ISRAEL JOURNAL OF MATHEMATICS, Vol. 38, Nos. 1-2, 1981

DIVISION ALGEBRA COUNTEREXAMPLES OF DEGREE 8

BY
LOUIS H. ROWEN[†]

ABSTRACT
An example is given of a non-crossed product of degree 8 and exponent 4. On the other hand, every division algebra of degree 8 (arbitrary exponent) has a solvable splitting field; other positive results are also given.

Introduction

In the last few years, considerable general information has been determined about division algebras of degree 8, in the following order:

FACT 1. Amitsur [3]. There is a non-crossed product (of exponent 8).

FACT 2. Rowen [6]. If the exponent is 2, then there is a maximal subfield Galois with group $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$ over the center.

FACT 3. Tignol [9]. If the exponent is 2, then it is similar to a tensor product of 4 quaternion algebras (over the center).

FACT 4. Amitsur–Rowen–Tignol [5]. Notwithstanding Fact 3, there is an example of exponent 2 which is *not* a product of quaternion subalgebras.

The object of this note is to answer negatively a natural question arising from these facts:

QUESTION 1. Is there a non-crossed product of exponent 4?

The counterexample to Question 1 is an application of [8] to generic abelian crossed products [4]. Note that in [4] the roles of K and F are reversed. Some

[†] The research of the author is supported by the Anshel Pfeffer Chair.
Received June 11, 1979 and in revised form March 14, 1980

positive results also are given, including a solvable splitting field for every division algebra of degree 8.

§1. General facts

We recall from [4, lemma 1.2] that for an abelian crossed product R having maximal subfield K Galois over center F with Galois group $G = \langle\sigma_1\rangle \times \langle\sigma_2\rangle \times \cdots \times \langle\sigma_q\rangle$ there are elements $U = \{u_{ij} \mid 1 \leqq i, j \leqq q\}$ and $B = \{b_i \mid 1 \leqq i \leqq q\}$ satisfying the equations for all i, j, k (where N_i denotes the norm with respect to the automorphism σ_i):

$$u_{ii} = 1 \quad \text{and} \quad u_{ij} = u_{ji}; \tag{1}$$

$$\sigma_i(u_{jk})\sigma_j(u_{ki})\sigma_k(u_{ij}) = u_{jk}u_{ki}u_{ij}; \tag{2}$$

$$N_i(N_j(u_{ij})) = 1; \tag{3}$$

$$\sigma_j(b_i)b_i^{-1} = N_i(u_{ji}), \tag{4}$$

and (3) follows from (4).

We write $R = (K, G, U, B)$; as explained in [4, §1], K, G, U, and B determine R up to isomorphism. The generic abelian crossed product built from K, G, and U satisfying (1)–(3) above is also treated in [4, §2]; we shall denote it as (K, G, U). (Recall (K, G, U) is the quotient ring of the skew polynomial ring $K[x_1, \cdots, x_q]$ where $x_ix_j = u_{ij}x_jx_i$ and $x_iw = \sigma_i(w)x_i$ for each w in K, $1 \leqq i, j \leqq q$; then

$$b'_i = x_i^{n_i},$$

$$K' = K(b'_1, \cdots, b'_q).$$

Extend G naturally to K' by the rule $\sigma_j(b'_i) = b'_iN_i(u_{ji})$; by construction $(K, G, U) = (K', G, U, B')$. Also define: F' is the fixed field of K' under the action of G.)

With notation as above, if $R = (K, G, U, B)$ then it follows easily from (4) that $b'_ib_i^{-1}$ is fixed by each σ_j, and thus is in F'. So define

$$\alpha_i = b'_ib_i^{-1}, \qquad 1 \leqq i \leqq q.$$

Remark 1.1. Suppose $\{u_{\sigma,\tau} \mid \sigma, \tau \in G\}$ is a factor set defined in the usual way, i.e., z_σ are chosen such that $z_\sigma w z_\sigma^{-1} = \sigma(w)$ for all w in K, and $u_{\sigma\tau} = z_\sigma z_\tau z_{\tau\sigma}^{-1}$ for all σ, τ in G. Then we could define U and B as above by putting

$$u_{ij} = u_{\sigma,\tau} u_{\tau,\sigma}^{-1} \qquad \text{for } \sigma = \sigma_i, \quad \tau = \sigma_j,$$

$$b_i = \prod_{j=0}^{n_i-1} u_{\tau_j,\tau} \qquad \text{for } \tau_j = \sigma_i^j, \quad \tau = \sigma_i.$$

