ISRAEL JOURNAL OF MATHEMATICS 96 (1996), 527–552

# SEMIDIRECT PRODUCT DIVISION ALGEBRAS*

BY

LOUIS H. ROWEN

*Department of Mathematics and Computer Science*
*Bar-Ilan University, Ramat-Gan 52900, Israel*
*e-mail: rowen@macs.biu.ac.il*

AND

DAVID J. SALTMAN

*Department of Mathematics, The University of Texas at Austin*
*Austin, TX 78712, USA*
*e-mail: saltman@math.utexas.edu*

ABSTRACT

Suppose $D$ is a division algebra of degree $p$ over its center $F$, which contains a primitive $p$-root of 1. Also suppose $D$ has a maximal separable subfield over $F$ whose Galois group is the semidirect product of the cyclic groups $C_pC_q$, where $q = 2, 3, 4$, or 6 and is relatively prime to $p$. (In particular this is the case when $p$ is prime $\leq 7$ and $D$ has a maximal separable subfield whose Galois group is solvable.) Then $D$ is cyclic. The proof involves developing a theory of a wider class of algebras, which we call accessible, and proving that they are cyclic.

## Introduction

One of the main open questions in the theory of finite dimensional division algebras is the cyclicity of a division algebra $D$ of prime degree $p \geq 5$. In this paper we consider the following approach to this question. $D$ has a maximal separable subfield $K$. If $E$ is the normal closure of $K$ and $G$ is the Galois group of $E/F$,

* Research supported in part by US–Israel Binational Science Foundation grant #92-00255. The second author is grateful for support under NSF grant DMS-9400650. Also, the authors thank the referee for several very helpful suggestions.
Received May 6, 1995 and in revised form December 11, 1995

then $G$ is a transitive subgroup of $S_n$. Thus, given a group $G$, can one somehow modify $K$ and prove $D$ is cyclic? One positive result is from [RS], in which it was proved (under a few additional hypotheses) that if $G$ is dihedral then $D$ is cyclic. In [Ti2] Tignol shows that if $G = C_5 \rtimes C_4$ then $D$ is cyclic assuming $F$ has a Henselian valuation. We shall prove (assuming $F$ has a primitive $p$-root of 1) the cyclicity of any division algebra having a maximal subfield whose Galois group is a semidirect product of $C_p$ by $C_q$, for $q = 3, 4, 6$ and $p$ relatively prime to $q$. In particular, if $D$ has prime degree $\leq 7$ and has a maximal separable subfield whose splitting field has solvable Galois group then $D$ is cyclic. In the course of our analysis, we will actually study so-called accessible division algebras. In the cases $q = 2, 3, 4, 6$ we will show accessible division algebras are cyclic.

It turns out that there are a variety of methods to achieve our goals. We will purposely use each of these methods for parts of our results. We believe this will maximize the intuition to be derived from our paper. The case $q = 2$ was done in [RS] by explicitly presenting a cyclic maximal subfield. In [MT] the same result was proven by a computation of the corestriction in algebraic K-theory. We do the case $q = 4$ by, essentially, exhibiting a cyclic maximal subfield. We do the cases $q = 3$ and 6 by a K-theory computation. When $F$ contains an algebraically closed field in characteristic 0, we also do the $q = 3$ case as follows. We show that the generic accessible algebra has center the function field of the projective space $\mathbb{P}^2$. We explicitly compute the ramification locus of this algebra, and then apply a result of Tim Ford ([Fo]) to know that the algebra is cyclic.

Throughout this paper $F$ will be a field of characteristic prime to $n$ containing $\rho$, a primitive $n$th root of one. Frequently we will be considering division algebras and properties of maximal subfields. However, when dealing with central simple algebras looking at subfields is insufficient. To remedy this, we make the following definition. Suppose $B/K$ is a central simple algebra of degree $n$. We say $L \subset B$ is a splitting subring if $L \supset K$, $L$ is a direct sum of fields, and $L/K$ has dimension $n$. In a similar vein we will discuss Galois extensions $L/K$ where only $K$ is assumed to be a field, and we note that $L$ is necessarily a direct sum of fields Galois over $K$. Finally, we note that Kummer theory applies to such $L$, and we refer the reader to [S] p. 254 for further details.

## 1. Accessible algebras

Assume $D/F$ is a division algebra of degree $n$, and $q$ is an integer such that the

g.c.d $(n, q) = 1$. Suppose $D$ has a maximal subfield $K$ such that the following holds. There is a field $E \supset K$ such that $E/F$ is Galois, with Galois group the semidirect product $G = C_n \rtimes C_q$.

Let $\sigma$ be a fixed generator of $C_n$. We want to reduce to the case $n$ is a prime power. Suppose $n = n_1 n_2$ where $(n_1, n_2) = 1$. Then $C_n = C_{n_1} \times C_{n_2}$ where the $C_{n_i}$ are cyclic subgroups of order $n_i$. Clearly, the $C_{n_i}$ are $C_q$-invariant. Set $\sigma_{3-i}$ to be a generator of $C_{n_i}$. Let $E_i$ denote the fixed subfield $E^{\sigma_i}$ and $K_i = E_i \cap K$. Then $K = K_1 \otimes_F K_2$ where $[K_i\colon F] = n_i$. Moreover, $E_i/F$ is Galois with group $C_{n_i} \rtimes C_q$. Finally, $D = D_1 \otimes_F D_2$ where each $D_i$ has degree $n_i$. It follows that $K_i$ is isomorphic to a maximal subfield of $D_i$. Clearly, $D$ is cyclic if and only if each $D_i$ is cyclic. Thus we may assume $n = p^m$ is a prime power. Note that we can assume $n$ is odd. In fact, if $n$ is a power of 2, $\phi(n)$ is also a power of 2. Thus any homomorphism $\eta\colon C_q \longrightarrow \mathrm{Aut}(C_n)$ must be trivial because $(n, q) = 1$.

Let $L = E^\sigma$ be the fixed field. By Kummer theory, $E = L(\alpha)$ where $\alpha^n = a \in L^*$ and $\sigma(\alpha) = \rho\alpha$. Take $R$ to be the ring $\mathbb{Z}/n\mathbb{Z}$. Let $\tau$ be a generator of $C_q$. Then $\tau\sigma = \sigma^r\tau$ where $r^q \equiv 1 \bmod (n)$. Note that we may take $r \in R$ and then $\alpha^r$ is well defined $\pmod{(L^*)^n}$, and our condition is that $r^q = 1$ in $R$. Let $t \in R$ be such that $rt = 1$. $L/F$ is cyclic Galois of degree $q$ with Galois group generated by $\tau$. In addition, $E/L$ is cyclic Galois of degree $n$ with Galois group generated by $\sigma$. Since $E = K \otimes_F L$, $E$ is a maximal subfield of $D' = D \otimes_F L$. In particular, $D'$ is a cyclic algebra. By standard theory (e.g. [D], p. 78) there is a $\beta \in D'$ such that $\beta\alpha = \rho\alpha\beta$ and $\beta^n = b \in L^*$. We write $D' = (a, b)_{L,n}$ and call $D'$ a symbol algebra. We will omit the subscripts $L$ and $n$ when no ambiguity arises. Since $D'$ is a division algebra, $a$ and $b$ must have order $n$ modulo $(L^*)^n$. Finally, $\tau$ acts as $1 \otimes \tau$ on $D' = D \otimes_F L$ and this action extends the action on $E$.

