ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 9, Number 2, Spring 1979

A CHARACTERIZATION OF QUATERNION DIVISION ALGEBRAS

KIRBY C. SMITH

ABSTRACT. Let D be a division ring with center F of characteristic not two. Let $W_F(D)$ be the set of all $a \in D$ such that $a^n \in F$ for some positive integer n. If n is minimal such that $a^n \in F$ then n is called the rank of a. It is shown that if $W_F(D) \neq F$ and if $W_F(D)$ has the property that whenever $a, b \in W_F(D)$ have the same rank then $a + b \in W_F(D)$, then D is a quaternion division algebra over F.

Let D be a division ring with center F. A well-known theorem due to Kaplansky says that if D has the property that for every $a \in D$ there exists a positive integer n, depending on a, such that $a^n \in F$ then $D = F$. If Q is a (generalized) quaternion division algebra over F (of characteristic not two) then every pure quaternion $q = \alpha_1 i + \alpha_2 j + \alpha_3 k$, $\alpha_i \in F$, has the property that $q^2 \in F$ and so Q "almost" satisfies the hypothesis of Kaplansky's theorem.

If A is an algebra over the field F let

$$W_F(A) = \{a \in A\colon a^n \in F \text{ for some } n > 0\}.$$

For $a \in W_F(A)$ let n be the least positive integer such that $a^n \in F$ and call n the *rank* of a over F. We shall say that $W_F(A)$ is *nondegenerate* if $W_F(A) \neq F$, and $W_F(A)$ is *weakly closed* if it has the property that whenever $a, b \in W_F(A)$ such that a and b have the same rank over F, then $a + b \in W_F(A)$. It is easily verified that if Q is a quaternion algebra over F then $W_F(Q)$ is nondegenerate and weakly closed. We shall prove that quaternion division algebras are the only algebraic division algebras of characteristic not two with this property.

The first lemma is similar to Kaplansky's lemma ([3], page 77) with an analogous proof.

LEMMA 1. *Let K be an extension field of F. Assume $W_F(K)$ is nondegenerate and weakly closed. Let W_S be the subset of $W_F(K)$ consisting of the separable elements over F. If $W_S \neq F$ then either*

(i) *$a^2 \in F$ for all $a \in W_S$, or*

(ii) *F has characteristic $p \neq 0$ and it is algebraic over its prime subfield P.*

Received by the editors on February 9, 1977.
AMS 1971 *Subject Classification*: 16A46, 16A50.
Key words and phrases: Quaternion alggebra, division algebra.

Proof. Assume (i) is not true. Then there exists an $a \in W_S$ such that a has rank $n > 2$. If n is not a power of 2 then a may be reselected so that its rank is a prime different from 2. If n is a power of 2 then the element a may be reselected so that a has rank 4. Hence we may assume n is either 4 or a prime different from 2. We imbed $F(a)$ in a Galois extension L of F, so there is an F-automorphism Φ of L which moves a. In fact, since $a^n \in F$ and n is either 4 or a prime different from 2, then $\Phi(a) = \lambda a \neq a$ where λ is a primitive nth root of unity.

There is an integer k, $1 < k < n$, such that a^k has rank n. For each $i \in P$ the element $a + ia^k$ belongs to both W_s and L. We have

$$\Phi(a + ia^k) = \mu_i(a + ia^k)$$

where μ_i is an $m_i{}^{\text{th}}$ root of unity for some integer m_i. Thus

$$\mu_i(a + ia^k) = \Phi(a + ia^k) = \lambda a + i\lambda^k a^k.$$

We cannot have $\mu_i = \lambda^k$ since otherwise $\lambda^k = \lambda$ or $\lambda^{k-1} = 1$ contradicting λ being a primitive n^{th} root of unity. This means $ia^{k-1} = (\mu_i - \lambda)/(\lambda^k - \mu_i)$. Since μ_i and λ are algebraic over P, so are ia^{k-1} and a.

Assume F has characteristic 0. Then $\{ia^{k-1}\colon i \in P\}$ is an infinite set which means $\{\mu_i\colon i \in P\}$ is infinite. Let L_0 be a Galois extension of P containing a and hence containing $a + ia^k$ for all $i \in P$. It is easy to verify that μ_i belongs to L_0 for all $i \in P$ and thus L_0 is a finite extension of F containing infinitely many distinct roots of 1. This is impossible, so F must be a modular field.

