EMBEDDINGS OF A $p$-ADIC FIELD AND ITS RESIDUE FIELD IN THEIR POWER SERIES RINGS

NICHOLAS HEEREMA

I. Introduction. Let $K$ denote a $p$-adic field [5, p. 226, Definition 2] with residue field $k$. Let $R$ represent the ring of integers of $K$ and let $H$ represent the corresponding place of $K$.

In this paper we show that every embedding of $k$ in its power series ring $k[[x_1, \ldots, x_n]]$ or $k[[x]]_n$ in $n$ indeterminates is induced by an embedding of $K$ in its power series $K[[Y]]_n$ in $n$ indeterminates.

It follows from this that every automorphism of $k[[X]]_n$ is induced by an automorphism of $K[[Y]]_n$.

Let $S$ be a complete regular local ring which is not ramified and let $M = (u_1, \ldots, u_m)$ be the maximal ideal of $S$, where $u_1, \ldots, u_m$ is a minimal set of generators of $M$. If $P_i$ denotes the ideal $(u_1, \ldots, u_i)$ for $i = 1, \ldots, m$ then our concluding result asserts that every automorphism of $S/P_i$ is induced by an automorphism of $S$. This result is, of course, well known in the case $n = 1$.

We are able to establish the result on induced embeddings by an argument which is much like that used in [4] to show that each derivation on $k$ (into $k$) is induced by a derivation on $K$. This is not surprising in view of the close connection between derivations and embeddings in power series rings [2; 3].

We define an embedding of a commutative ring $S$ in a power series ring $S'[[X]]_n$, where $S'$ is a commutative ring containing $S$, to be an isomorphism $\theta$ of $S$ into $S'[[X]]_n$ subject to the following condition. Let $\phi$ represent the natural mapping $S'[[X]]_n$ onto $S'$. Then $\theta$ has the property that $a = \phi\theta(a)$ for all $a \in S$. If $S' = S$ we call $\theta$ simply an embedding of $S$.

The homomorphism $H$ of $R$ onto $k$ is extended to a homomorphism $H'$ of $R[[Y]]_n$ onto $k[[X]]_n$ by the condition

$$H'\left(\sum_{I \in S^*} a_I Y^I\right) = \sum_{I \in S^*} H(a_I) X^I,$$

where $I$ represents an $n$-tuple of ordinary non-negative integers $i_1, \ldots, i_n$, $X^I = X_1^{i_1}X_2^{i_2} \cdots X_n^{i_n}$, and $S^*$ is the set of all such $n$-tuples. An embedding $\phi$ of $k$ is induced by an embedding $\theta$ of $R$ if for each $a$ in $R$ we have

Presented to the Society, November 17, 1961, under the title Embeddings of a $p$-adic field; received by the editors May 3, 1962.

1 This research was supported by NSFG-11292 and NSF-G19912.
EMBEDDINGS OF A $\mathfrak{p}$-ADIC FIELD

575

II. The embedding theorem.

Theorem. Each embedding $\varnothing$ of $k$ is induced by an embedding of $R$, or, equivalently, by an embedding of $K$.

Proof. We let $k_0$ represent the maximal perfect subfield of $k$. It follows that $\varnothing$, restricted to $k_0$, is the identity mapping [3, Lemma 1]. Let $K_0$ be the $\mathfrak{p}$-adic subfield of $K$ with residue field $k_0$ and let $\theta_0$ be the identity mapping on $K_0$ regarded as an isomorphism of $K_0$ into $K[[Y]]_n$.

Next we choose a set $S$ of units in $R$ with the property that the set $S = H(S)$ is a $\mathfrak{p}$-basis for $k$ and we observe in the following way that $\theta_0$ can be extended to an embedding $\theta$ of $K_1 = K_0(S)$ into $K[[Y]]_n$ such that condition (1) holds for every integral element $a$ in $K_1$. The fact that $S$ is a $\mathfrak{p}$-basis implies that $S$ and $\bar{S}$ are algebraically independent over $K_0$ and $k_0$ respectively. Assume that $\theta_0$ has been extended to an integral embedding $\theta$ on $\tilde{K} = K(S_1)$ where $S_1$ is a proper subset of $S$, such that $\theta$ satisfies condition (1) for every integral element $a$ in $\tilde{K}$. We choose $\overline{a}$ in $\bar{S}$ and not in $S$. Let $\varnothing(a) = \sum a_i X^i$. Necessarily $a_0, \ldots, a_{n-1} = \overline{a}$. We next choose $a_0, \ldots, a_{m-1}$ in $S$ and $a_i$ in $K$, for each $i$ in $S^*$, so that $H(a_i) = a_i$. Finally, the mapping $\theta$ is extended to an isomorphism $\theta^*$ of $K^* = \tilde{K}(a_0, \ldots, a_m)$ into $K[[Y]]_n$, by the condition $\theta^*(a_0, \ldots, a_m) = \sum a_i X^i$. By construction $\theta^*$ is an integral embedding which satisfies condition (1) for every integer in $K^*$. Thus, by a standard Zorn's lemma argument we conclude that $\theta_0$ can be extended to an integral embedding $\theta$ of $K_1$ into $K[[Y]]_n$, for which condition (1) holds.