In view of [4, theorem 1.4], one has the following result (where R^t is defined as $R \otimes_F \cdots_F \otimes R$ taken t times):

PROPOSITION 1.2 (communicated to me by Amitsur). *Put* $U^t = \{u_{ij}^t \mid 1 \leqq i, j \leqq q\}$ *and* $B^t = \{b_i^t \mid 1 \leqq i \leqq q\}$. *In the Brauer group of* F, $[(K, G, U, B)]^t = [(K, G, U^t, B^t)]$.

REMARK 1.3. Suppose (K, G, U, B) has exponent t, in the Brauer group, i.e., $[(K, G, U, B)]^t = 1$. Then by Proposition 1.2 and [4, theorem 1.4] there are elements a_i in K such that $1 = N_i(a_i)b_i^t$ and $1 = \sigma_i(a_j)a_i a_j^{-1}\sigma_j(a_i)^{-1}u_{ij}^t$, $1 \leqq i, j \leqq q$. Writing $(K, G, U) = (K', G, U, B')$ as above and putting $b_i' = \alpha_i b_i$, we get $[(K, G, U)]^t \approx [(K', G, U'', B'')]$, where each $u_{ij}'' = 1$ and each $b_i'' = \alpha_i^t$. But by [4, lemma 1.5], (K', G, U'', B'') is a tensor product of the cyclic algebras $(K_i', \sigma_i, \alpha_i^t)$, where each K_i' is the fixed field of K' under all σ_j, $j \neq i$. This yields the following result, stated to me by Saltman, generalizing the case $t = 2$ in [5]:

PROPOSITION 1.4 (Saltman). *If G has exponent dividing t (i.e., every element of G has order t) and (K, G, U, B) has exponent dividing t, then (K, G, U) also has exponent dividing t.*

PROOF. Continuing Remark 1.3, each $[K_i', \sigma_i, \alpha_i^t] = [K_i', \sigma_i, \alpha_i]^t = 1$ (since $[K_i' : F']$ divides t); so $[(K, G, U)]^t \approx$ a tensor product of matric algebras, which is a matric algebra. Q.E.D.

§2. The counterexample — a non-crossed product of exponent 4

Take $G = \langle\sigma_1\rangle \times \langle\sigma_2\rangle$, where $\sigma_1^4 = 1$ and $\sigma_2^2 = 1$. Suppose G acts on the field K. Then we can write $K = K_1K_2$, where σ_2 fixes K_1 and σ_1 fixes K_2. Let K_0 be the fixed subfield of K_1 under σ_1^2. We examine (K, G, U, B) for suitable U, B. Note $U = \{u_{11} = 1, u_{12}, u_{21} = u_{12}^{-1}, u_{22} = 1\}$, and (2) is superfluous. *Notation as preceding Remark* 1.1; define $K_i' = K_i(\alpha_1, \alpha_2)$, for $0 \leqq i \leqq 2$.

PROPOSITION 2.1. *(K, G, U) has a maximal subfield Galois over its center with Galois group $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$, iff there is some element k in K with $b_1 \in Fk\sigma_1^2(k)$.*

PROOF. ($\Leftarrow$) Recalling $x_1^4 = b_1'$, we see $K = K_0'K_2'F'(kx_1^2)$.

($\Rightarrow$) We have eight commuting F'-independent elements whose squares are in F'; taking "leading monomials" we may assume these elements are of the form $k_i x_1^{i_1} x_2^{i_2}$, $1 \leqq i \leqq 8$, $0 \leqq i_1 \leqq 3$, $0 \leqq i_2 \leqq 1$, $k_i \in K$. (This argument is spelled out in [7, proposition 4.4].) Clearly then $i_1 \in \{0, 2\}$. We are done if $(i_1, i_2) = (2, 0)$ for some i. Otherwise $(i_1, i_2) = (0,0)$ or $(0,1)$ or $(2,1)$, $1 \leqq i \leqq 8$. For $(i_1, i_2) = (0,0)$ we have $k_i \in K_0 K_2$ and thus have at most four such elements. We examine the remaining four elements.

