ON NONASSOCIATIVE DIVISION ALGEBRAS[1]

BY

A. A. ALBERT

1. **Introduction.** A nonassociative ring $\mathfrak{D}$ may be called a *division ring* if the set $\mathfrak{D}^*$ of all nonzero elements of $\mathfrak{D}$ forms a loop with respect to the product operation of $\mathfrak{D}$. The identity element of this loop is the unity element e of $\mathfrak{D}$, and the center of $\mathfrak{D}$ is a field $\mathfrak{F}$ whose unity quantity is e. The ring $\mathfrak{D}$ is an algebra over $\mathfrak{F}$, and we may indicate the fact that $\mathfrak{F}$ is the center of $\mathfrak{D}$ by saying that $\mathfrak{D}$ is a *central* algebra over $\mathfrak{F}$. When $\mathfrak{D}$ is a finite ring, the field $\mathfrak{F}$ is a finite field $GF(p^m)$, and $\mathfrak{D}$ is a finite-dimensional central division algebra over $\mathfrak{F}$.

The first of our results is concerned with the question of the existence of commutative central division algebras of degree two. We shall show that such algebras can exist only when $\mathfrak{F}$ has characteristic two, and then the elements of $\mathfrak{D}$ which are not in $\mathfrak{F}$ generate inseparable quadratic extensions of $\mathfrak{F}$. We shall also give a construction of such algebras.

One of our main results is a generalization of the Wedderburn-Artin Theorem on finite division algebras. We shall show that *every finite power-associative division algebra of characteristic $p>5$ is a finite field.* The result depends upon the Wedderburn Theorem and the results of the author on commutative power-associative algebras. It can be extended to algebras of characteristic 3 and 5 if we assume[2] that the center has more than five elements, and it includes the Artin generalization for algebras of characteristic $p\neq 2$.

The remainder of the paper is devoted to showing that the Wedderburn Theorem for finite division algebras depends upon some assumption such as power-associativity. In the associative case the dimension n of a central division algebra is a square and there exist no finite central division algebras. It is also evident that there exist no nontrivial commutative associative central division algebras. We shall show here that *there exists a finite commutative central division algebra of every dimension n* (necessarily with $n>2$) *over any finite field $\mathfrak{F}$ of characteristic not two.* Indeed we shall give a construction, in the case where n is odd, which is valid over every field $\mathfrak{F}$ of characteristic not two such there exists a cyclic field of degree n over $\mathfrak{F}$. We shall also construct a set of noncommutative finite division algebras of odd dimension and characteristic two. The algebras all have dimension $n>2$ over the center

Presented to the Society, September 7, 1951; received by the editors July 20, 1951.

(1) This paper was sponsored, in part, by the Office of Naval Research.

(2) See §3 for the explicit added assumption which we require and which then includes the case of alternative algebras over any field of characteristic not two.

and so show that the Wedderburn Theorem does not hold without an assumption like power-associativity.

2. **Algebras of degree 2.** A division algebra $\mathfrak{D}$ will be said to have *degree two* if $1, x, x^2$ are linearly dependent in $\mathfrak{F}$ for every x of $\mathfrak{D}$.

THEOREM 1. *Let $\mathfrak{D}$ be a commutative division algebra of degree two over its center $\mathfrak{F}$. Then $\mathfrak{F}$ has characteristic two and $\mathfrak{F}[x]$ is an inseparable quadratic field over $\mathfrak{F}$ for every x of $\mathfrak{D}$ which is not in $\mathfrak{F}$.*

For let the characteristic of $\mathfrak{F}$ be different from two. If x is in $\mathfrak{D}$ and not in $\mathfrak{F}$, there exists an element $u=\xi+x$ such that $u^2=\alpha$ in $\mathfrak{F}$. Since $\mathfrak{D}$ is a central division algebra, we know that $\mathfrak{D}\neq\mathfrak{F}[u]$, and there exists an element y not in $\mathfrak{F}[u]$. But then it is known(3) that there exists an element b in $\mathfrak{F}[u]$ such that if $w=y-b$, then $wu+uw=0$. Also $\mathfrak{D}$ is commutative and so $2wu=0$, $wu=0$, w is not in $\mathfrak{F}[u]$, $w\neq 0$, $u\neq 0$. This contradicts the hypothesis that $\mathfrak{D}$ is a division algebra.

We now assume that $\mathfrak{D}$ has characteristic two and that there exists an element u in $\mathfrak{D}$ such that $\mathfrak{F}[u]$ is a separable quadratic field over $\mathfrak{F}$. Then we may select u so that $u^2=u+\alpha$ where α is in $\mathfrak{F}$. Let v be in $\mathfrak{D}$ and not in $\mathfrak{F}[u]$ so that $1, u, v$ are linearly independent in $\mathfrak{F}$. When $\mathfrak{F}$ is a finite field, the fields $\mathfrak{F}[u]$ and $\mathfrak{F}[v]$ are necessarily isomorphic; we may take $v^2=v+\alpha$ and $(u+v)^2=u^2+v^2=u+\alpha+v+\alpha=u+v$, $(u+v)(u+v-1)=0$ which is impossible. Hence $\mathfrak{F}$ is an infinite field. Write $v^2=\beta v+\gamma$ where β and γ are in $\mathfrak{F}$, and form $(u+\xi v)^2=\lambda(u+\xi v)+\mu=u^2+\xi^2v^2=u+\alpha+\xi^2(\beta v+\gamma)$. Then $\lambda=1$, $\xi^2\beta=\xi$. If $\beta=0$ and $\xi=1$ we obtain a contradiction. Otherwise $\beta\neq 0$, and we may take $\xi\neq 1$ to obtain a contradiction. This completes the proof.

COROLLARY I. *There exists no commutative central division algebra of degree two over a perfect field.*

The result above implies, in particular, that no commutative division algebra of degree two over a finite center $\mathfrak{F}$ exists. However, commutative central division algebras of degree two do exist. Indeed let $\mathfrak{F}$ be any field of characteristic two such that a purely inseparable field $\mathfrak{K}$ of *degree* (that is, dimension) $n=2^r>2$, and *exponent* (that is, degree in our present sense) two over $\mathfrak{F}$ exists(4). Let $t(x)$ be a linear function on $\mathfrak{K}$ to $\mathfrak{F}$ such that $t(x)$ is not identically zero and $t(\alpha)=0$ for every α of $\mathfrak{F}$. Such a function can always be defined by selecting a basis $1, u_2, \cdots, u_n$ of $\mathfrak{K}$ over $\mathfrak{F}$ and writing $x=\xi_1+\xi_2u_2+\cdots+\xi_nu_n$ for ξ_i in $\mathfrak{F}$, $t(x)=\xi_2$.

Let $\mathfrak{D}$ be the algebra which is the same vector space as $\mathfrak{K}$ over $\mathfrak{F}$, and whose product $x\cdot y$ is defined in terms of the product xy of $\mathfrak{K}$ by

(3) See Lemma 1 of the author's *Absolute-valued algebraic algebras*, Bull. Amer. Math. Soc. vol. 55 (1949) pp. 763–768.