The fact that $E/F$ is $G$-Galois puts significant restrictions on $a$. To be precise, we compute $\sigma(\tau(\alpha)) = \tau\sigma^t(\alpha) = \tau(\rho^t\alpha) = \rho^t\tau(\alpha)$. It follows that $\tau(\alpha) = \alpha^t z$ where $z \in L^*$. Taking $n$th powers we have

$$\tau(a) = a^t z^n. \tag{1}$$

By (1), the subgroup of $L^*/(L^*)^n$ generated by the image of $a$ is a certain $R[C_q]$-module. To explain this, it is useful to change notation and add some definitions. The multiplicative group $A = L^*/(L^*)^n$ can be viewed as a module over the group ring $R[C_q]$, if we write the operation of $A$ additively (which we shall do whenever possible). Suppose $S \supset R$ is a commutative ring and $\theta \in S$

satisfies $\theta^q = 1$. Let $S_\theta$ be the following module over the group ring $S[C_q]$. As an $S$ module $S_\theta = S$, but the action of $\tau$ is defined by $\tau(s) = \theta s$ for all $s \in S$. The discussion above says precisely that $Ra \subset A$ is an $R[C_q]$-module which is an image of $R_t$.

Let us record some easy facts about $A$ and modules over $S$. In the result to follow, let $A \wedge A$ be the wedge product as abelian groups with the diagonal $C_q$ action. If $\alpha \in A \wedge A$, we say $\alpha$ is **simple** if $\alpha$ has order $n$ and can be written $\alpha = a \wedge b$ for $a, b \in A$. We will say a module over $R[C_q]$ has rank $m$ if it is projective and has $R$-rank $m$.

PROPOSITION 1.1: *Assume $S \supset R$ is a local ring which is finitely generated and free as an $R$-module. Let $n$ be a power of the prime $p$.*

(i) *$A$ (as defined above) is a free $R$-module.*

(ii) *Suppose $M$ is a module over $S[C_q]$ which is free over $S$. Then $M$ is projective over $S[C_q]$. In particular, the modules $S_\theta$ are projective.*

(iii) *If $M$ is a free $R$- or $R[C_q]$-submodule of $A$, then $M$ is a direct summand as an $R$- or $R[C_q]$-module respectively.*

(iv) *The modules $S_\theta$ are indecomposable.*

(v) *The Krull–Schmidt Theorem applies to modules over $S[C_q]$.*

(vi) *If $S^*$ contains $\mu_q$, a cyclic group of order $q$, then $S[C_q] \cong \bigoplus_{\theta \in \mu_q} S_\theta$.*

(vii) *If $S$ is as in* (vi), *and $M$ is an $S[C_q]$ module that is free over $S$, then $M$ is a direct sum of $S_\theta$'s for various $\theta$'s.*

(viii) *There is a one to one correspondence between isomorphism classes of indecomposable finitely generated projective $R[C_q]$ modules and irreducible $R/pR[C_q]$ modules. The correspondence is given by $P \longrightarrow P/pP$.*

(ix) *There is a one to one correspondence between $R$-submodules $R\alpha \subset A \wedge A$ generated by simple $\alpha$ and rank 2 free $R$ submodules $M \subset A$ such that if $M$ has basis $a, b$ then we can take $\alpha = a \wedge b$. $M$ is a $R[C_q]$ module if and only if $R\alpha$ is.*

*Proof:* We begin with (i). A minimal generating set for $A$ is the inverse image of an $R/pR$ basis for $A/pA$. It suffices, then, to show that any element of $A$ of order $< n$ lies in $pA$. To perform this we have to look at $L^*$ and use multiplicative notation. Suppose $x \in L^*$ has order $m < n$ modulo $(L^*)^n$. Then $x^m = y^n$ for $y \in L^*$. Thus $x = \rho' y^{(n/m)}$ where $\rho'$ is an $m$ root of one. It follows that $\rho' = (\rho)^r$ where $r$ is a multiple of $(n/m)$. Thus $x = (y')^{n/m}$ for some $y' \in L^*$. Since $n$ is a

$p$ power, part (i) is proven.

Since $q$ is invertible in $S$, $S[C_q]$ is separable as an algebra over $S$. Part (ii) follows from [DI] p. 48. Part (iii) follows because $R$ is self injective, and because $A/M$ being $R$ projective implies it is $R[C_q]$ projective. Because $S$ is local, $S_\theta$ is indecomposable over $S$ and hence over $S[C_q]$. This is (iv). Since $S[C_q]$ is Artinian, Krull–Schmidt applies (which is (v)).

Let $J$ be the Jacobson radical of $S$, so $J$ is nilpotent. The map $S^* \longrightarrow (S/J)^*$ is therefore an isomorphism on subgroups of each side of order prime to $p$. Also, Hensel's lemma (or equivalently, lifting idempotents) shows that $x^q - 1$ has $q$ roots in $S$ which, of course, must be the elements of $\mu_q$. Thus $x^q - 1 = \Pi_{\theta \in \mu_q}(x - \theta)$. Now $S[C_q] \cong S[x]/(x^q - 1)$ and $x - \theta$ are mutually relatively prime and so (vi) follows. Part (vii) is a direct result of (v) and (vi).

Part (viii) is standard, so we only outline the argument. If $P$ is indecomposable and $R[C_q]$ projective then lifting idempotents shows that $\mathrm{End}_{R[C_q]}(P)$ is local and $P/pP$ is irreducible. If $\phi$: $P/pP \cong Q/qQ$ is an isomorphism for $P, Q$ finitely generated projective $R[C_q]$ modules, then $\phi$ lifts to $\phi'$: $P \longrightarrow Q$ which must be an isomorphism because it has an invertible determinant.

Finally, the first sentence of part (ix) is easy and well known. The second sentence follows from the first. ∎

Let us return to the fields and division algebras $D/F$, $K/F$, $E/F$, $L/F$ and $D' = D \otimes_F L$ we started with. We have written $D' = (a, b)_n$ and we have obtained some information about $a$. We claim there is a symmetric statement about $b$.

