A GENERALIZATION OF A THEOREM OF ALBERT

R. D. SCHAFER[1]

A celebrated theorem of J. H. M. Wedderburn states that any finite associative division ring is a field. A. A. Albert has recently extended this result by proving that any finite *power-associative* division ring of characteristic $p>5$ is a field [2].[2] We use Albert's method to prove a still more general theorem about finite power-associative rings.

A different generalization of the Wedderburn theorem is N. Jacobson's result that any associative ring in which every element a satisfies an equation of the form $a^{n(a)}=a$, $n(a)$ an integer >1, is commutative [5, Theorem 11]. The proof of this depends on Jacobson's structure theory for arbitrary associative rings. Because no such theory is known at present for arbitrary power-associative rings, we restrict our attention to finite rings and prove the following

THEOREM. *Let $\mathfrak{R}$ be a finite power-associative ring without elements of additive order* 2, 3, *or* 5. *If every element a of $\mathfrak{R}$ satisfies an equation of the form $a^{n(a)}=a$, $n(a)$ an integer >1, then either*

(i) *$\mathfrak{R}$ is a direct sum of finite fields, or*

(ii) *the attached commutative ring $\mathfrak{R}^+$ contains an ideal which is the unique* 3-*dimensional classical central simple Jordan algebra without nilpotent elements $\neq 0$ over some finite field*; *in this latter case, $\mathfrak{R}^+$ is a direct sum of fields and such* 3-*dimensional algebras* (*over possibly different finite fields*).

PROOF. The argument given in [5, pp. 702–703], reducing Jacobson's theorem to the case of an algebraic algebra without nilpotent elements $\neq 0$ over a finite field, does not depend on the associativity of the ring. Hence we know that $\mathfrak{R}$ is a (finite) direct sum of rings, each of which is a power-associative algebra of finite dimension over a finite field. We may as well assume that $\mathfrak{R}$ is a power-associative algebra of finite dimension over a finite field F of characteristic $p>5$.

There are no nilpotent elements $\neq 0$ in $\mathfrak{R}$. Since F is perfect, $\mathfrak{R}^+$ is a Jordan algebra over F.[3] Also the radical of $\mathfrak{R}^+$ (the maximal

Presented to the Society, December 29, 1952; received by the editors October 30, 1952.

[1] This research was supported in part by a grant from the National Science Foundation.

[2] Numbers in brackets refer to the references cited at the end of the paper.

[3] [2, Theorem 3]. This theorem is stated for algebraic division algebras, but the proof is valid for algebraic algebras without nilpotent elements $\neq 0$.

nilideal) is $\{0\}$, so that $\mathfrak{R}^+$ is semisimple. Then $\mathfrak{R}$ is the direct sum of subspaces $\mathfrak{T}_i$ such that $\mathfrak{T}_i^+$ is a simple Jordan algebra and $\mathfrak{T}_i^+$ is an ideal of $\mathfrak{R}^+$. In order to prove that any $\mathfrak{T}_i$ is an ideal of $\mathfrak{R}$, it is sufficient to prove that $\mathfrak{T}_i$ is a subalgebra, since the $\mathfrak{T}_i$ are orthogonal subspaces of $\mathfrak{R}$ by [1, Theorem 3].

Let $\mathfrak{Z}$ be the center of the simple Jordan algebra $\mathfrak{T}_i^+$. Then $\mathfrak{Z}$ is a separable extension $\mathfrak{Z}=F[z]$ of F. If $\mathfrak{T}_i^+=\mathfrak{Z}=F[z]$, then, because $\mathfrak{T}_i$ is generated by the single element z, we have $\mathfrak{T}_i=\mathfrak{Z}$, a field. Also $\mathfrak{T}_i$ is an ideal of $\mathfrak{R}$. If $\mathfrak{T}_i^+\neq\mathfrak{Z}$, then it follows, exactly as in the proof [2, p. 301] of Albert's theorem, that $\mathfrak{T}_i^+$ is a classical central simple Jordan algebra over the finite field $\mathfrak{Z}$, and is therefore included in the following list.[4] We show that, except for one 3-dimensional algebra, every algebra in the list contains a nilpotent element $\neq 0$.

$\mathrm{A_I}$. The algebra $\mathfrak{M}_t^+$, where $\mathfrak{M}_t$ is the algebra of all t-rowed square matrices over $\mathfrak{Z}$, and $t\geqq 2$. The element e_{12} is nilpotent.

