AUTOMORPHISM GROUPS OF JORDAN ALGEBRAS

E. RAY BOBO

Introduction and the Jordan algebras. In his development of a structure theory for Jordan algebras of characteristic two, E.C. Paige [1] introduces an important class of central simple Jordan algebras $S[2^n]$. It is the purpose of this paper to completely determine the automorphism groups of the algebras $S[2^n]$. The automorphisms will be represented as matrices operating on a natural basis for the underlying vector space of the algebra. Using this characterization, generators and relations will be obtained for each of the automorphism groups. In this way, we will produce an infinite family of finite 2-groups.

DEFINITION. Let $S[2^n]$ be the vector space over the field J_2 of two elements with basis $\{u_{-1}, u_0, u_1, \cdots, u_m\}$ where $m = 2^n - 2$ for $n \geq 2$. Let

$$u_0 u_i = u_i \text{ for } -1 \leq i \leq 2^n - 2,$$

$$u_{-1}^2 = 0,$$

$$u_j u_{-1} = u_{j-1} \text{ for } 0 \leq j \leq 2^n - 2,$$

$$u_i u_j = u_j u_i \text{ for } -1 \leq i, j \leq 2^n - 2.$$

For $n = 2$, set $u_1 u_2 = u_1^2 = u_2^2 = 0$. For $k > 2$, consider $S[2^k]$ as a subspace of $S[2^{k+1}]$. Then define

$$u_{r+i} u_j = g_{i,j} u_{r+i+j}$$

for $r = 2^k$, $-1 \leq i \leq r - 2$, and $0 \leq j \leq r - 2$ when $u_i u_j = g_{i,j} u_{i+j}$ where $g_{i,j}$ is 0 or 1. Also define

$$u_{r+i} u_{r+j} = 0$$

for $r = 2^k$ and $-1 \leq i, j \leq r - 2$.

1. The automorphisms.

DEFINITION. Define a set of 2^n by 2^n matrix forms A_n inductively as follows: Let

Received April 18, 1967.

This paper represents a portion of the author's doctoral dissertation written at the University of Virginia under the direction of Professor Eugene C. Paige.

$$A_2 = \begin{pmatrix} 1 & 0 & a_1 & a_2 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

where a_1 and a_2 are elements of the field J_2. Set $r = 2^k$, $s = 2^{k-1}$, and $t = 2^{k+1}$. Assume that $A_k = (b_{i,j})$ is defined in terms of elements a_e of J_2 where $1 \leq e \leq r-2$ and $-1 \leq i, j \leq r-2$. Then define $A_{k+1} = (c_{i,j})$ in terms of elements a_e of J_2 where $1 \leq e \leq t-2$ and $-1 \leq i, j \leq t-2$ by

$$\begin{cases} c_{i,j} = b_{i,j} \\ c_{r+i,\,r+j} = b_{i,j} \\ c_{r+i,\,j} = 0 \end{cases}$$

for $-1 \leq i, j \leq r-2$, and

$$\begin{cases} c_{i,\,r+j} = h_{i,\,s+j}a_{s+e} \\ c_{i,\,r+s+j} = h_{i,\,s+j}a_{r+e} \\ c_{s+i,\,r+s+j} = h_{i,\,s+j}a_{s+e} \\ c_{s+i,\,r+j} = 0 \end{cases}$$

for $-1 \leq i, j \leq s-2$ and $1 \leq e \leq r-2$ when $b_{i,\,s+j} = h_{i,\,s+j}a_e$ where $h_{i,\,s+j}$ is 0 or 1.

THEOREM 1. *The matrices of form A_n are precisely the matrices of the automorphisms of the Jordan algebra $S[2^n]$ over the field J_2 with respect to the canonical basis.*

Proof. The proof is by induction on n. It is straightforward to show that the theorem is true for $n = 2$.

For the remainder of this paper, set $r = 2^k$, $s = 2^{k-1}$, and $t = 2^{k+1}$. Let $\mathscr{A}_n$ be the set of all automorphisms of $S[2^n]$ over J_2. Suppose that the matrices of form A_k are precisely the matrices of the elements of $\mathscr{A}_k$ with respect to the canonical basis elements u_i where $-1 \leq i \leq r-2$. We will show that the matrices of form A_{k+1} are precisely the matrices of the elements of $\mathscr{A}_{k+1}$ with respect to the canonical basis elements u_i where $-1 \leq i \leq t-2$.

