PACIFIC JOURNAL OF MATHEMATICS
Vol. 124, No. 1, 1986

ALTERNATIVE ALGEBRAS HAVING SCALAR INVOLUTIONS

R. A. KUNZE AND S. SCHEINBERG

An involution of an algebra over a field of characteristic different from two is called *scalar* if the sum of each element and its involute is a scalar (multiple of the unit). Certain algebras having scalar involutions have played an important role in the construction of metaplectic representations and the applications of that theory to problems in number theory and automorphic forms. They also arise in an analytic context related to homomorphic discrete series and in questions about invariants of classical groups. This paper deals with determining the structure of the most general algebras having scalar involutions.

1. Non-singular subalgebras and the radical.

1.1. *Singular composition algebras.* We shall classify all algebras, including the infinite-dimensional ones, that admit a particularly restrictive type of involution. By "algebra" we mean an alternative algebra A with unit 1 over a commutative field F of characteristic different from 2. An F-linear involution $a \to a'$ of A is called *scalar* if $a + a' \in F1$ for every $a \in A$. This is equivalent to the condition: $a = a'$ precisely for $a \in F1$. It is also equivalent to the condition: $aa' \in F1$ for all $a \in A$; a is invertible if and only if $aa' \neq 0$, in which case $a^{-1} = (aa')^{-1}a'$. We normally abuse the notation to the extent of identifying $F1$ with F. With this convention, the formula

$$(a \mid b) = \tfrac{1}{2}(ab' + ba') \tag{1}$$

$a \to a'$ being a scalar involution, defines a symmetric bilinear form an A which satisfies the law of composition

$$(ab \mid ab) = (a \mid a)(b \mid b). \tag{2}$$

In [7], Jacobson defines a *composition algebra* as an algebra with scalar involution for which the associated form (1) is nondegenerate. We shall call such algebras *non-singular composition algebras*. Their structure has been the subject of many investigations, e.g., [1], [2], [6], [9], and is well known. They are necessarily semisimple and finite dimensional, in fact, of diffeomorphism 1, 2, 4 or 8 over the ground field. Here we drop the nondegeneracy condition and study the possibly singular case, i.e., arbitrary algebras with scalar involutions.

Some comments on our assumptions are in order. The classical Hurwitz problem was to determine all finite dimensional algebras (not necessarily alternative) with a non-singular symmetric form satisfying (2). Such an algebra is necessarily alternative and is in fact a non-singular composition algebra as defined above. In [8] Kaplansky proved that there are no infinite dimensional algebras, alternative or not, with non-singular symmetric forms admitting composition. If one drops the non-singularity assumption in the context considered by Kaplansky, it cannot be concluded that the algebra is alternative. We have constructed a non-alternative algebra of infinite dimension with a non-zero singular quadratic form that satisfies (2).

In contrast to the non-singular case, the more general composition algebras that we study need not be semisimple and may well have a radical of infinite dimension, the radical being the union of all 2-sided nilpotent ideals. The radical may also be characterized as the radical of the associated form and also as the orthogonal complement of any maximal non-singular subalgebra.

THEOREM 1.2. *Let A be an algebra with scalar involution, R the radical of the associated form, and B a maximal non-singular subalgebra of A. Then $B^{\perp} = A^{\perp} = R$, $A = B \oplus R$ a vector space direct sum, R is a 2-sided ideal of skew-symmetric elements of A and B is isomorphic to A/R.*

Proof. Much of the proof can be lifted from [7, Chap. IV, Sect. 3] and will only be sketched.

Standard arguments show that the form (1.1.1) associated with A is such that

$$(a|b) = (b'|a') \tag{1}$$

$$(ab|c) = (b|a'c) = (b|ca') \tag{2}$$

$$(ac|bc) = (a|b)(c|c) \tag{3}$$

for all a, b, c in A. Since B is finite dimensional, $A = B \oplus B^{\perp}$ where

$$B^{\perp} = \{c \in A: bc + cb' = 0 \text{ for all } b \in B\}. \tag{4}$$

Taking $b = 1$ in (4), one sees that $B^{\perp}$ is a linear space of skew-symmetric elements. By (2)

$$BB^{\perp} \subseteq B^{\perp}. \tag{5}$$

If there is no non-isotropic vector in $B^{\perp}$, then the form is trivial on $B^{\perp}$, and this implies $B^{\perp} = A^{\perp} = R$. On the contrary, assume $B^{\perp}$ contains a

non-isotropic vector c. Then by (5), $Bc \subseteq B^{\perp}$. Hence, $B + Bc = B \oplus Bc$. By (3)

$$(ac \mid bc) = (a \mid b)(c \mid c)$$

for all a, b in B. Because the form is non-singular on B, it follows that Bc is a non-isotropic subspace of $B^{\perp}$ of the same dimension as B. At this point, more complicated arguments in [7] which involve the alternative assumption and the Moufang identities imply that $B \oplus Bc$ is a non-singular subalgebra of A and that B is necessarily associative. But since B is already maximal, it follows that every element of $B^{\perp}$ is isotropic and hence that $B^{\perp} = A^{\perp} = R$. Now (2) and the observation after (4) imply that R is a 2-sided ideal of skew-symmetric elements. Hence, A/R is again an algebra with scalar involution, and from the decomposition $A = B \oplus R$ it follows that B and A/R are isomorphic as algebras with scalar involutions.

