

EQUIVALENCE CLASSES OF MAXIMAL ORDERS

SUSAN WILLIAMSON

Introduction. Let k denote the quotient field of a complete discrete rank one valuation ring R . The purpose of this paper is to establish a relationship between the Brauer group of k and the set of maximal orders over R which are equivalent to crossed products over tamely ramified extensions of R .

The Brauer group $B(k)$ of k is the union of groups $H^2(G, U(L))$ where L ranges over the set of all finite Galois extensions of k and G denotes the Galois group of L over k (see pp. 206-207 of [2]). The subset $V(k) = \cup H^2(G, U(L))$ where L ranges over all unramified extensions of k forms a subgroup of $B(k)$. In Section 1 we associate to each element of $V(k)$ a positive integer called its Brauer number. Then we define $T(k)$ to be the set of elements of $V(k)$ whose Brauer numbers are relatively prime to the characteristic of \bar{R} , and prove that $T(k)$ is a subgroup of $B(k)$. The object of the paper is to prove the following main theorem.

THEOREM. *Let k denote the quotient field of a complete discrete rank one valuation ring R . A maximal order over R in a central simple k -algebra Σ is equivalent to a crossed product over a tamely ramified extension of R if and only if the Brauer class of Σ is in the subgroup $T(k)$ of $B(k)$.*

The method of proof employs the theory of crossed products, and entails the construction of certain wildly ramified Galois extensions of k . For this, a separate treatment of the equicharacteristic case and the case of unequal characteristic is necessary (Sections 2 and 3 respectively).

We obtain as a corollary to the main theorem the fact that if R is an equicharacteristic ring of characteristic zero, then every maximal R -order is equivalent to a crossed product over a tamely ramified extension of R . We then exhibit the existence of a maximal R -order which is not equivalent to a

Received November 18, 1966.

crossed product in the case when R is a complete discrete rank one valuation ring with perfect residue class field.

The following notation shall be in use throughout the paper. The multiplicative group of units of a ring R shall be denoted by $U(R)$, and the radical of R by $\text{rad } R$. Unless otherwise stated, R shall always denote a complete discrete rank one valuation ring, π its prime element, and k its quotient field. The definitions of *crossed product* and *hereditary order* may be found in [10]. For the definitions of *tame* and *wild* ramification we refer the reader to [9]. The definition of the i^{th} ramification group is given on p. 73 of [7].

For the convenience of the reader we define the notions of equivalence which shall be used in the paper. A pair of central simple algebras Σ_1 and Σ_2 over a field k are said to be *equivalent* if there exist finite dimensional vector spaces V_1 and V_2 over k together with a k -algebra isomorphism

$$\Sigma_1 \otimes_R \text{Hom}_k(V_1, V_1) \approx \Sigma_2 \otimes_R \text{Hom}_k(V_2, V_2).$$

The set of equivalence classes of central simple algebras over a field k forms an Abelian group called the *Brauer group* of k . The inverse of the equivalence class determined by the central simple algebra Σ is the equivalence class determined by its opposite algebra Σ^0 (see Section 5 of [3]).

Let R denote a discrete rank one valuation ring. The set of maximal orders $M'(R)$ over R forms a subset of the set $H'(R)$ of hereditary orders over R (see [4]). In [3] Auslander and Goldman have defined a pair of hereditary R -orders Λ_1 and Λ_2 to be *equivalent* if there exist finitely generated free R -modules E_1 and E_2 and an R -algebra isomorphism

$$\Lambda_1 \otimes_R \text{Hom}_R(E_1, E_1) \approx \Lambda_2 \otimes_R \text{Hom}_R(E_2, E_2).$$

An hereditary order equivalent to a maximal order is itself a maximal order. The set of maximal orders in a fixed central simple algebra are isomorphic. Finally we mention that the equivalence relation on the set of maximal orders over R is induced by the Brauer group of the quotient field k of R . That is to say, if Σ_1 and Σ_2 are equivalent central simple algebras over the quotient field of a discrete rank one valuation ring, then the maximal orders of Σ_1 are equivalent to the maximal orders of Σ_2 (see Lemma 2.1 of [11]).

1. The Brauer number. Let k denote the quotient field of a complete discrete rank one valuation ring R and consider the subset $V(k)$ of the

Brauer group $B(k)$ of k defined by $V(k) = \cup H^2(G, U(L))$ where the union is taken over the set of all unramified Galois extensions L of k . It is well known that $V(k) = B(k)$ when \bar{R} is perfect. For an example to show that $V(k)$ need not equal $B(k)$ see Exer. 2 p. 224 of [7].

PROPOSITION 1.1 *The set $V(k)$ is a subgroup of the Brauer group of k .*

Proof. Consider crossed products $\Sigma_1 = \mathcal{A}(f_1, L_1, G_1)$ and $\Sigma_2 = \mathcal{A}(f_2, L_2, G_2)$ where the L_i are unramified Galois extensions of k and G_i denotes the Galois group of L_i over k . In order to prove the proposition it suffices to show that the Brauer class of $\mathcal{A}(f_1, L_1, G_1) \otimes_k \mathcal{A}(f_2, L_2, G_2)^0$ is in $V(k)$ where $\mathcal{A}(f_2, L_2, G_2)^0$ denotes the opposite ring of $\mathcal{A}(f_2, L_2, G_2)$.

The compositum L_1L_2 of L_1 and L_2 is an unramified extension of k according to Cor. 3-2-8 of [9]. For $i = 1, 2$ let g_i denote the image of f_i under the inflation map $Z^2(G_i, U(L_i)) \longrightarrow Z^2(G_1G_2, U(L_1L_2))$ where G_1G_2 denotes the Galois group of L_1L_2 over k . It is well known that $\mathcal{A}(f_i, L_i, G_i)$ is equivalent to $\mathcal{A}(g_i, L_1L_2, G_1G_2)$ for $i = 1, 2$ (see for example Thm. 8.5 E of [1]). Therefore $\Sigma_1 \otimes \Sigma_2^0$ is equivalent to $\mathcal{A}(g_1, L_1L_2, G_1G_2) \otimes \mathcal{A}(g_2^{-1}, L_1L_2, G_1G_2)$ since $\mathcal{A}(g_2^{-1}, L_1L_2, G_1G_2)$ represents the Brauer class of Σ_2^0 . The fact that $\mathcal{A}(g_1, L_1L_2, G_1G_2) \otimes \mathcal{A}(g_2^{-1}, L_1L_2, G_1G_2)$ is equivalent to $\mathcal{A}(g_1g_2^{-1}, L_1L_2, G_1G_2)$ (see Thm. 8.5 A of [1] or pp. 404-405 of [3]) implies that the Brauer class of $\Sigma_1 \otimes \Sigma_2^0$ is in $V(k)$.

For convenience of notation we shall always denote the Brauer class in $B(k)$ of a central simple k -algebra Σ by $\tilde{\Sigma}$. We proceed to define the Brauer number of an element of $V(k)$. A central simple k -algebra Σ for which $\tilde{\Sigma}$ is in $V(k)$ is equivalent to a crossed product $\mathcal{A}(f, L, G)$ for some unramified Galois extension L of k with Galois group G . Let S denote the integral closure of R in L and consider the exact sequence of cohomology groups

$$(1) \longrightarrow H^2(G, U(S)) \longrightarrow H^2(G, U(L)) \xrightarrow{\phi} H^2(G, Z^+) \longrightarrow (1)$$

defined explicitly on p. 193 of [7].

DEFINITION. The *Brauer number* of an element $\tilde{\Sigma}$ of $V(k)$ is defined to be the order of the image of the cohomology class $[f]$ in $H^2(G, Z^+)$ under the map ϕ .

Observe that the Brauer number of $\tilde{\Sigma}$ is the least positive integer n such that $[f^n]$ is in the image of the natural map $H^2(G, U(S)) \longrightarrow H^2(G, U(L))$. Therefore when the Brauer number of $\tilde{\Sigma}$ is 1, we know by Thm. 2.3 of [11] that a maximal order in Σ is equivalent to a crossed product over a tamely ramified extension of R .

The Brauer number is well defined according to the next proposition.

PROPOSITION 1.2. *The Brauer number of an element $\tilde{\Sigma}$ of $V(k)$ is independent of the choice of representative of $\tilde{\Sigma}$ as a crossed product over an unramified extension of k .*

Proof. Let $\Delta(f_1, L_1, G_1)$ and $\Delta(f_2, L_2, G_2)$ denote equivalent central simple k -algebras, where L_1 and L_2 are unramified Galois extensions of k with Galois groups G_1 and G_2 respectively. Let L_1L_2 denote the compositum of L_1 and L_2 , and G_1G_2 the Galois group of L_1L_2 over k . Observe that L_1L_2 is an unramified extension of k . For $i = 1, 2$ let $[g_i]$ denote the image of $[f_i]$ under the inflation map $H^2(G_i, U(L_i)) \longrightarrow H^2(G_1G_2, U(L_1L_2))$. The assumption that $\Delta(f_1, L_1, G_1)$ is equivalent to $\Delta(f_2, L_2, G_2)$ implies that $[g_1] = [g_2]$. Therefore in order to prove the proposition it is sufficient to prove that the order of $\phi([f_1])$ is equal to the order of $\phi^*([g_1])$ where $\phi: H^2(G_1, U(L_1)) \longrightarrow H^2(G_1, Z^+)$ and $\phi^*: H^2(G_1G_2, U(L_1L_2)) \longrightarrow H^2(G_1G_2, Z^+)$ are the maps used in the definition of the Brauer number.

Consider the following diagram.

$$\begin{array}{ccc} H^2(G_1, U(L_1)) & \xrightarrow{\text{inf}} & H^2(G_1G_2, U(L_1L_2)) \\ \downarrow \phi & & \downarrow \phi^* \\ H^2(G_1, Z^+) & \xrightarrow{\text{inf}} & H^2(G_1G_2, Z^+) \end{array}$$

It is easy to verify that the above diagram is commutative. Therefore, in order to prove the proposition, it is sufficient to prove that the order of an element of $H^2(G_1, Z^+)$ is preserved under the inflation map. So consider an element $[h]$ of $H^2(G_1, Z^+)$, and let $[h^*]$ denote the image of $[h]$ in $H^2(G_1G_2, Z^+)$. We proceed to show that the order s of $[h]$ is equal to the order t of $[h^*]$. The inequality $t \leq s$ is clear. To establish the opposite inequality we observe that since t is the order of $[h^*]$ there exists a map $\Psi: G_1G_2 \longrightarrow Z^+$ such that $(h^*(\alpha, \beta))^t = \Psi(\alpha) + \Psi(\beta) - \Psi(\alpha\beta)$ for all elements α and β of G_1G_2 . The equalities $0 = (h^*(1, 1))^t = \Psi(1) + \Psi(1) - \Psi(1)$ imply that $\Psi(1) = 0$.

Denote the Galois group of L_1L_2 over L_1 by G . We next observe that $\Psi(\alpha) = 0$ whenever α is in the subgroup G of G_1G_2 . For since h^* is the image of h under inflation it follows that $0 = (h(1, 1))^t = (h^*(\alpha, \alpha))^t = 2\Psi(\alpha) - \Psi(\alpha^2)$ for α in G . Proceeding inductively one may show that $0 = (\text{ord } \alpha)\Psi(\alpha) - \Psi(\alpha^{\text{ord } \alpha})$ where $\text{ord } \alpha$ denotes the order of the element α of G , and therefore $\Psi(\alpha) = 0$ for every element α of G . Finally we observe that if $\bar{\alpha} = \bar{\beta}$ then $\Psi(\alpha) = \Psi(\beta)$, where $\bar{\alpha}$ denotes the image of α under the natural map of G_1G_2 onto $G_1G_2/G = G_1$. For, writing $\alpha = r\beta$ for some element r of G , and using the fact that $\Psi(r) = 0$, one may obtain the equalities $0 = (h(\bar{1}, \bar{\beta}))^t = (h^*(r, \beta))^t = \Psi(r) + \Psi(\beta) - \Psi(r\beta) = \Psi(\beta) - \Psi(\alpha)$. Therefore $\Psi(\alpha) = \Psi(\beta)$. We may now consider the (well-defined) map $\theta: G_1 \rightarrow Z^+$ defined by $\theta(\bar{\alpha}) = \Psi(\alpha)$. The fact that $(h(\bar{\alpha}, \bar{\beta}))^t = \theta(\bar{\alpha}) + \theta(\bar{\beta}) - \theta(\overline{\alpha\beta})$ implies that $[h]^t = [1]$. Therefore $s \leq t$, and this completes the proof.

We next define $T(k)$ to be the set of all elements of $V(k)$ whose Brauer numbers are relatively prime to the characteristic of \bar{R} . We adopt the convention that every number is relatively prime to zero, so that $T(k) = B(k)$ when \bar{R} has characteristic zero.

The following lemma shall be useful in proving that $T(k)$ is a subgroup of $V(k)$.

LEMMA 1.3. *Let Σ denote a central simple k -algebra such that $\tilde{\Sigma}$ is in $V(k)$, and let Σ^0 denote the opposite ring of Σ . Then $\tilde{\Sigma}$ and $\tilde{\Sigma}^0$ have the same Brauer number.*

Proof. Let $\mathcal{A}(f, L, G)$ be a representative of $\tilde{\Sigma}$ with L an unramified Galois extension of k . The k -algebra isomorphism $\mathcal{A}(f, L, G)^0 \approx \mathcal{A}(f^{-1}, L, G)$ implies that $\tilde{\Sigma}^0$ may be represented by $\mathcal{A}(f^{-1}, L, G)$. Consider the map $\phi: H^2(G, U(L)) \rightarrow H^2(G, Z^+)$. Since $\phi([f])$ and $\phi([f^{-1}])$ have the same order it now follows that $\tilde{\Sigma}$ and $\tilde{\Sigma}^0$ have the same Brauer number.

PROPOSITION 1.4. *The set $T(k)$ is a subgroup of $V(k)$.*

Proof. Let $\Sigma_1 = \mathcal{A}(f_1, L_1, G_1)$ and $\Sigma_2 = \mathcal{A}(f_2, L_2, G_2)$ be central simple k -algebras whose Brauer classes $\tilde{\Sigma}_1$ and $\tilde{\Sigma}_2$ are in $T(k)$, and let n_1 and n_2 denote the Brauer numbers of $\tilde{\Sigma}_1$ and $\tilde{\Sigma}_2$ respectively. Form the tensor product $\Sigma = \Sigma_1 \otimes \Sigma_2$ and recall that the Brauer number of $\tilde{\Sigma}_2^0$ is n_2 according to Lemma 1.3. To prove the proposition it suffices to show that the Brauer number of $\tilde{\Sigma}$ is relatively prime to the characteristic of \bar{R} .

For $i = 1, 2$ let g_i denote the image of f_i under the inflation map $Z^2(G_i, U(L_i)) \longrightarrow Z^2(G_1G_2, U(L_1L_2))$ where L_1L_2 is the compositum of L_1 and L_2 and G_1G_2 is the Galois group of L_1L_2 over k , and observe that Σ is equivalent to $\mathcal{A}(g_1g_2^{-1}, L_1L_2, G_1G_2)$. Consider the map $\phi: H^2(G_1G_2, U(L_1L_2)) \longrightarrow H^2(G_1G_2, Z^+)$ defined at the beginning of this section. Since $(\phi([g_1]))^{n_1} = [1]$ and $(\phi([g_2^{-1}]))^{n_2} = [1]$ it is clear that $(\phi([g_1g_2^{-1}]))^{n_1n_2} = [1]$ so that the Brauer number of $\widetilde{\Sigma}$ divides n_1n_2 and is hence relatively prime to the characteristic of \bar{R} .

REMARK 1.5. *The subgroup $T(k)$ need not equal $V(k)$.*

For consider the following example. Let $R = Z_p$ be the ring of p -adic integers, and $k = Q_p$ the quotient field of R . It is well known (see for example Prop. 3-2-12 of [9]) that there exists a (unique) unramified extension L of k with degree p . It is of the form $L = k(\zeta)$ where ζ denotes a primitive $(p^p - 1)^{st}$ root of unity. Furthermore, L is a cyclic Galois extension of k (see Remark 3-5-5 of [9]) and we denote the Galois group of L over k by G . Consider now the central simple k -algebra $\Sigma = \mathcal{A}(f, L, G)$ where f is the element of $Z^2(G, U(L))$ which corresponds to $p \bmod N(U(L))$ under the canonical identification $H^2(G, U(L)) = U(k) / N(U(L))$ which holds because G is a cyclic group. It is easy to verify that the Brauer number of $\widetilde{\Sigma}$ is p since p is not a norm from L . We may conclude therefore that $T(k)$ is properly contained in $V(k)$.

We have thus defined the following chain of subgroups of the Brauer group

$$B(k) \supset V(k) \supset T(k) \supset (1).$$

These groups shall be useful for studying equivalence classes of maximal orders over R .

We terminate Section 1 with some remarks concerning ramification. The ramification index of an hereditary order A over a discrete rank one valuation ring R can be defined according to Thm. 6.1 of [5]. For let π denote a prime element of R . Since the ideal πA is an invertible A -ideal, there exists a positive integer t such that $(\text{rad } A)^t = \pi A$.

DEFINITION. Let A be an hereditary order over a discrete rank one valuation ring R , and let π denote a prime element of R . The positive

integer t for which $(\text{rad } A)^t = \pi A$ is called the *ramification index* of A over R and is denoted by $r(A/R)$.

PROPOSITION 1.6. *The ramification index of an hereditary order A over a discrete rank one valuation ring R depends only upon the equivalence class of A .*

Proof. Let \mathcal{Q} denote an hereditary R -order which is equivalent to A . Then there exist finitely generated free R -modules E_1 and E_2 and an R -algebra isomorphism $A \otimes_R \text{Hom}_R(E_1, E_1) \approx \mathcal{Q} \otimes_R \text{Hom}_R(E_2, E_2)$. Since $\text{Hom}_R(E_1, E_1)$ is a central separable R -algebra it follows that $\text{rad}(A \otimes_R \text{Hom}_R(E_1, E_1)) = (\text{rad } A) \otimes_R \text{Hom}_R(E_1, E_1)$ according to the proof of Prop. 8.6 of [3]. Therefore $r(A \otimes_R \text{Hom}_R(E_1, E_1)/R) = r(A/R)$, and similarly $r(\mathcal{Q} \otimes_R \text{Hom}_R(E_2, E_2)/R) = r(\mathcal{Q}/R)$. From the above isomorphism we may now conclude that $r(A/R) = r(\mathcal{Q}/R)$.

