ISRAEL JOURNAL OF MATHEMATICS, Vol. 33, No. 2, 1979

DIVISION ALGEBRAS OF DEGREE 4 AND 8 WITH INVOLUTION

BY

S. A. AMITSUR, L. H. ROWEN† AND J. P. TIGNOL††

ABSTRACT

We develop necessary and sufficient conditions for central simple algebras to have involutions of the first kind, and to be tensor products of quaternion subalgebras. The theory is then applied to give an example of a division algebra of degree 8 with involution (of the first kind), without quaternion subalgebras, answering an old question of Albert; another example is a division algebra of degree 4 with involution (*) has no (*)-invariant quaternion subalgebras.

§0. Introduction

In this paper, F denotes an arbitrary field of characteristic $\neq 2$, and R is a central simple F-algebra. An *involution* (of the first kind) of R is an anti-automorphism of degree 2 fixing F. The classic reference on central simple algebras, with or without involution, is [1] (especially section X), and some positive general results were given in [4].

It is well known that $[R : F] = n^2$ for some n; n is called the *degree* of R. Then, for some uniquely determined natural number k and some division algebra D, we have $R \approx M_k(D)$, the algebra of $k \times k$ matrices with entries in D. If $\deg(R) = 2$, we call R a *quaternion F-algebra.* In this case, there are elements a_1, a_2, in R such that $0 \neq a_1^2 \in F$, $0 \neq a_2^2 \in F$, $a_1a_2 = -a_2a_1$ and $R = F + Fa_1 + Fa_2 + Fa_1a_2$; letting $\alpha_i = a_i^2$, we denote R by the symbol $(\alpha_1, \alpha_2; F)$. R has an involution (*), given by

$$(\gamma_1 + \gamma_2a_1 + \gamma_3a_2 + \gamma_4a_1a_2)^* = \gamma_1 - \gamma_2a_1 - \gamma_3a_2 - \gamma_4a_1a_2.$$

†The research of the second author is supported by the Anshel Pfeffer Chair.

††The third author would like to express his gratitude to Professor J. Tits for many stimulating conversations.

Received December 10, 1978

Conversely, given α_1, α_2 in F, we can construct $(\alpha_1, \alpha_2; F)$ by taking formal elements a_i, $i = 1, 2$, and defining $R = F + Fa_1 + Fa_2 + Fa_1a_2$, with multiplication induced by the rules $a_i^2 = \alpha_i$ and $a_1a_2 = -a_2a_1$.

Any tensor product (over F) of m quaternion F-algebras is of degree 2^m, and has an involution given by the tensor product of the respective involutions. On the other hand, any central division algebra D with involution has degree 2^m for some m, and Albert [1] showed D is a tensor product of quaternion subalgebras when $m = 2$. The following famous question thus arises:

QUESTION A. If a central simple F-algebra of degree 2^m has an involution, is it isomorphic to a tensor product of quaternion F-algebras?

It suffices to consider only division algebras, and the first stage to consider is $m = 3$. A related question of interest is

QUESTION B. Suppose R is a tensor product of quaternion algebras and has a given involution $(*)$. Is R then a tensor product of (possibly different) $(*)$-invariant quaternion subalgebras?

The main object of this paper is to give a negative answer to Question A; we have a division algebra D of degree 8 with involution, which is not a tensor product of quaternions. It is noteworthy that by a theorem of Tignol [5], $M_2(D)$ is a tensor product of quaternions. (Our construction also works for $m \geqq 3$.)

We also provide a counterexample to Question B, of degree 4. Namely, there is a division algebra $Q_1 \otimes Q_2$ with involution $(*)$ without any $(*)$-invariant quaternion subalgebra. (In this case, the involution must be of orthogonal type, by [4, theorem B]). The method is to study abelian crossed products (cf. [2]), giving necessary and sufficient conditions for an involution to exist. Comparing these criteria with the structure of tensor products of quaternion algebras, applied to "generic abelian crossed products", we arrive at the counterexamples.

§1. Tensor products of quaternions

Let R be a central simple algebra with a center F. A set of elements $S = \{r_i\}$ is called a quaternion generating set, or in short a q-generating set, if:

(1) $0 \neq r_i^2 \in F$,

(2) $r_ir_j = \pm r_jr_i$,

(3) if $i \neq j$, then there exists $r_k \in S$ such that r_k commutes with one of $\{r_i, r_j\}$ and anticommutes with the other.
Note that if $r_i r_j = -r_j r_i$ we can choose $r_k = r_i$.

PROPOSITION 1.1. (i) *A q-generating set S is F-independent.*

(ii) *If $\{r_1, r_2\}$ is a q-generating set, then also $\{1, r_1, r_2, r_1 r_2\}$ is a q-generated set, and $Q = F + Fr_1 + Fr_2 + Fr_1 r_2$ is a quaternion F-algebra.*

PROOF. (i) Let $\sum_{i=1}^{k} \alpha_i r_i = 0$, with k minimal. If some $\alpha_i \neq 0$, then at least two of them are non-zero; say $\alpha_1, \alpha_2 \neq 0$. By definition, there exists an $r \in S$ such that $[r, r_1] = rr_1 - r_1 r = 0$ but $[r, r_2] \neq 0$. Then

$$0 = \left[r, \sum \alpha_i r_i \right] = \sum{}' \alpha_i [r r_i] = -2 \sum{}' \alpha_i r_i r$$

where the sum ranges over all i such that $0 \neq [r, r_i] = -2 r_i r$. In particular the sum will contain α_2 but not α_1; hence, by the minimality of k we must have $\alpha_i = 0$ in Σ', which is a contradiction since $\alpha_2 \neq 0$.

Part (ii) is straightforward. Q.E.D.

PROPOSITION 1.2. *Suppose* $\deg(R) = 2^t$. *R is a tensor product of quaternion F-algebras, iff R has a q-generating set S containing 4^t elements (in which case, S is a base of R).*

PROOF. Suppose $R = Q_1 Q_2 \cdots Q_t \approx Q_1 \otimes \cdots \otimes Q_t$, where $Q_i = F + Fr_{1i} + Fr_{2i} + Fr_{3i}$, is a quaternion F-algebra and $r_{3i} = r_{1i} r_{2i}$. Put $r_{0i} = 1$. Then $S = \{r_{i_1 1} r_{i_2 2} \cdots r_{i_t t} \mid i_u = 0, 1, 2, 3\}$ is the required base.

Conversely, suppose such a q-generating set S exists, take r_1, r_2 in S with $r_1 r_2 = -r_2 r_1$, and let Q_1 be the quaternion subalgebra generated by r_1 and r_2, cf. Proposition 1.1. Then $R = Q_1 R_1 \approx Q_1 \otimes_F R_1$, where R_1 is the centralizer of Q_1 in R. We claim that $S_1 = S \cap R_1$ is a q-generating set having 4^{t-1} elements; since $\deg(R_1) = 2^{t-1}$ we could then conclude by induction.

To prove our claim, note that if $r_u \in S$, either $r_u \in R_1$ or $r_u \notin R_1$; and if $r_u \notin R_1$, then either $r_u r_1 = -r_1 r_u$ or $r_u r_2 = -r_2 r_u$. Write $r_u = \rho_0 + \rho_1 r_1 + \rho_2 r_2 + \rho_3 r_1 r_2$, where $\rho_i \in R_1$. One sees easily that exactly one of the ρ_i is non-zero. Thus $S = T_0 \cup T_1 r_1 \cup T_2 r_2 \cup T_3 r_1 r_2$ with $T_i \subseteq R_1$. Since these elements are F-independent, the number of elements of each T_i is at most $[R_1 : F] = 4^{t-1}$. The total number is $4^t = 4 \cdot 4^{t-1}$, so T_0 contains 4^{t-1} elements; clearly $T_0 = S \cap R_1$ is a q-generating set. Q.E.D.

