ISRAEL JOURNAL OF MATHEMATICS, Vol. 29, Nos. 2-3, 1978

CENTRAL SIMPLE ALGEBRAS[†]

BY
LOUIS HALLE ROWEN

ABSTRACT

Wedderburn's factorization of polynomials over division rings is refined and used to prove that every central division algebra of degree 8, with involution, has a maximal subfield which is a Galois extension of the center (with Galois group $\mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2$). The same proof, for an arbitrary central division algebra of degree 4, gives an explicit construction of a maximal subfield which is a Galois extension of the center, with Galois group $\mathbf{Z}_2 \oplus \mathbf{Z}_2$. Use is made of the generic division algebras, with and without involution.

§0. Introduction and preliminaries

Suppose R is a ring. The *center* of R is $\{c \in R \mid cr = rc \text{ for all } r \text{ in } R\}$. If R is simple (i.e. no proper nonzero ideals), then the center of R is obviously a field F, over which R is a finite dimensional vector space; if the dimension is finite then we call R a *central simple F-algebra.* There is little doubt that central simple algebras lie at the heart of noncommutative algebra. The study of central simple F-algebras has taken two directions—the arithmetic approach (based on assumptions on F) and the algebraic approach (describing the structure of R, without regard to the arithmetic of F). Of course, these two methods have considerable interplay (cf. [2]), but there are a number of positive algebraic results not requiring arithmetic, and this paper will be purely algebraic in nature. The classical work on central simple algebras is [1], from which we shall quote a number of standard results at the outset.

F always denotes a field. If A is an F-algebra then $[A:F]$ denotes the dimension of A as an F-vector space. The obvious example of a central simple algebra is $M_n(F)$, the algebra of $n \times n$ matrices with entries in F. Another example of a central simple algebra is a division algebra (of finite dimension over its center), and, by a celebrated theorem of Wedderburn, any central simple

[†] This work was supported by the Israel Committee for Basic Research and the Anshel Pfeffer Chair.

Received February 22, 1977

F-algebra has the form $M_m(D) \approx M_m(F) \otimes_F D$, for suitable number m and suitable division algebra D. Thus, the study of central simple algebras can largely be reduced to the study of division algebras, and we shall concentrate henceforth on division algebras. (In §5 another method will be given of using facts about division algebras to prove theorems about central simple algebras in general.) By [1, theor. 4.28], if F is finite then $M_n(F)$ is the only central simple F-algebra, and the structure theory is quite trivial; so *all of our fields are assumed to be infinite.*

Henceforth, C is a field and D is a central simple C-algebra. It is easy to see that $D \otimes_C \bar{C}$ is a central simple $\bar{C}$-algebra, for any extension field $\bar{C}$ of C. In particular, if $\bar{C}$ is the algebraic closure of C then $D \otimes_C \bar{C} \approx M_m(D_1)$, for suitable m and suitable division algebra D_1 of finite dimension over $\bar{C}$. But for any element d_1 of D_1, the subfield $\bar{C}(d_1)$ of D is a finite dimensional extension of $\bar{C}$, implying $\bar{C}(d_1) = \bar{C}$, so $D_1 = \bar{C}$. Thus $[D : C] = [M_m(\bar{C}) \colon \bar{C}] = m^2$, and we call m the *degree* of D. Division algebras of degree 2 are called *quaternion algebras.*

By *C-subfield* of D we mean subfield of D containing C. If $d \in D$, $C(d)$ denotes the C-subalgebra of D generated by d, easily seen to be a C-subfield. Every C-subfield of D can be embedded in a maximal subfield, which is obviously a C-subfield, and we shall be very interested in the set of maximal subfields of D.

Given subsets A, B of D, write $[A, B]$ to denote $\{ab - ba \mid a \in A, b \in B\}$. Given a subalgebra A of D, $A' = \{d \in D \mid [d, A] = 0\}$ is also a subalgebra of D, called the *centralizer of* A; if A is a C-subfield then $A' \approx M_t(A)$, where $t[A : C] =$ degree of D (by [1, theor. IV.12]). Moreover, if A is a maximal subfield, then clearly $t = 1$ (for otherwise A' contains a subfield of D which properly contains A), implying $[A : C]$ is the degree of D. Thus the maximal subfields of a division algebra of degree n are precisely the subfields which are n-dimensional over the center.

If A is a C-subalgebra of D and A is also a central simple C-subalgebra, then, for $B =$ centralizer of A, we have $D \approx A \otimes_C B$ (by [1, theor. IV.13]), implying B is also central C-simple.

Suppose A is any simple C-subalgebra of D and φ is an automorphism of A which fixes C. Then by the famous Skolem–Noether theorem ([1, theor. IV.14]), there exists an element d in D, such that $dad^{-1} = \varphi(a)$ for all elements a of A; i.e. φ can be lifted to an inner automorphism of D. We shall use the Skolem–Noether theorem repeatedly in our applications. The underlying principle is, given a separable field extension K of C, one has nontrivial automorphisms of K, fixing C, and these automorphisms can be realized via elements of D.

Let us present an important example of this method. If D has degree n, and if there exists a maximal subfield K Galois over C with Galois group G, then each element φ_i of G can be realized by a map of the form $k \mapsto d_i k d_i^{-1}$ for all k in K. Since $G = [K : C] = n$, we have n such elements $d_1 = 1, d_2, \cdots, d_n$, and one can easily prove that $D = Kd_1 + Kd_2 + \cdots + Kd_n$ (by [1, theor. V.2]). This gives us considerable information about D. Call such a division algebra a *crossed product.* Every division algebra of degree 2, 3, 4, 6, or 12 is a crossed product (cf. [1, 8]) although not every division algebra is a crossed product (cf. [2]). Using the method of [8], developed and refined in §1, we shall give an explicit way of constructing the maximal subfield which is Galois, for $n = 4$, and show for $n = 8$ that every division algebra with involution (cf. §5) is a crossed product. These results are made clearer through the use of the generic division algebras with and without involution, defined respectively in §5 and §2.

In the process of building a Galois extension of C in D, when D has even degree, we are first interested in building quadratic extensions. Thus, call an element d *square-central* if $d \notin C$ but $d^2 \in C$. Maps will be written exponentially, i.e. a^{φ} for $\varphi(a)$. Also, the symbol $\subset$ denotes *proper* inclusion. If $C \subset K_1 \subset K_2$ are C-subalgebras of D, then obviously $[K_1 : C]$ is a proper divisor of $[K_2 : C]$.

