JOURNAL OF ALGEBRA 92, 81–103 (1985)

Separable Alternative Algebras over Commutative Rings

ROBERT BIX

Department of Mathematics,
The University of Michigan,
Flint, Michigan 48502

Communicated by Nathan Jacobson

Received May 15, 1983

Let A be a unital alternative algebra over a commutative ring R. The unital universal multiplication envelope $U_R(A)$ of A is an associative algebra such that there is a one-to-one correspondence between left $U_R(A)$-modules and alternative A-bimodules. We call A separable over R if $U_R(A)$ is a separable associative R-algebra.

Our main theorem states that a unital alternative R-algebra A is separable over R if and only if A is the direct sum of ideals B and C such that

(i) B is a separable associative R-algebra,

(ii) C is finitely spanned and projective of rank 8 over its center $Z(C)$,

(iii) C has a nondegenerate quadratic form $n(x)$ over $Z(C)$ such that $n(xy) = n(x)\, n(y)$ for all $x, y \in C$, and

(iv) $Z(C)$ is a separable associative R-algebra.

In Section 1 we establish basic properties of separable alternative algebras. In Section 2 we prove the main theorem in the case where R is isomorphic to the center of A. We show in Section 3 that a commutative associative algebra is separable in the associative sense if and only if it is separable as an alternative algebra. The results of Sections 2 and 3 are combined to prove the main theorem in Section 4.

All rings, algebras, subalgebras, modules, bimodules, and homomorphisms are assumed to be unital. Throughout this paper, R denotes a commutative ring and A an alternative R-algebra [11, p. 27]. For any R-algebra B, let $Z(B)$ be the center of B [11, p. 14]. If $x, y \in B$, let $x \circ y = xy + yx$ and $[x, y] = xy - yx$. If S and T are subsets of B, let $[S, T]$ be the set of all $[x, y]$, $x \in S$, $y \in T$. If S is a subset of B, let $\langle S \rangle$ be the subalgebra of B generated by the elements of S (and 1). We call B finitely spanned over R if it is finitely spanned as a R-module.

0021-8693/85 $3.00

Certain properties of modules and separable associative algebras over commutative rings are summarized in [2, pp. 113–115]. References of the form [*Mi*] and [*Ai*], *i* an integer, refer to these.

In [9], Müller formulated a concept of separability for an arbitrary nonassociative R-algebra finitely spanned and projective over R and its center. He proved parts of our Lemmas 1.5, 1.8, and 1.9 in this context. This point of view was pursued further by Wisbauer in [12].

1. Basic Properties of Separable Algebras

Basic properties of separable Jordan algebras over commutative rings containing $\frac{1}{2}$ are presented in Sections 1 and 2 of [2]. We establish the analogous results for alternative algebras in this section. In particular, if A is separable over R, then A is finitely spanned and projective over $Z(A)$ and there is a one-to-one correspondence between the ideals of A and the ideals of $Z(A)$. If A is finitely spanned over R, then A is separable over R if and only if A/mA is separable in the classical sense over R/m for every maximal ideal m of R.

Let $U_R(A)$ be the *unital* universal multiplication envelope of A [7, p. 103]. $U_R(A)$ is an associative R-algebra such that there is a natural correspondence between left $U_R(A)$-modules and alternative A-bimodules. There are R-module homomorphisms λ and ρ from A to $U_R(A)$ such that

$$U_R(A) = \langle A^\lambda, A^\rho \rangle, \tag{1}$$

$$(a^2)^\lambda = (a^\lambda)^2 \quad \text{and} \quad (a^2)^\rho = (a^\rho)^2, \tag{2}$$

$$(ab)^\lambda - a^\lambda b^\lambda = [a^\lambda, b^\rho], \tag{3}$$

and

$$(ab)^\rho - b^\rho a^\rho = [b^\rho, a^\lambda] \tag{4}$$

for all $a, b \in A$ [7, p. 86]. Setting $b = a$ in (3) and using (2) shows that

$$[a^\lambda, a^\rho] = 0. \tag{5}$$

Linearizing (2) shows that

$$(a \circ b)^\lambda = a^\lambda \circ b^\lambda \quad \text{and} \quad (a \circ b)^\rho = a^\rho \circ b^\rho. \tag{6}$$

Since $-(ax)\,b + a(xb) = (bx)\,a - b(xa)$ holds in any alternative algebra [11, p. 27], it follows as in [7, p. 96] that

$$[a^\lambda, b^\rho] = [a^\rho, b^\lambda] = -[b^\lambda, a^\rho] = -[b^\rho, a^\lambda]. \tag{7}$$

In order to extend the results of [2] to alternative algebras, we need to observe that, if A is finitely spanned over R, then so is $U_R(A)$. We prove a more general result below for use in Section 4.

LEMMA 1.1. *Let S be a subalgebra of $Z(A)$ such that A is finitely spanned over S and*

$$\langle S^\lambda, S^\rho \rangle \subset Z[U_R(A)]. \tag{8}$$

Then $U_R(A)$ is finitely spanned over $\langle S^\lambda, S^\rho \rangle$.

Proof. Let T denote $\langle S^\lambda, S^\rho \rangle$. By (8), we can consider $U_R(A)$ as an algebra over T. Let $V = \{a_1, \ldots, a_p\}$ span A over S. Equations (3), (4), and (8) imply that $(sa_i)^\lambda = s^\lambda a_i^\lambda$ and $(sa_i)^\rho = s^\rho a_i^\rho$ for $s \in S$ and $a_i \in V$, so

$$A^\lambda \subset \sum Ta_i^\lambda, \quad A^\rho \subset \sum Ta_i^\rho. \tag{9}$$

Then (1) shows that $U_R(A)$ is generated as a T-algebra by the a_i^λ and a_i^ρ. Thus $U_R(A)$ is spanned as a T-module by elements of the form

$$b_1^{\gamma_1} \cdots b_d^{\gamma_d}, \qquad b_i \in V, \quad \gamma_i \in \{\lambda, \rho\}. \tag{10}$$

We call an element of the form (10) a monomial of degree d.

Claim 1. Every monomial f of the form (10) is a T-linear combination of monomials of the form

$$b_1^\lambda \cdots b_k^\lambda b_{k+1}^\rho \cdots b_d^\rho, \qquad b_i \in V. \tag{11}$$

We prove this by induction on the degree d of f. If all the γ_i in f are ρ's, then f has the required form. Assume that some γ_i is λ, and let γ_s be the first such γ_i. If $s > 1$, we use (3) in the form

$$b_{s-1}^\rho b_s^\lambda = b_s^\lambda b_{s-1}^\rho - (b_s b_{s-1})^\lambda + b_s^\lambda b_{s-1}^\lambda$$

together with (8) and (9) to write f as a T-linear combination of monomials of degree $\leqslant d$ which have $\gamma_{s-1} = \lambda$. Repeating this argument shows that f is a T-linear combination of monomials of degree $\leqslant d$ which have $\gamma_1 = \lambda$. Then $f = \Sigma a_i^\lambda g_i$, where each g_i is a T-linear combination of monomials of degree at most $d-1$. By induction, each g_i is a T-linear combination of monomials of the form (11), and hence so is f.

Let M_d be the T-subspace of $U_R(A)$ spanned by the monomials of the form (11) having degree d. We write $a_i < a_j$ if $i < j$. We call a monomial of the form (11) ordered if $b_1 < \cdots < b_k$ and $b_{k+1} < \cdots < b_d$.

Claim 2. Every monomial g of the form (11) is a T-linear combination of ordered monomials. We prove this by induction on the degree d of g. If $b_i > b_{i+1}$ for some i such that $1 \leqslant i < k$, then (6), (8), and (9) imply that g is congruent modulo M_{d-1} to -1 times a monomial of the form (11) where $b_i < b_{i+1}$ and the other b's are as in g. If $b_i = b_{i+1}$ for some i such that $1 \leqslant i < k$, then (2), (8), and (9) imply that $g \in M_{d-1}$. It follows that g is congruent modulo M_{d-1} to either zero or $\pm$ a monomial of form (11) satisfying $b_1 < \cdots < b_k$. Applying the analogous argument to $b_{k+1}, \ldots, b_d$ shows that g is congruent modulo M_{d-1} to either zero or $\pm$ an ordered monomial. The claim follows by induction.