PROPOSITION 1.3. *Suppose* $\deg(R) = 2^t$ *and* R *has an involution* $(*)$. R *is a product of* $(*)$*-invariant quaternion subalgebras iff* R *has a* q*-generating set* $S = \{r_u \mid 1 \leqq u \leqq 4^t\}$ *satisfying Proposition* 1.2, *with* $r_u^* = \pm r_u$ *for each* r_u.

PROOF. As in Proposition 1.2, taking note of the additional facts that Q_1 is $(*)$-invariant if $r_i^* = \pm r_i$ for $i = 1, 2$, in which case the centralizer of Q_1 is also $(*)$-invariant.

§2. Abelian crossed products

This section is based on [2], with the roles of K and F reversed. Suppose R has a maximal subfield K which is Galois over F, having abelian Galois group $G = \langle\sigma_1\rangle \oplus \cdots \oplus \langle\sigma_q\rangle$, a direct sum of cyclic groups of order 2, i.e. $G \approx \mathbf{Z}_2 \oplus \cdots \oplus \mathbf{Z}_2$. Define $N_i(x) = x\sigma_i(x)$, the norm with respect to σ_i. N_i is multiplicative and commutes with all σ_j and N_j. By the Skolem–Noether theorem we may choose z_i such that $\sigma_i(x) = z_i x z_i^{-1}$ for all x in K. Define $u_{ij} = z_i z_j z_i^{-1} z_j^{-1}$ and $b_i = z_i^{n_i}$, $1 \leqq i \leqq q$. All u_{ij} and b_i are in the centralizer of K, which is K itself. Write U for $\{u_{ij} \mid 1 \leqq i, j \leqq q\}$ and B for $\{b_i \mid 1 \leqq i \leqq q\}$. By [2, lemma 1.2], the following conditions are satisfied:

(1) $u_{ii} = 1$ and $u_{ij}^{-1} = u_{ji}$ for all i, j;

(2) $\sigma_i(u_{jk})\sigma_j(u_{ki})\sigma_k(u_{ij}) = u_{jk}u_{ki}u_{ij}$ 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, suppose K is any abelian extension of F with Galois group $G = \langle\sigma_1\rangle \oplus \cdots \oplus \langle\sigma_q\rangle$, and suppose $U, B \subseteq K$ satisfy conditions (1)–(4). Then, by [2], there is a central simple F-algebra R uniquely determined (up to isomorphism), having K as a maximal subfield, and $\{z_1, \cdots, z_q\} \subseteq R$ such that the above system holds. Thus K, G, U, and B determine R, and we denote R as (K, G, U, B).

Note that we can replace any $b \in B$ by αb, for arbitrary α in F, for (4) is still satisfied. Using [2], we also have the following observation:

REMARK 2.0. (i) Condition (2) is subsumed by condition (1) except when i, j, k are distinct;

(ii) if U, B satisfy (1), (2), and (4), then U satisfies (3);

(iii) conversely, if U satisfies (1), (2), and (3) then there is some B, whose elements are uniquely determined up to multiplication by elements of F, satisfying (4).

Indeed, (i) is obvious, and (ii) is clear because $N_j(N_i(u_{ji})) = N_j(\sigma_j(b_i)b_i^{-1}) = 1$. To see (iii), we get B from the generalization of Hilbert's theorem 90 ([2, lemma 2.4]), in particular from [2, equation (14)] (which has a misprint which should read $a_k\sigma_i(a_k^{-1}) = v_{ik} = N_k(u_{ik})$ for all $i \neq k$), where we choose $b_i = a_i^{-1}$. The uniqueness is clear from (4).

THEOREM 2.1. *Let $\tau \in G$ and suppose $R = (K, G, U, B)$. The following conditions are equivalent:*

(i) *R has an involution of the first kind;*

(ii) *R has an involution whose restriction to K is τ;*

(iii) *By modifying suitably U and B, we may write $R = (K, G, U, B)$ also satisfying the following additional conditions:*

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

(6) *$\tau(b_i) = b_i$ for all i.*

In fact, we can then select the involution $(*)$ such that for arbitrary $\mu_i = \pm 1$, $z_i^* = \mu_i z_i$, and the restriction of $(*)$ to K is τ.

PROOF. (i) $\Rightarrow$ (ii) parallels [4, proposition 5.4 and 5.5] and is omitted; (ii) $\Rightarrow$ (i) is trivial.

(ii) $\Rightarrow$ (iii). Suppose $(*)$ is an involution on R whose restriction to K is τ, then it is clearly of the first kind. For all k in K, $z_i k = \sigma_i(k)z_i$; taking $(*)$ on both sides yields $\tau(k)z_i^* = z_i^*\tau(\sigma_i(k))$. Replacing k by $\tau(\sigma_i(k))$ yields $\sigma_i(k)z_i^* = z_i^* k$. Thus $z_i^{-1}z_i^* k = z_i^{-1}\sigma_i(k)z_i^* = kz_i^{-1}z_i^*$, so $z_i^{-1}z_i^*$ centralizes K, implying $z_i^{-1}z_i^* \in K$. Hence $z_i^* \in z_i K$, so $z_i + \alpha z_i^* \in z_i K$ for each α in F. Since all elements of $z_i K - \{0\}$ are invertible, inducing σ_i as their inner automorphism, we may replace z_i by $\bar{z}_i = z_i + \mu_i z_i^*$ for suitable μ_i in $\{+1, -1\}$; then $\bar{z}_i^* = \mu_i \bar{z}_i$. Let $\bar{b}_i = \bar{z}_i^2$ and $\bar{u}_{ij} = \bar{z}_i\bar{z}_j\bar{z}_i^{-1}\bar{z}_j^{-1}$. Clearly $\tau(\bar{b}_i) = \bar{z}_i^* = \mu_i^2\bar{z}_i^2 = \bar{b}_i$, yielding (6); also,

$$\tau(\bar{u}_{ij}) = (\bar{z}_i\bar{z}_j\bar{z}_i^{-1}\bar{z}_j^{-1})^* = \mu_i^2\mu_j^2\bar{z}_i^{-1}\bar{z}_i^{-1}\bar{z}_j\bar{z}_i = \bar{z}_j^{-1}\bar{z}_i^{-1}\bar{u}_{ji}\bar{z}_i\bar{z}_j = \sigma_i\sigma_j(\bar{u}_{ji}),$$

since $\bar{u}_{ji}\bar{z}_i\bar{z}_j = \bar{z}_j\bar{z}_i$, yielding (5) in view of (1).

