DERIVATIONS ON \( p \)-ADIC FIELDS\(^{(1)} \)

BY

NICKOLAS HEEREMA

1. Introduction. Let \( K \) be a \( p \)-adic field as defined in Schilling [2, p. 226, Definition 2] with exponential valuation \( V \) and associated place \( H \). Let \( k \) be the residue field of \( K \) and \( R_K \) the ring of integers of \( K \). In this paper we investigate the following connection between derivations on \( K \) into \( K \) and derivations on \( k \) into \( k \). Let \( D \) be an integral derivation on \( K \), i.e., one which maps integers onto integers. The mapping \( d \) on \( k \) given by \( d[H(a)] = H[D(a)] \), for all \( a \in R_K \) is a derivation on \( k \) and we say that \( d \) is induced by \( D \).

An integral derivation on \( K \) is an analytic derivation, that is, it is a continuous map in the valuation topology. The following is an almost immediate consequence of the definition:

**Proposition 1.** A derivation \( D \) on \( K \) is analytic if and only if for some positive integer \( n \) and every \( a \in R_K \), \( V[D(a)] \geq -n \).

If \( D \) is a derivation on \( K \) then so is \( p^rD \) where \( r \) is an integer. Thus \( K \) possesses a derivation \( D \) which maps \( R_K \) into \( R_K \) but not into \( (p) \), the maximal ideal in \( R_K \), if and only if \( K \) possesses a nontrivial analytic derivation. Such a derivation induces a nontrivial derivation on \( k \). However \( k \) possesses a nontrivial derivation (into \( k \)) if and only if \( k \) is not perfect, so we have

**Proposition 2.** If \( k \) is perfect \( K \) has no nontrivial analytic derivations.

In this paper we show that, not only is the converse of Proposition 2 true, but every derivation on \( k \) is induced by a derivation on \( K \) (Theorem 1). Thus if \( k \) is not perfect \( K \) possesses a nontrivial analytic derivation which fact is used to prove Theorem 2. This theorem asserts the converse of a theorem of Teichmüller [3, p. 144] which states that if \( K' \) is a \( p \)-adic field [2, p. 227, Definition 3] with the same residue field \( k \) then \( K \) is uniquely embedded in \( K' \) if \( k \) is perfect.

2. Construction of analytic derivations. Let \( S = \{s_\alpha\}_{\alpha \in I} \) be a set of integers in \( K \) with the property that \( S' = \{\bar{s}_\alpha\}_{\alpha \in I} \), where \( \bar{s}_\alpha = H(s_\alpha) \), is a \( p \)-basis for \( k \). It is well known that, given any set of elements \( \{\bar{u}_\alpha\}_{\alpha \in I} \) in \( k \), there is one and only one derivation \( d \) on \( k \) such that \( d(\bar{s}_\alpha) = \bar{u}_\alpha \) for all \( \alpha \in I \), the indexing set of \( S \). \( S \) is a purely transcendental set over \( k_0 \) the maximal perfect subfield of \( k \). Every derivation on \( k_0(S) \) into \( k \) has one and only one extension to \( k \).

Let \( K_0 \) be the \( p \)-adic subfield of \( K \) having residue field \( k_0 \). Again, \( S \) is a purely transcendental set over \( K_0 \). Let \( d \) be an arbitrary derivation on \( k_0(S) \)

---

\(^{(1)}\) This research was supported by NSF G-11292.

Presented to the Society, December 12, 1960; received by the editors March 14, 1961.
DERIVATIONS ON $p$-ADIC FIELDS

into $k$ and let $S_1$ be a proper subset of $S$. Now if $D$ is an integral $K_0$ derivation (trivial on $K_0$) on $K_1 = K_0(S_1)$ into $K$ which induces $d$ restricted to $k_1 = K_0(S_1)$ and $s_\alpha \in S - S_1$, then we can extend $D$ to an integral derivation $D'$ on $K_1(s_\alpha)$ which induces $d$ on $k_1(s_\alpha)$ by choosing $D'(s_\alpha)$ so that $H(D'(s_\alpha)) = d(s_\alpha)$. By a straightforward argument based on Zorn’s Lemma we conclude that every derivation $d$ on $k_0(S)$ into $k$ is induced by a $K_0$ derivation on $K_0(S)$ into $K$.

Thus the problem of finding a derivation on $K$ which induces a given derivation on $k$ is reduced to the problem of extending an integral $K_0$ derivation on $K_0(S)$ into $K$ to an integral derivation on $K$. This is done in a way suggested by the usual proof [4, p. 128] of the fact that if $L$ and $F$ are fields such that $L$ is a separable extension of $F$ then any derivation on $F$ can be extended to a derivation on $L$.

