CROSSED PRODUCTS AND HEREDITARY ORDERS

SUSAN WILLIAMSON

Introduction. Let S be the integral closure of a discrete rank one valuation ring R in a finite Galois extension of the quotient field of R, and denote the Galois group of the quotient field extension by G. It has been proved by Auslander and Rim in [4] that the trivial crossed product $\Delta(1, S, G)$ is an hereditary order for tamely ramified extensions S of R, and that $\Delta(1, S, G)$ is a maximal order if and only if S is an unramified extension of R. The purpose of this paper is to study the crossed product $\Delta(f, S, G)$ where $[f]$ is any element of $H^2(G, U(S))$ and S is a tamely ramified extension of R with multiplicative group of units $U(S)$.

The main theorem of Section 1 states that for an extension S of R the following three properties are equivalent:

(1) S is a tamely ramified extension of R

(2) the crossed product $\Delta(f, S, G)$ is an hereditary order for each $[f]$ in $H^2(G, U(S))$

(3) the trivial crossed product $\Delta(1, S, G)$ is an hereditary order.

We then give an example to show that not every hereditary order is equivalent to a crossed product over a tamely ramified extension.

In Section 2 we study the number of maximal two-sided ideals in the crossed product $\Delta(f, S, G)$. It has been proved by Harada in [6] that the number of maximal two-sided ideals in an hereditary order Λ over a discrete rank one valuation ring R in a central simple algebra Σ over the quotient field of R is equal to the length of a saturated chain of orders over R in Σ containing Λ. This is the main motivation for our study. Given a crossed product $\Delta(f, S, G)$ over a tamely ramified extension S of R we define the conductor group H_f of $\Delta(f, S, G)$ to be a certain subgroup of the inertia group of a maximal ideal of S. Then we show that the number of maximal two-sided ideals in $\Delta(f, S, G)$ is equal to the order of the conductor group H_f. In particular, the number

Received June 8, 1963.

of maximal two-sided ideals in the trivial crossed product is equal to the ramification index.

In Section 3 we motivate the naming of the conductor group of the crossed product $\Delta = \Delta(f, S, G)$ by proving that if Γ denotes any maximal order containing Δ, and $C_\Gamma(\Delta)$ is the conductor of Γ in Δ, then the length of $S/C_\Gamma(\Delta) \cap S$ is equal to $g(h-1)$ where g is the number of maximal ideals of S and h is the order of the conductor group H_f of $\Delta(f, S, G)$.

The following notation shall be in constant use throughout the paper. If R is a local ring, then $\overline{R}$ shall denote its residue class field. The multiplicative group of units of a ring R shall be denoted by $U(R)$. Unless otherwise stated, R shall always denote a discrete rank one valuation ring, S the integral closure of R in a finite Galois extension of the quotient field of R, and G the Galois group of the quotient field extension.

Let G be a finite group, R a commutative ring with identity element, and A a G-ring over R. Then each element f in $Z^2(G, U(A))$ gives rise to the *crossed product* $\Delta(f, A, G)$, namely the R-algebra which is the free (left) A-module with free generators u_σ indexed by the elements of G and with multiplication defined by $(au_\sigma)(bu_\tau) = ab^\sigma f(\sigma, \tau)u_{\sigma\tau}$ for a and b in A. The crossed product $\Delta(f, A, G)$ depends up to isomorphism only on the cohomology class $[f]$. Furthermore, given $[f]$ in $H^2(G, U(A))$ we can always choose the 2-cocycle f such that $f(\tau, 1) = f(1, \tau)$ for each element τ in G. Thus we shall always assume that the cocycle f is normalized so that u_1 is the identity element of $\Delta(f, A, G)$.

Let R be a domain with quotient field k, and let Σ be a central simple k-algebra. Then a subring Λ of Σ is said to be an *order* over R if Λ is a finitely generated R-module which spans Σ over k. An order is said to be an *hereditary order* if it is hereditary as a ring.

Let an extension S of a local ring R be an integral extension of integrally closed domains, such that the quotient field extension is finite and Galois with Galois group G. If f is an element of $Z^2(G, U(S))$, then $\Delta(f, S, G)$ is an order over R. The ring S is said to be a *tamely ramified* extension of R if there exists a maximal ideal P in S such that $\overline{S}_P$ is separably algebraic over $\overline{R}$ and the order of the inertia group of P is relatively prime to the field characteristic of $\overline{R}$. Since all the maximal ideals are conjugates, it follows that if

one maximal ideal of S has the above property, so does each maximal ideal.

The author expresses her appreciation of the direction given to her by Dr. Dock Sang Rim for the preparation of this paper, and also for the introduction to the study of hereditary orders given to her by Dr. Maurice Auslander.

1. The crossed product $\Delta(f, S, G)$

The main purpose of this section is to prove that every crossed product over a tamely ramified extension S of a discrete rank one valuation ring R is an hereditary order. The method of proof will be to reduce the problem to the inertial case by considering the inertia ring U of S over R.

The first theorem is a generalization of Maschke's Theorem on the semi-simplicity of the group ring, and will be useful in proving the assertion in the inertial case.

THEOREM 1.1. *Let G be a finite group of order n, and let k be a field of characteristic p such that p is relatively prime to n. If G operates trivlally on k, then every crossed product $\Delta = \Delta(f, k, G)$ is k-separable.*

Proof. Consider the exact sequence

$$0 \longrightarrow J \longrightarrow \Delta \otimes_k \Delta^\circ \xrightarrow{\varphi} \Delta \longrightarrow 0$$

of left $\Delta \otimes \Delta^\circ$-modules where Δ° denotes the opposite ring of Δ and φ is defined by $\varphi(\delta_1 \otimes \delta_2) = \delta_1 \delta_2$. This sequence splits if and only if there exists an element j_0 in J such that $jj_0 = j$ for all j in J.

Since p is relatively prime to n, we have that $1/n$ is in k. Now define $j_0 = \frac{1}{n} \sum_\sigma \left(1 \otimes 1 - \frac{1}{f(\sigma, \sigma^{-1})} u_\sigma \otimes u_{\sigma^{-1}}\right)$. Since J is generated as a left ideal in $\Delta \otimes \Delta^\circ$ by elements of the form $1 \otimes u_\tau - u_\tau \otimes 1$ where τ runs through all the elements of G, it suffices to show that $(1 \otimes u_\tau - u_\tau \otimes 1) j_0 = 1 \otimes u_\tau - u_\tau \otimes 1$ for any element τ in G; and this is true provided that

$$\sum \frac{f(\sigma^{-1}, \tau)}{f(\sigma, \sigma^{-1})} u_\sigma \otimes u_{\sigma^{-1}\tau} - \sum \frac{f(\tau, \sigma)}{f(\sigma, \sigma^{-1})} u_{\tau\sigma} \otimes u_{\sigma^{-1}} = 0$$

Consider $u_{\tau\rho} \otimes u_{\rho^{-1}}$ for some element ρ in G, and let ω in G satisfy $\omega = \tau\rho$. By repeated application of the associativity relation satisfied by the cocycle f, we can observe that $f(\omega^{-1}, \tau) f(\rho, \rho^{-1}) = f(\tau, \rho) f(\omega, \omega^{-1})$, so that

https://doi.org/10.1017/S0027763000011211 Published online by Cambridge University Press

$$\frac{f(\omega^{-1}, \tau)}{f(\omega, \omega^{-1})} u_\omega \otimes u_{\omega^{-1}\tau} = \frac{f(\tau, \rho)}{f(\rho, \rho^{-1})} u_{\tau\rho} \otimes u_{\rho^{-1}}.$$

Therefore $(1 \otimes u_\tau - u_\tau \otimes 1) \sum \frac{1}{f(\sigma, \sigma^{-1})} u_\sigma \otimes u_{\sigma^{-1}} = 0$, since the terms cancel in pairs. Hence the sequence splits, and we know that Δ is $\Delta \otimes \Delta^\circ$-projective, i.e. that Δ is k-separable.

