A USEFUL PROPOSITION FOR DIVISION ALGEBRAS OF SMALL DEGREE

DARRELL HAILE

(Communicated by Donald S. Passman)

ABSTRACT. Let F be a field and let D be an F -central division algebra of degree n . We present a short, elementary proof of the following statement: There is an $n-1$ -dimensional F -subspace V of D such that for every nonzero element v of V , $\text{Tr}(v) = \text{Tr}(v^{-1}) = 0$. We then indicate how one can use this result to obtain the basic structural results on division algebras of degree three and four (results of Wedderburn and Albert, respectively).

In this note we present a simple proposition about reduced traces in division algebras and show how it can be used to obtain easily the basic structure theorems for division algebras of degree three and four. The proposition is implicit in the paper [2] of Brauer but his argument uses the more sophisticated theory of Brauer factor sets.

Let F be a field and if D is an F -central division algebra let $\text{Tr}: D \rightarrow F$ denote the reduced trace.

Proposition. *Let D be an F -central division algebra of degree n . Let K be a maximal subfield. Then:*

- (1) *There is an element $d \in D^\times$ such that $\text{Tr}(kd) = 0$ for all $k \in K$.*
- (2) *Let d be as in (1). There is an F -subspace V of K such that $\dim V = n-1$ and $\text{Tr}(k^{-1}d) = \text{Tr}(d^{-1}k) = 0$ for all $k \in V - \{0\}$.*

In particular there is an $(n-1)$ -dimensional subspace W of D such that $\text{Tr}(w) = \text{Tr}(w^{-1}) = 0$ for all $w \in W - \{0\}$.

Proof. (1) There is an F -linear transformation U from D to K^* (the dual space of K) given by $U(d)(k) = \text{Tr}(kd)$ for $d \in D$, $k \in K$. Since $\dim_F D > \dim_F K$, the result follows.

(2) Given d as in (1), there is an F -functional S on K given by $S(k) = \text{Tr}(d^{-1}k)$. Let $k \in \ker(S) - \{0\}$. Then $\text{Tr}(k^{-1}d) = 0$ by the choice of d and $\text{Tr}(d^{-1}k) = 0$ because $k \in \ker(S)$. But $\dim_F \ker(S) \geq n-1$, so we may choose V to be any $(n-1)$ -dimensional subspace of $\ker(S)$.

Finally if we let $W = d^{-1}V$, then $\text{Tr}(w) = \text{Tr}(w^{-1}) = 0$, for all $w \in W$.

Received by the editors July 20, 1988.

1980 *Mathematics Subject Classification* (1985 Revision). Primary 16A16, 13A20.

©1989 American Mathematical Society
0002-9939/89 \$1.00 + \$.25 per page

Remark. Since the kernel of the map U of part (1) has dimension at least $n^2 - n$, we see that if $n \geq 3$, then we may choose $d \in \ker(U)$ such that $d \notin K$. We will use this remark later. Of course if K/F is separable, then in fact $\ker(U) \cap K = 0$.

Corollary 1. *If D is an F -central division algebra of degree 4, then D contains a quadratic field extension of F .*

Proof. Choose W as in the proposition and let $d \in W - \{0\}$. Because $\text{Tr}(d) = \text{Tr}(d^{-1}) = 0$, the minimal polynomial of d over F is either quadratic or quartic with no cubic or linear term. In the latter case the minimal polynomial has the form $x^4 + \alpha x^2 + \beta$, for some $\alpha, \beta \in F$, $\beta \neq 0$. But then $F(d)$ contains a quadratic extension of F , so in any case D contains a quadratic field extension. $\square$

Given this corollary Albert [1, Lemma 11.4] showed that one can easily infer that D is a crossed product with group $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Corollary 2. *If D is an F -central division algebra of degree three then there is an element $d \in D - F$ such that $d^3 \in F$.*

Proof. By the proposition there is an element $d \in D^\times$ such that $\text{Tr}(d) = \text{Tr}(d^{-1}) = 0$. It follows that the minimal polynomial of d over F is of the form $x^3 - \alpha$ for some $\alpha \in F^\times$, that is $d^3 \in F$. $\square$

Again Albert [1, Theorem 11.4] showed that one can use the result of this corollary to prove that division algebras of degree three are cyclic (a theorem of Wedderburn [3]). However the proof in this case is not as simple as that for algebras of degree four. We therefore proceed to show how one can use ideas similar to those in the proposition to obtain Wedderburn's theorem.