Since $U_R(S)$ is spanned over T by monomials of the form (10), Claims 1 and 2 imply that $U_R(S)$ is spanned by ordered monomials. Hence $U_R(S)$ is finitely spanned over T. ∎

In the case $S = R1 \subset Z(A)$, Lemma 1.1 yields the following result.

LEMMA 1.2. *If A is finitely spanned over R, then so is $U_R(A)$.*

Let B be a nonassociative algebra over a field R. We call B *semisimple* if it is finite dimensional over R and a direct sum of simple ideals. We call B *classically separable* if $B \otimes_R F$ is semisimple, where F is the algebraic closure of R.

LEMMA 1.3. *Let A be finite-dimensional over a field R. Then A is classically separable if and only if $U_R(A)$ is classically separable.*

Proof. If F is the algebraic closure of R, $U_F(A \otimes_R F)$ is isomorphic to $U_R(A) \otimes_R F$ [7, p. 88]. Thus, by field extension, we can assume that R is algebraically closed. If A is semisimple, the representation theory of alternative algebras shows that every A-bimodule is completely reducible [8]. Then every left $U_R(A)$-module is completely reducible, so $U_R(A)$ is semisimple [6, p. 400]. Conversely, if $U_R(A)$ is semisimple, then A is a direct sum of irreducible $U_R(A)$-modules [6, p. 400], so A is a direct sum of simple ideals. ∎

We call A *separable* over R if $U_R(A)$ is a separable associative R-algebra. A separable R-algebra A is called *central separable* if the map $r \to r1$ is an isomorphism of R onto $Z(A)$.

As observed in [2, p. 125], Lemmas 1.2 and 1.3 imply that the results 1.1–1.8, 2.1–2.5, 2.8, and 2.9 of [2] extend to alternative algebras. This yields the following six results,

LEMMA 1.4. *If R is a field, then A is separable over R if and only if A is classically separable over R.*

LEMMA 1.5. *Let A be finitely spanned over R. Then A is separable over R if and only if A/mA is either zero or classically separable over R/m for every maximal ideal m of R. A is central separable over $R1$ $(1 \in A)$ if and only if A/mA is either zero or central simple over R/m for every maximal ideal m of R.*

LEMMA 1.6. *If A is separable over R, there is an idempotent $e \in U_R(A)$ such that*

$$e1 = 1, \qquad xe = (x1)^{\lambda} e = (x1)^{\rho} e \qquad (1 \in A, \quad x \in U_R(A)). \tag{12}$$

Accordingly, $eA = Z(A)$ is a direct summand of A as an R-module. e is called a separability idempotent *of A.*

LEMMA 1.7. *If A is separable over R, then A is central separable, finitely spanned, and projective over $Z(A)$.*

LEMMA 1.8. *Let A be separable over R.*

(i) *If S is a commutative associative R-algebra, then $A \otimes_R S$ is either zero or separable over S, and $Z(A \otimes_R S) \cong Z(A) \otimes_R S$.*

(ii) *If I is an ideal of A, then A/IA is either zero or separable over R/I and $Z(A/IA) \cong Z(A)/IZ(A)$.*

(iii) *If ϕ is an algebra homomorphism of A onto an R-algebra B, then B is separable over R and $Z(B) = \phi[Z(A)]$.*

(iv) *If S is a commutative associative R-algebra and A is an S-algebra such that R acts on A via $R1 \subset S$, then A is separable over S.*

LEMMA 1.9. *If A is separable over R, there is a one-to-one correspondence between the ideals I of A and the ideals α of $Z(A)$ given by $I \to I \cap Z(A)$ and $\alpha \to \alpha A$.*

2. STRUCTURE OF CENTRAL SEPARABLE ALGEBRAS

We prove that A is central separable over R if and only if R is the direct sum of ideals R_1 and R_2 such that $R_1 A$ is a central separable associative R_1-algebra and $R_2 A$ is an octonion R_2-algebra. To establish this, we extend the results in Section 3 of [2] to alternative algebras and show that a separable alternative algebra is a direct sum of homogeneous components. We prove that the nonassociative component is an octonion algebra over its center by extending the results on generic minimum polynomials in Sections 1 and 2 of [4] to alternative algebras.

Let $R[n^2]$ denote the associative R-algebra of n-by-n matrices over R, n a positive integer. Let $\{e_{ij}\}$ be the usual basis of $R[n^2]$. Let d be the involution of $R[4]$ determined by $e_{11}^d = e_{22}$, $e_{22}^d = e_{11}$, $e_{12}^d = -e_{12}$, $e_{21}^d = -e_{21}$, and R-linearity. We define an alternative R-algebra $R[8]$ as follows: let $R[8]$ be isomorphic to $R[4] \oplus R[4]$ as an R-module, let $b_1 + vb_2 \in R[8]$ denote the image of $(b_1, b_2) \in R[4] \oplus R[4]$ under this isomorphism, and define multiplication in $R[8]$ by

$$(b_1 + vb_2)(b_3 + vb_4) = (b_1 b_3 + b_4 b_2^d) + v(b_1^d b_4 + b_3 b_2) \tag{13}$$

[11, p. 47].

If R is an algebraically closed field, the $R[i]$ represent the distinct isomorphism classes of finite-dimensional simple alternative R-algebras [11, p. 56]. Since $R[i]$ is i-dimensional over R, the isomorphism class of a finite-dimensional simple alternative algebra over an algebraically closed field is determined by its dimension. Together with Lemmas 1.4–1.9, this implies that proofs of Theorem 3.1 and Corollary 3.3 of [2] can be extended from associative to alternative algebras. This yields the following two lemmas. Let X be the union of $\{8\}$ and the set of all squares of positive integers.

LEMMA 2.1. *If A is separable, it can be written uniquely as a direct sum of ideals $A(i)$, $i \in X$, such that the following condition is satisfied: if S is any commutative ring such that A is a separable S-algebra, m is any maximal ideal of S, and F is the algebraic closure of S/m, then*

$$A(i)/mA(i) \otimes_{S/m} F$$

is either zero or a finite direct sum of algebras isomorphic to $F[i]$. Only finitely many of the $A(i)$ are nonzero. Each nonzero $A(i)$ is a projective $Z(A_i)$-module of rank i.

LEMMA 2.2. *Let A be separable over R.*

(i) *If S is a commutative associative R-algebra, then $(A \otimes_R S)(i) \cong A(i) \otimes_R S$.*

(ii) *If I is an ideal of R, then $(A/IA)(i) \cong A(i)/IA(i)$.*

(iii) *If ϕ is a homomorphism of A onto an R-algebra B, then $B(i) = \phi[A(i)]$.*

Using Lemmas 1.6 and 1.7, we can extend the proof of Lemma 5.3 of [2] to alternative algebras. This yields:

LEMMA 2.3. *If A is central separable over R, there is a Noetherian subring R' of R and an R'-subalgebra A' of A such that A' is central separable over R' and $A' \otimes_{R'} R$ is isomorphic to A.*

LEMMA 2.4. *In* $R[n^2]$, *set* $a_1 = 0$ *and*

$$a_s = \sum_{i=2}^{s} e_{i-1,i} + e_{i,i-1}$$

for $2 \leqslant s \leqslant n$. *Then* $R[n^2]$ *is generated as an* R*-algebra by* a_n *and* e_{nn}.

Proof. We induct on n, the case $n = 1$ being clear. $\langle a_n, e_{nn} \rangle$ contains $a_n e_{nn} = e_{n-1,n}$ and $e_{nn} a_n = e_{n,n-1}$, so it also contains

$$a_n - e_{n-1,n} - e_{n,n-1} = a_{n-1}$$

and

$$e_{n-1,n} e_{n,n-1} = e_{n-1,n-1}.$$

Then $\langle a_n, e_{nn} \rangle$ contains $\langle a_{n-1}, e_{n-1,n-1} \rangle$, and the latter contains all e_{ij} for $1 \leqslant i,j \leqslant n-1$ by induction. Then $\langle a_n, e_{nn} \rangle$ contains $e_{i,n-1} e_{n-1,n} = e_{in}$ and $e_{n,n-1} e_{n-1,i} = e_{ni}$ for $1 \leqslant i \leqslant n-1$, so $\langle a_n, e_{nn} \rangle$ contains all e_{ij}, $1 \leqslant i,j \leqslant n$. ∎

LEMMA 2.5. *If* A *is separable, then* $\oplus A(n^2)$ *is associative.*

Proof. We can assume that $A = A(n^2)$ and $R = Z(A)$ [Lemma 1.8].

