INERTIAL ISOMORPHISMS OF V-RINGS

N. HEEREMA

1. Introduction. Throughout this paper R and R_n will denote v-rings, that is, complete discrete rank-one valuation rings of characteristic zero, having a common residue field k of characteristic p. R is assumed unramified and R_n has ramification index n. Let π be a prime element in R_n. Then $R_n = R[\pi]$, where π is a root of an Eisenstein polynomial $f = x^n + pf_{n-1}x^{n-1} + \ldots + pf_0$ with coefficients in R and f_0 a unit. Thus R_n is inertially isomorphic to $R[[x]]/fR[(x)]$, that is, the rings are isomorphic by a mapping which induces the identity mapping on the common residue field. $R[[x]]$ represents the power series ring in the indeterminate x over R. In this paper we identify R_n with $R[[x]]/fR[[x]]$, R with its natural embedding in R_n, and π with $x + fR[[x]]$.

Let S be a local ring with maximal ideal M. Let $G_{S,r}$ represent the group of automorphisms α on S such that $\alpha(a) - a$ is in M^r for all $a \in S$. Let $H_{S,r}$ be the subgroup of $G_{S,r}$ having the additional property that $\alpha(a) - a$ is in M^{r+1} for a in M. We then have a sequence of ramification groups

$$G_{S,1} \supset H_{S,1} \supset G_{S,2} \supset H_{S,2} \supset \ldots, \tag{1}$$

each of which is a normal subgroup of the automorphism group of S. The elements of $G_{S,1}$ are called inertial automorphisms. Finally, an inertial embedding of R in R_n or in $R[[x]]$ is an isomorphism $R \to R_n(R \to R[[x]])$ which induces the identity mapping on the common residue field.

Some questions about mappings of rings R_n can be settled by lifting them to $R[[x]]$. For example, if k is perfect, then every automorphism of R_n lifts to $R[[x]]$. If R_n is tamely ramified, then this fact can be used to determine necessary and sufficient conditions for two such rings to be isomorphic in terms of the automorphism structure of k (**2**, Corollary 4). If R_p ($p \neq 2$) is an extension of R by a root of $f = x^p + pf_{p-1}x^{p-1} + \ldots + pf_0$, then the quotient field of R_p is normal over the quotient field of R if and only if the residue of $f_0/(p-1)f_{p-1}$ has a $(p-1)$th root in k (**9**, Theorem 4.15). This result is obtained by constructing suitable inertial automorphisms in $R[[x]]$ which induce automorphisms on R_n.

Thus, in this paper we investigate the relationship between inertial automorphisms of rings R_n and inertial automorphisms of $R[[x]]$. In particular, we show that, for $m = 1, 2, \ldots, \alpha$ in $G_{R_n,m}(H_{R_n,m})$ can be lifted to $G_{R[[x]],m}$ $(H_{R[[x]],m})$. This is a corollary to Theorem 1 which states that every inertial embedding of R in R_n lifts to an inertial embedding of R in $R[[x]]$. The former result gains significance from the analysis of inertial automorphisms of $R[[x]]$ found in (**6**).

Received January 19, 1966. This research was supported by NSF GP-1084.

https://doi.org/10.4153/CJM-1967-046-2 Published online by Cambridge University Press

Theorem 2 states that an isomorphism of R_n onto R'_n which leaves the common residue field fixed (an inertial isomorphism) can be lifted to an inertial automorphism on $R[[x]]$. Theorem 3 asserts that if R_n and R'_n are extensions of R by Eisenstein polynomials f and f', then R_n and R'_n are inertially isomorphic if and only if there is an infinite higher derivation $\{D^{(i,j)}\}_{i,j=0}^{\infty}$ (the definition follows) on $R[[x]]$ such that f and

$$\sum_{i,j=0}^{\infty} D^{(i,j)}(f')p^i x^j$$

are associate primes in $R[[x]]$.

Definition. An infinite higher derivation on two indices, defined on a ring S into a containing ring S', is a sequence of maps $\{D^{(i,j)}\}_{i,j=0}^{\infty}$ of S into S' with the following properties:

(i) $D^{(i,j)}(a + b) = D^{(i,j)}(a) + D^{(i,j)}(b)$,

(ii) $D^{(i,j)}(ab) = \sum_{\substack{r \leqslant i \\ s \leqslant j}} D^{(r,s)}(a)D^{(i-r,j-s)}(b)$,

(iii) $D^{(0,0)}$ is the identity map.

An infinite higher derivation $\{D^{(0)}, D^{(1)}, D^{(2)}, \ldots\}$ is similarly defined. The relationship between infinite higher derivations and inertial automorphisms of $R[[x]]$ is investigated in **(6)**.

