PACIFIC JOURNAL OF MATHEMATICS
Vol. 122, No. 2, 1986

CROSSED PRODUCT AND HEREDITARY ORDERS

GERALD H. CLIFF AND ALFRED R. WEISS

Let Λ be the crossed product order $(O_L/O_K, G, \rho)$ where L/K is a finite Galois extension of local fields with Galois group G, and ρ is a factor set with values in O_L^*. Let $\Lambda_0 = \Lambda$, and let Λ_{i+1} be the left order $O_l(\text{rad}\,\Lambda_i)$ of rad Λ_i. The chain of orders $\Lambda_0, \Lambda_1, \ldots, \Lambda_s$ ends with a hereditary order Λ_s. We prove that Λ_s is the unique minimal hereditary order in $A = K\Lambda$ containing Λ, that Λ_s has e/m simple modules, each of dimension f over the residue class field $\overline{K}$ of O_K, and that $s = d - (e-1)$. Here d, e, f are the different exponent, ramification index, and inertial degree of L/K, and m is the Schur index of A.

1. Introduction. Let O_K be a complete discrete valuation ring having field of fractions K and finite residue class field $\overline{K}$. Let L be a finite Galois extension of K, with Galois group G, and let O_L be the valuation ring in L. Let ρ be a factor set on $G \times G$ with values in the units of O_L. We are interested in the crossed product order $\Lambda = (O_L/O_K, G, \rho)$ contained in the simple algebra $A = (L/K, G, \rho)$. If ρ is trivial, Auslander-Goldman [**1**] showed that Λ is a maximal order in A if and only if L/K is unramified, and Auslander-Rim [**2**] showed that Λ is hereditary if and only if L/K is tamely ramified. Williamson [**8**] extended the Auslander-Rim result to the case that ρ is any factor set. We are interested in the wild case. Benz-Zassenhaus [**3**] showed that Λ is contained in a unique minimal hereditary order in A.

We set $\Lambda_0 = \Lambda$, and define inductively

$$\Lambda_{j+1} = \{x \in A\colon x\,\text{rad}\,\Lambda_j \subseteq \text{rad}\,\Lambda_j\} = O_l(\text{rad}\,\Lambda_j).$$

Then we have the sequence of orders

$$\Lambda_0 \subsetneqq \Lambda_1 \subsetneqq \Lambda_2 \subsetneqq \cdots \subsetneqq \Lambda_s = \Lambda_{s+1}$$

for some integer s. Since $\Lambda_s = O_l(\text{rad}\,\Lambda_s)$, it follows that Λ_s is hereditary ([**6**, 39.11, 39.14]). From the theory of hereditary orders (see [**6**, 39.14]) Λ_s may be described as follows: if $A \cong M_n(D)$, the ring of $n \times n$ matrices over a division ring D, and if Δ is the unique maximal order in D, then Λ_s is the set of block matrices, with entries in Δ, where there are r diagonal blocks of size $n_i \times n_i$, and blocks above the diagonal have entries in rad Δ. The positive integer r is called the type number of Λ_s, and is also equal to the number of simple Λ_s-modules. Our main result is the following.

THEOREM. (1) *Λ_s is the unique minimal hereditary O_K-order in A containing Λ.*

(2) rad $\Lambda_s = P_L\Lambda_s$, *where P_L denotes the maximal ideal of O_L.*

(3) $r = e/m$, *where e is the ramification index of L/K and m is the Schur index of A.*

(4) $n_1 = n_2 = \cdots = n_r = f$, *the inertial degree of L/K.*

(5) $s = d - (e - 1)$, *where d is the exponent $P_L^d = \mathcal{D}$ of the different of L/K.*

We prove this by first considering the split case (when $\rho = 1$), and then taking an unramified extension K' of K which splits A, and considering $A \otimes_K K'$ which is a crossed product $(L'/K', G, 1)$, where $L' = L \otimes_K K'$. Then L' is not in general a field, but a Galois algebra over K', and we find it convenient to prove the Theorem when L is a Galois algebra over K to begin with; we take O_L to be the integral closure of O_K in L, we replace P_L by rad O_L, and we give suitable definitions of d, e, and f in §2. We deal with the split case in §3, and the general case in §4. We find generators for the hereditary order Λ_s in §5, in the totally ramified split case. In §6 we show how our results yield those of Auslander-Goldman-Rim-Williamson, as well as some others.

We cite Reiner [**6**] as a general reference.

2. Galois algebras. Let L be a commutative Galois algebra over K, with finite Galois group G, by which we mean that L is a commutative separable K-algebra with G a group of automorphisms of L fixing K such that the fixed subalgebra $L^G = K$ and $|G| = \dim_K L$. Let O_L be the integral closure of O_K in L. Let E denote the set of primitive idempotents of L. Then for $\varepsilon \in E$, the integral closure $O_{L\varepsilon}$ of O_K in the field $L\varepsilon$ is a complete discrete valuation ring, and $O_{L\varepsilon} = O_L\varepsilon$. Since $L^G = K$, G acts transitively on E.