The fields $k_0(S)$ and $k_0$ are linearly disjoint over $[k_0(S)]_p = k_0(S_0)$ by virtue of the fact that $S$ is a $p$-basis for $k$. Thus if the set $\{u_\beta\}_{\beta \in J}$ is a basis for $k_0$ as a vector space over $k_0(S)$ then $\{u_\beta\}_{\beta \in J}$ is also a basis for $k_0(S) [k_0]$ over $k_0(S)$. But $k_0(S) [k_0] = k$. Thus $\{u_\beta\}_{\beta \in J}$ is a basis for $k$ over $k_0(S)$. Hence $\{u_\beta\}_{\beta \in J}$ is a basis for $k_0$ over $k_0(S)$. Repeating the argument $n$ times we conclude that the set $\{u_\beta^n\}_{\beta \in J}$ is a basis for $k$ over $k_0(S)$.

For each $\beta \in J$ we choose $u_\beta \in K$ so that $H(u_\beta) = u_\beta$. The set $U_n = \{u_\beta^n\}_{\beta \in J}$ is clearly linearly independent over $K_0(S)$. Moreover, each coset of the ideal $(p^n)$ in $R_K$ contains an element of the form $\sum a_\alpha u_\alpha^n$ where the $a_\alpha$ are integers in $K_0(S)$ (unless otherwise indicated $\sum$ will indicate a finite sum in the elements of $U_n$ with coefficients which are integers in $K_0(S)$). This follows from the fact that $H$ maps the linear space spanned by the set $U_n$ over $K_0(S)$ onto $k$.

Let $D$ denote an arbitrary integral derivation on $K_0(S)$ into $K$. We define a mapping $D_n$ on $R_K/(p^n)$ as follows. Let $x + (p^n)$ be an arbitrary element of $R_K/(p^n)$. There is then an element $\sum a_\alpha u_\alpha^n$ in the set $x + (p^n)$. We let $D_n(x + (p^n)) = \sum D(a_\alpha)u_\alpha^n + (p^n)$. $D_n$ is a well-defined mapping since if the element $\sum b_\alpha u_\alpha^n$ is in the coset $x + (p^n)$ then for all $\alpha$, $b_\alpha \equiv a_\alpha \mod p^n$, and $D(a_\alpha) \equiv D(b_\alpha) \mod p^n$, since $D$ is integral.

In order to verify that $D_n$ is a derivation we must show that the coset $u_\alpha^n u_\beta^n + (p^n)$ contains an element of a certain form. To this end we use the following:

**LEMMA 1.** For all positive integers $r$ and $m$

\[
\left[ \sum c_\alpha u_\alpha^r \right]^{p^m} = \sum_{i=0}^{m-1} p^i \sum s_{i,\alpha} c_\alpha^{p^m-i} u_\alpha^{p^m+i}, \quad \mod p^m,
\]

where $s_{i,\alpha}$ is a rational integer and $c_\alpha$ is an integer in $K_0(S)$ for all $i$ and $\alpha$.

**Proof.** Let $[p^m, q]$ denote an ordered partition of the integer $p^m$ into $q$ nonnegative summands and let $C[p^m, q]$ represent the corresponding multinomial coefficient. If $p^*$ is the highest power of $p$ to divide the integers in

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
$[p^m, q]$ then $p^{m-q}$ divides $c[p^m, q]$ i.e. $c[p^m, q] = p^{m-q}c'[p^m, q]$. Thus, in a multinomial expansion to the power $p^m$ each term having $c[p^m, q]$ as a coefficient is a $p^q$ power.

With these preliminaries we proceed to the proof of (1) by induction on $m$. Clearly (1) holds for $m = 1$. We assume then that (1) holds for $m < n$. Now

$$[\sum c_{a\alpha} x^a]^{p^m} = \sum c_{a\alpha} x^{p^{m-n}} + \sum_{i=1}^{n-1} p^{i} \sum c'[p^n, q] A[p^n, q], \mod p^n,$$

by the above remarks on a multinomial expansion to the power $p^n$. Now,

$$A[p^n, q] = \sum c_{[p^n, q], a\alpha}^{p^{m-i}}, \mod p,$$

and hence

$$A[p^n, q] = [\sum c_{[p^n, q], a\alpha}^{p^{m-i}}]^{p^{n-i}}, \mod p^{n-i}.$$

However, by the induction hypothesis

$$[\sum c_{[p^n, q], a\alpha}^{p^{m-i}}]^{p^{n-i}} = \sum_{i=0}^{n-i-1} p^{i} \sum s_{[p^n, q], i, c[p^n, q], i, a\alpha}^{p^{m-i}}, \mod p^{n-i}.$$

Substituting (3) for $A[p^n, q]$ in (2) yields an expression of the form (1) and the lemma is proved.

