ON RAMIFIED COMPLETE DISCRETE VALUATION RINGS

NICKOLAS HEEREMA

1. Introduction. A discrete valuation ring R is a commutative integral domain with a single prime element q (to within a unit). R becomes a topological ring by defining the neighborhoods of zero to be the ideal (q) and all powers of (q). R is a complete discrete valuation ring if it is complete with respect to this topology.

A non-Archimedean discrete valuation V can be defined on R by letting $V(0)=\infty$ and $V(a)$ $(a\neq 0)$ be the highest power of q to divide a. This valuation can be extended in the natural way to the quotient field K of R. The nonzero elements of R are then the quantities in K with non-negative valuation. Conversely, given a field K with non-Archimedean discrete valuation, the elements in K with non-negative valuation are the nonzero elements of a discrete valuation ring R, the ring of integers of K. R is complete if and only if K is complete. Again K is the quotient field of R.

It is largely in this context that complete discrete valuation rings have been studied. It has been shown that if R is complete and has the same characteristic as its residue class field F then R is isomorphic to the ring of power series $F[[x]]$. Moreover, in the remaining case (R has characteristic infinity and F has characteristic p), R is uniquely determined by F if R is unramified, i.e., if p is prime in R. Also there exists an R for any given F. If $V(p)=n$, $n>1$, R is said to be ramified with ramification index n. For references see [2].

This paper is concerned with some aspects of the structure of ramified complete discrete valuation rings. Throughout this paper, the symbols R, R', R_n etc., will denote complete discrete valuation rings of characteristic zero having the same residue field F of characteristic p. The subscript on the ring symbol will designate the ramification index or if there is none the ring is unramified.

Rings R_n have been studied extensively, largely as a part of algebraic number theory. Thus, as indicated below, a number of the results of this paper are known, however the methods are new and simple.

Theorem 1 provides a description of an arbitrary ring R_n in terms of the unique unramified R and is closely related to the theorem [3, p. 237, Theorem 11] which states that every R_n is an $R(t)$ where t is a root of an Eisenstein equation. This characterization is then used

Presented to the Society, November 30, 1957 under the title of *Note on complete discrete valuation rings*; received by the editors August 7, 1958.

(Theorem 2) to establish the known fact [3, p. 236, Corollary] that R is uniquely imbedded in R_n if F is perfect. The method of proof hinges on the fact that a perfect field has no nontrivial derivations. As a matter of fact it can be shown that if $n \leqq p$ the various ways in which R is imbedded in R_n are determined by certain sequences of $n-1$ derivations on F.

Theorems 3, 4, and 5 deal with the isomorphism question for rings R_n. Corollary 3 and the fact illustrated by the example which follows it are known, the former for normal extensions at any rate.

2. The characterization.

THEOREM 1. *Let R_n and R be complete discrete valuation rings of characteristic zero whose isomorphic residue fields have characteristic p and let R be unramified. Then R_n is isomorphic to $R[[x]]/I$ where $R[[x]]$ is the ring of power series in x over R and I is a principal ideal generated by $p-ux^n$ where u is a unit in $R[[x]]$ and n is the ramification index of R_n. Conversely, any such ring $R[[x]]/I$ is a complete discrete valuation ring with ramification index n and residue field isomorphic to that of R.*

PROOF. That $R[[x]]/I$ is a complete discrete valuation ring with the stated properties follows from the following three observations which will be discussed in turn. Lower case letters in the early part of the alphabet will be used for elements in $R[[x]]$ which are also in R.

(1) Each element v in $R[[x]]$ is congruent to an element of the form $\sum b_i x^i (v \equiv \sum b_i x^i)$ where each b_i is a unit or zero. (Throughout this paper congruence is with respect to I and $\sum$ indicates a summation from 0 to ∞.)

(2) If $\sum a_i x^i$ and $\sum b_i x^i$ are congruent and are in the form (1) then the indices of their first nonzero coefficients are equal.

(3) If a_0 is a unit $\sum a_i x^i$ is a unit.