§1. Wedderburn's method of splitting polynomials

Let $D[\lambda] = D \otimes_C C[\lambda]$, λ a commutative indeterminate over C; i.e. $D[\lambda]$ is the ring of polynomials in D. In this section we recall Wedderburn's method [8] of factorization in $D[\lambda]$. Given polynomials $f(\lambda)$, $g(\lambda)$, we divide $f(\lambda)$ into $g(\lambda)$ by writing $g(\lambda) = q(\lambda)f(\lambda) + r(\lambda)$, where $r(\lambda), g(\lambda) \in D[\lambda]$ and either $r(\lambda) = 0$ or $\deg r(\lambda) < \deg f(\lambda)$; i.e. we perform divisions from the right. Since $D[\lambda]$ is a domain, this procedure is well defined. If $r(\lambda) = 0$, we say *f divides g*. Writing a polynomial $g(\lambda) = \Sigma d_i \lambda^i$, we define $g(d)$ to be $\Sigma d_i d^i$, for d in D.

LEMMA 1.1. *If $f(\lambda) = \lambda - d$, then $r(\lambda) = g(d)$, so $\lambda - d$ divides $g(\lambda) - g(d)$.*

PROOF. Induction on $\deg g(\lambda)$. If $g(\lambda) = \Sigma_{i=0}^{t} d_i \lambda^i$ then $g(\lambda) - d_t \lambda^{t-1} f(\lambda) = (d_{t-1} + d_t d)\lambda^{t-1} + \Sigma_{i=0}^{t-2} d_i \lambda^i$. By induction, dividing f into $g - d_t \lambda^{t-1} f$ yields a remainder $(d_{t-1} + d_t d)d^{t-1} + \Sigma_{i=0}^{t-2} d_i d^i = \Sigma_{i=0}^{t} d_i d^t = g(d)$. But this remainder is clearly also $r(\lambda)$. Hence $r(\lambda) = g(d)$, and f divides $q(\lambda)f(\lambda) = g(\lambda) - g(d)$.

Q.E.D.

COROLLARY 1.2. *$(\lambda - d)$ divides $g(\lambda)$ iff $g(d) = 0$.*

PROPOSITION 1.3. *Suppose $\lambda - d_0$ divides $g(\lambda)h(\lambda)$ and not $h(\lambda)$. Let $d = h(d_0)$. Then $(\lambda - dd_0d^{-1})$ divides $g(\lambda)$.*

Proof. From Lemma 1.1, $\lambda - d_0$ divides $h(\lambda)-h(d_0)=h(\lambda)-d$, and $d\neq 0$. Thus $\lambda - d_0$ divides $g(\lambda)h(\lambda)-g(\lambda)d$. But $\lambda - d_0$ divides $g(\lambda)h(\lambda)$ by assumption; thus $\lambda - d_0$ divides $g(\lambda)d$. Write $g(\lambda)d=q(\lambda)(\lambda-d_0)$. Then $g(\lambda)=(q(\lambda)d^{-1})(d(\lambda-d_0)d^{-1})=q(\lambda)d^{-1}(\lambda-dd_0d^{-1})$, implying $\lambda-dd_0d^{-1}$ divides $g(\lambda)$. Q.E.D.

If $d\in D$, we mean the usual by "minimal polynomial" of d and "characteristic polynomial" of d; i.e. these polynomials have coefficients in C, but may be viewed in $D[\lambda]$ since $C[\lambda]\subset D[\lambda]$ canonically. For convenience, we assume these polynomials are *monic*, i.e. with leading coefficient $+1$.

Lemma 1.4. *If $g(\lambda)\in D[\lambda]$ and $g(d)=0$ for all conjugates d of an element x_0 in D, then $g(\lambda)$ is a multiple of the minimal polynomial of x_0.*

Proof. Take a supposed counterexample $g(\lambda)=\Sigma_{i=0}^{t} d_i\lambda^i$, with t minimal; multiplying on the left by d_t^{-1}, we may assume that $d_t=1$.

For any nonzero y in D, we see that $y^{-1}dy$ is a conjugate of d (thus of x_0), so $0=\Sigma_{i=0}^{t} d_i(ydy^{-1})^i=\Sigma d_iyd^iy^{-1}$, implying $\Sigma_{i=0}^{t}(y^{-1}d_iy)d^i=0$. But we also have $\Sigma_{i=0}^{t} d_id^i=0$. Subtracting, we get $0=\Sigma_{i=0}^{t}(y^{-1}d_iy-d_i)d^i=-y^{-1}\Sigma[y,d_i]d^i$; thus $\Sigma_{i=0}^{t}[y,d_i]d^i=0$.

In other words, if $h_y(\lambda)=\Sigma_{i=0}^{t}[y,d_i]\lambda^i$, then $h_y(d)=0$ for every conjugate d of x_0. But $[y,d_t]=[y,1]=0$, so $h_y(\lambda)$ has degree $\leqq t-1$. Hence, by induction, the minimal polynomial $m(\lambda)$ of x_0 divides $h_y(\lambda)=[y,g(\lambda)]$. Now write $g(\lambda)=f(\lambda)m(\lambda)+r(\lambda)$, with $\deg r(\lambda)<\deg m(\lambda)$. Then $h_y(\lambda)=[y,f(\lambda)]m(\lambda)+[y,r(\lambda)]$, for each y in D, implying $r(\lambda)\in C[\lambda]$. But $r(d)=g(d)-(fm)(d)=0$ since the coefficients of $m(\lambda)$ are in C (and thus commute with d). Since $r(\lambda)$ has smaller degree than the minimal polynomial of d, we conclude $r(\lambda)=0$. Q.E.D.

Theorem 1.5. *Let $p(\lambda)$ be an irreducible monic polynomial in $C[\lambda]$. If $p(d_1)=0$ for some element d_1 in D, then $p(\lambda)$ "splits" into linear factors in $D[\lambda]$, and $p(\lambda)$ is the minimal polynomial of d_1.*

Proof. Write $p(\lambda)=g(\lambda)(\lambda-d_t)\cdots(\lambda-d_1)$, such that $g(\lambda)$ has minimal possible degree. Let $h(\lambda)=(\lambda-d_t)\cdots(\lambda-d_1)$, knowing that $t\geqq 1$ by assumption. We claim that $h(d)=0$ for every conjugate d of d_1. Otherwise if $h(d)\neq 0$, we still have $p(d)=0$ since $p(\lambda)\in C[\lambda]$, so, by Propositon 1.3, $(\lambda-h(d)dh(d)^{-1})$ divides $g(\lambda)$. Thus we can write $d_{t+1}=h(d)dh(d)^{-1}$ and write $p(\lambda)=g'(\lambda)h'(\lambda)$ where $g(\lambda)=g'(\lambda)(\lambda-d_{t+1})$ and $h'(\lambda)=(\lambda-d_{t+1})h(\lambda)$, contrary to the minimality of the degree of g. This proves the claim.

But, by Lemma 1.4, the minimal polynomial $m(\lambda)$ of d_1 divides $h(\lambda)$, and thus

$p(\lambda)$. Since $p(\lambda)$ is irreducible in $C[\lambda]$, we conclude that $m(\lambda) = h(\lambda) = p(\lambda)$, proving the theorem. Q.E.D.

Remark 1.6. In the proof of Theorem 1.5, we can take d_2 to be $[y, d_1]d_1[y, d_1]^{-1}$, where y is any element not commuting with d_1.