We proceed to prove the assertion in the inertial case. Throughout the rest of this section we shall make use of the following fact which has been proved by Auslander and Goldman (see p. 5 of [3]).

LEMMA. *Let R be a discrete rank one valuation ring. If Λ is an R-algebra which is a finitely generated torsion free R-module such that the radical of Λ is left Λ-projective, then Λ is both left and right hereditary.*

PROPOSITION 1.2. *Let the extension S of R be a tamely ramified inertial extension of discrete rank one valuation rings such that the quotient field extension is finite and Galois with Galois group G. Then the radical of the crossed product $\Delta = \Delta(f, S, G)$ is $\Pi\Delta$, where Π denotes the prime element of S. Hence Δ is an hereditary order.*

Proof. Define $\bar{\Delta}$ to be the crossed product $\Delta(\bar{f}, \bar{S}, G)$ where the action of G on $\bar{S}$ is given by the natural homomorphism $G \to Aut(\bar{S}/\bar{R})$, and $\bar{f}$ is the image of f under the natural map $Z^2(G, U(S)) \to Z^2(G, U(\bar{S}))$. We observe that $\bar{\Delta}$ is semi-simple. For, since S is an inertial extension of R, we know that $\bar{S} = \bar{R}$, so that G acts trivially on $\bar{S}$. From the assumption that S is tamely ramified over R, it follows that the field characteristic of $\bar{S}$ is relatively prime to the order of G. Hence by Theorem 1.1 we have that $\bar{\Delta}$ is $\bar{S}$-separable and hence semi-simple.

By the preceding lemma it remains to show that $\operatorname{rad} \Delta = \Pi\Delta$. Since Δ is a finitely generated S-module, and $\Pi\Delta$ is a two-sided ideal in Δ, we know that $\Pi\Delta$ is contained in $\operatorname{rad} \Delta$. It is easily seen that $\bar{\Delta} = \Delta/\Pi\Delta$. Therefore $\Delta/\Pi\Delta$ is semi-simple and so $\operatorname{rad} \Delta = \Pi\Delta$. Using the fact that $\Pi\Delta$ is a free Δ-module, it follows from the lemma that Δ is an hereditary order.

PROPOSITION 1.3. *Let the extension S of R be a tamely ramified extension of discrete rank one valuation rings such that the quotient field extension is finite and Galois with Galois group G. Then the radical of the crossed product*

https://doi.org/10.1017/S0027763000011211 Published online by Cambridge University Press

$\Delta = \Delta(f, S, G)$ is $\Pi\Delta$ where Π is the prime element of S. Hence Δ is an hereditary order.

Proof. Let U be the inertial ring of S over R. By virtue of Proposition 1.2, we may as well suppose that U properly contains R. Since S is tamely ramified over R, we know that $\bar{S} = \bar{U}$ since $\bar{U}$ is the separable closure of $\bar{R}$ in $\bar{S}$. Therefore the extension S of U is a tamely ramified inertial extension of discrete rank one valuation rings. The Galois group of S over U is G_I, the inertia group of S. We now define $\Delta_I = \Delta(f_I, S, G_I)$ where f_I is the restriction of f to $G_I \times G_I$. By Proposition 1.2 we know that $\operatorname{rad}\Delta_I = \Pi\Delta_I$.

Let $\bar{\Delta} = \Delta/\Pi\Delta$ and $\bar{\Delta}_I = \Delta_I/\Pi\Delta_I$ and note that there is a natural injection of $\bar{\Delta}_I$ into $\bar{\Delta}$. We observe that $(\operatorname{rad}\bar{\Delta}) \cap \bar{\Delta}_I = 0$. For $(\operatorname{rad}\bar{\Delta}) \cap \bar{\Delta}_I$ is a nilpotent two-sided ideal in $\bar{\Delta}_I$. Therefore it is contained in $\operatorname{rad}\bar{\Delta}_I$, and hence $(\operatorname{rad}\bar{\Delta}) \cap \bar{\Delta}_I = 0$.

We prove finally that $\operatorname{rad}\bar{\Delta} = 0$. Note that $\bar{\Delta} = \Delta(\bar{f}, \bar{U}, G)$ where $\bar{f}$ is induced by f. Let $G = \bigcup_i G_I g_i$ be a right coset decomposition of G with respect to G_I. Then each element δ in can be written as $\delta = \sum_{i=1}^{t(\delta)} \delta_i$ where $\delta_i = \sum_h c_h^{(i)} u_{hg_i}$ with h in G_I and $c_h^{(i)}$ in $\bar{U}$. Let δ be an element in $\operatorname{rad}\bar{\Delta}$, and write $\delta = \sum_{i=1} \delta_i$. We claim that $\delta = 0$. The proof is by induction on $t(\delta)$. If $t(\delta) = 1$, then δ is in $(\operatorname{rad}\bar{\Delta}) \cap \bar{\Delta}_I$, and so $\delta = 0$. Let $t(\delta) = t$, and assume that $\gamma = 0$ for each element γ in $\operatorname{rad}\bar{\Delta}$ such that $t(\gamma) < t$. Since $\bar{S}$ is a Galois extension of $\bar{R}$ we can write $\bar{S} = \bar{R}(\theta)$ for some element θ in $\bar{S}$. Now consider the element $\alpha = \theta\delta - \delta g_t^{-1}(\theta) = \sum_{i=1}^{t-1} (\theta - g_i g_t^{-1}(\theta))\delta_i$. Since α is in $\operatorname{rad}\bar{\Delta}$, and $t(\alpha) < t$, we conclude from the induction hypothesis that $\alpha = 0$. Since $\theta - g_i g_t^{-1}(\theta) \neq 0$ for $i \neq t$, it follows that $\delta_i = 0$ for $i \neq t$, so that $\delta = \delta_t$. Then $\delta u_{g_t^{-1}}$ is in $(\operatorname{rad}\bar{\Delta}) \cap \bar{\Delta}_I$ and hence $\delta u_{g_t^{-1}} = 0$ and finally $\delta = 0$. This concludes the proof.

Finally we delete the requirement that S be a discrete rank one valuation ring, and prove the following theorem.

PROPOSITION 1.4. *Let S be a tamely ramified extension of a discrete rank one valuation ring R, such that the quotient field extension is finite and Galois with Galois group G. Then each crossed product $\Delta = \Delta(f, S, G)$ is an hereditary order.*

Proof. Let $\hat{R}$ be the completion of R, and consider $\hat{\Delta} = \Delta \otimes_R \hat{R}$. Since $\hat{R}$ is R-flat it is clear that Δ is an hereditary order over R if and only if $\hat{\Delta}$ is an

https://doi.org/10.1017/S0027763000011211 Published online by Cambridge University Press

hereditary order over $\hat{R}$ (see p. 7 of [3]). Note that $\hat{\Delta} = \hat{S}\Delta = \Delta(f, \hat{S}, G)$ whsre $\hat{S} = S \otimes_R \hat{R} = S_1 \oplus \cdots \oplus S_g$, and S_i denotes the completion of the localization of S at the maximal ideal P_i of S. If we let e_i be the identity element of S_i then G acts as a transitive permutation group on the set $(e_1, \ldots, e_g)$. We shall denote by G_i the decomposition group of P_i in the extension S of R.