(4) For example, let $\mathfrak{P}$ be any finite field of characteristic 2, $\mathfrak{K}=\mathfrak{P}(\xi_1, \cdots, \xi_r)$, $\mathfrak{F}=\mathfrak{P}(\xi_1^2, \cdots, \xi_r^2)$, where $\xi_1, \cdots, \xi_r$ are independent indeterminates over $\mathfrak{F}$ and $r>1$.

$$x \cdot y = xy - t(x)t(y). \tag{1}$$

It should be evident that $x \cdot y$ is a bilinear function on $\mathfrak{K}\mathfrak{K}$ to $\mathfrak{K}$, and that it defines an n-dimensional commutative algebra $\mathfrak{D}$ over $\mathfrak{F}$. Since $t(\alpha) = 0$ for every α of $\mathfrak{F}$, we have $\alpha \cdot x = \alpha x$ for every x of $\mathfrak{D}$ and the unity element of $\mathfrak{K}$ is the unity element of $\mathfrak{F}$. We shall use the following well known result.

LEMMA 1. *Let $\mathfrak{D}$ be an algebra of finite dimension over $\mathfrak{F}$ and let $\mathfrak{D}$ have a unity element. Then $\mathfrak{D}$ is a division algebra if and only if $\mathfrak{D}$ contains no divisors of zero.*

In our special case suppose that $x \neq 0$, $y \neq 0$, $x \cdot y = 0$. Then $\beta = xy = t(x)t(y)$ is in $\mathfrak{F}$ and so $y = \beta x^{-1}$. However $x^2 = \alpha$ in $\mathfrak{F}$ for every x of $\mathfrak{K}$. If $x \neq 0$ is in $\mathfrak{F}$ we know that $t(x) = 0$, $\beta = xy \neq 0$, whereas $\beta = t(x)t(y) = 0$, a contradiction. Hence let x be not in $\mathfrak{F}$ and therefore assume that the equation $\lambda^2 = \alpha$ has no root in $\mathfrak{F}$. But $x^{-1} = \alpha^{-1}x$, $y = \beta\alpha^{-1}x$, $xy = \beta\alpha^{-1}xx = \beta = t(x)t(\beta\alpha^{-1}x) = \beta\alpha^{-1}[t(x)]^2$, $\alpha = [t(x)]^2$ contrary to hypothesis. This completes our proof of a part of the following result.

THEOREM 2. *The algebra $\mathfrak{D}$ defined by* (1) *is a central division algebra over $\mathfrak{F}$.*

To complete our proof assume that c is in the center $\mathfrak{C}$ of $\mathfrak{D}$. We form $c \cdot (y \cdot z) = c \cdot [yz - t(y)t(z)] = c(yz) - t(c)t(yz) - ct(y)t(z)$ and $(c \cdot y) \cdot z = (cy)z - t(z)t(cy) - zt(y)t(c)$. Since c is in $\mathfrak{C}$, these two expressions must be equal and so

$$t(z)t(cy) + zt(y)t(c) = t(c)t(yz) + ct(y)t(z) \tag{2}$$

for every y and z of $\mathfrak{K}$. If $t(c) = 0$, we take $y = z = u$ to be an element of $\mathfrak{K}$ such that $t(u) = 1$. Then, by (2), c is clearly in $\mathfrak{F}$. Hence let $t(c) \neq 0$ so that c is not in $\mathfrak{F}$. Since $n > 2$, there exists an element z in $\mathfrak{K}$ such that $t(z) = 1$ and $1, c, z$ are linearly independent in $\mathfrak{F}$. For $\mathfrak{K}$ must contain $n > 2$ linearly independent elements and if $1, c, w$ are linearly independent and $t(w) = 0$, we may take $z = [t(c)]^{-1}c + w$. In case $t(w) \neq 0$ we may take $z = [t(w)]^{-1}w$. Take $y = z$ in (2) and obtain $t(y) = 1$, $zt(c) - c = t(c)t(z^2) - t(z)t(cz)$. This relation contradicts the assumption that $1, c$, and z are linearly independent and our proof is complete.

3. **Power-associative algebras.** An algebra $\mathfrak{D}$ over a field $\mathfrak{F}$ is said to be *power-associative* if the polynomial subalgebra $\mathfrak{F}[x]$ is associative for every x of $\mathfrak{D}$. When the characteristic of $\mathfrak{F}$ is not two, we may attach a commutative algebra $\mathfrak{D}^{(+)}$ to $\mathfrak{D}$. This is the same vector space as $\mathfrak{D}$ but is defined relative to the product

$$x \cdot y = (xy + yx)/2,$$

where xy is the product of $\mathfrak{D}$. When $\mathfrak{D}$ is power-associative, powers relative to $x \cdot y$ coincide with powers relative to xy, and so the subalgebras $\mathfrak{F}[x]$ of $\mathfrak{D}$ coincide with the corresponding subalgebras of $\mathfrak{D}^{(+)}$.

The theory of power-associative commutative algebras[5] has been developed for algebras over a field $\mathfrak{F}$ whose characteristic is not 2, 3, or 5. The theory can be extended to include algebras of characteristic 3 and 5 if we alter our definition of power-associativity as follows.

DEFINITION. *A power-associative algebra $\mathfrak{D}$ over a field $\mathfrak{F}$ of characteristic not two is said to be strictly power-associative if $(\mathfrak{D}^{(+)})_{\mathfrak{K}}$ is power-associative for every scalar extension $\mathfrak{K}$ of $\mathfrak{F}$.*

Every power-associative algebra of characteristic $p \neq 2, 3, 5$ is strictly power-associative. For $\mathfrak{D}^{(+)}$ is known to be power-associative if and only if $(x^2 \cdot x) \cdot x = x^2 \cdot x^2$ for every x of $\mathfrak{D}$. However, this fourth-power identity is *equivalent*, when p is prime to 30, to a multilinear identity which is clearly preserved under scalar extension. When $p = 3, 5$ the assumption that $\mathfrak{F}$ has more than five elements is sufficient to insure that every power-associative algebra over $\mathfrak{F}$ is strictly power-associative and our results on commutative power-associative algebras are valid.

We may now write[6]

$$\mathfrak{D} = \mathfrak{D}_e(1) + \mathfrak{D}_e(1/2) + \mathfrak{D}_e(0),$$

where e is any idempotent of $\mathfrak{D}$, the vector subspaces $\mathfrak{D}_e(\lambda)$ are supplementary in their sum, and $D_e(\lambda)$ consists of all elements x of $\mathfrak{D}$ such that $ex_\lambda + x_\lambda e = 2\lambda x_\lambda$, where $\lambda = 0, 1/2, 1$. The subspaces $\mathfrak{D}_e(1)$ and $\mathfrak{D}_e(0)$ are orthogonal with respect to the product operation of $\mathfrak{D}$ and $ex_1 = x_1 e = x_1$, $ex_0 = x_0 e = 0$ for every x_1 of $\mathfrak{D}_e(1)$ and every x_0 of $\mathfrak{D}_e(0)$. We shall now proceed to use these properties in a discussion of finite power-associative division rings.

A nonassociative ring $\mathfrak{D}$ will be called a *quasi-division ring* if the set $\mathfrak{D}^*$ of the nonzero elements of $\mathfrak{D}$ forms a quasigroup with respect to the product operation of $\mathfrak{D}$. Then $\mathfrak{D}$ is a division ring if $\mathfrak{D}$ has a unity element. When $\mathfrak{D}$ is an algebra we call $\mathfrak{D}$ a *quasi-division algebra* if it is a quasi-division ring, and the resulting definition of a division algebra coincides with the one given earlier.

A finite quasi-division ring $\mathfrak{D}$ is an algebra over the field $\mathfrak{P}$ of p elements, where p is the characteristic of $\mathfrak{D}$. We shall prove that a finite power-associative quasi-division ring has a unity element. It suffices to prove the following theorem on algebras.

