EQUIVALENCE OF TAMELY RAMIFIED $\nu$-RINGS

NICHOLAS HEEREMA

1. Introduction. Let $R$ be a $\nu$-ring, that is, an unramified complete discrete valuation ring of characteristic zero with residue field $k$ having characteristic $p \neq 0$. Let $R_e$ and $R'_e$ be totally ramified extensions of $R$ of degree $e$. The symbol $H$ represents the natural map of a local ring onto its residue field. We say that an automorphism $\tilde{\tau}$ on $k$ lifts to an automorphism $\tau$ on $R_e$, and $\tau$ induces $\tilde{\tau}$, if $H\tau = \tilde{\tau}H$. In this note we shall prove the following theorem and a number of corollaries.

Theorem 1. Assume that $(e, p) = 1$ and let $\pi$ and $\pi' = \nu$ be prime elements of $R_e$ and $R'_e$ respectively. Then we have $\pi = \pi' \nu = \pi' \nu'$ where $u$ and $u'$ are units in $R_e$ and $R'_e$. If $\tilde{\tau}$ is the automorphism on $k$ induced by the isomorphism $\tau : R_e \to R'_e$ then $H(u'^{-1})\tilde{\tau}H(u)$ has an eth root in $k$. Conversely, if $\tilde{\tau}$ is an automorphism on $k$ such that $H(u'^{-1})\tilde{\tau}H(u)$ has an eth root in $k$ then there exists an isomorphism $\tau$ of $R_e$ onto $R'_e$ such that $\tau$ induces $\tilde{\tau}$. Moreover, $\tau$ can be chosen so that $\tau(R) = R$.

We shall discuss a number of corollaries of Theorem 1 and defer the proof of the theorem.

Corollary 1. An automorphism $\tilde{\tau}$ on $k$ lifts to an automorphism of $R_e$ if and only if $H(u'^{-1})\tilde{\tau}H(u)$ has an eth root in $k$.

Corollary 2. If the automorphism $\tilde{\tau}$ on $k$ lifts to an isomorphism $\tau$ of $R_e$ onto $R'_e$ then $\tilde{\tau}$ lifts to an isomorphism of $R_e$ onto $R'_e$ which maps $R$ onto itself.

Let $G$ denote the automorphism group of $R_e$ with identity mapping $\epsilon$. Let $G_t = \{ \alpha \mid \alpha \in G, \alpha - \epsilon(R_e) \subset \epsilon^t R_e \}$ and $H_t = \{ \alpha \mid \alpha \in G_t, \alpha - \epsilon(\Pi) \subset \epsilon^{t+1} R_e \}$.

It is well known and not difficult to show that if $(e, p) = 1$ then $H_t = G_t$ for $t > 1$. Thus, in this case we have the extended chain of ramification groups

Received by the editors July 24, 1965.

1 This research was supported by NSF GP-4007.
All the factors of (1) save $G/G_1$ are evaluated in [1, Theorem 5]. Also, see [3, Theorem 6 and Corollary]. As an immediate consequence of Corollary 1 we have

**Corollary 3.** The group $G/G_1$ is isomorphic to the group of all automorphisms $\bar{\tau}$ on $k$ such that $H(u)^{-1}\bar{\tau}H(u)$ has an eth root in $k$.

It was shown in the middle thirties (for a discussion, see MacLane [3, p. 423]) that an unramified $v$-ring is determined by its residue field. A long standing question has been the following—can one characterize the isomorphically distinct rings $R_e$ in terms of the structure of the residue field $k$ and if so, how? In the tamely ramified case, $(e, p) = 1$, the answer is yes and the solution is given by [1, Theorem 3] in the case in which $k$ is perfect. Corollary 4 below yields the same conclusion without restriction on $k$.

As in [1, p. 495] we consider the equivalence relation "$\sim_e$" on $k^*$, the nonzero elements of $k$, in which $a \sim_e b$ if there is an automorphism $\bar{\tau}$ on $k$ such that $a^{-1}\bar{\tau}(b)$ is in $k^e$, the set of eth powers in $k^*$. Let $[a]$ represent the equivalence class containing $a$ and let $E$ be the set of all classes $[a]$.

**Corollary 4.** The rings $R_e$ and $R'_e$ of Theorem 1 are isomorphic if and only if $[H(u)] = [H(u')]$, thus the mapping $R_e \to [H(u)]$ induces a one to one correspondence between classes of isomorphic rings $R_e$ and $E$.