LEMMA 2.1. *Let I be a non-zero O_L-submodule of L which is G-invariant. Then $I = (\text{rad}\, O_L)^i$ for some integer i.*

Proof. For any primitive idempotent ε of L, $I\varepsilon$ is a non-zero $O_{L\varepsilon}$-submodule of $L\varepsilon$, and therefore $I\varepsilon = (\text{rad}\, O_{L\varepsilon})^{i_\varepsilon}$ for some $i_\varepsilon \in \mathbf{Z}$, since $O_{L\varepsilon}$ is a discrete valuation ring. Because G acts transitively on E

and I is G-invariant, it follows that $i_\varepsilon = i$ is independent of ε. Then

$$I = \sum_{\varepsilon \in E} I\varepsilon = \sum_{\varepsilon \in E} (\operatorname{rad} O_{L\varepsilon})^i = \sum_{\varepsilon \in E} (\operatorname{rad} O_L)^i \varepsilon = (\operatorname{rad} O_L)^i$$

as desired.

First, let $I = P_K O_L$. Then $P_K O_L = (\operatorname{rad} O_L)^e$ for some integer e, and we call e the *ramification index* of L/K.

Next, let $\operatorname{tr}_{L/K}\colon L \to K$ be the trace map, and let

$$\tilde{O}_L = \{x \in L\colon \operatorname{tr}_{L/K}(xO_L) \subseteq O_K\}$$

be the complementary module to O_L under the trace. Since

$$\operatorname{tr}_{L/K}(x) = \sum_{g \in G} g(x), \qquad x \in L,$$

it follows that $\tilde{O}_L$ is a G-invariant O_L-submodule of L, so $\tilde{O}_L = (\operatorname{rad} O_L)^{-d}$ for some integer d. We call d the *different exponent* of L/K (and $(\operatorname{rad} O_L)^d$ the different $\mathcal{D}_{L/K}$ of L/K).

Define the *inertial degree* f of L/K to be $\dim_{\bar{K}}(O_L/\operatorname{rad} O_L)$.

Let $\rho\colon G \times G \to O_L^*$ be a factor set on G with values in the units of O_L. The crossed product algebra $A = (L/K, G, \rho)$ is the free left L-module with basis u_g, $g \in G$, with multiplication given by

$$xu_g \cdot yu_h = xg(y)\rho(g,h)u_{gh}, \qquad x, y \in L,\ g, h \in G.$$

The order $\Lambda = (O_L/O_K, G, \rho)$ is the O_L-submodule of A spanned by u_g, $g \in G$. We assume that $\rho(g,1) = \rho(1,g) = 1$, so that O_L may be identified inside Λ as $\{xu_1\colon x \in O_L\}$.

LEMMA 2.2. (1) *L has a normal K-basis with respect to G.*

(2) *A is a central simple K-algebra, and A is isomorphic to a full matrix ring over K if and only if the class of ρ in $H^2(G, L^*)$ is* 1.

(3) *The reduced trace* trd : $A \to K$ *is given by*

$$\operatorname{trd}\left(\sum_{g \in G} a_g u_g\right) = \operatorname{tr}_{L/K}(a_1).$$

Proof. These results are well known if L is a field, and the proofs are essentially the same if L is a Galois algebra. We omit the details.

3. The split case. In this section we assume that L/K is a Galois algebra, and we prove the theorem in the case that $\rho = 1$, with P_L replaced by $\operatorname{rad} O_L$, and with d, e, f defined as in §2. Since $\rho = 1$, then

$A \cong M_n(K)$, $n = |G|$. Let V be a simple A-module. The structure theory for hereditary orders ([**6**, 39.18]) provides a Λ_s-submodule M contained in V with the following properties:

(a) r is the unique positive integer such that $(\operatorname{rad}\Lambda_s)^r M = P_K M$, (since $\operatorname{End}_A(V) = K$).

(b) $\Lambda_s = \{x \in A\colon x(\operatorname{rad}\Lambda_s)^i M \subseteq (\operatorname{rad}\Lambda_s)^i M, 0 \le i < r\}$.

(c) $\operatorname{rad}\Lambda_s = \{x \in A\colon x(\operatorname{rad}\Lambda_s)^i M \subseteq (\operatorname{rad}\Lambda_s)^{i+1} M, 0 \le i < r\}$.

(d) $(\operatorname{rad}\Lambda_s)^{i-1}M/(\operatorname{rad}\Lambda_s)^i M$, $1 \le i \le r$, are a full set of simple Λ_s-modules.

(e) $n_i = \dim_{\bar{K}}(\operatorname{rad}\Lambda_s)^{i-1}M/(\operatorname{rad}\Lambda_s)^i M$, $1 \le i \le r$.

The algebra A acts on L, via

$$\left(\sum x_g u_g\right)\cdot y = \sum x_g g(y), \quad \sum x_g u_g \in A,\ y \in L,$$

and acts irreducibly on L, so we may take L to be V. The non-zero Λ-submodules of L are O_L-submodules of L which are G-stable, so they are precisely $(\operatorname{rad} O_L)^i$, $i \in \mathbf{Z}$, by Lemma 2.1. We denote the Λ-module $(\operatorname{rad} O_L)^i$ by M_i.