LEMMA 2. *Let $\mathfrak{D}$ be a strictly power-associative finite-dimensional algebra without nilpotent elements. Then $\mathfrak{D}$ has a unity element.*

---

(5) See the author's *A theory of power-associative commutative algebras*, Trans. Amer. Math. Soc. vol. 69 (1950) pp. 503–527. Most of the results referred to in this section as *known* will be found in that paper, and the remaining results in *Power-associative rings*, Trans. Amer. Math. Soc. vol. 64 (1948) pp. 552–593. The results were derived for algebras of characteristic $p > 5$ but they have been extended to strictly power-associative algebras of characteristic $p \neq 2$ in a Ph.D. dissertation by Mr. Louis Kokoris.

(6) *Power-associative rings*, Theorem 2.

For if x is any element of $\mathfrak{D}$ the algebra $\mathfrak{F}[x]$ is not nilpotent. Hence $\mathfrak{D}$ contains an idempotent. Since $\mathfrak{D}$ is finite-dimensional, there exists an element e which is a principal idempotent of $\mathfrak{D}^{(+)}$. Then all elements of $\mathfrak{D}_e(0)$ and $\mathfrak{D}_e(1/2)$ are known to be nilpotent and so $\mathfrak{D}_e(0)=\mathfrak{D}_e(1/2)=0$, $\mathfrak{D}=\mathfrak{D}_e(1)$ has e as its unity element.

The following result is also known.

LEMMA 3. *Let $\mathfrak{D}$ be a strictly power-associative algebra and u and v be orthogonal idempotents of $\mathfrak{D}^{(+)}$. Then $(u\cdot y)\cdot v=u\cdot(y\cdot v)$ for all elements y of $\mathfrak{D}$.*

We shall apply this result first for algebraic algebras possibly of infinite dimension over $\mathfrak{F}$.

THEOREM 3. *Let $\mathfrak{D}$ be a strictly power-associative algebraic division algebra over a perfect field of characteristic not two. Then $\mathfrak{D}^{(+)}$ is a Jordan algebra.*

We may take $\mathfrak{F}$ to be the center of $\mathfrak{D}$ and suppose that x is an element of $\mathfrak{D}$. The Jordan identity $(x\cdot y)\cdot x^2=x\cdot(y\cdot x^2)$ holds trivially if x is in $\mathfrak{F}$. Otherwise there exists a scalar extension $\mathfrak{K}$ of $\mathfrak{F}$ such that $x=\xi_1e_1+\cdots+\xi_ne_n$ for pairwise orthogonal idempotents e_i of $\mathfrak{B}=(\mathfrak{D}^{(+)})_{\mathfrak{K}}$ and elements ξ_i in $\mathfrak{K}$. The algebra $\mathfrak{B}$ is power-associative and $(e_i\cdot y)\cdot(e_j\cdot e_k)=e_i\cdot[y\cdot(e_j\cdot e_k)]$ for every $i, j, k=1, \cdots, n$ since both sides vanish when $j\neq k$ and we may apply Lemma 3 when $j=k$. But then the Jordan identity holds in $\mathfrak{D}^{(+)}$.

When $\mathfrak{F}$ is not perfect we can prove the following partial conclusion for *commutative* algebras.

THEOREM 4. *Let $\mathfrak{D}$ be a commutative strictly power-associative algebraic division algebra over a center $\mathfrak{F}$ of characteristic $p\neq 2$. Then $\mathfrak{D}$ is either a Jordan algebra or $\mathfrak{F}[x]$ is a purely inseparable extension of $\mathfrak{F}$ for every x of $\mathfrak{D}$.*

For suppose that $\mathfrak{D}$ is not a Jordan algebra. If $\mathfrak{D}$ contains a separable subfield $\mathfrak{F}[x]$ of degree $n\geqq 3$ over $\mathfrak{F}$, there exists a scalar extension $\mathfrak{K}$ of $\mathfrak{F}$ such that the central simple algebra $\mathfrak{D}_{\mathfrak{K}}$ contains three orthogonal idempotents. It is then known that $\mathfrak{D}_{\mathfrak{K}}$ is a Jordan algebra and so $\mathfrak{D}$ is a Jordan algebra. It follows that either every $\mathfrak{F}[x]$ is purely inseparable over $\mathfrak{F}$ or that $\mathfrak{D}$ contains a quadratic separable subfield $\mathfrak{F}[i]$ where $i^2=\zeta$ in $\mathfrak{F}$. Let $\mathfrak{K}=\mathfrak{F}[w]$ where $w^2=\zeta$, and make the scalar extension $\mathfrak{D}_{\mathfrak{K}}=\mathfrak{A}$. Then $\mathfrak{A}$ contains $u=(1/2)(1-w^{-1}i)$ and $v=(1/2)(1+w^{-1}i)$, and we know that u and v are orthogonal idempotents. We form $\mathfrak{A}=\mathfrak{A}_u(1)+\mathfrak{A}_u(1/2)+\mathfrak{A}_u(0)$ and see that if x is in $\mathfrak{A}_u(1/2)$, then $xu=x/2=(1-w^{-1}i)x/2$. But then $ix=0$. However we can write $x=y+wz$ for y and z in $\mathfrak{D}$ and $ix=0$ if and only if $iy=iz=0$. Since $\mathfrak{D}$ is a division algebra and $i\neq 0$, we know that $y=z=0$, $x=0$, $\mathfrak{A}_u(1/2)=0$. It follows that $\mathfrak{A}$ is the direct sum of its subalgebras $\mathfrak{A}_u(1)$ and $\mathfrak{A}_u(0)$ and is not simple. However, $\mathfrak{D}$ has $\mathfrak{F}$ as its center and $\mathfrak{D}_{\mathfrak{K}}$ is simple for every scalar extension $\mathfrak{K}$, a contradiction.

Let us turn now to our generalization of the Wedderburn Theorem

which states that every *finite associative division algebra is a field*(7). As we remarked in the Introduction, since an alternative algebra is strictly power-associative, our result will include Artin's generalization(8) for algebras of characteristic $p \neq 2$. We shall actually use Lemma 2 to state our final result in the following form.

THEOREM 5. *Every finite strictly power-associative quasi-division ring of characteristic $p \neq 2$ is a finite field.*

We have already seen that $\mathfrak{D}$ has a unity element e and a center $\mathfrak{F}$, and that $\mathfrak{F}[x]$ is a field for every x of $\mathfrak{D}$. If there were an idempotent $u \neq e$ in $\mathfrak{D}$, then $(e-u)u = u-u = 0$ contrary to our hypothesis that $\mathfrak{D}$ is a division algebra. By Theorem 3 the algebra $\mathfrak{D}^{(+)}$ is a semisimple Jordan algebra. If $\mathfrak{D}^{(+)}$ were not simple there would be an idempotent $u \neq e$ in $\mathfrak{D}$ and we have seen that this is impossible. Hence $\mathfrak{D}^{(+)}$ is a simple Jordan algebra with center Z.

Since $\mathfrak{F}$ is a finite field, the field $\mathfrak{Z}$ is a separable extension $\mathfrak{Z} = \mathfrak{F}[z]$ of $\mathfrak{F}$. If $\mathfrak{D}^{(+)} = \mathfrak{Z} = \mathfrak{F}[z]$, then $\mathfrak{D} = \mathfrak{F}[z]$ is a field.