If one element has the form $k_1 x_1^2 x_2$ and another has the form $k_2 x_2$ then, taking their product, we see $k_1 \sigma_1^2 \sigma_2(k_2) \sigma_1^2(b_2) x_1^2$ has square in F, so we are done with $k^{-1} = k_1 \sigma_1^2 \sigma_2(k_2) \sigma_1^2(b_2)$. Thus we may assume our four elements are either all of the form $k_i x_1^2 x_2$, or all of the form $k_i x_2$, $1 \leqq i \leqq 4$. We eliminate the former possibility, the latter being analogous. So assume $k_i x_1^2 x_2$ a e commuting F'-independent, with squares in F. Then

$$0 = [k_1 x_1^2 x_2, k_i x_1^2 x_2] = (k_1 \sigma_1^2 \sigma_2(k_i) - k_i \sigma_1^2 \sigma_2(k_1)) b_1 b_2,$$

implying $k_1 k_i^{-1}$ is fixed under $\sigma_1^2 \sigma_2$; also $k_i \sigma_1^2 \sigma_2(k_i) b_1 b_2 = (k_i x_1^2 x_2)^2 \in F$, implying $(k_1 k_i^{-1})^2 \in F$, so $k_1 k_i^{-1} \in K_0 K_2$. It follows that $k_1 k_i^{-1} \in K_0$ (since $\sigma_1^2 \sigma_2$ does not fix K_2), $1 \leqq i \leqq 4$, contrary to them being F-independent.

Thus $(i_1, i_2) = (2, 0)$ for some i, after all. Q.E.D.

We now require a fact about cyclic field extensions which probably has an easy proof, but whose proof below is quite roundabout. (Albert [1] gives an arithmetic proof in the special case $t = 2$.)

Lemma 2.2. *Suppose L is a cyclic extension of F (an infinite field) with Galois group $\langle \sigma \rangle$, with $\sigma^{2t} = 1$, and let K_1 be the fixed subfield with respect to σ^t. For $x \in K_1$, define $N_1(x) = x\sigma(x) \cdots \sigma^{t-1}(x) \in F$. Suppose for some k in K_1 the following nondegeneracy condition holds:*

(*) *For some k in K_1, $N_1(k)$ is not a square in K_1.*

Then $-1 \in N_1(K_1)$.

Proof. Let $b = N_1(k)$. Then (L, σ, b) is a cyclic algebra and b^2 is a norm, so (L, σ, b) has exponent 2. In view of the nondegeneracy condition (*), $K_1(\sqrt{b})$ is a field, so by [7, theorem 3.5], $-b \in N_1(K_1)$. Hence $-1 = (b)(-b)^{-1} \in N_1(K)$. Q.E.D.

Proposition 2.3. *Let H be any field with $\frac{1}{2}$. Then, for suitable fields $K \supset F$ containing H, there is some (K, G, U, B) of exponent 4, such that (K, G, U) has exponent 4 but does* not *have a maximal subfield of Galois group $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$ over F'.*

PROOF. We continue the set-up described at the beginning of this section. Note that $R=(K,G,U,B)$ has exponent $\leqq 4$ if the centralizer of K_2 in R has exponent 2 (or equivalently an involution of first kind), i.e. if

$$(5)\qquad -b_1=a\sigma_1(a)\qquad \text{for some } a \text{ in } K_0K_2\qquad \text{(by [1, theorem 1])}.$$

In this case (K,G,U) has exponent $\leqq 4$ by Proposition 1.4, so by Proposition 2.1 it is enough to show

$$(6)\qquad b_1\notin Fk\sigma_1^2(k)\qquad \text{for all } k \text{ in } K.$$

Of course we also need to satisfy

$$(7)\qquad \sigma_2(b_1)b_1^{-1}=N_1(u_{21}).$$

Given (7) we automatically get (3), and then by Hilbert's theorem 90 we can find b_2 in K such that (4) holds; recapitulating, it is enough to find the field $K=K_1K_2$ with elements u_{21}, b_1, a satisfying (5), (6), and (7).