LEMMA 3.1. *For each integer* $j \ge 0$,

(1) M_i *is a* Λ_j*-module*, $i \in \mathbf{Z}$, *and every non-zero* Λ_j*-submodule of* V *is* M_i *for some* i.

(2) $(\operatorname{rad}\Lambda_j)M_i = M_{i+1}$.

Proof. If (1) holds for some j, then $(\operatorname{rad}\Lambda_j)M_i \subsetneq M_i$, by Nakayama's Lemma, so $(\operatorname{rad}\Lambda_j)M_i \subseteq M_{i+1}$, since M_{i+1} is the unique maximal Λ_j-submodule of M_i. But $\operatorname{rad} O_L \subseteq \operatorname{rad}\Lambda_j$, since $(\operatorname{rad} O_L)M_i \subsetneq M_i$ for each i, and $(\operatorname{rad} O_L)M_i = M_{i+1}$, so $(\operatorname{rad}\Lambda_j)M_i = M_{i+1}$, proving (2). For (1), we use induction on j, having noted that it holds for Λ_0. Then for $j+1$,

$$\begin{aligned}\Lambda_{j+1}M_i &= \Lambda_{j+1}\left(\operatorname{rad}\Lambda_j\right)M_{i-1} \quad \text{(by (2) for } j)\\ &\subseteq \left(\operatorname{rad}\Lambda_j\right)M_{i-1} \quad \text{(by definition of } \Lambda_{i+1})\\ &= M_i\end{aligned}$$

so M_i is a Λ_{j+1}-module, $i \in \mathbf{Z}$. Since any Λ_{j+1}-module is also a Λ-module, the proof is complete.

LEMMA 3.2. (1) $\Lambda_s = \{x \in A\colon xM_i \subseteq M_i,\ i \in \mathbf{Z}\}$.

(2) $\operatorname{rad}\Lambda_s = \{x \in A\colon xM_i \subseteq M_{i+1},\ i \in \mathbf{Z}\}$.

(3) $\operatorname{rad}\Lambda_s = (\operatorname{rad} O_L)\Lambda_s = \Lambda_s(\operatorname{rad} O_L)$.

Proof. The structure of Λ_s is given in terms of a Λ_s-submodule M contained in V. From Lemma 3.1, any Λ_s-submodule of V must be M_k for some integer k. We have, from (b) and Lemma 3.1,

$$\Lambda_s = \{x \in A: xM_{k+i} \subseteq M_{k+i}, 0 \le i < r\}.$$

From (a), $M_{k+r} = (\text{rad}\,\Lambda_s)^r M_k = P_K M_k$, and since P_K is a principal ideal of O_K, then $M_{k+r} \cong M_k$ as Λ_s-modules. Then for $i \in \mathbf{Z}$,

$$(\text{rad}\,\Lambda_s)^i M_{k+r} = M_{i+k+r} \cong (\text{rad}\,\Lambda_s)^i M_k = M_{i+k}$$

so $M_{i+r} \cong M_i$ as Λ_s-modules, $i \in \mathbf{Z}$. Thus

$$\Lambda_s = \{x \in A: xM_i \subseteq M_i, i \in \mathbf{Z}\},$$

proving (1), and (2) follows from (1). Since $\text{rad}\,O_L \subseteq \text{rad}\,\Lambda_s$ and $(\text{rad}\,O_L)M_i = M_{i+1} = (\text{rad}\,\Lambda_s)M_i$, $i \in \mathbf{Z}$, (3) follows from (2).

Parts (1)–(4) of the Theorem are now straightforward in this case. If Γ is a hereditary order in A containing Λ, then applying the structure theory to Γ, there is a Γ-submodule M of V such that

$$\Gamma = \left\{x \in A: x(\text{rad}\,\Gamma)^i M \subseteq (\text{rad}\,\Gamma)^i M, 1 \le i \le \text{type number of } \Gamma\right\}.$$

Since $\Lambda \subseteq \Gamma$, M is a Λ-module, so $M = M_j$ for some integer j. Also, since $(\text{rad}\,O_L)M_i \subsetneq M_i$, $i \in \mathbf{Z}$, then $\text{rad}\,O_L \subseteq \text{rad}\,\Gamma$, and then $(\text{rad}\,\Gamma)^i M_j = M_{j+i}$, $i \in \mathbf{Z}$. It follows from Lemma 3.2 that $\Lambda_s \subseteq \Gamma$, proving (1) of the theorem. Part (2) is contained in Lemma 3.2. For (3), we know from (a) that r is the integer such that $(\text{rad}\,\Lambda_s)^r M_k = P_K M_k$. But

$$P_K M_k = P_K O_L M_k = (\text{rad}\,O_L)^e M_k = M_{k+e}$$

so $r = e$. (Note that $m = 1$ here.) For (4),

$$\begin{aligned}&(\text{rad}\,\Lambda_s)^{i-1} M_k/(\text{rad}\,\Lambda_s)^i M_k \\ &\quad = M_{k+i-1}/M_{k+i} = (\text{rad}\,O_L)^{k+i-1}/(\text{rad}\,O_L)^{k+i}\end{aligned}$$

and as $\overline{K}$-modules $(\text{rad}\,O_L)^{k+i-1}/(\text{rad}\,O_L)^{k+i} \cong O_L/\text{rad}\,O_L$ so

$$n_i = \dim_{\overline{K}} O_L/\text{rad}\,O_L = f, 1 \le i \le r.$$

In order to prove (5), we use the following result.