Next we turn to the problem of showing that the geometric radical R in (1.2) is the radical of the algebra.

THEOREM 1.3. *If A is an algebra with scalar involution, then the radical of the associated form is the union of the nilpotent ideals of A.*

Proof. Let A be an algebra with scalar involution and $R = A^{\perp}$. Then for r in R, $r' = -r$, and

$$ar = ra' \tag{1}$$

for all $a \in A$. In particular, for all $r \in R$

$$r^2 = 0. \tag{2}$$

Consider a nilpotent element b; b is not invertible; therefore $bb' = b'b = 0$. Thus, $b^2 = (b + b')b$, and by induction $b^n = (b + b')^{n-1}b$. Since $b^n = 0$ for large n, and $b + b' \in F1$, we conclude that $b + b' = 0$ for nilpotent b. Now if every element of a left ideal Ab is nilpotent, then for every a we have $0 = ab + (ab)' = ab + b'a' = ab - ba'$. That is, $2(a \mid b) = ab' + ba' = -ab + ba' = 0$. Therefore, $b \in A^{\perp} = R$. In particular, if Ab is a nilpotent left ideal, $Ab \subseteq R$. It follows that R contains the union of all nilpotent (left) ideals of A.

Next we observe, as in [7], that the alternative law and $a + a' \in F1$ imply $a(a'b) = (a \mid a)b$. Thus, by linearization,

$$a(c'b) + c(a'b) = 2(a \mid c)b = (ba)c' + (bc)a' \tag{3}$$

for all a, b, c in A.

Now suppose $c \in R$. Then $c' = -c$ and (3) implies $(bc)a' = (ba)c$ for all a, b in A. Because $bc \in R$, it follows from (1) that

$$a(bc) = (ba)c \tag{4}$$

for all a, b in A. Hence, Ac is a left (and automatically right) ideal in A. Moreover, by (4), the alternative law, and (2), $(ac)(bc) = (b(ac))c = ((ab)c)c = (ab)c^2 = 0$ for arbitrary a, b in A. Thus, $(Ac)^2 = 0$ and R is the union of the nilpotent ideals of A.

COROLLARY 1.4. *For each $r \in R$, Ar is a 2-sided ideal in A such that $(Ar)^2 = 0$.*

The results obtained and used in the proof of (1.3) may be extended to show that the radical R is itself a nilpotent ideal; in fact, $R^4 = 0$. But the exponent 4 is best possible only when $A/R = F1$ and A is not associative. For example, $R = 0$, at the opposite extreme, when $\dim(A/R) = 8$. In qualitative terms, the exponent required to annihilate R decreases as the dimension of A/R increases. The precise result is the following:

THEOREM 1.5. *Let A be an algebra with scalar involution and R the radical of A. The dimension of A/R is 2^n where $0 \leq n \leq 3$. For this n, $R^{4-n} = \{0\}$. In the case that A is associative, $0 \leq n \leq 2$, and $R^{3-n} = \{0\}$.*

To prove this it is convenient to proceed in relatively easy stages with some preparatory results.

LEMMA 1.6. *Let B be a subalgebra of A and c an element of A orthogonal to B. Then B is orthogonal to Bc, $B + Bc$ is a subalgebra of A and multiplication in $B + Bc$ is such that*

$$(b_1c)b_2 = (b_1b_2')c$$

$$b_1(b_2c) = (b_2b_1)c$$

$$(b_1c)(b_2c) = c^2(b_2'b_1)$$

for all b_1, b_2 in B.

Proof. This follows from (1.3.3), the alternative law, and the Moufang identities just as in the non-singular case [7].

The following is an immediate Corollary of (1.6).

COROLLARY 1.7. *Let x and y be elements of A such that* 1, x, *and y are mutually orthogonal. Then x and y anticommute in the sense that $xy = -yx$; the elements* 1, x, y, xy *are mutually orthogonal, and their linear span is the subalgebra $F[x, y]$ generated by x and y.*

The next result is a direct consequence of (1.6) and (1.7).

COROLLARY 1.8. *Let x and y be as in* (1.7) *and z orthogonal to $F[x, y]$. Then*

$$1, x, y, xy, z, xz, yz, (xy)z$$

are mutually orthogonal, and their linear span is the subalgebra $F[x, y, z]$ generated by x, y and z.