**Proof.** The first sentence follows immediately from Theorem 1. Thus the mapping $R_e \to [H(u)]$ is well defined, a fact which can be observed directly. Given $a \in k^*$ choose $u$ in $R$ such that $H(u) = a$. Thus $R_e = R(\pi)$, where $\pi$ is a root of $x^e - pu$, maps onto $[a]$. Thus the induced mapping is onto.

II. **Proof of Theorem 1.**

**Lemma 1.** Let $R_e$ and $R'_e$ be tamely ramified extensions of $R$ and let $\tau: R_e \to R'_e$ be an isomorphism which induces the automorphism $\bar{\tau}$ on the residue field $k$. Then there exists an isomorphism $\eta: R_e \to R'_e$ such that $\eta(R) = R$ and $\eta = \bar{\tau}$.

**Proof.** Since every automorphism on $k$ lifts to $R$ there is an automorphism $\alpha$ on $R$ such that $\alpha = \bar{\tau}^{-1}$. Then $\tau\alpha: R \to R'_e$ has the property $\tau\alpha - \epsilon(R) \subset \pi'R'_e$. Thus, by [2, Theorem 4] $\tau\alpha$ can be extended to an automorphism $\beta$ on $R'_e$ such that $\beta - \epsilon(R'_e) \subset \pi'R'_e$. Now $\tau^{-1}\beta(R) = \tau^{-1}\tau\alpha(\bar{\tau}) = R$. Let $\eta = \beta^{-1}\tau$. Then we have $\eta(R) = R$ and $\eta = \bar{\tau}^{-1}\tau = \bar{\tau}$.
Now, let \( \tau: R_e \to R'_e \) be an isomorphism. By Lemma 1 there exists an isomorphism \( \eta: R_e \to R'_e \) such that \( \eta(R) = R \) and \( \eta = \tau \). It follows from Theorem 3 of [1, p. 494] that \( H(u'^-1)\tau H(u) \) is in \( k^* \). The converse follows immediately from the same Theorem [1, Theorem 3] and the fact that every automorphism on \( k \) lifts to \( R \).

III. An example. Again we assume that \( (e, p) = 1 \).

Using product as the operation we write \( k_e \) for the group \( k^*/k_e \). The automorphisms of \( k \) induce a group \( G \) of automorphisms on \( k_e \). Let \( \phi \) represent the natural map of \( k^* \) onto \( k_e \). For \( x \) in \( k_e \) let \([x]_a\) denote the set of elements in \( k_e \) conjugate to \( x \) with respect to \( G \). We state without proof.

**Proposition 1.** Let \( a \) be in \( k^* \). The correspondence \([a] \to [\phi(a)]_a\) is a one to one correspondence between \( E \) and the classes of conjugate elements in \( k_e \) with respect to \( G \).

We consider the case in which \( k = GF(p^r) \), the field with \( p^r \) elements. Let \( n = (e, p^r - 1) \). Then for any \( b \) in \( k^* \), \( a \sim_b b \) if and only if \( a \sim_n b \). Also \( k_e \) is the cyclic group of order \( n \). Since all elements in a given conjugate class have the same order it follows that the number of conjugate classes is

\[
\sum_{q \mid n} \frac{\phi(q)}{I(q)}
\]

where \( \phi \) is the Euler \( \phi \) function and \( I(q) \) is the least positive integer \( s \) such that \( q \mid p^r - 1 \). We also require that \( \phi(1) = I(1) = 1 \). Thus, if \( N(e, k) \) is the number of isomorphically distinct rings \( R_e \) with residue field \( k \), we have,

\[
N(e, GF(p^r)) = \sum_{q \mid (e, p^r - 1)} \frac{\phi(q)}{I(q)}.
\]

In particular, if \( (e, p^r - 1) = 1 \), \( N(e, GF(p^r)) = 1 \), and if \( (e, p^r - 1) \mid p - 1 \)

\[
N(e, GF(p^r)) = \sum_{q \mid (e, p^r - 1)} \phi(q).
\]

Finally we note that the automorphisms on \( k \) which lift to \( R_e \) in the tamely ramified case are exactly those automorphisms \( \alpha \) such that \( \phi H(u) \) is left fixed by the mapping \( \alpha \) induces on \( k_e \). Thus every automorphism on \( GF(p^r) \) lifts to \( R_e \) if and only if \( (e, p^r - 1) \mid p - 1 \).
References

3. S. MacLane, Subfields and automorphism groups of p-adic fields, Ann. of Math. 40 (1939), 423-442.

Florida State University