LEMMA 3.3. *Suppose that a is an integer ≥ 0 such that $(\text{rad}\,\Lambda_s)^a$ is the largest left Λ_s-ideal contained in Λ. Then $s = a$.*

Proof. If $a = 0$, then $\Lambda_s \subseteq \Lambda$, so $\Lambda_s = \Lambda$, and $s = 0$. Assuming that $a > 0$, we show that $(\text{rad}\,\Lambda_s)^{a-1}$ is the largest left Λ_s-ideal contained in Λ_1. First,

$$(\text{rad}\,\Lambda_s)^{a-1}\text{rad}\,\Lambda \subseteq (\text{rad}\,\Lambda_s)^{a-1}\text{rad}\,\Lambda_s = (\text{rad}\,\Lambda_s)^a.$$

Now $(\operatorname{rad}\Lambda_s)^a \subseteq \Lambda$ by hypothesis, and $\operatorname{rad}\Lambda_s \cap \Lambda \subseteq \operatorname{rad}\Lambda$, by Lemma 3.2. Thus $(\operatorname{rad}\Lambda_s)^a \subseteq \operatorname{rad}\Lambda$. Then $(\operatorname{rad}\Lambda_s)^{a-1}(\operatorname{rad}\Lambda) \subseteq \operatorname{rad}\Lambda$, so $(\operatorname{rad}\Lambda_s)^{a-1} \subseteq \Lambda_1$.

Next, if L is a left Λ_s-ideal contained in Λ_1, then $L \operatorname{rad}\Lambda \subseteq \operatorname{rad}\Lambda$, so $L \operatorname{rad}\Lambda \subseteq (\operatorname{rad}\Lambda_s)^a$. Then

$$L \operatorname{rad}\Lambda_s = L(\operatorname{rad}\Lambda)\Lambda_s \subseteq (\operatorname{rad}\Lambda_s)^a.$$

Since $\operatorname{rad}\Lambda_s$ is invertible, $L \subseteq (\operatorname{rad}\Lambda_s)^{a-1}$ as desired.

Now by induction, the length of the chain $\Lambda_1 \subseteq \Lambda_2 \subseteq \cdots \subseteq \Lambda_s$ is $a-1$, so $s = a$, and the proof is complete.

Let $\operatorname{trd}: A \to K$ be the reduced trace, and for an O_K-submodule L of A with $KL = A$, let

$$\tilde{L} = \{x \in A : \operatorname{trd}(xL) \subseteq O_K\}$$

be the complementary module.

LEMMA 3.4. *Let Γ be any hereditary O_K-order contained in the split simple algebra $A = M_n(K)$. Then*

$$\tilde{\Gamma} = P_K^{-1} \operatorname{rad}\Gamma.$$

Proof. Suppose that Γ has type number r, invariants $n_1, \dots, n_r$, and Γ consists of block matrices as mentioned in section 1. Let π_K be a prime element of O_K. For integers i, j, $1 \le i, j \le n$, let Y_{ij} denote the matrix whose i, j-entry is π_K if the i, j-position is above the diagonal of blocks of Γ, or 1 otherwise, and all of whose other entries are 0 (so $Y_{ij} \in \Gamma$.) Let y_{ij} denote the non-zero entry of Y_{ij}. Let $X = (x_{ij})$ be any element of A. Then XY_{ij} has at most one non-zero entry on the main diagonal, namely $x_{ij}y_{ji}$. We have $\operatorname{trd}(XY_{ij})$ = trace of matrix $XY_{ij} = x_{ij}y_{ji}$. Then $X \in \tilde{\Gamma}$ $\Leftrightarrow x_{ij}y_{ji} \in O_K$, all i, j $\Leftrightarrow$ when X is partitioned according to the block partition induced by Γ, the entries below the diagonal of blocks are in P_K^{-1}, and the other entries are in O_K. But such matrices are precisely those in $P_K^{-1} \operatorname{rad}\Gamma$. Since the Y_{ij} give a free basis for Γ over O_K, the result follows.

LEMMA 3.5. *Let $w = d - (e-1)$. Then $(\operatorname{rad}\Lambda_s)^w$ is the largest left Λ_s-ideal contained in Λ.*

Proof. From Lemma 3.2, we have $\operatorname{rad}\Lambda_s = (\operatorname{rad} O_L)\Lambda_s$, so $(\operatorname{rad}\Lambda_s)^w = (\operatorname{rad} O_L)^{d-(e-1)}\Lambda_s$. From Lemma 3.4

$$\tilde{\Lambda}_s = P_K^{-1} \operatorname{rad}\Lambda_s = (\operatorname{rad} O_L)^{-e}(\operatorname{rad} O_L)\Lambda_s = (\operatorname{rad} O_L)^{-e+1}\Lambda_s,$$

so

$$(\operatorname{rad} \Lambda_s)^w = (\operatorname{rad} O_L)^d \tilde{\Lambda}_s = \left((\operatorname{rad} O_L)^{-d} \Lambda_s\right)^{\sim}.$$

