JOURNAL OF ALGEBRA 57, 111–143 (1979)

Separable Jordan Algebras over Commutative Rings. I.

ROBERT BIX*

University of Michigan–Flint, Flint, Michigan 48503

Submitted by Nathan Jacobson

Received August 24, 1977

This paper presents a theory of separable Jordan algebras over commutative rings. We define a Jordan algebra over a commutative ring with $\frac{1}{2}$ to be separable if its unital universal multiplication algebra is a separable associative algebra.

In Section 1 we develop the basic properties of separable Jordan algebras over commutative rings. In Section 2 we prove that a central separable R-algebra J is an R-progenerator and that there is a one-to-one correspondence between the ideals of J and the ideals of R.

The rest of the paper centers around the decomposition theorem of Section 6, that a separable Jordan algebra is a direct sum of homogenous components corresponding to the isomorphism classes of finite-dimensional simple Jordan algebras over an algebraically closed field. In Section 3, we obtain analogous decompositions for separable associative algebras and separable associative algebras with involution. In Sections 7 and 8 we apply the decomposition theorems to study the structure of central separable Jordan algebras and their universal envelopes. In particular, we relate the decompositions of separable Jordan algebras and separable associative algebras with involution.

More precisely, the decomposition theorem states that a separable Jordan R-algebra J can be written $J = J_1 \oplus \cdots \oplus J_s$ for distinct ordered pairs $(p_1, q_1), \ldots, (p_s, q_s)$ such that, if m is a maximal ideal of R and F is the algebraic closure of R/m, then $(J_i/mJ_i) \otimes_{R/m} F$ is a direct sum of simple F-algebras of degree p_i and dimension q_i. We note that the isomorphism class of a finite-dimensional simple algebra over an algebraically closed field is determined by its degree and dimension.

The key fact needed to prove the decomposition theorem is that, if J is separable with center $Z(J)$, its special universal envelope $S_{Z(J)}(J)$ is finitely spanned $Z(J)$-projective along with J. This implies that $Z(J)$ is the direct sum of ideals C_i such that C_iJ and $S_{C_i}(C_iJ)$ have constant rank over C_i. On the other hand,

* Portions of the results presented here are contained in the author's doctoral dissertation, written at Yale University under the direction of Professor N. Jacobson. The author would like to express his gratitude to Professor Jacobson for his guidance and encouragement.

0021-8693/79/030111–33$02.00/0

the degree and dimension of a finite-dimensional simple Jordan algebra K over an algebraically closed field F are determined by $\dim_F K$ and $\dim_F S_F(K)$. It follows that the $C_i J$ are the desired components of J.

In Section 5 we prove that $S_R(J)$ is R-projective when J is R-central separable. We reduce to the case where (R, m) is complete local Noetherian and J/mJ is a reduced R/m-algebra. In Section 4 we classify such J's and construct the corresponding $S_R(J)$'s, showing that they are free R-modules.

In a subsequent article we will apply the decomposition theorem to prove that each component of a central separable algebra has a generic minimum polynomial with the standard properties. Results of Harris and McCrimmon on derivations and centralizers and results of Jacobson on structure groups and Lie algebras will be extended to separable algebras over commutative rings. We will establish special cases of Wedderburn–Malcev decompositions over commutative rings. Finally we will present an analogous theory of separable alternative algebras.

In [10], Müller defined an arbitrary nonassociative algebra A over a commutative ring R to be separable if its multiplication algebra is a separable associative R-algebra. To ensure the functoriality of this definition, he had to assume that A is finitely spanned R-projective and a progenerator over its center. Under these assumptions he established our Proposition 1.7 (without the results on the centers), Theorem 1.8, and one direction of Theorem 2.5, for arbitrary nonassociative algebras. This point of view was continued by Wisbauer [13], who established parts of Corollaries 2.6 and 2.7 for arbitrary nonassociative algebras under the same assumptions.

0. Preliminaries

In this section we establish notation and list certain assumed results about Jordan and separable associative algebras for later reference.

All algebras in this paper are defined over commutative rings containing $\frac{1}{2}$. All commutative rings, algebras, subalgebras, bimodules, and homomorphisms are assumed to be unital.

Throughout this paper, let J be a Jordan algebra and R a commutative ring. Let $Z(J)$ be the center of J.

Let $M_n(D)$ be the associative algebra of $n \times n$ matrices over D. If (A, j) is an associative algebra with involution, let $H(A, j)$ be the Jordan algebra of j-symmetric elements of A. Let $H(M_n(C), j)$ be the Jordan algebra of j-symmetric $n \times n$ matrices over a composition algebra C, where j is the "standard involution" conjugate transpose and C is associative if $n \geqslant 3$ [3, p. 127].

For $a, b, c \in J$, let $[a, b, c] = (a \cdot b) \cdot c - a \cdot (b \cdot c)$. Let $[J, J, J] = \{\sum [a_i, b_i, c_i] \mid a_i, b_i, c_i \in J\}$.

The basic results on Jordan algebras over fields of characteristic $\neq 2$ presented in [3] immediately extend to Jordan algebras over commutative rings containing $\frac{1}{2}$. We will use such results without further comment. In particular, we use the definitions and basic properties of Jordan algebras, invertible elements, associative specializations and special universal envelopes, and Peirce decompositions [3, Chapters I.1, I.7, I.11, I.12, II.1–II.3, II.9–II.11, and III.1].

Let $S_R(J)$ be the *unital* special universal envelope of J as an R-algebra and let $\sigma: J \to S_R(J)$ be the natural map. Let $U_R(J)$ be the *unital* universal multiplication envelope of J as an R-algebra and let $\rho: J \to U_R(J)$ be the natural map. An R-module M is a J-bimodule if and only if M is a module for the associative R-algebra $U_R(J)$ and the action of J on M is given by $az = a^\rho z$, for $a \in J$ and $z \in M$.

We list the basic properties of universal envelopes for later reference.

J1. $U_T(J \otimes_R T) \cong U_R(J) \otimes_R T$ and $S_T(J \otimes_R T) \cong S_R(J) \otimes_R T$ for a commutative R-algebra T [3, pp. 66 and 88].

J2. $U_{R/I}(J/IJ) \cong U_R(J)/IU_R(J)$ and $S_{R/I}(J/IJ) \cong S_R(J)/IS_R(J)$ for an ideal I of R [J1].

J3. An R-algebra homomorphism $\phi: J \to J'$ induces algebra homomorphisms $U_R(J) \to U_R(J')$ and $S_R(J) \to S_R(J')$ which are surjective if ϕ is [3, pp. 65 and 88].

J4. If $N \subset J$ is an ideal, $U_R(J/N) \cong U_R(J)/\langle N^\rho \rangle$ and $S_R(J/N) \cong S_R(J)/\langle N^\sigma \rangle$, where $\langle K \rangle$ denotes the ideal generated by K [3, pp. 66 and 88].

J5. $U_R(\oplus J_i) \cong \oplus U_R(J_i) \quad \oplus_{i<j} [S_R(J_i) \otimes_R S_R(J_j)]$ and $S_R(\oplus J_i) \cong \oplus S_R(J_i)$ [3, pp. 73 and 105].

J6. If J is a finitely spanned R-module, so are $U_R(J)$ and $S_R(J)$ [3, pp. 66 and 97].

J7. Let J be finite-dimensional over a field F. Then J is separable (in the classical sense) if and only if $U_F(J)$ is. If J is separable, then $S_F(J)$ is, and the converse holds if J is special [3, p. 286].

Next we list several definitions and basic facts about modules over commutative rings.

M1. An R-module M is called an *R-progenerator* if it is finitely spanned, projective, and faithful.

M2. If M is finitely spanned and projective over a local ring (R, m), then M is a free R-module. In fact, if $\{x_1 + mM, \ldots, x_t + mM\}$ is a vector space basis for M/mM over R/m, then $\{x_1, \ldots, x_t\}$ is a free basis for M over R [2, p. 24]. Thus a direct summand of M, being projective, is free.

M3. A finitely spanned, projective R-module M is said to have rank d if $M \otimes_R R_p$ is a free R_p-module of rank d for every prime p of R, where R_p is the localization of R at p. If S is a commutative R-algebra and M has rank d over R, then $M \otimes_R S$ has rank d over S [2, p. 27].

M4. If M is finitely spanned R-projective, we can write R as a direct sum of ideals R_i such that R_iM has rank t_i over R_i for distinct integers t_i [5, p. 23].

M5. Let M be finitely spanned R-projective and let $f: M \times M \to R$ be a symmetric bilinear form. f is called nondegenerate if it satisfies the following equivalent conditions [1]:

(1) f induces an isomorphism of M onto $\mathrm{Hom}_R(M, R)$ by $x \to f(x, (\ ))$.

(2) $M \otimes_R M \cong \mathrm{Hom}_R(M, M)$ by $y \otimes z \to f_{y,z}$, where $f_{y,z}(x) = f(x, y)z$ for $x, y, z \in M$.

(3) f induces a nondegenerate symmetric bilinear form from M/mM to R/m for every maximal ideal m of R.

M6. (Nakayama's Lemma) If $N \subset M$ are R-modules, M finitely spanned, and $M = N + mM$ for every maximal ideal m of R, then $M = N$ [2, p. 7].

M7. Let $f: M \to N$ be an R-module homomorphism, where M is finitely spanned and N is finitely spanned, R-projective. If f induces an isomorphism $M/mM \to N/mN$ for every maximal ideal m of R, then f is an isomorphism. (Apply [M6] as in [12, p. 5].)

Finally, we list the basic properties of separable associative algebras over commutative rings for later use and for comparison with the Jordan case. Let A be an associative algebra and let $Z(A)$ be the center of A. Let A^o be the opposite algebra with multiplication $a^o b^o = (ba)^o$ for $a, b \in A$. A is an $A \otimes_R A^o$-module via left and right multiplication.

A1. An R-algebra A is called R-separable if A is a projective $A \otimes_R A^o$-module. A separable R-algebra A is called central separable if $R \cong Z(A)$ by $r \to r1$. A is R-separable if and only if A is $Z(A)$-separable and $Z(A)$ is R-separable [2, p. 46].

A2. An R-algebra A is R-separable if and only if there exists $e \in A \otimes_R A^o$ such that $e(1) = 1$ for $1 \in A$ and $(a \otimes 1^o - 1 \otimes a^o)e = 0$ for all $a \in A$. e is necessarily an idempotent and is called a separability idempotent for A [2, p. 40].

A3. An algebra A over a field F is called classically separable if A is finite dimensional and remains semisimple under arbitrary field extensions. An F-algebra A is F-separable if and only if it is classically separable [2, p. 50].

A4. A finitely spanned R-algebra A is R-separable if and only if A/mA is either zero or classically separable for every maximal ideal m of R [2, p. 72].

A5. Let A be R-separable. If T is a commutative R-algebra, then $A \otimes_R T$ is T-separable and $Z(A \otimes_R T) \cong Z(A) \otimes_R T$. If $\phi: A \to A'$ is an R-algebra homomorphism, then $\phi(A)$ is R-separable and $Z[\phi(A)] = \phi[Z(A)]$. $A \otimes_R A^o$ is also R-separable [2, pp. 42–44].

A6. Let A be R-separable. A short exact sequence of A-modules split over R is split over A. An A-module which is R-projective is A-projective [2, p. 48, proof of Proposition 2.3].

A7. A central separable R-algebra is an R-progenerator containing R as an R-direct summand [2, pp. 51–52].

A8. If A is R-central separable, there is a one-to-one correspondence between the ideals I of A and the ideals α of R by $I \to I \cap R$ and $\alpha \to \alpha A$ [2, p. 54].

A9. If A is R-central separable and M is a two-sided A/R-module, then $M \cong A \otimes_R M^A$, where $M^A = \{x \in M \mid ax = xa \text{ for all } a \in A\}$ [2, p. 54].

A10. If M is an R-progenerator, $\mathrm{End}_R(M) \equiv \mathrm{Hom}_R(M, M)$ is a central separable R-algebra [2, p. 56].

A11. An R-algebra A is R-central separable if and only if A is an R-progenerator and $A \otimes_R A^o \cong \mathrm{End}_R(A)$ via left and right multiplication [2, p. 52].

1. Basic Properties of Separable Algebras

In this section we present the basic properties of separable Jordan algebras over commutative rings. These parallel the properties of separable associative algebras. Specifically, we define a Jordan algebra J to be R-separable if $U_R(J)$ is a separable associative R-algebra. This definition is functorial. If J is finitely spanned and special, J is R-separable if and only if J is a projective $U_R(J)$-module. A finitely spanned R-algebra J is separable if and only if J/mJ is separable in the classical sense over R/m for every maximal ideal m of R. If A is a finitely spanned, separable associative algebra, then A^+ is a separable Jordan algebra; moreover, if A has an involution j, $H(A, j)$ is a separable Jordan algebra. A key result for our work is that, if J is R-separable, then $U_R(J)$ contains an idempotent which ensures that $Z(J)$ is functorial.

Definition 1.1. An R-algebra J is called *R-separable* if $U_R(J)$ is a separable associative R-algebra. J is called *R-central separable* if J is R-separable and the map $r \to r1$ is an isomorphism of R onto $Z(J)$.

An R-algebra J is spanned as a $U_R(J)$-module by $1 \in J$. Thus there is an exact sequence of $U_R(J)$-homomorphisms μ: $U_R(J) \to J \to 0$, where $\mu(b) = b(1)$ for $b \in U_R(J)$.

Proposition 1.2. *If J is R-separable, the exact sequence of $U_R(J)$-homomorphisms μ: $U_R(J) \to J \to 0$ splits.*

Proof. The canonical map ρ: $J \to U_R(J)$ splits μ in the category of R-modules (since $a = a^\rho 1$, $a \in J$). Then μ splits in the category of $U_R(J)$-modules, since $U_R(J)$ is a separable associative R-algebra [A6].

For a J-bimodule M, set $M^J = \{z \in M \mid (a \cdot b)z = a(bz),\ a, b \in J\}$. Equivalently, $M^J = \{z \in M \mid uz = (u1)z,\ u \in U_R(J)\}$, where $u1$ denotes u applied to

$1 \in J$. Also, M^J is the intersection of M and the center of the split null extension $J \oplus M$ [3, p. 79]. In particular, $J^J = Z(J)$. Clearly, any homomorphism $M \to M'$ of J-bimodules induces a homomorphism $M^J \to M'^J$ of R-modules. Thus $M \to M^J$ defines a functor from the category of J-bimodules to the category of R-modules.

DEFINITION 1.3. $e \in U_R(J)$ is called a *separability idempotent* for an R-algebra J if $e \in U_R(J)^J$ and $e(1) = 1$, $1 \in J$.

