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 are cyclic algebras. It is easily verified that his proof is actually correct for 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 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 of the following theorem:

THEOREM. Let be a normal division algebra of degree over a field of characteristic , and let be prime to . Then if has a normal splitting field of degree over , with a cyclic subfield of degree over , it follows that the algebra is a cyclic algebra.

In our proof we shall use the following known theorems§ on normal division algebras of degree over arbitrary fields :

**Lemma 1.** Let have degree prime to . Then is a division algebra.

**Lemma 2.** Let have degree over and split . Then is equivalent to a (maximal) subfield of .

**Lemma 3.** Let have a cyclic subfield of degree . Then 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 of characteristic not , Transactions of this Society, vol. 36 (1934), pp. 885–892, and for of characteristic , ibid., vol. 39 (1936), pp. 183–188.
Lemma 4. Let $D$ of prime degree $n = p$ over $K$ have a splitting field $Y = K(y)$, such that $y^p = y$ in $K$. Then $D$ is a cyclic algebra.

To make our proof we let $G$ be the automorphism group of $B$ over $K$ and $H$ the subgroup of $G$ corresponding to $L$. Then $H$ is a normal divisor of $G$ and is of prime order $p$; $H = [S]$ is a cyclic group. The group of the cyclic field $S$ over $K$ is the quotient group $G/H$ and is a cyclic group $[ST]$. Here $T$ is an automorphism of $G$ and $T^m = S^e$ in $H$. But then $[ST^p] = [ST]$ since $p$ is prime to $m$, $(ST)^p = ST^p$, and $T^pm = S^{pa} = 1$. Hence we may assume without loss of generality that $T^m = 1$. Since $ST$ has order $m$ so does $T$. The cyclic subgroup $T = [T]$ of $G$ corresponds to a subfield $B_0$ of degree $p$ over $K$ and $B$, and we have the following lemma:

**Lemma 5.** The field $B_0$ splits $D$.

For clearly $B$ is the composite of $B_0$ and $L$, and $B = (B_0)g$. Now $D$ has prime degree, and either $B_0$ splits $D$ or $D_B$ is a division algebra. In the latter case by Lemma 1 the algebra $(D_B)_g = D_B$ is a division algebra, contrary to our hypothesis that $B$ splits $D$.

Since $H$ is a normal divisor of $G$ we have $TH = HT, TS = S^eT$. If $e = 1$, then the group $[T]$ is a normal divisor of $H$, and $B_0$ is cyclic of degree $p$ over $K$. By Lemmas 5 and 3 the algebra $D$ is cyclic. There remains the case $e > 1$.

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

$$e^m \equiv 1 \pmod{p},$$

$$0 < e \leq p - 1.$$

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

$$m = vq, \quad p - 1 = \mu v$$

for integers $\mu$ and $q$. Notice that the group $[T]$ is not a normal divisor of $G$, so that $B_0$ is not a cyclic field over $K$.

By Lemmas 2, 5 the algebra $D$ has a subfield $B$ of degree $p$ over $K$ equivalent to $B_0$. Evidently $B_0$ is equivalent to $B$, and $B_0 = B \times B$. But the group of $B$ over $K$ is $H$; $B_0$ is cyclic of degree $p$ over $K$ with generating automorphism which we shall designate by $S$. Moreover if $z$ is in $B_0$, the automorphism $S$ which is given by $z \longleftrightarrow z^a$ goes into $z^e \longleftrightarrow (z^e)^a = (z^a)^e$ which is the automorphism $S^e$ of $B_0$.

