ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 20, Number 1, Winter 1990

AZUMAYA ALGEBRAS WHICH ARE NOT SMASH PRODUCTS

LINDSAY N. CHILDS

Let R be a commutative ring, let H be an R-Hopf algebra (always with antipode), finitely generated and projective as an R-module, and let $H^* = \mathrm{Hom}_R(H, R)$ be the dual Hopf algebra. Let $\mathrm{Gal}(H)$ denote the set of isomorphism classes (as R-algebras and H-modules) of Galois H-extensions (that is, Galois H^*-objects, in the sense of [**3**, §7]). Let $\mathrm{Az}(R)$ denote the set of isomorphism classes (as R-algebras) of Azumaya R-algebras. Gamst and Hoechsmann [**15**] showed that if S is a Galois H-extension and T a Galois H^*-extension, then the smash product $S \# T$ is an Azumaya R-algebra, so yields a map

$$\# : \mathrm{Gal}(H) \times \mathrm{Gal}(H^*) \to \mathrm{Az}(R)$$

given by $[S] \times [T] \mapsto [S \# T]$.

The smash product generalizes the cyclic crossed product. As we will show in §2 below, for rank 2 Hopf algebras, Sweedler's crossed product based on Hopf algebra cohomology also is a special case of the smash product.

Let $\mathrm{Br}(R)$ be the Brauer group of R, and $\{\ \}$ denote the class map, $\mathrm{Az}(R) \to \mathrm{Br}(R)$. If H is commutative and cocommutative, then $\mathrm{Gal}(H)$ and $\mathrm{Gal}(H^*)$ are abelian groups, and $\{\ \#\ \}$ is bilinear. (See [**15**] for an interpretation of $\{\ \#\ \}$ as a cup product map.) In the special case where R is a field containing $1/n$ and a primitive n^{th} root of unity and $H = RG$, G cyclic of order n, then $H \cong H^*$, $\mathrm{Gal}(H) \cong U(R)/U(R)^n$ and the smash product map $\{\ \#\ \}$ specializes to the norm residue map which Merkurjev and Suslin showed maps onto the n-torsion part of the Brauer group.

Thus, over number fields, every Azumaya algebra is isomorphic to a smash product, and over many fields every Azumaya algebra is at least similar to a product of smash products.

Received by the editors on February 25, 1987 and in revised form on April 30, 1987.

Over commutative rings the smash product is a much less effective construction. The purpose of this paper, a sequel to [**7**], is to indicate how inadequate the smash product is for describing Azumaya algebras over number rings.

Let K be a number field with ring of integers R. Consider the smash product maps

$$\mathrm{Gal}(H) \times \mathrm{Gal}(H^*) \to \mathrm{Az}_2(R)$$

for all possible Hopf R-algebras H of rank 2, where $\mathrm{Az}_2(R)$ is the set of isomorphism classes of rank four Azumaya R-algebras. We show

THEOREM 4.1. *Let n be an even integer. With at most finitely many exceptions, for every totally real number field K of dimension $n = [K : \mathbf{Q}]$, there exists an isomorphism class of rank 4 Azumaya algebras over the ring of integers of K which is not representable by a smash product.*

Theorem 4.1 applies in particular to real quadratic fields. However, for R the ring of integers of $K = \mathbf{Q}(\sqrt{p})$, p a prime, we obtain a precise count of the number of isomorphism classes of Azumaya algebras of rank 4 which are smash products (there are at most 3 such), and show that there are rank 4 Azumaya algebras which are not isomorphic to smash products for all primes $p > 3$. In particular, if $p \equiv 1 \pmod 4$, there are no non-trivial smash products.

DeMeyer and Ford [**9**] have found commutative rings arising in a geometric context for which the Merkurjev-Suslin theorem fails. Our results for the ring of integers of $\mathbf{Q}(\sqrt{p}), p \equiv 1 \pmod 4$ show that the analogue of the Merkurjev-Suslin theorem for smash products over these rings is not valid.

2. Crossed products and smash products. The term "smash product" is used in two different contexts in the literature.

If S is a Galois H-extension and T a Galois H^*-extension, then the smash product $S \# T$ is the R-module $S \otimes_R T$ with multiplication

$$(s \# t) \cdot (s' \# t') = \sum_{(s')(t)} s s'_{(1)} \# \langle t_{(2)}, s'_{(2)} \rangle t_{(1)} t',$$

where the map $S \to S \otimes H^*$ induced from the H-action on S is given by $s \mapsto \sum_{(s)} s_{(1)} \otimes s_{(s)}$ (Sweedler's notation) and similarly for the map $T \to T \otimes H$, and $\langle\ ,\ \rangle$ is the evaluation map from $H \otimes H^*$ to R. See [**15**, **2**].

