

ORBITS OF THE AUTOMORPHISM GROUP OF THE EXCEPTIONAL JORDAN ALGEBRA

BY

JOHN R. FAULKNER⁽¹⁾

Abstract. Necessary and sufficient conditions for two elements of a reduced exceptional simple Jordan algebra $\mathfrak{J}$ to be conjugate under the automorphism group $\text{Aut } \mathfrak{J}$ of $\mathfrak{J}$ are obtained. It was known previously that if $\mathfrak{J}$ is split, then such elements are exactly those with the same minimum polynomial and same generic minimum polynomial. Also, it was known that two primitive idempotents are conjugate under $\text{Aut } \mathfrak{J}$ if and only if they have the same norm class. In the present paper the notion of norm class is extended and combined with the above conditions on the minimum and generic minimum polynomials to obtain the desired conditions for arbitrary elements of $\mathfrak{J}$.

In this paper we characterize the orbits of the automorphism group $\text{Aut } \mathfrak{J}$ of a reduced exceptional simple Jordan algebra $\mathfrak{J} = \mathfrak{J}(\mathfrak{D}_3, \gamma)$ over a field Φ of characteristic not two or three. Since Jacobson [2, Theorem 9] has shown that in case the octonion (Cayley-Dickson) algebra $\mathfrak{D}$ is split then such an orbit consists of exactly those elements with the same minimum polynomial and the same generic minimum polynomial, we shall restrict our attention to octonion division algebras. In particular, we shall assume Φ is infinite.

Recall that $\mathfrak{J}(\mathfrak{D}_3, \gamma)$ is the Jordan algebra of 3×3 symmetric matrices with entries in $\mathfrak{D}$ with respect to the involution $x \mapsto \gamma^{-1} \bar{x}^t \gamma$, $\gamma = \text{diag } \{\gamma_1, \gamma_2, \gamma_3\}$, $0 \neq \gamma_i \in \Phi$, and with multiplication $x \cdot y = \frac{1}{2}(xy + yx)$, xy the usual matrix multiplication. An element $x \in \mathfrak{J}(\mathfrak{D}_3, \gamma)$ is of the form

$$(1) \quad x = \sum \alpha_i e_{ii} + \sum a_i [jk] \quad \text{with } \alpha_i \in \Phi, a_i \in \mathfrak{D}, \quad i = 1, 2, 3,$$

where (i, j, k) is a cyclic permutation of $(1, 2, 3)$ and $a[ij] = \gamma_j a e_{ij} + \gamma_i \bar{a} e_{ji}$. We have the mapping $x \mapsto x^\#$ defined by

$$(2) \quad x^\# = \sum (\alpha_j \alpha_k - \gamma_j \gamma_k n(a_i)) e_{ii} + \sum (\gamma_i (a_j a_k)^- - \alpha_i a_i) [jk]$$

where x is as in (1) and n is the norm on $\mathfrak{D}$. If $x \neq 0$ and $x^\# = 0$, we say x is of *rank one*. Also, we write $x \times y = (x + y)^\# - x^\# - y^\#$. For $x, y \in \mathfrak{J}$ write $T(x, y) = T(x \cdot y)$ where $T(z)$ is the usual trace.

Received by the editors January 27, 1970.

AMS 1969 Subject Classifications. Primary 1740.

Key Words and Phrases. Automorphism group, exceptional Jordan algebra, norm class.

(¹) This research was done while the author was a National Science Foundation Graduate Fellow.

Copyright © 1970, American Mathematical Society

For $a \in \mathfrak{F}$, we consider the quadratic form F_a on $\mathfrak{F}$ defined by $F_a(x) = T(a, x^\#)$. If e is a primitive idempotent and R is the radical of F_e , then it is known that $R = \mathfrak{F}_1(e) + \mathfrak{F}_{1/2}(e)$, where $\mathfrak{F}_i(e)$ is the Peirce i -space of e , and $\mathfrak{F}/R$ is the orthogonal direct sum of a hyperbolic plane and a subspace equivalent to $\mathfrak{F}_{23}$ equipped with the form Q where $Q(x) = T(x^\#)$ and $\mathfrak{F}_{23}$ is the Peirce (23)-space relative to an embedding of e in a set of pairwise orthogonal primitive idempotents $e = e_1, e_2, e_3$. Recall that the *norm class* of e is defined to be $\kappa(e) = -F_e(u)N^*$, where u is a non-isotropic vector with $u + R$ orthogonal to the hyperbolic plane and where $N^* = \{n(x) \neq 0 \mid x \in \mathfrak{D}\}$. In particular, $\kappa(e_{11}) = -Q(1[23])N^* = \gamma_2\gamma_3N^*$. A corollary to a result of Springer is that two primitive idempotents e and e' of $\mathfrak{F}$ lie in the same orbit of $\text{Aut } \mathfrak{F}$ if and only if $\kappa(e) = \kappa(e')$. (See [2, Theorem 6, Corollary] or [4, p. 427].)

If Ω is any extension field of Φ , we shall use the notation $N_\Omega^* = \{n(u) \neq 0 \mid u \in \mathfrak{D}_\Omega\}$ and $M_\Omega^* = \{\prod n(u_i) \neq 0 \mid u_i \in \Omega[v_i], v_i \in \mathfrak{D}\}$. Thus, $N^* = N_\Phi^* \subseteq M_\Phi^* \subseteq N_\Omega^*$.

We can now state our main result.