LEMMA 1.9. *If* 1, a, b, ab *and c are mutually orthogonal elements of A, then a, b and c anti-associate; that is*

$$a(bc) = -(ab)c.$$

Proof. By (1.3.3), $a(cb) + c(ab) = 0$. By (1.7), $cb = -bc$ and $c(ab) = -(ab)c$. Hence, $a(bc) = -(ab)c$.

Now we can prove the key combinatorial lemma required for the proof of (1.5)

LEMMA 1.10. *Let x, y and z be as in* (1.8) *and w orthogonal to $F[x, y, z]$. Then every product of the four elements x, y, z, w in any order and any grouping by parentheses is* 0.

Proof. By (1.8), if a, b, c are any three of x, y, z, w, then the elements

$$1, a, b, c, ab, ac, bc, (ab)c \tag{1}$$

are mutually orthogonal. Hence, by (1.7) any two of (1) other than 1 anti-commute. Therefore, any product of the four elements equals $\pm$ a product in which, reading from left to right and ignoring parentheses w is last. Thus, since x, y, and z are interchangeable, it is enough to show that

$$x(y(zw)) = x((yz)w) = (xy)(zw) = ((xy)z)w = 0.$$

For this we shall use anti-associativity repeatedly. By assumption w is orthogonal to $F[x, y, z]$. Hence, by (1.6), (1.7), and (1.8) the elements

$$1, x, y, xy, z, xz, yz, (xy)z, w, zw$$

are mutually orthogonal. Thus, by (1.9),

$$x(y(zw)) = -(xy)(zw) = ((xy)z)w = -(x(yz))w$$
$$= x((yz)w) = -x(y(zw)) = 0.$$

Proof of 1.5. Let x, y, z, and w be skew elements selected sequentially, starting with x, to satisfy the hypotheses of (1.10) and with as many as possible non-isotropic, as in (1.2). The non-isotropic vectors (if any) generate a maximal non-singular subalgebra B, and since $R = A^{\perp} = B^{\perp}$, the remainder of the list belong to R. From (1.10) we have that the product of x, y, z, and w in any order and with any grouping by parentheses in 0.

In case $B = F$, all of x, y, z, w belong to R and any product of the four elements is 0; if A is associative, (1.9) implies that any product of three of them is 0.

In case $\dim B = 2$, $B = F[x]$ and y, z, and w belong to R. Let p be any product of y, x and w. Then $xp = 0$. Since $xx' = -x^2 \neq 0$ and A is alternative, we can cancel x to find that $p = 0$. That is, $R^3 = \{0\}$. By (1.9) $x(yz) = -(xy)z$; so if A is associative, $x(yz) = 0$ and, cancelling x, we have $yz = 0$. That is, when A is associative, $R^2 = \{0\}$.

When $\dim B = 4$, $B = F[x, y]$, and z and w belong to R. $x(y(zw)) = 0$. Cancel x, then y (since $y^2 \neq 0$) to obtain $zw = 0$. Thus, $R^2 = \{0\}$. As earlier anti-associativity of x, y, z and associativity of A would imply $x(yz) = 0$; hence $z = 0$. So in this case, if A is associative, $R = \{0\}$.

Finally, if $\dim B = 8$, $B = F[x, y, z]$ and $w \in R$. $x(y(zw)) = 0$; cancelling x, then y, then z (since $z^2 \neq 0$), we obtain $w = 0$. That is, $R = \{0\}$ when $\dim B = 8$. $A = B$, which is not associative.

2. Structure analysis. At this point we have shown that $A = B \oplus R$, with B a maximal non-singular subalgebra and R the radical. As in the proof of Theorem (1.5) B has the form F $(= F1)$, $F[x]$, $F[x, y]$, or $F[x, y, z]$, according to the dimension of A/R, which is 2^n for $n = 0, 1, 2$, or 3, respectively. We have seen that $R^{4-n} = \{0\}$ ($R^{3-n} = \{0\}$ in case A is associative.) The structure of A is, of course, determined by the structure of B, the structure of R, and the interaction of B and R. In this section we make these things more explicit and thereby complete the classification of A.

The structure of the non-singular algebra B is known; the following summary will suffice for the moment.

THEOREM 2.1. *Let B be a non-singular alternative algebra with scalar involution over a field F (commutative of characteristic $\neq 2$). Then* $\dim B = 1, 2, 4,$ *or* $8,$ *and we have the following*

(a) *If* $\dim B = 1$, *then* $B = F$.

(b) *If* $\dim B = 2$, *either B is a (commutative) field or else B is isomorphic to the algebra $F^2 = F \oplus F$ with coordinate-wise algebraic operations and involution* $(\alpha, \beta)' = (\beta, \alpha)$.

(c) *If* $\dim B = 4$, *either B is a (non-commutative) division ring (a so-called quaternion ring) or else B is isomorphic to the algebra $F^{2\times 2}$ of* 2×2 *matrices over F, with* $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)' = \left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$.

(d) *If* $\dim B = 8$, *either B has no divisors of zero or else B is isomorphic to the Cayley extension of $F^{2\times 2}$ by an element whose square is* 1.