LEMMA 1.2: *We can write $D' = (a, b)_n$, in such a manner that $a$ generates a submodule of $A$ isomorphic to an image of $R_t$ and $b$ generates a submodule of $A$ isomorphic to an image of $R_r$.*

*Proof:* We fix $a$ as above. Then $b$ is determined in $L^*$ up to an element from the norm group $N_{E/L}(E^*)$. Let $\bar{b}$ be the image of $b$ in $L^*/N_{E/L}(E^*)$. Now

$$[(a, b)_n] = [D'] = \tau([D']) = [(\tau(a), \tau(b))_n] = [(a^t, \tau(b))_n].$$

Since $[(a, b)_n] = [(a^t, b^r)_n]$ we have that $\tau(b)/b^r \in N_{E/L}(E^*)$. In other words, there is an $R[C_q]$-homomorphism $R_r \longrightarrow L^*/N_{E/L}(E^*)$ taking 1 to $\bar{b}$. The lemma follows because $R_r$ is indecomposable projective. ∎

The above description of $D'$ can be improved and generalized. To make the generalization, consider the pairing $A \times A \longrightarrow \mathrm{Br}(L)$ which takes the pair $(c, d)$

to the class $[(c,d)_n]$. This is a skew pairing and so defines a $R[C_q]$-module map $\phi$: $A \wedge A \longrightarrow \mathrm{Br}(L)$. Let $a, b$ be as in 1.2. Then $a \wedge b$ is $C_q$-invariant and $\phi(a \wedge b) = [D']$.

With the example of $D$ in mind, let us make the following definition. Suppose $D/F$ is a central simple algebra of degree $n$. We say $D$ is $q$-**accessible** if there is a $C_q$-Galois extension $L/F$ such that $[D \otimes_F L]$ is the image under $\phi$ of a $C_q$-invariant simple element $\alpha$ of $A \wedge A$. By 1.1 (ix), $\alpha$ defines a rank 2 $R[C_q]$-submodule $M \subset A$. Since clearly $M \wedge M \cong R\alpha$, the following definition makes sense. If $M$ is a rank 2 $R[C_q]$-module, we say $M$ is **accessible** if and only if $M \wedge M$ has trivial $C_q$ action. Of course, rank 2 accessible $R[C_q]$-submodules of $A$ are precisely the ones which correspond to simple $C_q$-fixed elements of $A \wedge A$.

Note that we assume above in the definition of accessibility that $[D \otimes_F L]$ is the image of an element of $A \wedge A$ of order $n$. This convenience will not lessen the generality of our results, because of the following observation. Suppose $[D \otimes_F L]$ is the image of $a \wedge b \in (A \wedge A)^{C_q}$ of order $p^r < n$. Let $p^s = n/p^r$. Since $A$ is $R$-free, we can assume $a$ has order $n$ (since if $p^i$ divides $a$ we can move $p^i$ over to the right side) and $b = p^s b'$ where $a, b'$ are linearly independent. Set $A' = A/p^r A$ and $\alpha' \in A' \wedge A'$ the image of $a \wedge b'$. Then $\alpha'$ is $\tau$ fixed and defines a rank 2 $(R/p^r R)[C_q]$-submodule $M' \subset A'$. It follows from 1.1 (viii) that $M' = M/p^r M$ where $M$ is a rank 2 projective $R[C_q]$ module. The embedding $M' \subset A'$ lifts to a map $M \longrightarrow A$ which must be an injection. Let $\alpha \in A \wedge A$ correspond to $M$. Then we can assume (after adjusting by a unit of $R$) that $\alpha' = \alpha + p^r(A \wedge A)$, and so $p^s \alpha = a \wedge b$. Since $M' \wedge M'$ has trivial $C_q$ action so does $M \wedge M$ and $\alpha$ is $C_q$-fixed. Using the argument of 1.3 below, it follows that $[D] = (n/m)[D']$ where $D'/F$ has degree $n$, and $D' \otimes_F L$ is the image of $\alpha$. (Note that if the original $D$ was a division algebra, then $a \wedge b$ must have order $n$ because such a $D$ cannot be an $p^s$ power of a degree $n$ algebra unless $p^s = 1$.)

Thus if $D$ is $q$-accessible, there is an associated accessible $M \subset A$. This association is far from unique because the map $A \wedge A \longrightarrow \mathrm{Br}(L)$ is not injective. However, if $D$ is associated to $M$ with respect to any embedding $M \longrightarrow L^*/(L^*)^n$, we say $D$ is $(q, M)$-accessible.

It is important to see that there is a converse to the above discussion. Assume $L/F$ is $C_q$-Galois. Suppose $M$ is an accessible $R[C_q]$-module and there is an inclusion of $C_q$-modules $M \subset A = L^*/(L^*)^n$. Let $\alpha \in A \wedge A$ be a simple element defining $M$.

THEOREM 1.3: *There is a $(q, M)$-accessible central simple $D/F$ of degree $n$ such that $[D' \otimes_F L]$ is the image of $\alpha$ under $A \wedge A \longrightarrow \mathrm{Br}(L)$. $D$ is unique up to choice of $\alpha$, and changing $\alpha$ changes $D$ by a prime-to-$n$ power in $\mathrm{Br}(F)$.*

*Proof:* Let $[D']$ be the image of $\alpha$ in $\mathrm{Br}(L)$, where $D'/L$ has degree $n$. That is, $D' = (c, d)_n$ where $c \wedge d = \alpha$. Since $\alpha$ is $C_q$-invariant, so is $[D']$. It is well known that this implies $[D']$ is in the image of $\mathrm{Br}(F)$, but a reference is hard to find, so we supply a proof.

From Hilbert's theorem 90 and the Hochschild–Serre spectral sequence we have the exact sequence:

$$0 \longrightarrow H^2(C_q, L^*) \longrightarrow \mathrm{Br}(F) \longrightarrow \mathrm{Br}(L)^{C_q} \longrightarrow H^3(C_q, L^*)$$

and the claim follows since $H^3(C_q, L^*) = H^1(C_q, L^*) = 0$.

Let $[D']$ be the image of some $[A] \in \mathrm{Br}(F)$. Since $D'$ has degree $n$, we can choose a representative $A$ of degree $nq$. Write $A = A_1 \otimes A_2$ where $A_1$ has degree $n$ and $A_2$ has degree $q$. Then $[A_1 \otimes_F L] = [D']$ and so $A_1 \otimes_F L \cong D'$. We can set $D = A_1$. Since $q$ is prime to $n$, $D$ is unique in the Brauer group and hence is unique. If we change $\alpha$, we change $D'$ by a power prime to $n$, and so change $D$ by the same power. ∎

We have observed above that if a division algebra $D$ has a maximal subfield in a $C_n \rtimes C_q$ Galois extension, then $D$ is $q$-accessible. The case when $D$ is only central simple is essentially identical. The next result shows that the converse holds when $C_n$ has enough automorphisms.