The field $P(a)$ is a finite field having, say p^m elements. We have $a^s = 1$ where $s = p^m - 1$, and if $\alpha \in F$ then $F(\alpha a)$ is finite, so $(\alpha a)^t = 1$ for some $t > 0$. This means

$$1 = (\alpha a)^{ts} = \alpha^{ts} a^{ts} = \alpha^{ts}$$

and F is algebraic over P.

Lemma 2. *Let D be a division ring with center F of characteristic not two. If $W_F(D)$ is nondegenerate and weakly closed then $W_F(D)$ contains an element not in F which is separable over F.*

Proof. Assume $W_F(D)$ contains only purely inseparable elements. Then F has characteristic $p \neq 0$ and $W_F(D)$ contains an element $j \notin F$ such that $j^p \in F$. From the proof of Theorem 3.2.1, page 78 of [3] there exists a $t \in D$ such that

$$tj = j(t + 1). \tag{1}$$

If t is algebraic over F it cannot be purely inseparable over F, for otherwise $t = 1 + jtj^{-1}$ whence $t^{p^k} = 1 + (jtj^{-1})^{p^k} = 1 + t^{p^k}$ for some integer k, which is impossible. If t is algebraic and inseparable over F then there is an integer k such that $s = t^{pk}$ is separable over F with $s \notin F$. From (1) we have $sj = j(s + 1)$. The above implies that the element t in (1) may be selected so that the field $K = F(t)$ contains no inseparable elements over F.

The field $K = F(t)$ has an automorphism ∂ defined by $t^{\partial} = j^{-1}tj = t + 1$. Since $j - t^{-1}jt = t^{-1}j$ belongs to $W_F(D)$ then $(t^{-1}j)^n \in F$ where n is the rank of $t^{-1}j$. Since $t^{-1}j = j(t^{\partial})^{-1}$ we have

$$(t^{-1}j)^n = j^n(t^{\partial}t^{\partial^2} \cdots t^{\partial^n})^{-1}, \tag{2}$$

an element of F. The field $F(j)$ is a purely inseparable extension of F so the only elements common to both $F(j)$ and K are the elements of F. Equation (2) implies that both j^n and $t^{\partial}t^{\partial^2} \cdots t^{\partial^n}$ *belong to F*. This means p divides n, say $n = pk$, and $t^{\partial}t^{\partial^2} \cdots t^{\partial^n} = (t^{\partial}t^{\partial^2} \cdots t^{\partial^p})^k$ belongs to F. If $k > 1$ then $t^{\partial}t^{\partial^2} \cdots t^{\partial^p}$ belongs to both K and $W_F(D)$, an impossibility since $W_F(D)$ contains only purely inseparable elements. We now have $k = 1$ and

$$t^{\partial}t^{\partial^2} \cdots t^{\partial^p} = (t + 1)(t + 2) \cdots (t) \in F. \tag{3}$$

This means K is a Galois extension of F of degree p with Galois group $\langle \partial \rangle$.

For $s = 1, 2, \cdots, p - 1$ and all $k \in K$ we have $kj^s \in W_F(D)$ with rank p since $(kh^s)^p = kk^{\partial^s} \cdots k^{\partial^{(p-1)s}}(j^s)^p \in F$. Let $D_1 = (K, \partial, j^p)$ be the cyclic subalgebra of D generated by j and t. Then D_1 satisfies the hypothesis of the lemma and

$$W_F(D_1) \supset \{jk_1 + j^2k_2 + \cdots + j^{p-1}k_{p-1} : k_i \in K\}.$$

We show now that $W_F(D_1)$ is not weakly closed. From (3) the minimal polynomial for t over F is

$$m(x) = x^p + (p - 1)x + \alpha \tag{4}$$

for some $\alpha \neq 0 \in F$. Since $p > 2$ we have $jt + j^2t^{\partial} \in W_F(D_1)$ and it is purely inseparable of rank p. So F contains

$$(jt + j^2t^{\partial})^p = j^p(t^{\partial^{p-1}} + jt)(t^{\partial^{p-2}} + jt^{\partial^{p-1}}) \cdots (t + jt^{\partial}).$$

The coefficient of j in the above product is $\beta j^p t$ where β is the sum of the products of the roots of $m(x)$ taken $p - 1$ at a time. By (4) we have $\beta = p - 1 \neq 0$, hence $(jt + j^2t^{\partial}) \notin W_F(D)$, a contradiction. So $W_F(D)$ must contain separable elements not in F.

