GENERIC SPLITTING FIELDS OF COMPOSITION ALGEBRAS

BY

J. C. FERRAR

Witt [7] proved that one can assign to each generalized quaternion algebra $\mathcal{A}$ over a field $K$, a field $F(\mathcal{A})$ containing $K$ which splits $\mathcal{A}$ and has the property: if $F(\mathcal{A})$ splits a quaternion algebra $\mathcal{B}$ over $K$ then either $\mathcal{B}$ is split over $K$ or $\mathcal{B}$ is isomorphic to $\mathcal{A}$. 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 $\mathcal{C}$, a field $F(\mathcal{C})$ containing $K$, prove that $F(\mathcal{C})$ is an invariant under isomorphisms, and prove

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

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

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

1. **Composition algebras.** A composition algebra $\mathcal{C}$ 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 $\mathcal{C}$. 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 $\mathcal{C}$ is alternative with involution $\tau: x = a1 + u$, 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 $x \in \mathcal{C}$ can be uniquely represented in the form $x = a1 + u$, $\alpha \in K$, $N(u, 1) = 0$ and one has $N(x)1 = (\alpha 1 + u)(\alpha 1 - u)$.

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

2. If $\mathcal{B}$ is a composition subalgebra of $\mathcal{C}$ (necessarily having associated quadratic form the restriction of $N$ to $\mathcal{B}$), and $u \in \mathcal{B}^\perp \subseteq C$, $N(u) \neq 0$, then $\mathcal{B} + Bu$,
\( \mathcal{B}u = \{ bu \mid b \in \mathcal{B} \} \), is a composition subalgebra of \( \mathcal{C} \) with structure determined completely by the structure of \( \mathcal{B} \) and the element \( N(u) \in K \). \( \mathcal{B}u \) is orthogonal to \( \mathcal{B} \) with respect to the nondegenerate form \( N(x, y) \) and hence \( \dim (\mathcal{B} + \mathcal{B}u) = 2 \dim \mathcal{B} \).

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

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

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

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

For convenience we shall denote by \( \lambda x \), \( \lambda \in F \), \( x \in \mathcal{C} \), the element \( \lambda \otimes x \) of \( \mathcal{C}_F \).

II. Construction of the generic splitting field. We assume now that \( \mathcal{C} \) is an arbitrary composition algebra of dimension \( 2^k \), \( k > 0 \), over \( K \) of characteristic other than two. Let \( u_i \), \( 1 \leq i \leq m+1 \), \( m = 2^k - 1 \), be elements of \( \mathcal{C} \) such that \( N(u_i) \neq 0 \) for all \( i \), \( N(u_i, u_j) = 0 \) for \( i \neq j \), and \( u_i \), \( 1 \leq i \leq m \), span a composition algebra \( \mathcal{B} \subseteq \mathcal{C} \). We take \( L(\mathcal{C}) \) 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

\[
\lambda(u) = N(u_1)^{-1}N\left(\sum_{i=2}^{m} u_i x_i + u_{m+1}\right) = N(u_1)^{-1}\left(\sum_{i=2}^{m} x_i^2 N(u_i) + N(u_{m+1})\right)
\]

in \( L(\mathcal{C}) \).

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

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

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

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

\[
\alpha v_1 + \sum_{i=2}^{m} x_i v_i + v_{m+1} = \sum_{i=1}^{m} \xi_i (bu_i) + bu_{m+1} = b\left(\sum_{i=1}^{m} \xi_i u_i + u_{m+1}\right)
\]

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

\[
0 = N\left(\alpha v_1 + \sum_{i=2}^{m} x_i v_i + v_{m+1}\right) = N(b)N\left(\sum_{i=1}^{m} \xi_i u_i + u_{m+1}\right)
\]
and, since $N(b) \neq 0$, \( \xi_i^2 = -N(u_i)^{-1}(\sum \xi_j^2N(u_i_i) + N(u_{m+1})) \). Since the \( \xi_i \) generate \( L(\mathcal{C})((-\lambda(v))^{1/2}) \) over \( K \), it follows that there is an isomorphism of \( L(\mathcal{C})((-\lambda(v))^{1/2}) \) onto \( L(\mathcal{C})((-\lambda(v))^{1/2}) \) mapping \( x_i \) onto \( \xi_i \), \( 2 \leq i \leq m \), and \( (-\lambda(u))^{1/2} \) onto \( \xi_1 \).