PROPOSITION 1.4. *The following conditions on an R-algebra J are equivalent:*

(1) *J is a projective $U_R(J)$-module.*

(2) *The exact sequence of $U_R(J)$-homomorphisms μ: $U_R(J) \to J \to 0$ splits.*

(3) *J has a separability idempotent e. e is necessarily an idempotent and $eM = M^J$ for every J-bimodule M. In particular, $eJ = Z(J)$.*

(4) *Every exact sequence of J-bimodules $M \to N \to 0$ induces an exact sequence of R-modules $M^J \to N^J \to 0$.*

Proof. (1) $\Leftrightarrow$ (2) is clear. (2) $\Rightarrow$ (3). Let ψ: $J \to U_R(J)$ be a $U_R(J)$-homomorphism splitting μ. Set $e = \psi(1)$. Since $1 \in J^J$, $e = \psi(1) \in U_R(J)^J$. $e(1) = \mu(e) = 1$, so e is a separability idempotent for J. Now let e be any separability idempotent for J. Since $e \in U_R(J)^J$, $ue = (u1)^\rho e$ for $u \in U_R(J)$. In particular, $e^2 = (e1)^\rho e = 1^\rho e = e$, so e is an idempotent. Let M be a J-bimodule and let $z \in M$. The relation $a^\rho b^\rho e = (a \cdot b)^\rho e$ in $U_R(J)$, $a, b \in J$, implies that $a^\rho(b^\rho(ez)) = (a^\rho b^\rho e)z = ((a \cdot b)^\rho e)z = (a \cdot b)^\rho(ez)$. Thus $eM \subset M^J$. Conversely, let $z \in M^J$. Then $ez = (e1)^\rho z = 1^\rho z = z$. Hence $eM = M^J$. In particular, $eJ = J^J = Z(J)$. (3) $\Rightarrow$ (2). If e is a separability idempotent for J, define ψ: $J \to U_R(J)$ by $\psi(a) = a^\rho e$. Then ψ is a $U_R(J)$-homomorphism, since $a^\rho\psi(b) = a^\rho b^\rho e = (a \cdot b)^\rho e = \psi(a^\rho b)$ for $a, b \in J$. Moreover, ψ splits μ, since $\mu[\psi(a)] = [\psi(a)]1 = (a^\rho e)1 = a^\rho 1 = a$. (3) $\Rightarrow$ (4). If $M \to N \to 0$ is exact, then so is $eM \to eN \to 0$. Thus $M^J \to N^J \to 0$ is exact, by (3). (4) $\Rightarrow$ (3). In the exact sequence of $U_R(J)$-modules μ: $U_R(J) \to J \to 0$, choose a preimage $e \in U_R(J)^J$ of $1 \in J^J$, by (4).

By Proposition 1.2, a separable R-algebra J satisfies the equivalent conditions of Proposition 1.4. In particular, it has a separability idempotent. In Theorem 1.12 we prove that the conditions of Proposition 1.4 are equivalent to R-separability if J is finitely spanned and special. We remark that the condition that J is $U_R(J)$-projective is the exact analogue of the definition that an associative algebra A is R-separable if it is $A \otimes_R A^o$-projective, since $U_R(A) \cong A \otimes_R A^o$ for the variety of associative R-algebras [3, p. 85].

In general, a separable Jordan algebra has many separability idempotents. In fact, if $e \in U_R(J)$ is a separability idempotent for J and $g \in U_R(J)$ satisfies $g(1) = 1$ for $1 \in J$, then eg is also a separability idempotent for J.

As examples of separability idempotents, consider $J = H(M_n(F), j)$, F a field and $n \geqslant 3$. We claim that

$$e = \left\{-(n-2)e_{11}^{\rho} + 2 \sum_{i \neq 1} [(e_{i1} + e_{1i})^{\rho}]^2\right\} [2e_{11}^{\rho}e_{11}^{\rho} - e_{11}^{\rho}]$$

is a separability idempotent for J. In fact, every J-bimodule is completely reducible and every irreducible J-bimodule is isomorphic to a subbimodule of $M_n(F)$, where J acts on $M_n(F)$ by $a^{\rho}x = \frac{1}{2}(ax + xa)$, $a \in J$ and $x \in M_n(F)$ [3, pp. 272–284]. Under this action, $e(e_{11}) = e_{11} + \cdots + e_{nn}$ and $e(e_{ij}) = 0$ for $(i, j) \neq (1, 1)$. Then $e(1) = 1$ for $1 \in J$ and $eM \subset M^J$ for every J-bimodule M. Thus $a^{\rho}b^{\rho}e = (a \cdot b)^{\rho}e$ for $a, b \in J$, so e is a separability idempotent for J. The corresponding definition of e also works for $J = M_n(F)^+$, $n \geqslant 3$, and $J = H(M_3(O), j)$ for an octonion algebra O over a field.

LEMMA 1.5. *If J is R-separable, $Z(J)$ is a $Z(J)$-direct summand of J.*

Proof. Let $e \in U_R(J)$ be an separability idempotent for J. Then $eJ = Z(J)$, and $J = eJ \oplus (1 - e)J$ is a direct decomposition of J as a $Z(J)$-module since the actions of $Z(J)$ and $U_R(J)$ on J commute.

We call a Jordan or associative algebra over a field *classically separable* if it is finite-dimensional and remains semisimple under arbitrary field extensions.

PROPOSITION 1.6. *Let J be an algebra over a field F. Then J is F-separable if and only if J is classically separable.*

Proof. If J is finite-dimensional over F, so is $U_F(J)$ [J6]. The converse holds since $J = U_F(J)1$. By definition, J is F-separable if and only if $U_F(J)$ is a separable associative F-algebra. This holds if and only if $U_F(J)$ is classically separable [A3]. And $U_F(J)$ is classically separable if and only if J is classically separable, by [J7] and the fact that J is finite-dimensional if and only if $U_F(J)$ is.

We note that we have assumed $\frac{1}{2} \in R$, avoiding the quadratic theory of McCrimmon, to ensure that J classically separable over a field F implies that $U_F(J)$ is classically separable. Counterexamples to this result in characteristic two appear in [4, pp. 42–44]. In [7], Loos studies separable Jordan algebras and Jordan pairs without assuming that $\frac{1}{2} \in R$, by using schemes. He extends Theorem 6.3 to these cases.

PROPOSITION 1.7. *Let J be R-separable with separability idempotent e.*

(1) *Let S be a commutative R-algebra. Then $J \otimes_R S$ is either zero or S-separable with separability idempotent $e \otimes 1 \in U_R(J) \otimes S \simeq U_S(J \otimes S)$. Also $Z(J) \otimes S \simeq Z(J \otimes S)$ under the natural map.*

(2) *If I is an ideal of R, J/IJ is either zero or R/I-separable. Also*

$$Z(J)/IZ(J) \simeq Z(J/IJ).$$

(3) *Let ϕ be a homomorphism of J onto an R-algebra J'. Then J' is R-separable and $Z(J') = \phi[Z(J)]$. J' has separability idempotent $\psi(e)$, where ψ: $U_R(J) \to U_R(J')$ is the homomorphism induced by ϕ.*

(4) *Let S be a commutative R-algebra and let J be an S-algebra. Consider J as an R-algebra via $R1 \subset S$. If J is R-separable, then J is S-separable. In particular, a separable R-algebra J is $Z(J)$-separable, so any separable algebra can be considered as a central separable algebra.*

Proof. (1). Assume that $J \otimes S \neq 0$, so $U_S(J \otimes S) \cong U_R(J) \otimes S \neq 0$ [J1]. Since $U_R(J)$ is a separable associative R-algebra, $U_R(J) \otimes S$ is a separable associative S-algebra [A5]. Thus $J \otimes S$ is S-separable. $e \otimes 1$ is clearly a separability idempotent for $J \otimes S$. Then $Z(J \otimes S) = (e \otimes 1)(J \otimes S)$ is the image in $J \otimes S$ of $(eJ) \otimes S = Z(J) \otimes S$. Moreover, the map from $Z(J) \otimes S$ to $J \otimes S$ is injective, since $Z(J)$ is an R-direct summand of J [Lemma 1.5]. (2) follows from (1). (3) ϕ induces a homomorphism ψ of $U_R(J)$ onto $U_R(J')$ [J3]. Then $U_R(J')$ is a separable associative R-algebra [A5], so J' is R-separable. $\psi(e)$ is clearly a separability idempotent for J', so $Z(J') = \psi(e)J' = \phi(eJ) = \phi[Z(J)]$. (4) Since $U_S(J)$ is a homomorphic image of $U_R(J) \otimes S$, $U_S(J)$ is a separable associative S-algebra, so J is S-separable.

THEOREM 1.8. *Let J be a finitely spanned R-algebra. J is R-separable if and only if J/mJ is either zero or classically R/m-separable for every maximal ideal m of R. J is central separable over $R1$ $(1 \in J)$ if and only if J/mJ is either zero or R/m-central simple for every maximal ideal m of R.*

Proof. By definition, J is R-separable if and only if $U_R(J)$ is a separable associative R-algebra. Since $U_R(J)$ is finitely spanned, this holds if and only if $U_R(J)/mU_R(J)$ is either zero or R/m-separable for every maximal ideal m of R [J6, A4]. Since $U_R(J)/mU_R(J) \cong U_{R/m}(J/mJ)$, this holds if and only if J/mJ is either zero or classically R/m-separable for every maximal ideal m of R [J2, Proposition 1.6].

If J is R-separable and $Z(J) = R1$, J/mJ is either zero or R/m-central separable [Proposition 1.7(2)]. In the latter case, J/mJ is simple, since it is classically separable and its center is a field. Conversely, assume that J/mJ is either zero or R/m-central simple for every maximal ideal m of R. J is R-separable as above, and $Z(J) \subset R1 + mJ$. Then $Z(J) = R1 + mZ(J)$ and $Z(J)$ is finitely spanned over R, since $Z(J)$ is an R-direct summand of J [Lemma 1.5]. Hence $Z(J) = R1$ [M6].

COROLLARY 1.9. *If J is finitely spanned R-separable, then $S_R(J)$ is a separable associative R-algebra.*

Proof. For every maximal ideal m of R, J/mJ is either zero or classically separable [Theorem 1.8]. Then $S_{R/m}(J/mJ) \cong S_R(J)/mS_R(J)$ is either zero or classically separable [J2, J7]. Since $S_R(J)$ is finitely spanned, $S_R(J)$ is a separable associative R-algebra [J6, A3].

EXAMPLE 1.10. (1) Let A be a finitely spanned, separable associative R-algebra. Then A^+ is R-separable and $Z(A) = Z(A^+)$.

(2) Let A be a separable associative R-algebra with involution j. Then $H(A, j)$ is R-separable and $Z[H(A, j)] = Z(A) \cap H(A, j)$.

Proof. We can assume that R is a field, by Theorem 1.8. By field extension, we can assume that R is algebraically closed, whence the result is clear.

The next example follows from Theorem 1.8, [M5], and the corresponding statement over fields [3, p. 179].

EXAMPLE 1.11. Let M be a finitely generated, projective R-module and let $J = R \oplus M$ be the Jordan algebra determined by a symmetric bilinear form f on M. Then J is R-separable if and only if f is nondegenerate. Moreover, in this case, J is R-central if and only if $\operatorname{rank}_p M \geqslant 2$ for all primes p of R.

We remark that, if J is R-separable, so is any isotope $J^{(c)}$, since $U_R(J) \simeq U_R(J^{(c)})$ [3, p. 106].

THEOREM 1.12. *Let J be a finitely spanned and special R-algebra. Then J is R-separable if and only if J satisfies the equivalent conditions of Proposition* 1.4.

Proof. We must prove that J is R-separable if it contains a separability idempotent e. Define τ, τ': $J \to S_R(J) \otimes S_R(J)^o$ by $\tau(a) = a^\sigma \otimes 1^o$ and $\tau'(a) = 1 \otimes a^{\sigma o}$, $a \in J$. τ and τ' are commuting associative specializations of J in $S_R(J) \otimes S_R(J)^o$, so $\frac{1}{2}(\tau + \tau')$ is a multiplicative specialization [3, p. 99]. Then there is a homomorphism ϕ: $U_R(J) \to S_R(J) \otimes S_R(J)^o$ such that $\phi(a^\rho) = \frac{1}{2}(a^\sigma \otimes 1^o + 1 \otimes a^{\sigma o})$, $a \in J$. Let $f = \phi(e)$, so $f \in S_R(J) \otimes S_R(J)^o$ is an idempotent. For $a, x \in J$, $(a \cdot x)^\sigma = \frac{1}{2}(a^\sigma x^\sigma + x^\sigma a^\sigma) = \phi(a^\rho)x^\sigma$, where $\phi(a^\rho) \in S_R(J) \otimes S_R(J)^o$ acts on $S_R(J)$ by left and right multiplication. It follows that $(b(x))^\sigma = \phi(b)x^\sigma$ for $b \in U_R(J)$ and $x \in J$. Thus $f(1^\sigma) = \phi(e)(1^\sigma) = (e(1))^\sigma = 1^\sigma$.

Apply ϕ to the equation $a^\rho b^\rho e = (a \cdot b)^\rho e = b^\rho a^\rho e$, for $a, b \in J$. This gives $[a^\sigma b^\sigma \otimes 1^o + a^\sigma \otimes b^{\sigma o} + b^\sigma \otimes a^{\sigma o} + 1 \otimes (b^\sigma a^\sigma)^o]f = [a^\sigma b^\sigma \otimes 1^o + b^\sigma a^\sigma \otimes 1^o + 1 \otimes (a^\sigma b^\sigma)^o + 1 \otimes (b^\sigma a^\sigma)^o]f = [b^\sigma a^\sigma \otimes 1^o + a^\sigma \otimes b^{\sigma o} + b^\sigma \otimes a^{\sigma o} + 1 \otimes (a^\sigma b^\sigma)^o]f$. Equating the first and last expressions yields

$$([a^\sigma, b^\sigma] \otimes 1^o - 1 \otimes [a^\sigma, b^\sigma]^o)f = 0, \, a, b \in J, \tag{*}$$

where $[a^\sigma, b^\sigma] = a^\sigma b^\sigma - b^\sigma a^\sigma$. Equating the first and second expressions and setting $a = b$ yields

$$(a^\sigma \otimes 1^o - 1 \otimes a^{\sigma o})^2 f = 0, \qquad a \in J. \tag{**}$$

Let m be a maximal ideal of R and let F be an algebraic closure of R/m. It suffices to prove that $J/mJ \otimes F$ is semisimple [Theorem 1.8]. Suppose not, so $N = \text{rad}\,(J/mJ \otimes F) \neq 0$. By the Albert–Penico–Taft theorem, $J/mJ \otimes F$ contains a semisimple subalgebra K such that $J/mJ \otimes F \simeq K \oplus N$ as vector spaces [3, p. 292]. Since N is a nonzero solvable ideal, it contains an ideal $N^{(2)}$ such that $N/N^{(2)} \neq 0$ and $[N/N^{(2)}]^2 = 0$ [3, p. 192]. Then $K \oplus N/N^{(2)}$ is a finite-dimensional split null extension [3, p. 91].

