GENERIC SPLITTING FIELDS OF COMPOSITION ALGEBRAS

BY
J. C. FERRAR[1]

Witt [7] proved that one can assign to each generalized quaternion algebra $\mathscr{A}$ over a field K, a field $F(\mathscr{A})$ containing K which splits $\mathscr{A}$ and has the property: if $F(\mathscr{A})$ splits a quaternion algebra $\mathscr{B}$ over K then either $\mathscr{B}$ is split over K or $\mathscr{B}$ is isomorphic to $\mathscr{A}$. Amitsur [2] has generalized this result to obtain generic splitting fields for all central simple associative algebras of dimension greater than one over K (cf. Roquette [6]). In this paper we generalize the result of Witt in another direction, studying splitting fields of composition algebras of dimension greater than one over K of characteristic other than two. We assign to each such algebra $\mathscr{C}$, a field $F(\mathscr{C})$ containing K, prove that $F(\mathscr{C})$ is an invariant under isomorphisms, and prove

THEOREM 2. *Let $\mathscr{C}$ be a composition algebra of dimension greater than one over K. Then*

1. *$\mathscr{C}_{F(\mathscr{C})}$ is split.*
2. *If $F\supseteq K$ is any field, then $\mathscr{C}_F$ is split if and only if there is a K-place of $F(\mathscr{C})$ into $F\cup\infty$.*
3. *If $\mathscr{C}'$ is any composition algebra over K such that $\mathscr{C}'_{F(\mathscr{C})}$ is split, then either $\mathscr{C}'$ is split or $\mathscr{C}$ is isomorphic to a subalgebra of $\mathscr{C}'$.*

Thus we generalize the result of Witt to quadratic and generalized Cayley algebras.

I. **Composition algebras.** A composition algebra $\mathscr{C}$ over a field K is an algebra over K, with identity 1, together with a nondegenerate quadratic form N such that $N(xy)=N(x)N(y)$ for any x, y in $\mathscr{C}$. The structure of such algebras has been completely determined and we refer to [1] or [4] for proofs of the following results.

1. A composition algebra $\mathscr{C}$ is alternative with involution $\tau\colon \alpha 1+u\to\alpha 1-u$, for u orthogonal to 1 with respect to the nondegenerate, symmetric, bilinear form $N(x, y)=\frac{1}{2}\{N(x+y)-N(x)-N(y)\}$. Each $x\in\mathscr{C}$ can be uniquely represented in the form $x=\alpha 1+u$, $\alpha\in K$, $N(u, 1)=0$ and one has $N(x)1=(\alpha 1+u)(\alpha 1-u)$.

If V is a subspace of $\mathscr{C}$, we shall denote by $V^{\perp}$ the orthogonal complement of V in $\mathscr{C}$ with respect to $N(x, y)$.

2. If $\mathscr{B}$ is a composition subalgebra of $\mathscr{C}$ (necessarily having associated quadratic form the restriction of N to $\mathscr{B}$), and $u\in\mathscr{B}^{\perp}\subseteq C$, $N(u)\neq 0$, then $\mathscr{B}+\mathscr{B}u$,

Received by the editors August 28, 1966.

[1] Research partially supported by the National Science Foundation Grant GP-6368.

$\mathscr{B}u = \{bu \mid b \in \mathscr{B}\}$, is a composition subalgebra of $\mathscr{C}$ with structure determined completely by the structure of $\mathscr{B}$ and the element $N(u) \in K$. $\mathscr{B}u$ is orthogonal to $\mathscr{B}$ with respect to the nondegenerate form $N(x, y)$ and hence $\dim(\mathscr{B}+\mathscr{B}u) = 2 \dim \mathscr{B}$.

3. Every composition algebra $\mathscr{C}$ has dimension 1, 2, 4, or 8 over K and possesses composition subalgebras of dimension 2^e for all e such that $2^e \leqq \dim \mathscr{C}$.

4. If φ is an isomorphism from a composition algebra $\mathscr{C}$ with quadratic form N onto a composition algebra $\mathscr{C}'$ with quadratic form N', then $N'(x\varphi) = N(x)$ for all $x \in \mathscr{C}$.

5. A composition algebra is called split if there is $u \in \mathscr{C}$, $u \neq 0$, such that $N(u) = 0$. If $\mathscr{C}$ is split, the form $N(x, y)$ has maximal Witt index. If $\mathscr{C}$ is not split, $\mathscr{C}$ is a division algebra.

6. If $F \supseteq K$ is a field, the algebra $\mathscr{C}_F = \mathscr{C} \otimes_K F$ is again a composition algebra (over F) with associated quadratic form N_F, the natural extension of N to $\mathscr{C}_F$.

For convenience we shall denote by λx, $\lambda \in F$, $x \in \mathscr{C}$, the element $\lambda \otimes x$ of $\mathscr{C}_F$.