On the other hand, Sweedler in [**27**] considers the analogue for Hopf algebra cohomology of the crossed product map in group cohomology, and calls it a smash product, namely $S \#_f H$, where S is an H-Galois extension and $f : H \otimes H \to S$ is a 2-cocycle. Here $S \#_f H = S \otimes H$ as R-module, with multiplication

$$(2.1) \qquad (s \otimes h) \cdot (s' \otimes h') = \sum_{(h),(h')} s(h_{(1)} \cdot s') f(h_{(2)} \cdot h'_{(1)}) \otimes h_{(3)} h'_{(2)}.$$

We will call this the crossed product associated to the cocycle f.

If $H = RG$, G a finite cyclic group, then, as is well known, every 2-cocycle $f : G \times G \to U(S)$, $U(S)$ = group of units of S, is cohomologous to a cocycle with image in R, from which it follows that any crossed product $S \#_f RG$ is isomorphic to a smash product $S \# T$, T a Galois RG^*-extension. We show that the same is true for rank 2 Hopf algebras. The result for rank p Hopf algebras, p an odd prime, if true, appears to be more difficult, and is not needed below.

Notation. If $2 = ab$ in R, H_b is the free rank 2 Hopf R-algebra of the form $H_b = R[x]$, where $x^2 = bx$ and $\Delta(x) = x \otimes 1 + 1 \otimes x - a(x \otimes x)$ $(= \sum_{(x)} x_{(1)} \otimes x_{(2)}$, by definition) [**21**, **28**]. In particular, $H_1 = RG^* = \operatorname{Hom}_R(RG, R)$, and $H_2 = RG$.

THEOREM 2.2. *Let R be an integrally closed Noetherian domain and let H be a Hopf R-algebra which is projective of rank 2 as R-module, S a Galois H-extension of R, and $f : H \otimes H \to S$ a Sweedler 2-cocycle. Then there exists a Galois H^*-extension T so that $S \#_f H \cong S \# T$ as R-algebras.*

PROOF. Let $f : H \times H \to S$ be a 2-cocycle. If f is normalized, that is, $f(y, z) = \varepsilon(y)\varepsilon(z)$ if either y or z is in R, then, we claim f must have its values in R. Since R is the intersection of its localizations at the prime ideals of R, it suffices to show that the image of f is in R assuming that R is local. In that case, H is a free R-module, $H = H_b = R[x], x^2 = bx$ for some b in R.

If $f : H \otimes H \to S$ is a normalized 2-cocycle, then, since $\varepsilon(x) = 0$, we have $f(1,1) = 1, f(1,x) = f(x,1) = 0$, and f is completely determined by $f(x,x)$.

Now f is a cocycle if, for all y, z, w in H, we have

$$\sum (y_{(1)} \cdot f(z_{(1)}, w_{(1)}))f(y_{(2)}, z_{(2)}w_{(2)}) = \sum f(y_{(1)}z_{(1)}, w)f(y_{(2)}, z_{(2)}).$$

Explicitly computing this equation with y, z, and w all equal to x, it can be verified that $x \cdot f(x,x) = 0$, which means that $f(x,x)$ is in the fixed ring $S^H = R$.

We now rewrite the multiplication in $S \#_f H$.

The action of H on S may be described in terms of the H^*-comodule structure on S by

$$h \cdot s = \sum_{(s)} s_{(1)} \langle h, s_{(2)} \rangle.$$

Thus, since the cocycle f has values in R, we may rewrite formula (2.1) above as

$$(s \otimes h) \cdot (s' \otimes h') = \sum ss'_{(1)} \otimes \langle h_{(1)}, s_{(2)} \rangle f(h_{(2)}, h'_{(1)}) h_{(3)} h'_{(2)}.$$

It remains to identify H with multiplication

$$h \cdot h' = \sum_{(h)(h')} f(h_{(1)}, h'_{(1)}) h_{(2)} h'_{(2)}$$

as a Galois H^*-extension. But this is exactly how Galois H^*-extensions ($= H$-Galois algebras, in the terminology of [**11**]) with normal basis are defined in Proposition 1.6 of Early and Kreimer [**11**]. If we call H with multiplication altered by f by H_f, then $S \#_f H = S \# H_f$, the smash product of S and the Galois H^*-extension H_f. □

As a consequence of this theorem, an upper bound on the number of isomorphism classes of smash products is also an upper bound on the number of isomorphism classes of crossed products.