(iii) $\Rightarrow$ (ii). Define $(*)$ on R as follows: Writing a typical element of R (uniquely) as $\Sigma_\alpha k_\alpha z_1^{\alpha_1}\cdots z_q^{\alpha_q}$ summed over all $\alpha = (\alpha_1, \cdots, \alpha_q) \in \{0, 1\}^q$, with k_α in K, define $(\Sigma_\alpha k_\alpha z_1^{\alpha_1}\cdots z_q^{\alpha_q})^* = \Sigma_\alpha z_q^{\alpha_q}\cdots z_1^{\alpha_1}\tau(k)$. The following verification check $(*)$ is an anti-automorphism:

(i) $(k_1k_2)^* = \tau(k_1k_2) = \tau(k_2k_1) = (k_2k_1)^*$;

(ii) $(kz_i)^* = z_i\tau(k) = z_i^* k^*$;

(iii) $(z_i^2)^* = b_i^* = \tau(b_i) = b_i = (z_i^*)^2$ (here we used (6));

(iv) for $i < j$, $(z_iz_j)^* = z_jz_i = z_j^* z_i^*$;

(v) for $i > j$, $(z_i z_j)^* = (u_{ij} z_j z_i)^* = z_i z_j \tau(u_{ij}) = z_i z_j \sigma_i \sigma_j(u_{ji}) = u_{ji} z_i z_j = z_j z_i = z_j^* z_i^*$ (here we used (5)).

But (*) has degree 2, and so is an involution. An analogous argument works defining $(\Sigma_\alpha k_\alpha z_1^{\alpha_1} \cdots z_q^{\alpha_q})^* = \Sigma_\alpha \mu_1^{\alpha_1} \cdots \mu_q^{\alpha_q} z_q^{\alpha_q} \cdots z_1^{\alpha_1}(k)$ for arbitrary $\mu_i = \pm 1$. The involution is of the first kind, since F is the center and it is τ-invariant.

Q.E.D.

Write (K, G, U, B, τ) to denote the abelian crossed product (K, G, U, B) with involution whose restriction to K is τ (satisfying (5) and (6)). *For the remainder of the section,* $G \approx \mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2$, so that, for suitable ξ_i, $K = F(\xi_1, \xi_2, \xi_3)$, with $\alpha_i = \xi_i^2 \in F$, $\sigma_i(\xi_i) = -\xi_i$, and $\sigma_i(\xi_j) = \xi_j$ for $i \neq j$. Choose $\tau = \sigma_1\sigma_2\sigma_3$. Then the conditions in the previous theorem have a simpler form. Write Σ_3 for the symmetric group, i.e., all permutations of $(1, 2, 3)$; for π in Σ_3, write $\operatorname{sg} \pi$ for the sign (± 1) of π.

Further relations between the set U and B, to be used later, is given in the following results:

THEOREM 2.2. *Suppose* $U \subseteq K$ *satisfies* (1), (2) *and* (5) *for* $\tau = \sigma_1\sigma_2\sigma_3$. *Put* $v_3 = u_{12}$, $v_2 = u_{31}$ *and* $v_1 = u_{23}$; *we have* $v_{\pi 3} = (u_{\pi 1, \pi 2})^{\operatorname{sg} \pi}$ *for all* $\pi \in \Sigma_3$, *and*:

(i) *The* v_i*'s satisfy the following two relations*:

(2′) $v_1 v_2 v_3 = \pm 1$,

(3′) $N_i(v_i) = 1$ *for* $i = 1, 2, 3$.

(ii) *There exists a set* $B = \{b_1, b_2, b_3\}$, *uniquely determined up to multiples by elements of* F, *which satisfy for every* $\pi \in \Sigma_3$

(4′) $\sigma_{\pi 1}(b_{\pi 2}) b_{\pi 2}^{-1} = N_{\pi 2}(v_{\pi 3})^{\operatorname{sg} \pi}$,

(5′) $\sigma_i(b_i) = b_i$.

(iii) *The set* $\{U, B\}$ *satisfies all the six conditions* (1)–(6).

PROOF. (i) For $\pi \in \Sigma_3$, $\tau = \sigma_1\sigma_2\sigma_3 = \sigma_{\pi 1}\sigma_{\pi 2}\sigma_{\pi 3}$; so by (5):

$$1 = \sigma_{\pi 1}\sigma_{\pi 2}\sigma_{\pi 3}(u_{\pi 1, \pi 2})\sigma_{\pi 1}\sigma_{\pi 2}(u_{\pi 1, \pi 2}) = \sigma_{\pi 1}\sigma_{\pi 2}(N_{\pi 3}(v_{\pi 3})^{\operatorname{sg} \pi})$$

yielding (3′). Thus $\sigma_i(v_i) = v_i^{-1}$ for all i, and (2) implies that:

$$v_1^{-1} v_2^{-1} v_3^{-1} = \sigma_1(v_1)\sigma_2(v_2)\sigma_3(v_3) = \sigma_1(u_{23})\sigma_2(u_{31})\sigma_3(u_{12}) = u_{23}u_{31}u_{12} = v_1 v_2 v_3.$$

Thus $(v_1 v_2 v_3)^2 = 1$ proving (2′).

(ii) First we observe that U satisfies also (3); indeed, by (2′):

$$N_{\pi 1} N_{\pi 2}(u_{\pi 1, \pi 2}) = N_{\pi 1} N_{\pi 2}(v_{\pi 3})^{\operatorname{sg} \pi} = N_{\pi 1} N_{\pi 2}(v_{\pi 1}^{-1} v_{\pi 2}^{-1})^{\operatorname{sg} \pi}$$

$$= N_{\pi 2}(N_{\pi 1}(v_{\pi 1}))^{-\operatorname{sg} \pi} \cdot N_{\pi 1}(N_{\pi 2}(v_{\pi 2}))^{-\operatorname{sg} \pi} = 1$$

yielding (3).

The existence of the set B satisfying (4) follows now by (iii) of Remark 2.0. For $i = j$, (4) yields $\sigma_i(b_i) = b_i$, that is (5'), and for $i \neq j$, it yields (4') by definition of the v's.

(iii) It remains to show that B satisfies also (6). By taking a permutation in which $\pi 1$ and $\pi 2$ change places and another in which $\pi 1$ and $\pi 3$ changed, we obtain from (4') and (3'):

$$\sigma_{\pi 2}(b_{\pi 1})b_{\pi 1}^{-1} = N_{\pi 1}(v_{\pi 3})^{-\mathrm{sg}\,\pi} = N_{\pi 1}(v_{\pi 1}v_{\pi 2})^{\mathrm{sg}\,\pi} = N_{\pi 1}(v_{\pi 2})^{\mathrm{sg}\,\pi} = \sigma_{\pi 3}(b_{\pi 1})b_{\pi 1}^{-1}.$$

Thus, $\sigma_{\pi 2}(b_{\pi 1}) = \sigma_{\pi 3}(b_{\pi 1})$. Consequently, by (5'):

$$\tau(b_{\pi 1}) = \sigma_{\pi 1}\sigma_{\pi 2}\sigma_{\pi 3}(b_{\pi 1}) = \sigma_{\pi 2}\sigma_{\pi 3}(b_{\pi 1}) = \sigma_{\pi 2}^2(b_{\pi 1}) = b_{\pi 1}$$

proving (6).

The converse of this theorem also holds. Namely,

THEOREM 2.3. *Given v_1, v_2, v_3 in K satisfying* (2') *and* (3'), *we can define for every $\pi \in \Sigma_3$, $u_{\pi 1 \pi 2} = (v_{\pi 3})^{\mathrm{sg}\,\pi}$ and $u_{ii} = 1$; then $U = \{u_{ij}\}$ is well defined and satisfies* (1), (2) *and* (5) *for $\tau = \sigma_1\sigma_2\sigma_3$, and hence all conditions of Theorem* 2.2.