Theorem 4 states that if R_n is tamely ramified (p does not divide n) every inertial embedding of R in R_n can be extended to an inertial automorphism on R_n. Theorem 5 identifies the factor groups of the ramification groups (1) in the case in which R_n is tamely ramified, completing in this particular case the analysis made by Neggers **(8**, Theorem 6**)**.

2. The Embedding Theorem. The symbols listed below appear repeatedly in the body of the paper and always have the meaning here given. Some have been introduced already. The others will be identified again when they first appear. Nevertheless they are collected here for ease of reference.

R: unramified v-ring.
$R[[x]]$: power series ring in indeterminate x over R.
R_n: $R[[x]]/fR[[x]]$, where f is an Eisenstein polynomial of degree n.
$\pi: x + fR[[x]]$.
k: common residue field of R and R_n.
(2) k_0: maximal perfect subfield of k.
R_0: complete subring of R having residue field k_0.
K_0: field of quotients of R_0.
M: maximal ideal of $R[[x]]$.
ϵ: identity map on a given ring.
η: natural map of a ring onto a residue class ring.
ϕ: inertial embedding of R in R_n.
t: inertial index of ϕ (see below).

Let S be a local ring with maximal ideal I and let S_1 be a subring of S. An isomorphism $\xi: S_1 \to S$ is said to have inertial index r if $(\xi - \epsilon)(S_1) \subset I^r$ but $(\xi - \epsilon)(S_1) \not\subset I^{r+1}$.

Let ϕ be an embedding of R in $R_n = R[[x]]/fR[[x]]$ where f is an Eisenstein polynomial of degree n. It is assumed that ϕ has inertial index $t > 0$. Our objective is the construction of an embedding θ of R in $R[[x]]$ which induces ϕ and has inertial index equal to or greater than t. We obtain θ as a limit of a sequence $\{\theta_1, \theta_2, \ldots\}$ of isomorphisms where $\theta_m: R/p^mR \to R[[x]]/M^m$ and the following coset inclusion holds:

$$\langle\theta_{m+1}(a + p^{m+1}R)\rangle \subset \langle\theta_m(a + p^mR)\rangle. \tag{3}$$

We shall frequently wish to regard cosets of residue class rings of $R[[x]]$ as subsets of $R[[x]]$. This view is indicated by the use of the grouping symbols $\langle\ \rangle$. The maps θ_m and ϕ induce isomorphisms $\bar{\theta}_m$ and $\bar{\phi}_m$, respectively, of R/p^mR into R_n/π^mR_n. We shall construct θ_m so that $\bar{\theta}_m = \bar{\phi}_m$. By virtue of (3) the sequence $\{\theta_m\}$ determines a limit map θ which will induce ϕ. The method used to construct θ is similar to that used to construct a derivation on R which induces a given derivation on k (**4**, Section 2). Thus, we shall omit some of the details. It should be mentioned that θ can also be obtained by use of the Teichmüller Embedding Process in a manner resembling the proof of I. S. Cohen's Embedding Theorem (**1**, Theorem 11 and Corollary 1).

The symbols k_0, R_0, and K_0 will represent the maximal perfect subfield of k, the complete subring of R with residue field k_0, and the quotient field of R_0 respectively.

LEMMA 1. *The restriction, ϕ_0, of ϕ to R_0 is the identity mapping.*

Proof. If ϕ_0 is not the identity mapping, it has inertial index $m > 0$. The mapping ϕ'_0 defined by $\phi'_0(a) = (\phi_0(a) - a)/\pi^m$ induces a derivation on k_0 into k, which, by definition of m, must be a non-trivial mapping. But k_0, being perfect, has no non-trivial derivations. Thus ϕ_0 must be the identity mapping.

Let $\mathfrak{S}$ represent a subset of R which maps biuniquely under η, onto a p-basis $\bar{\mathfrak{S}}$ for k. The set $\bar{\mathfrak{S}}$ is algebraically independent over k_0. Hence, $\mathfrak{S}$ is algebraically independent over K_0. We construct an isomorphism θ' of $R \cap K_0(\mathfrak{S})$ into $R[[x]]$ which will prove to be the restriction of θ to $R \cap K_0(\mathfrak{S})$. This is done as follows:

(i) θ' is the identity mapping on K_0,

(ii) $\theta'(s) = \phi'(s)$ for s in $\mathfrak{S}$, where $\eta\phi'(s) = \phi(s)$ and $\phi'(s) - s \in M^t$. A method for constructing $\phi'(s)$ is given below. We note, first, that conditions (i) and (ii) determine a homomorphism which satisfies the conditions:

$$\theta' - \epsilon(R \cap K_0(\mathfrak{S})) \subset M^t \tag{4}$$

and

$$\eta\theta'(a) = \phi(a), \qquad \text{for } a \text{ in } R \cap K_0(\mathfrak{S}). \tag{5}$$

https://doi.org/10.4153/CJM-1967-046-2 Published online by Cambridge University Press

It follows from (4) that θ' is in fact an isomorphism.