Denote $e_i \hat{\Delta} e_i$ by Δ_i, and let $[f_i]$ be the image of $[f]$ under the natural map $H^2(G, U(S)) \to H^2(G_i, U(S_i))$. Then $\Delta_i = \Delta(f_i, S_i, G_i)$ and since the quotient field extension of the extension S_i of R has Galois group G_i, we know by Proposition 1.3 that Δ_i is an hereditary order and that $\operatorname{rad}\Delta_i = P_i\Delta_i$.

Next we observe that $\Delta_i \cap \operatorname{rad}\Delta$ is contained in $\operatorname{rad}\Delta_i$. For suppose that δ is in $\Delta_i \cap \operatorname{rad}\Delta$, and let δ_i be any element of Δ_i. Then $t_i(1+\delta_i\delta) = 1$ for some element t_i in Δ_i. Hence $e_i t_i e_i(e_i + \delta_i\delta) = e_i$ in Δ_i, and so δ is in $\operatorname{rad}\Delta_i$.

We show finally that $\operatorname{rad}\hat{\Delta} = (\operatorname{rad} S)\hat{\Delta}$. Suppose that δ is in $\hat{\Delta}$. Then we can write $\delta = \sum e_i\delta$. Let σ be any element of G and suppose that $\sigma(e_i) = e_k$. If δ is in $\operatorname{rad}\hat{\Delta}$, then by the above remark, $e_i\delta u_\sigma e_i$ is in $\operatorname{rad}\Delta_i$. Now suppose that δ is in $\operatorname{rad}\hat{\Delta}$, and write $\delta = \sum s_\tau u_\tau$ where s_τ is in $\hat{S}$ and τ is in G. Let ω and ρ be defined by $\tau = \sigma^{-1}\omega$ and $\rho = \sigma^{-1}\tau\sigma$. Then $\tau(e_k) = e_i$ if and only if $\sigma\tau(e_k) = e_k$, from which it follows that $e_i\delta u_\tau e_i = \sum_\rho e_i s_{\rho\sigma^{-1}} f(\rho\sigma^{-1}, \sigma) u_\rho$ for elements ρ in G_i. This equality together with the fact that $e_i\delta u_\sigma e_i$ is in $\operatorname{rad}\Delta_i$ implies that $e_i s_{\rho\sigma^{-1}} = e_i s_\tau$ is in $P_i\Delta_i$ for each τ in G. Hence $\operatorname{rad}\hat{\Delta}$ is contained in $(\operatorname{rad} S)\hat{\Delta}$. Since $(\operatorname{rad}\hat{S})\hat{\Delta}$ is a two-sided ideal in $\hat{\Delta}$, we conclude that $\operatorname{rad}\hat{\Delta} = (\operatorname{rad}\hat{S})\hat{\Delta}$. If $P_i = \Pi S_i$ then $\operatorname{rad}\hat{S}$ is the principal ideal $(\Pi_1, \ldots, \Pi_g)$. Since $(\operatorname{rad}\hat{S})\hat{\Delta}$ is a free-$\hat{\Delta}$ module, we conclude from the lemma to Proposition 1.1 that $\hat{\Delta}$ is an hereditary order over $\hat{R}$. Hence Δ is an hereditary order over R.

We shall make use of the following proposition which is due to Auslander and Rim (see [4]).

PROPOSITION 1.5. *Given an extension S of R, the trivial crossed product $\Delta(1, S, G)$ is hereditary if and only if S is a tamely ramified extension of R.*

Thus we have established the following theorem.

THEOREM 1.6. *Let R be a discrete rank one valuation ring, and S the integral closure of R in a finite Galois extension of the quotient field of R with Galois group G. Then the following statements are equivalent:*

(1) *S is a tamely ramified extension of R*

https://doi.org/10.1017/S0027763000011211 Published online by Cambridge University Press

(2) *the crossed product* $\Delta(f, S, G)$ *is an hereditary order for each* $[f]$ *in* $H^2(G, U(S))$

(3) *the trivial crossed product* $\Delta(1, S, G)$ *is an hereditary order.*

An equivalence relation on the set of hereditary orders $H'(R)$ over a discrete rank one valuation ring R is introduced in [2]. Namely, if Λ_1, and Λ_2 are in $H'(R)$, then Λ_1 is said to be equivalent to Λ_2 if there exist finitely generated free R-modules E_1 and E_2 such that

$$\Lambda_1 \otimes_R \mathrm{Hom}_R(E_1, E_1) \cong \Lambda_2 \otimes_R \mathrm{Hom}_R(E_2, E_2).$$

It is established in [2] that each separable order is equivalent to a crossed product over a Galois extension of R.

Remark. An hereditary order need not be equivalent to a crossed product over a tamely ramified extension. We show that this is true by an example.

For let R be the ring of 2-adic integers. Denote the quotient field of R by k, and let $K = k(\sqrt{2})$. Then the integral closure S of R in K is $R[\sqrt{2}]$. It is easily seen that S is a local domain with maximal ideal $(\sqrt{2})$, and the Galois group G of K over k is cyclic of order two, $G = (1, \sigma)$. Let $\Delta = \Delta(1, S, G)$. Then $\mathrm{rad}\,\Delta = (\sqrt{2}, 1 + u_\sigma)$. We define Γ by adjoining the element $(1 + u_\sigma)/2$ to Δ. Then Γ is an order, and $\mathrm{rad}\,\Gamma = \sqrt{2}\,\Gamma$. Since the radical of Γ is a free Γ-module, it follows that Γ is an hereditary order. Suppose that Γ is equivalent to a crossed product $\Delta(f, T, H)$ where T is an extension of R. Then there exist finitely generated free R-modules E_1 and E_2 such that

$$\Gamma \otimes_R \mathrm{Hom}_R(E_1, E_1) \cong \Delta(f, T, H) \otimes_R \mathrm{Hom}_R(E_2, E_2).$$

If $\mathrm{rad}\,T = (\alpha)$, then the above isomorphism must map $\sqrt{2}$ into αu where u is a unit in $\Delta(f, T, H) \otimes_R \mathrm{Hom}_R(E_2, E_2)$, so that $\alpha^2 = 2v$ for some unit v in T. Hence the ramification index of T over R must be two, and so T can not be a tamely ramified extension of R.

2. The conductor group of $\Delta(f, S, G)$

The purpose of this section is to give a criterion for determining the number of maximal two-sided ideals in the crossed product $\Delta(f, S, G)$ when S is a tamely ramified extension of a discrete rank one valuation ring. We first restrict the problem to the case when S is also a discrete rank one

https://doi.org/10.1017/S0027763000011211 Published online by Cambridge University Press

valuation ring, and then reduce the general problem to this case by taking completion with respect to the prime ideal of R.

Let the extension S of R be an integral extension of discrete rank one valuation rings such that their quotient field extension is finite and Galois. Then if we denote by G the Galois group of the quotient field extension, we have the exact sequence

$$(1) \to G_I \to G \to G(\bar{S}/\bar{R}) \to (1)$$

where G_I is the inertia group of S.

PROPOSITION 2.1. *Let the extension S of R be a tamely ramified extension of discrete rank one valuation rings such that the quotient field extension is finite and Galois with Galois group G. Then*

a) the inertia group G_I is cyclic and its order e is not divisible by the field characteristic of $\bar{R}$. Furthermore, $\bar{S}$ contains all the e^{th} roots of unity.

b) for each element τ in G, we have that $\tau(\zeta) = \zeta^{n(\tau)}$ for each e^{th} root of unity ζ in $\bar{S}$ where $n(\tau)$ is an integer defined modulo e by the relation $\tau\sigma\tau^{-1} = \sigma^{n(\tau)}$ and σ is a generator of G_I.