Assume now that $\mathfrak{D}^{(+)} \neq \mathfrak{Z}$. Then $\mathfrak{D}^{(+)}$ contains an element x not in $\mathfrak{Z}$ and $\mathfrak{Z}[x]$ is a separable field of degree $n \geqq 2$ over $\mathfrak{Z}$. There will then exist a scalar extension $\mathfrak{K}$ of $\mathfrak{Z}$ such that the central simple Jordan algebra $\mathfrak{D}_{\mathfrak{K}}^{(+)}$ contains at least two pairwise orthogonal idempotents. But then $\mathfrak{D}^{(+)}$ is a classical Jordan algebra and the Wedderburn Theorem implies that $\mathfrak{D}^{(+)}$ is one of the algebras of the following list(9).

(a) An algebra $\mathfrak{B} = z + u_2 z + \cdots + u_s z$ where $u_i^2 = a_i \neq 0$ in z, $u_i u_j = 0$ for $i \neq j$, and $s > 2$.

(b) The algebra $\mathfrak{M}_t^{(+)}$, where $\mathfrak{M}_t$ is the t-rowed total matric algebra over $\mathfrak{Z}$.

(c) The algebra $\mathfrak{E}^{(+)}$ of all three-rowed Hermitian matrices with elements in a Cayley algebra.

(d) The algebra $\mathfrak{S}^{(+)}$ of all elements $a = a^J$ in $\mathfrak{M}_t$, where J is an involution of $\mathfrak{M}_t$.

The algebra $\mathfrak{D}^{(+)}$ cannot be an algebra of type b, c, or d since each such algebra contains an idempotent $u \neq e$. This result is obvious for $\mathfrak{D}^{(+)}$ of type b or c. Indeed we take u to be the matrix e_{11} with unity in the first row and column. Let $\mathfrak{B}^{(+)}$ be of type d. If J does not leave the elements of $\mathfrak{Z}$ unaltered, it induces an automorphism $\xi \to \bar{\xi}$ of order two in $\mathfrak{Z}$ and we may write $a^J = g\bar{a}'g^{-1}$ where we may always take $g = \bar{g}'$. By a similarity transformation we may take g to be a diagonal matrix and $u = e_{11}$ is in $\mathfrak{S}^{(+)}$. If J is an

(7) *A theorem on finite algebras*, Trans. Amer. Math. Soc. vol. 6 (1905) pp. 349–352.

(8) *Über einen Satz von Herrn J. H. M. Wedderburn*, Abh. Math. Sem. Hamburgischen Univ. vol. 5 (1928) pp. 245–250.

(9) See F. D. Jacobson and N. Jacobson, *Classification and representations of semi-simple Jordan algebras*, Trans. Amer. Math. Soc. vol. 65 (1949) pp. 141–169. This list of algebras of characteristic p is derived under the hypothesis that the split algebras are the classical simple Jordan algebras and this result is now known.

involution over $\mathfrak{Z}$ we have $a^J = ga'g^{-1}$ for $g = \pm g'$ and in the former case we can take g to be diagonal and $u = e_{11}$. In the latter case $t = 2s$ for $s \geqq 2$ and we may take

$$g = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}, \qquad a = \begin{pmatrix} A_1 & A_2 \\ A_3 & A_1' \end{pmatrix} = ga'g^{-1},$$

for s-rowed square matrices A_1, $A_2 = -A_2'$, $A_3 = -A_3'$ with elements in $\mathfrak{Z}$. We take $A_2 = A_3 = 0$ and A_1 to be a singular idempotent matrix in u and have completed our proof that $\mathfrak{D}^{(+)}$ is of type a. Then $\mathfrak{D}$ contains elements u and v such that $u^2 = a$, $v^2 = b$, $u \cdot v = 0$, where a and b are nonsquares in $\mathfrak{Z}$ and 1, u, v are linearly independent in $\mathfrak{Z}$. There is a unique quadratic extension of $\mathfrak{Z}$ and thus we may take $a = b$. If c is any element of $\mathfrak{Z}$ and $w = c \cdot u + v$, the field $\mathfrak{Z}[w]$ is isomorphic to $\mathfrak{Z}[u]$ and so $w^2 = (c^2+1) \cdot a = d^2 \cdot a$ where d is in $\mathfrak{Z}$. We let k range over all elements of the field $\mathfrak{P}$ of p elements and see that if $k = c^2$, then $k+1 = d^2$ for d in $\mathfrak{Z}$. It follows that all elements of $\mathfrak{P}$ are squares in $\mathfrak{Z}$ and that $-1 = c^2$ for c in $\mathfrak{Z}$, $(c \cdot u + v)^2 = -a + a = 0$. This contradicts the hypothesis that $\mathfrak{D}$ is a division algebra and completes our proof.

4. **Commutative algebras of even order.** L. E. Dickson has provided a construction of algebras of the following type. We let $\mathfrak{Z}$ be a cyclic field of degree n over $\mathfrak{F}$, g be a nonzero element of $\mathfrak{Z}$, S be an automorphism

$$z \to z' = zS$$

of $\mathfrak{Z}$ over $\mathfrak{F}$. Define an algebra

$$\mathfrak{D} = \mathfrak{Z} + j\mathfrak{Z} = \{Z, S, g\}$$

of order $2n$ over $\mathfrak{F}$ with a product defined in terms of the product ab of $\mathfrak{Z}$ by

$$(a + jb)(c + jd) = (ac + b'd'g) + j(ad + bc) \tag{3}$$

for all a, b, c, d in $\mathfrak{Z}$. The algebra $\mathfrak{D}$ is commutative, $\mathfrak{Z}$ is a subalgebra of $\mathfrak{D}$, and the unity element of $\mathfrak{Z}$ is the unity element of $\mathfrak{D}$. If $\mathfrak{K}$ is the subfield of $\mathfrak{Z}$ consisting of all elements $k = k'$ in $\mathfrak{Z}$, it should be clear from the definition (3) that $\mathfrak{D}$ is an algebra over the field $\mathfrak{K}$. Hence there is no loss of generality if we assume that S generates the cyclic Galois group of $\mathfrak{Z}$ over $\mathfrak{F}$ and we shall make this assumption.

THEOREM 6. *The algebra* $\mathfrak{D} = \{Z, S, g\}$ *is central simple over* $\mathfrak{F}$.

For assume that $\mathfrak{B}$ is a nonzero proper ideal of $\mathfrak{D}$. If $\mathfrak{B}$ contains either a nonzero element a of $\mathfrak{Z}$ or an element bj for $b \neq 0$ in $\mathfrak{Z}$, then $\mathfrak{B} = \mathfrak{D}$ since $\mathfrak{B}$ contains $1 = aa^{-1}$ in the former case and $1 = [(jb)j](b'g)^{-1}$ in the latter case. Hence every nonzero element w of $\mathfrak{B}$ has the form $w = a + jb$ where $a \neq 0$, $b \neq 0$. But $wb^{-1} = ab^{-1} + j = c + j$ is in $\mathfrak{B}$ and so are $(c+j)j = g + jc$ and $(c+j)(1+bj) = (c+b'g) + j(bc+1)$. If $g \neq c^2$, then $\mathfrak{B}$ contains $(c+j) - (g+jc)c^{-1} = c - gc^{-1} \neq 0$ in $\mathfrak{Z}$ which has already been shown to be impossible. Hence

$g=c^2$, $(c+j)(1-jc^{-1})=c-(c')^{-1}g$ is in $\mathfrak{B}$ and must vanish, $cc'=c^2$, $c'=c$ is in $\mathfrak{F}$. There exists an element b in $\mathfrak{Z}$ such that $b\neq b'$, $bc+1\neq 0$, $c+b'g\neq(bc+1)c=bg+c$. But then $\mathfrak{B}$ contains $[(c+j)(1+bj)](bc+1)^{-1}=d+j$, where we have just shown that $d\neq c$. It follows that $d-c$ is a nonzero element of $\mathfrak{Z}$ which is in $\mathfrak{B}$, and we arrive at a contradiction which implies that $\mathfrak{D}$ must be simple.

