TWO-GROUPS AND JORDAN ALGEBRAS

JAMES EDWARD WARD
TWO-GROUPS AND JORDAN ALGEBRAS

JAMES E. WARD, III

Stroud and Paige have introduced an important class of central simple Jordan algebras $B(2^n)$ of characteristic two. This paper determines the automorphism groups of the algebras $B(2^n)$ and, in so doing, produces an infinite family of finite 2-groups. This is accomplished by characterizing the automorphisms of $B(2^n)$ as matrices operating on the natural basis for the underlying vector space of $B(2^n)$ and then using this characterization to obtain generators and commuting relations for the automorphism groups.

Throughout the paper let $q = 2^{n-2}$, $r = 2^{n-1}$, $s = 2^n$, and $t = 2^{n+1}$. $\delta_{i,j}$ is the Kronecker delta.

1. The algebras. In 1965 J. B. Stroud [3], pursuing some earlier work of E. C. Paige [2], defined the following class of vector spaces and proved that they are central simple Jordan Algebras of characteristic two:

**DEFINITION.** Let $B(2^n)$ for $n \geq 2$ be the vector space over the field $\mathbb{Z}_2$ of two elements with basis $u_{-1}, u_0, u_1, \ldots, u_{s-2}, v_1, v_2, \ldots, v_s$ and with multiplication in $B(2^n)$ defined inductively as follows:

The products $u_iu_j$ for $-1 \leq i, j \leq s - 2$ are defined by:

(1) $u_0u_i = u_i$ for $-1 \leq i \leq s - 2$,

(2) $u_{i+1} = 0, u_{i-1} = u_{i+1}$ for $0 \leq i \leq s - 2$,

(3) $u_iu_j = u_ju_i$ for $-1 \leq i, j \leq s - 2$,

(4) $u_i^2 = u_iu_2 = 0$.

Assuming the products $u_iu_j$ are defined for $-1 \leq i, j \leq 2k - 2$ where $2 \leq k \leq n - 1$, let $p = 2^k$ and define

(5) $u_{p+i}u_j = H_{i,j}u_{p+i+j}$ when $u_iu_j = H_{i,j}u_{i+j}$, $j \neq -1$ with $H_{i,j}$ in $\mathbb{Z}_2$,

(6) $u_{p+i}u_{p+j} = 0$.

For $k \geq 1$, $m \geq 0$, $p = 2^k$, define the products $u_iu_j$ by:

(7) $u_iv_j = v_ju_i$ for $-1 \leq i \leq s - 2$, $1 \leq j \leq s$,

(8) $u_0v_j = v_j$ for $1 \leq j \leq s$,

(9) $u_{-1}v_j = v_j + v_{j-1}$, $v_0 = 0$ for $1 \leq j \leq s$,

(10) $u_{p+i}v_{(2m)p+j} = v_{(2m+1)p+j-1} + v_{(2m+1)p+j}$ for $1 \leq j \leq p$,

(11) $u_{p+i}v_{(2m)p+j} = d_{i,j}v_{(2m+1)p+i+j} + e_{i,j}v_{(2m+1)p+i+j+1}$ when

(12) $u_{i}v_j = d_{i,j}v_{i+j} + e_{i,j}v_{i+j+1}$ for $0 \leq i \leq p - 2$, $1 \leq j \leq p$ and $d_{i,j}$, $e_{i,j}$ in $Z_2$,

(13) $u_{p+i}v_{(2m+1)p+j} = 0$ for $-1 \leq i \leq p - 2$, $1 \leq j \leq p$. 

821
Finally, define the products $v_i v_j$ by:

(14) $v_i v_j = v_j v_i$ for $1 \leq i, j \leq s$,

(15) $v_0 = u_0$,

(16) $v_i v_j = \begin{cases} u_{j-3} + u_{j-2}, & j \text{ even} \\ u_{j-3}, & j \text{ odd} \end{cases}$

where $u_j = 0$ for $j < -1$,

(17) $v_{p+i} v_j = D_{i,j} u_{p+i+j-4} + E_{i,j} u_{p+i+j-3}$

when

(18) $v_i v_j = D_{i,j} u_{i+j-4} + E_{i,j} u_{i+j-3}$ for $1 \leq i \leq p$, $2 \leq j \leq p$ and $D_{i,j}$, $E_{i,j}$ in $Z_2$,

(19) $v_{p+i} v_{p+j} = 0$, $1 \leq i, j \leq p$.

