DIHEDRAL ALGEBRAS ARE CYCLIC

PASCAL MAMMONE AND JEAN-PIERRE TIGNOL

Abstract. This note gives a simple proof of the following theorem of Rowen and Saltman: Every central simple algebra split by a Galois extension of rank \(2n\) (\(n\) odd) with dihedral Galois group is cyclic if the center contains a primitive \(n\)th root of unity.

The aim of this note is to provide a short conceptual proof of the following theorem of Rowen and Saltman [3].

**Theorem.** Let \(n\) be an odd (positive) integer and let \(F\) be a field containing a primitive \(n\)th root of unity. Every central simple \(F\)-algebra split by a Galois extension of \(F\) of rank \(2n\) with dihedral Galois group is also split by a cyclic extension of \(F\).

The proof given here only uses basic properties of symbols and of the corestriction map, and can be adapted to the case where \(\text{char } F = n\) (instead of \(F\) containing a primitive \(n\)th root of unity), to yield a particular case of a general theorem of Albert [1].

Henceforth, we fix an odd integer \(n\) and a field \(F\) containing a primitive \(n\)th root of unity, and a Galois extension \(K/F\) with dihedral Galois group generated by two elements \(\sigma, \tau\) subject to the relations:

\[
\sigma^n = 1, \quad \tau^2 = 1, \quad \sigma \tau \sigma = \tau.
\]

Let \(L\) be the fixed field of \(\sigma\) in \(K\).

**Lemma.** There is an element \(a \in L^n\) such that \(K = L(a^{1/n})\) and \(N_{L/F}(a) \in F^{x^n}\).

**Proof.** Since \(K/L\) is cyclic of rank \(n\) and \(L\) contains a primitive \(n\)th root of unity \(\zeta\), one can find \(\alpha \in K\) such that \(K = L(\alpha)\) and \(\sigma(\alpha) = \zeta \alpha\). Applying \(\sigma \tau\) to both sides of this equation yields \(\tau(a) = \zeta \sigma \tau(\alpha)\), and it follows that \(\alpha \tau(\alpha)\) is fixed under \(\sigma\). This element is clearly fixed under \(\tau\) too, so \(\alpha \tau(\alpha) \in F^x\). Denoting \(\alpha^n = a\), we have \(K = L(a^{1/n})\) and \(N_{L/F}(a) = (\alpha \tau(\alpha))^n \in F^{x^n}\), as required. Q.E.D.

**Proof of the Theorem.** Let \(A\) be a central simple \(F\)-algebra split by \(K\). By [2, Theorem 14, p. 68], \(A\) decomposes as \(A_1 \otimes_F A_2\) where the degree of \(A_1\) is a power of 2 and the degree of \(A_2\) is odd. Both \(A_1\) and \(A_2\) are split by \(K\), hence \(A_1\) is split by \(L\), and it suffices to prove that \(A_2\) is split by a cyclic extension of \(F\).
Since the degree of $A_2$ is odd, $A_2$ is similar (in the Brauer group of $F$) to an even power of itself: let $A_2 \sim A_2^{2m}$ for some integer $m$. By [2, Lemma 9, p. 54], $A_2^2 \sim \text{Cor}_{L/F}(A_2 \otimes_F L)$, hence raising both sides to the $m$th power, we get

$$A_2 \sim \text{Cor}_{L/F}(A_2^m \otimes_F L).$$

Now, since $K = L(a^{1/n})$ splits $A_2$, hence also $A_2^n \otimes L$, there exists $b \in L^x$ such that $A_2^n \otimes L$ is similar to the symbol algebra $(a, b)$ of degree $n$ over $L$ (denoted by $(a, b; n, L, \zeta)$ in [2]; see [2, Lemma 1, p. 78]), hence

$$A_2 \sim \text{Cor}_{L/F}(a, b).$$

We complete the proof by showing that the corestriction of $(a, b)$ is a symbol algebra: this readily follows from the “projection formula” [2, Theorem 7, p. 88] if $b \in F$, so we can assume $b \notin F$. (Note that $a \notin F$, or else the lemma would imply $a \in F^{\times n}$, a contradiction.) Since $[L:F] = 2$, one can then find $a', b' \in F$, both nonzero, such that $aa' + bb' = 0$ or 1. Then $(aa', bb') \sim 1$, so that

$$(a, b) \sim (a, b')^{-1} \otimes (a', bb')^{-1}.$$

Taking the corestriction of both sides, we get by the “projection formula”:

$$\text{Cor}_{L/F}(a, b) \sim \left(N_{L/F}(a), b'\right)^{-1} \otimes \left(a', N_{L/F}(bb')\right)^{-1}.$$

The lemma shows that the first factor on the right-hand side is trivial, hence $\text{Cor}_{L/F}(a, b)$ is similar to a symbol algebra. Q.E.D.

**Remark.** This proof can be readily adapted to the case where char $F = n$ (prime), by replacing symbols $(a, b)$ by $n$-symbols $(a, b)$: one first shows that $K = L(a)$ for some $a$ such that $a^2 = a^2 - a \in L$ and $\text{Tr}_{L/F}(a) = a^2 - a$ for some $a \in F$; the same arguments as above then show that it suffices to prove that $\text{Cor}_{L/F}(a, b)$ is a symbol algebra (for any $b \in L$), and this follows from a decomposition:

$$\text{Cor}_{L/F}(a, b) \sim \left[\text{Tr}_{L/F}(a), b'\right] \otimes \left[a', N_{L/F}(b'')\right].$$

**References**


Université de Mons-Hainaut, B-7000 Mons, Belgium
Université Catholique de Louvain, B-1348 Louvain-la-Neuve, Belgium