The elements $\phi'(s)$ are chosen in the following way. Let

$$s_0 + s_1 x + \ldots + s_{n-1} x^{n-1}$$

be the unique polynomial of degree less than n in $\langle \phi(s) - s \rangle$ and let $t = qn + r$ where $0 \leqslant r < n$. Then, since $\phi(s) - s$ is in $\pi^{qn+r} R_n$ we have

$$(6) \qquad \begin{aligned} s_i &= s_i' p_b, && \text{for } i > r, \\ s_i &= s_i' p^{q+1}, && \text{for } i \leqslant r. \end{aligned}$$

The coset of p in R_n contains an element $x^n u$ where

$$u = -(f_0 + f_1 x + \ldots + f_{n-1} x^{n-1})^{-1}.$$

We substitute $x^n u$ for p in (6), obtaining elements s_j'' such that

$$s''_0 + s''_1 x + \ldots + s''_{n-1} x^{n-1}$$

is in $M^t \cap \langle \phi(s) - s \rangle$. Thus we choose $\phi'(s)$ to be

$$s + s''_0 + s''_1 x + \ldots + s''_{n-1} x^{n-1}.$$

The extension of θ' to θ involves the procedure referred to at the beginning of §2. Let $\mathfrak{U}$ be a set of elements in R such that η maps $\mathfrak{U}$ biuniquely onto a basis $\bar{\mathfrak{U}}$ for k as a linear space over $k_0(\bar{\mathfrak{S}})$. The element 1 is assumed to be in $\mathfrak{U}$. Then, for any positive integer m, the set $\mathfrak{U}^{p^m}$ of p^mth powers of the elements in $\mathfrak{U}$ also maps onto a basis for k over $k_0(\bar{\mathfrak{S}})$ (**4**, p. 347). Thus if a is in R,

$$a = \sum_{i=1}^{r} a_i u_i^{p^m} \mod p^m,$$

where the u_i are in $\mathfrak{U}$, the a_i are in $R_0 \cap K_0(\mathfrak{S})$ and are uniquely determined, mod p^m. Thus, every coset of $p^m R$ has the form

$$(7) \qquad \sum a_i u_i^{p^m} + p^m R, \qquad a_i \in R \cap K_0(\mathfrak{S}), u_i \in \mathfrak{U},$$

a form which we shall use repeatedly below. We define θ_m: $R/p^m R \to R[[x]]/M^m$ by

$$(8) \qquad \theta_m(a + p^m R) = \sum \theta'(a_i) u_i^{p^m} + M^m.$$

The mapping θ_m is well defined since the a_i are unique, mod p^m. Moreover, θ_m preserves sums and has the following two properties:

$$(9) \qquad \theta_m(a + p^m R) = a + M^m \mod M^t,$$

and

$$(10) \qquad \theta_m(xy) = \theta_m(x)\theta_m(y).$$

Property (9) follows from (4) and we prove (10) below.

Let $x = \sum a_i u_i^{p^m} + p^m R$ and $y = \sum b_i u_i^{p^m} + p^m R$ using (7). Then

$$xy = \sum a_i b_j u_i^{p^m} u_j^{p^m} + p^m R.$$

But, using (7), we have $u_i u_j = \sum c_k u_k$, mod p, and, hence

$$u_i^{p^m} u_j^{p^m} = [\sum c_k u_k]^{p^m} \mod p^{m+1}.$$

By Lemma 1 of (**4**, p. 347) with $r = 0$ we have that

$$u_i^{p^m} u_j^{p^m} = \sum_{k=0}^{m-1} p^k \sum_l s_{i,j,k,l} c_{i,j,k,l}^{p^{m-k}} u_l^{p^m} \mod p^m,$$

where $s_{i,j,k,l}$ is a rational integer and $c_{i,j,k,l}$ is in $R \cap K_0(\mathfrak{S})$. Thus

$$xy = \sum_{i,j} a_i b_j \sum_{k,l} p^k s_{i,j,k,l} c_{i,j,k,l}^{m-k} u_l^{p^m} + p^m R$$

and

$$\theta_m(xy) = \sum \theta'(a_i b_j p^k s_{i,j,k,l} c_{i,j,k,l}^{p^{m-k}}) u_l^{p^m} + M^m.$$

