The Nullstellensatz over $\mathfrak{p}$-adically closed fields

(23)

By Moshe JARDEN and Peter ROQUETTE

(Received July 25, 1978)

1. Introduction. Statement of principal results.

The Nullstellensatz in its most direct version, is concerned with the polynomial ring $K[x_1, \cdots, x_n]$ over a base field K. For brevity we write $K[x]$ where $x=(x_1, \cdots, x_n)$ denotes an n-tuple of indeterminantes over K. Given finitely many polynomials $f_1(x), \cdots, f_r(x)$ in $K[x]$ we consider their common zeros, i.e. those n-tuples $a=(a_1, \cdots, a_n)\in K^n$ which satisfy

$$f_i(a)=0 \qquad (1\leqq i\leqq r).$$

In contrast to the usual procedure in algebraic geometry we insist that the coordinates a_i are contained in the base field K (and not only in some overfield of K). Accordingly we shall speak more precisely of the *K-rational zeros* of $f_1, \cdots, f_r$. The Nullstellensatz is concerned with the following question: What can be said about those polynomials $g(x)\in K[x]$ which vanish at all K-rational zeros of $f_1, \cdots, f_r$?

If the base field K is algebraically closed then the answer to this question is given by the classical Nullstellensatz of Hilbert: g is contained in the nilradical of the $K[x]$-ideal generated by $f_1, \cdots, f_r$. In other words: some power g^N admits a representation of the form

$$g^N=\lambda_1 f_1+\cdots+\lambda_r f_r$$

with coefficients $\lambda_i\in K[x]$. However, if K is not algebraically closed then the situation is quite different in general. The case of real closed base fields is well known.

In the present paper we propose to study the case of $\mathfrak{p}$-adically closed base fields of finite ramification.[1)]

The notion of $\mathfrak{p}$-adically closed field as defined by Kochen [8] and others, is in complete analogy to the classical and well known notion of real closed field. Its definition and main properties will be discussed in section 4 below. The most important examples of $\mathfrak{p}$-adically closed fields are the ordinary $\mathfrak{p}$-

1) Our results will include those of Kochen [8] and Ziegler [21] as special cases.

adic fields in the sense of Hensel, i.e. those fields which can be represented as completion of some finite algebraic number field with respect to a non-archimedean valuation. In fact our investigation started with the Nullstellensatz over these fields, and it was only at a later stage that we observed our results to be valid over an arbitrary $\mathfrak{p}$-adically closed field of finite ramification. In our proof we have to use general results about the model theory of those fields, namely the model completeness theorem (theorem 4.3). However, in the case of ordinary $\mathfrak{p}$-adic fields in the sense of Hensel it is possible to avoid model theory by using the results of [**15**] which are based on compactness arguments. (See remark 5.3 in section 5.)

In this paper we work over a fixed $\mathfrak{p}$-adically closed base field of finite ramification, and we use the following notation.

K the given field which is $\mathfrak{p}$-adically closed and of finite ramification
$\mathfrak{p}$ the canonical place of K
q the number of elements in the residue field $K\mathfrak{p}$
$\mathfrak{o}$ the ring of integers of K, consisting of those $c\in K$ for which $c(\mathfrak{p})\neq\infty$
v the canonical valuation of K; we have $v(\mathfrak{o})\geqq 0$
π a prime element of K; we have $v(\pi)=1$
γ the $\mathfrak{p}$-adic Kochen operator.

By definition, $\gamma=\gamma(z)$ is a rational function in one variable z, namely:

$$\gamma(z)=\frac{1}{\pi}\cdot\frac{z^q-z}{(z^q-z)^2-1}.$$

In the theory of $\mathfrak{p}$-adic fields, γ plays a similar role as does the square operator in the theory of real fields. In the latter case, we know that squares are always positive. Correspondingly in the $\mathfrak{p}$-adic case, $\gamma(z)$ is always integral, which is to say that $v(\gamma z)\geqq 0$ for arbitrary $z\in K$. This is easily verified by means of the definition of γ. Conversely, if c is an arbitrary integral element in K, i.e. if $v(c)\geqq 0$, then there exists $z\in K$ such that $c=\gamma(z)$; this is an immediate consequence of Hensel's lemma which holds in every $\mathfrak{p}$-adically closed field. Thus we see that

$$\gamma K=\mathfrak{o}.$$

This is the $\mathfrak{p}$-adic analogue of the fact that in a real closed field, the squares are precisely the positive elements. The Kochen operator enters essentially into the statement of the $\mathfrak{p}$-adic Nullstellensatz whose first version can now be formulated. We consider the following situation:

$K[x]$ the polynomial ring in n indeterminates $x=(x_1,\cdots,x_n)$ over the $\mathfrak{p}$-adically closed base field K of finite ramification
f_i, g finitely many polynomials in $K[x]$ $(1\leqq i\leqq r)$.

THEOREM 1.1. *The necessary and sufficient condition for g to vanish at all K-rational zeros of $f_1, \cdots, f_r$ is, that some power g^N admits a representation*

$$g^N=\lambda_1 f_1+\cdots+\lambda_r f_r$$

where the λ_i are rational functions in $F=K(x)$ of the form

$$\lambda_i=\frac{s_i}{1-\pi t_i}$$

with

$$s_i\in K[x, \gamma F], \qquad t_i\in \boldsymbol{Z}[\gamma F].$$

Here γF denotes the set of those elements in F which are of the form $\gamma(z)$ with $z\in F$. As usual, we write $\boldsymbol{Z}[\gamma F]$ to denote the subring of F which is generated by γF over $\boldsymbol{Z}$; similarly $K[x, \gamma F]$ is the ring generated by x and γF over K.

The condition of theorem 1.1 can be written in a somewhat more manageable form after introducing the *Kochen ring* R of the field $F=K(x)$, defined as follows:

$$R=\left\{\frac{t'}{1-\pi t} \text{ with } t, t'\in \boldsymbol{Z}[\gamma F]\right\}.^{2)} \tag{1.1}$$

In other words: R is the ring of quotients of $\boldsymbol{Z}[\gamma F]$, with respect to the multiplicative semigroup of elements$\equiv 1 \bmod \pi$. The ring $R\cdot K[x]$, generated by R and $K[x]$, consists of all quotients $s/1-\pi t$ of the form as specified in theorem 1.1. Thus the condition of that theorem says that

$$\lambda_i\in R\cdot K[x] \qquad (1\leqq i\leqq r).$$

In other words: some power g^N should be contained in the $R\cdot K[x]$-ideal generated by $f_1, \cdots, f_r$; hence g should be in the nilradical of that ideal. In this way we see that the $\mathfrak{p}$-adic Nullstellensatz is of quite similar type as the ordinary Hilbert Nullstellensatz for algebraically closed base field, the only difference being that the polynomial ring $K[x]$ is to be replaced by the larger ring $R\cdot K[x]$. This raises the question as to the birational interpretation of the ring $R\cdot K[x]$, as well as to its ideal theoretic structure. These questions will be discussed in section 2 below. In the rest of this section we continue with the description of our principal result, explaining certain generalizations of theorem 1.1 which are of importance in $\mathfrak{p}$-adic diophantine analysis.

2) This definition applies also to an arbitrary extension field F of K. Thus we should write more precisely $R=R(F)$ in order to indicate the functorial dependence of R on the field F. However, since it will be clear from the context which field F we are referring to, we prefer to write R for brevity.

The first generalization is obtained if we regard the polynomials $f(x) \in K[x]$ as functions not on the whole affine space K^n, but only on some open subset of K^n. We observe that K^n carries a natural topology, canonically defined by the $\mathfrak{p}$-adic valuation v of K. For any point $c=(c_1, \cdots, c_n) \in K^n$ and any $0 \neq \varepsilon \in K$, the ε-neighborhood of c consists of those $a \in K^n$ which satisfy the conditions

$$v(a_i - c_i) \geqq v(\varepsilon) \quad (1 \leqq i \leqq n).$$

These conditions can be interpreted as saying that the polynomials $u_i(x) = \frac{1}{\varepsilon}(x_i - c_i)$ should assume integral values at the point a, i.e. $v(u_i(a)) \geqq 0$. More generally, let us consider an arbitrary finite family $u=(u_1, \cdots, u_m)$ of polynomials $u_j \in K[x]$; the points $a \in K^n$ satisfying the integrality conditions

$$v(u_j(a)) \geqq 0 \quad (1 \leqq j \leqq m) \tag{1.2}$$

form an open and closed subset of K^n. The open-closed subsets of K^n obtained in this way constitute a basis for the $\mathfrak{p}$-adic topology of K^n; therefore these sets will be called "*basic $\mathfrak{p}$-adic sets*" of K^n.

Now let $f_1, \cdots, f_r \in K[x]$. There arises the question: What can be said about those $g \in K[x]$ which vanish at all K-rational zeros of $f_1, \cdots, f_r$ contained in a given basic $\mathfrak{p}$-adic set? The answer will be quite similar to theorem 1.1, the only difference being that the Kochen ring R is to be replaced by the ring

$$R_u = \left\{ \frac{t'}{1-\pi t} \text{ with } t, t' \in \boldsymbol{Z}[u, \gamma F] \right\}. \tag{1.3}$$

Here, $u=(u_1, \cdots, u_m)$ denotes the family of polynomials u_j which define the basic $\mathfrak{p}$-adic set by the integrality conditions (1.2) as explained above. *R_u is called the Kochen ring over u of the field F.* If u is empty, i.e. if $m=0$ then R_u coincides with the ordinary Kochen ring R of F.

A still further generalization is obtained if, in all of the above considerations, the affine space is replaced by some affine variety V defined over K. Accordingly K^n has to be replaced by the space $V(K)$ of K-rational points on V. In this context the symbol $x=(x_1, \cdots, x_n)$ denotes a generic point of V over K and $F=K(x)$ is the algebraic function field of the variety V. As it will turn out, all of the above statements hold in this general case, *provided* that the variety V is nonsingular. Clearly, this nonsingularity assumption is satisfied in the case of theorem 1.1 where V is the full affine space. Thus we see that the following contains theorem 1.1 as a special case.

We consider the following situation:

V an affine variety defined over the $\mathfrak{p}$-adically closed field K of finite ramification

x $=(x_1, \cdots, x_n)$ a generic point of V over K

$K[x]$ its coordinate ring; the elements in $K[x]$ are regarded as polynomial functions defined on V

F $=K(x)$ the field of rational functions on V over K

u $=(u_1, \cdots, u_m)$ a finite family of elements in $K[x]$

R_u the corresponding Kochen ring of F as defined above (1.3)

$V(K)$ the space of K-rational points on V

$V_u(K)$ the basic $\mathfrak{p}$-adic subset of $V(K)$ defined by u; it consists of those points $a \in V(K)$ which satisfy the integrality conditions (1.2) above

f_i, g finitely many elements in $K[x]$ $(1 \leqq i \leqq r)$.

THEOREM 1.2. *Suppose that $V_u(K)$ contains at least one point which is simple on V.*

If g vanishes at all zeros of $f_1, \cdots, f_r$ in $V_u(K)$ then some power g^N admits a representation

$$g^N = \lambda_1 f_1 + \cdots + \lambda_r f_r$$

with

$$\lambda_i \in R_u \cdot K[x] \quad (1 \leqq i \leqq r).$$

Conversely, if this condition is satisfied then g vanishes at all those zeros of $f_1, \cdots, f_r$ in $V_u(K)$ which are simple on V.

Consequently, if the variety V is nonsingular, then the above condition is necessary and sufficient for g to vanish at all common zeros of $f_1, \cdots, f_r$ in $V_u(K)$.

This Nullstellensatz will be complemented by the following criterion for $V_u(K)$ to contain a simple point. It seems remarkable that this criterion is of birational nature, referring only to the function field F and not to the particular variety V.

DEFINITION. The field F is called formally $\mathfrak{p}$-adic over u if π is not a unit in $\boldsymbol{Z}[u, \gamma F]$.

