CROSSED PRODUCTS AND RAMIFICATION

SUSAN WILLIAMSON

Introduction. Let S be the integral closure of a complete discrete rank one valuation ring R in a finite Galois extension of the quotient field of R, and let G denote the Galois group of the quotient field extension. Auslander and Rim have shown in [3] that the trivial crossed product $\Delta(1, S, G)$ is an hereditary order if and only if S is a tamely ramified extension of R. And the author has proved in [7] that if the extension S of R is tamely ramified then the crossed product $\Delta(f, S, G)$ is a Π-principal hereditary order for each 2-cocycle f in $Z^2(G, U(S))$. (See Section 1 for the definition of Π-principal hereditary order.) However, the author has exhibited in [8] an example of a crossed product $\Delta(f, S, G)$ which is a Π-principal hereditary order in the case when S is a wildly ramified extension of R. The purpose of this paper is to present necessary and sufficient conditions for a crossed product $\Delta(f, S, G)$ to be a Π-principal hereditary order when the extension S of R has a separable residue class field extension.

Let S be an extension of R (with separable residue class field extension) and let C denote the center of the first ramification group. In Section 1 we define for each element $[f]$ of $H^2(G, U(S))$ a subgroup R_f of C called the radical group of $[f]$. The main theorem of the paper states that the crossed product $\Delta(f, S, G)$ is a Π-principal hereditary order if and only if the radical group of $[f]$ is trivial. As a corollary we obtain the result of Harada (see [10]) that if R has perfect residue class field, then $\Delta(f, S, G)$ is a Π-principal hereditary order if and only if S is a tamely ramified extension of R. In an appendix we present some facts concerning the cohomology of groups which shall be referred to in the paper.

The following notation shall be employed throughout the entire paper. If R is a ring then its multiplicative group of units shall be denoted by $U(R)$, and its radical by rad R. If R is a local ring, then $\overline{R}$ shall denote its residue

Received January 24, 1966.

class field. Unless otherwise stated, S shall always denote the integral closure of a complete 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. Since R is complete, S is also a complete discrete rank one valuation ring, and Π shall denote a prime element of S. The i^{th} ramification group of the extension S of R shall be denoted by G_i. That it to say, G_i is the set of all elements σ of G such that $\sigma(s) \equiv s \bmod \Pi^{i+1}$ for all s in S. Each group G_i is a normal subgroup of G, and the inertia group G_0 acts trivially on $\bar{S}$.

More generally, if G is a finite group and A is a G-ring over a unitary commutative ring R, then $[f]$ shall denote the cohomology class in $H^2(G, U(A))$ of the 2-cocycle f of $Z^2(G, U(A))$. Furthermore, if A is a local ring, then $\bar{f}$ shall denote the image of f under the natural map $Z^2(G, U(A)) \to Z^2(G, U(\bar{A}))$. For the definitions of crossed product and hereditary order we refer the reader to [7]. The definitions of tame ramification and wild ramification are given on pp. 88-89 of [6].

For the convenience of the reader we summarize some important facts about ramification groups which may be found in Chapter IV of [5]. Let S denote the integral closure of a complete discrete rank one valuation ring R in a finite Galois extension of the quotient field of R such that the residue class field extension is separable. If $\bar{R}$ has characteristic zero then the first ramification group vanishes. If the characteristic p of $\bar{R}$ is non-zero then G_1 is a p-group. The factor group G_0/G_1 is a cyclic group whose order is relatively prime to p. For $i \geq 1$, each factor group G_i/G_{i+1} is an Abelian p-group of type $(p, p, \ldots, p)$.

1. The radical group. Let S denote the integral closure of a complete discrete rank one valuation ring R in a finite Galois extension K of the quotient field k of R, and let G denote the Galois group of K over k. If $[f]$ is an element of $H^2(G, U(S))$ then the crossed product $\Delta(f, S, G)$ is an R-order in the central simple k-algebra $\Delta(f, K, G)$. If Π denotes a prime element of S it is easy to verify from the definition of crossed product that the left ideal $\Delta(f, S, G)\Pi$ of $\Delta(f, S, G)$ is in fact a two-sided ideal. Therefore Π is always contained in the radical of $\Delta(f, S, G)$ according to Lemma 1.4. In the case when $\Delta(f, S, G)\Pi$ is precisely the radical of $\Delta(f, S, G)$ we may conclude that the crossed product $\Delta(f, S, G)$ is an hereditary order by the Corollary to

Theorem 2.2 of [2], since $\Delta(f, S, G)\Pi$ is a free left $\Delta(f, S, G)$-module. This leads us to make the following definition.

DEFINITION. A crossed product $\Delta(f, S, G)$ is called *a Π-principal hereditary order* if its radical is generated by the prime element Π of S.

We have already established the existence of a large class of Π-principal hereditary orders, namely each crossed product $\Delta(f, S, G)$ in the case when S is a tamely ramified extension of R. The purpose of this paper is to study Π-principal hereditary orders in the more general case when the residue class field extension is separable. Observe that the crossed product $\Delta(f, S, G)$ is a Π-principal hereditary order if and only if the crossed product $\Delta(\bar{f}, \bar{S}, G)$ is a semi-simple ring.

Let S be an extension of R with $\bar{S}$ separable over $\bar{R}$, and let C denote the center of the first ramification group. In Sections 2 and 3 the question of the semi-simplicity of $\Delta(\bar{f}, \bar{S}, G)$ shall be reduced to the question of the semi-simplicity of $\Delta(\bar{f}, \bar{S}, C)$.

Therefore our object of study in Section 1 is the crossed product $\Delta(f, F, C)$ where C is an Abelian p-group which acts trivially on a field F of characteristic p. We shall define for each element $[f]$ of $H^2(C, U(F))$ a subgroup R_f of C and prove that $\Delta(f, F, C)$ is semi-simple if and only if R_f is trivial. The following remark establishes notation which shall be in constant use throughout this section.

Remark 1.1. Let $C = E_1 \times \cdots \times E_t$ be a decomposition of an Abelian p-group C into a direct product of cyclic p-groups. It is well known that such a decomposition of C is unique up to isomorphism except for the order of the cyclic components, (see Theorem 3.3.2 of [4]). Let F be a field of characteristic p such that C acts trivially on F. If $[f]$ is an element of $H^2(C, U(F))$ we may assume according to Cor. A. 3 that f has been normalized in the sense of Abelian p-groups, so that $f = f_1 \cdots f_t$ where each element f_i of $Z^2(E_i, U(F))$ is normalized in the sense of cyclic groups. The symbol $h_i(X)$ for $1 \leq i \leq t$ shall denote the polynomial $h_i(X) = X^{e_i} - a_i$ in $F[X]$ where e_i is the order of E_i, and a_i is an element of $U(F)$ such that $[f_i]$ corresponds to a_i mod $[U(F)]^{e_i}$ under the canonical identification $H^2(E_i, U(F)) = U(F)/[U(F)]^{e_i}$.

We next observe that the crossed product $\Delta(f, F, C)$ is isomorphic to a tensor product over F of factor rings of the polynomial ring $F[X]$.

PROPOSITION 1.2. *The crossed product* $\Delta(f, F, C)$ *is* F*-algebra isomorphic to the tensor product* $A_1 \otimes A_2 \otimes \cdots \otimes A_t$ *over* F *where* $A_i = F[X]/(h_i(X))$ *for* $1 \leq i \leq t$.

Proof. The proof is by induction on the number t of cyclic components of the Abelian p-group C. If $t=1$, then C is cyclic. Since f is normalized in the sense of cyclic groups, the map $\psi : \Delta(f, F, C) \to F[X]/(h_1(X))$ induced by defining $\psi(u_\sigma) = X$ is an F-algebra isomorphism where σ denotes a generator of C.

For the inductive step we now suppose that C has n cyclic components, say $C = E_1 \times \cdots \times E_{n-1} \times E_n$, and consider the subgroup $C_{n-1} = E_1 \times \cdots \times E_{n-1}$. Then $\Delta(f, F, C) = \Delta(gf_n, F, C_{n-1} \times E_n)$ where $g = f_1 \cdots f_{n-1}$. Using the fact that f is normalized in the sense of Abelian p-groups one can easily verify that the natural map

$$\psi : \Delta(gf_n, F, C_{n-1} \times E_n) \to \Delta(g, F, C_{n-1}) \otimes_F \Delta(f_n, F, E_n)$$

is an F-algebra isomorphism. The induction hypothesis states that the assertion of the proposition is true for Abelian p-groups with $n-1$ cyclic components. Therefore the crossed product $\Delta(g, F, C_{n-1})$ is F-algebra isomorphic to $A_1 \otimes \cdots \otimes A_{n-1}$. And since E_n is cyclic, it follows from the first part of the proof that $\Delta(f_n, F, E_n)$ is F-algebra isomorphic to A_n. Combining these results we conclude that $\Delta(f, F, C)$ is F-algebra isomorphic to $A_1 \otimes \cdots \otimes A_n$.

The next object is to establish a criterion for the semi-simplicity of $\Delta(f, F, C)$ in terms of the irreducibility of the polynomials $h_i(X)$ and thus establish a connection between the semi-simplicity of $\Delta(f, F, C)$ and cohomology. In order to do this we first prove two lemmas.

LEMMA 1.3. *Let* F *be a field, and let* $H(X)$ *be a non-constant polynomial in* $F[X]$. *Denote the factor ring* $F[X]/(H(X))$ *by* L_2. *If* L_1 *is a field containing* F, *then the tensor product* $L_1 \otimes_F L_2$ *is* L_1*-algebra isomorphic to* $L_1[Y]/(H(Y))$.

Proof. Define the map $\varphi : L_1 \otimes L_2 \to L_1[Y]/(H(Y))$ by $\varphi(\sum a_i \otimes f_i(X)/H(X)) = \sum a_i f_i(Y)/(H(Y))$ where the a_i are in L_1 and the f_i are in $F[X]$. It is easy to verify that φ is a well-defined L_1-algebra epimorphism.

In order to prove that φ is a monomorphism we first observe that $(1, X, \ldots, X^{n-1})$ is a generating set for L_2 over F where n is the degree of

https://doi.org/10.1017/S0027763000023977 Published online by Cambridge University Press

$H(X)$. Therefore any element of $L_1 \otimes L_2$ may be written in the form $\sum_{i=0}^{n-1} a_i \otimes X^i/(H(X))$ where the a_i are in L_1. Suppose now that $\sum a_i \otimes X^i/(H(X))$ is in the kernel of φ. Then the equalities $\varphi(\sum a_i \otimes X^i/(H(X))) = \sum a_i Y^i/(H(Y)) = 0$ imply that the polynomial $\sum_{i=0}^{n-1} a_i Y^i$ of $L_1[Y]$ is in the principal ideal generated by $H(Y)$, so that $\sum a_i Y^i = g(Y)H(Y)$ for some element $g(Y)$ of $L_1[Y]$. Now the degree of $\sum_{i=0}^{n-1} a_i Y^i$ is less than or equal to $n-1$. However, the degree of $g(Y)H(Y)$ is less than n if and only if $g(Y)$ is the zero polynomial since $H(Y)$ has degree n and L_1 is a field. Therefore $g(Y)$ is the zero polynomial, and so the equality $\sum a_i Y^i = g(Y)H(Y)$ implies that $a_i = 0$ for $0 \leq i \leq n-1$. Therefore $\ker \varphi = (0)$ and so φ is a monomorphism.