$\mathrm{A_{II}}$. The algebra $\mathfrak{S}^+$, where $\mathfrak{S}$ is the set of all J-symmetric matrices $a=a^J=g\bar{a}'g^{-1}$ of $\mathfrak{M}_t\times\mathfrak{Z}(\theta)$ for $t\geqq 2$ where g is a nonsingular diagonal matrix in $\mathfrak{M}_t$ and $\mathfrak{Z}(\theta)$ is a quadratic extension of $\mathfrak{Z}$ with nontrivial automorphism $\alpha\rightarrow\bar{\alpha}$. $\mathfrak{S}^+$ contains a subalgebra of type $\mathrm{A_{II}}$ and degree 2 (dimension 4) which is isomorphic to an algebra of type D (below) containing a nilpotent element $\neq 0$.

B.[5] The algebra $\mathfrak{S}^+$, where $\mathfrak{S}$ is the set of all J-symmetric matrices $a=a^J=ga'g^{-1}$ of $\mathfrak{M}_t$ for $t\geqq 2$ and $g=g'$. We may always choose a basis so that g is replaced by cgc' for any nonsingular c. If $t>2$ the quadratic form $f(\xi)=\xi g\xi'$ is a null form, a result actually equivalent to the fact that there are no quaternion division algebras over any finite field. Use a nonzero solution ξ as the first row of c and (by the usual devices of the theory of congruent matrices) it may then be argued easily that c may be chosen so that

$$g=\begin{pmatrix}0&1&0\\1&0&0\\0&0&h\end{pmatrix}.$$

Then $ge_{21}g^{-1}=e_{12}$, e_{12} is in $\mathfrak{S}$, $e_{12}^2=0$. When $t=2$ and $\xi g\xi'$ is a null form this proof is still valid. There remains the case where $\xi g\xi'$ is not

[4] We take our list of (classical) special Jordan algebras over a finite field from [4]. The (classical) exceptional Jordan algebras (type E) have been determined in [6]; for it follows from [4, Theorem 3] that the proof of the lemma and Theorem 1 of [6] remain valid for characteristic $\neq 2$.

[5] The argument given in this paragraph is substantially the referee's revision of our original proof. He points out that it is the case for a finite field of the following general result: there exists a nilpotent matrix $a=ga'g^{-1}(\neq 0)$ if and only if the associated quadratic form $f(\xi)=\xi g\xi'$ is a null form.

a null form. Then $\xi g\xi' - \eta^2$ (being a form in three variables) is a null form, $\xi g \xi'$ represents 1, and for *any* nonsquare $-\pi$ in $\mathfrak{Z}$ we may choose c so that

$$g = \begin{pmatrix} 1 & 0 \\ 0 & \pi \end{pmatrix}$$

(since the product of any two nonsquares is a square in $\mathfrak{Z}$). Then $\mathfrak{S}^+$ is the unique 3-dimensional Jordan algebra of all matrices

$$a = \begin{pmatrix} \alpha & \beta \\ \pi\beta & \gamma \end{pmatrix}$$

for $-\pi$ a nonsquare in $\mathfrak{Z}$. Then $a \neq 0$ is never nilpotent since otherwise a has zero trace, $\gamma = -\alpha$, and $a^2 = (\alpha^2 + \pi\beta^2)I$ is a nonzero scalar matrix.

C. The algebra $\mathfrak{S}^+$, where $\mathfrak{S}$ is the set of all J-symmetric matrices $a = a^J = ga'g^{-1}$ of $\mathfrak{M}_{2t}$ where

$$g = \begin{pmatrix} 0 & I_t \\ -I_t & 0 \end{pmatrix}$$

and $t \geqq 2$. There is a subalgebra of type A_I (above) and degree $t \geqq 2$.

D. An algebra $\mathfrak{B} = \mathfrak{Z} + u_2\mathfrak{Z} + \cdots + u_s\mathfrak{Z}$ where $u_i^2 = \alpha_i \neq 0$ in $\mathfrak{Z}$, $u_i u_j = 0$ for $i \neq j$, and $s \geqq 3$. For any a in $u_2\mathfrak{Z} + \cdots + u_s\mathfrak{Z}$, we have $a^2 = f(\xi)$, a (diagonal) quadratic form in $s-1$ variables. If $s \geqq 4$, $f(\xi)$ is a null form and there is an element $a \neq 0$ such that $a^2 = 0$. If $s = 3$, then $\mathfrak{B}$ is isomorphic to an algebra of type B and dimension 3 which may be without nilpotent elements $\neq 0$, as we have seen above.