Notice that, in any case, π is contained in $\boldsymbol{Z}[u, \gamma F]$. In fact: we have seen above already that $\mathfrak{o} = \gamma K \subset \gamma F$ and therefore

$$\boldsymbol{Z}[u, \gamma F] = \mathfrak{o}[u, \gamma F].$$

Hence every element in $\mathfrak{o}$, and in particular π, is contained in $\boldsymbol{Z}[u, \gamma F]$. If π is a non-unit in $\boldsymbol{Z}[u, \gamma F]$ then π remains a non-unit in R_u; this is immediate from the above definition of R_u as ring of quotients. We see that F is formally $\mathfrak{p}$-adic over u if and only if

$$\frac{1}{\pi} \notin R_u.$$

If u is empty (i.e. $m=0$) then we obtain the ordinary notion of formally $\mathfrak{p}$-

adic field (see section 4).

The following theorem refers to the situation of theorem 1.2.

THEOREM 1.3. *The necessary and sufficient condition for* $V_u(K)$ *to contain a simple point is that the function field* F *is formally* $\mathfrak{p}$*-adic over* u.

If the variety V is nonsingular then this yields a necessary and sufficient condition for $V_u(K)$ to be nonempty.

2. Holomorphic functions on the Riemann space: the three main theorems.

In this section we shall reformulate the statements of section 1 in birational manner. More precisely, we shall replace the variety V by the Riemann space S of the function field $F|K$ and we shall show that and how theorems 1.2 and 1.3 can be deduced from the corresponding theorems 2.2 and 2.3 for S. Moreover we shall give a birational description of the rings $R_u \cdot K[x]$ which appear in the Nullstellensatz: these rings are holomorphy rings of certain basic subsets of the Riemann space (theorem 2.1). First let us recall some definitions and facts concerning the Riemann space.

As above K denotes a fixed $\mathfrak{p}$-adically closed base field of finite ramification (for definition, see section 4). We consider a finitely generated field extension F of K, i. e. the function field of some affine variety over K. We assume the reader to be familiar with the basic notions and facts about *places*. We consider those places of F which are trivial on K. For any such place P, its residue field FP is an extension field of K. If $FP=K$ then P is called a *K-rational place* of $F|K$. The space of all such K-rational places is called the *Riemann K-space of* $F|K$ and is denoted by $S_K(F|K)$. In order to simplify the notation we shall use the symbol S instead of $S_K(F|K)$, and we shall briefly speak of the "Riemann space". *It should be kept in mind, however, that K-rational places only are involved.* It is possible that S is empty. A necessary and sufficient criterion for $F|K$ to admit a non-empty Riemann space S will be contained in our results below (theorem 2.3).

The image of $z \in F$ with respect to the place P will be denoted by $z(P)$ or briefly zP. If P ranges over S then we obtain a function $z: S \to K \cup \infty$. This function is *continuous* with respect to the $\mathfrak{p}$-adic topologies which are canonically defined on S and on $K \cup \infty$. Let $u=(u_1, \cdots, u_m)$ be a finite family of elements in F, and consider the set S_u of those places $P \in S$ which satisfy the integrality conditions

$$v(u_j P) \geqq 0 \quad (1 \leqq j \leqq m).$$

S_u is $\mathfrak{p}$-adically open and closed in S. The subsets S_u of S obtained in this way form a basis for the $\mathfrak{p}$-adic topology of S; *this fact can be used as a definition for the $\mathfrak{p}$-adic topology*. Every such S_u will be called a *basic $\mathfrak{p}$-adic*

subset of S. If u is empty then $S_u=S$.

There is also the *Zariski topology* on S. Let $x=(x_1, \cdots, x_n)$ be a finite family of elements in F. Consider the set S^x of those places $P\in S$ which satisfy the holomorphy conditions

$$x_iP\neq\infty \quad (1\leqq i\leqq n).$$

S^x is open in the Zariski-topology. The subsets $S^x\subset S$ obtained in this way form a basis for the Zariski topology on S; *this fact can be used as a definition for the Zariski topology.* Every such S^x will be called a *basic Zariski subset* of S. If x is empty then $S^x=S$.

We also consider sets of the form

$$S_u^x=S_u\cap S^x,$$

intersection of a basic $\mathfrak{p}$-adic set with a basic Zariski set. *Any such set will be called a basic subset of* S.

Let $P\in S$. An element $z\in F$ is called *holomorphic* at P if $z(P)\neq\infty$, i.e. if z is contained in the valuation ring $\mathfrak{O}_p$ of F belonging to P. For any subset $T\subset S$, its *holomorphy ring* consists of all those $z\in F$ which are holomorphic at every place $P\in T$. By definition, this holomorphy ring is the intersection of the valuation rings $\mathfrak{O}_p$ belonging to the places $P\in T$. If T is empty then this intersection is to be interpreted as being the whole field F.

Now we are going to state three main theorems about basic subsets of S and their holomorphy rings. These theorems are of central importance in algebraic function theory over $\mathfrak{p}$-adic fields. We shall see that they imply the validity of our results announced in section 1.

Let us repeat the description of the situation.

$F|K$ an algebraic function field over the $\mathfrak{p}$-adically closed base field K of finite ramification

S the Riemann space of K-rational points of $F|K$

x $=(x_1, \cdots, x_n)$ a finite family of elements in F

u $=(u_1, \cdots, u_m)$ ditto

S_u^x the corresponding basic subset of S as defined above

R_u the Kochen ring of F over u, defined by formula (1.3).

THEOREM 2.1. *The holomorphy ring of* S_u^x *coincides with* $R_u\cdot K[x]$. *In other words: a function* $z\in F$ *is holomorphic on* S_u^x *if and only if* z *admits a representation of the form*

$$z=\frac{s}{1-\pi t}$$

with

$$s\in K[x, u, \gamma F] \quad \textit{and} \quad t\in \boldsymbol{Z}[u, \gamma F].$$

This theorem contains an explicit and constructive description of holomorphic functions on basic sets. On the other hand, the theorem can also be regarded as providing a birational interpretation of the rings $R_u \cdot K[x]$, thus "explaining" why these rings appear in the Nullstellensatz of section 1. Perhaps the following special cases are worthwhile mentioning: First, if u is empty then $R_u = R$ is the ordinary Kochen ring; we conclude that $R \cdot K[x]$ is the holomorphy ring of the basic Zariski set S^x. Secondly, if x is empty then we see that $R_u \cdot K$ is the holomorphy ring of the basic $\mathfrak{p}$-adic set S_u. Finally, if both u and x are empty then $R \cdot K$ *appears as the holomorphy ring of the whole Riemann space* S.

THEOREM 2.2. *Suppose* S_u^x *to be non-empty. Let* $f_1, \cdots, f_r, g \in F$ *be holomorphic functions on* S_u^x.

The necessary and sufficient condition for g *to vanish at all common zeros* $P \in S_u^x$ *of* $f_1, \cdots, f_r$, *is that some power* g^N *admits a representation of the form*

$$g^N = \lambda_1 f_1 + \cdots + \lambda_r f_r$$

where the $\lambda_i \in F$ *are holomorphic functions on* S_u^x. *By theorem* 2.1 *this means that*

$$\lambda_i \in R_u \cdot K[x] \quad (1 \leqq i \leqq r).$$

This is the *Nullstellensatz for holomorphy rings*. Notice that this theorem is of birational nature; it does not refer to any variety which generates the function field F. Moreover, the conditions for the coefficients λ_i are the same as the hypothesis for f_i and g, namely they should be holomorphic functions on S_u^x. Therefore theorem 2.2 can be interpreted as a statement about the radical ideal structure of the ring of holomorphic functions on S_u^x as follows. Let us recall the notion of Jacobson ring[3]: this is a ring A (commutative with unity) such that, for every ideal $\mathfrak{a} \subset A$ the Jacobson radical of $\mathfrak{a}$ coincides with the nilradical of $\mathfrak{a}$. In other words: the intersection of maximal A-ideals above $\mathfrak{a}$ coincides with the ideal of those elements of A which are nilpotent modulo $\mathfrak{a}$. This notion of Jacobson ring is generally considered to be adequate in order to describe the ideal theoretic situation in connection with the classical Hilbert Nullstellensatz. Now in our present situation the ring A of holomorphic functions on S_u^x is in general not Jacobson. However in view of theorem 2.2 the Jacobson property holds for every *finitely generated* A-ideal $\mathfrak{a} = A \cdot f_1 + \cdots + A \cdot f_m$. To see this, we observe that every place $P \in S_u^x$ determines a maximal ideal of the holomorphy ring A, namely its *center* on A, consisting of all those functions in A which vanish at P.[4] Therefore, if $g \in A$ is contained in the

3) Some authors use the term "Hilbert ring" [6].

4) The center M of P on A is indeed maximal. This is because its residue field A/M is contained in $FP = K$; on the other hand K is contained in A and hence $K \subset A/M$. It follows $K = A/M$.

Jacobson radical of $\mathfrak{a}=A\cdot f_1+\cdots+A\cdot f_m$ then g vanishes at all common zeros $P\in S_u^x$ of the f_i; hence theorem 2.2 implies that g is nilpotent modulo $\mathfrak{a}$. Let us define a *generalized Jacobson ring* by the property that for every *finitely generated* ideal the Jacobson radical coincides with the nilradical. This is a generalization in the same direction as Bezout rings are generalized principal ideal rings, or Prüfer rings are generalized Dedekind rings. In this generalized sense we thus have the following

COROLLARY TO THEOREM 2.2. *The holomorphy ring of every basic set S_u^x is a generalized Jacobson ring.*

In this statement we did not have to exclude the case when S_u^x is empty. For in that case the holomorphy ring of S_u^x is the whole field F and hence, trivially, a Jacobson ring.

REMARK. In addition to the generalized Jacobson property, the holomorphy rings of basic sets have the *Bezout property*, i. e. every finitely generated ideal is principal (see theorem 3.3).

Theorem 2.2 will be complemented by the following criterion for S_u^x to be non-empty.

THEOREM 2.3. *S_u^x is non-empty if and only if the field F is formally $\mathfrak{p}$-adic over u. In particular, taking $u=x=\emptyset$ we conclude: The Riemann space S of $F|K$ is non-empty if and only if F is formally $\mathfrak{p}$-adic.*

We observe that the condition of theorem 2.3 does not depend on x. Hence if S_u is non-empty then S_u^x is non-empty too, for arbitrary choice of x. Now we recall that S_u is a basic set with respect to the $\mathfrak{p}$-adic topology of S, and $S_u^x=S_u\cap S^x$ is its intersection with the basic set S^x with respect to the Zariski topology. Hence we obtain the following statement as a corollary to theorem 2.3.

DENSITY THEOREM. *Every Zariski-open subset of S is $\mathfrak{p}$-adically dense in S.*

If the base field K is a $\mathfrak{p}$-adic field in the sense of Hensel, hence locally compact, then the density theorem is already contained in our paper [**15**]. The generalization to arbitrary $\mathfrak{p}$-adically closed fields has been given by R. Transier in his thesis [**16**]. However, in this thesis a somewhat different notion of "$\mathfrak{p}$-adically closed field" is used and hence the results of [**16**] cannot be used *verbatim* in the present context; therefore we have chosen to include theorem 2.3 in the present paper. In connection with the density theorem we refer also to the interesting work of Eršov [**5b**].