Next, let us consider the possible algebraic structures on R, the radical.

PROPOSITION 2.2. *Let R be an alternative algebra (without unit) over F in which $r^2 = 0$ for every r. Then multiplication in R is anti-commutative and anti-associative. The map $r \to -r$ is an F-linear involution of R, and every product of four elements of R is* 0.

Proof. Because all squares are 0, $0 = (r + s)^2 = r^2 + rs + sr + s^2 = rs + sr$; so multiplication is anti-commutative. Then for $r, s,$ and t in R, because R is alternative,

$$\begin{aligned} 0 = (r + t)^2 s &= (r + t)[(r + t)s] = (r + t)(rs + ts) \\ &= r(rs) + r(ts) + t(rs) + t(ts) = r^2 s + r(ts) + t(rs) + t^2 s \\ &= r(ts) + t(rs) = -r(st) - (rs)t; \end{aligned}$$

so multiplication is anti-associative. The F-linear map $r \to -r$ is an involution by anti-commutativity. The proof of (1.10) shows that in an algebra with anti-commutative anti-associative multiplication every product of four elements vanishes.

COROLLARY 2.3. *Let R be an alternative algebra over F in which $r^2 = 0$ for every r. Then R is associative if and only if every product of three elements is* 0.

The most general R in Proposition (2.2) can be analyzed as follows. Let $W = \{r\colon\ rR = \{0\}\}$, let V be any vector space complement to $R^2 + W$ in R^2, and let U be any vector space complement to $V + W$ in

R. Select a basis $\{u_i; i \in I\}$ for U, and for i, j, k in I let $v_{ij} \in V$, $w_{ij} \in W$ and $w_{ijk} \in W$ be determined by the equations;

(1) $u_iu_j = v_{ij} + w_{ij}$ and $u_iv_{jk} = w_{ijk}$. Because $R^4 = \{0\}$, we have

(2) $V \cdot V = R \cdot W = \{0\}$, by definition of V and W. Because multiplication in R is anti-commutative and anti-associative,

(3) v_{ij}, w_{ij}, and w_{ijk} are anti-symmetric as functions of the indices i, j, k. For example,

$$\begin{aligned} w_{jik} &= u_j(v_{ik}) = u_j(u_iu_k - w_{ik}) = u_j(u_iu_k) \\ &= -(u_iu_k)u_j = u_i(u_ku_j) = -u_i(u_ju_k) \\ &= -u_i(u_ju_k - w_{jk}) = -w_{ijk}. \end{aligned}$$

From the definitions of U, V and W and the fact that $V \subseteq R^2$ and $U \cdot V \subseteq W$ it is easy to verify that

(4) the collection $\{u_{ij}\}$ spans V, and

(5) for $\lambda_{jk} \in F$, whenever $\Sigma\lambda_{jk}v_{jk} = 0$, we have $\Sigma\lambda_{jk}w_{ijk} = 0$ for all i.

Finally, by definition of W, if $r \in U + V$ and $r \neq 0$ there is $u \in U$ so that $ru \neq 0$.

Conversely, if U, V, and W are any three vector spaces, possibly including $\{0\}$, with elements u_i, collectively a basis for U, v_{ij} in V, and w_{ij} and w_{ijk} in W, define the vector space R as $U \oplus V \oplus W$. If (3), (4), and (5) are satisfied, we can define a multiplication in R by (1) and (2) and their anticommutative analogues and the linear extensions of all of them. Because of (4) and (5) the multiplication is well-defined, and because of (1), (2), and (3) all squares r^2 are 0.

An immediate consequence is this portion of the structure theorem.

THEOREM 2.4(a). *An alternative algebra with scalar involution and F as its maximal non-singular subalgebra is precisely an algebra $F \oplus R$, in which $r^2 = 0$ for all r in R and $r' = -r$. Such an R has a description in terms of subspaces U, V, and W as given above, and $R^4 = \{0\}$. The algebra is associative if and only if $R^3 = \{0\}$.*

REMARKS.

(1) R is associative if and only if $V = \{0\}$, i.e., $W \supseteq R^2$.

(2) The simplest R for which $R^3 \neq \{0\}$ is the 7-dimensional algebra in which U is spanned by $\{r_1, r_2, r_3\}$, V is spanned by $\{r_1r_2, r_1r_3, r_2r_3\}$, and W is spanned by $\{r_1(r_2r_3)\}$, with the obvious anti-commutative, anti-associative multiplication.

Next consider $\dim B = 2$. $R^3 = \{0\}$; so the algebraic structure of R is determined by an anti-commutative pairing $U \times U \to W$, where W is the multiplicative annihilator of R and U is a vector space complement to W in R. However, the action of B on R must be taken into account. As in Theorem 2.1b there are two cases. First consider the case that B is a degree 2 field extension of F. $B = F[x]$, where x is a skew element; let $x^2 = \alpha \in F$. Because B is field, α is not a square in F. Recall that if r and s are elements of R, the elements x, r, and s anti-commute in pairs and anti-associate as a triple (in any order).