E. The algebra $\mathfrak{S}^+$, where $\mathfrak{S}$ is the set of all J-symmetric elements $a = a^J = g\bar{a}'g^{-1}$ of $\mathfrak{M}_3 \times \mathfrak{C}$ where $g = \text{diag}\ \{\pi_1, \pi_2, \pi_3\}$ in $\mathfrak{M}_3$ and $\mathfrak{C}$ is a Cayley algebra over $\mathfrak{Z}$. By Albert's theorem (or merely by the fact that the norm form $n(x)$ in eight variables is a null form), $\mathfrak{C}$ is not a division algebra and there exists $x \neq 0$ in $\mathfrak{C}$ such that $n(x) = x\bar{x} = \bar{x}x = 0$. Then $a^2 = 0$ for

$$a = \begin{pmatrix} 0 & x & 0 \\ \pi_2\pi_1^{-1}\bar{x} & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

This completes the proof of our theorem.

Over a given $GF(p^n)$, $p \neq 2$, there are exactly two nonisomorphic 3-dimensional algebras $\mathfrak{S}^+$, one without nilpotent elements $\neq 0$, the other having nilpotent elements $\neq 0$. We remark that, in case $p = 4m + 3$ with n odd, then -1 is a nonsquare in $GF(p^n)$, and the algebra

$\mathfrak{H}^+$ of all 2×2 symmetric matrices is the algebra without nilpotent elements $\neq 0$. In case $p=4m+3$ with n even, or $p=4m+1$, then -1 is a square in $GF(p^n)$, and $\mathfrak{H}^+$ is the algebra with nilpotent elements $\neq 0$.

Clearly Albert's theorem is a particular case of the theorem in this note. For, if $\mathfrak{R}$ is a finite division ring, power-associativity insures that every nonzero element a generates a (finite) multiplicative group; then $a^{n(a)}=a$ for $n(a)>1$. The possibility (ii) cannot occur since any 3-dimensional algebra $\mathfrak{S}^+$ contains a pair of orthogonal idempotents. Also there can be only one summand in (i).

It follows from the same considerations as for associative algebras [5, pp. 699, 702] that every element a of an algebraic power-associative algebra without nilpotent elements $\neq 0$ over a finite field satisfies an equation $a^{n(a)}=a$, $n(a)>1$. It is easy to see that the same conclusion holds for any ring which is a finite direct sum of such algebras.

Albert has subsequently pointed out to us the possible complexity of an algebra $\mathfrak{A}$ in the case where some of the components of $\mathfrak{A}^+$ are 3-dimensional Jordan algebras. Each such component is a subset $\mathfrak{B}_i$ of the associative algebra $\mathfrak{A}_i$ of all two rowed square matrices. Thus $\mathfrak{A}$ is the vector space direct sum $\mathfrak{A}=\mathfrak{B}_1+\cdots+\mathfrak{B}_t+\mathfrak{B}_0$, where $\mathfrak{B}_0$ is a subalgebra of $\mathfrak{A}$ which is the direct sum of fields. Define the product $x*y$ in $\mathfrak{A}$ in terms of the product xy in the associative algebra $\mathfrak{C}=\mathfrak{A}_1\oplus\cdots\oplus\mathfrak{A}_t\oplus\mathfrak{B}_0$ by $x*y=(1/2)(xy+yx)+(xy-yx)T$, where T is any linear mapping of $\mathfrak{C}$ into $\mathfrak{A}$.[6] The result is a power-associative algebra $\mathfrak{A}$ with the required $\mathfrak{A}^+$. Actually $\mathfrak{B}_0$ is an ideal of $\mathfrak{A}$ orthogonal to $\mathfrak{B}_1+\cdots+\mathfrak{B}_t=\mathfrak{D}$, but $\mathfrak{D}$ need not even be a subalgebra of $\mathfrak{A}$. It may even be that this is the most general power-associative algebra with the required property.

References

1. A. A. Albert, *Power-associative rings*, Trans. Amer. Math. Soc. vol. 64 (1948) pp. 552–593.

2. ———, *On nonassociative division algebras*, Trans. Amer. Math. Soc. vol. 72 (1952) pp. 296–309.

3. ———, *New simple power-associative algebras*, Summa Brasiliensis Mathematicae vol. 2 (1951) pp. 183–194.

4. F. D. Jacobson and N. Jacobson, *Classification and representation of semisimple Jordan algebras*, Trans. Amer. Math. Soc. vol. 65 (1949) pp. 141–169.

5. N. Jacobson, *Structure theory for algebraic algebras of bounded degree*, Ann. of Math. vol. 46 (1945) pp. 695–707.

6. R. D. Schafer, *The exceptional simple Jordan algebras*, Amer. J. Math. vol. 70 (1948) pp. 82–94.

University of Pennsylvania

[6] This is the construction used in [3].