Proof. a) Replacing R by the inertia ring, we may assume that S is a tamely ramified inertial extension of R, so that $\bar{S} = \bar{R}$. Let Π be the prime element of S. For each element τ in G, we can write $\tau(\Pi) = s_\tau \Pi$ where s_τ is a unit in S. The map $\psi: G \to U(\bar{R})$ defined by $\psi(\tau) = \tau(\Pi)/\Pi \bmod (\Pi)$ is a group homomorphism. Since S is tamely ramified over R, it follows from Hilbert's ramification theory that the higher ramification groups vanish (see Theorem 25, p. 295 of [8]). The kernel of ψ is the second ramification group. Therefore ψ is a monomorphism and G is cyclic.

Let σ be a generator of G. Then $1 = \psi(\sigma)^e$ and so $\psi(\sigma)$ must be a primitive e^{th} root of unity, since ψ is a monomorphism.

Let ζ be the primitive e^{th} root of unity in $\bar{S}$ defined by $\zeta = \sigma(\Pi)/\Pi \bmod(\Pi)$ where σ is a generator of the inertia group G_I, and observe that ζ does not depend on the choice of the prime element Π. Then $\tau(\zeta) = \tau\sigma\tau^{-1}\tau(\Pi)/\tau(\Pi) \bmod(\Pi) = \sigma^{n(\tau)}(\Pi)/\Pi \bmod(\Pi) = \zeta^{n(\tau)}$.

Now let S and R be as above and consider a crossed product $\Delta(f, S, G)$ where $[f]$ is in $H^2(G, U(S))$. The number of maximal two-sided ideals in

https://doi.org/10.1017/S0027763000011211 Published online by Cambridge University Press

$\Delta(f, S, G)$ is the same as the number of simple components in $\Delta(\bar{f}, \bar{S}, G)$ where $[\bar{f}]$ is the image of $[f]$ under the canonical map $H^2(G, U(S)) \to H^2(G, U(\bar{S}))$. Thus the problem reduces to the following:

Given 1) a finite Galois field extension K of k and a finite group G together with an exact sequence

$$(1) \to G_I \to G \to G(K/k) \to (1)$$

such that G_I is a cyclic group whose order e is not divisible by the field characteristic of k;

2) that K contaius all the e^{th} roots of unity and if τ is any element of G, then $\tau(\zeta) = \sigma^{n(\tau)}$ for all the e^{th} roots of unity ζ where $n(\tau)$ is an integer defined modulo e by the relation $\tau\sigma\tau^{-1} = \sigma^{n(\tau)}$ and σ is a generator of G_I;

3) the cohomology class $[f]$ in $H^2(G, U(K))$

Problem Determine the number of simple components in $\Delta(f, K, G)$.

In order to do this we define for each cohomology class $[f]$ two subgroups of G_I associated with $[f]$.

Definition The group Γ_f is defined to be the maximal subgroup of G_I such that the image of Γ_f under the restriction map $H^2(G, U(K)) \to H^2(\Gamma_f, U(K))$ is trivial. The group H_f is defined to be the maximal subgroup of G_I such that $[f]$ is in the image of the inflation map $H^2(G/H_f, U(K)) \to H^2(G, U(K))$.

We shall call H_f *conductor group* of $\Delta(f, K, G)$; its meaning will be justified in the main theorem of this section. The group Γ_f is of technical nature.

The group H_f is contained in Γ_f, since the composition map $H^2(G/H_f, U(K)) \to H^2(G, U(K)) \to H^2(H_f, U(K))$ is trivial. If $G = G_I$, then it will follow from Proposition 2.3 that $H_f = \Gamma_f$.

Remark. The conductor group H_f need not equal Γ_f.

For let R be the ring of 3-adic integers, k its quotient field, and $K = k(i, \sqrt{3})$. Then the integral closure S of R in K is $R[i, \sqrt{3}]$ and the inertia ring U is $R[i]$. The inertia group $G_I = (1, \sigma)$ is the cyclic group of order two, and the Galois group G of K over k is the Klein four group $G = (1, \sigma, \tau, \sigma\tau)$. Define $f : G \times G \to U(S)$ by $f(\sigma, \sigma) = f(\tau, \tau) = f(\tau, \sigma) = f(\sigma\tau, \sigma) = f(\tau, \sigma\tau) = 1$, and $f(\sigma, \tau) = f(\sigma, \tau\sigma) = f(\sigma\tau, \tau) = f(\sigma\tau, \sigma\tau) = -1$. Then it can be verified by

https://doi.org/10.1017/S0027763000011211 Published online by Cambridge University Press

computation that f is in $Z^2(G, U(S))$, that $H_f = (1)$, and $\Gamma_f = G_I$.

We observe that, given $[f]$ in $H^2(G, U(K))$, we may assume that the restriction of f to $\Gamma_f \times \Gamma_f$ is trivial. For, it follows from the definition of Γ_f that there exists a map $\phi: \Gamma_f \to U(K)$ such that $f(\sigma, \tau) = \phi(\sigma)\phi^\sigma(\tau)/\phi(\sigma\tau)$ for all σ and τ in Γ_f. Extend the map $\phi: \Gamma_f \to U(K)$ to $\phi: G \to U(K)$ by defining $\phi(\rho) = \phi(\rho)$ if ρ is in Γ_f and $\phi(\rho) = 1$ if ρ is not in Γ_f. Set $f'(\sigma, \tau) = f(\sigma, \tau)\phi(\sigma\tau)/\phi(\sigma)\phi^\sigma(\tau)$. Then $[f'] = [f]$ and $f'(\sigma, \tau) = 1$ when both σ and τ are in Γ_f. From now on we shall always assume that each cocycle f is *properly normalized*, i.e. that $f(\sigma, \tau) = 1$ for all σ and τ in Γ_f.

Given a 2-cocycle f we have the following chain of crossed products:

$$\Delta(f, K, G) \supset \Delta(f_I, K, G_I) \supset \Delta(f_\Gamma, K, \Gamma_f) \supset \Delta(f_H, K, H_f)$$

where f_T denotes the restriction of f to $T \times T$. We have

PROPOSITION 2.2. *The number of simple components of $\Delta(f_I, K, G_I)$ is equal to the number of simple components of $\Delta(f_\Gamma, K, \Gamma_f)$ and the primitive orthogonal idempotents are given by*

$$\eta_i = \frac{1}{m}\sum_{k=1}^{m}(\zeta_i u_\gamma)^k$$

for $i = 1, \ldots, m$ where γ is a generator of Γ_f, m is the order of Γ_f and $\zeta_1, \zeta_2, \ldots, \zeta_m$ are the distinct m^{th} roots of unity.

