Canad. Math. Bull. Vol. 30 (3), 1987

NON-ISOMORPHIC EQUIVALENT AZUMAYA ALGEBRAS

BY
LINDSAY N. CHILDS

ABSTRACT. We explicitly describe an infinite collection of pairs of Azumaya algebras over the ring of integers of real quadratic number fields K which are maximal orders in the usual quaternion algebra over K, hence Brauer equivalent, but are not isomorphic. The result follows from an identification of the groups of norm one units, using the classification of Coxeter.

In [10], R. G. Swan constructed a pair of Azumaya algebras over the ring of integers R of a quartic extension of the rational numbers which were equivalent in the Brauer group of R but were not isomorphic. In this note we describe an infinite collection of such pairs over rings of integers of quadratic fields.

Let m be a rational integer congruent to 3 (mod 4), and $R = \mathbb{Z}[\sqrt{m}]$, the ring of integers of $K = \mathbb{Q}(\sqrt{m})$. Suppose $2R = b^2R$, the square of a principal ideal. (This will always be the case if m is prime, for then R has odd class number.) Let $\bar{b}$ be the conjugate of b. Our examples are both maximal orders over R in the usual quaternion algebra $H(K)$ over K, the algebra generated over K by i and j with $i^2 = j^2 = -1$, $ij = -ji = k$.

The two examples have bases as free R-modules as follows:

$$A = \left\langle 1, \frac{1+i}{\bar{b}}, \frac{1+j}{b}, \frac{1+i+j+k}{2} \right\rangle;$$

$$D = \left\langle 1, \frac{\sqrt{m}+i}{2}, j, \frac{\sqrt{m}j+k}{2} \right\rangle.$$

Both may be seen to be Azumaya R-algebras by recognizing them as smash products. Gamst and Hoechsmann [8] have shown that if S, T are Galois objects (in the sense of [2]) with respect to a dual pair of Hopf algebras $H, H^* = \mathrm{Hom}_R(H, R)$, then the smash product $S \# T$ is an Azumaya R-algebra.

Now D is the smash product of a Galois $(RG)^*$-object S and a Galois RG-object T. Here

$$S = R\left[\frac{\sqrt{m}+1}{2}\right]$$

Received by the editors January 29, 1986, and, in revised form, September 18, 1986.
AMS Subject Classification (1980): 16A16, 16A18.

https://doi.org/10.4153/CMB-1987-048-8 Published online by Cambridge University Press

is the ring of integers of the unramified extension $L = K[i]$ of K, hence S is a Galois extension of R with group $G = \mathrm{Gal}(L/K)$ in the sense of [1], hence a Galois $(RG)^*$-object; and

$$T = R[j], \; j^2 + 1 = 0$$

is a G-graded R-algebra and a Galois RG-object.

If we let H_b be the free Hopf R-algebra, $H_b = R[x]$ with $x^2 = bx$ and comultiplication $\triangle$, counit ϵ and antipode λ defined by

$$\begin{aligned} \triangle(x) &= x \otimes 1 + 1 \otimes x - \frac{2}{b}(x \otimes x) \\ \epsilon(x) &= 0 \\ \lambda(x) &= x, \end{aligned}$$

then $A = S \# T$ where

$$\begin{aligned} S &= R[w], \quad w^2 = \bar{b}w - b/\bar{b} \\ T &= R[z], \quad z^2 = \bar{b}z - \bar{b}/b \end{aligned}$$

are Galois H-objects for $H = H_b$ and $H_{\bar{b}} = H_b^*$, respectively. Then $S \# T$ embeds in $H(K)$ by $w \# 1 \to \dfrac{1+i}{\bar{b}}$, $1 \# z \to \dfrac{1+j}{b}$.

THEOREM. *The algebras A and D are in the same class in Br(R) but are not isomorphic.*

PROOF. Since the map from $Br(R)$ to $Br(K)$ is $1 - 1$ and A and D are both orders over R in the same K-algebra $H(K)$, A and D are in the same class in $Br(R)$. To show A and D are not isomorphic, let A_o^*, D_o^* denote the groups of units of A, D, respectively, of norm 1, where

$$n(\alpha) = n(a + bi + cj + dk) = a^2 + b^2 + c^2 + d^2$$

is the usual norm from H to K. A result of Eichler (c.f. Swan [10], Remark 2) shows that A_o^* and D_o^* are finite. We show that A_o^* and D_o^* are not isomorphic. In fact, we show that

$$A_o^* = \{\pm 1, \pm i, \pm j, \pm k, (\pm 1 \pm i \pm j \pm k)/2\}$$

a group of order 24, in Coxeter's notation of [6], $A_o^* = \langle 2, 3, 3\rangle$; while D_o^* is a dicyclic group.

Now A_o^*, D_o^*, being finite, are made up of roots of unity in $H(K)$. Since $H(K)$ is a skew field, if ζ is a primitive e th root of 1 in $H(K)$, then $\mathbb{Q}(\zeta)$ is a commutative subfield of $H(K)$. So $\mathbb{Q}(\zeta)$: $\mathbb{Q} \leq 4$, hence $\phi(e) \leq 4$, where ϕ is Euler's function. Now $\phi(e) = 1$ for $e = 1, 2$; $\phi(e) = 2$ for $e = 3, 4, 6$; $\phi(e) = 4$ for $e = 5, 8, 10, 12$, and $\phi(e) > 4$ for all other e.

https://doi.org/10.4153/CMB-1987-048-8 Published online by Cambridge University Press

If $\phi(e) = 4$, then $\mathbb{Q}(\zeta) \supset K$. But the only real quadratic subfield of $\mathbb{Q}(\zeta)$ for $e = 5, 8, 10$ or 12 is $\mathbb{Q}(\sqrt{m})$ where $m = 5, 2, 5$ and 3, respectively. So $H(K)$ has no elements of order 5 or 8, and no element of order 12 unless $m = 3$.