PROPOSITION 1.4: *Suppose $n$ is a prime power $p^m$, and $q$ divides $p - 1$. Let $D/F$ be a central simple algebra of degree $n$. Then $D$ is $q$-accessible if and only if $D$ has a splitting subring $K$, with $K \subset E$ and $E/F$ Galois with group of the form $C_n \rtimes C_q$.*

*Proof:* We need to show that if $D$ is $q$-accessible, then it has the required $K$. Suppose $L/F$ is $C_q$-Galois and $M \subset A = L^*/(L^*)^n$ is an associated accessible module. Let $\alpha \in A \wedge A$ be a simple element defining $M$, where $D' = D \otimes_F L$ is the image of $\alpha$. By 1.1 (vii), $M \cong R_\theta \oplus R_{\theta'}$ for some $\theta$, $\theta'$ which are $q$-roots of 1. If $a$ generates $R_\theta$ and $b$ generates $R_{\theta'}$, then $(a \wedge b)$ generates $M \wedge M$. By changing $b$ by a unit in $R$, we may assume $a \wedge b = \alpha$ and so $D' \cong (a, b)_n$. $D'$ has a maximal commutative subring $E$ generated over $L$ by $\alpha$ where $\alpha^n = a$. Then

$E/F$ is Galois with group $C_n \rtimes C_q$ and $K$ is the fixed subring of $C_q$. Note for future use that since $\alpha$ is $C_q$-fixed, $a \wedge b$ is $C_q$-fixed and $\theta\theta' = 1$. ∎

It can happen that there are $q$-accessible $D$ without the added condition $q|(p-1)$. The question comes down to finding for which $n$ and $q$ there are accessible $M$. We answer this in the next result. To state the result let us make the following definitions.

As usual, let $n$ be a prime power $p^m$, and $R = \mathbb{Z}/n\mathbb{Z}$. Assume $q$ is prime to $p$. Set $\bar{R} = R/pR$, a finite field, and $\bar{\theta}$ a primitive $q$-root of 1 over $\bar{R}$. Let $\bar{S} = \bar{R}(\bar{\theta})$ be the field extension generated by $\theta$. Since $pR$ is nilpotent, there is a unique Galois $S/R$ such that $S/pS = \bar{S}$. By Hensel's lemma, there is a $\theta \in S$ which is a preimage of $\bar{\theta}$ and such that $\theta^q = 1$. Of course, $\bar{S}/\bar{R}$ is cyclic Galois with Galois group generated by the Frobenius map. Thus $S/R$ is cyclic Galois with Galois group generated by $\eta$ where $\eta(s) \in s^p + pS$ for all $s \in S$. Since the group generated by $\theta$ maps isomorphically to $\bar{S}^*$, we have that $\eta(\theta) = \theta^p$.

We say a $C_q$-module is **faithful** is there is no nontrivial subgroup of $C_q$ which acts trivially on $M$.

PROPOSITION 1.5: *Let $n = p^m$ be an odd prime power, and take $q$ prime to $p$. The following are equivalent.*

(a) *There is an accessible $R[C_q]$-module $M$ which is faithful over $C_q$.*

(b) *$q|(p-1)$ or $q|(p+1)$.*

*Proof:* Assume (b). If $q|(p-1)$, then $S = R$ and we are done. If not, the Galois group of $S/R$ must be of order 2. Let $\eta$ be as above. $\eta$ also generates the Galois group of $S[C_q]/R[C_q]$. Let $\theta \in S^*$ be as above. By assumption $\eta(\theta) = \theta^{-1}$. Let $M' = S_\theta \oplus S_{\theta^{-1}}$. It is clear that there is a $\eta$-semilinear automorphism of $M'$ defined by $\eta'(s_1, s_2) = (s_2, s_1)$. If $M$ is the set of $\eta'$-fixed elements of $M'$, then by Galois descent $M$ is a rank 2 module over $R[C_q]$.

Let $a_1, a_2$ be generators of $S_\theta$ and $S_{\theta^{-1}}$ respectively. Then $\alpha = a_1 \wedge a_2 \in M' \wedge_S M'$ is $C_q$-fixed. Since $(M \wedge M) \otimes_R S = M' \wedge_S M'$ it follows that any simple generator of $M \wedge M$ is $C_q$-fixed. Since $M'$ is faithful it is clear that $M$ is faithful and (a) is proved.

Conversely, assume (a). Set $M' = M \otimes_R S$ which by 1.1 (vii) has the form $S_\delta \oplus S_\theta$. Since any element of $M \wedge M$ is $C_q$-fixed, the same is true of $M' \wedge_S M' = (M \wedge M) \otimes_R S$. Thus $\theta = \delta^{-1}$. That is, we can write $M' = S_\theta \oplus S_{\theta^{-1}}$. Let $\eta'$ be the $\eta$ semilinear automorphism of $M'$ given by Galois descent. By Krull–Schmidt

it is clear that $\eta'(S_\theta) = S_\theta$ or $S_{\theta^{-1}}$ and so $\eta(\theta) = \theta$ or $\theta^{-1}$. Since $M$ is faithful, $\theta$ must be a primitive $q$-root of 1. In the first case $q|(p-1)$ and in the second case $q|(p+1)$. ∎

For each accessible $M$ we would like to write down generic $(q, M)$-accessible $D$. To understand this, we must consider which $C_q$-modules in $L^*$ give rise to $M \subset L^*/(L^*)^n$. In this regard the following theorem is crucial.

THEOREM 1.6: *Suppose we are given a $\mathbb{Z}[C_q]$-module $P$ which is $\mathbb{Z}$-free, with a morphism $P \longrightarrow M$. Suppose $L/F$ is $C_q$-Galois and $M \longrightarrow L^*/(L^*)^n$ is a $C_q$-morphism. Then*

(a) *There is a $C_q$-morphism $f\colon P \longrightarrow L^*$ such that the diagram*

$$\begin{array}{ccc} P & \xrightarrow{f} & L^* \\ \downarrow & & \downarrow \\ M & \longrightarrow & L^*/(L^*)^n \end{array}$$

*commutes.*

(b) *If we fix $f = f_0$ as above, the full set of choices of $f$ is precisely the set of $f_0 g\colon P \longrightarrow L^*$, where $g\colon P \longrightarrow (L^*)^n$ is an arbitrary $C_q$-morphism. (Here we mean the pointwise product.)*

*Proof:* Part (b) is clear. To prove (a), note that by composition we have a map

$$\bar{f}\colon P \longrightarrow L^*/(L^*)^n.$$

The multiplication by $n$ map on $L^*$ has kernel $\mu_n$, the subgroup of order $n$. Thus we have an exact sequence

$$0 \longrightarrow L^*/\mu_n \xrightarrow{n} L^* \longrightarrow L^*/(L^*)^n \longrightarrow 0$$

which defines a long exact sequence which includes:

$$\mathrm{Hom}_{C_q}(P, L^*) \longrightarrow \mathrm{Hom}_{C_q}(P, L^*/(L^*)^n) \longrightarrow \mathrm{Ext}_{C_q}(P, L^*/\mu_n) \longrightarrow \mathrm{Ext}_{C_q}(P, L^*).$$

It suffices to show that $\bar{f}$ has image 0 in $\mathrm{Ext}_{C_q}(P, L^*/\mu_n)$. The $n$ power map $L^* \longrightarrow L^*$ induces the multiplication by $n$ map $\mathrm{Ext}_{C_q}(P, L^*) \longrightarrow \mathrm{Ext}_{C_q}(P, L^*)$, which factors as

$$\mathrm{Ext}_{C_q}(P, L^*) \xrightarrow{g_1} \mathrm{Ext}_{C_q}(P, L^*/\mu_n) \xrightarrow{g_2} \mathrm{Ext}_{C_q}(P, L^*).$$

Since $P$ is $\mathbb{Z}$-free we have (e.g. [B] p. 61) that

$$\mathrm{Ext}_{C_q}(P, L^*) = H^1(C_q, \mathrm{Hom}(P, L^*)),$$

which is annihilated by $q$. Thus the map $g_2 \circ g_1$, which is given by multiplication by $n$, is an isomorphism.