The image e' of e in $[U_R(J) \otimes_R R/m] \otimes_{R/m} F \cong U_F(J/mJ \otimes_{R/m} F)$ is a separability idempotent for $J/mJ \otimes F$. Since $K \oplus N/N^{(2)}$ is a homomorphic image of $K \oplus N \simeq J/mJ \otimes F$, the image of e' in $U_F(K \oplus N/N^{(2)})$ is a separability idempotent for $K \oplus N/N^{(2)}$.

We claim that the split null extension $K \oplus N/N^{(2)}$ is special. If K is not special, it contains an ideal isomorphic to $H(M_3(O), j)$ for an octonion algebra O [3, p. 204], so K does not satisfy Glennie's identity [3, pp. 49–51]. This contradicts the fact that J satisfies Glennie's identity since it is special. Thus K is special. Write $K = \oplus K_i$, K_i simple, and let $N/N^{(2)} = \oplus_{j \leqslant k}(N/N^{(2)})_{j,k}$ be the corresponding Peirce decomposition. The subalgebra $K \oplus_{j<k}(N/N^{(2)})_{j,k}$ is special [3, p. 105]. We apply the representation theory of finite-dimensional simple algebras over an algebraically closed field [3, pp. 273 and 284]. If $K \oplus N/N^{(2)}$ is not special, some $K_i \simeq H(M_3(Q), j)$ for a quaternion algebra Q and $N/N^{(2)}$ contains a K_i-subbimodule isomorphic to $H(M_3(\text{cay}\, Q), j)$, where $\text{cay}\, Q = \{x' \mid x \in Q\}, j(x') = -x'$, and $a \in Q$ acts on x' by $a(x') = (xa)'$ and $(x')a = (x\bar{a})'$ [3, pp. 278–283]. Let $X = 1[12]$, $Y = 1[23]$, and $Z = u[21] + v[13] + 1'[32]$ be elements of the split null extension $H(M_3(Q), j) \oplus H(M_3(\text{cay}\, Q), j)$, where u and v are non-commuting elements of Q and $a[ij] = ae_{ij} + \bar{a}e_{ji}$. Then the proof on [3, pp. 50–51] shows that X, Y, and Z fail to satisfy Glennie's identity, contradicting the fact that J does. Thus $K \oplus N/N^{(2)}$ is special, as claimed.

In short, if the theorem is false, we can find a semisimple algebra K over an algebraically closed field F and a nonzero K-bimodule M such that the split null extension $K \oplus M$ is finite dimensional, special, and has a separability idempotent. Let M' be an irreducible K-subbimodule of M. Write $K = \oplus K_i$, K_i simple, and let 1_i be the unit element of K_i. M' is either in the Peirce 1-space of some 1_r or the Peirce $\frac{1}{2}$-space of some 1_s and 1_t. Then either $K_r \oplus M'$ or $K_s \oplus K_t \oplus M'$ is a homomorphic image of $K \oplus M$, and can be used in place of $K \oplus M$. We treat both cases simultaneously, writing K for K_r or $K_s \oplus K_t$ and M for M'.

We apply the classification of finite-dimensional. simple Jordan algebras over an algebraically closed field [3, p. 204]. Take $f \in S_F(K \oplus M) \otimes S_F(K \oplus M)^o$, as in the first paragraph of the proof.

First suppose that $K = K_r = F1$. Then $M = Fx$ and $S_F(K \oplus M) = F1^\sigma \oplus Fx^\sigma$, where $(x^\sigma)^2 = 0$. $S_F(K \oplus M) \otimes S_F(K \oplus M)^o = F(1^\sigma \otimes 1^{\sigma o}) \oplus P$, where P is a nilpotent ideal. Since f is a nonzero idempotent, $f = 1^\sigma \otimes 1^{\sigma o}$. Then $(x^\sigma \otimes 1^o - 1 \otimes x^{\sigma o})^2 f = 0$ (**) implies that $-2(x^\sigma \otimes x^{\sigma o}) = 0$, a contradiction.

Next suppose that $K = K_s \oplus K_t$, where $K_s = F1_s$ and $K_t = F1_t$. Then

$M = Fx$ and $S_F(K \oplus M) = F1_s{}^\sigma \oplus F1_t{}^\sigma \oplus Fx^\sigma$, where $(x^\sigma)^2 = 0$. $S_F(K \oplus M) \otimes S_F(K \oplus M)^o = \oplus_{i,j \in \{s,t\}} F(1_i{}^\sigma \otimes 1_j^{\sigma o}) \oplus P$, where the $1_i{}^\sigma \otimes 1_j^{\sigma o}$ are orthogonal idempotents and P is a nilpotent ideal. Write $f = \sum \alpha_{i,j}(1_i{}^\sigma \otimes 1_j^{\sigma o}) + p$, $\alpha_{i,j} \in F$ and $p \in P$. Since $f(1^\sigma) = 1^\sigma$, $\alpha_{s,s} = 1 = \alpha_{t,t}$. Since $0 = (1_s{}^\sigma \otimes 1^o - 1 \otimes 1_s^{\sigma o})^2 f \equiv \alpha_{s,t}(1_s{}^\sigma \otimes 1_t^{\sigma o}) - \alpha_{t,s}(1_t{}^\sigma \otimes 1_s^{\sigma o})$ (mod P) (**), $\alpha_{s,t} = 0 = \alpha_{t,s}$. Then $f \equiv 1$ (mod P). Since f is an idempotent, $f = 1$. Then $(x^\sigma \otimes 1^o - 1 \otimes x^{\sigma o})^2 f = 0$ becomes $-2(x^\sigma \otimes x^{\sigma o}) = 0$, a contradiction.

Henceforth we exclude the two cases above, so we can assume that the degrees of K_r and K_s are at least 2. Let $A = \{a \in S_F(K \otimes M) \mid (a \otimes 1^o - 1 \otimes a^o)f = 0\}$. A is a subalgebra of $S_F(K \oplus M)$. We assert that $A = S_F(K \oplus M)$. If so, f is an associative separability idempotent for $S_F(K \oplus M)$ (since $f(1^\sigma) = 1^\sigma$, by the first paragraph), so $S_F(K \oplus M)$ is a separable associative algebra [A2]. Then $K \oplus M$ is a separable Jordan algebra, since it is special [J7]. This contradicts the fact that rad $(K \oplus M) = M$ is nonzero, establishing the theorem. Hence we need only prove that $A = S_F(K \oplus M)$. Since A is a subalgebra of $S_F(K \oplus M)$, it suffices to show in turn that K^σ and M^σ are contained in A.

In the case $K = K_s \oplus K_t$, we note that $(x^\sigma \otimes y^{\sigma o})f = 0$ for $x \in K_i$ and $y \in K_j$, $i \neq j$. This follows by multiplying $(1_i{}^\sigma \otimes 1^o - 1 \otimes 1_i^{\sigma o})^2 f = 0$ (**) on the left by $x^\sigma \otimes y^{\sigma o}$.

We claim that $K_i{}^\sigma \subset A$ when K_i has degree 2, $i \in \{r, s, t\}$. K_i has a basis $\{1_i, v_1, ..., v_n\}$, $n \geqslant 2$, where $v_h{}^2 = 1_i$ and $v_h \cdot v_k = 0$ for $h \neq k$. Multiply $(v_h{}^\sigma \otimes 1^o - 1 \otimes v_h^{\sigma o})^2 f = 0$ on the left by $\frac{1}{2}(v_h{}^\sigma \otimes 1_i^{\sigma o})$. This yields $(v_h{}^\sigma \otimes 1_i^{\sigma o} - 1_i{}^\sigma \otimes v_h^{\sigma o})f = 0$. Applying the last paragraph if $K = K_s \oplus K_t$, we obtain $(v_h{}^\sigma \otimes 1^o - 1 \otimes v_h^{\sigma o})f = 0$ in either case. Then $v_h{}^\sigma \in A$, so $K_i{}^\sigma \subset A$.

Next we prove that $K_i{}^\sigma \subset A$ when K_i has degree at least 3, $i \in \{r, s, t\}$. $K_i \cong H(M_n(C), j)$ for an associative composition algebra C, $n \geqslant 3$, and $S_F(K_i) \cong M_n(C)$ [3, pp. 204 and 143]. We note that $S_F(K_i)$ is generated as an associative algebra without 1 by $\{[x^\sigma, y^\sigma] \mid x, y \in K_i\}$, so the same holds for the image of $S_F(K_i)$ in $S_F(K \oplus M)$. By (*), $[x^\sigma, y^\sigma] \in A$, so $K_i{}^\sigma \subset A$.

We have shown that $K_i{}^\sigma \subset A$ if K_i has degree at least 2, $i \in \{r, s, t\}$. Thus $K^\sigma \subset A$, if $K = K_r$ or if $K = K_s \oplus K_t$ and K_t has degree at least 2. The only case remaining is $K = K_s \oplus F1_t$. Here $K_s{}^\sigma \subset A$ and $(1_s \oplus 1_t)^\sigma \in A$, so $K^\sigma \subset A$ in every case.

Let K_i denote K_r or K_s, so K_i has degree at least 2. We claim that $[K_i, K_i, M] \neq 0$. Suppose not. It follows that $(d \cdot [a, b, c])m = 0$ for $a, b, c, d \in K_i$ and $m \in M$. Moreover, K_i is generated as a Jordan algebra without 1 by $[K_i, K_i, K_i]$, by the classification theorem. Then $K_i M = 0$, a contradiction. Thus $[K_i, K_i, M] \neq 0$.

$[a, b, m]^\sigma = \frac{1}{4}[b^\sigma, [a^\sigma, m^\sigma]]$ for $a, b \in K_i$ and $m \in M$, by computation. Thus $[K_i, K_i, M]^\sigma \subset A$, since $[a^\sigma, m^\sigma] \in A$ by (*) and $b^\sigma \in K^\sigma \subset A$. Moreover, M is generated as a K-bimodule by $[K_i, K_i, M]$, since M is irreducible and $[K_i, K_i, M] \neq 0$. Then M^σ is contained in the subalgebra of $S_F(K \oplus M)$

generated by K^σ and $[K_i, K_i, M]^\sigma$, so $M^\sigma \subset A$. Hence $(K \oplus M)^\sigma \subset A$ and $A = S_F(K \oplus M)$, as required.

2. Central Separable Algebras

In this section we prove several fundamental results about central separable algebras. We show that a central separable R-algebra J is an R-progenerator and that there is a one-to-one correspondence between the ideals of J and the ideals of R.

Theorem 2.1, the Jordan analogue of [A7], is crucial to our work.

Theorem 2.1. *A central separable R-algebra is an R-progenerator.*

Proof. Let J be R-central separable; we identify R and $Z(J)$. Let S be the center of $U_R(J)$. For $s \in S$, the map from J to itself taking $x \to sx$ belongs to the centroid of J. Then $s1 \in R$ and $sx = s(x^\rho 1) = x^\rho(s1) = (s1)x$ for $x \in J$ [3, p. 206]. Since $U_R(J)$ is a separable associative R-algebra with center S, $U_R(J)$ is an S-progenerator [A7]. Thus there exist $u_1, \ldots, u_n \in U_R(J)$ and $f_1, \ldots, f_n \in \mathrm{Hom}_S(U_R(J), S)$ such that $u = \sum f_i(u)u_i$ for all $u \in U_R(J)$. For $a \in J$, $a = a^\rho 1 = \sum f_i(a^\rho)u_i 1$. Since $f_i(a^\rho) \in S$, $a = \sum (f_i(a^\rho)1)(u_i 1)$, where $f_i(a^\rho)1 \in R$. Define $g_i \in \mathrm{Hom}_R(J, R)$ by $g_i(a) = f_i(a^\rho)1$. Then $a = \sum g_i(a)(u_i 1)$, so $\{g_i, u_i 1\}$ is a dual basis for J as an R-module. Hence J is finitely spanned R-projective, and so an R-progenerator.

Combining Lemma 1.5 and Theorem 2.1 yields:

Corollary 2.2. *A separable R-algebra J is finitely spanned over R if and only if Z(J) is finitely spanned over R.*

Proposition 2.3. *Let J be R-central separable with separability idempotent $e \in U_R(J)$. Let ϕ: $U_R(J) \to \mathrm{End}_R(J)$ be the natural algebra homomorphism. Then ϕ restricts to an isomorphism of $U_R(J)\,eU_R(J)$ onto $\mathrm{End}_R(J)$ and $U_R(J) = [U_R(J)\,eU_R(J)] \oplus [\ker \phi]$. Moreover, ϕ induces an R-module isomorphism of $eU_R(J)$ onto $\mathrm{Hom}_R(J, R)$.*

Proof. We first show that $\phi[U_R(J)\,eU_R(J)] = \mathrm{End}_R(J)$. Let m be a maximal ideal of R. Let $e' \in U_{R/m}(J/mJ)$ be the image of e under the natural map from $U_R(J)$ to $U_{R/m}(J/mJ)$. Let ϕ': $U_{R/m}(J/mJ) \to \mathrm{End}_{R/m}(J/mJ)$ be the natural homomorphism. We have the following commutative diagram:

$$\begin{array}{ccc} U_R(J)\,eU_R(J) & \longrightarrow & \mathrm{End}_R(J) \\ \downarrow & & \downarrow \\ U_{R/m}(J/mJ)\,e'U_{R/m}(J/mJ) & \longrightarrow & \mathrm{End}_{R/m}(J/mJ) \end{array}$$

By Theorem 1.8, J/mJ is either zero or R/m-central simple. In either case, $\phi'[U_{R/m}(J/mJ)] = \mathrm{End}_{R/m}(J/mJ)$ [3, p. 239]. Then

$$\phi'[U_{R/m}(J/mJ)\, e'\, U_{R/m}(J/mJ)] = \mathrm{End}_{R/m}(J/mJ)\, \phi'(e')\, \mathrm{End}_{R/m}(J/mJ)$$

is an ideal in the simple algebra $\mathrm{End}_{R/m}(J/mJ)$. $\phi'(e') \neq 0$ (unless $J/mJ = 0$), since $[\phi'(e')](1) = e'(1) = 1$. Thus $\phi'[U_{R/m}(J/mJ)e'U_{R/m}(J/mJ)] = \mathrm{End}_{R/m}(J/mJ)$ and the bottom map of the diagram is surjective. Moreover, $\mathrm{End}_{R/m}(J/mJ) \cong \mathrm{End}_R(J)/m\,\mathrm{End}_R(J)$, since J is finitely spanned, R-projective [Theorem 2.1]. It follows from the diagram that $\mathrm{End}_R(J) = \phi[U_R(J)\, eU_R(J)] + m\,\mathrm{End}_R(J)$. $\mathrm{End}_R(J)$ is finitely spanned, since J is finitely spanned, R-projective. Hence $\mathrm{End}_R(J) = \phi[U_R(J)\, eU_R(J)]$ [M6].