**Lemma 2.** The mapping $D_n$ is a derivation on $R_K/(p^n)$.

**Proof.** $D_n$ is clearly an additive mapping. In order to verify that $D_n(xy) = xD_n(y) + yD_n(x)$ we proceed as follows. Let $x = \sum a_{a\alpha} u^a + (p^n)$ and $y = \sum b_{b\beta} u^b + (p^n)$. Then, $xy = \sum a_{a\alpha} b_{b\beta} u^{a+b} + (p^n)$. But $u_{a\alpha} u_{b\beta} = \sum c_{a\alpha} c_{b\beta} \mod p$, and hence, $u_{a\alpha} u_{b\beta} = \sum c_{a\alpha} c_{b\beta} u^{a+b} \mod p^n$. Using Lemma 1 with $r = 0$ we have

$$u_{a\alpha} u_{b\beta} = \sum_{i=0}^{n-i-1} p^{i} \sum s_{a\alpha, i, c_{a\alpha}, i, c_{b\beta}, i, c_{b\beta}}^{p^{m-i}}, \mod p^n,$$

or,

$$xy = \sum a_{a\alpha} b_{b\beta} \sum_{i=0}^{n-i-1} p^{i} \sum s_{a\alpha, i, c_{a\alpha}, i, c_{b\beta}, i, c_{b\beta}}^{p^{m-i}} + (p^n).$$

Thus,

$$D_n(xy) = \sum D(a_{a\alpha} b_{b\beta} s_{a\alpha, i, c_{a\alpha}, i, c_{b\beta}, i, c_{b\beta}}^{p^{m-i})} u^a + (p^n),$$

$$= \sum [a_{a\alpha} D(b_{b\beta}) + b_{b\beta} D(a_{a\alpha})] s_{a\alpha, i, c_{a\alpha}, i, c_{b\beta}, i, c_{b\beta}}^{p^{m-i}} + (p^n),$$

$$= \sum [a_{a\alpha} D(b_{b\beta}) + b_{b\beta} D(a_{a\alpha})] u^a u^b + (p^n),$$

$$= xD_n(y) + yD_n(x).$$
We define a mapping $D$ on $R_K$ as follows. $D(x) = \bigcap_{n=1}^\infty D_n(x + (p^n))$ and we assume that $u_1$ and $u_1$ are the unity elements of $k$ and $K$.

**Lemma 3.** The mapping $D$ on $R_K$ is a derivation and its restriction to $R_K \cap K_0(S)$ is $D$.

**Proof.** We first show that for all $n$, $D_n[x + (p^n)] \supset D_{n+1}[x + (p^{n+1})]$. Let $u_p = \sum c_n u_n, \mod p$. Thus $u_p^{p+1} = \left[ \sum c_n u_n \right]^{p+1}, \mod p^n$. Or, using Lemma 1,

$$u_a^{p^n} = \sum_{i=0}^{n-1} \sum_{i=0}^n s_{a,i,\beta} c_a s_{a,i,\beta} u_\beta, \mod p^n.$$

We have $x + (p^{n+1}) = \sum b_n u_n^{p^{n+1}} + (p^{n+1})$ and, by (4),

$$x + (p^i) = \sum b_n \beta a_{i,\beta} s_{a,i,\beta} u_\beta + (p^i).$$

Now

$$D_n[x + (p^n)] = \sum D(b_n) s_{a,i,\beta} c_a s_{a,i,\beta} u_\beta + (p^n),$$

$$= \sum D(b_n)\beta a_{i,\beta} s_{a,i,\beta} u_\beta + (p^n),$$

$$= \sum D(b_n) u_a^{p^{n+1}} + (p^n).$$

Also, we have

$$D_{n+1}[x + (p^{n+1})] = \sum D(b_n) u_n^{p^{n+1}} + (p^{n+1}),$$

and it follows that $D_{n+1}[x + (p^{n+1})]$ is a subset of $D_n[x + (p^n)]$. The cosets $\{D_n[x + (p^n)]\}$ form a nested sequence. Thus the mapping $D$ is a derivation mod $p^n$ for all positive integers $n$. It follows that $D$ is a derivation, and it is obviously integral.

It remains to show that $D$ agrees with $D$ on $K_0(S) \cap R_K$. Let $a \in K_0(S) \cap R_K$. Then $D_n[a + (p^n)] = D_n[au_a^{p^n} + (p^n)] = D(a) + (p^n)$. Hence $D(a) = \bigcap_{n=1}^\infty D_n[a + (p^n)] = D(a)$.

Now we started this construction with an arbitrary integral derivation on $K_0(S)$. Extending $D$ to $K$ the quotient field of $R_K$ we conclude that every integral derivation on $K_0(S)$ has an integral extension to $K$.

**Theorem 1.** Every derivation on $k$ is induced by a derivation on $K$.

**Proof.** Each derivation $d$ on $k$ is the unique extension of a derivation $d'$ on $k_0(S)$ into $k$. There exists a derivation $D$ on $K_0(S)$ into $K$ which induces $d'$. But we have shown that $D$ can be extended to an integral derivation on $K$ which induces a derivation on $k$ which is in turn an extension of $d'$.