LEMMA 1.4. *Let the extension S of R be a ring extension. If S is a finitely generated left R-module and (rad $R)S = S($rad $R)$ then rad R is contained in rad S.*

Proof. To show that rad R is contained in rad S it suffices to show that if M is a finitely generated left S-module and $S(\text{rad } R)M = M$, then $M = 0$. The fact that $S(\text{rad } R) = (\text{rad } R)S$ implies that $S(\text{rad } R)M = (\text{rad } R)SM = (\text{rad } R)M$. Since M is a finitely generated left S-module and S is a finitely generated left R-module it follows that M is a finitely generated left R-module. Therefore the equality $(\text{rad } R)M = M$ implies that $M = (0)$. Hence $S(\text{rad } R)$ is contained in rad S.

PROPOSITION 1.5. *Let F be a field of characteristic $p \neq 0$, and let $H_i(X)$ for $1 \leq i \leq t$ be elements of $F[X]$ of the form $H_i(X) = X^{e_i} - a_i$ where each e_i is a p^{th} power. Let A denote the tensor product $L_1 \otimes \cdots \otimes L_t$ over F where $L_i = F[X]/(H_i(X))$. Then the following statements are equivalent*

1) *A is semi-simple*

2) *A is a field*

3) *each polynomial $H_i(X)$ is irreducible in a splitting field for $\prod_{j<i} H_j(X)$ over F.*

Proof. The proof is by induction on the number t of polynomials $H_i(X)$. We first prove that the statements are equivalent when $t = 1$. In this case A is of the form $A = F[X]/(H(X))$ where $H(X) = X^e - a$ and e is a p^{th} power. Since F has characteristic p, a factorization of $H(X)$ into a product of irreducible

https://doi.org/10.1017/S0027763000023977 Published online by Cambridge University Press

polynomials of $F[X]$ is of the form $H(X)=(X^m-b)^{e/m}$ where $b^{e/m}=a$ and m is a divisor of e. The radical of the commutative Artin ring $F[X]/(X^e-a)$ is generated by the residue class of the polynomial X^m-b. Therefore A is semi-simple if and only if $m=e$, that is if and only if $H(X)$ is irreducible in $F[X]$. Therefore 1) is equivalent to 3). However, the polynomial $H(X)$ is irreducible in $F[X]$ if and only if $F[X]/(H(X))$ is a field. Therefore 3) is equivalent to 2) and this completes the proof in the case when $t=1$.

For the inductive step we assume the equivalence of the statements for $t<n$, and prove their equivalence for $t=n$. Throughout the rest of the proof it shall be convenient to use the notation $A_i=L_1\otimes\cdots\otimes L_i$ for $1\leq i\leq n$, and $A_0=F$.

We show first that 1) implies 2). So suppose that $A=A_n$ is semi-simple. Using the induction hypothesis we shall prove that each A_i for $1\leq i\leq n-1$ must be a field. Observe that the natural map $A_i\to A$ is an injection because each A_i is a free F-module. Since A is a finitely generated commutative A_i-algebra, the radical of A_i is contained in the radical of A according to Lemma 1.4. From the semi-simplicity of A we conclude that A_i has zero radical. Hence A_i is semi-simple because it is an Artin ring. The induction hypothesis implies therefore that A_i is a field for $1\leq i\leq n-1$.

Now we may prove that 1) implies 2). For since A_{n-1} is a field, and $A=A_{n-1}\otimes L_n$, we know that A is A_{n-1}-algebra isomorphic to $A_{n-1}[Y]/(Y^{e_n}-a_n)$ by Lemma 1.3. Thus we have reduced the problem to the case $t=1$, and so the assumption that A is semi-simple implies that A is a field.

In order to prove that 1) implies 3) we first observe that if A is semi-simple, then each A_i for $1\leq i\leq n$ is a splitting field over F for the polynomial $\sum_{j\leq i}H_j(X)$. For by the above, the semi-simplicity of A implies that each A_i for $1\leq i\leq n$ is a field and is therefore A_{i-1}-algebra isomorphic to $A_{i-1}[Y]/(H_i(Y))$ according to Lemma 1.3. It now follows easily by induction that A_i is a splitting field for $\prod_{j\leq i}H_j(X)$ over F. Now we may prove that 1) implies 3). For the fact that A_i is A_{i-1}-algebra isomorphic to $A_{i-1}[Y]/(Y^{e_i}-a_i)$ together with the fact that A_i is a field implies that $H_i(Y)$ is irreducible over A_{i-1} which is a splitting field for $\prod_{j<i}H_j(X)$.

We prove next that 3) implies 2). Consider the n polynomials $H_i(X)$ and assume that each polynomial $H_i(X)$ is irreducible in a splitting field for $\prod_{j<i}H_j(X)$.

Then certainly each $H_i(X)$ for $i<n$ is irreducible in a splitting field for $\prod_{j<i} H_j(X)$. By the induction hypothesis we may conclude therefore that A_{n-1} is a field. We have already shown that if A_{n-1} is a field it is necessarily a splitting field for $\prod_{j<n} H_j(X)$. Now $A = A_{n-1} \otimes L_n$ is A_{n-1}-algebra isomorphic to $A_{n-1}[Y]/(H_n(Y))$ by Lemma 1.3. Since $H_n(X)$ is irreducible in $A_{n-1}[Y]$ we conclude that A is a field.

The trivial observation that 2) implies 1) completes the proof of the proposition.

Prop. 1.5 motivates the definition of the radical group which we present next. An element $[f]$ of $H^2(C, U(F))$ gives rise to a chain of fields $L_0 \subseteq L_1 \subseteq \cdots \subseteq L_{t-1}$ defined inductively in the following way. Let $L_0 = F$. When L_i has been defined, we then define L_{i+1} to be a splitting field for the polynomial $h_{i+1}(X)$ over L_i, (see Remark 1.1).

We define $R_{f,i}$ for $1 \leq i \leq t$ to be the maximal subgroup of E_i with the property that the image of $[f_i]$ under the natural map $H^2(E_i, U(F)) \to H^2(R_{f,i}, U(L_{i-1}))$ is trivial.

Definition. *The radical group R_f of an element $[f]$ of $H^2(C, U(F))$* is defined to be the direct product $R_{f,1} \times \cdots \times R_{f,t}$ where the $R_{f,i}$ are defined as above.

Observe that the definition of R_f depends upon the order of the cyclic components E_i of C. However, the non-triviality of R_f shall be seen to be independent of the order of the cyclic components of C (see Theorem 1.10). Once the order of the E_i has been fixed, the definition of R_f depends only upon the cohomology class of f.

It is convenient to make the following definition now.

Definition. Let the extension S of R have a separable residue class field extension, and let $[f]$ be an element of $H^2(G, U(S))$. Then *the radical group R_f of* $[f]$ is defined to be the radical group of $[\bar{f}]$ where $[\bar{f}]$ is the image of $[f]$ under the natural maps

$$H^2(G, U(S)) \to H^2(G, U(\bar{S})) \to H^2(C, U(\bar{S}))$$

and C is the center of the first ramification group of S over R.

The following observation is immediate from the definition of the radical group, since the higher ramification groups of a tamely ramified extension vanish.

PROPOSITION 1.6. *If S is a tamely ramified extension of R, then $R_f=(1)$ for each element $[f]$ of $H^2(G, U(S))$.*

The following example shows that R_f need not equal C.

EXAMPLE 1.7. Let $R=Z[X]_{(2)}$ and $S=R[\sqrt{2}]$. Then S is a wildly ramified extension of R and $C=(1, \sigma)$ is cyclic of order two. Let f be the element of $Z^2(C, U(S))$ defined by $f(\sigma, \sigma)=X$. Then since $h(Y)=Y^2-X$ is irreducible over $\bar{S}=(Z/(2Z))(X)$ we conclude that $R_f=(1)$.

The following proposition states necessary and sufficient conditions for the i^{th} component of the radical group to be trivial.

PROPOSITION 1.8. *The group $R_{f,i}$ is trivial if and only if $h_i(X)$ is irreducible in $L_{i-1}[X]$.*

Proof. Let $h_i(X)=X^{e_i}-a_i=(X^{m_i}-b_i)^{e_i/m_i}$ be a factorization of $h_i(X)$ in $L_{i-1}[X]$ with $X^{m_i}-b_i$ irreducible. Note that $b_i^{e_i/m_i}=a_i$. We shall prove that $R_{f,i}=(\sigma^{m_i})$ where σ is a generator of the cyclic group E_i. To show that (σ^{m_i}) is contained in $R_{f,i}$ we observe that f_i is cohomologous to the trivial 2-cocycle. For the order of (σ^{m_i}) is e_i/m_i and $H^2((\sigma^{m_i}), U(L_{i-1}))=U(L_{i-1})/[U(L_{i-1})]^{e_i/m_i}$.

It remains to show that $R_{f,i}$ is contained in (σ^{m_i}). Let σ^x denote a generator of $R_{f,i}$. Then $a_i=c_i^{e_i/x}$ for some element c_i in $U(L_{i-1})$. From the inclusion $(\sigma^{m_i})\subseteq R_{f,i}$ it follows that e_i/m_i divides e_i/x so that $(e_i/m_i)d=x$ for some positive integer d. The equalities $b_i^{e_i/m_i}=c_i^{e_i/x}=(c_i^d)^{e_i/m_i}$ imply that $b_i=c_i^d$. Therefore $X^{m_i}-b_i=(X^x-c_i)^d$. Since $X^{m_i}-b_i$ is irreducible over L_{i-1} we conclude that $d=1$ and so $x=m_i$. Therefore $R_{f,i}$ is contained in (σ^{m_i}).

The group $R_{f,i}$ is trivial therefore if and only if $m_i=e_i$, that is if and only if $h_i(X)$ is irreducible in $L_{i-1}[X]$.

PROPOSITION 1.9. *The radical group R_f is trivial if and only if each polynomial $h_i(X)$ is irreducible in a splitting field for $\prod_{j<i} h_j(X)$ over F.*

Proof. The radical group R_f is trivial if and only if each cyclic component $R_{f,i}$ is trivial. By Prop. 1.7, the group $R_{f,i}$ is trivial if and only if $h_i(X)$ is irreducible in $L_{i-1}[X]$. However, the field L_{i-1} was defined to be a splitting field for $\prod_{j<i} h_j(X)$ over F.

Now we may prove the main theorem of this section.

THEOREM 1.10. The following statements are equivalent

1) the crossed product $\Delta(f, F, C)$ is semi-simple

2) $\Delta(f, F, C)$ is a field

3) the radical group R_f is trivial

Proof. By Prop. 1.2, the crossed product $\Delta(f, F, C)$ is F-algebra isomorphic to the tensor product $A_1 \otimes \cdots \otimes A_t$ over F where $A_i = F[X]/(h_i(X))$. Combining the results of Prop. 1.5 and Prop. 1.9 we arrive at the desired equivalence.

The following corollary gives technical information about the radical of $\Delta(f, F, C)$ in the case when $\Delta(f, F, C)$ is not a field which shall be of use in Section 2. Let $C = E_1 \times \cdots \times E_t$ be a decomposition of the Abelian p-group C into a direct product of cyclic groups; and for convenience of notation let $E_0 = (1)$.

