On Automorphisms of Order Three of Division Algebras*

L. G. Sweet and J. A. MacDougall

Department of Mathematics and Computer Science
University of Prince Edward Island
Charlottetown, Prince Edward Island, Canada

Submitted by Richard A. Brualdi

ABSTRACT

Let $A$ be a finite dimensional division algebra (not necessarily associative) over a field. The automorphisms of $A$ having order three are characterized by giving a canonical matrix representation for each of the possible types (there are three). Examples are given to show that each type does exist. Some general results concerning automorphisms of prime power order are included.

INTRODUCTION

In this paper all algebras considered are finite dimensional, not necessarily associative, and may not contain a unity. An algebra is a division algebra if it contains no zero divisors (some authors use the term quasidivision algebra). In [2] Sweet studied involutions of division algebras. In this paper we consider automorphisms of order 3 of division algebras. We determine canonical forms for all such automorphisms and construct examples of each type. First some general results are established as to the canonical forms of automorphisms of order $p^a$ where $p$ is a prime. The main result of [2] will be seen as the special case where $p^a = 2$.

If $A$ is an algebra and $x \in A$, then $L_x$ denotes left multiplication by $x$. Since $A$ is a division algebra, $L_x$ is always invertible. Also $x^k$ denotes

*This research was supported by NSERC Grant A5232.

1Address for correspondence: J. A. MacDougall, Department of Mathematics, The University of Newcastle, N.S.W. 2308, Australia.
$L^{-1}_x(x)$, and if $\lambda$ is an eigenvalue of an automorphism $\sigma$, then $A_\lambda$ will denote the corresponding eigenspace.

I. SOME GENERAL RESULTS

**Lemma 1.** Let $A$ be a division algebra of dimension $n$ over a field $K$. Suppose $\sigma \in \text{Aut}(A)$ has eigenvalues $\lambda$ and $\mu$. Then

(i) $\lambda \mu$ is also an eigenvalue of $\sigma$;
(ii) $\lambda^i$ is an eigenvalue of $\sigma$ for any $i \in \mathbb{Z}$;
(iii) $\dim A_\lambda = \dim A_\mu$;
(iv) $\dim A_\lambda \leq n/2$.

**Proof.** (i): If $\sigma(x) = \lambda x$ and $\sigma(y) = \mu y$, then $\sigma(xy) = \lambda \mu (xy)$.
(ii): If $i$ is a positive integer, then the result follows directly from (i). But $\sigma$ can only have a finite number of eigenvalues, so $\lambda^i = 1$ for some positive integer $k$, and hence the result is true for all integers.
(iii): Let $\{e_1, e_2, \ldots, e_r\}$ be a basis for $A_\lambda$, and suppose $a \in A_\mu$. It is easy to show that $\{ae_1, ae_2, \ldots, ae_r\}$ is an independent subset of $A_\mu$. Therefore $\dim A_\lambda \leq \dim A_\mu$. But it follows from (ii) that $\lambda^{-1}$ is also an eigenvalue of $\sigma$ and so

$$\dim A_\lambda \leq \dim A_\mu \leq \dim A_{(\mu \lambda)^{-1}} = \dim A_\mu.$$ 

Similarly

$$\dim A_\mu \leq \dim A_\lambda$$

and so

$$\dim A_\lambda = \dim A_\mu.$$  

(iv): This is the lemma of [2].

**Theorem 1.** Let $A$ be a division algebra over a field $K$, and suppose $\sigma \in \text{Aut}(A)$ has order $p^a$ where $p$ is a prime and $\alpha$ is a positive integer. If $\text{char } K = p$, then $\sigma$ is similar to $J \oplus \cdots \oplus J$, where

$$J = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & 1 & 0 & \cdots & 0 \\ 0 & 1 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & 1 \end{bmatrix}$$

is a $p^a \times p^a$ matrix.
Proof. Let \( m(x) \) be the minimum polynomial of \( \sigma \). Then \( m(x) \) must divide \( x^{p^s} - 1 \). But \( x^{p^s} - 1 = (x - 1)^{p^s} \), so \( m(x) = (x - 1)^s \) for some positive integer \( s \), and \( \sigma \) is similar to its Jordan form, namely \( J_i \oplus \cdots \oplus J_l \), where each \( J_i \) is a Jordan block with 1's on the diagonal.

