FINITE NONCOMMUTATIVE DIVISION ALGEBRAS[1]

A. A. ALBERT

1. **Introduction.** The purpose of this note is to provide the first known class of nonassociative finite division algebras with unity elements and characteristic *two*. Indeed, let $\mathfrak{F}$ be the field of $q=p^m$ elements, $\mathfrak{K}$ be the field of degree n over $\mathfrak{F}$, where p is the characteristic of $\mathfrak{F}$. Assume that

$$q > 2, \qquad n > 2. \tag{1}$$

Select c to be any element of $\mathfrak{K}$ such that

$$c \neq -1, \qquad c \neq a^{q-1}, \tag{2}$$

for any a of $\mathfrak{K}$. For each such $\mathfrak{K}$ and c we shall define a division algebra $\mathfrak{D}=\mathfrak{D}(\mathfrak{K}, c)$, such that $\mathfrak{D}$ has a unity element. We shall prove that each such algebra $\mathfrak{D}$ is actually *noncommutative* and so must be nonassociative. Our result yields non-Desarguesian finite projective planes[2] of order q^n for all $q>2$ and $n>2$, and these are new orders when $q=2^m$ and mn is odd.

2. **The construction.** Let $\mathfrak{F}$ and $\mathfrak{K}$ be as above so we may write

$$\tau = q^n - 1 = \sigma(q-1), \qquad \sigma = 1 + q + q^2 + \cdots + q^{n-1}. \tag{3}$$

Then τ is the order of the multiplicative group $\mathfrak{K}^*$ of all nonzero elements of $\mathfrak{K}$, $\mathfrak{K}^*$ is a cyclic group whose generators w are called the *primitive* elements of $\mathfrak{K}$, and every nonzero element a of $\mathfrak{K}$ is a power w^λ of a primitive element w of $\mathfrak{K}$. If $c=a^{q-1}$ then $c=w^{(q-1)\lambda}$. The period (multiplicative order) of w^{q-1} is σ, and so $c=a^{q-1}$ if and only if the period of c divides σ. When $q>2$ we know that $\tau>\sigma$ and so, in particular, w itself is a possible c. We shall show now that (2) can sometimes be satisfied even for c in $\mathfrak{F}$.

THEOREM 1. *Let c be a primitive element of $\mathfrak{F}$. Then $c\neq a^{q-1}$ for any a in $\mathfrak{K}$ if and only if $q-1$ does not divide n.*

For it is clear that $q\equiv 1 \pmod{q-1}$ and so (3) implies that

Presented to the Society April 24, 1958 under the title *Finite division algebras and finite planes*; received by the editors March 13, 1958.

[1] This paper was sponsored, in part, by NSF Grant G-4792.

[2] For a list of the values of the orders of non-Desarguesian planes see the paper by Marshall Hall entitled *Finite projective planes*, Amer. Math. Monthly vol. 62 (1955) pp. 18–23.

$\sigma \equiv n \pmod{q-1}$ and $q-1$ divides σ if and only if $q-1$ divides n. But c has period $q-1$ and so the argument above shows that $c=a^{q-1}$ if and only if $q-1$ divides σ and hence n.

Let us now observe a property of the algebra $\mathfrak{M}_n$ of *all* linear transformations on $\mathfrak{K}$. The algebra $\mathfrak{K}$ is commutative and associative and so is a vector space of dimension n over $\mathfrak{F}$ with a product

$$xy = yx = xR(y). \tag{4}$$

The mapping

$$x \rightarrow R(x) \tag{5}$$

is an isomorphism of $\mathfrak{K}$ onto the set of all linear transformations $R(x)$. The field $\mathfrak{K}$ is cyclic over $\mathfrak{F}$ and the mapping S defined by

$$x \rightarrow xS = x^q \tag{6}$$

generates the cyclic Galois group of $\mathfrak{K}$ over $\mathfrak{F}$. The norm, over $\mathfrak{F}$, of any element x in $\mathfrak{K}$ is given by the formula

$$\nu(x) = x(xS)(xS^2) \cdots (xS^{n-1}) = x^\sigma, \tag{7}$$

so that x^σ is in $\mathfrak{F}$ for every x of $\mathfrak{K}$. If $x=\xi$ is in $\mathfrak{F}$ we have

$$\nu(\xi) = \xi^n = \xi^\sigma, \tag{8}$$

which follows from the fact already noted that $n \equiv \sigma \pmod{q-1}$. The powers of S are automorphisms, and so $(xy)S^i=(xS^i)(yS^i)$, that is,

$$[R(y)]S^i = S^iR(yS^i) \qquad (i = 0, 1, \cdots, n-1). \tag{9}$$

The set of all linear transformations

$$T = R(x_0) + SR(x_1) + \cdots + S^{n-1}R(x_{n-1}) \qquad (x_i \text{ in } \mathfrak{K}), \tag{10}$$

is then an associative algebra, and it is well known and easy to show that this algebra has dimension n^2 over $\mathfrak{F}$ and so is $\mathfrak{M}_n$. But then *every linear transformation T on $\mathfrak{K}$ is uniquely expressible in the form* (10).