II. **Construction of the generic splitting field.** We assume now that $\mathscr{C}$ is an arbitrary composition algebra of dimension 2^k, $k > 0$, over K of characteristic other than two. Let u_i, $1 \leqq i \leqq m+1$, $m = 2^{k-1}$, be elements of $\mathscr{C}$ such that $N(u_i) \neq 0$ for all i, $N(u_i, u_j) = 0$ for $i \neq j$, and u_i, $1 \leqq i \leqq m$, span a composition algebra $\mathscr{B} \subseteq \mathscr{C}$. We take $L(\mathscr{C})$ to be the rational function field in $m-1$ indeterminates $x_2, \ldots, x_m$ over K, assuming as a convention that this will be K if $m = 1$, and define

$$\lambda(u) = N(u_1)^{-1} N\left(\sum_2^m u_i x_i + u_{m+1}\right) = N(u_1)^{-1}\left(\sum_2^m x_i^2 N(u_i) + N(u_{m+1})\right)$$

in $L(\mathscr{C})$.

The generic splitting field $F(\mathscr{C})$ is defined as follows: $F(\mathscr{C}) = L(\mathscr{C})$ if $\mathscr{C}$ is split; $F(\mathscr{C}) = L(\mathscr{C})((-\lambda(u))^{1/2})$ if $\mathscr{C}$ is not split.

We show now that $F(\mathscr{C})$ is dependent, up to isomorphism, only on $\mathscr{C}$, and not on the choice of the u_i, proving first

LEMMA 1. *Let $\mathscr{C}$ be a composition division algebra over K, u_i, v_i, $1 \leqq i \leqq m+1$ sets of elements of $\mathscr{C}$ satisfying the conditions above and such that u_i, $1 \leqq i \leqq m$, and v_i, $1 \leqq i \leqq m$, span the same subalgebra $\mathscr{B}$ of $\mathscr{C}$. Then $L(\mathscr{C})((-\lambda(u))^{1/2})$ is isomorphic to $L(\mathscr{C})((-\lambda(v))^{1/2})$.*

Proof. By (2), $\mathscr{C} = \mathscr{B} + \mathscr{B}u_{m+1}$ and $\mathscr{B}^{\perp} = \mathscr{B}u_{m+1}$. Thus there is $b \in \mathscr{B}$ such that $v_{m+1} = bu_{m+1}$, $N(b) \neq 0$. Since bu_i, $1 \leqq i \leqq m$ span $\mathscr{B}$,

$$\alpha v_1 + \sum_2^m x_i v_i + v_{m+1} = \sum_1^m \xi_i (bu_i) + bu_{m+1} = b\left(\sum_1^m \xi_i u_i + u_{m+1}\right)$$

for any $\alpha \in L(\mathscr{C})((-\lambda(v))^{1/2})$, where ξ_i, $1 \leqq i \leqq m$, are K-linear combinations of α and the x_i, $2 \leqq i \leqq m$, and conversely. For $\alpha = (-\lambda(v))^{1/2}$,

$$0 = N\left(\alpha v_1 + \sum_2^m x_i v_i + v_{m+1}\right) = N(b) N\left(\sum_1^m \xi_i u_i + u_{m+1}\right)$$

and, since $N(b)\neq 0$, $\xi_1^2=-N(u_1)^{-1}(\sum_2^m \xi_i^2 N(u_i)+N(u_{m+1}))$. Since the ξ_i generate $L(\mathscr{C})((-\lambda(v))^{1/2})$ over K, it follows that there is an isomorphism of $L(\mathscr{C})((-\lambda(u))^{1/2})$ onto $L(\mathscr{C})((-\lambda(v))^{1/2})$ mapping x_i onto ξ_i, $2\leqq i\leqq m$, and $(-\lambda(u))^{1/2}$ onto ξ_1.

We shall obtain our results on the independence of $F(\mathscr{C})$ from the choice of the u_i, and on the invariance of $F(\mathscr{C})$ under isomorphism of $\mathscr{C}$, as corollaries to

THEOREM 1. *Let u_i, v_i, $1\leqq i\leqq m+1$ be elements of a division composition algebra $\mathscr{C}$, satisfying the criteria given for the u_i in defining $F(\mathscr{C})$. Let u_i, $1\leqq i\leqq m$, span the subalgebra $\mathscr{B}$ and let v_i, $1\leqq i\leqq m$, span the subalgebra $\mathscr{B}'$. Then $L(\mathscr{C})((-\lambda(u))^{1/2})$ is isomorphic to $L(\mathscr{C})((-\lambda(v))^{1/2})$.*

Proof. We consider the separate cases $m=1$, 2, or 4.

Case 1. $m=1$. The only one-dimensional composition subalgebra of $\mathscr{C}$ is $K1$, hence $\mathscr{B}=\mathscr{B}'$ and the result follows from Lemma 1.

Case 2. $m=2$. If $\mathscr{B}=\mathscr{B}'$, Lemma 1 again yields the desired result. Thus we may assume $\mathscr{B}\cap\mathscr{B}'=K1$.