THEOREM. (a) *If Ω is the splitting field of the minimum polynomial of $a \in \mathfrak{F}$ and if $u \in \Omega[a] \subseteq \mathfrak{F}_\Omega$ is of rank one, then there exists a primitive idempotent $e \in \mathfrak{F}$ with $T(e, u) \neq 0$. Also, $\kappa'(u) \equiv T(e, u)\kappa(e)M_\Omega^*$ is independent of the choice of e and hence of the orbit in $\mathfrak{F}_\Omega$ of u under $\text{Aut } \mathfrak{F}$.*

(b) *If $a, a' \in \mathfrak{F}$ have the same minimum polynomial and the same generic minimum polynomial whose splitting field is Ω and if the natural isomorphism of $\Omega[a]$ with $\Omega[a']$ sending a to a' is denoted by $x \mapsto x'$, then a and a' lie in the same orbit of $\text{Aut } \mathfrak{F}$ if and only if $\kappa'(u) = \kappa'(u')$ for all $u \in \Omega[a]$ of rank one.*

The proof of the theorem consists of a case by case consideration of the various possibilities for the minimum and generic minimum polynomials, yielding in some cases a stronger result than the theorem itself. Since a can clearly be replaced by $\alpha a + \beta$ where $\alpha, \beta \in \Phi$, $\alpha \neq 0$, we have the following possibilities for the minimum polynomial $\mu(\lambda)$ and generic minimum polynomial $m(\lambda)$ of $a \in \mathfrak{F}$, $a \neq 0, 1$:

- I. $\mu(\lambda) = \lambda(\lambda - 1)$, $m(\lambda) = \lambda^2(\lambda - 1)$; i.e., a is a primitive idempotent.
- II. $\mu(\lambda) = \lambda^2$, $m(\lambda) = \lambda^3$.
- III. $\mu(\lambda) = m(\lambda) = \lambda^3$.
- IV. $\mu(\lambda) = m(\lambda) = \lambda^2(\lambda - 1)$.
- V. $\mu(\lambda) = m(\lambda) = (\lambda - \mu_1)(\lambda - \mu_2)(\lambda - \mu_3)$, $\mu_i \in \Phi$ and distinct.
- VI. $\mu(\lambda) = m(\lambda) = (\lambda - \mu_1)(\lambda - \mu_2)(\lambda - \mu_3)$, $\mu_i \in \Omega \setminus \Phi$ and distinct.
- VII. $\mu(\lambda) = m(\lambda) = (\lambda - \mu_1)(\lambda - \mu_2)(\lambda - \mu_3)$, $\mu_1 \in \Phi$, $\mu_2, \mu_3 \in \Omega \setminus \Phi$ and the μ_i are distinct.

Note that if $m(\lambda)$ has a double root then all of the roots necessarily lie in Φ .

Before considering the cases, we first prove two more general lemmas.

LEMMA 1. *If $a \in \mathfrak{F}$ and if $\{e_1, e_2, e_3\}$ is a set of pairwise orthogonal primitive idempotents, then there exists an isomorphism $\eta: \mathfrak{F} \rightarrow \mathfrak{F}(\mathfrak{D}_3, \gamma)$ for some γ such that $e_i^\eta = e_{ii}$ and $a^\eta \in \mathfrak{F}(P_3, \gamma)$ where P is a quadratic subfield of $\mathfrak{D}$.*

Proof. If in the Peirce decomposition of $\mathfrak{J}$ relative to e_1, e_2, e_3 the $(1, j)$ component of $a, a_{1j}, j=2, 3$ is not zero, then set $x_{1j}=a_{1j}$. Otherwise, let x_{1j} be an arbitrary nonzero element of $\mathfrak{J}_{1j}$. Since $\mathfrak{D}$ is a division algebra, x_{1j} is invertible in $\mathfrak{J}_{11} + \mathfrak{J}_{jj} + \mathfrak{J}_{1j}$. Thus, by the Jacobson Coordinatization Theorem (see [1]), there exists $\eta: \mathfrak{J} \rightarrow \mathfrak{H}(\mathfrak{D}_3, \gamma)$ with $e_i^\eta = e_{ii}$ and $x_{1j}^\eta = 1[1j]$. Since all of the entries of a^η with possible exception of the $(2, 3)$ component are in Φ , we see that $a^\eta \in \mathfrak{H}(P_3, \gamma)$ where P is a quadratic extension of Φ generated by Φ and a single element $u \in \mathfrak{D}, u \notin \Phi$.

In the sequel whenever we have an isomorphism $\eta: \mathfrak{J} \rightarrow \mathfrak{H}(\mathfrak{D}_3, \gamma)$ and a quadratic subfield P of $\mathfrak{D}$, we shall abuse notation and consider the elements of $\mathfrak{H}(P_3, \gamma)^{n-1}$ as endomorphisms of a vector space V over P with basis v_1, v_2, v_3 which are self-adjoint with respect to the Hermitian form h defined by $h(v_i, v_j) = \delta_{ij}\gamma_j^{-1}; i, j=1, 2, 3$.

If $yU_x = 2(y \cdot x) \cdot x - y \cdot x^2, x, y \in \mathfrak{J}$ then it is known that $U_y U_x = U_x U_y U_x$ and $yU_x = T(x, y)x - x^\# \times y$ (see [3]). In particular, if $u, v \in \mathfrak{J}$ with v of rank one, then $uU_v = T(u, v)v$. It is also well known that the elements of rank one are of the form αu where $0 \neq \alpha \in \Phi$, and u is either a primitive idempotent or $u^2 = 0$.

We say that a set of primitive idempotents $\{f_0, f_1, \dots, f_n\}$ is an (e, e') -orthogonal chain of length n if $f_0 = e, f_n = e'$, and f_i is orthogonal to $f_{i+1}, i=0, 1, \dots, n-1$.

LEMMA 2. (a) For any two primitive idempotents e, e' of $\mathfrak{J}$ there exists an (e, e') -orthogonal chain of length ≤ 3 .