Since $g_2(\bar{f}) = 0$ in $\mathrm{Ext}_{C_q}(P, L^*)$ it suffices to show $g_2$ is injective, which will follow if $g_1$ is surjective. We have the exact sequence

$$\mathrm{Ext}_{C_q}(P, L^*) \xrightarrow{g_1} \mathrm{Ext}_{C_q}(P, L^*/\mu_n) \longrightarrow \mathrm{Ext}^2_{C_q}(P, \mu_n)$$

and so it suffices to show that $\mathrm{Ext}^2_{C_q}(P, \mu_n) = 0$. By [B] p. 61 again this group is equal to $H^2(C_q, \mathrm{Hom}(P, \mu_n))$ which is annihilated by both $n$ and $q$. ∎

For the moment let $P$ be an arbitrary finitely generated $\mathbb{Z}$-free module over $\mathbb{Z}[C_q]$. We call such a $P$ a $C_q$-lattice. Let $F[P]$ be the group algebra, which is also a commutative domain. $F[P]$ has a natural action by $C_q$. If $L/K$ is $C_q$-Galois, then any $C_q$-morphism $f\colon P \longrightarrow L^*$ induces a $C_q$-invariant algebra morphism $\psi_f\colon F[P] \longrightarrow L$. With part (b) above in mind, we are interested in the class of all maps $\psi_{fg}$ where $g\colon P \longrightarrow L^*$ is a $C_q$-morphism with image in $(L^*)^n$. We show that the set of all such $\psi_{fg}$'s is "dense".

THEOREM 1.7: *Suppose $L/K$ is $C_q$-Galois and $f\colon P \longrightarrow L^*$ is a $C_q$-morphism. Assume $0 \neq s \in F[P]$. Then there is a $C_q$-morphism $g\colon P \longrightarrow L^*$ such that $g(P) \subset (L^*)^n$ and $\psi_{fg}(s) \neq 0$.*

*Proof:* Consider the group ring $L[P]$. $C_q$ acts naturally on this ring by acting on both $P$ and $L$. Given any $C_q$-morphism $h\colon P \longrightarrow L^*$, there is a natural unique extension to an $L$-algebra $C_q$-invariant $\phi_h\colon L[P] \longrightarrow L$. Since $F[P] \subset L[P]$, it suffices to show:

LEMMA 1.8: *Suppose $0 \neq s \in L[P]$. There is a $C_q$-morphism $g\colon P \longrightarrow (L^*)^n \subset L^*$ such that $\phi_{fg}(s) \neq 0$.*

Recall that a permutation $C_q$-lattice is a $C_q$-lattice with $\mathbb{Z}$ basis that is permuted by $C_q$. By [CTS] p. 181 and p. 184 there is an exact sequence $0 \longrightarrow P \longrightarrow Q \longrightarrow I \longrightarrow 0$ of $C_q$-lattices such that $Q$ is a permutation lattice and $I$ is a direct summand of a permutation lattice. It follows that $\mathrm{Ext}_{C_q}(I, L^*)$ is a direct summand of a sum of cohomology groups of the form $H^1(H, L^*)$ where $H \subset C_q$.

That is, $\mathrm{Ext}_{C_q}(I, L^*) = 0$. We conclude that $f$ extends to an $f'\colon Q \longrightarrow L^*$. But now it suffices to prove 1.8 for $Q$. That is, we may assume $P$ is a permutation lattice.

Write $P = P' \oplus \mathbb{Z}[C_q/H]$ for $P'$ a permutation lattice of smaller rank. We can write $L[P] = L[P'][\mathbb{Z}[C_q/H]]$. Write $s = \sum s_i m_i$ where $s_i \in L[P'] \subset L[P]$ and $m_i$ are in the image of $\mathbb{Z}[C_q/H]$. Let $f'\colon P' \longrightarrow L^*$ be the restriction of $f$. By induction on the rank of $P$, there is a $g'\colon P' \longrightarrow (L^*)^n \subset L^*$ such that $\phi_{f'g'}(s_i) \neq 0$ for some $i$. $\phi_{f'g'}$ induces $\phi'_{f'g'}\colon L[P][\mathbb{Z}[C_q/H]] \longrightarrow L[\mathbb{Z}[C_q/H]]$ such that $\phi_{f'g'}(s) = s' \in L[\mathbb{Z}[C_q/H]]$ is nonzero. If $f''\colon \mathbb{Z}[C_q/H] \longrightarrow L^*$ is the restriction of $f$, it suffices to find a $g''\colon \mathbb{Z}[C_q/H] \longrightarrow (L^*)^n \subset L^*$ such that $\phi_{f''g''}(s') \neq 0$. In other words we may assume $P = \mathbb{Z}[C_q/H]$.

In other language, $L[P]$ is the Laurent polynomial ring $L[x_{gH}, x_{gH}^{-1}\colon gH \in C_q/H]$, where $C_q$ acts on the $x_{gH}$'s via $g'(x_{gH}) = x_{g'gH}$. Then $s = \sum a_i m_i$ where $a_i \in L$ and the $m_i$ are monomials in the $x_{gH}$'s. Write $0 \neq b_i = f(m_i)$. Then it suffices to find $g\colon P \longrightarrow (L^*)^n \subset L^*$ such that $\sum a_i b_i g(m_i) \neq 0$. To do this it suffices to find $h\colon P \longrightarrow L^*$ such that $\sum a_i b_i h(m_i^n) \neq 0$, and then set $g = h^n$. Finally, it suffices to show:

LEMMA 1.9: *Suppose $s \in L[P]$ is nonzero. Then there is a $C_q$-morphism $h\colon P \longrightarrow L^*$ such that $\phi(h)(s) \neq 0$.*

*Proof:* We can view $P \subset \mathbb{Z}[C_q]$ and so reduce to the case $P = \mathbb{Z}[C_q]$. Now the lemma is just the "algebraic independence of the Galois group elements" which is proven in, for example, [BAI] p. 283. Thus 1.9, 1.8 and hence 1.7 are proven. ∎

We can now construct a generic $(q, M)$-accessible algebra. Let $M$ be an accessible $R[C_q]$-module and $P \longrightarrow M$ a surjective $C_q$-morphism, where $P$ is a finitely generated $\mathbb{Z}$-free $\mathbb{Z}[C_q]$-module. Form the group algebra $F[P]$ with field of fractions $F(P)$. The group $C_q$ acts on these rings and we set $T = F[P]^{C_q}$ and $K = F(P)^{C_q}$ to be the fixed ring and field.