We now prove that $U_R(J) = [U_R(J)eU_R(J)] \oplus [\ker \phi]$, so ϕ maps $U_R(J)eU_R(J)$ isomorphically onto $\mathrm{End}_R(J)$. $\mathrm{End}_R(J)$ becomes a $U_R(J) \otimes U_R(J)^o$-module under $(u \otimes v)\alpha = (\phi u)\, \alpha(\phi v)$ for $u, v \in U_R(J)$ and $\alpha \in \mathrm{End}_R(J)$. This makes ϕ a $U_R(J) \otimes U_R(J)^o$-homomorphism of $U_R(J)$ onto $\mathrm{End}_R(J)$. $\mathrm{End}_R(J)$ is $U_R(J) \otimes U_R(J)^o$-projective, since it is R-projective and $U_R(J) \otimes U_R(J)^o$ is a separable associative R-algebra [A5, A6]. Thus ϕ has a splitting map ψ: $\mathrm{End}_R(J) \to U_R(J)$ over $U_R(J) \otimes U_R(J)^o$. Let $id_J \in \mathrm{End}_R(J)$ be the identity map and set $g = \psi(id_J)$. Then g is a central idempotent of $U_R(J)$, $g(a) = a$ for $a \in J$, and $U_R(J) = [gU_R(J)] \oplus [\ker \phi]$. Since $ge = (g1)^o e = 1^o e = e$, $U_R(J)\, eU_R(J) \subset gU_R(J)$. Since $\phi[U_R(J)\, eU_R(J)] = \mathrm{End}_R(J)$ by the last paragraph, $U_R(J)\, eU_R(J) = gU_R(J)$, as required.

Identify $\mathrm{Hom}_R(J, R)$ with the R-submodule of $\mathrm{End}_R(J)$ of endomorphisms mapping J into R. Then $\phi[eU_R(J)] \subset \mathrm{Hom}_R(J, R)$. Conversely, if $u \in U_R(J)$ satisfies $\phi(u) \in \mathrm{Hom}_R(J, R)$, then $\phi(u) = \phi(eu)$. It follows from the above paragraph that ϕ maps $eU_R(J)$ isomorphically onto $\mathrm{Hom}_R(J, R)$.

COROLLARY 2.4. *An R-algebra J is R-central separable if and only if J is an R-progenerator and the natural homomorphism ϕ: $U_R(J) \to \mathrm{End}_R(J)$ is surjective.*

Proof. The reverse implication remains to be shown. Let m be a maximal ideal of R. ϕ induces a surjection of $U_R(J)/mU_R(J)$ onto $\mathrm{End}_R(J)/m\,\mathrm{End}_R(J)$. $U_R(J)/mU_R(J) \cong U_{R/m}(J/mJ)$ and $\mathrm{End}_R(J)/m\,\mathrm{End}_R(J) \cong \mathrm{End}_{R/m}(J/mJ)$ since J is R-projective. Thus the natural homomorphism from $U_{R/m}(J/mJ)$ to $\mathrm{End}_{R/m}(J/mJ)$ is surjective. Then J/mJ is an irreducible $U_{R/m}(J/mJ)$-module with commutant R/m. Since J/mJ is finite-dimensional, it is R/m-central simple. Thus J is R-central separable [Theorem 1.8].

It is not true that ϕ: $U_R(J) \to \mathrm{End}_R(J)$ is an isomorphism if J is R-central separable, as in the associative case [A11]. This corresponds to the fact that there are J-bimodules which are not spanned by images of the regular bimodule J.

Proposition 2.3 is the key step in proving the following analogue of [A8].

THEOREM 2.5. *Let J be a central separable R-algebra. Then there is a one-to-one correspondence between the ideals of J and the ideals of R given by:*

$$I \to I \cap R, \text{ if } I \text{ is an ideal of } J$$
$$\alpha \to \alpha J, \text{ if } \alpha \text{ is an ideal of } R.$$

Proof. We must show that $\alpha = (\alpha J) \cap R$ and $I = (I \cap R)J$. Let $e \in U_R(J)$ be a separability idempotent for J. Then $(\alpha J) \cap R = e\alpha J = \alpha e J = \alpha R = \alpha$. By Proposition 2.3,

$$I = \text{End}_R(J)I = \phi[U_R(J)\, eU_R(J)]I = U_R(J)\, eI = U_R(J)[I \cap R] = (I \cap R)J.$$

Let rad J be the radical of J defined in [8] as the maximal quasi-regular ideal of J.

COROLLARY 2.6. *Let J be R-central separable. Then* $(\text{rad}\, R)J = \bigcap mJ = \bigcap M = \text{rad}\, J$, *as m runs over the maximal ideals of R and M runs over the maximal ideals of J.*

Proof. The first equality holds because J is R-projective [Theorem 2.1]. The second holds by Theorem 2.5. We show that $\bigcap mJ = \text{rad}\, J$. For any maximal ideal m of R, J/mJ is simple, so rad $J/mJ = 0$. Then the image of rad J in J/mJ is zero, so rad $J \subset \bigcap mJ$. Conversely, let $x \in \bigcap mJ$. Then $U_{1-x}J + mJ = J$ for every maximal ideal m of R. Since J is finitely spanned, $U_{1-x}J = J$ and x is quasi-invertible [M6]. Then $\cap\, mJ$ is a quasi-regular ideal of J, so $\bigcap mJ = \text{rad}\, J$.

COROLLARY 2.7. *If J is R-separable,* rad $J = \bigcap M$ *as M runs over the maximal ideals of J. If J is also finitely spanned, these equal $\bigcap mJ$ as m runs over the maximal ideals of R. If J is R-projective as well, these equal* $(\text{rad}\, R)J$.

Proof. If J is R-separable, J is central separable over $Z(J)$, so rad $J = \bigcap M$. If J is also finitely spanned over R, rad $J = \bigcap mJ$ by the proof of Corollary 2.6, since J/mJ is semisimple for every maximal ideal m of R.

The next two propositions are Jordan analogues of [A1] and [A9].

PROPOSITION 2.8. *Let J be a finitely spanned R-algebra. Then J is R-separable if and only if J is $Z(J)$-separable and $Z(J)$ is R-separable.*

Proof. First assume that J is R-separable. Then J is $Z(J)$-separable [Proposition 1.7(4)]. For every maximal ideal m of R, $Z(J)/mZ(J) \cong Z(J/mJ)$ [Proposition 1.7(2)]. $Z(J/mJ)$ is a direct sum of separable field extensions of R/m, since J/mJ is classically separable over R/m [3, p. 239]. Then $Z(J)$ is R-separable, since it is finitely spanned [A4, Corollary 2.2].

Conversely, assume that J is $Z(J)$-separable and $Z(J)$ is R-separable. It suffices to show that J/mJ is R/m-separable for any maximal ideal m of R [Theorem 1.8]. $Z(J/mJ)$ is the image of $Z(J)$ in J/mJ (by [Proposition 1.7(3)] for J and J/mJ as $Z(J)$-algebras). Then $Z(J/mJ)$ is R/m-separable, so $Z(J/mJ) = F_1 \oplus \cdots \oplus F_n$, where each F_i is a finite-dimensional separable field extension of R/m. $J/mJ = F_1(J/mJ) \oplus \cdots \oplus F_n(J/mJ)$, where each $F_i(J/mJ)$ is F_i-central separable. Thus J/mJ is classically separable over R/m [3, p. 239], as required.

PROPOSITION 2.9. *Let J be R-central separable and let M be a J-bimodule. Then $JM^J \simeq J \otimes_R M^J$.*

Proof. Consider the homomorphism of $J \otimes M^J$ onto JM^J taking $a \otimes m$ to am. Assume that $\sum a_i \otimes m_i$ is in the kernel, so $\sum a_i m_i = 0$. By Proposition 2.3, the identity map on J is induced by an element of $U_R(J)$ of the form $\sum u_j e v_j$, $u_j, v_j \in U_R(J)$. Then $\sum a_i \otimes m_i = \sum (u_j e v_j a_i) \otimes m_i = \sum u_j 1 \otimes (e v_j a_i) m_i$ (since $eJ = R$) $= \sum u_j 1 \otimes e v_j (a_i m_i)$ (since $m_i \in M^J$) $= 0$, as required.

We note that it is not true that every bimodule M for a central separable Jordan algebra J satisfies $M = JM^J$. This again follows from the fact that M need not be spanned by images of the regular bimodule J.

Finally, we observe that the basic results of the first two sections (1.1–1.8, 2.1–2.5, 2.8, 2.9) depend on only two special properties of Jordan algebras over commutative rings with $\frac{1}{2}$: that $U_R(J)$ satisfies [J6] and [J7]. Thus the above results generalize to any variety of algebras where $U_R(J)$ has these two properties.

More precisely, let I be any set of identities and let $V(I)$ be the class of all unital nonassociative algebras satisfying them [3, p. 25]. For an R-algebra A in $V(I)$, Jacobson has defined an associative R-algebra $U_R(A)$ determined by A, I, and R—the unital universal multiplication envelope of A [3, p. 88]. $U_R(A)$ satisfies properties [J1]–[J4]. If R is a field with algebraic closure T, call an R-algebra A classically separable if A is finite-dimensional over R and $A \otimes_R T$ is a direct sum of simple T-algebras. A-bimodules relative to I are defined via split null extensions and correspond to $U_R(A)$-modules [3, p. 79]. For an A-bimodule M, let M^A be the intersection of M and the center of the split null extension $A \oplus M$. Define an R-algebra A in $V(I)$ to be R-separable if $U_R(A)$ is a separable associative R-algebra. Then, if the algebras in $V(I)$ are such that $U_R(A)$ satisfies [J6] and [J7], the results listed above hold.

In particular, in a subsequent article, we will note that alternative algebras have the two required properties and we will present further results on separable alternative algebras.

3. ASSOCIATIVE DECOMPOSITION THEOREMS

In this section, we prove decomposition theorems for separable associative algebras and separable associative algebras with involution. That is, we show that any such algebra is a direct sum of homogenous components corresponding to distinct isomorphism classes of simple algebras (simple algebras with involution) over an algebraically closed field. We present these results here for comparison with the more complicated Jordan case and because the decomposition of separable associative algebras with involution corresponds to the decomposition of separable Jordan algebras.

We first prove the decomposition theorem for separable associative algebras. This theorem follows directly from two facts: that a separable associative algebra is finitely spanned and projective over its center and that the isomorphism class of a simple associative algebra over an algebraically closed field is determined by its dimension. For 3.1–3.3, we suspend our assumption that $\frac{1}{2} \in R$.

THEOREM 3.1. *Let A be a separable associative R-algebra. Then $A = A_1 \oplus \cdots \oplus A_s$ for distinct integers $r_1, \ldots, r_s$ such that, if m is any maximal ideal of R and F is the algebraic closure of R/m, then $(A_i/mA_i) \otimes_{R/m} F$ is a direct sum of algebras isomorphic to $M_{r_i}(F)$. If the A_i are chosen for A as a separable $Z(A)$-algebra, they also work for A as an R-algebra.*

The A_i are uniquely determined if A is finitely spanned over R. In particular, the A_i chosen over $Z(A)$ are always unique.

Proof. A is finitely spanned, $Z(A)$-projective [A1, A7]. Then $Z(A) = C_1 \oplus \cdots \oplus C_s$, a direct sum of ideals such that C_iA has constant rank t_i over C_i for distinct integers t_i [M4]. Let $A_i = C_iA$, so $A = A_1 \oplus \cdots \oplus A_s$ is a direct sum of ideals. A_i is R-separable and $Z(A_i) = C_i$ [A5]. For any maximal ideal M of C_i, $\dim_{C_i/M} A_i/MA_i = t_i$.

Let m be a maximal ideal of R and let F be the algebraic closure of R/m. $A_i/mA_i = B_1 \oplus \cdots \oplus B_v$, where each B_j is a finite-dimensional, simple R/m-algebra [A4]. Let k be an integer, $1 \leqslant k \leqslant v$. Let $\phi\colon A_i \to A_i/mA_i$ be the natural homomorphism and let $M = C_i \cap \phi^{-1}[\oplus_{j \neq k} Z(B_j)]$. Since ϕ maps C_i onto $Z(A_i/mA_i)$, $A_i/MA_i \simeq B_k$ and $C_i/M \simeq Z(B_k)$ [A5]. Thus $\dim_{Z(B_k)} B_k = \dim_{C_i/M} A_i/MA_i = t_i$. Since $Z(B_k) \otimes_{R/m} F = F_1 \oplus \cdots \oplus F_w$ where each $F_j \simeq F$, $B_k \otimes F = F_1(B_k \otimes F) \oplus \cdots \oplus F_w(B_k \otimes F)$ where $F_j(B_k \otimes F)$ is a central simple F-algebra of dimension t_i. Since F is algebraically closed, $F_j(B_k \otimes F) \simeq M_{r_i}(F)$, where $r_i^2 = t_i$. Thus $(A_i/mA_i) \otimes F = \oplus (B_k \otimes F) \simeq \oplus M_{r_i}(F)$ for $r_i = t_1^{1/2}$. The r_i are distinct, since the t_i are.

It remains to prove the uniqueness of the A_i when A is finitely spanned over R. Let $A = A_1' \oplus \cdots \oplus A_t'$ be another such decomposition. We can assume that the same integer r_i corresponds to A_i and A_i'. For any maximal ideal m of R, $A_i/mA_i = A_i'/mA_i'$ is the sum of the simple components of A/mA of degree r_i. Then $A_i = A_iA_i' + mA_i$, since A_i is a direct summand of A. Since A_i is finitely spanned over R, $A_i = A_iA_i'$ [M6]. Thus $A_i = A_iA_i' = A_i'$, by symmetry.

We remark that finite spanning is required for uniqueness in Theorem 3.1. For example, Q is Z-separable [5] and $Q/mQ = 0$ for every maximal ideal m of Z. Thus, if $A = Q \oplus M_{r_1}(Z) \oplus M_{r_2}(Z)$, $r_1 \neq r_2$, we can take $A_1 = Q \oplus M_{r_1}(Z)$ and $A_2 = M_{r_2}(Z)$ or else $A_1 = M_{r_1}(Z)$ and $A_2 = Q \oplus M_{r_2}(Z)$.

