A NOTE ON FINITE DIVISION RINGS

KEVIN MCCRIMMON

A celebrated theorem of Wedderburn says that a finite associative division ring is a finite (commutative) field. An elegant proof of this, due to E. Artin [3, p. 72], reduces the problem to showing the reduced (or generic) norm has a nontrivial zero, and then applies the theorem (conjectured by Artin and proved by Chevalley) that a polynomial with coefficients in a finite field and zero constant term has a nontrivial zero in that field if its degree is less than the number of variables.

The Wedderburn theorem was generalized by A. A. Albert to finite strictly power-associative division rings of characteristic $\neq 2$ in [1, p. 301] and [2, p. 11] (see also [5]). The proof reduced the power-associative case to the associative case by using the properties of Jordan division algebras. It is the purpose of this note to show that Artin's method carries over directly to the power-associative case using the generic norm introduced by N. Jacobson [4]. By avoiding Jordan algebras one is able to extend Albert's result to the characteristic 2 case.

The usual definition of a division ring requires that left and right multiplications by a nonzero element be bijective. If the ring is finite it is necessarily an algebra, over a finite field Φ, which is algebraic (even finite-dimensional) and without zero divisors. Also, as we shall see later, the algebra necessarily has a unit element.

We wish to consider something slightly more general. For our purposes we say an algebraic power-associative algebra is a *division algebra* if it is unital and no element $x \neq 0$ is a zero divisor in the subalgebra $\Phi[x]$ it generates (since $\Phi[x]$ is finite-dimensional, this is equivalent to saying x is invertible in $\Phi[x]$). Our conditions are less restrictive, since the Jordan algebra of a quadratic form can be a division algebra in our sense with zero divisors. With this definition we have

THEOREM. *A finite strictly power-associative division ring is a finite (commutative, associative) field.*

PROOF. The proof is exactly the same as in the associative case. For completeness, we go through the details. Let $\{x_1, \cdots, x_n\}$ be a basis for the division algebra $\mathfrak{A}$ over the finite field Φ. If $\Omega = \Phi(\eta_1, \cdots, \eta_n)$ is the field obtained by adjoining n indeterminates $\eta_1, \cdots, \eta_n$ then $\mathfrak{A}_\Omega = \Omega \otimes_\Phi \mathfrak{A}$ is still power-associative by our assump-

Received by the editors March 7, 1969.

tion that $\mathfrak{A}$ is *strictly* power-associative, and it still has dimension n over Ω.

Let $M(\lambda)=\lambda^m+M_{m-1}(\eta_1, \cdots, \eta_n)\lambda^{m-1}+\cdots+M_0(\eta_1, \cdots, \eta_n)$ be the minimum polynomial of the (generic) element $y=\eta_1 x_1+\cdots+\eta_n x_n$ in $\mathfrak{A}_\Omega$ over Ω. We are mainly interested in the *generic norm* $N(\eta_1, \cdots, \eta_n)=(-1)^m M_0(\eta_1, \cdots, \eta_n)$. This is a homogeneous polynomial in $\Phi[\eta_1, \cdots, \eta_n]$ of degree m with the property that $N(\alpha_1, \cdots, \alpha_n)=0$ for $\alpha_i \in \Phi$ if and only if $x=\alpha_1 x_1+\cdots+\alpha_n x_n$ is a zero divisor in $\Phi[x]$ (see [4, pp. 27–28] or [6, pp. 535–538]). Thus the condition that $\mathfrak{A}$ be a division algebra is that N have no nontrivial zeros,

$$N(\alpha_1, \cdots, \alpha_n) = 0 \Rightarrow (\alpha_1, \cdots, \alpha_n) = (0, \cdots, 0).$$

By the theorem of Artin-Chevalley referred to above, the homogeneous polynomial $N(\eta_1, \cdots, \eta_n)$ over the finite field Φ will have a nontrivial zero if its degree m is less than the number of variables n. Thus our N must have $m \geqq n$.