We shall define an algebra $\mathfrak{K}_0$ over $\mathfrak{F}$ which is a mathematical system consisting of the vector space $\mathfrak{K}$ and a new product operation (x, y). It will be important to differentiate the elements of $\mathfrak{K}$, called *vectors*, from the elements of the base field $\mathfrak{F}$ called *scalars*, and so we shall designate the unity element of $\mathfrak{K}$ by e and that of $\mathfrak{F}$ by 1. We shall define another algebra $\mathfrak{D}$ on the same vector space $\mathfrak{K}$ later, and $\mathfrak{D}$ will have a unity element $f \neq e$. Note that

$$\nu(c) = c^\sigma = \alpha e, \tag{11}$$

where α is in $\mathfrak{F}$. Then we have

$$(12) \qquad \alpha \neq 1,$$

since (2) is in fact equivalent to (12).

Define $\mathfrak{K}_0$ by the product formula[3]

$$(13) \qquad (x, y) = xR_y^{(0)} = yL_x^{(0)} = x(yS) - (cy)(xS),$$

for any c satisfying (2).

THEOREM 2. *The algebra $\mathfrak{K}_0$ is a division algebra.*

For $(x, y)=0$, for nonzero elements x and y in $\mathfrak{K}$, if and only if $(xy)(y^{q-1}-cx^{q-1})=0$, that is, $c=a^{q-1}$ with $a=yx^{-1}$. This contradicts our hypothesis (2).

Observe now that (13) is equivalent to

$$(14) \qquad R_y^{(0)} = R(yS) - SR(cy), \qquad L_x^{(0)} = SR(x) - R[c(xS)].$$

Theorem 2 implies that both $R_y^{(0)}$ and $L_x^{(0)}$ are nonsingular for every nonzero x and y of $\mathfrak{K}$. In particular, $R_e^{(0)}$ and $L_e^{(0)}$ are nonsingular and we note that $e=eS$,

$$(15) \qquad (e, e) = eR_e^{(0)} = eL_e^{(0)} = f = e - c.$$

Define linear transformations P and Q by

$$(16) \qquad P^{-1} = R_e^{(0)} = I - SR(c), \qquad Q^{-1} = L_e^{(0)} = S - R(c),$$

and see that

$$(17) \qquad fP = fQ = fPS = fQS = e.$$

We shall now define an algebra $\mathfrak{D}=\mathfrak{D}(\mathfrak{K}, c)$ consisting of the vector space $\mathfrak{K}$ and the product operation defined by

$$(18) \qquad x\cdot y = (xP, yQ) = (xP)(yQS) - c(xPS)(yQ).$$

We then have the following result.

THEOREM 3. *The algebra $\mathfrak{D}(\mathfrak{K}, c)$ is a division algebra, and $f=e-c$ is its unity element.*

For $x\cdot y=0$ for x and y in $\mathfrak{K}$ means that $(xP, yQ)=0$ and we have seen that this implies that $xP=0$ or $yQ=0$, $x(PP^{-1})=x=0$ or $y(QQ^{-1})=y=0$. By (17), we see that $f\cdot y=yQS-cyQ=yQ[S-R(c)]$ $=yQQ^{-1}=y$, and $x\cdot f=xP-c(xPS)=xP[I-SR(c)]=xPP^{-1}=x$, so our proof is complete.

[3] This formula is essentially that given on page 304 of the author's *On nonassociative division algebras*, Trans. Amer. Math. Soc. vol. 72 (1952) pp. 296–309.

3. **Inversion of P^{-1} and Q^{-1}.** The definition of $\mathfrak{D}$ given by (18) cannot be regarded as being complete until we express P and Q in the form (10), a form which enables us to actually compute products. We shall first define an element c_i in $\mathfrak{K}$ by

$$[SR(c)]^i = S^iR(c_i) \qquad (i = 1, \cdots, n), \tag{19}$$

and it should be clear from (9) that

$$c_i = c(cS) \cdots (cS^{i-1}) \qquad (i = 1, \cdots, n). \tag{20}$$

Then

$$c_1 = c, \qquad c_{i+1} = (c_iS)c = c_i(cS^i) \qquad (i = 1, \cdots, n-1), \tag{21}$$

and we also have

$$(c_{n-1}S)c = c_n = \nu(c) = c^\sigma = \alpha e \neq e. \tag{22}$$

If T is any linear transformation on $\mathfrak{K}$ the identity $(I - T) \cdot(I+T+T^2+ \cdots +T^{n-1})=I-T^n$ holds and, if we take $T=SR(c)$, we have $T^n=\alpha I$, $I-T^n=(1-\alpha)I$. But then the relation

$$(1 - \alpha)P = I + SR(c_1) + S^2R(c_2) + \cdots + S^{n-1}R(c_{n-1}) \tag{23}$$

is a correct formula, and we also have

$$(1 - \alpha)PS = R(c_{n-1}S) + S + S^2R(c_1S) + \cdots + S^{n-1}R(c_{n-2}S). \tag{24}$$

