INERTIAL AUTOMORPHISMS OF A CLASS OF WILDLY RAMIFIED v-RINGS

BY NICKOLAS HEEREMA(1)

I. Introduction. Let R_e be a ramified v-ring with ramification e. That is, R_e is a complete, discrete, rank one, valuation ring having characteristic zero with residue field k of characteristic p ($p \neq 0$, 2) and pR_e is the eth power of the maximal ideal M of R_e . Let \mathfrak{G} represent the group of automorphisms of R_e , e being the identity map. Then, for i > 0, $\mathfrak{G}_i = \{\alpha \mid \alpha \in \mathfrak{G}; \alpha = e, \text{ mod } M^i\}$ and $\mathfrak{G}_i = \{\alpha \mid \alpha \in \mathfrak{G}_i, \alpha(m) - m \in M^{i+1} \text{ for } m \in M\}$. The ramification groups \mathfrak{G}_i and \mathfrak{F}_i are invariant in \mathfrak{G} . The object of this paper is to evaluate the factor groups of the series (1) of

ramification groups in that case in which e = p. A second objective is the determination of those automorphisms in \mathfrak{G}_1 which are derivation automorphisms (see below).

Neggers has shown [3, Theorem 6] that for any e and $i \ge (e+p)/(p-1)$, $\mathfrak{G}_i/\mathfrak{G}_{i+1}$ is isomorphic to $\mathscr{D}(R_e)/\pi\mathscr{D}(R_e)$ where $\mathscr{D}(R_e)$ is the additive group of derivations on the ring R_e and $\pi\mathscr{D}(R_e) = \{\pi d \mid d \in \mathscr{D}(R_e)\}$ where π is a prime element in R_e . In addition he proved that $\mathfrak{F}_i/\mathfrak{G}_{i+1}$ is isomorphic to the additive group of those derivations on k which lift to R_e where again $i \ge (e+p)/(p-1)$. The map used by Neggers to evaluate $\mathfrak{G}_i/\mathfrak{G}_{i+1}$ also shows that if $i \ge (e+p)/(p-1)$, then $\mathfrak{G}_i/\mathfrak{F}_i$ is isomorphic to $\mathscr{D}(R_e)/\mathscr{D}^*(R_e)$ where $\mathscr{D}^*(R_e) = \{d \mid d \in \mathscr{D}(R_e), d(\pi) \in \pi R_e\}$ [3, proof of Theorem 6]. The principal tool of this investigation is the convergent higher derivation [2]. Let $D = \{D_i\}_{i=1}^\infty$ be a higher derivation on $R_e(D_i(R_e) \subseteq R_e)$ for i > 0. D is convergent if, for $a \in R_e$, $\sum D_i(a)$ is a convergent series in the π -adic topology. If D converges the map α_D : $a \to \sum_{i=0}^\infty D_i(a)(D_0(a) = a)$ is an inertial automorphism (see Theorem B). The group \mathfrak{G}_D of all derivation automorphism α_D is an invariant subgroup of \mathfrak{G} .

Throughout this paper R will denote a v-ring in R_e such that $[R_e:R]=e$, and R is unramified. Thus R has the same residue field k as R_e . For a in R_e , \bar{a} will denote the image of a under the natural map of R_e onto k, π always represents a prime element in R_e . We have

$$\pi^e + pu = 0, \quad \bar{u} \neq 0.$$

If e = p and $\bar{u} \in k^p$ then π can be chosen so that

(3)
$$\pi^p + p(1 + \pi^t v) = 0, \quad t > 0, \quad \bar{v} \neq 0,$$

or $\pi^p + p = 0$. We note that the conditions

(4)
$$\bar{u} \notin k^p$$
; $t = p$ and $\bar{v} \notin k^p$; as well as \bar{v} if $1 \le t < p$

Presented to the Society, September 1, 1967; received by the editors February 16, 1967.

(1) This research supported by NSF GP-4007.

are all independent of the choice of π , assuming (3) to be satisfied for all but the first listed. Throughout this paper the symbols u and v will represent the quantities given in (2) and (3). The considerations (4) determine, to a large extent, the structure of the groups (1) as is seen in the following two theorems which summarize the results of this study. $\mathfrak{G}(R_p; R)$ is the group of automorphism of R_p over R.

THEOREM 1. Every inertial automorphism on R_p is a derivation automorphism, i.e. $\mathfrak{G}_1 = \mathfrak{G}_D$, unless $\bar{u} \in k^p$ and t = p - 1, in which case the following are equivalent.

- (a) \bar{v} is a (p-1)th root in k.
- (b) R_p is Galois over R.
- (c) $\mathfrak{G}_2 \neq \mathfrak{H}_2$.
- (d) $\mathfrak{G}_2|\mathfrak{F}_2$ is the group of order p.

If R_p is Galois over R then $\mathfrak{G}(R_p; R) \subset \mathfrak{G}_D$ if and only if $\bar{v} \notin k^p$. In any case, $\mathfrak{G}_1 = \mathfrak{G}_D \cdot \mathfrak{G}(R_p; R)$.

THEOREM 2. If $\bar{u} \notin k^p$ then for $i \geq 1$, $\mathfrak{F}_i/\mathfrak{G}_{i+1}$ is isomorphic to the subgroup $\overline{\mathscr{D}}$ of those $\delta \in \mathscr{D}(k)$ which lift to R_p . Also, $\overline{\mathscr{D}} = \{\delta \mid \delta \in \mathscr{D}(k), \delta(\bar{u}) = 0\}$. In this case $\mathfrak{G}_i/\mathfrak{F}_i$ is isomorphic to k^+ , the additive group of k.

If $\bar{u} \in k^p$, then for $i \ge 1$, $\mathfrak{S}_i/\mathfrak{S}_{i+1}$ is isomorphic to $\mathfrak{D}(k)$ unless t=p and i=1. If t=p, $\mathfrak{S}_1/\mathfrak{S}_2$ is isomorphic to the subgroup of those $\delta \in \mathfrak{D}(k)$ such that $\delta(\bar{v})=0$. Also, $\mathfrak{S}_i=\mathfrak{S}_i$, $i \ge 1$, unless t=p-1, i=2 and one of the four equivalent conditions of Theorem 1 holds.

By Neggers' results referred to above [3, 'proof of Theorem 6] we have

COROLLARY. $\mathcal{D}(R_p)/\mathcal{D}^*(R_p)$ is isomorphic to k^+ if $\bar{u} \notin k^p$ and is trivial if $\bar{u} \in k^p$.