The construction of $\sum b_i x^i$ in (1) can be described as follows: Let $v = \sum a_i x^i$. For each n we will construct $\sum a_i^{(n)} x^i \equiv v$ such that $a_j^{(n)} = b_j$ for all $j < n$. If $a_0 = 0$ or a unit let $a_i^{(1)} = a_i$ for all i. If $a_0 = dp^m$ for some $m > 0$ where d is a unit substitute $d(ux^n)^m \equiv a_0$ in v to obtain a new series $\sum a_i^{(1)} x^i \equiv v$ in which $a_0^{(1)} = 0 = b_0$.

Suppose that $\sum a_i^{(r)} x^i \equiv v$ has been obtained in which then, $a_i^{(r)} = b_i$ for $i < r$. If $a_r^{(r)}$ is a unit or zero let $a_i^{(r+1)} = a_i^{(r)}$ for all i. If $a_r^{(r)} = d_1 p^s$ where d_1 is a unit and $s > 0$, substitute $d_1(ux^n)^s$ for $a_r^{(r)}$ obtaining $\sum a_i^{(r+1)} x^i \equiv v$. The set $\{v - \sum a_i^{(r)} x^i\}_r$ forms a Cauchy sequence with limit $v - \sum b_i x^i$ which is in I since I is closed.

Since the coefficient of x^0 in $p-ux^n$ is neither zero nor a unit it follows that the first nonzero coefficient of each element in I is a

nonunit. Thus, if $\sum a_i x^i$ and $\sum b_i x^i$ of (2) have different indices for their first nonzero terms, their difference cannot be in I.

A standard argument establishes property (3). Properties (1) and (2) together show that $R[[x]]/I$ has no zero divisors and that every v in $R[[x]]$ is congruent to an element of the form $x^s \sum c_i x^i$ where c_0 is a unit in R, $\sum c_i x^i$ has the form (1) and s is invariant under congruence. If $s>0$, $x^s \sum c_i x^i$ cannot have an inverse since every element of the form $v(x^s \sum c_i x^i) - 1$ has leading coefficient -1 and, hence, cannot be in I.

Thus $R[[x]]/I$ is a discrete valuation ring with but one prime element q, the coset of x. The facts that $R[[x]]/I$ is complete, has ramification index n, and residue field isomorphic to the residue field of R, follow directly from the method of construction.

In establishing the rest of the theorem we observe that R_n contains a subring R' isomorphic to R which, under the natural homomorphism of R_n onto K, also maps onto K [**3**, p. 236, Lemma 42]. It will be convenient to identify R' with R.

Let q be prime in R_n. Each coset of the ideal $\{q\}$ in R contains an element of R. Thus if a is in R_n there exists an a_0 in R such that $a - a_0$ is in $\{q\}$ or $a = a_0 + a^{(0)}q$. Again, there exists an a_1 in R such that $a^{(0)} - a_1$ is in $\{q\}$ or $a = a_0 + a_1 q + a^{(1)}q^2$. Proceeding inductively we see that for each a in R_n, $a = \sum a_i q^i$ where a_i is in R for all i. Thus under the mapping π where $\pi(\sum a_i x^i) = \sum a_i q^i$, $R[[x]]$ maps homomorphically onto R_n. Let J be the kernel of π. Since R_n has ramification index n, $p = q^n \sum a_i q^i$ where again the a_i are in R and $\sum a_i q^i$ is a unit. Thus the ideal I generated by $p - x^n \sum a_i x^i$ is in J and R_n is a homomorphic image of $R[[x]]/I$. However, we have already observed that $R[[x]]/I$ is a complete discrete valuation ring. Hence, it has no proper homomorphic image which is an integral domain aside from its residue class field. It follows that R_n is isomorphic to $R[[x]]/I$. Henceforth, we will identify R with the isomorphic subring of $R[[x]]/I$ consisting of all cosets of the form $a + I$ where $a \in R$.

3. **Applications.** Let R' denote an unramified subring of $R_n = R[[x]]/\{p - x^n u\}$ which under the natural map ξ of R_n onto F (the symbol ξ will be reserved henceforth for this map) also maps onto F. Let $\bar{v}'$ be a unit in R'. We wish to show that, if F is perfect, there is a unit $\bar{v}$ in $R \cap R'$ such that $\bar{v} - \bar{v}' \in \{\bar{p}\}$, where $\bar{p}$ is the coset of p, and hence that $R = R'$.