PROPOSITION 1.7. *Let k denote the quotient field of a complete discrete rank one valuation ring R , and K a finite Galois extension of k with Galois group G . If the integral closure S of R in K is a tamely ramified extension of R , then the ramification index of a crossed product $\Delta(f, S, G)$ is equal to the ramification index of S over R .*

Proof. Since S is a tamely ramified extension of R it follows that the crossed product $\Delta = \Delta(f, S, G)$ is an hereditary R -order with radical $\Pi\Delta$ (see Prop. 1.3 of [10]), where Π denotes a prime element of S . Hence $r(\Delta/R) = r(S/R)$.

2. The case of unequal characteristic. Let R denote a complete discrete rank one valuation ring whose quotient field k has characteristic zero, and whose residue class field \bar{R} has characteristic $p \neq 0$. The purpose of this section is to prove that if $\tilde{\Sigma}$ is an element of $V(k)$ whose Brauer number is equal to p , then a maximal order in Σ is not equivalent to a crossed product over a tamely ramified extension of R .

Recall that an element $\tilde{\Sigma}$ of $V(k)$ may be represented by a crossed product over an unramified Galois extension of k . Therefore, throughout this section Σ shall denote a crossed product of the form $\Sigma = \Delta(f, L, G)$ where L is an unramified extension of k , and it shall be assumed that the Brauer number of $\tilde{\Sigma}$ is equal to the characteristic p of \bar{R} .

In order to prove that a maximal order Γ in such a central simple k -

algebra Σ is not equivalent to a crossed product over a tamely ramified extension of R , we shall prove that the ramification index $r(\Gamma/R)$ of Γ over R is divisible by p , so that Γ cannot be equivalent to a crossed product over a tamely ramified extension according to Prop. 1.7.

The method of proof is to reduce the problem to a study of crossed products by constructing a central simple k -algebra $\Sigma_w = \mathcal{A}(g, L_w, G_w)$ equivalent to $\mathcal{A}(f, L, G)$ and such that g is in $Z^2(G_w, U(S_w))$ where S_w , the integral closure of R in L_w , is a wildly ramified extension of R . We shall then construct a maximal order Γ_w in Σ_w such that Γ_w contains the crossed product $\mathcal{A}(g, S_w, G_w)$. Making use of this inclusion, we shall then prove that $r(\Gamma_w/R) = r(S_w/R)$.

In order to construct the desired crossed product $\mathcal{A}(g, L_w, G_w)$ we first construct the Galois extension L_w of k . Let L_t denote the extension of L obtained by adjoining a primitive p^{th} root of unity. Observe that the extension L_t of L is tamely ramified since its degree is less than or equal to $p-1$. Let S_t denote the integral closure of R in L_t . According to Prop. 3-4-2 of [9] we may select prime elements π and π_t of R and S_t respectively in such a way that $\pi_t^e = \pi$ where e denotes the ramification index of S_t over R .

Now L_w is defined to be the extension of L_t obtained by adjoining a root Π of the polynomial $F(X) = X^p - \pi_t$. Observe that L_w is a Galois extension of k since L_w contains a primitive p^{th} root of unity; we denote the Galois group of L_w over k by G_w . The extension L_w of L_t is a wildly ramified inertial extension of degree p and Π is a prime element of the integral closure S_w of R in L_w . By virtue of Prop. 1.2 we may as well assume that the integral closure S of R in L is the inertia ring of L_w over k .

Before constructing the 2-cocycle g of $Z^2(G_w, U(S_w))$ we summarize the ramification properties of the extension S_w of R .

LEMMA 2.1. *Let G_i denote the i^{th} ramification group of S_w over R . Then*

- i) G_1 is cyclic of order p
- ii) G_0/G_1 is cyclic of order e relatively prime to p
- iii) $G_0 = G_1 \times G_0/G_1$ (semi-direct product)
- iv) $G_i = G_1$ and $G_{i+1} = (1)$ for $i = a/(p-1)$ where a denotes the absolute ramification index of L_w .

Proof. Assertion i) is clear from the definition of the extension S_w of S_t . The second and third statements follow from Corollaries 1 and 4 respectively on p. 75 of [7], and the fourth statement follows from Ex. 4 p. 79 of [7].

The next lemma describes the action of the inertia group G_0 on the prime element Π of S_w . According to Lemma 2.1 we may view G_0/G_1 as a subgroup of G_0 .

LEMMA 2.2. *Let τ denote an element of G_1 and σ an element of G_0/G_1 . Then $\tau(\Pi) = \zeta_\tau \Pi$ for some p^{th} root of unity ζ_τ , and $\sigma(\Pi) = \xi_\sigma \Pi$ for some e^{th} root of unity ξ_σ , where e denotes the order of G_0/G_1 .*

Proof. It is clear from the definition of S_w that the conjugates of Π relative to S_t are of the form $\zeta^i \Pi$ for $1 \leq i \leq p$ where ζ denotes a primitive p^{th} root of unity, so that $\tau(\Pi) = \zeta_\tau \Pi$ for some p^{th} root of unity ζ_τ .

On the other hand we know that S contains a primitive e^{th} root of unity ξ according to Cor. 2-2-7 of [9]. Recall that the prime elements π of R and π_t of S_t were chosen so that $\pi_t^e = \pi$. Hence $X^{pe} - \pi$ is the minimal polynomial of Π over S . The pe conjugates of Π relative to S are therefore given by $\zeta^i \xi^j \Pi$ for $1 \leq i \leq p$ and $1 \leq j \leq e$. If σ is in G_0/G_1 then $\sigma^e(\Pi) = \Pi$ from which it follows that $\sigma(\Pi) = \xi_\sigma \Pi$ for some e^{th} root of unity ξ_σ .

Notation. Throughout the rest of this section τ shall denote a fixed generator of the cyclic group G_1 , and ζ the primitive p^{th} root of unity defined by $\tau(\Pi) = \zeta \Pi$.

The group G_1 is a normal subgroup of G_w . For each element σ of G_w we may therefore consider the integer $n(\sigma)$ defined modulo (p) by the equality $\sigma\tau\sigma^{-1} = \tau^{n(\sigma)}$. The next lemma presents properties of $n(\sigma)$ which shall be useful in this section.

LEMMA 2.3. *Let $n(\sigma)$ be defined as above. Then*

- i) $n(\sigma) = 1$ if and only if $\sigma = 1$ for σ in G_0/G_1
- ii) $\sigma(\zeta) = \zeta^{n(\sigma)}$ for each element σ of G_w .

Proof. Consider an element σ of G_0/G_1 . By the definition of $n(\sigma)$ it follows that $n(\sigma) = 1$ if and only if $\sigma\tau = \tau\sigma$ which holds if and only if $\sigma\tau(\Pi) =$

$\tau\sigma(\Pi)$ since τ is in G_1 and $S_w = S[\Pi]$. Let ζ_σ be the e^{th} root of unity satisfying $\sigma(\Pi) = \zeta_\sigma \Pi$. Then $\sigma\tau(\Pi) = \sigma(\zeta \Pi) = \zeta^\sigma \zeta_\sigma \Pi$ and $\tau\sigma(\Pi) = \tau(\zeta_\sigma \Pi) = \zeta_\sigma \zeta \Pi$. Therefore $n(\sigma) = 1$ if and only if $\zeta^\sigma = \zeta$, that is to say if and only if $\sigma = 1$. This proves statement i).

Now according to Lemma 2.2 we know the conjugates of Π relative to k . Therefore if σ is an element of G_w we have that $\sigma(\Pi) = u\Pi$ for some element u of $U(S_t)$. Then $\sigma\tau\sigma^{-1}(\Pi) = \sigma\tau(\Pi / \sigma^{-1}(u)) = \sigma(\zeta \Pi / \sigma^{-1}(u)) = \zeta^\sigma \Pi$. But $\sigma\tau\sigma^{-1}(\Pi) = \tau^{n(\sigma)}(\Pi) = \zeta^{n(\sigma)} \Pi$, so that $\zeta^\sigma = \zeta^{n(\sigma)}$.

This completes the study of the extension S_w of R , and we proceed now to construct the desired 2-cocycle g . The fact that the image of $[f]$ in $H^2(G, Z^+)$ has order p implies that there exists a map $\phi: G \rightarrow U(L)$ such that the 2-cocycle h of $Z^2(G, U(L))$ defined by $h(\sigma, \rho) = f^p(\sigma, \rho)\phi(\sigma\rho) / \phi(\sigma)\phi^\sigma(\rho)$ takes values in $U(S)$. Since $\phi(\sigma)$ is in $U(L)$ we may write $\phi(\sigma)$ in the form $\phi(\sigma) = \alpha_\sigma \pi^{\beta(\sigma)}$ where α_σ is in $U(S)$ and $\beta(\sigma)$ is an integer. Define the map $\phi_w: G_w \rightarrow U(L_w)$ by $\phi_w(\sigma) = \Pi^{e\beta(\bar{\sigma})}$ where e is the order of G_0/G_1 and $\bar{\sigma}$ denotes the image of σ under the natural map of G_w onto G . Let f_w denote the image of f under the inflation map $Z^2(G, U(L)) \rightarrow Z^2(G_w, U(L_w))$, and define the 2-cocycle g of $Z^2(G_w, U(L_w))$ by

$$g(\sigma, \rho) = f_w(\sigma, \rho)\phi_w(\sigma\rho) / \phi_w(\sigma)\phi_w^\sigma(\rho).$$

Observe that g is cohomologous to f_w in $Z^2(G_w, U(L_w))$ by definition, so that the central simple k -algebra $\mathcal{A}(g, L_w, G_w)$ is equivalent to $\mathcal{A}(f, L, G)$ (see for example Thm. 8.5 E of [1]). The next three propositions present some useful properties of the 2-cocycle g .

PROPOSITION 2.4. *The element g of $Z^2(G_w, U(L_w))$ defined above is in the image of the natural map $Z^2(G_w, U(S_t)) \rightarrow Z^2(G_w, U(L_w))$.*

Proof. We prove first that g is in the image of the natural map $Z^2(G_w, U(S_w)) \rightarrow Z^2(G_w, U(L_w))$. In order to verify that g takes values in $U(S_w)$ it clearly suffices to show that g^p takes values in $U(S_w)$. From the definition of g we obtain the equalities

$$\begin{aligned} g^p(\sigma, \rho) &= [f_w(\sigma, \rho)\phi_w(\sigma\rho) / \phi_w(\sigma)\phi_w^\sigma(\rho)]^p \\ &= [h(\bar{\sigma}, \bar{\rho})\phi(\bar{\sigma})\phi^{\bar{\sigma}}(\bar{\rho}) / \phi(\bar{\sigma}\bar{\rho})] [\phi_w(\sigma\rho) / \phi_w(\sigma)\phi_w^\sigma(\rho)]^p \end{aligned}$$

where σ and ρ are elements of G_w , and $\bar{\sigma}$ denotes the image of σ under

the natural map of G_w onto G . The definition of the map ϕ_w together with the equality $\Pi^{pe} = \pi$ implies that $\phi(\bar{\sigma}) / [\phi_w(\sigma)]^p = \alpha_{\bar{\sigma}}$ and $\phi(\bar{\rho}) / [\phi_w(\rho)]^p = \alpha_{\bar{\rho}}$. Therefore $g^p(\sigma, \rho) = h(\bar{\sigma}, \bar{\rho}) \alpha_{\bar{\sigma}} \alpha_{\bar{\rho}} / \alpha_{\bar{\sigma}\bar{\rho}}$ from which it follows that g^p , and hence g , takes values in $U(S_w)$.

It remains to show that g in fact takes values in $U(S_t)$. From the definitions of g and ϕ_w we obtain the equality

$$g(\sigma, \rho) = f_w(\sigma, \rho) \Pi^{e\beta(\bar{\sigma}\bar{\rho})} / \Pi^{e\beta(\bar{\sigma})} \sigma(\Pi^{e\beta(\bar{\rho})})$$

for elements σ and ρ of G_w . According to Lemma 2.2 we may write $\sigma(\Pi) = \zeta_\sigma \xi_\sigma \Pi$ where ζ_σ and ξ_σ are p^{th} and e^{th} roots of unity respectively. Since $f_w(\sigma, \rho)$ is in $U(L)$ we may write $f_w(\sigma, \rho) = \alpha_{\sigma, \rho} \pi^{\tau(\sigma, \rho)}$ where $\alpha_{\sigma, \rho}$ is in $U(S)$ and $\tau(\sigma, \rho)$ is in Z . Using the fact that $\Pi^{pe} = \pi$ one may now conclude that $pe\tau(\sigma, \rho) + e\beta(\bar{\sigma}\bar{\rho}) = e\beta(\bar{\sigma}) + e\beta(\bar{\rho})$ since $g(\sigma, \rho)$ is in $U(S_w)$. Combining these observations we obtain that $g(\sigma, \rho) = \alpha_{\sigma, \rho} / \zeta_\sigma^{e\beta(\bar{\rho})}$. Therefore $g(\sigma, \rho)$ is in $U(S_t)$, since $\alpha_{\sigma, \rho}$ is in $U(S)$ and ζ_σ is in $U(S_t)$.

PROPOSITION 2.5. *The 2-cocycle g defined above has the following properties*

- i) $g(\sigma, \rho) = 1$ for every σ in G_w and ρ in G_0
- ii) $g(\sigma, \rho)$ is a p^{th} root of unity for every σ in G_1 and ρ in G_w
- iii) $g(\sigma, \rho) = 1$ for every σ in $G_0 | G_1$ and ρ in G_w
- iv) \bar{g} is in the image of the inflation map $Z^2(G_w | G_1, U(\bar{S})) \longrightarrow Z^2(G_w, U(\bar{S}))$

where \bar{g} denotes the image of g under the natural map $Z^2(G_w, U(S_w)) \longrightarrow Z^2(G_w, U(\bar{S}))$.

Proof. We first observe that $\beta(1) = 0$ where $\beta: G \longrightarrow Z$ is the function used to define the 2-cocycle g . From the definition of h we obtain the equalities $1 = h(1, 1) = f^p(1, 1) \alpha_1 \pi^{\beta(1)} / (\alpha_1 \pi^{\beta(1)})^2$ from which it follows that $1 = 1 / \alpha_1 \pi^{\beta(1)}$, so that $\beta(1) = 0$.

Now let σ denote an element of G_w and ρ an element of G_0 , and observe that $f_w(\sigma, \rho) = f_w(\rho, \sigma) = 1$ by the definition of f_w . Then $g(\sigma, \rho) = f_w(\sigma, \rho) \phi_w(\sigma\rho) / \phi_w(\sigma) \phi_w(\rho) = \Pi^{e\beta(\bar{\sigma}\bar{\rho})} / \Pi^{e\beta(\bar{\sigma})} \sigma(\Pi^{e\beta(\bar{\rho})}) = 1$ since $\bar{\rho} = \bar{1}$ and $\beta(\bar{1}) = 0$.

When σ is in G_1 and ρ is an element of G_w we have the equalities $g(\sigma, \rho) = f_w(\sigma, \rho) \phi_w(\sigma\rho) / \phi_w(\sigma) \phi_w(\rho) = \Pi^{e\beta(\bar{\sigma}\bar{\rho})} / \Pi^{e\beta(\bar{\sigma})} \sigma(\Pi^{e\beta(\bar{\rho})}) = \Pi^{e\beta(\bar{\rho})} / \sigma(\Pi^{e\beta(\bar{\rho})})$. Therefore $g(\sigma, \rho)$ is a p^{th} root of unity since $\sigma(\Pi^{e\beta(\bar{\rho})}) = [\sigma(\Pi)]^{e\beta(\bar{\rho})} = (\zeta_\sigma \Pi)^{e\beta(\bar{\rho})}$ for some p^{th} root of unity ζ_σ since σ is in G_1 .

Next let σ denote an element of G_0/G_1 and ρ any element of G_w . Then $g(\sigma, \rho) = \Pi^{e\beta(\bar{\sigma})} / \sigma(\Pi^{e\beta(\bar{\rho})})$. Since $\sigma(\Pi) = \xi_\sigma \Pi$ for some e^{t_h} root of unity ξ_σ according to Lemma 2.2 we may conclude that $g(\sigma, \rho) = 1$.

Finally, in order to prove assertion iv) it suffices to observe that $\bar{g}(\sigma, \rho) = \bar{g}(\rho, \sigma) = \bar{1}$ for σ in G_1 and ρ in G_w according to parts i) and ii) of this proposition. One can then verify that the map $q: G_w/G_1 \times G_w/G_1 \rightarrow U(\bar{S})$ defined by $q(\bar{\sigma}, \bar{\rho}) = g(\sigma, \rho)$ is an element of $Z^2(G_w/G_1, U(\bar{S}))$ in the preimage of g .