II. **Proofs.** For S a subring of R_e , the symbols $\mathcal{H}(S, R_e)$, $\mathcal{H}_c(S, R_e)$ and $\mathcal{H}_u(S, R_e)$ will stand for the set of all higher derivations, all convergent higher derivations, and all uniformly convergent higher derivations with domain S and range R_e . We quote the following two theorems which will be used repeatedly. Theorem A provides the necessary freedom in the construction of $D \in \mathcal{H}_u(R_e, R_e)$. Theorem B implies that if $D \in \mathcal{H}_c(R_e, R_e)$, then α_D is indeed an inertial automorphism.

THEOREM A [2, Theorem 4]. Let $\overline{\mathcal{G}}$ be a p-basis for k and let $\mathcal{G} \subset R$ be a set of representatives of the elements of $\overline{\mathcal{G}}$. If I is the set of positive integers and f is a mapping from $\mathcal{G} \times I$ into R_e then there is one and only one $D \in \mathcal{H}(R, R_e)$ such that $D_i(s) = f(s, i)$ for all $s \in \mathcal{G}$ and $i \in I$. Moreover, D converges (uniformly) if and only if D converges (uniformly) on \mathcal{G} .

THEOREM B [2, Lemmas 1 and 5]. If D is in $\mathscr{H}_c(R_e, R_e)$ then $D_i(R_e) \subseteq \pi R_e$ and $D_i(\pi R_e) \subseteq \pi^2 R_e$ for i > 0.

Theorems 1 and 2 will be proved by means of a series of lemmas.

LEMMA 1. If $\mathscr S$ is a set of representatives in R of a p-basis $\overline{\mathscr S}$ for k and D in $\mathscr H(R,R_e)$ is such that $D_j(\mathscr S) \subset \pi^{t_j} R_e \subset \pi R_e$, $j \ge 1$, then $D_i(R) \subset \pi^{q_i} R_e$ where

$$q_i = \min_{\substack{j_1 + \cdots + j_i = i; t_0 = 0}} (t_{j_1} + \cdots + t_{j_i}), \quad i \ge 1.$$

Proof. For a given i we choose n sufficiently large so that $D_j(R^{p^n}) \subseteq \pi^{q_i} R_e$ for $j=1,\ldots,i$ [2, Lemma 6] where R^{p^n} is the subring of R generated by the p^n th powers of elements in R. Since every element in k has a representative in $R^{p^n}[\mathscr{S}]$, it follows that $R=R^{p^n}[\mathscr{S}]+p^{q_i}R$. If $b=as_1,\ldots,s_r$ where $a\in R^{p^n}$ and $s_1,\ldots,s_r\in\mathscr{S}$ then

$$D_{i}(b) = \sum_{i_{0} + \cdots + i_{r} = i} D_{i_{0}}(a)D_{i_{1}}(s_{1}), \ldots, D_{r}(s_{r})$$

is seen to be in $\pi^{q_i}R$ and hence, since $D_i(p^{q_i})=0$ for all j, $D_i(R) \subseteq \pi^{q_i}R_e$.

Let α , an automorphism of R_e , be in \mathfrak{F}_i , $i \ge 1$. Then $\alpha(a) = a + \pi^i \alpha^*(a)$ and the mapping α^* induces a derivation δ_{α} on k. The mapping

$$\phi_i \colon \alpha \to \delta_\alpha$$

is a homomorphism of \mathfrak{F}_i into $\mathfrak{D}(k)$ with kernel \mathfrak{G}_{i+1} .

LEMMA 2. If an automorphism α of R_p is in \mathfrak{F}_i , then $\delta_{\alpha}(\bar{u}) = 0$. If $\pi^p + p(1 + \pi^p v) = 0$, then $\delta_{\alpha}(\bar{v}) = 0$ for α in \mathfrak{F}_1 .

Proof. Since $\alpha(\pi) - \pi \in \pi^{i+1}R_p$ it follows that $\alpha(\pi^p) - \pi^p \in \pi^{p+i+1}R_p$. Thus by (2) $\alpha(u) - u$ is in $\pi^{i+1}R_p$ or $\alpha^*(u) \in \pi R_p$ which implies $\delta_{\alpha}(\bar{u}) = 0$. In the remaining case let $\alpha(\pi) = \pi + \pi^2 b$. Then $\alpha(\pi^p) - \pi^p \equiv \pi^{2p} b^p$, mod $\pi^{2p+1}R_p$, and $\alpha(p(1+\pi^p v)) - p(1+\pi^p v) \equiv p\pi^{p+1}\alpha^*(v)$, mod $\pi^{2p+2}R_p$. Hence $b \in \pi R_p$ and it follows that $\alpha^*(v) \in \pi R_p$ or $\delta_{\alpha}(\bar{v}) = 0$.

Given D and H in $\mathcal{H}(R_e, R_e)$, $D \circ H$ in $\mathcal{H}(R_e, R_e)$ is given by

$$(D\circ H)_{\mathfrak{i}}=\sum_{j=0}^{\mathfrak{i}}D_{j}H_{\mathfrak{i}-j}.$$

 $\mathcal{H}(R_e, R_e)$ is a group with respect to this composition and $\mathcal{H}_c(R_e, R_e)$, $\mathcal{H}_u(R_e, R_e)$ are subgroups [2, Theorems 1, 2]. Moreover, one can verify directly that, for D and H in $\mathcal{H}_c(R_e, R_e)$, $\alpha_{D \circ H} = \alpha_D \alpha_H$.

LEMMA 3. Let $\{D^{(n)}\}_{n=1}^{\infty}$ where $D^{(n)} \in \mathcal{H}_c(R_e, R_e)$ be such that $D_i^{(n)}(R_e) \subset \pi^{s_n} R_e$, $i \ge 1$, $n \ge 1$, and $\lim_n s_n = \infty$. Let $\alpha_n = \alpha_D^{(1)}, \ldots, \alpha_D^{(n)}$ and $\overline{D}^{(n)} = D^{(1)} \circ \cdots \circ D^{(n)}$. Then $\lim_n \alpha_n(a)$ and $\lim_n \overline{D}_i^{(n)}(a)$ exist for all i > 0 and $a \in R_e$. Moreover, $\alpha: a \to \lim_n \alpha_n(a)$ is an automorphism, $D = \{D_i\}$ is in $\mathcal{H}_c(R_e, R_e)$ where $D_i(a) = \lim_n \overline{D}_i^{(n)}(a)$ and $\alpha = \alpha_D$. If $D^{(n)} \in \mathcal{H}_u(R_e, R_e) n \ge 1$, then $D \in \mathcal{H}_u(R_e, R_e)$.