Assume that $a+jb$ is in the center $\mathfrak{C}$ of $\mathfrak{D}$. Then $(a+jb)j\cdot j=(b'g+ja)j=a'g+j(b'g)=(a+jb)j^2=(a+jb)g=ag+j(bg)$. It follows that $a=a'$ and $b=b'$ are in $\mathfrak{F}$. The computation $(a+jb)j\cdot c=(bg+ja)c=bgc+j(ac)=(a+jb)(jc)=gbc'+j(ac)$ yields $bgc=bgc'$, and if $c\neq c'$ we know that $bg=0$, $b=0$, $a+jb=a$ is in $\mathfrak{F}$ as desired. This completes our proof.

Dickson showed([10]) that $\mathfrak{D}$ is a division algebra if $N_{\mathfrak{Z}|\mathfrak{F}}(g)\neq[N_{\mathfrak{Z}|\mathfrak{F}}(a)]^2$ for any a of $\mathfrak{Z}$ where $N_{\mathfrak{Z}|\mathfrak{F}}(a)$ is the norm of the element a of the cyclic field $\mathfrak{Z}$. In the finite case we can improve this necessary condition and derive a necessary and sufficient condition.

THEOREM 7. *Let $\mathfrak{F}$ be a finite field of characteristic $p\neq 2$. Then $\mathfrak{D}=\{Z, S, g\}$ is a division algebra if and only if $g\neq z^2$ for any z of $\mathfrak{Z}$. Such algebras exist over any such field $\mathfrak{F}$ and for every n.*

For let $(a+jb)(c+jd)=0$ for $a+jb\neq 0$ and $c+jd\neq 0$. Then $ac+gb'd'=0=ad+bc$. If $a=0$ then $b\neq 0$ and $gb\neq 0$. Hence $d'=d=0=bc$ and $c=0$, a contradiction. It follows that $a\neq 0$, $c=-gb'd'a^{-1}$, $ad=bb'd'a^{-1}g$, and so we see that $\mathfrak{D}$ is a division algebra if and only if the equation

$$a^2d = bb'gd' \tag{4}$$

is impossible for any nonzero elements a, b, d of $\mathfrak{Z}$. The automorphism S is a power of the generating automorphism $z\to z^p$ of $\mathfrak{Z}$ over the field of p elements, and so there exists a positive integer t such that

$$z' = z^q, \qquad q = p^t$$

for every z of $\mathfrak{Z}$. Then (4) is equivalent to $g=a^2d^{1-q}b^{-q-1}=h^2$ where $h=ad^rb^{r-1}$ and $1-q=2r$. It follows that when $g\neq h^2$ for any h of $\mathfrak{Z}$ the algebra $\mathfrak{D}$ is a division algebra. The converse is an immediate consequence of the fact that if $g=h^2$ we have $(h-j)(h+j)=0$.

The field $\mathfrak{Z}$ is the Galois field $GF(p^\gamma)$ for some positive integer γ. The nonzero elements of $\mathfrak{Z}$ form a cyclic multiplicative group $\mathfrak{Z}^*$ of even order $\tau=p^\gamma-1$ and $\mathfrak{Z}^*$ consists of the powers of a generating element η. If $g=\eta^{2k+1}$ for any positive integer k the algebra $\mathfrak{D}$ is a division algebra. For otherwise $g=h^2=\eta^{2r}$ and so $\eta^{2k-2r+1}=1$, whereas τ is even and cannot divide $2(k-r)+1$.

([10]) See his *Linear algebras with associativity not assumed*, Duke Math. J. vol. 1 (1935) pp. 113–125. Dickson gave the construction and the sufficient condition we have stated here. He did not discuss the question as to whether the sufficient condition can be satisfied, and the concepts of center and central nonassociative algebra were not known when his paper was written.

This proves that finite division algebras of the Dickson type exist for every finite field $\mathfrak{F}$ of characteristic not two and every even dimension $2n$. Indeed we have constructed all division algebras of the given type since the remaining values η^{2k} of g will not yield division algebras.

The relation (4) implies that $[N(a)]^2N(d)=[N(b)]^2N(d)N(g)$, $N(g)=[N(h)]^2$ where $h=ab^{-1}$. This yields the sufficient condition that $\mathfrak{D}$ be a division algebra as given by Dickson. We may now construct division algebras $\mathfrak{D}$ in a number of cases where $\mathfrak{F}$ is an infinite field of characteristic not two. We assume that there exists a cyclic field $\mathfrak{Z}$ of degree n over $\mathfrak{F}$ and an element γ in $\mathfrak{F}$ such that $\gamma\neq\delta^2$ for any δ of $\mathfrak{F}$. We then apply the construction and criterion of Dickson to obtain a central division algebra of order $2n$ over $\mathfrak{F}$ in the following cases.

(1) Let n be odd and take g to be the element γ of $\mathfrak{F}$ defined above. Then $n=2m+1$, $N(\gamma)=(\gamma^m)^2\gamma\neq\delta^2$ for any δ of $\mathfrak{F}$, and $\mathfrak{D}$ is a division algebra.

(2) Let $n=2^em$ where m is odd and $e\geqq 1$. Assume that there exists a cyclic field $\mathfrak{W}$ of degree $2n$ over $\mathfrak{F}$, and take $\mathfrak{Z}$ to be the subfield of degree n. Then $\mathfrak{Z}$ contains a subfield $\mathfrak{Y}$ of degree 2^e which is a cyclic subfield of a subfield $\mathfrak{Y}_1$ of degree 2^{e+1} of $\mathfrak{W}$. It is known([11]) that $\mathfrak{Y}$ contains an element g such that $N_{\mathfrak{Y}|\mathfrak{F}}(g)=-1$. If we assume that $-1\neq\delta^2$ for any δ of $\mathfrak{F}$, the algebra $\mathfrak{D}$ defined by $\mathfrak{Z}$ and g has $N_{\mathfrak{Z}|\mathfrak{F}}(g)=(-1)^m=-1$ and $\mathfrak{D}$ is a division algebra.

(3) Let $\mathfrak{F}$ be any algebraic number field. We take p to be an odd prime, $\mathfrak{p}_{\mathfrak{F}}$ to be a prime ideal divisor of p in the ring $J_{\mathfrak{F}}$ of all integers of $\mathfrak{F}$. The Grünwald theorem implies the existence of a cyclic field $\mathfrak{Z}$ of degree n over $\mathfrak{F}$ such that $\mathfrak{p}_{\mathfrak{F}}$ is completely ramified in $\mathfrak{Z}$. Then $N_{\mathfrak{Z}|\mathfrak{F}}(P_{\mathfrak{F}})=\mathfrak{p}_{\mathfrak{F}}$ where $\mathfrak{p}_{\mathfrak{F}}=P_{\mathfrak{F}}^n$ and $P_{\mathfrak{F}}$ is a prime ideal in $J_{\mathfrak{Z}}$. Let g be an element of $P_{\mathfrak{Z}}$ which is not in $P_{\mathfrak{Z}}^2$. Then $N_{\mathfrak{Z}|\mathfrak{F}}(g)$ is divisible by $P_{\mathfrak{Z}}^n=\mathfrak{p}_{\mathfrak{F}}$ but not by $\mathfrak{p}_{\mathfrak{F}}^2$. Hence $N_{\mathfrak{Z}|\mathfrak{F}}(g)$ is a non-square and the corresponding algebra $\mathfrak{D}$ is a division algebra.