(b) If e'' is distinct from e and e' , then there exists an (e, e') -orthogonal chain which does not contain e'' .

Proof. (a) If $\{e=e_1, e_2, e_3\}$ is a set of pairwise orthogonal primitive idempotents and if $T(e_i, e')=1$ for $i=1, 2, 3$, then $e' = 1U_{e'} = 3e'$, a contradiction. Hence, to show (a) we need only to show that if $T(e, e') = \alpha \neq 1$, then there exists a primitive idempotent f_1 orthogonal to both e and e' . Let $f = e'U_{1-e}$; i.e., f is the $\mathfrak{J}_0(e)$ component of e' . Clearly, f is rank one (take $e_i = e_{ii}$ and use (2)). Now $f^2 = 1U_f = (1-e)U_{e'}U_{1-e} = (1-\alpha)f$. Hence, $g = (1-\alpha)^{-1}f$ is a primitive idempotent orthogonal to e . If $f_1 = 1 - e - g$, then f_1 is as required since $T(f, e')e' = 1U_{e'}U_{1-e}U_{e'} = 1U_{(1-\alpha)e'} = (1-\alpha)^2e'$ so $T(f_1, e')=0$.

(b) We first note that if g_1 and g_2 are orthogonal primitive idempotents, then there exists a primitive idempotent $g \neq g_2$ such that g is orthogonal to g_1 but not to g_2 . Indeed, we may assume $\mathfrak{J} = \mathfrak{H}(\mathfrak{D}_3, \gamma), g_i = e_{ii}, i=1, 2$, and take

$$g = \beta^{-1}\{\gamma_2\gamma_3n(v)e_{22} + \alpha^2e_{33} + \alpha v[23]\}$$

where $0 \neq v \in \mathfrak{D}, \beta = \gamma_2\gamma_3n(v) + \alpha^2$, and since Φ is infinite $\alpha \in \Phi$ can be chosen so that $\beta \neq 0$. Since g is of rank one and $T(g) = 1$, we see that g is a primitive idempotent. The other properties of g are clear.

In the proof of (b) we may now assume that neither e nor e' is orthogonal to e'' . Using (a), we have an (e, e') -orthogonal chain $\{f_0, f_1, \dots, f_n\}$ of length $n \leq 3$. Clearly, $f_1 \neq e'' \neq f_{n-1}$ and the proof is complete.

We now consider the seven cases.

(I) In view of Springer's result mentioned above, both parts of the theorem will follow from

LEMMA 3. *If e is a primitive idempotent, then $\kappa'(e) = \kappa(e)$.*

Proof. We need to show that if $e' \in \mathfrak{F}$ is a primitive idempotent with $T(e, e') = \alpha \neq 0$, then $\kappa(e) = \alpha\kappa(e')$. If f is any primitive idempotent orthogonal to e' with $T(e, f) = \beta \neq 0$, we claim $\beta\kappa(f) = \alpha\kappa(e')$. Indeed, take $\mathfrak{F} = \mathfrak{F}(\mathfrak{D}_3, \gamma)$, $e' = e_{11}$, $f = e_{22}$, and note that (2) implies $\alpha\beta = \gamma_1\gamma_2n(a_2)$ for some $a_2 \in \mathfrak{D}$. Hence, $\alpha\kappa(e_{11}) = \alpha\gamma_2\gamma_3N^* = \beta^{-1}\gamma_1\gamma_2n(a_3)\gamma_2\gamma_3N^* = \beta\kappa(e_{22})$.

By Lemma 2, we have an (e, e') -orthogonal chain $\{f_0, \dots, f_n\}$. If $T(f_{n-1}, e) \neq 0$, the above argument shows $e' = f_n$ may be replaced by f_{n-1} . Hence, we may assume that $T(f_{n-1}, e) = 0$ (i.e., f_{n-1} is orthogonal to e) and therefore that $n=2$. Take $\mathfrak{F} = \mathfrak{F}(\mathfrak{D}_3, \gamma)$ with $e' = e_{11}$ and $f_1 = e_{22}$. Then $e = \alpha e_{11} + (1 - \alpha)e_{33} + u[31]$ for some $0 \neq u \in \mathfrak{D}$. If $0 \neq y$ is in the Peirce $(2, 3)$ -space relative to $\{e, e_{22}, 1 - e - e_{22}\}$, then $\kappa(e) = -Q(y)N^*$ and y is of the form $y = v[12] + w[23]$, $v, w \in \mathfrak{D}$. Since $e \cdot y = 0$, we have $\alpha v = -\gamma_3 \overline{wu}$. Thus,

$$\begin{aligned} -Q(y) &= -T(y^\#) = \gamma_1\gamma_2n(v) + \gamma_2\gamma_3n(w) = \{\gamma_1\gamma_3\alpha^{-2}n(u) + 1\}\gamma_2\gamma_3n(w) \\ &= \{\alpha^{-1}(1 - \alpha) + 1\}\gamma_2\gamma_3n(w) \end{aligned}$$

(since $\gamma_1\gamma_3n(u) = \alpha(\alpha - 1) = \alpha^{-1}\gamma_2\gamma_3n(w)$). Since $w=0$ would imply $v=0$ and $y=0$, we have $\kappa(e) = \alpha\gamma_2\gamma_3N^* = \alpha\kappa(e')$.

(II) This case has also been mentioned by Springer and Veldkamp (see [4, p. 427]). We give here a proof of a more detailed result. We recall that since a is of rank one, the form F_a is similar to F_e where e is any primitive idempotent of $\mathfrak{F}$ (see [2, Lemma 3]). Thus, if R is the radical of F_a , then $\mathfrak{F}/R$ is the orthogonal direct sum of a hyperbolic plane and a subspace similar to $\mathfrak{F}_{23}$ equipped with the form Q . We define the *norm class* $\kappa(a) = -F_a(u)N^*$ where u is a nonisotropic vector with $u + R$ orthogonal to the hyperbolic plane. Clearly, $\kappa(a)$ is an invariant of the orbit of a .