Proof. By definition of product in $\mathcal{H}_c(R_e, R_e)$ we have

$$D_n^{(m+1)}(a) - D_n^{(m)}(a) = \sum_{i_1 + \cdots + i_{m+1} = n; i_{m+1} \neq 0} D_{i_1}^{(1)} \cdots D_{i_{m+1}}^{(m+1)}(a),$$

the right side of which is in $\pi^{s_{m+1}}R_e$ since for $D \in \mathcal{H}_c(R_e, R_e)$, $D_i(\pi^nR_e) \subset \pi^nR_e$ for all i and n by Theorem B. Thus, $\alpha_{m+1}(a) - \alpha_m(a) = \sum_{i=0}^{\infty} \overline{D}_i^{(m+1)}(a) - \sum_{i=0}^{\infty} \overline{D}_i^{(m)}(a) \in \pi^{s_{m+1}}R_e$. The rest of the lemma follows directly.

Since R_p is totally ramified over R and $[R_p:R]=p$ then $R_p=R[\pi]$ and the minimal polynomial f(x) of π over R is an Eisenstein polynomial, that is,

(6)
$$f(x) = x^{p} + pa_{p-1}x^{p-1} + \dots + pa_{1}x + pa_{0}$$

and a_0 is a unit. Clearly, $\bar{a}_0 = \bar{u}$ (see (2)). Also, if $\bar{u} \in k^p$ then $a_0 = b^p + pc$ where b and c are in R. By replacing π with $b^{-1}\pi$ we can assume that

(7)
$$a_0 = 1 + pb_0.$$

We note next that every $D \in \mathcal{H}(R, R_e)$ extends uniquely to a higher derivation D of the quotient field of R_e . Also, $D(R_e) \subset R_e$ if and only if $D(\pi) \in R_e$. If D converges on R, D will converge on R_e if and only if D converges at π [2, Lemma 3].

Let (r, s) denote an ordered set of r nonnegative integers whose sum is s and let |(r, s)| represent the largest integer in (r, s). We let $\sum_{(q, s)} D(a_1, \ldots, a_q)$ denote the sum of all products $D_{i_1}(a_1)D_{i_2}(a_2)\cdots D_{i_q}(a_q)$ such that $i_1+\cdots+i_q=s$ and $i_j \ge 0$. Also, f'(x) and $f^{D_i}(x)$ represent respectively the ordinary derivative of f and the polynomial obtained by replacing each coefficient in f with its image under D_i . With these conventions it is useful to write the expression for $D_i(\pi)$ derived from $D_i(f(\pi))=0$ as follows:

(8, i)
$$f'(\pi)D_{i}(\pi) = f^{D_{i}}(\pi) + \sum_{(p,i); |(p,i)| < i} D(\pi, \dots, \pi) + \sum_{j=0}^{p-1} p \sum_{(j+1,i); |(j+1,i)| < i} D(a_{j}, \pi, \dots, \pi).$$

Let v represent the exponential valuation on R_p . Note that $p \le v(f'(\pi)) \le 2p-1$.

LEMMA 4. A given $\delta \in \mathcal{D}(k)$ lifts to $d \in \mathcal{D}(R_p)$ if and only if $\delta(\bar{u}) = 0$.

Proof. A derivation $d \in \mathcal{D}(R_p)$ induces a derivation on k under the natural map of R_p onto k only if $d(\pi) \subseteq \pi R_p$. But $d(f(\pi)) = 0$ means $d(\pi) = -f^d(\pi)/f'(\pi)$. Thus $f^d(\pi) \in \pi^{p+1}R_p$ which means $d(a_0) \in \pi R_p$ and, hence, if d induces δ on k, $\delta(\bar{a}_0) = \delta(\bar{u}) = 0$. Conversely, every $\delta \in \mathcal{D}(k)$ lifts to d' on R [1, Theorem 1]. If $\delta(\bar{u}) = 0$, $d'(a_0) \in pR$ which means that $f^{d'}(\pi)/f'(\pi) \in \pi R_p$. Thus the extension d, of d', to R_p is in $\mathcal{D}(R_p)$ and induces δ since d' does.

LEMMA 5. Let $D \in \mathcal{H}_c(R, R_p)$ where $R_p = R[\pi]$ and $f(x) = x^p + \sum_{i=0}^{p-1} pa_i x^i$ is the minimum function of π over R. Let q > 2, $n \ge 1$, and m > p(n-1) be integers such that, using the same symbol for the extension of D to R_p ,

$$(9,1) D_{j}(\pi) \in \pi^{2}R_{p} if j < n,$$

$$(9,2) D_j(\pi) \in \pi^q R_p if n \leq j < m,$$

and, if $j \ge n$

(9, 3)
$$D_{i}(a_{s}) \in f'(\pi)\pi^{q-p-s}.$$

If q=3 then (9, 3) is assumed to hold only for $j \ge m$. Under these assumptions $\sum D_j(\pi)$ converges and $\sum_{j=n}^{\infty} D_j(\pi) \in \pi^q R_p.$

The proof of this lemma consists of checking the valuation v of the terms on the right side of (8). We show first that if $j \ge m$,

$$(10) D_i(\pi) \in \pi^q R_n.$$

Thus assuming (10) true for j < r where $r \ge m$ we consider (8, r). By (9, 3) $f^{D_r}(\pi)$ is in $f'(\pi)\pi^q R_p$. The term $D_{i_1}(\pi) \cdots D_{i_p}(\pi)$ of $A_r = \sum_{(p,r):|(p,r)| < r} D(\pi, \ldots, \pi)$ is in $\pi^{p+q}R_p$ in view of the fact that at least one $i_j > n$ and another is different from zero. The above term appears in A_r a multiple of p times unless $i_1 = i_2 = \cdots = i_p = r/p$ in which case it is in $\pi^{pq}R_p \subset f'(\pi)\pi^q R_p$, since $v(f'(\pi)) \le 2p-1$ and $p \ne 2$. Thus $A_r \in f'(\pi)\pi^q R_p$. A similar argument shows B_r , the remaining term on the right side of (8, r), to be in $f'(\pi)p^q R_p$. Thus by (8, r) $D_r(\pi) \in \pi^q R_p$.