First assume that (R, m) is local and that A/mA is isomorphic to $(R/m)[n^2]$. By Lemma 2.4, A/mA is generated by two elements. If $a, b \in A$ are preimages of these two elements, $A = \langle a, b \rangle + mA$. Since A is finitely spanned over R [Lemma 1.7], Nakayama's Lemma yields $A = \langle a, b \rangle$[M6]. Then A is associative, by Artin's theorem [11, p. 29].

Next assume that R is Noetherian. Let R^* be the completion of R in the m-topology for a maximal ideal m of R, and write $A \otimes_R R^*$ as A^*. As in the proof of [2, Lemma 5.2], there is a commutative associative R^*-algebra S such that S is a finitely spanned free R^*-module, (S, mS) is complete local Noetherian, and $(A^* \otimes_{R^*} S)/mS(A^* \otimes_{R^*} S)$ is isomorphic to $(S/mS)[n^2]$. The preceding paragraph shows that $A^* \otimes_{R^*} S$ is associative. Since S is a free R^*-module, A^* is associative. Since this holds for every maximal ideal m of R, it follows that A is associative [1, pp. 40, 108, 110].

Finally, let R be arbitrary. There is a Noetherian subring R' of R and an R'-subalgebra A' of A such that A' is central separable over R' and $A \cong A' \otimes_{R'} R$ [Lemma 2.3]. Lemma 2.2 implies that $A' = A'(n^2)$. The preceding paragraph shows that A' is associative, whence A is associative. ∎

LEMMA 2.6. *The following conditions are equivalent*:

(i) *A is a central separable alternative R-algebra such that $A = \oplus A(n^2)$.*

(ii) *A is a central separable associative R-algebra.*

Proof. We first note that a finitely spanned associative R-algebra B is separable in the alternative sense if and only if it is separable in the associative sense. This holds because B is separable in either sense if and only if B/mB is either zero or classically separable over R/m for every maximal ideal m of R [Lemma 1.5, A4].

If A satisfies (i), Lemma 2.5 shows that A is associative. Since A is finitely spanned over R [Lemma 1.7], the preceding paragraph shows that A satisfies (ii). Conversely, if A satisfies (ii), then A is finitely spanned over R [A7], so the paragraph above shows that A is central separable in the alternative sense. Since $F[8]$ is not associative for any field F [11, p. 47], Lemma 2.1 implies that $A(8)/mA(8)$ is zero for every maximal ideal m of R. Since A is finitely spanned over R, $A(8) = 0$ [M6] and $A = \oplus A(n^2)$. ∎

The proof of Lemma 3.21 of [11] yields:

LEMMA 2.7. *Let A have an ideal N such that $N^2 = 0$. Assume that $R[4]$ is a subalgebra of A and that there is $w \in A$ such that $w^2 \equiv 1$ and $aw \equiv wa^d \pmod N$ for all $a \in R[4]$. Then there is $v \in A$ such that $v \equiv w \pmod N$, $v^2 = 1$, and $av = va^d$ for all $a \in R[4]$.*

LEMMA 2.8. *If A is central separable over (R, m) complete local Noetherian and A/mA is isomorphic to $(R/m)[8]$, then A is isomorphic to $R[8]$.*

Proof. We identify A/mA with $(R/m)[8]$ and consider $(R/m)[4]$ as a subalgebra of $(R/m)[8]$. Let $\{e'_{ij}\}$ be the usual basis of $(R/m)[4]$, and let p be the canonical map of A onto $(R/m)[8]$. A is finitely spanned over R [Lemma 1.7], so A is complete in the m-topology [1, p. 108]. Since A is power-associative, the proof of [10, p. 51] shows that there is an idempotent $e_{11} \in A$ such that $pe_{11} = e'_{11}$. Set $e_{22} = 1 - e_{11}$, so the e_{ii} are orthogonal idempotents such that $e_{11} + e_{22} = 1$ and $pe_{ii} = e'_{ii}$. Let $A_{ij} = e_{ii}Ae_{jj}$ be the Peirce decomposition of A [11, p. 32]. Take $e_{12} \in A_{12}$ and $f_{21} \in A_{21}$ such that $pe_{12} = e'_{12}$ and $pf_{21} = e'_{21}$. $e_{12}f_{21} = e_{11} + a$ for $a \in mA_{11}$. Since A is complete in the m-topology, set $b = \Sigma(-1)^i a^i$, $i \geqslant 1$, and $e_{21} = f_{21}(e_{11} + b)$. Then $b \in mA_{11}$, $e_{21} \in A_{21}$, $pe_{21} = e'_{21}$, and

$$\begin{aligned} e_{12}e_{21} &= e_{12}(f_{21}(e_{11} + b)) \\ &= (e_{12}f_{21})(e_{11} + b) \qquad [11, \text{p. } 35] \\ &= (e_{11} + a)(e_{11} + b) = e_{11}. \end{aligned} \tag{14}$$

$e_{21}e_{12} \in A_{22}$ [11, p. 35], so $e_{21}e_{12} = e_{22} + c$, $c \in mA_{22}$. Then

$$\begin{aligned} e_{22} + c = e_{21}e_{12} &= (e_{21}e_{11})\,e_{12} \\ &= (e_{21}(e_{12}e_{21}))\,e_{12} \qquad \text{(by (14))} \\ &= (e_{21}e_{12})(e_{21}e_{12}) \qquad [11, \text{p. } 29] \\ &= (e_{22} + c)^2 \\ &= e_{22} + 2c + c^2, \end{aligned}$$

so $c = -c^2$. It follows that $c \in m^n A$ for every positive integer n, so $c = 0$ [1, p. 110]. Thus $e_{21}e_{12} = e_{22}$. Reference [11, p. 35] shows that $e_{12}^2 = 0 = e_{21}^2$. Since A is finitely spanned and projective over R [Lemma 1.7] and the $pe_{ij} = e'_{ij}$ are linearly independent over R/m, it follows that the e_{ij} are linearly independent over R [5, p. 24]. Thus A contains a subalgebra B isomorphic to $R[4]$ such that $pB = (R/m)[4]$. We identify B with $R[4]$.

Since A/mA is isomorphic to $(R/m)[8]$, there is $w \in A$ such that $w^2 \equiv 1$ and $aw \equiv wa^d \pmod{mA}$ for all $a \in R[4]$. Applying Lemma 2.7 to the ideal $N = mA/m^2A$ of A/m^2A shows that there is $w_1 \in A$ such that $w_1 \equiv w \pmod{mA}$, $w_1^2 \equiv 1 \pmod{m^2A}$, and $aw_1 \equiv w_1 a^d \pmod{m^2A}$ for all $a \in R[4]$. Then applying Lemma 2.7 to the ideal $N = m^2A/m^4A$ of A/m^4A shows that there is $w_2 \equiv w_1 \pmod{m^2A}$ such that $w_2^2 \equiv 1 \pmod{m^4A}$ and $aw_2 \equiv w_2 a^d \pmod{m^4A}$ for all $a \in R[4]$. It follows by induction that for every positive integer i there is $w_i \in A$ such that $w_i \equiv w_{i-1} \pmod{m^{2^{i-1}}A}$, $w_i^2 \equiv 1 \pmod{m^{2^i}A}$, and $aw_i \equiv w_i a^d \pmod{m^{2^i}A}$ for all $a \in R[4]$. Since A is complete in the m-topology, we can set $v = \lim w_i$. Then $v \equiv w \pmod{mA}$, $v^2 = 1$, and $av = va^d$ for all $a \in R[4]$. It follows as in [11, pp. 46–47] that multiplication in $R[4] + vR[4]$ is given by (13). Since the pe_{ij} and $p(ve_{ij})$ form a basis of A/mA over R/m and A is finitely spanned and projective over R, the e_{ij} and ve_{ij} form a basis of A as a free R-module [5, p. 24]. Hence A is isomorphic to $R[8]$. ∎

We require the following analogue of Lemma 1.1 of [4].