From Lemma 2.2, $\operatorname{trd}(\Sigma x_g u_g) = \operatorname{tr}_{L/K}(x_1)$, so

$$\tilde{\Lambda} = \mathscr{D}^{-1}\Lambda = (\operatorname{rad} O_L)^{-d}\Lambda \subseteq (\operatorname{rad} O_L)^{-d}\Lambda_s,$$

$$(\operatorname{rad} \Lambda_s)^w = \left((\operatorname{rad} O_L)^{-d}\Lambda_s\right)^{\sim} \subseteq \tilde{\tilde{\Lambda}} = \Lambda,$$

so $(\operatorname{rad} \Lambda_s)^w$ is contained in Λ. If L is any other left Λ_s-ideal contained in Λ, then $\tilde{L}$ is a right Λ_s-module containing $\tilde{\Lambda}$, so

$$\tilde{L} \supseteq \tilde{\Lambda}\Lambda_s = \mathscr{D}^{-1}\Lambda_s = (\operatorname{rad} O_L)^{-d}\Lambda_s,$$
$$L = \tilde{\tilde{L}} \subseteq \left((\operatorname{rad} O_L)^{-d}\Lambda_s\right)^{\sim} = (\operatorname{rad} \Lambda_s)^w,$$

completing the proof.

Now (5) of the Theorem follows from Lemmas 3.3 and 3.5.

4. The general case. In this section we continue with the assumption that L/K is a Galois algebra, and we prove the Theorem in the case that ρ is any factor set with values in O_L^*. Since $\bar{K}$ is finite, there is an unramified field extension K' of K such that the algebra $A' = A \otimes_K K'$ splits ([7, Prop. 2, p. 191].) Let O' be the integral closure of O_K in K', and let $\Lambda' = \Lambda \otimes_{O_K} O'$.

LEMMA 4.1. *If Γ is an O_K-order, then*

$$\operatorname{rad}\left(\Gamma \otimes_{O_K} O'\right) = (\operatorname{rad}\Gamma) \otimes_{O_K} O'.$$

Proof. Denote O_K by O, and P_K by P. Clearly

$$(\operatorname{rad}\Gamma) \otimes_O O' \subseteq \operatorname{rad}\left(\Gamma \otimes_O O'\right).$$

For the reverse inclusion, we have

$$\left(\Gamma \otimes_O O'\right)/(\operatorname{rad}\Gamma) \otimes_O O' \cong (\Gamma/\operatorname{rad}\Gamma) \otimes_O O'.$$

Since $P \subseteq \operatorname{rad}\Gamma$, then $\Gamma/\operatorname{rad}\Gamma$ is an O/P-module, and

$$(\Gamma/\operatorname{rad}\Gamma) \otimes_O O' \cong (\Gamma/\operatorname{rad}\Gamma) \otimes_{O/P} \left(O'/PO'\right).$$

Since K'/K is unramified, then O'/PO' is field, which is separable over $\bar{K}$ since $\bar{K}$ is finite. Then the semi-simple O/P-algebra $\Gamma/\operatorname{rad}\Gamma$ remains semi-simple after tensoring with O'/PO', so $\Gamma \otimes_O O'/(\operatorname{rad}\Gamma) \otimes_O O'$ is semi-simple, and the result follows.

We let G act on $L' = L \otimes_K K'$ by

$$g(x \otimes y) = g(x) \otimes y, \qquad x \in L,\ y \in K',\ g \in G.$$

Then L' is a Galois algebra over K' with Galois group G. We have $O_{L'} = O_L \otimes_{O_K} O'$, and

$$\Lambda' = \Lambda \otimes_{O_K} O' = \left(O_{L'}/O', G, \rho\right).$$

Let us show that in going from L/K to L'/K', the numbers d, e, f are unchanged.

Applying Lemma 4.1 to the O_K-order O_L, we have $\operatorname{rad} O_{L'} = (\operatorname{rad} O_L) \otimes_{O_K} O'$. Since the maximal ideal P' of O' is $P_K O'$, then

$$P' O_{L'} = (P_K O_L) \otimes_{O_K} O' = (\operatorname{rad} O_L)^e \otimes_{O_K} O' = (\operatorname{rad} O_{L'})^e$$

so the ramification index of L'/K' is still e. Similarly,

$$\dim_{\overline{K}'}(O_{L'}/\operatorname{rad} O_{L'}) = \dim_{\overline{K}}(O_L/\operatorname{rad} O_L) = f.$$

For the different exponent of L'/K', since

$$\operatorname{tr}_{L'/K'}(x \otimes y) = \operatorname{tr}_{L/K}(x) \otimes y, \qquad x \in L,\ y \in K',$$

then clearly $\tilde{O}_L \otimes_{O_K} O' \subseteq \tilde{O}_{L'}$; since $\tilde{O}_L = (\operatorname{rad} O_L)^{-d}$, and $\operatorname{rad} O_{L'} = (\operatorname{rad} O_L) \otimes_{O_K} O'$, then $(\operatorname{rad} O_{L'})^{-d} \subseteq \tilde{O}_{L'}$. If $(\operatorname{rad} O_{L'})^{-d-1} \subseteq \tilde{O}_{L'}$, then $(\operatorname{rad} O_L)^{-d-1} \subseteq \tilde{O}_L$, which is not so. Therefore $\tilde{O}_{L'} = (\operatorname{rad} O_{L'})^{-d}$.

