FINITE POWER-ASSOCIATIVE DIVISION RINGS

KEVIN McCRIMMON[1]

The classical Wedderburn theorem [**5**, p. 37] states that any finite associative division ring is a (commutative) field. A. A. Albert generalized this to finite strictly power-associative division rings of characteristic $\neq 2$. His proof used the classification of central simple Jordan algebras and proceeded by case-checking (types A, B, C, D in [**1**, p. 301] and type E in [**2**, p. 11]). The purpose of this paper is to give a uniform proof of his results.

Throughout the paper all algebras will be *nonassociative algebras over a field* Φ *of characteristic* $\neq 2$; since simple rings (in particular, division rings) are simple algebras over their centroids there is no loss in generality in restricting ourselves to algebras. An algebra is a division algebra if left and right multiplications by a nonzero element are bijections; for finite-dimensional algebras this is equivalent to the nonexistence of proper zero divisors. Following N. Jacobson, we define a *Jordan division algebra* to be a commutative Jordan algebra with identity element such that every nonzero element x is *regular* with *Jordan inverse* y: $xy=1$, $x^2y=x$. For special algebras the inverse is just the usual inverse in the associative sense. An algebraic Jordan algebra is a Jordan division algebra if and only if each nonzero x generates a subfield $\Phi[x]$, the inverse being a polynomial in x [**7**, p. 1157]. (Note that this condition is weaker than being a division algebra—if $\mathfrak{Q}$ is an associative quaternion division algebra then $\mathfrak{Q}^+$ is a Jordan division algebra with zero divisors).

The following lemma is due to Albert [**1**, p. 299].

LEMMA 1. *A finite-dimensional strictly power-associative algebra which is a division algebra contains an identity element.*

PROOF. Any nonzero element is nonnilpotent, so the finite-dimensional associative subalgebra it generates contains an idempotent. If e is an idempotent in our algebra $\mathfrak{D}$ we have a Peirce decomposition [**3**, p. 560]

$$(1)\qquad \begin{aligned} \mathfrak{D} &= \mathfrak{D}_1 + \mathfrak{D}_{1/2} + \mathfrak{D}_0, \\ \mathfrak{D}_{1/2} &= \{x \mid ex + xe = x\}, \\ \mathfrak{D}_i &= \{x \mid ex = xe = ix\} \qquad (i = 0, 1). \end{aligned}$$

Received by the editors February 28, 1966.

[1] This research was supported by an AFOSR Postdoctoral Fellowship.

If $\mathfrak{D}$ is a division algebra clearly $\mathfrak{D}_0=0$. If $[x, y, z]$ denotes the associator $(xy)z-x(yz)$, the associativity of third and fourth powers is given by

$$[x, x, x] = 0, \qquad [x^2, x, x] = 0.$$

By strict power-associativity we may linearize the latter to obtain

$$[x^2, x, y] + [x^2, y, x] + [xy + yx, x, x] = 0.$$

Setting $y=e$, $x\epsilon\mathfrak{D}_{1/2}$ we obtain

$$\begin{aligned} 0 &= [x^2, x, e] + [x^2, e, x] \\ &= (x^2x)e + (x^2e)x - x^2(xe + ex) \\ &= (x^2x)e \end{aligned}$$

since $x^2\epsilon\mathfrak{D}_1+\mathfrak{D}_0=\mathfrak{D}_1$ by the Peirce relations [**3**, p. 559]. This is impossible in a division algebra unless $x=0$, so $\mathfrak{D}_{1/2}=0$ and e is the identity for $\mathfrak{D}=\mathfrak{D}_1$.

The next lemma is also Albert's [**1**, p. 300].