DEFINITION 3.2. Let A be a separable associative R-algebra. For every positive integer r, define $A(r)$ to be the component of A corresponding to r over $Z(A)$ in Theorem 3.1. Then $A = \oplus A(r)$, where almost all $A(r) = 0$.

COROLLARY 3.3. (1) *Let A be a separable associative R-algebra and let S be a commutative R-algebra. Then $A \otimes S = \oplus [A(r) \otimes S]$ is the decomposition of $A \otimes S$ as a separable S-algebra, i.e., $[A \otimes S](r) = A(r) \otimes S$.*

(2) *Let A be a separable associative R-algebra and let T be a homomorphism from A to another R-algebra. Then $T(A) = \oplus T[A(r)]$ is the decomposition of $T(A)$ as a separable R-algebra, i.e., $[T(A)](r) = T[A(r)]$.*

Proof. (1) By the proof of Theorem 3.1, $A(r)$ is separable of rank r^2 as a projective module over $Z[A(r)]$. Thus $A(r) \otimes S$ is separable of module rank r^2 over its center $Z[A(r)] \otimes S$ [M3, A5]. Then the proof of Theorem 3.1 shows that $A \otimes S = \oplus [A(r) \otimes S]$ is the required decomposition of $A \otimes S$.

(2) $T(A) = \oplus T[A(r)]$ is a direct sum of ideals. Let N be a maximal ideal of $T(Z[A(r)])$ and let M be its inverse image in $Z[A(r)]$. Then M is a maximal ideal of $Z[A(r)]$, so $A(r)/MA(r)$ is central simple over $Z[A(r)]/M$ [A8]. Thus T induces an isomorphism of $A(r)/MA(r)$ and $T[A(r)]/NT[A(r)]$. These algebras have centers $Z[A(r)]/M$ and $T(Z[A(r)])/N$. Hence the dimension of $T[A(r)]/NT[A(r)]$ over $T(Z[A(r)])/N$ equals the dimension of $A(r)/MA(r)$ over $Z[A(r)]/M$, which equals r^2. The corollary follows from the proof of Theorem 3.1.

Next we prove the analogous decomposition theorem for a separable associative R-algebra with involution (A, j). We reinstate our assumption that $\frac{1}{2} \in R$. Setting $Z(A, j) = Z(A) \cap H(A, j)$, (A, j) is a separable $Z(A, j)$-algebra with involution. (A, j) is called j-simple if A has no j-invariant ideals except itself and 0. One easily sees that, if A is finite-dimensional semi-simple over a field, then (A, j) is a direct sum of j-simple ideals.

Let (A, j) be a separable associative R-algebra with involution. The two facts needed to prove the decompsition theorem for (A, j) are that A and $H(A, j)$ are finitely spanned $Z(A, j)$-projective and that, if (A, j) is finite-dimensional j-simple over an algebraically closed field F, the isomorphism class of (A, j) is determined by $\dim_F A$ and $\dim_F H(A, j)$.

$H(A, j)$ is a direct summand of A as $Z(A, j)$-modules, since $\frac{1}{2} \in R$. Thus, to prove that both A and $H(A, j)$ are finitely spanned, $Z(A, j)$-projective, it suffices to show this for A. A more general result is established in Lemma 3.4.

We define Galois extensions of commutative rings as in [2, p. 84]. If G is a group of automorphisms of a commutative ring S, let S^G be the subring of G-invariant elements. The following theorem is a special case of a result in [6, p. 426]:

THEOREM (KREIMER). *Let $R \subset S$ be commutative rings. Then the following conditions are equivalent:*

(1) *S is a separable R-algebra and $R = S^G$ for some finite group G of automorphisms of S.*

(2) *There is a finite set of orthogonal idempotents $\{e_i\}$ in R such that $\sum e_i = 1$ and Se_i is a Galois extension of Re_i (relative to some finite group of automorphisms of Se_i).*

Let $K \subset L$ be a Galois extension of commutative rings. Then L is finitely generated, K-projective [2, p. 81]. Also there is a one-to-one correspondence between the ideals α of K and the G-invariant ideals β of L given by $\alpha \to \alpha L$ and $\beta \to \beta \cap K$ [11, p. 21]. Combining these facts with Kreimer's theorem yields:

LEMMA. *Let S be a commutative, separable R-algebra. Let G be a finite group of R-algebra automorphisms of S. Then S is finitely spanned S^G-projective and there is a one-to-one correspondence between ideals α of S^G and G-invariant ideals β of S given by $\alpha \to \alpha S$ and $\beta \to \beta \cap S^G$.*

LEMMA 3.4. *Let A be a separable associative R-algebra and let G be a finite group of automorphisms and anti-automorphisms of A. Then A is a $Z(A)^G$-progenerator. Also, there is a one-to-one correspondence between the G-invariant ideals I of A and the ideals α of $Z(A)^G$ by $I \to I \cap Z(A)^G$ and $\alpha \to \alpha A$.*

Proof. G induces a finite group of automorphisms of $Z(A)$, so $Z(A)$ is a $Z(A)^G$-progenerator by the lemma. Since A is a $Z(A)$-progenerator, A is a $Z(A)^G$-progenerator. By the lemma, there is a one-to-one correspondence between ideals α of $Z(A)^G$ and G-invariant ideals β of $Z(A)$ by $\alpha \to \alpha Z(A)$ and $\beta \to \beta \cap Z(A)^G$. There is also a one-to-one correspondence between ideals β of $Z(A)$ and ideals I of A by $\beta \to \beta A$ and $I \to I \cap Z(A)$ [A8]. Since this correspondence takes G-invariant ideals to G-invariant ideals, the lemma follows.

Let F be an algebraically closed field. We show that the isomorphism class of a finite-dimensional j-simple F-algebra with involution (A, j) is determined by $\dim_F A$ and $\dim_F H(A, j)$. We list the distinct isomorphism classes of finite-dimensional, j-simple F-algebras as follows [3, p. 209]: for $p = 1, 2, \ldots$ set

$$(F(p, 1), j) = (M_p(F), t) \text{ where } t \text{ is transposition,}$$

$$(F(p, 2), j) = (M_p(F) \oplus M_p(F), j) \text{ where } j(a, b) = (b^t, a^t),$$

$$(F(p, 4), j) = (M_{2p}(F), j) \text{ where } j(X) = S^{-1}(X^t)S$$

for

$$S = \operatorname{diag}\{Q, \ldots, Q\} \quad \text{and} \quad Q = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

LEMMA 3.5. *Let (A, j) be a finite-dimensional, j-simple algebra with involution over an algebraically closed field F. Then the integers p and q such that $(A, j) \cong (F(p, q), j)$ are determined by the integers $\dim_F A$ and $\dim_F H(A, j)$, and this correspondence is independent of F.*

Proof. One checks that the ordered pairs (dim A, dim $H(A,j)$) in Table I are distinct, as required.

We can now prove the decomposition theorem for a separable associative R-algebra with involution (A,j). By Lemma 3.4, A and $H(A,j)$ are finitely spanned, $Z(A,j)$-projective. Then the proof in [5, p. 23] shows that $Z(A,j) = C_1 \oplus \cdots \oplus C_s$ such that $\text{rank}_{C_i} C_iA = r_i$ and $\text{rank}_{C_i} C_iH(A,j) = t_i$ for distinct ordered pairs (r_i, t_i). As in the proof of Theorem 3.1, it follows from Lemma 3.5 that $(A,j) = \oplus (C_iA, j)$ is the required decomposition. (The assumption that $\frac{1}{2} \in R$ ensures that $H(A,j)$ and $Z(A,j)$ are preserved under a change of rings.)

TABLE I

Form of (A,j)	dim A	dim $H(A,j)$
$(F(p, 1), j)$	p^2	$p(p+1)/2$
$(F(p, 2), j)$	$2p^2$	p^2
$(F(p, 4), j)$	$4p^2$	$p(2p-1)$

THEOREM 3.6. *Let (A,j) be a separable associative R-algebra with involution. Then $(A,j) = (A_1, j) \oplus \cdots \oplus (A_s, j)$ for distinct ordered pairs $(p_1, q_1), \ldots, (p_s, q_s)$ such that, if m is any maximal ideal of R and F is the algebraic closure of R/m, then $(A_i/mA_i \otimes_{R/m} F, j \otimes 1)$ is a finite direct sum of algebras isomorphic to $(F(p_i, q_i), j)$. In fact, if the (A_i, j) are chosen over $Z(A,j)$, they also work for A as an R-algebra.*

The A_i are uniquely determined if A is finitely spanned over R. Thus the A_i chosen over $Z(A,j)$ are always unique.

DEFINITION 3.7. Let (A,j) be a separable associative R-algebra with involution. For each ordered pair (p, q) let $(A(p, q), j)$ be the component of (A,j) corresponding to (p, q) over $Z(A,j)$ in Theorem 3.6. $(A,j) = \oplus (A(p, q), j)$.

COROLLARY 3.8. (1) *Let (A,j) be a separable associative R-algebra with involution and let S be a commutative R-algebra. Then $(A \otimes S, j \otimes 1)(p, q) = (A(p, q) \otimes S, j \otimes 1)$.*

(2) *Let (A,j) be a separable associative R-algebra with involution and let T be a homomorphism from (A,j) to another R-algebra with involtuion. Then $(T(A), j)(p, q) = (T[A(p, q)], j)$.*

4. SEPARABLE ALGEBRAS OVER COMPLETE LOCAL RINGS

In this section we classify finitely spanned, separable Jordan algebras J over a complete local Noetherian ring (R, m) such that J/mJ is reduced. We present these results both for their own sake and for use in Section 5 in proving that $S_{Z(J)}(J)$ is $Z(J)$-projective for any separable algebra J.

We begin with a series of definitions and lemmas. We recall that a finite-dimensional Jordan algebra J over a field F is called reduced if we can write $1 = \sum e_i$ for orthogonal idempotents e_i such that every element of $J_1(e_i)$ has the form $\alpha e_i + z$ for $\alpha \in F$ and z nilpotent.

LEMMA 4.1. *Let J be finitely spanned over a complete local Noetherian ring (R, m). Then a set of orthogonal idempotents in J/mJ lifts to a set of orthogonal idempotents in J.*

Proof. Inducting on the number of idempotents and applying the Peirce identities, it suffices to prove the following claim: if $e \in J$ is an idempotent and $f \in J/mJ$ is an idempotent orthogonal to the image of e in J/mJ, then f lifts to an idempotent in J orthogonal to e. To prove the claim, let $g \in J_0(e)$ be a preimage of f. Let $\mathrm{Cl}(R[g])$ be the closure of $R[g]$ in J. $\mathrm{Cl}(R[g])$ is a commutative, associative subalgebra of J. Then the proof in [12, pp. 50–51] shows there is an idempotent in $\mathrm{Cl}(R[g])$ congruent to g (mod mJ). Since $\mathrm{Cl}(R[g]) \subset J_0(e)$, this is the required idempotent.

LEMMA 4.2. *Let J be finitely spanned and separable over a complete local Noetherian ring (R, m). Assume that J/mJ is reduced. Then $J = J_1 \oplus \cdots \oplus J_v$, where each J_i/mJ_i is simple and reduced. Each J_i is central separable over the complete local Noetherian ring $R1_i$, where 1_i is the unit element of J_i.*

Proof. J/mJ is a direct sum of simple reduced algebras K_i with unit elements e_i. By Lemma 4.1, the e_i lift to orthogonal idempotents f_i in J. Since $J/mJ = \oplus K_i = \oplus (J/mJ)_1(e_i)$ and J is finitely spanned, $J = \sum J_1(f_i)$ [M6]. Since the $J_1(f_i)$ are orthogonal ideals, setting $J_i = J_1(f_i)$ gives the required decomposition. Since each J_i/mJ_i is finite-dimensional, simple, and reduced, the structure theory over fields shows that it has center R/m [3, p. 203]. Then J_i has center $R1_i$ [Theorem 1.8].

LEMMA 4.3. *Let (R, m) be complete local Noetherian and let F be a finite-dimensional extension field of R/m. Then there is a finite free commutative R-algebra S such that (S, mS) is complete local Noetherian and $S/mS \cong F$.*

Proof. Inducting on the dimension of F, we can assume that F is a primitive extension of R/m. Let $f \in R/m[x]$ be a monic polynomial such that $F \cong (R/m[x])/(f)$. Let $g \in R[x]$ be a monic lift of f and set $S = R[x]/(g)$. S is a finite free extension of R and S is Noetherian. $mS \subset \mathrm{rad}\, S$, since S is finitely spanned over R [12, p. 4]. $S/mS \cong F$ is a field, so (S, mS) is a local ring. Since S is finitely spanned over R, S is complete in the m-adic—equivalently, the mS-adic—topology.

DEFINITION 4.4. An R-algebra with involution (D, d) is called a *composition algebra* if (1) D is finitely spanned R-projective, (2) D is alternative with 1, and (3) $xx^d = Q(x)1 = x^d x$ $(x \in D)$, where Q is a quadratic form from D to R whose associated bilinear form is nondegenerate [M5].

Using [M2], it follows as in [3, pp. 163–164] that an algebra with involution (D, d) over a local ring (R, m) is a composition algebra if and only if there is a series of subalgebras V_i of D which satisfy the following conditions: (1) $R1 = V_0 \subset V_1 \subset \cdots \subset V_n = D$, where $0 \leqslant n \leqslant 3$, (2) each V_i is free over R of rank 2^i, (3) $V_{i+1} = V_i \oplus V_i q_{i+1}$ for some $q_{i+1} \in V_{i+1}$ such that $q_{i+1}^2 = \mu_{i+1}$ is a unit of R and $q_{i+1}^d = -q_{i+1}$, and (4) the elements of V_{i+1} multiply by

$$(a + bq_{i+1})(c + eq_{i+1}) = (ac + \mu_{i+1} e^d b) + (ea + bc^d)q_{i+1} \quad \text{for } a, b, c, e \in V_i.$$

D is associative if and only if rank $D \leqslant 4$. We refer to the above method of obtaining V_{i+1} from V_i as the doubling process.