Observe that if S is any subspace of R which is invariant under (left) multiplication by x, and if $r \notin S$, the span of $\{r, xr\}$ meets S in $\{0\}$. For if $\lambda r + \mu xr \in S$ we could conclude $r \in S$ if $\lambda + \mu x$ were invertible; so $0 = (\lambda + \mu x)(\lambda + \mu x)' = (\lambda + \mu x)(\lambda - \mu x) = \lambda^2 - \mu^2 x^2 = \lambda^2 - \mu^2\alpha$. Since α is not a square in F, $\mu^2 = 0$. Thus, $\lambda^2 = 0$ also; so $\lambda r + \mu xr = 0$.

The equation $r_1(xr_2) = -(xr_2)r_1 = x(r_2r_1) = -x(r_1r_2)$ shows that the subspace W defined earlier is invariant under multiplication by x. By the observation in the preceding paragraph and an argument based on Zorn's Lemma we can select a maximal linearly independent set of the form $\{r_i, xr_i\colon i \in I\}$ with span disjoint from W, except for $\{0\}$. Call U the span of the set $\{r_i, xr_i\colon i \in I\}$. Define w_{ij} by $r_ir_j = w_{ij} \in W$; as a function of i and j w_{ij} is anti-symmetric. $(xr_i)r_j = -x(r_ir_j) = -xw_{ij}$, $(xr_i)(xr_j) = -(xr_i)(r_jx) = -x(r_ir_j)x = x^2(r_ir_j) = \alpha w_{ij}$, where the second equality is a Moufang law; this can also be seen as in the proof of Theorem 1.3.

Conversely, let U and W be arbitrary vector spaces, each of which has an automorphism X (for convenience we use the same symbol) such that X^2 is α times the identity. Select a basis for U of the form $\{u_i, Xu_i\colon i \in I\}$ and choose any elements $w_{ij} \in W$, subject to the condition $w_{ji} = -w_{ij}$. The vector space $A = F[x] \oplus U \oplus W$ becomes an alternative algebra with radical $R = U \oplus W$ if we define multiplication by these rules and their linear extensions: $u_iu_j = w_{ij}$, $xu = -ux = Xu$ for $u \in U$, $xw = -wx = Xw$ for $w \in W$, $(Xu_i)u_j = -u_j(Xu_i) = -Xw_{ij}$, $(Xu_i)(Xu_j) = \alpha w_{ij}$, $RW = WR = \{0\}$. Note that W is the multiplicative annihilator of R if and only if the multiplication $U \times U \to W$ is nonsingular in the sense that for every $u \neq 0$ there is a u^* so that $uu^* \neq 0$.

Next, suppose α is a square in F. Replacing x by $x/\sqrt{\alpha}$ we may suppose $x^2 = 1$. Then left multiplication by x has two (potential) eigenvalues, $+1$ and -1, it is completely diagonalizable on every invariant subspace, and every invariant subspace has a complementary invariant subspace. If $xS \subseteq S$ for a space S, then $S = S_+ \oplus S_-$, where $S_+ = \{s\colon s \in S \text{ and } xs = s\}$ and $S_- = \{s\colon s \in S \text{ and } xs = -s\}$. Therefore, if we

select W as before and U an x-invariant complement to W in R, we can write $R = U_+ \oplus U_- \oplus W_+ \oplus W_-$. Consider the equation $(xr_1)r_2 = -x(r_1r_2) = x(r_2r_1) = -(xr_2)r_1 = r_1(xr_2)$. Let $r_1 \in U_+$ and $r_2 \in U_-$ and compare the first and last terms; we obtain $r_1r_2 = 0$. So $U_+ \cdot U_- = U_- \cdot U_+ = \{0\}$. Let r_1 and r_2 both belong to U_+; $(xr_1)r_2 = -x(r_1r_2)$ shows that $r_1r_2 \in W_-$. That is $U_+ \cdot U_+ \subseteq W_-$; similarly, $U_- \cdot U_- \subseteq W_+$.

Conversely if $U_\pm$, $W_\pm$ are any four vector spaces and $U_+ \times U_+ \to W_-$ and $U_- \times U_- \to W_+$ are arbitrary anti-commutative multiplications, define $R = U_+ \oplus U_- \oplus W_+ \oplus W_-$ and $A = F[x] \oplus R$ as vector spaces. A becomes an alternative algebra with radical R if we define multiplication on A by utilizing the given multiplications $U_+ \times U_+ \to W_-$ and $U_- \times U_- \to W_+$, by putting $R(W_+ + W_-) = (W_+ + W_-)R = 0$, and by defining $U_+ \cdot U_- = U_- \cdot U_+ = \{0\}$, $rx = -xr$ for all r, $xu = \pm u$ for $u \in U_\pm$, and $xw = \pm w$ for $w \in W_\pm$. The vector spaces $U = U_+ + U_-$ and $W = W_+ + W_-$ have the roles assigned in the preceding paragraph if and only if the multiplications on U_+ and on U_- are non-singular.

