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 $F$ be the field of $q = p^m$ elements, $K$ be the field of degree $n$ over $F$, where $p$ is the characteristic of $F$. Assume that

(1) \[ q > 2, \quad n > 2. \]

Select $c$ to be any element of $K$ such that

(2) \[ c \neq -1, \quad c \neq a^{q-1}, \]

for any $a$ of $K$. For each such $K$ and $c$ we shall define a division algebra $D = D(K, c)$, such that $D$ has a unity element. We shall prove that each such algebra $D$ 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 $F$ and $K$ be as above so we may write

(3) \[ \tau = q^n - 1 = \sigma(q - 1), \quad \sigma = 1 + q + q^2 + \cdots + q^{n-1}. \]

Then $\tau$ is the order of the multiplicative group $K^*$ of all nonzero elements of $K$, $K^*$ is a cyclic group whose generators $w$ are called the primitive elements of $K$, and every nonzero element $a$ of $K$ is a power $w^a$ of a primitive element $w$ of $K$. If $c = a^{q-1}$ then $c = w^{(q-1)a}$. The period (multiplicative order) of $w^{q-1}$ is $\sigma$, and so $c = a^{q-1}$ if and only if the period of $c$ divides $\sigma$. 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 $F$.

Theorem 1. Let $c$ be a primitive element of $F$. Then $c \neq a^{q-1}$ for any $a$ in $F$ 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

\[ \tau = q^n - 1 = \sigma(q - 1), \quad \sigma = 1 + q + q^2 + \cdots + q^{n-1}. \]
Let us now observe a property of the algebra $M_n$ of all linear transformations on $F$. The algebra $F$ is commutative and associative and so is a vector space of dimension $n$ over $F$ with a product

$$xy = yx = xR(y).$$

The mapping

$$x \mapsto R(x)$$

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

$$x \mapsto xS = x^q$$

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

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

so that $x^\sigma$ is in $F$ for every $x$ of $F$. If $x = \xi$ is in $F$ we have

$$\nu(\xi) = \xi^n = \xi^\sigma,$$

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,

$$[R(y)]S^i = S^iR(yS^i) \quad (i = 0, 1, \cdots, n - 1).$$

The set of all linear transformations

$$T = R(x_0) + SR(x_1) + \cdots + S^{n-1}R(x_{n-1}) \quad (x_i \text{ in } F),$$

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

We shall define an algebra $F_0$ over $F$ which is a mathematical system consisting of the vector space $F$ and a new product operation $(x, y)$. It will be important to differentiate the elements of $F$, called vectors, from the elements of the base field $F$ called scalars, and so we shall designate the unity element of $F$ by $e$ and that of $F$ by $1$. We shall define another algebra $\mathcal{D}$ on the same vector space $F$ later, and $\mathcal{D}$ will have a unity element $f \neq e$. Note that

$$\nu(c) = c^\sigma = \alpha e,$$

where $\alpha$ is in $F$. Then we have

$$\sigma = n \pmod{q-1} \quad \text{and} \quad q - 1 \text{ divides } \sigma \text{ if and only if } q - 1 \text{ divides } n. \quad \text{But } c \text{ has period } q - 1 \text{ and so the argument above shows that } c = a^{q-1} \text{ if and only if } q - 1 \text{ divides } \sigma \text{ and hence } n.
(12) \[ \alpha \neq 1, \]

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

Define \( \mathfrak{K}_0 \) by the product formula\(^3\)

\[ (x, y) = xR_y^{(0)} = yL_x^{(0)} = x(yS) - (cy)(xS), \]

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 \( (xy)(yq^{-1} - cx^{q-1}) = 0 \), that is, \( c = ay^{q-1} \) with \( a = yx^{-1} \). This contradicts our hypothesis (2).

Observe now that (13) is equivalent to

\[ (13) \quad (x, y) = xR_y = yL_x = x(yS) - (cy)(xS), \]

for any \( c \) satisfying (2).

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 \( e = eS \)

\[ (e, e) = eR_e^{(0)} = eL_e^{(0)} = I = e - c. \]

Define linear transformations \( P \) and \( Q \) by

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

and see that

\[ (17) \quad fP = fQ = fPS = fQS = e. \]

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

\[ (18) \quad x \cdot y = (xP, yQ) = (xP)(yQS) - c(xPS)(yQ). \]

We then have the following result.

**Theorem 3.** The algebra \( \mathcal{D}(\mathfrak{K}, c) \) 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 \( yQ = 0 \) 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 $\mathcal{D}$ 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 $\mathcal{F}$ by

$$[SR(c)]^i = S_i R(c) \quad (i = 1, \cdots, n),$$

and it should be clear from (9) that

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

Then

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

and we also have

$$\langle c_{n-1}S \rangle c = c_n = \nu(c) = c^\sigma = \alpha e \neq e.$$
for every \(x\) and \(y\) in \(\mathfrak{A}\). This is equivalent to the relation
\[
(28) \quad (QS)R(xP) - QR[c(xPS)] = PR(xQS) - (PS)R[c(xQ)].
\]
We use (23), (24), (25), (26) and compute the constant term in (28) to obtain
\[
(29) \quad xP - (xPS)[(c_{n-1}S)c] = (xQS) - (xQ)[(c_{n-1}S)c].
\]
Since \((c_{n-1}S)c = c_{n} = \nu(c) = \alpha\) this relation is equivalent to
\[
(30) \quad P(I - \alpha S) = Q(S - \alpha I).
\]
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
\[
(31) \quad PS[R(c - \alpha e)] = Q[R(c - \alpha e)].
\]
If \(c \neq \alpha e\) the transformation \(R(c - \alpha e)\) is nonsingular, (31) is equivalent to \(PS = Q, S^{-1}P^{-1} = Q^{-1}, P^{-1} = SQ^{-1}, I - SR(c) = S^{2} - SR(c), I = S^{2},\) \(\text{which is true only when } n = 2\). Thus our hypothesis that \(n > 2\) implies that \(\mathfrak{D}\) is not commutative except when \(c = \alpha e\) is in \(e\mathfrak{A}\). In this case \(c = c^{2} = c^{n}\), and
\[
(32) \quad c_{n-1} = c^{n-1} = e, \quad c_{i} = c^{i}.
\]
We then compute the coefficient of \(S^{n-1}\) in (28) and obtain
\[
(33) \quad c(xP) - c(xPS) = xQS - xQ,
\]
for all \(x\), from which, since \(c = \alpha\),
\[
(34) \quad \alpha P(I - S) = Q(S - I).
\]
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 \(\mathfrak{D} = \mathfrak{D}(\mathfrak{A}, -1)\) is actually commutative. We state our result as follows.

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