PROOF. Clearly U is well defined and satisfies (1). Reversing the first line of (i) shows that (3') yields (5). Finally, by (3') and (2'), it follows that $\sigma_1(v_1)\sigma_2(v_2)\sigma_3(v_3) = v_1^{-1}v_2^{-1}v_3^{-1} = v_1v_2v_3$, so (2) follows from Remark 2.0(i).

The preceding theorems also yield an interesting consequence on the elements of B:

COROLLARY 2.4. *Let $B = \{b_1, b_2, b_3\}$ be determined in* (ii) *of Theorem* 2.2, *then for every $\pi \in \Sigma_3$, $b_{\pi 1} \in F(\xi_{\pi 2}\xi_{\pi 3}) \cap F(\xi_{\pi 2})N_{\pi 1}(K)$. In particular*

(7) $b_1 \in F(\xi_2\xi_3) \cap F(\xi_2)N_1(K) \cap F(\xi_3)N_1(K)$.

PROOF. By (5') $\sigma_{\pi 1}(b_{\pi 1}) = b_{\pi 1}$, and by the proof of (iii) of Theorem 2.2, it follows that $\sigma_{\pi 2}(b_{\pi 1}) = \sigma_{\pi 3}(b_{\pi 1})$. That is, $b_{\pi 1}$ is invariant under $\sigma_{\pi 1}$ and $\sigma_{\pi 2}\sigma_{\pi 3}$ yielding $b_{\pi 1} \in F(\xi_{\pi 2}\xi_{\pi 3})$.

By (3') and Hilbert's theorem 90, there exists $y \in K$ with $v_{\pi 3} = \sigma_{\pi 3}(y)y^{-1}$. Since $\sigma_{\pi 3}(b_{\pi 1}) = \sigma_{\pi 2}(b_{\pi 1})$, we apply (4') and get:

$$\sigma_{\pi 3}(b_{\pi 1})b_{\pi 1}^{-1} = \sigma_{\pi 2}(b_{\pi 1})b_{\pi 1}^{-1} = N_{\pi 1}(v_{\pi 3})^{-\mathrm{sg}\,\pi} = N_{\pi 1}(\sigma_{\pi 3}(y)y^{-1})^{-\mathrm{sg}\,\pi},$$

proving that $w = b_{\pi 1}N_{\pi 1}(y)^{\mathrm{sg}\,\pi}$ is invariant under $\sigma_{\pi 3}$. But both $b_{\pi 1}$ (by (5')) and $N_{\pi 1}(y)$ are invariant under $\sigma_{\pi 1}$ proving that $b_{\pi 1} \in F(\xi_{\pi 2})N_1(K)$, since $w \in F(\xi_{\pi 2})$.

By taking successively, $\pi = (1,2,3)$, the identity, and $\pi = (1,2,3)$ we obtain (7).

The converse of Corollary 2.4 also holds:

THEOREM 2.5. *Suppose* $0 \neq b \in F(\xi_2\xi_3) \cap F(\xi_2)N_1(K) \cap F(\xi_3)N_1(K)$. *Then there exists* $V = \{v_1, v_2, v_3\}$ *(and hence a set U, by Theorem* 2.3*) satisfying* (2′), (3′) *and a corresponding* $B = \{b_1, b_2, b_3\}$ *(of Theorem* 2.2*) satisfying* (4′) *and* (5′)— *and* $b_1 = b$.

PROOF. Write $b = a_2N_1(y_2) = a_3N_1(y_3^{-1})$ with $a_i \in F(\xi_i)$ and $y_i \in K$. Put $v_2 = \sigma_2(y_3)^{-1}y_3$, $v_3 = \sigma_3(y_2)^{-1}y_2$, and $v_1 = (v_2v_3)^{-1}$.

By definition (2′) holds, and also $N_2(v_2) = N_3(v_3) = 1$. Moreover,

$$N_1(v_3)^{-1} = N_1(y_2)^{-1}\sigma_3(N(y_2)) = b^{-1}\sigma_3(b) = b^{-1}\sigma_2(b),$$

since $\sigma_3(a_2) = a_2$; $N_1(v_2) = N_1(y_3)\sigma_2(N_1(y_3))^{-1} = b^{-1}\sigma_2(b) = b^{-1}\sigma_3(b)$. Thus $N_1(v_1) = N_1(v_2v_3)^{-1} = N_1(v_2)^{-1}N_1(v_3)^{-1} = 1$, yielding (3′). Therefore, by Theorem 2.5, we have B satisfying (4′) and (5′). Moreover, from (5′) and the assumption of our theorem, it follows that $bb_1^{-1} \in F(\xi_2\xi_3)$. Hence:

$$\sigma_2(bb_1^{-1})(bb_1^{-1})^{-1} = \sigma_2(b)b^{-1}(\sigma_2(b_1)b_1^{-1})^{-1} = N_1(v_3)^{-1}N_1(v_3) = 1,$$

and likewise $\sigma_3(bb_1^{-1})(bb_1^{-1})^{-1} = 1$, proving $bb_1^{-1} \in F$. We can now, clearly, replace b_1 by b as desired. Q.E.D.

§3. Generic abelian crossed products with involution

Let K be a Galois extension of F, with abelian Galois group $G = \langle\sigma_1\rangle \oplus \cdots \oplus \langle\sigma_q\rangle$, each σ_i having order 2, and let $U = (u_{ij})$ be a set of elements in K satisfying equations (1), (2), (3) of §2. The "generic abelian crossed product" of [2] determined by U is defined as follows:

Consider the ring of polynomials $K[x_1, \cdots, x_q]$ in noncommutative indeterminates satisfying the relations

$$x_ik = \sigma_i(k)x_i, \quad k \in K; \qquad x_ix_j = u_{ij}x_jx_i \quad \text{for all } i, j.$$

Then $K[x_1, \cdots, x_q]$ is an Ore domain over with a ring of quotients which is a division ring written $K(x_1, \cdots, x_q)$, whose structure can be described as follows (cf. [2, theorem 2.3]):

Take $B = \{b_1, \cdots, b_q\}$ as in Remark 2.0, which satisfy (4), and define $y_i = b_i^{-1}x_i^2$. Then the Cent $K(x_1, \cdots, x_q) = F(y_1, \cdots, y_q)$ which we denote by F'. The

algebra $K(x_1, \cdots, x_q)$ is also a crossed product of the group G —in our notation, of the form (K', G, U, B'), where $B' = (x_1^2, \cdots, x_q^2)$ and $K' = K(y_1, \cdots, y_q)$ with the automorphisms $\sigma \in G$ extended to K' by setting $\sigma(y_i) = y_i$ for all i. The invariant field of K' is then $F(y_1, \cdots, y_q)$.

This is readily obtained (cf. [2]) when the x_i take the place of the z_i of section 2; and $b_i' = x_i^2 = b_i(b_i^{-1}x_i^2) = b_i y_i \in K'$. The set $\{U, B\}$, now satisfies (1)–(4), since the $b_i' = x_i^2$ are multiples of the b_i by central elements.

Note also that $K(x_1, \cdots, x_q)$ is thus a finite dimensional algebra over its center F', and $K(x_1, \cdots, x_q)$ as well as the polynomial ring $K[x_1, \cdots, x_q]$ are PI-domains. Therefore, $K(x_1, \cdots, x_q)$ is the ring of *central* quotients (cf. [3]) of $K[x_1, \cdots, x_q]$.