From this definition it is clear that $B(2^n)$ is commutative ((3), (7), (14)) and that $u_0$ is its identity element ((1), (8)). Moreover, for all $i, j, a, b$ (i.e., $-1 \leq i, j \leq s - 2$ and $1 \leq a, b \leq s$),

$$u_i u_j = h_{i,j} u_{i+j} \quad \text{where } h_{i,j} = 0 \text{ or } 1,$$

$$v_i v_a = \begin{cases} g_{i,a}(v_{i+a} + v_{i+a-1}), & v_0 = 0, \text{ when } i \equiv 1 \pmod{2} \\ g_{i,a} v_{i+a} & \text{when } i \equiv 0 \pmod{2} \end{cases}$$

where $g_{i,a} = 0$ or 1, and

$$v_a v_b = \begin{cases} f_{a,b} u_{a+b-4} & \text{when } a \equiv b \pmod{2} \\ f_{a,b}(u_{a+b-4} + u_{a+b-3}) & \text{when } a \equiv b \pmod{2} \end{cases}$$

where $f_{a,b} = 0$ or 1.

The multiplication table for $B(4)$ is easily computed to be

<table>
<thead>
<tr>
<th></th>
<th>$u_{-1}$</th>
<th>$u_0$</th>
<th>$u_1$</th>
<th>$u_2$</th>
<th>$v_1$</th>
<th>$v_2$</th>
<th>$v_3$</th>
<th>$v_4$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$u_{-1}$</td>
<td>0</td>
<td>$u_{-1}$</td>
<td>$u_0$</td>
<td>$u_1$</td>
<td>$v_1$</td>
<td>$v_1 + v_2$</td>
<td>$v_2 + v_3$</td>
<td>$v_3 + v_4$</td>
</tr>
<tr>
<td>$u_0$</td>
<td>$u_{-1}$</td>
<td>$u_0$</td>
<td>$u_1$</td>
<td>$u_2$</td>
<td>$v_1$</td>
<td>$v_2$</td>
<td>$v_3$</td>
<td>$v_4$</td>
</tr>
<tr>
<td>$u_1$</td>
<td>$u_0$</td>
<td>$u_1$</td>
<td>0</td>
<td>0</td>
<td>$v_2 + v_3$</td>
<td>$v_3 + v_4$</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$u_2$</td>
<td>$u_1$</td>
<td>$u_2$</td>
<td>0</td>
<td>0</td>
<td>$v_3$</td>
<td>$v_4$</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$v_1$</td>
<td>$v_1$</td>
<td>$v_1$</td>
<td>$v_2 + v_3$</td>
<td>$v_3$</td>
<td>0</td>
<td>$u_{-1} + u_0$</td>
<td>$u_0$</td>
<td>$u_1 + u_2$</td>
</tr>
<tr>
<td>$v_2$</td>
<td>$v_1 + v_2$</td>
<td>$v_2$</td>
<td>$v_3 + v_4$</td>
<td>$v_4$</td>
<td>$u_{-1} + u_0$</td>
<td>$u_0$</td>
<td>$u_1 + u_2$</td>
<td>$u_2$</td>
</tr>
<tr>
<td>$v_3$</td>
<td>$v_2 + v_3$</td>
<td>$v_3$</td>
<td>0</td>
<td>0</td>
<td>$u_0$</td>
<td>$u_1 + u_2$</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$v_4$</td>
<td>$v_3 + v_4$</td>
<td>$v_4$</td>
<td>0</td>
<td>0</td>
<td>$u_1 + u_2$</td>
<td>$u_2$</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

and the following table summarizes the inductive definition of $B(2p)$ if the multiplication table of $B(p)$ is known:
The numbers indicate the equation used to determine the particular block of the multiplication table, COMMUTATIVITY in a block means that the block in question is determined from a corresponding block by the commutativity of \( B(2^n) \), and ZERO denotes a block all of whose entries are zero.

