EQUIVALENCE OF TAMELY RAMIFIED $v$-RINGS

NICKOLAS HEEREMA

1. Introduction. Let $R$ be a $v$-ring, that is, an unramified complete discrete valuation ring of characteristic zero with residue field $k$ having characteristic $p \neq 0$. Let $R\epsilon$ and $R\epsilon'$ 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 $R\epsilon$, 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 $\pi'$ be prime elements of $R\epsilon$ and $R\epsilon'$ respectively. Then we have $p = \pi^ru$ and $p = \pi'^ru'$ where $u$ and $u'$ are units in $R\epsilon$ and $R\epsilon'$. If $\tilde{\tau}$ is the automorphism on $k$ induced by the isomorphism $\tau: R\epsilon \rightarrow R\epsilon'$ 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 $R\epsilon$ onto $R\epsilon'$ 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 $R\epsilon$ 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 $R\epsilon$ onto $R\epsilon'$ then $\tilde{\tau}$ lifts to an isomorphism of $R\epsilon$ onto $R\epsilon'$ which maps $R$ onto itself.

Let $G$ denote the automorphism group of $R\epsilon$ with identity mapping $e$. Let

$$G_t = \{ \alpha \mid \alpha \in G, \alpha - e(R\epsilon) \subseteq \Pi^tR\epsilon \}$$

and

$$H_t = \{ \alpha \mid \alpha \in G_t, \alpha - e(\Pi) \subseteq \Pi^{t+1}R\epsilon \}.$$

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 $\tilde{\tau}$ on $k$ such that $H(u)^{-1}\tilde{\tau}H(u)$ has an $e$th root in $k$.

It was shown in the middle thirties (for a discussion, see MacLane [3, p. 423]) that an unramified $\nu$-ring is determined by its residue field. A long standing question has been the following—can one characterize the isomorphically distinct rings $\mathcal{R}_e$ 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 $\tilde{\tau}$ on $k$ such that $a^{-1}\tilde{\tau}(b)$ is in $k^e$, the set of $e$th 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 $\mathcal{R}_e$ and $\mathcal{R}_{e'}$ of Theorem 1 are isomorphic if and only if $[H(u)] = [H(u')]$, thus the mapping $\mathcal{R}_e \to [H(u)]$ induces a one to one correspondence between classes of isomorphic rings $\mathcal{R}_e$ and $E$.

**Proof.** The first sentence follows immediately from Theorem 1. Thus the mapping $\mathcal{R}_e \to [H(u)]$ is well defined, a fact which can be observed directly. Given $a \in k^*$ choose $u$ in $R$ such that $H(u) = a$. Thus $\mathcal{R}_e = R(\pi)$, 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 $\mathcal{R}_e$ and $\mathcal{R}_{e'}$ be tamely ramified extensions of $R$ and let $\tau: \mathcal{R}_e \to \mathcal{R}_{e'}$ be an isomorphism which induces the automorphism $\tilde{\tau}$ on the residue field $k$. Then there exists an isomorphism $\eta: \mathcal{R}_e \to \mathcal{R}_{e'}$ such that $\eta(R) = R$ and $\eta = \tilde{\tau}$.

**Proof.** Since every automorphism on $k$ lifts to $R$ there is an automorphism $\alpha$ on $R$ such that $\alpha = \tilde{\tau}^{-1}$. Then $\tau\alpha: R \to \mathcal{R}_{e'}$ has the property $\tau\alpha - \epsilon(R) \subseteq \pi' \mathcal{R}_{e'}$. Thus, by [2, Theorem 4] $\tau\alpha$ can be extended to an automorphism $\beta$ on $\mathcal{R}_{e'}$ such that $\beta - \epsilon(\mathcal{R}_{e'}) \subseteq \pi' \mathcal{R}_{e'}$. Now $\tau^{-1}\beta(R) = \tau^{-1}\tau\alpha(R) = R$. Let $\eta = \beta^{-1}\tilde{\tau}$. Then we have $\eta(R) = R$ and $\eta = \tilde{\beta}^{-1}\tilde{\tau} = \tilde{\tau}$. 

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
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 $\bar{\eta} = \bar{\tau}$. It follows from Theorem 3 of [1, p. 494] that $H(u'^{-1})\bar{\tau}H(u)$ 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 $[x]_G$ 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 $[a] \to [\phi(a)]_G$ 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 $k^*$, $a \sim b$ 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

$$\sum_{q|n} \frac{\varphi(q)}{I(q)}$$

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

$$N(e, GF(p^r)) = \sum_{q|n} \frac{\varphi(q)}{I(q)}.$$

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

$$N(e, GF(p^r)) = \sum_{q|n} \varphi(q).$$

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 $(e, p^r - 1) \mid p - 1$. 

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
References

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

Florida State University