This algebra will have an involution, if in addition we shall assume that $U = \{u_{ij}\}$ with respect to $\tau \in G$ will satisfy (5) and B', or equivalently B, will satisfy (6). The second requirement is superfluous in two cases:

$\tau = 1$; or, by Theorem 2.2, if $q = 3$, $\tau = \sigma_1\sigma_2\sigma_3$, where the U need only satisfy (1), (2) and (5). In these cases $K(x_1, \cdots, x_q)$ will have an involution $(*)$ whose restriction to K' is τ. Note that τ fixes F' and so $(*)$ is of the first kind.

NOTATION. The generic crossed product (K', G, U, B', τ) will be denoted henceforth by (K, U, τ). Write $K[x]$ for $K[x_1, \cdots, x_q]$. Each element of $K[x]$ can be written uniquely in the form $f = \Sigma k_\mu x_1^{\mu_1} \cdots x_q^{\mu_q}$, write $\nu(f)$ for the element $k_\mu x_1^{\mu_1} \cdots x_q^{\mu_q}$ with largest $\mu = (\mu_1, \cdots, \mu_q)$, $k_\mu \neq 0$ when ordered lexicographically. Also note that $(*)$ acts on $K[x]$ by $(\Sigma k_\mu x_1^{\mu_1} \cdots x_q^{\mu_q})^* = \Sigma x_q^{\mu_q} \cdots x_1^{\mu_1} \tau(k_\mu)$.

PROPOSITION 3.1. *$\nu(f_1 f_2) = \nu(f_1)\nu(f_2)$; if $f \neq 0$ then $\nu(f) \neq 0$; $\nu(f^*) = \nu(f)^*$.*

PROOF. Clear by the definition. Q.E.D.

PROPOSITION 3.2. *If the algebra $A = (K, U, \tau)$ is a product of quaternions, then A has a q-generating set S containing 4^q elements of the following form: Each element of S has the form $k_i x_1^{\mu_1} \cdots x_q^{\mu_q}$, where $k_i \in K$ and $\mu_1, \cdots, \mu_q \in \{0, 1\}$; moreover for each (μ) there are 2^q elements of S of the form $k_i x_1^{\mu_1} \cdots x_q^{\mu_q}$, and, in particular, there are 2^q elements of $S \cap K$.*

PROOF. A has degree 2^q so, by Proposition 1.2, A has a q-generating set $S_1 = \{a_1, \cdots, a_t\}$, where $t = 4^q$. Write $a_i = f_i g_i^{-1}$, $f_i \in K[x]$, $g_i \in \text{Cent}(K[x])$, $1 \leqq i \leqq t$. Then $\{f_1, \cdots, f_t\}$ is a q-generating set, so $\{\nu(f_1), \cdots, \nu(f_t)\}$ is a q-generating set. But each $\nu(f_i)$ can be written as $a_i x_1^{i_1} \cdots x_q^{i_q}$, $a_i \in K$. Putting

$j_1 = [i_1/2], \cdots, j_q = [i_q/2]$ and $c_i = y_1^{j_1} \cdots y_q^{j_q} = (b_1^{j_1} \cdots b_q^{j_q})^{-1} x_1^{2j_1} \cdots x_q^{2j_q}$ elements of the center, we have $\nu(f_i)c_i^{-1}$ is the desired form $k_i x_1^{\mu_1} \cdots x_q^{\mu_q}$; since $c_i \in F'$, we see $S = \{\nu(f_1)c_1^{-1}, \cdots, \nu(f_t)c_t^{-1}\}$ is a q-generating set.

For each (μ), the number of possible F'-independent elements with $\mu_j \in \{0, 1\}$ of the form $k_i x_1^{\mu_1} \cdots x_q^{\mu_q}$ is at most 2^q, and the number of different monomial $x_1^{\mu_1} \cdots x_q^{\mu_q}$, is also 2^q; on the other hand the elements of the total number is 4^q; since the elements of S are F'-independent, this bound must be achieved in S in each subset $\{k_i x_1^{\mu_1} \cdots x_q^{\mu_q}\}$ for each (μ) as required. Q.E.D.

We are in a position to present an important criterion for a generic abelian crossed product with Galois $\mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2$ to be a tensor product of quaternions. From now on we restrict ourselves to the case $q = 3$.

THEOREM 3.3. *Suppose* $\tau = \sigma_1\sigma_2\sigma_3$, *$U$ satisfies* (1), (2), (3) *and B chosen by Remark* 2.0 *to satisfy* (4). *Then the generic abelian crossed product $A = (K, U, \tau)$ is a product of quaternions iff* $b_1 \in FN_1(K)$.

PROOF. If A is a product of quaternions then the q-generating set of Proposition 3.2 will contain some element kx_1, and so $(kx_1)^2 \in F' = \text{Cent}(A)$. But $(kx_1)^2 = k\sigma_1(k)x_1^2 = k\sigma_1(k)b_1y_1$ (where $y_1 = b_1^{-1}x_1^2 \in F'$), implying $k\sigma_1(k)b_1 \in F' \cap K = F$, i.e. $b_1 \in FN_1(K)$.

Conversely, if $b_1k\sigma_1(k) \in F$ for some k in K, then (ξ_1, kx_1) is a q-generating set of A (notation as preceding Theorem 2.2), so by Proposition 1.1(ii), A has an F'-quaternion subalgebra Q_1; thus $A \approx Q_1 \otimes_{F'} A'$, where A' is the centralizer of Q_1 in A. Now A has exponent 2 in the Brauer group, by [1, p. 161, theorem 19] so A' has exponent 2, implying A' is a product of quaternions, hence A is a product of quaternions. Q.E.D.

When (K, U, τ) is a tensor product of quaternions, our next result is a necessary and sufficient condition for one factor to be invariant under the involution.

THEOREM 3.4. *Suppose U and B satisfy* (1)–(6) *with respect to* $\tau = 1$. *If $A = (K, U, \tau)$ is a product of quaternions invariant under the involution* (*) *described above, then* $b_1 = \alpha N_1(k)$ *for suitable* $\alpha \in F$, $k \in K$, *with* $\sigma_1(k) = \pm k$.

PROOF. By Proposition 1.3, A has a q-generating set of elements $\{r_1, \cdots, r_t\}$ where $t = 2^q$, with $r_i^* = \pm r_i$, $1 \leqq i \leqq t$. In the construction of S in Proposition 3.2, we see $(c_i^{-1}\nu(r_i))^* = c_i^{-1}\nu(r_i^*) = \pm c_i^{-1}\nu(r_i)$. Thus, S has some element kx_1 with $(kx_1)^2 \in F'$ and $(kx_1)^* = \pm kx_1$. Hence $b_1 \in FN_1(k^{-1})$ as in Theorem 3.3, and $\pm kx_1 = (kx_1)^*x_1k$, implying $\sigma_1(k^{-1}) = \pm k^{-1}$. Q.E.D.

Conversely, if $b = \alpha N_1(k)$ with $\sigma_1(k) = \pm k$, then (ξ_1, kx_1) are a q-generating set with $(kx_1)^* = kx_1$, so A has a $(*)$-invariant quaternion subalgebra.

We now can give our criteria.