If 1, u are an orthogonal basis for $\mathscr{B}$, $v\in\mathscr{B}^\perp$, then 1, v also span a subalgebra, say $\mathscr{D}$, of $\mathscr{C}$. Taking $u_1=1$, $u_2=u$, $u_3=v$, $u_1'=1$, $u_2'=v$, $u_3'=u$, we see easily that since $\lambda(u)=N(u)x_1^2+N(v)$, $\lambda(u')=N(v)x_1^2+N(u)$, the mapping taking x_1 onto x_1^{-1}, $(-\lambda(u))^{1/2}$ onto $x_1^{-1}(-\lambda(u'))^{1/2}$ determines an isomorphism of $L(\mathscr{C})((-\lambda(u))^{1/2})$ onto $L(\mathscr{C})((-\lambda(u'))^{1/2})$.

Since $\mathscr{B}^\perp$, $(\mathscr{B}')^\perp$ are two-dimensional subspaces of the three dimensional space $(K1)^\perp$, there is $z\in\mathscr{B}^\perp\cap(\mathscr{B}')^\perp$, $z\neq 0$. By the above observation and Lemma 1, $L(\mathscr{C})((-\lambda(u))^{1/2})$, $L(\mathscr{C})((-\lambda(v))^{1/2})$ are isomorphic to fields $L(\mathscr{C})((-\lambda(u'))^{1/2})$, $L(\mathscr{C})((-\lambda(v'))^{1/2})$ respectively, where $u_1'=1=v_1'$, $u_2'=z=v_2'$. By Lemma 1 the latter fields are isomorphic and the result follows.

Case 3. $m=4$. Again, if $\mathscr{B}=\mathscr{B}'$ we are finished. To complete the proof we shall show the result follows in the event $\dim(\mathscr{B}\cap\mathscr{B}')=2$, and shall give a method of reducing the case $\mathscr{B}\cap\mathscr{B}'=K1$ to the case $\dim(\mathscr{B}\cap\mathscr{B}')=2$.

We show first that if $\mathscr{D}$ is a composition subalgebra of $\mathscr{B}$ of dimension 2 with orthogonal basis 1, a_1, $a_2\in\mathscr{B}\cap\mathscr{D}^\perp$, $a_3\in\mathscr{B}^\perp$, and we take $u_1=1$, $u_2=a_1$, $u_3=a_2$, $u_4=a_1a_2$, $u_5=a_3$, $u_1'=1$, $u_2'=a_1$, $u_3'=a_3$, $u_4'=a_1a_3$, $u_5'=a_2$ (such sets are easily seen to satisfy the necessary criteria for use in defining $F(\mathscr{C})$, then $L(\mathscr{C})((-\lambda(u))^{1/2})$ is isomorphic to $L(\mathscr{C})((-\lambda(u'))^{1/2})$. For $\alpha\in L(\mathscr{C})((-\lambda(u))^{1/2})$,

$$\alpha 1+x_1a_1+x_2a_2+x_3a_1a_2+a_3 = (\alpha 1+x_1a_1+a_3)+(x_21+x_3a_1)a_2$$

and since, for $\alpha=(-\lambda(u))^{1/2}$, $N(\alpha 1+x_1a_1+x_2a_2+x_3a_1a_2+a_3)=0$, we have $N((x_21+x_3a_1)^{-1}(\alpha 1+x_1a_1+a_3)+a_2)=0$. Since $(x_21+x_3a_1)^{-1}=(x_2^2+x_3^2N(a_1))^{-1}\times(x_21-x_3a_1)$ by (1) we have, carrying out the multiplication term by term, and converting,

$$N\left(\sum_1^4 \xi_i u_i'+u_5'\right) = \sum_1^4 \xi_i^2 N(u_i')+N(u_5') = 0,$$

where

$$\xi_1 = (x_2^2+x_3^2N(a_1))^{-1}(\alpha x_2+x_1x_3N(a_1))$$

$$\xi_2 = (x_2^2+x_3^2N(a_1))^{-1}(x_1x_2-\alpha x_3)$$

$$\xi_3 = (x_2^2+x_3^2N(a_1))^{-1}x_2$$

$$\xi_4 = -(x_2^2+x_3^2N(a_1))^{-1}x_3.$$

In $K(\xi_1, \xi_2, \xi_3, \xi_4) \subseteq L(\mathscr{C})((-\lambda(u))^{1/2})$ are the elements

$$\xi_3^2+\xi_4^2N(a_1) = (x_2^2+x_3^2N(a_1))^{-1},$$

and hence x_2, x_3; $x_2(\alpha x_2+x_1x_3N(a_1))-x_3N(a_1)(x_1x_2-\alpha x_3)=\alpha(x_2^2+x_3^2N(a_1))$, hence α; and finally x_1. Thus $K(\xi_1, \xi_2, \xi_3, \xi_4)=L(\mathscr{C})((-\lambda(u))^{1/2})$ when $\alpha=(-\lambda(u))^{1/2}$, and the mapping taking x_i onto ξ_i, $2 \leqq i \leqq 4$, and $(-\lambda(u'))^{1/2}$ onto ξ_1 determines an isomorphism of $L(\mathscr{C})((-\lambda(u'))^{1/2})$ onto $L(\mathscr{C})((-\lambda(u))^{1/2})$ since