Proof. If $[y, d_1] \neq 0$ then $yd_1y^{-1} \neq d$, and so, writing $p(\lambda) = f(\lambda)(\lambda - d_1)$, we have (by Proposition 1.3) $\lambda - d_2$ divides $f(\lambda)$, where

$$\begin{aligned} d_2 &= (yd_1y^{-1} - d_1)(yd_1y^{-1})(yd_1y^{-1} - d_1)^{-1} \\ &= [y, d_1]y^{-1}yd_1y^{-1}y[y, d_1]^{-1} \\ &= [y, d_1]d_1[y, d_1]^{-1}. \end{aligned}$$

Remark 1.7. In the proof of Theorem 1.5, if $[d_2, d_1] \neq 0$, we can take $d_3 = [d_2, d_1]d_2[d_2, d_1]^{-1}$.

Proof. Write $p(\lambda) = f(\lambda)(\lambda - d_2)(\lambda - d_1) = f(\lambda)(\lambda^2 - (d_1 + d_2)\lambda + d_2d_1)$. But, by hypothesis, $(d_2)^2 - (d_1 + d_2)d_2 + d_2d_1 = [d_2, d_1] \neq 0$. Hence by Proposition 1.3, we can take $d_3 = [d_2, d_1]d_2[d_2, d_1]^{-1}$.

Remark 1.8. If $g(\lambda)$ has coefficients in C and $g(\lambda) = q(\lambda)f(\lambda)$ then $g(\lambda) = f(\lambda)q(\lambda)$.

Proof. $(f(\lambda)q(\lambda))f(\lambda) = f(\lambda)(q(\lambda)f(\lambda)) = f(\lambda)g(\lambda) = g(\lambda)f(\lambda)$. Since $D[\lambda]$ is a domain, $f(\lambda)q(\lambda) = g(\lambda)$.

Corollary 1.9. *If $p(\lambda) = (\lambda - d_t)\cdots(\lambda - d_1)$ and $p(\lambda) \in C[\lambda]$, then, for each i, $p(\lambda) = (\lambda - d_i)\cdots(\lambda - d_1)(\lambda - d_t)\cdots(\lambda - d_{i+1})$.*

Proof. Put $q(\lambda) = (\lambda - d_t)\cdots(\lambda - d_{i+1})$ and $f(\lambda) = (\lambda - d_i)\cdots(\lambda - d_1)$ and apply Remark 1.8.

§2. The role of generic division algebras

We shall give a brief presentation of the famous division algebras of generic matrices of Amitsur [2], recast through the use of central polynomials in [5]. First we fix n. Let F be an infinite field, and let $F(\xi) \equiv F(\xi_{ij}^{(k)})$ be the polynomial algebra in commutative indeterminates $\xi_{ij}^{(k)}$ over F, $1 \leqq i, j \leqq n$, $1 \leqq k < \infty$. The *algebra of generic $n \times n$ matrices* $F^{(n)}\{Y\}$ is defined to be the F-subalgebra of $M_n(F(\xi))$ generated by all generic matrices $Y_k = (\xi_{ij}^{(k)})$, $1 \leqq i, j \leqq n$, for $1 \leqq k < \infty$. The elements of $F^{(n)}\{Y\}$ can be written in the form $f(Y_1, \cdots, Y_k)$, where $f(X_1, \cdots, X_k)$ is a formal polynomial in k (noncommuting) indeterminates

$X_1,\cdots,X_k$. Given a central simple F-algebra R of degree n, it is easy to show that $f(Y_1,\cdots,Y_k)=0$ iff, for all elements r_i of R, $f(r_1,\cdots,r_k)=0$. (In this case $f(X_1,\cdots,X_k)$ is called an *identity of* R.) Now let C_0 be the center of $F^{(n)}\{Y\}$. C_0 is contained in $F(\xi)$ (viewing $F(\xi)$ as scalar matrices). Let $F^{(n)}(Y)$ be the subring of $M_n(F(\xi))$ generated by $F^{(n)}\{Y\}$ and the inverses of all elements of C_0. $F^{(n)}(Y)$ is a division algebra of degree n, called the algebra of generic $n\times n$ matrices, and is a division algebra cf. [5, §3]. This result is due to Amitsur, who proved in [2] that $\mathbf{Q}^{(n)}(Y)$ does *not* have a maximal subfield which is a Galois extension of the center, if n is divisible by 8 or the square of an odd prime. Let us now state

THEOREM A (i) *If $F^{(n)}(Y)$ has a maximal subfield which is a Galois extension of* Cent $F^{(n)}(Y)$, *with Galois group G, then every central simple division F-algebra of degree n has a maximal subfield which is a Galois extension of F, with the same Galois group G.*

(ii) *If $n>2$ then $F^{(n)}(Y)$ has no central quaternion subalgebras.*

Indeed, the first assertion is [2, theor. 5] (cf. proof in [4, theor. 4]). The second assertion follows immediately from [5, theor. 2].

One can improve on Theorem A by making the following observation, which is well-known:

PROPOSITION 2.1. *If $f_i(Y_1,\cdots,Y_t)g_i(Y_1,\cdots,Y_t)^{-1}$ are nonzero elements of $F^{(n)}(Y)$, $1\leqq i\leqq m$, where $f_i(Y_1,\cdots,Y_t)$, $g_i(Y_1,\cdots,Y_t)$ are elements of $F^{(n)}\{Y\}$, then, for each central simple division F-algebra D, there are elements $d_1,\cdots,d_t$ of D, such that $f_i(d_1,\cdots,d_t)g_i(d_1,\cdots,d_t)^{-1}\neq 0$ for all i; moreover, in such a set-up, we may always assume $g_i(Y_1,\cdots,Y_t)\in C_0$.*

PROOF. Write f_i for $f_i(Y_1,\cdots,Y_t)$, for convenience. We know already that $f_ig_i^{-1}$ has the form $f_i'(g_i')^{-1}$ where $f_i'\in F^{(n)}\{Y\}$ and $g_i'\in C_0$. Thus $f_i'=f_ig_i^{-1}g_i'=f_ig_i'g_i^{-1}$, implying $0=f_i'g_i-f_ig_i'$, so $f_i'g_i-f_ig_i'$ is an identity of D. On the other hand, $\Pi f_if_i'g_ig_i'$ is *not* an identity of D, the product taken over all i between 1 and m, so, for suitable elements $d_1,\cdots,d_t$ of D,

$$\prod_i f_i(d_1,\cdots,d_t)f_i'(d_1,\cdots,d_t)g_i(d_1,\cdots,d_t)g_i'(d_1,\cdots,d_t)\neq 0.$$

It follows immediately that

$$0\neq f_i(d_1,\cdots,d_t)g_i(d_1,\cdots,d_t)^{-1}=f_i'(d_1,\cdots,d_t)g_i'(d_1,\cdots,d_t)^{-1}$$

for each i, and the assertions follow immediately. Q.E.D.