If e_1, e_2, e_3 are pairwise orthogonal primitive idempotents of $\mathfrak{F}$ with $T(e_i, u) = 0$, $i = 1, 2, 3$, where u is of rank one, then $u = 0$ by (2), a contradiction. Thus, the first statement of part (a) of the theorem holds. The remainder of the theorem follows in this case from

LEMMA 4. *If $0 \neq a \in \mathfrak{F}$ with $a^2 = 0$, then there exists a primitive idempotent e with $a \in \mathfrak{F}_0(e)$. If e is any such idempotent and $\sigma \in \kappa(a)$, then there exist pairwise orthogonal primitive idempotents $e = e_1, e_2, e_3$ and an isomorphism $\eta: \mathfrak{F} \rightarrow \mathfrak{F}(\mathfrak{D}_3, \delta)$ where $\delta = \text{diag}\{1, \sigma, -\sigma\}$ with $e_i^\eta = e_{ii}$, $i = 1, 2, 3$ and $a^\eta = -e_{22} + e_{33} - \sigma^{-1}[23]$. Moreover, if f is a primitive idempotent with $T(f, a) = \alpha \neq 0$, then $\kappa(a) = \alpha\kappa(f)$.*

Proof. Let $\{f_1 = f, f_2, f_3\}$ be a set of pairwise orthogonal primitive idempotents with $T(f, a) = \alpha \neq 0$. Let $\eta_1: \mathfrak{F} \rightarrow \mathfrak{F}(\mathfrak{D}_3, \gamma)$ be the isomorphism of Lemma 1 with

$\gamma_1 = 1$, so that $f_i^n = e_{ii}$ and $a^n \in \mathfrak{S}(P_3, \gamma)$. We shall use the notation established after Lemma 1. Write $v_1 a = \alpha v_1 + \alpha_2 v_2 + \alpha_3 v_3$ with $\alpha_i \in P$. If $\alpha_2 = \alpha_3 = 0$, then $a^2 = 0$ implies $\alpha^2 = 0$, a contradiction. Hence v_1 and $v_1 a$ are linearly independent. Since $h(v_1, v_1 a) = \alpha \neq 0$, v_1 and $v_1 a$ span a nonisotropic subspace W of V invariant under a . Hence, $V = W \oplus W^\perp$ and $W^\perp a \subseteq W^\perp$ since a is selfadjoint with respect to h . Since $W^\perp$ is one-dimensional, there exists $\rho \in P$ with $wa = \rho w$, $w \in W^\perp$. But $a^2 = 0$ implies $\rho = 0$ and $W^\perp a = 0$.

One easily sees that if $0 \neq u_1 \in W^\perp$,

$$u_2 = v_1 - \frac{1}{2}(\alpha^{-1} + 1)v_1 a, \quad \text{and} \quad u_3 = v_1 - \frac{1}{2}(\alpha^{-1} - 1)v_1 a,$$

then u_1, u_2, u_3 is a basis for V relative to which a has the matrix $A = -e_{22} + e_{33} + e_{23} - e_{32}$ and h the matrix $\text{diag}\{\rho, -\alpha, \alpha\}$ where $\rho = h(u_1, u_1) \neq 0$. Since $h(u_1, v_1) = h(u_1, v_1 a) = 0$, we have $u_1 = \rho_2 v_2 + \rho_3 v_3$ where $\rho_i \in P$ and $\alpha_2 \rho_2 \gamma_2^{-1} + \alpha_3 \rho_3 \gamma_3^{-1} = 0$. In particular $n(\alpha_2)n(\rho_2)\gamma_2^{-2} = n(\alpha_3)n(\rho_3)\gamma_3^{-2}$. Also, since $a^2 = 0$, we have

$$\alpha^2 + \gamma_2^{-1}n(\alpha_2) + \gamma_3^{-1}n(\alpha_3) = 0.$$

If say $\alpha_2 \neq 0$, then

$$\begin{aligned} \rho &= h(u_1, u_1) = n(\rho_2)\gamma_2^{-1} + n(\rho_3)\gamma_3^{-1} = n(\alpha_2)^{-1}n(\alpha_3)n(\rho_3)\gamma_2\gamma_3^{-2} + n(\rho_3)\gamma_3^{-1} \\ &= \gamma_2\gamma_3^{-1}(\gamma_2^{-1}n(\alpha_2) + \gamma_3^{-1}n(\alpha_3))n(\rho_3)n(\alpha_2)^{-1} \\ &= -\gamma_2\gamma_3^{-1}\alpha^2 n(\rho_3)n(\alpha_2)^{-1} \in -\kappa(f). \end{aligned}$$

Similarly, if $\alpha_3 \neq 0$, then $\rho \in -\kappa(f)$. Thus, $h' = \rho^{-1}h$ is a form similar to h and $h'(u_i, u_j) = \delta_{ij}\lambda_j^{-1}$, $i, j = 1, 2, 3$, where $\lambda_1 = 1$ and $\lambda_2 = -\lambda_3 \in \alpha\kappa(f)$. We have an isomorphism η_2 of $\mathfrak{S}(P_3, \gamma)^{\eta_1^{-1}}$ onto $\mathfrak{S}(P_3, \lambda)$ mapping a onto A which can be extended to an isomorphism $\eta_2: \mathfrak{S} \rightarrow \mathfrak{S}(\mathfrak{D}_3, \lambda)$. (Use the Jacobson Coordinatization Theorem with $e_{ii}^{\eta_2^{-1}}$, $i = 1, 2, 3$; $1[12]^{\eta_2^{-1}}$; and $1[13]^{\eta_2^{-1}}$.)