In order to extend $\theta$ to the desired integral embedding on all of $K$ we proceed as follows. Let $U$ be a set of units in $R$ which contains $1$ and has the property that $U = H(U)$ is a basis for $k$ as a linear space over $k_1$. Then for any positive integer $m$ the set $U^m$ of $m$ powers of the elements in $U$ is also a basis for $k$ over $k_1$ [4, p. 347].

Let $a$ be in $R$. The coset $a + (p^m)$ has a representative of the form $\sum a_i u_i^{m^i}$ where the $a_i$ are integral in $K_1$ and $\sum$ denotes a finite sum. Moreover, the $a_i$ are uniquely determined mod $p^m$. In the remainder of this paper the coefficients $a_i$ in an expression of the form $\sum a_i u_i^{m^i}$, $u_i \in U$, will be integral in $K_1$. Let $R_m$ denote the ring $R/(p^m)$, and let $R[[Y]]_{(a,m)}$ represent the ring $R[[Y]]/(p^m, Y_p^m, \ldots, Y_n^m)$. We define a mapping $\theta_m$ of $R_m$ into $R[[Y]]_{(a,m)}$ by the following:

$$\theta_m(\sum a_i u_i^{m^i} + (p^m)) = \sum u_i^{m^i} \theta(a_i) + (p^m, Y_p^m, \ldots, Y_n^m).$$
We will show first that \( \theta_m \) is an isomorphism with the property that, for all \( a \in R, \theta_m(a + (p^m)) = a, \mod(Y_1, \cdots, Y_n) \). The \( \theta_m \) determine a limit function which will prove to be the desired embedding of \( R \) in \( R[[Y]]_s \). To this end we have the following preliminaries.

For \( I \) and \( J \) in \( s^* \), we write \( J \leq I \) if each component of \( J \) is less than or equal to the corresponding component of \( I \), \( I + J \) is obtained by component-wise addition. If \( p \) divides each integer in \( I \) we say \( p \) divides \( I \), \( (p \divides I) \), and denote the \( n \)-tuple of quotients by \( I/p \). The largest integer in \( I \) is represented by \( |I| \), and \( kI \) represents the \( n \)-tuple obtained by component-wise multiplication of \( I \) by the integer \( k \).

For \( a \) integral in \( K_1 \), \( \bar{a} = \sum a_I Y^I \) where \( a_I \) is in \( R \) for all \( I \) and \( a_0, \ldots, a = a \). Let \( \Pi_I \) be the mapping given by \( \Pi_I(a) = a_I \). Then for all \( a \) and \( b \) integral in \( K_1 \) and all \( I \) in \( s^* \)

(i) \( \Pi_I(a + b) = \Pi_I(a) + \Pi_I(b) \), and

(ii) \( \Pi_I(ab) = \sum_{J \leq I} \Pi_I(a) \Pi_{I-J}(b) \).

The symbol \( \mathfrak{s} \) will represent the nonzero \( n \)-tuples of \( s^* \).

**Lemma 1.** Let \( a \) be an integral element in \( K_1 \). Then for each \( I \) in \( s \) and \( m > 0 \),

\[(3) \quad \Pi_I(a \tilde{a}^m) = 0, \mod p^m, \quad \text{if } p \divides |I|, \]

\[(4) \quad \Pi_I(a \tilde{a}^m) = [\Pi_{I/p}(a \tilde{a}^{m-1})]^p + p \sum_{J \leq I/p} c_J [\Pi_J(a \tilde{a}^{m-1})]^p + \cdots + p^{m-1} \sum_{J \leq I/p} c_J [\Pi_J(a)]^p, \mod p^m, \text{ if } p \nmid |I|, \]

where the \( c_J \) and \( c_J \) are in \( R \).