$$\xi_1^2 = -N(u_1')^{-1}\left(\sum_2^4 \xi_i^2N(u_i')+N(u_5')\right).$$

Now if $\mathscr{B} \cap \mathscr{B}' = \mathscr{D}$ is two-dimensional, and $z \in \mathscr{B}^\perp \cap (\mathscr{B}')^\perp$, the latter intersection being nontrivial from dimensionality arguments as in Case 2, we may use the above result and Lemma 1 to show $L(\mathscr{C})((-\lambda(u))^{1/2})$, $L(\mathscr{C})((-\lambda(v))^{1/2})$ are isomorphic respectively to fields $L(\mathscr{C})((-\lambda(u'))^{1/2})$, $L(\mathscr{C})((-\lambda(v'))^{1/2})$ where u_i', $1 \leqq i \leqq 4$, and v_i', $1 \leqq i \leqq 4$, span the same subalgebra $\mathscr{D}+\mathscr{D}z$. Lemma 1 then completes the argument.

If $\mathscr{B} \cap \mathscr{B}' = K1$, we have again a nontrivial $z \in \mathscr{B}^\perp \cap (\mathscr{B}')^\perp$ and we take subalgebras $\mathscr{D}, \mathscr{D}'$ of dimension 2 in $\mathscr{B}, \mathscr{B}'$ respectively. Again it follows that $L(\mathscr{C})((-\lambda(u))^{1/2})$ is isomorphic to $L(\mathscr{C})((-\lambda(u'))^{1/2})$ where u_i', $1 \leqq i \leqq 4$, span $\mathscr{D}+\mathscr{D}z$, and that $L(\mathscr{C})((-\lambda(v))^{1/2})$ is isomorphic to $L(\mathscr{C})((-\lambda(v'))^{1/2})$, where v_i', $1 \leqq i \leqq 4$, span $\mathscr{D}'+\mathscr{D}'z$. Since $(\mathscr{D}+\mathscr{D}z) \cap (\mathscr{D}'+\mathscr{D}'z)$ is the algebra spanned by 1 and z, we have reduced the argument to the case $\mathscr{B} \cap \mathscr{B}'$ two-dimensional and are finished.

COROLLARY 1. *The field $F(\mathscr{C})$ is independent of the choice of the $u_i \in \mathscr{C}$ used in defining it.*

Proof. If $\mathscr{C}$ is split, $F(\mathscr{C})$ depends only on the dimension of $\mathscr{C}$ for its definition. If $\mathscr{C}$ is not split, Theorem 1 shows the independence from u_i.

COROLLARY 2. *If $\mathscr{C}$ is isomorphic to $\mathscr{C}'$ then $F(\mathscr{C})$ is isomorphic to $F(\mathscr{C}')$.*

Proof. If φ is an isomorphism of $\mathscr{C}$ onto $\mathscr{C}'$, $N'(x\varphi)=N(x)$ for all $x \in \mathscr{C}$ by (4). If u_i, $1 \leqq i \leqq m+1$, are chosen as above to define $F(\mathscr{C})$ and u_i, $1 \leqq i \leqq m$, span $\mathscr{B} \subseteq \mathscr{C}$, the elements $u_i\varphi$ in $\mathscr{C}'$ are orthogonal, have $N'(u_i\varphi) \neq 0$ and $u_i\varphi$, $1 \leqq i \leqq 4$, span the composition subalgebra $\mathscr{B}\varphi\subseteq\mathscr{C}'$. Thus $u_i\varphi$, $1\leqq i\leqq m+1$ may be used to define $F(\mathscr{C}')$. Now $L(\mathscr{C})$ is clearly isomorphic to $L(\mathscr{C}')$ and

$$\begin{aligned}\lambda(u) &= N(u_1)^{-1}\left(\sum_2^m N(u_i)x_i^2+N(u_{m+1})\right)\\ &= N'(u_1\varphi)^{-1}\left(\sum_2^m N'(u_i\varphi)x_i^2+N'(u_{m+1}\varphi)\right) = \lambda(u\varphi)\end{aligned}$$

so $F(\mathscr{C})=L(\mathscr{C})((-\lambda(u))^{1/2})$ is isomorphic to $L(\mathscr{C}')((-\lambda(u\varphi))^{1/2})=F(\mathscr{C}')$.