The known list of finite groups of real quaternions ([11], p. 17) shows that since A_o^*, D_o^* contain no elements of order 5 or 8, each must be isomorphic either to E_{24}, the binary tetrahedral group of order 24, or to a dicyclic group of order $4n$.

Now

$$E_{24} = \{\pm 1, \pm i, \pm j, \pm k, (\pm 1 \pm i \pm j \pm k)/2\} \subseteq A_o^*;$$

hence A_o^* is not dicyclic, so $A_o^* = E_{24}$.

To see that $D_o^* \not\cong A_o^*$ we show that if $m > 3$ D_o^* contains no cube roots of 1, while if $m = 3$ D_o^* contains a 12^{th} root of 1.

Now any element of D is of the form

$$\tau = \frac{\alpha}{2} + \frac{\beta}{2} i + \frac{\gamma}{2} j + \frac{\delta}{2} k, \quad \alpha, \beta, \gamma, \delta \in R.$$

If τ is a primitive 3rd or 6th root of unity, then $\tau^2 \pm \tau + 1 = 0$. Also $n(\tau) = \tau(\alpha - \tau) = 1$, so $\tau^2 - \alpha\tau + 1 = 0$, so $\alpha = 1$ or -1. Thus

$$n(\tau) = \frac{1}{4} + \frac{\beta^2}{4} + \frac{\gamma^2}{4} + \frac{\delta^2}{4} = 1$$

or

$$(*) \qquad \beta^2 + \gamma^2 + \delta^2 = 3$$

Setting $\beta = c + d\sqrt{m}$, $\gamma = e + f\sqrt{m}$, $\delta = g + h\sqrt{m}$, c, d, e, f, g, h in $\mathbb{Z}$, (*) becomes

$$(**) \qquad \begin{cases} c^2 + md^2 + e^2 + mf^2 + g^2 + mh^2 = 3 \\ cd + ef + gh = 0 \end{cases}$$

If $m > 3$, the only solution of (**) is $c^2 = e^2 = g^2 = 1$. But, as is easily seen, $(\pm 1 \pm i \pm j \pm k)/2$ is not in D. Thus D_o^* has no elements of order 3, hence cannot be isomorphic to $E_{24} = A_o^*$.

If $m = 3$, D_o^* contains $\dfrac{\sqrt{3} + i}{2}$, a primitive 12^{th} root of 1. Since E_{24} has no elements of order 12, again D_o^* is dicyclic for $m = 3$, and, in particular, not isomorphic to A_o^*. That completes the proof.

A bit more computation (which we omit) shows that, in Coxeter's notation of [16], $D_o^* = \langle 2, 2, 2\rangle$ for $m > 3$, while for $m = 3$, $D_o^* = \langle 2, 2, 6\rangle$.

REMARKS. The algebras A and D, being non-isomorphic representatives of the non-trivial class of $Br(R)$ give further explicit examples of the failure of cancellation of projective modules [10] and of the failure of the Skolem-Noether theorem for Azumaya algebras [3], [4].

Using Eichler's class number formula [7], Theorem, and a closed form description of the zeta function of K evaluated at 2 found in [9], page 40, one can show (not without some difficulty) that the number t of isomorphism types of maximal orders in the quaternion algebra $H(K)$, $K = \mathbb{Q}(\sqrt{p})$, satisfies $t = 2$ if and only if $p = 3$. Thus the algebras A and D represent all isomorphism types of maximal orders in $H(\mathbb{Q}(\sqrt{p}))$, $p \equiv 3 \pmod 4$, if and only if $p = 3$. We omit the details, some of which may be found in [5].

My thanks to the referee for pointing out reference [11].

References

1. S. U. Chase, D. K. Harrison, A. Rosenberg, *Galois theory and Galois cohomology of commutative rings*. Memoirs Amer. Math. Soc. **52** (1965), pp. 15–33.

2. S. U. Chase, M. E. Sweedler, *Hopf Algebras and Galois Theory*. Springer Lecture Notes in Mathematics **97** (1968).

3. L. N. Childs, F. R. DeMeyer, *On automorphism of separable algebras*. Pacific J. Math. **23** (1967), pp. 25–34.

4. L. N. Childs, *On projective modules and automorphisms of central separable algebras*. Canad. J. Math. **21** (1969), pp. 44–53.

5. L. N. Childs, *Azumaya algebras which are not smash products*. Rocky Mount. J. (to appear).

6. H. S. M. Coxeter, *The binary polyhedral groups and other generalizations of quaternion groups*. Duke Math. J. **7** (1940), pp. 367–379.

7. M. Eichler, *Uber die Idealklassenzahl total definiter Quaternionalgebren*. Math. Z. **43** (1937), pp. 102–109.

8. J. Gamst, K. Hoechsmann, *Quaternions generalises*. C.R. Acad. Sci. Paris **269** (1969), pp. 560–562.

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

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

11. M.-F. Vigneras, *Arithmétique des Algebras de Quaternions*. Springer LNM 800 (1980).

Department of Mathematics and Statistics
State University of New York at Albany
Albany, NY 12222