Clearly the first statement of the lemma holds. If now $a \in \mathfrak{S}_0(e)$ for a primitive idempotent e , then after imbedding e in a set $\{f_1 = f, f_2 = e, f_3\}$ of pairwise orthogonal primitive idempotents with $T(f, a) \neq 0$, we may argue as before to obtain an isomorphism $\eta_2: \mathfrak{S} \rightarrow \mathfrak{S}(\mathfrak{D}_3, \lambda)$ with $a^{\eta_2} = A$. Since $v_2 = v_2 e$, we have $h(v_2, v_1 a) = h(v_2, v_1 a e) = 0$ so $v_2 \in W^\perp$. Thus, $e^{\eta_2} = e_{11}$. To complete the proof of the lemma, we need only show that $\kappa(a) = \alpha\kappa(f)$ and that λ_2 may be replaced by any $\sigma \in \kappa(a)$. The first follows from a direct calculation which shows that if R is the radical of F_A in $\mathfrak{S}(\mathfrak{D}_3, \lambda)$ then $e_{11} + R$ and $e_{22} + R$ span a hyperbolic plane in $\mathfrak{S}(\mathfrak{D}_3, \lambda)/R$ and $-F_A(1[12])N^* = \lambda_2 N^* = \alpha\kappa(f)$. The second follows by considering the isomorphism $\eta: \mathfrak{S} \rightarrow \mathfrak{S}(\mathfrak{D}_3, \delta)$ (with $\delta_1 = 1$) given by the Jacobson Coordinatization Theorem using $e_{ii}^{\eta^{-1}}$, $i = 1, 2, 3$; $u[12]^{\eta^{-1}}$; and $u[13]^{\eta^{-1}}$ where $u \in \mathfrak{D}$ with $\sigma = \lambda_2 n(u)$. We have $\delta_2 = -Q(u[12]) = \lambda_2 n(u) = \sigma$ and $\delta_3 = -Q(u[13]) = -\sigma$. Since $2u[12] \cdot u[13] = n(u)[23]$, we see $a^\eta = A$.

(III) This case can be handled by proving that any two elements of this type are in the same orbit of $\text{Aut } \mathfrak{S}$ (see [2, §6, Exercise 4]). We use Lemma 1 and the notation following it. Choose $v = v_1, v_2$, or v_3 so that $va^2 \neq 0$. Thus, $w_i = va^{i-1}$, $i = 1, 2, 3$,

is a basis for V relative to which a has the matrix $e_{12} + e_{23}$ and h the matrix $h_1 e_{11} + h_2(e_{12} + e_{21}) + h_3(e_{13} + e_{22} + e_{31})$ where $h_i \in \Phi$, $i = 1, 2, 3$, since a is selfadjoint with respect to h and $a^3 = 0$. Also, $h_3 \neq 0$. Replacing v first by $w_1 - \frac{1}{2}h_2 h_3^{-1} w_2$ and then by $w_1 - \frac{1}{2}h_1 h_3^{-1} w_3$, we may assume $h_1 = h_2 = 0$. Replacing h by $h_3^{-1}h$, we see there is an isomorphism η of a simple subalgebra $\mathfrak{A}$ of $\mathfrak{F}$ containing a onto the algebra of all symmetric matrices over Φ relative to the involution $X \mapsto Q^{-1}X^tQ$ where $Q = e_{13} + e_{22} + e_{31}$ such that $a^n = e_{12} + e_{23}$. If a' has the same minimum polynomial as a and if η' is the corresponding isomorphism, then $\eta\eta'^{-1}$ can be extended to an automorphism of $\mathfrak{F}$ by [2, Theorem 3].

(IV) If $e = a^2$ and $u = a(a-1)$, then e and u are elements of rank one. Indeed, e is an idempotent of trace 1 and hence primitive and $u^2 = 0$. Moreover, $u \in \mathfrak{F}_0(e)$. Using Lemma 4, we see that if $\sigma \in \kappa(u) = \kappa'(u)$, then there exists an isomorphism $\eta: \mathfrak{F} \rightarrow \mathfrak{F}(\mathfrak{D}_3, \delta)$ where $\delta = \text{diag}\{1, \sigma, -\sigma\}$ with $e^n = e_{11}$ and $u^n = -e_{22} + e_{33} - \sigma^{-1}[23]$. Since $a = e - u$, we have $a^n = e_{11} + e_{22} - e_{33} + \sigma^{-1}[23]$ and the theorem follows for this case.

(V) Let $e_i = (\mu_i - \mu_j)^{-1}(\mu_i - \mu_k)^{-1}(a - \mu_j)(a - \mu_k)$ where i, j, k are distinct. Clearly the e_i are pairwise orthogonal primitive idempotents. If $\gamma = \text{diag}\{1, \gamma_2, \gamma_3\}$ with $\gamma_2 \in \kappa(e_3) = \kappa'(e_3)$ and $\gamma_3 \in \kappa(e_2) = \kappa'(e_2)$, then by the Jacobson Coordinatization Theorem we have an isomorphism $\eta: \mathfrak{F} \rightarrow \mathfrak{F}(\mathfrak{D}_3, \gamma)$ such that $e_i^n = e_{ii}$. Since $a = \sum \mu_i e_i$, we have $a^n = \sum \mu_i e_{ii}$, and we are done in this case.