**Corollary.** $K$ possesses no nontrivial analytic derivations if and only if $k$ is perfect.
Proof. If \( K \) possesses a nontrivial analytic derivation, it then has an integral derivation which induces a nontrivial derivation on \( k \), hence \( k \) is not perfect. If \( k \) is not perfect there is a nontrivial derivation \( d \) on \( k \), and the result follows from the theorem.

3. An application. A well-known theorem of Teichmüller [3, p. 144] states that if \( K' \) is a \( p \)-adic field with residue field \( k \), then \( K \) is uniquely embedded in \( K' \) if \( k \) is perfect.

We will show that if \( K \) possesses a nontrivial integral derivation then \( K \) is not uniquely embedded in \( K' \).

Let \( R_K[[x]] \) represent the power series ring in \( x \) over \( R_K \). Then \( R_K \), is a homomorphic image of \( R_K[[x]] \) with kernel \( I=(p-x^n) \) where \( n \) is a unit and \( n \) is the ramification index of \( K' \) [1, Theorem 1].

Let \( D \) represent a nontrivial derivation on \( R_K \) such that for \( a \in R_K, V(D(a)) \geq 2 \) and equality is obtained for some element in \( R_K \). The mapping \( \tau \) given by

\[
\tau(a) = \sum_{i=0}^{n} (D^i(a)/i!)x^i \quad (D^0 \text{ being the identity map})
\]

is an isomorphism of \( R_K \) into \( R_K[[x]] \) and, moreover, \( V(D^i(a)/i!) > i \) for all integers \( i > 0 \). Let \( \xi \) denote the natural map of \( R_K[[x]] \) onto \( R_K[[x]]/I \). Then \( \xi \) is an isomorphism and we wish to show that \( \xi \tau(R_K) \) contains cosets not of the form \( b+I \) for \( b \in R_K \). Equivalently, we wish to show that for some \( a \in R_K \) there is no \( b \in R_K \) such that \( \sum_{i=0}^{n} (D^i(a)/i!)x^i \) is congruent to \( b \), mod \( I \). We consider then the equation

\[ (5) \quad \sum_{i=0}^{n} \frac{D^i(a)}{i!} x^i = b + \left( p - x^n \sum_{i=0}^{n} u_i x^i \right) \sum_{i=0}^{n} c_i x^i \]

where \( u = \sum_{i=0}^{n} u_i x^i \) and \( u_0 \) is a unit in \( R_K \).

In order for this equation to have a solution \( c = \sum_{i=0}^{n} c_i x^i \) for some \( b \) we must have

\[ a = b + p c_0, \]

\[ \frac{D^i(a)}{i!} = p c_i, \quad i = 1, \ldots, n - 1, \]

\[ \frac{D^{n+i}(a)}{(n+j)!} = p c_{n+j} - \sum_{k=0}^{j} (u_k c_{j-k}), \quad j = 0, 1, \ldots. \]

We choose \( a \) so that \( V(D(a)) = 2 \) and, hence \( V(c_1) = 1 \). Assume first that \( V(c_0) \leq 1 \). Since \( V(D^i(a)/i!) > n \) it follows that \( V(p c_n) = V(c_0) = 0 \) and \( V(c_n) = 1 \). Necessarily \( V(c_i) > 1 \) for \( 1 < i < n \). It follows by letting \( j = n \) in (6) that \( V(p c_n) = V(c_n) \) which is a contradiction since \( c_n \in R_K \). Assume next that \( V(c_0) > 1 \). Again, letting \( j = 1 \) in (6) we conclude that \( V(p c_{n+1}) = V(c_1) \) or \( V(c_{n+1}) = 0 \). As before, it follows that \( V(p c_{n+1}) = V(c_{n+1}) \) which is a contradiction. Thus equation (5) has no solution \( \sum_{i=0}^{n} c_i x^i \) for any \( b \in R_K \) and it follows that the embedding \( \xi \tau(R_K) \) in \( R_K[[x]]/I \) is distinct from the canonical embedding. It follows that the quotient field of \( \xi \tau(R_K) \) is distinct.
from the canonical embedding of $K$ in the quotient field of $R_K[[x]]/I$. Appealing to Theorem 1 for the existence of the derivation $D$ if $k$ is not perfect we have

**Theorem 2.** $K$ is uniquely embedded in $K'$ if and only if $k$ is perfect.

We note in conclusion that the unique embedding of $K$ in $K'$ in case $k$ is perfect can be proved by an argument which depends directly on the fact that $k$ possesses no nontrivial derivations [1, p. 493].

**References**


**Florida State University,**
**Tallahassee, Florida**