LEMMA 4.2. *If Γ is an O_K-order contained in a semi-simple algebra A, then*

$$O_l(\operatorname{rad} \Gamma) \otimes_{O_K} O' = O_l\left(\operatorname{rad}\left(\Gamma \otimes_{O_K} O'\right)\right).$$

Proof. It is clear that the left side is contained in the right. There is an isomorphism

$$\phi\colon O_l(\operatorname{rad} \Gamma) \to \operatorname{Hom}_\Gamma(\operatorname{rad} \Gamma, \operatorname{rad} \Gamma),$$

where $\operatorname{rad} \Gamma$ is considered as a right Γ-module. Similarly, there is an isomorphism

$$\psi\colon O_l(\operatorname{rad} \Gamma') \to \operatorname{Hom}_{\Gamma'}(\operatorname{rad} \Gamma', \operatorname{rad} \Gamma'),$$

where $\Gamma' = \Gamma \otimes_O O'$. Since Γ is noetherian, then $\operatorname{rad} \Gamma$ is finitely presented over Γ, so from [**6**, 2.37] we have an isomorphism

$$\begin{aligned}\sigma\colon \operatorname{Hom}_\Gamma(\operatorname{rad} \Gamma, \operatorname{rad} \Gamma) \otimes_O O' &\to \operatorname{Hom}_{\Gamma \otimes_O O'}\left(\operatorname{rad} \Gamma \otimes_O O', \operatorname{rad} \Gamma \otimes_O O'\right)\\ &= \operatorname{Hom}_{\Gamma'}(\operatorname{rad} \Gamma', \operatorname{rad} \Gamma')\end{aligned}$$

from Lemma 4.1. The map

$$\psi^{-1}\sigma(\phi \otimes 1)\colon O_l(\operatorname{rad}\Gamma) \otimes_{O_K} O' \to O_l(\operatorname{rad}\Gamma')$$

is the identity, and the result is proved.

LEMMA 4.3. *Let $\Lambda = (O_L/O_K, G, \rho)$ be a crossed product order in $A = (L/K, G, \rho)$ and suppose that A splits over K. Then $\Lambda \cong (O_L/O_K, G, 1)$.*

Proof. Since the algebra A is split over K, the class of ρ in $H^2(G, L^*)$ is 1. We shall show that the map $H^2(G, O_L^*) \to H^2(G, L^*)$ is one-to-one, and then the class of ρ in $H^2(G, O_L^*)$ will be 1, and the result will follow.

Let E be the set of primitive idempotents of L and let $M = \oplus_{\varepsilon \in E} Z\varepsilon$ be the free Z-module with basis E; G acts on M via its action on E. For ε in E, let v_ε be the normalized valuation on the field $L\varepsilon$, and define $v\colon L^* \to M$ by

$$v(x) = \sum_{\varepsilon \in E} v_\varepsilon(x\varepsilon)\varepsilon, \qquad x \in L^*.$$

Then we get an exact sequence of G-modules

$$o \to O_L^* \to L^* \xrightarrow{v} M \to o,$$

giving rise to the exact sequence

$$H^1(G, M) \to H^2(G, O_L^*) \to H^2(G, L^*).$$

Since M is a permutation module, M is isomorphic to the induced module $\operatorname{Ind}_H^G(\mathbf{Z}) = \mathbf{Z}G \otimes_{ZH} \mathbf{Z}$, where H is the stabilizer of an idempotent in E, and $H^1(G, M) = H^1(H, \mathbf{Z}) = 0$, since H is finite. Then $H^2(G, O_L^*) \to H^2(G, L^*)$ is one-to-one, as desired.

From Lemma 4.2, the chains

$$\Lambda_0 \subseteq \Lambda_1 \subseteq \cdots \subseteq \Lambda_s$$

$$\Lambda'_0 \subseteq \Lambda'_1 \subseteq \cdots \subseteq \Lambda'_s$$

have the same length, and Λ'_s is hereditary. Since the Theorem has been proved in the split case, and since $\Lambda' \cong (O_{L'}/O', G, 1)$, which follows from Lemma 4.3, we find that $s = d - (e - 1)$. If Γ is a hereditary order in A containing Λ, then $\Gamma' = \Gamma \otimes_{O_K} O'$ is a hereditary order in A' containing A', and since Λ'_s is the unique minimal hereditary order in A' containing A', then $\Lambda'_s \subseteq \Gamma'$. We may embed Γ in Γ' as $\Gamma \otimes_{O_K} 1$, and A in A' as $A \otimes_K 1$, and then $\Gamma = \Gamma' \cap A \supseteq \Lambda'_s \cap A = \Lambda_s$, so Λ_s is the unique minimal hereditary order in A containing Λ.