Relation (4) implies the following:

$$\text{(11)} \qquad \theta'(c_{i,j,k,l}^{p^{m-k}}) = c_{i,j,k,l}^{p^{m-k}} \mod M^{m-k}.$$

Hence,

$$\begin{aligned}\theta_m(xy) &= \sum \theta'(a_i)\theta'(b_j) p^k s_{i,j,k,l} c_{i,j,k,l}^{p^{m-k}} u_l^{p^m} + M^m \\ &= \sum \theta'(a_i)\theta'(b_j) p_i^{p^m} u_j^{p^m} + M^m = \theta_m(x)\theta_m(y).\end{aligned}$$

Thus θ_m is a homomorphism and relation (9) implies the following lemma.

LEMMA 2. *The mapping θ_m defined by* (8) *is an isomorphism.*

LEMMA 3. *The mapping θ: $R \to R[[x]]$ given by*

$$\theta(a) = \bigcap_{m=1}^{\infty} \theta_m(a + p^m R)$$

is an embedding which agrees with θ' on $R \cap K_0(\mathfrak{S})$. Moreover, $\theta - \epsilon(R) \subset M^\iota$.

Proof. We first establish the relation (3) as follows. For each $u \in \mathfrak{U}$ we have $u^p = \sum c_i u_i$, mod p, where the c_i are in $R \cap K_0(\mathfrak{S})$. Thus $u^{p^{m+1}} = [\sum c_i u_i]^{p^m}$, mod p^m. Or, using Lemma 1 of (**4**, p. 347).

$$\text{(12)} \qquad u_i^{p^{m+1}} = \sum_{j=0}^{m-1} p^j \sum s_{i,j,k} c_{i,j,k}^{p^{m-i}} u_k^{p^m} \mod p^m.$$

Using (7), $a + p^{m+1}R = \sum b_i u_i^{p^{m+1}} + p^{m+1}R$ and, by (12),

$$a + p^m R = \sum b_i p^j s_{i,j,k} c_{i,j,k}^{p^{m-i}} u_k^{p^m} + p^m R.$$

With the aid of (11) we have that

$$\begin{aligned}\theta_m(a + p^m R) &= \sum \theta'(b_i) p^j s_{i,j,k} c_{i,j,k}^{p^{m-i}} u_k^{p^m} + M^m \\ &= \sum \theta'(b_i) u_i^{p^{m+1}} + M^m\end{aligned}$$

https://doi.org/10.4153/CJM-1967-046-2 Published online by Cambridge University Press

and

$$\theta_{m+1}(a + p^{m+1}R) = \sum \theta'(b_i)u_i^{p^{m+1}} + M^{m+1}.$$

Relation (3) follows. Since

$$\bigcap_{i=1}^{\infty} M^i = 0,$$

θ is well defined and is an isomorphism by Lemma 2. It follows from relation (9) and the definition of θ that $\theta - \epsilon(R) \subset M^i$. In particular, then, θ is an embedding. Since 1 is in $\mathfrak{U}$, we have $\theta_m(a) = \theta'(a) + M^m$ for a in $R \cap K_0(\mathfrak{S})$ and all m. Hence $\theta(a) = \theta'(a)$.

We wish to show finally that θ induces ϕ. Given a in R and some positive integer m, we have, using the form (7), $a = \sum a_i u_i^{p^m}$, mod p^m, where the a_i are in $R \cap K_0(\mathfrak{S})$. Thus,

$$\phi(a) = \phi(\sum a_i u_i^{p^m}) \mod p^m.$$

However, since ϕ is inertial,

$$\phi(u_i^{p^m}) = u_i^{p^m} \mod \pi^m;$$

thus,

$$\phi(a) = \sum \phi(a_i)u_i^{p^m} \mod \pi^m. \tag{13}$$

From relation (5) we have

$$\phi(a_i) = \theta'(a_i) + fR[[x]]. \tag{14}$$

Substitution of (14) in (13) and an appeal to the definition of θ yield

$$\phi(a) = \theta(a) + fR[[x]] \mod \pi^m.$$

This being true for arbitrary m, we have proved the following theorem.

THEOREM 1. *Every inertial embedding ϕ of R in R_n lifts to an embedding θ of R in $R[[x]]$. If, for some positive integer m, $\phi - \epsilon(R) \subset \pi^m R_n$, then θ can be chosen so that $\theta - \epsilon(R) \subset M^m$.*

3. Applications. We recall that an inertial isomorphism $\bar{\tau}$ of R_n into R_n' is one which induces the identity mapping on their common residue field.