2. The automorphisms.

**DEFINITION.** Define a set of \( t \times t \) matrix forms \( A_n \) for \( n \geq 2 \) inductively as follows: Let

\[
A_2 = \begin{bmatrix}
1 & a_0 & a_1 & a_2 & 0 & a_0 & 0 & b_1 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & a_0 & 0 & 0 & a_0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & a_0 & 0 & b_1 & 1 & a_0 & a_1 + a_2 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & a_0 & 0 & 0 & 1 & a_0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{bmatrix}
\]

where \( a_0, a_1, a_2 \) and \( b_1 \) are in \( \mathbb{Z}_2 \).

Assuming that the matrix \( A_n = (c_{i,j}) \) where \(-1 \leq i, j \leq t - 2\) is defined in terms of elements \( a_e \) and \( b_m \) of \( \mathbb{Z}_2 \) with \( 0 \leq e \leq s - 2 \) and
0 \leq m \leq s$, we define the matrix $A_{n+1} = (d_{i,j})$ for $-1 \leq i, j \leq 2t - 2$ in terms of elements $a_e$ and $b_m$ of $\mathbb{Z}_2$ with $0 \leq e \leq t - 2$ and $0 \leq m \leq t$ as follows: For $-1 \leq i, j \leq s - 2$,

(i) $d_{i,j} = d_{i+s,j+s} = c_{i,j}$.

(ii) $d_{i,j+t} = d_{i+s,j+3s} = c_{i,j+s}.

(iii) $d_{i+1,j} = d_{i+3s,j+s} = c_{i+s,j}.

(iv) $d_{i+1,j+t} = d_{i+3s,j+3s} = c_{i+s,j+s}.

(v) $d_{i+s,j} = d_{i+s,j+t} = d_{i+3s,j} = d_{i+3s,j+t} = 0.

(vi) $d_{i,j+s} = \begin{cases} 0 & \text{if } i = j \\ p_{i,j}a_{j+s} & \text{if } i \neq j \end{cases}$ where $p_{i,j}$ is in $\mathbb{Z}_2$ and $c_{i,j} = p_{i,j}a_e$.

(vii) $d_{i,j+3s} = p_{i,j+s}b_{m+s}$ where $p_{i,j+s}$ is in $\mathbb{Z}_2$ and $c_{i,j+s} = p_{i,j+s}b_m$ with $a_0 = b_0$.

(viii) $d_{i+s,j+s} = p_{i+s,j+s}b_{m+s}$ where $p_{i+s,j+s}$ is in $\mathbb{Z}_2$ and $c_{i+s,j+s} = p_{i+s,j+s}b_m$ with $a_0 = b_0$.

(ix) $d_{i+s,j+s} = \begin{cases} 0 & \text{if } i = j \\ p_{i+s,j+s}a_{e+s} + q_{i+s,j+s}a_{e+s+1} & \text{if } i \neq j \end{cases}$ where $p_{i+s,j+s}$ and $q_{i+s,j+s}$ are in $\mathbb{Z}_2$ and $c_{i+s,j+s} = p_{i+s,j+s}a_e + q_{i+s,j+s}a_{e+1}$ with the convention that if $c_{i+s,j+s} = a_w$, then $e = w$.

The matrices $A_n$ can be summarized by the following figure. If the $2^k \times 2^k$ matrix $A_k$ is known, then $A_{k+1}$ is the $2^{k+1} \times 2^{k+1}$ matrix given in block form by

$$A_{k+1} = \begin{bmatrix}
A_k & UR(A_k) + 2^k \\
0_{2^k} & UR(A_k) + 2^k
\end{bmatrix}$$

where, for $m = 2^k-1$ or $2^k$, $0_m$ is the $m \times m$ zero matrix and $UR(A_k) + m$ is the $2^k \times 2^k$ matrix obtained by adding $m$ to each subscript of the $2^k \times 2^k$ block in the upper right hand corner of $A_k$ under the convention that if an entry in the upper right hand block of $A_k$ is zero, then the corresponding entry in $UR(A_k) + m$ is also zero.