Proof. Since G_I is cyclic, we have a canonical isomorphism $H^2(G_I, U(K)) \cong U(K)/U(K)^e$ where e is the order of G_I. Let $[f]$ correspond to a mod $U(K)^e$ under the above identification. Then m is the maximal divisor of e such that $a^{e/m}$ is in $U(K)^e$, i.e. e/m is the order of a in $U(K)/U(K)^e$. Let c be an element of $U(K)$ satisfying $a = c^m$. Then $\Delta(f_I, K, G_I) = K[X]/(X^e - a)$, and so the number of simple components of $\Delta(f_I, K, G_I)$ is equal to the number of irreducible factors of $X^e - a = \prod_{i=1}^{m}(X^{e/m} - \zeta_i c)$ in $K[X]$. Since K contains all the e^{th} roots of unity, it follows that each $X^{e/m} - \zeta_i c$ is irreducible over K. For let $\varphi(X)$ be an irreducible factor of $X^{e/m} - \zeta_i c$ in $K[X]$, and let α be a root of $\varphi(X)$. Then $N_{K(\alpha)/K}(\alpha) = \alpha^d\eta$ where η is an m^{th} root of unity and $d = \deg \varphi(X) = e/m$. Since $\alpha^d\eta$ and η are in K, we have that α^d is in K. Now $a^d = c^{md} = (\zeta_i c)^{md} = \alpha^{(c/m)md} = (\alpha^d)^e$, so that a^d is in $U(K)^e$. Hence $d \equiv 0 \mod (e/m)$. Since $d \leq e/m$, we must have $d = e/m$. Therefore deg $\varphi(X) = e/m$ and

https://doi.org/10.1017/S0027763000011211 Published online by Cambridge University Press

consequently $X^{e/m}-\zeta_i c$ is irreducible. Therefore the number of simple components of $\Delta(f_l, K, G_l)$ is equal to $m=$ the order of Γ_f.

On the other hand, assuming that f is properly normalized, we have an isomorphism $K[X]/(X^m-1)\cong\Delta(f_\Gamma, K, \Gamma_f)$ defined by $X\to u_\tau$ where γ is a generator of Γ_f. Consequently the number of simple components of $\Delta(f_\Gamma, K, \Gamma_f)$ is equal to $m=$ the order of Γ_f, since K contains all the m^{th} roots of unity. Since $\Delta(f_\Gamma, K, \Gamma_f)\subset\Delta(f_l, K, G_l)$ is an inclusion of commutative algebras, we conclude that the idempotent elements of $\Delta(f_l, K, G_l)$ are present in $\Delta(f_\Gamma, K, \Gamma_f)$. In order to compute the primitive idempotents, we next observe that $K[X]/(X^m-1)$ is the algebra direct sum of the ideals generated by $\frac{X^m-1}{X-\zeta_i}$. However, the fact that $mX^{m-1}=\sum_{i=1}^{m}\frac{X^m-1}{X-\zeta_i}$ implies that the primitive idempotents of $\Delta(f_l, K, G_l)$ are of the form $\eta_i=\frac{1}{m}[(\zeta_i u_\tau)^m+(\zeta_i u_\tau)^{m-1}+\cdots+(\zeta_i u_\tau)]$.

PROPOSITION 2.3. *Let f be a properly normalized 2-cocycle, and ρ an element of Γ_f. Then the cyclic group (ρ) generated by ρ is contained in H_f if and only if $f(\tau, \rho)=f(\rho^{n(\tau)}, \tau)$ for each element τ in G.*

Proof. If ρ is in H_f, then by the definition of H_f there exists a map $\phi: G\to U(K)$ together with a 2-cocycle g such that $f(\tau, \sigma)=g(\tau, \sigma)\phi(\tau\sigma)/\phi(\tau)\phi^\tau(\sigma)$ for τ and σ in G, and $g(\tau, \sigma)=1$ if τ or σ is in H_f. Then $f(\tau, \rho)=\phi(\tau\rho)/\phi(\tau)\phi^\tau(\rho)$ and $f(\rho^{n(\tau)}, \tau)=\phi(\tau\rho)/\phi(\rho^{n(\tau)})\phi(\tau)$. Since f and g are both trivial on $H_f\times H_f$, it follows that $\phi(\rho)=\eta$ for some t^{th} root of unity η where $t=$ the order of H_f. Using condition 2), we have that $\phi^\tau(\rho)=\tau(\eta)=\eta^{n(\tau)}=[\phi(\rho)]^{n(\tau)}$, and so we conclude that $f(\tau, \rho)=f(\rho^{n(\tau)}, \tau)$ for each τ in G.

Conversely, assume that ρ is in Γ_f, and that $f(\tau, \rho)=f(\rho^{n(\tau)}, \tau)$ for each τ in G. If ρ^i is any element of (ρ), we can observe that $f(\tau, \rho^i)=f(\rho^{in(\tau)}, \tau)$ for each τ in G. For by repeated application of the associativity relation for 2-cocycles together with the fact that f is trivial on $\Gamma_f\times\Gamma_f$ we have the equalities:

$$f(\tau, \rho^i)=\prod_{k=0}^{i-1}f(\tau\rho^k, \rho) \text{ and } f(\rho^{in(\tau)}, \tau)=\prod_{k=0}^{i-1}f(\rho^{n(\tau)}, \tau\rho^k)$$

It now follows from the assumption on f and ρ that $f(\tau, \rho^i)=f(\rho^{in(\tau)}, \tau)$ for each element τ in G.

https://doi.org/10.1017/S0027763000011211 Published online by Cambridge University Press

In order to show that (ρ) is contained in H_f we shall show that f is cohomologous to a 2-cocycle g with the property that $g(\tau, \sigma) = 1$ if τ or σ is in (ρ). Let $G = \bigcup_j (\rho)\tau_j$ be a right coset decomposition of G with respect to (ρ), and define $\phi: G \to U(K)$ by $\phi(\rho^i\tau_j) = 1/f(\rho^i, \tau_j)$. Now define g by $g(\tau, \sigma) = f(\tau, \sigma)\phi(\tau\sigma)/\phi^\tau(\sigma)\phi(\tau)$ for τ and σ in G. Let τ be any element of G and σ any element of (ρ). Using the above coset decomposition of G, write $\tau = \omega\tau_j$ where ω is in (ρ). Then from the definition of g together with the associativity relation and the assumption satisfied by f, it follows that $g(\tau, \sigma) = g(\omega\tau_j, \sigma) = f(\omega\sigma^{n(\tau)}, \tau_j) f(\omega, \sigma^{n(\tau)})/f(\omega\sigma^{n(\tau)}, \tau_j) = 1$ and that $g(\sigma, \tau) = f(\sigma\omega, \tau_j) f(\sigma, \omega)/f(\sigma\omega, \tau_j) = 1$. Thus g has the desired property and we conclude that (ρ) is in H_f.

PROPOSITION 2.4. *The number of simple components of $\Delta(f, K, G)$ is equal to the order of the conductor group H_f.*

Proof. The number of simple components of $\Delta(f, K, G)$ is equal to the number of primitive orthogonal idempotents required to generate the center of $\Delta(f, K, G)$. Since G_I is the kernel of the map $G \to G(K/k) \to (1)$, it follows that the center of $\Delta(f, K, G)$ is contained in $\Delta(f_I, K, G_I)$. For let $\delta = \sum k_\tau u_\tau$ be an element in the center of $\Delta(f, K, G)$, with $k_\tau \neq 0$. Let $K = k(\theta)$. Then $\delta\theta = \sum \tau(\theta) k_\tau u_\tau$, so that $\theta\delta = \delta\theta$ if and only if $\tau(\theta) = \theta$, i.e. if and only if τ is in G_I. Hence the center of $\Delta(f, K, G)$ is in $\Delta(f_I, K, G_I)$. Since we are assuming that f is properly normalized, we conclude that the idempotent elements in the center of $\Delta(f, K, G)$ are precisely those partial sums P of elements η_i such that P is in the center of $\Delta(f, K, G)$ where the η_i are defined as in Proposition 2.2.