COROLLARY 1.11. *If the crossed product $\Delta(f, F, C)$ is not a field, then there exists an element of the form $u_\tau - \delta$ in rad $\Delta(f, F, C)$ where $\tau \neq 1$ is in E_q for some $q \geq 1$, and δ is in the subring $\Delta(f, F, E_1 \times \cdots \times E_{q-1})$.*

Proof. We assume as usual that the 2-cocycle f has been normalized in the sense of Abelian p-groups. The assumption that $\Delta(f, F, C)$ is not a field implies that the radical group R_f of $[f]$ is non-trivial according to the theorem. We may therefore consider the least positive integer q for which the component $R_{f,q}$ is non-trivial. By the choice of q it is clear that the crossed product $\Delta(f, F, E_1 \times \cdots \times E_{q-1})$ is a field which shall henceforth be denoted by L. Let σ denote a generator of E_q. Then the L-algebra map $\psi : \Delta(f, F, E_1 \times \cdots \times E_q) \to L[X]/(h_q(X))$ induced by defining $\psi(u_\sigma) = X$ is an L-algebra isomorphism. If $h_q(X) = (X^m - b)^{e/m}$ is a factorization of $h_q(X)$ in $L[X]$ with $X^m - b$ irreducible, then the fact that $L[X]/(h_q(X))$ is not a field implies that $m < e$. The radical of $L[X]/(h_q(X))$ is generated by the residue class of the element $X^m - b$, whose preimage in $\Delta(f, F, E_1 \times \cdots \times E_q)$ under ψ is of the form $u_\tau - \delta$ where $\tau = \sigma^m$ and δ is in $\Delta(f, F, E_1 \times \cdots \times E_{q-1})$. Note that $\tau \neq 1$ because $1 \leq m < e$. The fact that $\Delta(f, F, C)$ is a finitely generated commutative $\Delta(f, F, E_1 \times \cdots \times E_q)$-algebra now implies that $u_\tau - \delta$ is in rad $\Delta(f, F, C)$.

2. p-groups. In Section 1 we noted that the crossed product $\Delta(f, S, G)$ is a Π-principal hereditary order if and only if $\Delta(\bar{f}, \bar{S}, G)$ is a semi-simple ring. The purpose of this section is to establish that $\Delta(\bar{f}, \bar{S}, G_1)$ is semi-simple if and only if $\Delta(\bar{f}, \bar{S}, C)$ is semi-simple, where C denotes the center of the first ramification group G_1. Our object of study in this section is therefore the crossed product $\Delta(f, F, G_1)$ where G_1 is a p-group with trivial action on a field F of characteristic p.

The notion of a splitting field of a cohomology class shall play an important role in Sections 2 and 3 by reducing questions concerning semi-simplicity to the case of a trivial crossed product.

Definition. Let G be a finite group, and F and K fields such that K is a G-ring over F. Let $[f]$ be an element of $H^2(G, U(K))$. Then an extension field L of K is called *a splitting field of* $[f]$ if $[f]$ is in the kernel of the natural map $H^2(G, U(K)) \to H^2(G, U(L))$ induced by the inclusion of K in L. If L is a splitting field for $[f]$ we say that L is a splitting field of the crossed product $\Delta(f, K, G)$. Finally, if a splitting field L of $\Delta(f, K, G)$ is a purely inseparable extension of K we call L a *purely inseparable splitting field of* $\Delta(f, K, G)$.

Lemma 2.1. *Let F be a field of characteristic $p \neq 0$, and C an Abelian p-group with trivial action on F. Let $[f]$ be an element of $H^2(C, U(F))$. Then the crossed product $\Delta(f, F, C)$ has a purely inseparable splitting field L. In the case when $\Delta(f, F, C)$ is a field we may take $L = \Delta(f, F, C)$.*

Proof. Let $C = E_1 \times \cdots \times E_t$ be a decomposition of C into a direct product of cyclic groups. We may assume that f is normalized in the sense of Abelian p-groups, and write $f = f_1 \cdots f_t$ where the element f_i of $Z^2(E_i, U(F))$ is normalized in the sense of cyclic groups. Let a_i be an element of $U(F)$ such that $[f_i]$ corresponds to a_i mod $[U(F)]^{e_i}$ under the canonical identification $H^2(E_i, U(F)) = U(F)/[U(F)]^{e_i}$ where e_i denotes the order of E_i. Let L be the field obtained by adjoining the roots of the polynomials $X^{e_i} - a_i$ to F. Then L is a purely inseparable extension of F and $[f]$ is in the kernel of the map $H^2(C, U(F)) \to H^2(C, U(L))$ induced by the inclusion of F in L.

In the case when $\Delta(f, F, C)$ is a field let $L = \Delta(f, F, C)$. To verify that L is a splitting field of $\Delta(f, F, C)$ it is sufficient to observe that $X^{e_i} - a_i = (X - u_\sigma)^{e_i}$

https://doi.org/10.1017/S0027763000023977 Published online by Cambridge University Press

so that each polynomial $X^{e_i}-a_i$ splits into linear factors in $L[X]$. Since L is a splitting field for the polynomial $\prod_i (X^{e_i}-a_i)$ over F it is clear that L is a purely inseparable extension of F.

Let G_1 be a p-group with trivial action on a field F of characteristic p. The main theorem of this section states that the crossed product $\Delta(f, F, G_1)$ is semi-simple if and only if $\Delta(f, F, C)$ is a field where C is the center of G_1. The proof involves an inductive process.

Consider the following chain of subgroups of the p-group G_1

$$C_n \supset \cdots \supset C_i \supset \cdots \supset C_0 \supset C_{-1}$$

where the groups C_i are defined inductively in the following way. Let $C_{-1}=(1)$. When C_i has been defined, we then define C_{i+1} to be the preimage of $\overline{C_{i+1}}$ in G_1 where $\overline{C_{i+1}}$ is the center of G_1/C_i. Note that $C_0=C$ where C is the center of G_1, and $C_n=G_1$. It is easy to verify that each C_i is a normal subgroup of G_1. Furthermore, each inclusion $C_i\subset C_{i+1}$ is strict since G_1 is a p-group. The following lemma states a property of the subgroups C_i which shall be useful later in this section.

Lemma 2.2. *Let ρ be an element of C_k/C_{k-2} not in the subgroup C_{k-1}/C_{k-2}. Then there exists an element τ in G_1/C_{k-2} such that the commutator $c=\tau\rho\tau^{-1}\rho^{-1}$ is in C_{k-1}/C_{k-2} and $c\neq 1$.*

Proof. Suppose that $\tau\rho=\rho\tau$ for all elements τ in G_1/C_{k-2}. Since C_{k-1}/C_{k-2} is by definition the center of G_1/C_{k-2} it would then follow that ρ is in C_{k-1}/C_{k-2} which contradicts the assumption on ρ. Therefore we may consider an element τ of G_1/C_{k-2} such that $\tau\rho\neq\rho\tau$.

Now the isomorphism $(G_1/C_{k-2})/(C_{k-1}/C_{k-2})\approx G_1/C_{k-1}$ together with the fact that C_k/C_{k-1} is the center of G_1/C_{k-1} implies that τ commutes with ρ modulo C_{k-1}/C_{k-2}. Therefore $\tau\rho=c\rho\tau$ for some element c in C_{k-1}/C_{k-2} with $c\neq 1$.

The lemma concerning the existence of purely inseparable splitting fields shall be used to prove the next proposition.

Proposition 2.3. *Let G_1 be a p-group with trivial action on a field F of characteristic p, and let $[f]$ be an element of $H^2(G_1, U(F))$. Then there exists a chain of fields*

$$F=L_0\subset L_1\subset\cdots\subset L_i\subset\cdots\subset L_n$$

and 2-cocycles g_i in $Z^2(G_1, U(L_i))$ such that

1) *each extension $L_i \subset L_{i+1}$ is purely inseparable*

2) *g_i is cohomologous to the image of f in $Z^2(G_1, U(L_i))$ for each i*

3) *each g_i is in the image of the inflation map $Z^2(G_1/C_{i-1}, U(L_i)) \to Z^2(G_1, U(L_i))$*

Proof. The construction of the fields L_i and the 2-cocycles g_i is done inductively. Let $L_0 = F$ and $g_0 = f$. It is clear that L_0 and g_0 satisfy statements 1), 2), and 3). When L_i and g_i have been defined, we then define L_{i+1} and g_{i+1} in the following way.

For convenience of notation we denote the preimage of g_i in $Z^2(G_1/C_{i-1}, U(L_i))$ by g_i also. Then the field L_{i+1} is defined to be a purely inseparable splitting field for the crossed product $\Delta(g_i, L_i, C_i/C_{i-1})$. The existence of such a field L_{i+1} is guaranteed by Lemma 2.1; when $\Delta(g_i, L_i, C_i/C_{i-1})$ is a field we take $L_{i+1} = \Delta(g_i, L_i, C_i/C_{i-1})$.

We next use L_{i+1} in order to define the 2-cocycle g_{i+1}. Let $\hat{g}_i$ denote the image of g_i in $Z^2(G_1, U(L_{i+1}))$ under the map of $Z^2(G_1, U(L_i))$ into $Z^2(G_1, U(L_{i+1}))$ induced by the inclusion of L_i in L_{i+1}. From the definition of L_{i+1} it follows that the preimage of $[\hat{g}_i]$ in $H^2(G_1/C_{i-1}, U(L_{i+1}))$ is trivial on $C_i/C_{i-1} \times C_i/C_{i-1}$.

Consider the following diagram

$$\begin{array}{ccc}
H^2((G_1/C_{i-1})/(C_i/C_{i-1}),\ U(L_{i+1})) & \xrightarrow{\phi} & H^2(G_1/C_i,\ U(L_{i+1})) \\
\downarrow \text{inf} & & \downarrow \text{inf} \\
H^2(G_1/C_{i-1},\ U(L_{i+1})) & \xrightarrow{\text{inf}} & H^2(G_1,\ U(L_{i+1})) \\
\downarrow \text{res} & & \\
H^2(C_i/C_{i-1},\ U(L_{i+1})) & &
\end{array}$$

where the map ϕ is induced by the second Noether isomorphism theorem. It may be verified from the definitions of the maps that the diagram is commutative. Furthermore, by Prop. A.7 we know that the column is exact. By diagram chasing we conclude that there exists a 2-cocycle g_{i+1} in $Z^2(G_1, U(L_{i+1}))$ cohomologous to $\hat{g}_i$ and in the image of the inflation map $Z^2(G_1/C_i, U(L_{i+1})) \to Z^2(G_1, U(L_{i+1}))$. Observe that since the map $H^2(G_1/C_i, U(L_{i+1})) \to H^2(G_1, U(L_{i+1}))$ is an injection, we may assume that the preimage of g_{i+1} in $Z^2(G_1/C_i, U(L_{i+1}))$ is normalized on $C_{i+1} \times C_{i+1}$ in the sense of Abelian p-groups.

The notation used in the statement of Prop. 2.3 shall be in use throughout the rest of Section 2. The next object is to prove that each crossed product

https://doi.org/10.1017/S0027763000023977 Published online by Cambridge University Press

$\Delta(g_i, L_i, C_i/C_{i-1})$ is a field whenever $\Delta(f, F, C)$ is a field. In order to do this we present three lemmas. The first two are of a general nature and shall be referred to several times in the paper. The third lemma gives technical information about the g_i and L_i of Prop. 2.3.