PROPOSITION 2.6. *There exists an element σ in G_w such that $g(\tau^{n(\sigma)}, \sigma) \neq 1$.*

Proof. We first prove by contradiction that there exists an element σ of G_w for which $g(\tau, \sigma) \neq 1$. For suppose that $g(\tau, \sigma) = 1$ for each element σ of G_w . From the proof of part ii) of Prop. 2.5 we know that $g(\tau, \sigma) = \zeta^{e\beta(\bar{\sigma})}$ where ζ is the primitive p^{t_h} root of unity defined by $\tau(\Pi) = \zeta \Pi$. Since e is relatively prime to p , the assumption that $g(\tau, \sigma) = 1$ implies that $\beta(\bar{\sigma})$ is divisible by p . For each element σ of G_w we may define an integer $r(\bar{\sigma})$ by $\beta(\bar{\sigma}) = pr(\bar{\sigma})$ where $\bar{\sigma}$ denotes the image of σ under the natural map of G_w onto $G_w/G_0 = G$. We proceed to prove that $[f]$ is in the image of the natural map $H^2(G, U(S)) \rightarrow H^2(G, U(L))$ and thus contradict the assumption on the Brauer number of Σ where $\Sigma = \Delta(f, L, G)$. Return once again to the notation used in the definition of g . We may now express the 2-cocycle h of $Z^2(G, U(S))$ in the form $h(\sigma, \rho) = f^p(\sigma, \rho) \alpha_{\sigma\rho} \pi^{pr(\sigma\rho)} / \alpha_{\sigma\rho} \pi^{pr(\sigma)} \alpha_{\rho\sigma} \pi^{pr(\rho)}$. Define the map $\Psi: G \rightarrow U(L)$ by $\Psi(\sigma) = \pi^{r(\sigma)}$. Then the 2-cocycle q of $Z^2(G, U(L))$ defined by $q(\sigma, \rho) = f(\sigma, \rho) \Psi(\sigma\rho) / \Psi(\sigma) \Psi(\rho)$ is cohomologous to f and takes values in $U(S)$, so that $[f]$ is in the image of the natural map $H^2(G, U(S)) \rightarrow H^2(G, U(L))$. From this contradiction we conclude that there exists an element σ of G_w for which the p^{t_h} root of unity $g(\tau, \sigma)$ is not equal to 1.

It remains to prove that $g(\tau^{n(\sigma)}, \sigma) \neq 1$ for this element σ . We first prove inductively that $g(\tau^i, \sigma) = (g(\tau, \sigma))^i$. The assertion is trivial for $i = 1$. So we must prove that $g(\tau^{i+1}, \sigma) = (g(\tau, \sigma))^{i+1}$ under the assumption that $g(\tau^i, \sigma) = (g(\tau, \sigma))^i$. From the associativity property of g we obtain the equality $g(\tau^{i+1}, \sigma)g(\tau^i, \tau) = g(\tau^i, \tau\sigma)g^{\tau^i}(\tau, \sigma)$, so that $g(\tau^{i+1}, \sigma) = g(\tau^i, \tau\sigma)g(\tau, \sigma)$ since $g(\tau^i, \tau) = 1$ and $g(\tau, \sigma)$ is in $U(S_i)$. Now $g(\tau^i, \tau\sigma) = g(\tau^i, \sigma\tau^{n(\sigma^{-1})})$ so that we obtain once again by associativity the equality $g(\tau^i, \tau\sigma)g^{\tau^i}(\sigma, \tau^{n(\sigma^{-1})}) =$

$g(\tau^i \sigma, \tau^{n(\sigma-1)})g(\tau^i, \sigma)$ from which it follows that $g(\tau^i, \tau \sigma) = g(\tau^i, \sigma)$ according to part i) of Prop. 2.5. Combining these results we conclude that $g(\tau^{i+1}, \sigma) = g(\tau^i, \sigma)g(\tau, \sigma)$. The induction hypothesis now implies that $g(\tau^{i+1}, \sigma) = (g(\tau, \sigma))^{i+1}$. Therefore $g(\tau^{n(\sigma)}, \sigma) = (g(\tau, \sigma))^{n(\sigma)}$. Since $g(\tau, \sigma)$ is a p^{th} root of unity different from 1, and $n(\sigma)$ is relatively prime to p , we conclude at last that $g(\tau^{n(\sigma)}, \sigma) \neq 1$.

For convenience of notation we denote the crossed product $\Delta(g, S_w, G_w)$ by Δ_w and $\Delta(g, L_w, G_w)$ by Σ_w . Observe that Δ_w is an R -order in Σ_w .

We next construct an order Γ_w in Σ_w containing the crossed product Δ_w . Let θ denote the element of Σ_w defined by $\theta = \frac{1}{1-\zeta}(u_\tau - 1)$. Then Γ_w is defined to be the ring obtained by adjoining the element θ to Δ_w ; i.e. $\Gamma_w = \Delta_w[\theta]$. Most of this section is devoted to proving that Γ_w is a maximal order and to the computation of its unique maximal two-sided ideal.

We must first verify that the ring Γ_w defined above is in fact an order in Σ_w . Since Γ_w contains Δ_w , it is clear that Γ_w spans Σ_w over k . To prove that Γ_w is a finitely generated R -module, we show next that θ satisfies a polynomial equation over the subring $\Delta(1, S_w, G_1)$ of Δ_w . Observe that θ is an element of the subring $\Delta(1, L_w, G_1)$ of Σ_w .

LEMMA 2.7. *Let Z_p denote the ring of p -adic integers, and ζ a primitive p^{th} root of unity. Let v denote the element of Z_p defined by the equality $(1 - \zeta)^{p-1} = vp$. Then $v \equiv -1 \pmod{(1 - \zeta)}$.*

Proof. Since $Z_p[\zeta]$ is a tamely ramified inertial extension of Z_p of degree $p - 1$ and with prime element $1 - \zeta$, it is clear that $(1 - \zeta)^{p-1} = vp$ for some unit v of $Z_p[\zeta]$. It is a well known fact (see p. 258 of [9]) that $p = (1 - \zeta)(1 - \zeta^2) \cdots (1 - \zeta^{p-1})$. The equality $1 - \zeta^i = (1 - \zeta)(1 + \zeta + \cdots + \zeta^{i-1})$ implies that $\zeta^i \equiv 1 \pmod{(1 - \zeta)}$ for every integer i , so that $1 + \zeta + \cdots + \zeta^i \equiv i + 1 \pmod{(1 - \zeta)}$. Factoring the right hand side of the above expression for p we obtain the equality $p = (1 - \zeta)^{p-1}(1 + \zeta)(1 + \zeta + \zeta^2) \cdots (1 + \zeta + \cdots + \zeta^{p-2})$. But according to the above, $(1 + \zeta)(1 + \zeta + \zeta^2) \cdots (1 + \zeta + \cdots + \zeta^{p-2}) \equiv (p - 1)! \pmod{(1 - \zeta)}$. By Wilson's theorem (p. 118 of [8]) we know that $(p - 1)! \equiv -1 \pmod{(p)}$. Therefore $v \equiv -1 \pmod{(1 - \zeta)}$.

LEMMA 2.8. *Let C_i be the integer defined for $1 \leq i \leq \frac{p-1}{2}$ by $C_i =$*

$(-1)^i \left[\frac{(p-1)(p-2) \cdots (p-i+1)}{i!} \right] (p-2i)$. Then $C_1 + C_2 + \cdots + C_{\frac{p-1}{2}}$
 $\equiv -1 \pmod{p}$.

Proof. Since $C_i \equiv (-2)(-1)^i(p-1) \cdots (p-i+1)/(i-1)! \pmod{p}$, it suffices to observe that $(p-1)(p-2) \cdots (p-(i-1)) \equiv (-1)^{i-1}(i-1)! \pmod{p}$ in order to establish the fact that $C_i \equiv 2 \pmod{p}$ for $1 \leq i \leq (p-1)/2$. Therefore $C_1 + \cdots + C_{(p-1)/2} \equiv -1 \pmod{p}$ since there are $(p-1)/2$ summands.

LEMMA 2.9. Let $\Delta_1 = \Delta(1, S_w, G_1)$ and consider the left Δ_1 -submodule $\Delta_1(u_\tau - 1, (u_\tau - 1)\theta)$ of $\Delta(1, L_w, G_1)$ generated by the elements $u_\tau - 1$ and $(u_\tau - 1)\theta$. The element θ has the property that $\theta^p - \theta$ is in $\Delta_1(u_\tau - 1, (u_\tau - 1)\theta)$.

Proof. We consider first the case of an odd prime p . Observe that $1 - \zeta$ is in the center of $\Delta(1, L_w, G_1)$. By expanding $(u_\tau - 1)^p$ according to the binomial theorem and combining terms with the same binomial coefficient one may obtain the equality

$$\theta^p = \frac{p}{(1-\zeta)^{p-1}} \sum_i (-1)^i \left[\frac{(p-1) \cdots (p-i+1)}{i!} \right] \left[\frac{1}{1-\zeta} (u_\tau^{p-2i} - 1) u_\tau^i \right]$$

for $1 \leq i \leq (p-1)/2$. For convenience of notation let $A_i = (-1)^i(p-1) \cdots (p-i+1)/i!$. By writing $u_\tau^{p-2i} - 1$ in the form $u_\tau^{p-2i} - 1 = (u_\tau^{p-2i-1} + \cdots + 1)(u_\tau - 1)$ we have that

$$\theta^p = \frac{p}{(1-\zeta)^{p-1}} \left[\sum A_i (u_\tau^{p-i-1} + \cdots + u_\tau^i) \right] \theta.$$

We next observe that $(u_\tau^{p-i-1} + \cdots + u_\tau^i) - (p-2i)$ is in $\Delta_1(u_\tau - 1)$, since there are precisely $p-2i$ summands in the expression $u_\tau^{p-i-1} + \cdots + u_\tau^i$. This now implies that $\theta^p - \frac{p}{(1-\zeta)^{p-1}} \left[\sum A_i (p-2i) \right] \theta$ is in $\Delta_1((u_\tau - 1)\theta)$. Since $p/(1-\zeta)^{p-1} \equiv -1 \pmod{1-\zeta}$ (see Lemma 2.7) and $\sum A_i (p-2i) \equiv -1 \pmod{p}$ according to Lemma 2.8 we conclude at last that $\theta^p - \theta$ is in $\Delta_1(u_\tau - 1, (u_\tau - 1)\theta)$.

In the case $p=2$, one can verify by an easy computation that $\theta^2 - \theta = -2\theta = -(u_\tau - 1)$ and this completes the proof.

COROLLARY 2.10. The element θ of the ring Γ_w has the property that $\theta^p - \theta \equiv 0 \pmod{(1-\zeta)\Gamma_w}$.

Proof. The proof is immediate from the lemma since the element $u_\tau - 1$ is in $(1 - \zeta)\Gamma_w$.

PROPOSITION 2.11. *The ring Γ_w is generated as both a left and a right $\mathcal{A}(g, S_w, G_w)$ -module by $\{1, \theta, \dots, \theta^{p-1}\}$.*

Proof. We prove first that Γ_w is generated as a right \mathcal{A}_w -module by powers of θ . The inclusion $\mathcal{A}_w(\theta) \subset (1, \theta)\mathcal{A}_w$ may be obtained by showing that $(\alpha_\rho u_\rho)\theta$ is contained in $(1, \theta)\mathcal{A}_w$ for every element ρ of G_w and α_ρ of S_w . Using the fact that $g(\tau^{n(\rho)}, \rho) = \eta$ is a p^{th} root of unity (see Prop. 2.5) together with the fact that $(1 - \zeta^\rho) = v(1 - \zeta)$ for some element v of $U(S_i)$ one may obtain the equality

$$(\alpha_\rho u_\rho)\theta = \frac{1}{1 - \zeta} \left[u_\tau^{n(\rho)} \tau^{-n(\rho)} (\alpha_\rho / \eta v) - \alpha_\rho / v \right] u_\rho.$$

Part iv) of Lemma 2.1 implies that $\tau^{-n(\rho)}(\alpha_\rho / \eta v) \equiv \alpha_\rho / \eta v \pmod{\langle \Pi(1 - \zeta) \rangle}$. Since $\eta \equiv 1 \pmod{\langle \Pi(1 - \zeta) \rangle}$ we may write $\tau^{-n(\rho)}(\alpha_\rho / \eta v) = \alpha_\rho / v + s\Pi(1 - \zeta)$ for some element s of S_w . Writing $u_\tau^{n(\rho)} - 1$ in the form $u_\tau^{n(\rho)} - 1 = (u_\tau - 1)(u_\tau^{n(\rho)-1} + \dots + 1)$ we next obtain that

$$(\alpha_\rho u_\rho)\theta = \theta(u_\tau^{n(\rho)-1} + \dots + 1)(\alpha_\rho / v) + (u_\tau^{n(\rho)} - 1)s\Pi$$

from which it may be seen at once that $\mathcal{A}_w(\theta)$ is contained in $(1, \theta)\mathcal{A}_w$.

It now follows inductively that $\mathcal{A}_w(\theta^i)$ is contained in $(\theta^{i-1}, \theta^i)\mathcal{A}_w$ for every positive integer i . Since θ satisfies an equation of degree p over $\mathcal{A}(1, S_w, G_1)$ (see Lemma 2.9) we conclude that Γ_w is generated as a right \mathcal{A}_w -module by $\{1, \theta, \dots, \theta^{p-1}\}$.

By a similar computation one can show that Γ_w is generated as a left \mathcal{A}_w -module by $\{1, \theta, \dots, \theta^{p-1}\}$.

PROPOSITION 2.12. *The ring Γ_w is an R -order in the central simple k -algebra $\mathcal{A}(g, L_w, G_w)$.*

Proof. To prove that Γ_w is an order in $\Sigma_w = \mathcal{A}(g, L_w, G_w)$ we must show that Γ_w is a finitely generated R -module such that $k\Gamma_w = \Sigma_w$. Since $\mathcal{A}_w = \mathcal{A}(g, S_w, G_w)$ is an order in Σ_w and Γ_w contains \mathcal{A}_w , it follows that $k\Gamma_w = \Sigma_w$. And, Γ_w is a finitely generated R -module since Γ_w is a finitely generated \mathcal{A}_w -module and \mathcal{A}_w is a finitely generated R -module.

The object now is to prove that the radical of Γ_w is generated by the prime element Π of S_w . The following general observation concerning orders shall be useful, (see Lemma 1.7 of [13]).

LEMMA 2.13. *Let R denote a discrete rank one valuation ring with quotient field k , and let A_1 and A_2 be orders over R in the same central simple k -algebra. If $(\text{rad } A_2) \cap A_1$ is a two-sided ideal of A_1 , then $(\text{rad } A_2) \cap A_1$ is contained in $\text{rad } A_1$. In particular if A_1 is contained in A_2 , then $(\text{rad } A_2) \cap A_1$ is contained in $\text{rad } A_1$.*

Proof. Let π denote the prime element of R . The fact that $\pi A_2 = A_2 \pi$ together with the fact that A_2 is a finitely generated left R -module implies that π is contained in $\text{rad } A_2$ (see Lemma 1.4 of [12]). And for similar reasons π is contained in $\text{rad } A_1$.

The residue class ring $A_2/\pi A_2$ is an Artin ring, so that its radical is nilpotent. Let x be a positive integer for which $(\text{rad } A_2/\pi A_2)^x = (0)$ and observe that $(\text{rad } A_2)^x$ is contained in πA_2 . Since A_1 and A_2 are orders in the same central simple k -algebra there exists a positive integer y such that $\pi^y A_2$ is contained in A_1 (see p. 2 of [4]). Combining these observations we now obtain that $[(\text{rad } A_2) \cap A_1]^{x(y+1)}$ is contained in πA_1 . It now follows from the assumption on $(\text{rad } A_2) \cap A_1$ that its image under the natural map of A_1 onto $A_1/\pi A_1$ is a nilpotent two-sided ideal. Using the fact that $A_1/\pi A_1$ is an Artin ring we may now conclude that $(\text{rad } A_2) \cap A_1$ is contained in $\text{rad } A_1$.

If A_1 is contained in A_2 , then $(\text{rad } A_2) \cap A_1$ is a two-sided ideal of A_1 and is therefore contained in $\text{rad } A_1$ according to the above.

LEMMA 2.14. *Let Π denote the prime element of S_w . Then*

- i) $\Pi \Gamma_w = \Gamma_w \Pi$
- ii) Π is contained in $\text{rad } \Gamma_w$
- iii) $\text{rad } \Delta_w = (\Pi, u_\tau - 1) \Delta_w = \Delta_w (\Pi, u_\tau - 1)$
- iv) $\Gamma_w \Pi \cap \Delta_w = \text{rad } \Delta_w$.

Proof. Since $\Delta_w \Pi = \Pi \Delta_w$ because Δ_w is a crossed product over S_w , it suffices to show that $\theta^i \Pi$ is in $\Pi \Gamma_w$ for $1 \leq i \leq p-1$ in order to obtain the inclusion $\Gamma_w \Pi \subset \Pi \Gamma_w$. Now $\theta \Pi = \Pi \theta + \frac{\Pi}{1-\zeta} \left[\frac{\tau(\Pi)}{\Pi} - 1 \right] u_\tau$ so that $\theta \Pi$

is in $\Pi\Gamma_w$ because $\frac{1}{1-\zeta} \left[\frac{\tau(\Pi)}{\Pi} - 1 \right]$ is in S_ζ . It follows inductively that $\theta^i\Pi$ is in $\Pi\Gamma_w$ for $1 \leq i \leq p-1$ so that $\Gamma_w\Pi$ is contained in $\Pi\Gamma_w$. The opposite inclusion may be obtained by a similar computation, and therefore $\Gamma_w\Pi = \Pi\Gamma_w$.

The fact that $\Pi\Gamma_w = \Gamma_w\Pi$ implies that Π is in $\text{rad } \Gamma_w$ according to Lemma 1.4 of [12].

In order to prove iii) we first observe that the radical of the subring $\mathcal{A}_1 = \mathcal{A}(1, S_w, G_1)$ of \mathcal{A}_w is generated as a right ideal by Π and $u_\tau - 1$ where τ denotes as usual a generator of G_1 . For, the \bar{S} -algebra isomorphism $\mathcal{A}(1, \bar{S}, G_1) \approx \bar{S}[X]/(X^p - 1)$ induced by defining $u_\tau \rightarrow X$ implies that the radical of the commutative ring $\mathcal{A}(1, \bar{S}, G_1)$ is generated by $u_\tau - 1$. The natural isomorphism $\mathcal{A}_1 / \Pi\mathcal{A}_1 \approx \mathcal{A}(1, \bar{S}, G_1)$ together with the fact that Π is in $\text{rad } \mathcal{A}_1$ implies that $\text{rad } \mathcal{A}_1 = (\Pi, u_\tau - 1)\mathcal{A}_1$. Now Props. 3.1 and 3.4 of [12] together imply that $\text{rad } \mathcal{A}_w = (\text{rad } \mathcal{A}_1)\mathcal{A}_w$. Combining the above observations we conclude that $\text{rad } \mathcal{A}_w = (\Pi, u_\tau - 1)\mathcal{A}_w$.