Let $C \in \mathscr{A}_{k+1}$ and denote

https://doi.org/10.1017/S0027763000026647 Published online by Cambridge University Press

$$C(u_i) = \sum_{e=-1}^{t-2} c_{i,e}u_e \text{ for } -1 \leq i \leq t-2.$$

Let $\delta_{i,j}$ denote the Kronecker delta. It is fairly easy to verify each of the following relations:

$$c_{0,e} = \delta_{0,e} \text{ for } -1 \leq e \leq t-2,$$

$$c_{i,0} = \delta_{i,0} \text{ for } -1 \leq i \leq t-2,$$

(1) $$c_{i,-1} = \delta_{i,-1} \text{ for } -1 \leq i \leq t-2,$$

(2) $$c_{i,r-1} = c_{i+1,r} \text{ for } 0 \leq i \leq t-3.$$

A straightforward, but lengthy, simultaneous double induction yields that:

(3)
$$\begin{cases} c_{i,e} = 0 \text{ for } -1 \leq e < i \leq t-2 \\ c_{i,i} = 1 \text{ for } -1 \leq i \leq t-2 \\ c_{i,i+1} = 0 \text{ for } -1 \leq i \leq t-1. \end{cases}$$

We shall next prove that

(4) $$c_{i,j} = \delta_{i,j} \text{ for } -1 \leq i, j \leq t-2 \text{ and } i \equiv 0 \pmod 2.$$

By (3), we know that $C(u_{t-2}) = u_{t-2}$. Suppose $C(u_{t-2e+2}) = u_{t-2e+2}$ where $2 \leq e \leq r$. We need to show that $C(u_{t-2e}) = u_{t-2e}$.

Now $$C(u_{t-2e+1}) = C(u_{t-2e+2})C(u_{-1}) =$$

$$(u_{t-2e+2})(u_{-1} + \sum_{h=1}^{t-2} c_{-1,h}u_h) =$$

$$u_{t-2e+1} + \sum_{j=1}^{2e-4} c_{-1,j}g_{j,t-2e+2}u_{t-2e+2+j}$$

where $u_m u_n = g_{m,n}u_{m+n}$. (Our convention is that summations from m to n are taken to be zero whenever $m > n$.) Then $C(u_{t-2e}) = C(u_{t-2e+1})C(u_{-1}) =$

$$u_{t-2e} + \sum_{h=1}^{2e-3} c_{-1,h}g_{h,t-2e+1}u_{t-2e+1+h} +$$

$$\sum_{j=1}^{2e-4} c_{-1,j}g_{j,t-2e+2}u_{t-2e+1+j} +$$

$$\sum_{h,j=1}^{2e-5} c_{-1,h}c_{-1,j}g_{j,t-2e+2}g_{h,t-2e+2+j}u_{t-2e+2+j+h} =$$

$$u_{t-2e} + c_{-1,2e-3}g_{2e-3,t-2e+1}u_{t-2} +$$

$$\sum_{j=1}^{2e-4} c_{-1,j}(g_{j,t-2e+1} + g_{j,t-2e+2})u_{t-2e+1+j} +$$

https://doi.org/10.1017/S0027763000026647 Published online by Cambridge University Press

$$\sum_{j=1}^{e-2} (c_{-1,j})^2 g_{j,t-2e+2} g_{j,t-2e+2+j} u_{t-2e+2+2j} +$$
$$\sum_{h=1}^{e-3} \left[\sum_{j=h+1}^{2e-4-h} c_{-1,h} c_{-1,j} (g_{h,t-2e+2} g_{j,t-2e+2+h} +$$
$$g_{j,t-2e+2} g_{h,t-2e+2+j}) u_{t-2e+2+h+j} \right].$$

It can easily be seen that for $2 \leq e \leq r$ and $1 \leq j \leq t-4$ we have both $g_{2e-3,t-2e+1} = 0$ and $g_{j,t-2e+1} = g_{j,t-2e+2}$. Also, for $3 \leq e \leq r$ and $1 \leq j \leq e-2$, we have

$$g_{j,t-2e+2} g_{j,t-2e+2+j} = 0.$$

It can be shown that

$$g_{h,t-2e+2} g_{j,t-2e+2+h} = g_{j,t-2e+2} g_{h,t-2e+2+j}$$

for $4 \leq e \leq r$, $1 \leq h \leq e-3$, and $h+1 \leq j \leq 2e-4-h$. Therefore, $C(u_{t-2e}) = u_{t-2e}$ and (4) is obtained.