The reader will notice that we have formulated theorems 1.2 and 1.3 in such a way that they appear entirely similar to theorems 2.2 and 2.3. We are now going to show that the former can be easily deduced from the latter. So let us consider the situation of theorems 1.2 and 1.3; we use the notations as introduced in section 1. In particular $x=(x_1, \cdots, x_n)$ is a generic point over

K of the variety V and $F=K(x)$ is the function field of V. Also, the elements u_j, f_i, g are now supposed to be contained in $K[x]$. We consider the Riemann space S of $F|K$ and its basic subset S^x. If $P\in S^x$ then $x_iP\neq\infty$ $(1\leqq i\leqq n)$. Hence

$$xP=(x_1P, \cdots, x_nP)$$

is a point of K^n. In fact, xP is a specialization of x over K and hence xP is a K-rational point of the variety V. If we assign to every $P\in S^x$ the point $xP\in V(K)$ then we obtain the *projection map:*

$$S^x\to V(K).$$

If $P\in S_u^x$ then P satisfies the integrality conditions $v(u_jP)\geqq 0$ $(1\leqq j\leqq m)$. Considering $u_j=u_j(x)$ as a polynomial expression in $K[x]$ we see that $u_jP=u_j(xP)$. This shows that the projection point $xP\in V(K)$ satisfies the integrality conditions $v(u_j(xP))\geqq 0$ and hence $xP\in V_u(K)$. Conversely, if $xP\in V_u(K)$ then the same arguments show that $P\in S_u^x$. We obtain:

LEMMA 2.4. *A place $P\in S^x$ is contained in S_u^x if and only if its projection xP is contained in $V_u(K)$. In other words: S_u^x is the inverse image of $V_u(K)$ with respect to the projection map $S^x\to V(K)$.*

We also have:

LEMMA 2.5. *The image of S_u^x with respect to the projection map contains at least all simple points of $V_u(K)$.*

In other words: If a is a simple K-rational point of V then there exists a place $P\in S^x$ such that $xP=a$. Equivalently, the specialization $x\to a$ can be extended to a K-rational place P of $F|K$ such that $xP=a$. This is a well known result from algebraic geometry and holds for arbitrary base fields, not necessarily $\mathfrak{p}$-adically closed. For the convenience of the reader we shall include a proof in the appendix of this paper (see corollary A3).

PROOF OF THEOREM 1.2 (using theorem 2.2). By hypothesis of theorem 1.2 there exists a simple point $a\in V_u(K)$. It follows from lemma 2.5 that S_u^x is non-empty. Therefore the hypothesis of theorem 2.2 is satisfied and hence that theorem may be applied.

First we suppose that $g(x)$ vanishes at all common zeros $a\in V_u(K)$ of the $f_i(x)$. This means that the following statement holds for all $a\in V_u(K)$.

$$\left\{\begin{matrix} f_i(a)=0 \\ 1\leqq i\leqq r \end{matrix}\right\} \Rightarrow g(a)=0. \tag{2.1}$$

In particular this holds for those points $a\in V_u(K)$ which are projections of places $P\in S_u^x$. For such points a we have $a=xP$ and hence

$$f_i(a)=f_iP, \qquad g(a)=gP.$$

Using lemma 2.4 we conclude that the following statement holds for all places $P \in S_u^x$.

$$\left\{ \begin{matrix} f_i P = 0 \\ 1 \leqq i \leqq r \end{matrix} \right\} \Rightarrow gP = 0 . \tag{2.2}$$

Applying theorem 2.2 we see that some power g^N admits a representation

$$g^N = \sum_{1 \leqq i \leqq r} \lambda_i f_i \quad \text{with} \quad \lambda_i \in R_u \cdot K[x] . \tag{2.3}$$

Conversely, assume that some power g^N admits a representation of the form (2.3). By theorem 2.2 this implies statement (2.2) to be valid for all $P \in S_u^x$. Hence statement (2.1) holds for all those points $a \in V_u(K)$ which are projections $a = xP$ of some $P \in S_u^x$. In view of lemma 2.5 this includes all simple points $a \in V_u(K)$. Hence (2.1) holds for all simple points $a \in V_u(K)$.

Q. E. D.

PROOF OF THEOREM 1.3 (using theorem 2.3). First, suppose that F is not formally $\mathfrak{p}$-adic over u. By theorem 2.3 it follows that S_u^x is empty. We conclude from lemma 2.5 that there are no simple points in $V_u(K)$.

Conversely, suppose that F is formally $\mathfrak{p}$-adic over u. By theorem 2.3 there exists a place $P \in S_u^x$. We try to choose P in such a way that its projection $a = xP$ is simple; if this is done then it follows that $V_u(K)$ contains at least one simple point. Now, the generic point x is simple on V. Therefore, writing down a system of defining equations for x over K and its Jacobian matrix $J(x)$, we see that $J(x)$ has rank $n-d$ where d denotes the dimension of V. Let us choose one nonvanishing $n-d$ minor of $J(x)$, say $D = D(x)$. Every point $a \in V$ with $D(a) \neq 0$ is simple on V. Thus we have to look for a place $P \in S_u^x$ whose projection $a = xP$ satisfies $D(a) = DP \neq 0$; putting $y = D^{-1}$ this means $yP \neq \infty$, i. e. $P \in S^y$. In other words: P should be contained in $S_u^x \cap S^y = S_u^{(x, y)}$ where $(x, y) = (x_1, \cdots, x_n, y)$. Now theorem 2.3 may be applied to (x, y) showing that $S_u^{(x, y)}$ does indeed contain at least on place P.

Q. E. D.

The proof of theorem 2.1-2.3 will be found in sections 5 and 6. The next two sections 3 and 4 will be of auxiliary nature, containing a review about the relevant notions and facts from the theory of formally $\mathfrak{p}$-adic fields which we are going to use. Section 7 contains the main theorem on integral definite functions, deduced as a consequence of theorem 2.3.

3. Generalities on formally $\mathfrak{p}$-adic fields.

In the general context of this section we consider an arbitrary field K, equipped with a place $\mathfrak{p}$ and corresponding valuation v subject only to the following conditions:

(I) *The residue field* $K\mathfrak{p}$ *is finite, say with* q *elements.*

(II) *The value group* $v(K)$ *admits a smallest positive element, say* $v(\pi)$ *with* $\pi\in K$.

Every element $\pi\in K$ as in (II) is called a $\mathfrak{p}$-*adic prime element of* K. In the following discussion π denotes a fixed such prime element, with the understanding that the results are independent of the choice of π. As usual we identify the ordered group of integers $\boldsymbol{Z}$ with a subgroup of the value group $v(K)$ by putting

$$v(\pi)=1$$

and, consequently, $v(\pi^n)=n$ for every $n\in\boldsymbol{Z}$. After this identification the number 1 is the smallest positive element in $v(K)$ and hence $\boldsymbol{Z}$ is an *isolated* subgroup of $v(K)$, in the sense of ordered groups.

It is conceivable that the theory of formally $\mathfrak{p}$-adic fields admits a setting in a more general framework where condition (I) or (II) or both are not satisfied. However, we shall not discuss this here. We suppose that the base field K satisfies the conditions (I) and (II). Later in the course of discussion we shall add a third condition (III) which says that K should be finitely ramified (section 4).

Consider an extension field F of K and let $\mathfrak{P}$ be a place of F which extends the given place $\mathfrak{p}$ of K. The $\mathfrak{p}$-adic residue field $K\mathfrak{p}$ is contained in the $\mathfrak{P}$-adic residue field $F\mathfrak{P}$ of F, and similarly for the corresponding value groups.

DEFINITION. $\mathfrak{P}$ is called a $\mathfrak{p}$-place if $F\mathfrak{P}=K\mathfrak{p}$ and moreover, if π remains a $\mathfrak{P}$-adic prime element in F.

The second of these conditions may be expressed by saying that $v(\pi)=1$ is the smallest positive element in the $\mathfrak{P}$-adic value group of F. Hence in this sense, $\mathfrak{P}$ is *unramified* over $\mathfrak{p}$.

A criterion for the existence of a $\mathfrak{p}$-place $\mathfrak{P}$ of F is given by the following theorem. This theorem refers to the $\mathfrak{p}$-adic Kochen operator $\gamma(z)$. The definition of $\gamma(z)$ has been given in section 1 already, namely:

$$\gamma(z)=\frac{1}{\pi}\cdot\frac{z^q-z}{(z^q-z)^2-1}\,. \tag{3.1}$$

Let γF denote the set of elements $\gamma(z)$ with $z\in F$ such that $\gamma(z)\neq\infty$, i.e. $z^q-z\neq\pm1$. Let $\mathfrak{o}$ denote the $\mathfrak{p}$-adic valuation ring of K and consider the ring $\mathfrak{o}[\gamma F]$ generated by γF over $\mathfrak{o}$. If

$$\frac{1}{\pi}\notin\mathfrak{o}[\gamma F]$$

then the field F is said to be *formally* $\mathfrak{p}$-*adic*. If this is so then there exists a $\mathfrak{p}$-place $\mathfrak{P}$ of F, and conversely [12]. More generally, let

$$u=(u_1, \cdots, u_m)$$

be a finite family of elements in F. We are interested in those $\mathfrak{p}$-places $\mathfrak{P}$ of F which lie above u. This means that $\mathfrak{P}$ satisfies the integrality conditions

$$v_{\mathfrak{P}}(u_j)\geqq 0 \quad (1\leqq j\leqq m),$$

$v_{\mathfrak{P}}$ denoting the $\mathfrak{P}$-adic valuation of F. In [12] we have studied $\mathfrak{p}$-places which lie above a given subring of F; if we take $\mathfrak{o}[u]$ to be that subring we obtain the following theorem. For the proof see [12] page 191.

THEOREM 3.1. *The necessary and sufficient condition for F to admit a $\mathfrak{p}$-place over u, is that* $\frac{1}{\pi}\notin \mathfrak{o}[u, \gamma F]$.

If the condition $\frac{1}{\pi}\notin \mathfrak{o}[u, \gamma F]$ is satisfied then we say that *the field F is formally $\mathfrak{p}$-adic over u.*[5] Hence theorem 3.1 can be stated in the following form:

If F is formally $\mathfrak{p}$-adic over u then there exists a $\mathfrak{p}$-place of F, and conversely.

An element $f\in F$ is called *totally $\mathfrak{p}$-integral* if

$$v_{\mathfrak{P}}(f)\geqq 0$$

for all $\mathfrak{p}$-places $\mathfrak{P}$ of F. If this holds for all $\mathfrak{p}$-places $\mathfrak{P}$ over u then f is called *totally $\mathfrak{p}$-integral over u*. All these elements f form a subring of F, namely the intersection of the valuation rings $\mathfrak{O}_{\mathfrak{P}}$ belonging to the $\mathfrak{p}$-places $\mathfrak{P}$ of F over u. This subring can be described by means of the *Kochen ring over u* of the field F, denoted by R_u. As explained in section 1 already, R_u is defined to be a ring of quotients of $\mathfrak{o}[u, \gamma F]$, as follows.

$$R_u=\left\{\frac{t'}{1-\pi t} \text{ with } t, t'\in \mathfrak{o}[u, \gamma F]\right\}. \tag{3.2}$$

THEOREM 3.2. *The Kochen ring R_u consists precisely of those $f\in F$ which are totally $\mathfrak{p}$-integral over u. Hence if $\mathfrak{P}$ ranges over all $\mathfrak{p}$-places of F over u then*

$$R_u=\bigcap_{\mathfrak{P}}\mathfrak{O}_{\mathfrak{P}}.$$

For the proof of theorem 3.2 we refer to [12] page 191. Actually the proof in [12] uses the additional assumption that F is formally $\mathfrak{p}$-adic over u. Although this is the main case which we are interested in, it will be necessary below to use theorem 3.2 also in the exceptional case when F is not formally

5) If the base field K is $\mathfrak{p}$-adically closed then $\mathfrak{o}=\gamma K$ (see lemma 4.1). It follows that $\mathfrak{o}[u, \gamma F]=\boldsymbol{Z}[u, \gamma F]$ in this case.