Now each \( J_i \) is of the form \( J = I + N \) where \( N \) is a nilpotent matrix and \( J^{p^s} = I + N^{p^s} \). It is easy to see that if the order of \( \sigma \) is \( p^a \) then we must have at least one Jordan block of size \( p^a \times p^a \). So without loss of generality we may assume that \( J_i \) is of size \( p^a \times p^a \).

We now show that every \( J_i \) is of size \( p^a \times p^a \); so suppose not. In particular assume that \( |J_i| < |J_l| \). This implies that if \( J_i \) is \( k \times k \) then \( x_k \) is an eigenvector of \( \sigma \), but \( x_{n-k} \) is not, where \( \{ x_i \} \) is the Jordan basis already chosen for \( \sigma \). Let \( L = (\alpha_{ij}) \) be the matrix representation for left multiplication by \( \sigma \) with respect to this Jordan basis. Note that if \( x_i \) is an eigenvector of \( \sigma \), then \( \sigma L x = L x, \sigma \). We use this equation to obtain a contradiction. Let \( x_j \) be any eigenvector of \( \sigma \). Since \( x_j \) is also an eigenvector, Lemma 1(i) implies that the last column of \( L x_j \) has at most \( t \) nonzero entries and that they can only occur in the rows corresponding to the eigenvectors. Thus \( \alpha_{k,n} \) is the first entry in column \( n \) that might be nonzero. Now using the equation above and comparing entries in the 1st row, we find that the last \( k \) entries of the 1st row of \( L x_j \) must be 0. Using these together with the 2nd row, we find that the last \( k - 1 \) entries of the 2nd row of \( L x_j \) are 0. Similarly the last \( k - 2 \) entries of the 3rd row of \( L x_j \) are 0, and continuing, we conclude that the \( (k, n) \) entry of \( L x_j \) is 0. Our choice of eigenvector \( x_i \) was arbitrary, so the \( (k, n) \) entry is 0 for all \( t \) of the \( L x_j \). Thus we have \( t \) matrices \( L x_j \), all of which have nonzero entries in at most the same \( t - 1 \) positions in the last column. It follows that some nontrivial linear combination of the \( L x_j \) has only 0's in the last column and hence is not invertible. This is a contradiction, since \( \sigma \) is a division algebra.

If \( \text{char} \, K \neq p \), we cannot expect such a nice result. However, we do have the following theorem.

**Theorem 2.** Let \( A \) be a division algebra over a field \( K \), and suppose \( \sigma \in \text{Aut}(A) \) has order \( p^a \), where \( p \) is a prime and \( a \) is a positive integer. If \( \text{char} \, K \neq p \) but the minimum polynomial of \( \sigma \) splits into linear factors over \( K \), then \( \sigma \) is similar to

\[
I_k \oplus \lambda I_k \oplus \lambda^2 I_k \oplus \cdots \oplus \lambda^{p^a - 1} I_k
\]

where \( \lambda \) is a primitive \( p^a \)th root of unity.
Proof. We first show that $\sigma$ must have an eigenvalue $\lambda \neq 1$ in $K$. Suppose not. Then the minimum polynomial of $\sigma$ is $m(x) = (x - 1)^t$, and $\sigma$ is similar to its Jordan form $J_t \oplus \cdots \oplus J_t$, where each $J_t$ is of the form

$$J_t = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & 1 & 0 & \cdots & 0 \\ 0 & 1 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & 1 \end{bmatrix}$$

But $J_t^p = I$. Thus either the $(2,1)$ entry of $J_t^p$ must be 0, which implies that $p^\alpha = 0$, which contradicts the fact that $\text{char } K \neq p$, or else $J_t$ is a $1 \times 1$ matrix. But if each $J_t$ is a $1 \times 1$ matrix, then $\sigma = I$, which is false. Hence $\sigma$ has an eigenvalue $\lambda \neq 1$.