Summarizing the foregoing we have the next portion of the structure theorem.

THEOREM 2.4(b). *An alternative algebra with scalar involution and maximal non-singular subalgebra of the form $F[x]$ is precisely an algebra $F[x] \oplus R$, where the description is one of those given just above. The algebra is associative if and only if $R^2 = \{0\}$ (i.e., $U = \{0\}$).*

Now consider the case that B is of the form $F[x, y]$, where x and y are orthogonal skew elements. In this case $R^2 = \{0\}$; so we need only describe the vector space structure of R and the endomorphisms given by left multiplication by elements of B. Recall 1.3(4): $a(br) = (ba)r$ for a and b in B and r in R. Thus $a'(b'r) = (b'a')r = (ab)'r$. In other words $b \to$ left multiplication by b' is a representation of B by endomorphisms of R.

In the case that B is a division ring, it is well known that every representation φ of B on a vector space R ($\neq 0$) can be decomposed: R is a direct sum of copies of the vector space B, and on each copy of B each $\varphi(b)$ acts by left multiplication by b. Thus, $A = B \oplus \Sigma_j \oplus B_j$ (each $B_j = B$), where multiplication in $\Sigma_j \oplus B_j$ is trivial and $b(\Sigma_j \oplus b_j) = \Sigma_j \oplus b'b_j = -(\Sigma_j \oplus b_j)b$. Conversely, if we define $R = \Sigma \oplus B_j$, each $B_j = B$, and we let $A = B \oplus R$ with the multiplication just given, we easily verify that the result is an alternative algebra with radical R and maximal non-singular subalgebra B.

In the other case for dim $B = 4$ B is isomorphic to $F^{2\times 2}$, the algebra of 2×2 matrices over F. As is well known, every representation φ of B by endomorphisms of a vector space R decomposes: $R = \Sigma \oplus W_j$ (each $W_j = F^{2\times 1}$ = the 2×1 column vectors over F), and on each W_j each $\varphi(b)$ is left multiplication by b. This means that $A = F^{2\times 2} \oplus \Sigma \oplus W_j$ (each $W_j = F^{2\times 1}$), where multiplication on ΣW_j is trivial and $b(\Sigma \oplus w_j) = \Sigma \oplus b'w_j = -(\Sigma \oplus w_j)b \in F^{2\times 2}$. Conversely, any such $A = F^{2\times 2} \oplus \Sigma \oplus W_j$, with the above multiplication, is clearly an alternative algebra with $B = F^{2\times 2}$ as maximal non-singular subalgebra and $\Sigma \oplus W_j$ as radical.

Summarizing this, we have

THEOREM 2.3(c). *An alternative algebra A with scalar involution and maximal non-singular subalgebra B of diffeomorphism 4 is one of the following*:

(i) *B is a division algebra; $A = B \oplus (\Sigma \oplus B)$ with multiplication as given above, or*

(ii) *B has divisors of zero; $A = F^{2\times 2} \oplus (\Sigma \oplus F^{2\times 1})$, with multiplication as given above.*

In either case A is associative if and only if $A = B$ (i.e., $R = \{0\}$).

The last portion of the structure theorem needs no further elaboration.

THEOREM 2.3(d). *An alternative algebra with maximal non-singular subalgebra B of diffeomorphism 8 is simply B itself. $R = \{0\}$, and the algebra is not associative.*

As we have seen in Theorem 2.1 and Theorem 2.3 there is a dichotomy in the description of the structure of a non-singular composition algebra B (and of any $A = B \oplus R$), according to whether B has divisors of zero. This can be characterized by whether a certain quadratic form represents 0 or 1 in F. The case $B = F$ is completely trivial; so assume dim $B = 2, 4$, or 8. As in the proof of Theorem 1.5, let $B = F[x]$, $F[x, y]$, or $F[x, y, z]$, where the elements x, y, z are chosen successively, each orthogonal to the algebra generated by the preceding ones and each nonisotropic. That is, x^2, y^2, and z^2 (as many as exist) are nonzero elements of F.

For completeness we state the next, well-known proposition.

PROPOSITION 2.4. *Let $B = F[x]$ be a non-singular composition algebra, and define $\alpha = x^2 \neq 0$. Then B is a (commutative) field if and only if $\alpha X^2 \neq 1$ for all X in F.*

The essential features of the next proposition are known. We include a proof because we need certain details later.

PROPOSITION 2.5. *Let $B = F[x, y]$ be a 4-dimensional non-singular composition algebra, with $\alpha = x^2 \neq 0$ and $\beta = y^2 \neq 0$ The following are equivalent.*

(a) *B is a division algebra*

(b) *$\alpha X^2 + \beta Y^2 \neq 1$ for all X and Y in F*

(c) *$\alpha X^2 + \beta Y^2 \neq 0, 1$ for all X and Y in F other than $X = Y = 0$.*

Proof.