Now we may prove iv). The equality $u_\tau - 1 = \theta(1 - \zeta)$ implies that $u_\tau - 1$ is in $\Gamma_w\Pi \cap \mathcal{A}_w$ since $1 - \zeta$ is in S_w . Since $\text{rad } \mathcal{A}_w = (\Pi, u_\tau - 1)\mathcal{A}_w$ according to part iii), we may conclude that $\text{rad } \mathcal{A}_w$ is contained in $\Gamma_w\Pi \cap \mathcal{A}_w$. On the other hand, the intersection $\Gamma_w\Pi \cap \mathcal{A}_w$ is contained in $\text{rad } \mathcal{A}_w$ by Lemma 2.13. This completes the proof of statement iv).

Since $\Gamma_w\Pi$ is a two-sided ideal of Γ_w we may form the residue class ring $\Gamma_w / \Gamma_w\Pi$, which shall henceforth be denoted by $\bar{\Gamma}_w$. According to Prop. 2.5 we may consider an element of $Z^2(G_w / G_1, U(\bar{S}))$ in the preimage of \bar{g} under the inflation map $Z^2(G_w / G_1, U(\bar{S})) \rightarrow Z^2(G_w, U(\bar{S}))$ which for convenience of notation shall also be denoted by \bar{g} . The following isomorphism shall be useful in establishing the semi-simplicity of $\bar{\Gamma}_w$.

LEMMA 2.15. *The residue class ring $\bar{\Gamma}_w$ is \bar{R} -algebra isomorphic to $\mathcal{A}(\bar{g}, \bar{S}, G_w / G_1)[\bar{\theta}]$ in a natural way, where $\bar{\theta}$ denotes the residue class of θ modulo $\Gamma_w\Pi$.*

Proof. Using the fact that \bar{g} is in the image of the inflation map $Z^2(G_w / G_1, U(\bar{S})) \rightarrow Z^2(G_w, U(\bar{S}))$ we may observe that the crossed product $\mathcal{A}(\bar{g}, \bar{S}, G_w / G_1)$ is isomorphic to $\mathcal{A}_w / (\Pi, u_\tau - 1)\mathcal{A}_w$ in a natural way. Parts iii) and iv) of Lemma 2.14 imply that $\Gamma_w\Pi \cap \mathcal{A}_w = (\Pi, u_\tau - 1)\mathcal{A}_w$, so that

there is a natural injection of $\mathcal{A}_w / (\Pi, u_\tau - 1)\mathcal{A}_w$ into $\bar{\Gamma}_w$. By identifying $\mathcal{A}(\bar{g}, \bar{S}, G_w / G_1)$ with its image under the maps

$$\mathcal{A}(\bar{g}, \bar{S}, G_w / G_1) \longrightarrow \mathcal{A}_w / (\Pi, u_\tau - 1)\mathcal{A}_w \longrightarrow \bar{\Gamma}_w$$

we may conclude that $\bar{\Gamma}_w$ is R -algebra isomorphic to $\mathcal{A}(\bar{g}, \bar{S}, G_w / G_1)[\bar{\theta}]$ since Γ_w is generated as a left \mathcal{A}_w -module by $\{1, \theta, \dots, \theta^{p-1}\}$.

LEMMA 2.16 A. *The intersection $(\Pi\Gamma_w) \cap \mathcal{A}(g, S_w, G_0)[\theta]$ is contained in $\Pi\mathcal{A}(g, S_w, G_0)[\theta]$.*

Proof. Consider an element δ of $(\Pi\Gamma_w) \cap \mathcal{A}(g, S_w, G_0)[\theta]$. Since δ is in $\Pi\Gamma_w$ we may write δ in the form $\delta = \Pi \sum \delta_i \theta^i$ with the δ_i in $\mathcal{A}(g, S_w, G_w)$ according to Prop. 2.11.

We now use some properties of crossed products to show that each δ_i is in $\mathcal{A}(g, L_w, G_0)$. Since $\mathcal{A}(g, S_w, G_0)[\theta]$ is contained in $\mathcal{A}(g, L_w, G_0)$ it follows that $\sum \delta_i \theta^i$ is in $\mathcal{A}(g, L_w, G_0)$. Consider a disjoint (left) coset decomposition $G_w = \cup \omega_j G_0$ of G_w with respect to the subgroup G_0 , with $\omega_1 = 1$. According to Lemma 2.5 of [12], $\mathcal{A}(g, L_w, G_w)$ is a free right $\mathcal{A}(g, L_w, G_0)$ -module with free basis $\{u_{\omega_j}\}$. Since each δ_i is in $\mathcal{A}(g, S_w, G_w)$ we may therefore write δ_i uniquely in the form $\delta_i = \sum u_{\omega_j} \delta_j^{(i)}$ where the $\delta_j^{(i)}$ are elements of $\mathcal{A}(g, L_w, G_0)$. The equality $\sum \delta_i \theta^i \equiv \sum_j u_{\omega_j} (\sum \delta_j^{(i)} \theta^i)$ now implies that $j = 1$ because $\sum \delta_i \theta^i$ is in $\mathcal{A}(g, L_w, G_0)$. Therefore $\delta_i = \delta_1^{(i)}$ for each i , and so each δ_i is in $\mathcal{A}(g, L_w, G_0)$.

Using the fact that $\mathcal{A}(g, L_w, G_w)$ is a free (left) L_w -module with free basis $\{u_\sigma\}$ for all σ in G_w , it is easy to see that the intersection $\mathcal{A}(g, S_w, G_w) \cap \mathcal{A}(g, L_w, G_0)$ is contained in $\mathcal{A}(g, S_w, G_0)$. Therefore each δ_i is in $\mathcal{A}(g, S_w, G_0)$ and hence δ is in $\Pi\mathcal{A}(g, S_w, G_0)[\theta]$.

LEMMA 2.16 B. *The subring $\mathcal{A}(1, \bar{S}, G_0 / G_1)[\bar{\theta}]$ of $\bar{\Gamma}_w$ is a commutative semi-simple ring.*

Proof. We prove first that the ring $\mathcal{A}(1, \bar{S}, G_0 / G_1)[\bar{\theta}]$ is commutative. Now the crossed product $\mathcal{A}(1, \bar{S}, G_0 / G_1)$ is commutative because G_0 / G_1 is a cyclic group with trivial action on \bar{S} . Let ρ denote a generator of G_0 / G_1 . Since $\bar{\theta}$ commutes with the elements of \bar{S} it suffices to show that u_ρ commutes with $\bar{\theta}$ in order to prove that $\mathcal{A}(1, \bar{S}, G_0 / G_1)[\bar{\theta}]$ is a commutative ring. Let i be the integer defined by $\rho(\zeta) = \zeta^i$. Since $i = n(\rho)$ according

to Lemma 2.3, we obtain the congruence $u_\rho \theta \equiv \frac{1}{1-\zeta^i} (u_\tau^i - 1) u_\rho \pmod{\Pi\Gamma_w}$. The equalities $1 - \zeta^i = (1 - \zeta)(1 + \zeta + \dots + \zeta^{i-1})$ and $u_\tau^i - 1 = (u_\tau - 1)(u_\tau^{i-1} + \dots + 1)$ in Γ_w imply that $1 - \zeta^i \equiv i(1 - \zeta) \pmod{\Pi\Gamma_w}$ and $u_\tau^i - 1 \equiv i(u_\tau - 1) \pmod{\Pi\Gamma_w}$ since $\zeta \equiv 1 \pmod{\Pi\Gamma_w}$ and $u_\tau \equiv 1 \pmod{\Pi\Gamma_w}$. These congruences imply that $u_\rho \bar{\theta} = \bar{\theta} u_\rho$ in $\bar{\Gamma}_w$ and we conclude therefore that $\mathcal{A}(1, \bar{S}, G_0 / G_1)[\bar{\theta}]$ is a commutative subring of $\bar{\Gamma}_w$.

In order to prove semi-simplicity, we first prove that $\mathcal{A}(1, \bar{S}, G_0 / G_1)[\bar{\theta}]$ is a free (left) $\mathcal{A}(1, \bar{S}, G_0 / G_1)$ -module with free basis $\{1, \bar{\theta}, \dots, \bar{\theta}^{p-1}\}$. The proof is by contradiction. So suppose that there exist elements $\bar{\delta}_i$ of $\mathcal{A}(1, \bar{S}, G_0 / G_1)$ such that $\sum_{i=0}^x \bar{\delta}_i \bar{\theta}^i = \bar{0}$ with $\bar{\delta}_x \neq \bar{0}$ and $x \leq p-1$. Then $\sum_{i=0}^x \bar{\delta}_i \bar{\theta}^i \bar{\theta}^{(p-1-x)} = \bar{0}$ so that we may consider an expression $\sum_{i=0}^{p-1} \bar{\delta}_i \bar{\theta}^i = \bar{0}$ where $\bar{\delta}_{p-1} \neq \bar{0}$. The method of proof shall be to contradict the assumption that $\bar{\delta}_{p-1}$ is non-zero. It is clear that we may choose representatives δ_i in Γ_w of the residue classes $\bar{\delta}_i$ such that each δ_i is in $\mathcal{A}(g, S_w, G_0)$. Now the equality $\sum \bar{\delta}_i \bar{\theta}^i = \bar{0}$ implies that $\sum \delta_i \theta^i$ is in $(\Pi\Gamma_w) \cap \mathcal{A}(g, S_w, G_0)[\theta]$, and therefore $\sum \delta_i \theta^i$ is in $\Pi\mathcal{A}(g, S_w, G_0)[\theta]$ according to Lemma 2.16 A. Since $\mathcal{A}(g, S_w, G_0)[\theta]$ is generated as a left $\mathcal{A}(g, S_w, G_0)$ -module by $\{1, \theta, \dots, \theta^{p-1}\}$, it follows that $(1 - \zeta)^{p-1} \sum \delta_i \theta^i$ is in $\Pi\mathcal{A}(g, S_w, G_0)$. Finally, the fact that $(1 - \zeta)^{p-1} \sum_{i=0}^{p-2} \delta_i \theta^i$ is in $\Pi\mathcal{A}(g, S_w, G_w)$ implies that $(1 - \zeta)^{p-1} \delta_{p-1} \theta^{p-1} = \delta_{p-1} (u_\tau - 1)^{p-1}$ is in $\Pi\mathcal{A}(g, S_w, G_0)$. It remains to show that δ_{p-1} is in $\Pi\Gamma_w$. Consider a disjoint (left) coset decomposition $G_0 = \cup \omega_i G_1$ of G_0 with respect to the subgroup G_1 , and recall that $\mathcal{A}(g, S_w, G_0)$ is a free right $\mathcal{A}(1, S_w, G_1)$ -module with free basis $\{u_{\omega_i}\}$. We may therefore consider a (unique) expression for δ_{p-1} of the form $\delta_{p-1} = \sum_i u_{\omega_i} \gamma_i$ with the γ_i in $\mathcal{A}(1, S_w, G_1)$. The equality $\delta_{p-1} (u_\tau - 1)^{p-1} = \sum u_{\omega_i} \gamma_i (u_\tau - 1)^{p-1}$ together with the fact that $\delta_{p-1} (u_\tau - 1)^{p-1}$ is in $\Pi\mathcal{A}(g, S_w, G_0)$ now implies that $\gamma_i (u_\tau - 1)^{p-1}$ is in $\Pi\mathcal{A}(1, S_w, G_1)$ for each i . The radical of $\mathcal{A}(1, S_w, G_1)$ is generated as a left ideal by Π and $u_\tau - 1$, and the residue class ring $\mathcal{A}(1, S_w, G_1) / \text{rad } \mathcal{A}(1, S_w, G_1)$ is isomorphic to \bar{S} . We may consider therefore for each γ_i an element s_i of S and elements α_i and β_i of $\mathcal{A}(1, S_w, G_1)$ such that $\gamma_i = s_i + \alpha_i \Pi + \beta_i (u_\tau - 1)$. Then $\gamma_i (u_\tau - 1)^{p-1} = s_i (u_\tau - 1)^{p-1} + \alpha_i \Pi (u_\tau - 1)^{p-1} + \beta_i (u_\tau - 1)^p$. Since $(u_\tau - 1)^p$ and $\gamma_i (u_\tau - 1)^{p-1}$ are in $\Pi\mathcal{A}(1, S_w, G_1)$ it now follows that $s_i (u_\tau - 1)^{p-1}$ is in $\Pi\mathcal{A}(1, S_w, G_1)$. Using the fact that $\mathcal{A}(1, S_w, G_1)$ is a free (left) S_w -module

with free basis $\{u_{\tau^i}\}$ for $0 \leq i \leq p - 1$ we may conclude that s_i is in ΠS for each i , and therefore each r_i is in $\text{rad } \mathcal{A}(1, S_w, G_1)$. The element $u_{\tau} - 1$ is in $\Pi \mathcal{A}(g, S_w, G_1)[\theta]$, so we obtain at last that δ_{p-1} is in $\Pi \Gamma_w$. Thus we have established that $\mathcal{A}(1, \bar{S}, G_0 / G_1)[\bar{\theta}]$ is a free left $\mathcal{A}(1, \bar{S}, G_0 / G_1)$ -module with free basis $\{1, \bar{\theta}, \dots, \bar{\theta}^{p-1}\}$.

Consider the polynomial ring $\mathcal{A}(1, \bar{S}, G_0 / G_1)[Y]$ and form the residue class ring $\mathcal{A}(1, \bar{S}, G_0 / G_1)[Y] / (Y^p - Y)$. Define a map $\varphi: \mathcal{A}(1, \bar{S}, G_0 / G_1)[\bar{\theta}] \rightarrow \mathcal{A}(1, \bar{S}, G_0 / G_1)[Y] / (Y^p - Y)$ in the following way. An element of $\mathcal{A}(1, \bar{S}, G_0 / G_1)[\bar{\theta}]$ has a unique expression in the form $\sum_{i=0}^{p-1} \bar{\delta}_i \bar{\theta}^i$ with the $\bar{\delta}_i$ in $\mathcal{A}(1, \bar{S}, G_0 / G_1)$ according to the above. Define $\varphi(\sum \bar{\delta}_i \bar{\theta}^i) = \sum \bar{\delta}_i Y^i + (Y^p - Y)$. Cor. 2.10 implies that $\bar{\theta}^p = \bar{\theta}$, from which it follows that φ is a monomorphism. It is easy to verify that φ is in fact an R -algebra isomorphism.

Now we may establish the semi-simplicity of $\mathcal{A}(1, \bar{S}, G_0 / G_1)[\bar{\theta}]$. Since the order of G_0 / G_1 is relatively prime to the characteristic of \bar{S} , the group ring $\mathcal{A}(1, \bar{S}, G_0 / G_1)$ is semi-simple. The polynomial $Y^p - Y$ factors into linear factors with no repeated roots in $\bar{S}[Y]$, namely $Y^p - Y = Y \prod_{i=1}^{p-1} (Y - \xi^i)$ where ξ is a primitive $(p - 1)^{st}$ root of unity in \bar{S} whose existence is guaranteed by the fact that \bar{S} has characteristic p . For convenience of notation let $h_0(Y) = Y$ and $h_i(Y) = Y - \xi^i$ for $1 \leq i \leq p - 1$. By the Chinese Remainder Theorem we have that the ring $\mathcal{A}(1, \bar{S}, G_0 / G_1)[Y] / (Y^p - Y)$ is isomorphic to $\bigoplus_{i=0}^{p-1} \mathcal{A}(1, \bar{S}, G_0 / G_1)[Y] / (h_i(Y))$. Each polynomial $h_i(Y)$ is linear so that each summand is isomorphic to $\mathcal{A}(1, \bar{S}, G_0 / G_1)$. Therefore $\mathcal{A}(1, \bar{S}, G_0 / G_1)[Y] / (Y^p - Y)$ is isomorphic to a direct sum of semi-simple rings and is therefore itself semi-simple. The fact that $\mathcal{A}(1, \bar{S}, G_0 / G_1)[\bar{\theta}]$ is isomorphic to $\mathcal{A}(1, \bar{S}, G_0 / G_1)[Y] / (Y^p - Y)$ now implies that $\mathcal{A}(1, \bar{S}, G_0 / G_1)[\bar{\theta}]$ is semi-simple.

LEMMA 2.16 C. *The residue class ring $\bar{\Gamma}_w$ is a finitely generated free left $\mathcal{A}(1, \bar{S}, G_0 / G_1)[\bar{\theta}]$ -module with free basis $\{u_{\sigma_i}\}$ where $G_w / G_1 = \cup (G_0 / G_1)\sigma_i$ is a disjoint right coset decomposition of G_w / G_1 with respect to the subgroup G_0 / G_1 .*

Proof. It follows at once from Prop. 2.11 that $\bar{\Gamma}_w$ is generated as a right $\mathcal{A}(\bar{g}, \bar{S}, G_w / G_1)$ -module by $\{1, \bar{\theta}, \dots, \bar{\theta}^{p-1}\}$. Therefore an element λ of $\bar{\Gamma}_w$ can be written in the form $\lambda = \sum \bar{\theta}^i \delta_i$ with the δ_i in $\mathcal{A}(\bar{g}, \bar{S}, G_w / G_1)$. Consider the elements σ_i defined in the statement of the lemma. The

crossed product $\mathcal{A}(\bar{\theta}, \bar{S}, G_w / G_1)$ is generated as a free (left) $\mathcal{A}(1, \bar{S}, G_0 / G_1)$ -module by the $\{u_{\sigma_i}\}$ (see Lemma 2.5 of [12]). Therefore each δ_i can be written in the form $\delta_i = \sum_j r_j^{(\epsilon_i)} u_{\sigma_j}$, with the $r_j^{(\epsilon_i)}$ in $\mathcal{A}(1, \bar{S}, G_0 / G_1)$. Since $\lambda = \sum_i \bar{\theta}^i \sum_j r_j^{(\epsilon_i)} u_{\sigma_j} = \sum_j (\sum_i \bar{\theta}^i r_j^{(\epsilon_i)}) u_{\sigma_j}$, we may conclude that the $\{u_{\sigma_i}\}$ generate $\bar{\Gamma}_w$ as a left $\mathcal{A}(1, \bar{S}, G_0 / G_1)[\bar{\theta}]$ -module.