III. **Properties of** $F(\mathscr{C})$. In this section we prove a sequence of lemmas leading to the proof of our main theorem. We first prove

LEMMA 2. *Let $K(x_1,\dots,x_n)$ be the rational function field in n indeterminates $x_1,\dots,x_n$, F a field extension of K, $\alpha_1,\dots,\alpha_n\in F$. Then there is a K-place of $K(x_1,\dots,x_n)$ into $F\cup\infty$ mapping x_i onto α_i, $1\leqq i\leqq n$.*

Proof. By induction on n. The result is well known if $n=1$ and the place can, in fact, be defined explicitly. If $n>1$, we use the induction hypothesis, with K replaced by $K(x_1)$ to claim there is a $K(x_1)$-place ψ of $K(x_1)(x_2,\dots,x_n)$ into $K(x_1)(\alpha_2,\dots,\alpha_n)$ such that x_i maps to α_i, $i>1$. Now by the validity of the result for one indeterminate, there is a place φ of $K(x_1)(\alpha_2,\dots,\alpha_n)=K(\alpha_2,\dots,\alpha_n)(x_1)$ into $F\cup\infty$ fixing the elements of $K(\alpha_2,\dots,\alpha_n)\subseteq F$ and mapping x_1 onto α_1. $\psi\varphi$ is then a K-place of $K(x_1,\dots,x_n)$ into $F\cup\infty$ with the desired property.

COROLLARY. *Let $\lambda\in K(x_1,\dots,x_n)$ such that $K(x_1,\dots,x_n)(\lambda^{1/2})$ is a quadratic extension of $K(x_1,\dots,x_n)$, $\alpha_1,\dots,\alpha_n\in F$, F a field extension of K. Then there is a K-place φ of $K(x_1,\dots,x_n)$ into $F\cup\infty$ mapping x_i onto α_i for all $1\leqq i\leqq n$ and, if $\lambda\varphi$ is a square in F, φ can be extended to a K-place of $K(x_1,\dots,x_n)(\lambda^{1/2})$ into $F\cup\infty$ mapping λ onto a square root of $\lambda\varphi$ in F.*

Proof. That φ exists follows from Lemma 2. It is known (e.g., [3]), that a place from $K(x_1,\dots,x_n)$ into $F\cup\infty$ can be extended to a place φ' of $K(x_1,\dots,x_n)(\lambda^{1/2})$ into $F'\cup\infty$, F' the algebraic closure of F. Since, however, $(\lambda^{1/2})\varphi'$ must be a square root of $\lambda\varphi$ in F', and since the square roots of $\lambda\varphi$ in F' are in fact, in F, $(\lambda^{1/2})\varphi'\in F$ and φ' maps $K(x_1,\dots,x_n)(\lambda^{1/2})$ into $F\cup\infty$.

If $\mathscr{C}$ is a composition algebra over K, F a field extension of K, we say F splits $\mathscr{C}$ (F is a splitting field of $\mathscr{C}$) if $\mathscr{C}_F$ is split.

LEMMA 3. *$L=K(x_1,\dots,x_n)$, the field of rational functions in n indeterminates, $n\geqq 0$, splits $\mathscr{C}$ if and only if $\mathscr{C}$ is split over K.*

Proof. We show that, if $K(x_1,\dots,x_n)$ splits $\mathscr{C}$, $n\geqq 1$, then $K(x_1,\dots,x_{n-1})$ also splits $\mathscr{C}$ and hence, by induction, K splits $\mathscr{C}$ so $\mathscr{C}$ is split.

Let $u_1,\dots,u_e$ be an orthogonal basis for $\mathscr{C}$ with respect to $N(x,y)$. This is also an orthogonal basis for $\mathscr{C}_L$ over L and, if $\mathscr{C}_L$ is split, there are $\xi_i\in L$, $1\leqq i\leqq e$, such that $N(\sum_1^e \xi_i u_i)=0$. Clearing the denominators of the ξ_i we have, since $N(\alpha x) =\alpha^2 N(x)$ for $\alpha \in L$, polynomials p_i in $K[x_1, \ldots, x_n]$, not all $p_i\equiv 0$, such that $N(\sum_1^e p_i u_i)=\sum_1^e p_i^2 N(u_i)=0$. We assume, without loss of generality, that x_n occurs in some p_i and we let k be the maximum of the degrees of the polynomials p_i, considered as polynomials in x_n over $K(x_1, \ldots, x_{n-1})$. We can write each $p_i=x_n^k q_i+r_i$ where $q_i \in K[x_1, \ldots, x_{n-1}]$, $r_i \in K[x_1, \ldots, x_n]$, r_i of degree less than k in x_n. Then $\sum_1^e (x_n^k q_i+r_i)^2 N(u_i)=0$ and, since the x_i are algebraically independent, we must have $(\sum_1^e q_i^2 N(u_i))x_n^{2k}=0$, hence $\sum_1^e q_i^2 N(u_i)=0$ in $K(x_1, \ldots, x_{n-1})$. Thus $K(x_1, \ldots, x_{n-1})$ splits $\mathscr{C}$. Induction completes the proof that $\mathscr{C}$ is split over K.