**Proof.** We argue by induction on \( m \).

\[(5) \quad \Pi_I(a \tilde{a}) = \sum_{\{p, I\}} C_{p, r_1, \ldots, r_s} \Pi_{J_1}(a) \cdots \Pi_{J_p}(a), \]

where \([p, I]\) represents the set of all ordered partitions of \( I \) into \( p \) summands from \( s^* \), the integers \( r_1, \cdots, r_s \) are the multiplicities of the distinct \( n \)-tuples in the partition \( J_1, \cdots, J_p \) of \( I \), and \( C_{p, r_1, \ldots, r_s} \) is the indicated multinomial coefficient. If \( p \divides |I| \) then, necessarily, \( p \divides C_{p, r_1, \ldots, r_s} \). Hence \( \Pi_I(a \tilde{a}) = 0, \mod p \). If \( p \nmid |I| \) then the only term in (5) not having \( p \) as a factor is \([\Pi_{I/p}(a)]^p\). Thus the lemma holds for \( m = 1 \). We assume the result for \( j < m \). Again,

\[(6) \quad \Pi_I(a \tilde{a}^{m-1}) = \sum_{\{p, I\}} C_{p, r_1, \ldots, r_s} \Pi_{J_1}(a \tilde{a}^{m-2}) \cdots \Pi_{J_p}(a \tilde{a}^{m-2}). \]
As before, if $p \mid I$, then for each partition $J_1, \ldots, J_p$ in $[p, I]$, $p \mid C_{p,r_1}, \ldots, r_s$ and for some $i, p \mid J_i$. Thus, using the inductive hypothesis, we have $\Pi_I(a^{m^n}) = 0, \mod p^m$.

If $p \mid I$,

$$\Pi_I(a^{m^n}) = [\Pi_{I/p}(a^{m^n})]^p + \sum C_{p,r_1,\ldots, r_s} \Pi_{J_1}(a^{m^{n-1}}) \cdots \Pi_{J_s}(a^{m^{n-1}}).$$

The range of the sum is clear. Each coefficient $C_{p,r_1,\ldots, r_s}$ is divisible by $p$. If $p \mid J_i$ for some $i$ then by the inductive hypothesis, the term containing $\Pi_{J_i}(a^{m^{n-1}})$ is zero, $\mod p^m$. Thus we have

$$\Pi_I(a^{m^n}) = [\Pi_{I/p}(a^{m^n})]^p + \sum_{I_j \subseteq J \supseteq I/p} c_j \Pi_{J_j}(a^{m^{n-1}}), \mod p^m,$$

for some set of elements $c_j$ in $R$, where $I_0$ denotes the $n$-tuple of zeros. The result now follows by substituting for $\Pi_{I/p}(a^{m^n})$ using relation (4).

By a straightforward induction argument on $m \geq 0$ using Lemma 1 we have

**Lemma 2.** $\Pi_I(a^{m^{n+1}}) = 0, \mod p^m$, if $0 < |I| < p^{m+1}$.

By definition of the mappings $\Pi_I$, $\tilde{\theta}(a) = \sum_{I \in \mathcal{G}} \Pi_I(a) Y^I$. Hence, using Lemma 2 we have,

**Lemma 3.** For all integers $a$ in $K_1$,

$$\tilde{\theta}(a^{m^{n+1}}) = a^{m^{n+1}} \mod (p^m, Y^{m_n}, \ldots, Y^{m_1}).$$

**Lemma 4.** The mapping $\theta_m$ is an isomorphism with the property that $\theta_m(a) = a, \mod (Y_1, \ldots, Y_n)$, for all $a$ in $R_m$.

**Proof.** It is clear that $\theta_m$ is additive. Since for $b$ an integer in $K_1$, $\tilde{\theta}(b) = b, \mod (Y_1, \ldots, Y_n)$, it follows that for $a$ in $R_m$, $\theta_m(a) = a, \mod (Y_1, \ldots, Y_n)$. Hence, $\theta_m$ is one-to-one. It remains to show that products are preserved.

Let $a = \sum a_i u_i^{m^{n+1}} + (p^m)$ and $b = \sum b_i u_i^{m^{n+1}} + (p^m)$. Then,

$$\theta_m(ab) = \theta_m(\sum a_i b_i u_i^{m^{n+1}} + (p^m)).$$

Now by [4, proof of Lemma 2]

$$u_i^{m^{n+1}} w_j^{m^{n+1}} = \sum_{k=0}^{m-1} p^k \sum_{i,j,k} c_{i,j,k,l}^{m^{n+1}-k} u_j^{m^{n+1}}, \mod p^m,$$

where $s_{i,j,k,l}$ is a rational integer and $c_{i,j,k,l}$ is integral in $K_1$. Hence,
\[ \vartheta_m(ab) = \vartheta_m \left[ \sum a_i b_j \sum_{k=0}^{m-1} p^k \sum_{i,j,k,l} c_{i,j,k,l}^p m^{m+1-k} u_{i,j,k,l}^m + (p^m) \right]. \]

