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 $\mathfrak{K}$ are cyclic algebras. It is easily verified that his proof is actually correct for $\mathfrak{K}$ 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 Weddenburn 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 $\mathfrak{K}$ of characteristic p, and let m be prime to p. Then if $\mathfrak{D}$ has a normal splitting field $\mathfrak{W}$ of degree pm over $\mathfrak{K}$, with a cyclic subfield $\mathfrak{L}$ of degree m over $\mathfrak{K}$, 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 $\mathfrak{K}$:

LEMMA 1. *Let $\mathfrak{L}$ have degree prime to n. Then $\mathfrak{D}_{\mathfrak{L}}$ is a division algebra.*

LEMMA 2. *Let $\mathfrak{Z}_0$ have degree n over $\mathfrak{K}$ and split $\mathfrak{D}$. Then $\mathfrak{Z}_0$ 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.

‡ Transactions of this Society, vol. 36 (1934), pp. 388–394.

§ 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 $\mathfrak{K}$ of characteristic not p, Transactions of this Society, vol. 36 (1934), pp. 885–892, and for $\mathfrak{K}$ of characteristic p, ibid., vol. 39 (1936), pp. 183–188.

LEMMA 4. *Let $\mathfrak{D}$ of prime degree $n=p$ over $\mathfrak{K}$ have a splitting field $\mathfrak{Y}=\mathfrak{K}(y)$, such that $y^p=\gamma$ in $\mathfrak{K}$. Then $\mathfrak{D}$ is a cyclic algebra.*

To make our proof we let $\mathfrak{G}$ be the automorphism group of $\mathfrak{W}$ over $\mathfrak{K}$ and $\mathfrak{H}$ the subgroup of $\mathfrak{G}$ corresponding to $\mathfrak{L}$. Then $\mathfrak{H}$ is a normal divisor of $\mathfrak{G}$ and is of prime order p; $\mathfrak{H}=[S]$ is a cyclic group. The group of the cyclic field $\mathfrak{L}$ over $\mathfrak{K}$ is the quotient group $\mathfrak{G}/\mathfrak{H}$ and is a cyclic group $[\mathfrak{H}T]$. Here T is an automorphism of $\mathfrak{G}$ and $T^m=S^\alpha$ in $\mathfrak{H}$. But then $[\mathfrak{H}T^p]=[\mathfrak{H}T]$ since p is prime to m, $(\mathfrak{H}T)^p=\mathfrak{H}T^p$, and $T^{pm}=S^{p\alpha}=I$. Hence we may assume without loss of generality that $T^m=I$. Since $\mathfrak{H}T$ has order m so does T. The cyclic subgroup $\mathfrak{T}=[T]$ of $\mathfrak{G}$ corresponds to a subfield $\mathfrak{Z}_0$ of degree p over $\mathfrak{K}$ of $\mathfrak{W}$, and we have the following lemma:

LEMMA 5. *The field $\mathfrak{Z}_0$ splits $\mathfrak{D}$.*

For clearly $\mathfrak{W}$ is the composite of $\mathfrak{Z}_0$ and $\mathfrak{L}$, and $\mathfrak{W}=(\mathfrak{Z}_0)_{\mathfrak{L}}$. Now $\mathfrak{D}$ has prime degree, and either $\mathfrak{Z}_0$ splits $\mathfrak{D}$ or $\mathfrak{D}_{\mathfrak{Z}_0}$ is a division algebra. In the latter case by Lemma 1 the algebra $(\mathfrak{D}_{\mathfrak{Z}_0})_{\mathfrak{L}}=\mathfrak{D}_{\mathfrak{W}}$ is a division algebra, contrary to our hypothesis that $\mathfrak{W}$ splits $\mathfrak{D}$.

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

Now $T^2S=TS^eT=S^{e^2}T, \cdots, T^mS=S^{e^m}T^m=S=S^{e^m}$. Since S has order p we have

$$e^m \equiv 1 \pmod{p}, \qquad 0 < e \leqq p-1. \tag{1}$$

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

$$m = \nu q, \qquad p-1=\mu\nu \tag{2}$$

for integers μ and q. Notice that the group $[T]$ is not a normal divisor of $\mathfrak{G}$, so that $\mathfrak{Z}_0$ *is not a cyclic field over* $\mathfrak{K}$.