Conversely, if $\mathscr{C}$ is split over K and F is any field containing K, there is $u \in \mathscr{C}$, $u\neq 0$ such that $N(u)=0$. But $u \in \mathscr{C}$ implies $u \in \mathscr{C}_F$ so, since $N_F(u)=N(u)=0$, $\mathscr{C}_F$ is split. In particular $\mathscr{C}_L$ is split.

Lemma 4. *Let $\mathscr{C}$ be a composition algebra over K, F, F' field extensions of K, φ a K-place of F into $F' \cup \infty$. If C_F is split, so is $\mathscr{C}_{F'}$.*

Proof. We show first that if $\lambda_1, \ldots, \lambda_n$ are elements of F, not all zero, there is some j such that $(\lambda_j^{-1}\lambda_i)\varphi \in F'$, $i=1, \ldots, n$. Let j be such that $\lambda_j\neq 0$ and such that the number t of i for which $(\lambda_j^{-1}\lambda_i)\varphi=\infty$ is minimal. If $t=0$ we are done. If not, we may assume, without loss of generality, that $(\lambda_j^{-1}\lambda_i)\varphi=\infty$, $1\leqq i\leqq t$, $(\lambda_j^{-1}\lambda_i)\varphi \in F'$, $t<i\leqq n$. $\lambda_t\neq 0$ since otherwise $(\lambda_j^{-1}\lambda_t)\varphi=0\varphi=0\neq\infty$. Thus $(\lambda_t^{-1}\lambda_i)\varphi=((\lambda_j^{-1}\lambda_t)^{-1} \times(\lambda_j^{-1}\lambda_i))\varphi=0$ for $t<i\leqq n$, and $(\lambda_t^{-1}\lambda_t)\varphi=1\varphi=1 \in F'$ and hence for λ_t there are at most $(t-1)$ i such that $(\lambda_t^{-1}\lambda_i)\varphi=\infty$, a contradiction to the minimality of t. Thus $t=0$.

Now if $\mathscr{C}_F$ is split, and u_i, $i=1, \ldots, n$, are an orthogonal basis of $\mathscr{C}$ over K, hence of $\mathscr{C}_F$ over F and of $\mathscr{C}_{F'}$ over F', there are $\lambda_i \in F$ such that not all λ_i are zero and $N_F(\sum_1^n \lambda_i u_i)=\sum_1^n \lambda_i^2 N(u_i)=0$. For λ_j such that $(\lambda_j^{-1}\lambda_i)\varphi \in F'$ for all i,

$$\sum_1^n (\lambda_j^{-1}\lambda_i)^2 N(u_i) = 0$$

and hence, $\sum_1^n (\lambda_j^{-1}\lambda_i)^2\varphi N(u_i)=0$. Since $(\lambda_j^{-1}\lambda_i)^2\varphi=((\lambda_j^{-1}\lambda_i)\varphi)^2$, it follows that $N_{F'}(\sum_1^n (\lambda_j^{-1}\lambda_i)\varphi u_i)=0$ and, since $(\lambda_j^{-1}\lambda_j)\varphi=1\neq 0$, $\mathscr{C}_{F'}$ is split.

Lemma 5. *Let $\mathscr{C}$ be a division composition algebra over K, $\lambda \in K$, and suppose $L=K(\lambda^{1/2})$ is a quadratic extension of K. Then $\mathscr{C}_L$ is split if and only if there is $u \in (K1)^\perp \subseteq \mathscr{C}$ such that $N(u)=-\lambda$.*

Proof. If there is $u \in (K1)^\perp$ with $N(u)=-\lambda$, then $x=(\lambda^{1/2})1+u \in \mathscr{C}_L$ clearly has $N_L(x)=0$, so $\mathscr{C}_L$ is split. Conversely, if $\mathscr{C}_L$ is split, then there is $x=a+(\lambda^{1/2})b$, $a, b \in \mathscr{C}$, such that $x\neq 0$, $N_L(x)=0$. But $N_L(x)=N(a)+\lambda N(b)+2N(a, b)(\lambda^{1/2})$ and thus $N(a, b)=0$, $N(ab^{-1})=N(a)N(b)^{-1}=-\lambda$. Since $N(ab^{-1}, 1)=N(a, b)N(b^{-1})=0$, $u=ab^{-1}$ satisfies the criteria.

Finally we give a slight generalization of a result of Jacobson [4], first defining subspaces V, V' of composition algebras $\mathscr{C}$, $\mathscr{C}'$ respectively, to be equivalent if there is a nonsingular linear transformation φ of V onto V' such that $N'(x\varphi)=N(x)$ for all $x \in V$, N, N' denoting the respective quadratic forms of $\mathscr{C}$ and $\mathscr{C}'$.