So let $P = \sum_{i=1}^{p} \eta_i$ be any partial sum of η_i with a suitable reordering of the η_i. Since the elements of G_I act trivially on K, it follows that P is in the center of $\Delta(f, K, G)$ if and only if $u_\tau P = P u_\tau$ for each τ in G. But

$$u_\tau P = \sum_{k=1}^{m} \sum_{i=1}^{p} \frac{1}{m} \tau(\zeta_i^k) \frac{f(\tau, \gamma^k)}{f(\gamma^{kn(\tau)}, \tau)} u_\tau^{kn(\tau)} u_\tau$$

From condition 2) we have that $\tau(\zeta_i^k) = \zeta_i^{kn(\tau)}$, so that $u_\tau P = P u_\tau$ if and only if $f(\tau, \gamma^k) = f(\gamma^{kn(\tau)}, \tau)$ for each τ in G and each integer k such that $\sum_{i=1}^{p} \tau(\zeta_i^k)$ is non-zero. It now follows that P is in the center of $\Delta(f, K, G)$ if and only if

https://doi.org/10.1017/S0027763000011211 Published online by Cambridge University Press

P is in $\Delta(f_H, K, H_f)$, by an application of Proposition 2.3. Therefore $\Delta(f, K, G)$ has precisely as many simple components as $\Delta(f_H, K, H_f)$, and this number is equal to the order of H_f since f_H is trivial.

Throughout the rest of this section, S shall denote the integral closure of a discrete rank one valuation ring R in a finite Galois extension of the quotient field of R, and G the Galois group of the quotient field extension. Let $[f]$ be an element of $H^2(G, U(S))$. We shall compute the number of maximal two-sided ideals in $\Delta = \Delta(f, S, G)$ by considering the crossed product $\hat{\Delta} = \Delta \otimes_R \hat{R} = \Delta(f, \hat{S}, G)$ which is formed by taking the completion of Δ. As in the preceding section, $\hat{R}$ denotes the completion of R, and $\hat{S} = S_1 \oplus \cdots \oplus S_g$ where S_i is the completion of the localization of S at the maximal ideal P_i of S. Now $\hat{\Delta}$ contains the crossed product $\Delta_1 = \Delta(f_1, S_1, G_1)$ where G_1 is the decomposition group of P_1 and $[f_1]$ in $H^2(G_1, U(S_1))$ is defined by $f_1(\tau, \sigma) = e_1 f(\tau, \sigma)$ where e_1 is the identity element of S_1. If the extension S of R is tamely ramified, then we know from Section 1, that $\hat{\Delta}/\mathrm{rad}\,\hat{\Delta} = \Delta(\bar{f}, \oplus \bar{S}_i, G)$ and $\Delta_1/\mathrm{rad}\,\Delta_1 = \Delta(\bar{f}_1, \bar{S}_1, G_1)$, where $\bar{f}$ and $\bar{f}_1$ are induced by f in the obvious way. Hence the inclusion of crossed products $\hat{\Delta} \supset \Delta_1$ gives rise to the inclusion $\Delta(\bar{f}, \oplus \bar{S}_i, G) \supset \Delta(\bar{f}_1, \bar{S}_1, G_1)$.

If $[f]$ is an element of $H^2(G, U(S))$, then we define the *conductor group* H_f of $\Delta(f, S, G)$ to be the conductor group of the crossed product $\Delta(\bar{f}_1, \bar{S}_1, G_1)$. Thus the conductor group of $\Delta(f, S, G)$ is determined up to conjugation in G.

THEOREM 2.5. *Let S be a tamely ramified extension of a discrete rank one valuation ring R, and $[f]$ an element of $H^2(G, U(S))$. Then the number of maximal two-sided ideals in the crossed product $\Delta(f, S, G)$ is equal to the order of the conductor group of $\Delta(f, S, G)$.*

Proof. For convenience of notation, let $\Delta = \Delta(f, S, G)$. Since $\Delta/\mathrm{rad}\,\Delta = \hat{\Delta}/\mathrm{rad}\,\hat{\Delta}$, it follows that the number of maximal two-sided ideals in Δ is equal to the number of simple components of $\hat{\Delta}/\mathrm{rad}\,\hat{\Delta} = \Delta(\bar{f}, \oplus \bar{S}_i, G)$. To prove the theorem, we shall establish a one-to-one correspondence between the primitive orthogonal idempotents of $\Delta(\bar{f}, \oplus \bar{S}_i, G)$ and $\Delta(\bar{f}_1, \bar{S}_1, G_1)$. Since S is a tamely ramified extension of R it will then follow by applying Proposition 2.4 to the crossed product $\Delta(\bar{f}_1, \bar{S}_1, G_1)$ that the number of maximal two-sided ideals in Δ is precisely the order of H_f. For since the extension S of R is

https://doi.org/10.1017/S0027763000011211 Published online by Cambridge University Press

tamely ramified, the field extension $\overline{S}_1$ of $\overline{R}$ and the exact sequence

$$(1) \to G_I \to G_1 \to G(\overline{S}_1/\overline{R}) \to (1)$$

satisfy the hypothesis of Proposition 2.4, where G_I denotes the inertia group of P_1.

So, if η is an idempotent in the center of $\Delta(\bar{f}_1, \overline{S}_1, G_1)$, we define $x = \sum_j (u_{\tau_j})^{-1}\eta(u_{\tau_j})$ where $G = \bigcup_j G_1\tau_j$ is a left coset decomposition of G with respect to G_1. The element x is clearly an idempotent, and we next show that x is in the center of $\Delta(\bar{f}, \oplus\overline{S}_i, G)$. It is easily seen that x commutes with the elements of $\oplus\overline{S}_i$, and to prove that $(u_\tau)^{-1}(x)u_\tau = x$ for each τ in G, we shall show that the effect of conjugating x by u_τ is the permutation of the terms $(u_{\tau_j})^{-1}(x)u_{\tau_j}$ in the expression of x. So let τ be any element of G, and let $G_1\tau_k$ be the coset containing $\tau_j\tau$, so that $\tau_j\tau = \rho\tau_k$ for some element ρ in G_1. Then

$$\begin{aligned}(u_\tau)^{-1}&[(u_{\tau_j})^{-1}\eta u_{\tau_j}]u_\tau \\ &= \frac{\bar{f}(\tau^{-1}, \tau_j^{-1})\bar{f}^{\tau_\kappa^{-1}}(\rho^{-1}, \rho)\bar{f}^{\tau_k^{-1}\rho^{-1}}(\tau_j, \tau)\bar{f}(\tau_k^{-1}, \tau_k)}{\bar{f}(\tau^{-1}, \tau)\bar{f}^{\tau^{-1}}(\tau_j^{-1}, \tau_j)\bar{f}(\tau_k^{-1}, \rho^{-1})\bar{f}^{\tau_k^{-1}\rho^{-1}}(\rho, \tau_k)} = (u_{\tau_k})^{-1}\eta u_{\tau_k} \\ &= (u_{\tau_k})^{-1}\eta u_{\tau_k}\end{aligned}$$

since by the associativity property of $\bar{f}$ we have the relations

$$\bar{f}(\tau^{-1}, \tau) = \frac{\bar{f}(\tau_k^{-1}, \tau_k)\bar{f}^{\tau_k^{-1}}(\rho^{-1}, \rho)\bar{f}^{\tau_k^{-1}\rho^{-1}}(\tau_j, \tau)}{\bar{f}(\tau_k^{-1}, \rho^{-1})\bar{f}^{\tau_k^{-1}\rho^{-1}}(\rho, \tau_k)\bar{f}(\tau_k^{-1}\rho^{-1}, \tau_j)}$$

$$\bar{f}(\tau^{-1}, \tau_j^{-1}) = \frac{\bar{f}^{\tau^{-1}}(\tau_j^{-1}, \tau_j)}{\bar{f}(\tau_k^{-1}\rho^{-1}, \tau_j)}$$

Therefore $(u_\tau)^{-1}(x)u_\tau = x$, and it follows that each idempotent in the center of $\Delta(\bar{f}_1, \overline{S}_1, G_1)$ defines an idempotent in the center of $\Delta(\bar{f}, \oplus\overline{S}_i, G)$ in the above way.