(a) $\rightarrow$ (b): If (b) fails, then $\alpha X^2 + \beta Y^2 = 1$; so

$$(1 + Xx + Yy)(1 - Xx - Yy) = 0.$$

(b) $\rightarrow$ (c): If (b) holds while (c) fails, then $\alpha X^2 + \beta Y^2 = 0$ for some $(X, Y) \neq (0, 0)$. Since $\beta \neq 0$, X cannot be 0, for that would imply $Y = 0$. Now $\alpha(X\lambda)^2 + \beta(Y\mu)^2 = \alpha X^2(\lambda^2 - \mu^2)$. This will equal 1 if $\lambda = (1 + \alpha^{-1}X^{-2})/2$ and $\mu = \lambda - 1$, contradicting (b).

(c) $\rightarrow$ (a): If (c) holds while (a) fails, we shall obtain a contradiction as follows. There $z \in F[x, y]$ for which $zz' = 0$ while $z \neq 0$. Write $z = \lambda + \mu x + \nu y + \pi xy$ and $w = \lambda - \pi xy$. Now if $w = 0$, $0 = zz' = \alpha\mu^2 + \beta\nu^2$, contrary to (c). Thus, $w \neq 0$. Now $\alpha ww' = \alpha(\lambda^2 + \alpha\beta\pi^2) = \alpha\lambda^2 + \beta(\alpha\pi)^2$, which is not zero, by (c). Therefore, w^{-1} exists. Put $u = zw$; $u \neq 0$, while $uu' = 0$. We calculate $u = (\lambda^2 + \alpha\beta\pi^2) + \delta x + \varepsilon y = \gamma + \delta x + \varepsilon y$, for $\gamma, \delta, \varepsilon$ in F, with $\gamma \neq 0$. However, $0 = uu' = \gamma^2 - \alpha\delta^2 - \beta\varepsilon^2$, or $\alpha(\delta/\gamma)^2 + \beta(\varepsilon/\gamma)^2 = 1$, contrary to (c).

PROPOSITION 2.6. *Let $B = F[x, y, z]$ be an 8-dimensional non-singular composition algebra with $\alpha = x^2 \neq 0$, $\beta = y^2 \neq 0$, and $\gamma = z^2 \neq 0$. The following are equivalent:*

(a) *B has no divisors of zero;*

(b) *$\alpha X^2 + \beta Y^2 + \gamma Z^2 + \alpha\beta\gamma W^2 \neq 1$ if X, Y, Z, and W belong to F;*

(c) *$\alpha X^2 + \beta Y^2 + \gamma Z^2 + \alpha\beta\gamma W^2 = 0, 1$ for all X, Y, Z, W in F except $X = Y = Z = W = 0$.*

Proof.

a $\rightarrow$ b: If (b) fails, put $u = 1 + Xx + Yy + Zz + W(xy)z$; then $uu' = 0$.

b → c: If (b) is true while (c) fails, then $\alpha X^2 + \beta Y^2 + \gamma Z^2 + \alpha\beta\gamma W^2 = -uu' = 0$ for some $u = Xx + Yy + Zz + W(xy)z \neq 0$. We may assume $W \neq 0$. (If not, we could replace u by $v = u(yz)$, $u(xz)$, or $u(xy)$, a linear combination of x, y, z, and $(xy)z$ with coefficient of $(xy)z$ not zero, and $vv' = 0$.) Note that $\alpha(X\mu)^2 + \beta(Y\mu)^2 + \gamma(Z\mu)^2 + \alpha\beta\gamma(W\lambda)^2 = \alpha\beta\gamma W^2(\lambda^2 - \mu^2)$. This will be 1 if $\lambda = (1 + (\alpha\beta\gamma)^{-1}W^{-2})/2$ and $\mu = \lambda - 1$.

c → a: Suppose (c) holds and yet (a) fails. Then there is w in B with $0 \neq w$ but $ww' = 0$. Write $w = a + bz$, with a and b in $F[x, y]$. b cannot be 0, because of (c) and Proposition 2.5, which show that a cannot be a zero divisor (in $F[x, y]$). Now because of Proposition 2.5 and the fact that $b \neq 0$, we have b^{-1} exists. $b^{-1}w = b^{-1}a + z$ is then also a zero divisor. $b^{-1}a \neq 0$, since z is not a zero divisor. Write $b^{-1}a = \lambda + \mu x + \nu y + \pi xy$ and $c = \lambda - \pi xy$. If c were 0, $v = b^{-1}a + z = \mu x + \nu y + z$ is a zero divisor. However, $0 = vv'$ leads to $\alpha\mu^2 + \beta\nu^2 + \gamma 1^2 = 0$, contrary to (c). So $c \neq 0$; as in the proof of Proposition 2.5 we obtain $cc' = \delta \neq 0$. Let $d = c(b^{-1}a + z)$, which is another zero divisor. Direct computation yields $d = \delta + \varepsilon x + \rho y + \sigma z + \tau(xy)z$, where δ, ε, ρ, σ, τ are elements of F and $\delta = cc' \neq 0$. Finally, $0 = dd' = \delta^2 - \alpha\varepsilon^2 - \beta\rho^2 - \gamma\sigma^2 - (\alpha\beta\gamma)\tau^2$; so $\alpha(\tau/\delta)^2 + \beta(\rho/\delta)^2 + \gamma(\sigma/\delta)^2 + \alpha\beta\gamma(\tau/\delta)^2 = 1$, contrary to (c).