LEMMA 2.9. *Let $A = A(8)$ be central separable over (R, m) complete local Noetherian. Then there is a commutative associative R-algebra S such that*

(i) *S is a free R-module of finite rank and (S, mS) is complete local Noetherian, and*

(ii) *$A \otimes_R S \cong Z[8] \otimes_Z S$, where $Z[8]$ is central separable over Z.*

Proof. As in he proof of [2, Lemma 5.2], there is a commutative associative R-algebra S satisfying (i) such that $(A \otimes_R S)/m(A \otimes_R S)$ is

isomorphic to $(S/mS)[8]$. Lemmas 1.8 and 2.8 imply that $A \otimes_R S$ is isomorphic to $S[8]$. Clearly $S[8] \cong Z[8] \otimes_Z S$, while Lemma 1.5 and [11, p. 56] show that $Z[8]$ is central separable over Z. ∎

A quadratic form $n(x)$ on a finitely spanned, projective R-module is called nondegenerate if its associated bilinear form $n(x, y) = n(x + y) - n(x) - n(y)$ is nondegenerate in the sense of [M5].

An *octonion algebra* C over R is a (unital) nonassociative R-algebra C such that

(i) C is a finitely spanned, projective R-module of rank 8, and

(ii) C has a nondegenerate quadratic form $n(x)$ over R such that $n(xy) = n(x)\, n(y)$ for all $x, y \in C$.

If C_1 and C_2 are octonion algebras over commutative rings R_1 and R_2, it follows that $C_1 \oplus C_2$ is an octonion algebra over $R_1 \oplus R_2$.

LEMMA 2.10. *If C is a nonassociative R-algebra, the following conditions are equivalent:*

(i) *C is a central separable alternative R-algebra such that $C = C(8)$.*

(ii) *C is an octonion algebra over R.*

Moreover, let C be an octonion algebra over R, and set $t(x) = n(x, 1)$ and $x^d = t(x)\, 1 - x$. Then d is an involution of C, $x^2 - t(x)\, x + n(x)\, 1 = 0$, and $xx^d = n(x)\, 1 = x^d x$ for all $x \in C$.

Proof. Let C satisfy (i). Using Lemmas 1.7–1.9, 2.1–2.3, and 2.9, we can extend the results 1.3–2.3 of [4] on generic minimum polynomials to alternative algebras. Thus there is a linear map t and a quadratic map n from C to R such that $x^2 - t(x)\, x + n(x)\, 1 = 0$ for all $x \in C$, where $t(x) = n(x, 1)$, $n(xy) = n(x)\, n(y)$, n is nondegenerate, $x^d \equiv t(x)\, 1 - x$ is an involution of C, and $xx^d = n(x)\, 1 = x^d x$ for all $x, y \in C$. C is a projective R-module of rank 8 [Lemma 2.1], so C is an octonion algebra over R.

Conversely, let C be an octonion algebra over R. $n(x) = n(1x) = n(1)\, n(x)$ for $1, x \in C$. Since n is nondegenerate, R is generated as an additive group by the $n(x)$, $x \in C$. Thus $n(1) = 1$, so it follows as in [8] that C is alternative. For every maximal ideal m of R, C/mC is an octonion algebra over R/m, so C/mC is central simple over R/m [8]. Hence C is central separable over $R1$, $1 \in C$ [Lemma 1.5]. Since C is projective of rank 8 over R, localization shows that C is a faithful R-module [5, p. 24], so $R \cong R1 \subset C$. The last sentence of Lemma 2.1 implies that $C = C(8)$ since C has rank 8 over R. Thus C satisfies (i). ∎

PROPOSITION 2.11. *The following conditions on a nonassociative R-algebra B are equivalent:*

(i) *B is a central separable alternative R-algebra.*

(ii) *R is the direct sum of ideals R_1 and R_2 such that R_1B is a central separable associative R_1-algebra and R_2B is an octonion algebra over R_2.*

Proof. If B satisfies (i), let R_1 be the preimage in R of $\oplus Z[B(n^2)]$, and let R_2 be the preimage in R of $Z[B(8)]$. Then $R = R_1 \oplus R_2$, $R_1B = \oplus B(n^2)$, and $R_2B = B(8)$. Each R_iB is central separable over R_i, $R_1B = \oplus (R_1B)(n^2)$, and $R_2B = (R_2B)(8)$ [Lemmas 1.8, 2.2]. R_1B is a central separable associative R_1-algebra [Lemma 2.6], and R_2B is an octonion algebra over R_2 [Lemma 2.10]. Conversely, if B satisfies (ii), Lemmas 2.6 and 2.10 show that each R_iB is a central separable alternative R_i-algebra. Then $B = R_1B \oplus R_2B$ is an alternative algebra whose center is naturally isomorphic to $R_1 \oplus R_2 = R$. Since each $U_{R_i}(R_iB)$ is a separable associative R_i-algebra, $U_R(B) \cong \oplus U_{R_i}(R_iB)$ is a separable associative R-algebra [5, p. 47]. Hence (i) is satisfied. ∎

3. Centers of Separable Algebras

We prove that a commutative associative algebra is separable in the alternative sense if and only if it is separable in the associative sense. The proofs are analogous to those in Section 1 of [3].

Lemmas 1.5, 1.6, and 1.8 show that the proof of Proposition 1.1 of [3] can be generalized to alternative algebras. This yields:

Lemma 3.1. *If A is separable over R, then $Z(A)$ is a separable associative R-algebra.* ∎

If B is an associative R-algebra, we observe that

$$[ab, c] = [a, c]\, b + a[b, c], \qquad [a, b] = -[b, a] \tag{15}$$

for $a, b, c \in B$. We define the opposite algebra $B^\circ = \{b^\circ \mid b \in B\}$ to be an R-algebra with operations $r(a^\circ) = (ra)^\circ$, $a^\circ + b^\circ = (a + b)^\circ$, and $a^\circ b^\circ = (ba)^\circ$, $a, b \in B$, $r \in R$.

In $U_R(A)^\circ$, (2) implies that

$$(a^2)^{\lambda\circ} = (a^{\lambda\circ})^2, \qquad (a^2)^{\rho\circ} = (a^{\rho\circ})^2. \tag{16}$$

Also

$$\begin{aligned}(ab)^{\rho\circ} - a^{\rho\circ}b^{\rho\circ} &= ((ab)^\rho - b^\rho a^\rho)^\circ \\ &= [b^\rho, a^\lambda]^\circ \qquad \text{(by (4))} \\ &= [b^\lambda, a^\rho]^\circ \qquad \text{(by (7))} \\ &= [a^{\rho\circ}, b^{\lambda\circ}] \end{aligned} \tag{17}$$

and

$$\begin{aligned}(ab)^{\lambda o} - b^{\lambda o}a^{\lambda o} &= ((ab)^{\lambda} - a^{\lambda}b^{\lambda})^{o} \\ &= [a^{\lambda}, b^{\rho}]^{o} \qquad \text{(by (3))} \\ &= [a^{\rho}, b^{\lambda}]^{o} \qquad \text{(by (7))} \\ &= [b^{\lambda o}, a^{\rho o}]. \end{aligned} \tag{18}$$

Comparing (2), (3), and (4) with (16), (17), and (18), respectively, shows that there is an R-algebra homomorphism from $U_R(A)$ to $U_R(A)^o$ taking a^{λ} to $a^{\rho o}$ and a^{ρ} to $a^{\lambda o}$ for all $a \in A$ [7, p. 88]. Hence there is an antiautomorphism of $U_R(A)$ exchanging a^{λ} and a^{ρ} for all $a \in A$. We call this the canonical involution of $U_R(A)$.

LEMMA 3.2. *If S is a commutative associative R-algebra, then*

$$\begin{aligned}&[a^{\lambda}, b^{\rho}] \in Z[U_R(S)], \\ &[a^{\lambda}, b^{\rho}][a^{\lambda}, c^{\rho}] = 0\end{aligned} \tag{19}$$

for all $a, b, c \in S$.