Now
\[ \vartheta(a \cdot b \cdot p^k s_{i,j,k,l} c_{i,j,k,l}^{p^{(m^2+1)-k}}) = \vartheta(a) \vartheta(b) \cdot p^k s_{i,j,k,l} c_{i,j,k,l}^{p^{(m^2+1)-k}}. \]

If \( k \leq m-1 \), then \( 2m^2+1-k > m^2+1 \). Thus, by Lemma 3,
\[ \vartheta(a \cdot b \cdot p^k s_{i,j,k,l} c_{i,j,k,l}^{p^{(m^2+1)-k}}) = \vartheta(a) \vartheta(b) \cdot p^k s_{i,j,k,l} c_{i,j,k,l}^{p^{(m^2+1)-k}}, \text{ mod } (p^m, Y_{p^m}, \ldots, Y_{p^m}). \]

Hence,
\[ \vartheta_m(ab) = \sum \vartheta(a) \vartheta(b) \cdot u_{i,j,k,l}^{p^{m+1}} + (p^m, Y_{p^m}, \ldots, Y_{p^m}), \]
or,
\[ \vartheta_m(ab) = \vartheta_m(a) \vartheta_m(b). \]

Regarding \( \vartheta(a+(p^m)) \) as a set of elements in \( R[[Y]] \) we have

**Lemma 5.** \( \vartheta_m(a+(p^m)) \supseteq \vartheta_{m+1}(a+(p^{m+1})) \) for all integers \( a \) in \( K \).

**Proof.** For each \( u_i \) in \( U \), \( u_i^{p^{m+1}} = \sum c_i u_j \), mod \( p \). Hence, \( (u_i^{p^{m+1}})_{p^{m+1}} = (\sum c_i u_j)^{p^{m+1}} \), mod \( p^{2m+1} \). By [4, Lemma 1] this becomes
\[ u_i^{p^{2m+1}} = \sum_{i=0}^{2m^2} \sum_{i,j,k,l} c_{i,j,k,l}^{p^{m+1}+1} u_{i,j,k,l}^m, \text{ mod } p^{2m+1}. \]

Thus we have, for \( a \) in \( R \),
\[ a + (p^{m+1}) = \sum b_r u_r^{p^{(m^2+1)+1}} + (p^{m+1}), \]
\[ = \sum b_r \sum_{i=0}^{2m^2} \sum_{i,j,k,l} c_{i,j,k,l}^{p^{m^2+1}+1} u_{i,j,k,l} + (p^{m+1}). \]

Hence,
\[ \vartheta_m[a + (p^m)] \]
\[ = \sum \vartheta(b_r) \sum_{i=0}^{2m^2} \sum_{i,j,k,l} c_{i,j,k,l}^{p^{m^2+1}+1} u_{i,j,k,l} + (p^m, Y_{p^m}, \ldots, Y_{p^m}) \]
\[ = \sum \vartheta(b_r) u_r^{p^{2m+1}} + (p^m, Y_{p^m}, \ldots, Y_{p^m}). \]

Also,
The lemma follows.

We now let \( \theta(a) = \bigcap_{m=1}^{n} \theta_m[a + (p^m)] \) for each \( a \) in \( R \). By Lemma 5, \( \theta \) is a well-defined mapping of \( R \) into \( R[[Y]]_n \). It preserves sums and products \( \mod (p^m, Y_m, \ldots, Y_n) \) for all \( m \), hence is a homomorphism. It has the property that \( \theta(a) = a \mod (Y_1, \ldots, Y_m) \), by virtue of the fact that \( \theta_m(a) = a \mod (Y_1, \ldots, Y_n) \), for all \( m \). Thus \( \theta \) is an isomorphism and hence an embedding of \( R \) in \( R[[Y]]_n \).

In order to show that \( \theta \) coincides with \( \theta \) on \( K_1 \) we choose an integral element \( a \) in \( K_1 \). Then, one being in \( U \), we have

\[
\theta \big[ a + (p^m) \big] = \theta(a) + (p^m, Y_1, \ldots, Y_n)
\]

and thus

\[
\theta(a) = \bigcap_{m=1}^{n} \theta_m[a + (p^m)] = \theta(a).
\]

Finally we note that \( \theta \) induces an embedding \( \sigma' \) on \( k \) which coincides with \( \sigma \) on \( k_1 \). However, since \( k_1 \) contains a \( p \)-basis for \( k \), and an embedding on \( k \) is uniquely determined by its action on a \( p \)-basis \([3, \text{Theorem 1}]\) it follows that \( \sigma' = \sigma \) and the theorem is proved.