On the other hand, if x is an idempotent in the center of $\Delta(\bar{f}, \oplus\overline{S}_i, G)$ then $x = \sum_j e_j x$ where e_j is the identity element of $\overline{S}_j$, and $e_1 x$ is an idempotent in the center of $\Delta(\bar{f}_1, \overline{S}_1, G_1)$. Let τ be an element of G such that $\tau^{-1}(e_1) = e_k$. Then $(u_\tau)^{-1}(e_1x)u_\tau = e_k x$, so that $x = \sum_j (u_{\tau_j})^{-1}(e_1x)u_{\tau_j}$.

Thus if x is an idempotent in the center of $\Delta(\bar{f}, \oplus\overline{S}_i, G)$, then x is of the form $x = \sum_j (u_{\tau_j})^{-1}\eta u_{\tau_j}$ where η is an idempotent in the center of $\Delta(\bar{f}_1, \overline{S}_1, G_1)$. Since x is primitive if and only if η is primitive, it follows that $\Delta(\bar{f}, \oplus\overline{S}_i,$

G) and $\Delta(\bar{f}_1, \overline{S}_1, G_1)$ have the same number of simple components, and this concludes the proof.

COROLLARY 2.6. *Let S be a tamely ramified extension of a discrete rank one valuation ring R. Then the number of maximal two-sided ideals in the trivial crossed product $\Delta(1, S, G)$ is equal to the order of the inertia group of any maximal of S in the extension S of R.*

Proof. If $[f]$ is trivial in $H^2(G, U(S))$, then $[\bar{f}_1]$ is trivial in $H^2(G_1, U(S_1))$. By the definition of the group H_f it follows that H_f is the inertia group whenever $[\bar{f}_1]$ is trivial.

3. The length of the conductor

Let S be a tamely ramified extension of a discrete rank one valuation ring R, and Γ a maximal order over R containing the hereditary order $\Delta = \Delta(f, S, G)$. The conductor $C_\Gamma(\Delta)$ of Γ in Δ is defined to be the set of all elements δ in Δ such that $\delta\Gamma$ is contained in Δ. We may also consider the ideal $C'_\Gamma(\Delta)$ defined by $C'_\Gamma(\Delta) = C_\Gamma(\Delta) \cap S$. Then $C'_\Gamma(\Delta)$ is the set of all elements s in S such that $s\Gamma$ is contained in Δ. The purpose of this section is to motivate the naming of the conductor group H_f of $\Delta(f, S, G)$ by proving that the length of $S/C'_\Gamma(\Delta)$ is equal to $g(h-1)$ where g is the number of maximal ideals of S, and h is the order of H_f.

As in the preceding sections we shall consider the completion $\hat{\Delta} = \Delta(f, \hat{S}, G)$ of Δ. Letting Γ_i for $i = 1, \ldots, h$ denote the maximal orders containing Δ, then the maximal orders containing $\hat{\Delta}$ are given by $\hat{\Gamma}_i = \Gamma_i \otimes_R \hat{R}$. For convenience of notation we shall denote the conductor of $\hat{\Gamma}_i$ in $\hat{\Delta}$ by C_i. From Theorem 3.3 of [6] we know that the conductors C_i are the minimal two-sided idempotent ideals of $\hat{\Delta}$. In order to compute the conductors C_i, we shall make use of the following well-known facts.

PROPOSITION 3.1. *Let the extension S of R be a tamely ramified extension of complete discrete rank one valuation rings, and let U denote the inertia ring of S over R. Then U contains a primitive n^{th} root of unity ζ, where n is the order of the inertia group. If σ is a generator of the inertia group, then $\sigma(\Pi) = \zeta\Pi$ for a proper choice of the prime element Π of S.*

Proof. From section 2 we know that $\overline{S} = \overline{U}$ contains a primitive n^{ih} root

https://doi.org/10.1017/S0027763000011211 Published online by Cambridge University Press

of unity. Since U is a complete local ring, it follows from Hensel's lemma that U contains a primitive n^{th} root of unity. Let P denote any prime element of S. Since S is totally ramified over U we know that $P^n = \pi u$ for some unit u in S, where π denotes the prime element of R. It follows from the fact that $\overline{S} = \overline{U}$ that there exists an element v in U such that $u \equiv v \bmod (P)$. Hence $u/v \equiv 1 \bmod (P)$, and we consider the polynomial $f(X) = X^n - u/v$ in $S[X]$. Then the polynomial $\bar{f}(X) = X^n - 1$ in $\overline{U}[X]$ is separable since the field characteristic of $\overline{U}$ is relatively prime to n. Since $\bar{f}(1) = 0$, it now follows from Hensel's lemma, that $f(X)$ has a root, say α, in S. Then $\alpha^n = u/v$ and $(P/\alpha)^n - \pi v = 0$, so we choose $\Pi = P/\alpha$.

We proceed to define the elements of $\hat{\Delta}$ which generate the ideals C_i. Let P_1 be a maximal ideal in the tamely ramified extension S, and denote by G_1, G_I, and U the decomposition group, inertia group, and inertia ring of P_1 respectively. If $[f]$ is any element of $H^2(G, U(S))$, let f_1 and f_I be the elements of $Z^2(G_1, U(S_1))$ and $Z^2(G_I, (S_1))$ induced by f in the usual way. We may assume that f_I is normalized in the sense of cyclic groups. If f_I corresponds to the element a of $U(U)$ under the canonical identification $H^2(G_I, U(S_1)) = U(U)/N(U(S_1))$, where $N(U(S_1))$ denotes the norm of $U(S_1)$ in $U(U)$, then it follows by an application of Hensel's lemma to the polynomial $X^e - a$, that $a = b^m$ for some element b in U where e is the order of G_I and m is the order of $\Gamma_{\bar{f}_1}$. Denoting the order of H_f by h, we define $c = b^{m/h}$, so that $c^h = a$.

We now define elements λ_i in $\hat{\Delta}$ for $i = 1, \ldots, h$ by

$$\lambda_i = \frac{1}{h} \sum_{k=1}^{h} \left(\frac{\zeta_i}{c} u_\sigma \right)^k$$

where the ζ_i are the distinct h^{th} roots of unity in U and σ is a generator of H_f. By a computation similar to that of Proposition 2.2 it follows that the λ_i form a system of mutually orthogonal idempotents in $\hat{\Delta}$.