Thus many explicit constructions for $F^{(n)}(Y)$ give general constructions for all central simple division F-algebras, and proofs by constructing the suitable object in $F^{(n)}(Y)$ will be called *explicit proofs*. We feel that explicit proofs are very desirable, especially since they build up knowledge about $F^{(n)}(Y)$.

§3. Division algebras of degree 3

In this section we assume that D is a division algebra of degree 3, i.e. $[D:C]=3^2=9$. In this case, Wedderburn [8] proved that there is an element $d_0 \in D - C$ such that $d_0^3 \in C$. Since the proof is beautiful and short, we include it here.

Suppose that there are elements d_1 and y, such that d_1 does not commute with $d_2=[y,d_1]d_1[y,d_1]^{-1}$, and let $p(\lambda)=\Sigma_{i=0}^{t}\alpha_i\lambda^i(\alpha_i$ in $C, \alpha_t=1)$ be the minimal polynomial of d_1. Then $t=[C(d_1):C]$, a divisor of 3, so $t=3$. By Theorem 1.5 and Remark 1.6, we can write $p(\lambda)=(\lambda-d_3)(\lambda-d_2)(\lambda-d_1)$ for suitable d_3 in D. We claim that $d_0=[d_1,d_2]$ "works". First we note that $-\alpha_2=d_3+d_2+d_1$; commuting with d_1 yields $[d_3,d_1]=[d_1,d_2]=d_0$. Similarly, commuting α_2 with d_2 yields $[d_2,d_3]=[d_1,d_2]=d_0$. Note that by Corollary 1.9, $p(\lambda)=(\lambda-d_{\pi 3})(\lambda-d_{\pi 2})(\lambda-d_{\pi 1})$ for each cyclic permutation π of $(1,2,3)$, and we just saw that $[d_{\pi 2},d_{\pi 1}]=\pm d_0\neq 0$. By Remark 1.7, we can take $d_{\pi 3}=[d_{\pi 2},d_{\pi 1}]d_{\pi 2}[d_{\pi 2},d_{\pi 1}]^{-1}=d_0d_{\pi 2}d_0^{-1}$. But since $d_{\pi 3}$ is determined by $d_{\pi 2}$ and $d\pi_1$, $d_{\pi 3}$ *must* necessarily equal this value. Thus (taking subscripts modulo 3) we have $d_{i+1}=d_0d_id_0^{-1}$, for each i. We claim this implies $d_0^3\in C$. Otherwise $[C(d_0^3):C]=3$, implying $C(d_0^3)$ is a maximal subfield (and thus its own centralizer). In this case, d_1 and d_2 would be elements of $C(d_0^3)$, which is nonsense since $d_1d_2\neq d_2d_1$. This yields the claim.

So all we have to do is compute d_1 and d_2 for the generic division algebra $F^{(3)}(Y)$. This is trivial: take $d_1=Y_1$ and $y=Y_2$. Clearly in this case $0\neq[d_1,d_2]=[Y_1,[Y_2,Y_1]Y_1[Y_2,Y_1]^{-1}]$, seen by specializing Y_1, Y_2 to suitable matrices with integral coefficients. Schacher and Small (unpublished) computed the corresponding polynomial whose cube is central. Anyway, we have proved here

THEOREM 3.1. *Any division algebra of degree* 3 *has an element not in the center, whose cube is in the center.*

§4. Division algebras of degree 4

The structure of division algebras of degree 4 is well-known, e.g. there exists a maximal subfield K of D such that $\mathrm{Gal}(K/C)=\mathbf{Z}_2\oplus\mathbf{Z}_2$ (cf. Albert [1, theor. XI.9]). We shall obtain this result by constructing the subfield K in the case $D=F^{(4)}(Y)$, which then gives us a general construction, by Theorem A. For purposes of later application, our first theorem is given for any division algebra, of arbitrary degree.

We carry the following notation: Suppose D has an element d_1 of (reduced) trace 0, having degree 4. Then the minimal polynomial $p(\lambda)$ of d_1 has the form $\lambda^4+\alpha_2\lambda^2+\alpha_1\lambda+\alpha_0$, where $\alpha_i\in C$. Using Theorem 1.5, we have $p(\lambda)=(\lambda^2+a'\lambda+b')(\lambda^2+a\lambda+b)$ for suitable elements a, b, a', b' of D. In fact, in the notation of Theorem 1.5, $b=d_2d_1$ and $a=-(d_1+d_2)$.

THEOREM 4.1. *In the above notation, if* $3\nmid[D:C]$ *and* $[C(a):C]\leqq 4$, *then either* $a^2\in C$ *or* $[C(a^2):C]=2$. *If, moreover,* $[C([a,b]):C]\leqq 4$, *then either* $[a,b]^2\in C$ *or* $[C([a,b]^2):C]=2$.

PROOF. Matching coefficients in $p(\lambda)$ yields $0=a'+a$, so $a'=-a$, and

$$\alpha_2=a'a+b+b'=-a^2+b+b',$$

$$\alpha_1=a'b+b'a=-ab+b'a,$$

$$\alpha_0=b'b.$$

Substituting $b'=\alpha_0b^{-1}$ yields the two equations

$$\alpha_2=-a^2+b+\alpha_0b^{-1}, \tag{1}$$

$$\alpha_1=-ab+\alpha_0b^{-1}a. \tag{2}$$

Case I. $[a,b]=0$. Then $\alpha_1=(\alpha_0b^{-1}-b)a$, so

$$\alpha_1^2=((\alpha_0b^{-1}+b)^2-4\alpha_0)a^2=((\alpha_2+a^2)^2-4\alpha_0)a^2$$
$$=(a^2)^3+2\alpha_2(a^2)^2+(\alpha_2^2-4\alpha_0)a^2.$$

Thus $[C(a^2):C]\leqq 3$ and is relatively prime to 3 (since $3\nmid[D:C]$, by hypothesis). Hence, either $a^2\in C$ or $[C(a^2):C]=2$.

Case II. $[a,b]\neq 0$. Then from (1), $0=[\alpha_2,b]=-[a^2,b]$, implying $C(a^2)\subset C(a)$. (Obviously $a\notin C(a^2)$, since $ab\neq ba$ and $a^2b=ba^2$.) Thus $[C(a^2):C]<[C(a):C]=4$, and we again conclude $a^2\in C$ or $[C(a^2):C]=2$.

This proves the first assertion, that $a^2\in C$ or $[C(a^2):C]=2$. Now we continue with $w=[a,b]$. As noted already in case II, $0=[a^2,b]=a[a,b]+[a,b]a$, implying $aw=-wa$. Hence $w\notin C(w^2)$, so we have $[C(w^2):C]<[C(w):C]=4$, so, as before, we conclude that either $w^2\in C$ or $[C(w^2):C]=2$. Q.E.D.