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

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

**Proof.** We consider the separate cases \( m=1, 2, \) or \( 4 \).

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

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

If \( 1, u \) are an orthogonal basis for \( \mathcal{B}, v \in \mathcal{B}^1 \), then \( 1, v \) also span a subalgebra, say \( \mathcal{D} \), of \( \mathcal{C} \). 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 \( L(\mathcal{C})((-\lambda(u))^{1/2}) \) onto \( L(\mathcal{C})((-\lambda(u'))^{1/2}) \).

Since \( \mathcal{B}^2, (\mathcal{B}')^2 \) are two-dimensional subspaces of the three dimensional space \( (K1)^4 \), there is \( z \in \mathcal{B}^2 \cap (\mathcal{B}')^2, z \neq 0 \). By the above observation and Lemma 1, \( L(\mathcal{C})((-\lambda(u))^{1/2}) \), \( L(\mathcal{C})((-\lambda(u'))^{1/2}) \) are isomorphic to fields \( L(\mathcal{C})((-\lambda(u'))^{1/2}) \), \( L(\mathcal{C})((-\lambda(u'))^{1/2}) \) 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 \( \mathcal{B} = \mathcal{B}' \) we are finished. To complete the proof we shall show the result follows in the event \( \dim (\mathcal{B} \cap \mathcal{B}') = 2 \), and shall give a method of reducing the case \( \mathcal{B} \cap \mathcal{B}' = K1 \) to the case \( \dim (\mathcal{B} \cap \mathcal{B}') = 2 \).

We show first that if \( \mathcal{D} \) is a composition subalgebra of \( \mathcal{B} \) of dimension 2 with orthogonal basis \( 1, a_1, a_2 \in \mathcal{B} \cap \mathcal{D}^1, a_3 \in \mathcal{B}^1 \), and we take \( u_1 = 1, u_2 = a_1, u_3 = a_2, u_4 = a_1a_2, u_5 = a_3, u'_1 = 1, u'_2 = a_1, u'_3 = a_3, u'_4 = a_1a_2, u'_5 = a_2 \) (such sets are easily seen to satisfy the necessary criteria for use in defining \( F(\mathcal{C}) \)), then \( L(\mathcal{C})((-\lambda(u))^{1/2}) \) is isomorphic to \( L(\mathcal{C})((-\lambda(u'))^{1/2}) \). For \( \alpha \in L(\mathcal{C})((-\lambda(u))^{1/2}) \),

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

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,

\[
N \left( \sum_{i=1}^{4} \xi_i u'_i + u'_5 \right) = \sum_{i=1}^{4} \xi_i^2 N(u'_i) + N(u'_5) = 0
\]
where

\[ \xi_1 = (x^2_1 + x^2_3 N(a_1))^{-1}(\alpha x_2 + x_1 x_3 N(a_1)) \]
\[ \xi_2 = (x^2_1 + x^2_3 N(a_1))^{-1}(x_1 x_2 - \alpha x_3) \]
\[ \xi_3 = (x^2_1 + x^2_3 N(a_1))^{-1} x_2 \]
\[ \xi_4 = -(x^2_1 + x^2_3 N(a_1))^{-1} x_3. \]