Theorem (Wedderburn). *Let D be a division algebra of degree 3. Then there is an element $d \in D - F$, such that $d^3 \in F$. Moreover if x is any element of $D - F$ such that $x^3 \in F$, then D contains a cyclic maximal subfield L such that $x \notin L$ and $xLx^{-1} = L$.*

Proof. By the corollary there is an element x in $D - F$ such that $x^3 \in F$. Let $x^3 = a$. Let $K = F(x)$.

For later use we note that if U and V are two-dimensional F -subspaces of K , then there is an element $k \in K$ such that $kU = V$: There exist F -functionals f and g in K^* such that $U = \ker(f)$ and $V = \ker(g)$. Because K^* is a one-dimensional K -space there is an element $k \in K^\times$ such that $kg = f$. But then $kU = V$. To motivate the proof of the theorem, we first observe that if there is a cyclic maximal subfield $L = F(\theta)$ with $xLx^{-1} = L$, then $(\theta x)^3 = N_{L/F}(\theta)a \in F$ and similarly $(\theta x^2)^3 \in F$. Conversely if there is an element $\theta \in D - K$ such that $(\theta x)^3, (\theta x^2)^3 \in F$, then $L = F(\theta)$ satisfies $xLx^{-1} = L$ (and so is our desired extension): It suffices to show that θ and $x\theta x^{-1}$ commute (because $\theta \notin K$). Let $N: D \rightarrow F$ denote the reduced norm.

Because $x^3, (\theta x)^3, (\theta x^2)^3 \in F$, it follows that $N(x) = a$, $N(\theta x) = (\theta x)^3$ and $N(\theta x^2) = (\theta x^2)^3$. Moreover $N(\theta x^2) = N(\theta x)N(x)$ and hence $(\theta x^2)^3 = a(\theta x)^3$. It follows that $x\theta x^2\theta x = a\theta x\theta$, and so $x\theta x^{-1}\theta = \theta x\theta x^{-1}$.

So it suffices to find $\theta \in D - K$ such that $(\theta x)^3, (\theta x^2)^3 \in F$. Now for any $y \in D$, we define $K_y = \{k \in K \mid \text{Tr}(y^{-1}k) = 0\}$. It is then easy to see that if $k \in K$, then $K_{ky} = kK_y$.

By the remark following the proposition there is an element $d \in D - K$ such that $\text{Tr}(kd) = 0$ for all $k \in K$. We claim there is an element $k \in K^x$ such that $K_{kd} \supseteq Fx + Fx^2$. To see this note that either $K_d = K$ (in which case the claim is proved) or $[K_d : F] = 2$. In this second case because K_d and $Fx + Fx^2$ are two-dimensional subspaces of K , there is an element $k \in K$ such that $kK_d = Fx + Fx^2$. Since $kK_d = K_{kd}$, we have proved the claim. Letting $\theta = kd$, we have $\text{Tr}(\theta x) = \text{Tr}((\theta x)^{-1}) = \text{Tr}(\theta x^2) = \text{Tr}((\theta x^2)^{-1}) = 0$. Hence $(\theta x)^3, (\theta x^2)^3 \in F$, so we are done.

REFERENCES

1. A. A. Albert, *Structure of algebras*, AMS Colloquium Series, vol. 24, 2nd ed., Amer. Math. Soc., Providence, R.I., 1961.
2. R. Brauer, *On normal division algebras of index five*, P.N.A.S., vol. 24 (1938), 243–246.
3. J. H. M. Wedderburn, *On division algebras*, Trans. Amer. Math. Soc. 22 (1921), 129–135.

DEPARTMENT OF MATHEMATICS, INDIANA UNIVERSITY, BLOOMINGTON, INDIANA 47405