$\mathfrak{p}$-adic over u. In this case there are no $\mathfrak{p}$-places of F over u (theorem 3.1) and the empty intersection in theorem 3.2 is to be interpreted as being the whole field F. Thus if F is not formally $\mathfrak{p}$-adic then the assertion of theorem 3.2 says that

$$R_u=F. \tag{3.3}$$

To see this we observe that π is a unit in the ring $\mathfrak{o}[u, \gamma F]$ since F is not formally $\mathfrak{p}$-adic over u. Hence *every* element $s\in\mathfrak{o}[u, \gamma F]$ is representable in the form $s=1-t$ with $t\in\mathfrak{o}[u, \gamma F]$. In view of the definition (3.2) of R_u we conclude: R_u is the quotient field of $\mathfrak{o}[u, \gamma F]$. That is, we have

$$R_u=K(u, \gamma F).$$

From this we deduce the validity of (3.3) with the help of the following lemma:

$$K(\gamma F)=F. \tag{3.4}$$

This lemma is of purely field theoretic nature and has nothing to do with the theory of formally $\mathfrak{p}$-adic fields. A proof has been given in Merckel's thesis [**11**] page 59. For the convenience of the reader we shall present another proof of Merckel's lemma 3.4 in appendix B below.

Theorem 3.2 shows that the Kochen ring R_u is the intersection of valuation rings all of whose residue fields are finite with the same number of elements. Hence the principal ideal theorem [**13**] may be applied and yields the following

THEOREM 3.3. *The Kochen ring R_u is a Bezout ring with F as its field of quotients. Consequently, every overring of R_u in F is a Bezout ring too.*

We have mentioned this fact already in the foregoing section.—The following theorem gives a characterization of $\mathfrak{p}$-places over u; for its proof we refer to [**12**] page 189.

THEOREM 3.4. *Let $\mathfrak{P}$ be a place of F which extends $\mathfrak{p}$. If $\mathfrak{P}$ lies above the Kochen ring R_u then $\mathfrak{P}$ is a $\mathfrak{p}$-place over u. The converse is also true in view of theorem* 3.2: *if $\mathfrak{P}$ is a $\mathfrak{p}$-place over u then $\mathfrak{P}$ lies above R_u.*

Now let us consider those places P of F which lie above K, i.e. which are trivial on the base field K. For such P the residue field FP is an extension of K. There arises the question as to when the residue field FP is formally $\mathfrak{p}$-adic? More generally consider our given family $u=(u_1, \cdots, u_m)$ of elements in F. Under which condition is FP formally $\mathfrak{p}$-adic over $uP=(u_1P, \cdots, u_mP)$? This question makes sense only if every $u_jP\neq\infty$. Let us agree to the following terminology: if we say "FP is formally $\mathfrak{p}$-adic over uP" then this should include the statement that $u_jP\neq\infty$ $(1\leqq j\leqq m)$.

THEOREM 3.5.a. *If $F|K$ admits a place P whose residue field FP is formally $\mathfrak{p}$-adic over uP, then F is formally $\mathfrak{p}$-adic over u.*

THEOREM 3.5.b. *Now suppose F is formally $\mathfrak{p}$-adic over u and let P be any place of $F|K$. The necessary and sufficient condition for FP to be formally $\mathfrak{p}$-adic over uP is, that P lies above the Kochen ring R_u of F over u. If this is so then the image $R_u \cdot P$ coincides with the Kochen ring FP over uP.*

The last contention can be expressed by the formula

$$R_u(F) \cdot P = R_{uP}(FP)$$

where we have written more precisely $R_u(F)$ to denote the Kochen ring of F over u, and similarly for FP over uP.

PROOF OF THEOREM 3.5.a.

(i) We have to show that π is not a unit in the ring $\mathfrak{o}[u, \gamma F]$. We compare this ring with the corresponding ring in FP. We shall show below in (ii) that

$$(\gamma F) \cdot P = \gamma(FP) \tag{3.5}$$

and hence

$$\mathfrak{o}[u, \gamma F] \cdot P = \mathfrak{o}[uP, \gamma(FP)]\,. \tag{3.6}$$

Now if $\frac{1}{\pi}$ were contained in $\mathfrak{o}[u, \gamma F]$ then from (3.6)

$$\left(\frac{1}{\pi}\right)P = \frac{1}{\pi} \in \mathfrak{o}[uP, \gamma(FP)]$$

contradicting the fact that FP is formally $\mathfrak{p}$-adic over P.

(ii) It remains to prove (3.5). For every $z \in F$ we have

$$\gamma(z) \cdot P = \gamma(zP) \tag{3.7}$$

with the understanding that some of the terms in this formula may have the value ∞; in this case the usual rules apply concerning the calculus with the symbol ∞. On the other hand we recall that the definition of γF *excludes* the value ∞, i. e. γF consists of the elements of the form $\gamma(z)$ with $z \in F$ and $\gamma(z) \neq \infty$. Similarly, in the definitions FP and $\gamma(FP)$ the value ∞ is excluded. Therefore, in order to deduce (3.5) from (3.7) we have to discuss carefully the possible appearance of ∞ in (3.7).

Let $z \in F$ such that $zP \neq \infty$ and $\gamma(zP) \neq \infty$. Then $\gamma(zP)$ is a typical element in $\gamma(FP)$. From (3.7) we conclude that $\gamma(z) \neq \infty$, hence $\gamma(z) \in \gamma F$, and that $\gamma(zP) = \gamma(z) \cdot P \in (\gamma F) \cdot P$. Hence

$$\gamma(FP) \subset (\gamma F) \cdot P\,.$$

More precisely, we have shown that

$$\gamma(FP) = (\gamma X) \cdot P$$

where X denotes the subset of F given by:

$$X=\{z\in F:\ zP\neq\infty,\ \gamma(zP)\neq\infty\}\ .$$

It remains to show that for $z\in F\setminus X$, we still have $\gamma(z)\cdot P\in\gamma(FP)$.

If $zP=\infty$ then $\gamma(zP)=0$ since the denominator of the rational function γ is of larger degree than its numerator. On the other hand $0=\gamma(1)$ by definition of γ. Hence we conclude from (3.7) that $\gamma(z)\cdot P=0=\gamma(1)\in\gamma(FP)$ in this case.

Thus we may assume that $zP\neq\infty$. In this case we claim that $\gamma(zP)\neq\infty$, i.e. that z actually lies in X. Let us put $a=zP$. Suppose $\gamma(a)=\infty$; then $a^q-a=\pm1$. Since FP is formally $\mathfrak{p}$-adic (by hypothesis) there exists a $\mathfrak{p}$-place of FP; let $\bar{a}$ denote the image of a with respect to that $\mathfrak{p}$-place. From $a^q-a=\pm1$ we conclude that $\bar{a}\neq\infty$ and $\bar{a}^q-\bar{a}=\pm1$. But this contradicts the fact that the residue field of the $\mathfrak{p}$-place has q elements and hence $\bar{a}^q-\bar{a}=0$. Hence indeed $\gamma(zP)\neq\infty$ as asserted. Q.E.D.

PROOF OF THEOREM 3.5.b.

(i) First we assume that FP is formally $\mathfrak{p}$-adic over uP; then we know from the above proof that (3.6) holds. We claim that P lies above R_u. Consider a typical element of R_u

$$z=\frac{s}{1-\pi t}$$

where $s,\ t\in\mathfrak{o}[u,\ \gamma F]$. From (3.6) we infer that $sP,\ tP\in\mathfrak{o}[uP,\ \gamma(FP)]$. Moreover, since F is formally $\mathfrak{p}$-adic over uP it follows that $tP\neq\pi^{-1}$ and hence $1-\pi\cdot tP\neq0$. Therefore

$$zP=\frac{sP}{1-\pi\cdot tP}\neq\infty\ . \tag{3.8}$$

This holds for arbitrary $z\in R_u$. In other words: R_u is contained in the valuation ring $\mathfrak{O}_P$, which is to say that P lies above R_u.

Moreover, from (3.6) we see that the right hand side of (3.8) is a typical element of the Kochen ring of FP with respect to uP. Hence that Kochen ring coincides with the image $R_u\cdot P$ of R_u.

(ii) Conversely, we now assume that P lies above R_u. We claim that FP is formally $\mathfrak{p}$-adic over uP. We cannot yet use (3.6) since in the proof of that formula we had assumed FP to be formally $\mathfrak{p}$-adic over uP. However from (3.7) we see that in any case, every element $\gamma(zP)\in\gamma(FP)$ admits an inverse image in γF, namely $\gamma(z)$. Accordingly every element $\bar{t}\in\mathfrak{o}[uP,\ \gamma(FP)]$ admits an inverse image $t\in\mathfrak{o}[u,\ \gamma F]$ such that

$$tP=\bar{t}\ .$$

We have $1-\pi t\neq0$ since otherwise $t=\frac{1}{\pi}\in\mathfrak{o}[u,\ \gamma F]$, contradicting the hypo-

thesis that F is formally $\mathfrak{p}$-adic over u. Moreover $1-\pi t$ is a unit in R_u, by the very definition of the Kochen ring. Since P lies above R_u it follows that $1-\pi t$ is a unit in the valuation ring $\mathfrak{O}_P$. Hence

$$(1-\pi t)\cdot P=1-\pi\bar{t}\neq 0\,.$$

This holds for arbitrary $\bar{t}\in\mathfrak{o}[uP, \gamma(FP)]$. We conclude that $\frac{1}{\pi}\notin\mathfrak{o}[uP, \gamma(FP)]$ i.e. that FP is formally $\mathfrak{p}$-adic over uP. Q.E.D.

Now we consider the *K-rational places* P of $F|K$. By definition we have $FP=K$. Under which condition is K formally $\mathfrak{p}$-adic over uP? According to theorem 3.1 this is the case if and only if there exists a $\mathfrak{p}$-place of K over uP. But the base field K admits only one $\mathfrak{p}$-place, namely $\mathfrak{p}$ itself. Hence the place $\mathfrak{p}$ should lie above uP which means that

$$v(u_jP)\geqq 0 \quad (1\leqq j\leqq m)\,.$$

Therefore we obtain from theorems 3.5 the following

COROLLARY 3.6.a. *If $F|K$ admits a K-rational place P satisfying the integrality conditions*

$$v(u_jP)\geqq 0 \quad (1\leqq j\leqq m)$$

then F is formally $\mathfrak{p}$-adic over u.

COROLLARY 3.6.b. *Now suppose F is formally $\mathfrak{p}$-adic over u and let P be any K-rational place of $F|K$. The necessary and sufficient condition for P to satisfy the above integrality condition is, that P lies above the Kochen ring R_u. If this is so then $R_u\cdot P=\mathfrak{o}$.*

Now let us consider a ring of the form

$$R_u\cdot K[x]$$

where $u=(u_1, \cdots, u_m)$ is as above and $x=(x_1, \cdots, x_n)$ is another family of elements in F. Such rings are of interest in view of our discussion in the foregoing sections. From theorem 3.3 we infer that $R_u\cdot K[x]$ is a Bezout ring; in particular it is integrally closed in F. Therefore $R_u\cdot K[x]$ is the intersection of the valuation rings $\mathfrak{O}_P$ of the places P of F lying above $R_u\cdot K[x]$. These places P can be characterized as follows. First, P has to lie above K which is to say that P has to be a place of F over K. Secondly, P has to lie above R_u which by theorem 3.5.b means that FP has to be formally $\mathfrak{p}$-adic over uP. Thirdly, P has to lie above x. We obtain:

THEOREM 3.7. *Suppose F to be formally $\mathfrak{p}$-adic over u. A place P of $F|K$ lies above $R_u\cdot K[x]$ if and only if P lies above x and the residue field FP is formally $\mathfrak{p}$-adic over uP. If P ranges over all places of $F|K$ with these properties then*

$$R_u \cdot K[x] = \bigcap_P \mathfrak{O}_P .$$

Again, let us specialize this statement considering *K-rational* places only. In view of corollaries 3.6 we obtain:

COROLLARY 3.8. *Suppose F to be formally $\mathfrak{p}$-adic over u. A K-rational place P of $F|K$ lies above $R_u \cdot K[x]$ if and only if it satisfies simultaneously the holomorphy conditions*

$$x_i P \neq \infty \quad (1 \leqq i \leqq n)$$

and the integrality conditions

$$v(u_j P) \geqq 0 \quad (1 \leqq j \leqq m) .$$

If P ranges over all K-rational places with these properties then

$$R_u \cdot K[x] \subset \bigcap_P \mathfrak{O}_P .$$

In general it cannot be expected that the equality sign holds in the last formula. Theorem 2.1 contends that under certain additional hypotheses the equality sign indeed holds. These additional hypotheses are twofold: the first is about the structure of the field extension $F|K$; it is required that F is finitely generated over K. In other words: $F|K$ should be an algebraic function field. The second hypothesis is concerned with the structure of the $\mathfrak{p}$-adic base field K; it is required that K is *$\mathfrak{p}$-adically closed and of finite ramification.* These notions will be explained in the next section.