Given $i \ge 0$, we assume for some integer $s \ge m$ that if j > s, then $D_j(\pi) \in \pi^{i+q} R_p$ and, for $h = 0, \ldots, p-1$

(11)
$$D_i(a_h) \in f'(\pi)\pi^{i+q-p+1}R_p.$$

Let s'=ps and let j>s'. Then $f^{D_j}(\pi) \in f'(\pi)\pi^{i+q+1}R_p$ and, by an analysis like that above, A_j and B_j are seen to be in $f'(\pi)\pi^{i+q+1}R_p$. Thus $D_j(\pi) \in \pi^{i+q+1}R_p$. Since D converges on R, given $i \ge 0$, there is an s such that (11) holds for j>s. It follows that $\sum D_j(\pi)$ converges, and in view of (10) $\sum_{j=n}^{\infty} D_j(\pi) \in \pi^q R_p$.

LEMMA 6. If $\alpha \in \mathfrak{H}_i$, $i \geq 1$, then there is a $D \in \mathcal{H}_u(R_p, R_p)$ such that $\alpha^{-1}\alpha_D \in G_{i+1}$. Moreover, $\mathfrak{H}_i/\mathfrak{G}_{i+1}$ is isomorphic to the subgroup of those δ in $\mathfrak{D}(k)$ for which $\delta(\bar{u}) = 0$ with the following exception. If $\bar{u} \in k^p$ and, for suitable choice of π we have $\pi^p = p(1 + \pi^p v)$ then $\mathfrak{H}_i/\mathfrak{G}_2$ is isomorphic to the subgroup of those

$$\delta \in \mathcal{D}(k) \ni \delta(\bar{v}) = 0.$$

Proof. By Lemma 2, it will be sufficient to find $D \in \mathcal{H}_u(R_p, R_p)$ such that $\phi_i(\alpha_D)$ (see (5)) is a given δ for which $\delta(\bar{u}) = 0$, or, in the exceptional case, $\delta(\bar{v}) = 0$. Let (6) be the minimum function of π over R.

Case 1. $v(f'(\pi)) < 2p-1$, i > 1. Let δ be any derivation on k for which $\delta(\bar{u}) = \delta(\bar{a}_0) = 0$ and let $H = \{H_j\}$ be any higher derivation in $\mathcal{H}(R, R)$ satisfying the two conditions (a) H_1 induces δ , (b) $H_j(a_0) \in pR$, $j = 1, \ldots, p-1$. Specifically, every derivation on k lifts to R [1, Theorem 1] which fact makes H_1 available. Let $H_j = H_1^j/j!$ for $j = 2, \ldots, p-1$. By Theorem A, maps H_j , $j \ge p$, can be defined so that $H = \{H_j\} \in \mathcal{H}(R, R)$. Let $D = \{D_j\}$ where

$$(12) D_i = \pi^{ji} H_i.$$

Clearly, $D \in \mathcal{H}_u(R, R_p)$. We now show that

$$(13) D_j(\pi) \in \pi^{i+1}R_p, j \ge 1,$$

and

(14)
$$\sum D_j(\pi) \text{ converges,}$$

from which, with (12), it will follow that, using the same symbol for the extended higher derivation, $D \in \mathcal{H}_u(R_p, R_p)$, $\alpha_D \in \mathfrak{H}_i$ and $\Phi_i(\alpha_D) = \delta$.

Let $v(f'(\pi)) = p + r - 1$. Thus r is the least positive integer such that a_r is a unit. Looking to the conditions of Lemma 5 we note that $f'(\pi)\pi^{i+1-p-s}R_p = \pi^{i+r-s}R_p$. If $s \ge r$, $D_j(a_s) \in \pi^{ji}R_p \subset \pi^{i+r-s}R_p$ for $j \ge 1$. If r > s > 0, $a_s \in pR$; hence, $H_j(a_s) \in pR$ and thus $D_j(a_s) \in \pi^{ij+p}R_p \subset \pi^{i+r-s}R_p$ for $j \ge 1$. Finally, $D_j(a_0) = \pi^{ij}H_j(a_0)$. If j < p, $H_j(a_0) \in pR_p$ and $\pi^{ij}H_j(a_0) \in \pi^{ij+p}R_p \subset \pi^{i+r}R_p$. If $j \ge p$, $ij \ge i+r$. Hence, $D_j(a_0) \in \pi^{i+r}R_p$ for $j \ge 1$. Thus conditions (9, 1) to (9, 3) are satisfied with q = i+1 and n = m = 1. Hence (13) and (14) hold.

Case 2. $v(f'(\pi)) < 2p-2$, i=1. We define D as in Case 1 and note by inspection of (8, j) for $j=1, \ldots, p$ that $D_1(\pi) \in \pi^2 R_p$, $D_j(\pi) \in \pi^3 R_p$ for $j=2, \ldots, p$. Also, in this case, $f'(\pi)\pi^{3-p-s}R_p \supset \pi^{p-s}R_p \supset \pi^p R_p$ and, by (12) $D_j(a_s) \in \pi^p R_p \subseteq f'(\pi)\pi^{3-p-s}R_p$ for $j \ge p$ and $s=0, \ldots, p-1$. Thus conditions (9, 1) to (9, 3) are satisfied for n=2, m=p+1 and q=3. Hence $\sum D_i(\pi)$ converges and is in $\pi^2 R_p$. Thus, $\alpha_D \in \mathfrak{F}_1$ and $\phi_1(\alpha_D) = \delta$.

Case 3. $v(f'(\pi)) = 2p - 2$, i = 1. We consider a number of subcases. In each case D is constructed by the method of Theorem A.