LEMMA 3. *Let D be a division ring which is algebraic over its center F of characteristic not 2. If $W_F(D)$ is nondegenerate and weakly closed then every element of $W_F(D)$ is separable over F.*

PROOF. By Lemma 2 $W_F(D)$ contains a separable element, say $a \notin F$. The extension field $F(a)$ of F satisfies the hypotheses of Lemma 1 so either $a^2 \in F$ or else F has characteristic $p \neq 0$ and it is algebraic over its prime subfield P. The latter case is impossible since it implies D is algebraic over P and hence commutative ([4], page 183, *Theorem* 2). So we must have $a^2 \in F$ for all separable a in $W_F(D)$.

Assume $W_F(D)$ contains purely inseparable elements. Then F has characteristic $p \neq 0$ and $W_F(D)$ contains an inseparable element $j \notin F$ such that $j^p \in F$. As in the proof of Lemma 2 there is a $t \in D$ such that $tj = j(t + 1)$ where $K = F(t)$ contains no inseparable elements over F. The element $\mu = t^{\partial}t^{\partial^2} \cdots t^{\partial^p}$ belongs to both K and $W_F(D)$, whence μ has rank 1 or 2. If μ has rank 1 then $D_1 = (K, \partial, j^p)$ is a division subalgebra such that $W_F(D_1)$ should, but doesn't, have the desired properties. Hence we may assume μ has rank 2.

We have $K = F(t) \supset F(\mu) \supset F$ where $(F(t) : F(\mu)) = p$ and $(F(\mu) : F) = 2$. The cyclic subalgebra $D_1 = (K, \partial, j^p)$ has degree p over $F(\mu)$. As in the proof of Lemma 2 the elements jt and j^2t^{∂} both belong to $W_F(D)$ and have rank $2p$. Hence $jt + j^2t^{\partial}$ belongs to $W_F(D)$ and it has rank p or $2p$. But as before $(jt + j^2t^{\partial})^p$ does not belong to $F(\mu)$, hence $(jt + j^2t^{\partial})^{2p}$ cannot belong to F. So $W_F(D)$ can contain only separable elements.

THEOREM. *Let D be an algebraic division algebra with center F of characteristic not two. If $W_F(D)$ is nondegenerate and weakly closed then D is a quaternion algebra over F.*

PROOF. By Lemma 3 and its proof every element of $W_F(D)$ is separable over F and $a^2 \in F$ for all $a \in W_F(D)$. Since $W_F(D)$ is nondegenerate it contains elements of rank 2. Let V_2 be the subset of $W_F(D)$ consisting of the rank 2 elements and let $V = V_2 \cup \{0\}$. It is easy to verify that V forms a vector space over F. Moreover V has the property that $ab + ba \in F$ for all $a, b \in V$. The map $(a, b) \to ab + ba$ is a nondegenerate symmetric bilinear form on V. If V has dimension greater than 3 over F then there exists linearly independent vectors a_1, a_2, a_3, $a_4 \in V$ such that $(a_i, a_j) = 0$, $i \neq j$. Let D_1 be the subalgebra of D generated by $\{a_1, a_2, a_3, a_4\}$, a division algebra over F of dimension $\leqq 2^4$. By [2], page 39, D_1 is a homomorphic image of the Clifford algebra A over F on four generators. But $A \cong Q_1 \otimes Q_2$ where Q_1 and Q_2 are quaternion algebras over F and so A is simple, whence $A \cong D_1$. But

$W_F(A)$ does not have the desired properties since $(i \otimes 1)^2$ and $(1 \otimes j)^2$ belong to F but $(i \otimes 1 + 1 \otimes j)^2$ does not. This means $A \cong D_1$ is impossible and we must have $(V : F) \leqq 3$.

By the Cartan-Brauer-Hua theorem V generates D and so $(D : F) \leqq 2^3$. Since $(D : F)$ is a perfect square we must have $(D : F) = 4$ and D is a quaternion algebra.

The following corollary is immediate.

COROLLARY. *Let A be a finite dimensional central simple algebra over F of characteristic not two. If $W_F(A)$ is nondegenerate and weakly closed then A is a quaternion algebra over F.*

REFERENCES

1. A. Albert, *Structure of Algebras,* Amer. Math. Soc. Colloq. Publ., XXIV, 1939.
2. C. Chevalley, *Algebraic Theory of Spinors,* Columbia University Press, New York, 1954.
3. J. Herstein, *Noncommutative Rings,* Carus Math. Monograph **15**, M.A.A., 1968.
4. N. Jacobson, *Structure of Rings,* Amer. Math. Soc. Colloq. Publ., XXXVII, 1964.

DEPARTMENT OF MATHEMATICS, TEXAS A&M UNIVERSITY, COLLEGE STATION, TEXAS 77843