It now follows immediately from (2) and (4) that

(5) $$c_{i,r-1} = \delta_{i,r-1} \text{ for } 0 \leq i \leq t-3.$$

We now claim that:

(6) If B is defined by

$$B(u_i) = \sum_{e=-1}^{r-2} c_{i,e} u_e \text{ for } -1 \leq i \leq r-2,$$

then $B \in \mathscr{A}_k$.

Let $-1 \leq i, j \leq r-2$. Since $C(u_i u_j) = C(u_i) C(u_j)$, a linear independence argument yields that

$$B(u_i u_j) = B(u_i) B(u_j) + (c_{i,-1} c_{j,r-1} + c_{i,r-1} c_{j,-1}) u_{r-2}.$$

But by (1) and (5), we have

$$c_{i,-1} c_{j,r-1} + c_{i,r-1} c_{j,-1} = 0$$

in all possible cases. Hence $B \in \mathscr{A}_k$.

A rather combinatorial, several case argument utilizing (1) and (3) proves the following partial converse to (6):

(7) Let $B \in \mathscr{A}_k$ with

https://doi.org/10.1017/S0027763000026647 Published online by Cambridge University Press

$$B(u_i) = \sum_{e=-1}^{r-2} b_{i,e}u_e \text{ for } -1 \leq i \leq r-2.$$

If C is defined by

$$C(u_i) = \sum_{e=-1}^{r-2} b_{i,e}u_e \text{ for } -1 \leq i \leq r-2$$

and

$$C(u_i) = \sum_{e=r-1}^{t-2} b_{i-r,e-r}u_e \text{ for } r-1 \leq i \leq t-2,$$

then $C \in \mathscr{A}_{k+1}$.

It *now* follows immediately from (6), (7), and the induction hypothesis that the matrix $(c_{i,j})$ of an element of $\mathscr{A}_{k+1}$ has

$$c_{i,j} = b_{i,j} \text{ for } -1 \leq i, j \leq r-2$$

where $(b_{i,j})$ is a matrix of form A_k. Note that (3) says $c_{r+i,j} = 0$ for $-1 \leq i, j \leq r-2$. That the matrix of an element of $\mathscr{A}_{k+1}$ satisfies each of the five other properties required for it to be of the form A_{k+1} is reasonably direct to establish by invoking some combinatorics, linear independence, (3), and (4).

Conversely, let $A = (c_{i,j})$ where $-1 \leq i, j \leq t-2$ be any matrix of form A_{k+1}. We will show that $A \in \mathscr{A}_{k+1}$. It is clear from the definition, that appropriate analogues of (3) and (4) are true for matrices of form A_{k+1}. Since A is triangular with non-zero diagonal entries, A is a non-singular linear transformation of $S[2^{k+1}]$ onto itself.

We must prove that if $u_iu_j = g_{i,j}u_{i+j}$, then

$$g_{i,j}A(u_{i+j}) = A(u_i)A(u_j)$$

for $-1 \leq i, j \leq t-2$. This is trivial when both i and j are even. When i is even and j is odd, it follows since

$$g_{i,j}c_{i+j,i+n} = c_{j,n}g_{i,n}$$

for $j+2 \leq n \leq t-2-i$.

Suppose i and j are both odd. Since

$$c_{i,i+h}g_{j,i+h} = c_{j,j+h}g_{i,j+h}$$

for $2 \leq h \leq t-2-i-j$, we have $A(u_i)A(u_j) =$

$$g_{i,j}u_{i+j} + \sum_{m,n=2}^{t-4-i-j} c_{i,i+m}c_{j,j+n}g_{i+m,j+n}u_{i+j+m+n} .$$

https://doi.org/10.1017/S0027763000026647 Published online by Cambridge University Press

If $i = j$, then $[A(u_i)]^2 =$

$$g_{i,i}u_{2i} + \sum_{m=2}^{r-1-i} [c_{i,i+m}]^2 g_{i+m,i+m}u_{2i+2m} +$$

$$\sum_{m,n} 2\, c_{i,i+m}c_{i,i+n}g_{i+m,i+n}u_{2i+m+n}$$

where the last summation is taken over all m and n such that both $2 \leq m < n \leq t-4-2i$ and $m+n \leq t-2-2i$. Since $g_{h,h} = 0$ for $h \neq 0$, $[A(u_i)]^2 = 0 = A(u_i^2)$. If $i < j$, then

$$c_{i,i+m}c_{j,j+n}g_{i+m,j+n} = 0$$

for $2 \leq m$, $n \leq t-4-i-j$. Hence $A(u_i)A(u_j) = g_{i,j}u_{i+j} = g_{i,j}A(u_{i+j})$.