4. $\mathfrak{p}$-adically closed fields of finite ramification.

We consider the same situation as in the foregoing section 3. That is, K is a field equipped with a place $\mathfrak{p}$ satisfying the conditions (I) and (II) of section 3. F is an extension field of K.

DEFINITION. F is said to be $\mathfrak{p}$-adically closed if F is formally $\mathfrak{p}$-adic, and if there does not exist any proper algebraic formally $\mathfrak{p}$-adic field extension of F.

Some properties of $\mathfrak{p}$-adically closed fields are stated in the following lemma.

LEMMA 4.1. *Suppose F is $\mathfrak{p}$-adically closed. Then:*

(i) *there is one and only one $\mathfrak{p}$-place $\mathfrak{P}$ of F;*

(ii) *F is Henselian with respect to $\mathfrak{P}$;*

(iii) *the $\mathfrak{P}$-adic valuation ring $\mathfrak{O}_{\mathfrak{P}}$ is given by $\mathfrak{O}_{\mathfrak{P}} = \gamma F$;*

(iv) *the $\mathfrak{P}$-adic value group $\Gamma = v_{\mathfrak{P}}(F)$ is a $\boldsymbol{Z}$-group in the sense that the factor group $\Gamma|\boldsymbol{Z}$ is divisible.*

REMARK. It follows from the definition of $\mathfrak{p}$-place that the additive group $\boldsymbol{Z}$ is embedded into the value group Γ as an isolated subgroup, the value of the

prime element π being $1 \in Z$. The divisibility property of Γ/Z is equivalent to saying that for every natural number $n \in N$ the factor group Γ/n is of order n, and that its cosets are uniquely represented by $0, 1, \cdots, n-1$. This last property is usually taken as the definition for Γ to be a Z-group.

PROOF OF LEMMA 4.1.

(i) Since F is formally $\mathfrak{p}$-adic we infer from theorem 3.1 that there exists at least one $\mathfrak{p}$-place of F. For any $\mathfrak{p}$-place $\mathfrak{P}$ of F we are going to prove the validity of statements (ii)-(iv); in particular it follows from (iii) that $\mathfrak{P}$ is uniquely determined (up to equivalence of places).

(ii) Let F', $\mathfrak{P}'$ denote the Henselization of F, $\mathfrak{P}$. Then F' is a certain algebraic and separable field extension of F, and $\mathfrak{P}'$ is a place of F' which extends $\mathfrak{P}$. Moreover $\mathfrak{P}'$ is an *immediate* extension of $\mathfrak{P}$, which is to say that the residue fields and the value groups of $\mathfrak{P}'$ and of $\mathfrak{P}$ coincide. From this we conclude that $\mathfrak{P}'$ is a $\mathfrak{p}$-place too, for the definition of $\mathfrak{p}$-place refers to the residue field and the value group only. Thus we see that the field F' admits a $\mathfrak{p}$-place and hence F' is formally $\mathfrak{p}$-adic (theorem 3.1). We conclude $F'=F$ since F is $\mathfrak{p}$-adically closed.

(iii) If $a \in \mathfrak{O}_{\mathfrak{P}}$ then the equation

$$a=\gamma(z)=\frac{1}{\pi}\cdot\frac{z^q-z}{(z^q-z)^2-1}$$

has a solution $z \in \mathfrak{O}_{\mathfrak{P}}$; this is immediate from Hensel's lemma. Hence $\mathfrak{O}_{\mathfrak{P}} \subset \gamma F$. On the other hand theorem 3.2 implies that $\gamma F \subset \mathfrak{O}_{\mathfrak{P}}$. It follows $\gamma F=\mathfrak{O}_{\mathfrak{P}}$.[6]

(iv) If Γ/Z were not divisible then there would exist an element $\alpha \in \Gamma$ and a prime number n such that α is not n-divisible in Γ modulo Z. In this situation we can construct a formally $\mathfrak{p}$-adic field extension $F' \supset F$ of degree n, contradicting the fact that F is $\mathfrak{p}$-adically closed. The construction of F' is as follows:

Let $a \in F$ be such that $v_{\mathfrak{P}}(a)=\alpha$ and let b be an n-th root of a. Let us put $F'=F(b)$. Then $[F' : F] \leqq n$. Let $\mathfrak{P}'$ be a place of F' which extends $\mathfrak{P}$, and put $\beta=v_{\mathfrak{P}'}(b)$. Then β is contained in the value group $\Gamma'=v_{\mathfrak{P}'}(F')$. From $b^n=a$ it follows $n\beta=\alpha$. Since α is not n-divisible in Γ and n is a prime number we conclude that β is of order n modulo Γ. Hence

$$[\Gamma' : \Gamma] \geqq n \geqq [F' : F]. \tag{4.1}$$

On the other hand it is known from general valuation theory that the index of value groups is not larger than the field degree. We conclude

6) For later use we observe from this proof that the equation $\mathfrak{O}_{\mathfrak{P}}=\gamma F$ holds whenever F is Henselian with respect to $\mathfrak{P}$.

(4.2) $$[\Gamma' : \Gamma]=n=[F' : F].$$

Moreover it follows that $\mathfrak{P}'$ is the only extension of $\mathfrak{P}$ to F' and that the residue field of $\mathfrak{P}'$ coincides with the residue field of $\mathfrak{P}$. We claim that $\mathfrak{P}'$ is a $\mathfrak{p}$-place; for this it remains to show that 1 is the smallest positive element in the $\mathfrak{P}'$-adic value group Γ'. Suppose that there exists $\xi\in\Gamma'$ such that $0<\xi<1$; then $0<n\xi<n$. From (4.2) it follows that $n\xi\in\Gamma$. Since Z is isolated in Γ we conclude that $n\xi=m\in Z$. On the other hand, since β is of order n modulo Γ it follows from (4.2) that β generates Γ' modulo Γ; hence ξ is represented in the form $\xi=k\beta+\omega$ with $\omega\in\Gamma$ and $k\in Z$, $0<k<n$. (We have $k\neq 0$ since $\xi\notin\Gamma$.) It follows $n\xi=m=k\alpha+n\omega$. From this we see that $k\alpha$ and hence α is n-divisible in Γ modulo Z, contrary to the choice of α. (Observe that n is a prime number, hence k is relatively prime to n because $0<k<n$.)

We have seen that $\mathfrak{P}'$ is a $\mathfrak{p}$-place of F'. From theorem 3.1 we conclude that F' is formally $\mathfrak{p}$-adic, as contended. Q. E. D.

Now assume F to be formally $\mathfrak{p}$-adic (not necessarily closed). Among the algebraic extension fields F' of F which are formally $\mathfrak{p}$-adic there exists a maximal one by Zorn's lemma; this is called the $\mathfrak{p}$-*adic closure* of F. In general it is not unique. If $\mathfrak{P}$ is a given $\mathfrak{p}$-place of F then there exists a $\mathfrak{p}$-adic closure F' whose canonical $\mathfrak{p}$-place $\mathfrak{P}'$ extends $\mathfrak{P}$. To show this we may replace F, $\mathfrak{P}$ by its Henselization, in other words: we may assume that F, $\mathfrak{P}$ is Henselian. But then we have $\mathfrak{O}_{\mathfrak{P}}=\gamma F$ and hence $\mathfrak{P}$ is the only $\mathfrak{p}$-place of F (see footnote 6)). If F' is an arbitrary $\mathfrak{p}$-adic closure of F then its $\mathfrak{p}$-place $\mathfrak{P}'$ induces a $\mathfrak{p}$-place in F which, by the above uniqueness property, must coincide with $\mathfrak{P}$. Hence $\mathfrak{P}'$ extends $\mathfrak{P}$. We have shown:

LEMMA 4.2. *Let $\mathfrak{P}$ be a $\mathfrak{p}$-place of F. Then there exists a $\mathfrak{p}$-adic closure F' of F whose canonical place $\mathfrak{P}'$ is an extension of $\mathfrak{P}$.*

Now we come to the description of the main theorem which governs the theory of $\mathfrak{p}$-adically closed fields. As to our present knowledge, this theorem is restricted to the case of *finitely ramified* fields. This means that K should satisfy condition (III) below, in addition to conditions (I) and (II) as stated in section 3 already. For convenience let us repeat conditions (I) and (II) so that all three conditions are now listed together.

(I) *The residue field $K\mathfrak{p}$ is finite, say with q elements.*

(II) *The value group $v(K)$ admits a smallest positive element, say $v(\pi)$ with $\pi\in K$.*

(III) *The value $v(p)$ of the residue characteristic p is a multiple of $v(\pi)$, say $v(p)=e\cdot v(\pi)$ with $e\in N$.*

The integer e as in (III) is called the *ramification degree of the field K*. After the identification $v(\pi)=1$ (as explained in section 3) we have

$$v(p)=e\,.$$

Condition (III) implies that K is of characteristic zero. For otherwise $p=0$ in K and hence $v(p)=+\infty$, contradicting (III).

From now on we suppose that K is finitely ramified in the above sense. We observe that any formally $\mathfrak{p}$-adic field extension F of K is again finitely ramified, with respect to each $\mathfrak{p}$-place $\mathfrak{P}$ of F. This is evident because the condition (III) concerns the residue characteristic p and a prime element π of K only; both p and π keep their meaning in F with respect to $\mathfrak{P}$. Hence (III) implies

$$v_{\mathfrak{P}}(p)=e\cdot v_{\mathfrak{P}}(\pi)=e$$

showing that $F, \mathfrak{P}$ is indeed finitely ramified. Moreover, we see that the $\mathfrak{P}$-adic ramification degree of F coincides with the $\mathfrak{p}$-adic ramification degree e of the base field K. Now the main theorem reads as follows:

THEOREM 4.3. *Let F', F'' be two $\mathfrak{p}$-adically closed extension fields of K. If $F'\subset F''$ then F'' is an elementary extension of F'.*

This means that if Σ is any sentence about F' as a valued field then Σ holds in F' if and only if Σ holds in F''. It is assumed that Σ is expressed in a formal language of lower predicate calculus; its vocabulary consists of the relations belonging to the theory of valued fields, and of names for the individual elements of F'.

The above theorem is called the *model-completeness theorem* because is expresses the fact that the theory of $\mathfrak{p}$-adically closed fields (of given residue degree q and ramification degree e) is model-complete. In case of unramified fields ($e=1$) the model completeness theorem was proved by Ax and Kochen and, independently, by Eršov. For a proof in the general case we refer to Eršov [**5a**] or Ziegler [**20**] or Weispfenning [**17**] or Basarab [**3**].

We shall apply theorem 4.3 in the following version which evidently is equivalent to the theorem itself.

COROLLARY 4.4. *Suppose that the base field K is $\mathfrak{p}$-adically closed. Then every $\mathfrak{p}$-adically closed field $F'\supset K$ is an elementary extension of K, in the sense of valued fields.*

REMARK 4.5. The most prominent example of $\mathfrak{p}$-adically closed fields are those which are *locally compact* with respect to the given valuation. Locally compact fields of characteristic zero are finitely ramified; they can be characterized as the completions of finite algebraic number fields with respect to a nonarchimedean valuation.