THEOREM 1.10: *Let $n = p^m$ be an odd prime power and $q$ such that $(n, q) = 1$. There is a division algebra $D/K$ of degree $n$ which is generic for the class of all $(q, M)$-accessible algebras centrally containing $F$. That is, there is a $0 \neq s \in T$ and an Azumaya $B/T'$ where $T' = T(1/s)$ such that the following holds:*

(a) $B \otimes_{T'} K = D$.

(b) *Suppose $E/K'$ is $(q,M)$-accessible, $F \subset K$, and $0 \neq t \in T$. Then there is an $F$-map $\phi\colon T' \longrightarrow K'$ such that $B \otimes_\phi K'$ is a prime to $n$ power of $E$ and $\phi(t) \neq 0$.*

*Proof:* Set $L = F(P)$, so $L/K$ is $C_q$-Galois. There is a natural inclusion $P/nP \subset A = L^*/(L^*)^n$. By 1.1 (iii), $M$ is a direct summand of $P/nP$ and so there is an inclusion $M \subset A$. Let $\alpha \in A \wedge A$ be the simple $C_q$-invariant element given by $M$ and $D/K$ the $(q,M)$-accessible algebra given by 1.3. $D$ is a division algebra because $D \otimes_K F(P)$ has the form $(x,y)_n$ where $x, y$ are part of a basis of $P$ and hence a transcendence basis for $F(P)$. Thus $(x,y)_n$ is a division algebra, which implies $D$ is also because $q$ is prime to $n$. By the proof of e.g. [OS] p.136 or [KO] p. 97 there is a $T'$ as above and an Azumaya algebra $B/T'$ such that (a) holds.

Suppose $E/K'$ is $(q,M)$-accessible, with respect to the $C_q$-Galois extension $L'/K'$. Then $E \otimes_{K'} L'$ is defined by $M \subset A' = L'^*/(L'^*)^n$. There is an induced map $P \longrightarrow A'$. Let $f\colon P \longrightarrow L'^*$ be a $C_q$-morphism given by 1.6. Using 1.7, we can assume that $\psi_f(st) \neq 0$, and so $\psi_f$ defines a $C_q$-invariant algebra morphism $\psi\colon F[P](1/s) \longrightarrow L'$ such that $\psi(t) \neq 0$. Let $\phi\colon T' \longrightarrow K'$ be the restriction of $\psi$ and set $E' = B \otimes_\phi K'$. It suffices to show that $E'$ is a prime to $n$ power of $E$. It suffices by 1.3 to show that $E'$ is associated to $M \subset A'$. That is, that $E' \otimes_{K'} L'$ is the image of a generator of $M \wedge M \subset A' \wedge A'$. Set $A = L^*/(L^*)^n$ and $\alpha \in M \wedge M \subset A \wedge A$ the element with image $[D \otimes_K L]$ in $\mathrm{Br}(L)$. Write $\alpha = a \wedge b$. Since $M$ is a submodule of $P/nP$, we can view $a, b$ as elements of $P$. We can then define the Azumaya symbol algebra $B' = (a,b)_n$ with center $F[P]$. Clearly $[B']$ is a preimage of $[D' \otimes_K L]$ under the natural map $\mathrm{Br}(F[P]) \longrightarrow \mathrm{Br}(L)$. But this map is injective (e.g. [Mi] p.145), so $B' \otimes_{F[P]} F[P](1/s)$ and $B \otimes_{T'} F[P](1/s)$ are equal in the Brauer group of $F[P](1/s)$. Since $M \longrightarrow P/nP \longrightarrow M$ is the identity, and since $E' \otimes_{K'} L' = (B \otimes_{T'} F[P](1/s)) \otimes_\psi L'$, it follows that $E' \otimes_{K'} L'$ is the image of $\alpha$, which is what we needed to prove. ∎

The generic algebra above is useful because of the following easy fact.

COROLLARY 1.11: *Suppose $D/K$ from 1.10 is cyclic. If $E'/K'$ is $(q,M)$ accessible, and $K' \supset F$, then $E'$ is cyclic.*

*Proof:* Write $D$ to be the cyclic algebra $\Delta(L'/K, \eta, z)$. By e.g. [S2] p. 528 there is a $t' \in T$ and a cyclic extension $V/T(1/t')$ such that as cyclic extensions $L = V \otimes_{T(1/t')} K$. Write $z = t''/t$ where $t, t'' \in T$. By changing $t'$ to $st'tt''$, we may assume that $z$ is invertible in $T'' = T(1/t') \supset T'$. Then $D \cong K \otimes_{T(1/t')} B'$

where $B' = \Delta(V/T'', \eta, z)$. Since $B \otimes_{T'} K \cong B' \otimes_{T''} K$, there is a $r \in T$ such that $B \otimes_{T'} T''(1/r) \cong B' \otimes_{T''} T''(1/r)$. By replacing $r$ with $st'tt''r$ we may assume $T''(1/r) = T'(1/r)$.

By 1.10 there is a $\phi$: $T' \longrightarrow K'$ such that $\phi(r) \neq 0$ and $B \otimes_\phi K'$ is a prime to $n$ power of $E'$. Since $\phi$ extends to $T'(1/r)$, $B \otimes_\phi K' = B' \otimes_\phi K'$ is a cyclic algebra. Since $E$ is a prime to $n$ power of $B \otimes_\phi K'$, $E$ is a cyclic algebra. ∎

Of course, in the generic algebra constructed in 1.10 the transcendence degree is the rank of $P$. Since $M$ has rank 2, clearly the minimum rank of $P$ is 2. It is of interest, then, to find out when $P$ can also have rank 2. The full result is:

THEOREM 1.12: *Let $M$ be a faithful accessible module over $C_q$. The minimum rank of a $C_q$-lattice $P$ with a surjection $P \longrightarrow M$ is the maximum of 2 and $\phi(q)$, where $\phi$ is the Euler $\phi$ function.*

*Proof:* Since $M$ is faithful, it is obvious that $P$ is faithful over $C_q$. Furthermore, $P \otimes_{\mathbb{Z}} \mathbb{Q}$ is a faithful $C_q$-module over $\mathbb{Q}$. The minimum dimension of such a module is $\phi(q)$. Since $M$ has rank 2, $P$ must have rank at least 2. Thus one direction is easy.

