EMBEDDINGS OF A p-ADIC FIELD AND ITS RESIDUE FIELD IN THEIR POWER SERIES RINGS[1]

NICKOLAS 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 $k[[x_1, \cdots, x_n]]$ 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 $M=(u_1, \cdots, u_n)$ be the maximal ideal of S, where $u_1, \cdots, u_n$ is a minimal set of generators of M. If P_i denotes the ideal $(u_1, \cdots, u_i)$ for $i=1, \cdots, n$ 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 θ of S into $S'[[X]]_n$ subject to the following condition. Let ψ represent the natural mapping $S'[[X]]_n$ onto S'. Then θ has the property that $a=\psi\theta(a)$ for all $a\in S$. If $S'=S$ we call θ 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

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

where I represents an n-tuple of ordinary non-negative integers $i_1, \cdots, i_n$, $X^I=X_1^{i_1}X_2^{i_2}\cdots X_n^{i_n}$, and $\mathcal{I}^*$ is the set of all such n-tuples. An embedding Θ of k is induced by an embedding θ 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.

$$H'\theta(a) = \ominus H(a). \tag{1}$$

II. The embedding theorem.

THEOREM. *Each embedding $\ominus$ 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 $\ominus$, restricted to k_0, is the identity mapping [3, Lemma 1]. Let K_0 be the p-adic subfield of K with residue field k_0 and let θ_0 be the identity mapping on K_0 regarded as an isomorphism of K_0 into $K[[Y]]_n$.

Next we choose a set $\mathcal{S}$ of units in R with the property that the set $\bar{\mathcal{S}} = H(\mathcal{S})$ is a p-basis for k and we observe in the following way that θ_0 can be extended to an embedding $\tilde{\theta}$ of $K_1 = K_0(\mathcal{S})$ into $K[[Y]]_n$ such that condition (1) holds for every integral element a in K_1. The fact that $\bar{\mathcal{S}}$ is a p-basis implies that $\mathcal{S}$ and $\bar{\mathcal{S}}$ are algebraically independent over K_0 and k_0 respectively. Assume that θ_0 has been extended to an integral embedding $\hat{\theta}$ on $\hat{K} = K(\mathcal{S}_1)$ where $\mathcal{S}_1$ is a proper subset of $\mathcal{S}$, such that $\hat{\theta}$ satisfies condition (1) for every integral element a in $\hat{K}$. We choose $\bar{a}$ in $\bar{\mathcal{S}}$ and not in $\mathcal{S}_1$. Let $\ominus(\bar{a}) = \sum \bar{a}_I X^I$. Necessarily $\bar{a}_{0,\ldots,0} = \bar{a}$. We next choose $a_{0,\ldots,0}$ in $\mathcal{S}$ and a_I in K, for each I in $\mathcal{J}^*$, so that $H(a_I) = \bar{a}_I$. Finally, the mapping $\hat{\theta}$ is extended to an isomorphism θ^* of $K^* = \hat{K}(a_{0,\ldots,0})$ into $K[[Y]]_n$ by the condition $\theta^*(a_{0,\ldots,0}) = \sum_{I\in\mathcal{J}^*} a_I Y^I$. By construction θ^* is an integral embedding which satisfies condition (1) for every integer in K^*. Thus, by a standard Zorn's lemma argument we conclude that θ_0 can be extended to an integral embedding $\tilde{\theta}$ of K_1 into $K[[Y]]_n$ for which condition (1) holds.

In order to extend $\tilde{\theta}$ 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 $\bar{U} = H(U)$ is a basis for k as a linear space over k_1. Then for any positive integer m the set $\bar{U}^{p^m}$ of p^m powers of the elements in $\bar{U}$ 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 $\sum a_i u_i^{p^m}$ 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 $\sum a_i u_i^{p^m}$, $u_i \in U$, will be integral in K_1. Let R_m denote the ring $R/(p^m)$, and let $R[[Y]]_{(n,m)}$ represent the ring $R[[Y]]_n/(p^m, Y_1^{p^m}, \cdots, Y_n^{p^m})$. We define a mapping θ_m of R_m into $R[[Y]]_{(n,m)}$ by the following:

$$\theta_m\Big(\sum a_i u_i^{p^{2m^2+1}} + (p^m)\Big) = \sum u_i^{p^{2m^2+1}} \tilde{\theta}(a_i) + (p^m, Y_1^{p^m}, \cdots, Y_n^{p^m}). \tag{2}$$

We will show first that θ_m is an isomorphism with the property that, for all a in R, $\theta_m(a+(p^m))\equiv a$, mod$(Y_1, \cdots, Y_n)$. The θ_m determine a limit function which will prove to be the desired embedding of R in $R[[Y]]_n$. To this end we have the following preliminaries.