We now prove the characterization theorem.

**Theorem.** A linear transformation $A$ of the Jordan algebra $B(2^n)$ over $\mathbb{Z}_2$ with $n \geq 2$ is an automorphism of $B(2^n)$ if and only
if its matrix relative to the canonical basis of $B(2^n)$ is of the form $A_n$.

**Proof.** The proof is outlined by several lemmas.

First we establish some general results about the automorphisms of $B(2^n)$. If $A$ is an automorphism of $B(2^n)$ with matrix $(c_{i,j})$, $-1 \leq i, j \leq t - 2$, $c_{i,j}$ in $Z_2$, relative to the canonical basis of $B(2^n)$ then we can show:

**Lemma 1.** $c_{i,j} = c_{s+i,s+j} = c_{s+i,s+j} = 0$ for $-1 \leq j < i \leq s - 2$.

**Lemma 2.** $c_{i,i} = 1$ for $-1 \leq i \leq t - 2$ and $c_{s+i,s+i} = 0$ for $-1 \leq i \leq s - 2$.

**Lemma 3.** $c_{i,j} = \delta_{i,j}$ for $-1 \leq i, j \leq t - 2$ and $i \equiv 0 \pmod{2}$.

**Lemma 4.** $c_{s+i,s+j} = c_{s+i,s+j}$ for $-1 \leq i, j \leq s - 2$. In particular, $c_{s+i,s+j} = c_{s+i,s+j} = 0$ for $-1 \leq i, j \leq s - 2$ and $j = 1 \pmod{2}$.

**Lemma 5.** For $-1 \leq i, j \leq r - 2$, $c_{i,j} = c_{r+i,r+j}$; $c_{s+i,s+j} = c_{r+i,s+j}$; $c_{s+i,s+j} = c_{3r+i,3r+j}$; and $c_{s+i,s+j} = c_{3r+i,3r+j}$.

**Lemma 6.** For $-1 \leq i \leq j \leq r - 2$,

(i) $c_{i,r+j} = \begin{cases} 0 & \text{if } i = j \\
p_{i,j}c_{i,r+j-i-1} & \text{if } i \neq j \end{cases}$ where $p_{i,j}$ is in $Z_2$.

(ii) $c_{i,3r+j} = \begin{cases} 0 & \text{if } i = j \\
q_{i,j}c_{i,3r+j-i-1} & \text{if } i \neq j \end{cases}$ where $q_{i,j}$ is in $Z_2$.

(iii) $c_{s+i,3r+j} = \begin{cases} 0 & \text{if } i = j \\
m_{i,j}c_{s+i,3r+j-i-1} + k_{i,j}c_{s+i,3r+j-i-2} & \text{if } i \neq j \text{ and } j \equiv 0 \pmod{2} \\
m_{i,j}c_{s+i,3r+j-i-1} & \text{if } i \neq j \text{ and } j \equiv 1 \pmod{2} \end{cases}$

where $m_{i,j}$ and $k_{i,j}$ are in $Z_2$.

To establish the necessity of the condition of the theorem, we proceed by induction on $n$. The case $n = 2$ is straightforward in view of the preceding lemmas and, for the induction step, we make the following definitions and state a lemma about them:

**Definition.** If $A$ is an automorphism of $B(2^{n+1})$ with matrix
(c_{i,j}, -1 \leq i, j \leq 2t - 2, relative to the canonical basis of B(2^{n+1}),
then the restriction of A to B(2^n) is the linear transformation A' of 
B(2^n) onto itself whose matrix (d_{i,j}), -1 \leq i, j \leq t - 2, relative to 
the canonical basis of B(2^n) is defined by:

\[
d_{i,j} = \begin{cases}
c_{i,j} & \text{for } -1 \leq i, j \leq s - 2 \\
c_{s+i,j} & \text{for } s - 1 \leq i \leq t - 2 \text{ and } -1 \leq j \leq s - 2 \\
c_{i,s+j} & \text{for } -1 \leq i \leq s - 2 \text{ and } s - 1 \leq j \leq t - 2 \\
c_{s+i,s+j} & \text{for } s - 1 \leq i, j \leq t - 2 .
\end{cases}
\]

