A NOTE ON NORMAL DIVISION ALGEBRAS
OF PRIME DEGREE*

A. A. ALBERT

Wedderburn has proved† that all normal division algebras of degree three over a non-modular field \( \mathfrak{A} \) are cyclic algebras. It is easily verified that his proof is actually correct for \( \mathfrak{A} \) of any characteristic not three, and I gave a modification of his proof‡ showing the result also valid for the remaining characteristic three case. Attempts to generalize Wedderburn's proof to algebras of prime degree \( p > 3 \) have thus far been futile, and it is not yet known whether there are any non-cyclic algebras of prime degree. One notes that in both Wedderburn's proof and my modification one starts by studying a non-cyclic cubic field and thus a subfield of a normal splitting field of degree six with a quadratic (cyclic) subfield. I have generalized this property to the case of arbitrary prime degree and have now provided a new proof of the Wedderburn theorem for algebras of degree three in the characteristic three case. The result is the special case \( p = 3, m = 2 \) of the following theorem:

THEOREM. Let \( \mathfrak{D} \) be a normal division algebra of degree \( p \) over a field \( \mathfrak{A} \) of characteristic \( p \), and let \( m \) be prime to \( p \). Then if \( \mathfrak{D} \) has a normal splitting field \( \mathfrak{B} \) of degree \( pm \) over \( \mathfrak{A} \), with a cyclic subfield \( \mathfrak{L} \) of degree \( m \) over \( \mathfrak{A} \), it follows that the algebra \( \mathfrak{D} \) is a cyclic algebra.

In our proof we shall use the following known theorems§ on normal division algebras \( \mathfrak{D} \) of degree \( n \) over arbitrary fields \( \mathfrak{A} \):

**Lemma 1.** Let \( \mathfrak{B} \) have degree prime to \( n \). Then \( \mathfrak{D} \) is a division algebra.

**Lemma 2.** Let \( \mathfrak{B}_0 \) have degree \( n \) over \( \mathfrak{A} \) and split \( \mathfrak{D} \). Then \( \mathfrak{B}_0 \) is equivalent to a (maximal) subfield of \( \mathfrak{D} \).

**Lemma 3.** Let \( \mathfrak{D} \) have a cyclic subfield of degree \( n \). Then \( \mathfrak{D} \) is a cyclic algebra.

---

* Presented to the Society, April 8, 1938.
† Transactions of this Society, vol. 22 (1921), pp. 129–135.
§ Cf. Deuring's *Algebren* for our notation and the proofs of the results of Lemmas 1, 2, 3. Lemma 4 was proved by the author for \( \mathfrak{A} \) of characteristic not \( p \), Transactions of this Society, vol. 36 (1934), pp. 885–892, and for \( \mathfrak{A} \) of characteristic \( p \), ibid., vol. 39 (1936), pp. 183–188.
LEMMA 4. Let \( \mathfrak{D} \) of prime degree \( n = p \) over \( \mathfrak{R} \) have a splitting field \( \mathfrak{J} = \mathfrak{R}(\gamma) \), such that \( \gamma^p = \gamma \) in \( \mathfrak{R} \). Then \( \mathfrak{D} \) is a cyclic algebra.

To make our proof we let \( \mathfrak{G} \) be the automorphism group of \( \mathfrak{B} \) over \( \mathfrak{R} \) and \( \mathfrak{S} \) the subgroup of \( \mathfrak{G} \) corresponding to \( \mathfrak{Y} \). Then \( \mathfrak{S} \) is a normal divisor of \( \mathfrak{G} \) and is of prime order \( p \); \( \mathfrak{S} = [\mathfrak{S}] \) is a cyclic group. The group of the cyclic field \( \mathfrak{Y} \) over \( \mathfrak{R} \) is the quotient group \( \mathfrak{G}/\mathfrak{S} \) and is a cyclic group \( [\mathfrak{S}T] \). Here \( T \) is an automorphism of \( \mathfrak{G} \) and \( T^m = S^p \) in \( \mathfrak{S} \).

But then \( [\mathfrak{S}T^p] = [\mathfrak{S}T] \) since \( p \) is prime to \( m \), \( (\mathfrak{S}T)^p = \mathfrak{S}T^p \), and \( T^{pm} = S^{pa} = I \). Hence we may assume without loss of generality that \( T^m = I \). Since \( \mathfrak{S}T \) has order \( m \) so does \( T \). The cyclic subgroup \( \mathfrak{T} = [T] \) of \( \mathfrak{G} \) corresponds to a subfield \( \mathfrak{B}_0 \) of degree \( p \) over \( \mathfrak{R} \) of \( \mathfrak{B} \), and we have the following lemma:

LEMMA 5. The field \( \mathfrak{B}_0 \) splits \( \mathfrak{D} \).