For I and J in $\mathfrak{g}^*$, we write $J\leqq I$ 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, $(p|I)$, 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, $\bar{\theta}(a)=\sum a_I Y^I$ where a_I is in R for all I and $a_{0,\ldots,0}=a$. Let $\bar{\Pi}_I$ be the mapping given by $\bar{\Pi}_I(a)=a_I$. Then for all a and b integral in K_1 and all I in $\mathfrak{g}^*$

(i) $\bar{\Pi}_I(a+b) = \bar{\Pi}_I(a)+\bar{\Pi}_I(b)$, and

(ii) $\bar{\Pi}_I(ab)=\sum_{J\leq I}\bar{\Pi}_I(a)\bar{\Pi}_{I-J}(b)$.

The symbol $\mathfrak{g}$ will represent the nonzero n-tuples of $\mathfrak{g}^*$.

LEMMA 1. *Let a be an integral element in K_1. Then for each I in $\mathfrak{g}$ and $m>0$,*

$$\bar{\Pi}_I(a^{p^m}) \equiv 0, \text{ mod } p^m, \qquad \textit{if } p\nmid I, \tag{3}$$

$$\begin{aligned}\bar{\Pi}_I(a^{p^m}) \equiv [\bar{\Pi}_{I/p}(a^{p^{m-1}})]^p + p \sum_{J\leq I/p} c_J[\bar{\Pi}_J(a^{p^{m-2}})]^p + \cdots \\ + p^{m-1} \sum_{J\leq I/p} c_J' [\bar{\Pi}_J(a)]^p, \text{ mod } p^m, \textit{ if } p\mid I,\end{aligned} \tag{4}$$

where the c_J and c_J' are in R.

PROOF. We argue by induction on m.

$$\bar{\Pi}_I(a^p) = \sum_{[p,I]} C_{p;r_1,\ldots,r_s}\bar{\Pi}_{J_1}(a) \cdots \bar{\Pi}_{J_p}(a), \tag{5}$$

where $[p, I]$ represents the set of all ordered partitions of I into p summands from $\mathfrak{g}^*$, 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 $p\nmid I$ then, necessarily, $p|C_{p;r_1,\ldots,r_s}$. Hence $\bar{\Pi}_I(a^p)\equiv 0$, mod p. If $p|I$ the only term in (5) not having p as a factor is $[\bar{\Pi}_{I/p}(a)]^p$. Thus the lemma holds for $m=1$. We assume the result for $j<m$. Again,

$$\bar{\Pi}_I(a^{p^m}) = \sum_{[p,I]} C_{p;r_1,\ldots,r_s}\bar{\Pi}_{J_1}(a^{p^{m-1}}) \cdots \bar{\Pi}_{J_p}(a^{p^{m-1}}).$$

As before, if $p \nmid I$, then for each partition $J_1, \cdots, J_p$ in $[p, I]$, $p \mid C_{p;r_1,\cdots,r_s}$ and for some i, $p \nmid J_i$. Thus, using the inductive hypothesis, we have $\bar{\Pi}_I(a^{p^m}) \equiv 0$, mod p^m.

If $p \mid I$,

$$\bar{\Pi}_I(a^{p^m}) = [\bar{\Pi}_{I/p}(a^{p^{m-1}})]^p + \sum C_{p;r_1,\cdots,r_s}\bar{\Pi}_{J_1}(a^{p^{m-1}}) \cdots \bar{\Pi}_{J_p}(a^{p^{m-1}}).$$

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

$$\bar{\Pi}_I(a^{p^m}) \equiv [\bar{\Pi}_{I/p}(a^{p^{m-1}})]^p + \sum_{I_0 < J \leq I/p} c_J \bar{\Pi}_{pJ}(a^{p^{m-1}}), \text{ mod } p^m,$$

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 $\bar{\Pi}_{pJ}(a^{p^{m-1}})$ using relation (4).

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

LEMMA 2. $\bar{\Pi}_I(a^{p^{m^2+1}}) \equiv 0$, mod p^m, *if* $0 < |I| < p^{m+1}$.