**Definition.** If A is an automorphism of B(2^n) with matrix 
(c_{i,j}), -1 \leq i, j \leq t - 2, relative to the canonical basis of B(2^n),
then the linear transformation of B(2^{n+1}) induced by A is the linear 
transformation A* of B(2^{n+1}) onto itself whose matrix (b_{i,j}), -1 \leq i, 
JAMES E. WARD, III

\[
A^{*} = \begin{pmatrix}
\cdots & \cdots & \cdots & \cdots \\
\cdots & \cdots & \cdots & \cdots \\
\cdots & \cdots & \cdots & \cdots \\
\cdots & \cdots & \cdots & \cdots
\end{pmatrix}
\]

\[
de_{i,j} = \begin{cases}
c_{i,j} & \text{for } -1 \leq i, j \leq s - 2 \\
c_{s+i,j} & \text{for } s - 1 \leq i \leq t - 2 \text{ and } -1 \leq j \leq s - 2 \\
c_{i,s+j} & \text{for } -1 \leq i \leq s - 2 \text{ and } s - 1 \leq j \leq t - 2 \\
c_{s+i,s+j} & \text{for } s - 1 \leq i, j \leq t - 2 .
\end{cases}
\]

**Lemma 7.** (i) If A is an automorphism of B(2^{n+1}), then the 
restriction A' of A to B(2^n) is an automorphism of B(2^n).

(ii) If A is an automorphism of B(2^n), then the linear trans-
formation A* of B(2^{n+1}) induced by A is an automorphism of B(2^{n+1}).

The induction step then proceeds as follows: We assume that 
every automorphism of B(2^n) has matrix of the form A_n relative to 
the canonical basis of B(2^n) and we let A be an automorphism of 
B(2^{n+1}) with matrix (d_{i,j}), -1 \leq i, j \leq 2t - 2, relative to the canonical 
basis of B(2^{n+1}). We must show that (d_{i,j}) satisfies (i)-(ix).

By the induction hypothesis and Lemmas 5 and 7, we have (i)-(iv).
Lemma 1 establishes (v) and (vi)-(ix) follow from the induction 
hypothesis and Lemmas 4 and 6. Thus we have that (d_{i,j}), -1 \leq i, 
JAMES E. WARD, III

\[
de_{i,j} = \begin{cases}
c_{i,j} & \text{for } -1 \leq i, j \leq s - 2 \\
c_{s+i,j} & \text{for } s - 1 \leq i \leq t - 2 \text{ and } -1 \leq j \leq s - 2 \\
c_{i,s+j} & \text{for } -1 \leq i \leq s - 2 \text{ and } s - 1 \leq j \leq t - 2 \\
c_{s+i,s+j} & \text{for } s - 1 \leq i, j \leq t - 2 .
\end{cases}
\]

\[
de_{i,j} = \begin{cases}
c_{i,j} & \text{for } -1 \leq i, j \leq s - 2 \\
c_{s+i,j} & \text{for } s - 1 \leq i \leq t - 2 \text{ and } -1 \leq j \leq s - 2 \\
c_{i,s+j} & \text{for } -1 \leq i \leq s - 2 \text{ and } s - 1 \leq j \leq t - 2 \\
c_{s+i,s+j} & \text{for } s - 1 \leq i, j \leq t - 2 .
\end{cases}
\]

**Lemma 7.** (i) If A is an automorphism of B(2^{n+1}), then the 
restriction A' of A to B(2^n) is an automorphism of B(2^n).

(ii) If A is an automorphism of B(2^n), then the linear trans-
formation A* of B(2^{n+1}) induced by A is an automorphism of B(2^{n+1}).