For clearly \( \mathfrak{B} \) is the composite of \( \mathfrak{B}_0 \) and \( \mathfrak{L} \), and \( \mathfrak{B} = (\mathfrak{B}_0)\mathfrak{L} \). Now \( \mathfrak{D} \) has prime degree, and either \( \mathfrak{B}_0 \) splits \( \mathfrak{D} \) or \( \mathfrak{D}_{\mathfrak{B}_0} \) is a division algebra.

In the latter case by Lemma 1 the algebra \( (\mathfrak{D}_{\mathfrak{B}_0})\mathfrak{R} = \mathfrak{D}_{\mathfrak{B}_0} \mathfrak{R} \) is a division algebra, contrary to our hypothesis that \( \mathfrak{B} \) splits \( \mathfrak{D} \).

Since \( \mathfrak{S} \) is a normal divisor of \( \mathfrak{G} \) we have \( TS = S^aT \), \( TS = S^aT \). If \( e = 1 \), then the group \( [T] \) is a normal divisor of \( \mathfrak{G} \), and \( \mathfrak{B}_0 \) is cyclic of degree \( p \) over \( \mathfrak{R} \). By Lemmas 5 and 3 the algebra \( \mathfrak{D} \) is cyclic. There remains the case \( e > 1 \).

Now \( T^eS = S^eT \), \( T^eS = S^eT \), \( T^mS = S^{em}T^m = S = S^eS \). Since \( S \) has order \( p \) we have

\[
e^m \equiv 1 \pmod{p}, \quad 0 < e \leq p - 1.
\]

We let \( \nu \) be the least positive integer such that \( e^\nu \equiv 1 \pmod{p} \). Now \( \nu 
eq 1 \), and \( \nu \) must divide both \( p - 1 \) and \( m \). It follows that

\[
m = \nu q, \quad p - 1 = \nu q,
\]

for integers \( \mu \) and \( q \). Notice that the group \( [T] \) is not a normal divisor of \( \mathfrak{G} \), so that \( \mathfrak{B}_0 \) is not a cyclic field over \( \mathfrak{R} \).

By Lemmas 2, 5 the algebra \( \mathfrak{D} \) has a subfield \( \mathfrak{B} \) of degree \( p \) over \( \mathfrak{R} \) equivalent to \( \mathfrak{B}_0 \). Evidently \( \mathfrak{B}_0 \) is equivalent to \( \mathfrak{B}_0 \mathfrak{L} \), and \( \mathfrak{B}_0 = \mathfrak{B}_0 \mathfrak{R} \). But the group of \( \mathfrak{B} \) over \( \mathfrak{L} \) is \( \mathfrak{S} \); \( \mathfrak{B}_0 \) is cyclic of degree \( p \) over \( \mathfrak{L} \) with generating automorphism which we shall designate by \( S \). Moreover if \( z \) is in \( \mathfrak{B}_0 \), the automorphism \( S \) which is given by \( z \mapsto z^a \) goes into \( z^a \mapsto (z^a)^{e^a} = (z^a)^{e^\nu} \) which is the automorphism \( S^e \) of \( \mathfrak{B}_0 \).

By Lemma 3 we have \( \mathfrak{D}_0 = \mathfrak{D} \times \mathfrak{L} = (\mathfrak{B}_0, S, g) \) for \( g \) in \( \mathfrak{L} \). This algebra has the automorphism

\[
d \mapsto d, \quad \lambda \mapsto \lambda^T, \quad d \text{ in } \mathfrak{D}, \quad \lambda \text{ in } \mathfrak{L}.
\]
Apply this automorphism to $\mathfrak{D} \times \mathfrak{S}$ and obtain

$$(4) \quad \mathfrak{D} \times \mathfrak{S} = (\mathfrak{B}_v, S^\ast, g^T).$$

But then it is known that

$$(5) \quad \mathfrak{D} = (\mathfrak{B}_v, S, (g^T)^f) \sim (\mathfrak{B}_v, S, g^T)^f,$$

where $f$ is chosen so that $ef \equiv 1 \pmod{p}$. It follows that

$$(6) \quad \mathfrak{D} \sim (\mathfrak{B}_v, S, g^T)^f, \quad j = 1, 2, \ldots, n.$$