LEMMA 4.5. *Let J be finitely spanned over a complete local Noetherian ring (R, m). Let J contain elements $v_1, \ldots, v_n$ such that $v_i \cdot v_j = \delta_{ij}$, the Kronecker delta. Assume there exists $u \in J$ such that $u^2 \equiv 1$ and $u \cdot v_i \equiv 0 \pmod{mJ}$. Then there exists $v \in J$ such that $v \equiv u \pmod{mJ}$, $v^2 = 1$, and $v \cdot v_i = 0$.*

Proof. Apply [3, Lemma 2, p. 290] to the R-algebra J/m^2J and the ideal mJ/m^2J whose square is zero. Then there exists $u_1 \in J$ such that $u_1 \equiv u \pmod{mJ}$, $u_1^2 \equiv 1 \pmod{m^2J}$ and $u_1 \cdot v_i \equiv 0 \pmod{m^2J}$. Now applying the same lemma to the image of u_1 in J/m^4J and the ideal m^2J/m^4J, we obtain $u_2 \in J$ such that $u_2 \equiv u_1 \pmod{m^2J}$, $u_2^2 \equiv 1 \pmod{m^4J}$, and $u_2 \cdot v_i \equiv 0 \pmod{m^4J}$. By induction, define $u_n \in J$ such that $u_n \equiv u_{n-1} \pmod{m^{2^{n-1}}J}$, $u_n^2 \equiv 1 \pmod{m^{2^n}J}$ and $u_n \cdot v_i \equiv 0 \pmod{m^{2^n}J}$. Then $v = \lim u_n$ has the required properties.

The next lemma follows from Lemma 4.5 as on [3, pp. 290–291].

LEMMA 4.6. *Let (R, m) be complete local Noetherian. Let (D, d) be an alternative R-algebra with involution which is a finite free R-module. Assume that $(D/mD, d)$ is a composition R/m-algebra built by a doubling process which adjoins $q_i \in D/mD$ such that $q_i^2 = 1$. Then (D, d) is a composition algebra built by a doubling process which adjoins elements t_i such that $t_i^2 = 1$.*

LEMMA 4.7. *Let (R, m) be local. Then the following statements are equivalent:*

(1) *J is the Jordan algebra of a nondegenerate symmetric bilinear form over R.*

(2) *J has a free R-basis $\{1, v_1, \ldots, v_n\}$, where $v_i^2 \in R$ is a unit and $v_i \cdot v_j = 0$ for $i \neq j$.*

Proof. (1) $\Rightarrow$ (2). Let J be determined by a nondegenerate bilinear form f on an R-module M. If $M \neq 0$, $f(M, M) = R$, since M is R-free and $f(M, (\ ))$ induces $\mathrm{Hom}_R(M, R)$ [M2, M5]. By linearization, there is $v \in M$ such that

$f(v, v)$ is a unit of R. Then $f(Rv, Rv) = R$, so $M = Rv \oplus v^{\perp}$. Moreover, f induces a nondegenerate symmetric bilinear form on $v^{\perp}$ [M5(3)], so we are done by induction on the rank of M. (2) $\Rightarrow$ (1) is clear.

Let (D, d) be an R-algebra with involution. Set $\gamma = \text{diag}\{1, \gamma_2, \ldots, \gamma_n\} \in M_n(D)$, where the γ_i are symmetric invertible elements of the nucleus of D. Define an involution j_γ of $M_n(D)$ by $j_\gamma(X) = \gamma^{-1}X^{dt}\gamma$, where X^{dt} is the d-conjugate transpose of X. In particular, if (D, d) is a composition algebra, the γ_i are units of R.

THEOREM 4.8. *Let (R, m) be complete local Noetherian. Then J is R-central separable such that J/mJ is reduced if and only if J has one of the following forms:*

(1) $J \cong R$.

(2) *J is the Jordan algebra of a nondegenerate symmetric bilinear form f on a finite free R-module M, where rank $M \geqslant 2$ and there exists $v \in M$ with $f(v, v) = 1$. (Equivalently, J has a free R-basis $\{1, v_1, \ldots, v_n\}$, $n \geqslant 2$, such that v_i^2 is a unit of R, $v_1^2 = 1$, and $v_i \cdot v_j = 0$ for $i \neq j$.)*

(3) *$J \cong H(M_n(D), j_\gamma)$, $n \geqslant 3$, where (D, d) is a composition algebra which is associative if $n \geqslant 4$.*

Moreover, an R-algebra J is finitely spanned R-separable such that J/mJ is reduced if and only if J is a finite direct sum of ideals J_i which have the above form over $R1_i$.

Proof. The last paragraph follows from the first by Lemma 4.2. If J has one of the given forms, then J is a finitely spanned, faithful Jordan R-algebra. J/mJ is R/m-central simple [3, p. 203], so J is R-central separable [Theorem 1.8].

Conversely, let J be R-central separable such that J/mJ is reduced. Since J/mJ is simple [Theorem 1.8], we apply the classification of finite-dimensional reduced simple algebras over a field [3, p. 203].

(1) If $J/mJ \cong R/m$, then $J \cong R$.

(2) Let $J/mJ = R/m \oplus W$ be the Jordan algebra of a nondegenerate symmetric bilinear form g on W, where dim $W \geqslant 2$ and there is $w \in W$ with $g(w, w) = 1$. Let W have basis $\{w_1, \ldots, w_n\}$, $n \geqslant 2$, such that $w_i^2 = \tau_i \in R/m$, $\tau_i \neq 0$, and $w_i \cdot w_j = 0$ for $i \neq j$. By Lemma 4.3, there is a finite free R-algebra S such that (S, mS) is complete local Noetherian and $S/mS \cong R/m(\tau_1^{1/2}, \ldots, \tau_n^{1/2})$. Then $(J \otimes S)/m(J \otimes S)$ has basis $\{1, y_1, \ldots, y_n\}$ such that $y_i \cdot y_j = \delta_{ij}$. By Lemma 4.5 and induction, $J \otimes S$ contains elements $z_1, \ldots, z_n$ such that z_i lies over y_i and $z_i \cdot z_j = \delta_{ij}$. Moreover, $J \otimes S$ is a finite free S-module, since $J \otimes S$ is S-central separable and S is local. Thus $\{1, z_1, \ldots, z_n\}$ is a free S-basis of $J \otimes S$ [M2]. Since $n \geqslant 2$, it follows that $J \otimes S = S \oplus [J \otimes S, J \otimes S, J \otimes S]$ and $[J \otimes S, J \otimes S, J \otimes S]^2 \subset S$. Since S is a free R-module, this implies that $J = R \oplus [J, J, J]$ and $[J, J, J]^2 \subset R$. Then $[J, J, J]$ is a finite free R-module [M2] and multiplication defines a symmetric bilinear form f from

$[J, J, J]$ to $R.f$ is nondegenerate since it induces g [M5]. Finally, by assumption, W contains an element w with $w^2 = 1$. Thus there is $v \in [J, J, J]$ with $v^2 \equiv 1 \pmod{mJ}$. Since $v^2 \in R$ and $\frac{1}{2} \in R$, there is a unit $\alpha \in R$ such that $(\alpha^{-1}v)^2 = 1$ [3, p. 150]. The equivalent form of (2) follows from the proof of Lemma 4.7.

(3) Finally, let $J/mJ \cong H(D'_n, j_\gamma)$, $n \geqslant 3$. By Lemma 4.1, J has n orthogonal idempotents f_i lying over the diagonal idempotents e_i of J/mJ. For $i \neq j$, there is $u \in (J/mJ)_{1/2}(e_i) \cap (J/mJ)_{1/2}(e_j)$ such that $U_u[(J/mJ)_1(e_i + e_j)] = (J/mJ)_1(e_i + e_j)$. Let v be a preimage of u in $J_{1/2}(f_i) \cap J_{1/2}(f_j)$, so $J_1(f_i + f_j) \subset U_v[J_1(f_i + f_j)] + mJ$. Then $J_1(f_i + f_j) = U_v[J_1(f_i + f_j)] + mJ_1(f_i + f_j)$ and $J_1(f_i + f_j)$ is finitely spanned, since $J_1(f_i + f_j)$ is an R-direct summand of J. Thus $J_1(f_i + f_j) = U_v[J_1(f_i + f_j)]$ [M6]. The Coordinatization Theorem applies without change to Jordan algebras over commutative rings with $\frac{1}{2}$, by the proof in [3, pp. 133–137]. Hence $J = H(M_n(D), j_\gamma)$, where (D, d) is an alternative algebra with involution. If $n \geqslant 4$, D is associative [3, p. 127]. D is a finite free R-module, since J is [M2]. It remains to show that (D, d) is actually a composition algebra.

$(D/mD, d)$ is a composition algebra, by the proof in [3, p. 203]. Let D/mD be built by a doubling process which adjoins elements q_i such that $q_i^2 = \mu_i \in R/m$, $\mu_i \neq 0$. Then $F = R/m(\mu_1^{1/2}, \ldots, \mu_d^{1/2})$ is a finite-dimensional extension field of R/m such that $D/mD \otimes_{R/m} F$ is a composition algebra built by adjoining elements p_i such that $p_i^2 = 1$. By Lemma 4.3, there is a finite free R-algebra S such that (S, mS) is complete local Noetherian and $S/mS \cong F$. By Lemma 4.6, $D \otimes S$ is a composition algebra over S, so $xx^d = x^d x \in S$ for $x \in D \otimes S$. Then $xx^d = x^d x \in R$ for $x \in D$. The associated bilinear form is nondegenerate, since it induces a nondegenerate bilinear form on D/mD. Thus (D, d) is a composition algebra, as required.

For $\beta_1, \ldots, \beta_n \in R$, define a unital associative R-algebra $C(\beta_1, \ldots, \beta_n)$ with free R-basis $\{1, v_{i_1} \cdots v_{i_t}$ for $1 \leqslant i_1 < \cdots < i_t \leqslant n$, $1 \leqslant t \leqslant n\}$, where the monomials multiply by juxtaposition and the rules $v_i^2 = \beta_i$ and $v_j v_i = -v_i v_j$ for $i < j$.

COROLLARY 4.9. *Let (R, m) be complete local Noetherian. Let J be R-central separable such that J/mJ is reduced. Then $S_R(J)$ has one of the following forms*:

(1) *if $J \cong R$, then $S_R(J) \cong R$,*

(2) *if J has basis $\{1, v_1, \ldots, v_n\}$ where $v_i^2 = \beta_i$ and $v_i \cdot v_j = 0$ for $i \neq j$, then $S_R(J) \cong C(\beta_1, \ldots, \beta_n)$,*

(3) *if $J \cong H(M_n(D), j_\gamma)$, $n \geqslant 3$, and* rank $D \leqslant 4$, *then $S_R(J) \cong M_n(D)$,*

(4) *if $J \cong H(M_3(D), j_\gamma)$ and* rank $D = 8$, *then $S_R(J) = 0$.*

In particular, $S_R(J)$ is a finite free R-module in every case.

Proof. By Theorem 4.8, it suffices to establish the statements (1)–(4). In each case the given algebra is clearly an associative specialization of J, so there is a homomorphism ϕ from $S_R(J)$ to this algebra. ϕ induces an isomorphism under tensoring by R/m, by the structure theory of reduced R/m-algebras [3, pp. 203, 209, and 261]. Since $S_R(J)$ is finitely spanned and the given algebras are finite free R-modules, ϕ is an isomorphism [J6, M7].

We remark that Corollary 4.9 actually classifies $S_R(J)$ when J is finitely spanned and separable over a complete local Noetherian ring (R, m) and J/mJ is reduced. Write $J = \oplus J_i$, as in the last paragraph of Theorem 4.8. Then $S_R(J) = \oplus S_R(J_i) \cong \oplus S_{R1_i}(J_i)$, where each $S_{R1_i}(J_i)$ has the form of Corollary 4.9 as an $R1_i$-algebra.

5. Projectivity of $S_{Z(J)}(J)$

In this section we apply Corollary 4.9 to deduce that $S_R(J)$ is R-projective for a central separable R-algebra J. This is the key result in proving the decomposition theorem for Jordan algebras.

We require two lemmas, 5.2 and 5.3. Lemma 5.2 reduces the study of a separable Jordan algebra J over a complete local Noetherian ring (R, m) to the case where J/mJ is reduced.

Sublemma 5.1. *Let J be separable over a field F. Then there is a finite-dimensional extension field E of F such that $J \otimes E$ is a reduced E-algebra.*

Proof. Let F' be the algebraic closure of F. In $J \otimes F'$ we can write 1 as the sum of orthogonal idempotents e_i such that $(J \otimes F')_1(e_i) = F'e_i$ [3, p. 202]. Let E be a finite-dimensional extension field of F containing the elements of F' needed to write each e_i as a linear combination of elements of J. Then $J \otimes E$ contains idempotents f_i lying over the e_i. The f_i are orthogonal idempotents whose sum is 1 and which satisfy $(J \otimes E)_1(f_i) = Ef_i$.

Combining Sublemma 5.1 and Lemma 4.3 yields:

Lemma 5.2. *Let J be separable over (R, m) complete local Noetherian. Then there is a finite free R-algebra S such that (S, mS) is complete local Noetherian and $(J \otimes S)/mS(J \otimes S)$ is a reduced S/mS-algebra.*

The next lemma reduces the study of separable Jordan algebras over commutative rings to algebras over Noetherian rings. It is a generalized Jordan analogue of a result on separable associative algebras in [12, p. 135].

Lemma 5.3. *Let J be finitely spanned R-separable. Then there is a Noetherian subring R' of R and an R'-subalgebra J' of J such that J' is finitely spanned R'-separable and $J = RJ'$. If J is also R-projective, we can ensure that J' is R'-projective and that $J \cong J' \otimes_{R'} R$. If J is R-central, we can ensure that J' is R'-central.*

Proof. Fix a finite spanning set $\{v_i\}$ for J over R. We will let R' be a finitely generated subring of R such that $J' = \sum R'v_i$ has the required properties. Writing $v_i \cdot v_j = \sum r_{ijk}v_k$ and $1 = \sum s_i v_i$ for r_{ijk}, $s_i \in R$, we can ensure that J' is an R'-subalgebra of J by taking r_{ijk}, $s_i \in R'$. Let $f \in U_R(J) \otimes_R U_R(J)^o$ be an associative separability idempotent for $U_R(J)$ [A2]. By adjoining finitely many elements of R to R', we can ensure that f is the image of some $f' \in U_{R'}(J') \otimes_{R'} U_{R'}(J')^o$ under the natural map. The equation $(v_i{}^\rho \otimes 1^o - 1 \otimes v_i^{\rho o})f = 0$ holds in $U_R(J) \otimes_R U_R(J)^o$, where $U_R(J) \otimes_R U_R(J)^o$ is isomorphic to the free associative algebra on $\{v_i{}^\rho, v_i^{\rho o}\}$ modulo the ideal I generated by the defining relations of $U_R(J)$, $U_R(J)^o$, and the tensor product. Adjoin the elements of R needed to express $(v_i{}^\rho \otimes 1^o - 1 \otimes v_i^{\rho o})f$ as an element of I, where everything is written in terms of $v_i{}^\rho$ and $v_i^{\rho o}$. Then $(v_i{}^\rho \otimes 1^o - 1 \otimes v_i^{\rho o})f' = 0$ in $U_{R'}(J') \otimes_{R'} U_{R'}(J')^o$. Likewise, we can ensure that $f'(1) = 1$, $1 \in U_{R'}(J')$. Then f' is an associative separability idempotent for $U_{R'}(J')$, so J' is R'-separable.