5. Existence theorems for rational places.

We are now returning to the situation of section 2. In preparation of our proof of the three main theorems 2.1-2.3 we are going to prove two existence theorems for rational places (theorems 5.1 and 5.4). We consider the following situation.

K $\mathfrak{p}$-adically closed field of finite ramification
v the canonical valuation of K
$F|K$ an algebraic function field, i.e. a finitely generated field extension
x $=(x_1, \cdots, x_n)$ a finite family of elements in F
u $=(u_1, \cdots, u_m)$ ditto.

THEOREM 5.1. *Suppose F to be formally $\mathfrak{p}$-adic over u. Then there exists a K-rational place P of $F|K$ satisfying simultaneously the holomorphy conditions*

$$x_iP \neq \infty \quad (1 \leqq i \leqq n)$$

and the integrality conditions

$$v(u_jP) \geqq 0 \quad (1 \leqq j \leqq m).$$

Hence S_u^x is non-empty.

Here S_u^x denotes the basic subset of the Riemann space S of $F|K$ determined by the above holomorphy and integrality conditions; this notation has been introduced in section 2.

PROOF.

(i) Let x' be a finite family of elements in F containing x. If the theorem is true for x' and u then clearly, it is also true for x and u. Hence in order to prove the theorem we may replace x by x' if convenient. In other words: we may enlarge x by adding finitely many more elements of F. After suitable such enlargement we may assume, firstly, that x generates the field F over K:

$$F=K(x).$$

Let V denote the irreducible variety over K whose generic point is $x=(x_1, \cdots, x_n)$. Thus V is an affine variety in n-space and F is the function field of F. Secondly, we may assume that every u_j appears among the x_i. After suitable renumbering of the x_i we may then assume that $u=(u_1, \cdots, u_m)$ consists of the first m coordinates of x. Thus we have $m \leqq n$ and

$$u_j=x_j \quad (1 \leqq j \leqq m).$$

(ii) By hypothesis of the theorem F is formally $\mathfrak{p}$-adic over u. Hence there exists a $\mathfrak{p}$-place $\mathfrak{P}$ of F over u (theorem 3.1). Let F' be a $\mathfrak{p}$-adic closure of F whose canonical $\mathfrak{p}$-place $\mathfrak{P}'$ lies above $\mathfrak{P}$ (lemma 4.2). Then $\mathfrak{P}'$ lies above

u, which is to say that $v'(u_j)\geqq 0$ $(1\leqq j\leqq m)$. Here v' denotes the $\mathfrak{P}'$-adic valuation of F'. Since $u_j=x_j$ we may write this in the form

$$v'(x_j)\geqq 0 \quad (1\leqq j\leqq m).$$

In other words: the first m coordinates of the point $x\in V$ are $\mathfrak{P}'$-adically integral in F'. Observe that x is a simple point of V since x is generic in V over K. Hence we see that the following statement holds over the $\mathfrak{p}$-adically closed field F':

(Σ') *There exists an F'-rational simple point in V whose first m coordinates are integral.*

We envisage V as being defined by a finite system of polynomial equations over K. The condition for a point to be simple on V can be expressed by saying that at least one of the proper minors of the Jacobian matrix does not vanish. Hence we see that the above statement can be expressed in formal language of lower predicate calculus, the vocabulary of that language belonging to the theory of valued fields and containing constants for the individual elements of K.

(iii) At this point we use the model completeness theorem 4.4. Consequently, since the above statement holds over some $\mathfrak{p}$-adically closed field F' it also holds over the $\mathfrak{p}$-adically closed base field K. We conclude:

(Σ) *There exists a K-rational simple point in V whose first m coordinates are integral.*

Let $a=(a_1, \cdots, a_n)\in V(K)$ be such point. Then a is a specialization of x over K. Since a is simple on V it follows that the specialization $x\to a$ can be extended to a K-rational place P of F (see appendix, lemma A3). We now have $a=xP$. In particular,

$$x_iP=a_i\neq\infty \quad (1\leqq i\leqq n)$$

which means that P satisfies the holomorphy conditions of the theorem. Considering the first m coordinates we have $u_jP=x_jP=a_j$ $(1\leqq j\leqq m)$. By construction, the first m coordinates $a_1, \cdots, a_m$ are integral in K. Hence

$$v(u_jP)=v(a_j)\geqq 0 \quad (1\leqq j\leqq m)$$

showing that P satisfies the integrality conditions too. Q. E. D.

REMARK 5.2. The above proof is the only instance in this paper where the model completeness theorem is used. All other arguments are independent of general model theory.

REMARK 5.3. If the base field K is *locally compact* and of characteristic zero then a different proof of theorem 5.1 has been given in [**15**] theorem 1.4.

That proof is based on compactness arguments and does not use the model completeness theorem. In view of remark 5.2 we see that the present paper does also yield a "classical" proof of the Nullstellensatz, without using model theory, in the case of locally compact base fields of characteristic zero.

Now we turn to the second existence theorem. This will be a direct generalization of the first existence theorem 5.1, and both theorems could have been proved simultaneously. The reason why we have preferred to separate these two theorems is given in remark 5.2; we wanted to localize that part of our proof where the model completeness theorem is used. The proof of theorem 5.4 will be a straightforward deduction from theorem 5.1, without resorting once more to arguments from general model theory.

THEOREM 5.4. *In the same situation as in theorem* 5.1, *suppose again that* F *is formally* $\mathfrak{p}$*-adic over* u. *Given any element* $y \in R_u \cdot K[x]$ *which is not a unit in* $R_u \cdot K[x]$ *there exists a* K*-rational place* $P \in S_u^x$ *such that*

$$yP = 0 .$$

In other words: y *admits at least one zero in* S_u^x.

PROOF.

(i) Since y is not a unit there exists a maximal ideal $M \subset R_u \cdot K[x]$ containing y. Applying the general existence theorem for places we conclude that there exists a place Q of F lying above $R_u \cdot K[x]$ which is centered at M. This means that every element in M vanishes at Q. In particular

$$yQ = 0 .$$

By construction Q lies above K and hence the residue field FQ contains an isomorphic copy of K. After identifying K naturally with its isomorphic copy we may assume that $K \subset FQ$. Moreover Q does now appear as a place over K.

Since Q lies above R_u it follows from theorem 3.5.b that its residue field FQ is formally $\mathfrak{p}$-adic over uQ. Moreover we know that Q lies above x which implies that $xQ = (x_1Q, \cdots, x_nQ)$ is a finite family of elements in FQ.

(ii) If the residue field FQ is finitely generated over K then we may apply theorem 5.1 to FQ and the families of elements xQ, uQ in FQ. It follows that there exists a K-rational place $\bar{P}$ of $FQ|K$ satisfying the holomorphy and integrality conditions

$$x_iQ \cdot \bar{P} \neq \infty , \qquad v(u_jQ \cdot \bar{P}) \geqq 0 .$$

Consider the composite place

$$P = Q \circ \bar{P} .$$

This is a K-rational place of $F|K$ satisfying the holomorphy and integrality conditions

$$x_iP\neq\infty\,,\qquad v(u_jP)\geqq 0\,.$$

Moreover we have

$$yP=yQ\cdot\bar{P}=0\,.$$

Hence P solves the conditions of the theorem.

(iii) If $FQ|K$ is not finitely generated we try to replace the above place Q by some other place Q' of $F|K$ whose residue field is finitely generated; in addition Q' should satisfy the same conditions as Q. More precisely, we require that

$$uQ'=uQ\,,\qquad xQ'=xQ\,,\qquad yQ'=yQ \tag{5.1}$$

and

$$FQ'\subset FQ\,. \tag{5.2}$$

Recall that FQ is formally $\mathfrak{p}$-adic over uQ; this property is inherited by every subfield of FQ which contains K and uQ. Therefore we conclude from (5.1) and (5.2) that FQ' is formally $\mathfrak{p}$-adic over uQ'; this is equivalent to saying that Q' lies above R_u (theorem 3.5.b). Moreover, it follows from (5.1) that Q' lies above x; we conclude that Q' lies above $R_u\cdot K[x]$. Finally, the last relation in (5.1) shows that $yQ'=0$.

Thus we have reduced our problem to the existence of a place Q' of $F|K$ satisfying (5.1) and (5.2) and such that FQ' is finitely generated over K. If such Q' has been found then the arguments of part (ii) may be applied to Q' instead of Q, yielding a K-rational place of $F|K$ with the required properties. Now the existence of Q' is guaranteed by the following lemma which is well known from algebraic geometry.

LEMMA 5.5. *Let $F|K$ be an arbitrary algebraic function field of characteristic zero. Let $x=(x_1,\cdots,x_n)$ be a finite family of elements in F and suppose there exists a place Q of $F|K$ such that $x_iQ\neq\infty$ $(1\leqq i\leqq n)$. Then there exists a place Q' of $F|K$ such that*

$$xQ'=xQ$$

and

$$FQ'\subset FQ$$

and moreover, FQ' is finitely generated over K.

Notice that in the statement of this lemma we have slightly changed notation: instead of writing (u, x, y) as in condition (5.1) we have written x in lemma 5.5 in order to simplify the notation.

PROOF OF LEMMA 5.5. Let x' be a finite family of elements in the valuation ring $\mathfrak{O}_Q$ such that x' contains x. If the lemma holds for x' then clearly, it also holds for x. Hence we may replace x by x' if convenient. In other

words: In order to prove lemma 5.5 we may enlarge x by adding finitely many elements of $\mathfrak{O}_Q$. After suitable such enlargement we may assume, firstly that x generates the function field $F|K$, i. e.

$$F=K(x).$$

Let V denote the irreducible variety over K whose generic point is $x=(x_1, \cdots, x_n)$. Thus V is an affine variety in n-space and F is the function field of V. The place Q is centered on V at the point $xQ=(x_1Q, \cdots, x_nQ)$. Secondly, after further suitable enlargement of x we may assume that xQ is a *simple point* of V. This is the content of Zariski's local uniformization theorem which holds over an arbitrary base field of characteristic zero [**19**].

Let us put $a=xQ$. Since a is a simple point on V, the specialization $x\to a$ can be extended to a place Q' of $F|K$ such that

$$FQ'=K(a)$$

(see appendix, lemma A2). This shows that FQ' is finitely generated over K. Moreover we have by construction

$$xQ'=a=xQ. \qquad \text{Q. E. D.}$$

6. Proof of the three main theorems.

We consider the situation of theorems 2.1-2.3 and we use the notation as introduced there.

PROOF OF THEOREM 2.1. We have proved already in corollary 3.8 that

$$R_u\cdot K[x]\subset\bigcap_P \mathfrak{O}_P \tag{6.1}$$

where P ranges over the places in S_u^x. Hence every $z\in R_u\cdot K[x]$ is holomorphic on S_u^x. We have to show that the equality sign holds in (6.1). Let us first deal with the (trivial) case that F is not formally $\mathfrak{p}$-adic over u. In this case we know from (3.3) that $R_u=F$. Hence *a fortiori* $R_u\cdot K[x]=F$ and the equality sign in (6.1) holds trivially.

Now suppose that F is formally $\mathfrak{p}$-adic over u. Let $z\notin R_u\cdot K[x]$, $z\in F$. We have to show that z is not holomorphic on S_u^x. This means that there should exist a place $P\in S_u^x$ such that $z(P)=\infty$. We observe that $R_u\cdot K[x]$ is a Bezout ring with F as its field of quotients (theorem 3.3). Therefore the fractional $R_u\cdot K[x]$-ideal generated by z and 1 is principal. Let t be a generator. Since 1 is a multiple of t we have

$$t=\frac{1}{y} \quad \text{with } y\in R_u\cdot K[x].$$

On the other hand z is a multiple of t; since $z \notin R_u \cdot K[x]$ it follows that y is not a unit in $R_u \cdot K[x]$. Applying theorem 5.4 we obtain a place $P \in S_u^x$ such that $y(P)=0$, hence

$$t(P)=\infty .$$

By definition of t there is a relation of the form

$$t=\lambda z+\mu \quad \text{with } \lambda,\ \mu \in R_u \cdot K[x] .$$

We have seen in (6.1) that λ, μ are holomorphic at P. Hence from $t(P)=\infty$ we conclude $z(P)=\infty$. Q. E. D.