Note that if $a^2\in C$ and $w^2\in C$ then the subalgebra of D generated by a and w is quaternion. However, this is usually not the case.

THEOREM 4.2. *In $D = F^{(4)}(Y)$, take $d_1 = [Y_1, Y_2]$, $d_2 = [Y_3, d_1]d_1[Y_3, d_1]^{-1}$, $a = d_1 + d_2 = [Y_3, d_1^2][Y_3, d_1]^{-1}$, and $b = d_2 d_1$. Then $[C(a^2): C] = 2$ and $[C([a, b]^2): C] = 2$.*

PROOF. By specializing to matrices, one sees easily that $a^2 \notin C$ and $[a, b]^2 \notin C$. On the other hand, $\mathrm{tr}(d_1) = 0$, and clearly $[C(a): C] \leqq 4$ and $[C([a, b]): C] \leqq 4$, because the characteristic polynomial of each element has degree $\leqq 4$.

Thus, in view of Remark 1.6 and Theorem 4.1, we have $[C(a^2): C] = 2$ and $[C[a, b]^2: C] = 2$. Q.E.D.

PROPOSITION 4.3. *With notation as in Theorem 4.2, $C(a^2)$ and $C([a, b]^2)$ are separable extensions of C.*

PROOF. If $\mathrm{char}(F) \neq 2$ this is immediate. Even if $\mathrm{char}(F) = 2$ we know that $(a^2)^2 \notin C$ by specializing

LEMMA 4.4. *Suppose D is a division algebra with an element d, such that $C(d)$ is a separable quadratic extension of C. If $x \in D$ and $d_1 = [x, d] \neq 0$, then $[d_1, d] \neq 0$, $[d_1^2, d] = 0$ and $C(d_1^2) \subset C(d_1)$.*

PROOF. Since $[C(d): C] = 2$, we can find elements c, c' in C, with $d^2 = cd + c'$. Then $dd_1 + d_1 d = [x, d^2] = c[x, d] = cd_1$, implying $dd_1 = d_1(c - d)$. Clearly $d \neq c - d$ (since otherwise $2d = c \in C$, implying $2 = 0$, since $d \notin C$; then $c = 0$ and d is inseparable over C, contrary to hypothesis). Thus $dd_1 \neq d_1 d$. But $dd_1^2 = d_1(c - d)d_1 = d_1^2 d$, implying $[d_1^2, d] = 0$ and $C(d_1^2) \subset C(d_1)$ (since $[d_1, d] \neq 0$). Q.E.D.

THEOREM 4.5. *If D has degree 4 then D has a maximal subfield K, which is a Galois extension of C with Galois group $\mathbf{Z}_2 \oplus \mathbf{Z}_2$. In fact, in $F^{(4)}(Y)$, notation as in Theorem 4.2, K can be taken to be the product of the fields $C(a^2)$ and $C([Y_4, a^2]^2)$, each of which is a quadratic extension of C.*

PROOF. By Theorem A, it is enough to prove the second assertion. Let $d = a^2$ and $d_1 = [Y_4, d]$. By Proposition 4.3 and Lemma 4.4, we have $[d_1, d] \neq 0$, $[d_1^2, d] = 0$, and, thus, $C(d_1^2) \subset C(d_1)$. It is a simple matter to verify that $d_1^2 \notin C$ (although one can argue this matter indirectly by showing that if $d_1^2 \in C$ then D would have a quaternion C-subalgebra which, by Theorem A, is an absurdity).

Thus $[C(d_1^2): C]$ is a divisor of 4 other than 1, and $[C(d_1^2): C] < [C(d_1): C] \leqq 4$; hence $[C(d_1^2): C] = 2$. Since d_1^2 and d commute, $C(d_1^2)C(d)$ is a field, and it remains only to show $C(d_1^2) \cap C(d) = C$. Indeed, otherwise, $d \in C(d_1^2)$, implying $[d, d_1] = 0$, which is false. Q.E.D.

It has long been known that every division algebra of degree 4 had a maximal subfield which is a Galois extension of the center, with Galois group $\mathbf{Z}_2 \oplus \mathbf{Z}_2$, as shown in [1, theor. XI.9]. However, Albert's proof is quite complicated, and fails to give an explicit construction of the maximal subfield.

§5. General facts about involutions

An *involution* of a ring is an anti-automorphism of degree 2. Any involution $(*)$ induces an automorphism of the center of degree 1 or 2; we say $(*)$ has *first* (resp. *second*) kind if $(*)$ has degree 1 (resp. degree 2) when restricted to the center. We write x^* to denote $(*)$ acting on the element x. One can induce an involution on $F^{(n)}(Y)$ from the map switching Y_{2i-1} and Y_{2i} for each natural number i; one concludes from [6, theor. 25] that this involution has the second kind. Thus, in view of Theorem A, the existence of an involution of second kind does not yield additional information (in terms of crossed products or quaternion subalgebras) about a division algebra. Consequently, we shall restrict our attention to involutions of the first kind; by *"involution" we shall mean "involution of the first kind"*. We shall often want to modify the involution; to do this we want some results of Albert. $(R, *)$ will denote a ring R with involution $(*)$. Call an element r in R *$(*)$-nice* if $r^* = \pm r$. If φ_1, φ_2 are maps from R to R, we write $\varphi_1\varphi_2$ to denote the map $x \mapsto (x^{\varphi_1})^{\varphi_2}$.

REMARK 5.1. If r is a nice, invertible element of a ring with involution $(R, *)$, then the map J: $x \mapsto rx^*r^{-1}$ (for all x in R) is an involution.

PROPOSITION 5.2. *Suppose $C = \mathrm{Cent}(R)$ is a domain, every automorphism of R fixing C is inner, and $(*)$ and J are involutions of R. Then there exists an invertible, $(*)$-nice element r in R, such that $x^J = rx^*r^{-1}$ for all r in R. Moreover, $r^* = r^J$.*

PROOF. Clearly, $*J$ is an automorphism of R fixing the center; thus, by hypothesis, there is an invertible element r in R, with $x^{*J} = rxr^{-1}$ for all x in R. Replacing x by x^*, we have $x^J = rx^*r^{-1}$ for all x in R.

We claim that r is $(*)$-nice. Indeed, for all x in R, $(r^*r^{-1})x^J(r^*r^{-1})^{-1} = r^*x^*(r^{-1})^* = (r^{-1}xr)^* = (x^{J*})^* = x^J$, implying $r^*r^{-1} \in C$. Thus $r^* = cr$ for some c in C. Hence $r = (r^*)^* = (cr)^* = c^2r$, implying $(c^2 - 1)r = 0$. Since r is invertible, we have $c^2 = 1$. Hence $(c-1)(c+1) = 0$; since C is a domain, we conclude $c = \pm 1$, so r is $(*)$-nice. The last assertion is immediate. Q.E.D.

The above proof was essentially that of Albert [1, theor X.11], but we have included it because it motivates the other general results of this section. First, we call $(*)$ and (J) *equivalent* if the element r of Proposition 5.2 is symmetric (i.e.