THEOREM 3.5. *Suppose $q = 3$, notation as before Lemma 2.2, and $\tau = \sigma_1\sigma_2\sigma_3$. If there exists b satisfying (7), i.e. $b \in F(\xi_2\xi_3) \cap F(\xi_2)N_1(K) \cap F(\xi_3)N_1(K)$ but $b \notin FN_1(K)$ then there is a generic abelian crossed product $A = (K, U, \tau)$ for some U, such that A is a division algebra of degree 8, with involution, which is not isomorphic to a tensor product of quaternion algebras.*

PROOF. By Theorem 2.5, we get v_1, v_2, v_3 and B, with $b_1 = b$, satisfying (2')–(5'); using Theorem 2.2, we get U satisfying (1)–(6), yielding a generic abelian crossed product $A = (K, U, \tau)$ with involution. By Theorem 3.3, A is not a product of quaternions.

THEOREM 3.6. *Suppose $q = 2$, $K = F(\xi_1, \xi_2)$, with $\xi_i^2 \in F$ and $\sigma_i(\xi_i) = -\xi_i$, $\sigma_j(\xi_i) = \xi_i$ for $j \neq i$. If $b \in FN_1(K)$ and $b \notin Fa^2$ for all $a \in F(\xi_2)$, then, for $\tau = 1$, the generic abelian crossed product with involution $A = (K, G, U, \tau)$ is a tensor product of quaternions but has no quaternion subalgebra invariant under the involution.*

PROOF. Write $b = \alpha N_1(k)$, for $\alpha \in F$, $k \in K$. Let $u_{11} = u_{22} = 1$, $u_{21} = \sigma_1\sigma_2(k)k^{-1}$, and $u_{12} = u_{21}^{-1}$. Then (1), (2), (3), and (5) hold and, by Remark 2.0, there exists $B = (b_1, b_2)$ satisfying (4) (and trivially satisfying (6)). Also $b_1b^{-1} \in F$ since $\sigma_1(b_1b^{-1}) = b_1b^{-1}$ and $\sigma_2(b_1b^{-1})(b_1b^{-1})^{-1} = (\sigma_2(b_1)b_1^{-1})(\sigma_2(b)b^{-1})^{-1}$

$$N_1(u_{21})(\sigma_2(N_1(k))N_1(k)^{-1})^{-1} = N_1(u_{21})N_1(u_{21})^{-1} = 1.$$

Hence we may replace b_1 by b. Construct (K, U, τ), which by Theorem 3.4, will be a product of $(*)$-invariant quaternions iff $b \in FN_1(a_0)$ with $\sigma_1(a_0) = \pm a_0$. Then for some a in $F(\xi_2)$, either $a_0 = a$ or $a_0 = a\xi_1$, implying in either case $b = Fa^2$ contrary to hypothesis.

§4. Equivalent conditions

To show there exist fields K and an element b which satisfy the hypothesis of Theorem 3.6, we replace these conditions by equivalent or weaker ones. A different method of obtaining these results will be given in section 6.

Suppose $H \supset L$ is a finite field extension and T is a subset of H. Write

$N(T; H/L)$ for $\{\text{norm}(x) \mid x \in T\}$, the norm taken from H to L, and write $N(H/L)$ for $N(H; H/L)$. We take $K = F(\xi_1, \xi_2, \xi_3)$ as described preceding Theorem 2.2. Note that $N_i(\xi_i) = -\xi_i^2 = -\alpha_i$, and $N_i(\xi_j) = \xi_j^2 = \alpha_j$ for $j \neq i$. Let $F_1 = F(\xi_2\xi_3)$.

LEMMA 4.1. $N_1(K) \cap F_1 = N(F_1(\xi_1)/F_1)N(F_1(\xi_1\xi_2)/F_1)$.

PROOF. $(\supseteq)$ is trivial, because each norm on the right is contained in the left.

To prove $(\subseteq)$, suppose $a = N_1(u) \in F_1$. If $u \in F_1(\xi_1)$ then $a = N_1(u) \in N(F_1(\xi_1)/F_1) \cdot 1$ and we are done; thus we may assume $u \notin F_1(\xi_1)$. Then $u = u_1(u_2 + \xi_2)$ for suitable u_1, u_2 in $F_1(\xi_1)$, since $1, \xi_2$ are a base of K over $F_1(\xi_1) = F(\xi_1, \xi_2\xi_3)$; hence $a = N_1(u) = N_1(u_1)N_1(u_2 + \xi_2) \in F_1$, implying $N_1(u_2 + \xi_2) \in F_1$. But $N_1(u_2 + \xi_2) = N_1(u_2) + \xi_2(u_2 + \sigma_1(u_2)) + \alpha_2$, so $u_2 + \sigma_1(u_2) = 0$, implying $u_2 = w\xi_2$ for some w in F_1. Now,

$$a = N_1(u) = N_1(u_1)(-N_1(w)\alpha_1 + \alpha_2) = N_1(u_1\xi_1)N_1(w + \alpha_1^{-1}\xi_1\xi_2)$$

$$\in N(F_1(\xi_1)/F_1)N(F_1(\xi_1\xi_2)/F_1). \qquad \text{Q.E.D.}$$

COROLLARY 4.2. *If* $b \in FN_1(K) \cap F(\xi_2\xi_3)$, *then*

$$N(b; F_1/F) \in N(F(\xi_1)/F)[N(F(\xi_1\xi_2)/F) \cap N(F(\xi_2\xi_3)/F].$$

PROOF. Write $b = \alpha a$ for $\alpha \in F$, $a \in N_1(K) \cap F_1$, and we use our notation $F_1 = F(\xi_2\xi_3)$. By Lemma 4.1, $a \in N(F_1(\xi_1)/F_1)N(F_1(\xi_1\xi_2)/F_1)$, so

$$N(b; F_1/F) = \alpha^2 N(a; F_1/F) \in \alpha^2 N(N(F_1(\xi_1)/F_1); F_1/F) \cdot N(N(F_1(\xi_1\xi_2)/F_1); F_1/F).$$

Now $N(N(F_1(\xi_1)/F_1); F_1/F) = N(F_1(\xi_1)/F) = N[N(F_1(\xi_1)/F(\xi_1)); F(\xi_1)/F] \subseteq N[F(\xi_1)/F]$; and likewise $N[N(F_1(\xi_1\xi_2)/F_1); F_1/F] = N[F_1(\xi_1\xi_2)/F] = N[N(F_1(\xi_1\xi_2)/F(\xi_1\xi_2)); F(\xi_1\xi_2)/F] \subseteq N[F(\xi_1\xi_2)/F]$, and also $N(F_1(\xi_1\xi_2)/F) = N(N(F_1(\xi_1\xi_2)/F_1); F_1/F) \subseteq N(F_1/F)$. Thus

$$N(b; F_1/F) \in \alpha^2 N[F(\xi_1)/F][N(F(\xi_1\xi_2)/F) \cap N(F_1/F)]$$

$$\subseteq N[F(\xi_1)/F][N(F(\xi_1\xi_2)/F) \cap N(F(\xi_2\xi_3)/F],$$

$F_1 = F(\xi_2\xi_3)$.

The conditions for b in Theorem 3.5 can be modified by the following result.

LEMMA 4.3. *Let* $b \in F(\xi_2, \xi_3)$, *then* $b \in F(\xi_2)N_1(K)$ *iff* $N_3(b) \in N(F(\xi_1, \xi_2)/F(\xi_2))$.