PROOF OF THEOREM 2.2.

(i) For brevity let us write A for the holomorphy ring of S_u^x. According to theorem 2.1, $A=R_u \cdot K[x]$. We know that A is a Bezout ring (theorem 3.3). Hence the A-ideal generated by $f_1, \cdots, f_r$ is principal. Let f be a generator. The zeros $P \in S_u^x$ of f are precisely the common zeros of $f_1, \cdots, f_r$. Therefore, in order to prove theorem 2.2 we may replace $f_1, \cdots, f_r$ by f. (In other words: it suffices to prove theorem 2.2 in the case $r=1$.) We may assume that $g \neq 0$ because otherwise theorem 2.2 is trivial.

(ii) First we suppose that g vanishes at every zero of f in S_u^x; we have to show that some power g^N is contained in the ideal $A \cdot f$. Let us put

$$y=\frac{1}{g}$$

and consider the basic set

$$S_u^x \cap S^y = S_u^{(x,\,y)} .$$

If $P \in S_u^{(x,\,y)}$ then $y(P) \neq \infty$ and hence $g(P) \neq 0$; we conclude that P cannot be a zero of f. Therefore f has no zero in $S_u^{(x,\,y)}$ which implies that $\frac{1}{f}$ is holomorphic on this set. Applying theorem 2.1 to the basic set $S_u^{(x,\,y)}$ we conclude that

$$\frac{1}{f} \in R_u \cdot K[x,\ y]=A[y]=A\left[\frac{1}{g}\right] .$$

Hence $\frac{1}{f}$ admits a representation as a polynomial in the form

$$\frac{1}{f}=\lambda_0+\lambda_1 \cdot \frac{1}{g}+ \cdots +\lambda_N \cdot \left(\frac{1}{g}\right)^N$$

with coefficients $\lambda_i \in A$. The number N denotes the degree of the polynomial on the right hand side. Multiplying the above relation by g^N and by f we obtain

$$g^N=\lambda f$$

where

$$\lambda=\lambda_0\cdot g^N+\lambda_1\cdot g^{N-1}+\cdots+\lambda_N\,.$$

We see that $\lambda\in A$ and hence $g^N\in A\cdot f$.

(iii) The converse is trivial: if some power g^N is contained in $A\cdot f$ then clearly $f(P)=0$ implies $g(P)=0$, for every $P\in S_u^x$. Q. E. D.

PROOF OF THEOREM 2.3.

(i) If F is formally $\mathfrak{p}$-adic over u then we have proved in theorem 5.1 already that S_u^x is non-empty.

(ii) Conversely, assume that S_u^x contains a place P. By definition, P is a K-rational place satisfying the integrality conditions

$$v(u_jP)\geqq 0\quad(1\leqq j\leqq m)\,.$$

Now corollary 3.6.a shows that F is formally $\mathfrak{p}$-adic over u. Q. E. D.

7. On integral definite functions.

The study of integral definite functions is of importance for various problems in $\mathfrak{p}$-adic diophantine geometry. The following results have been included in this paper because their proof is an immediate consequence of the main theorems in section 2. In the case of locally compact base fields, theorem 7.2 has been obtained in [**15**] already using compactness arguments. It seems noteworthy that these results remain valid over an arbitrary $\mathfrak{p}$-adically closed base field of finite ramification.

We consider the same situation as in theorems 2.1–2.3 and we use the same notation. In particular,

$$S_u^x=S_u\cap S^x$$

denotes the basic subset of the Riemann space S of $F|K$, defined by the integrality conditions

$$v(u_jP)\geqq 0\quad(1\leqq j\leqq m)$$

and holomorphy conditions

$$x_iP\neq\infty\quad(1\leqq i\leqq n)\,.$$

DEFINITION. An element $z\in F$ is said to be integral definite on S_u^x if $v(zP)\geqq 0$ for every place $P\in S_u^x$. That is, the values $z(P)$ for $P\in S_u^x$ should be $\mathfrak{p}$-adic integers.

Let $z\in F$ be integral definite on S_u^x. Consider the function

$$z\colon S\to K\cup\infty$$

which is given by $P \mapsto z(P)$. Let $T \subset S$ denote the inverse image of $\mathfrak{o}$. In other words: T is the largest subset of S on which z is integral definite. Since $\mathfrak{o}$ is closed in $K \cup \infty$ and the function z is continuous it follows that T is closed in S. Here we refer to the $\mathfrak{p}$-adic topology on S. We conclude that T contains the $\mathfrak{p}$-adic closure of S_u^x. Now we know that S_u^x is dense in S_u (density theorem, section 2). Hence the $\mathfrak{p}$-adic closure of S_u^x contains S_u, and in fact it coincides with S_u since S_u is closed by definition. We have shown that $S_u \subset T$ which is to say that z is integral definite on S_u. Thus we have proved the following

LEMMA 7.1. *If an element $z \in F$ is integral definite on S_u^x then z is integral definite on S_u already.*

We are now going to characterize the integral definite functions on S_u. If S_u is empty then every element $z \in F$ is integral definite on S_u. In the following let us suppose that S_u is non-empty, which is equivalent to saying that F is formally $\mathfrak{p}$-adic over u (theorem 2.3).

THEOREM 7.2. *Suppose F to be formally $\mathfrak{p}$-adic over u. Then the Kochen ring R_u coincides with the ring of integral definite functions on S_u In other words: an element $z \in F$ is integral definite on S_u if and only if z admits a representation of the form*

$$z = \frac{s}{1 - \pi s}$$

with $s, t \in \boldsymbol{Z}[u, \gamma F]$.

PROOF.

(i) If $z \in R_u$ then $z(P) \in \mathfrak{o}$ according to corollary 3.6.b.

(ii) Now suppose that $z \notin R_u$. We have to show that there exists $P \in S_u$ such that $z(P) \notin \mathfrak{o}$. By theorem 3.2 there exists a $\mathfrak{p}$-place $\mathfrak{P}$ of F over u such that $z \notin \mathfrak{O}_{\mathfrak{P}}$ which is to say that

$$v_{\mathfrak{P}}(z) < 0,$$

$v_{\mathfrak{P}}$ denoting the $\mathfrak{P}$-adic valuation of F. It follows

$$v_{\mathfrak{P}}\left(\frac{1}{z}\right) > 0$$

hence

$$v_{\mathfrak{P}}\left(\frac{1}{z}\right) \geqq 1 = v(\pi)$$

because of the defining properties of $\mathfrak{p}$-places. For brevity let us put $w = \dfrac{1}{\pi z}$; then

$$v_{\mathfrak{P}}(w) \geqq 0.$$

That is, $\mathfrak{P}$ lies above w. By construction $\mathfrak{P}$ lies also above u. Hence $\mathfrak{P}$ lies above (u, w). We conclude that F is formally $\mathfrak{p}$-adic over (u, w) (theorem 3.1). Therefore the basic $\mathfrak{p}$-adic set $S_{(u,w)} \subset S$ is non-empty (theorem 2.3). In other words: there exists a K-rational place P of $F|K$ which satisfies the integrality conditions

$$v(u_j P) \geqq 0 \quad (1 \leqq j \leqq m)$$

$$v(wP) \geqq 0 .$$

The first m of these conditions say that $P \in S_u$. As to the last condition, we have

$$wP = \frac{1}{\pi \cdot zP}$$

and hence that condition implies

$$v(zP) \leqq -1 < 0 .$$

Q. E. D.

Appendix A: Simple points and rational places.

The following results are known from algebraic geometry [1]. They have been included here for the convenience of the reader. First we consider the following general situation.

R a local integral domain[7]

M its maximal ideal

$\bar{R}$ $= R/M$ its residue class field

F the quotient field of R.

LEMMA A1. *Suppose that R is regular in the sense of local rings. Then there exists a place P of F dominating R such that $\bar{R} = FP$.*

As usual, we say that a place P dominates R if P lies above R and if, moreover, M is the center of P on R. If this is the case then the residue field $\bar{R}$ is naturally contained in FP:

$$\bar{R} \subset FP .$$

Lemma A1 says that with suitable choice of P the equality sign holds.

PROOF.[8] For $0 \neq z \in R$ the R-degree $d_R(z)$ is defined to be the largest integer exponent d such that $z \in M^d$. Since the local ring R is regular, its degree function $d_R(z)$ yields a valuation of R and hence of its quotient field F. By

7) It should be noted that in this appendix the symbol R does *not* denote the Kochen ring.

8) For the general theory of regular local rings, see e.g. Zariski-Samuel, Commutative Algebra, vol. II.

definition, this valuation dominates R. Hence if $\bar{F}$ denotes the residue field of F with respect to the degree valuation then

$$\bar{R}\subset\bar{F}.$$

The corresponding place $F\to\bar{F}$ will be denoted by a bar; if $z\in F$ then $\bar{z}\in\bar{F}\cup\infty$. If $z\in R$ then $\bar{z}$ coincides with the residue class of z modulo M.

Let $t_1, \cdots, t_n$ be a minimal system of generators of the ideal M. Then $n=\dim R$. Let us put

$$u_i=\frac{t_i}{t_n}\quad(1\leqq i\leqq n-1).$$

It is a straightforward verification that

$$\bar{F}=\bar{R}(\bar{u}_1, \cdots, \bar{u}_{n-1}).$$

To see this let $0\neq\bar{z}$ be a typical element of $\bar{F}$. We can write $z=\frac{x}{y}$ where $x, y\in R$. Since $d_R(z)=0$ we see that $d_R(x)=d_R(y)=d$, say. Hence x and y can be represented in the form

$$x=\Phi(t_1, \cdots, t_n),\qquad y=\Psi(t_1, \cdots, t_n)$$

where both Φ, Ψ are homogeneous polynomials in n variables of degree d, with coefficients in R. Let us dehomogenize these polynomials:

$$\frac{\Phi(t_1, \cdots, t_n)}{t_n^d}=f(u_1, \cdots, u_{n-1})$$

$$\frac{\Psi(t_1, \cdots, t_n)}{t_n^d}=g(u_1, \cdots, u_{n-1})$$

where f, g are polynomials in $n-1$ variables of degree $\leqq d$ with coefficients in R. Let $\bar{f}, \bar{g}$ denote the polynomials over $\bar{R}$ obtained from f, g by reducing their coefficients modulo M. Then

$$z=\frac{f(u_1, \cdots, u_{n-1})}{g(u_1, \cdots, u_{n-1})}$$

and hence

$$\bar{z}=\frac{\bar{f}(\bar{u}_1, \cdots, \bar{u}_{n-1})}{\bar{g}(\bar{u}_1, \cdots, \bar{u}_{n-1})}$$

which shows that $\bar{z}\in\bar{R}(\bar{u}_1, \cdots, \bar{u}_{n-1})$. Note that $\bar{g}(\bar{u}_1, \cdots, \bar{u}_{n-1})\neq 0$ since

$$d_R(g(u_1, \cdots, u_{n-1}))=d_R\left(\frac{y}{t_n^d}\right)=d_R(y)-d=0.$$

We have now shown that $\bar{F}$ is generated over $\bar{R}$ by $\bar{u}_1, \cdots, \bar{u}_{n-1}$. We now claim that these generators $\bar{u}_1, \cdots, \bar{u}_{n-1}$ are algebraically independent over $\bar{R}$. Suppose there is a relation of the form $\bar{f}(\bar{u}_1, \cdots, \bar{u}_{n-1})=0$ where $\bar{f}$ is a polynomial in $n-1$ variables over $\bar{R}$. Let f denote a foreimage of $\bar{f}$ over R, say of degree d. We have

$$f(u_1, \cdots, u_{n-1})=\frac{\Phi(t_1, \cdots, t_n)}{t_n^d}$$

where Φ is obtained from f by the process of homogenization. By definition Φ is a homogeneous polynomial of degree d in n variables, and the coefficients of Φ coincide essentially with those of f. Now since $\bar{f}(\bar{u}_1, \cdots, \bar{u}_{n-1})=0$ it follows $d_R(f(u_1, \cdots, u_{n-1}))>0$ and hence $d_R(\Phi(t_1, \cdots, t_n))>d$. This means that

$$\Phi(t_1, \cdots, t_n)\in M^{d+1}.$$

Recall that Φ as a polynomial is of degree d. Therefore, using the fact that $t_1, \cdots, t_n$ is a *regular* system of generators of M, it follows that all the coefficients of Φ are contained in M. Hence the same is true for the coefficients of f, i.e. we have $\bar{f}=0$.