It remains to show that the $\{u_{\sigma_i}\}$ are linearly independent over $\mathcal{A}(1, \bar{S}, G_0 / G_1)[\bar{\theta}]$. So suppose that $\sum_{i=1}^t A_i u_{\sigma_i} = 0$ for elements A_i of $\mathcal{A}(1, \bar{S}, G_0 / G_1)[\bar{\theta}]$. If the A_i are not all zero, define $t(\{A_i\})$ to be the largest integer i such that $A_i \neq 0$; if $A_i = 0$ for each i , define $t(\{A_i\}) = 0$. The proof is by induction on $t(\{A_i\})$. If $t(\{A_i\}) = 1$, then $A_1 = A_1 u_{\sigma_1} (u_{\sigma_1})^{-1} = 0$ contradicting the assumption that $t(\{A_i\}) = 1$. For the inductive step consider a set of elements $\{A_i\}$ of $\mathcal{A}(1, \bar{S}, G_0 / G_1)[\bar{\theta}]$ such that $\sum A_i u_{\sigma_i} = 0$ and $t(\{A_i\}) = t$. The induction hypothesis states that if $\{B_i\}$ is a set of elements of $\mathcal{A}(1, \bar{S}, G_0 / G_1)[\bar{\theta}]$ such that $\sum B_i u_{\sigma_i} = 0$ and $t(\{B_i\}) < t$, then $B_i = 0$ for each i . Observe that G_w / G_0 is the Galois group of \bar{S} over \bar{K} and consider an element α of \bar{S} such that $\bar{S} = \bar{K}(\alpha)$. The assumption that $\sum A_i u_{\sigma_i} = 0$ implies that $0 = \alpha(\sum A_i u_{\sigma_i}) - (\sum A_i u_{\sigma_i}) \sigma_t^{-1}(\alpha) = \sum (\alpha - \sigma_t \sigma_t^{-1}(\alpha)) A_i u_{\sigma_i}$. Since $\sigma_t \sigma_t^{-1}(\alpha) = \alpha$ if and only if $i = t$, we have that $t(\{(\alpha - \sigma_t \sigma_t^{-1}(\alpha)) A_i\}) < t$. Using the induction hypothesis we may now conclude that $A_i = 0$ for $1 \leq i \leq t-1$. Therefore $A_t u_{\sigma_t} = 0$ since $\sum A_i u_{\sigma_i} = 0$ and we obtain that $A_t = A_t u_{\sigma_t} (u_{\sigma_t})^{-1} = 0$ contradicting the assumption that $A_t \neq 0$. We have established therefore that an equality $\sum A_i u_{\sigma_i} = 0$ with the A_i in $\mathcal{A}(1, \bar{S}, G_0 / G_1)[\bar{\theta}]$ implies that $A_i = 0$ for each i .

The semi-simplicity of $\bar{\Gamma}_w$ now follows from that of its subring $\mathcal{A}(1, \bar{S}, G_0 / G_1)[\bar{\theta}]$.

LEMMA 2.17. *The ring $\bar{\Gamma}_w$ is a semi-simple ring.*

Proof. For convenience of notation we shall denote the subring $\mathcal{A}(1, \bar{S}, G_0 / G_1)[\bar{\theta}]$ of $\bar{\Gamma}_w$ by $\bar{\Gamma}_0$ throughout the proof of this lemma. We shall make use of the fact that $(\text{rad } \bar{\Gamma}_w) \cap \bar{\Gamma}_0$ is contained in $\text{rad } \bar{\Gamma}_0$ (see Lemma 2.4 of [12]).

The first step is to prove that $\text{rad } \bar{\Gamma}_w = (\text{rad } \bar{\Gamma}_0) \bar{\Gamma}_w$. Consider a disjoint right coset decomposition $G_w / G_1 = \cup (G_0 / G_1) \sigma_i$ of G_w / G_1 with respect to the subgroup G_0 / G_1 . According to Lemma 2.16 C, an element λ of $\bar{\Gamma}_w$

can be written uniquely in the form $\lambda = \sum_{i=1}^t \lambda_i u_{\sigma_i}$, where the λ_i are in $\bar{\Gamma}_0$. For $\lambda \neq 0$, define $t(\lambda)$ to be the largest integer i for which $\lambda_i \neq 0$, and define $t(0) = 0$. The proof is by induction on $t(\lambda)$. If λ is an element of $\text{rad } \bar{\Gamma}_w$ for which $t(\lambda) = 1$, then λ is of the form $\lambda = \lambda_1 u_{\sigma_1}$ with λ_1 in $\bar{\Gamma}_0$ so that $\lambda_1 = \lambda(u_{\sigma_1})^{-1}$ is in $(\text{rad } \bar{\Gamma}_w) \cap \bar{\Gamma}_0$ and hence in $\text{rad } \bar{\Gamma}_0$ according to the remark at the beginning of the proof. Therefore λ is in $(\text{rad } \bar{\Gamma}_0) \bar{\Gamma}_w$. For the inductive step we assume that if $r = \sum r_i u_{\sigma_i}$ is an element of $\text{rad } \bar{\Gamma}_w$ for which $t(r) < t$ then each element r_i of $\bar{\Gamma}_0$ is in $\text{rad } \bar{\Gamma}_0$. Now let $\lambda = \sum \lambda_i u_{\sigma_i}$ be an element of $\text{rad } \bar{\Gamma}_w$ such that $t(\lambda) = t$. Recall that G_w / G_0 is the Galois group of \bar{S} over \bar{R} , and consider an element α of \bar{S} for which $\bar{S} = \bar{R}(\alpha)$. In order to apply the induction hypothesis we form the element $r = \alpha \lambda - \lambda \sigma_t^{-1}(\alpha)$ and observe that $r = \sum (\alpha - \sigma_i \sigma_i^{-1}(\alpha)) \lambda_i u_{\sigma_i}$ is in $\text{rad } \bar{\Gamma}_w$. Since $\sigma_i \sigma_i^{-1}(\alpha) = \alpha$ if and only if $i = t$, we may conclude that $r = \sum_{i=1}^{t-1} (\alpha - \sigma_i \sigma_i^{-1}(\alpha)) \lambda_i u_{\sigma_i}$ is an element of $\text{rad } \bar{\Gamma}_w$ for which $t(r) < t$. Since $\alpha - \sigma_i \sigma_i^{-1}(\alpha) = 0$ for $1 \leq i \leq t-1$, the induction hypothesis now implies that λ_i is in $\text{rad } \bar{\Gamma}_0$ for $1 \leq i \leq t-1$. Therefore $\lambda_i u_{\sigma_i}$ is in $\text{rad } \bar{\Gamma}_w$, so that $\lambda_i = \lambda(u_{\sigma_i})^{-1}$ is in $(\text{rad } \bar{\Gamma}_w) \cap \bar{\Gamma}_0$ and therefore in $\text{rad } \bar{\Gamma}_0$. We have now established that $\text{rad } \bar{\Gamma}_w$ is contained in $(\text{rad } \bar{\Gamma}_0) \bar{\Gamma}_w$.

The ring $\bar{\Gamma}_0$ is semi-simple according to Lemma 2.16 B. Therefore $\text{rad } \bar{\Gamma}_0 = (0)$ and we obtain that $\text{rad } \bar{\Gamma}_w = (\text{rad } \bar{\Gamma}_0) \bar{\Gamma}_w = (0)$. Since $\bar{\Gamma}_w$ is an Artin ring with zero radical we conclude that $\bar{\Gamma}_w$ is semi-simple.

PROPOSITION 2.18. *The ring Γ_w is an hereditary order with radical $\Gamma_w \Pi$.*

Proof. The fact that $\Gamma_w \Pi$ is contained in $\text{rad } \Gamma_w$ (Lemma 2.14) together with the fact that $\Gamma_w / \Gamma_w \Pi$ is semi-simple (Lemma 2.17) implies that $\text{rad } \Gamma_w = \Gamma_w \Pi$. It is easy to verify using the definition of crossed product that $\Gamma_w \Pi$ is a free left Γ_w -module. Therefore Γ_w is an hereditary order according to the Corollary to Theorem 2.2 of [4].

In order to prove that Γ_w is a maximal order it remains to show that $\Gamma_w \Pi$ is the unique maximal two-sided ideal of Γ_w , i.e. that $\bar{\Gamma}_w$ is a simple ring. Since $\bar{\Gamma}_w$ is a semi-simple ring (Lemma 2.17), its number of simple components is equal to the number of primitive orthogonal idempotents required to generate its center. We shall prove that the idempotents in the center of $\bar{\Gamma}_w$ are contained in \bar{R} and thus conclude that $\bar{\Gamma}_w$ is simple.

LEMMA 2.19. *The center of $\bar{\Gamma}_w$ is contained in the subring $\bar{S}[\bar{\theta}]$.*

Proof. Once again we denote $\mathcal{A}(1, \bar{S}, G_0/G_1)[\bar{\theta}]$ by $\bar{\Gamma}_0$. We show first that the center $C(\bar{\Gamma}_w)$ of $\bar{\Gamma}_w$ is contained in the subring $\bar{\Gamma}_0$ of $\bar{\Gamma}_w$. Consider a disjoint right coset decomposition $G_w/G_1 = \cup (G_0/G_1)\sigma_i$ of G_w/G_1 with respect to the subgroup G_0/G_1 , with $\sigma_1 = 1$. Let δ denote a non-zero element of $C(\bar{\Gamma}_w)$. According to Lemma 2.16 C δ may be written uniquely in the form $\delta = \sum_{i=1}^t \delta_i u_{\sigma_i}$ with the δ_i in $\bar{\Gamma}_0$ and $\delta_i \neq 0$. Let α denote an element of \bar{S} for which $\bar{S} = \bar{R}(\alpha)$. Since δ is in $C(\bar{\Gamma}_w)$ we must have $\alpha\delta = \delta\alpha$ so that

$$\begin{aligned} & \alpha\delta_1 + (\alpha\delta_2)u_{\sigma_2} + \cdots + (\alpha\delta_t)u_{\sigma_t} \\ &= \alpha\delta_1 + (\sigma_2(\alpha)\delta_2)u_{\sigma_2} + \cdots + (\sigma_t(\alpha)\delta_t)u_{\sigma_t}. \end{aligned}$$

Therefore $\alpha\delta_i = \sigma_i(\alpha)\delta_i$ for $1 \leq i \leq t$ because $\bar{\Gamma}_w$ is a free left $\bar{\Gamma}_0$ -module with free basis $\{u_{\sigma_i}\}$ (see Lemma 2.16 C). Write each element δ_i of $\bar{\Gamma}_0$ in the form $\delta_i = \sum \lambda_j^{(i)} \bar{\theta}^j$ with the $\lambda_j^{(i)}$ in $\mathcal{A}(1, \bar{S}, G_0/G_1)$. The equalities $\alpha\delta_i = \sigma_i(\alpha)\delta_i$ imply that $\sum_j \alpha \lambda_j^{(i)} \bar{\theta}^j = \sum_j \sigma_i(\alpha) \lambda_j^{(i)} \bar{\theta}^j$ for each i . Using the fact that $\bar{\Gamma}_0$ is a free left $\mathcal{A}(1, \bar{S}, G_0/G_1)$ -module with free basis $\{1, \bar{\theta}, \dots, \bar{\theta}^{p-1}\}$ (see the proof of Lemma 2.16 B) we conclude that $\alpha \lambda_j^{(i)} = \sigma_i(\alpha) \lambda_j^{(i)}$ for every i and j . From the definition of crossed product it now follows that $\alpha = \sigma_i(\alpha)$ for each i . Since $\sigma_i(\alpha) = \alpha$ if and only if $i = 1$, we obtain finally that $t = 1$ and so δ is in $\bar{\Gamma}_0$.

It remains to prove that $\bar{\Gamma}_0 \cap C(\bar{\Gamma}_w)$ is contained in $\bar{S}[\bar{\theta}]$. Consider an element δ of $\bar{\Gamma}_0 \cap C(\bar{\Gamma}_w)$ and write δ in the form $\delta = \sum \lambda_i \bar{\theta}^i$ with the λ_i in $\mathcal{A}(1, \bar{S}, G_0/G_1)$. Since δ is in $C(\bar{\Gamma}_w)$ we must have that $u_\tau \delta = \delta u_\tau$. Since u_τ commutes with $\bar{\theta}$ we now obtain the equality $\sum_i u_\tau \lambda_i \bar{\theta}^i = \sum_i \lambda_i u_\tau \bar{\theta}^i$. The fact that $\bar{\Gamma}_0$ is a free left $\mathcal{A}(1, \bar{S}, G_0/G_1)$ -module with free basis $\{1, \bar{\theta}, \dots, \bar{\theta}^{p-1}\}$ (Lemma 2.16 B) implies that $u_\tau \lambda_i = \lambda_i u_\tau$ for each i . Write each element λ_i of $\mathcal{A}(1, \bar{S}, G_0/G_1)$ in the form $\lambda_i = \sum_\rho \alpha_\rho^{(i)} u_\rho$ with the ρ in G_0/G_1 and the $\alpha_\rho^{(i)}$ in \bar{S} . Then the equality $u_\tau \lambda_i = \lambda_i u_\tau$ implies that $\sum_\rho \alpha_\rho^{(i)} u_\tau u_\rho = \sum_\rho \alpha_\rho^{(i)} u_\tau u_\rho$ where $n(\rho)$ is the integer defined modulo (p) by $\rho \tau \rho^{-1} = \tau^{n(\rho)}$. According to Lemma 2.3 $n(\rho) = 1$ if and only if $\rho = 1$. Therefore $\tau \rho = \tau^{n(\sigma)} \sigma$ for elements ρ and σ of G_0/G_1 if and only if $\rho = 1$ and $\sigma = 1$, from which it follows that each λ_i is in \bar{S} , and hence that δ is in $\bar{S}[\bar{\theta}]$.

LEMMA 2.20. *The idempotents in the center of $\bar{\Gamma}_w$ are contained in \bar{R} .*

Proof. We first observe that the idempotents of $\bar{S}[\bar{\theta}]$ are present in $\bar{R}[\bar{\theta}]$. In the proof of Lemma 2.16 B it was shown that the ring $\mathcal{A}(1, \bar{S}, G_0/G_1)[\bar{\theta}]$ is a free left $\mathcal{A}(1, \bar{S}, G_0/G_1)$ -module with free basis $\{1, \bar{\theta}, \dots, \bar{\theta}^{p-1}\}$. From this it follows at once that $\bar{S}[\bar{\theta}]$ is a free \bar{S} -module with free basis $\{1, \bar{\theta}, \dots, \bar{\theta}^{p-1}\}$ and that $\bar{R}[\bar{\theta}]$ is a free \bar{R} -module with free basis $\{1, \bar{\theta}, \dots, \bar{\theta}^{p-1}\}$. These observations imply that $\bar{S}[\bar{\theta}]$ is isomorphic to $\bar{S}[Y]/(Y^p - Y)$ and that $\bar{R}[\bar{\theta}]$ is isomorphic to $\bar{R}[Y]/(Y^p - Y)$. Recall from Lemma 2.16 B that $Y^p - Y = \prod_{i=0}^{p-1} h_i(Y)$ is a factorization of $Y^p - Y$ into linear factors in $\bar{R}[Y]$ where $h_0(Y) = Y$ and $h_i(Y) = Y - \xi^i$ for $1 \leq i \leq p-1$, and ξ denotes a primitive $(p-1)^{st}$ root of unity in \bar{R} . By the Chinese Remainder Theorem we obtain the isomorphisms $\bar{R}[Y]/(Y^p - Y) \approx \bigoplus \bar{R}[Y]/(h_i(Y))$ and $\bar{S}[Y]/(Y^p - Y) \approx \bigoplus \bar{S}[Y]/(h_i(Y))$. The natural map of $\bigoplus \bar{R}[Y]/(h_i(Y))$ into $\bigoplus \bar{S}[Y]/(h_i(Y))$ maps the set of primitive orthogonal idempotents of $\bigoplus \bar{R}[Y]/(h_i(Y))$ into such a system for $\bigoplus \bar{S}[Y]/(h_i(Y))$. We conclude therefore that the idempotents of $\bar{S}[\bar{\theta}]$ are already present in $\bar{R}[\bar{\theta}]$.

In order to prove the lemma it suffices to show that the intersection $C(\bar{\Gamma}_w) \cap \bar{R}[\bar{\theta}]$ is contained in \bar{R} since $C(\bar{\Gamma}_w)$ is contained in $\bar{S}[\bar{\theta}]$ according to Lemma 2.19. Let λ denote a non-zero element of $C(\bar{\Gamma}_w) \cap \bar{R}[\bar{\theta}]$ and express λ in the form $\lambda = \sum_{i=0}^t r_i \bar{\theta}^i$ where $0 \leq t \leq p-1$ and $r_t \neq 0$. To prove that $C(\bar{\Gamma}_w) \cap \bar{R}[\bar{\theta}]$ is contained in \bar{R} we shall assume that $t > 0$ and contradict the fact that $r_t \neq 0$.

Now according to Prop. 2.6 there exists an element σ of G_w such that $g(\tau^{n(\sigma)}, \sigma) \neq 1$. Therefore $g(\tau^{n(\sigma)}, \sigma)$ must be of the form $g(\tau^{n(\sigma)}, \sigma) = \zeta^a$ for the primitive p^{th} root of unity ζ and some integer a satisfying $1 \leq a \leq p-1$ (see Prop. 2.5). We shall now establish the equality $u_\sigma \bar{\theta} = \left(\bar{\theta} + \frac{a}{n(\sigma)}\right) u_{\bar{\sigma}}$ where $\bar{\sigma}$ denotes the image of σ under the natural map of G_w onto G_w/G_1 . From the definition of θ together with the fact that $g(\sigma, \tau) = 1$ (see Prop. 2.5) we obtain the equality $u_\sigma \theta = \frac{1}{(1-\zeta^\sigma)\zeta^a} \left[(u_\tau^{n(\sigma)} - 1) + (1 - \zeta^a) \right] u_\sigma$. According to Lemma 2.3, $\zeta^a = \zeta^{n(\sigma)}$. And the congruence $\zeta \equiv 1 \pmod{\Pi S_w}$ implies that $\zeta^{n(\sigma)-1} + \dots + 1 \equiv n(\sigma) \pmod{\Pi S_w}$. From these observations we obtain the congruence $u_\sigma \theta \equiv \frac{1}{n(\sigma)} \left[\frac{1}{1-\zeta} (u_\tau^{n(\sigma)} - 1) + \frac{1-\zeta^a}{1-\zeta} \right] u_\sigma \pmod{\Gamma_w \Pi}$. Observe that $u_\tau^{n(\sigma)} - 1 = (u_\tau - 1)(u_\tau^{n(\sigma)-1} + \dots + 1)$ so that $u_\tau^{n(\sigma)} - 1 \equiv n(\sigma)(u_\tau - 1)$

mod $\Gamma_w \Pi$ since $u_\tau \equiv 1 \pmod{\Gamma_w \Pi}$. This fact together with the congruence $\frac{1-\zeta^a}{1-\zeta} \equiv a \pmod{\Gamma_w \Pi}$ enables us to write $u_{\bar{\sigma}} \bar{\theta} = \left(\bar{\theta} + \frac{a}{n(\bar{\sigma})} \right) u_{\bar{\sigma}}$.