We may also derive the formula

$$\begin{aligned}(1 - \alpha)Q = S^{n-1} &+ S^{n-2}R(c_1S^{n-1}) + S^{n-3}R(c_2S^{n-2}) \\ &+ \cdots + R(c_{n-1}S),\end{aligned} \tag{25}$$

and the accompanying formula

$$(1 - \alpha)QS = S^{n-1}R(c_1) + \cdots + SR(c_{n-1}S^2) + I. \tag{26}$$

For suppose that Q is defined by (25). We form

$$\begin{aligned}&[S - R(c)](1 - \alpha)Q \\ &\quad = I + S^{n-1}R(c_1S^{n-1}) + \cdots + SR(c_{n-1}S) \\ &\qquad - [S^{n-1}R(c_1S^{n-1}) + S^{n-2}R(c_1S^{n-1}cS^{n-2}) + \cdots + R(cc_{n-1}S)] \\ &\quad = I - \alpha I = (1 - \alpha)I,\end{aligned}$$

and $Q^{-1}=S-R(c)$ as desired. This completes our construction of $\mathfrak{D}$.

4. **The noncommutativity of $\mathfrak{D}$.** We *assume* that $\mathfrak{D}$ is a *commutative* algebra, that is, that

$$(xP)(yQS) - c(xPS)(yQ) = (yP)(xQS) - c(yPS)(xQ) \tag{27}$$

for every x and y in $\mathfrak{K}$. This is equivalent to the relation

$$(28)\qquad (QS)R(xP) - QR[c(xPS)] = PR(xQS) - (PS)R[c(xQ)].$$

We use (23), (24), (25), (26) and compute the constant term in (28) to obtain

$$(29)\qquad xP - (xPS)[(c_{n-1}S)c] = (xQS) - (xQ)[(c_{n-1}S)c].$$

Since $(c_{n-1}S)c = c_n = \nu(c) = \alpha$ this relation is equivalent to

$$(30)\qquad P(I - \alpha S) = Q(S - \alpha I).$$

However, our definition (16) implies that

$$P(I - \alpha S) = P[I - SR(c) + SR(c - \alpha e)] = I + PSR(c - \alpha e)$$

and $Q(S - \alpha I) = Q[S - R(c) + R(c - \alpha e)] = I + QR(c - \alpha e)$. Hence (30) is equivalent to

$$(31)\qquad PS[R(c - \alpha e)] = Q[R(c - \alpha e)].$$

If $c \neq \alpha e$ the transformation $R(c - \alpha e)$ is nonsingular, (31) is equivalent to $PS = Q$, $S^{-1}P^{-1} = Q^{-1}$, $P^{-1} = SQ^{-1}$, $I - SR(c) = S^2 - SR(c)$, $I = S^2$, *which is true only when* $n = 2$. Thus our hypothesis that $n > 2$ implies that $\mathfrak{D}$ is not commutative except when $c = \alpha e$ is in $e\mathfrak{F}$. In this case $c = c^\sigma = c^n$, and

$$(32)\qquad c_{n-1} = c^{n-1} = e, \qquad c_i = c^i.$$

We then compute the coefficient of S^{n-1} in (28) and obtain

$$(33)\qquad c(xP) - c(xPS) = xQS - xQ,$$

for all x, from which, since $c = \alpha$,

$$(34)\qquad \alpha P(I - S) = Q(S - I).$$

Subtract (34) from (30) to obtain $(1 - \alpha)P = Q(1 - \alpha)$ and $P = Q$, $P^{-1} = Q^{-1}$. This contradicts our definition of P^{-1} and Q^{-1} in (16) unless $c = -e$, contrary to our hypothesis. Observe that if $c = -e$ then $P = Q$, and $\mathfrak{D} = \mathfrak{D}(\mathfrak{K}, -1)$ is actually commutative. We state our result as follows.

THEOREM 4. *Let $\mathfrak{K}$ be a field of degree $n > 2$ over the field $\mathfrak{F}_q$ of $q > 2$ elements, and c be any element of $\mathfrak{K}$ such that $c \neq -1$, $c \neq a^{q-1}$ for any a of $\mathfrak{K}$. Then $\mathfrak{D} = \mathfrak{D}(\mathfrak{K}, c)$ is an algebra with a unity element and is noncommutative. In particular, if w is a primitive element of $\mathfrak{K}$, the algebra $\mathfrak{D}(\mathfrak{K}, w)$ is noncommutative.*

THE UNIVERSITY OF CHICAGO