By Lemma 3 we have $D_0 = D \times B = (B_0, S, g)$ for $g$ in $B$. This algebra has the automorphism

$$d \longleftrightarrow d, \quad \lambda \longleftrightarrow \lambda^e, \quad d \text{ in } D, \lambda \text{ in } B.$$
Apply this automorphism to \( \mathfrak{D} \times \mathfrak{I} \) and obtain
\[
(4) \quad \mathfrak{D} \times \mathfrak{I} = (\mathfrak{B}_q, S', g^r).
\]
But then it is known that
\[
(5) \quad \mathfrak{D} = (\mathfrak{B}_q, S, (g^r)^f) \sim (\mathfrak{B}_q, S, g^r)^f,
\]
where \( f \) is chosen so that \( ef \equiv 1 \pmod{p} \). It follows that
\[
(6) \quad \mathfrak{D} \sim (\mathfrak{B}_q, S, g^r)^f^j, \quad j = 1, 2, \ldots, n.
\]

We form \( g_0 = gg^r \cdots g^{r(q-1)} \) which is in the cyclic subfield \( A \) of \( \mathfrak{I} \) of degree \( v \) over \( \mathfrak{I} \). Now
\[
(7) \quad \mathfrak{I} = (\mathfrak{B}_q, S, g) \times (\mathfrak{B}_q, S, g^r) \times \cdots \times (\mathfrak{B}_q, S, g^{r(q-1)}) \sim (\mathfrak{B}_q, S, g_0)
\]
over \( \mathfrak{I} \). But \( \mathfrak{I} \sim (\mathfrak{D}_q)^n \), where by (6) we have
\[
(8) \quad \alpha = 1 + f^r + f^{2r} + \cdots + f^{(q-1)r} \equiv q \pmod{p},
\]
since \( e^r \equiv 1 \pmod{p} \), \( ef \equiv 1 \pmod{p} \), and \((ef)^r \equiv f^r \equiv 1 \pmod{p} \). Now \( q \) is prime to \( p \); hence \( qq_0 \equiv 1 \pmod{p} \), and \( \mathfrak{I} \sim (\mathfrak{B}_q, S, g_0) \sim (\mathfrak{D}_q)^n \sim \mathfrak{D}_q \), where \( g_0 \gamma_0 \) 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
\[
(9) \quad (\mathfrak{D}_q)^r \sim (\mathfrak{B}_q, S, g) \times (\mathfrak{B}_q, S, g^r) \times \cdots \times (\mathfrak{B}_q, S, g^{r-1}) \sim (\mathfrak{B}_q, S, g_0),
\]
where
\[
(10) \quad \gamma_0 = \prod_{k=1}^r (g^r)^f.
\]
But then
\[
(11) \quad \gamma_0^T = \prod_{k=1}^r (g^r)^{f+k}, \quad \gamma_0^e = \prod_{k=1}^r (g^r)^{f+k}.
\]
Since \( ef \equiv 1 \pmod{p} \) we have
\[
(12) \quad \gamma_0^T = \lambda_0 \gamma_0^e, \quad \lambda_0 \text{ in } \Lambda.
\]
Now \( \nu \gamma_0 \equiv 1 \pmod{p} \) and \((\mathfrak{D}_q)^{re} \sim \mathfrak{D}_q \sim (\mathfrak{B}_q, S, \gamma_1) \), where \( \gamma_1 = \gamma_0 \gamma_0^e \), and
(12) implies that
\[
(13) \quad \gamma_1^T = \lambda \gamma_1^e, \quad \lambda \text{ in } \Lambda.
\]
Since \( \mathfrak{D}_q \) and \((\mathfrak{B}_q, S, \gamma_1) \) have the same order, they are equivalent, and we have proved the following lemma:
Lemma 6. The algebra $\mathcal{D}_g$ has the generation $\mathcal{D}_g = (\mathcal{B}_g, S, \gamma)$ where $\gamma_1$ is in $\Lambda$ and (13) holds.

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

$$\gamma_1^{x^j} = \lambda_j y_1^x, \quad j = 0, 1, \cdots, v - 1;$$

and if

$$y = y_1 + \lambda_1 y_1 e^t + \lambda_2 y_1 e^{2t} + \cdots + \lambda_{v-1} y_1 e^{(v-1)t},$$

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

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

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

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