The induction step then proceeds as follows: We assume that 
every automorphism of B(2^n) has matrix of the form A_n relative to 
the canonical basis of B(2^n) and we let A be an automorphism of 
B(2^{n+1}) with matrix (d_{i,j}), -1 \leq i, j \leq 2t - 2, relative to the canonical 
basis of B(2^{n+1}). We must show that (d_{i,j}) satisfies (i)-(ix).

By the induction hypothesis and Lemmas 5 and 7, we have (i)-(iv).
Lemma 1 establishes (v) and (vi)-(ix) follow from the induction 
hypothesis and Lemmas 4 and 6. Thus we have that (d_{i,j}), -1 \leq i, 
JAMES E. WARD, III

\[
de_{i,j} = \begin{cases}
c_{i,j} & \text{for } -1 \leq i, j \leq s - 2 \\
c_{s+i,j} & \text{for } s - 1 \leq i \leq t - 2 \text{ and } -1 \leq j \leq s - 2 \\
c_{i,s+j} & \text{for } -1 \leq i \leq s - 2 \text{ and } s - 1 \leq j \leq t - 2 \\
c_{s+i,s+j} & \text{for } s - 1 \leq i, j \leq t - 2 .
\end{cases}
\]

\[
de_{i,j} = \begin{cases}
c_{i,j} & \text{for } -1 \leq i, j \leq s - 2 \\
c_{s+i,j} & \text{for } s - 1 \leq i \leq t - 2 \text{ and } -1 \leq j \leq s - 2 \\
c_{i,s+j} & \text{for } -1 \leq i \leq s - 2 \text{ and } s - 1 \leq j \leq t - 2 \\
c_{s+i,s+j} & \text{for } s - 1 \leq i, j \leq t - 2 .
\end{cases}
\]

To establish the sufficiency of the condition we first show that 
det A_n = 1 for n \geq 2. This is accomplished by expanding det A_n by 
the cofactors of its first column, expanding the resulting (t - 1) x (t - 1)
determinant by the cofactors of its first row, expanding the resulting \((t - 2) \times (t - 2)\) determinant by the cofactors of its first column, and continuing to alternate in this manner. In view of Lemmas 1, 3 and 4, after \(t - 2\) such steps we have

\[
\det A_n = \begin{vmatrix} 1 & c_{-1,0} \\ 0 & 1 \end{vmatrix} = 1.
\]

This fact about the determinant says that \(A_n\) is the matrix relative to the canonical basis of \(B(2^n)\) of a nonsingular linear transformation \(A\) of \(B(2^n)\) onto itself. Hence it only remains to show that \(A\) preserves products of the basis elements of \(B(2^n)\) and this may be checked by a straightforward but lengthy calculation. This completes the proof.

3. The automorphism groups. At this point we know that the automorphism group \(\mathcal{A}_n\) of \(B(2^n)\) over \(Z\) is the group formed by all matrices of the form \(A_n\) under matrix multiplication. From the definition of the matrices \(A_n\), \(n \geq 2\), it follows that such a matrix has \(3q\) elements \(a_i\) and \(r - 1\) elements \(b_j\) in its first row. Since any matrix of the form \(A_n\) is completely determined by the elements of its first row, this says that the order of \(\mathcal{A}_n\) is \(2^{3q + r - 1} = 2^{5q - 1}\).

In order to examine the structure of \(\mathcal{A}_n\), we make the following DEFINITION. For \(n \geq 2\), let

\[
\begin{align*}
I^*_1 &= \{i: 0 \leq i \leq s - 2, \ i \neq 3 \ (\text{mod } 4)\}, \\
I^*_2 &= \{s + 2i - 2: 2 \leq i \leq r\} \quad \text{and} \\
I^*_n &= I^*_1 \cup I^*_2.
\end{align*}
\]

Then \(I^*_n\) is a subset of \(\{i: 0 \leq i \leq t - 2\}\) and consists of \(5q - 1\) elements.

For \(i\) in \(I^*_n\), define \(G_i\) as follows:

(i) If \(i\) is in \(I^*_1\), \(G_i\) is the matrix of the form \(A_n\) with \(a_i = 1\), \(a_j = 0\) for \(j\) in \(I^*_n\) and \(j \neq i\), and \(b_{2k} = 0\) for \(2 \leq k \leq r\).