LEMMA 2. *A commutative strictly power-associative algebra with identity such that each nonzero element x generates a finite separable extension $\Phi[x]$ of Φ is necessarily a Jordan division algebra.*

PROOF. By assumption it is algebraic and each nonzero element x contains a (Jordan) inverse in $\Phi[x]$, so it remains only to verify the Jordan identity

$$[x^2, y, x] = 0. \tag{2}$$

Since $\Phi[x]$ is separable there is an extension Ω of Φ in which x splits into a linear combination $x=\sum\omega_ie_i$ of orthogonal idempotents, so (2) becomes $\sum\omega_i^2\omega_j[e_i, y, e_j]=0$. Now the terms $[e_i, y, e_i]$ vanish by commutativity, and since the algebra obtained by extending the base field is still strictly power-associative it suffices to prove

$$[e, y, e'] = 0 \tag{3}$$

for orthogonal idempotents e, e' in any commutative strictly power-associative algebra $\mathfrak{D}$.

Corresponding to the decomposition (1) relative to e we have a decomposition

$$\mathfrak{D} = \mathfrak{D}_1' + \mathfrak{D}_{1/2}' + \mathfrak{D}_0' \tag{1)$'$ (}$$

relative to e'. The Peirce relations [**3**, p. 559], [**4**, p. 505] and [**8**, pp. 366–367] imply

$$(4)\qquad \begin{gathered} \mathfrak{D}_i^2 \subset \mathfrak{D}_i,\ \mathfrak{D}_i\mathfrak{D}_j = 0,\ \mathfrak{D}_i\mathfrak{D}_{1/2} \subset \mathfrak{D}_{1/2} + \mathfrak{D}_j \quad (j = 1 - i, i = 0, 1) \\ z\epsilon\mathfrak{D}_i \Rightarrow U_z\mathfrak{D}_{1/2} \subset \mathfrak{D}_j \qquad (U_z = 2L_z^2 - L_{z^2}) \end{gathered}$$

(and dually for $\mathfrak{D}_1'$, $\mathfrak{D}_{1/2}'$, $\mathfrak{D}_0'$). We have

$$(5)\qquad \mathfrak{D}_{1/2} + \mathfrak{D}_1 \subset \mathfrak{D}_{1/2}' + \mathfrak{D}_0'$$

(and dually) because the $\mathfrak{D}_1'$ component x_1' of $x = x_{1/2} + x_1(x_i\epsilon\mathfrak{D}_i)$ is $U_{e'}x = U_{e'}x_{1/2}\epsilon\mathfrak{D}_1$ by (4) since $e'\epsilon\mathfrak{D}_0$, so $x_1'\epsilon\mathfrak{D}_1' \cap \mathfrak{D}_1$, hence $x_1' = e'x_1'\epsilon\mathfrak{D}_0\mathfrak{D}_1 = 0$.

Since $e\epsilon\mathfrak{D}_1$, $e'\epsilon\mathfrak{D}_0$, the orthogonality relations (4) imply (3) if $y\epsilon\mathfrak{D}_1 + \mathfrak{D}_0$. For $y\epsilon\mathfrak{D}_{1/2}$ by (5) we have $y\epsilon\mathfrak{D}_{1/2}' + \mathfrak{D}_0'$, $ye'\epsilon\mathfrak{D}_{1/2}' \subset \mathfrak{D}_{1/2} + \mathfrak{D}_0$; but $ye'\epsilon\mathfrak{D}_{1/2}\mathfrak{D}_0 \subset \mathfrak{D}_{1/2} + \mathfrak{D}_1$ by (4), so $ye'\epsilon\mathfrak{D}_{1/2}$. From this we see $[e, y, e'] = (\frac{1}{2}y)e' - \frac{1}{2}(ye') = 0$, and (3) is proved in all cases.

The following lemma is well known.