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

LEMMA 3. *For all integers a in K_1,*

$$\tilde{\theta}(a^{p^{m^2+1}}) \equiv a^{p^{m^2+1}}, \quad \text{mod } (p^m, Y_1^{p^m}, \cdots, Y_n^{p^m}).$$

LEMMA 4. *The mapping θ_m is an isomorphism with the property that* $\theta_m(a) \equiv a$, mod $(Y_1, \cdots, Y_n)$, *for all a in R_m.*

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

Let $a = \sum a_i u_i^{p^{m^2+1}} + (p^m)$ and $b = \sum b_i u_i^{p^{m^2+1}} + (p^m)$. Then,

$$\theta_m(ab) = \theta_m[\sum a_i b_j u_i^{p^{2m^2+1}} u_j^{p^{2m^2+1}} + (p^m)].$$

Now by [4, proof of Lemma 2]

$$u_i^{p^{2m^2+1}} u_j^{p^{2m^2+1}} \equiv \sum_{k=0}^{m-1} p^k \sum s_{i,j,k,l} c_{i,j,k,l}^{p^{2m^2+1-k}} u_l^{p^{2m^2+1}}, \text{ mod } p^m,$$

where $s_{i,j,k,l}$ is a rational integer and $c_{i,j,k,l}$ is integral in K_1. Hence,

$$\theta_m(ab) = \theta_m\Big[\sum a_i b_j \sum_{k=0}^{m-1} p^k \sum s_{i,j,k,l}\, c_{i,j,k,l}^{p^{2m^2+1-k}} u_l^{p^{2m^2+1}} + (p^m)\Big].$$

Now

$$\bar\theta\big(a_i b_j p^k s_{i,j,k,l}\, c_{i,j,k,l}^{p^{(2m^2+1)-k}}\big) = \bar\theta(a_i)\bar\theta(b_j) p^k s_{i,j,k,l}\,\bar\theta\big(c_{i,j,k,l}^{p^{(2m^2+1)-k}}\big).$$

If $k \leqq m-1$, then $2m^2+1-k > m^2+1$. Thus, by Lemma 3,

$$\bar\theta\big(a_i b_j p^k s_{i,j,k,l}\, c_{i,j,k,l}^{p^{m^2+1-k}}\big)$$
$$\equiv \bar\theta(a_i)\bar\theta(b_j) p^k s_{i,j,k,l}\, c_{i,j,k,l}^{p^{(2m^2+1)-k}}, \bmod (p^m, Y_1^{p^m}, \cdots, Y_n^{p^m}).$$

Hence,

$$\theta_m(ab) = \sum \bar\theta(a_i)\bar\theta(b_j) u_i^{p^{2m^2+1}} u_j^{p^{2m^2+1}} + (p^m, Y_1^{p^m}, \cdots, Y_n^{p^m}),$$

or,

$$\theta_m(ab) = \theta_m(a)\theta_m(b).$$

Regarding $\theta_i(a+(p^i))$ as a set of elements in $R[[Y]]_n$ we have

LEMMA 5. *$\theta_m(a+(p^m)) \supset \theta_{m+1}(a+(p^{m+1}))$ for all integers a in K.*

PROOF. For each u_i in U, $u_i^{p^{4m+2}} \equiv \sum c_j u_j$, mod p. Hence, $(u_i^{p^{4m+2}})^{p^{2m^2+1}} \equiv (\sum c_j u_j)^{p^{2m^2+1}}$, mod p^{2m^2+1}. By [4, Lemma 1] this becomes

$$u_i^{p^{2(m+1)^2+1}} \equiv \sum_{t=0}^{2m^2} p^t \sum s_{i,t,k}\, c_{i,t,k}^{p^{2m^2+1-t}} u_k^{p^{2m^2+1}}, \bmod p^{2m^2+1}.$$

Thus we have, for a in R,

$$a + (p^{m+1}) = \sum b_r u_r^{p^{2(m+1)^2+1}} + (p^{m+1}),$$
$$= \sum b_r \sum_{t=0}^{2m^2} p^t \sum s_{r,t,k}\, c_{r,t,k}^{2m^2+1-t} u_k^{p^{2m^2+1}} + (p^{m+1}).$$