LEMMA 2.4. *Let the extension S of R be an extension of Artin rings. Then* (*rad* S) $\cap R$ *is a nilpotent two-sided ideal of* R. *Therefore* (*rad* S) $\cap R$ *is contained in rad* R.

Proof. Since S is an Artin ring it is well known that rad S is a nilpotent two-sided ideal of S. It follows easily now that (rad S) $\cap R$ is a nilpotent two-sided ideal of R and is therefore contained in rad R.

LEMMA 2.5. *Let G be a finite group, R a unitary commutative ring, and A a G-ring over R. Let $G = \cup H\tau_i$ be a disjoint right coset decomposition of G relative to the subgroup H of G. If $[f]$ is an element of $H^2(G, U(A))$, then the crossed product $\Delta(f, A, G)$ is a free left $\Delta(f, A, H)$-module with free generators* $\{u_{\tau_i}\}$.

Proof. Clearly the set $\{u_{\tau_i}\}$ generates $\Delta(f, A, G)$ as a left $\Delta(f, A, H)$-module. In order to show that $\{u_{\tau_i}\}$ is a free basis we shall show that if $\delta = \sum \delta_i u_{\tau_i} = 0$ with the δ_i in $\Delta(f, A, H)$, then $\delta_i = 0$ for each i. Write $\delta_i = \sum_h a_h^{(i)} u_h$ where each $a_h^{(i)}$ is in A and each h is in H. Then $\delta = \sum_i \sum_h a_h^{(i)} f(h, \tau_i) u_{h\tau_i}$. The coefficient of $u_{h\tau_i}$ is therefore $a_h^{(i)} f(h, \tau_i)$. Since $\Delta(f, A, G)$ is a free left A-module with free generators u_τ for τ in G, and the $f(h, \tau_i)$ are in $U(A)$, we conclude that $a_h^{(i)} = 0$ for each h and i. Therefore $\delta_i = 0$ for each i.

Denote the crossed product $\Delta(g_{k-1}, L_{k-1}, C_k/C_{k-2})$ by Δ_k and the crossed product $\Delta(g_{k-1}, L_{k-1}, C_{k-1}/C_{k-2})$ by Δ_{k-1}. Observe that Δ_{k-1} is a subring of Δ_k.

LEMMA 2.6. *The crossed products Δ_k and Δ_{k-1} satisfy the following rules*

1) $u_\tau(\text{rad } \Delta_k)(u_\tau)^{-1} \subset \text{rad } \Delta_k$ *for each τ in G_1/C_{k-2}*

2) $(\text{rad } \Delta_k) \cap \Delta_{k-1} \subset \text{rad } \Delta_{k-1}$

3) *Δ_{k-1} is contained in the center of Δ_k*

Proof. In order to prove statement 1) we first observe that rad Δ_k is a nilpotent two-sided ideal of Δ_k since Δ_k is an Artin ring. Using the fact that rad Δ_k is two-sided together with the fact that C_k/C_{k-2} is a normal subgroup of G_1/C_{k-2} we can conclude that $u_\tau(\text{rad } \Delta_k)(u_\tau)^{-1}$ is a two-sided ideal of Δ_k.

And the nilpotency of $u_\tau(\text{rad } \Delta_k)(u_\tau)^{-1}$ follows immediately from that of rad Δ_k. Therefore, since $u_\tau(\text{rad } \Delta_k)(u_\tau)^{-1}$ is a nil ideal of Δ_k we know that it is contained in rad Δ_k.

Assertion 2) follows immediately from Lemma 2.4.

We shall make use of Prop. A. 1 to prove that Δ_{k-1} is contained in the center of Δ_k. For let $\lambda = \sum a_\rho u_\rho$ denote any element of Δ_{k-1}, where the elements ρ are in C_{k-1}/C_{k-2} and the a_ρ are in L_{k-1}. Since C_k/C_{k-2} acts trivially on L_{k-1}, we know that λ is in the center of Δ_k if and only if $\lambda u_\tau = u_\tau \lambda$ for each element τ of C_k/C_{k-2}. Now $\lambda u_\tau = \sum a_\rho g_{k-1}(\rho, \tau) u_{\rho\tau}$. On the other hand, $u_\tau \lambda = \sum a_\rho g_{k-1}(\tau, \rho) u_{\tau\rho} = \sum a_\rho g_{k-1}(\rho, \tau) u_{\rho\tau}$ since C_{k-1}/C_{k-2} is in the center of C_k/C_{k-2} and $g_{k-1}(\tau, \rho) = g_{k-1}(\rho, \tau)$ according to Prop. A. 1. Therefore $\lambda u_\tau = u_\tau \lambda$ for every λ in Δ_{k-1} and τ in C_k/C_{k-2}, and so Δ_{k-1} is contained in the center of Δ_k.

It is in the next proposition that we make use of the fact that the extension L_{i+1} of L_i is purely inseparable for each i.

PROPOSITION 2.7. *If the crossed product $\Delta(f, F, C)$ is a field then each crossed product $\Delta(g_i, L_i, C_i/C_{i-1})$ is a field.*

Proof. The proof is by contradiction. Suppose therefore that not all the commutative rings $\Delta(g_i, L_i, C_i/C_{i-1})$ are fields. By hypothesis, $\Delta(g_0, L_0, C_0) = \Delta(f, F, C)$ is a field so we may consider the least positive integer k such that $\Delta(g_k, L_k, C_k/C_{k-1})$ is not a field. We shall show first that the assumption that $\Delta(g_k, L_k, C_k/C_{k-1})$ is not semi-simple implies that $\Delta(g_{k-1}, L_{k-1}, C_k/C_{k-2})$ is not semi-simple. Then we shall show that the semi-simplicity of $\Delta(g_{k-1}, L_{k-1}, C_{k-1}/C_{k-2})$ implies the semi-simplicity of the crossed product $\Delta(g_{k-1}, L_{k-1}, C_k/C_{k-1})$ and thus arrive at a contradiction.

We proceed to show that $\Delta(g_{k-1}, L_{k-1}, C_k/C_{k-2})$ is not semi-simple. The first step is to establish a connection between $\Delta(g_{k-1}, L_{k-1}, C_k/C_{k-2})$ and the commutative ring $\Delta(g_k, L_k, C_k/C_{k-1})$. It follows from Prop. A. 7 that the sequence $(1) \to H^2(C_k/C_{k-2}, U(L_k)) \to H^2(C_k, U(L_k))$ is exact. Since g_k is cohomologous to g_{k-1} in $Z^2(C_k, U(L_k))$ we conclude therefore that their preimages are cohomologous in $Z^2(C_k/C_{k-2}, U(L_k))$ by some map $\phi : C_k/C_{k-2} \to U(L_k)$. Then the map $\psi : \Delta(g_k, L_k, C_k/C_{k-2}) \to \Delta(g_{k-1}, L_k, C_k/C_{k-2})$ induced by defining $\psi(au_\rho) = a\phi(\rho)u_\rho$ for a in L_k and ρ in C_k/C_{k-2} is an L_k-algebra isomorphism. The following diagram establishes the desired relation between the crossed products $\Delta(g_{k-1}, L_{k-1}, C_k/C_{k-2})$ and $\Delta(g_k, L_k, C_k/C_{k-1})$. Observe that the columns are exact.

$$\begin{array}{ccc} \Delta(g_k, L_k, C_k/C_{k-2}) & \xrightarrow{\psi} & \Delta(g_{k-1}, L_k, C_k/C_{k-2}) \\ \downarrow \alpha & & \uparrow \\ \Delta(g_k, L_k, C_k/C_{k-1}) & & \Delta(g_{k-1}, L_{k-1}, C_k/C_{k-2}) \\ \downarrow & & \uparrow \\ (1) & & (1) \end{array}$$

Explicitly, the map α is defined as follows. Let N be the left ideal of $\Delta(g_k, L_k, C_k/C_{k-2})$ generated by the set of all elements of the form $1-u_\rho$ for ρ in C_{k-1}/C_{k-2}. The ideal N is in fact two-sided, and the natural map $\Delta(g_k, L_k, C_k/C_{k-2})/N \to \Delta(g_k, L_k, C_k/C_{k-1})$ is an L_k-algebra isomorphism. Then α is defined to be the composition of the natural maps

$$\Delta(g_k, L_k, C_k/C_{k-2}) \to \Delta(g_k, L_k, C_k/C_{k-2})/N \to \Delta(g_k, L_k, C_k/C_{k-1}).$$

Note that the preimage of rad $\Delta(g_k, L_k, C_k/C_{k-1})$ is contained in rad $\Delta(g_k, L_k, C_k/C_{k-2})$ since N is contained in rad $\Delta(g_k, L_k, C_k/C_{k-2})$.

Now let $C_k/C_{k-1} = E_1 \times \cdots \times E_t$ be a decomposition of the Abelian p-group C_k/C_{k-1} into a direct product of cyclic groups. The assumption that $\Delta(g_k, L_k, C_k/C_{k-1})$ is not semi-simple implies by Cor. 1.11 that there exists an element of the form $u_{\bar\tau} - \bar\delta$ in rad $\Delta(g_k, L_k, C_k/C_{k-1})$ where $\bar\tau$ is an element different from $\bar 1$ in E_q for some q satisfying $1 \le q \le t$ and $\bar\delta$ is in $\Delta(g_k, L_k, E_1 \times \cdots \times E_{q-1})$. We may therefore consider an element $u_\tau - \delta$ of rad $\Delta(g_k, L_k, C_k/C_{k-2})$ in the preimage of $u_{\bar\tau} - \bar\delta$.

We now use the element $u_\tau - \delta$ to produce a non-zero element x in the radical of $\Delta(g_{k-1}, L_{k-1}, C_k/C_{k-2})$. Write $\psi(\delta)$ in the form $\psi(\delta) = \sum a_\rho u_\rho$ where each ρ is in C_k/C_{k-2} and the elements a_ρ are in L_k. Now by the assumption on k we have taken $L_k = \Delta(g_{k-1}, L_{k-1}, C_{k-1}/C_{k-2})$, so we may consider the isomorphism

$$\theta : L_k \to \Delta(g_{k-1}, L_{k-1}, C_{k-1}/C_{k-2})$$

of subfields of $\Delta(g_{k-1}, L_k, C_k/C_{k-2})$ which leaves L_{k-1} element-wise fixed. Define the element x of $\Delta(g_{k-1}, L_{k-1}, C_k/C_{k-2})$ by setting $x = \phi(\tau)u_\tau - \delta_1$ where $\delta_1 = \sum \theta(a_\rho)u_\rho$.