We have seen that $\bar{F}$ is generated over $\bar{R}$ by $n-1$ elements which are algebraically independent over $\bar{R}$. In other words: $\bar{F}$ is a rational function field in $n-1$ variables over $\bar{R}$. Hence clearly, there exists an $\bar{R}$-rational place of $\bar{F}|\bar{R}$; such place $\bar{P}$ can e.g. be obtained by successively specializing the variables $\bar{u}_1, \cdots, \bar{u}_{n-1}$ to 0. Now consider the place P of F, defined by

$$z(P)=\bar{z}(\bar{P}) \quad (z\in F).$$

This place P is the composite of the two places $F\to\bar{F}$ (residue map of the R-degree valuation) and $\bar{F}\to\bar{R}$ (modulo $\bar{P}$). In particular we conclude that P dominates R and that $FP=\bar{F}\bar{P}=\bar{R}$. Q.E.D.

Now let us specialize the above lemma to the following geometric situation:

K a field

V an affine irreducible variety defined over K

x $=(x_1, \cdots, x_n)$ a generic point of V over K

F $=K(x)$ the function field of V over K

a $=(a_1, \cdots, a_n)$ some point on V; the coordinates of a are contained in some overfield of K.

COROLLARY A2. *Suppose that a is simple on V. Then there exists a place P of $F|K$ such that $xP=a$ and $FP=K(a)$.*

PROOF. We apply lemma A1 to the local ring $R_a\subset F$ of the point a. By definition, R_a is the ring of quotients of $K[x]$ with respect to those denominators $g(x)$ which do not vanish at a, i.e. $g(a)\neq 0$. The residue field R_a/M_a

is naturally isomorphic to $K(a)$ and both fields may be identified. After this identification the residue map $R_a \to \bar{R}_a = K(a)$ maps x onto a, i.e. $\bar{x}=a$. Notice that R_a is regular since a is simple on V. Thus lemma A1 leads to a place P of F with the required properties. Q.E.D.

COROLLARY A3. *In the same situation as in corollary A2 suppose in addition that a is K-rational, i.e. $K(a)=K$. Then there exists a K-rational place P of $F|K$ such that $xP=a$.*

Appendix B: Merckel's lemma.

The following lemma has been used in the proof of theorem 3.2 for the "exceptional" case of non-formally $\mathfrak{p}$-adic fields. The lemma itself, however, is of general nature and does not refer to the theory of formally $\mathfrak{p}$-adic fields. We consider the following general situation:

K an arbitrary field

F an extension field of K

$\gamma(x)$ a rational function in $K(x)$ such that its differential $d\gamma(x)\neq 0$.

The condition $d\gamma(x)\neq 0$ is equivalent to saying that $\gamma(x)$ should not be constant and, if the characteristic of K is a prime number $p>0$, then $\gamma(x)$ should not be a function of x^p. Obviously this condition is satisfied if $\gamma(x)$ is the Kochen operator as defined in the text above. Again in the general case, let γF denote the set of elements $\gamma(f)$ where $f\in F$ and $\gamma(f)\neq\infty$, i.e. $\gamma(f)$ should be defined as an element in F. The field $K(\gamma F)$ generated by γF over K, is then a subfield of F.

LEMMA B1. *If the base field K is infinite then $K(\gamma F)=F$.*

REMARK. Merckel [**11**] page 59 has proved this lemma also for finite fields, *provided* that F has at least $(k+1)^2$ elements, k being the maximum of the degree of numerator and denominator of the rational function $\gamma(x)$. If F has less than $(k+1)^2$ elements then the assertion $K(\gamma F)=F$ may be false. We shall prove Merckel's lemma for infinite base field only; this is sufficient for our present purpose.

PROOF OF LEMMA B1.

(i) First we consider the case that F is the rational function field in one variable:

$$F=K(x).$$

For brevity let us put

$$F_0=K(\gamma F).$$

We have to show that $F_0=F$. The field F_0 contains the non-constant rational function $\gamma(x)$; hence F_0 is transcendental over K. It follows that F is algebraic and of finite degree over F_0. Moreover F is separable over F_0, in view of our

hypothesis that the differential $d\gamma(x)$ does not vanish. It follows that there are only finitely many places P of $F|K$ which are ramified over F_0 (these places need not be rational over K).

Now let us consider the automorphism group G of $F|K$. It is well known that every $\sigma\in G$ can be represented in the form

$$x\sigma=\frac{ax+b}{cx+d}$$

with coefficients $a, b, c, d\in K$ and nonvanishing determinant. (We write σ as right operator.) For any $f=f(x)\in F$ we have

$$f\sigma=f\left(\frac{ax+b}{cx+d}\right).$$

Since $\gamma(f)\cdot\sigma=\gamma(f\sigma)$ we conclude

$$(\gamma F)\cdot\sigma=\gamma F$$

$$F_0\sigma=F_0.$$

Thus every automorphism $\sigma\in G$ maps the field F_0 onto itself. Consequentiy G permutes the finitely many places of F which are ramified over F_0.

Recall that G acts naturally on the places P of $F|K$; the image σP of P is given by the formula

$$x\cdot\sigma P=x\sigma\cdot P.$$

We do not assume that P is K-rational; thus P is an arbitrary place of F over K with values in the algebraic closure $\tilde{K}$ of K. In the above formula, the values $x\cdot\sigma P$ and $x\sigma\cdot P$ are understood to be elements in $\tilde{K}\cup\infty$.

Let G_0 denote the normal subgroup of G which leaves every ramified place of $F|F_0$ fixed. By what has been said above G_0 is of finite index in G. It follows that G_0 contains infinitely many translations τ of the form

$$x\tau=x+b$$

with $b\in K$. Notice that the field K is supposed to be infinite; hence indeed the group T of all translations $\tau\in G$ is infinite and thus $G_0\cap T$ is infinite too. Let $\tau\in G_0\cap T$, $\tau\neq 1$. Then $b\neq 0$. If the place P of $F|K$ is ramified over F_0 then $\tau P=P$ and hence

$$xP=x\cdot\tau P=x\tau\cdot P=(x+b)\cdot P=xP+b.$$

Since $b\neq 0$ we conclude $xP=\infty$. Hence there is at most one place P of $F|K$ which is ramified over F_0, namely the pole of x. After replacing x by x^{-1} the pole of x becomes the zero of x^{-1}; hence the pole of x is not ramified either.

In other words: F is unramified over F_0.

From Lüroth's theorem we know that F_0 is a rational function field over K. Now a rational function field does not admit any proper separable-algebraic field extension which is unramified and preserves the field of constants; this is well known from the general ramification theory of function fields. We conclude $F=F_0$, as contended.

(ii) Now let F be an arbitrary extension field of K. Let x be an indeterminate over F. In (i) we have proved that $x\in K(\gamma K(x))$. This means that there is a relation of the form

$$(*) \qquad x=\Phi(\gamma(f_1(x)), \cdots, \gamma(f_n(x)))$$

where Φ denotes a rational function in n variables with coefficients in K, and where $f_1, \cdots, f_n\in K(x)$. Let $a\in F$ be such that all rational functions involved on the right hand side of $(*)$ are defined at a, and that the specialization $x\to a$ yields the relation

$$(**) \qquad a=\Phi(\gamma(f_1(a)), \cdots, \gamma(f_n(a)))\,.$$

This condition excludes only finite number of elements in F. For all remaining $a\in F$ we infer from $(**)$ that $a\in K(\gamma K(a))\subset K(\gamma K)$. Thus we have seen that $K(\gamma F)$ contains all but finitely many elements $a\in F$. Since F is infinite this implies in fact that $K(\gamma F)=F$. Q. E. D.

References

[1] S. Abhyankar, On the valuations centered in a local domain, Amer. J. Math., 78 (1956), 321-348.

[2] J. Ax and S. Kochen, Diophantine problems over local fields I, II, Amer. J. Math., 87 (1965), 605-648; III, Ann. of Math., 83 (1966), 437-456.

[3] S. A. Basarab, A model theoretic transfer theorem for Henselian valued fields, J. Reine Angew. Math., 311/312 (1979), 1-30.

[4] O. Endler, Valuation theory, Springer, 1972.

[5a] Ju. L. Eršov, On elementary theories of maximal normed fields III (Russian), Algebra Logika Sem., 6, Nr. 3 (1967), 31-38.

[5b] Ju. L. Eršov, On rational points over Henselian fields (Russian), Algebra Logika Sem., 6, Nr. 3 (1967), 39-49.

[6] I. Kaplansky, Commutative Rings, Boston, 1970.

[7] J. J. Kelleher, Rings of meromorphic functions on non-compact Riemann surfaces, Canad. J. Math., 21 (1969), 284-300.

[8] S. Kochen, Integer valued rational functions over the p-adic numbers: A p-adic analogue of the theory of real fields, Proc. Symp. Pure Math., 12, Number Theory, 57-73.

[9] W. Krull, Jacobsonsche Ringe, Hilbertscher Nullstellensatz, Dimensionstheorie, Math. Zeitschr., 54 (1951), 354-387.

[10] S. Lang, Some applications of the local uniformization theorem, Amer. J. Math.,

76 (1954), 362-374.
[11] M. Merckel, Wertbereiche rationaler Funktionen, Diplomarbeit, Heidelberg, 1975.
[12] P. Roquette, Bemerkungen zur Theorie der formal p-adischen Körper, Beiträge z. Algebra u. Geometrie, 1 (1971), 177-193.
[13] P. Roquette, Principal ideal theorems for holomorphy rings in fields, J. Reine Angew. Math., 262/263 (1973), 361-374.
[14] P. Roquette, On the Riemann p-space of a field: The p-adic analogue of Weierstrass' approximation theorem and related problems, Abh. Math. Sem. Univ. Hamburg, 47 (1978), 236-259.
[15] P. Roquette, A criterion for rational places over local fields, J. Reine Angew. Math., 292 (1977), 90-108.
[16] R. Transier, Untersuchungen zu einer allgemeinen Theorie formal p-adischer Körper, Dissertation, Heidelberg, 1977.
[17] V. Weispfenning, On the elementary theory of Hensel fields, Ann. Math. Logic, 10 (1976), 59-93.
[18] V. Weispfenning, Nullstellensätze—A model theoretic framework, Z. Math. Logik Grundlagen Math., 23 (1977), 539-545.
[19] O. Zariski, Local uniformization on algebraic varieties, Ann. of Math., ser. 2, 41 (1940), 852-896.
[20] M. Ziegler, Die elementare Theorie der Henselschen Körper, Dissertation, Köln, 1972.
[21] M. Ziegler, Nullstellensätze für lokale Körper, Mimeographed Notes.

Morshe JARDEN
Department of Mathematics
Tel Aviv University
Ramat Aviv, Tel Aviv
Israel

Peter ROQUETTE
Mathematisches Institut
Universität Heidelberg
6900 Heidelberg
Germany