3. Bounding the number of smash products.

THEOREM 3.1. *Let R be the ring of integers of a number field K. Then the number of isomorphism classes of rank 4 Azumaya R-algebras which are smash products is bounded by a constant depending only on $n = [K : Q]$ and the size of the 2-torsion part of the class group of R.*

PROOF. From Corollary 17.6 of [**5**], if S is a Galois H-extension, there is a unique Galois H_1-extension S_1 contained in S, and, given a Galois H_1-extension S_1 and a rank 2 Hopf algebra H, there is at most one H-Galois extension S containing S_1. The number of isomorphism classes of Galois H_1-extensions of R is given by $|\mathrm{U}(R)/\mathrm{U}(R)^2| \cdot |\mathrm{Cl}_2(R)| = f$, where $\mathrm{U}(R)$ denotes the units of R and $\mathrm{Cl}_2(R)$ the elements of the class group of R of order 2. The number of rank 2 Hopf algebras is bounded by $e = \prod_{i=1}^{g}(e_i + 1)$, where the factorization of the ideal $2R$ into primes is given by $2R = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$, by Proposition 3.3 of [**5**]. Thus the number of isomorphism classes of smash products is bounded above by $e \cdot f^2$. By the Dirichlet Units Theorem, the order of the group of units $|\mathrm{U}(R)/\mathrm{U}(R)^2|$ is bounded above by 2^{n+1}, and e is bounded (rather crudely) by $(n+1)^n$. □

COROLLARY 3.2. *Let R be the ring of integers of $\mathbf{Q}(\sqrt{m})$. Then the number s of isomorphism classes of rank 4 smash products over R satisfies $s \leq 64 \cdot 2^{2r} = 2^{2r+6}$, where r is the number of primes dividing m.*

For $|\mathrm{U}(R)/\mathrm{U}(R)^2| = 4$,

$$e = \begin{cases} 3, & \text{if } m \equiv 2 \text{ or } 3 (\mathrm{mod}\, 4), \\ 4, & \text{if } m \equiv 1 (\mathrm{mod}\, 8), \\ 2, & \text{if } m \equiv 5 (\mathrm{mod}\, 8), \end{cases}$$

and (c.f., [**8**, **14**]) $|\mathrm{Cl}_2(R)| \leq 2^r$.

In certain cases this bound can be much improved, as we shall see in §5.

4. Applying the Eichler class number formula.

THEOREM 4.1. *Let n be an even integer. With finitely many exceptions, for every totally real number field K of dimension $n = [K : \mathbf{Q}]$, there exists an isomorphism class of rank 4 Azumaya algebras over the ring of integers of K which is not representable by a smash product.*

PROOF. For any number field K with ring of integers R, the number s of smash products is bounded by $\kappa \cdot |\mathrm{Cl}_2(R)|^2$ where κ depends only on n. Let $|\mathrm{Cl}_2(R)| = h_2$. Then $h_2 \leq h_o$, the class number of K. Any class in the class group of K has an integral ideal with norm $\leq (2/\pi)^2 \cdot \sqrt{D} = D_1$, where D is the discriminant of K [**1**, p. 222]. So h_o is $\leq$ the number of integral ideals with norm $\leq D_1$. Now the number of ideals with norm $\leq D_1$ is bounded by $\sum_{a=1}^{D_1} d(a)^n$, where $d(a)$ is the number of divisors of a [**1**, p. 220], and, for any $\varepsilon > 0$, there exists some c so that, for all a, $d(a) \leq ca^{\varepsilon}$ [**17**, Theorem 315]. So

$$\begin{aligned}\sum_{a=1}^{D_1} d(a)^n &\leq d(b)^n \cdot D_1, \quad \text{for some } b \leq D_1, \\ &\leq c^n b^{\varepsilon n} D_1 \\ &\leq c^n D_1^{1+\varepsilon n}.\end{aligned}$$

Thus $s \leq \kappa h_2^2 \leq \kappa (c^n D_1^{1+\varepsilon n})^2 = kc^{2n} D^{1+\varepsilon n}$ for some constants k, κ, and, so, for fixed n and any $\varepsilon > 0, s \leq \mathrm{O}(D^{1+\varepsilon})$.

Now let $\mathbf{H}(K)$ be a totally definite quaternion algebra over K with invariants $1/2$ at all the infinite primes of K and 0 at all the finite primes [**23**, p. 293]. Then $\mathbf{H}(K)$ is in the image of the 1-1 map from $\mathrm{Br}(R)$ to $\mathrm{Br}(K)$ [**22**, p. 78]. Let t be the number of isomorphism types of maximal orders, all Azumaya R-algebras, in $\mathbf{H}(K)$.

To investigate t, we use Eichler's class number formula [**12**]:

$$\frac{2h_0\zeta_K(2)|D|^{3/2}}{(2\pi)^{2n}} \prod_{p|\partial} (Np - 1) = \sum_{\nu} \frac{1}{w_\nu} \tag{4.2}$$

(note a misprint in the formula as reproduced in [**26**]), where

$$\partial = \text{ the discriminant ideal of } \mathbf{H}(K)$$

(that is, the discriminant of a maximal order of $\mathbf{H}(K)$, which is 1 since the maximal orders in $\mathbf{H}(K)$ are Azumaya)

$$\begin{aligned} h_0 &= \text{ class number of } K \\ D &= \text{ discriminant of } K \\ n &= \text{ degree of } K \text{ over } \mathbf{Q}, \text{ which } \textit{equals } 2 \\ \zeta_K(s) &= \text{ Dedekind zeta function of } K. \end{aligned}$$

Let A be a maximal order in $\mathbf{H}(K)$, $J_1, \ldots, J_h$ be a set of representatives of the h isomorphism classes of left ideals of A, and $A_1, \ldots, A_h$ be the right orders of $J_1, \ldots, J_h$ (all maximal by [**10**; page 75, Satz 12]). Then $w_\nu = [U(A_\nu) : U(R)]$ for $\nu = 1, \ldots, h$.