The next step is to show that x is in rad $\Delta(g_{k-1}, L_k, C_k/C_{k-2})$; and to do this it suffices to show that the image $\overline{\psi^{-1}(x)}$ of $\psi^{-1}(x)$ in $\Delta(g_k, L_k, C_k/C_{k-1})$

https://doi.org/10.1017/S0027763000023977 Published online by Cambridge University Press

is in the radical. Since $\Delta(g_k, L_k, C_k/C_{k-1})$ is a commutative Artin ring, $\overline{\psi^{-1}(x)}$ is in the radical if and only if $\overline{\psi^{-1}(x)}$ is nilpotent. In order to prove the nilpotency of $\overline{\psi^{-1}(x)}$ we prove first that $\bar{\delta}^P = \overline{\psi^{-1}(\delta_1)}^P$ where P is the degree of L_k over L_{k-1}. (Since L_k is purely inseparable over L_{k-1} we have the inclusion $L_k^P \subset L_{k-1}$.) Now $\bar{\delta} = \overline{\psi^{-1}(\sum a_\rho u_\rho)}$ so that

$$\bar{\delta}^P = \sum [\overline{\psi^{-1}(a_\rho)\psi^{-1}(u_\rho)}]^P = \sum \overline{\psi^{-1}(a_\rho^P)\psi^{-1}(u_\rho^P)}.$$

On the other hand, using the fact that a_ρ^P is in L_{k-1} and is therefore left fixed by θ we obtain the equalities

$$\begin{aligned}\overline{\psi^{-1}(\delta_1)}^P &= \sum \overline{\psi^{-1}(\theta(a_\rho^P))\psi^{-1}(u_\rho^P)} = \sum \overline{\psi^{-1}(a_\rho^P)\psi^{-1}(u_\rho^P)} \\ &= \bar{\delta}^P\end{aligned}$$

Since $u_{\bar{\tau}} - \bar{\delta}$ is in the radical of an Artin ring, we have that $(u_{\bar{\tau}} - \bar{\delta})^N = 0$ for some positive integer N. It is easy now to verify that $\overline{\psi^{-1}(x)}$ is nilpotent. For $\overline{\psi^{-1}(x)}^{PN} = [u_{\bar{\tau}} - \overline{\psi^{-1}(\delta_1)}]^{PN} = u_{\bar{\tau}}^{PM} - \bar{\delta}^{PN} = [u_{\bar{\tau}} - \bar{\delta}]^{PN} = \bar{0}$. This concludes the proof of the assertion that x is in rad $\Delta(g_{k-1}, L_k, C_k/C_{k-2})$.

Since x is in (rad $\Delta(g_{k-1}, L_k, C_k/C_{k-2})) \cap \Delta(g_{k-1}, L_{k-1}, C_k/C_{k-2})$ we conclude from Lemma 2.4 that x is in rad $\Delta(g_{k-1}, L_{k-1}, C_k/C_{k-2})$.

It remains to show that x is non-zero. It may be observed from the first part of the proof that $\tau \not\equiv \rho \mod C_{k-1}/C_{k-2}$ for any element ρ in the expression $\delta = \psi^{-1}(\sum a_\rho u_\rho)$, from which it certainly follows that $\tau \neq \rho$ for any such ρ. Since the crossed product $\Delta(g_{k-1}, L_{k-1}, C_k/C_{k-2})$ is a free left L_{k-1}-module with free generators u_σ for σ in C_k/C_{k-2} we conclude that $x \neq 0$. Therefore $\Delta(g_{k-1}, L_{k-1}, C_k/C_{k-2})$ is not semi-simple, and this concludes the first part of the proof.

The rest of the proof involves showing that the semi-simplicity of $\Delta(g_{k-1}, L_{k-1}, C_{k-1}/C_{k-2})$ implies the semi-simplicity of $\Delta(g_{k-1}, L_{k-1}, C_k/C_{k-2})$. As in Lemma 2.6 we use the notation $\Delta_{k-1} = \Delta(g_{k-1}, L_{k-1}, C_{k-1}/C_{k-2})$ and $\Delta_k = \Delta(g_{k-1}, L_{k-1}, C_k/C_{k-2})$. Let $C_k/C_{k-2} = \bigcup_i (C_{k-1}/C_{k-2})\rho_i$ be a disjoint right coset decomposition of C_k/C_{k-2} relative to the subgroup C_{k-1}/C_{k-2}. Then an element δ of Δ_k can be written uniquely in the form $\delta = \sum_{i=1}^{t(\delta)} \delta_i u_{\rho_i}$ where each δ_i is in Δ_{k-1}. We may assume that $\rho_1 = 1$.

The proof that Δ_k is semi-simple is by induction on $t(\delta)$. If $t(\delta) = 1$, then δ is in (rad $\Delta_k) \cap \Delta_{k-1}$, so that δ is in rad Δ_{k-1} by Lemma 2.6. Since Δ_{k-1} is semi-simple we conclude that $\delta = 0$. Now let $\delta = \sum_{i=1}^{t} \delta_i u_{\rho_i}$ be an element of rad Δ_k, with $\delta_t \neq 0$ and $\rho_1 = 1$. The induction hypothesis states that if γ is an element of rad Δ_k and $t(\gamma) < t$, then $\gamma = 0$. Consider the element ρ_t of C_k/C_{k-2}. By Lemma 2.2 there exists an element τ in G_1/C_{k-2} such that $\tau\rho_t\tau^{-1}\rho_t^{-1} = c_t$ is in C_{k-1}/C_{k-2} and $c_t \neq 1$. For $1 \leq i \leq t-1$, let c_i be defined by $c_i = \tau\rho_i\tau^{-1}\rho_i^{-1}$ and observe that each c_i is in C_{k-1}/C_{k-2}.

Now form the element $\gamma = \delta - u_\tau\delta(u_\tau)^{-1}$. By Lemma 2.6 it follows that γ is in rad Δ_k. Using the fact that Δ_{k-1} is contained in the center of Δ_k together with the definition of the c_i one may obtain the equalities

$$\begin{aligned}\gamma &= \sum_{i=1}^{t}\delta_i u_{\rho_i} - u_\tau\Big(\sum_{i=1}^{t}\delta_i u_{\rho_i}\Big)(u_\tau)^{-1}\\ &= \sum_{i=1}^{t}\delta_i\Big[1 - \frac{g_{k-1}(\tau, \rho_i)\, g_{k-1}(\tau\rho_i, \tau^{-1})}{g_{k-1}(\tau, \tau^{-1})g_{k-1}(c_i, \rho_i)}u_{c_i}\Big]u_{\rho_i}\end{aligned}$$

For convenience of notation, let $\lambda_i = 1 - \dfrac{g_{k-1}(\tau, \rho_i)g_{k-1}(\tau\rho_i, \tau^{-1})}{g_{k-1}(\tau, \tau^{-1})g_{k-1}(c_i, \rho_i)}u_{c_i}$ for $1 \leq i \leq t$, and note that each λ_i is in Δ_{k-1}. It is easy to check that $c_1 = 1$ and $\lambda_1 = 0$ since $\rho_1 = 1$. Therefore $\gamma = \sum_{i=2}^{t}(\delta_i\lambda_i)u_{\rho_i}$ with $\delta_i\lambda_i$ in Δ_{k-1} for $2 \leq i \leq t$. Hence γ is an element of rad Δ_k such that $t(\gamma) < t$. By the induction hypothesis we may conclude that $\gamma = 0$, and so $\delta_i\lambda_i = 0$ for $2 \leq i \leq t$. But $\lambda_t \neq 0$ since $c_t \neq 1$, so that $\delta_t = 0$ because Δ_{k-1} is a field. This contradicts the assumption that $\delta_t \neq 0$. Therefore rad $\Delta_k = (0)$, and so Δ_k is semi-simple.

LEMMA 2.8. *If the crossed product $\Delta(g_i, L_i, C_i/C_{i-1})$ is a field for some i, then the radical of $\Delta(g_i, L_i, C_i)$ is generated as a right ideal by the radical of $\Delta(1, L_i, C_{i-1})$.*

Proof. Recall that $g_i = 1$ on $C_{i-1} \times C_{i-1}$. Let N denote the right ideal of the trivial crossed product $\Delta(1, L_i, C_{i-1})$ generated by the set of all elements of the form $1 - u_\sigma$ with σ in C_{i-1}. It follows at once from the exercise on p. 435 of [9] that N is the radical of $\Delta(1, L_i, C_{i-1})$. Therefore Lemma 1.4 now implies that $N\Delta(g_i, L_i, C_i)$ is contained in rad $\Delta(g_i, L_i, C_i)$. In order to conclude that $N\Delta(g_i, L_i, C_i)$ is the radical of $\Delta(g_i, L_i, C_i)$, observe that the factor ring $\Delta(g_i, L_i, C_i)/N\Delta(g_i, L_i, C_i)$ is isomorphic to the crossed product $\Delta(g_i, L_i, C_i/C_{i-1})$ and is therefore simple by hypothesis.

PROPOSITION 2.9. *Let G_1 be a p-group with trivial action on a field F of characteristic p. Then the crossed product $\Delta(f, F, G_1)$ is semi-simple if and only if $\Delta(f, F, C)$ is a field where C denotes the center of G_1.*

Proof. If $\Delta(f, F, G_1)$ is semi-simple, the fact that rad $\Delta(f, F, C)$ is contained in rad $\Delta(f, F, G_1)$ (see Lemma 1.4) implies that $\Delta(f, F, C)$ is also semi-simple. Therefore $\Delta(f, F, C)$ is a field according to Theorem 1.10.

To prove the assertion in the other direction recall first of all that the assumption that $\Delta(f, F, C)$ is a field implies that each crossed product $\Delta(g_i, L_i, C_i/C_{i-1})$ is a field by Prop. 2.7. We shall use this fact to prove inductively that $\Delta(f, F, C_i)$ is semi-simple for $0 \leq i \leq n$. Note that $\Delta(f, F, C_0)$ is semi-simple by hypothesis. So suppose that $\Delta(f, F, C_{i-1})$ is semi-simple. In order to prove that $\Delta(f, F, C_i)$ is semi-simple consider the sequence of maps

$$\Delta(f, F, C_i) \longrightarrow \Delta(f, L_i, C_i) \xrightarrow{\psi} \Delta(g_i, L_i, C_i) \longrightarrow \Delta(g_i, L_i, C_i/C_{i-1})$$

where ψ is the L_i-algebra isomorphism defined by $\psi(au_\tau) = a\phi(\tau)u_\tau$ for a in L_i and τ in C_i, and $\phi : C_i \to U(L_i)$ is the map by which f is cohomologous to g_i in $Z^2(C_i, U(L_i))$. The other maps are the obvious ones.

Let δ denote any element of rad $\Delta(f, F, C_i)$. We shall use the above sequence to prove that $\delta = 0$. By applying Lemma 1.4 we may conclude that δ is in rad $\Delta(f, L_i, C_i)$, so that $\psi(\delta)$ is in rad $\Delta(g_i, L_i, C_i)$ since ψ is an isomorphism. According to Lemma 2.8 the fact that $\Delta(g_i, L_i, C_i/C_{i-1})$ is a field implies therefore that we may write $\psi(\delta)$ in the form $\psi(\delta) = \sum n_i\delta_i$ where each n_i is in rad $\Delta(1, L_i, C_{i-1})$ and each δ_i is in $\Delta(g_i, L_i, C_i)$. Therefore $\delta = \sum \psi^{-1}(n_i)\psi^{-1}(\delta_i)$. From the definition of the isomorphism ψ, it follows that each element $\psi^{-1}(n_i)$ is in rad $\Delta(f, L_i, C_{i-1})$. Consider now a disjoint right coset decomposition $C_i = \bigcup_j C_{i-1}\rho_j$ of C_i relative to the subgroup C_{i-1}. Then each element $\psi^{-1}(\delta_i)$ has a unique expression in the form $\psi^{-1}(\delta_i) = \sum_j \lambda_j^{(i)} u_{\rho_j}$ where the $\lambda_j^{(i)}$ are in $\Delta(f, L_i, C_{i-1})$. Therefore $\delta = \sum_j [\sum_i \psi^{-1}(n_i)\lambda_j^{(i)}]u_{\rho_j}$. The fact that δ is in $\Delta(f, F, C_i)$ implies now that $\sum_i \psi^{-1}(n_i)\lambda_j^{(i)}$ is in $\Delta(f, F, C_{i-1})$ for each j, so that $\sum_i \psi^{-1}(n_i)\lambda_j^{(i)}$ is in (rad $\Delta(f, L_i, C_{i-1})) \cap \Delta(f, F, C_{i-1})$. It follows from Lemma 2.4 that (rad $\Delta(f, L_i, C_{i-1})) \cap \Delta(f, F, C_{i-1})$ is contained in the radical of $\Delta(f, F, C_{i-1})$. By the induction hypothesis, rad $\Delta(f, F, C_{i-1}) = (0)$. Therefore $\sum \psi^{-1}(n_i)\lambda_j^{(i)} = 0$ for each j, and so we conclude finally that $\delta = 0$.