Now assume that J is also R-projective. As an R-module, $J \cong gR^n$, where $g \in M_n(R)$ is an idempotent and $M_n(R)$ acts on R^n via the basis $e_1 = (1, 0,..., 0),..., e_n = (0,..., 0, 1)$. Let R' contain the entries of g and take $v_i = g(e_i)$ in the last paragraph. Let $g' \in M_n(R')$ have the same entries as g and let $M_n(R')$ act on R'^n. Then $\sum R'g(e_i) \cong g'R'^n$ as R'-modules, so $J' = \sum R'g(e_i)$ is R'-projective. Since $R'^n \cong [\sum R'g(e_i)] \oplus [\sum R'(1-g)(e_i)]$, the natural isomorphism of $R'^n \otimes_{R'} R$ and R^n induces an isomorphism of $[\sum R'g(e_i)] \otimes_{R'} R$ and $gR^n \cong J$, as required.

Finally, let J be R-central separable. Since J is finitely spanned R-projective, we can choose J' and R' as in the last paragraph. Since $J' \otimes_{R'} R \cong J$, it follows that the natural map of $J' \otimes_{Z(J')} R$ onto J is an isomorphism. $Z(J')$ is Noetherian, since it is finitely spanned over R' [Corollary 2.2]. Thus we can replace R' by $Z(J')$, as required.

THEOREM 5.4. *If J is R-central separable, then $S_R(J)$ is finitely spanned R-projective. If σ: $J \to S_R(J)$ is the canonical map, $\sigma(J)$ and $S_R(J)/\sigma(J)$ are finitely spanned R-projective and $\sigma(J)$ is an R-direct summand of $S_R(J)$.* ker σ *is finitely spanned R-projective and an R-direct summand of J.*

Proof. Since J is finitely spanned over R, so is $S_R(J)$ [J6]. By Lemma 5.3, there is a Noetherian subring R' of R and an R'-subalgebra J' of J such that J' is R'-central separable and $J' \otimes_{R'} R \cong J$. If we show that $S_{R'}(J')$ is R'-projective, then $S_R(J) \cong S_{R'}(J') \otimes_{R'} R$ is R-projective. Thus we can assume that R is Noetherian.

Let m be a maximal ideal of R, let R^* be the completion of R localized at m, and let J^* denote $J \otimes_R R^*$. By Lemma 5.2, there is a finite free extension T of R^* such that (T, mT) is complete local Noetherian, $J^* \otimes_{R^*} T$ is T-central separable, and $(J^* \otimes T)/mT(J^* \otimes T)$ is a reduced T/mT-algebra. Then $S_T(J^* \otimes_{R^*} T)$ is a free T-module, by Corollary 4.9. Since T is a free R^*-module and $S_{R^*}(J^*) \otimes_{R^*} T$

$\cong S_T(J^* \otimes_{R^*} T)$, $S_{R^*}(J^*)$ is a free R^*-module [M2]. Then $S_R(J) \otimes_R R^* \cong S_{R^*}(J^*)$ is a free R^*-module for every maximal ideal m of R. Since $S_R(J)$ is finitely spanned, this implies that $S_R(J)$ is R-projective [5, pp. 12–14]. Similarly, one proves that $S_R(J)/\sigma(J)$ is R-projective (since tensoring is right exact). Then $\sigma(J)$ is a direct summand of $S_R(J)$ and thus R-projective. Then σ: $J \to \sigma[S_R(J)]$ splits, so ker σ is a direct summand of J and R-projective.

6. Jordan Decomposition Theorem

We now apply Theorem 5.4 to prove the decomposition theorem for Jordan algebras. We need only observe that the isomorphism class of a finite-dimensional simple algebra J over an algebraically closed field F is determined by $\dim_F J$ and $\dim_F S_F(J)$.

Definition 6.1. For an algebraically closed field F, let $F[p, q]$ be a Jordan F-algebra as follows:

$F[1, 1] = F$.

$F[2, q] = F \oplus V$, the Jordan algebra of a nondegenerate symmetric bilinear form on a vector space V of dimension q, $q \geqslant 2$.

$F[p, q] = H(M_p(D), j)$ for a composition algebra D of dimension q, where $(p, q) = (3, 8)$ or $p \geqslant 3$ and $q \in \{1, 2, 4\}$.

The $F[p, q]$ represent the distinct isomorphism classes of finite-dimensional simple Jordan F-algebras.

Lemma 6.2. *Let J be finite-dimensional and simple over an algebraically closed field F. Then the integers p and q such that $J \cong F[p, q]$ are determined by* $\dim_F J$ *and* $\dim_F S_F(J)$, *and this correspondence is independent of F.*

Proof. One verifies that the ordered pairs (dim J, dim $S_F(J)$) in Table II are distinct.

TABLE II

J	dim J	dim $S_F(J)$
$F[1, 1]$	1	1
$F[2, q]$, $q \geqslant 2$	$q + 1$	2^q
$F[p, 1]$, $p \geqslant 3$	$p(p + 1)/2$	p^2
$F[p, 2]$, $p \geqslant 3$	p^2	$2p^2$
$F[p, 4]$, $p \geqslant 3$	$p(2p - 1)$	$4p^2$
$F[3, 8]$	27	0

The decomposition theorem for a separable Jordan algebra J can now be proved in the same manner as Theorems 3.1 and 3.6. By Theorem 5.4, both J and $S_{Z(J)}(J)$ are finitely spanned $Z(J)$-projective. Then $Z(J) = C_1 \oplus \cdots \oplus C_s$ such that $\operatorname{rank}_{C_i} C_i J = r_i$ and $\operatorname{rank}_{C_i} C_i S_{Z(J)}(J) = t_i$ for distinct ordered pairs (r_i, t_i). It follows from Lemma 6.2 that $J = \oplus\, C_i J$ is the desired decomposition.

THEOREM 6.3. *Let J be R-separable. Then $J = J_1 \oplus \cdots \oplus J_s$ for distinct ordered pairs $(p_1, q_1), \ldots, (p_s, q_s)$ such that, if m is any maximal ideal of R and F is the algebraic closure of R/m, then $J_i/mJ_i \otimes_{R/m} F$ is a finite direct sum of algebras isomorphic to $F[p_i, q_i]$. If the J_i are chosen for J as a $Z(J)$-algebra, they also work for J as an R-algebra.*

The J_i are uniquely determined if J is finitely spanned over R. Thus the J_i chosen over $Z(J)$ are always uniquely determined.

DEFINITION 6.4. Let J be R-separable. For an ordered pair (p, q), let $J(p, q)$ be the component of J corresponding to (p, q) over $Z(J)$ in Theorem 6.3. Then $J = \oplus\, J(p, q)$.

COROLLARY 6.5. (1) *Let J be R-separable and let S be a commutative R-algebra. Then $(J \otimes S)(p, q) = J(p, q) \otimes S$.*

(2) *Let J be R-separable and let $T: J \to J'$ be an R-algebra homomorphism. Then $[T(J)](p, q) = T[J(p, q)]$.*

7. STRUCTURE OF SEPARABLE JORDAN ALGEBRAS AND THEIR SPECIAL UNIVERSAL ENVELOPES

In this section we apply Theorem 6.3 to study the structure of separable Jordan algebras and their special universal envelopes. We start by relating the decomposition of separable Jordan algebras and separable associative algebras with involution. We require the following proposition:

PROPOSITION 7.1. *Let J be finitely spanned, R-separable. Then $S_R(J) \cong S_{Z(J)}(J)$.*

Proof. Let $\sigma: J \to S_R(J)$ and let $a \in Z(J)$ and $x \in J$. We must show that $a^\sigma x^\sigma = (a \cdot x)^\sigma = x^\sigma a^\sigma$. By Lemma 5.3, there is a Noetherian subring R' of R and an R'-subalgebra J' of J such that J' is finitely spanned R'-separable and $J = RJ'$. By enlarging R', we can assume that $a, x \in J'$. Since J is a homomorphic image of $J' \otimes_{R'} R$, $S_R(J)$ is a homomorphic image of $S_{R'}(J') \otimes_{R'} R$. Thus we can assume that R is Noetherian to prove that $a^\sigma x^\sigma = (x \cdot a)^\sigma = x^\sigma a^\sigma$. As in the proof of Theorem 5.4, we can further assume that (R, m) is complete local Noetherian and J/mJ is reduced. Then $J = \oplus\, J_i$, where $Z(J_i) = R1_i$ [Lemma 4.2]. Since $S_R(J) \cong \oplus\, S_R(J_i)$ [J5], the proposition follows.

Let π denote the main involution of $S_R(J)$, so $\pi(x^\sigma) = x^\sigma$ for $x \in J$ [3, p. 65].

THEOREM 7.2. *Let R be a commutative ring with $\frac{1}{2}$. There is an isomorphism between the category of finitely spanned, separable Jordan R-algebras J such that $J = \oplus J(p, q)$ ($p \geqslant 3$ and $q \leqslant 4$) and the category of finitely spanned, separable, associative R-algebras with involution (A, j) such that $(A, j) = \oplus (A(p, q), j)$ ($p \geqslant 3$). This isomorphism takes J to $(S_R(J), \pi)$ and (A, j) to $H(A, j)$. If J and (A, j) correspond, then $Z(J) = Z(A, j)$ and the components $J(p, q)$ and $(A(p, q), j)$ correspond.*

Proof. Let J be finitely spanned, R-separable such that $J = J(p, q)$ for $p \geqslant 3$ and $q \leqslant 4$. Let $\sigma: J \to H(S_R(J), \pi)$ be the natural map. We show that σ is an isomorphism and that $(S_R(J), \pi) = (S_R(J)(p, q), \pi)$. By Proposition 7.1, we can assume that $R = Z(J)$. Let m be a maximal ideal of R. Tensoring σ by R/m gives the canonical map σ': $J/mJ \to H(S_{R/m}(J/mJ), \pi)$. σ' is an isomorphism, since $J/mJ = (J/mJ)(p, q)$ is a finite-dimensional, special, central simple R/m-algebra of degree $p \geqslant 3$ [3, p. 209]. Then σ is an isomorphism, since both J and $H(S_R(J), \pi)$ are finitely spanned R-projective [Theorem 5.4, M7]. Moreover, if F is the algebraic closure of R/m, $J/mJ \otimes_{R/m} F \cong F[p, q]$, so

$$(S_F(J/mJ \otimes F), \pi) \cong (F(p, q), j)$$

[3, p. 210]. Hence $(S_R(J), \pi) = (S_R(J)(p, q), \pi)$.

Conversely, let $(A, j) = (A(p, q), j)$ be a finitely spanned, separable associative R-algebra with involution, $p \geqslant 3$. As above, $H(A, j) = [H(A, j)](p, q)$. Let ϕ: $(S_R[H(A, j)], \pi) \to (A, j)$ be the canonical homomorphism. We show that ϕ is an isomorphism. By Proposition 7.1 and Example 1.10(2), we can assume that $R = Z(A, j) = Z[H(A, j)]$. Let m be a maximal ideal of R. Tensoring ϕ by R/m gives the canonical homomorphism ϕ': $S_{R/m}[H(A/mA, j)] \to (A/mA, j)$. Since $(A/mA, j)$ is R/m-central simple of degree $p \geqslant 3$, ϕ' is an isomorphism [3, p. 209]. Then ϕ is an isomorphism, since A is finitely spanned R-projective and $S_R[H(A, j)]$ is finitely spanned [Lemma 3.4, J6, M7]. The theorem follows by taking direct sums [J5].

PROPOSITION 7.3. *Let J be finitely spanned, R-separable. Set $B = \oplus J(p, q)$ for $(p, q) \neq (3, 8)$, and consider the decomposition $J = B \oplus J(3, 8)$. B is R-special and $S_R[J(3, 8)] = 0$. Thus $J(3, 8)$ is the kernel of σ: $J \to S_R(J)$.*

Proof. By Proposition 7.1, we can assume that $R = Z(J)$. Let $\sigma: B \to S_R(B)$. For any maximal ideal m of R, σ induces σ': $B/mB \to S_R(B)/mS_R(B) \cong S_{R/m}(B/mB)$. σ' is injective, since B/mB is special. Thus ker $\sigma \subset mB$. By Theorem 5.4, ker σ is an R-direct summand of B, so ker $\sigma = m$(ker σ) and ker σ is finitely spanned. Then ker $\sigma = 0$ [M6], and B is special. For every maximal ideal m of R, $S_R[J(3, 8)]/mS_R[J(3, 8)] \cong S_{R/m}[(J/mJ)(3, 8)] = 0$. Hence $S_R[J(3, 8)] = 0$

[M6, J6]. The last sentence of the theorem follows, since $S_R(J) \cong S_R[J(3, 8)] \oplus S_R(B)$ [J5].

Next, we apply the results of McCrimmon in [9]. He defines an R-algebra J to be *4-interconnected* if $1 \in J$ can be written as $1 = \sum e_i$, where the e_i are orthogonal idempotents such that, for each i, there are at least three other e_j's satisfying $e_i \in U_{J_{ij}}(J_{jj})$. He calls J *latently 4-interconnected* if there is a faithfully flat commutative R-algebra S such that $J \otimes_R S$ is 4-interconnected. We define J to be *weakly 4-interconnected* if $J \otimes_R R_m$ is latently 4-interconnected for every maximal ideal m of R.

Proposition 7.4. (1) *A weakly 4-interconnected algebra is special and reflexive.*

(2) *Let J be finitely spanned R-separable such that $J = \oplus J(p, q)$ for $p \geqslant 4$. Then J is weakly 4-interconnected.*

Proof. By [9], a latently 4-interconnected algebra is special and reflexive. (1) follows by localization. Localizing (2), it suffices to assume that (R, m) is local and prove that J is latently 4-interconnected. First suppose that (R, m) is Noetherian local. Let R^* be the completion of R and let J^* denote $J \otimes_R R^*$. By Lemma 5.2, there is a free R^*-algebra S such that (S, mS) is complete local Noetherian and $(J^* \otimes_{R^*} S)/mS(J^* \otimes_{R^*} S)$ is a reduced S/mS-algebra. Since $J^* \otimes_{R^*} S = \oplus [J^* \otimes_{R^*} S](p, q)$ for $p \geqslant 4$, Theorem 4.8 shows that $J^* \otimes_{R^*} S$ is a direct sum of matrix algebras of degree at least 4. Thus $J \otimes_R S \cong (J \otimes_R R^*) \otimes_{R^*} S = J^* \otimes_{R^*} S$ is 4-interconnected. Moreover, S is a faithfully flat R-algebra, since R^* is. Hence J is latently 4-interconnected.