(VIa) and (VIIa) Throughout the last two cases we let

$$e_i = (\mu_i - \mu_j)^{-1}(\mu_i - \mu_k)^{-1}(a - \mu_j)(a - \mu_k)$$

where i, j, k are distinct. The e_i are primitive idempotents in $\mathfrak{F}_\Omega$ and every element of rank one in $\Omega[a]$ is of the form αe_i , $i = 1, 2$, or 3 ; $\alpha \in \Omega$. If π is an element of the Galois group $\text{Gal}(\Omega/\Phi)$, let π also denote the corresponding permutation of $\{1, 2, 3\}$ and also the π -semiautomorphism of $\mathfrak{F}_\Omega$ fixing $\mathfrak{F}$. Thus, $\mu_i^\pi = \mu_{i\pi}$ and $e_i^\pi = e_{i\pi}$, $i = 1, 2, 3$.

We first note that if $u \in \Omega[a]$ is of rank one and $u \neq \rho v$, $v \in \mathfrak{F}$, $\rho \in \Omega$, then $T(u, e) = 0$ for at most one primitive idempotent $e \in \mathfrak{F}$. To see this, write $u = \alpha e_i$. In case (VI), since $\text{Gal}(\Omega/\Phi)$ is transitive on $\{1, 2, 3\}$, we see $T(e, e_i) = 0$ implies $T(e) = T(e, 1) = 0$, a contradiction. In case (VII) $i \neq 1$ and $T(e, e_i) = 0$ implies $T(e, e_{i\pi}) = 0$ where $\pi = (2, 3)$. Hence $e = e_1$.

Now let $u \in \Omega[a]$ be of rank one and let $e \in \mathfrak{F}$ be a primitive idempotent with $T(e, u) = \alpha \neq 0$. If $u = \beta v$ with $v \in \mathfrak{F}$, $\beta \in \Omega$, we may assume we are in case (VII) and $v = e_1$. Thus, by (I) we see $\kappa(e) = T(e, e_1)\kappa(e_1) = \alpha\beta^{-1}\kappa(e_1)$ and $T(e, u)\kappa(e)M_\Omega^* = \beta\kappa(e_1)M_\Omega^*$ is independent of the choice of e . If $u \neq \beta v$ for any $v \in \mathfrak{F}$, $\beta \in \Omega$, then if $e' \in \mathfrak{F}$ is a primitive idempotent with $T(e', u) = \alpha' \neq 0$, then by the above note and Lemma 2(b), we may assume e is orthogonal to e' . Using Lemma 1 with $e_1 = e$, $e_2 = e'$, and $e_3 = 1 - e_2 - e_3$, we get $\eta: \mathfrak{F} \rightarrow \mathfrak{F}(\mathfrak{D}_3, \gamma)$ with $e_i^n = e_{ii}$ and $a^n \in \mathfrak{F}(P_3, \gamma)$. Extending η to $\mathfrak{F}_\Omega$, we have $u^n \in \mathfrak{F}(P'_3, \gamma)$ where $P' = P_\Omega$. Thus by (2), $\alpha\alpha' = \gamma_1\gamma_2\eta(v)$ for some $v \in P'$. Hence, $\alpha\kappa(e)M_\Omega^* = (\alpha\alpha')\alpha'\gamma_2\gamma_3M_\Omega^* = \alpha'\gamma_1\gamma_2M_\Omega^* = \alpha'\kappa(e')M_\Omega^*$.

(VIb) Let η be given by Lemma 1 so that $a^n \in \mathfrak{S}(P_3, \gamma)$ and use the notation following Lemma 1. If $0 \neq v \in V$, then v, va, va^2 form a basis for V relative to which a has the matrix

$$A = \begin{vmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ \delta_1 & \delta_2 & \delta_3 \end{vmatrix}$$

where $\delta_1 = \mu_1\mu_2\mu_3$, $\delta_2 = -(\mu_1\mu_2 + \mu_2\mu_3 + \mu_3\mu_1)$, and $\delta_3 = \mu_1 + \mu_2 + \mu_3$, and the form h has the matrix

$$H = \begin{vmatrix} h_1 & h_2 & h_3 \\ h_2 & h_3 & h_4 \\ h_3 & h_4 & h_5 \end{vmatrix}$$

where $h_i \in \Phi$. Clearly we have a subalgebra $\mathfrak{A}$ of $\mathfrak{S}(P_3, \gamma)^{n-1}$ which we may view as endomorphisms of $W = \Phi v + \Phi va + \Phi va^2$ symmetric with respect to $h|W$. Also, $a \in \mathfrak{A}$.

Now let P be any subfield $\subset \mathfrak{D}$. Since H is diagonalizable, there is an isomorphism $\tau: \mathfrak{A} \rightarrow \mathfrak{S}(\Phi_3, \gamma)$ for some γ which may be extended to $\tau: \mathfrak{S} \rightarrow \mathfrak{S}(\mathfrak{D}_3, \gamma)$. Now $\mathfrak{S}(P_3, \gamma)^{n-1}$ may be viewed as endomorphisms of W_P selfadjoint with respect to the Hermitian form h defined by H . If $0 \neq v' \in W_P$, then relative to the basis $v', v'a, v'a^2$, a has the matrix A and h has the matrix H' where h'_i replaces h_i in H . In particular, if $0 \neq x \in P_\Omega$ with $x = r(\mu_1)$, $r \in P[\lambda]$, let $v' = vr(a)$. Then since $v'a^i = va^i r(a)$ and $HA^i = AH$, we see $H = RH\bar{R}^t = R\bar{R}H$ where $R = r(A)$. Induction shows that if $0 \neq x_i \in P_\Omega^{(i)}$, $i = 1, 2, \dots, n$, if $x_i = r_i(\mu_1)$, $r_i \in P^{(i)}[\lambda]$, and if $R_i = r_i(A)$, then there is an isomorphism τ of a subalgebra of $\mathfrak{S}$ containing a onto the algebra of all matrices X over Φ with $H'X^t = XH'$ where $H' = R_1\bar{R}_1 \cdots R_n\bar{R}_nH$ such that $a^t = A$.