Let $\sum a_i x^i \in \bar{v}'$. There is an element $\bar{v}_1'$ in R' such that $a_0 + \sum_{i=1}^{n-1} a_i^{(1)} x^i \in \bar{v}_1'$ with the property

(4) $\bar{v}' - \bar{v}_1' \in \{\bar{p}\}$.

(5) The first nonzero coefficient $a_m^{(1)}$ of $\sum_{i=1}^{n-1} a_i^{(1)}x^i$, if any, is a unit. Suppose that $\bar{v}_2' \ni a_0' + \sum_{i=1}^{n-1} a_i^{(2)}x^i$ and also fulfills conditions (4) and (5) with first nonzero coefficient $a_r^{(2)}$ in $\sum_{i=1}^{n-1} a_i^{(2)}x^i$. Then, since $\bar{v}_1' - \bar{v}_2' \in \{\bar{p}\}$, it follows that $a_0' = a_0$, mod p, $r = m$, and $a_r^{(2)} = a_m^{(1)}$, mod p.

With each element $\alpha \in F$ we associate the element $\eta_1(\alpha)$ determined as follows. Choose $\bar{v}'$ in R' which under ξ, of R_n onto F, maps onto α. With $\bar{v}'$ is associated an a_0 and an $a_1^{(1)}$ both uniquely determined, mod p, by α. Let $\eta_1(\alpha) = \xi(a_1^{(1)})$. The map η_1 is a derivation on F, i.e., $\eta_1(\alpha_1+\alpha_2) = \eta_1(\alpha_1) + \eta_1(\alpha_2)$ and $\eta_1(\alpha_1\alpha_2) = \alpha_1\eta(\alpha_2) + \alpha_2\eta(\alpha_1)$. But, if F is perfect, it has no nontrivial derivation hence $a_1^{(1)} = 0$ for all units $\bar{v}'$ in R. Assume that it has been shown that $a_s^{(1)} = 0$ for $0 < s < k < n$. The map $\eta_k(\alpha) = \xi(a_k^{(1)})$ is then a derivation from which it follows that $a_k^{(1)} = 0$ for all units $\bar{v}'$ in R'. Thus if F is perfect $\bar{v}_1' \ni a_0$ and, hence, $\bar{v}_1' \in R \cap R'$.

We will say that the unramified complete discrete valuation ring R' is imbedded in R_n if both $R' \subset R_n$ and, if, under the map ξ of R_n onto F, R' maps onto F. We have shown that

THEOREM 2. *R is uniquely imbedded in any complete discrete valuation R_n with the same residue field F if F is perfect.*

Let $R_n = R[[x]]/\{p - x^n u\}$ and $R_n' = R'[[x]]/\{p - x'^n v\}$ where $u = \sum a_i x^i$ and $v' = \sum a_i' (x')^i$. We wish to investigate the manner in which u and v must be related relative to an isomorphism π of R onto R' in order that π can be extended to an isomorphism $\bar{\pi}$ of R_n onto R_n'.

LEMMA 3. *Every isomorphism $\bar{\pi}$ of R_n onto R_n' such that $\bar{\pi}(R) = R'$ is induced by an isomorphism $\bar{\pi}^*$ of $R[[x]]$ onto $R'[[x']]$ with the properties that*

(6) $\bar{\pi}^*(R) = R'$,

(7) $\bar{\pi}^*(p - x^n u) = w'(p - (x')^n v')$,

and conversely, each such isomorphism $\bar{\pi}^*$ induces an isomorphism $\bar{\pi}$ of R_n onto R_n' such that $\bar{\pi}(R) = R'$.

PROOF. Given the isomorphism $\bar{\pi}$ define $\bar{\pi}^*$ to agree with $\bar{\pi}$ on R. Let $\bar{\pi}^*(x) = s'x'$ where $\bar{\pi}[x + \{p - x^n u\}] = s'x' + \{p - (x')^n v'\}$. Let $\bar{\pi}^*(\sum b_i x^i) = \sum \bar{\pi}^*(b_i)(s'x')^i$. The map $\bar{\pi}^*$ is an isomorphism of $R[[x]]$ onto $R'[[x']]$. Now $\bar{\pi}$ is necessarily continuous. It follows that $\bar{\pi}[p - x^n u + \{p - x^n u\}] = p - (s'x')^n \sum \bar{\pi}(a_i)(s'x')^i + \{p - (x')^n v\} = \{p - (x')^n v\}$ from which it follows that $\bar{\pi}^*$ satisfies Condition (7) as well as (6). The converse is immediate.