Now let (R, m) be any local ring. By Lemma 5.3, there are a Noetherian subring R' of R and an R'-subalgebra J' of J such that J' is finitely spanned R'-separable and $J = RJ'$. Let $m' = m \cap R'$. Localizing R' and J' at m', we can assume that R' is Noetherian local. Writing $J' = \oplus J'(p, q)$ yields $J = \oplus RJ'(p, q)$. $RJ'(p, q) = [RJ'(p, q)](p, q)$ by Corollary 6.5, since $RJ'(p, q)$ is a homomorphic images of $R \otimes_{R'} J'(p, q)$. Thus $J' = \oplus J'(p, q)$ for $p \geqslant 4$. By the last paragraph, there is a faithfully flat R'-algebra S' such that $J' \otimes_{R'} S'$ is 4-interconnected. Set $S = R \otimes_{R'} S'$, so S is a faithfully flat R-algebra. Moreover $J \otimes_R S \cong J \otimes_{R'} S'$ contains $J' \otimes_{R'} S'$ as a subalgebra. Then $J \otimes_R S$ is 4-interconnected, so J is latently 4-interconnected.

Corollary 7.5. *Let J be finitely spanned, R-separable such that $J = \oplus J(p, q)$ for $p \geqslant 4$. Then any R-algebra B containing J as a subalgebra is special and reflexive.*

Proof. By Proposition 7.4(2), J is weakly 4-interconnected. Then B is weakly 4-interconnected, so B is special and reflexive [Proposition 7.4(1)].

Next we consider central separable algebras of the form $J = \oplus J(2, q)$ ($q \geqslant 2$ assumed).

PROPOSITION 7.6. *J is R-central separable such that $J = \bigoplus J(2, q)$ if and only if $J = R \oplus M$ is the Jordan algebra of a nondegenerate symmetric bilinear form on M, where M is an R-progenerator such that* $\operatorname{rank}_p M \geqslant 2$ *for all primes p of R. In fact, $M = [J, J, J]$. $J = J(2, q)$ if and only if M has constant* rank q.

Proof. Let J be R-central separable such that $J = \bigoplus J(2, q)$. We claim that $J = R \oplus [J, J, J]$ and $[J, J, J]^2 \subset R$. We can assume that (R, m) is complete local Noetherian and J/mJ is reduced. Then the claim follows from Theorem 4.8.

Since $J = R \oplus [J, J, J]$ and $[J, J, J]^2 \subset R$, multiplication defines a symmetric bilinear form f from $[J, J, J]$ to R, and J is the Jordan algebra determined by f. $[J, J, J]$ is finitely spanned R-projective, since J is R-central separable. Then f is nondegenerate and $\operatorname{rank}_p M \geqslant 2$, by Example 1.11. M is R-faithful, since it has positive rank at every prime. The converse is Example 1.11.

PROPOSITION 7.7. *Let $J = J(2, q)$ be R-central separable, $q \geqslant 2$.*

(1) *If q is even, $S_R(J)$ is R-central separable.*

(2) *If q is odd, $S_R(J)$ is R-separable and $Z[S_R(J)]$ is a Galois extension of R with Galois group $\{1, \pi\}$, where π is the canonical involution of $S_R(J)$.*

Proof. (1) $S_R(J)$ is R-faithful, by the standard reductions. For any maximal ideal m of R, $S_R(J)/mS_R(J) \cong S_{R/m}(J/mJ)$ is R/m-central simple [3, p. 263]. Then $S_R(J)$ is R-central separable, by the associative analogue of Theorem 1.8.

(2) $S_R(J)$ is R-separable by Corollary 1.9 and R-faithful by the standard reductions. $\{1, \pi\}$ induces a group of automorphisms of $Z[S_R(J)]$ over R. For every maximal ideal m of R, π induces a nontrivial automorphism of $Z[S_R(J)]/mZ[S_R(J)] \cong Z[S_{R/m}(J/mJ)]$ with fixed ring R/m [3, p. 263]. Then $H(Z[S_R(J)], \pi) = R$ [M6], and $Z[S_R(J)]$ is a Galois extension of R with Galois group $\{1, \pi\}$ [2, p. 81, Proposition 1.2.5].

8. UNIVERSAL MULTIPLICATION ENVELOPES OF CENTRAL SEPARABLE ALGEBRAS

Lastly, we apply the decomposition theorem to study the universal multiplication envelope of a central separable R-algebra J, extending the theory in [3, pp. 264–285]. By [J5], we can assume that $J = J(p, q)$. We represent $U_R(J)$ as a direct sum of algebras of the form $\operatorname{End}_S(M)$, where M is an S-progenerator and $S = R$ or $Z[S_R(J)]$.

First assume that $J = J(2, q)$. For $0 \leqslant k \leqslant q$, let V_k be the R-submodule of of $S_R(J)$ spanned by $\{a_1^\sigma \cdots a_k^\sigma \mid a_i \in J\}$. Since $1 \in J$, $V_j \subset V_k$ for $j < k$. V_j and V_k/V_j, $j < k$, are R-progenerators, by our standard reductions and Corollary 4.9. For any R-algebra J, let τ: $U_R(J) \to S_R(J) \otimes_R S_R(J)$ be the homomorphism determined by $\tau(a^\rho) = \frac{1}{2}(a^\sigma \otimes 1 + 1 \otimes a^\sigma)$, $a \in J$ [3, p. 100].

PROPOSITION 8.1. *Let J be R-central separable such that $J = J(2, q)$ for $q = 2k$ even. Set $T_0 = V_1$, $T_1 = V_3/V_1, \dots, T_i = V_{2i+1}/V_{2i-1}, \dots, T_{k-1} = V_{q-1}/V_{q-3}$, $T_k = V_q/V_{q-1}$. Then $U_R(J) \cong \bigoplus \operatorname{End}_R(T_i)$ where each T_i is an R-progenerator of* rank $C_{q+1,2i+1}$. *Moreover, τ is injective.*

Proof. $S_R(J)$ is an associative $U_R(J)$-module under $a^\rho s = \frac{1}{2}(a^\sigma s + s a^\sigma)$, $a \in J$ and $s \in S_R(J)$ [3, p. 267]. Each V_{2i+1} is a submodule [3, p. 268], so each T_i is a $U_R(J)$-module and there is a homomorphism ϕ: $U_R(J) \to \bigoplus \operatorname{End}_R(T_i)$. Since the T_i are finitely spanned R-projective, tensoring ϕ by R/m induces the corresponding homomorphism ϕ' for J/mJ. ϕ' is an isomorphism, by [3, pp. 267–269]. Thus ϕ is an isomorphism, since $\bigoplus \operatorname{End}_R(T_i)$ is finitely spanned R-projective and $U_R(J)$ is finitely spanned [M7, J6]. Hence τ is injective, since ϕ factors through τ [3, p. 267].

The next proposition follows in the same manner from [3, p. 272].

PROPOSITION 8.2. *Let J be R-central separable such that $J = J(2, q)$ for $q = 2k - 1$ odd ($k \geq 2$, since $q \geq 2$). Write $J = R \oplus M$ as the Jordan algebra of a nondegenerate symmetric bilinear form f on M [Proposition 7.6]. Let $J' = R \oplus M \oplus Rw$ be the Jordan algebra of a nondegenerate symmetric bilinear form g on $M \oplus Rw$, where $Rw \cong R$, g restricts to f on $M \times M$, $g(M, w) = 0$, and $g(w, w) = 1$. Consider $J \subset J'$ and $V_i \subset S_R(J) \subset S_R(J')$. If k is odd, set*

$$T_1 = V_1,\ T_3 = V_3/V_1, \dots, T_{k-2} = V_{k-2}/V_{k-4},$$
$$T_0 = V_0 w,\ T_2 = V_2 w/V_0 w, \dots, T_{k-1} = V_{k-1}w/V_{k-3}w, \text{ and}$$
$$X = S_R(J)/(Z[S_R(J)]V_{k-2}).$$

If k is even, set

$$T_1 = V_1,\ T_3 = V_3/V_1, \dots, T_{k-1} = V_{k-1}/V_{k-3},$$
$$T_0 = V_0 w,\ T_2 = V_2 w/V_0 w, \dots, T_{k-2} = V_{k-2}w/V_{k-4}w, \text{ and}$$
$$X = S_R(J)/(Z[S_R(J)]V_{k-2}w).$$

Then $U_R(J) \cong \bigoplus \operatorname{End}_R(T_i) \oplus \operatorname{End}_{Z[S_R(J)]}(X)$, where T_i is an R-progenerator of rank $C_{q+i,i}$ *and X is a $Z[S_R(J)]$-progenerator of* rank $\frac{1}{2}C_{q+1,k}$. *Moreover, τ is injective.*

Finally, we consider $U_R(J)$ when J is R-central separable and $J = J(p, q)$, $p \geq 3$.

PROPOSITION 8.3. *Let J be R-central separable such that $J = J(3, 8)$. Then $U_R(J) \cong \operatorname{End}_R(J)$, where J is an R-progenerator of* rank 27.

Proof. Let ϕ: $U_R(J) \to \operatorname{End}_R(J)$ be the natural homomorphism. Let m be a maximal ideal of R. Since J is finitely spanned R-projective, tensoring ϕ by R/m induces the natural homomorphism ϕ': $U_{R/m}(J/mJ) \to \operatorname{End}_{R/m}(J/mJ)$. ϕ' is an isomorphism [3, p. 284], so ϕ is an isomorphism [M7].

For an R-algebra J, let $V_R(J)$ be the subalgebra of $S_R(J) \otimes S_R(J)$ fixed by the automorphism exchanging $S_R(J) \otimes 1$ and $1 \otimes S_R(J)$. $\tau[U_R(J)] \subset V_R(J)$, τ as above. Since $\frac{1}{2} \in R$, $V_R(J)$ is an R-direct summand of $S_R(J) \otimes S_R(J)$ preserved under changes of rings. In particular, $V_R(J)$ is finitely spanned R-projective if J is R-central separable [Theorem 5.4]. Applying the results on central simple algebras in [3, pp. 272 and 285], one can prove the next proposition in the same manner as Proposition 8.3.

PROPOSITION 8.4. *Let J be R-central separable such that $J = J(p, q)$, $p \geqslant 3$. Then $\tau[U_R(J)] = V_R(J)$. Moreover, τ is an isomorphism of $U_R(J)$ onto $V_R(J)$ if $p \geqslant 4$ or $p = 3$ and $q = 1$ or 2.*

If (A, j) is an associative algebra with involution, let $Sk(A, j)$ be the set of j-skew elements of A. Applying the same argument for the results in [3, p. 272] yields:

PROPOSITION 8.5. *Let J be R-central separable such that $J = J(p, 1)$ or $J = J(p, 4)$, $p \geqslant 3$. Then $V_R(J) \cong \mathrm{End}_R(H[S_R(J), \pi]) \oplus \mathrm{End}_R(Sk[S_R(J), \pi])$. $H[S_R(J), \pi]$ and $Sk[S_R(J), \pi]$ are R-progenerators of respective ranks $p(p+1)/2$ and $p(p-1)/2$ if $J = J(p, 1)$ and ranks $p(2p-1)$ and $p(2p+1)$ if $J = J(p, 4)$.*

PROPOSITION 8.6. *If J is R-central separable, then $U_R(J)$ is an R-progenerator.*

Proof. We must show that $U_R(J)$ is R-projective. We can assume that $J = J(p, q)$. If $J = J(1, 1)$, then $J = R$. By Propositions 8.1–8.4, it remains to consider $J = J(3, 4)$. As usual, we can assume (R, m) is complete local Noetherian and that J/mJ is reduced. By Theorem 4.8, $J \cong H(M_3(D), j_\gamma)$ where rank $D = 4$ and $\gamma = \mathrm{diag}\{1, \gamma_2, \gamma_3\}$ for units $\gamma_i \in R$. As in the proof of Theorem 4.8, we can assume that the γ_i have square roots in R, so $J \cong H(M_3(D), j)$ [3, p. 60]. Likewise we can assume that $(-1)^{1/2} \in R$ and that D is built by a doubling process which adjoins elements q_i such that $q_i^2 = 1$. Then we can identify (D, d) with $(M_2(R), d)$ where $X^d = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) X^t \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, $X \in M_2(R)$, and t denotes transposition [3, p. 128]. Let $(C, d) = (e_{11}M_2(R), -1_C)$, and let $a \in M_2(R)$ act on $m \in C$ by $a(m) = ma$ and $(m)a = ma^d$. Then $H(M_3(C), j')$ is a J-bimodule, where j' is d-conjugate transpose [3, p. 279]. Let $\phi: U_R(J) \to V_R(J) \oplus \mathrm{End}_R\, H(M_3(C), j')$ be the natural homomorphism. ϕ is an isomorphism, since it induces an isomorphism modulo m [3, p. 284], so $U_R(J)$ is R-projective.

REFERENCES

1. H. BASS, "Lectures on Topics in Algebraic K-Theory," Tata Institute of Fundamental Research, Bombay, 1967.
2. F. DEMEYER AND E. INGRAHAM, "Separable Algebras over Commutative Rings," Lecture Notes in Mathematics 181, Springer–Verlag, Heidelberg, 1971.

3. N. Jacobson, "Structure and Representations of Jordan Algebras," Colloq. Publ. 39, American Mathematical Society, Providence, R. I., 1968.
4. N. Jacobson and K. McCrimmon, Quadratic Jordan algebras of quadratic forms with base point, *J. Indian Math. Soc.* **35** (1971), 1–45.
5. M.-A. Knus and M. Ojanguren, "Théorie de la Descente et Algèbres d'Azumaya," Lecture Notes in Mathematics 389, Springer–Verlag, Heidelberg, 1974.
6. H. F. Kreimer, A note on the outer Galois theory of rings, *Pacific J. Math.* **31** (1969), 417–432.
7. O. Loos, Separable Jordan pairs over commutative rings, *Math. Ann.* **233** (1978), 137–144.
8. K. McCrimmon, The radical of a Jordan algebra, *Proc. Nat. Acad. Sci. U.S.A.* **62** (1969), 671–678.
9. K. McCrimmon, Specialty and reflexivity of quadratic Jordan algebras, to appear.
10. G. N. Müller, Nicht assoziative separable Algebren über Ringen, *Abh. Math. Sem. Univ. Hamburg* **40** (1974), 115–131.
11. T. Nakayama, On a generalized notion of Galois extensions of a ring, *Osaka Math. J.* **15** (1963), 11–23.
12. M. Orzech and C. Small, "The Brauer Group of Commutative Rings," Lecture Notes in Pure and Applied Mathematics 11, Marcel Dekker, New York, 1975.
13. R. Wisbauer, Radikale von separablen Algebren über Ringen, *Math. Z.* **139** (1974), 9–13.