We may simplify the right side of (4.2) as follows. If h is the class number of $\mathbf{H}(K)$, then

$$h \sum_{i=1}^{t} |P_R(B_i)|,$$

where B_i runs through a set of representatives for the t isomorphism classes of maximal orders of $\mathbf{H}(K)$ and $P_R(B)$ is the group of isomorphism classes of projective left B-modules P with $\mathrm{Hom}_B(P,P)^{\mathrm{opp}} = B$ [**6**].

We have the short exact sequence

$$1 \to \mathrm{Out}(B) \to \mathrm{Cl}(R) \to P_R(B) \to 1 \quad [\mathbf{24}] \tag{4.3}$$

where $\mathrm{Out}(B)$ is the group of R-algebra automorphisms of B modulo inner automorphisms. Hence $|P_R(B)| \leq h_0$ for each B, and the right side of (4.2) may be written as

$$\sum_{\nu=1}^{h} \frac{1}{w_\nu} = \sum_{i=1}^{t} \sum_{|P_R(B_i)|} \frac{1}{w_i} \leq h_0 \sum_{i=1}^{t} \frac{1}{w_i} \leq h_0 t,$$

where $w_i = [U(B_i) : U(R)]$. Thus (4.2) becomes

$$\frac{2\zeta_K(2)|D|^{3/2}}{(2\pi)^{2n}} \leq t.$$

Now, for all K,

$$\zeta_K(2) = \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^2},$$

(where the sum runs over all integral ideals of R)

$$\geq \sum_{a=2}^{\infty} \frac{1}{N(aR)^2} = \sum_{a=2}^{\infty} \frac{1}{a^{2n}} > \frac{1}{4^n}.$$

Hence, for n fixed, $t \geq \mathrm{O}(D^{3/2})$. Thus, for all sufficiently large discriminants D, $t > s$. Since (Hermite [**1**, page 129]) there exist only a finite number of fields $K, [K : \mathbf{Q}] = n$, with given discriminant D, it follows that, for each n, we have $t > s$ for all but a finite number of totally real fields K with $[K : \mathbf{Q}] = n$. □

5. Smash products over $\mathbf{Z}[\sqrt{\mathbf{p}}]$. The bound of §3 for the number of isomorphism classes of smash products can be much improved in certain cases. In this section we will compute the number of such classes in case $R = \mathbf{Z}[\sqrt{p}], K = \mathbf{Q}(\sqrt{p})$, where p is a prime. For such R, the bound of §3 is 32, 48 or 64, depending on whether $p \equiv 5 (\mathrm{mod}\, 8)$, $\equiv 2$ or $3 (\mathrm{mod}\, 4)$, or $\equiv 1 (\mathrm{mod}\, 8)$ (i.e., depending on whether the ideal (2) remains prime, ramifies or splits in R), since the class group of R is odd [**8**, **14**]. In fact, however, we have

THEOREM 5.1. *Let R be the ring of integers of $K = \mathbf{Q}(\sqrt{p}), p$ prime. The number of isomorphism classes of Azumaya R-algebras of rank 4 which are smash products is*

$$\begin{cases} 3, & \text{if } p \equiv 3 (\mathrm{mod}\, 4) \\ 2, & \text{if } p = 2 \\ 1, & \text{if } p \equiv 1 (\mathrm{mod}\, 4). \end{cases}$$

PROOF. First, there is, up to isomorphism, a unique maximal order (which is Azumaya) in $\mathrm{End}_K(K^2)$, the trivial rank 4 Azumaya K-algebra. This follows, since the class number h is odd, by results of Eichler and Schilling (e.g., [**25**] or [**6**, page 48]), or by a direct argument. This maximal order is represented by the trivial smash product $RG^* \# RG \cong \mathrm{End}_R(RG^*)$.

We now determine the number of smash products which are maximal orders in the quaternion algebra $\mathbf{H}(K)$ which is the image in $\mathrm{Br}(K)$ of the non-trivial class in $\mathrm{Br}(R)$. If $K = \mathbf{Q}[\sqrt{m}], m$ squarefree, and $m \not\equiv 1 (\mathrm{mod}\, 8), \mathbf{H}(K)$ is the usual quaternion algebra; if $m \not\equiv 1 (\mathrm{mod}\, 8), \mathbf{H}(K)$ is the algebra generated by u and v with $uv = -vu, u^2 = -1, v^2 = -q$, where q is a prime $\equiv 3 (\mathrm{mod}\, 4)$ such that $\left(\frac{m}{q}\right) = -1$ [**13**].