PROOF. If $b = a_2 N_1(k)$ for $a_2 \in F(\xi_2)$, then

$$N_3(b) = N_3(a_2)N_3(N_1(k)) = a_2^2 N_1(N_3(k)) = N_1(a_2 N_3(k)),$$

and $a_2 N_3(k) \in F(\xi_1, \xi_2)$.

Conversely, suppose $N_3(b) = N_1(k_0)$ for some $k_0 \in F(\xi_1, \xi_2)$, and let $k = b + k_0$. Writing k_0' for $k_0 + \sigma_1(k_0) \in F(\xi_2)$, we have

$$N_1(k) = N_1(b + k_0) = b^2 + bk_0' + N_1(k_0) = b^2 + bk_0' + N_3(b) = b(b + \sigma_3(b) + k_0').$$

But $(b + \sigma_3(b)) + k_0' \in F(\xi_2)$, we are done unless $k = 0$; then

$$b = -k_0 \in F(\xi_2, \xi_3) \cap F(\xi_1, \xi_2) = F(\xi_2),$$

and we can take $k = 1$. Q.E.D.

If $b \in F_1$ then $\sigma_3(b) = \sigma_2(b)$, and the analogous result to Lemma 4.3 with σ_2 and σ_3 reversed yields:

COROLLARY 4.4. *An element b satisfies* (7). *That is, if $b \in F(\xi_2\xi_3)$, then $b \in F(\xi_2)N_1(K) \cap F(\xi_3)N_1(K)$ iff*

$$N_2(b) = N_3(b) \in N[F(\xi_1, \xi_2)/F(\xi_2)] \cap N[F(\xi_1, \xi_3)/F(\xi_3)].$$

§5. The counterexamples

THEOREM 5.1. *Let $F = Q(\lambda)$, the field of rational functions in an indeterminate over the rationals Q. There is a Galois extension $K = F(\xi_1, \xi_2, \xi_3)$ over F of degree* 8, *with $\xi_i^2 \in F$, and $U = (u_{ij}) \subset K$ satisfying equations* (1), (2), (3), (5), *such that (K, U, τ) is a domain algebra of degree* 8 *with involution (of First Kind), not isomorphic to a tensor product of quaternions. (Here $G = \langle\sigma_1\rangle \oplus \langle\sigma_2\rangle \oplus \langle\sigma_3\rangle$ has exponent* 2.)

PROOF. Take $\xi_1^2 = -1$, $\xi_2^2 = -(\lambda^2 + 1)$, and $\xi_3^2 = \lambda$. By Theorem 3.5, we need only find $b \in F(\xi_2\xi_3) \cap F(\xi_2)N_1(K) \cap F(\xi_3)N_1(K)$ with $b \notin FN_1(K)$. Take $b = \xi_2\xi_3 \in F(\xi_2\xi_3)$. Then

$$N_2(b) = N_3(b) = \lambda(\lambda^2 + 1)$$

$$= N_1(\tfrac{1}{2}\xi_2[(\lambda - 1 - \xi_2) + (\lambda - 1 + \xi_2)\xi_1] = N_1[(\xi_1\xi_3)(\lambda\xi_1 - 1)]$$

so, by Corollary 4.4, $b \in F(\xi_2)N_1(K) \cap F(\xi_3)N_1(K)$.

It remains to show $b \notin FN_1(K)$, which is more difficult. By Corollary 4.2, we need to prove

$$N(b; F_1/F) = N_2(b) \notin N(F(\xi_1)/F)[N(F(\xi_1\xi_2)/F) \cap N(F(\xi_2\xi_3)/F)].$$

We shall in fact obtain a contradiction, from its negation that

$$\lambda(\lambda^2+1) = N_1(f_1)N(f_2; F(\xi_1\xi_2)/F) = N_1(f_1)N(f_3; F(\xi_2\xi_3)/F)$$

for suitable f_1 in $F(\xi_1)$, f_2 in $F(\xi_1\xi_2)$, f_3 in $F(\xi_2\xi_3)$. There exist polynomials $0 \neq g$, $g_1, g_2, g_3, g_4, g_5, g_6 \in \mathbf{Z}[\lambda]$ such that $f_1^{-1} = (g_1 + g_2\xi_1)g^{-1}$, $f_2 = (g_3 + g_4\xi_1\xi_2)g^{-1}$, and $f_3 = (g_5 + g_6\xi_2\xi_3)g^{-1}$. Clearing out g, we get

(8) $\lambda(\lambda^2+1)(g_1^2+g_2^2) = g_3^2 - (\lambda^2+1)g_4^2 = g_5^2 + \lambda(\lambda^2+1)g_6^2$.

However, we shall show (8) is impossible; otherwise choose a solution with the greatest common divisor of $g_1, g_2, g_3, g_4, g_5, g_6$ (in $\mathbf{Z}[\lambda]$) equal to 1. Taking the canonical homomorphism in $(\mathbf{Z}/2\mathbf{Z})[\lambda]$ (and noting that $(\bar{c}+\bar{d})^2 = \bar{c}^2 + \bar{d}^2$) yields

(9) $\bar{\lambda}(\bar{\lambda}+1)^2(\bar{g}_1+\bar{g}_2)^2 = (\bar{g}_3 + (\bar{\lambda}+1)\bar{g}_4)^2 = \bar{g}_5^2 + \bar{\lambda}(\bar{\lambda}+1)^2\bar{g}_6^2$.

By unique factorization, noting that $\bar{\lambda}$ occurs to an odd power in the left-hand side and to an even power in the middle, we get all sides equal to 0. Hence

(10) $\bar{g}_1 = \bar{g}_2$,

(11) $\bar{g}_3 = (\bar{\lambda}+1)\bar{g}_4$,

(12) $\bar{g}_5^2 = \bar{\lambda}(\bar{\lambda}+1)^2\bar{g}_6^2$.

Applying the same argument to (12) yields $\bar{g}_5 = 0$, so $\bar{g}_6 = 0$. Thus $2|g_5$ and $2|g_6$, implying $4|(g_5^2 + \lambda(\lambda^2+1)g_6^2)$. Thus, by (7), $4|(\lambda^2+1)(g_1^2+g_2^2)$, yielding

(13) $4|(g_1^2+g_2^2)$;

likewise

(14) $4|g_3^2 - (\lambda^2+1)g_4^2$.

From (10) we can write $g_1 = g_2 + 2h_1$ for some $h_1 = \mathbf{Z}[\lambda]$; then, by (13), 4 divides $2g_2^2 + 4g_2h_1 + 4h_1^2$, implying $2|g_2$, and therefore also $2|g_1$.

From (11) we also can write $g_3 = (\lambda+1)g_4 + 2h_3$ for some h_3 in $\mathbf{Z}[\lambda]$. By (13), 4 divides $(((\lambda+1)g_4 + 2h_3)^2 - (\lambda^2+1)g_4^2) = 2\lambda g_4^2 + 4(\lambda+1)g_4h_3 + 4h_3^2$, so $2|g_4$; thus $2|g_3$ also. Hence $2|g_i$ for each i, contrary to their g.c.d. being 1. This contradiction shows (13) holds. Q.E.D.

The second counterexample is easier.