- (3, i). $\bar{a}_{p-1} \notin k^p$, $\bar{a}_0 \notin k^p$, \bar{a}_{p-1} and \bar{a}_0 p-independent. As before, we initiate the construction of $D \in \mathscr{H}_u(R, R_p)$ by letting $D_j = \pi^j H_j$, $j = 1, \ldots, p-1$, where $\{H_j\}_1^{p-1}$ are chosen so that H_1 , a derivation on R_p induces a given $\delta \in \mathscr{D}(k)$ such that $\delta(\bar{a}_0) = 0$ and $H_j(a_0) \in pR$ for $j = 2, \ldots, p-1$. Let \mathscr{S} be a set of representatives in R of a p-basis $\overline{\mathscr{S}}$ of k. We may assume both a_0 and a_{p-1} in \mathscr{S} . By inspection of (8, 1) to (8, p-1) we have $D_1(\pi) \in \pi^2 R_p$ and $D_j(\pi) \in \pi^3 R_p$, $j = 2, \ldots, p-1$. Considering (8, p), each summand of A_p and B_p is in $\pi^{2p+1}R_p$, except the term $[D_1(\pi)]^p$ which is in $\pi^{2p}R_p$ but not in $\pi^{2p+1}R_p$. Thus, we define D_p by $D_p(s) = 0$ for $s \in \mathscr{S} \{a_0\}$ and $D_p(a_0)$ is so chosen that $f^{D_p}(\pi) + A_p + B_p$ is in $f'(\pi)\pi^3R_p$. Thus, $D_p(a_0) \in \pi^pR_p$ and $D_p(\pi) \in \pi^3R_p$. For j > p we let $D_j(s) = 0$ for $s \in \mathscr{S}$. By Lemma 1 $D_j(a_s) \in \pi^{p+1}R_p$ for j > p. It follows that conditions (9) of Lemma 5 are fulfilled for n = 2, m = p + 1 and q = 3. Thus by Theorem A the extension of D to R_p converges uniformly $\alpha_D \in \mathfrak{F}_1$ and $\Phi_1(\alpha_D) = \delta$.
- (3, ii) $\bar{a}_{p-1} \notin k^p$, $\bar{a}_0 \notin k^p$, \bar{a}_{p-1} and \bar{a}_0 p-dependent. Let $H_1 \in \mathcal{D}(R)$ induce $\delta \in \mathcal{D}_k$ where $\delta(\bar{a}_0) = 0$ (Lemma 4) and let \mathscr{S} be a set of representatives of a p-basis for k which contains a_0 . $H \in \mathscr{H}_u(R, R)$ is defined by the conditions $H_j(s) = 0$ for j > 1 and $s \in \mathscr{S}$. Let $D_j = \pi^j H_j$ for $j \ge 1$. Now $H_1(a_{p-1}) \in pR_p$ since $H_1(a_0) \in pR_p$ and the elements \bar{a}_0 , \bar{a}_{p-1} are p-dependent. Thus by (8, 1), $D_1(\pi) \in \pi^3 R_p$. Also $D_j(a_s) \in f'(\pi)\pi^{3-p-s}R_p = \pi^{p+1-s}R_p$ for $j \ge 1$, $s = 0, \ldots, p-1$. Thus, conditions (9) of Lemma 5 are satisfied for n = 1, m = 2, q = 3 and again $D \in \mathscr{H}_u(R_p, R_p)$, $\alpha_D \in \mathfrak{H}_1$ and $\Phi_1(\alpha_D) = \delta$.
- (3, iii) $\bar{a}_{p-1} \in k^p$, $\bar{a}_0 \notin k^p$. A higher derivation D in $\mathcal{H}_u(R, R_p)$ is chosen as in (3, ii). Since $a_{p-1} = b_{p-1}^p + pc$, $H_1(a_{p-1}) \in pR_p$. Thus $D_1(\pi) \in \pi^3 R_p$ and for the rest the argument of (3, ii) applies.
 - (3, iv) $\bar{a}_{p-1} \notin k^p$, $\bar{a}_0 \in k^p$. We choose π so that $a_0 = 1 + pb_0$. Let \mathscr{S} be a set of

representatives of a p-basis for k. We can assume a_{p-1} in \mathscr{S} . Let H_1 in $\mathscr{D}(R)$ induce δ in $\mathscr{D}(k)$. For $j=2,\ldots,p-1$ and $s\in\mathscr{S}$ we let $H_j(s)=0$. For $j=1,\ldots,p-1$ let $D_j=\pi^jH_j$. By (8,1), $D_1(\pi)\in\pi^2R_p$ ($D_1(\pi)\in\pi^3R_p$ unless $D_1(a_{p-1})\notin\pi^2R_p$). Also, $D_j(\pi)\in\pi^3R_p$ for $j=2,\ldots,p-1$. The terms A_p+B_p of (8,p) have $[D_1(\pi)]^p$ as the unique summand of minimum valuation, if $D_1(\pi)\notin\pi^3R_p$. In any case, D_p is defined by $D_p(s)=0$ for $s\in\mathscr{S}$, $s\neq a_{p-1}$ and $D_p(a_{p-1})\in\pi^2R_p$ is chosen so that $D_p(\pi)$ is in π^3R_p . Finally $D_j(s)=0$ for $s\in\mathscr{S}$ and j>p. Again by Theorem A these conditions determine D in $\mathscr{H}_u(R,R_p)$. By Lemma 1 $D_j(R)\subseteq\pi^3R_p$ for j>p. Again we invoke Lemma 5 with n=2, m=p+1 and q=3 to show that $D\in\mathscr{H}_u(R_p,R_p)$, $\alpha_D\in\mathfrak{H}_1$ and $\Phi_1(\alpha_D)=\delta$.

(3, v) $\bar{a}_0 \in k^p$, $\bar{a}_{p-1} \in k^p$. Again it may be assumed that $a_0 = 1 + pb_0$. We choose any $H \in \mathcal{H}(R, R)$ such that H_1 induces a given $\delta \in \mathcal{D}(k)$ and let $D_j = \pi^j H_j$, $j \ge 1$. Lemma 5 applies with n = 1, m = 2 and q = 3.

Case 4. $v(f'(\pi)) = 2p - 1$, $\bar{a}_0 \notin k^p$, i > 1. Let $H \in \mathcal{H}(R, R)$ be chosen so that $H_j(a_0) \in pR_p$ for $j = 1, \ldots, p - 1$ and H_1 induces a given $\delta \in \mathcal{D}(k)$ for which $\delta(\bar{a}_0) = 0$. Let $D = \{\pi^{ij}H_j\}$. Since by (8, 1) $D_1(\pi) \in \pi^{i+1}R_p$ and, by inspection, $D_j(a_s) \in f'(\pi)\pi^{i+1-p}$, $s = 0, \ldots, p-1$, $j \ge 1$, we see by Lemma 5 that $\sum D_j(\pi) \in \pi^{i+1}R_p$. Thus $\alpha_D \in \mathfrak{H}_i$ and $\Phi_i(\alpha_D) = \delta$. Clearly, $D \in \mathcal{H}_u(R_p, R_p)$.

