DIHEDRAL ALGEBRAS ARE CYCLIC
LOUIS H. ROWEN¹ AND DAVID J. SALTMAN²,³

ABSTRACT. Any central simple algebra of degree $n$ split by a Galois extension with
dihedral Galois group of degree $2n$ is, in fact, a cyclic algebra. We assume that the
centers of these algebras contain a primitive $n$th root of unity.

In his book [1], Albert has a proof that every division algebra of degree 3 is
cyclic. In this paper we will generalize this result, and derive the theorem below.
Our argument is very close to that of Albert, and arose as part of a close
examination of his proof. Fix $n$ to be an odd positive integer, and $F$ a field of
characteristic prime to $n$. Denote by $D_n$ the dihedral group of order $2n$. We assume
the reader is familiar with the basics of the theory of finite dimensional simple
algebras as presented, for example, in Albert’s book.

Theorem 1. Let $D$ be a simple algebra of degree $n$ with center $F$. Assume $F$
contains a primitive $n$th root of one. Suppose $D$ is split by a Galois extension $L/F$
with Galois group $D_n$. Then $D$ is a cyclic algebra, that is, $D$ is split by a cyclic Galois
extension of degree $n$.

Before beginning the proof of the above theorem, we note that Snider [4] has
already shown that such $D$ are similar (in the Brauer group) to a tensor product of
cyclic algebras.

The group $D_n$ is generated by $o$, $r$ where $o^n = 1$, $r^2 = 1$ and $o r = r o^{-1}$. Given
$L/F$ as in the theorem, we let $K$ denote the fixed field of $o$ in $L$, and $L_0$ the fixed
field of $o$. Clearly $L$ splits $D_0 F K$, which also has degree $n$. Since $L/K$ has degree
2 and $n$ is odd, $D_0 F K$ is already split. That is, $K$ splits $D$. So $K$ can be assumed
to be a subfield of $D$.

Since $L/L_0$ is cyclic, there is an $o ∈ L$ such that $o^n ∈ L_0$ and $o(o) = ρ o$ where
$ρ$ is a primitive $n$th root of one. View $L$ as a subfield of $D_0 F L_0$. Then there is a
unit $β ∈ D_0 F L_0$ such that $oβ = ρ o β$. Let $τ$ act on $D_0 F L_0$ via its action on $L_0$.
This next lemma, essentially in [1, p. 177], is included here because it is not stated
there with the generality we require. For convenience, we provide a proof.

Lemma 2. We may assume $τ(β) = β^{-1}$.

Received by the editors February 17, 1981.
1980 Mathematics Subject Classification. Primary 16A39, 12E15.
Key words and phrases. Central simple algebra, cyclic algebra.
¹The first author is currently on sabbatical at Yale University.
²The second author is grateful for support under a N.S.F. Postdoctoral Fellowship and a Sloan
Foundation Fellowship for Basic Research.
³Both authors would like to thank the Yale Health Plan for its hospitality.
DIHEDRAL ALGEBRAS ARE CYCLIC 163

Proof. Since $a(\tau(a)) = \tau(a)^{-1}a = a^{-1}\tau(a)$, we have $\tau(a) = a\tau(a)^{-1}$, where $a \in L_0$. In fact, since $a = \tau^2(a) = \tau(aa\tau(a)) = \tau(a)a\tau(a)$, we have $\tau(a) = a$ and so $a \in F$.

Let $r = (n + 1)/2$ and set $\beta' = \beta'\tau(\beta)^{-r}$. Compute that $a\beta' = r\beta'\alpha$ and $\tau(\beta') = \beta'^{-r}$. Q.E.D.

With $\beta$ as in Lemma 2, $L_0(\beta)$ is Galois over $F$ with group $D_{2n}$. (If $D$ is not a division algebra, $L_0(\beta)$ may be a direct sum of fields, but this does not affect our argument.) Applying Lemma 2 again (reversing the roles of $\alpha$ and $\beta$), we may also assume $\tau(\alpha) = \alpha^{-1}$. To prove the theorem, it suffices to find $\eta \in D$ such that $0 \neq \eta^n \in F$ and $\eta^m \not\in F$ for $1 < m < n$. That $\eta \in D$ is equivalent to saying $\eta \in D \otimes F L_0$ and $\eta$ is fixed by $1 \otimes \tau$. The key step in finding such an $\eta$ is the following.