PROPOSITION 3.2. *Let S be a tamely ramified extension of a discrete rank one valuation ring R, and $[f]$ an element of $H^2(G, U(S))$. Then*

1) *the two-sided ideals (λ_i) are the minimal two-sided idempotent ideals of $\hat{\Delta} = \Delta(f, \hat{S}, G)$, and therefore $C_i = (\lambda_i)$.*

2) *the elements λ_i satisfy the relation $\Pi^{-t}\lambda_i\Pi^t = \lambda_{i+t}$ for a proper choice of the prime element Π of S_1.*

https://doi.org/10.1017/S0027763000011211 Published online by Cambridge University Press

Proof. To prove 1), it suffices to show that the λ_i generate the simple components of $\hat{\Delta}/\mathrm{rad}\,\hat{\Delta}$. Recall that $\hat{\Delta}/\mathrm{rad}\,\hat{\Delta} = (\bar{f}, \oplus\overline{S}_i, G)$ where $\bar{f}$ is the image of f under the natural map $Z^2(G, U(S)) \to Z^2(G, U(\oplus\overline{S}_i))$. We observe next that $\bar{f}$ is cohomologous to a cocycle g in $Z^2(G, U(\oplus\overline{S}_i))$ such that g_1 is a properly normalized element of $Z^2(G_1, U(\overline{S}_1))$. For we know from Section 2 that $\bar{f}_1$ is cohomologous by some map $\phi_1\colon G_1 \to U(\overline{S}_1)$ to a cocycle g_1 in $Z^2(G_1, U(\overline{S}_1))$ such that g_1 is properly normalized. Extend ϕ_1 to a map $\phi\colon G \to U(\oplus\overline{S}_i)$ by defining $\phi(\tau) = 1$ if τ is in $G - G_1$, and $\phi(\tau) = \phi_1(\tau) + \sum_{i\neq 1} e_i$ if τ is in G_1. By setting $g(\tau, \sigma) = f(\tau, \sigma)\phi(\tau)\phi^{\tau}(\sigma)/\phi(\tau\sigma)$ we define a cocycle g with the desired property. We know from section 2 that the elements $\eta_i = \frac{1}{h}\sum_{k=1}^{h}(\zeta_i u_\sigma)^k$ generate the simple components of $\Delta(g, \oplus\overline{S}_i, G)$. Under the canonical isomorphism $\Delta(g, \oplus\overline{S}_i, G) \cong \Delta(\bar{f}, \oplus\overline{S}_i, G)$, the elements η_i are mapped onto the λ_i. It now follows that the λ_i generate the simple components of $\Delta(f, \oplus\overline{S}_i, G)$. Therefore by Lemma 3.2 of [6] the λ_i generate the minimal two-sided idempotent ideals of $\Delta(f, \hat{S}, G)$. By Theorem 3.3 of [6] we conclude that $C_i = (\lambda_i)$.

It follows from Proposition 3.1 that $\Pi^{-t}\lambda_i\Pi^t = \lambda_{i+t}$.

Let $G = \bigcup_j G_1\tau_j$ be a right coset decomposition of G with respect to the decomposition group G_1. Define Π_j in $\hat{S}$ by $\Pi_j = \tau_j^{-1}(\Pi)$ where Π is a prime element of S_1 satisfying the statement of Proposition 3.1. Then $N = \bigoplus_j \Pi_j$ is a generator of the radical of $\hat{S}$. From the above proposition it follows that $C_i = (\lambda_i) = (y_i)$ where y_i is the element of $\hat{\Delta}$ defined by $y_i = \sum_j (u_{\tau_j})^{-1}\lambda_i u_{\tau_j}$. The y_i are related by $N^{-i}y_1N^i = y_{i+1}$.

We know by Theorem 3.3 of [6] that each order containing $\Delta(f, S, G)$ is a union of minimal orders containing $\Delta(f, S, G)$.

PROPOSITION 3.3. *Let S be a tamely ramified extension of a discrete rank one valuation ring R. Then the minimal orders containing $\Delta(f, \hat{S}, G)$ are given by $\Lambda_i = \hat{\Delta}[y_i N^{e-1}/\pi]$ for $i = 1, \ldots, h$ where h is the order of the conductor group H_f, e is the order of the inertia group, and the brackets denote ring adjunction.*

Proof. The maximal two-sided idempotent ideals of $\Delta(f, \hat{S}, G)$ are the two-sided ideals D_i generated by the elements $y_1, \ldots, y_i^*, \ldots, y_h$ where y_i^* means to omit y_i. Since the $\bar{y}_j$ are in the center of $\Delta(\bar{f}, \oplus\overline{S}_i, G)$, the D_i are generated

https://doi.org/10.1017/S0027763000011211 Published online by Cambridge University Press

as left ideals in $\hat{\Delta}$ by elements of the form y_jN^t where $t=0, \ldots, h-1$ and $j \neq i$ when $t=0$. By Proposition 1.7 of [6], the fact that D_i is a maximal two-sided idempotent ideal implies that $\mathrm{End}(D_i)$ is a minimal order containing $\hat{\Delta}$ where $\mathrm{End}(D_i)$ denotes the left endomorphism ring of the $\hat{\Delta}$-module D_i. We next observe that the element y_iN^{e-1}/π is in $\mathrm{End}(D_i)$. For $(y_jN^t)(y_iN^{e-1}/\pi) = 0$ or y_jN^{t+e-1}/π with $t \geqq 1$, and in either case is in $\hat{\Delta}$. By the minimality of $\mathrm{End}(D_i)$, we conclude that $\mathrm{End}(D_i) = \hat{\Delta}[y_iN^{e-1}/\pi]$.

PROPOZITION 3.4. *Let S be a tamely ramified extension of a discrete rank one valuation ring R, and $[f]$ an element of $H^2(G, U(S))$. If Γ is a maximal order containing the crossed product $\Delta(f, S, G)$, then the length of $S/C'_\Gamma(\Delta)$ is equal to $g(h-1)$ where g is the number of maximal ideals of S and h is the order of the conductor group H_f of $\Delta(f, S, G)$.*

Proof. From Proposition 3.3 together with Theorem 3.3 of [6] we know that

$$\hat{\Gamma} = \hat{\Delta}[y_1N^{e-1}/\pi, \ldots, (y_iN^{e-1}/\pi)^*, \ldots, y_hN^{e-1}/\pi]$$

for some $i=1, \ldots, h$ where $(\ )^*$ indicates omission. The order $\hat{\Gamma}$ is generated as a right $\hat{\Delta}$-module by elements of the form $y_{i-k}N^{(e-1)(h-k)}/\pi^{(h-k)}$ for $k=1, \ldots, h-1$. Consider the element $y_{i-1}N^{(e-1)(h-1)}/\pi^{(h-1)}$. The least positive integer x for which $N^x y_{i-1}N^{(e-1)(h-1)}/\pi^{(h-1)}$ is in $\hat{\Delta}$ must satisfy $x+(e-1)(h-1) = e(h-1)$ so that $x=h-1$. It follows that $C'_\Gamma(\Delta) = (\mathrm{rad}\ S)^{h-1}$; therefore $S/C'_\Gamma(\Delta)$ has length $g(h-1)$.

References

[1] E. Artin, C. Nesbitt and R. Thrall, *Rings with Minimum Condition*, Michigan, (1955).

[2] M. Auslander and O. Goldman, *The Brauer group of a commutative ring*, Trans, Amer. Math. Soc. vol. **97** (1960), pp. 367-409.

[3] M. Auslander and O. Goldman, *Maximal orders*, Trans, Amer. Math. Soc. vol. **97** (1960), pp. 1-24.

[4] M. Auslander and D. S. Rim, *Ramification Index and Multiplicity*, Ill. J. of Math., Vol. **7** (1963) pp. 566-581.

[5] H. Cartan and S. Eilenberg, *Homological Algebra*, Princeton, (1956).

[6] M. Harada, *Hereditary orders*, Trans, Amer. Math. Soc. Vol. **107** (1963) pp. 273-290.

[7] D. G. Northcott, *An Introduction to Homological Algebra*, Cambridge University Press (1960).

[8] O. Zariski and P. Samuel, *Commutative Algebra*, Vol I, Van Nostrand, (1958).

[9] O. Zariski and P. Samuel, *Commutative Algebra*, Vol II, Van Nostrand, (1960).

Brandeis University
Waltham, Massachusetts