The Hopf R-algebras of rank 2 correspond to the ideal factors of the ideal $2R$ [**5**, Proposition 3.3]. If $\mathfrak{b}$ is an ideal dividing $2R$, denote by $H_{\mathfrak{b}}$ the corresponding Hopf R-algebra. If $\mathfrak{b}\mathfrak{c} = 2R$, then $H_{\mathfrak{b}}$ and $H_{\mathfrak{c}}$ are dual (i.e., $H_{\mathfrak{c}} = H_{\mathfrak{b}}^*$). If $\mathfrak{b} = \mathfrak{b}R$, write $H_{\mathfrak{b}} = H_{\mathfrak{b}}$.

There are four isomorphism classes of H_1-Galois extensions. These are orders over R in $L = K[z]$ where $z^2 = 1, -1, \varepsilon$ or $-\varepsilon$, ε the fundamental unit of R. These four elements of R generate the group $\mathrm{U}(R)/\mathrm{U}(R)^2$ which classifies Galois H_1-extensions with normal basis [**21**, **19**]. Since R has odd class number, every Galois H_1-extension has normal basis [**3**]. Denote the Galois H_1-extension contained in $L = K[z], z^2 = w$, by $S_1(w)$.

If S is a Galois $H_{\mathfrak{b}}$-extension, then there exists a unique Galois H_1-extension S_1 contained in S [**5**, Theorem 17.5]). Thus any Galois $H_{\mathfrak{b}}$-extension S must be an order over R in $L = K[z], z^2 = 1, -1, \varepsilon, -\varepsilon$, as before. If there exists such a Galois $H_{\mathfrak{b}}$-extension contained in $L = K[z], z^2 = w$, denote it by $S_{\mathfrak{b}}(w)$.

If $A = S_{\mathfrak{b}}(w) \# S_{\mathfrak{b}'}(w')$ then $H_{\mathfrak{b}'} \cong H_{\mathfrak{b}}^*$, so $\mathfrak{b}' = 2R \cdot \mathfrak{b}^{-1}$. If $A \otimes K \cong \mathbf{H}(K)$, we must have $w, w' < 0$; otherwise, $A \otimes K$ is split (c.f. [**7**]). Thus w and w' must be in the set $\{-1, -\varepsilon\}$. □

LEMMA 5.2. [**5**; Propositions 12.2, 13.4]. *Let $\mathfrak{p}$ be a prime divisor of $2R, R_{\mathfrak{p}}$ be the localization of R at $\mathfrak{p}, \mathfrak{p}R_{\mathfrak{p}} = \pi R_{\mathfrak{p}}$, and $\mathfrak{b}$ be a divisor of $2, \mathfrak{b}_{\mathfrak{p}} = \mathfrak{p}^q R_{\mathfrak{p}}$. If w is in $\mathrm{U}(R)$, then there exists a Galois $H_{\mathfrak{b}}$-extension $S_{\mathfrak{b}}(w)$ if and only if $ws^2 = 1 + \pi^{2q+1}u$ for some u in $R_{\mathfrak{p}}$ and some s in K.*

We now consider various cases, depending on p.

$p \equiv 3 (\mathrm{mod}\, 4)$. In this case, $2R = \mathfrak{b}^2 R$, the square of a principal ideal. Thus we have three Hopf R-algebras of rank $2, H_1, H_{\mathfrak{b}}$ and H_2. We

may choose $\mathfrak{b}$ so that $\mathfrak{b}^2 = 2\varepsilon$, ε the fundamental unit of R (see Lemma 6.3 below). H_1 and H_2 are dual (i.e., $H_2 \cong H_1^*$) and $H_{\mathfrak{b}}$ is self-dual.

Since the extension $K[i]/K$ is unramified at all finite primes, the ring of integers of $K[i]$ is a Galois H_2-extension, hence is $S_2(-1)$. Thus, by Lemma 5.2, $-s^2 = 1 + \mathfrak{b}^5 u$ for some u in $R_{\mathfrak{b}}, s$ in K, and so, again by Lemma 5.2, there are three Galois H-extensions contained in $K[z], z^2 = -1$, namely $S_1(-1), S_{\mathfrak{b}}(-1)$ and $S_2(-1)$. There is a unique Galois H-extension in $K[z], z^2 = -\varepsilon$, namely the Galois H_1-extension $S_1(-\varepsilon) = R[z], z^2 = -\varepsilon$. One sees this by utilizing the fact that $\mathfrak{b}$ may be chosen with $\mathfrak{b}^2 = 2\varepsilon$ to show that $\varepsilon \equiv \sqrt{p} (\mathrm{mod}\, 2R)$ (hence $-\varepsilon = 1+(1-\sqrt{p})+2u$ for some u) and $\mathfrak{b}R_{\mathfrak{b}} = (1-\sqrt{p})R_{\mathfrak{b}}$. If $-\varepsilon = 1+\mathfrak{b}u$, u a unit, then there exists no s in K such that $-\varepsilon s^2 = 1+\mathfrak{b}^{2q+1}v$ for v in $R_{\mathfrak{b}}, q > 0$. Thus there are at most three different possibilities for smash products inside $\mathbf{H}(K)$: $A = S_1(-1)\#S_2(-1)$, $A' = S_{\mathfrak{b}}(-1)\#S_{\mathfrak{b}}(-1)$ and $A'' = S_1(-\varepsilon)\#S_2(-1)$.