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

\[ \xi^2_3 + \xi^2_4 N(a_1) = (x^2_1 + x^2_3 N(a_1))^{-1}, \]

and hence \( x_2, x_3; x_2(\alpha x_2 + x_1 x_3 N(a_1)) - x_3 N(a_1)(x_1 x_2 - \alpha x_3) = \alpha(x^2_1 + x^2_3 N(a_1)) \), hence \( \alpha \); and finally \( x_1 \). Thus \( K(\xi_1, \xi_2, \xi_3, \xi_4) = L(\mathcal{C})((-\lambda(u))^{1/2}) \) when \( \alpha = (-\lambda(u))^{1/2} \), and the mapping taking \( x_i \) onto \( \xi_i, 2 \leq i \leq 4 \), and \( (-\lambda(u'))^{1/2} \) onto \( \xi_1 \) determines an isomorphism of \( L(\mathcal{C})((-\lambda(u'))^{1/2}) \) onto \( L(\mathcal{C})((-\lambda(u))^{1/2}) \) since

\[ \xi_1^2 = -N(u_i)^{-1} \left( \sum_{2}^{4} \xi^2 N(u_i) + N(u_2) \right). \]

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

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

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

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

**Corollary 2.** If \( \mathcal{C} \) is isomorphic to \( \mathcal{C}' \) then \( F(\mathcal{C}) \) is isomorphic to \( F(\mathcal{C}') \).

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

\[
\lambda(u) = N(u_1)^{-1} \left( \sum_{i=2}^{m} N(u_i)x_i^2 + N(u_{m+1}) \right)
\]

\[
= N'(u_2 \varphi)^{-1} \left( \sum_{i=2}^{m} N'(u_i \varphi)x_i^2 + N'(u_{m+1} \varphi) \right) = \lambda(u \varphi)
\]

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

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

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

**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 \( \varphi \) of \( K(x_1)(x_2, \ldots, x_n) \) into \( K(x_1)(\alpha_2, \ldots, \alpha_n) \) such that \( x_i \) maps to \( \alpha_i \), \( i > 1 \). Now by the validity of the result for one indeterminate, there is a place \( \varphi \) of \( K(x_1)(\alpha_2, \ldots, \alpha_n) = K(\alpha_2, \ldots, \alpha_n)(x_1) \) into \( F \cup \infty \) fixing the elements of \( K(\alpha_2, \ldots, \alpha_n) \subseteq F \) and mapping \( x_1 \) onto \( \alpha_1 \). \( \varphi \varphi \) is then a \( K \)-place of \( K(x_1, \ldots, x_n) \) into \( F \cup \infty \) with the desired property.

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

**Proof.** That \( \varphi \) exists follows from Lemma 2. It is known (e.g., [3]), that a place from \( K(x_1, \ldots, x_n) \) into \( F \cup \infty \) can be extended to a place \( \varphi' \) of \( K(x_1, \ldots, x_n)(\lambda^{1/2}) \) 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 \( \varphi' \) maps \( K(x_1, \ldots, x_n)(\lambda^{1/2}) \) into \( F \cup \infty \).

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

**Lemma 3.** \( L = K(x_1, \ldots, x_n) \), the field of rational functions in \( n \) indeterminates, \( n \geq 0 \), splits \( \mathcal{C} \) if and only if \( \mathcal{C} \) is split over \( K \).

**Proof.** We show that, if \( K(x_1, \ldots, x_n) \) splits \( \mathcal{C} \), \( n \geq 1 \), then \( K(x_1, \ldots, x_{n-1}) \) also splits \( \mathcal{C} \) and hence, by induction, \( K \) splits \( \mathcal{C} \) so \( \mathcal{C} \) is split.