5. **Twisted fields.** All of the known types of central division algebras have been constructed by procedures which yield algebras necessarily of composite dimension. We shall give a new construction here which will yield central algebras, necessarily not associative, of quite arbitrary odd dimension.

Let $\mathfrak{F}$ be a field *subject only to the restriction that there exists a cyclic field* $\mathfrak{Z}$ *of odd degree* n *over* $\mathfrak{F}$, and let S be a generating automorphism of the Galois group of $\mathfrak{Z}$ over $\mathfrak{F}$. We let $\gamma\neq 1, 0$ be an element of $\mathfrak{F}$, and define an algebra $[\gamma, \mathfrak{Z}, S]$ which is the same vector space over $\mathfrak{F}$ as $\mathfrak{Z}$ but which has a product operation (x, y) defined in terms of the product operation xy of $\mathfrak{Z}$ by

$$(x, y) = (1-\gamma)^{-1}[x(yS)-\gamma(xS)y]. \tag{5}$$

LEMMA 4. *There are no divisors of zero in* $[\gamma, \mathfrak{Z}, S]$ *if and only if* $\gamma^n\neq 1$.

For if $\gamma^n=1$, then $N(\gamma)=1$ and a well known theorem of Hilbert([12])

([11]) This is the case $p=2$, $\zeta=-1$ of Theorem 9.10 of the author's *Modern higher algebra*.

([12]) Ibid. Theorem 9.5.

implies that $\gamma = x(xS)^{-1}$ for some x of $\mathfrak{Z}$. If $[\gamma, \mathfrak{Z}, S]$ contains no divisors of zero, this is impossible since $(x, 1) = (1-\gamma)^{-1}(x - \gamma xS) = 0$. Conversely if $\gamma^n \neq 1$ and $(x, y) = 0$ for $x \neq 0, y \neq 0$ in $[\gamma, \mathfrak{Z}, S]$, then $x(yS) = \gamma(xS)y$, $N(x)N(y) = \gamma^n N(x)N(y)$, which is impossible.

Let us now investigate the conditions on $\mathfrak{F}$ which would enable us to satisfy the restriction $\gamma^n \neq 1$. If $\mathfrak{F}$ is any infinite field, some element γ of $\mathfrak{F}$ is not a root of the equation $\gamma^n = 1$ and defines a corresponding algebra $[\gamma, \mathfrak{Z}, S]$. When $\mathfrak{F}$ is a field of $p^\nu = q+1$ elements, every $\gamma \neq 0$ is a root of $\gamma^q = 1$. Thus $[\gamma, \mathfrak{Z}, S]$ has divisors of zero for every γ of $\mathfrak{F}$ unless q does not divide n. When $p > 2$ the integer q is even and so $[\gamma, \mathfrak{Z}, S]$ has no divisors of zero for some γ in $\mathfrak{F} = GF(p^\nu)$ and every odd n. The value of $\gamma = -1$ is allowable when p is odd, and $[-1, \mathfrak{Z}, S]$ is commutative in this case. We shall now define an isotope of $[\gamma, \mathfrak{Z}, S]$ which has a unity element and so is a division algebra.

The linear transformation $x \to (x, y) = xR_y^{(0)}$ on the vector space $\mathfrak{Z}$ is expressible in terms of the multiplication $x \to xy = xR_y$ of $\mathfrak{Z}$ by

$$R_y^{(0)} = \delta(R_{yS} - \gamma S R_y), \qquad \delta^{-1} = 1 - \gamma. \tag{6}$$

Similarly $y \to (x, y) = yL_x^{(0)}$ where

$$L_x^{(0)} = \delta(SR_x - \gamma R_{xS}). \tag{7}$$

Since $R_y^{(0)}$ and $L_y^{(0)}$ are nonsingular for every $y \neq 0$ of $\mathfrak{Z}$, the transformations $(R_e^{(0)})^{-1}$ and $(L_e^{(0)})^{-1}$ exist where $e = 1$ is the unity element of $\mathfrak{Z}$. But $eS = e$, $R_e = R_{eS} = I$ is the identity transformation, and so

$$P = (R_e^{(0)})^{-1} = (1-\gamma)(I - \gamma S)^{-1}, \quad Q = (L_e^{(0)})^{-1} = (1-\gamma)(S - \gamma I)^{-1}. \tag{8}$$

Moreover $e(S - \gamma I) = e(I - \gamma S) = (1-\gamma)e$, and so $eP = eQ = e$, that is, $cP = cQ = c$ for every c of the subfield $e\mathfrak{F}$ of $\mathfrak{Z}$.

We are now ready to define the isotope of $[\gamma, \mathfrak{Z}, S]$ given by the product

$$x \cdot y = (xP, yQ) = \delta[(xP)(yQS) - \gamma(xPS)(yQ)]. \tag{9}$$

We shall call this algebra a *twisted field* and shall designate it by $(\gamma, \mathfrak{Z}, S)$.

LEMMA 5. *A twisted field is a division algebra. If $\mathfrak{Y}$ is a subfield of $\mathfrak{Z}$, the algebra $(\gamma, \mathfrak{Y}, S)$ is defined and is a subalgebra of $(\gamma, \mathfrak{Z}, S)$. The transformation S is an automorphism of $(\gamma, \mathfrak{Z}, S)$.*

For $x \cdot e = \delta x(P - \gamma PS) = \delta xP(I - \gamma S) = x$, and $e \cdot y = \delta yQ(S - \gamma I) = y$ for every x and y of $\mathfrak{Z}$. Thus $(\gamma, \mathfrak{Z}, S)$ has the same unity element as $\mathfrak{Z}$ and is a division algebra. If $\mathfrak{Y}$ is any subfield of $\mathfrak{Z}$, the field $\mathfrak{Y}$ is cyclic over $\mathfrak{F}$ and the automorphism S of $\mathfrak{Z}$ induces a generating automorphism $y \to yS$ of $\mathfrak{Y}$. Thus $(\gamma, \mathfrak{Y}, S)$ is defined with respect to the product $x \cdot y$ of $(\gamma, \mathfrak{Z}, S)$, and so $(\gamma, \mathfrak{Y}, S)$ is a subalgebra of $(\gamma, \mathfrak{Z}, S)$. Both Q and P are polynomials in S and

commute with S. Hence $(x\cdot y)S=\delta[(xPS)(yQSS)-\gamma(xPSS)(yQS)]=xS\cdot yS$ and S is an automorphism of $(\gamma, \mathfrak{Z}, S)$ *as well as of* $(\gamma, \mathfrak{Y}, S)$ *for every subfield* $\mathfrak{Y}$ *of* $\mathfrak{Z}$.

We may now prove

THEOREM 8. *Every twisted field* $(\gamma, \mathfrak{Z}, S)$ *is a central division algebra over* $\mathfrak{F}$. *It is power-commutative if and only if it is the commutative algebra* $(-1, \mathfrak{Z}, S)$.

