures on forms in many variables. Benjamin, New York, 1969

[H] Hartshorne, R.: Algebraic Geometry. Springer, GTM **52**, 1977

[M-B] Moret-Bailly, L.: Groupes de Picard et problèmes de Skolem I, II. Ann. Sci. Ec. Norm. Super. **22** (1989) 161–179, 181–194

[M] Mumford, D.: The Red Book of Varieties and Schemes. Springer Verlag LNM **1358** 1988

[P] Pop, F.: Fields of totally Σ-adic numbers. manuscript 1990

[P2] Pop, F.: On the Galois Theory of function fields of one variable over number fields. J. reine angew. Math. **406** (1990) 200–218

[Pr-S] Prestel, A.; Schmidt, J.: Existentially closed domains with radical relations: An axiomatization of the ring of algebraic integers. J. reine angew. Math. **407** (1990) 178–201

[Rob] Robinson, A.: Complete theories. North Holland (1956)

[R1] Roquette, P.: Zur Theorie der Konstantenreduktion algebraischer Mannigfaltigkeiten. J. reine angew. Math. **200** (1958) 1–44

[R2] Roquette, P.: Solving diophantine equations over the ring of all algebraic integers. Atas de 8ᵉ Escola de Algebra. Vol 2, IMPA 84

[R3] Roquette, P.: Reciprocity in valued function fields. J. reine angew. Math. **375/376** (1987) 238–258

[Ru1] Rumely, R.: Arithmetic over the ring of all angebraic integers. J. reine angew. Math. **368** (1986) 127–133

[Ru2] Rumely, R.: Capacity theory on algebraic curves. Springer L. N. M. **1378** Berlin Heidelberg New-York 1989

[S] Serre, J. P.: Groupes Algébriques et Corps de Classes. Hermann, Paris 1959

Barry Green, Florian Pop, Peter Roquette
Mathematisches Institut, Universität Heidelberg,
D-69120 Heidelberg

(Eingegangen 10. 10. 1994)