Let \( u_1, \ldots, u_e \) be an orthogonal basis for \( \mathcal{C} \) with respect to \( N(x, y) \). This is also an orthogonal basis for \( \mathcal{C}_L \) over \( L \) and, if \( \mathcal{C}_L \) is split, there are \( \xi_i \in L \), \( 1 \leq i \leq e \), such
that \( N(\sum \xi_i u_i) = 0 \). Clearing the denominators of the \( \xi_i \) we have, since \( N(ax) = a^2 N(x) \) for \( a \in L \), polynomials \( p_i \) in \( K[x_1, \ldots, x_n] \), not all \( p_i \equiv 0 \), such that \( N(\sum p_i u_i) = \sum p_i^2 N(u_i) = 0 \). 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 \( \sum (x_n^k q_i + r_i)^2 N(u_i) = 0 \) and, since the \( x_i \) are algebraically independent, we must have \( \sum q_i^2 N(u_i) = 0 \) in \( K(x_1, \ldots, x_{n-1}) \). Thus \( K(x_1, \ldots, x_{n-1}) \) splits \( \mathcal{C} \). Induction completes the proof that \( \mathcal{C} \) is split over \( K \).

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

**Lemma 4.** Let \( \mathcal{C} \) be a composition algebra over \( K \), \( F, F' \) field extensions of \( K \), \( \varphi \) a \( K \)-place of \( F \) into \( F' \cup \infty \). If \( \mathcal{C}_F \) is split, so is \( \mathcal{C}_F' \).

**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 \( (\lambda_j^{-1} \lambda_i) \varphi = \infty \) for \( 1 \leq i \leq t \), \( (\lambda_j^{-1} \lambda_i) \varphi \in F' \), \( t < i \leq n \). \( \lambda_i \neq 0 \) since otherwise \( (\lambda_j^{-1} \lambda_i) \varphi = 0 \) for \( 1 < i \leq n \). Thus \( (\lambda_j^{-1} \lambda_i) \varphi = ((\lambda_j^{-1} \lambda_i)^{-1} \times (\lambda_j^{-1} \lambda_i) \varphi = 0 \) for \( t < i \leq n \), and \( (\lambda_j^{-1} \lambda_i) \varphi = 1 \) if \( 1 \in F' \) and hence for \( \lambda_i \) there are at most \( (t-1) \) \( i \) such that \( (\lambda_j^{-1} \lambda_i) \varphi = \infty \), a contradiction to the minimality of \( t \). Thus \( t = 0 \).

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

\[
\sum_i (\lambda_j^{-1} \lambda_i)^2 N(u_i) = 0
\]

and hence, \( \sum_i (\lambda_j^{-1} \lambda_i)^2 \varphi N(u_i) = 0 \). Since \( (\lambda_j^{-1} \lambda_i)^2 \varphi = ((\lambda_j^{-1} \lambda_i) \varphi)^2, \) it follows that \( N_F(\sum (\lambda_j^{-1} \lambda_i) \varphi u_i) = 0 \) and, since \( (\lambda_j^{-1} \lambda_i) \varphi = 1 \neq 0 \), \( \mathcal{C}_F' \) is split.

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

**Proof.** If there is \( u \in (K(1))^{\perp} \) with \( N(u) = -\lambda \), then \( x = (\lambda^{1/2})1 + u \in \mathcal{C}_L \) clearly has \( N_L(x) = 0 \), so \( \mathcal{C}_L \) is split. Conversely, if \( \mathcal{C}_L \) is split, then there is \( x = a + (\lambda^{1/2})b, a, b \in \mathcal{C}, \) 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 \( \mathcal{C}, \mathcal{C}' \) respectively, to be equivalent if there...
is a nonsingular linear transformation \( \varphi \) of \( V \) onto \( V' \) such that \( N'(x \varphi) = N(x) \) for all \( x \in V, N, N' \) denoting the respective quadratic forms of \( C \) and \( C' \).

**Lemma 6.** If a composition algebra \( C \) is equivalent to a subspace of a composition algebra \( C' \), then \( C \) is isomorphic to a subalgebra of \( C' \).