It suffices to find a $P$ of rank 2 or $\phi(q)$ and a surjection $P \longrightarrow M$. If $\phi(q) = 1$ then $q = 2$ and $M = R_{-1} \oplus R_{-1}$. We can set $P = \mathbb{Z}_{-1} \oplus \mathbb{Z}_{-1}$ and we are done with this case. Thus we assume $q > 2$. Let $\delta$ be a primitive $q$th root of 1 over $\mathbb{Q}$. Then the faithful $\mathbb{Q}[C_q]$-module of rank $\phi(q)$ can be written as $\mathbb{Q}(\delta)$ and this contains a lattice $P = \mathbb{Z}[\delta]$. To construct a surjection $\mathbb{Z}[\delta] \longrightarrow M$ it suffices to check two things. First, that $M$ is cyclic. Second, that if $\tau$ is a generator of $C_q$ and $f(x) \in \mathbb{Z}[x]$ is the cyclotomic polynomial which has $\delta$ as a root, then $f(\tau)M = 0$.

The second fact is quite easy as follows. Recall that $S \supset R$ was generated by $\theta$ such that $\theta^q = 1$. $M \otimes_R S = S_\theta \oplus S_{\theta^{-1}}$. Since $x^q - 1$ has distinct roots over $\mathbb{Z}/p\mathbb{Z} = R/pR$, $\theta$ and $\theta^{-1}$ must be roots of the image $\bar{f}(x) \in R[x]$. In other language, $f(\tau)S_\theta = f(\tau)S_{\theta^{-1}} = 0$.

As for the first fact, we consider the two cases $S/R$ has rank 1 or 2. In the first case, $M = R_\theta \oplus R_{\theta^{-1}}$ and the sum of generators of each piece generates $M$. In the second case, $M \otimes_R S = S_\theta \oplus S_{\theta^{-1}}$ and $M$ is the fixed module of a semilinear automorphism $\eta'$ of $M \otimes_R S$ which switches the direct summands. If $a$ generates $S_\theta$ then $a + \eta'(a)$ generates $M$. ∎

COROLLARY 1.13: *There is a $P$ as in 1.12 of rank 2 if and only if $q = 2, 4, 3, 6$.*

It will useful to have a more concrete description of the generic algebra $D$ from 1.10. More precisely, we give a description of $D'$ and the semilinear map $\tau'$. To achieve this, let $P \longrightarrow M$ be a surjection where $P, M$ are as in 1.12, and fix an embedding $M \subset P/nP$. Since $P/nP \cong (1/n)P/P$, there is a lattice $P' \supset P$ such that $P'/P \cong M$. Fixing a simple generator $a \wedge b$ of $M \wedge M$ defines an isomorphism (of $C_q$-modules) $M \wedge M \cong \mathbb{Z}/n\mathbb{Z}$. We thus have the induced $C_q$-invariant map $\phi$: $P' \wedge P' \longrightarrow \mathbb{Z}/n\mathbb{Z}$.

View $P'$ as an additive group. There is a well known natural map

$$\Psi\colon \operatorname{Hom}(P' \wedge P', \mathbb{Z}/n\mathbb{Z}) \longrightarrow H^2(P', \mathbb{Z}/n\mathbb{Z})$$

defined as follows. Let $\eta \in \operatorname{Hom}(P' \wedge P', \mathbb{Z}/n\mathbb{Z})$ be viewed as an alternating bilinear map $\eta$: $P' \times P' \longrightarrow \mathbb{Z}/n\mathbb{Z}$. Since $n$ is odd it is not hard to see that there is a bilinear $\eta'$: $P' \times P' \longrightarrow \mathbb{Z}/n\mathbb{Z}$ such that $\eta(p, p') = \eta'(p, p') - \eta'(p', p)$. Define a new product on $\mathbb{Z}/n\mathbb{Z} \times P'$ by setting

$$(q, p)(q', p') = (q + q' + \eta'(p, p'), p + p').$$

This defines an extension of $P'$ by $\mathbb{Z}/n\mathbb{Z}$, and hence an element of $H^2(P', \mathbb{Z}/n\mathbb{Z})$. Since $P'$ is free abelian, $\Psi(\eta)$ is independent of the choice of $\eta'$, and one can show that $\Psi$ is an isomorphism. The inverse associates an extension $1 \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow N \longrightarrow P' \longrightarrow 1$ to the alternating map $\eta(p, p') = u_p u_{p'} u_p^{-1} u_{p'}^{-1}$ where $u_p \in N$ is an inverse image of $p \in P'$. It is immediate that the map $\Psi$ is $C_q$-invariant.

Since $C_q$ acts on $P'$ we can form the semidirect product $G = P' \rtimes C_q$. Since $(q, n) = 1$ we have

$$\begin{aligned} H^1(C_q, H^1(P', \mathbb{Z}/n\mathbb{Z})) &= H^2(C_q, H^1(P', \mathbb{Z}/n\mathbb{Z})) \\ &= H^2(C_q, \mathbb{Z}/n\mathbb{Z}) = H^3(C_q, \mathbb{Z}/n\mathbb{Z}) \end{aligned}$$

which is 0. It follows from the Hochschild–Serre spectral sequence that

$$H^2(G, \mathbb{Z}/n\mathbb{Z}) \cong H^2(P', \mathbb{Z}/n\mathbb{Z})^{C_q} = \operatorname{Hom}(P' \wedge P', \mathbb{Z}/n\mathbb{Z})^{C_q}.$$

In particular, there is an extension of $G$ by $\mathbb{Z}/n\mathbb{Z}$ corresponding to $\phi$. An easy exercise shows that this extension must have the form $N \rtimes C_q$ where $1 \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow N \longrightarrow P' \longrightarrow 1$ corresponds to $\phi$ as an element of $H^2(P', \mathbb{Z}/n\mathbb{Z})$. In particular, this $N$ has a natural action by $C_q$.

Embed $\mathbb{Z}/n\mathbb{Z} \subset F^*$ by sending $1+n\mathbb{Z}$ to our fixed root $\rho$ of 1. Then $\phi$ induces $\phi \in H^2(P', F^*)$. Form the twisted group algebra $B = F_\phi[P']$. Clearly $B$ has a natural action by $C_q$. Direct computation shows that $B$ is an Azumaya symbol algebra $(a,b)_n$ defined over $F[P]$. Note that $a$ is the image of $1 \in \mathbb{Z}[\delta] = P$ and $b$ is the image of $\delta \in \mathbb{Z}[\delta] = P$. We can set $D' = B \otimes_{F[P]} F(P)$ which has an induced $C_q$-action.

PROPOSITION 1.14: *The invariant ring $D = D'^{C_q}$ is the generic algebra of 1.10.*

*Proof:* This is clear because $D$ is unique once the simple element $a \wedge b$ is fixed. ∎

## 2. $q = 2$ and $q = 4$

Let us first apply the machinery of Section 1 to the case $q = 2$. Since 2 is prime, the accessible $M$ is either trivial or faithful. The trivial one is $M = R \oplus R$ with trivial $C_2$ action. The proof of 1.4 shows that if $D$ is $(2, M)$ accessible for this $M$, then $D' = D \otimes_F L$ has a maximal subfield that is $C_n \oplus C_2$ Galois over $F$. The $C_2$ fixed field is then a cyclic maximal subfield of $D$. Thus we may assume that $M$ is faithful accessible.