LEMMA 6. *If a composition algebra $\mathscr{C}$ is equivalent to a subspace of a composition algebra $\mathscr{C}'$, then $\mathscr{C}$ is isomorphic to a subalgebra of $\mathscr{C}'$.*

Proof. The proof is essentially that of Jacobson [4]. Let φ be the mapping of $\mathscr{C}$ into $\mathscr{C}'$ such that $N'(x\varphi)=N(x)$ for all $x \in \mathscr{C}$ and suppose that $\mathscr{B}$, $\mathscr{B}'$ are isomorphic composition subalgebras of $\mathscr{C}$, $\mathscr{C}'$ respectively. By (4), $\mathscr{B}$ and $\mathscr{B}'$ are equivalent and, since $\mathscr{B}$ and $\mathscr{B}\varphi$ are clearly equivalent, $\mathscr{B}'$ and $\mathscr{B}\varphi$ are equivalent subspaces of $\mathscr{C}'$. By Witt's Theorem for bilinear forms, $(\mathscr{B}')^\perp$ and $(\mathscr{B}\varphi)^\perp$ are equivalent in $\mathscr{C}'$. Thus, if there is $u \in \mathscr{B}^\perp$ with $N(u)\neq 0$, which is the case unless $\mathscr{B}=\mathscr{C}$, then there is $u' \in (\mathscr{B}')^\perp$ such that $N'(u')=N'(u\varphi)=N(u)$. Then the algebras $\mathscr{B}+\mathscr{B}u$, $\mathscr{B}'+\mathscr{B}'u'$ are composition subalgebras of $\mathscr{C}$, $\mathscr{C}'$ respectively which are isomorphic by (2). Beginning with $\mathscr{B}=K1$, $\mathscr{B}'=K1'$ one can, in successive steps, thus construct an isomorphism of $\mathscr{C}$ into $\mathscr{C}'$.

Since in this proof, whenever $2 \dim \mathscr{B}=\dim \mathscr{C}$, we need only produce elements u, u' in $\mathscr{B}^\perp$, $(\mathscr{B}')^\perp$ respectively with $N(u)=N'(u')\neq 0$, we can clearly weaken the hypotheses to obtain the

COROLLARY. *Let $\mathscr{C}$ be a $2n$-dimensional composition algebra, V a nonisotropic ($N(x, y)$ nondegenerate when restricted to V) subspace of $\mathscr{C}$ of dimension $n+1$ which contains an n-dimensional composition subalgebra $\mathscr{B}$ of $\mathscr{C}$. Then if V is equivalent to a subspace of a composition algebra $\mathscr{C}'$, $\mathscr{C}$ is isomorphic to a subalgebra of $\mathscr{C}'$.*

We are now prepared to restate and prove

THEOREM 2. *Let $\mathscr{C}$ be a composition algebra of dimension greater than one over K. Then*

1. *$\mathscr{C}_{F(\mathscr{C})}$ is split.*
2. *If $F \supseteq K$ is any field, then $\mathscr{C}_F$ is split if and only if there is a K-place of $F(\mathscr{C})$ into $F \cup \infty$.*
3. *If $\mathscr{C}'$ is any composition algebra over K such that $\mathscr{C}'_{F(\mathscr{C})}$ is split, then either $\mathscr{C}'$ is split over K or $\mathscr{C}$ is isomorphic to a subalgebra of $\mathscr{C}'$.*

Proof. As in the definition of $F(\mathscr{C})$ in §II, we pick a set u_i, $1 \leqq i \leqq m+1$, $m=2^{k-1}$, where $2^k=\dim \mathscr{C}$, and denote by $\mathscr{B}$ the composition subalgebra of $\mathscr{C}$ spanned by u_i, $1 \leqq i \leqq m$. We may assume, by Lemma 1, that $u_1=1$ and hence

$$\lambda(u) = N\left(\sum_2^m x_i u_i + u_{m+1}\right).$$

Proof of 1. If $\mathscr{C}$ is split, Lemma 3 yields the result since $F(\mathscr{C})=L(\mathscr{C})$ is a rational function field in $m-1$ indeterminates over K. If $\mathscr{C}$ is not split, neither is $\mathscr{C}_{L(\mathscr{C})}$ by Lemma 3, and since $\lambda(u)$ is by definition $N(\sum_2^m x_i u_i+u_{m+1})$, where $\sum_2^m x_i u_i+u_{m+1} \in (L(\mathscr{C})1)^\perp$, Lemma 5 yields the result.

Proof of 2. If there is a K place from $F(\mathcal{C})$ to $F \cup \infty$, $\mathcal{C}_F$ is split, by Lemma 4 and Part 1 of this theorem.

If $\mathcal{C}$ is split, $\mathcal{C}_F$ is split for any $F \supseteq K$. By Lemma 2, there is a K-place of $F(\mathcal{C}) = K(x_2, \ldots, x_m)$ into $F \cup \infty$ for any $F \supseteq K$ as desired.