Lemma 3. Suppose $c \in K$. Set $\eta = (\beta + \beta^{-1})c$. Denote by $X^n + c_1X^{n-1} + \cdots + c_n$ the characteristic polynomial of $\eta$. Then $c_i = 0$ for all $i$ odd such that $1 < i < n$.

Proof. To start off with, assume $F$ has characteristic 0. If $r$ is odd and $1 < r < n$, then $\eta^r$ is a sum of terms of the form $d\beta^n$ where $d \in L$, $s$ is odd, and $-r < s < r$. Thus $\eta^r$ has reduced trace zero. Using Newton’s identity (e.g. [3, p. 135]), this case of the lemma is done.

To prove the lemma in general, we use a specialization argument, which we only outline. Let $R_1$ be the number ring $Z(\rho)(1/n)$. Set $T$ to be the localized polynomial ring $R_1[x,y,z_1, \ldots , z_n](1/w)$ where $w$ is the $\sigma$ norm of $yx(x^2 - 1)(y^2 - 1)$. Let $D_n$ act on $T$ via $\sigma(x) = \rho x$, $\tau(x) = x^{-1}$, $\sigma(y) = y$, $\tau(y) = y^{-1}$, $\tau(y) = y$, and $\sigma(z_1) = z_i$, and $\sigma(z_1) = z_{i+1}$ (indices modulo $n$). The fixed ring of $D_n$ on $T$ we call $R$, while we let $S$ denote the fixed ring of $\sigma$ on $T$. One can show that $T/R$ is a Galois extension of commutative rings with group $D_n$. $T/R$ is a generic model for $L/F$, with $S$ corresponding to $L_0$, $x$ corresponding to $a$, $y$ corresponding to $\beta^n$, and $z_i$ corresponding to $c_i$.

Form the cyclic Azumaya algebra $A = (T/S, \sigma, y)$, and take $v \in A$ such that $v^n = y$ and $v^{-1}wv = \sigma(a)$ for $a \in T$. Extend $\tau$ to $A$ by setting $\tau(v) = v^{-1}$. Of course, $A$ is a generic model for $D \otimes_F L_0$, with $v$ corresponding to $\beta$.

Consider $\eta' = (v + v^{-1})z_1$. Let $\eta'$ have characteristic polynomial $X^n + d_1X^{n-1} + \cdots + d_n$, where $d_i \in R$. By considering $A \otimes Z Q$, we conclude that $d_i = 0$ if $i$ is odd and less than $n$. Then lemma now follows by specialization. Q.E.D.

To finish the proof of Theorem 1, set $\eta = (\beta + \beta^{-1})(\alpha + \alpha^{-1})^{-1}$, and suppose $X^n + c_1X^{n-1} + \cdots + c_n$ is the characteristic polynomial of $\eta$. We have $c_1 = c_3 = \cdots = c_{n-2} = 0$. We claim $\beta + \beta^{-1}$, and hence $\eta$, can be assumed to be a unit. But $\beta + \beta^{-1}$ has reduced norm $\beta^n + \beta^{-n} \in F$ so it suffices to show that we can assume $\beta^n + \beta^{-n} \neq 0$. But if $\beta^n + \beta^{-n} = 0$ then $(\beta^n)^2 = 1$ so $\beta^n = -1$ and $D$ is a split algebra, a case which is trivial. Now $\eta^{-1} - (\alpha + \alpha^{-1})(\beta + \beta^{-1})^{-1}$ has characteristic polynomial $X^n + (c_{n-1}/c_n)X^{n-1} + \cdots + (1/c_n)$. Lemma 3 also applies to $\eta^{-1}$ by symmetry, $c_{n-1} = c_{n-3} = \cdots = c_2 = 0$. Thus $\eta^n = -c_n \in F$. It is trivial to see that $\eta^m \not\in F$ for $m < n$, and so the theorem is proved.
As a final remark, note that the result corresponding to Theorem 1 for $D_p$ and fields of characteristic $p$ is a consequence of the more general theorem in [2].

REFERENCES