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

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

$$d\longleftrightarrow d,\quad \lambda\longleftrightarrow\lambda^T, \qquad d \text{ in } \mathfrak{D},\ \lambda \text{ in } \mathfrak{L}. \tag{3}$$

Apply this automorphism to $\mathfrak{D}\times\mathfrak{L}$ and obtain

$$\mathfrak{D}\times\mathfrak{L} = (\mathfrak{Z}_{\mathfrak{L}}, S^e, g^T). \tag{4}$$

But then it is known that

$$\mathfrak{D} = (\mathfrak{Z}^{\mathfrak{L}}, S, (g^T)^f) \sim (\mathfrak{Z}_{\mathfrak{L}}, S, g^T)^f, \tag{5}$$

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

$$\mathfrak{D} \sim (\mathfrak{Z}\ , S, g^{T^j})^{f^j}, \qquad j = 1, 2, \cdots, n. \tag{6}$$

We form $g_0 = gg^{T^\nu}\cdots g^{T^{\nu(q-1)}}$ which is in the cyclic subfield Λ of $\mathfrak{L}$ of degree ν over $\mathfrak{K}$. Now

$$\mathfrak{A} = (\mathfrak{Z}_{\mathfrak{L}}, S, g)\times(\mathfrak{Z}_{\mathfrak{L}}, S, g^{T^\nu})\times\cdots\times(\mathfrak{Z}_{\mathfrak{L}}, S, g^{T^{\nu(q-1)}}) \sim (\mathfrak{Z}_{\mathfrak{L}}, S, g_0) \tag{7}$$

over $\mathfrak{L}$. But $\mathfrak{A}\sim(\mathfrak{D}_{\mathfrak{L}})^\alpha$, where by (6) we have

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

since $e^\nu\equiv 1 \pmod p$, $ef\equiv 1 \pmod p$, $(ef)^\nu\equiv f^\nu\equiv 1 \pmod p$. Now q is prime to p; hence $qq_0\equiv 1 \pmod p$, and $\mathfrak{A}^{q_0}\sim(\mathfrak{Z}_{\mathfrak{L}}, S, g_0^{q_0})\sim(\mathfrak{D}^{qq_0})_{\mathfrak{L}}\sim\mathfrak{D}_{\mathfrak{L}}$, where $g_0^{q_0}$ is in Λ. It follows that there is no loss of generality if we assume that g is in Λ. We shall make this assumption.

By (6) we have

$$\begin{aligned}(\mathfrak{D}_{\mathfrak{L}})^\nu \sim (\mathfrak{Z}_{\mathfrak{L}}, S, g)\times(\mathfrak{Z}^{\mathfrak{L}}, S, g^T)^f\times\cdots \\ \times(\mathfrak{Z}_{\mathfrak{L}}, S, g^{T^{\nu-1}})^{f^{\nu-1}} \sim (\mathfrak{Z}_{\mathfrak{L}}, S, \gamma_0),\end{aligned} \tag{9}$$

where

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

But then

$$\gamma_0^T = \prod_{k=1}^{\nu}(g^{T^{k+1}})^{fk},\quad \gamma_0^e = \prod_{k=1}^{\nu}(g^{T^k})^{ef^k}. \tag{11}$$

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

$$\gamma_0^T = \lambda_0^p\gamma_0^e, \qquad \lambda_0 \text{ in } \Lambda. \tag{12}$$

Now $\nu\nu_0\equiv 1 \pmod p$ and $(\mathfrak{D}_{\mathfrak{L}})^{\nu\nu_0}\sim\mathfrak{D}_{\mathfrak{L}}\sim(\mathfrak{Z}_{\mathfrak{L}}, S, \gamma_1)$, where $\gamma_1 = \gamma_0^{\nu_0}$, and (12) implies that

$$\gamma_1^T = \lambda^p\gamma_1^e, \qquad \lambda \text{ in } \Lambda. \tag{13}$$

Since $\mathfrak{D}_{\mathfrak{L}}$ and $(\mathfrak{Z}_{\mathfrak{L}}, S, \gamma_1)$ have the same order, they are equivalent, and we have proved the following lemma:

LEMMA 6. *The algebra* $\mathfrak{D}_{\mathfrak{L}}$ *has the generation* $\mathfrak{D}_{\mathfrak{L}} = (\mathfrak{Z}_{\mathfrak{L}}, S, \gamma)$ *where* γ_1 *is in* Λ *and* (13) *holds.*

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

$$\gamma_1^{T^j} = \lambda_j^p \gamma_1^{e^j}, \qquad j = 0, 1, \cdots, \nu - 1; \tag{14}$$

and if

$$y = y_1 + \lambda_1 y_1^e + \lambda_2 y_1^{e^2} + \cdots + \lambda_{\nu-1} y_1^{e^{\nu-1}}, \tag{15}$$

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

$$y^p = \gamma_1 + \gamma_1^T + \cdots + \gamma_1^{T^{\nu-1}} = \gamma \text{ in } \mathfrak{K}. \tag{16}$$

Now $\mathfrak{L}(y) = [\mathfrak{K}(y)]_{\mathfrak{L}}$, and $\mathfrak{K}(y)$ splits $\mathfrak{D}$ by the proof of Lemma 5. By Lemma 4, $\mathfrak{D}$ 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 $\mathfrak{K}$ has characteristic p.

THE UNIVERSITY OF CHICAGO

---

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