Case 5. $v(f'(\pi)) = 2p - 1$, $\bar{a}_0 \in k^p$, i > 1. We can assume that $a_0 = 1 + pb_0$. Let $H \in \mathcal{H}(R, R)$ be such that H_1 induces a given $\delta \in \mathcal{D}_k$. Let $D = \{\pi^{ij}H_j\}$ and argue as above.

Case 6. $v(f'(\pi)) = 2p-1$, $\bar{a}_0 \notin k^p$, i=1. Let $\delta \in \mathcal{D}(k)$, $\delta(\bar{a}_0) = 0$, and let H_1 in $\mathcal{D}(R)$ induce δ . Let \mathscr{S} be a set of representatives in R of a p-basis for k with a_0 in \mathscr{S} . We define $K_1 \in \mathcal{D}(R)$ as follows: $K_1(a_0) = \pi^{-p}(H_1(a_0))$ and $K_1(s) = 0$ for $s \in \mathscr{S}$, $s \neq a_0$. By Theorem A, these conditions determine a derivation on R. The derivation $D_1 = \pi H_1 - \pi^{p+1} K_1$ has the property $D_1(a_0) = 0$ and is the first map of $D \in \mathscr{H}_u(R, R_p)$. For the rest, we define $D_j(s) = 0$ for $s \in \mathscr{S}$ and j > 1. By Theorem A, $D \in \mathscr{H}_u(R, R_p)$. By Lemma 1 $D_1(R) \subseteq \pi R_p$ and $D_j(R) \subseteq \pi^2 R_p$ for $j \ge 1$. The conditions of Lemma 5 are fulfilled for n = 1, m = 1 and q = 3. Moreover, $\phi_1(\alpha_D) = \delta$.

Case 7. $v(f'(\pi)) = 2p-1$, $\bar{a}_0 \in k^p$, i=1. Again, π is chosen so that $a_0 = 1 + pb_0$. We have the situation (3) with $t \ge p$ and $\bar{v} = \bar{b}_0$. Thus, in deference to Lemma 2, we choose $\delta \in \mathcal{D}(k)$ so that $\delta(\bar{b}_0) = 0$ and let $H_1 \in \mathcal{D}(R)$ induce δ . Let $H \in \mathcal{H}(R, R)$ be any higher derivation on R with the given H_1 as the first map. Let $D = \{D_j\}$ where $D_j = \pi^j H_j$, $j \ge 1$. Let n = m = 1, q = 3 in Lemma 5 and we conclude that $\sum D_j(\pi) \in \pi^3 R_p$. Again we have the desired conclusion and Lemma 6 is proved.

The next series of lemmas are concerned with automorphisms in the "gap" between \mathfrak{G}_i and \mathfrak{H}_i .

LEMMA 7. If π is a prime element of R_p and $\pi^p = -pu$ where $\bar{u} \notin k^p$, then, given $i \ge 2$, there is a $D \in \mathcal{H}_u(R_p, R_p)$ such that $\alpha_D \in \mathfrak{G}_i$ and $\alpha_D(\pi) = \pi + \pi^i a$ where \bar{a} is any given element of k. Hence $\mathfrak{G}_i/\mathfrak{S}_i$ is isomorphic to k^+ .

Proof. We assume (6) to be the minimum function of π over R and thus $\bar{a}_0 \notin k^p$.

Let \mathscr{S} be a set of representatives in R of a p-basis for k with $a_0 \in \mathscr{S}$. With a chosen arbitrarily in R_p we define a derivation D_1 mapping R into R_p by $D_1(a_0) = -p^{-1}f'(\pi)\pi^i a$ and $D_1(s) = 0$ for $s \in \mathscr{S}$, $s \neq a_0$. Then $D_1(R) \subseteq f'(\pi)\pi^{i-p}R_p$ by Lemma 1 and by (8.1), $D_1(\pi) \equiv \pi^i a$, mod $\pi^{i+1}R_p$. Let $D_j(s) = 0$, $s \in \mathscr{S}$, $j = 2, \ldots, p-1$. If i=2, the term $[D_1(\pi)]^p$ in A_p of (8, p) makes it necessary to consider cases.

Case 1. i>2 or $v(f'(\pi))<2p-2$. In this case we let $D_j(s)=0$, $s\in \mathcal{S}, j>p-1$. Thus, by Lemma 1, $D_j(R)\subset [f'(\pi)\pi^{i-p}]^jR_p$, $j\ge 1$, and if j>1, $D_j(R)\subset f'(\pi)\pi^{i+1-p}$ since $f'(\pi)\in \pi^pR_p$. The conditions of Lemma 5 are fulfilled for n=2, m=p+1 and q=i+1. Thus D extends to R_p , is uniformly convergent on R_p and $\sum_{j=2}^{\infty}D_j(\pi)\in \pi^{i+1}R_p$. In particular then, $\sum_{j=1}^{\infty}D_j(\pi)\equiv \pi^i a$, mod $\pi^{i+1}R_p$.

Case 2. i=2, $v(f'(\pi)) \ge 2p-2$. In this case we choose $D_p(s)=0$, $s \in \mathcal{S}$, $s \ne a_0$ and $D_p(a_0) \in \pi^p R_p$ so that $D_p(\pi)$ will be in $\pi^3 R_p$. Again, we let $D_j(s)=0$ for j>p, $s \in \mathcal{S}$ and apply Lemma 5 with n=2, m=p+1 and q=3, obtaining the same conclusion as in Case 1.

The map τ_i : $\mathfrak{G}_i \to k^+$ given by $\tau_i(\alpha) = \bar{a}$ where $\alpha(\pi) = \pi + \pi^i a$, is a homomorphism with kernel \mathfrak{F}_i and evidently maps onto k^+ if $i \ge 2$.

LEMMA 8. If π is a prime element of R_p , $\pi^p = -pu$, and $\bar{u} \in k^p$ then $\mathfrak{G}_i = \mathfrak{F}_i$ for i > 1 unless i = 2 and t of (3) is p - 1. If t = p - 1 the following are equivalent.