3. Hereditary orders. Let S be the integral closure of a complete discrete rank one valuation ring R in a finite Galois extension of the quotient field of R, and let G denote the Galois group of the quotient field extension. Assume

https://doi.org/10.1017/S0027763000023977 Published online by Cambridge University Press

moreover that the residue class field extension $\bar{S}$ of $\bar{R}$ is separable. The purpose of this section is to prove the main theorem of the paper, namely that the crossed product $\Delta(f, S, G)$ is a Π-principal hereditary order if and only if the radical group R_f is trivial. (See Section 1 for the definition of radical group.)

The results of Sections 1 and 2 together imply that $\Delta(\bar{f}, \bar{S}, G_1)$ is semi-simple if and only if $R_f = (1)$, where G_1 denotes the first ramification group of S over R. The crossed product $\Delta(f, S, G)$ is a Π-principal hereditary order if and only if $\Delta(\bar{f}, \bar{S}, G)$ is semi-simple. Therefore our next object is to prove that $\Delta(\bar{f}, \bar{S}, G)$ is semi-simple if and only if $\Delta(\bar{f}, \bar{S}, G_1)$ is semi-simple.

The first step is to reduce the problem to the inertial case. For the sake of completeness we prove the following proposition which has already been established by Harada in [10].

PROPOSITION 3.1. *Let S be an integrally closed extension of a complete discrete rank one valuation ring R, and let G_0 denote the inertia group of S over R. Let $[f]$ denote an element of $H^2(G, U(S))$. Then the radical of the crossed product $\Delta(f, S, G)$ is generated as a right ideal by the radical of $\Delta(f, S, G_0)$.*

Proof. Let Π denote a prime element of S. Since Π is in rad $\Delta(f, S, G)$ and in rad $\Delta(f, S, G_0)$ it suffices to prove that the radical of $\Delta(\bar{f}, \bar{S}, G)$ is generated as a right ideal by the radical of $\Delta(\bar{f}, \bar{S}, G_0)$. For convenience of notation we let $\bar{\Delta} = \Delta(\bar{f}, \bar{S}, G)$ and $\bar{\Delta}_0 = \Delta(\bar{f}, \bar{S}, G_0)$.

Let U denote the inertia ring of S over R. Since $\bar{S}$ is a purely inseparable extension of $\bar{U}$, the inertia group G_0 acts trivially on $\bar{S}$. Furthermore, $\bar{U} = \bar{R}(\theta)$ for some element θ of $\bar{U}$ since $\bar{U}$ is a finite separable extension of $\bar{R}$.

Observe that the intersection (rad $\bar{\Delta}$) $\cap \bar{\Delta}_0$ is contained in rad $\bar{\Delta}_0$ under the natural injection of $\bar{\Delta}_0$ into $\bar{\Delta}$ according to Lemma 2.4.

Now we may prove the proposition. Let $G = \cup G_0\tau_i$ be a disjoint right coset decomposition of G relative to the normal subgroup G_0. Let δ be an element of rad $\bar{\Delta}$ and write $\delta = \sum_{i=1}^{t(\delta)} \delta_i u_{\tau_i}$ where $\delta_i = \sum c_h^{(i)} u_h$ with the h in G_0 and the $c_h^{(i)}$ in $U(\bar{S})$. Note that the elements δ_i are unique by Lemma 2.5. We shall prove by induction on $t(\delta)$ that each δ_i is in rad $\bar{\Delta}_0$. For suppose that $t(\delta) = 1$. Then $\delta = \delta_i u_{\tau_i}$ where δ_i is in $\bar{\Delta}_0$. The element $\delta(u_{\tau_i})^{-1}$ is therefore in (rad $\bar{\Delta}$) $\cap \bar{\Delta}_0$. By the above observation we conclude that δ_i is in rad Δ_0.

Now let $\delta = \sum_{i=1} \delta_i u_{\tau_i}$ be an element of rad $\bar{\Delta}$ for which $t(\delta) = t$. The induction hypothesis states that if $t(\gamma)<t$ for an element γ of rad $\bar{\Delta}$ then each γ_i is in rad $\bar{\Delta}_0$ where $\gamma=\sum \gamma_i u_{\tau_i}$. Consider the element $\alpha=\theta\delta-\delta\tau_t^{-1}(\theta)=\sum_{i=1}^{t-1}(\theta-\tau_i\tau_t^{-1}(\theta))\delta_i u_{\tau_i}$. Since α is in rad $\bar{\Delta}$ and $t(\alpha)<t$ it follows from the induction hypothesis that $(\theta-\tau_i\tau_t^{-1}(\theta))\delta_i$ is in rad $\bar{\Delta}_0$ for each i such that $1\leq i\leq t-1$. Since G/G_0 is the Galois group of $\bar{U}$ over $\bar{R}$ (see p. 32 of [5]) we have that $\tau_i\tau_t^{-1}(\theta)=\theta$ if and only if $i=t$. Therefore δ_i is in rad $\bar{\Delta}_0$ for $1\leq i\leq t-1$. Finally we observe that $\delta_t u_{\tau_t}$ is in rad $\bar{\Delta}$ so that $\delta_t=\delta_t u_{\tau_t}(u_{\tau_t})^{-1}$ is in (rad $\bar{\Delta}$) $\cap\,\bar{\Delta}_0$ and hence in rad $\bar{\Delta}_0$. Therefore δ_i is in rad $\bar{\Delta}_0$ for $1\leq i\leq t$ and this concludes the proof.

As in Section 2 we shall use the notion of a splitting field of a crossed product to reduce computations to the case of a trivial crossed product.

PROPOSITION 3.2. *Let f be an element of $Z^2(G_0, U(S))$. Then there exists a finite purely inseparable extension L of $\bar{S}$ and a 2-cocycle g of $Z^2(G_0, U(L))$ such that g is in the image of the inflation map $Z^2(G_0/G_1, U(L))\to Z^2(G_0, U(L))$ and is cohomologous to the image of $\bar{f}$ in $Z^2(G_0, U(L))$.*

Proof. The proof is by induction on the number of ramification groups. Let

$$G_{\alpha(0)}\supset G_{\alpha(1)}\supset\cdots\supset G_{\alpha(n)}\supset G_{\alpha(n+1)}=(1)$$

be the sequence of (distinct) ramification groups of the extension S of R, observing that $\alpha(0)=0$ and $\alpha(1)=1$. We first construct a chain of fields $\bar{S}=L_0\subset L_1\subset\cdots\subset L_n$ and 2-cocycles g_i of $Z^2(G_0, U(L_i))$ such that each L_{i+1} is a purely inseparable extension of L_i, and each g_i is in the image of the inflation map $Z^2(G_0/G_{\alpha(n+1-i)}, U(L_i))\to Z^2(G_0, U(L_i))$ and is cohomologous to the image of $\bar{f}$ in $Z^2(G_0, U(L_i))$.

We define $L_0=\bar{S}$ and $g_0=\bar{f}$. It is a trivial observation that L_0 and g_0 have the desired properties. When L_i and g_i have been defined, we then define L_{i+1} and g_{i+1} in the following way. For convenience of notation we denote the preimage of g_i in $Z^2(G_0/G_{\alpha(n+1-i)}, U(L_i))$ by g_i also. Then L_{i+1} is defined to be a finite purely inseparable splitting field for the crossed product $\Delta(g_i, L_i, G_{\alpha(n-i)}/G_{\alpha(n+1-i)})$. The existence of such a field L_{i+1} is guaranteed by Lemma 2.1, since $G_{\alpha(n-i)}/G_{\alpha(n+1-i)}$ is an Abelian p-group with trivial action on L_i. By an argument entirely similar to that used in the proof of Prop. 2.3 we may conclude the existence of a 2-cocycle g_{i+1} in $Z^2(G_0, U(L_{i+1}))$ which is in the image of the inflation map $Z^2(G_0/G_{\alpha(n-i)}, U(L_{i+1}))\to Z^2(G_0, U(L_{i+1}))$ and

https://doi.org/10.1017/S0027763000023977 Published online by Cambridge University Press

is cohomologous to the image of $\bar{f}$ in $Z^2(G_0, U(L_{i+1}))$. We may prove the proposition now by taking $L = L_n$ and $g = g_n$.

The notation established in Prop. 3.2 shall be used throughout the rest of Section 3.

PROPOSITION 3.3. *The radical of the crossed product $\Delta(g, L, G_0)$ is generated as a right ideal by the radical of $\Delta(1, L, G_1)$.*

Proof. Let N denote the right ideal of $\Delta(1, L, G_1)$ generated by the set of all elements of the form $1 - u_\sigma$ with σ in G_1. Since G_1 is a p-group and L has characteristic p, it follows at once from the exercise on p. 435 of [9] that N is the radical of the trivial crossed product $\Delta(1, L, G_1)$.

It remains to show that $N\Delta(g, L, G_0)$ is the radical of $\Delta(g, L, G_0)$. Using the fact that g is in the image of the inflation map $Z^2(G_0/G_1, U(L)) \to Z^2(G_0, U(L))$ together with the fact that G_1 is a normal subgroup of G_0, one may conclude from the definition of N that the right ideal $N\Delta(g, L, G_0)$ is equal to the left ideal $\Delta(g, L, G_0)N$. Lemma 1.4 now implies that $N\Delta(g, L, G_0)$ is contained in rad $\Delta(g, L, G_0)$. To prove that $N\Delta(g, L, G_0)$ is the radical of $\Delta(g, L, G_0)$ it suffices therefore to show that the factor ring $\Delta(g, L, G_0)/N\Delta(g, L, G_0)$ is semi-simple. Now $\Delta(g, L, G_0)/N\Delta(g, L, G_0)$ is isomorphic to the crossed product $\Delta(g, L, G_0/G_1)$ in a natural way. Since G_0/G_1 acts trivially on L, and the order of G_0/G_1 is relatively prime to the characteristic of L, it follows from Theorem 1.1 of [7] that $\Delta(g, L, G_0/G_1)$ is L-separable and therefore semi-simple.