Proof. Interchanging a and b in (3) and using the commutativity of S shows that $(ab)^{\lambda} - b^{\lambda}a^{\lambda} = [b^{\lambda}, a^{\rho}]$. Subtracting (3) from this gives

$$\begin{aligned}[a^{\lambda}, b^{\lambda}] &= [b^{\lambda}, a^{\rho}] - [a^{\lambda}, b^{\rho}] \\ &= -2[a^{\lambda}, b^{\rho}] \qquad \text{(by (7))}.\end{aligned} \tag{20}$$

Applying the canonical involution to (20) gives $[b^{\rho}, a^{\rho}] = -2[b^{\lambda}, a^{\rho}] = 2[a^{\lambda}, b^{\rho}]$, by (7). Together with (20), this yields

$$[a^{\lambda}, b^{\lambda}] = [a^{\rho}, b^{\rho}]. \tag{21}$$

Direct verification shows that

$$\begin{aligned}[[a^{\lambda}, b^{\lambda}], c^{\lambda}] &= (c^{\lambda} \circ b^{\lambda}) \circ a^{\lambda} - (c^{\lambda} \circ a^{\lambda}) \circ b^{\lambda} \\ &= 4[(cb)\,a - (ca)\,b]^{\lambda} \qquad \text{(by (6))} \\ &= 0.\end{aligned}$$

Together with (21), this gives

$$[[a^{\rho}, b^{\rho}], c^{\lambda}] = 0. \tag{22}$$

We have

$$[[a^\lambda, b^\rho], a^\rho] = [[a^\lambda, a^\rho], b^\rho] + [a^\lambda, [b^\rho, a^\rho]] \quad \text{(by (15))}$$
$$= 0 \quad \text{(by (5) and (22)).} \tag{23}$$

Applying the canonical involution to (23) gives

$$0 = [a^\lambda, [b^\lambda, a^\rho]]$$
$$= -[a^\lambda, [a^\lambda, b^\rho]] \quad \text{(by (7)).} \tag{24}$$

Then

$$(a^2b)^\lambda = (ab)^\lambda a^\lambda + [(ab)^\lambda, a^\rho] \quad \text{(by (3))}$$
$$= a^\lambda b^\lambda a^\lambda + [a^\lambda, b^\rho] a^\lambda + [a^\lambda b^\lambda + [a^\lambda, b^\rho], a^\rho] \quad \text{(by (3))}$$
$$= a^\lambda b^\lambda a^\lambda + a^\lambda [a^\lambda, b^\rho] + [a^\lambda b^\lambda, a^\rho] \quad \text{(by (23) and (24))}$$
$$= a^\lambda b^\lambda a^\lambda + a^\lambda [a^\lambda, b^\rho] + a^\lambda [b^\lambda, a^\rho] + [a^\lambda, a^\rho] b^\lambda \quad \text{(by (15))}$$
$$= a^\lambda b^\lambda a^\lambda \quad \text{(by (5) and (7)).} \tag{25}$$

Hence

$$(a^2bc)^\lambda = a^\lambda (bc)^\lambda a^\lambda \quad \text{(by (25))}$$
$$= a^\lambda b^\lambda c^\lambda a^\lambda + a^\lambda [b^\lambda, c^\rho] a^\lambda \quad \text{(by (3)).} \tag{26}$$

On the other hand,

$$(a^2bc)^\lambda = (a^2b)^\lambda c^\lambda + [(a^2b)^\lambda, c^\rho] \quad \text{(by (3))}$$
$$= a^\lambda b^\lambda a^\lambda c^\lambda + [a^\lambda b^\lambda a^\lambda, c^\rho] \quad \text{(by (25)).}$$

Subtracting (26) from this gives

$$0 = a^\lambda b^\lambda [a^\lambda, c^\lambda] - a^\lambda [b^\lambda, c^\rho] a^\lambda + [a^\lambda b^\lambda a^\lambda, c^\rho]$$
$$= -2a^\lambda b^\lambda [a^\lambda, c^\rho] - a^\lambda [b^\lambda, c^\rho] a^\lambda + [a^\lambda, c^\rho] b^\lambda a^\lambda$$
$$+ a^\lambda [b^\lambda, c^\rho] a^\lambda + a^\lambda b^\lambda [a^\lambda, c^\rho] \quad \text{(by (20) and (15))}$$
$$= -a^\lambda b^\lambda [a^\lambda, c^\rho] + [a^\lambda, c^\rho] b^\lambda a^\lambda$$
$$= [b^\lambda, a^\lambda][a^\lambda, c^\rho] - b^\lambda a^\lambda [a^\lambda, c^\rho] + [[a^\lambda, c^\rho], b^\lambda] a^\lambda$$
$$+ b^\lambda [a^\lambda, c^\rho] a^\lambda$$
$$= [b^\lambda, a^\lambda][a^\lambda, c^\rho] + [[a^\lambda, c^\rho], b^\lambda] a^\lambda \quad \text{(by (24)).} \tag{27}$$

Replacing a by $a+1$ in (27) gives

$$0 = [b^\lambda, a^\lambda + 1][a^\lambda + 1, c^\rho] + [[a^\lambda + 1, c^\rho], b^\lambda](a^\lambda + 1)$$
$$= [b^\lambda, a^\lambda][a^\lambda, c^\rho] + [[a^\lambda, c^\rho], b^\lambda](a^\lambda + 1).$$

Subtracting (27) from this gives

$$0 = [[a^\lambda, c^\rho], b^\lambda]. \tag{28}$$

Applying the canonical involution to (28) yields

$$0 = [b^\rho, [c^\lambda, a^\rho]]. \tag{29}$$

Equation (19) follows from (1), (28), and (29). Then

$$\begin{aligned}
[a^\lambda, b^\rho][a^\lambda, c^\rho] &= [[a^\lambda, b^\rho]\, a^\lambda, c^\rho] && \text{(by (19))}\\
&= [(ab)^\lambda\, a^\lambda - a^\lambda b^\lambda a^\lambda, c^\rho] && \text{(by (3))}\\
&= [(ab)^\lambda\, a^\lambda - (a^2 b)^\lambda, c^\rho] && \text{(by (25))}\\
&= [-[(ab)^\lambda, a^\rho], c^\rho] && \text{(by (3))}\\
&= 0 && \text{(by (19)).} \quad \blacksquare
\end{aligned}$$

LEMMA 3.3. *Let S be a commutative separable associative R-algebra, and let I be the ideal of $U_R(S)$ generated by $[S^\lambda, S^\rho]$. Then $U_R(S)/I$ is a commutative separable associative R-algebra, and there is an R-algebra isomorphism of $S \otimes_R S$ onto $U_R(S)/I$ taking $a \otimes b$ to $a^\lambda b^\rho + I$, $a, b \in S$.*

Proof. Let $a^{\lambda\prime}$ and $a^{\rho\prime}$ denote the images of a^λ and a^ρ in $U_R(S)/I$, $a \in S$. (3) and (4) imply that $a^{\lambda\prime}b^{\lambda\prime} = (ab)^{\lambda\prime}$ and $a^{\rho\prime}b^{\rho\prime} = (ab)^{\rho\prime}$, $a, b \in S$. Thus there is an R-algebra homomorphism ϕ from $S \otimes_R S$ to $U_R(S)/I$ taking $a \otimes b$ to $a^{\lambda\prime}b^{\rho\prime}$, $a, b \in S$, since $[S^{\lambda\prime}, S^{\rho\prime}] = 0$. Since (2), (3), and (4) hold in $S \otimes_R S$ if we replace each a^λ by $a \otimes 1$ and each a^ρ by $1 \otimes a$, $a \in S$, there is an R-algebra homomorphism from $U_R(S)$ to $S \otimes_R S$ taking $a^\lambda b^\rho$ to $a \otimes b$ [7, p. 88]. Since $S \otimes_R S$ is commutative, this induces an R-algebra homomorphism ψ from $U_R(S)/I$ to $S \otimes_R S$ taking $a^{\lambda\prime}b^{\rho\prime}$ to $a \otimes b$, $a, b \in S$. Equation (1) implies that ϕ and ψ are inverse isomorphisms. Since S is a commutative separable associative R-algebra, so is $S \otimes_R S$ [10, p. 12], and hence so is $U_R(S)/I$. $\blacksquare$

LEMMA 3.4. *Let S be a commutative separable associative R-algebra. If I is the ideal of S generated by $[S^\lambda, S^\rho]$, then $I = I^t$ for every positive integer t.*

Proof. We write $U_R(S)$ as U. Since U/I is commutative [Lemma 3.3],

$$[U, U] \subset I. \tag{30}$$

If $a, b \in S$ and $x, y \in U$,

$$\begin{aligned}[x, [a^\lambda, b^\rho]\, y] &= [a^\lambda, b^\rho][x, y] && \text{(by (19))} \\ &\subset I^2 && \text{(by (30)).}\end{aligned}$$

Then

$$[U, I] \subset I^2, \tag{31}$$

since (19) implies that I is spanned by elements of the form $[a^\lambda, b^\rho]\, y$.