THEOREM 2. *Every inertial isomorphism $\bar{\tau}$ of R_n onto R'_n can be lifted to an inertial automorphism τ on $R[[x]]$. If $\bar{\tau}(R) = R$, then τ can be chosen to agree with $\bar{\tau}$ on R.*

Proof. Let $\bar{\tau}$ be an inertial isomorphism of R_n onto R'_n. The mapping ϕ obtained by restricting $\bar{\tau}$ to R is an embedding of R in R'_n. We apply Theorem 1 and lift ϕ to an embedding θ of R in $R[[x]]$. If $\bar{\tau}(R) = R$ we may assume θ to be ϕ. We define τ by the conditions $\tau(a) = \theta(a)$ for a in R and $\tau(x)$ is the unique polynomial $g = pa_0 + a_1 x + \ldots + a_{n-1} x^{n-1}$ of degree less than n in $\langle \bar{\tau}(\pi) \rangle$.

https://doi.org/10.4153/CJM-1967-046-2 Published online by Cambridge University Press

Necessarily a_1 is a unit and the demonstration that τ, so defined, is an inertial automorphism is straightforward. Since $\bar{\tau}(a + fR[[x]]) = \tau(a) + fR[[x]]$ for a in R and $\bar{\tau}(x + fR[[x]]) = \tau(x) + fR[[x]]$, it follows that τ induces $\bar{\tau}$.

The following example illustrates the fact that rings R_n and R'_n can be isomorphic without being inertially isomorphic. Let R be the unramified v-ring with residue field GF(27), the field with 27 elements. Let R_{13} and R'_{13} be extensions of R by roots of the Eisenstein polynomials $x^{13} - 3a$ and $x^{13} - 3a^3$ where $\bar{a}$, the residue of a, is a primitive 26th root of unity. An inertial isomorphism of R_{13} onto R'_{13} has the identity mapping as its restriction to R. By Theorem 3 of **(2)** the identity mapping on R extends to an inertial isomorphism of R_{13} onto R'_{13} if and only if the equation $\bar{a}z^{13} = \bar{a}^3$ has a solution in GF(27). However $\bar{a}^2$ is a primitive 13th root of unity and cannot itself be a thirteenth power. Thus R_{13} and R'_{13} are not inertially isomorphic. However, the Frobenius automorphism τ on R such that $\overline{\tau(a)} = \bar{a}^3$ can be extended to an isomorphism of R_{13} onto R'_{13} **(2**, Theorem 3**)**.

COROLLARY 1. *Each automorphism in $G_{R_n,m}$ ($H_{R_n,m}$) can be lifted to a mapping in $G_{R[[x]],m}$ ($H_{R[[x]],m}$) for $m = 1, 2, \ldots$.*

Proof. We let $R'_n = R_n$ in Theorem 2 and modify the construction of τ as follows. Again, let ϕ represent the restriction of $\bar{\tau}$ to R. The assumption that $\bar{\tau}$ is in $G_{R_n,m}$ means that $\phi(a) - a$ is in $\pi^m R_n$ for all a in R. Thus, by Theorem 1, ϕ lifts to an embedding θ of R in $R[[x]]$ such that $\theta(a) - a$ is in M^m for all a in R. Let the automorphism τ on $R[[x]]$ be defined by

(i) $\tau = \theta$ on R

and

(ii) $\tau(x) - x \in \langle\bar{\tau}(\pi) - \pi\rangle \cap M^m$ if $\bar{\tau} \in G_{R_n,m}$

and $\tau(x) - x \in \langle\bar{\tau}(\pi) - \pi\rangle \cap M^{m+1}$ if $\bar{\tau} \in H_{R_n,m}$.

An element in $\langle\bar{\tau}(\pi) - \pi\rangle \cap M^m$ ($\langle\bar{\tau}(\pi) - \pi\rangle \cap M^{m+1}$) can be found by the process used to construct an element in $M^t \cap \langle\phi(s) - s\rangle$ (see the paragraph which contains (6)). The mapping τ so constructed induces $\bar{\tau}$ and is in $G_{R[[x]],m}$. If $\bar{\tau}$ is in $H_{R_n,m}$, then, by construction, τ is in $H_{R[[x]],m}$.