(ii) If \(i\) is in \(I^*_2\), \(G_i\) is the matrix of the form \(A_n\) with \(b_{i-s+2} = 1\), \(b_{j-s+2} = 0\) for \(j\) in \(I^*_n\) and \(j \neq i\), and \(a_k = 0\) for \(k\) in \(I^*_n\).

Denote by \((i_1, i_2, \ldots, i_m)\), where \(i_j\) is in \(I^*_n\) for \(1 \leq j \leq m\) and \(i_1 < i_2 < \cdots < i_m\), the matrix of the form \(A_n\) in which for each \(j = 1, 2, \ldots, m\), \(a_{i_j} = 1\) if \(i_j\) is in \(I^*_1\) and \(b_{i_j-s+2} = 1\) if \(i_j\) is in \(I^*_2\) while \(a_k = 0\) for \(k\) in \(I^*_n\) and \(k \neq i_j\) for any \(j = 1, 2, \ldots, m\) and \(b_{k-s+2} = 0\) for \(k\) in \(I^*_n\) and \(k \neq i_j\) for any \(j = 1, 2, \ldots, m\). Clearly any element of \(\mathcal{A}_n\) can be expressed in the form \((i_1, i_2, \ldots, i_m)\) for some \(i_1, i_2, \ldots, i_m\).

Using a technique due to Bobo [1], we can show that the set \(\{G_i: i \in I^*_n\}\) generates \(\mathcal{A}_n\). Finally, we determine the commutator subgroup of \(\mathcal{A}_n\) by using a straightforward induction on \(n\) together.
with the properties of matrix multiplication and matrices of the form \( G_i \). The results are summarized in the following

**Theorem.** The automorphism group \( \mathcal{A}_n \) of the Jordan algebra \( B(2^n) \), \( n \geq 2 \), can be described abstractly as the group generated by the \( 5(2^{n-1}) - 1 \) generators \( G_i \) where \( i \) is in \( I^n \) and where \( G_i = 1 \) for all \( i \) in \( I^* \), \( I^* \) being the \( t \times t \) identity matrix. Moreover, the commuting relations among the generators of \( \mathcal{A}_n \) may be described inductively as follows:

In \( \mathcal{A}_n \), \( G_0 G_1 \neq G_1 G_0 \) but \( G_0 G_1 = G_2 G_0 G_1 G_0 \). For all other \( i \) and \( j \) in \( I^* \), \( G_i G_j = G_j G_i \).

If the commuting relations among the generators \( G_i \), \( i \) in \( I^{n-1} \), of \( \mathcal{A}_{n-1} \) are known, the commuting relations in \( \mathcal{A}_n \) are given by:

- If \( i \) and \( m \) are in \( I^{n-1} \) with \( i \neq m \) and \( i \neq m \) and if \( j \) and \( k \) are in \( I^{n-1} \) with \( j \neq k \), then
  
  (a) If \( i \equiv 1 \pmod{4} \),
  
  \[ G_0 G_i = G_{i+1} G_{i+i+1} G_i G_0, \]
  
  \[ G_0 G_{i+r} = G_{r+i+1} G_{r+i+1} G_{i+r} G_0, \]
  
  \[ G_i G_r = G_{r+i+1} G_i, \text{ and} \]
  
  \[ G_i G_{r+i+r} = G_{r+i+r} G_i. \]

  (b) If \( G_i G_m = G_{i+m} G_i G_m \),
  
  \[ G_i G_m = G_{i+m+1} G_m G_i, \text{ and} \]
  
  \[ G_i G_{m+i+r} = G_{r+i+m+1} G_{m+i+r} G_i. \]

  (c) If \( G_i G_j = G_{i+j+1} G_j G_i \),
  
  \[ G_i G_{j+r} = G_{r+i+j+1} G_{r+j} G_i; \]
  
  \[ G_i G_{j+s} = G_{s+i+j+1} G_{j+s} G_i, \text{ and} \]
  
  \[ G_i G_{j+r} = G_{r+i+j+1} G_{j+r} G_i. \]

Otherwise, \( G_e G_f = G_f G_e \) for \( e \) and \( f \) in \( I^* \).