Let $p: U \to U/I$ and $q: I \to I/I^2$ be the canonical maps. We can make I/I^2 a two-sided associative U/I-module by defining $(px)(qy) = q(xy)$ and $(qy)(px) = q(yx)$, $x \in U$, $y \in I$. Fix $z \in U$. Equations (30) and (31) imply that there is a well-defined map ϕ from U/I to I/I^2 such that $\phi(px) = q[z, x]$ for all $x \in U$. ϕ is a derivation of U/I into its two-sided module I/I^2, since

$$\begin{aligned}\phi((px)(py)) = \phi(p(xy)) &= q[z, xy] \\ &= q(x[z, y] + [z, x]\, y) && \text{(by (15))} \\ &= (px)(q[z, y]) + (q[z, x])(py) \\ &= (px)(\phi y) + (\phi x)(py)\end{aligned}$$

for $x, y \in U$. Since U/I is a separable associative R-algebra [Lemma 3.3], every derivation from U/I to a two-sided associative module is inner [10, p. 43]. The image of any inner derivation of U/I into I/I^2 is contained in

$$\begin{aligned}[U/I, I/I^2] = [pU, qI] &= q[U, I] \\ &\subset q(I^2) && \text{(by (31))} \\ &= 0.\end{aligned}$$

Hence $\phi = 0$. Then $[U, U] \subset I^2$, so $I \subset I^2$, and the lemma follows. ∎

LEMMA 3.5. *If S is a commutative separable associative R-algebra, then $U_R(S)$ is commutative.*

Proof. First assume that R is a field. Let F be the algebraic closure of R. $S \otimes_R F$ is spanned over F by orthogonal idempotents [A3], so the Peirce relations imply that $U_F(S \otimes_R F)$ is commutative [11, p. 34]. Since $U_F(S \otimes_R F)$ is isomorphic to $U_R(S) \otimes_R F$ [7, p. 88], $U_R(S)$ is commutative.

Now let R be arbitrary. Since S is a separable associative R-algebra, so is $S \otimes_R S$ [10, p. 12]. Let

$$\sum (w_i \otimes x_i) \otimes (y_i \otimes z_i)^o \in (S \otimes_R S) \otimes_R (S \otimes_R S)^o$$

be a separability idempotent for $S \otimes_R S$ as a separable associative R-algebra [A2]. Then

$$\sum w_i y_i \otimes x_i z_i = 1 \otimes 1 \in S \otimes_R S \tag{32}$$

and

$$0 = \sum (aw_i \otimes bx_i) \otimes (y_i \otimes z_i)^o - (w_i \otimes x_i) \otimes (y_i a \otimes z_i b)^o \tag{33}$$

for all $a, b \in S$.

Let $V = \{w_i, x_i, y_i, z_i\}$. Let K be the ideal of $U_R(S)$ generated by all $[a^\lambda, b^\rho]$, $a \in V$, $b \in S$. Write $U_R(S)/K$ as B. We claim that B is a separable associative R-algebra.

Let a^ℓ and a^r denote the images of a^λ and a^ρ in B. Equation (7) and the definition of B imply that

$$[a^\ell, b^r] = 0 = [b^\ell, a^r], \qquad a \in V, \quad b \in S. \tag{34}$$

Then (3) and (4) yield

$$a^\ell b^\ell = (ab)^\ell = b^\ell a^\ell, \qquad a \in V, \quad b \in S, \tag{35}$$

and

$$a^r b^r = (ab)^r = b^r a^r, \qquad a \in V, \quad b \in S, \tag{36}$$

since S is commutative. Let $\phi: S \otimes_R S \to B$ be the R-module homomorphism taking $a \otimes b$ to $a^\ell b^r$, $a, b \in S$. Let ϕ^o: $(S \otimes_R S)^o \to B^o$ take $(a \otimes b)^o$ to $(a^\ell b^r)^o$.

Set

$$f = \sum w_i^l x_i^r \otimes (y_i^l z_i^r)^o \in B \otimes_R B^o.$$

Let $\mu: B \otimes_R B^o \to B$ be the R-module homomorphism taking $a \otimes b^o$ to ab, $a, b \in B$. Then

$$\begin{aligned}
\mu f &= \sum w_i^\ell x_i^r\, y_i^\ell z_i^r \\
&= \sum w_i^\ell y_i^\ell x_i^r z_i^r && \text{(by (34))} \\
&= \sum (w_i y_i)^\ell (x_i z_i)^r && \text{(by (35) and (36))} \\
&= \phi\left(\sum w_i y_i \otimes x_i z_i\right) \\
&= \phi(1 \otimes 1) && \text{(by (32))} \\
&= 1. && (37)
\end{aligned}$$

If $a, b \in S$,

$$
\begin{aligned}
&(a^t b^* \otimes 1^\circ - 1 \otimes (a^t b^*)^\circ) f \\
&\quad = \sum a^t b^* w_i^t x_i^* \otimes (y_i^t z_i^*)^\circ - w_i^t x_i^* \otimes (y_i^t z_i^* a^t b^*)^\circ \\
&\quad = \sum a^t w_i^t b^* x_i^* \otimes (y_i^t z_i^*)^\circ - w_i^t x_i^* \otimes (y_i^t a^t z_i^* b^*)^\circ \qquad \text{(by (34))} \\
&\quad = \sum (aw_i)^t (bx_i)^* \otimes (y_i^t z_i^*)^\circ - w_i^t x_i^* \otimes ((y_i a)^t (z_i b)^*)^\circ \\
&\qquad \text{(by (35) and (36))} \\
&\quad = (\phi \otimes \phi^\circ)\left[\sum (aw_i \otimes bx_i) \otimes (y_i \otimes z_i)^\circ - (w_i \otimes x_i) \otimes (y_i a \otimes z_i b)^\circ\right] \\
&\quad = (\phi \otimes \phi^\circ)(0) \qquad \text{(by (33))} \\
&\quad = 0. \qquad (38)
\end{aligned}
$$

If we write $a_i^t b_i^*$ as c_i for $a_i, b_i \in S$, induction on n shows that

$$(c_1 \cdots c_n \otimes 1^\circ) f = (1 \otimes (c_1 \cdots c_n)^\circ) f: \qquad (39)$$

the case $n = 1$ is Eq. (38), and, if $n > 1$,

$$
\begin{aligned}
&(c_1 \cdots c_n \otimes 1^\circ) f \\
&\quad = (c_1 \cdots c_{n-1} \otimes 1^\circ)(c_n \otimes 1^\circ) f \\
&\quad = (c_1 \cdots c_{n-1} \otimes 1^\circ)(1 \otimes c_n^\circ) f \qquad \text{(by (38))} \\
&\quad = (c_1 \cdots c_{n-1} \otimes c_n^\circ) f \\
&\quad = (1 \otimes c_n^\circ)(c_1 \cdots c_{n-1} \otimes 1^\circ) f \\
&\quad = (1 \otimes c_n^\circ)(1 \otimes (c_1 \cdots c_{n-1})^\circ) f \qquad \text{(by induction)} \\
&\quad = (1 \otimes (c_1 \cdots c_n)^\circ) f.
\end{aligned}
$$

Equations (39) and (1) imply that $(x \otimes 1^\circ) f = (1 \otimes x^\circ) f$ for all $x \in B$. Together with (37), this shows that f is a separability idempotent in the associative sense for B, so B is a separable associative R-algebra [A2].

Write $Z(B)$ as Z, and let m be a maximal ideal of Z. $S \otimes_R Z/m$ is a separable associative Z/m-algebra [A5]. Thus the first paragraph of the proof shows that $U_{Z/m}(S \otimes_R Z/m)$ is commutative. $U_{Z/m}(S \otimes_R Z/m)$ is isomorphic to $U_R(S) \otimes_R Z/m$ [7, p. 88], and there is a homomorphism of the latter algebra onto $B \otimes_Z Z/m \cong B/mB$. Hence B/mB is commutative. The preceding paragraph shows that B is a separable associative R-algebra, so

the center of B/mB is the image of Z in B/mB [A5]. Thus $B = Z + mB$ for every maximal ideal m of Z. B is finitely spanned over Z, since B is a separable associative R-algebra [A7]. Hence Nakayama's Lemma yields $B = Z$ [M6], so B is commutative.

