BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 1, Number 4, July 1979

DIVISION ALGEBRAS OF DEGREE 4 AND 8 WITH INVOLUTION

BY S. A. AMITSUR, L. H. ROWEN[1], AND J. P. TIGNOL[2]

ABSTRACT. Examples are given of division algebras with involution (*) of the first kind, one of degree 8 which is not a tensor product of quaternion subalgebras, the other of degree 4 which is not a tensor product of (*)-invariant quaternion subalgebras.

Suppose D is a division algebra with center F, and $[D: F] < \infty$. Then $[D: F] = n^2$ for suitable n; n is the *degree* of D, and D is a *quaternion F-algebra* when $\deg(D) = 2$. We further assume D has characteristic $\neq 2$, and has an involution (*) of the first kind, i.e. (*) is an anti-automorphism of degree 2 which fixes F. This situation is treated in depth in [1, Chapter 10], and it arises if and only if D has exponent 2 in the Brauer group, i.e. $D \otimes D^{\mathrm{op}} \approx M_{n^2}(F)$, the algebra of $n^2 \times n^2$ matrices over F. Thus, in this case, the degree of D is a power of 2. Until now, the only known such algebras were tensor products of quaternion F-subalgebras.

QUESTION 1. Is D necessarily a tensor product of quaternion F-subalgebras?

QUESTION 2. Is D necessarily a tensor product of (*)-invariant quaternion F-subalgebras?

Question 1 dates back about 60 years; Albert [1] showed it is true when $\deg(D) \leqslant 4$. The main object of this paper is to give a counterexample for degree 8. Also, we shall give a counterexample to Question 2 for degree 4, which is clearly sharp. (Incidentally, for *symplectic* involutions, question 2 has no counterexample of degree 4, cf. [3, Theorem B].) Our counterexample makes the following result of Tignol [4] sharp: If $\deg(D) = 8$ then $M_2(D)$ is a tensor product of quaternion subalgebras. A more detailed description of our methods will appear in the *Israel Journal of Mathematics*.

The main idea is to use the generic abelian crossed products of [2], modified slightly to account for the presence of an involution. Suppose R is an abelian crossed product, i.e. D has a maximal subfield K Galois over F, having Galois group $G = \langle \sigma_1 \rangle \oplus \cdots \oplus \langle \sigma_q \rangle$, a direct sum of cyclic groups, and for our purposes we assume that σ_i has order 2. Then, choosing z_i such that $\sigma_i(x) = z_i x z_i^{-1}$ for all x in K, we define $u_{ij} = z_i z_j z_i^{-1} z_j^{-1}$ and $b_i = z_i^2$, elements of K. [2, Lemma 1.2] gives the following conditions for all i (where $N_i(x) = x\sigma_i(x)$ by definition).

Received by the editors November 16, 1978.
AMS (MOS) subject classifications (1970). Primary 16A40, 16A28; Secondary 15A66.
[1]Research of the second author is supported by the Anshel Pfeffer Chair.
[2]The third author is grateful to Professor J. Tits for enlightening conversations.

0002-9904/79/0000-0319/$02.00

(1) $u_{ii} = 1$ and $u_{ij}^{-1} = u_{ji}$ for all i;
(2) $\sigma_i(u_{jk})\sigma_j(u_{ki})\sigma_k(u_{ij}) = u_{ij}u_{jk}u_{ki}$ for all i, j, k;
(3) $N_i(N_j(u_{ij})) = 1$ for all i, j;
(4) $\sigma_j(b_i)b_i^{-1} = N_i(u_{ji})$ for all i, j.

Conversely, these conditions for given elements of a Galois field extension K of F with abelian Galois group G, define a simple F-algebra R of dimension G^2 and center F.

THEOREM 1. *Notation as above, R has an involution iff, modifying the u_{ij} and b_i suitably, we can satisfy* (1)–(4) *above, as well as the following extra conditions, where $\tau \in G$ is arbitrarily chosen*:

(5) $\tau(u_{ij})\sigma_i\sigma_j(u_{ij}) = 1$ *for all i, j,*
(6) $\tau(b_i) = b_i$ *for all i.*

Proof. ($\Rightarrow$) Using the proof of [3, Propositions 5.4 and 5.5], one sees easily that R has an involution iff R has some involution $(*)$ whose restriction to K is τ. For all elements k in K, $z_ik = \sigma_i(k)z_i$, taking $(*)$ on both sides, and substituting, shows $z_i^* \in z_iK$, so we can replace z_i by $z_i \pm z_i^*$, (5) and (6) follow easily.

($\Leftarrow$) Define $(*)$ by $(\Sigma k_\alpha z_1^{\alpha_1} \cdots z_q^{\alpha_q})^* = \Sigma z_q^{\alpha_q} \cdots z_1^{\alpha_1}\tau(k_\alpha)$, k_α in K, using (5) and (6) to prove $(*)$ is an involution. Q.E.D.

Write U for $\{u_{ij} | 1 \leqslant i, j \leqslant q\}$ and B for $\{b_i | 1 \leqslant i \leqslant 3\}$. We restrict ourseves to the case $q = 3$, i.e. K is a given Galois extension of F with Galois group $\mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2$. Thus, we can write $K = F(\xi_1, \xi_2, \xi_3)$ with $\xi_i^2 \in F$, $\sigma_i(\xi_i) = -\xi_i$, and $\sigma_i(\xi_j) = \xi_j$ for $j \neq i$. Also take $\tau = \sigma_1\sigma_2\sigma_3$.