COROLLARY 2. *Let R_n and R'_n be tamely ramified extensions of R by roots of Eisenstein polynomials*

$$f = x^n + pf_{n-1}x^{n-1} + \ldots + pf_0$$

and

$$g = x^n + pg_{n-1}x^{n-1} + \ldots + pg_0$$

respectively. R_n and R'_n are inertially isomorphic if and only if $\eta(g_0f_0^{-1})$ is an nth power in the residue field k.

Proof. Let $\bar{\tau}$: $R'_n \to R_n$ be an inertial isomorphism. Then, by Theorem 2, $\bar{\tau}$ lifts to an inertial automorphism τ on $R[[x]]$ having the property

$$\tau(g) = f\sum w_i x^i. \tag{15}$$

https://doi.org/10.4153/CJM-1967-046-2 Published online by Cambridge University Press

Comparing the coefficients of x^0 and x^n on either side of (15), remembering that $\eta\tau(g_0) = \eta(g_0)$, we conclude that $\eta(g_0) = \eta(f_0 w_0)$ and $\eta(t_i^n) = \eta(w_0)$ where $\tau(x) = pt_0 + t_1 x + \ldots$. It follows that $\eta(g_0 f_0^{-1})$ is an nth power in k.

Conversely, if $\eta(g_0 f_0^{-1})$ is an nth power in k, then we consider the possibility of choosing $t_1, t_2, \ldots$ in R, t_1 a unit, so that there is a unit

$$\sum_{i=0}^{\infty} w_i x^i$$

for which

$$g(t_1 x + t_2 x^2 + \ldots) = f(x) \sum w_i x^i. \tag{16}$$

Equating coefficients on either side of (16), we obtain

$$pg_0 = pf_0 w_0, \tag{17, 0}$$

$$pF_i = p(f_0 w_i + \ldots + f_i w_0), \qquad 0 < i < n,$$

$$t_1^n + pF_n = w_0 + p\left(\sum_{j=0}^{n-1} f_j w_{n-j}\right), \qquad i = n, \tag{17, i}$$

$$nt_1^{n-1} t_{i-n+1} + G_{i-n} + pF_i = W_{i-n} + p\left(\sum_{j=0}^{n-1} f_j w_{i-j}\right), \qquad i > n,$$

where G_i and F_i are polynomials in $t_1, \ldots, t_i$ over R. Equality (17, 0) determines w_0. If $\eta(g_0 f_0^{-1})$ is an nth power in k, then $\eta(w_0)$ is an nth power and t_1 can be chosen so that $\eta(t_1^n) = \eta(w_0)$. We next choose w_1 so that (17, 1) is true. Suppose that $t_1, \ldots, t_r$ and $w_0, \ldots, w_r$ have been selected so that

(a) $(17.i)$ is true for $i = 0, \ldots, r$.

(b) $\eta[nt_1^{n-1} t_{i-n+1} + G_{i-n}] = \eta w_{i-n}$ for $i = n, \ldots, n + r - 1$. We choose t_{r+1} so that (b) holds for $i = n + r$ and then select w_{r+1} so that $(17, r + 1)$ is true. This selection is always possible since when $r \geqslant n$ condition (b) holds for $i = n, \ldots, n + r$, which includes $i = r$.

Corollary 2 is related to Theorem 3 of **(2)**, which states that a given automorphism on R extends to an isomorphism of R_n onto R'_n if and only if a condition similar to that of Corollary 2 is satisfied.

THEOREM 3. *Let R_n and R'_n be extensions of R by roots of Eisenstein polynomials f and f'. Then there is an inertial isomorphism of R_n onto R'_n if and only if there is an infinite higher derivation $\{D^{(i,j)}\}$ on $R[[x]]$, such that* (i) $1 + D^{(0,1)}(x)$ *is a unit and* (ii) f' *and*

$$\sum_{i,j=0}^{\infty} D^{(i,j)}(f') p^i x^j$$

are associate primes.

Proof. This is an immediate consequence of Theorem 2 and the fact that every inertial automorphism on $R[[x]]$ is of the form

$$A \to \sum_{i,j=0}^{\infty} D^{(i,j)}(A) p^i x^i$$

for some infinite higher derivation $\{D^{(i,j)}\}$ on $R[[x]]$ such that $1 + D^{(0,1)}(x)$ is a unit (**6**, Theorem 31).

The following theorem offers a sufficient condition on R_n that every embedding of R in R_n be extendable to an inertial automorphism. It is clearly not necessary since if k is perfect the only embedding of R in R_n is the identity mapping which does extend to an inertial automorphism.