LEMMA 3. *A commutative alternative ring without nonzero nilpotent elements is associative.*

PROOF. We will show $[x, y, z]^3 = 0$ for all x, y, z. We have $3[x, y, z] = [x, y, z] - [x, z, y] + [z, x, y] = [xy, z] + x[z, y] + [z, x]y = 0$ by alternativity and commutativity, so associators are annihilated by 3. By Artin's Theorem [**9**, p. 29] any subring generated by two element is a commutative associative ring, so $(u - v)^3 = u^3 - v^3 - 3(u - v)uv$ and $(uv)^3 = u^3v^3$. Setting $u = (xy)z$, $v = x(yz)$ in the first of these we have $u - v = [x, y, z]$, so $3(u - v) = 0$ by the above, and $[x, y, z]^3 = \{(xy)z\}^3 - \{x(yz)\}^3$. Using the second relation this becomes $(x^3y^3)z^3 - x^3(y^3z^3) = \{x(xy^3)x\}z^3 - x\{x(y^3z^3)x\} = x\{(xy^3)(xz^3)\} - x\{(xy^3)(z^3x)\} = 0$ by the Moufang identities [**9**, p. 28].

Finally, we come to a lemma of J. M. Osborn. A *$*$-simple* ring is a ring with an involution $*$ which has no proper $*$-invariant ideals.

LEMMA 4. *A $*$-simple associative ring with involution generated by its symmetric elements and such that the nonzero symmetric elements are invertible is either a division ring or a direct sum of two anti-isomorphic division rings.*

PROOF. Let $\mathfrak{Z}_r$ be the set of elements without right inverses, $\mathfrak{Z}_l$ those without left inverses, $\mathfrak{Z} = \mathfrak{Z}_r \cup \mathfrak{Z}_l$ the singular elements, and $\mathfrak{H} = \mathfrak{H}(\mathfrak{A}, *)$ the symmetric elements of our ring $\mathfrak{A}$ under the involution $*$. We claim

$$(6)\qquad \mathfrak{Z}_r = \mathfrak{Z}_l = \mathfrak{Z}.$$

It suffices to show $\mathfrak{Z}_r \subset \mathfrak{Z}_l$. If $z \in \mathfrak{Z}_r$ then $zz^* \in \mathfrak{Z}_r \cap \mathfrak{H}$, so by assumption $zz^*=0$. Since z is a left zero divisor it can't have a left inverse, and $z\in\mathfrak{Z}_l$.

If $\mathfrak{Z}=0$, $\mathfrak{A}$ is a division ring.

Suppose $\mathfrak{Z}\neq 0$. Now $\mathfrak{Z}^*=\mathfrak{Z}$, and from (6) we have

$$\mathfrak{A}\mathfrak{Z}\subset\mathfrak{Z},\qquad \mathfrak{Z}\mathfrak{A}\subset\mathfrak{Z}. \tag{7}$$

By $*$-simplicity $\mathfrak{Z}$ cannot be an ideal, so there must be z, $w\in\mathfrak{Z}$ with $z+w\notin\mathfrak{Z}$. If $z+w=x$ is invertible we have $e+f=1$ for $e=zx^{-1}$, $f=wx^{-1}\in\mathfrak{Z}$. By (7) e and e^* are orthogonal (e.g., $ee^*\in\mathfrak{Z}\cap\mathfrak{H}=0$), so $e^*=e^*1=e^*f$; similarly $f^*=f^*e$, and applying the involution gives $f=e^*f=e^*$, so $1=e+e^*$ is a sum of two orthogonal idempotents in $\mathfrak{Z}$. By (7) $e\mathfrak{H}e^*$ and $e^*\mathfrak{H}e$ are contained in $\mathfrak{Z}\cap\mathfrak{H}$, so $e\mathfrak{H}e^*=e^*\mathfrak{H}e=0$. Thus $\mathfrak{H}=1\mathfrak{H}1\subset e\mathfrak{A}e+e^*\mathfrak{A}e^*$. By assumption $\mathfrak{H}$ generates $\mathfrak{A}$, so $\mathfrak{A}=\mathfrak{B}\oplus\mathfrak{B}^*$ for $\mathfrak{B}=e\mathfrak{A}e$. Clearly the nonzero elements of $\mathfrak{B}$ must be invertible, so $\mathfrak{A}$ is a direct sum of two anti-isomorphic division rings.