Suppose $\mathcal{C}$ is not split, $\mathcal{C}_F$ is split. By (5), $\mathcal{C}_F$ contains a totally isotropic subspace W of dimension m over F. By a dimensionality argument W intersects $Fu_1 + \cdots + Fu_{m+1}$ so there is $u = \beta u_1 + \sum_2^{m+1} \beta_i u_i$ in $\mathcal{C}_F$, $u \neq 0$, with $N_F(u) = 0$. Thus

$$\beta^2 = -\sum_2^{m+1} \beta_i^2 N(u_i)$$

and, if $\beta_{m+1} \neq 0$,

$$(\beta\beta_{m+1}^{-1})^2 = -\sum_2^m (\beta_i\beta_{m+1}^{-1})^2 N(u_i) - N(u_{m+1}).$$

By Lemma 2, corollary, there is a K-place φ of $F(\mathcal{C}) = K(x_2, \ldots, x_m)((-\lambda(u))^{1/2})$ into $F \cup \infty$ mapping x_i to $\beta_i\beta_{m+1}^{-1}$, $(-\lambda(u))^{1/2}$ to $\pm\beta\beta_{m+1}^{-1}$.

If $\beta_{m+1} = 0$, some β_i, $i \neq m+1$ must be nonzero, since $0 = \beta^2 + \sum_2^m \beta_i^2 N(u_i)$ and not all of β, β_i are zero. We assume, without loss of generality, that $\beta_m \neq 0$. Then $(\beta\beta_m^{-1})^2 = \sum_2^m (\beta_i\beta_m^{-1})^2 N(u_i)$. Again by the corollary to Lemma 2, there is a K-place of $F(\mathcal{C}) = K(x_2, \ldots, x_m)((-\lambda(u))^{1/2}) = K(x_2x_m^{-1}, \ldots, x_{m-1}x_m^{-1}, x_m^{-1})(x_m^{-1}(-\lambda(u))^{1/2})$ into $F \cup \infty$ mapping $x_ix_m^{-1}$ to $\beta_i\beta_m^{-1}$, $2 \leqq i < m$, x_m^{-1} to zero, and $(x_m^{-1}(-\lambda(u))^{1/2})$ to $\pm\beta\beta_m^{-1}$, since $x_ix_m^{-1}$, $2 \leqq i < m$, x_m^{-1} are algebraically independent over K.

Proof of 3. If $\mathcal{C}$ is split, $F(\mathcal{C})$ is a rational function field over K and hence, if $\mathcal{C}'_{F(\mathcal{C})}$ is split, $\mathcal{C}'$ is split over K by Lemma 3.

If $\mathcal{C}$, $\mathcal{C}'$ are not split over K and $\mathcal{C}'_{F(\mathcal{C})}$ is split, then since $\mathcal{C}_{L(\mathcal{C})}$ is not split and $F(\mathcal{C})$ is a quadratic extension of $L(\mathcal{C})$, Lemma 5 implies there is $u' \in (1')^{\perp} \subseteq \mathcal{C}'_{L(\mathcal{C})}$ such that $N'_{L(\mathcal{C})}(u') = \lambda(u)$. Thus in $\mathcal{C}'_{L(\mathcal{C})(x_1)}$,

$$N'_{L(\mathcal{C})(x_1)}(x_1 1 + u') = x_i^2 + \sum_2^m x_i^2 N(u_i) + N(u_{m+1}).$$

It follows easily from a result of Pfister ([5], Satz 3) that the subspace $Ku_1 + \cdots + Ku_{m+1}$ is equivalent to a subspace of $\mathcal{C}'$. By the Corollary to Lemma 6, $\mathcal{C}$ is isomorphic to a subalgebra of $\mathcal{C}'$.

We note finally that, in the event dim $\mathcal{C} = 4$, i.e., when $\mathcal{C}$ is a generalized quaternion algebra over K, a judicious choice of the elements u_i in the definition of $F(\mathcal{C})$ will give rise to the same splitting field obtained by Witt [7].

Bibliography

1. A. A. Albert, *Quadratic forms permitting composition*, Ann. of Math. **43** (1942), 161–177.

2. S. A. Amitsur, *Generic splitting fields of central simple algebras*, Ann. of Math. **62** (1955), 8–43.

3. M. Deuring, *Lectures on the theory of algebraic functions of one variable*, Tata Inst. of Fund. Res., Bombay, 1959.

4. N. Jacobson, *Composition algebras and their automorphisms,* Rend. Circ. Mat. Palermo (2) 7 (1958), 55–80.

5. A. Pfister, *Multiplikative quadratische formen,* Arch. Math. **16** (1965), 363–371.

6. P. Roquette, *On the Galois cohomology of the projective linear group and its applications to the construction of generic splitting fields of algebras,* Math. Ann. **150** (1963), 411–439.

7. E. Witt, *Über ein Gegenbeispiel zum Normensatz,* Math. Z. **39** (1934–1935), 462–567.

THE OHIO STATE UNIVERSITY,
COLUMBUS, OHIO