These algebras are subalgebras of the usual quaternion algebra $\mathbf{H}(K)$ with the following R-bases (c.f., [**7**]):

$$A = \langle 1, (1+i)/b\varepsilon^{-1}, (1+j)/b, (1+i+j+k)/2 \rangle.$$

In [**4**] we showed, by computing the groups of norm one units of A and A'', that A and A'' are not isomorphic. On the other hand, one can verify that $A' = A''$. Thus there are exactly two non-isomorphic smash products inside $\mathbf{H}(K)$. That completes the proof for $p \equiv 3 \,(\mathrm{mod}\, 4)$.

$p = 2$. The three rank 2 Hopf R-algebras are $H_1, H_{\sqrt{2}}$, and H_2. Since $(1+\sqrt{2})^2(-1) = 1+(\sqrt{2})^3(-1-\sqrt{2})$, using Lemma 5.2 there are Galois extensions $S_1(-1)$ and $S_{\sqrt{2}}(-1)$ but not $S_2(-1)$ (which corresponds to the fact that K has no non-trivial unramified extensions). On the other hand, $-\varepsilon = -(1+\sqrt{2})$, hence the only Galois H-extension contained in $K[z], z^2 = -\varepsilon$, is $S_1(-\varepsilon)$. Thus the only smash product in $\mathbf{H}(K)$ is $S_{\sqrt{2}}(-1) \# S_{\sqrt{2}}(-1)$.

$p \equiv 1 \,(\mathrm{mod}\, 4)$. In this case the fundamental unit ε satisfies $N(\varepsilon) = -1$, and, since p is prime, the narrow Hilbert class field has odd degree over K, so that K has no quadratic extensions which are unramified at all finite primes [**14**, Chapter 2]. Hence there are no non-trivial quadratic Galois extensions of R.

If $p \equiv 5 \,(\mathrm{mod}\, 8)$, then $2R$ is prime, so the only possible Galois H-extensions of rank 2 are either H_1-extensions or H_2-extensions. But

the latter are Galois extensions with group G cyclic of order 2, and those are all trivial. Thus there are no non-trivial smash products.

If $p \equiv 1 \pmod 8$, the same argument shows that there are no non-trivial smash products of the form $A = S_1(w) \# S_2(w')$. Now $2R = \mathfrak{b}\bar{\mathfrak{b}}$ where $\bar{\mathfrak{b}}$ is the conjugate of $\mathfrak{b}$, and $R/\mathfrak{b} \cong \mathbf{Z}/2\mathbf{Z}, R/\mathfrak{b}^2 \cong \mathbf{Z}/4\mathbf{Z}$, so the fundamental unit $\varepsilon \equiv 1$ or $-1 (\mathrm{mod}\, \mathfrak{b}^2 R)$. If w is a unit $\equiv -1 \pmod{\mathfrak{b}^2 R}$, then there is no Galois extension $S_b(w)$. Hence there is no Galois extension $S_{\mathfrak{b}}(-1)$, nor $S_{\bar{\mathfrak{b}}}(-1)$. If $-\varepsilon \equiv 1 \pmod{\mathfrak{b}^2 R}$, then $-\bar{\varepsilon} \equiv \varepsilon \equiv -1 \pmod{\bar{\mathfrak{b}}^2 R}$. Hence, if there exists a Galois extension $S_{\mathfrak{b}}(-\varepsilon)$, there does not exist a Galois extension $S_{\bar{\mathfrak{b}}}(-\varepsilon)$, and vice versa. So we do not have a pair of Galois extensions, one for $H_{\mathfrak{b}}$, one for $H_{\bar{\mathfrak{b}}}$, which will yield a non-trivial smash product. □

COROLLARY 5.3. *Let $p \equiv 1 \pmod 4$ be prime, $R =$ ring of integers of $K = \mathbf{Q}(\sqrt{p})$. Then, for any rank 2 Hopf R-algebra* H, *the smash product map* $\{ \# \} : \mathrm{Gal}(H) \times \mathrm{Gal}(H^*) \to \mathrm{Br}_2(R)$ *is trivial.*

Since $\mathrm{Br}_2(R)$ has order 2, Corollary 5.3 may be viewed as describing a collection of counterexamples to the analogue of Merkurjev's theorem in this context.