- (a) \bar{v} has a (p-1)th root in k.
- (b) R_v is Galois over R.
- (c) $\mathfrak{G}_2 \neq \mathfrak{H}_2$.
- (d) $\mathfrak{G}_2/\mathfrak{F}_2$ is the group of order p.

Proof. Let α be in \mathfrak{G}_i . Then $\alpha = \varepsilon + \pi^i \alpha^*$. The relation

$$[\alpha(\pi)]^p - \pi^p = p[1 + [\alpha(\pi)]^t \alpha(v)] - p(1 + \pi^t v)$$

becomes

(15)
$$p\pi^{i+p-1}\alpha^{*}(\pi) + \cdots + \pi^{ip}[\alpha^{*}(\pi)]^{p}$$

$$= p[\pi^{t} + t\pi^{t-1+i}\alpha^{*}(\pi) + \cdots + \pi^{ti}(\alpha^{*}(\pi))^{t}]\pi^{i}\alpha^{*}(v)$$

$$+ p[t\pi^{t-1+i}\alpha^{*}(\pi) + \cdots + \pi^{ti}(\alpha^{*}(\pi))^{t}]v.$$

If i>2 the unique term having minimal valuation on the left side of (15) is $p\pi^{i+p-1}\alpha^*(\pi)$. If $p\nmid t$ the unique term of minimal valuation on the right is $pt\pi^{t-1+i}v\alpha^*(\pi)$, unless $\alpha^*(\pi)$ is in πR_p . Thus, either $\alpha^*(\pi)\in\pi R_p$ or t+i-1=p+i-1, which cannot be. Thus, if i>2 and $p\nmid t$, then $\alpha\in\mathfrak{H}_i$ or $\mathfrak{H}_i=\mathfrak{H}_i$. If $p\mid t$ and $i\geq 2$ the left side of (15) has valuation less than the right side unless $\alpha^*(\pi)\in\pi R_p$. Thus again $\mathfrak{H}_i=\mathfrak{H}_i$.

If i=2 and $p \nmid t$, the unique term of minimal valuation on the left side of (15) is $\pi^{2p}[\alpha^*(\pi)]^p$, assuming $\alpha^*(\pi)$ to be a unit. The corresponding term on the right is $pt\pi^{t+1}\alpha^*(\pi)v$. Thus, 2p=p+t+1 or t=p-1. So, if $t\neq p-1$, $\mathfrak{G}_2=\mathfrak{H}_2$. If t=p-1, then by (15), $\pi^{2p}[\alpha^*(\pi)]^p \equiv p(p-1)\pi^p\alpha^*(\pi)v$, mod $\pi^{2p+1}R_p$, or, using (3), $[\alpha^*(\pi)]^{p-1} \equiv (p-1)v$, mod πR_p . Thus, $(p-1)\bar{v}$, or \bar{v} , is a (p-1)th root in k and the residue

of $\alpha^*(\pi)$ is a (p-1)th root of $(p-1)\bar{v}$. We have shown that $(c) \to (d) \to (a)$. A theorem of Wishart [4, Theorem 4.15] asserts that $(a) \to (b)$.

Suppose, finally, that α in \mathfrak{G}_1 leaves R element-wise fixed. Then, if $\alpha(\pi) = \pi + \pi^i b$, $\alpha \in \mathfrak{G}_i$. Thus, if $\alpha \neq \varepsilon$, then $\alpha \in \mathfrak{G}_r$, $\alpha \notin \mathfrak{F}_r$ for some r > 1. Evidently, r = 2 and $(b) \to (c)$. This fact was also observed by Wishart [4, Corollary 4.16] who noted that if $\bar{u} \in k^p$ then R_p is Galois over R if and only if $\mathfrak{G}_2 \neq \mathfrak{F}_2$. It follows from Lemma 7 that if $\bar{u} \notin k^p$, then \mathfrak{G}_2 can be different from \mathfrak{F}_2 without R_p being Galois over R.

LEMMA 9. If $\mathfrak{G}_2 \neq \mathfrak{F}_2$, then, for each $\alpha \in \mathfrak{G}_2$, there is a D in $\mathscr{H}_u(R_p, R_p)$ such that $\alpha \alpha_D^{-1} \in \mathfrak{F}_2$ if and only if, in (3), $\bar{v} \notin k^p$.

Proof. Assuming first that $\bar{v} \notin k^p$ it follows from Lemma 8 that in (3), t=p-1 and \bar{v} is a (p-1)th root in k. Assuming (6) to be the minimal polynomial of π over R, relation (3) with t=p-1 implies that a_1, \ldots, a_{p-2} are in pR, $\bar{a}_{p-1}(=-\bar{v})$ is a (p-1)th root in k, $v(f'(\pi))=2p-2$ and $a_0=1+pb_0$.

Let w be a unit in R_p such that \overline{w} is a (p-1)th root of $\overline{a}_{p-1}(p-1)$. We wish to construct $D \in \mathcal{H}_u(R_p, R_p)$ such that $\alpha_D \in \mathfrak{G}_2$ and $\alpha_D(\pi) \equiv \pi^2 w$, mod $\pi^3 R_p$.

Let $\mathscr S$ be a set of representatives in R for a p-basis of k chosen to include a_{p-1} . Then D_1 is defined by $D_1(a_{p-1}) = -f'(\pi)\pi^2w/p\pi^{p-1}$, $D_1(s) = 0$ for $s \in \mathscr S$, $s \neq a_{p-1}$. By Lemma 1 $D_1(R) \subset \pi^2 R_p$ and by (8.1) $D_1(\pi) \equiv \pi^2 w$, mod $\pi^3 R_p$. For $j = 2, \ldots, p-1$ and $s \in \mathscr S$, $D_j(s) = 0$. By (8, 2) to (8, p-1), $D_j(\pi) \in \pi^3 R_p$ for $j = 2, \ldots, p-1$. The term $[D_1(\pi)]^p$ in (8, p) leads us to define D_p by $D_p(a_{p-1}) = -\pi^{2p}w^p/p(\pi^{p-1})$ and $D_p(s) = 0$, $s \in \mathscr S$, $s \neq a_{p-1}$. Since each term of (8, p) in $A_p + B_p$ is in $\pi^{2p+1}R_p$ save $[D_1(\pi)]^p$ and $[D_1(\pi)]^p \equiv \pi^{2p}w^p$, mod $\pi^{2p+1}R_p$, we have $D_p(\pi) \in \pi^3 R_p$. Finally, we let $D_j(s) = 0$ for $s \in \mathscr S$ and j > p. Then $D_j(R) \subset \pi^2 R_p$ for j > p and by Lemma 5 with n = 2, m = p + 1 and q = 3, we conclude that $\sum D_j(\pi)$ converges and $\sum_{j=2}^\infty D_j(\pi) \in \pi^3 R_p$.