THEOREM 5.2. *The field $F = Q(\lambda)$ has an extension $K = F(\xi_1, \xi_2)$ with $\xi_i^2 \in F$, $U \subset K$, such that $(K, U, 1)$ does not have any quaternion subalgebras invariant under the given involution (Here $G = \langle\sigma_1\rangle \oplus \langle\sigma_2\rangle$.)*

PROOF. Take $\xi_1^2 = 2$, $\xi_2^2 = \lambda$, and $b = \lambda - 1 + 2\xi_2$. Then $b = N_1(\xi_2 + 1 - \xi_1)$; on the other hand, $f(\lambda)b$ is not a square in $F(\xi_2) = Q(\sqrt{\lambda})$, as can be easily seen through unique factorization in the ring $Q[\sqrt{\lambda}]$. Thus we are done by Theorem 3.6. Q.E.D.

REMARK 5.3. If we take K, F as in Theorem 5.1, and for $t > 3$, letting

$\xi_4, \cdots, \xi_t$ be commutative indeterminates over K, define $K_t = K(\xi_4, \cdots, \xi_t)$ and $F_t = F(\xi_4^2, \cdots, \xi_t^2) \subset K_t$; then K_t is Galois over F_t with Galois group $G_t = \mathbf{Z}_2 + \cdots + \mathbf{Z}_2$, taken t times.

Define U_t by taking $u_{ij} = 1$ whenever $i > 3$ or $j > 3$, otherwise take u_{ij} from U. One sees easily that $(K_t, G_t, U_t, \sigma_1\sigma_2\sigma_3)$ also is an abelian crossed product of degree 2^t with involution, not a product of quaternions. A similar construction will extend Theorem 5.2.

§6. Another proof of the results of §4

We can motivate the results of §4 through quadratic descent. Consider the quaternion F-algebra $Q = (\alpha, \beta; F)$. Then there are elements y_i in Q, with $y_1^2 = \alpha$, $y_2^2 = \beta$, such that $y_1y_2 = -y_2y_1$. We can view Q as a cyclic algebra with maximal subfield $F(y_1)$ whose nontrivial automorphism σ over F is given by conjugation by y_2. By Wedderburn's criterion, $Q \approx M_2(F)$ iff β is a norm (with respect to σ) of some element of $F(y_1)$. Let us follow the notation preceding Lemma 2.2.

REMARK 6.1. $b \in FN_1(K)$ iff, for some element α in F, $(\alpha^{-1}b, \alpha_1; F(\xi_2, \xi_3)) \approx M_2(F)$ which, by various easy, well-known properties of the quadratic symbol, says

$$(b, \alpha_1; F(\xi_2, \xi_3)) \approx (\alpha, \alpha_1; F) \otimes_F F(\xi_2, \xi_3).$$

LEMMA 6.2. *For any quadratic extension L of F, with nonzero elements β in F and x in L, we have some γ in F with $(\beta, x; L) \approx (\beta, \gamma; L)$, iff $(\beta, N(x); F) \approx M_2(F)$ (where N denotes the norm with respect to the nontrivial automorphism σ of L over F).*

PROOF. By [1, theorem X.16], $(\beta, N(x); F) \approx M_2(F)$ iff $(\beta, x; L)$ has an involution of the second kind whose restriction to $L(\sqrt{\beta})$ is an automorphism commuting with σ. Now this is certainly the case if $(\beta, x; L) \approx (\beta, \gamma; L)$, because $(\beta, \gamma; L) \approx (\beta, \gamma; F) \otimes_F L$, so we could take an involution $(*)$ of the first kind on $(\beta, \gamma; F)$ inducing the nontrivial automorphism of $F(\sqrt{\beta})$, and consider $* \otimes \sigma$; the converse is [1, theorem X.21]. Q.E.D.

LEMMA 6.3. *For any β_i, γ_i in F, if $(\beta_1, \gamma_1; F) \approx (\beta_2, \gamma_2; F)$, then, for some μ in F, we have $(\beta_1, \gamma_1; F) \approx (\beta_1, \mu; F) \approx (\beta_2, \mu; F) \approx (\beta_2, \gamma_2; F)$.*

PROOF. View $Q = (\beta_1, \gamma_1; F) = (\beta_2, \gamma_2; F)$. If $Q = M_2(F)$, take $\mu = 1$. Otherwise take x_i, y_i in Q such that $x_i^2 = \beta_i$ and $y_i^2 = \gamma_i$. If $[x_1, x_2] = 0$ then $x_2 = \gamma_1 x_1 + \gamma_2$ for suitable $\gamma_1 \neq 0$, γ_2 in F; since $x_2^2 \in F$ we get $\gamma_2 = 0$, so we can take $\mu = \gamma_1$. If $[x_1, x_2] \neq 0$ then $x_i[x_1, x_2] = -[x_1, x_2]x_i$ for $i = 1, 2$, so we can take $\mu = [x_1, x_2]^2$. Q.E.D.

We are now ready for an alternate proof of Corollary 4.2. By Remark 4.1, we may assume for suitable β in F, that

$$M_2(F(\xi_2, \xi_3)) \approx (\beta b, \alpha_1; F(\xi_2, \xi_3)) \cong (\beta b, \alpha_1; F_1) \otimes F(\xi_2, \xi_3),$$

implying $F(\xi_2, \xi_3)$ splits $(\beta b, \alpha_1; F_1)$ and is thus a maximal subfield. Thus, for some w in F_1, $(\alpha_1, \beta b, F_1) \approx (\beta b, \alpha_1; F_1) \approx (\alpha_2, w; F_1)$ (since $F(\xi_2, \xi_3) = F_1(\xi_2)$). By Lemma 6.3, for some w' in F_1, $(\alpha_1, \beta b; F_1) \approx (\alpha_1, w'; F_1) \approx (\alpha_2, w'; F_1)$. Thus $(\alpha_1\alpha_2, w'; F_1) \approx M_2(F_1)$, implying by Wedderburn's criterion $w' \in N_1(F_1(\xi_1\xi_2))$. Also $(\alpha_1, \beta b \cdot w'; F_1) \approx M_2(F_1)$, yielding $(\alpha_1, bw'; F_1) \approx (\alpha_1, \beta; F_1)$. By Lemma 6.2, $(\alpha_1, N_3(bw'); F) \approx M_2(F)$, so $N_3(bw') \in N_1(F(\xi_1))$ and $N_3(b) \in N_1(F(\xi_1)/F)N_3((w')^{-1})$. But $w' = N_1(k^{-1})$ for some $k \in F(\xi_1\xi_2, \xi_2\xi_3)$, so $N_3((w')^{-1}) = N_3(N_1(k)) = N_1(N_3(k))$, proving the assertion. Q.E.D.

REFERENCES

1. A. A. Albert, *Structure of Algebras*, Amer. Math. Soc. Colloq. Publ. **24**, Providence, R.I., 1961.

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

3. L. Rowen, *Some results on the center of a ring with polynomial identity*, Bull. Amer. Math. Soc. **79**(1973), 219–223.

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

5. J. Tignol, *Sur les classes de similitude de corps a involution* de degré 8, C. R. Acad. Sci. Paris **A286** (1978), 875–876.

6. J. Tignol, Decomposition et descente de produits tensoriels d'algebres de quaternions, Rapport Sem. Math. Pure UCL **76**(1978).

HEBREW UNIVERSITY OF JERUSALEM
JERUSALEM, ISRAEL

AND

INSTITUTE FOR ADVANCED STUDIES
MOUNT SCOPUS, JERUSALEM, ISRAEL

UNIVERSITE CATHOLIQUE DE LOUVAIN
LOUVAIN-LA-NEUVE, BELGIUM

AND

INSTITUTE FOR ADVANCED STUDIES
MOUNT SCOPUS, JERUSALEM, ISRAEL