**Proof.** The proof is essentially that of Jacobson [4]. Let \( \varphi \) be the mapping of \( C \) into \( C' \) such that \( N'(x \varphi) = N(x) \) for all \( x \in C \) and suppose that \( B, B' \) are isomorphic composition subalgebras of \( C, C' \) respectively. By (4), \( B \) and \( B' \) are equivalent and, since \( B \) and \( B \varphi \) are clearly equivalent, \( B' \) and \( B \varphi \) are equivalent subspaces of \( C' \). By Witt’s Theorem for bilinear forms, \( (B')^1 \) and \( (B \varphi)^1 \) are equivalent in \( C' \). Thus, if there is \( u \in B^1 \) with \( N(u) \neq 0 \), which is the case unless \( B = C \), then there is \( u' \in (B')^1 \) such that \( N'(u') = N'(u \varphi) = N(u) \). Then the algebras \( B + Bu, B' + B'u' \) are composition subalgebras of \( C, C' \) respectively which are isomorphic by (2). Beginning with \( B = K1, B' = K1' \) one can, in successive steps, thus construct an isomorphism of \( C \) into \( C' \).

Since in this proof, whenever \( 2 \dim B = \dim C \), we need only produce elements \( u, u' \) in \( B^1, (B')^1 \) respectively with \( N(u) = N'(u') \neq 0 \), we can clearly weaken the hypotheses to obtain the

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

We are now prepared to restate and prove

**Theorem 2.** Let \( C \) be a composition algebra of dimension greater than one over \( K \). Then

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

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

\[
\lambda(u) = N\left( \sum_{i=2}^{m} x_i u_i + u_{m+1} \right).
\]

**Proof of 1.** If \( C \) is split, Lemma 3 yields the result since \( F(C) = L(C) \) is a rational function field in \( m-1 \) indeterminates over \( K \). If \( C \) is not split, neither is \( C_{L(C)} \), by Lemma 3, and since \( \lambda(u) \) is by definition \( N(\sum_{i=2}^{m} x_i u_i + u_{m+1}) \), where \( \sum_{i=2}^{m} x_i u_i + u_{m+1} \in (L(C)1)^2 \), 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 $F u_1 + \cdots + F u_{m+1}$, so there is $u = \beta u_1 + \sum_{i=2}^{m+1} \beta_i u_i$ in $\mathcal{C}_F$, $u \neq 0$, with $N_F(u) = 0$. Thus

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

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

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

By Lemma 2, corollary, there is a $K$-place $\varphi$ 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 $\pm \beta_{m+1}^{-1}$.

If $\beta_{m+1} = 0$, some $\beta_i$, $i \neq m+1$ must be nonzero, since $0 = \beta^2 + \sum_{i=2}^{m} \beta_i^2 N(u_i)$ and not all of $\beta_i$ are zero. We assume, without loss of generality, that $\beta_m \neq 0$. Then

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

Again by the corollary to Lemma 2, there is a $K$-place of $F(\mathcal{C}) = K(x_2, \ldots, x_m)((-\lambda(u))^{1/2}) = K(x_2 x_{m-1}, \ldots, x_m x_{m-1}, x_m^{-1})((-\lambda(u))^{1/2})$ into $F \cup \infty$ mapping $x_i x_{m-1}$ to $\beta_i \beta_{m+1}^{-1}$, $2 \leq i < m$, $x_m^{-1}$ to zero, and $x_m^{-1}(-\lambda(u))^{1/2}$ to $\pm \beta_{m+1}^{-1}$, since $x_i x_{m-1}$, $2 \leq i < m$, $x_m^{-1}$ 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 $u' \in (1')^+ \subseteq \mathcal{C}_{L(\mathcal{C})}$ such that $N'_{L(\mathcal{C})}(u') = \lambda(u)$. Thus in $\mathcal{C}_{L(\mathcal{C})}(x_1)$,

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

It follows easily from a result of Pfister ([5], Satz 3) that the subspace $K u_1 + \cdots + K u_{m+1}$ 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**


THE OHIO STATE UNIVERSITY, COLUMBUS, OHIO