$r^* = r$). It is easy to see that this is an equivalence relation, and thus there are at most two equivalence classes of involutions for a ring R satisfying the hypotheses of Proposition 5.2; in fact, R has two equivalence classes of involutions precisely when R has invertible antisymmetric elements (under a suitable involution).

Say $(R,*)$ is *isomorphic* to (R,J) if there is an automorphism $\varphi\colon R \to R$ such that $*\varphi = \varphi J$, i.e. φ preserves the involutory structure. Now suppose $R = M_n(C)$ and C is algebraically closed. It is easy to show that two involutions (J) and $(*)$ are equivalent iff $(R,*)$ and (R,J) are isomorphic. In this case, one isomorphism class of involutions is represented by the *transpose* which we call (t); the other isomorphism class exists iff there exist invertible antisymmetric matrices in R, which is the case iff n is even and $\operatorname{char}(C) \neq 2$. If $n = 2m$, define the canonical *symplectic involution* (s) by

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}^s = \begin{pmatrix} D^t & -B^t \\ -C^t & A^t \end{pmatrix},$$

where A, B, C, D are $m \times m$ matrices. The canonical symplectic involution is a representative of the second equivalence class; indeed, if $(*) = (\mathrm{t})$ and $(J) = (s)$, then, in the notation of Proposition 5.2, we can take

$$r = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix},$$

where I denotes the $m \times m$ identity matrix.

Now let R be central simple of degree n, with involution $(*)$. Then, if $\bar{C}$ is the algebraic closure of $C = \operatorname{Cent}(R)$, $(*)$ induces an involution $(*)$ on $M_n(\bar{C}) \approx R \otimes_C \bar{C}$, given by $(\Sigma r_i \otimes \bar{c}_i)^* = \Sigma r_i^* \otimes \bar{c}_i$, where $r_i \in R$, $\bar{c}_i \in \bar{C}$. We say $(*)$ has *orthogonal* (resp. *symplectic*) *type* on R if $(*)$ is equivalent to (t) (resp. to (s)) on $M_n(\bar{C})$. The type is well-defined, and we are interested in symplectic type because of

PROPOSITION 5.3. *If $(R, {}^*)$ is a central simple algebra of degree n with symplectic involution, then every symmetric element has degree $\leqq n/2$.*

PROOF. Let $x^* = x$. If $\bar{C}$ is the algebraic closure of $C = \operatorname{Cent}(R)$, then x has degree $\leqq n/2$ over $\bar{C}$ (in $M_n(\bar{C})$), by [3, pp. 230–231] (which makes use of the "Pfaffian"). Using the properties of tensor product, one easily shows that x has degree $\leqq n/2$ over C. Q.E.D.

If D is a division algebra with involution, then n is a power of 2 (cf. [1, theor.

X.19]). Let us now record one more fact about transfer of involution, with proof as in Proposition 5.2.

Proposition 5.4. *Suppose $(D, *)$ is a central division algebra with involution, and K is a* nonmaximal *C-subfield of D. If K has an automorphism φ of degree $\leqq 2$, then the map $\varphi *$: $K \rightarrow K^{\varphi *}$ can be lifted to an inner automorphism of D, with respect to an element that can be chosen to be symmetric (resp. antisymmetric).*

Proof. $\varphi *$ is an isomorphism from the field K to the field $K^{\varphi *}$. Hence, there is an element y of D, such that $yky^{-1} = k^{\varphi *}$ for all k in K. Thus

$$(y^{-1}y^*)^{-1}k(y^{-1}y^*) = (y^*)^{-1}k^{\varphi *}y^* = (yk^{\varphi}y^{-1})^* = k^{**} = k,$$

so $[y^{-1}y^*, K] = 0$, implying $y^* \in yK'$, where K' is the centralizer of K. Thus $y + y^* \in yK'$ and $y - y^* \in yK'$. Since any nonzero element of yK' could be used in place of y, we are done unless every element of yK' is antisymmetric (resp. symmetric); i.e., for fixed $\mu \in \{-1, +1\}$, we would have $(ya)^* = \mu ya$ for all elements a in K'. In particular $1 \in K'$, so $y^* = \mu y$, implying $\mu ya = (ya)^* = a^*y^* = a^*\mu y$, so $yay^{-1} = a^*$ for all a in K'. In particular, for any elements a_1, a_2 of K', we would have $(a_1a_2)^* = a_2^*a_1^* = (ya_2y^{-1})(ya_1y^{-1}) = ya_2a_1y^{-1} = (a_2a_1)^*$, implying $a_1a_2 = a_2a_1$, so K' is commutative. This is impossible if K is nonmaximal, so we have a contradiction. Q.E.D.

Corollary 5.5 *Suppose $(D, *)$ is a central division algebra with involution, and K is a nonmaximal C-subfield of D with an automorphism φ of degree $\leqq 2$. Then there are a symplectic-type involution (J) and an orthogonal-type involution (J') which yield φ when restricted to K.*

Proof. By Proposition 5.4, there is a symmetric element y, as well as an antisymmetric element y', such that $yky^{-1} = y'ky'^{-1} = k^{\varphi *}$, for all elements k of K. Define $J: x \mapsto y^{-1}x^*y$ and $J': x \mapsto y'^{-1}x^*y'$. Obviously (J) and (J') are nonequivalent involutions. Moreover, for all elements k of K, $k^J = y^{-1}k^*y = y^{-1}(k^{\varphi})^{\varphi *}y = y^{-1}yk^{\varphi}y^{-1}y = k^{\varphi}$; analogously, $k^{J'} = k^{\varphi}$ for all elements k of K.

Q.E.D.

We would like to take the opportunity of apologizing for proving results which are quite trivial but are not readily accessible in the literature.

Incidentally, the structure of central division algebras of degree 4 with involution is now clear.

Theorem B. *If $(D, *)$ is a central division algebra with symplectic-type involution and D has degree 4, then $(D, *) \approx (Q_1, *) \otimes (Q_2, *)$, where Q_1, Q_2 are $*$-invariant quaternion subalgebras of D.*

PROOF. Take a symmetric element $d \notin C$. Then $[C(d):C] = 2$, so there exists a nontrivial automorphism φ of $C(d)$ over C. By Proposition 5.4, there is a symmetric element y of D, such that $ydy^{-1} = d^{\varphi}$. Thus d and y generate a quaternion subalgebra Q_1, invariant under $(*)$. Let Q_2 be the centralizer of Q_1. Then Q_2 is invariant under $(*)$ and $Q_1 \otimes Q_2 \approx D$. Q.E.D.

It follows immediately that every division algebra of degree 4 with involution and having characteristic $\neq 2$ is a tensor product of quaternion subalgebras. The characteristic 2 case is a bit more complicated, but can be done without difficulty via Theorem 4.2. The decomposition of division algebras of degree 4 with involution into quaternion subalgebras is due to Albert [1]. A famous conjecture is the following generalization of Albert's theorem.