Write $N(w)$ for $w\sigma_1^2(w)$. Note if $b_1=\alpha k\sigma_1^2(k)$ then

$$N_2(b_1)=N_2(\alpha N(k))=\alpha^2N(N_2(k))=N(\alpha N_2(k))\in N(K_1).$$

Thus we shall show

$$(6')\qquad N_2(b_1)\notin N(K_1).$$

Now take $C=H[\mu_1,\cdots,\mu_8]$, where $\mu_1,\cdots,\mu_8$ are commuting indeterminates over H, and let L be the field of fractions of C; defining $\sigma_1(\mu_i)=\mu_{i+1}$, subscripts modulo 8, let K_1 (resp. F) be the fixed subfield of L with respect to σ_1^4 (resp. σ_1). We have by Lemma 2.2 some element u_{12} of K_1 with $N_1(u_{12})=-1$. Write $K_2=F(\zeta_2)$ with $\zeta_2^2\in F$ to be determined. Then put $b_1=\zeta_2$, and (7) is automatic; it remains to check (5) and (6′).

Writing $\alpha_2=\zeta_2^2$ and $a=a_1(a_2+\zeta_2)$ for a_i in K_0, these conditions respectively become

$$(5')\qquad -\zeta_2=a_1\sigma_1(a_1)(a_2\sigma_1(a_2)+\alpha_2+(a_2+\sigma_1(a_2))\zeta_2),$$

$$(6'')\qquad -\alpha_2\neq N(w)\qquad \text{for all } w \text{ in } K_1.$$

Now matching components of 1 and ζ_2 in (5′) yields two equations:

$$(8)\qquad 0=a_2\sigma_1(a_2)+a_2,\quad \text{so}\quad \alpha_2=-a_2\sigma_1(a_2),$$

$$(9)\qquad -1=a_1\sigma_1(a_1)(a_2+\sigma_1(a_2)).$$

We can use (8) to define α_2, which leaves us to satisfy merely (9) and

$$(10) \qquad a_2\sigma_1(a_2) \neq w\sigma_1^2(w) \qquad \text{for all } w \text{ in } K_1.$$

Take $a_1 = \frac{1}{2}$ and $a_2 = -2 + p$, where $p = \zeta_1\zeta_3\zeta_5\zeta_7 - \zeta_2\zeta_4\zeta_6\zeta_8$. Then $\sigma_1(a_2) = -2 - p$, so (9) holds, and (10) becomes

$$4 - p^2 \neq w\sigma_1^2(w) \qquad \text{for all } w \text{ in } K_1.$$

Now the prime factorization of $4 - p^2$ in C is $(2-p)(2+p)$, each factor of which is in $K_0 \cap C$. But the degree of $2 - p$ in $w\sigma_1^2(w)$ must be even, so (10) is indeed impossible. Q.E.D.

On the other hand, there are division algebras over H of degree 8, exponent 2, whose maximal subfields Galois over the center all have Galois group $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$, cf. [3 theorem 3]. Confronting these two division algebras with [8, theorem 9] produces

THEOREM 2.4. *Saltman's generic division algebra over H of degree* 8, *exponent* 4 *is* not *a crossed product, for every field H with $\frac{1}{2}$. (Thus there are non-crossed products of exponent* 4 *and any degree* $8m$, *for m an integer.)*

§3. Positive results

A more natural attack on the non-crossed product question of exponent 4 may have been to construct a degenerate set of u_{ij}, according to [4, lemma 1.7]. However, the ensuing conditions are less tractable, in light of the following result.

THEOREM 3.1. *Suppose R is a division algebra of degree* 4, *with involution* $(*)$ *of the* second *kind, and let $F = \{\alpha \in Z(R) \mid \alpha^* = \alpha\}$. Assume $\frac{1}{2} \in F$. Then R has a maximal subfield L Galois over F, with Galois group $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$.*

PROOF. Modification of [6]. Note if $r \in R$ with $r^* = r$ then the coefficients of the minimal monic polynomial of r are symmetric; indeed if

$$r^t + \sum_{i=0}^{t-1} \alpha_i r^i = 0 \quad \text{then} \quad r^t + \sum_{i=0}^{t-1} \alpha_i^* r^i = 0^* = 0 \quad \text{so} \quad 0 = \sum_{i=0}^{t-1} (\alpha_i^* - \alpha_i) r^i,$$

implying each $\alpha_i^* = \alpha_i$.