Suppose the Jordan form of $\sigma$ is $J_t \oplus \cdots \oplus J_t$, where each

$$J_t = \begin{bmatrix} \lambda & 0 & 0 & \cdots & 0 \\ 1 & \lambda & 0 & \cdots & 0 \\ 0 & 1 & \lambda & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & \lambda \end{bmatrix}$$

As above, $J_t^p = I$ and the $(2,1)$ entry of $J_t^p$ is $p^\alpha \lambda_t^p = 0$, which implies that $p^\alpha = 0$, which contradicts the fact that $\text{char } K \neq p$, or else $J_t$ is a $1 \times 1$ matrix. Hence $\sigma$ is diagonalizable. But since $\sigma$ is of order $p^\alpha$, it follows that one of the eigenvalues, call it $\lambda$, must be the $p^\alpha$th primitive root of unity. By Lemma 1(ii), $\lambda'$ is also an eigenvalue of $\sigma$ for $1 \leq i \leq p^\alpha$. Also, from Lemma 1(iii), all the corresponding eigenspaces have the same dimension. Hence $\sigma$ is similar to

$$I_k \oplus \lambda I_k \oplus \cdots \oplus \lambda^{p^\alpha-1} I_k,$$

as required.

If we consider the case where $p = 2$ and $\alpha = 1$, then the automorphism is an involution and its minimum polynomial must divide $x^2 - 1$. It is easy to see that we can have only two cases—those described by Theorems 1 and 2. Thus we obtain the result of the main theorem of [2].
II. AUTOMORPHISMS OF ORDER 3 OF DIVISION ALGEBRAS

We now determine canonical forms for all automorphisms of order 3 of a division algebra. There are three different types. In the final section we construct examples of each type.

**Theorem 3.** Let $A$ be a division algebra of dimension $n$ over a field $K$, and suppose $\sigma \in \text{Aut}(A)$ is of order 3. Then $\sigma$ is similar to one of the following:

(i) $J \oplus \cdots \oplus J$, where

\[ J = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}; \]

(ii) $I_k \oplus \lambda I_k \oplus \lambda^2 I_k$, where $\lambda^3 = 1$;

(iii) $I_k \oplus J \oplus \cdots \oplus J$, where

\[ J = \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix} \quad \text{and} \quad 0 \leq k \leq \frac{n}{2}. \]

**Proof.** Since $\sigma$ is of order 3, the minimum polynomial $m(x)$ of $\sigma$ must divide $x^3 - 1$.

*Case 1:* $\text{char} K = 3$. Theorem 1 implies that $\sigma$ is similar to type (i).

*Case 2:* $\text{char} K \neq 3$ but $m(x)$ splits into linear factors over $K$. Theorem 2 implies that $\sigma$ is similar to type (ii).

*Case 3:* $\text{char} K \neq 3$ and $m(x)$ does not split into linear factors over $K$. Since $m(x) \neq x - 1$, the only possibilities are $m(x) = x^2 + x + 1$ or $m(x) = (x - 1)(x^2 + x + 1)$. If $m(x) = x^2 + x + 1$, then the rational canonical form of $\sigma$ is $J \oplus \cdots \oplus J$, where

\[ J = \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}. \]

If $m(x) = (x - 1)(x^2 + x + 1)$, then the rational canonical form of $\sigma$ is $I_k \oplus J \oplus \cdots \oplus J$, where each $J$ is the same as above but $k > 0$. It follows from Lemma 1(iv) that $k = \dim A \leq n/2$. \hfill \blacksquare
III. EXAMPLES OF AUTOMORPHISMS OF ORDER 3
OF DIVISION ALGEBRAS

We have constructed our finite examples of division algebras using the following method, which is not new (for example, see [1]). Let $K = \text{GF}(p)$ and $F$ be a finite extension of $K$. Let $A$ equal $F$ as a vector space over $K$, but define a new multiplication as

$$x \circ y = \mu x^{p^s} y^{p^t},$$  \hspace{1cm} (1)

where $s$ and $t$ are nonnegative integers and $\mu$ is a fixed element of $F$. Obviously $A$ is a division algebra over $K$.

For the construction of examples of type (ii) and (iii), it is useful to determine over which finite fields $x^2 + x + 1$ is irreducible. The following result is probably not new, but we include an easy proof.