From [**6**, 39.14] we have

$$\Lambda_s/\text{rad}\,\Lambda_s \cong \prod_{i=1}^{r} M_{n_i}(\bar{\Delta})$$

where $\bar{\Delta} = \Delta/\text{rad}\,\Delta$, and Δ is the unique maximal order in $\text{End}_A(V)$, with V a simple A-module. Then

$$\begin{aligned}\Lambda'_s/\text{rad}\,\Lambda'_s &\cong (\Lambda_s/\text{rad}\,\Lambda_s) \otimes_{O_K} O' \cong (\Lambda_s/\text{rad}\,\Lambda_s) \otimes_{\bar{K}} \bar{K}' \\ &\cong \prod_{i=1}^{r} M_{n_i}(\bar{\Delta} \otimes_{\bar{K}} \bar{K}').\end{aligned}$$

Now $\bar{\Delta} \otimes_{\bar{K}} \bar{K}' \cong (\bar{K}')^m$, where m is the Schur index of A, since $\bar{K}$ is finite ([**6**, 14.3]). Thus

$$\Lambda'_s/\text{rad}\,\Lambda'_s \cong \left(\prod_{i=1}^{r} M_{n_i}(\bar{K}')\right)^m.$$

Therefore the type number of $\Lambda'_s/\text{rad}\,\Lambda'_s$, known to be e from §3, is equal to mr, yielding

$$r = \frac{e}{m}.$$

Each invariant $n_i = f$, since the invariants n_i of Λ'_s are f. Therefore the proof of the theorem is complete.

5. Generators for Λ_s in the split case. In this section we find generators for Λ_s in the case that $\rho = 1$. To simplify the exposition, we assume that L is a field, which is totally ramified over K. We let P_L be the maximal ideal of O_L, and let v_L be the normalized valuation on L. Let M_i denote the Λ-module P_L^i, $i \in \mathbf{Z}$.

LEMMA 5.1. *Let $w = d - (e - 1)$, and let x be an element of L such that $v_L(x) = -w$. Let $\alpha = x\sum_{g \in G} u_g \in A$. Then $\alpha M_i \subseteq M_i$, $i \in \mathbf{Z}$ (so $\alpha \in \Lambda_s$, from Lemma 3.2), and unless $i \equiv -w \pmod e$, $\alpha M_i \subseteq M_{i+1}$, whereas if $i \equiv -w \pmod e$, $\alpha M_i \not\subseteq M_{i+1}$.*

Proof. Let tr denote the trace from L to K. We first compute $\text{tr}(P_L^i)$, $i \in \mathbf{Z}$. We have, for $j \in \mathbf{Z}$,

$$\begin{aligned}\text{tr}(P_L^i) \subseteq P_K^j &\Leftrightarrow \text{tr}(P_L^i P_K^{-j}) \subseteq O_K \\ &\Leftrightarrow \text{tr}(P_L^{i-ej}) \subseteq O_K \Leftrightarrow P_L^{i-ej} \subseteq \mathcal{D}^{-1} \\ &\Leftrightarrow P_L^{i-ej+d} \subseteq O_L \Leftrightarrow i - ej + d \geq 0 \\ &\Leftrightarrow j \leq \frac{i+d}{e}\end{aligned}$$

(we have used $\mathcal{D} = P_L^d$). Thus

$$\operatorname{tr}\left(P_L^i\right) = P_K^{[(i+d)/e]},$$

where [ ] denotes greatest integer. Since $\Sigma u_g \cdot y = \Sigma g(y) = \operatorname{tr} y$, $y \in L$, we have

$$O_L \alpha M_i = O_L x \operatorname{tr}\left(P_L^i\right) = x O_L P_K^{[(i+d)/e]} = x P_L^{e[(i+d)/e]}.$$

Write

$$\left[\frac{i+d}{e}\right] = \left[\frac{i+w}{e} + \frac{d-w}{e}\right] = \left[\frac{i+w}{e} + \frac{e-1}{e}\right].$$

If $(i+w)/e \notin \mathbf{Z}$, then $[(i+d)/e] > (i+w)/e$, so $e[(i+d)/e] \geq i+w$, and

$$O_L \alpha M_i \subseteq x P_L^{i+w+1} = P_L^{i+1} = M_{i+1}.$$

If $(i+w)/e \in \mathbf{Z}$, then $[(i+d)/e] = (i+w)/e$, so $e[(i+d)/e] = i+w$, and

$$O_L \alpha M_i = x P_L^{i+w} = M_i.$$

This completes the proof.

Let π_L be a prime element of O_L. Then from Lemma 3.2, we have $\pi_L^{-1} \Lambda_s \pi_L = \Lambda_s$. Let $\alpha = x \Sigma u_g$ be the element of Lemma 5.1, and define

