Canad. Math. Bull. Vol. **17** (5), 1975

ON INVOLUTIONS OF QUASI-DIVISION ALGEBRAS

BY
LOWELL SWEET

All algebras are assumed to be finite dimensional and not necessarily associative. An involution of an algebra is an algebra automorphism of order two. A quasi-division algebra is any algebra in which the non-zero elements form a quasi-group under multiplication. The purpose of this short paper is to determine the structure of all involutions of quasi-division algebras and to give an application of this result.

LEMMA. *Let A be a quasi-division algebra of dimension n over a field K and suppose that $\alpha \in \mathrm{Aut}\, A\backslash\{Id\}$ has an eigenvalue $\lambda \in K$. If $A_\alpha(\lambda)$ indicates the corresponding eigenspace then*

$$\text{dimension } A_\alpha(\lambda) \leq [n/2]$$

Proof. Since $\alpha \neq Id$ we may choose $e \in A\backslash\{0\}$ such that $\alpha(e) \neq e$. We now claim that

$$A_\alpha(\lambda) \cap A_\alpha(\lambda)\cdot e = \{0\} \tag{1}$$

For suppose

$$0 \neq x = y\cdot e \in A_\alpha(\lambda) \quad \text{with} \quad y \in A_\alpha(\lambda)$$

then

$$\begin{aligned} \alpha(x) &= \alpha(y\cdot e) \\ &= \alpha(y)\cdot\alpha(e) \\ \lambda x &= \lambda y\cdot\alpha(e) \\ x &= y\cdot\alpha(e) \end{aligned}$$

but this implies that $\alpha(e)=e$ which is a contradiction.

But now the fact that A is a quasi-division algebra implies that $\dim A_\alpha(\lambda)= \dim A_\alpha(\lambda)\cdot e$ and then (1) implies that

$$\begin{aligned} 2 \dim A_\alpha(\lambda) &\leq n \\ \dim A_\alpha(\lambda) &\leq [n/2] \end{aligned}$$

THEOREM 1. *Let A be a quasi-division algebra of* dim *n over a field K. Then*

(i) *If n is odd then* $\mathrm{Aut}(A)$ *contains no involutions*

(ii) *If n is even and* char $K\neq 2$ *and α is any involution of A then there exists a basis of A such that the corresponding matrix representation of α is*

$$\alpha = -I_{n/2} \oplus I_{n/2}$$

Received by the editors November 14, 1973.

https://doi.org/10.4153/CMB-1974-130-1 Published online by Cambridge University Press

(iii) *If n is even and* char $K=2$ *and* α *is any involution of A then there exists a basis of A such that the corresponding matrix representation of* α *is*

$$\alpha = A_1 \oplus A_2 \oplus \cdots \oplus A_{n/2}$$

$$\text{where each } A_i = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \quad \text{for} \quad 1 \leq i \leq n/2.$$

Proof. (i) Let α be any involution of A. Then the minimal polynomial of α must divide x^2-1. Suppose that char $K \neq 2$. Since $\alpha \neq Id$ and $-Id$ is never an automorphism of a non-zero algebra it follows that the minimal polynomial of α is $(x+1)(x-1)$. Since $\pm 1 \in K$ we may choose a basis of A so that the corresponding matrix representation of α is in Jordan Normal Form. That is, we may assume that

$$(1) \qquad \alpha = -I_r \oplus I_s$$

where $1 \leq r$, $s < n$ and $r+s=n$. Since n is odd, either $r > [n/2]$ or $s > [n/2]$ and so either dim $A_\alpha(-1) > [n/2]$ or dim $A_\alpha(1) > [n/2]$ both of which contradict the previous lemma. Hence we may assume that char $K=2$. In this case it follows that the minimal polynomial of α is $x^2+1=(x+1)^2$ and as above we assume that a basis of A has been chosen so that the corresponding matrix representation of α is in the Jordan Normal Form. That is

$$(2) \qquad \alpha = I_r \oplus A_1 \oplus A_2 \oplus \cdots \oplus A_k$$

where $A_i = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ for all i, $1 \leq i \leq k$. But then since n is odd it follows that $r \neq 0$ and so

$$\dim A_\alpha(1) = r+k > [n/2]$$

which again contradicts the previous theorem and hence in all cases, Aut(A) is involution free.

(ii) The proof is very similar to the above and follows easily since the lemma implies that

$$\dim A_\alpha(1) = \dim A_\alpha(-1) = n/2$$

(iii) Again the proof is similar to (i) above and the lemma implies that the only possibility for r in (2) above is $r=0$.

We now give an application of the above theorem. The following notation is due to Djoković [1].

DEFINITION. An algebra A over a field K is said to be extremely homogeneous if Aut(A) acts transitively on $A \backslash \{0\}$.

Extremely homogeneous algebras over finite fields have been investigated by Kostrikin and the following definition appears in his paper [4].

DEFINITION. Let $F=GF(2^n)$ and suppose μ is any fixed element in F. Let $\circ: F\times F\to F$ by the map defined by

$$(x, y) \to x \circ y = \mu(xy)^{2^{n-1}}$$

Then $A(n, \mu)$ denotes the algebra over $GF(2)$ obtained from F by replacing the usual multiplication in F by the map $\circ$.

The following two theorems are due to Gross [3].

THEOREM 2 (*Gross*). *If A is a non-zero, extremely homogeneous algebra over $GF(2)$ then A is a quasi-division algebra.*

THEOREM 3 (*Gross*). *If A is a non-zero algebra of* $\dim n$ *over $GF(2)$ such that* $\mathrm{Aut}(A)$ *contains a solvable subgroup H which acts transitively on $A\backslash\{0\}$ then $A\cong A(n, \mu)$ for some fixed $\mu \in GF^*(2^n)$.*

Now we have the following result:

THEOREM 4. *If A is a non-zero, extremely homogeneous algebra of odd* $\dim n$ *over $GF(2)$ then $A\simeq A(n, \mu)$ for some fixed $\mu \in GF^*(2^n)$.*

Proof. It follows from Theorem 2 that A is a quasi-division algebra. But then Theorem 1 implies that $\mathrm{Aut}(A)$ is of odd order and hence solvable by the Feit-Thompson Theorem [2]. The desired result now follows directly from Theorem 3.

ACKNOWLEDGEMENTS. This paper represents part of the author's thesis prepared at the University of Waterloo under the direction of D. Ž. Djoković. The author is indebted to the National Research Council of Canada and the University of Waterloo for their financial assistance and to Prof. Djoković for his guidance and encouragement.

REFERENCES

1. D. Ž . Djoković, *Real homogeneous algebras*, Proc. Amer. Math. Soc., **41** (1973), 457–462.

2. W. Feit and J. Thompson, *Solvability of groups of odd order*, Pacific J. Math., **13** (1963), 775–1029.

3. F. Gross, *Finite automorphic algebras over GF*(2), Proc. Amer. Math. Soc., **4** (1971), 349–353.

4. A. I. Kostrikin, *On homogeneous algebras*, Izvestia Acad. Nauk. U.S.S.R., **29** (1965), 471–484.

UNIVERSITY OF PRINCE EDWARD ISLAND
CHARLOTTETOWN, P.E.I.