A set \( \{ \Pi_I \} \) of mappings of a ring \( S \) into \( S \) is an embedding sequence on \( S \) if the conditions (i) and (ii), preceding Lemma 1, obtain for all \( I \). The correspondence between embeddings of \( S \) and embedding sequences on \( S \), as indicated by the paragraph preceding Lemma 1, leads to the following extension of the theorem which states that every derivation on \( k \) is induced by a derivation on \( R \) \([4, \text{Theorem 1}]\).

**Corollary 1.** Each embedding sequence \( \{ \tau_I \} \) on \( k \) is induced by an embedding sequence \( \{ \Pi_I \} \) on \( R \). That is, for all \( a \) in \( R \) and \( I \) in \( \mathcal{S} \), \( H \Pi_I(a) = \tau_I H(a) \).

An application. Let \( \Phi \) denote an automorphism on \( R[[Y]]_n \). The ideal \( (p) \) is invariant under \( \Phi \), hence \( \Phi \) induces, via \( H' \), an automorphism \( \phi \) on \( k[[X]]_n \). Let \( G \) represent the group of automorphisms of \( R[[X]]_n \), and \( G_0 \) the “inertial” subgroup of \( \alpha \) in \( G \) such that for all \( x \) in \( R[[X]]_n \), \( \alpha(x) \equiv x \mod p \). Then we have

**Theorem 2.** Every automorphism on \( k[[X]]_n \) is induced by an automorphism on \( R[[Y]]_n \). Moreover, the group of automorphisms of \( k[[X]]_n \) is isomorphic to \( G/G_0 \).

**Proof.** Let \( \phi \) be an automorphism on \( k[[X]]_n \). Let \( \phi_0 \) denote the
restriction of $\phi$ to $k$. Then for $a$ in $k$ $\phi_0(a) = \sum_{I \in I^*} a_I X^I$. The mapping $a \rightarrow a_0, \ldots, a_n$ is an automorphism $\Phi_0$ on $k$ which by a well known theorem is induced via $H$ by an automorphism $\Phi'$ on $R$. Clearly $\phi_0 = \phi' \phi_0'$ where $\phi'$ is the embedding mapping $a_0, \ldots, a_n \rightarrow \sum_{I \in I^*} a_I X^I$ where again $\phi_0(a) = \sum_{I \in I^*} a_I X^I$. Hence, by Theorem 1, there is an embedding mapping $\Phi'$ on $R$ such that $\Phi_0 = \Phi' \Phi_0'$ induces $\phi_0$. We extend $\Phi_0$ to an automorphism on $R[[X]]$ in the natural way, i.e., let $\Phi(Y) = \sum_{I \in I^*} a_{i,I} Y^I$ where the $a_{i,I}$ are so chosen that $\phi(X_i) = \sum_{I \in I^*} H(a_{i,I}) X^I$. The fact that $\phi$ is an automorphism and the manner in which the $\Phi(Y_i)$ are chosen assure that the endomorphism of $R[[X]]$, $\Phi$ determined by extending $\Phi_0$ to all of $R[[X]]$ in the indicated manner is in fact an automorphism which induces $\phi$. The remaining statement of the theorem is obvious.

Let $S$ represent a complete regular local ring which is not ramified and let $u_1, \ldots, u_n$ be a minimal basis for the maximal ideal $M$ of $S$. I. S. Cohen [1] has shown that $S$ is isomorphic to a power series ring in $n$-indeterminates over a field under a map which takes $u_i$ into the $i$th indeterminate or, in the unequal characteristic case $S$ is isomorphic to $R[[X]]$ for a suitable unramified complete discrete valuation ring $R$ under a map which takes $u_1$ (say) into $p$ and $u_i$ into $X_{i-1}$ for $i = 2, \ldots, n$.

Theorem 2 asserts that in the latter case every automorphism of $S/P_1$ where $P_1 = (u_1)$ is induced by an automorphism of $S$. The remaining cases which arise in the proof of the following corollary are immediate.

**Corollary 2.** Let $S$ be a complete regular local ring which is not ramified and let $u_1, \ldots, u_n$ be a minimal basis for the maximal ideal $M$ of $S$. If $P_i$ denotes the ideal generated by $u_1, \ldots, u_i$ ($i = 1, \ldots, n$) then every automorphism of $S/P_i$ is induced by an automorphism of $S$.

**References**


**Florida State University**