Since λ is in $C(\bar{\Gamma}_w)$ we must have that $u_{\bar{\sigma}} \lambda = \lambda u_{\bar{\sigma}}$. From the above we may then obtain the equality $\sum_{i=0}^t r_i \bar{\theta}^i = \sum_{i=0}^t r_i \left(\bar{\theta} + \frac{a}{n(\bar{\sigma})} \right)^i$. Using the fact that $\bar{R}[\bar{\theta}]$ is a free \bar{R} -module with free basis $\{1, \bar{\theta}, \dots, \bar{\theta}^{p-1}\}$ it follows from equating coefficients of $\bar{\theta}^{t-1}$ that $r_{t-1} = r_{t-1} + \frac{ta}{n(\bar{\sigma})} r_t$. Therefore $r_t = 0$, and this contradiction proves the lemma.

COROLLARY 2.21. *The ring $\bar{\Gamma}_w$ is a simple ring.*

Proof. The number of simple components of the semi-simple ring $\bar{\Gamma}_w$ is equal to the number of primitive orthogonal idempotents required to generate its center. Since the idempotent elements of $C(\bar{\Gamma}_w)$ are in \bar{R} according to the lemma, we conclude that $\bar{\Gamma}_w$ is simple.

PROPOSITION 2.22. *The R -order Γ_w in the central simple k -algebra $A(g, L_w, G_w)$ has the following properties*

- i) Γ_w is a maximal order with radical $\Gamma_w \Pi$
- ii) $r(\Gamma_w | R) = r(S_w | R)$.

Proof. Prop. 2.18 together with Cor. 2.21 implies that Γ_w is an hereditary order with unique maximal two-sided ideal. Therefore Γ_w is a maximal order according to Thm. 2.3 of [4].

Since $\Gamma_w \Pi$ is the radical of Γ_w (see Lemma 2.17) and Π is the prime element of S_w , it follows that the ramification index of Γ_w over R is equal to the ramification index of S_w over R .

Now we prove the main result of this section.

PROPOSITION 2.23. *Let k denote the quotient field of a complete discrete rank one valuation ring R of unequal characteristic, and let Σ denote a central simple k -algebra for which $\tilde{\Sigma}$ is in $V(k)$. If $\tilde{\Sigma}$ has Brauer number equal to the characteristic p of \bar{R} , then a maximal order of Σ is not equivalent to a crossed product over a tamely ramified extension of R .*

Proof. Let Γ denote a maximal order in a central simple algebra Σ such that $\tilde{\Sigma}$ satisfies the hypothesis of the theorem. If $\tilde{\Sigma}$ has Brauer number p there exists a maximal order Γ_w equivalent to Γ for which $r(\Gamma_w | R)$ is

divisible by p according to Prop. 2.22. Therefore $r(\Gamma/R)$ is divisible by p , since ramification index is preserved under equivalence (Prop. 1.6).

However Props. 1.6 and 1.7 together imply that a maximal order equivalent to a crossed product over a tamely ramified extension of R has ramification index relatively prime to the characteristic of \bar{R} .

3. The equicharacteristic case. The purpose of this section is to prove the assertion analogous to that of Prop. 2.23 in the case when R is an equicharacteristic ring. If R is an equicharacteristic ring of characteristic zero, then the Brauer number of $\bar{\Sigma}$ is relatively prime to the characteristic of \bar{R} for every central simple k -algebra Σ ; so for the purpose of this section we restrict our attention to the case of non-zero characteristic.

The following notation shall be in use throughout this section. The symbol R shall denote an equicharacteristic complete discrete rank one valuation ring of non-zero characteristic, and Σ shall denote a central simple algebra over the quotient field k of R for which Σ is in $V(k)$ and such that the Brauer number of Σ is equal to the characteristic p of \bar{R} . Since Σ is in $V(k)$, we may assume that Σ is of the form $\Sigma = \mathcal{A}(f, L, G)$ for some unramified Galois extension L of k .

Our object is to prove that under the assumption on the Brauer number of Σ , a maximal order in Σ cannot be equivalent to a crossed product over a tamely ramified extension of R .

The method of proof is similar to that used in Section 2. We shall construct a central simple k -algebra $\Sigma_w = \mathcal{A}(g, L_w, G_w)$ equivalent to $\Sigma = \mathcal{A}(f, L, G)$ with L_w a wildly ramified extension of k and with the 2-cocycle g in $Z^2(G_w, U(S_w))$, where S_w denotes the integral closure of R in L_w . As in Section 2 we then construct a maximal order Γ_w in Σ_w by adjoining an element θ of Σ_w to the crossed product $\mathcal{A}(g, S_w, G_w)$ and prove that the ramification index $r(\Gamma_w/R)$ is equal to the characteristic of \bar{R} .

In order to construct the desired central simple k -algebra Σ_w we first construct the extension L_w of k . Let S denote the integral closure of R in L and consider a prime element π of S . It follows from Eisenstein's criterion that the polynomial $F(X) = X^p - \pi^{p-1}X - \pi$ of $S[X]$ is irreducible in $L[X]$, and we define L_w to be the field obtained by adjoining a root Π of $F(X)$ to L .

PROPOSITION 3.1. *The chain of fields $L_w \supset L \supset k$ defined above has the following properties*

- i) *if Π denotes one root of $F(X) = X^p - \pi^{p-1}X - \pi$ then the other roots of $F(X)$ are given by $\Pi + \xi^i\pi$ for $1 \leq i \leq p-1$ where ξ denotes a primitive $(p-1)^{st}$ root of unity in R*
- ii) *L_w is a Galois extension of k*
- iii) *the extension L_w of L is wildly ramified of degree p , and Π is a prime element of L_w .*

Proof. Using the fact that k has characteristic p , together with the fact that $F(\Pi) = 0$, one may obtain that $F(\Pi + \xi^i\pi) = (\xi^{ip} - \xi^i)\pi^p$. But $\xi^p = \xi$ since ξ is a $(p-1)^{st}$ root of unity, and therefore $F(\Pi + \xi^i\pi) = 0$ for $1 \leq i \leq p-1$.

It is clear from statement i) that L_w is a Galois extension of k . The equality $\Pi^p = \pi(\pi^{p-2}\Pi + 1)$ implies that L_w is a wildly ramified inertial extension of L of degree p with prime element Π .

Henceforth G_w shall denote the Galois group of L_w over k , and S_w the integral closure of R in L_w . The next proposition describes the ramification groups of the extension L_w of k .

PROPOSITION 3.2. *Let G_i denote the i^{th} ramification group of L_w over k . Then*

- i) $G_0 = G_1$
- ii) G_1 is a cyclic group of order p
- iii) G_1 is contained in the center of G_w
- iv) $G_i = G_1$ and $G_{i+1} = (1)$ for $i = p-1$.

Proof. Statement i) is true because the extension L_w of k has no tame inertial part. Statement ii) follows at once from Prop. 3.1.

In order to prove that G_1 is contained in the center of G_w , consider the generator τ of G_1 defined by $\tau(\Pi) = \Pi + \xi\pi$ and an element σ of G_w . Since τ leaves the elements of S fixed, it follows that $\tau\sigma = \sigma\tau$ if and only if $\tau\sigma(\Pi) = \sigma\tau(\Pi)$. The conjugates of Π relative to k are precisely the conjugates of Π relative to L since the minimal polynomial $F(X)$ of Π is in $k[X]$. Therefore $\sigma(\Pi) = \Pi$ or $\sigma(\Pi) = \Pi + \xi^i\pi$ for some integer i such that $1 \leq i \leq p-1$ according to Prop. 3.1. When $\sigma(\Pi) = \Pi$ it is clear that

$\tau\sigma(\Pi) = \sigma\tau(\Pi)$. So consider the case when $\sigma(\Pi) = \Pi + \xi^i\pi$. Using the fact that ξ and π are in k it is easy to verify that $\tau\sigma(\Pi)$ and $\sigma\tau(\Pi)$ are both equal to $\Pi + \xi(1 + \xi^{i-1})\pi$. Therefore $\tau\sigma = \sigma\tau$ for all σ in G_w , and hence G_1 is in the center of G_w .

Finally we observe that $p-1$ is a discontinuity in the sequence of ramification groups of L_w over k . For if τ is the element of G_1 defined by $\tau(\Pi) = \Pi + \xi\pi$, then $\tau(\Pi) - \Pi = \xi\pi$ so that τ is in G_i if and only if $1 \leq i \leq p-1$.

In order to define the central simple k -algebra $\Sigma_w = \mathcal{A}(g, L_w, G_w)$ it remains to define the 2-cocycle g of $Z^2(G_w, U(L_w))$. Now the assumption that the Brauer number of Σ is p , where $\Sigma = \mathcal{A}(f, L, G)$, implies that the p^{th} power of the cohomology class $[f]$ is in the image of the natural map $H^2(G, U(S)) \rightarrow H^2(G, U(L))$. There exists therefore a map $\phi: G \rightarrow U(L)$ such that the 2-cocycle h of $Z^2(G, U(L))$ defined by $h(\sigma, \tau) = f^p(\sigma, \tau)\phi(\sigma\tau) / \phi(\sigma)\phi^p(\tau)$ takes values in $U(S)$. Since $\phi(\sigma)$ is in $U(L)$ we may write $\phi(\sigma) = \alpha_\sigma\pi^{\beta(\sigma)}$ where α_σ is in $U(S)$ and $\beta(\sigma)$ is an integer, and π denotes the prime element of S . Define now the map $\phi_w: G_w \rightarrow U(L_w)$ by $\phi_w(\sigma) = \Pi^{\beta(\bar{\sigma})}$ where $\bar{\sigma}$ denotes the image of σ under the natural map of G_w onto $G_w/G_1 = G$, and Π denotes the prime element of S_w . Define the element g of $Z^2(G_w, U(L_w))$ by

$$g(\sigma, \tau) = f_w(\sigma, \tau)\phi_w(\sigma\tau) / \phi_w(\sigma)\phi_w^p(\tau)$$

where f_w denotes the image of f under the inflation map $Z^2(G, U(L)) \rightarrow Z^2(G_w, U(L_w))$. The central simple k -algebra $\mathcal{A}(g, L_w, G_w)$ shall be denoted by Σ_w . The next three propositions present properties of the 2-cocycle g .

PROPOSITION 3.3. *The element g defined above is in the image of the natural map $Z^2(G_w, U(S_w)) \rightarrow Z^2(G_w, U(L_w))$.*

Proof. Using the method of Prop. 2.4 one can verify that g^p takes values in $U(S_w)$, from which it follows at once that g is in the image of the natural map $Z^2(G_w, U(S_w)) \rightarrow Z^2(G_w, U(L_w))$.

PROPOSITION 3.4. *The 2-cocycle g defined above has the following properties*

- i) $g(\sigma, \rho) = 1$ for every σ in G_w and ρ in G_1
- ii) $g(\sigma, \rho) \equiv 1 \pmod{(\Pi^{p-1})}$ for every σ in G_1 and ρ in G_w

iii) \bar{g} is in the image of the inflation map $Z^2(G, U(\bar{S})) \longrightarrow Z^2(G_w, U(\bar{S}))$ where \bar{g} denotes the image of g under the natural map $Z^2(G_w, U(S_w)) \longrightarrow Z^2(G_w, U(\bar{S}))$.

Proof. As in the proof of Prop. 2.5 one can easily show that $\beta(1) = 0$ where 1 denotes the identity element of G . Now let σ denote an element of G_w and ρ an element of G_1 . By the definition of f_w we have $f_w(\sigma, \rho) = f(\bar{\sigma}, \bar{\rho}) = 1$ where $\bar{\sigma}$ denotes the image of σ under the natural map of G_w onto G , so that $g(\sigma, \rho) = \phi_w(\sigma\rho) / \phi_w(\sigma)\phi_w^{\sigma}(\rho) = \Pi^{\beta(\bar{\sigma})} / \Pi^{\beta(\bar{\sigma})}\sigma(\Pi^{\beta(\bar{1})})$. Since $\beta(\bar{1}) = 0$, it follows that $g(\sigma, \rho) = 1$.

In order to prove statement ii), consider now an element σ of G_1 and an element ρ of G_w . The definition of g together with the fact that $\beta(\bar{1}) = 0$ implies that $g(\sigma, \rho) = [\Pi / \sigma(\Pi)]^{\beta(\bar{\rho})}$. According to Prop. 3.1 we have $\sigma(\Pi) = \Pi$ or $\sigma(\Pi) = \Pi + \xi^i\pi$ where ξ is a primitive $(p-1)^{st}$ root of unity and i is an integer satisfying $1 \leq i \leq p-1$. If $\sigma(\Pi) = \Pi$ it is clear that $g(\sigma, \rho) = 1$; so consider the case when $\sigma(\Pi) = \Pi + \xi^i\pi$ for some i . Observe that $\pi = \Pi^p - \pi^{p-1}\Pi$ since $F(\Pi) = 0$. Substituting this expression for π one then obtains that $\sigma(\Pi) / \Pi = (\Pi + \xi^i\pi) / \Pi = 1 + \xi^i(\Pi^{p-1} - \pi^{p-1})$, so that $\sigma(\Pi) / \Pi \equiv 1 \pmod{(\Pi^{p-1})}$. We may now conclude that $g(\sigma, \rho) \equiv 1 \pmod{(\Pi^{p-1})}$.

For the proof of part iii) we first observe that $\bar{g}(\sigma, \rho) = \bar{g}(\rho, \sigma) = \bar{1}$ for every σ in G_w and ρ in G_1 according to parts i) and ii) of this proposition. Using this observation it is easy to verify that the map $q: G \times G \longrightarrow U(\bar{S})$ defined by $q(\bar{\sigma}, \bar{\rho}) = \bar{g}(\sigma, \rho)$ is an element of $Z^2(G, U(\bar{S}))$ in the preimage of \bar{g} .

PROPOSITION 3.5. *For each non-trivial element τ of G_1 there exists an element σ of G_w for which $g(\tau, \sigma) \equiv 1 \pmod{(\Pi^{p-1})}$ and $g(\tau, \sigma) \not\equiv 1 \pmod{(\Pi^p)}$.*

Proof. Let $\beta: G \longrightarrow Z$ be the function used in the definition of the 2-cocycle g , and let $\bar{\sigma}$ denote the image of the element σ of G_w under the natural mapping of G_w onto G . We shall show first that there exists an element σ of G_w such that $\beta(\bar{\sigma})$ is relatively prime to p . We shall then use the equality $g(\tau, \sigma) = (\Pi^{\beta(\bar{\sigma})}) / \tau(\Pi^{\beta(\bar{\sigma})})$ to show that $g(\tau, \sigma) \not\equiv 1 \pmod{(\Pi^p)}$.

We now show that there exists an element σ of G_w for which $\beta(\bar{\sigma}) \not\equiv 0 \pmod{p}$. As in Prop. 2.6 the method of proof is to assume that $g(\bar{\sigma}) \equiv 0 \pmod{p}$ for every σ in G_w and then contradict the assumption on the Brauer number of $\tilde{\Sigma}$, where Σ denotes the central simple k -algebra $\Delta(f, L, G)$. If $\beta(\bar{\sigma}) \equiv 0 \pmod{p}$ for every σ in G_w , then each integer $\beta(\bar{\sigma})$

may be written in the form $\beta(\bar{\sigma}) = p\gamma(\bar{\sigma})$ for some integer $\gamma(\bar{\sigma})$. Define $\Psi: G \rightarrow U(L)$ by $\Psi(\sigma) = \pi^{\gamma(\sigma)}$. One can verify that the 2-cocycle q of $Z^2(G, U(L))$ defined by $q(\sigma, \rho) = f(\sigma, \rho)\Psi(\sigma\rho) / \Psi(\sigma)\Psi(\rho)$ is cohomologous to f and takes values in $U(S)$, so that $[f]$ is in the image of the natural map $H^2(G, U(S)) \rightarrow H^2(G, U(L))$. This contradicts the assumption that the Brauer number of $\tilde{\Sigma}$ is p . Therefore there must exist an element σ of G_w for which $\beta(\bar{\sigma}) \not\equiv 0 \pmod{p}$.

Finally we show that this σ satisfies the assertion of the proposition. Part ii) of Prop. 3.4 implies that $g(\tau, \sigma) \equiv 1 \pmod{(\Pi^{p-1})}$, so it remains to show that $\beta(\bar{\sigma}) \not\equiv 0 \pmod{p}$ implies that $g(\tau, \sigma) \not\equiv 1 \pmod{(\Pi^p)}$. We have already observed that $g(\tau, \sigma) = [\Pi / \tau(\Pi)]^{\beta(\bar{\sigma})}$ (see the proof of part ii) of Prop. 3.4). Let $u = \tau(\Pi) / \Pi$. Since τ was assumed to be non-trivial we must have that $\tau(\Pi) = \Pi + \xi^i \pi$ for some integer i . The equality $u = 1 + \xi^i(\Pi^{p-1} - \pi^{p-1})$ implies that $u \not\equiv 1 \pmod{(\Pi^p)}$. It is easy to see that $u^{\beta(\bar{\sigma})} \not\equiv 1 \pmod{(\Pi^p)}$ by writing $u^{\beta(\bar{\sigma})} - 1$ in the form $u^{\beta(\bar{\sigma})} - 1 = (u - 1)(u^{\beta(\bar{\sigma})-1} + \dots + 1)$. For the fact that $\beta(\bar{\sigma})$ is relatively prime to p implies that $u^{\beta(\bar{\sigma})-1} + \dots + 1$ is in $U(S_w)$, so that $u^{\beta(\bar{\sigma})} \equiv 1 \pmod{(\Pi^p)}$ if and only if $u \equiv 1 \pmod{(\Pi^p)}$. We may now conclude that $g(\tau, \sigma) \not\equiv 1 \pmod{(\Pi^p)}$.