CONJECTURE 5.6. *Every central division algebra with involution is the tensor product of quaternion subalgebras.*

For the rest of this paper we shall work towards positive partial results for division algebras of degree 8, stated and proved in the next section. Incidentally, the ease with which one can prove Albert's theorem via Theorem B leads one to believe that it is easier to work with the symplectic involution. Accordingly, let us quote some results from [6, §5].

Assume n is even and, as in §0, let $F(\xi)$ be the field generated by a set of commutative indeterminates $\xi_{ij}^{(k)}$ over F, $1 \leqq i, j \leqq n$, $1 \leqq k < \infty$. Fixing the set of matric units $\{e_{ij} \mid 1 \leqq i, j \leqq n\}$ of $M_n(F(\xi))$, we define the generic matrices $Y_k = \Sigma_{i,j=1}^{n} \xi_{ij}^{(k)} e_{ij}$ and their involutes Y_k^s, where (s) is the canonical symplectic involution of $M_n(F(\xi))$. Let $F^{(n)}\{Y, Y^s\}$ be the F-subalgebra of $M_n(F(\xi))$ generated by all the Y_k and all Y_k^s. Note that any element of $F^{(n)}\{Y, Y^s\}$ is a "polynomial" in suitable $Y_1, Y_1^s, \cdots, Y_t, Y_t^s$ and will be written as $f(Y_1, Y_1^s, \cdots, Y_t, Y_t^s)$ to denote this fact. Obviously (s) induces an involution on $F^{(n)}\{Y, Y^s\}$ and, by [6, theor. 27], the central elements are scalars in $M_n(F(\xi))$ and are thus invertible. Let $F^{(n)}(Y, Y^s)$ be the F-subalgebra of $M_n(F(\xi))$ generated by $F^{(n)}\{Y, Y^s\}$ and all inverses of nonzero elements of $\mathrm{Cent}\, F^{(n)}\{Y, Y^s\}$. Again (s) induces an involution on $F^{(n)}(Y, Y^s)$, clearly of symplectic type (when $\mathrm{char}\, F \neq 2$).

THEOREM C ([6, theor. 29]). *$F^{(n)}(Y, Y^s)$ is a central simple algebra of degree n. $F^{(n)}(Y, Y^s)$ is a division algebra iff n is a power of 2.*

The following crucial fact is an easy consequence of [6, theor. 27] (and the technique of tensoring by the algebraic closure of F, as described before Proposition 5.3):

Proposition D. *Suppose R is an arbitrary central simple F-algebra of degree n, with involution $(*)$ of symplectic type. An element $f(Y_1, Y_1^s, \cdots, Y_t, Y_t^s)$ of $F^{(n)}\{Y, Y^s\}$ is zero iff, for all elements $r_1, \cdots, r_t$ of R, $f(r_1, r_1^*, \cdots, r_t, r_t^*) = 0$.*

The way we can use Proposition D is in

Theorem E. *Let $C = \operatorname{Cent} F^{(n)}(Y, Y^s)$, and suppose $K = K_1K_2 \cdots K_k$ is a subfield of $F^{(n)}(Y, Y^s)$, with $[K : C] = m$. Also suppose*

$$K_i = C(f_i(Y_1, Y_1^s, \cdots, Y_t, Y_t^s)g_i(Y_1, Y_1^s, \cdots, Y_t, Y_t^s)^{-1}),$$

where $f_i(Y_1, Y_1^s, \cdots)$ and $g_i(Y_1, Y_1^s, \cdots)$ are elements of $F^{(n)}\{Y, Y^s\}$, for each i. Then, for each central simple F-algebra D which is a division algebra of degree n with involution $(*)$ of symplectic type, there exist elements $d_1, \cdots, d_t$ of D, such that, for $L_i = F(f_i(d_1, d_1^s, \cdots, d_t, d_t^s)g_i(d_1, d_1^s, \cdots, d_t, d_t^s)^{-1})$, we have $L = L_1 \cdots L_k$ is a subfield of D and $[L : F] = m$.

Proof. For simplicity, write f for $f(Y_1, Y_1^s, \cdots, Y_t, Y_t^s)$, etc. We claim that it is enough to assume $g \in \operatorname{Cent} F^{(n)}\{Y, Y^s\}$. Indeed, by definition of $F^{(n)}(Y, Y^s)$, we know that there are elements f' in $F^{(n)}\{Y, Y^s\}$ and g' in $\operatorname{Cent} F^{(n)}\{Y, Y^s\}$, such that $fg^{-1} = f'(g')^{-1}$. Then $fg' = f'g$, so $fg' - f'g = 0$. Hence, for any $d_1, \cdots, d_t$ in D, such that $g'(d_1, d_1^s, \cdots, d_t, d_t^s) \neq 0$ and $g(d_1, d_1^s, \cdots, d_t, d_t^s) \neq 0$, we have

$$f(d_1, d_1^s, \cdots, d_t, d_t^s)g'(d_1, d_1^s, \cdots, d_t, d_t^s)$$
$$- f'(d_1, d_1^s, \cdots, d_t, d_t^s)g(d_1, d_1^s, \cdots, d_t, d_t^s) = 0.$$

Thus

$$f(d_1, d_1^s, \cdots, d_t, d_t^s)g(d_1, d_1^s, \cdots, d_t, d_t^s)^{-1}$$
$$= f'(d_1d_1^s, \cdots, d_t, d_t^s)g'(d_1, d_1^s, \cdots, d_t, d_t^s)^{-1},$$

and the claim is established.

The rest of the theorem is proved exactly as [6, theor. 30 (ii)]. Q.E.D.

The corresponding statement holds for quaternion subalgebras (cf. [6, theor. 30 (iii)], but we do not reproduce the proof because it is not relevant to the results presented in this paper.

§6. Division algebras of degree 8, with involution

The results of this section are given for $D = F^{(8)}(Y, Y^s)$, but, by Remark 5.1 and Theorem E, the structure theory goes over to every division F-algebra of degree 8 with involution. Our main concern will be to construct a maximal subfield K of D which is Galois over $C = \mathrm{Cent}(D)$, with Galois group $\mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2$. The strategy is simple; write $K = K_1K_2K_3$ where K_i are linearly disjoint, quadratic extensions of C. As in §4, the major step is to find K_1. This was first done by verifying formally a result about matrices (cf. Rowen and Schild [7]), but in fact there is the following easy proof:

Theorem 6.1. *Let*

$$d_1 = [Y_1 + Y_1^s, Y_2 - Y_2^s],$$

$$d_2 = [Y_3 - Y_3^s, d_1]d_1[Y_3 - Y_3^s, d_1]^{-1},$$

$$a = d_1 + d_2 = [Y_3 - Y_3^s, d_1^2][Y_3 - Y_3^s, d_1]^{-1}.$$

Then $[C(a^2): C] = 2$.