THEOREM 3. *If the ramification index n is prime to p an isomorphism π of R onto R' can be extended to an isomorphism $\bar{\pi}$ of R_n onto R_n' if and only if the equation $\xi[\pi(a_0)]z^n=\xi(a_0')$ has a solution $z=\gamma$ in F.*

PROOF. By Lemma 3 the problem of extending an isomorphism π to an isomorphism $\bar{\pi}$ is equivalent to the problem of extending π to an isomorphism $\bar{\pi}^*$. In order to do the latter it is necessary and sufficient to find a unit $s'=\sum b_i'(x')^i$ in $R'[[x']]$ such that if $\bar{\pi}^*(x)$ is chosen to be the element $s'y'$ there will exist a $w'=\sum c_i'(x')^i$ in $R'[[x']]$ such that condition (7) holds, or, such that,

$$p-(s'x')^n\sum\pi(a_i)(s'x')^i=[p-(x')^n(\sum a_i'(x')^i)]\sum c_i'(x')^i.$$

Equating coefficients of $(x')^j$ for $j=0, 1, \cdots$ we obtain the following, where a subscript following a grouping symbol denotes the coefficient of the corresponding power of x' when the inclosed quantity is written as a power series in x' over R'.

$$\begin{aligned}
&j=0,\ c_0'=1,\\
&0<j<n,\ c_j'=0,\\
&j=n,\ (b_0')^n\pi(a_0)+a_0'-pc_n',\\
&j=kn+i,\ k>0,\ 0\leqq i<n,\\
&\sum_{t=0}^{(k-1)n+i}[(s')^n]_t[\sum\pi(a_r)(s'x')^r]_{(k-1)n+i-t}\\
&\qquad=pc_{kn+i}-\sum_{t=0}^{(k-1)n+i}a_t'c'_{(k-1)n+i-t}.
\end{aligned}\tag{8}$$

Given the condition of the theorem one can find elements c_j' and b_0' such that (8) holds for $j\leqq n$. The term with highest subscript among the b_j' occurring in (8) for $j=kn+i$, $k\neq 0$, is $b'_{(k-1)n+i}$ with coefficient $n(b_0')^{n-1}\pi(a_0)$ which is a unit. Thus whatever the choice of c'_{kn+i} the expression has a solution $b'_{(k-1)n+i}$ which establishes the sufficiency of the given condition. The above discussion also implies the necessity of the given condition.

It follows from Theorem 3 that $R[[x]]/\{p-x^nu\}$ is isomorphic to $R[[x]]/\{pa-x^n\}$ where $u^{-1}=a+\sum_{i=1}^{\infty}a_ix^i$. Now $R[[x]]/\{pa-x^n\}$ is isomorphic to $R[x]/\{pa-x^n\}$. This leads us to

COROLLARY 3. *The ring $R[x]$ obtained by extending R by a primitive nth root of a prime element in R is a ring R_n. If n is prime to p every ring R_n is of this type.*

The following example will illustrate the known fact that, in gen-

eral, if n is not prime to p rings R_n exist which are not simple extensions of R by primitive nth roots of prime elements of R.

Let F be perfect and let $n=mp$. The ring

$$R_{n_1} = R[[x]]/\{p - (a_0 + a_1x)x^n\}$$

where a_1 is a unit cannot be isomorphic to a ring

$$R_{n_2} = R[[x]]/\{p - b_0x^n\}$$

for, in the first place, R is uniquely imbedded in them hence if they are isomorphic under a map π, say of R_{n_2} onto R_{n_1}, then π must map R onto itself but it is readily seen that condition (8) cannot be fulfilled for $j=n+1$.

We will say that two nonzero elements α and β in F are n congruent over R ($\alpha\sim\beta$) if there is an automorphism π on R such that with respect to the automorphism π^* induced on F under the map ξ of R onto F the equation $\pi^*(\alpha)z^n=\beta$ has a solution $z=\gamma$ in F. This is an equivalence relation with the following two properties

$$\alpha \sim \beta \Rightarrow \pi_1^*(\alpha) \sim \beta \tag{9}$$

for any automorphism π^* on F induced as above by an automorphism π_1 on R.

$$\alpha \sim \beta \Rightarrow \alpha(\alpha_1)^n \sim \beta(\beta_1)^n$$

for any nonzero α_1 and β_1 in K.