We form $g_0 = g g_T \cdots g^{T(r-1)}$ which is in the cyclic subfield $\Lambda$ of $\mathfrak{S}$ of degree $\nu$ over $\mathfrak{K}$. Now

$$(7) \quad \mathfrak{A} = (\mathfrak{B}_v, S, g) \times (\mathfrak{B}_v, S, g_T^f) \times \cdots \times (\mathfrak{B}_v, S, g^{T(r-1)}) \sim (\mathfrak{B}_v, S, g_0)$$

over $\mathfrak{S}$. But $\mathfrak{A} \sim (\mathfrak{D}_v)^\ast$, where by (6) we have

$$(8) \quad \alpha = 1 + f^r + f^{2r} + \cdots + f^{(r-1)r} \equiv q \pmod{p},$$

since $e^r \equiv 1 \pmod{p}$, $ef \equiv 1 \pmod{p}$, $(ef)^r \equiv f^r \equiv 1 \pmod{p}$. Now $q$ is prime to $p$; hence $qq_0 \equiv 1 \pmod{p}$, and $\mathfrak{A}_q \sim (\mathfrak{B}_v, S, g_0^q) \sim (\mathfrak{D}_v^q) \sim \mathfrak{D}_v$, where $g_0^q$ is in $\Lambda$. It follows that there is no loss of generality if we assume that $g$ is in $\Lambda$. We shall make this assumption.

By (6) we have

$$(9) \quad (\mathfrak{D}_v)^\ast \sim (\mathfrak{B}_v, S, g) \times (\mathfrak{B}_v, S, g_T^f) \times \cdots \times (\mathfrak{B}_v, S, g^{T(r-1)}) \sim (\mathfrak{B}_v, S, \gamma_0),$$

where

$$(10) \quad \gamma_0 = \prod_{k=1}^{r} (g^T)^{f^k}.$$

But then

$$(11) \quad \gamma_0^T = \prod_{k=1}^{r} (g^{T(k+1)})^{f^k}, \quad \gamma_0^\ast = \prod_{k=1}^{r} (g^T)^{f^k}.$$ 

Since $ef \equiv 1 \pmod{p}$ we have

$$(12) \quad \gamma_0^T = \lambda_0^{p^k} \gamma_0^e, \quad \lambda_0 \in \Lambda.$$ 

Now $p \nu_0 \equiv 1 \pmod{p}$ and $(\mathfrak{D}_v)^{p^k} \sim (\mathfrak{D}_v, S, \gamma_1)$, where $\gamma_1 = \gamma_0^\ast$, and

$$(13) \quad \gamma_1^T = \lambda^{p^k} \gamma_1^e, \quad \lambda \in \Lambda.$$ 

Since $\mathfrak{D}_v$ and $(\mathfrak{B}_v, S, \gamma_1)$ have the same order, they are equivalent, and we have proved the following lemma:
**Lemma 6.** The algebra $\mathbb{D}_Q$ has the generation $\mathbb{D}_Q = (\mathbb{F}_Q, S, \gamma)$ where $\gamma_1$ is in $\Lambda$ and (13) holds.

The cyclic algebra $\mathbb{D}_Q$ contains a quantity $y_0$ such that $y_0^p = \gamma_1$, and $\mathbb{L}(y_0)$ is a maximal subfield of $\mathbb{D}_Q$. Hence $\mathbb{L}(y_1) \cong \mathbb{L}(y_0)$ is a scalar splitting field of $\mathbb{D}_Q$. But by (13) we have

$$\gamma_1^{p^j} = \lambda_j \gamma_1^{e^j}, \quad j = 0, 1, \ldots, \nu - 1;$$

and if

$$y = y_1 + \lambda_1 y_1 e + \lambda_2 y_1 e^2 + \cdots + \lambda_{\nu-1} y_1 e^{\nu-1},$$

then $\mathbb{L}(y_1) = \mathbb{L}(y)$. For $0 < e \leq p - 1$, $e^j \equiv e^i \pmod{p}$ if and only if $i - j$ is divisible by $\nu$; $y$ is clearly not in $\mathbb{L}$, and $y$ in $\mathbb{L}(y_1)$ generates $\mathbb{L}(y_1)$. It follows that $\mathbb{L}(y)$ splits $\mathbb{D}_Q$. But $\mathbb{K}$ has characteristic $p$ and

$$\gamma^p = \gamma_1 + \gamma_1^e + \cdots + \gamma_1^{e^{\nu-1}} = \gamma \text{ in } \mathbb{K}.$$

Now $\mathbb{L}(y) = [\mathbb{K}(y)]_y$ and $\mathbb{K}(y)$ splits $\mathbb{D}$ by the proof of Lemma 5. By Lemma 4, $\mathbb{D}$ is a cyclic algebra.

In closing let us note that all of our proof is valid for arbitrary fields except the final result (16), which depends essentially upon the property that $\mathbb{K}$ has characteristic $p$.

---

* Added in proof: When $p = 3$ we may replace (13) by $\gamma_1^p = \gamma_1$, and direct computation shows that if $a$ is in $\mathbb{F}$ with trace zero and norm $a$, and $u = a(1 + y_1 + y_1^e)$, then $u^3 = a(2 + y_1 + y_1^e)$ in $\mathbb{K}$. This proves $\mathbb{D}$ cyclic for any characteristic.