THEOREM 4. *If R_n is tamely ramified, every inertial embedding of R in R_n can be extended to an inertial automorphism on R_n.*

Proof. Let ϕ be an inertial embedding of R in $R_n = R[[x]]/fR[[x]]$. We lift ϕ to an embedding θ of R in $R[[x]]$. If we extend θ to an inertial automorphism τ on $R[[x]]$ with the property that $\tau(f)$ is a multiple of f, then τ will induce an inertial automorphism $\bar{\tau}$ on R_n which is an extension of ϕ. To this end we define τ on $R[[x]]$ to agree with θ on R and let $\tau(x) = t_1 x + t_2 x^2 + \ldots$, where the t_i must be so chosen that t_1 is a unit and

$$\tau(f) = f\sum w_i x^i. \tag{18}$$

Equations (17) and the argument which follows them now apply with one modification: $pg_0 = pf_0 w_0$ becomes $pf_0 + p^2 a = pf_0 w_0$, where a is some element in R independent of $t_1, t_2, \ldots$. We note that in the present case $\eta(w_0) = 1$ and hence $\eta(t_1)$ is an nth root of unity. Moreover, we need to note for the proof of Theorem 5 that t_1 may be chosen arbitrarily save for this condition.

The author is indebted to the referee for supplying an example on which the following inertial embedding is based, an inertial embedding which does not extend to an inertial automorphism. Let k be any field which is not perfect. Choose a in R so that its residue $\eta(a) = \bar{a}$ is not in k^p and let $R_p = R[\pi]$ where π is a root of $x^p - pa$. Let $\{d^{(0)}, d^{(1)}, d^{(2)}, \ldots\}$ be a higher derivation on k such that $d^{(1)}(\bar{a}) = 1$ and $d^{(i)}(\bar{a}) = 0$, for $i > 1$ (**3**, Theorem 1). We lift $\{d^{(i)}\}$ to a higher derivation $\{D^{(i)}\}$ on R (**5**, Corollary 1). Thus $D^{(i)}$ induces $d^{(i)}$, via η, for all i. The mapping ϕ: $R \to R_b$ given by $\phi(b) = \sum \pi^i D^{(i)}(b)$ is an inertial embedding. If ϕ can be extended to an inertial automorphism ζ on R_b, then $\zeta(pa)$ $(= pa + \eta\pi, \bmod \pi^{p+2})$ must be a pth power in R_b. Thus, we assume there is a unit u such that

$$(u\pi)^p = pa + p\pi \mod \pi^{p+2} \quad \text{or} \quad (u^p - 1)\pi^p = p\pi \mod \pi^{p+2}.$$

This requires that $u^p - 1$ be in πR_p and not in $\pi^2 R_p$. But $u^p - 1 = (u - 1)^p$, mod π^p, and $(u - 1)^p$ is a unit or is in π^p. We have arrived at a contradiction.

It was first shown by MacLane (**7**, Corollary to Theorem 15) that

$$G_{R,m}/G_{R,m+1}, \qquad m = 1, 2, \ldots,$$

is isomorphic to the additive group of derivations of k. Since $\alpha(p) = p$ for every automorphism α of R, it follows that $H_{R,m} = G_{R,m}$ for all m. Neggers has shown (**8**, Theorem 6) that for $m \geqslant n + p/p - 1$, $H_{R_n,m}/G_{R_n,m+1}$ is isomorphic to the additive group of those derivations on k each of which lifts to R_n. He observed that if R_n is tamely ramified over R, then every derivation on k lifts to R_n (**8**, Corollary 2). The following result extends that of Neggers.

THEOREM 5. *If R_n is tamely ramified, then, for $m = 2, 3, \ldots$, $G_{R_n,m} = H_{R_n,m}$ and $G_{R_n,m}/G_{R_n,m+1}$ is isomorphic to the additive group of derivations on k, as is $H_{R_n,1}/G_{R_n,2}$. $G_{R_n,1}/H_{R_n,1}$ is isomorphic to the group of nth roots of unity in k.*

Proof. We show first that if $m > 1$, then $G_{R_n,m} = H_{R_n,m}$. It is sufficient to show that $\alpha(\pi') - \pi'$ is in $\pi^{m+1}R_n$ for all α in $G_{R_n,m}$ and some prime element π' of R_n. We choose π' to be an nth root of some prime element pb in R, b a unit (**2**, Corollary 3). Now α in $G_{R_n,m}$ has the form $\epsilon + \pi^m\alpha'$ where ϵ is the identity map. Thus,

$$\alpha(\pi')^n = (\pi' + \pi^m\alpha'(\pi'))^n = p(b + \pi^m\alpha'(b)),$$

or, expanding the left side, we obtain

$$(\pi')^n + n(\pi')^{n-1}\pi^m\alpha'(\pi') + \ldots = pb + p\pi^m\alpha'(b).$$

Since $m > 1$, the remaining terms on the left side are all in $\pi^{n+m}R_n$. Hence $n\pi^{n+m-1}\alpha'(\pi') - p\pi^m\alpha'(b) \in \pi^{n+m}R_n$. Since n is prime to p, it follows that $\alpha'(\pi')$ is in πR_n or $\alpha(\pi') - \pi' \in \pi^{m+1}R_n$.