Since there exists $w \in W$ with $h(w, w) \neq 0$ and since $h|W$ can be diagonalized by a basis for W containing w , we see that there is a primitive idempotent $e \in \mathfrak{A}$ with $we = w$. Replacing v by w , we may assume $h_1 = h(v, v) \neq 0$ and $ve = v$. Replacing h by $h_1^{-1}h$, we may also assume $h_1 = 1$. With these normalizations, we shall now give an expression for H in terms of $\alpha = T(e, e_1) \in \Omega$. If

$$Q = \begin{vmatrix} 0 & 0 & 1 \\ 0 & 1 & \delta_3 \\ 1 & \delta_3 & \delta_2 + \delta_3^2 \end{vmatrix}$$

then

$$Q^{-1} = \begin{vmatrix} -\delta_2 & -\delta_3 & 1 \\ -\delta_3 & 1 & 0 \\ 1 & 0 & 0 \end{vmatrix} \quad \text{and} \quad QA^t = AQ.$$

If $S = HQ^{-1}$, then $AS = HA^tQ^{-1} = SA$. Let S be the endomorphism of W corresponding to S . We have $vs = vp(a)$ where $p(\lambda) = h_1\lambda^2 + (h_2 - \delta_3h_1)\lambda + (h_3 - \delta_3h_2 - \delta_2h_1) \in \Phi[\lambda]$. Hence, $va^ts = vsa^t = vp(a)a^t = va^tp(a)$ and $S = p(A)$. In Ω , we calculate

$$\begin{aligned} p(\mu_1) &= h_3 + (\mu_1 - \delta_3)h_2 + (\mu_1^2 - \delta_3\mu_1 - \delta_2)h_1 = h_3 - (\mu_2 + \mu_3)h_2 + \mu_2\mu_3h_1 \\ &= h(v, v(a^2 - (\mu_2 + \mu_3)a + \mu_2\mu_3)) = (\mu_1 - \mu_2)(\mu_1 - \mu_3)h(v, ve_1) \\ &= (\mu_1 - \mu_2)(\mu_1 - \mu_3)\alpha. \end{aligned}$$

Thus, if $\tilde{Q} = t(A)Q$ where $t(\lambda) \in \Phi[\lambda]$ with $t(\mu_1) = (\mu_1 - \mu_2)(\mu_1 - \mu_3)$ and if $\alpha = q(\mu_1)$ where $q \in \Phi[\lambda]$, then $H = SQ = p(A)Q = t(A)q(A)Q = q(A)\tilde{Q}$.

Now let a' have the same minimum polynomial as a . Using the normalization above we have (with obvious notation) $H' = q'(A)\tilde{Q}$ where $T(e', e'_1) = \alpha' = q'(\mu_1)$. If $\kappa'(e_1) = \kappa'(e'_1)$, then $\alpha\kappa(e)M_\Omega^* = \alpha'\kappa(e')M_\Omega^*$ or $\alpha'\alpha^{-1} \in \beta M_\Omega^*$ where $0 \neq \beta \in \kappa(e)\kappa(e') \subseteq \Phi$. Write $\alpha'\alpha^{-1} = \beta n(x_1) \cdots n(x_n)$ with $x_i \in \Omega[v_i]$, $v_i \in \mathfrak{D} \setminus \Phi$, $i = 1, 2, \dots, n$. Since $\Omega[v_i] = P_\Omega^{(i)}$ where $P^{(i)} = \Phi[v_i]$, we may write $x_i = r_i(\mu_1)$ with $r_i \in P^{(i)}[\lambda]$. Thus, $\alpha'\alpha^{-1} = \beta r_1(\mu_1)\bar{r}_1(\mu_1) \cdots r_n(\mu_1)\bar{r}_n(\mu_1)$, $q'(A)q(A)^{-1} = \beta R_1\bar{R}_1 \cdots R_n\bar{R}_n$ where $R_i = r_i(A)$, and $H' = q'(A)q(A)^{-1}H = \beta R_1\bar{R}_1 \cdots R_n\bar{R}_nH$. Using the isomorphism τ above, we can easily construct an isomorphism σ mapping a subalgebra of $\mathfrak{F}$ (isomorphic to $\mathfrak{F}(\Phi_3, \gamma)$ for some γ) containing a onto a subalgebra of $\mathfrak{F}$ containing a' such that $a^\sigma = a'$. Clearly, σ can be extended to an automorphism of $\mathfrak{F}$. (Use the Jacobson Coordinatization Theorem or [2, Theorem 3].) We remark that the above proof was suggested by the methods used by Williamson in [5].

(VIIb) The methods of the previous case could be applied here, but we prefer to prove a somewhat stronger result using a Galois argument. We shall show that $\kappa'(u) = \kappa'(u')$ in the statement of (b) can be replaced in this case by $\kappa_\Omega(u) = \kappa_\Omega(u')$ where κ_Ω is the norm class in $\mathfrak{F}_\Omega$. This implies that a and a' lie in the same orbit of $\text{Aut } \mathfrak{F}$ if and only if they lie in the same orbit of $\text{Aut } \mathfrak{F}_\Omega$.