Let I be the ideal of $U_R(S)$ generated by all $[a^\lambda, b^\rho]$, $a, b \in S$. The preceding paragraph shows that $I \subset K$. If V has n elements, Lemma 3.2 implies that $K^{n+1} = 0$. Then Lemma 3.4 yields $I = I^{n+1} \subset K^{n+1} = 0$. Hence $U_R(S)$ is commutative, by Lemma 3.3. ∎

PROPOSITION 3.6. *Let S be a commutative associative R-algebra. Then S is separable as an alternative R-algebra if and only if S is separable as an associative R-algebra. If so, $U_R(S)$ is a commutative separable associative R-algebra, and there is an R-algebra isomorphism of $S \otimes_R S$ onto $U_R(S)$ taking $a \otimes b$ to $a^\lambda b^\rho$, $a, b \in S$.*

Proof. If S is separable as an alternative R-algebra, Lemma 3.1 shows that S is separable as an associative R-algebra. Conversely, if S is separable as an associative R-algebra, then $U_R(S)$ is commutative [Lemma 3.5]. It follows that $U_R(S)$ is a separable associative R-algebra isomorphic to $S \otimes_R S$ [Lemma 3.3], so S is separable as an alternative R-algebra. ∎

We remark that the results on Jordan algebras in [3] can be used to give a much shorter proof of Lemma 3.5 under the additional hypothesis that $\frac{1}{2} \in R$. To see this, let S be a commuative separable associative R-algebra, $\frac{1}{2} \in R$. Let $U_R^J(S)$ be the unital universal multiplication envelope of S considered as a Jordan algebra, and let τ be the canonical map from S to $U_R^J(S)$ [7, p. 103]. Let M be an alternative S-bimodule, so M is an associative $U_R(S)$-module. The split null extension $S \oplus M$ is an alternative algebra, so $(S \oplus M)^+$ is a Jordan algebra [7, pp. 15, 80]. Then M is a Jordan S-bimodule, so M is an associative $U_R^J(S)$-module such that $a^\tau x = \frac{1}{2}(a^\lambda + a^\rho)x$ for $a \in S$, $x \in M$. It is proved in [3, p. 349] that $U_R^J(S)$ is commutative. Thus, for any $a, b \in S$ and $x \in M$,

$$
\begin{aligned}
0 &= [a^\tau, b^\tau]x \\
&= \tfrac{1}{4}[a^\lambda + a^\rho, b^\lambda + b^\rho]x \\
&= \tfrac{1}{4}([a^\lambda, b^\lambda] + [a^\lambda, b^\rho] + [a^\rho, b^\lambda] + [a^\rho, b^\rho])x \\
&= \tfrac{1}{4}(-2[a^\lambda, b^\rho] + [a^\lambda, b^\rho] + [a^\lambda, b^\rho] - 2[a^\lambda, b^\rho])x \qquad \text{(by (7), (20), and (21))} \\
&= -\tfrac{1}{2}[a^\lambda, b^\rho]x.
\end{aligned}
$$

$U_R(S)$ is an associative $U_R(S)$-module via left multiplication, so it can be

considered an S-bimodule. Taking $x = 1 \in U_R(S)$ above shows that $[a^\lambda, b^\rho] = 0$ for all $a, b \in S$. Then $[a^\lambda, b^\lambda] = 0 = [a^\rho, b^\rho]$ by (20) and (21), so (1) implies that $U_R(S)$ is commutative.

4. Structure of Separable Algebras

We recall that A denotes an alternative R-algebra. We prove that A is separable over R if and only if A is the direct sum of a separable associative R-algebra and an algebra C octonion over $Z(C)$, where $Z(C)$ is a separable associative R-algebra. To prove this, we use Proposition 3.6 to reduce to the central separable case analyzed in Proposition 2.11.

Proposition 4.1. *If $Z(A)$ is a separable associative R-algebra, then $\langle Z(A)^\lambda, Z(A)^\rho \rangle$ is a separable associative R-algebra contained in the center of $U_R(A)$.*

Proof. We write $Z(A)$ as Z and $\langle Z^\lambda, Z^\rho \rangle$ as T. The inclusion $Z \subset A$ induces an R-algebra homomorphism from $U_R(Z)$ to $U_R(A)$ with image T [7, p. 88]. $U_R(Z)$ is a commutative separable associative R-algebra [Proposition 3.6], hence so is T [A5]. Let E denote the centralizer of T in $U_R(A)$. E is a subalgebra of $U_R(A)$, and E contains T since T is commutative. Since T is a separable associative R-algebra, every derivation of T into E is inner [10, p. 43]. Every inner derivation from T to E is zero, since T is in the center of E. Hence every derivation of T into E is zero.

Let $a \in A$, and let S be the subalgebra of A generated by a and Z. S is a commutative associative R-algebra, since A is power-associative [11, p. 29]. Hence Lemma 3.2 yields

$$[[a^{\gamma_1}, Z^{\gamma_2}], Z^{\gamma_3}] = 0, \tag{40}$$

$\gamma_i \in \{\lambda', \rho'\}$, where λ' and ρ' are the canonical maps from S to $U_R(S)$. The inclusion $S \subset A$ induces an algebra homomorphism from $U_R(S)$ to $U_R(A)$ [7, p. 88], so (40) holds for $\gamma_i \in \{\lambda, \rho\}$, where λ and ρ map A to $U_R(A)$. Thus $[a^{\gamma_1}, Z^{\gamma_2}] \subset E$ for $\gamma_i \in \{\lambda, \rho\}$. Hence (15) implies that $[a^\gamma, T] \subset E$ for $\gamma \in \{\lambda, \rho\}$, since $T = \langle Z^\lambda, Z^\rho \rangle$ is a subalgebra of E. Then $x \to [a^\gamma, x]$ is a derivation of T into E, so the preceding paragraph shows that $[a^\gamma, T] = 0$. Thus T is in the center of $U_R(A)$, by (1). ∎

The proof of Lemma 2.3 of [3] establishes:

Lemma 4.2. *Let S and T be commutative associative R-algebras. Let A be a separable S-algebra such that A is an R-algebra via $R1 \subset S$. Then $A \otimes_R T$ is either zero or separable over $S \otimes_R T$.*

We can use Lemmas 1.4, 1.8, and 4.2 to extend the proof of Lemma 2.4 of [3] to alternative algebras. This yields:

LEMMA 4.3. *Let S be a commutative separable associative algebra over a field R. Let A be a separable S-algebra such that A is an R-algebra via $R1 \subset S$. Then A is separable over R.*

PROPOSITION 4.4. *The following conditions are equivalent:*

(i) *A is separable over R.*

(ii) *A is separable over $Z(A)$ and $Z(A)$ is a separable associative R-algebra.*

Proof. Lemmas 1.7 and 3.1 show that (i) $\Rightarrow$ (ii). Conversely, assume that A satisfies (ii). Write $Z(A)$ as Z and $\langle Z^{\lambda}, Z^{\rho} \rangle$ as T, where $\lambda, \rho: A \to U_R(A)$. T is a commutative associative R-algebra [Proposition 4.1]. Let m be a maximal ideal of T. $A \otimes_R T/m$ is either zero or separable over $Z \otimes_R T/m$ [Lemma 4.2], and $Z \otimes_R T/m$ is zero or a separable associative T/m-algebra [A5]. Then $A \otimes_R T/m$ is zero or separable over T/m [Lemma 4.3], so $U_{T/m}(A \otimes_R T/m)$ is zero or a separable associative T/m-algebra. $U_{T/m}(A \otimes_R T/m)$ is isomorphic to $U_R(A) \otimes_R T/m$ [7, p. 88], so the latter is zero or separable over T/m. $U_R(A)$ is naturally a T-algebra, by Proposition 4.1. Thus there is a T/m-algebra homomorphism of $U_R(A) \otimes_R T/m$ onto

$$U_R(A) \otimes_T T/m \cong U_R(A)/mU_R(A).$$

Hence $U_R(A)/mU_R(A)$ is zero or a separable associative T/m-algebra [A5]. Then [A4] implies that $U_R(A)$ is a separable associative T-algebra, since $U_R(A)$ is finitely spanned over T by Lemmas 1.1 and 1.7 and Proposition 4.1. Since T is a separable associative R-algebra [Proposition 4.1] and $U_R(A)$ is separable over T, the transitivity of separability implies that $U_R(A)$ is a separable associative R-algebra [5, p. 46]. Thus A satisfies (i). ∎

THEOREM 4.5. *The following conditions on a nonassociative R-algebra B are equivalent:*

(i) *B is a separable alternative R-algebra.*

(ii) *B is the direct sum of ideals D and C such that D is a separable associative R-algebra, C is an octonion algebra over $Z(C)$, and $Z(C)$ is a separable associative R-algebra.*

Proof. First assume that B satisfies (i). B is central separable over $Z(B)$, and $Z(B)$ is a separable associative R-algebra [Proposition 4.4]. By

Proposition 2.11, B is the direct sum of ideals D and C such that D is a central separable associative $Z(D)$-algebra and C is an octonion algebra over $Z(C)$. Since $Z(B) = Z(D) \oplus Z(C)$ is a separable associative R-algebra, so are $Z(D)$ and $Z(C)$ [A5]. Then D is a separable associative R-algebra, since D is separable over $Z(D)$ and $Z(D)$ is separable over R [A1].