In order to determine $H_{R_n,1}/G_{R_n,2}$ and $G_{R_n,m}/G_{R_n,m+1}$, for $m > 1$, we let α be an automorphism in $H_{R_n,m}$ ($=G_{R_n,m}$ for $m > 1$). Again, $\alpha = \epsilon + \pi^m\alpha'$ and a simple calculation shows that α' induces a derivation d_α on k. The correspondence ξ: $\alpha \to d_\alpha$ maps $H_{R_n,m}$ homomorphically into the additive group of derivations on k with kernel $G_{R_n,m+1}$. To demonstrate that ξ is onto let d be any derivation on k. There is an infinite higher derivation $\{d^{(i)}\}$ on k such that $d^{(1)} = d$ (**3**, Theorem 1). We lift $\{d^{(i)}\}$ to an infinite higher derivation $\{D^{(i)}\}$ on R (**5**, Corollary 1). The correspondence ϕ: $R \to R[[x]]$ given by

$$\phi(a) = \sum_{i=0}^{\infty} D^{(i)}(a)x^{mi}$$

is an inertial embedding. We need to extend ϕ to an inertial automorphism τ on $R[[x]]$ such that $\tau(f) \in fR[[x]]$ and

$$\tau(x) = x + x^{m+1}(t_0 + t_1 xt \ldots) \tag{19}$$

for then τ will induce $\bar{\tau}$ in $H_{R_n,m}$, and $\xi(\bar{\tau})$ will be d.

In view of (19) and the fact that $\phi(a) - a$ is in $x^mR[[x]]$, we can replace the condition (18) by

$$\tau(f) - f = f\sum_{i=m}^{\infty} w_i x^i. \tag{20}$$

https://doi.org/10.4153/CJM-1967-046-2 Published online by Cambridge University Press

The proof that $t_0, t_1, \ldots$ can be chosen so that (20) holds for some series

$$\sum_{i=m}^{\infty} w_i x^i$$

goes much like the proof of Theorem 4. We let

$$\tau(f) - f = \sum_{i=m}^{\infty} a_i x^i.$$

Then $a_m \in pR$,

$$a_i = pF_i(t_0 \ldots t_{i-m-1}), \qquad \text{for } m < i < m + n,$$

and

$$a_i = nt_{i-m-n} + G_i(t_0 \ldots t_{i-m-n-1}) + pF_i(t_0 \ldots t_{i-m-1}), \qquad \text{for } i \geqslant m + n,$$

where again F_i and G_i are polynomials over R in the indicated quantities. A modification of the argument following (17) establishes the existence of the desired τ.

To determine G_1/H_1 we map α in G_1 onto $\xi(\alpha) = \eta(t_1)$ where $\alpha(\pi) = t_1 \pi$. The correspondence ξ is a homomorphism into the group of nth roots of unity in k and has kernel H_1. In view of the observation at the end of the proof of Theorem 4, ξ is onto.

REFERENCES

1. I. S. Cohen, *Structure of complete local rings*, Trans. Amer. Math. Soc., *59* (1946), 54–106.
2. N. Heerema, *On ramified complete discrete valuation rings*, Proc. Amer. Math. Soc., *10* (1959), 490–496.
3. ——— *Derivations and embeddings of a field in its power series ring, 11*, Michigan Math. J., *8* (1961), 129–134.
4. ——— *Derivations on p-adic fields*, Trans. Amer. Math. Soc., *102* (1962), 346–351.
5. ——— *Embeddings of a p-adic field and its residue field in their power series rings*, Proc. Amer. Math. Soc., *14* (1963), 37–43.
6. ——— *Derivations and inertial automorphisms of complete regular local rings*, Amer. J. Math., *88* (1966), 33–42.
7. S. MacLane, *Subfields and automorphism groups of p-adic fields*, Ann. of Math., 40 (1939), 423–442.
8. J. Neggers, *Derivations on $\bar{p}$-adic fields*, Trans. Amer. Math. Soc., *115* (1965), 496–504.
9. E. Wishart, *Higher derivations on $\bar{p}$-adic fields*, Dissertation, Florida State University (1965).

Florida State University