PROPOSITION 3.4. *The radical of the crossed product $\Delta(\bar{f}, \bar{S}, G_0)$ is generated as a right ideal by the radical of $\Delta(\bar{f}, \bar{S}, G_1)$.*

Proof. The first step is to prove that the radical of $\Delta(\bar{f}, L, G_0)$ is generated as a right ideal by the radical of $\Delta(\bar{f}, L, G_1)$. Consider the 2-cocycle g of $Z^2(G_0, U(L))$ whose existence is established by Prop. 3.2, and let $\phi : G_0 \to U(L)$ be the map by which $\bar{f}$ is cohomologous to g in $Z^2(G_0, U(L))$. It is well known that the map $\psi : \Delta(\bar{f}, L, G_0) \to \Delta(g, L, G_0)$ defined by $\psi(au_\tau) = a\phi(\tau)u_\tau$ for a in L and τ in G_0 is an L-algebra isomorphism. The radical of $\Delta(g, L, G_0)$ is generated as a right ideal by the radical of $\Delta(1, L, G_1)$ according to Prop. 3.3. Since $\psi^{-1}[\Delta(g, L, G_1)] = \Delta(\bar{f}, L, G_1)$ we may conclude therefore that the radical of $\Delta(\bar{f}, L, G_0)$ is generated as a right ideal by the radical of $\Delta(\bar{f}, L, G_1)$.

Now consider an element δ of rad $\Delta(\bar{f}, \bar{S}, G_0)$. It follows easily from

Lemma 1.4 that δ is also in rad $\Delta(\bar{f}, L, G_0)$, so that according to the first part of the proof we may write $\delta = \sum n_i \delta_i$ where each n_i is in rad $\Delta(\bar{f}, L, G_1)$ and the δ_i are in $\Delta(\bar{f}, L, G_0)$. Each element δ_i has a unique expression in the form $\delta_i = \sum_j \lambda_j^{(i)} u_{\rho_j}$ with the $\lambda_j^{(i)}$ in $\Delta(\bar{f}, L, G_1)$, where $G_0 = \cup G_1 \rho_j$ is a disjoint right coset decomposition of G_0 relative to the subgroup G_1. Therefore $\delta = \sum_j [\sum_i n_i \lambda_j^{(i)}] u_{\rho_j}$. Since δ is in $\Delta(\bar{f}, \bar{S}, G_0)$, the fact that $\Delta(\bar{f}, L, G_0)$ is a free left $\Delta(\bar{f}, L, G_1)$-module with free basis $\{u_{\rho_i}\}$ implies that $\sum_i n_i \lambda_j^{(i)}$ is in $\Delta(\bar{f}, \bar{S}, G_1)$ for each j. Therefore each $\sum_i n_i \lambda_j^{(i)}$ is in $(\text{rad } \Delta(\bar{f}, L, G_1)) \cap \Delta(\bar{f}, \bar{S}, G_1)$, which according to Lemma 2.4 is contained in rad $\Delta(\bar{f}, \bar{S}, G_1)$. The fact that an element δ of rad $\Delta(\bar{f}, \bar{S}, G_0)$ may be written in the form $\delta = \sum_j [\sum_i n_i \lambda_j^{(i)}] u_{\rho_j}$ with each $\sum_i n_i \lambda_j^{(i)}$ in rad $\Delta(\bar{f}, \bar{S}, G_1)$ establishes the assertion of the proposition.

Using Prop. 3.4 together with the results of Sections 1 and 2 we may now prove the main theorem of the paper.

THEOREM 3.5. *Let S be an integrally closed extension of a complete discrete rank one valuation ring R such that the residue class field extension is separable, and let $[f]$ be an element of $H^2(G, U(S))$. Then the crossed product $\Delta(f, S, G)$ is a Π-principal hereditary order if and only if the radical group R_f of $[f]$ is trivial.*

Proof. The crossed product $\Delta(f, S, G)$ is a Π-principal hereditary order if and only if the crossed product $\Delta(\bar{f}, \bar{S}, G)$ is semi-simple. By Prop. 3.1 we know that $\Delta(\bar{f}, \bar{S}, G)$ is semi-simple if and only if $\Delta(\bar{f}, \bar{S}, G_0)$ is semi-simple where G_0 denotes the inertia group of S over R. And the crossed product $\Delta(\bar{f}, \bar{S}, G_0)$ is semi-simple if and only if $\Delta(\bar{f}, \bar{S}, G_1)$ is semi-simple according to Prop. 3.4, where G_1 is the first ramification group of S over R. Prop. 2.9 implies in turn that $\Delta(\bar{f}, \bar{S}, G_1)$ is semi-simple if and only if $\Delta(\bar{f}, \bar{S}, C)$ is a field where C denotes the center of G_1. Finally, the fact that $\Delta(\bar{f}, \bar{S}, C)$ is a field if and only if R_f is trivial (see Theorem 1.10) establishes the assertion of the theorem.

We obtain at once from Theorem 3.5 the following result which has already been proved by Harada (see Theorem 2 of [10]).

COROLLARY 3.6. *Let R be a complete discrete rank one valuation ring with perfect residue class field, and let S denote an integrally closed extension of R. If $[f]$ is an element of $H^2(G, U(S))$, then the crossed product $\Delta(f, S, G)$ is a Π-*

principal hereditary order if and only if S is a tamely ramified extension of R.

Proof. In the case when S is a tamely ramified extension of R it was proved in [7] that $\Delta(f, S, G)$ is a Π-principal hereditary order.

We prove the assertion in the other direction by contradiction. So suppose that the extension S of R is not tamely ramified. Then the center C of the first ramification group G_1 is non-trivial. Since $\bar{R}$ is perfect, $\bar{f}$ is cohomologous to 1 on $C \times C$ by Cor. A. 5. From the definition of the radical group it now follows that $R_f = C$.

APPENDIX. COHOMOLOGY. In this appendix to the paper we present several general facts concerning cohomology which have application to the study of crossed products.

PROPOSITION A. 1. *Let F be a field of characteristic $p \neq 0$, and G a group which acts trivially on F. Suppose that σ and τ are elements of G such that $\sigma\tau = \tau\sigma$. If the order of τ is a p^{th} power, then $f(\sigma, \tau) = f(\tau, \sigma)$ for every 2-cocycle f in $Z^2(G, U(F))$.*

Proof. Let p^t denote the order of τ. By the associativity property of f we obtain the equalities

$$f(\tau, \sigma\tau^{p^t-1})f(\sigma, \tau^{p^t-1}) = f(\tau\sigma, \tau^{p^t-1})f(\tau, \sigma)$$
$$f(\tau, \tau^{p^t-1}\sigma)f(\tau^{p^t-1}, \sigma) = f(\tau, \tau^{p^t-1})$$
$$f(\sigma\tau, \tau^{p^t-1})f(\sigma, \tau) = f(\tau, \tau^{p^t-1})$$

Combining the above equalities we obtain that

$$f(\sigma, \tau^{p^t-1})f(\sigma, \tau) = f(\tau^{p^t-1}, \sigma)f(\tau, \sigma).$$

We next obtain an expression for $f(\tau^{p^t-1}, \sigma)$. Write $f(\tau^{p^t-i}, \sigma) = f(\tau^{p^t-i-1}\tau, \sigma)$ for $1 \le i \le p^t - 1$. By combining the equalities

$$f(\tau^{p^t-i-1}\tau, \sigma)f(\tau^{p^t-i-1}, \tau) = f(\tau^{p^t-i-1}, \tau\sigma)f(\tau, \sigma)$$
$$f(\tau^{p^t-i-1}, \sigma\tau)f(\sigma, \tau) = f(\tau^{p^t-i-1}\sigma, \tau)f(\tau^{p^t-i-1}, \sigma)$$

we get that

$$f(\tau^{p^t-i}, \sigma) = f(\tau, \sigma)f(\sigma\tau^{p^t-i-1}, \tau)f(\tau^{p^t-i-1}, \sigma)/f(\sigma, \tau)f(\tau^{p^t-i-1}, \tau)$$

for $1 \le i \le p^t - 1$. By repeated use of this equality it follows that

$$f(\tau^{p^t-1}, \sigma) = [f(\tau, \sigma)/f(\sigma, \tau)]^{p^t-1}\prod_{i=2}^{p^t} f(\sigma\tau^{p^t-i}, \tau)/f(\tau^{p^t-i}, \tau).$$

https://doi.org/10.1017/S0027763000023977 Published online by Cambridge University Press

On the other hand, we may write $f(\sigma, \tau^{p^t-i}) = f(\sigma, \tau^{p^t-i-1}\tau)$ and obtain an expression for $f(\sigma, \tau^{p^t-1})$. The associativity property of f implies that

$$f(\sigma, \tau^{p^t-i}) = f(\sigma\tau^{p^t-i-1}, \tau)f(\sigma, \tau^{p^t-i-1})/f(\tau^{p^t-i-1}, \tau).$$

By repeated use of this equality we obtain that

$$f(\sigma, \tau^{p^t-1}) = \prod_{i=2}^{p^t} f(\sigma\tau^{p^t-i}, \tau)/f(\tau^{p^t-i}, \tau).$$

Now we may conclude that $f(\sigma, \tau) = f(\tau, \sigma)$. For by substituting the above expressions for $f(\tau^{p^t-1}, \sigma)$ and $f(\sigma, \tau^{p^t-1})$ into the equality $f(\sigma, \tau^{p^t-1})f(\sigma, \tau) = f(\tau^{p^t-1}, \sigma)f(\tau, \sigma)$ we get that $[f(\sigma, \tau)]^{p^t} = [f(\tau, \sigma)]^{p^t}$. Since F has characteristic p, we conclude that $f(\sigma, \tau) = f(\tau, \sigma)$.

COROLLARY A.2. *Let F be a field of characteristic $p \neq 0$, and let E and G_p be groups with G_p a p-group. If E and G_p act trivially on F, then the natural map*

$$H^2(E\times G_p,\ U(F)) \to H^2(E,\ U(F)) \times H^2(G_p,\ U(F))$$

is an isomorphism.

Proof. Define a map

$$\varphi : Z^2(E\times G_p,\ U(F)) \to Z^2(E,\ U(F)) \times Z^2(G_p,\ U(F))$$

by $\varphi(f) = f_1f_2$ where f_1 is the restriction of f to $E\times E$ and f_2 is the restriction of f to $G_p\times G_p$. Then φ induces a well-defined map

$$\bar{\varphi} : H^2(E\times G_p,\ U(F)) \to H^2(E,\ U(F)) \times H^2(G_p,\ U(F)).$$

We shall show that the map $\bar{\varphi}$ is a group isomorphism.

It follows from the definition of φ that $\bar{\varphi}$ is a homomorphism of groups. We next observe that φ is an epimorphism. For let f_1f_2 be any element of $Z^2(E, U(F)) \times Z^2(G_p, U(F))$. Then define the map $f : (E\times G_p)\times(E\times G_p) \to U(F)$ by $f(\sigma_1\tau_1, \sigma_2\tau_2) = f_1(\sigma_1, \sigma_2)f_2(\tau_1, \tau_2)$ where σ_1 and σ_2 are in E and τ_1 and τ_2 are in G_p. It is easy to verify that f is an element of $Z^2(E\times G_p, U(F))$ and that $\varphi(f) = f_1f_2$. Since φ is an epimorphism we may conclude that $\bar{\varphi}$ is an epimorphism.

It remains to show that $\bar{\varphi}$ is a monomorphism. Since the order of each element of G_p is a p^{th} power, and E and G_p commute element-wise in $E\times G_p$, we know by Prop. A.1 that $f(\sigma, \tau) = f(\tau, \sigma)$ for each σ in E and τ in G_p where

f is any element of $Z^2(E\times G_p,\ U(F))$.