Since the 2-cocycle g is in $Z^2(G_w, U(S_w))$ we may consider the crossed product $\Delta_w = \Delta(g, S_w, G_w)$. Observe, moreover, that Δ_w is an R -order in Σ_w . In order to construct the desired order Γ_w containing Δ_w , we first introduce some notation; throughout the rest of this section τ shall denote a fixed generator of G_1 and ξ shall denote the primitive $(p-1)^{st}$ root of unity defined by $\tau(\Pi) = \Pi + \xi\pi$. Consider the element θ of Σ_w defined by $\theta = \frac{\Pi}{\pi}(u_\tau - 1)$. Now Γ_w is defined to be the ring obtained by adjoining the element θ to Δ_w , i.e. $\Gamma_w = \Delta_w[\theta]$. Our main object is to prove that Γ_w is a maximal order whose unique maximal two-sided ideal is generated by the prime element Π of S_w .

The next two lemmas shall be useful in proving that Γ_w is in fact an order over R in Σ_w .

LEMMA 3.6. *For $1 \leq i \leq p-1$, let a_i be the element of $\Delta(1, S_w, G_1)$ defined*

by $a_i = \frac{\Pi}{\pi} \left(\frac{u^i - 1}{u^i} \right) u_\tau$ where u is the element of $U(S_w)$ defined by $\tau(\Pi) = u\Pi$. Then $(\theta - a_{p-1})(\theta - a_{p-2}) \cdots (\theta - a_1)\theta = 0$.

Proof. Observe that each element a_i of $\mathcal{A}(1, L_w, G_1)$ defined above is in fact an element of the crossed product $\mathcal{A}(1, S_w, G_1)$ (apply part iv) of Prop. 3.2).

The first step is to prove inductively that $(\theta - a_i) \cdots (\theta - a_1)\theta = \left(\frac{\Pi}{\pi}\right)^{i+1} (u_\tau - 1)^{i+1}$. When $i = 1$ we obtain by an easy computation the equalities $(\theta - a_1)\theta = \theta^2 - a_1\theta = \left(\frac{\Pi}{\pi}\right)^2 [(uu_\tau - 1) - (u - 1)u_\tau] (u_\tau - 1) = \left(\frac{\Pi}{\pi}\right)^2 (u_\tau - 1)^2$. For the inductive step we assume that $(\theta - a_i) \cdots (\theta - a_1)\theta = \left(\frac{\Pi}{\pi}\right)^{i+1} (u_\tau - 1)^{i+1}$. Then

$$\begin{aligned} (\theta - a_{i+1})(\theta - a_i) \cdots (\theta - a_1)\theta &= (\theta - a_{i+1}) \left(\frac{\Pi}{\pi}\right)^{i+1} (u_\tau - 1)^{i+1} \\ &= \left(\frac{\Pi}{\pi}\right)^{i+2} [(u^{i+1}u_\tau - 1) - (u^{i+1} - 1)u_\tau] (u_\tau - 1)^{i+1} \\ &= \left(\frac{\Pi}{\pi}\right)^{i+2} (u_\tau - 1)^{i+2} \end{aligned}$$

and this completes the inductive step.

From the above we may now conclude that $(\theta - a_{p-1}) \cdots (\theta - a_1)\theta = \left(\frac{\Pi}{\pi}\right)^p (u_\tau - 1)^p$. But $(u_\tau - 1)^p = 0$ since $(u_\tau)^p = 1$ and k has characteristic p . Therefore $(\theta - a_{p-1}) \cdots (\theta - a_1)\theta = 0$.

LEMMA 3.7. The ring Γ_w is generated as both a left and right $\mathcal{A}(g, S_w, G_w)$ -module by $\{1, \theta, \dots, \theta^{p-1}\}$.

Proof. As in Prop. 2.11 we first prove that Γ_w is generated as a right \mathcal{A}_w -module by powers of θ . We shall obtain the inclusion $\mathcal{A}_w(\theta) \subset (1, \theta)\mathcal{A}_w$ by showing that $(\alpha_\rho u_\rho)\theta$ is contained in $(1, \theta)\mathcal{A}_w$ for every element ρ of G_w and α_ρ of S_w . Using the definition of θ one may obtain by a straightforward computation the equality

$$(\alpha_\rho u_\rho)\theta = \frac{\Pi}{\pi} [u_\tau \tau^{-1}(\alpha_\rho v / g(\tau, \rho)) - v\alpha_\rho] u_\rho$$

where v is the element of $U(S_w)$ defined by $\rho(\Pi) = v\Pi$. From part ii) of Prop. 3.4 we may obtain the congruence $\tau^{-1}(1/g(\tau, \rho)) \equiv 1 \pmod{(\Pi^{p-1})}$. The equality of ramification groups $G_1 = G_{p-1}$ (see Prop. 3.2) implies that

$\tau^{-1}(\alpha_\rho v) \equiv \alpha_\rho v \pmod{(\Pi^p)}$. These two congruences together imply that $\tau^{-1}(\alpha_\rho v / g(\tau, \rho)) \equiv \alpha_\rho v \pmod{(\Pi^{p-1})}$, so that $\tau^{-1}(\alpha_\rho v / g(\tau, \rho)) = \alpha_\rho v + s\Pi^{p-1}$ for some element s of S_w . Substituting into the above expression for $(\alpha_\rho u_\rho)\theta$ we may then obtain the equality $(\alpha_\rho u_\rho)\theta = \left[\frac{\Pi}{\pi}(u_\tau - 1)v\alpha_\rho u_\rho \right] + \left[\frac{\Pi}{\pi}u_\tau s\Pi^{p-1}u_\rho \right]$. The first summand is in $(\theta)\mathcal{A}_w$ and the second is in \mathcal{A}_w , so that $(\alpha_\rho u_\rho)\theta$ is in $(1, \theta)\mathcal{A}_w$.

It can now be proved inductively that $\mathcal{A}_w(\theta^i)$ is contained in $(\theta^{i-1}, \theta^i)\mathcal{A}_w$ for every positive integer i . Since θ satisfies an equation of degree p over $\mathcal{A}(1, S_w, G_1)$ (see Lemma 3.6) we conclude finally that Γ_w is generated as a right \mathcal{A}_w -module by $\{1, \theta, \dots, \theta^{p-1}\}$. A similar argument shows that Γ_w is generated as a left \mathcal{A}_w -module by $\{1, \theta, \dots, \theta^{p-1}\}$.

PROPOSITION 3.8. *The ring Γ_w is an order over R in the central simple k -algebra Σ_w .*

Proof. The proof of this assertion follows from Lemma 3.7 by an argument similar to that of Prop. 2.12.

We can prove that Γ_w is an hereditary order by proving that its radical is Γ_w -projective.

LEMMA 3.9. *Let Π denote the prime element of S_w . Then*

- i) $\Pi\Gamma_w = \Gamma_w\Pi$
- ii) Π is an element of $\text{rad } \mathcal{A}_w$
- iii) $\text{rad } \mathcal{A}_w = (\Pi, u_\tau - 1)\mathcal{A}_w$
- iv) $\Gamma_w\Pi \cap \mathcal{A}_w = \text{rad } \mathcal{A}_w$.

Proof. Since Γ_w is generated as a left \mathcal{A}_w -module by the elements $\{1, \theta, \dots, \theta^{p-1}\}$ (Lemma 3.7) and $\Pi\mathcal{A}_w = \mathcal{A}_w\Pi$, it suffices to prove that $\theta\Pi$ is in $\Pi\Gamma_w$ in order to establish the inclusion $\Gamma_w\Pi \subset \Pi\Gamma_w$. The equality $\theta\Pi = \Pi\theta + \frac{\Pi}{\pi}(\tau(\Pi) - \Pi)u_\tau$ may be obtained by an easy computation. It is easy to verify that the element $\frac{1}{\pi}(\tau(\Pi) - \Pi)$ is in S_w using the fact that there is a discontinuity in the sequence of ramification groups G_i at $i = p - 1$ (Prop. 3.2). Therefore $\theta\Pi$ is in $\Pi\Gamma_w$ and $\Gamma_w\Pi$ is contained in $\Pi\Gamma_w$. A similar computation yields the opposite inclusion. Therefore $\Gamma_w\Pi = \Pi\Gamma_w$. By Lemma 1.4 of [12] we may now conclude that Π is in $\text{rad } \Gamma_w$. This completes the proof of statements i) and ii).

The proof of part iii) is entirely similar to the proof of part iii) of Lemma 2.14.

It remains to prove assertion iv). Lemma 2.13 implies that $\Gamma_w \Pi \cap \mathcal{A}_w$ is contained in $\text{rad } \mathcal{A}_w$ since Π is in $\text{rad } \Gamma_w$ according to part ii). To obtain the opposite inclusion we make use of the fact that $\text{rad } \mathcal{A}_w = (\Pi, u_\tau - 1)\mathcal{A}_w$. The definition of θ implies that $u_\tau - 1$ is in $\Pi^{p-1}\Gamma_w = \Gamma_w \Pi^{p-1}$, from which it follows that $\text{rad } \mathcal{A}_w$ is contained in $\Gamma_w \Pi$.

By Lemma 3.9 we may now form the residue class ring $\Gamma_w / \Gamma_w \Pi$ which shall henceforth be denoted by $\bar{\Gamma}_w$. An argument similar to that of Lemma 2.16 shows that $\bar{\Gamma}_w$ is R -algebra isomorphic to $\mathcal{A}(\bar{g}, \bar{S}, G)[\bar{\theta}]$ in a natural way where $\bar{\theta}$ denotes the residue class of θ modulo $\Gamma_w \Pi$.

In a manner similar to that of Section 2, the semi-simplicity of $\bar{\Gamma}_w$ shall follow from that of its subring $\bar{S}[\bar{\theta}]$.

LEMMA 3.10. *For $1 \leq i \leq p-1$ let a_i denote the element of $\mathcal{A}(1, S_w, G_1)$ defined in Lemma 3.6, and let \bar{a}_i denote the image of a_i in $\bar{\Gamma}_w$. Then $\bar{a}_i = \bar{\xi}i$ where $\bar{\xi}$ denotes the primitive $(p-1)^{\text{st}}$ root of unity defined by $\tau(\Pi) = \Pi + \xi\pi$.*

Proof. From the definition of a_i we obtain the equality $a_i = \frac{\Pi}{\pi}(u-1) \left(\frac{u^{i-1} + \dots + 1}{u^i} \right) u_\tau$. Since $\frac{\Pi}{\pi}(u-1) = \frac{1}{\pi}(\tau(\Pi) - \Pi) = \xi$ we may write $a_i = \xi \left(\frac{u^{i-1} + \dots + 1}{u^i} \right) u_\tau$. The congruence $u_\tau \equiv 1 \pmod{\Gamma_w \Pi}$ holds because θ is in Γ_w . And $u \equiv 1 \pmod{\Pi S_w}$ since $G_{p-1} = G_1$ (see Prop. 3.2), so that $u^{i-1} + \dots + 1 \equiv i \pmod{\Pi S_w}$. Combining these observations we may now conclude that $\bar{a}_i = \bar{\xi}i$.

LEMMA 3.11. *The ring $\bar{\Gamma}_w$ is a semi-simple ring.*

Proof. The first step is to observe that the subring $\bar{S}[\bar{\theta}]$ of $\bar{\Gamma}_w$ is a commutative semi-simple ring. Consider an element $\bar{\alpha}$ of \bar{S} for which $\bar{S} = \bar{R}(\bar{\alpha})$. In order to establish the commutativity of $\bar{S}[\bar{\theta}]$ it suffices to prove that $\bar{\alpha}\bar{\theta} = \bar{\theta}\bar{\alpha}$. Now from the definition of θ we obtain the equality $\theta\alpha = \frac{\Pi}{\pi}(\tau(\alpha)u_\tau - \alpha)$ where α is an element of S_w in the preimage of $\bar{\alpha}$. It is easy to see that the congruence $\tau(\alpha) \equiv \alpha \pmod{(\Pi^p)}$ implies that $\theta\alpha = \alpha\theta \pmod{\Gamma_w \Pi}$. In order to prove that $\bar{S}[\bar{\theta}]$ is semi-simple we point out that a computation similar to that of Lemma 2.16 may be used to show that

$\bar{S}[\bar{\theta}]$ is a free \bar{S} -module with free basis $\{1, \bar{\theta}, \dots, \bar{\theta}^{p-1}\}$. From this it follows that $\bar{S}[\bar{\theta}]$ is isomorphic to the factor ring $\bar{S}[Y]/(H(Y))$ where $H(Y) = (Y - \bar{a}_{p-1}) \cdots (Y - \bar{a}_1)Y$. Since $\bar{a}_i = \bar{\xi}i$ according to Lemma 3.10, we see that $\bar{a}_i = \bar{a}_j$ if and only if $i = j$, so that $H(Y)$ is a polynomial without repeated roots. We may now conclude from the Chinese Remainder Theorem that $\bar{S}[Y]/(H(Y))$ is isomorphic to a direct sum of p copies of \bar{S} . This completes the proof that $\bar{S}[\bar{\theta}]$ is semi-simple.

An argument similar to that of Lemma 2.16 C shows that $\bar{\Gamma}_w$ is a free left $\bar{S}[\bar{\theta}]$ -module with free basis $\{u_{\sigma_i}\}$ where σ_i ranges over the elements of G . Using this fact one can now establish by the method of Lemma 2.17 that $\bar{\Gamma}_w$ is a semi-simple ring.

PROPOSITION 3.12. *The ring Γ_w is an hereditary R -order with radical $\Gamma_w \Pi$.*

Proof. Since Π is in $\text{rad } \Gamma_w$ and $\Gamma_w / \Gamma_w \Pi$ is semi-simple it follows that $\text{rad } \Gamma_w = \Gamma_w \Pi$. Thus Γ_w is an hereditary order by the Corollary to Thm. 2.2 of [4].

LEMMA 3.13. *The ideal $\Gamma_w \Pi$ is the unique maximal two-sided ideal of Γ_w .*

Proof. In order to prove that $\Gamma_w \Pi$ is the unique maximal two-sided ideal of Γ_w it suffices to prove that the semi-simple ring $\bar{\Gamma}_w$ is in fact a simple ring, and we do this by studying the idempotents in the center $C(\bar{\Gamma}_w)$ of $\bar{\Gamma}_w$.

An argument similar to that used in Lemma 2.19 shows that $C(\bar{\Gamma}_w)$ is contained in $\bar{S}[\bar{\theta}]$. It is easy to see that the idempotents of $\bar{S}[\bar{\theta}]$ are already present in $\bar{R}[\bar{\theta}]$. For consider the polynomial $H(Y) = (Y - \bar{a}_{p-1}) \cdots (Y - \bar{a}_1)Y$ of $\bar{S}[Y]$ and recall that the equation $H(Y) = 0$ is satisfied by $\bar{\theta}$. Lemma 3.10 implies that the \bar{a}_i are in $U(\bar{R})$, so that $H(Y)$ splits into p (distinct) linear factors in $\bar{R}[Y]$. Using the Chinese Remainder Theorem once again, we conclude that $\bar{R}[\bar{\theta}]$ has precisely p simple components. Since $\bar{R}[\bar{\theta}] \subset \bar{S}[\bar{\theta}]$ is an inclusion of commutative rings, we may now conclude that the idempotents of $\bar{S}[\bar{\theta}]$ are already present in $\bar{R}[\bar{\theta}]$.

We now use Prop. 3.5 to prove that the intersection $C(\bar{\Gamma}_w) \cap \bar{R}[\bar{\theta}]$ is contained in \bar{R} . The proof is by contradiction. Suppose that $\lambda = \sum r_i \bar{\theta}^i$ is a non-zero element of $C(\bar{\Gamma}_w) \cap \bar{R}[\bar{\theta}]$, where the r_i are in \bar{R} and t is the largest integer for which $r_t \neq 0$. Prop. 3.5 implies that there exists an

element σ of G_w such that $g(\tau, \sigma) \equiv 1 \pmod{(\Pi^{p-1})}$ and $g(\tau, \sigma) \not\equiv 1 \pmod{(\Pi^p)}$. Therefore we may write $g(\tau, \sigma) = 1 + w\Pi^{p-1}$ for some element w of $U(S_w)$. Using the definition of θ together with the fact that G_1 is contained in the center of G_w (Prop. 3.2) one may obtain by an easy computation the equality $u_{\bar{\sigma}}\bar{\theta} = (\bar{\theta} + \bar{w})u_{\bar{\sigma}}$. Since λ is in $C(\bar{\Gamma}_w)$ we must have $u_{\bar{\sigma}}\lambda = \lambda u_{\bar{\sigma}}$, so that $\sum r_i \bar{\theta}^i = \sum r_i (\bar{\theta} + \bar{w})^i$. This equality together with the fact that $\{1, \bar{\theta}, \dots, \bar{\theta}^{p-1}\}$ is a free basis for $\bar{R}[\bar{\theta}]$ over \bar{R} implies that $r_{t-1} = r_{t-1} + t\bar{w}r_t$. Therefore $r_t = 0$ and this contradiction establishes the desired inclusion.

Combining the above observations, we may conclude that the idempotent elements in the center of $\bar{\Gamma}_w$ are contained in \bar{R} . Therefore the semi-simple ring $\bar{\Gamma}_w$ is a simple ring, and $\Gamma_w\Pi$ is the unique maximal two-sided ideal of Γ_w .

The arguments used in Props. 2.22 and 2.23 may now be used to prove the next two propositions.