So in all cases, we have exhibited that a matrix of form A_{k+1} is the matrix of an element of $\mathscr{A}_{k+1}$ with respect to the canonical basis. This completes our main induction and hence the proof of Theorem 1.

2. The Automorphism groups.

DEFINITION. Let $\mathscr{B}_n$ be the group which is generated by $2^n - 2$ generators G_i where $1 \leq i \leq 2^n - 2$ and $n \geq 2$. Let

$$G_i^2 = I \text{ for } 1 \leq i \leq 2^n - 2.$$

Define commuting relations on the generators inductively as follows: In $\mathscr{B}_2$, let $G_1G_2 = G_2G_1$. Set $r = 2^k$ and $s = 2^{k-1}$. Assuming that $\mathscr{B}_k$ is defined, embed $\mathscr{B}_k$ as a subgroup into $\mathscr{B}_{k+1}$. Then for $1 \leq i \leq s-2$ and $-1 \leq j \leq s-2$ define

$$G_iG_{r+j} = \begin{cases} G_{r+1+i+j}G_{r+j}G_i \text{ when } G_iG_{s+j} = G_{s+1+i+j}G_{s+j}G_i \\ G_{r+j}G_i \text{ when } G_iG_{s+j} = G_{s+j}G_i \end{cases}$$

and

$$G_iG_{r+s+j} = \begin{cases} G_{r+s+1+i+j}G_{r+s+j}G_i \text{ when } G_iG_{s+j} = G_{s+1+i+j}G_{s+j}G_i \\ G_{r+s+j}G_i \text{ when } G_iG_{s+j} = G_{s+j}G_i. \end{cases}$$

Also for $-1 \leq i, j \leq s-2$ define

$$G_{s+i}G_{r+j} = \begin{cases} G_{r+s+1+i+j}G_{r+j}G_{s+i} \text{ when } i+j \text{ is odd and } i+j < s-2 \\ G_{r+j}G_{s+i} \text{ otherwise} \end{cases}$$

and

$$G_{s+i}G_{r+s+j} = G_{r+s+j}G_{s+i}.$$

https://doi.org/10.1017/S0027763000026647 Published online by Cambridge University Press

Finally for $-1 \leq i < j \leq r-2$ define

$$G_{r+i}G_{r+j} = G_{r+j}G_{r+i}.$$

THEOREM 2. *The automorphism group of the Jordan algebra $S[2^n]$ over the field J_2 is $\mathscr{B}_n$; that is, the set of all matrices of the form A_n forms a group under multiplication and is $\mathscr{B}_n$.*

Proof. The proof is by induction on n. Since it represents all automorphisms of $S[2^n]$ by Theorem 1, the set of all matrices of the form A_n forms a group $\mathscr{A}_n$ under multiplication. Clearly, the order of $\mathscr{A}_n$ is 2^{2^n-2}.

Let $[i_1, i_2, \cdots, i_m]$ denote that element of $\mathscr{A}_n$ with

$$a_{i_j} = \begin{cases} 1 & \text{for } 1 \leq j \leq m \\ 0 & \text{otherwise} \end{cases}$$

where $i_1 < i_2 < \cdots < i_m$ and $1 \leq m \leq 2^n - 2$.

We begin by considering $\mathscr{A}_2$. Let $G_1 = [1]$ and $G_2 = [2]$. Then $G_1^2 = G_2^2 = I$ and $G_1G_2 = [1,2] = G_2G_1$. So G_1 and G_2 generate $\mathscr{A}_2$. Hence $\mathscr{A}_2$ is $\mathscr{B}_2$.

Observe that $\mathscr{A}_k$ may be considered as a subgroup of $\mathscr{A}_{k+1}$ by identifying $[i_1, i_2, \cdots, i_m] \in \mathscr{A}_k$ with $[i_1, i_2, \cdots, i_m] \in \mathscr{A}_{k+1}$ where $1 \leq m \leq r-2$.

Let $G_i = [i]$. Suppose that $\mathscr{A}_k$ is $\mathscr{B}_k$ for this choice of the G_i. We will show that these G_i satisfy the defining relations of $\mathscr{B}_{k+1}$ and generate $\mathscr{B}_{k+1}$.