We next prove that for each element f of $Z^2(E\times G_p,\ U(F))$ there exists an element $\hat{f}$ of $Z^2(E\times G_p,\ U(F))$ cohomologous to f and such that $\hat{f}(\sigma_1\tau_1,\ \sigma_2\tau_2)=\hat{f}(\sigma_1,\ \sigma_2)\hat{f}(\tau_1,\ \tau_2)$ where σ_1 and σ_2 are in E and τ_1 and τ_2 are in G_p. Since each element of $E\times G_p$ can be written uniquely in the form $\sigma\tau$ with σ in E and τ in G_p we can define a map $\phi: E\times G_p\to U(F)$ by $\phi(\sigma\tau)=f(\sigma,\tau)$. Now define the 2-cocycle $\hat{f}$ by $\hat{f}(\rho,\ \omega)=f(\rho,\ \omega)\phi(\rho)\phi(\omega)/\phi(\rho\omega)$ for ρ and ω in $E\times G_p$. Note that $\hat{f}(\sigma,\ \tau)=1$ whenever σ is in E and τ is in G_p, since $\phi(\sigma\tau)=f(\sigma,\ \tau)$ and $\phi(\sigma)=\phi(\tau)=1$. We proceed to verify that $\hat{f}$ has the desired property. Now $\hat{f}(\sigma_1\tau_1,\ \sigma_2\tau_2)=\hat{f}(\sigma_1\tau_1\sigma_2,\ \tau_2)\hat{f}(\sigma_1\tau_1,\ \sigma_2)$ since $\hat{f}(\sigma_2,\ \tau_2)=1$, so that it suffices to prove that $\hat{f}(\sigma_1\tau_1\sigma_2,\ \tau_2)=\hat{f}(\tau_1,\ \tau_2)$ and $\hat{f}(\sigma_1\tau_1,\ \sigma_2)=\hat{f}(\sigma_1,\ \sigma_2)$. The equality $\hat{f}(\sigma_1\sigma_2\tau_1,\ \tau_2)\hat{f}(\sigma_1\sigma_2,\ \tau_1)=\hat{f}(\sigma_1\sigma_2,\ \tau_1\tau_2)\hat{f}(\tau_1,\ \tau_2)$ implies that $\hat{f}(\sigma_1\tau_1\sigma_2,\ \tau_2)=\hat{f}(\sigma_1\sigma_2\tau_1,\ \tau_2)=\hat{f}(\tau_1,\ \tau_2)$ since $\hat{f}(\sigma_1\sigma_2,\ \tau_1)=\hat{f}(\sigma_1\sigma_2,\ \tau_1\tau_2)=1$. On the other hand, the equality $\hat{f}(\sigma_1\tau_1,\ \sigma_2)\hat{f}(\sigma_1,\ \tau_1)=\hat{f}(\sigma_1,\ \tau_1\sigma_2)\hat{f}(\tau_1,\ \sigma_2)$ implies that $\hat{f}(\sigma_1\tau_1,\ \sigma_2)=\hat{f}(\sigma_1,\ \tau_1\sigma_2)$ since $\hat{f}(\sigma_1,\ \tau_1)=1$ and $\hat{f}(\tau_1,\ \sigma_2)=\hat{f}(\sigma_2,\ \tau_1)=1$. But $\hat{f}(\sigma_1,\ \tau_1\sigma_2)=\hat{f}(\sigma_1,\ \sigma_2\tau_1)$ and $\hat{f}(\sigma_1,\ \sigma_2\tau_1)\hat{f}(\sigma_2,\ \tau_1)=\hat{f}(\sigma_1\sigma_2,\ \tau_1)\hat{f}(\sigma_1,\ \sigma_2)$ together imply that $\hat{f}(\sigma_1\tau_1,\ \sigma_2)=\hat{f}(\sigma_1,\ \sigma_2)$. Therefore $\hat{f}(\sigma_1\tau_1,\ \sigma_2\tau_2)=\hat{f}(\sigma_1,\ \sigma_2)\hat{f}(\tau_1,\ \tau_2)$.

Now we may prove that $\bar{\varphi}$ is a monomorphism. For suppose that f is a 2-cocycle for which $\bar{\varphi}([f])=[1]$. Let $\hat{f}$ be the 2-cocycle cohomologous to f and satisfying $\hat{f}(\sigma_1\tau_1,\ \sigma_2\tau_2)=\hat{f}(\sigma_1,\ \sigma_2)\hat{f}(\tau_1,\ \tau_2)$, whose existence is established by the above. Then the fact that $\bar{\varphi}([\hat{f}])=[1]$ implies that $[\hat{f}_1]=[1]$ and $[\hat{f}_2]=[1]$. Let $\phi_1: E\to U(F)$ and $\phi_2: G_p\to U(F)$ be maps such that $\hat{f}_1(\sigma_1,\ \sigma_2)=\phi_1(\sigma_1)\phi_1(\sigma_2)/\phi_1(\sigma_1\sigma_2)$ and $\hat{f}_2(\tau_1,\ \tau_2)=\phi_2(\tau_1)\phi_2(\tau_2)/\phi_2(\tau_1\tau_2)$ where the σ_i are in E and the τ_i are in G_p. Then the map $\phi: E\times G_p\to U(F)$ defined by $\phi(\sigma\tau)=\phi_1(\sigma)\phi_2(\tau)$ for σ in E and τ in G_p satisfies $\hat{f}(\sigma_1\tau_1,\ \sigma_2\tau_2)=\phi(\sigma_1\tau_1)\phi(\sigma_2\tau_2)/\phi(\sigma_1\tau_1\sigma_2\tau_2)$ from which it follows that $[f]=[1]$.

The following statement follows immediately from Cor. A.2.

Corollary A.3. *Let F be a field of characteristic $p\neq 0$, and let $C=E_1\times\cdots\times E_t$ be a direct product of cyclic p-groups. If C acts trivially on F, then the natural map*

$$H^2(C,\ U(F))\to H^2(E_1,\ U(F))\times\cdots\times H^2(E_t,\ U(F))$$

induced by the restriction maps is an isomorphism.

Definition. Let $C=E_1\times\cdots\times E_t$ be an Abelian p-group which acts trivially on a field F of characteristic p. An element f of $Z^2(C, U(F))$ of the form $f = f_1 \cdots f_t$ where each element f_i of $Z^2(E_i, U(F))$ is normalized in the sense of cyclic groups (see p. 83 of [1]) is said to be *normalized in the sense of Abelian p-groups.*

According to Cor. A.3 we may always assume that an element f of $Z^2(C, U(F))$ has been normalized in the sense of Abelian p-groups.

COROLLARY A.4. *Let G be a group which acts trivially on a field F of characteristic $p \neq 0$. If the subgroup D of G is an Abelian p-group, then for each element f of $Z^2(G, U(F))$ there exists an element f' of $Z^2(G, U(F))$ cohomologous to f and such that the restriction of f' to $D \times D$ is normalized in the sense of Abelian p-groups.*

Proof. For convenience of notation let f_D denote the restriction of f to $D \times D$. By Cor. A.3 there exists a 2-cocycle f'_D of $Z^2(D, U(F))$ cohomologous to f_D such that f'_D is normalized in the sense of Abelian p-groups. Let $\phi_D : D \to U(F)$ be the map satisfying $f'_D(\sigma, \tau) = f_D(\sigma, \tau)\phi_D(\sigma)\phi_D(\tau)/\phi_D(\sigma\tau)$ for σ and τ in D. Extend ϕ_D to a map $\phi : G \to U(F)$ by defining $\phi(\sigma) = \phi_D(\sigma)$ if σ is in D, and $\phi(\sigma) = 1$ if σ is in $G - D$. Then the element f' of $Z^2(G, U(F))$ defined by $f'(\sigma, \tau) = f(\sigma, \tau)\phi(\sigma)\phi(\tau)/\phi(\sigma\tau)$ has the desired properties.

COROLLARY A.5. *Let F be a perfect field of characteristic $p \neq 0$, and C an Abelian p-group which acts trivially on F. Then $H^2(C, U(F)) = (1)$.*

Proof. Let $C = E_1 \times \cdots \times E_t$ be a decomposition of C into a direct product of cyclic p-groups. By Cor. A.3 it suffices to show that $H^2(E_i, U(F)) = (1)$ for each i. So consider an element $[f]$ of $H^2(E_i, U(F))$ and let a be an element of $U(F)$ such that $[f]$ corresponds to a mod $[U(F)]^{e_i}$ under the canonical identification $H^2(E_i, U(F)) = U(F)/[U(F)]^{e_i}$ where e_i denotes the order of E_i. Since F is a perfect field of characteristic p, it follows that a is an e_i^{th} power. Therefore $a \equiv 1$ mod $[U(F)]^{e_i}$ and $H^2(E_i, U(F)) = (1)$.

The following lemma shall be useful in proving a statement concerning the exactness of a sequence of cohomology groups.

LEMMA A.6. *Let G be a p-group and F a field of characteristic p upon which G acts trivially. Then $Z^1(G, U(F)) = (1)$.*

Proof. Let $f : G \to U(F)$ be an element of $Z^1(G, U(F))$. We show first that $f(1)=1$. For by the associativity property of f together with the fact that G acts trivially on F we obtain the equality $f(1)=[f(1)]^2$ so that $f(1)=1$. Now let σ denote any element of G and let p^t denote the order of σ. Then $1=f(1)=f(\sigma^{p^t})=[f(\sigma)]^{p^t}$ so that $f(\sigma)=1$ since F has characteristic p. Therefore $f=1$, and so $Z^1(G, U(F))=(1)$.

PROPOSITION A.7. *Let F be a field of characteristic $p \neq 0$, and G_p a normal subgroup of a group G. If G_p is a p-group which acts trivially on F then the sequence*

$$(1) \to H^2(G/G_p, U(F)) \to H^2(G, U(F)) \to H^2(G_p, U(F))$$

is exact where the maps are inflation and restriction.

Proof. Since G_p is a p-group and F has characteristic p, we know by Lemma A.6 that $H^1(G_p, U(F))=(1)$. It now follows from Prop. 5 p. 126 of [5] that the above sequence is exact.

REFERENCES

[1] E. Artin, C. Nesbitt and R. Thrall, *Rings with Minimum Condition*, Michigan (1955).
[2] M. Auslander and O. Goldman, *Maximal orders*, Trans. Amer. Math. Soc., vol. **97** (1960), pp. 1–24.
[3] M. Auslander and D. S. Rim, *Ramification index and multiplicity*, Ill. J. of Math., vol. **7** (1963), pp. 566–581.
[4] M. Hall, *The Theory of Groups*, The Macmillan Co. (1959).
[5] J. P. Serre, *Corps Locaux*, Paris, Hermann (1962).
[6] E. Weiss, *Algebraic Number Theory*, McGraw-Hill Co. (1963).
[7] S. Williamson, *Crossed products and hereditary orders*, Nagoya Math. J., vol. **23** (1963), pp. 103–120.
[8] S. Williamson, *Crossed products and maximal orders*, Nagoya Math. J., vol. **25** (1965), pp. 165–174.
[9] C. Curtis and I. Reiner, *Representation Theory of Finite Groups andAssociative Algebras*, Wiley and Sons (1962).
[10] M. Harada, *Some criteria for hereditarity of crossed products*, Osaka J. Math., vol. **1** (1964), pp. 69–80.

Regis College
Weston, Massachusetts

https://doi.org/10.1017/S0027763000023977 Published online by Cambridge University Press