**Lemma 3.** $x^2 + x + 1$ is irreducible over $\text{GF}(p^k)$ if and only if $p \equiv 2 \pmod 3$ and $k$ is odd.

**Proof.** Assume $p > 3$ and $k = 1$. Then $x^2 + x + 1$ is irreducible over $\text{GF}(p)$ if and only if $-3$ is a quadratic nonresidue mod $p$, in which case, using the Legendre symbol, we have $(-3/p) = -1$. If $p \equiv 2 \pmod 3$ and $p \equiv 3 \pmod 4$ then $(-3/p) = (3/p)(-1/p) = (3/p) = (p/3) = (2/3) = -1$. But if $p \equiv 2 \pmod 3$ and $p \equiv 1 \pmod 4$, then a similar argument also gives $(-3/p) = -1$. So $p \equiv 2 \pmod 3$ implies $(-3/p) = -1$. Similarly $p \equiv 1 \pmod 3$ implies $(-3/p) = 1$. Hence the result is true for $p > 3$ and $k = 1$. If $p \not\equiv 2 \pmod 3$, then $x^2 + x + 1$ is reducible over $\text{GF}(p)$ and hence over $\text{GF}(p^k)$ for any $k$. If $p \equiv 2 \pmod 3$, then $x^2 + x + 1$ is irreducible over $\text{GF}(p)$ but reducible over $\text{GF}(p^2)$ or any extension of $\text{GF}(p^2)$, and any such extension is isomorphic to $\text{GF}(p^{2n})$ for some $n$. Finally, the result is obvious if $p = 2$ or $p = 3$.

**Type (i)**

Consider $A = \text{GF}(3^{3k})$ as a vector space of dimension $3k$ over $K = \text{GF}(3)$. As above, define

$$x \circ y = \mu x^{3^s} y^{3^t}, \quad \text{where} \quad \mu \in \text{GF}(3^k).$$

Define $\sigma: A \rightarrow A$ as $\sigma(x) = x^3$. It is easy to check that $\sigma$ is an automorphism of type (i). A similar construction will produce an automorphism of type (i) for any prime power $p^n$. 

Type (ii)

Example 1. Let $p$ be a prime for which $x^2 + x + 1$ is reducible over $K = GF(p)$. Choose any irreducible polynomial of degree $3k$ over $K$ with root $\omega$. If we equip the vector space $K(\omega)$ with the multiplication (1) where $\mu \in GF(p^k)$, then we have a division algebra $A$ of dimension $3k$ over $K$. Define $\sigma : A \to A$ as $\sigma(x) = x^p$. Then $\sigma$ is an automorphism of type (ii). This algebra is associative only when $s = t = 0$ and $\mu = 1$, in which case it is just the usual extension field.

Example 2. Let $K = \mathbb{Q}(\lambda)$, where $\lambda$ is a primitive cube root of 1. Choose an irreducible polynomial of degree $3k$ over $K$, and let $\omega$ be a root of this irreducible. Let $A$ be the extension field $K(\omega)$. Then $A$ is an algebra of dimension $3k$ over $K$. Define $\sigma : A \to A$ by extending $\sigma(\omega) = \lambda \omega$ in the usual way. Then $\sigma$ is an automorphism of type (ii).

Type (iii)

Example 1. Let $p$ be a prime for which $x^2 + x + 1$ is irreducible over $K = GF(p)$. Let $A = GF(p^{3m})$, and equip $A$ with the multiplication (1) where $\mu \in GF(p^n)$. Define $\sigma : A \to A$ as $\sigma(x) = x^{p^m}$. Then $\sigma$ is an automorphism of type (iii). In this example $\sigma$ is similar to $I_m \oplus J_1 \oplus \cdots \oplus J_m$ where $\dim A = 3m$.

Example 2. Let $A = \mathbb{H}$, the quaternions, which forms a four-dimensional division algebra over $\mathbb{R}$. Then any rotation of $2\pi/3$ in $\mathbb{R}^3$ corresponds to an automorphism $\sigma$ of $\mathbb{H}$. Such an automorphism is of type (iii) and is similar to $I_2 \oplus J$.

REFERENCES


Received 7 December 1987; final manuscript accepted 15 December 1987