Proof. Letting $w = [Y_3 - Y_3^s, d_1]$, we see that d_1, w, and $[Y_3 - Y_3^s, d_1^2]$ are all symmetric with respect to (s). In particular, $[C(d_1): C] \leqq 4$, by Proposition 5.3. Let (J) be the involution given by (J): $d \mapsto wd^sw^{-1}$, all d in D. Then J is obviously of symplectic type, and

$$a^J = wa^sw^{-1} = w([Y_3 - Y_3^s, d_1^2]w^{-1})^sw^{-1}$$

$$= w(w^{-1}[Y_3 - Y_3^s, d_1^2])w^{-1} = [Y_3 - Y_3^s, d_1^2]w^{-1} = a.$$

Thus $[C(a): C] \leqq 4$, by Proposition 5.3. One sees easily (by specialization) that $a^2 \notin C$. Thus, by Theorem 4.1, $[C(a^2): C] = 2$. Q.E.D.

Theorem 6.2. *If* $1 + 1 \neq 0$ *in* C *then there are subfields* K_2 *and* K_3 *of* D *such that, with* $K_1 = C(a^2)$, a *as in Theorem* 6.1, $K_i \cap (K_jK_k) \neq 0$ *for each permutation* (i, j, k) *of* $(1, 2, 3)$, *and* $K = K_1K_2K_3$ *is a field. Moreover,* K *is a Galois extension of* C *with Galois group* $\mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2$.

Proof. First we observe that the second sentence is an immediate consequence of the first sentence. Now we give a nonexplicit proof of Theorem 6.2, although it can be transformed easily into an explicit, constructive proof. First observe that if $[C(x): C] = 2$ then some element of $C(x)$ is square central. (Indeed, if $x^2 + \alpha x + \beta = 0$ for α, β in C, then $(x + \alpha/2)^2 = (\alpha/4)^2 - \beta \in C$. In fact, it turns out, by [1, theor. VIII.13], that $\alpha = -\mathrm{tr}(x)/4$.)

So we have $K_1 = C(x)$, with x square-central. Note that if K_1 is contained in a central simple quaternion F-subalgebra Q_1 of D then we are done, because the centralizer Q_2 of Q_1 is central C-simple of degree 4 and thus, by Theorem 4.5, we can find a maximal subfield K_2K_3 of Q_2, such that $K_1K_2K_3$ satisfies the conclusion of this theorem. Thus, we shall assume K_1 is *not* contained in a central simple quaternion F-subalgebra.

Now $x \mapsto -x$ induces an automorphism of degree 2, of K over C. Thus, by Corollary 5.5, we have an involution (*) of symplectic type (on D), such that $x^* = -x$. By Proposition 5.4, taking $\varphi = 1$, we have an element y, such that $y^* = y$ and $yxy^{-1} = -x$. Clearly $[C(y): C] \leqq 4$ (by Proposition 5.3), and $[y^2, x] = 0$, implying $C(y^2) \subset C(y)$, so $[C(y^2): C] \leqq 2$. If $y^2 \in K_1$ then x, y generate a quaternion C-subalgebra of D, contrary to assumption, so $y^2 \notin K_1$. Hence $[C(y^2): C] = 2$ and $C(y^2) \cap K_1$ is a proper C-subfield of $C(y^2)$ (and is thus C). Let $K_2 = C(y^2)$.

K_2 has a nontrivial automorphism ψ over C. Let ϕ be the automorphism of K_1K_2, such that $x^\phi = -x$ and $k^\phi = k^\psi$ for all k in K_2. By Proposition 5.4, we have z such that $z^* = z$, $zxz^{-1} = x^{\phi *} = x$, and $zkz^{-1} = k^\psi$ for all k in K_2. Now $[C(z): C] \leqq 4$ and $z^2y^2 = y^2z^2$, implying $C(z^2) \subset C(z)$, so $[C(z^2): C] \leqq 2$. Let $K_3 = C(z^2)$. If $K_3 \subseteq K_1K_2$ then $z^2 = \alpha_1 + \alpha_2 x + \alpha_3 y^2 + \alpha_4 xy^2$ for suitable α_i in C, and also $z^2 = (z^2)^* = \alpha_1 - \alpha_2 x + \alpha_3 y^2 - \alpha_4 xy^2$, implying $2z^2 = 2\alpha_1 + 2\alpha_3 y^2$, so $z^2 \in K_2$; this would imply that y^2 and z generate a quaternion C-subalgebra of D, contrary to assumption.

Thus, $K_3 \nsubseteq K_1K_2$. In particular, $[K_3: C] = 2$ and $K_3 \cap K_1K_2 = C$. An identical argument shows $K_2 \cap K_1K_3 = C$. Finally, K_2K_3 contains only (*)-symmetric elements, so clearly $K_1 \cap K_2K_3 = C$. Since x, y^2, and z^2 all commute, we see that $K = K_1K_2K_3$ is our desired field. Q.E.D.

In the proof of Theorem 6.2, it is immediate how to build y, based on Lemma 4.4. The choice of z is a bit more complicated, but not overly difficult. Once we have found x, y^2, and z^2, we could write these three elements in the form (respectively) $f_i c_i^{-1}, 1 \leqq i \leqq 3$, where $f_i \in F^{(8)}\{Y, Y^s\}$; there is a canonical map $\mathbf{Z}^{(8)}\{Y, Y^s\} \rightarrow (\mathbf{Z}/2\mathbf{Z})^{(8)}\{Y, Y^s\}$, given by the map $\mathbf{Z} \rightarrow \mathbf{Z}/2\mathbf{Z}$, and if the images of the f_i are nonzero, then this would yield Theorem 6.2 even in the characteristic 2 case. (We leave out the details.) It should be a simple matter to check this out (by specialization), but we have not done this.

REFERENCES

1. A. A. Albert, *Structure of Algebras*, Amer. Math. Soc. Colloq. Publ. XXIV, 1961.

2. S. A. Amitsur, *On central division algebras*, Israel J. Math. **12** (1972), 408–422.

3. N. Jacobson, *Structure and Representation of Jordan Algebras*, Amer. Math. Soc. Colloq. Publ. XXXIX, 1968.

4. N. Jacobson, *PI-Algebras: An Introduction*, Springer-Verlag Lecture Notes in Mathematics **441**, 1975.

5. L. H. Rowen, *Universal PI-algebras and algebras of generic matrices*, Israel J. Math. **18** (1974), 65–74.

6. L. H. Rowen, *Identities in algebras with involution*, Israel J. Math. **20** (1975), 70–95.

7. L. H. Rowen and U. Schild, *A scalar expression for matrices with symplectic involution*, to appear.

8. J. H. M. Wedderburn, *On division algebras*, Trans. Amer. Math. Soc. **22** (1921), 129–135.

DEPARTMENT OF MATHEMATICS
BAR ILAN UNIVERSITY
RAMAT GAN, ISRAEL