On the other hand, by definition of the minimum polynomial of $y=\eta_1 x_1+\cdots+\eta_n x_n$ the elements $1, y, \cdots, y^{m-1}$ are independent, so $\mathfrak{A}_\Omega$ has dimension at least m over Ω, and $n \geqq m$.

Thus $n=m$, so $\{1, y, \cdots, y^{m-1}\}$ forms a basis for $\mathfrak{A}_\Omega$, and $\mathfrak{A}_\Omega=\Omega[y]$ is commutative and associative. But then $\mathfrak{A}$ was commutative and associative to begin with, hence a finite field.

The result can be slightly generalized.

THEOREM. *A generically algebraic division algebra over a finite field is a finite (commutative, associative) field.*

Here "generically algebraic" essentially means "has a generic minimum polynomial" [6, p. 533]. Recall that a generically algebraic algebra need not be finite-dimensional—examples are an infinite purely inseparable field extension of finite exponent, or the Jordan algebra of a quadratic form on an infinite-dimensional vector space. However, a generically algebraic division algebra over a finite field *is* necessarily finite-dimensional; indeed, by the Artin-Chevalley theorem its dimension is at most the degree of the generic norm. Thus the generically algebraic case immediately reduces to the finite case.

The generic norm depends heavily on the existence of a unit element. We now indicate why an algebraic strictly power-associative algebra without zero divisors necessarily has a unit. Since we want to include characteristic 2, neither the passage to $\mathfrak{A}^+$ nor the properties of Peirce decompositions are available to us, so we will have to modify

Albert's proof [1, p. 299], [5, p. 1173]. Each nonzero element x generates a subalgebra $\Phi[x]$ which is a finite-dimensional commutative associative algebra without zero divisors, hence a field. In particular, it has a unit, so there is an idempotent $e_x \neq 0$ with $e_x x = x e_x = x$. If we can show that all these idempotents e_x coincide, their common value e will be a unit for all of $\mathfrak{A}$: $ex = xe = x$. Thus we need only establish

LEMMA. *If e and f are two idempotents which are not zero divisors in the strictly power-associative algebra $\mathfrak{A}$, and if $\mathfrak{A}$ has no nilpotent elements, then $e = f$.*

PROOF. By strict power-associativity we can linearize

(i) $[x, x, x] = 0$,

(ii) $[x^2, x, x] = 0$,

to obtain

(iii) $[x, x, y] + [x, y, x] + [y, x, x] = 0$,

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

We first claim $ef + fe = z + f = w + e$ where $ez = ze = z$, $fw = wf = w$. To see this, define $z = ef + fe - f$, $w = ef + fe - e$. Setting $x = e$, $y = f$ in (iv) gives $0 = [e, e, f] + [e, f, e] + [ef + fe, e, e] = [ef + fe - f, e, e]$ (by (iii)) $= [z, e, e]$. Thus $(ze)e = ze$; since e is not a zero divisor, $ze = z$. Similarly we have $ez = z$, and analogously for w.

Thus $(e-f)^2 = e - (ef + fe) + f = e - z = f - w$, so $(e-f)^2 e = (e-z)e = e - z = (e-f)^2$ and $(e-f)^2 f = (f-w)f = f - w = (e-f)^2$. This shows $(e-f)^3 = (e-f)^2 e - (e-f)^2 f = 0$; our assumption that $\mathfrak{A}$ contains no nilpotent elements then implies $e = f$.

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. E. Artin, *The influence of J. H. M. Wedderburn on the development of modern algebra*, Bull. Amer. Math. Soc. **56** (1950), 65–72.

4. N. Jacobson, *The generic norm of an algebra*, Osaka J. Math. **15** (1963), 25–50.

5. K. McCrimmon, *Finite power-associative division rings*, Proc. Amer. Math. Soc. **17** (1966), 1173–1177.

6. ———, *Generically algebraic algebras*, Trans. Amer. Math. Soc. **127** (1967), 527–551.

UNIVERSITY OF VIRGINIA