Suppose $-1 \leq i, j \leq s-2$. By the definition of matrices of the form A_{k+1}, we can write

$$G_{s+i} = \begin{pmatrix} 1 & X & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & X \\ 0 & 0 & 0 & 1 \end{pmatrix} \text{ and } G_{r+j} = \begin{pmatrix} 1 & 0 & Y & 0 \\ 0 & 1 & 0 & Y \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

where X and Y are certain s by s matrices and 0 and 1 are the s by s zero and identity matrices respectively. Let $H \in \mathscr{A}_{k+1}$ with

$$G_{s+i}G_{r+j} = HG_{r+j}G_{s+i}.$$

Then

https://doi.org/10.1017/S0027763000026647 Published online by Cambridge University Press

$$H = \begin{pmatrix} 1 & 0 & 0 & Z \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

where $Z = XY - YX$. It can be shown that

$$\begin{pmatrix} 1 & 0 & 0 & XY \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

is $G_{r+s+1+i+j}$ when i is odd and $i + j < s - 2$ and is I otherwise. It follows that

$$H = \begin{cases} G_{r+s+1+i+j} & \text{when } i + j \text{ is odd and } i + j < s - 2 \\ I & \text{otherwise.} \end{cases}$$

The other commuting relations follow by similar block matrix arguments. Using the induction hypothesis it is easy to verify that $G_i^2 = I$ for all i.

We must still show that the set $\{G_i : 1 \leq i \leq t - 2\}$ generates $\mathscr{A}_{k+1}$. We will exhibit an algorithm for obtaining an element $[i_1, i_2, \cdots, i_m]$ of $\mathscr{A}_{k+1}$, where $1 \leq m \leq t - 2$, as a product of the G_i. This will be done by induction on m. For $m = 1$, $[i_1] = G_{i_1}$.

Suppose that $[i_1, i_2, \cdots, i_{m-1}]$ has been expressed as a product of the G_i. We will express $[i_1, i_2, \cdots, i_{m-1}, i_m]$ as a product of $[i_1, i_2, \cdots, i_{m-1}]$ and the G_i.

Now $G_e = [e] = (c_{i,j})$, where $1 \leq e \leq t - 2$, has the properties that

$$\begin{cases} c_{i,j} = \delta_{i,j} \text{ for } -1 \leq i \leq e, \ -1 \leq j \leq e - 1 \\ c_{-1,e} = 1 \\ c_{i,e} = \delta_{i,e} \text{ for } 0 \leq i \leq e. \end{cases}$$

Hence

$$[i_1, i_2, \cdots, i_{m-1}]G_{i_m} =$$
$$[i_1, i_2, \cdots, i_{m-1}, i_m, j_{1,1}, j_{1,2}, \cdots, j_{1,m_1}]$$

https://doi.org/10.1017/S0027763000026647 Published online by Cambridge University Press

where $j_{1,1} > i_m$ and $0 \leq m_1 \leq t - 2 - i_m$. If $m_1 = 0$, then we are done. If not, then

$$[i_1, i_2, \cdots, i_{m-1}]G_{i_m}G_{j_{1,1}} =$$
$$[i_1, i_2, \cdots, i_{m-1}, i_m, j_{2,1}, j_{2,2}, \cdots, j_{2,m_2}]$$

where $j_{2,1} > j_{1,1}$ and $0 \leq m_2 \leq t - 2 - j_{1,1}$. If $m_2 = 0$, then we are done. If not, then

$$[i_1, i_2, \cdots, i_{m-1}]G_{i_m}G_{j_{1,1}}G_{j_{2,1}} =$$
$$[i_1, i_2, \cdots, i_{m-1}, i_m, j_{3,1}, j_{3,2}, \cdots, j_{3,m_3}]$$

where $j_{3,1} > j_{2,1}$ and $0 \leq m_3 \leq t - 2 - j_{2,1}$. If $m_3 = 0$, then we are done. If not, then consider

$$[i_1, i_2, \cdots, i_{m-1}]G_{i_m}G_{j_{1,1}}G_{j_{2,1}}G_{j_{3,1}}.$$

It is clear that this process must terminate. This completes the proof of Theorem 2.

Reference

[1] E.C. Paige, Jr: *Jordan Algebras of Characteristic Two*, Dissertation, University of Chicago, Chicago, Illinois, (1954).

Georgetown University

https://doi.org/10.1017/S0027763000026647 Published online by Cambridge University Press