We claim now that there is an involution (J) of R over F (of second kind) and some $x^J = x$ in $R - F$ such that $x^2 \in F$. Indeed, take $d_1^* = d_1$ of degree 4 and reduced trace 0, writing $d_1^4 + \alpha_2 d_1^2 + \alpha_1 d_1 + \alpha_0 = 0$. Using the notation of [6, theorem 4.1] (so that a is the sum of d_1 and a certain conjugate of d_1), we see by the proof of [6, theorem 6.1] that a is symmetric with respect to some involution (J) over F; thus a has degree $\leqq 4$ over F. By the proof of [6, theorem 4.1], $[F(a^2):F]<[F(a):F]$, so a^2 has degree $\leqq 2$, proving the claim.

Now there is some y in R such that $yxy^{-1}=-x$, by the Skolem–Noether theorem. Then $xy^J=-y^Jx$, so replacing y by $y\pm y^J$, we may assume $y=\pm y^J$. Now $y^2x=xy^2$, so y^2 has degree $\leqq 2$ over C. Also y^2 is J-symmetric, so y^2 has degree $\leqq 2$ over F. If $y^2\in F(x)$ then F, x, y generate a (J)-invariant quaternion F-subalgebra of R, so we are done. Otherwise $Z(R)$, $F(x)$, and $F(y^2)$ generate the desired field F. Q.E.D.

A nice, positive general result comes from mimicking a proof of Albert [1, ch. 11]. Recall that a simple ring has *index t* if it can be written as matrices over a division algebra of degree t.

THEOREM 3.2. *If R has index* 8, *and* $\frac{1}{2}\in R$, *then there is a splitting field K of R with subfield L, such that K is Galois over L of Galois group* $\mathbf{Z}_2\times\mathbf{Z}_2\times\mathbf{Z}_2$, *and L is Galois over F of Galois group* $\mathbf{Z}_2\times\mathbf{Z}_2$.

PROOF. Let $F=Z(R)$. $R\otimes_F R$ has index $\leqq 4$ by [2, lemma 5.7], so has a splitting field L_1L_2, where $[L_i:F]=2$. Then $R\otimes_F L_1L_2$ has exponent 2, and thus has a splitting field K Galois over L_1L_2 with Galois group $\mathbf{Z}_2\times\mathbf{Z}_2\times\mathbf{Z}_2$, by [6, theorem 6.2]. Q.E.D.

COROLLARY 3.3. *Every simple algebra of index* 8 *of characteristic* $\neq 2$ *has a splitting field whose Galois group is a* 2-*group* (*and thus is solvable*).

REFERENCES

1. A. A. Albert, *A construction of non-cyclic normal division algebras*, Bull. Amer. Math. Soc. **38** (1932), 449–456.
2. A. A. Albert, *Structure of Algebras*, Amer. Math. Soc. Colloq. Publ. **24**, Providence, R.I., 1961.
3. S. A. Amitsur, *On central division algebras*, Israel J. Math. **12** (1972), 408–422.
4. S. A. Amitsur and D. Saltman, *Generic abelian crossed products and p-algebras*, J. Algebra **51** (1978), 76–87.
5. S. A. Amitsur, L. H. Rowen and J. P. Tignol, *Division algebras of degree* 4 *and* 8 *with involution*, Israel J. Math. **33** (1979), 133–148.
6. L. H. Rowen, *Central simple algebras*, Israel J. Math. **29** (1978), 285–301.
7. L. H. Rowen, *Central simple algebras with involution viewed through centralizers*, J. Algebra **63** (1980), 41–55.
8. D. Saltman, *Indecomposible division algebras*, Comm. Algebra, to appear.
9. J. Tignol, *Sur les classes de similitude de corps a involution de degre* 8, C. R. Acad. Sci. Paris, Ser. A **286** (1978), 875–876.

BAR-ILAN UNIVERSITY
RAMAT GAN, ISRAEL