PROPOSITION 3.14. *The R -order Γ_w in the central simple k -algebra Σ_w has the following properties*

- i) Γ_w is a maximal order with radical $\Gamma_w\Pi$
- ii) $r(\Gamma_w | R) = r(S_w | R)$.

PROPOSITION 3.15. *Let k denote the quotient field of a complete discrete rank one valuation ring R which is an equicharacteristic ring of characteristic $p \neq 0$, and let Σ denote a central simple k -algebra for which $\tilde{\Sigma}$ is in $V(k)$. If $\tilde{\Sigma}$ has Brauer number p , then a maximal order in Σ is not equivalent to a crossed product over a tamely ramified extension of R .*

Combining Propositions 2.23 and 3.15 we obtain the following theorem.

THEOREM 3.16. *Let k denote the quotient field of a complete discrete rank one valuation ring R such that the characteristic p of \bar{R} is non-zero, and let Σ denote a central simple k -algebra for which $\tilde{\Sigma}$ is in $V(k)$. If $\tilde{\Sigma}$ has Brauer number p , then a maximal order in Σ is not equivalent to a crossed product over a tamely ramified extension of R .*

4. Maximal orders and the Brauer group. Let k denote the quotient field of a complete discrete rank one valuation ring R . In this

section we prove the main theorem of the paper, namely that a maximal order in a central simple k -algebra Σ is equivalent to a crossed product over a tamely ramified extension of R if and only if $\tilde{\Sigma}$ is in $T(k)$. Both the necessity and sufficiency parts of the proof depend upon the main theorem on crossed products and maximal orders presented by the author in [11].

The following lemma shall be used to prove the sufficiency of the condition that $\tilde{\Sigma}$ be in $T(k)$.

LEMMA 4.1. *Let k denote the quotient field of a complete discrete rank one valuation ring R . Let L be an unramified extension of k , and $\Sigma = \Delta(f, L, G)$ a crossed product for which $\tilde{\Sigma}$ is in $T(k)$. Then there exists an extension L_t of L such that*

i) L_t is a tamely ramified Galois extension of k

ii) $[f_t]$ is in the image of the natural map $H^2(G_t, U(S_t)) \rightarrow H^2(G_t, U(L_t))$ where S_t is the integral closure of R in L_t , G_t denotes the Galois group of L_t over k , and f_t is the image of f under the inflation map $Z^2(G, U(L)) \rightarrow Z^2(G_t, U(L_t))$.

Proof. Let e denote the Brauer number of $\tilde{\Sigma}$. Since e is relatively prime to p , it follows that the extension $L(\xi)$ of L is unramified where ξ denotes a primitive e^{th} root of unity. Next let Π denote a root of the polynomial $X^e - \pi$ where π is the prime element of R . Define $L_t = L(\xi, \Pi)$. It is easy to verify that the field L_t is a tamely ramified Galois extension of k .

Let S denote the integral closure of R in L , and S_t the integral closure of R in L_t . It remains to construct a 2-cocycle g of $Z^2(G_t, U(L_t))$ such that g is cohomologous to f_t and such that g is in the image of the natural map $Z^2(G_t, U(S_t)) \rightarrow Z^2(G_t, U(L_t))$. Since the image of $[f]$ in $H^2(G, Z^+)$ has order e , it follows that there exists a map $\phi: G \rightarrow U(L)$ such that the 2-cocycle h of $Z^2(G, U(L))$ defined by $h(\sigma, \tau) = f^e(\sigma, \tau)\phi(\sigma\tau)/\phi(\sigma)\phi(\tau)$ takes values in $U(S)$. Write the element $\phi(\sigma)$ of $U(L)$ in the form $\phi(\sigma) = \alpha_\sigma \pi^{\beta(\sigma)}$ where α_σ is in $U(S)$ and $\beta(\sigma)$ is an integer. Define the map $\phi_t: G_t \rightarrow U(L_t)$ by $\phi_t(\sigma) = \Pi^{\beta(\bar{\sigma})}$ where $\bar{\sigma}$ denotes the image of σ under the natural map of G_t onto G . Define the element g of $Z^2(G_t, U(L_t))$ by $g(\sigma, \tau) = f_t(\sigma, \tau)\phi_t(\sigma\tau)/\phi_t(\sigma)\phi_t(\tau)$. Proceeding as in the proof of Prop. 2.4 one may easily verify

that $g^e(\sigma, \tau) = h(\sigma, \tau)\alpha_\sigma\alpha_\tau^e / \alpha_{\sigma\tau}$ from which it follows that the 2-cocycle g takes values in $U(S_t)$.

PROPOSITION 4.2. *If Σ is a central simple k -algebra for which $\tilde{\Sigma}$ is in $T(k)$, then a maximal order in Σ is equivalent to a crossed product over a tamely ramified extension of R .*

Proof. Consider a representative $\mathcal{A}(f, L, G)$ of $\tilde{\Sigma}$ where L is an unramified extension of k . Since $\tilde{\Sigma}$ is in $T(k)$ we may consider a field L_t satisfying the conclusion of Lemma 4.1. Theorem 2.3 of [11] now implies that a maximal order in $\mathcal{A}(f, L, G)$ is equivalent to a crossed product over a tamely ramified extension of R .

In order to prove the main theorem in the other direction we first prove two propositions.

PROPOSITION 4.3. *If a central simple k -algebra Σ is equivalent to a crossed product over a tamely ramified extension of k , then $\tilde{\Sigma}$ is in $V(k)$.*

Proof. According to the hypothesis we may consider a crossed product $\mathcal{A}(f, L, G)$ equivalent to Σ for which the extension L of k is tamely ramified. Let G_I denote the inertia group of L over k and let f_I denote the image of f under the restriction map $Z^2(G, U(L)) \rightarrow Z^2(G_I, U(L))$. We show first of all that f may be replaced by a 2-cocycle g whose restriction to $G_I \times G_I$ is normalized in the sense of cyclic groups. Consider a 2-cocycle g_I in $Z^2(G_I, U(L))$ which is cohomologous to f_I and which is normalized in the sense of cyclic groups. Let $\phi_I: G_I \rightarrow U(L)$ be a map for which $g_I(\sigma, \tau) = f_I(\sigma, \tau)\phi_I(\sigma)\phi_I^e(\tau) / \phi_I(\sigma\tau)$ for σ and τ in G_I . Extend ϕ_I to a map $\phi: G \rightarrow U(L)$ by defining $\phi(\sigma) = \phi_I(\sigma)$ for σ in G_I and $\phi(\sigma) = 1$ for σ in $G - G_I$. Then the 2-cocycle g of $Z^2(G, U(L))$ defined by $g(\sigma, \tau) = f(\sigma, \tau)\phi(\sigma)\phi^e(\tau) / \phi(\sigma\tau)$ is cohomologous to f and its restriction to $G_I \times G_I$ is normalized in the sense of cyclic groups. Since $[f] = [g]$ it follows that $\mathcal{A}(f, L, G)$ is k -algebra isomorphic to $\mathcal{A}(g, L, G)$.

Let L_I denote the fixed field of G_I and let a denote the element of $U(L_I)$ which defines the 2-cocycle g_I . Since L is a tamely ramified inertial extension of L_I , the natural map $H^2(G_I, U(S)) \rightarrow H^2(G_I, U(L))$ is an epimorphism, where S denotes the integral closure of R in L (see the proof of Cor. 2.4 of [11]). We may therefore assume that a is in $U(U)$ where U denotes the inertia ring of L over k .

We proceed to construct an unramified extension of L which will give rise to an unramified splitting field of Σ . Let e denote the order of G_I and consider the element \bar{a} of $U(\bar{U})$. Denote the order of \bar{a} in $U(\bar{U})/[U(\bar{U})]^e$ by e/m . There exists an element \bar{c} in $U(\bar{U})$ such that $\bar{a} = \bar{c}^m$, and the polynomial $X^{e/m} - \bar{c}$ is irreducible in $\bar{U}[X]$ (see the proof of Prop. 2.2 of [10]). Applying Hensel's lemma we may conclude that there exists an element c in $U(U)$ for which $c^m = a$. Observe that the polynomial $P(X) = X^m - c$ is irreducible in $L[X]$, and let $L(\alpha)$ be the field obtained by adjoining a root α of $P(X)$ to L . Since L_I contains a primitive e^{th} root of unity, it is clear that $L(\alpha)$ is a Galois extension of k . It is easy to see that $L(\alpha)$ is an unramified extension of L . For let S denote the integral closure of R in L and consider the ring $S[\alpha]$ where the brackets denote ring adjunction. According to Cor. 2 p. 66 of [7], the different D of $S[\alpha]$ over S is the principal ideal $(P'(\alpha))$. Since $P'(X) = (e/m)X^{(e/m)-1}$ it follows that $D = S[\alpha]$ since $(p, e/m) = 1$ and α is a unit in $S[\alpha]$. Hence $S[\alpha]$ is an unramified extension of S and is therefore integrally closed in $L(\alpha)$.

We establish some notation which shall be used in the remainder of the proof. Let G_α denote the Galois group of $L(\alpha)$ over k ; let G_{I_α} denote the inertia group of $L(\alpha)$ over k , and let L_{I_α} and U_α denote the inertia field and the inertia ring (respectively) of $L(\alpha)$ over k . Finally, denote by g_α the image of g under the inflation map $Z^2(G, U(L)) \longrightarrow Z^2(G_\alpha, U(L(\alpha)))$ and observe that the crossed product $\mathcal{A}(g_\alpha, L(\alpha), G_\alpha)$ is equivalent to $\mathcal{A}(f, L, G)$.

The extension $L(\alpha)$ of L has been constructed so that g_α shall be cohomologous to the trivial 2-cocycle on $G_{I_\alpha} \times G_{I_\alpha}$. For since the image of G_{I_α} under the natural map of G_α onto G is G_I , it follows from the definition of the inflation map that g_{I_α} is defined by the element a of $U(U)$ where g_{I_α} denotes the image of g under the restriction map $Z^2(G_\alpha, U(L(\alpha))) \longrightarrow Z^2(G_{I_\alpha}, U(L(\alpha)))$. It remains to show that $a \equiv 1 \pmod{N(U(L(\alpha)))}$ in $U(L_{I_\alpha})/N(U(L(\alpha)))$. Since $\alpha^e = a$ and α is in $U(U_\alpha)$ we have that $N(\alpha) = a$, and therefore g_{I_α} is cohomologous to 1.

Now we may complete the proof of the proposition. Since $H^1(G_I, U(L(\alpha))) = (1)$ according to Prop. 2 p. 158 of [7] it follows from Prop. 5 p. 126 of [7] that the sequence

$$(1) \longrightarrow H^2(G_\alpha / G_{I_\alpha}, U(L_{I_\alpha})) \xrightarrow{\text{inf}} H^2(G_\alpha, U(L(\alpha))) \longrightarrow H^2(G_{I_\alpha}, U(L(\alpha)))$$

is exact. Therefore the fact that $\text{res } [g_\alpha] = [1]$ implies that there exists a 2-

cocycle h in $Z^2(G_\alpha / G_{I_\alpha}, U(L_{I_\alpha}))$ such that $\text{inf } [h] = [g_\alpha]$. Now the crossed product $\Delta(h, L_{I_\alpha}, G_\alpha / G_{I_\alpha})$ is equivalent to $\Delta(g_\alpha, L(\alpha), G_\alpha)$ and therefore to Σ . Since L_{I_α} is an unramified extension of k , we have proved that $\widetilde{\Sigma}$ is in $V(k)$.

PROPOSITION 4.4. *Let k denote the quotient field of a complete discrete rank one valuation ring R , L a finite Galois extension of k with Galois group G , and f an element of $Z^2(G, U(L))$. If a maximal order Γ in $\Delta(f, L, G)$ is equivalent to a crossed product over a tamely ramified extension of R , then a maximal order Γ_x in $\Delta(f^x, L, G)$ is equivalent to a crossed product over a tamely ramified extension of R for every positive integer x .*

Proof. Suppose that Γ is equivalent to the crossed product $\Delta(g, S_t, G_t)$ where S_t is a tamely ramified extension of R , and G_t is the Galois group of the quotient field extension L_t of k . The first step is to prove inductively that the central simple k -algebra $\Delta(f^x, L, G)$ is equivalent to $\Delta(g^x, L_t, G_t)$. For $x=1$ the assertion is trivial. So assume now that $\Delta(f^{x-1}, L, G)$ is equivalent to $\Delta(g^{x-1}, L_t, G_t)$. Now $\Delta(f^{x-1}, L, G) \otimes_k \Delta(f, L, G)$ is equivalent to $\Delta(f^x, L, G)$ and similarly $\Delta(g^{x-1}, L_t, G_t) \otimes_k \Delta(g, L_t, G_t)$ is equivalent to $\Delta(g^x, L_t, G_t)$ (see Thm. 8.5 A p. 86 of [1]). We may conclude therefore from the induction hypothesis that $\Delta(f^x, L, G)$ is equivalent to $\Delta(g^x, L_t, G_t)$.

A maximal order Γ_x in $\Delta(f^x, L, G)$ is equivalent to a maximal order Ω_x in $\Delta(g^x, L_t, G_t)$ according to Lemma 2.1 of [11]. However, the fact that S_t is a tamely ramified extension of R , together with the fact that g is in $Z^2(G_t, U(S_t))$ implies that Ω_x is equivalent to a crossed product over a tamely ramified extension of R by Thm. 2.3 of [11].

Now we may complete the proof of the main theorem.

THEOREM 4.5. *Let k denote the quotient field of a complete discrete rank one valuation ring R , and let Γ be a maximal order in a central simple k -algebra Σ . Then Γ is equivalent to a crossed product over a tamely ramified extension of R if and only if the Brauer class $\widetilde{\Sigma}$ is in the subgroup $T(k)$ of $B(k)$.*

Proof. If $\widetilde{\Sigma}$ is in $T(k)$, then a maximal order in Σ is equivalent to a crossed product over a tamely ramified extension of R according to Prop. 4.2.

On the other hand, assume now that Γ is equivalent to a crossed product over a tamely ramified extension of R . Then $\widetilde{\Sigma}$ is in $V(k)$ according to Prop. 4.3, so that $\widetilde{\Sigma}$ may be represented by a crossed product

$\mathcal{A}(f, L, G)$ where L is an unramified extension of k . We prove by contradiction that the Brauer number n of $\tilde{\Sigma}$ must be relatively prime to p . The assertion is trivial when \bar{R} has characteristic zero. We assume therefore that n is divisible by $\text{char } \bar{R} = p \neq 0$, and write n in the form $n = mp^t$ where m is relatively prime to p and $t \geq 1$. Consider the central simple k -algebra $\Sigma_{n/p} = \mathcal{A}(f^{n/p}, L, G)$ and observe that the Brauer number of $\tilde{\Sigma}_{n/p}$ is p . If a maximal order in $\mathcal{A}(f, L, G)$ were equivalent to a crossed product over a tamely ramified extension of R , then a maximal order Ω in $\mathcal{A}(f^{n/p}, L, G)$ would be equivalent to a crossed product over a tamely ramified extension of R according to Prop. 4.4. But Ω cannot be equivalent to such a crossed product because the Brauer number of $\tilde{\Sigma}_{n/p}$ is p (see Thm. 3.16). This contradiction completes the proof of the theorem.

COROLLARY 4.6. *Let k denote the quotient field of a complete discrete rank one valuation ring R whose residue class field \bar{R} is perfect, and let Γ denote a maximal order in a central simple k -algebra Σ . Then the following statements are equivalent*

- i) Γ is equivalent to a crossed product over a tamely ramified extension of R
- ii) Γ is equivalent to a crossed product
- iii) the Brauer number of $\tilde{\Sigma}$ is relatively prime to the characteristic of \bar{R} .

Proof. The equivalence of i) and ii) follows from Theorem 2 of [6] since a maximal order is hereditary and \bar{R} is perfect. The equivalence of i) and iii) follows from the theorem.

COROLLARY 4.7. *Let R denote a complete discrete rank one valuation ring. If R is an equicharacteristic ring of characteristic zero, then every maximal order over R is equivalent to a crossed product over a tamely ramified extension of R .*

Proof. This assertion follows immediately from Thm. 4.5 since $T(k) = B(k)$ when R is an equicharacteristic ring of characteristic zero.

COROLLARY 4.8. *There exist maximal orders which are not equivalent to crossed products.*

Proof. Let R denote the ring of p -adic integers Z_p , and k the quotient field of R . In Remark 1.5 we observed that $T(k)$ is properly contained in $V(k)$. Since \bar{R} is perfect, it follows from Cor. 4.6 that not every maximal order is equivalent to a crossed product.

REFERENCES

- [1] E. Artin, C. Nesbitt and R. Thrall, *Rings with Minimum Condition*. Michigan, (1955).
- [2] E. Artin and J. Tate, *Class field theory*. Princeton notes, 1951. distributed by Harvard Univ.
- [3] M. Auslander and O. Goldman, *The Brauer group of a commutative ring*, Trans. Amer. Math. Soc. Vol. **97** (1960), pp. 367–409.
- [4] M. Auslander and O. Goldman, *Maximal orders*, Trans. Amer. Math. Soc. Vol. **97** (1960), pp. 1–24.
- [5] M. Harada, *Hereditary orders*, Trans. Amer. Math. Soc. Vol. **107** (1963), pp. 273–290.
- [6] M. Harada, *Some criteria for heredity of crossed products*, Osaka J. Math. Vol. **1** (1964), pp. 69–80
- [7] J.P. Serre, *Corps Locaux*, Paris, Hermann, (1962).
- [8] B.L. van der Waerden, *Modern Algebra*, Vol. **1**, Ungar, (1953).
- [9] E. Weiss, *Algebraic Number Theory*, McGraw-Hill Co., (1963).
- [10] S. Williamson, *Crossed products and hereditary orders*, Nagoya Math. J. Vol. **23** (1963), pp. 103–120.
- [11] S. Williamson, *Crossed products and maximal orders*, Nagoya Math. J. Vol. **25** (1965), pp. 165–174.
- [12] S. Williamson, *Crossed products and ramification*, Nagoya Math. J. Vol. **28** (1966) pp. 85–111.
- [13] A. Brumer, *The structure of hereditary orders*, Ph.D. Thesis, Princeton Univ., (1963).

Regis College
Weston, Massachusetts