6. Isomorphism types of non-trivial Azumaya algebras. Under the assumption that $R = \mathbf{Z}[\sqrt{p}], p \equiv 3 (\mathrm{mod}\, 4)$, prime, we can refine the class number formula of §4 to prove:

THEOREM 6.1. *For every prime $p \equiv 3 (\mathrm{mod}\, 4), p > 3$, there exists a rank 4 Azumaya R-algebra, $R = \mathbf{Z}[\sqrt{p}]$, which is not a smash product.*

The corresponding result for $p \equiv 1 \pmod 4$ is obvious from Corollary 5.3.

PROOF. It is appropriate to be more precise about the Eichler class number formula (4.2).

First, Knus and Ojanguren [**20**] have shown that if B is a rank 4 Azumaya R-algebra, then $\mathrm{Out}(B)$ is 2-torsion. Since R has odd class number, it follows from (4.3) that $\mathrm{Cl}(R) = P_R(B)$. Thus

$$\sum \frac{1}{w_\nu} = h_0 \sum_{i=1}^{t} \frac{1}{w_i},$$

where $w_i = [\mathrm{U}(B_i) : \mathrm{U}(R)]$ and $B_1, \ldots, B_t$ are representatives for the t isomorphism types of maximal orders of $\mathbf{H}(K)$. Two of these representatives are A and A'' (defined in the proof of Theorem 5.1).

Thus (4.2) becomes

$$\frac{2\zeta_K(2)(4p)^{3/2}}{(2\pi)^4} = \sum_{i=1}^{t} \frac{1}{w_i}. \tag{6.2}$$

We compute $w_B = [\mathrm{U}(B) : \mathrm{U}(R)]$ for $B = A, A''$, the two non-isomorphic orders found in §5.

The norm map n yields a short exact sequence

$$1 \to B_0^*/\{\pm 1\} \to \mathrm{U}(B)/\mathrm{U}(R) \xrightarrow{n} \mathrm{U}(R)/\mathrm{U}(R)^2,$$

where $B_0^* =$ the group of units of B with norm 1. Now $\mathrm{U}(R)/\mathrm{U}(R)^2 = \langle -1 \rangle \times \langle \varepsilon \rangle$. Since n is positive, -1 cannot be in the image of n. However, we have

LEMMA 6.3. *For any prime $p \equiv 3 \pmod 4$, ε is a norm from A and from A'', so, for $B = A$ or A'', $w_B = |B_0^*|$.*

PROOF. We first note that we may choose b in R so that $b^2 = 2\varepsilon$, ε the fundamental unit of R. For if $2R = b^2R$, then $b^2 = 2\varepsilon^h$ for some h. If h is odd, $h = 2k+1$, replacing b by $b\varepsilon^{-k}$ yields $b^2 = 2\varepsilon$. If h is even, $h = 2k$, then replacing b by $b\varepsilon^{-k}$ gives $b^2 = 2$. But one sees easily that no b in $\mathbf{Z}[\sqrt{p}]$ can satisfy $b^2 = 2$.

Now $\varepsilon = n(\tau)$, where $\tau = (b - b\sqrt{p})/2 + b((\sqrt{p}+i)/2)$ is an element of A; while $\varepsilon = n(\sigma)$, where $\sigma = (1+i)/b$ is an element of A''. □

From Lemma 6.3 and [**4**], A and A'' contribute to the right side of (6.2) as follows:

$$\begin{aligned} &\text{for } p=3, \quad 1/24+1/24=1/12; \\ &\text{for } p>3, \quad 1/24+1/8=1/6. \end{aligned} \tag{6.4}$$

Since $1/w_B \le 1$ for all B, using (6.4) when $p>3$, (6.2) becomes

$$\frac{2\zeta_K(2)8p^{3/2}}{16\pi^4} \le \frac{1}{6}+(t-2).$$

Now we need a good lower bound for $\zeta_K(2)$. We have

$$\zeta_K(s)=\zeta(s)\sum\Big(\frac{D}{m}\Big)m^{-s} \qquad [\textbf{18}; \text{ p. } 218, \text{ Example } 2],$$

where $\left(\frac{D}{m}\right)$ is the Jacobi symbol and D is the discriminant of K. Thus

$$\zeta_K(2)=\frac{\pi^2}{6}\Big(1+\Big(\frac{D}{2}\Big)\frac{1}{4}+\Big(\frac{D}{3}\Big)\frac{1}{9}+\cdots\Big).$$

Since $\left(\frac{D}{2}\right)=0$ or 1, this is

$$\begin{aligned} &\ge \frac{\pi^2}{6}\Big(1-\sum_{m=3}^{\infty}\frac{1}{m^2}\Big) \\ &\ge \frac{\pi^2}{6}\Big(1+\frac{5}{4}-\frac{\pi^2}{6}\Big), \end{aligned}$$

so

$$\zeta_K(2)\ge 7\pi^2/72.$$

Hence

$$t\ge \frac{7p^{3/2}}{72\pi^2}+\frac{11}{6}.$$

Thus $t>2$ for $p\ge 7$, and goes to ∞ with p. That completes the proof of Theorem 6.1. □

Using the formula of [**16**, p. 40] for $\zeta_K(2)$, one can explicitly compute $\zeta_K(2)$ for $p=3$, and, using (6.4), show that $t=2$. Thus the exception of Theorem 6.1 is genuine:

PROPOSITION 6.5. *Every rank* 4 *Azumaya* $\mathbf{Z}[\sqrt{3}]$*-algebra is isomorphic to a smash product.*

REFERENCES

1. Z.I. Borevich and I.R. Shafarevich, *Number Theory*, Academic Press, New York, 1966.

2. S.U. Chase, *On a variant of the Witt and Brauer groups*, Springer Lecture Notes in Math. **549**, Springer-Verlag, New York, 1976, 148–187.