It remains to show that α_D is in \mathfrak{G}_2 . We have shown that $\alpha_D(\pi) - \pi$ is in $\pi^2 R_p$ and it is shown below that

(16)
$$\alpha_D(s) - s \in \pi^2 R_v, \qquad s \in \mathscr{S}.$$

If $s \in \mathcal{S}$, $s \neq a_{p-1}$ then $\alpha_D(s) = s$ by definition of D. Since $D_j(a_{p-1}) = 0$ for $j \neq 1$, p it is sufficient to show that $D_1(a_{p-1}) + D_p(a_{p-1}) \in \pi^2 R_p$. Now, $f'(\pi) \equiv (p-1)a_{p-1}\pi^{p-2}$, mod $\pi^{p-1}R_p$. Also $w^{p-1} \equiv (p-1)a_{p-1}$, mod πR_p , by choice of w. Using these facts as well as the congruence $\pi^p \equiv -p$, mod $\pi^{p+1}R_p$, leads to the conclusion $D_1(a_{p-1}) + D_p(a_{p-1}) = -f'(\pi)\pi^2 w/p\pi^{p-1} - \pi^{2p}w^p/p\pi^{p-1} \in \pi^2 R_p$.

Since α_D is inertial, $\alpha_D(a^p) - a^p \in \pi^p R_p$ and every unit in R is, mod pR, a polynomial in elements of $\mathscr S$ with coefficients in R^p . It follows that $\alpha_D(a) - a \in \pi^2 R_p$ for a in R. Thus α is in $\mathfrak S_2$.

It was shown in the proof of Lemma 8 that if $\alpha \in \mathfrak{G}_2$ then $\alpha = \varepsilon + \pi^2 \alpha^*$ and $\alpha \in \mathfrak{F}_2$ or the residue of $\alpha^*(\pi)$ is a (p-1)th root of $(p-1)\bar{v} = \bar{a}_{p-1}(p-1)$. Thus if we choose w, in the construction of D, to be $\alpha^*(\pi)$, then $\alpha\alpha_D^{-1} \in \mathfrak{F}_2$.

If $\bar{v} \in k^p$ then $v = v_0^p + \pi v_1$. Thus $\bar{a}_{p-1} = \bar{v}_0^p$ and $\bar{b}_0 = \bar{v}_1$ where, again, $a_0 = 1 + pb_0$. We choose c_0 and c_1 in R so that $a_{p-1} = c_0^p + pc_1$. Let $D \in \mathcal{H}_c(R_p, R_p)$ be such that

 $\alpha_D \in \mathfrak{G}_2$, $\alpha_D \notin \mathfrak{F}_2$. There is, then, a first index j such that $f^{D_j}(\pi) \in f'(\pi)\pi^2 R_p$ and $f^{D_j}(\pi) \notin f'(\pi)\pi^3 R_p$. This requires that $D_j(a_{p-1}) = D_j(c_0^p + pc_1) \in \pi^2 R_p$ and $D_j(a_{p-1}) \notin \pi^3 R_p$. However, $D_j(R) \subseteq \pi R_p$ and hence $D_j(c_0^p + pc_1) \in \pi^p R_p$. We have a contradiction. Thus $\mathfrak{G}_2 \cap \mathfrak{G}_D \subseteq \mathfrak{F}_2$, and Lemma 9 is proved.

For i > 1 and $\alpha \in \mathfrak{F}_i$ there is a $D \in \mathscr{H}_u(R_p, R_p)$ such that $D(R_p) \subset \pi^i R_p$ (see (12)) and $\alpha \alpha_D \in \mathfrak{G}_{i+1}$. Also if i > 2 and $\alpha \in \mathfrak{G}_i$ then $\alpha \in \mathfrak{F}_i$ or there is a $D \in \mathscr{H}_u(R_p, R_p)$ such that $D(R_p) \subset \pi^i R_p$ and $\alpha \alpha_D \in \mathfrak{F}_i$. This follows from Lemma 7, Case 1 of the proof of Lemma 7 and Lemma 8. Thus, given $\alpha \in \mathfrak{F}_2$ there is a sequence $\{D^{(n)}\}$, $D^{(n)} \in \mathscr{H}_u(R_p, R_p)$ such that, $D^{(n)}(R_e) \subset \pi^{s_n} R_p$ where $\lim_n s_n = \infty$, and $\alpha = \alpha_{D_1} \alpha_{D_2} \cdots \alpha_{D_{2n}}$, mod \mathfrak{F}_{n+2} . By Lemma 3, there is a $D \in \mathscr{H}_u(R_p, R_p)$ such that $\alpha = \alpha_D$.

By Lemma 6 and Lemma 9, we conclude that \mathfrak{G}_D and $\mathfrak{G}(R_p, R)$ together generate \mathfrak{G} . If β is an automorphism on R and $D \in \mathscr{H}_c(R_e, R_e)$ then $H = \{H_i\}$ where $H_i = \beta^{-1}D_i\beta$ is also in $\mathscr{H}_c(R_e, R_e)$. If D converges uniformly so does H. Thus \mathfrak{G}_D is an invariant subgroup of G the automorphism group of R_p . Hence $\mathfrak{G}_1 = \mathfrak{G}_D \cdot \mathfrak{G}(R_p, R)$. These observations along with Lemmas 8 and 9 prove Theorem 1. Theorem 2 follows directly from Lemmas 2, 4, 6, 7 and 8.

REFERENCES

- 1. N. Heerema, Derivations on p-adic fields, Trans. Amer. Math. Soc. 102 (1962), 346-351.
- 2. ——, Convergent higher derivations on local rings, Trans Amer. Math. Soc. 132 (1968), 31-44.
 - 3. J. Neggers, Derivations on p-adic fields, Trans. Amer. Math. Soc. 115 (1965), 496-504.
- 4. E. Wishart, Higher derivations on p-adic fields, Dissertation, Florida State Univ., Tallahassee, 1965.

FLORIDA STATE UNIVERSITY, TALLAHASSEE, FLORIDA