$$\alpha_i = \pi_L^{-i} \alpha \pi_L^i, \qquad 0 \leq i < e.$$

From Lemma 5.2, it follows that α_i acts non-trivially on M_{-w+i}/M_{-w+i+1}, whereas α_i annihilates M_j/M_{j+1} if $j \not\equiv -w+i \pmod{e}$. Thus the simple Λ_s-modules M_0/M_1, $M_1/M_2, \ldots, M_{e-1}/M_e$ are non-isomorphic, and hence form a complete set of simple Λ_s-modules. Recall that $\Lambda_s/\operatorname{rad} \Lambda_s \cong \prod_{i=1}^r M_{n_i}(\overline{K})$, and each $n_i = f = 1$, since we are assuming that L/K is totally ramified. Hence $\Lambda_s/\operatorname{rad} \Lambda_s$ is commutative. Further, $r = e$, so $\dim_{\overline{K}}(\Lambda_s/\operatorname{rad} \Lambda_s) = e$. Then the elements $\alpha_i + \operatorname{rad} \Lambda_s$ generate $\Lambda_s/\operatorname{rad} \Lambda_s$ as a $\overline{K}$-module, $0 \leq i < e$. Since $\operatorname{rad} \Lambda_s = P_L \Lambda_s$, we see that $O_L \alpha_i$, $0 \leq i < e$, generate Λ_s as an O_K-module. So $\pi_L^j \alpha_i$, $0 \leq j < e$, $0 \leq i < e$, generate Λ_s as an O_K-module.

Finally, from the formula $\operatorname{tr}(P_L^i) = P_K^{[(i+d)/e]}$ from Lemma 5.1, if we set $i = -w$, then $i + d = e - 1$, so $\operatorname{tr}(P_L^{-w}) = O_K$. Thus we may find y in L with $v_L(y) = -w$ such that $\operatorname{tr}(y) = u$ is a unit of O_K. Then $x = u^{-1} y$ has $v_L(x) = -w$ and $\operatorname{tr}(x) = 1$. Now $(\Sigma u_g) x (\Sigma u_g) = \operatorname{tr}(x) \Sigma u_g = \Sigma u_g$, so $\alpha = x \Sigma u_g$ is idempotent. From the action of α on the simple modules M_i/M_{i+1}, we find that α is a primitive idempotent of Λ_s, and that the elements $\alpha_i + \operatorname{rad} \Lambda_s$ are all the primitive idempotents of $\Lambda_s/\operatorname{rad} \Lambda_s$.

6. Complements. The results of Auslander-Goldman-Rim-Williamson mentioned in the Introduction follow easily from our Theorem. If $\rho = 1$, Λ is a maximal order in $A \Leftrightarrow s = 0$, $r = 1 \Leftrightarrow e/m = 1 \Leftrightarrow e = 1$, since $m = 1$. For any ρ, Λ is hereditary $\Leftrightarrow s = 0 \Leftrightarrow d = e - 1 \Leftrightarrow L/K$ is tamely ramified, from **[7**, Prop. 13, p. 67].

We also recover a result of Janusz **[4]**, who showed that, in the tamely ramified case, Λ has type e/m and invariants f. (See also Merklen **[5]**.)

From the fact that $r = e/m$, we find a way to compute the Schur index m of A as follows: the centre of $\Lambda_s/\text{rad}\,\Lambda_s$ has e/m component fields (each of dimension m over $\bar{K}$).

It may be shown that the index

$$(\Lambda_s : \Lambda) = \pi_K^{n^2(d-(e-1))/2e}$$

where $n = [L : K]$. This follows from

$$(\tilde{\Lambda} : \Lambda) = (\tilde{\Lambda}_s : \Lambda_s)(\Lambda_s : \Lambda)^2.$$

Note that Lemma 3.4 (that $\tilde{\Lambda} = P_K^{-1}\,\text{rad}\,\Lambda$ if Λ is hereditary) also holds in the non-split case, as may be shown by tensoring with an unramified extension.

In the split case (§3), the Λ-lattices contained in a irreducible A-module V are linearly ordered, but this fails to be true if A is not split. However, it may be shown, in general, that the Λ-lattices M in V such that $\text{End}_\Lambda(M)$ is the maximal order in $\text{End}_A(V)$ are linearly ordered, and this can be used to prove the Theorem, just as in §3.

Note that we could have used right-orders $\Lambda'_{j+1} = O_r(\text{rad}\,\Lambda'_j)$ throughout, instead of left orders, and still obtain the same answer $s = d - (e - 1)$ for the length of the chain $\Lambda'_0 \subseteq \cdots \subseteq \Lambda'_s$. By uniqueness of Λ_s, we would get $\Lambda_s = \Lambda'_s$, but we do not know whether $\Lambda_j = \Lambda'_j$ for all j, $1 < j < s$.

References

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

[2] M. Auslander and D. S. Rim, *Ramification index and multiplicity*, Illinois J. Math., **7** (1963), 566–581.

[3] H. Benz and H. Zassenhaus, *Über verschränkte Produktordnungen*, J. Number Theory, **20** (1985), 282–298.

[4] G. Janusz, *Crossed product orders and the Schur index*, Comm. Algebra, **8** (1980), 697–706.

[5] H. Merklen, *Hereditary crossed product orders*, Pacific J. Math., **74** (1978), 391–406.
[6] I. Reiner, *Maximal Orders*, Academic Press, London, 1975.
[7] J.-P. Serre, *Corps Locaux*, Act. Sci. et Ind. 1296, Hermann, Paris, 1962.
[8] S. Williamson, *Crossed products and hereditary orders*, Nagoya Math. J., **23** (1963), 103–120.

Received September 21, 1984 and in revised form March 26, 1985. Supported by NSERC.

UNIVERSITY OF ALBERTA
EDMONTON, ALBERTA
CANADA T6G 2G1