Let $\eta: \mathfrak{F} \rightarrow \mathfrak{F}(\mathfrak{D}_3, \gamma)$ be given by Lemma 1 so that $a^n \in \mathfrak{F}(P_3, \gamma)$. Let $\mathfrak{A} = \mathfrak{F}(\Phi_3, \gamma)^{\eta^{-1}}$. We shall show $\mathfrak{A}_\Omega \cap \mathfrak{F}_{\Omega 12} \neq 0$ (where $\mathfrak{F}_{\Omega 12}$ is the Peirce (1, 2)-space of $\mathfrak{F}_\Omega$ relative to $e_i = (\mu_i - \mu_j)^{-1}(\mu_i - \mu_k)^{-1}(a - \mu_j)(a - \mu_k)$; i, j, k distinct). If $\pi = (2, 3)$, then $\mathfrak{A}_\Omega U_{e_1, e_2} = 0$ implies $\mathfrak{A}_\Omega U_{e_1, e_3} = (\mathfrak{A}_\Omega U_{e_1, e_2})^\pi = 0$ and $\mathfrak{A}_\Omega \cap \mathfrak{F}_{\Omega 1}(e_1) = 0$. If $f_i = e_i^{\eta^{-1}}$, $i = 1, 2, 3$, then $T(f_i, e_1) \neq 0$ for some i ; say $i = 1$. If the Peirce $\frac{1}{2}$ -component of f_1 relative to e_1 is zero, then (2) implies $f_1 = e_1$. But $\mathfrak{A}_\Omega \cap \mathfrak{F}_{\Omega 1}(f_1) = 0$ is a contradiction. Hence, we may choose $0 \neq u_{12} \in \mathfrak{A}_\Omega \cap \mathfrak{F}_{\Omega 12}$. Let $u_{13} = u_{12}^2$ and $u_{23} = u_{12} \cdot u_{13}$. If M is the space spanned by $e_1, e_2, e_3, u_{12}, u_{13}$, and u_{23} over Ω , then since $M \subseteq \mathfrak{A}_\Omega$ and $\dim M = \dim \mathfrak{A}_\Omega$, we have $M = \mathfrak{A}_\Omega$. Since $\kappa_\Omega(e_3) = \kappa_\Omega(e'_3)$, we can find $u'_{12} \in \mathfrak{F}'_{\Omega 12}$ (the Peirce (1, 2)-space of $\mathfrak{F}'_\Omega$ relative to e'_1, e'_2, e'_3) such that $Q(u'_{12}) = Q(u_{12})$. Now $u'_{13} \equiv u_{12}'^2 \in \mathfrak{F}'_{\Omega 13}$ and $Q(u'_{13}) = T(u_{13}^\#) = T(u_{12}'^\#) = Q(u_{12})^\# = Q(u_{13})$. Let $\rho: \mathfrak{F}_\Omega \rightarrow \mathfrak{F}(\mathfrak{D}_{\Omega 3}, \delta)$ be an isomorphism given by the Jacobson Coordinatization Theorem such that $e_i^\rho = e_{ii}$, $u_{12}^\rho = 1[12]$, and $u_{13}^\rho = 1[13]$, and let $\rho': \mathfrak{F}_\Omega \rightarrow \mathfrak{F}(\mathfrak{D}_{\Omega 3}, \delta')$ be a corresponding isomorphism for e'_i, u'_{12} , and u'_{13} . Since $Q(u_{12}) = Q(u'_{12})$ and $Q(u_{13}) = Q(u'_{13})$, we may take $\delta = \delta'$. Hence, $\sigma = \rho\rho'^{-1}$ is an automorphism of $\mathfrak{F}_\Omega$ such that

$e_i^\sigma = e_i'$; i.e., $a^\sigma = a'$. Now $e_i^{\sigma\pi} = e_i'^\pi = e_{i\pi}^\sigma = e_i^{\pi\sigma}$, $i = 1, 2, 3$, $u_{1j}^{\sigma\pi} = u_{1j}'^\pi = u_{1j\pi}^\sigma = u_{1j}^{\pi\sigma}$, $j = 2, 3$, and $u_{23}^{\sigma\pi} = (u_{12} \cdot u_{13})^{\sigma\pi} = (u_{12}' \cdot u_{13}')^\pi = u_{13}' \cdot u_{12}' = u_{23}^{\pi\sigma}$. Hence $\mathfrak{A}^\sigma$ is pointwise fixed by π . Since π generates $\text{Gal}(\Omega/\Phi)$, we see $\mathfrak{A}^\sigma \subset \mathfrak{F}$ and $\sigma|_{\mathfrak{A}}$ is an isomorphism of $\mathfrak{A}$ into $\mathfrak{F}$ such that $a^\sigma = a'$. Clearly, $\sigma|_{\mathfrak{A}}$ extends to $\mathfrak{F}$.

REFERENCES

1. N. Jacobson, *A coordinatization theorem for Jordan algebras*, Proc. Nat. Acad. Sci. U.S.A. **48** (1962), 1154–1160. MR **25** #3971.
2. ———, *Structure and representations of Jordan algebras*. Chapter IX, Amer. Math. Soc. Colloq. Publ., vol. 39, Amer. Math. Soc., Providence, R. I., 1969.
3. K. McCrimmon, *The Freudenthal-Springer-Tits constructions of exceptional Jordan algebras*, Trans. Amer. Math. Soc. **139** (1969), 495–510. MR **39** #276.
4. T. A. Springer and F. D. Veldkamp, *Elliptic and hyperbolic octave planes*. I, II, III, Nederl. Akad. Wetensch. Proc. Ser. A **66**=Indag. Math. **25** (1963), 413–451. MR **27** #5166a, b, c.
5. J. Williamson, *The equivalence of non-singular pencils of Hermitian matrices in an arbitrary field*, Amer. J. Math. **57** (1935), 475–490.

UNIVERSITY OF VIRGINIA,
CHARLOTTESVILLE, VIRGINIA 22901