We observe first that if $\gamma=-1$ the algebra $(\gamma, \mathfrak{Z}, S)$ is commutative and hence is power-commutative. Conversely let $(\gamma, \mathfrak{Z}, S)$ be power-commutative and $\mathfrak{W}$ be a subfield of $\mathfrak{Z}$ of prime degree p over $\mathfrak{F}$. Then $(\gamma, \mathfrak{W}, S)$ must be power-commutative. We begin our proof with a study of the case where p is the characteristic of $\mathfrak{F}$. Then p is odd and it is known[13] that $\mathfrak{W}=\mathfrak{F}[u]$ where $uS=u+1$. It follows that $u(I-\gamma S)=u-\gamma(u+1)=(1-\gamma)u-\gamma$, $uP(1-\gamma)=uP(I-\gamma S)+\gamma=(1-\gamma)u+\gamma$, and so

$$uP = u + \gamma\delta, \qquad uPS = u + 1 + \gamma\delta = u + \delta. \tag{10}$$

Similarly $u(S-\gamma I)=(1-\gamma)u+1$, $(1-\gamma)uQ=u(S-\gamma I)Q-1=(1-\gamma)u-1$,

$$uQ = u - \delta, \qquad uQS = u + 1 - \delta = u - \gamma\delta. \tag{11}$$

We now compute $u^2S=u^2+2u+1$, $u^2(I-\gamma S)=(1-\gamma)u^2-2\gamma u-\gamma$, $u^2(1-\gamma)P=(1-\gamma)u^2+2\gamma uP+\gamma=(1-\gamma)u^2+2u\gamma+2\gamma^2\delta+\gamma$,

$$u^2P = u^2 + 2\gamma\delta u + \gamma\delta^2(1 + \gamma), \quad u^2PS = u^2 + 2\delta u + \delta^2(1 + \gamma). \tag{12}$$

We also compute $u^2(S-\gamma I)=(1-\gamma)u^2+2u+1$, $(1-\gamma)u^2Q=(1-\gamma)u^2-2uQ-1=(1-\gamma)u^2-2u+2\delta-1$, and obtain

$$u^2Q = u^2 - 2u\delta + (1 + \gamma)\delta^2, \quad u^2QS = u^2 - 2\gamma\delta u + \delta^2\gamma(1 + \gamma). \tag{13}$$

We may now compute the square $u^{(2)}=u\cdot u=\delta[(u+\gamma\delta)(u-\gamma\delta)-\gamma(u+\delta)\cdot(u-\delta)]$, that is,

$$u^{(2)} = u^2 + \gamma\delta^2. \tag{14}$$

It can be observed at this point that $u\cdot u^{(2)}=u^{(2)}\cdot u$ if and only if $u\cdot u^2=u^2\cdot u$. However the product $u\cdot u^2=\delta[(uP)(u^2QS)-\gamma(uPS)(u^2Q)]=\delta\cdot(u+\gamma\delta)[u^2-2\gamma\delta u+\delta^2\gamma(1+\gamma)]-\gamma\delta(u+\delta)[u^2-2u\delta+(1+\gamma)\delta^2]=u^3+2\gamma\delta^2u-\gamma\delta^3(1+\gamma)$. Also $u^{(2)}\cdot u=\delta[(u^2P)(uQS)-\gamma(u^2PS)(uQ)]=\delta[u^2+2\gamma\delta u+\gamma\delta^2\cdot(1+\gamma)](u-\gamma\delta)-\gamma\delta[u^2+2\delta u+\delta^2(1+\gamma)](u-\delta)=u^3+2\gamma\delta^2u+\delta^3\gamma(1+\gamma)$. These products are equal if and only if $2\gamma\delta^3(1+\gamma)=0$, that is, $2(1+\gamma)=0$. Since we have assumed that $\mathfrak{F}$ has odd characteristic p, we have shown that $\gamma=-1$ in this case.

It will be convenient to show that $(-1, \mathfrak{W}, S)$ is not power-associative at this point. Our formulas (10), (11), (12), and (13) become

[13] Loc. cit. Theorem 9.1.

(15) $uP = u - 1/2,\ uPS = u + 1/2,\ u^2P = u^2 - u,\ u^2PS = u^2 + u,$

for $\gamma = -1$. Compute $u^3S = u^3+3u^2+3u+1$, $u^3(S+I) = 2u^3+3u^2+3u+1$, $2u^3P+3(u^2-u)+3(u-1/2)+1 = u^3(S+I)P = 2u^3 = 2u^3P+3u^2-1/2$. This computation results in the formulas

(16) $$u^3P = u^3 - (3/2)u^2 + 1/4, \qquad u^3PS = u^3 + (3/2)u^2 - 1/4.$$

Now $u \cdot u^{(2)} = u \cdot u^2 + \gamma\delta^2 u = u^3 + 3\gamma\delta^2 u$ by (14) where $\gamma = -1$ and $\delta = (1-\gamma)^{-1} = 1/2$. Thus

(17) $$u^{(3)} = u^3 - (3/4)u.$$

The fourth power in $(-1, \mathfrak{W}, S)$ is $u^{(4)} = u^{(3)} \cdot u = u^3 \cdot u - (3/4)u^{(2)} = (1/2) \cdot [(u^3 - (3/2)u^2 + 1/4)(u + 1/2) + (u^3 + (3/2)u^2 - 1/4)(u - 1/2)] - (3/4) \cdot (u^2 - 1/4) = (1/2)(u^4 - (3/2)u^3 + (1/4)u + (1/2)u^3 - (3/4)u^2 + 1/8 + u^4 + (3/2)u^3 - (1/4)u - (1/2)u^3 - (3/4)u^2 + 1/8) - (3/4)(u^2 - 1/4)$, and we have completed a derivation of the formula

(18) $$u^{(4)} = u^4 - (3/2)u^2 + 5/16.$$

However $u^{(2)} \cdot u^{(2)} = (u^2 - 1/4) \cdot (u^2 - 1/4) = u^2 \cdot u^2 - (1/2)u^2 + 1/16 = (u^2 - u) \cdot (u^2 + u) - (1/2)u^2 + 1/16 = u^4 - u^2 - (1/2)u^2 + 1/16$ and so

(19) $$u^{(2)} \cdot u^{(2)} = u^4 - (3/2)u^2 + 1/16.$$

Thus $u^{(4)} - u^{(2)} \cdot u^{(2)} = 1/4$ and $(-1, \mathfrak{W}, S)$ is not power-associative.

There remains the case where the degree p of $\mathfrak{W}$ is not the characteristic of $\mathfrak{F}$. In this case we may extend $\mathfrak{F}$ to a field $\mathfrak{K}$ containing a primitive pth root of unity ω. Then $(\gamma, \mathfrak{W}_{\mathfrak{K}}, S)$ is still a division algebra and there is actually no loss of generality if we assume that ω is in $\mathfrak{F}$. It is now known[14] that $\mathfrak{W} = \mathfrak{F}(u)$ where $u^p = \alpha$ in $\mathfrak{F}$ and $uS = \omega u$. It follows that $u^kS = \omega^k u^k$. Then $u^k(I - \gamma S) = u^k(1 - \gamma\omega^k)$ for all integers k. Since $\gamma^p \neq 1$ we know that $\gamma\omega^k \neq 1$ and so $u^k(1 - \gamma\omega^k)^{-1} = u^k(I - \gamma S)^{-1}$, that is,

(20) $$u^kP = (1 - \gamma)(1 - \gamma\omega^k)^{-1}u^k, \quad u^kPS = (1 - \gamma)\omega^k(1 - \gamma\omega^k)^{-1}u^k.$$

Also $u^k(S - \gamma I) = u^k(\omega^k - \gamma)$ and so

(21) $$u^kQ = (1 - \gamma)(\omega^k - \gamma)^{-1}u^k, \quad u^kQS = (1 - \gamma)\omega^k(\omega^k - \gamma)^{-1}u^k.$$

These two formulas imply that

(22) $$u^s \cdot u^t = f(\omega^s, \omega^t)u^{s+t},$$

where

(23) $$f(x, y) = (1 - \gamma)(1 - \gamma x)^{-1}(y - \gamma)^{-1}(y - \gamma x).$$

We put $f(x, y) = f(y, x)$ and see that $u^s \cdot u^t = u^t \cdot u^s$ if and only if

[14] Loc. cit. Theorem 8.22.