Conversely, let B satisfy (ii). Since D is a separable associative R-algebra, D is separable associative over $Z(D)$ and $Z(D)$ is separable associative over R [A1]. Proposition 2.11 shows that $B = D \oplus C$ is a central separable alternative algebra over $Z(B) = Z(D) \oplus Z(C)$. Since $Z(D)$ and $Z(C)$ are separable associative R-algebras, so is $Z(D) \oplus Z(C)$ [5, p. 77]. Hence B is a separable alternative R-algebra, by Proposition 4.4. ∎

Let B be a separable alternative R-algebra. We remark that the decomposition $B = D \oplus C$ described in Theorem 4.5(ii) is unique. To see this, let M be a maximal ideal of $Z(B)$. Since $Z(D)\,Z(C) = 0$, M contains either $Z(D)$ or $Z(C)$. If M contains $Z(D)$, then $B/MB \cong C/MC$ has dimension eight over $Z(C)/MZ(C)$. If M contains $Z(C)$, then $B/MB \cong D/MD$ is a central simple associative algebra over $Z(D)/MZ(D)$ [A5, A8], so its dimension is a perfect square. Since $B = \oplus B(i)$ where $B(i)$ has rank i over its center [Lemma 2.1], it follows that $D \equiv \oplus B(n^2)$ and $C \equiv B(8) \pmod{MB}$ for every maximal ideal M of $Z(B)$. Since B is finitely spanned over $Z(B)$ [Lemma 1.7], it follows as in [2, p. 126] that $D = \oplus B(n^2)$ and $C = B(8)$.

Combining Proposition 4.4 and Lemma 1.8 with the proofs of Theorems 3.1 and 3.2 of [3] yields the following two corollaries.

COROLLARY 4.6. *Let S be a commutative separable associative R-algebra, and let A be a separable alternative S-algebra such that A is an R-algebra via $R1 \subset S$. Then A is separable over R.*

COROLLARY 4.7. *Let $A = \oplus A_i$ be a finite direct sum of alternative R-algebras. Then A is separable over R if and only if each A_i is separable over R.*

COROLLARY 4.8. *If A is an associative R-algebra, the following conditions are equivalent:*

(i) *A is separable as an associative R-algebra, i.e., A is a projective $A \otimes_R A^0$-module.*

(ii) *A is separable as an alternative R-algebra, i.e., $U_R(A)$ is a separable associative R-algebra.*

(iii) *$A \otimes_R A^0$ is separable as an associative R-algebra.*

(iv) *A is a projective $U_R(A)$-module.*

(v) *There is an idempotent $e \in U_R(A)$ satisfying* (12).

Proof. Theorem 4.5 shows that (i) $\Rightarrow$ (ii).

(ii) $\Rightarrow$ (iii) Equations (2), (3), and (4) hold in $A \otimes_R A^\circ$ if we replace a^λ by $a \otimes 1^\circ$ and a^ρ by $1 \otimes a^\circ$ for all $a \in A$. Thus there is an R-algebra homomorphism of $U_R(A)$ onto $A \otimes_R A^\circ$ [7, p. 88]. Since $U_R(A)$ is a separable associative R-algebra, so is $A \otimes_R A^\circ$ [A5].

(iii) $\Rightarrow$ (i) First assume that A is finitely spanned and not separable over R. In this case there is a maximal ideal m of R such that, if F is the algebraic closure of R/m, then $A \otimes_{R/m} F$ conains a nonzero nilpotent ideal N [A4]. Then $N \otimes_F N^\circ$ is a nonzero nilpotent ideal of

$$\begin{aligned}(A/mA \otimes_{R/m} F) \otimes_F (A/mA \otimes_{R/m} F)^\circ \\ \cong A/mA \otimes_{R/m} (A/mA)^\circ \otimes_{R/m} F \\ \cong [(A \otimes_R A^\circ)/m(A \otimes_R A^\circ)] \otimes_{R/m} F,\end{aligned}$$

contradicting the fact that $A \otimes_R A^\circ$ is a separable associative R-algebra [A4].

Now let A be arbitrary. Write $Z(A \otimes_R A^\circ)$ as S. $A \otimes_R A^\circ$ acts on A via left and right multiplication. This induces an action of S on A which commutes with the action of $A \otimes_R A^\circ$. It follows that A is an S-algebra. Since $A \otimes_R A^\circ$ is a separable associative R-algebra, $A \otimes_R A^\circ$ is finitely spanned over S [A7]. Hence A is finitely spanned over S, since $A = (A \otimes_R A^\circ)\, 1$ for $1 \in A$. $A \otimes_S A^\circ$ is a homomorphic image of $A \otimes_R A^\circ \otimes_R S$, so $A \otimes_S A^\circ$ is a separable associative S-algebra [A5]. Thus the preceding paragraph shows that A is a separable associative S-algebra. Since $A \otimes_R A^\circ$ is a separable associative R-algebra, so is S [A1]. Then A is a separable associative R-algebra, since A is separable over S and S is separable over R [5, p. 46].

(ii) $\Rightarrow$ (iv) $\Leftrightarrow$ (v) These hold by the proofs of Propositions 1.2 and 1.4 of [2].

(v) $\Rightarrow$ (i) As in the proof of (ii) $\Rightarrow$ (iii), there is an R-algebra homomorphism ϕ of $U_R(A)$ onto $A \otimes_R A^\circ$ such that $\phi(a^\lambda) = a \otimes 1^\circ$ and $\phi(a^\rho) = 1 \otimes a^\circ$ for all $a \in A$. Equation (12) yields $(a \otimes 1^\circ)\, \phi e = \phi(a^\lambda e) = \phi(a^\rho e) = (1 \otimes a^\circ)\, \phi e$ for all $a \in A$. $va = (\phi v)\, a$ for all $v \in U_R(A)$ and $a \in A$, where $A \otimes_R A^\circ$ acts on A via left and right multiplication. Then $(\phi e)\, 1 = e1 = 1$ for $1 \in A$, by (12). Hence e is an associative separability idempotent for A, so A is a separable associative R-algebra [A2].

REFERENCES

1. M. F. ATIYAH AND I. G. MACDONALD, "Introduction to Commutative Algebra," Addison–Wesley, Reading, Mass., 1969.

2. R. BIX, Separable Jordan algebras over commutative rings, I, *J. Algebra* **57** (1979), 111–143.
3. R. BIX, Separable Jordan algebras over commutative rings, II, *J. Algebra* **79** (1982), 341–374.
4. R. BIX, Separable Jordan algebras over commutative rings, III, *J. Algebra* **86** (1984), 35–59.
5. F. DEMEYER AND E. INGRAHAM, "Separble Algebras over Commutative Rings," Lecture Notes in Mathematics No. 181, Springer-Verlag, New York/Berlin/Heidelberg, 1971.
6. J. GOLDHABER AND G. EHRLICH, "Algebra," Macmillan & Co., London, 1970.
7. N. JACOBSON, "Structure and Representations of Jordan Algebras," Colloquium Publications No. 39, Amer. Math. Soc., Providence, R. I., 1968.
8. K. MCCRIMMON, Manuscript on alternative algebras.
9. G. N. MÜLLER, Nicht assoziative separable Algebren über Ringen, *Abh. Math. Sem. Univ. Hamburg* **40** (1974), 115–131.
10. M. ORZECH AND C. SMALL, "The Brauer Group of Commutative Rings," Lecture Notes in Pure and Applied Mathematics No. 11, Dekker, New York, 1975.
11. R. SCHAFER, "An Introduction to Nonassociative Algebras," Academic Press, New York, 1966.
12. R. WISBAUER, Radikale von separablen Algebren über Ringen, *Math. Z.* **139** (1974), 9–13.