3. ——— and M.E. Sweedler, *Hopf algebras and Galois theory*, Springer Lecture Notes in Mathematics **97**, Springer-Verlag, New York, 1968.

4. L.N. Childs, *Non-isomorphic equivalent Azumaya algebras*, Canad. Math. Bull. **30** (1987), 340–343.

5. ———, *Taming wild extensions with Hopf algebras*, Trans. Amer. Math. Soc. **304** (1987), 111–140.

6. ———, *On projective modules and automorphisms of central separable algebras*, Canad. J. Math. **21** (1969), 44–53.

7. ———, *Representing classes in the Brauer group of quadratic number rings as smash products*, Pacific J. Math. **129** (1987), 243–255.

8. G. Cornell and M. Rosen, *Cohomological analysis of the class group extension problem*, Proc. Conf. Number Theory, Queen's Univ., Kingston, 1980, 287–308.

9. F.R. DeMeyer and T. Ford, *Computing the Brauer-Long group of* $\mathbf{Z}/2$ *dimodule algebras*, Pure Algebra **54** (1988), 197–208.

10. M. Deuring, *Algebren*, 2nd ed., Springer-Verlag, Berlin, 1968.

11. T. Early and H.F. Kreimer, *Galois algebras and Harrison cohomology*, J. Algebra **58** (1979), 136–147.

12. M. Eichler, *Über die Idealklassenzahl total definiter Quaternionalgebren*, Math. Z. **43** (1937), 102–109.

13. R.M. Fossum, *The Noetherian different of projective orders*, thesis, University of Michigan, 1965.

14. A. Fröhlich, *Central Extensions, Galois Groups and Ideal Class Groups of Number Fields*, Amer. Math. Soc. Contemp. Math. **24**, 1983.

15. J. Gamst and K. Hoechsmann, *Quaternions généralisés*, C. R. Acad. Sci. Paris **269** (1969), A560–A562.

16. W.F. Hammond, *The Hilbert modular surface of a real quadratic field*, Math. Ann. **200** (1973), 25–45.

17. G.H. Hardy and E.M. Wright, *An Introduction to the Theory of Numbers*, 4^{th} edition, Oxford, 1960.

18. H. Heilbronn, "Zeta-functions and L-functions," in J.W.S. Cassels and A. Fröhlich, eds. *Algebraic Number Theory*, Thompson Book Company, Washington, D. C., 1967.

19. S. Hurley, *Galois objects with normal bases for free Hopf algebras of prime degree*, J. Algebra **109** (1987), 292–318.

20. M.-A. Knus and M. Ojanguren, *Sur le polynôme caractéristique et les automorphisms des algèbres d'Azumaya*, Ann. Scuola Norm. Sup. Pisa **26** (1972), 225–231.

21. H.F. Kreimer, *Quadratic Hopf algebras and Galois extensions*, Amer. Math. Soc. Contemp. Math. **13** (1982), 353–362.

22. M. Orzech and C. Small, *The Brauer Group of Commutative Rings*, Lecture Notes in Pure and Applied Mathematics No. **11**, Marcel Dekker, 1975.

23. I Reiner, *Maximal Orders*, Academic Press, New York, 1975.

24. A. Rosenberg, D. Zelinsky, *Automorphisms of separable algebras*, Pacific J. Math. **2** (1961), 1107–1117.

25. O. Schilling, *Arithmetic in a special class of algebras*, Ann. of Math. (2) **38** (1937), 116–119.

26. R.G. Swan, *Projective modules over group rings and maximal orders*, Ann. of Math. **76** (1962), 55–61.

27. M.E. Sweedler, *Cohomology of algebras over Hopf algebras*, Trans. Amer. Math. Soc. **133** (1968), 205–239.

28. J.T. Tate and F. Oort, *Group schemes of prime order*, Ann. Scient. Ecole Norm. Sup. (4e serie) **3** (1970), 1–21.

29. W. Van der Kallen, *The Merkurjev-Suslin theorem*, Springer Lecture Notes in Math. **1142**, Springer-Verlag, New York (1985) 157–168.

30. K. Yokogawa, *On $S \otimes S$-module structure of S/R-Azumaya algebras*, Osaka J. Math. **12** (1975), 673–690.

State University of New York at Albany, Albany, NY 12222