Hence,

$$\theta_m[a + (p^m)]$$
$$= \sum_r \bar\theta(b_r) \sum_{t=0}^{2m^2} p^t \sum s_{r,t,k}\, c_{r,t,k}^{p^{2m^2+1-t}} u_k^{p^{2m^2+1}} + (p^m, Y_1^{p^m}, \cdots, Y_n^{p^m})$$
$$= \sum \bar\theta(b_r) u_r^{p^{2(m+1)^2+1}} + (p^m, Y_1^{p^m}, \cdots, Y_n^{p^m}).$$

Also,

$$\theta_{m+1}[a + (p^{m+1})] = \sum \tilde{\theta}(b_r) u_r^{p^{2(m+1)^2+1}} + (p^{m+1}, Y_r^{p^{m+1}}, \cdots, Y_n^{p^{m+1}}).$$

The lemma follows.

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

In order to show that θ coincides with $\tilde{\theta}$ on K_1 we choose an integral element a in K_1. Then, one being in U, we have

$$\theta_m[a + (p^m)] = \tilde{\theta}(a) + (p^m, Y_1^m, \cdots, Y_n^m)$$

and thus

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

Finally we note that θ induces an embedding $\ominus'$ on k which coincides with $\ominus$ 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**, Theorem **1**] it follows that $\ominus' = \ominus$ and the theorem is proved.

A set $\{\Pi_I\}_{\mathcal{I}}$ 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**, Theorem **1**].

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

AN APPLICATION. Let Φ denote an automorphism on $R[[Y]]_n$. The ideal (p) is invariant under Φ, hence Φ induces, via H', an automorphism ϕ on $k[[X]]_n$. Let G represent the group of automorphisms of $R[[X]]_n$, and G_0 the "inertial" subgroup of α 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 ϕ be an automorphism on $k[[X]]_n$. Let ϕ_0 denote the restriction of ϕ to k. Then for a in k $\phi_0(a)=\sum_{I\in\mathcal{J}^*} a_I X^I$. The mapping $a\to a_{0,\ldots,0}$ is an automorphism Φ_0' on k which by a well known theorem is induced via H by an automorphism Φ' on R. Clearly $\phi_0=\phi'\phi_0'$ where ϕ' is the embedding mapping $a_{0,\ldots,0}\to\sum_{I\in\mathcal{J}^*} a_I X^I$ where again $\phi_0(a)=\sum_{I\in\mathcal{J}^*} a_I X^I$. Hence, by Theorem 1, there is an embedding mapping Φ' on R such that $\Phi_0=\Phi'\Phi_0'$ induces ϕ_0. We extend Φ_0 to an automorphism on $R[[Y]]_n$ in the natural way, i.e., let $\Phi(Y_i)=\sum_{I\in\mathcal{J}} a_{i,I} Y^I$ where the $a_{i,I}$ are so chosen that $\phi(X_i)=\sum_{I\in\mathcal{J}} H(a_{i,I})X^I$. The fact that ϕ is an automorphism and the manner in which the $\Phi(Y_I)$ are chosen assure that the endomorphism of $R[[X]]_n$ Φ determined by extending Φ_0 to all of $R[[X]]_n$ in the indicated manner is in fact an automorphism which induces ϕ. The remaining statement of the theorem is obvious.

Let S represent a complete regular local ring which is not ramified and let $u_1, \cdots, u_n$ 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 ith indeterminate or, in the unequal characteristic case S is isomorphic to $R[[X]]_{n-1}$ 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 $i=2, \cdots, n$.

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 $u_1, \cdots, u_n$ be a minimal basis for the maximal ideal M of S. If P_i denotes the ideal generated by $u_1, \cdots, u_i$ $(i=1, \cdots, n)$ then every automorphism of S/P_i is induced by an automorphism of S.*

REFERENCES

1. I. S. Cohen, *Structure of complete local rings*, Trans. Amer. Math. Soc. **59** (1946), 54–106.

2. N. Heerema, *Derivations and embeddings of a field in its power series ring*, Proc. Amer. Math. Soc. **11** (1960), 188–194.

3. ———, *Derivations and embeddings of a field in its power series ring*. II, Michigan Math. J. **8** (1961), 129–134.

4. ———, *Derivations on p-adic fields*, Trans. Amer. Math. Soc. **102** (1962), 346–351.

5. O. F. G. Shilling, *The theory of valuation*, Math. Surveys, No. 4, Amer. Math. Soc., Providence, R. I., 1950.

FLORIDA STATE UNIVERSITY