REMARKS. (1) The condition $bb' \neq 0$ for a (variable) element of a non-singular non-commutative composition algebra B leads to a condition on a quadratic form in 4 or 8 variables, according to the dimension of B. Propositions 2.5 and 2.6 reduce the number of variables and simplify the form.

(2) One might expect by analogy with the cases of dimension 2 and 4, where the forms are αX^2 and $\alpha X^2 + \beta Y^2$, that a valid test form for dimension 8 might be $\alpha X^2 + \beta Y^2 + \gamma Z^2$. However, this is not the case. Consider the algebra $A = \mathbf{Q}[x, y, z]$, formed over the rationals $\mathbf{Q}$ in the canonical fashion by adjoining elements x, y, z, each orthogonal to the algebra generated by the preceding elements and 1, with $x^2 = 2$, $y^2 = 5$, and $z^2 = 10$. Because $[(xy)z]^2 = 100$, $(10 + (xy)z)(10 - (xy)z) = 0$; so A has divisors of zero. However, we can see that $2X^2 + 5Y^2 + 10Z^2 \neq 1$ for rational X, Y and Z.

If we assume that 1 is represented by this form, we obtain

$(*)$ $2X^2 + 5Y^2 + 10Z^2 = T^2$ for integers X, Y, Z, T, with $T > 0$.

Let T_0 be the smallest $T > 0$ for which $(*)$ has a solution. For any integer S, $S^2 = 0, 1$, or -1 (mod 5) and $2S^2 = 0, 2$, or -2 (mod 5). From $(*)$ we

obtain $2X^2 = T_0^2 \pmod 5$, which by the preceding sentence means $X = T_0 = 0 \pmod 5$. Put $X = 5X_1$, and $T_0 = 5T_1$. Then $(*)$ becomes $50X_1^2 + 5Y^2 + 10Z^2 = 25T_1^2$, or $10X_1^2 + Y^2 + 2Z^2 = 5T_1^2$, which modulo 5 is $Y^2 + 2Z^2 = 0$. Thus $Y = Z = 0 \pmod 5$. Write $Y = 5Y_1$ and $Z = 5Z_1$. $(*)$ then becomes $10X_1^2 + 25Y_1^2 + 50Z_1^2 = 5T_1^2$, or $2X_1^2 + 5Y_1^2 + 10Z_1^2 = T_1^2$. This contradicts the definition of T_0; so $(*)$ has no non-zero solution after all.

References

[1] A. A. Albert, *Structure of algebras*, AMS coloquium publications, volume **24**, 1939.

[2] _____, *Quadratic forms permitting composition*, Annals of Math., **43** (1942), 161–177.

[3] K. I. Gross and R. A. Kunze, *Bessel functions and representation theory* 11; *holomorphic discrete series and metaplectic representation*, J. Funct. Anal., **25** (1977), 1–49.

[4] _____, *Finite dimensional induction and new results on invariants for classical groups I*, Amer. J. Math., **106** (1984), 893–974.

[5] H. Jacquet and R. P. Langlands, *Automorphic Forms on GL(2)*, Lecture Notes in Math. **114**, Springer-Verlag, Berlin, Heidelberg, New York, 1970.

[6] N. Jacobson, *Composition algebras and their automorphisms*, Circolo Mathematica di Palermo, **2** (1953), 959–960.

[7] _____, *Structure and Representations of Jordan algebras*, AMS colloquium publications, volume **39**, 1968.

[8] I. Kapklansky, *Infinite-dimensional quadratic forms admitting composition*, Proc. Amer. Math. Soc., **4** (1953), 956–960.

[9] R. D. Schafer, *An Introduction to Non-Associative Algebras*, Academic Press, (1966).

[10] A. Weil, *Sur certains groupes d'operateurs unitaires*, Acta Math., **111** (1964), 143–211.

[11] _____, *Sur la formule e Siegel dans la theorie des groupes classiques*, Acta Math., **113** (1965), 1–87.

Received May 22, 1979 and in revised form June 26, 1982.

UNIVERSITY OF GEORGIA
ATHENS, GA 30602

AND

UNIVERSITY OF CALIFORNIA
IRVINE, CA 92717