By choosing $R=R'$ in Theorem 3 we are led to

THEOREM 4. *If F is perfect and n is prime to p there are as many distinct R_n as there are equivalence classes in F with respect to the above equivalence relation. Moreover, if $F=P$, the field of order p, there are as many distinct R_n as cosets of the subgroup of nth powers in the multiplicative group of nonzero elements in F.*

The last sentence in Theorem 4 follows from the fact that in this case the only automorphism on F is the identity.

It is known that every automorphism on F is induced by an automorphism on R if both K, the quotient field of R, is normal over its subfield of p-adic numbers and F is separable over P [1, Chapter 4, Theorem 8]. Thus, in this case we have

COROLLARY 4. *If F is perfect and n is prime to p there are as many distinct R_n as there are equivalence classes in F with respect to the following equivalence relation—α is equivalent to β ($\alpha\approx\beta$) if and only if there exists an automorphism π on F such that the equation $\pi(\alpha)z^n=\beta$ has a solution in F.*

Let R and R' be contained in R_n and R_n' respectively. Then $p=uq^n$ in R_n for any given prime q where u is a unit and $p=u'(q')^n$ in R_n'. Let a and a' be units in R and R' such that $\xi(a)=\xi(u)$ and $\xi(a')=\xi(u')$. We shall conclude with the following theorem.

THEOREM 5. *If F is perfect then R_n is isomorphic to R_n' if and only if under a given isomorphism π of R onto R' $\xi[\pi(a)]\sim\xi(a')$.*

PROOF. Let $\bar{\pi}$ denote an isomorphism of R_n onto R_n'. Then by Theorem 2 $\bar{\pi}(R)=R'$. Now R_n and R_n' are isomorphic respectively to $R[[x]]/\{p-x^na\}$ and $R'[[x']]/\{p-(x')^na'\}$ under maps η and η' which are the identity on R and R' respectively and map q and q' onto x and y. The map $\eta'\bar{\pi}\eta^{-1}$ is an isomorphism of $R[[x]]/\{p-x^na\}$ onto $R'[[y]]/\{p-(x')^na'\}$. It follows from Theorem 3 that $\xi\eta'\bar{\pi}\eta^{-1}(a)\sim\xi(a')$. But $\eta'\bar{\pi}\eta^{-1}(a)=\bar{\pi}(a)$, hence, $\xi\bar{\pi}(a)\sim\xi(a')$.

Now, let π_1 be an arbitrary isomorphism of R onto R'. The map π_2 given by $\bar{\pi}(b)\to\pi_1(b)$ is an automorphism on R' and induces the automorphism $\bar{\pi}_2$ on F. Thus, by property 9, $\xi(a')\sim\bar{\pi}_2\xi\bar{\pi}(a)=\xi\pi_2\bar{\pi}(a)=\xi\pi_1(a)$. This establishes the necessity of the condition.

To show that the condition is sufficient let π be an isomorphism of R onto R' such that $\xi\pi(a)=\xi(a')$. Again R_n and R_n' are isomorphic respectively to $R[[x]]/\{p-x^na\}$ and $R'[[x']]/\{p-(x')^na'\}$ under maps η and η which map q and q' onto x and y and which are the identity on R and R' respectively. The condition of Theorem 3 is fulfilled and $R[[x]]/\{p-x^na\}$ is isomorphic to $R'[[x']]/\{p-(x')^na'\}$.

Again, assuming the conditions of Corollary 4 on K and F we have

COROLLARY 5. *If F is perfect then R_n is isomorphic to R_n' if and only if under a given isomorphism π of R onto R' $\xi[\pi(a)]\approx\xi(a')$.*

BIBLIOGRAPHY

1. E. Artin, *Algebraic numbers and algebraic functions* I, Princeton University, New York University, 1950–1951.

2. S. MacLane, *Subfields and automorphism groups of p-adic fields*, Ann. of Math. vol. 40 (1939) pp. 423–442.

3. O. F. G. Schilling, *The theory of valuations*, Mathematical Surveys, no. 4, New York, 1950.

FLORIDA STATE UNIVERSITY