Now we put the results together.

THEOREM 1. *A Jordan division ring of characteristic $\neq 2$ generated by two elements is either of the form Δ^+ for Δ an associative division ring or $\mathfrak{H}(\Delta, *)$ for Δ an associative division ring with involution.*

The methods of Shirshov and Cohn (see [**6**, p. 207]) show that such a ring, being generated by two elements, is isomorphic to $\mathfrak{H}(\mathfrak{A}, *)$ for $\mathfrak{A}$ an associative ring with involution. We may assume $\mathfrak{A}$ is generated by its symmetric elements, and since a maximal $*$-invariant ideal $\mathfrak{M}$ induces an isomorphism of the (simple) Jordan division ring onto $\mathfrak{H}(\bar{\mathfrak{A}}, *)$ where $\bar{\mathfrak{A}}=\mathfrak{A}/\mathfrak{M}$ is $*$-simple we may as well assume from the start that $\mathfrak{A}$ is $*$-simple. Thus we can apply Lemma 4 to conclude $\mathfrak{A}=\Delta$ or $\mathfrak{A}=\Delta\oplus\Delta^*$, and in the latter case $\mathfrak{H}(\mathfrak{A}, *)$ is isomorphic to Δ^+.

For the next theorem we remark that the actual construction of Δ (see [**6**]) shows that Δ is finite-dimensional (or finite) if the Jordan ring is finite-dimensional (or finite).

THEOREM 2. *A finite Jordan division ring of characteristic $\neq 2$ is a finite (commutative, associative) field.*

By Lemma 3 it suffices to prove the ring is alternative, i.e., that every subring generated by two elements is associative, and this follows from Theorem 1 since the finite division ring of Theorem 1 is a (commutative, associative) field by Wedderburn's theorem and the Jordan ring is a subfield.

THEOREM 3. *A finite strictly power-associative ring which is a division ring of characteristic $\neq 2$ is a finite (commutative, associative) field.*

By Lemma 1 such an algebra $\mathfrak{D}$ contains an identity element. Each nonzero element x generates a finite extension $\Phi[x]$ of the centroid Φ which is separable since Φ is finite. Since passage to the symmetrized algebra does not affect multiplication in $\Phi[x]$, Lemma 2 shows $\mathfrak{D}^+$ is a finite Jordan division algebra. By Theorem 2 $\mathfrak{D}^+$ is a finite Jordan division algebra. By Theorem 2 $\mathfrak{D}^+$ is a finite field, hence a finite separable extension of Φ. By the theorem of the primitive element $\mathfrak{D}^+=\Phi[x]$. But then $\mathfrak{D}=\Phi[x]$ is again a field.

References

1. A. A. Albert, *On nonassociative division algebras*, Trans. Amer. Math. Soc. **72** (1952), 296–309.

2. ———, *A construction of exceptional Jordan division algebras*, Ann. of Math. (2) **67** (1958), 1–28.

3. ———, *Power associative rings*, Trans. Amer. Math. Soc. **64** (1948), 552–593.

4. ———, *A theory of power associative commutative algebras*, Trans. Amer. Math. Soc. **69** (1950), 503–527.

5. E. Artin, *Geometric algebra*, Interscience, New York, 1957.

6. N. Jacobson, *Associative algebras with involution and Jordan algebras*, Nederl. Akad. Wentensch. Proc. Ser. A **69** (1966), 202–212 (Indag. Math. **28**).

7. ———, *A coordinatization theorem for Jordan algebras*, Proc. Nat. Acad. Sci. U.S.A. **7** (1962), 1154–1160.

8. L. Kokoris, *New results on power-associative algebras*, Trans. Amer. Math. Soc. **77** (1954), 363–373.

9. R. D. Schafer. *An introduction to nonassociative algebras*, Academic Press, New York, 1966.

Massachusetts Institute of Technology