THEOREM 2. *Given B, we can find U satisfying* (1)–(6) *above iff there are elements v_1, v_2, v_3 in K satisfying*

(2)′ $v_1v_2v_3 = 1$,
(3)′ $N_i(v_i) = 1$,

as well as the following conditions for every permutation π of (1, 2, 3):

(4)′ $\sigma_{\pi 1}(b_{\pi 2})b_{\pi 2}^{-1} = (N_{\pi 2}(v_{\pi 3}))^{sg\pi}$;
(5)′ $b_{\pi 1} \in F(\xi_{\pi 2}\xi_{\pi 3})$.

PROOF. Straightforward computations, defining $v_1 = u_{23} = u_{32}^{-1}$, $v_2 = u_{31} = u_{13}^{-1}$, $v_3 = u_{12} = u_{21}^{-1}$, and $u_{11} = u_{22} = u_{33} = 1$. Q.E.D.

The proof of Theorem 2 also shows (1)–(5) imply (6).

THEOREM 3. *Given v_1, v_2, v_3 satisfying* (2)′, (3)′, *there exists B satisfying* (4)′ *and* (5)′ *such that, for every permutation π,*

$$b_{\pi 1} = F(\xi_{\pi 2}\xi_{\pi 3}) \cap F(\xi_{\pi 2})N_{\pi 1}(K) \cap F(\xi_{\pi 3})N_{\pi 1}(K).$$

PROOF. Define u_{ij} as in Theorem 2, so that (1), (2), and (3) are satisfied. By [2, equation (14)], which should read $a_k\sigma_i(a_k^{-1})$ etc., we obtain the elements

a_i, which we rename b_i, satisfying (4). We readily get (2)′–(5)′. By Hilbert's theorem 90, we have y_i such that $v_i = \sigma_i(y_i)y_i^{-1}$; $b_1N_1(y_3)$ is fixed under σ_3, so $b_1N_1(y_3) \in F(\xi_2)$ and $b_1 \in F(\xi_2)N_1(y_3^{-1})$. Likewise $b_1N_1(y_2^{-1}) \in F(\xi_3)$ etc. Q.E.D.

Suppose now we are given $b \in K$ satisfying

(7) $b \in F(\xi_2\xi_3) \cap F(\xi_2)N_1(K) \cap F(\xi_3)N_1(K)$.

Then, taking $b = a_2N_1(w) = a_3N_1(w')$, put $v_2 = w^{-1}\sigma_2(w)$, $v_3 = (w')^{-1}\sigma_3(w')$ and $v_1 = (v_2v_3)^{-1}$. Theorems 3 and 2 then apply, giving B and U; $b \in Fb_1$, so we replace b_1 by b. Form the corresponding abelian crossed product R. The generic abelian crossed product R' (cf. [2]) is a division ring with involution, by Theorem 1. If R' is a tensor product of quaternion subalgebras, then R' has some set of square-central elements $r_1', \ldots, r_{64}'$, independent over Cent(R') with $r_i'r_j' = \pm r_j'r_i'$ for all i, j. An argument based on taking leading monomials (cf. [2, Lemma 2.1]) then shows there is such a set of elements of R, each having the form $k_iz_1^{i_1}z_2^{i_2}z_3^{i_3}$, with $k_i \in K$. In particular, one of these elements must be of the form kz_1, implying some $\alpha = (kz_1)^2 = bN_1(k)$, so $b \in FN_1(K)$. Thus, to answer Question 1 negatively, we need to find F, $K = F(\xi_1, \xi_2, \xi_3)$, and $b \in K$, such that (7) holds and $b \notin FN_1(K)$. (The counterexample will be R'.)

Take $F = \mathbf{Q}(\lambda)$, the field of rational functions in one indeterminate λ and ξ_i such that $\xi_1^2 = -1$, $\xi_2^2 = -(\lambda^2 + 1)$, and $\xi_3^2 = \lambda$, with $b = \xi_2\xi_3$. Then (7) holds. If $b \notin FN(K)$ then $\lambda(\lambda^2 + 1) \in N_1(F(\xi_1))(N(F(\xi_1\xi_2)/F) \cap N(F(\xi_2\xi_3)/F))$, where $N(\ )$ denotes the norm of a field extension. (This step is not easy.) This is impossible, seen by taking polynomials modulo 2.

Similarly, Question 2 has a counterexample iff there is a field extension $K = F(\xi_1, \xi_2)$ of F and some $b \in FN_1(K)$, with $b \notin Fk^2$ for all k in $F(\xi_2)$. Take $F = \mathbf{Q}(\lambda)$, $\xi_1^2 = 2$, $\xi_2^2 = \lambda$, and $b = \lambda - 1 + 2\xi_2$.

REFERENCES

1. A. A. Albert, *Structure of algebras*, Amer. Math. Soc. Colloq. Publ. no. 24, Amer. Math. Soc., Providence, R.I., 1961.

2. S. A. Amitsur and D. Saltman, *Generic abelian crossed products*, J. Algebra **51** (1978), 76–87.

3. L. Rowen, *Central simple algebras*, Israel J. Math. 29 (1978), 285–301.

4. J. Tignol, *Sur les classes de similitude de corps à involution de degré* 8, C. R. Acad. Sci. Paris, Sér A 286 (1978), 875–876.

5. ———, *Décomposition et descente de produits tensoriels d'algebres de quaternions*, Rap. Sém. Math. Pure UCL 76 (1978).

DEPARTMENT OF MATHEMATICS, HEBREW UNIVERSITY OF JERUSALEM, JERUSALEM, ISRAEL

DEPARTMENT OF MATHEMATICS, BAR ILAN UNIVERSITY, RAMAT GAN, ISRAEL

DEPARTMENT OF MATHEMATICS, CATHOLIC UNIVERSITY OF LOUVAIN, LOUVAIN-LA-NEUVE, BELGIUM