The structure of the group \( \mathcal{A}_2 \) of order 16 becomes clearer if it is recognized as the direct product of two familiar groups. Since \( I^*_2 = \{0, 1, 2\} \) and \( I^*_2 = \{6\} \), \( \mathcal{A}_2 \) is generated by \( G_0, G_1, G_2, \) and \( G_6 \). Let \( H_1 \) be the subgroup of \( \mathcal{A}_2 \) generated by \( G_0 \) and \( G_1 \). Then, if \( a = G_i G_0 \) and \( b = G_6 \), direct computation using the commuting relations in \( \mathcal{A}_2 \) yields \( H_1 \) = \( \{I, a, b, ab, a^3, a^3, a^3 b, a^3 b\} \) as the dihedral group \( D_6 \). If \( H_2 = \{I, G_2\} \) then both \( H_1 \) and \( H_2 \) are normal in \( \mathcal{A}_2 \), \( H_1 \cap H_2 = \{I\} \), and \( H_1 H_2 = \mathcal{A}_2 \). Hence

\[ \mathcal{A}_2 \cong D_6 \times Z_2 \]

where \( D_6 \) is the dihedral group of order eight and \( Z_2 \) is the cyclic group of order two.

Detailed proofs of some of the results summarized in this paper
may be found in the author's doctoral thesis written at the University of Virginia under Eugene C. Paige.

REFERENCES


Received May 21, 1969. This research was supported in part by the Danforth Foundation.

BOWDOIN COLLEGE
BRUNSWICK, MAINE
Pacific Journal of Mathematics
Vol. 32, No. 3 March, 1970

Shair Ahmad, *Dynamical systems of characteristic $0^+$* ................. 561
Charles A. Akemann and Bernard Russo, *Geometry of the unit sphere of a C*-algebra and its dual* ........................................ 575
Philip Bacon, *The compactness of countably compact spaces* ............... 587
Richard Blaine Barrar and Henry Loeb, *On the continuity of the nonlinear Tschebyscheff operator* ........................................... 593
L. Carlitz, *Factorization of a special polynomial over a finite field* ........ 603
Joe Ebeling Cude, *Compact integral domains* .................................. 615
Frank Rimi DeMeyer, *On automorphisms of separable algebras. II* ....... 621
James B. Derr, *Generalized Sylow tower groups* .............................. 633
Raouf Doss, *Some inclusions in multipliers* ..................................... 643
Mary Rodriguez Embry, *The numerical range of an operator* .............. 647
John Froese, *Domain-perturbed problems for ordinary linear differential operators* ................................................................. 651
Zdeněk Frolík, *Absolute Borel and Souslin sets* ............................... 663
Ronald Owen Fulp, *Tensor and torsion products of semigroups* ........... 685
George Grätzer and J. Płonka, *On the number of polynomials of an idempotent algebra. I* ............................................................. 697
Newcomb Greenleaf and Walter Read, *Positive holomorphic differentials on Klein surfaces* ......................................................... 711
John Willard Heidel, *Uniqueness, continuation, and nonoscillation for a second order nonlinear differential equation* ......................... 715
Leon A. Henkin, *Extending Boolean operations* ................................ 723
R. Hirshon, *On hopfian groups* ...................................................... 753
Melvin Hochster, *Totally integrally closed rings and extremal spaces* ...... 767
R. Mohanty and B. K. Ray, *On the convergence of a trigonometric integral* ......................................................................................... 781
Michael Rich, *On a class of nodal algebras* .................................... 787
Emile B. Roth, *Conjugate space representations of Banach spaces* ....... 793
Rolf Schneider, *On the projections of a convex polytope* .................... 799
Bertram Manuel Schreiber, *On the coset ring and strong Ditkin sets* ...... 805
Edgar Lee Stout, *Some remarks on varieties in polydiscs and bounded holomorphic functions* ......................................................... 813
James Edward Ward, *Two-groups and Jordan algebras* ...................... 821