$\gamma(1+\gamma)(\omega^s-\omega^t)(1-\omega^s)(1-\omega^t)=0$. If $1\leqq s<t<p$ we obtain $\gamma(1+\gamma)=0$ and so $\gamma=-1$. This completes our proof that $(\gamma, \mathfrak{Z}, S)$ is power-commutative if and only if the nonzero parameter $\gamma=-1$.

Let us now consider the algebra $(-1, \mathfrak{W}, S)$ in the case where ω is in $\mathfrak{F}$. We compute $u^2\cdot u^2=4u^4(\omega^2+1)^{-2}\omega^2$ and $(u^2\cdot u^2)\cdot u=4\omega^2(\omega^2+1)^{-2}u^4\cdot u=8\omega^2(\omega^2+1)^{-2}(\omega^4+1)^{-1}(\omega+1)^{-1}(\omega^4+\omega)u^5=8\omega^3(\omega^2+1)^{-2}(\omega^4+1)^{-1}(\omega+1)^{-1}(\omega^3+1)u^5$. Also $u^2\cdot(u^2\cdot u)=2(\omega^2+1)^{-1}(\omega+1)^{-1}(\omega^2+\omega)u^2\cdot u^3=2\omega(\omega^2+1)^{-1}u^2\cdot u^3=4\omega(\omega^2+1)^{-1}(\omega^2+1)^{-1}(\omega^3+1)^{-1}(\omega^2+\omega^3)u^5=4\omega^3(\omega+1)(\omega^2+1)^{-2}(\omega^3+1)^{-1}u^5$. If $(-1, \mathfrak{W}, S)$ were power-associative we would have

$$2(\omega^3+1)^2=(\omega^4+1)(\omega+1)^2. \tag{24}$$

We also compute $(u^2\cdot u)\cdot u=2(u^3\cdot u)\omega(\omega^2+1)^{-1}=4\omega(\omega^2+1)^{-1}(\omega^3+1)^{-1}\cdot(\omega+1)^{-1}(\omega+\omega^3)u^4=4\omega^2(\omega^3+1)^{-1}(\omega+1)^{-1}u^4$ and $u^2\cdot(u\cdot u)=4(\omega+1)^{-2}\omega u^2\cdot u^2=16(\omega+1)^{-2}\omega^3(\omega^2+1)^{-2}u^4$. The assumption that $(-1, \mathfrak{W}, S)$ is power-associative may be used again, and we obtain

$$4(\omega^3+1)\omega=(\omega^2+1)^2(\omega+1). \tag{25}$$

It follows that $16(\omega^3+1)^2\omega^2=(\omega^2+1)^4(\omega+1)^2=8\omega^2(\omega^4+1)(\omega+1)^2$ and that $(\omega^2+1)^4=8\omega^2(\omega^4+1)$. But then $\omega^8+4\omega^6+6\omega^4+4\omega^2+1-8\omega^6-8\omega^2=(\omega^2-1)^4=0$, $\omega^2=1$, contrary to our hypothesis that ω is a primitive pth root of unity and that p is the degree of the subfield $\mathfrak{W}$ of the field $\mathfrak{Z}$ of odd degree, p is odd.

We have now shown that every subfield $\mathfrak{W}$ of $\mathfrak{Z}$ of prime degree over $\mathfrak{F}$ defines an algebra $(\gamma, \mathfrak{W}, S)$ which is not power-associative. We may now complete our proof that $(\gamma, \mathfrak{Z}, S)$ is central by showing that if the center $\mathfrak{C}$ of $(\gamma, \mathfrak{Z}, S)$ were a field of degree $m>1$ over $\mathfrak{F}$, it would have the form $\mathfrak{C}=(\gamma, \mathfrak{Y}, S)$ where $\mathfrak{Y}$ is the subfield of $\mathfrak{Z}$ of degree m over $\mathfrak{F}$. For then $\mathfrak{C}$ would be associative, $\mathfrak{Y}$ would contain a subfield $\mathfrak{W}$ of prime degree p over $\mathfrak{F}$, the nonassociative algebra $(\gamma, \mathfrak{W}, S)$ would be a subalgebra of $\mathfrak{C}$, which is impossible. The result is derived as follows.

The automorphism S of $(\gamma, \mathfrak{Z}, S)$ must induce an automorphism $c\rightarrow cS$ of the center field $\mathfrak{C}$. Since $(\gamma, \mathfrak{Z}, S)$ has dimension q over $\mathfrak{C}$ of degree m, we know that $n=qm$. However $\mathfrak{C}$ is a field and so S has order r in $\mathfrak{C}$ where r divides m. Then $\mathfrak{C}$ is contained in the subfield $\mathfrak{Y}$ of $\mathfrak{Z}$ consisting of all elements $y=yS^r$ of $\mathfrak{Z}$. Since r divides m, it also divides n and the index of the cyclic group generated by S^r is r, $\mathfrak{Y}$ has degree r over $\mathfrak{F}$, $\mathfrak{C}$ of dimension $m\geqq r$ is contained in $\mathfrak{Y}$ of dimension r, $\mathfrak{C}$ and $\mathfrak{Y}$ are equal vector spaces, $\mathfrak{C}=(\gamma, \mathfrak{Y}, S)$. This completes our proof of Theorem 8.

Theorems 7 and 8 may be combined in the case where $\mathfrak{F}$ is a finite field as follows.

THEOREM 9. *Let $\mathfrak{F}$ be any finite field of characteristic $p>2$ and n be any integer greater than 2. Then there exists a commutative central division algebra of dimension n over $\mathfrak{F}$.*

The result above is actually false for finite fields of characteristic two. Indeed it is not difficult to prove that there exists no commutative central division algebra of dimension three over the field of two elements. No central finite commutative division algebras of characteristic two are known and the question of their existence is a major problem of our theory.

We shall close by noting a generalization of our construction([15]) of twisted fields which might yield central division algebras over $GF(q+1)$ even when q divides n. The formula (5) may be modified in this case by taking γ to be an *element of* $\mathfrak{Z}$ such that $N(\gamma)\neq 1$. For example, let $\mathfrak{F}$ be the field of four elements, $n=3$, so that $\mathfrak{F}$ contains a primitive cube root of unity ω and $\mathfrak{Z}=\mathfrak{F}[u]$, $u^3=\omega$, $\gamma=u$. Then $[\gamma, \mathfrak{Z}, S]$ is an algebra without divisors of zero. A study of such algebras will be made later.

THE UNIVERSITY OF CHICAGO,
CHICAGO, ILL.

([15]) The following description of our construction of a twisted field should be observed. We begin with a field $\mathfrak{Z}$ and first pass to the nonassociative isotope defined by the product $x(yS)$ and which is norm preserving. We then pass to the quasi-equivalent algebra $[\gamma, \mathfrak{Z}, S]$. The final step in our construction is that of using the standard process of obtaining an isotope with a prescribed unity element. It is only the second step which could yield an algebra not a quasi-division algebra and it is necessary to verify that the final result is at least not the original field.