Since $n$ is odd, $-1 \in R = \mathbb{Z}/n\mathbb{Z}$ is always true and so by the proof of 1.5 the accessible faithful $M$ is $R_{-1} \oplus R_{-1}$. The generic $(2, M)$ accessible algebra can, by 1.14, be described as follows. $P = \mathbb{Z}_{-1} \oplus \mathbb{Z}_{-1}$ maps onto $M$. Thus $D'$ is the symbol algebra $(a,b)_n$ over $F(a,b)$ where $\tau(a) = a^{-1}$ and $\tau(b) = b^{-1}$. By 1.4, $D$ is a dihedral algebra in the sense of [RS] and so by 1.11 we have:

THEOREM 2.1: *Suppose $D$ is a 2-accessible algebra over $K$ where $K$ has characteristic 0 and contains a primitive $n = [D\colon K]$ root of 1. Then $D$ is cyclic.*

We can handle almost as quickly the case $q = 4$. Once again we can assume $M$ is faithful accessible. In this case, by the proof of 1.12, we can take $P = \mathbb{Z}[C_q]/(1+\tau^2)$ and $M = P/nP$. Again, $P' = (1/n)P$. Thus $P' = (1/n)(\mathbb{Z}[\rho]) = (1/n)(\mathbb{Z}[x]/(x^2+1))$. By 1.14, $D'$ is the symbol algebra $(a,b)_n$ over $F(a,b)$. Let $\alpha, \beta \in B \subset D'$ be the images of $(1/n) + (x^2+1), (1/n)x + (x^2+1) \in P'$. Then $\alpha^n = a$, $\beta^n = b$, $\alpha\beta\alpha^{-1}\beta^{-1}$ is a primitive $n$ root of one, $\tau(\alpha) = \beta$ and $\tau(\beta) = \alpha^{-1}$.

THEOREM 2.2: *Suppose $D$ is a 4-accessible algebra over $K$ where $K$ has characteristic 0 and contains a primitive $n = [D\colon K]$ root of 1. Then $D$ is cyclic.*

*Proof:* By 1.11 we can assume $D$ is the generic 4-accessible algebra. Consider $\gamma = (\alpha + \alpha^{-1})(\beta + \beta^{-1})^{-1} \in D'$. Then $\gamma$ is $\tau^2$ invariant and we compute that $\tau(\gamma) = \gamma^{-1}$. It follows that $D'^{\tau^2} = D \otimes_K L^{\tau^2}$ has a maximal subfield with dihedral Galois group over $K$. By [RS] again $D$ is cyclic. ∎

## 3. The $q = 3$ case

Fix $q = 3$. In this section we will make a detailed study of the generic 3-accessible division algebra described in 1.10. Along the way we will give two proofs that this generic division algebra is cyclic, one only applying in the case $F$ contains an algebraically closed field of characteristic 0. As usual, we can assume that $n$, the degree of the division algebra, is a prime power $p^m$ where $p \neq 2, 3$ by assumption. Let us note now that many of the computations in this section were done with Mathematica.

Just as in Section 2 we reduce to the case of $M$ faithful accessible over $C_3$. According to the proof of 1.12 such an $M$ must be the image of $P = \mathbb{Z}[C_q]/(1 + \tau + \tau^2)$ where $\tau$ is a generator of $C_q$. Since $P$ and $M$ have rank 2,

$$M = P/nP = R[C_q]/(1 + \tau + \tau^2).$$

Thus we set $L = F(P)$, $K = F(P)^{C_q}$, and construct the generic $D/K$ as in 1.14.

Let us be more concrete about all of this. $L = F(a, b)$, there is an automorphism $\tau$ of $L$ of order 3 such that $\tau(a) = b$, $\tau(b) = a^{-1}b^{-1}$, and $K$ is the $\tau$ fixed field. $D/K$ is uniquely defined by the property that $D' = D \otimes_K L$ is the symbol algebra $(a, b)_n$.

We derive yet another description of $L$. Form the rational field $L' = F(x_1, x_2, x_3)$ where $\tau(x_i) = x_{i+1}$ (index mod 3). If we set $a = x_1/x_2$, $b = x_2/x_3$ then $L \subset L'$ is the subfield of rational functions of degree 0 in the $x_i$'s. The $\tau$ action on $L$ is the restriction of the action of $\tau$ on $L'$.

The K theory techniques we will use involve the following elements of $K$. Let $B$ be the matrix whose $i$th row is $(\tau^{i-1}(a), \tau^{i-1}(b), \tau^{i-1}(ab))$. Substituting the $x_i$'s we compute that the determinant $d$ of $B$ is

$$\frac{x_1^4x_2^2 - x_1^2x_2^3x_3 - x_1^3x_2x_3^2 + x_2^4x_3^2 - x_1x_2^2x_3^3 + x_1^2x_3^4}{(x_1x_2x_3)^2}$$

which is certainly nonzero. By e.g. [BAI] p.281, $a, b, ab$ form a basis of $L$ over $K$. In particular, there are unique $c_i \in K$ such that

$$c_1a + c_2b + c_3ab = 1. \tag{2}$$

We want to derive expressions for the $c_i$. Let $\vec{c}$, $\vec{1}$ be the column vectors $(c_1, c_2, c_3)$, $(1,1,1)$ respectively. Applying $\tau^{i-1}$ to (2) for $i = 1,2,3$ we have $B\vec{c} = \vec{1}$. We can therefore apply Cramer's Rule to compute the $c_i$ as follows. Let $N_i$ be the matrix $B$ with the $i$ column replaced by $\vec{1}$. Then $c_i = n_i/d$ where $n_i$ is the determinant of $N_i$. We compute that

$$(3) \qquad \begin{aligned} n_1 &= \frac{x_1^4x_2x_3 + x_1x_2^4x_3 - 3(x_1x_2x_3)^2 + x_1x_2x_3^4}{(x_1x_2x_3)^2}, \\ n_2 &= \frac{x_1^3x_2^3 - 3(x_1x_2x_3)^2 + x_1^3x_3^3 + x_2^3x_3^3}{(x_1x_2x_3)^2} \end{aligned}$$

and

$$n_3 = \frac{-x_1^2x_2^4 + x_1^3x_2^2x_3 - x_1^4x_3^2 + x_1x_2^3x_3^2 + x_1^2x_2x_3^3 - x_2^2x_3^4}{(x_1x_2x_3)^2}.$$

The $c_i$ satisfy the relations in 3.1 below, which we can show in two ways. First, we can use the relation (2) to derive 3.1 (a) and (b) as we outline below. Second, we can verify 3.1(a) and (b) by substituting the expressions (3) for the $c_i$. We used Mathematica to do this.

LEMMA 3.1:

(a) $c_3 = -c_1^2 - c_2^2 + c_1c_2$.

(b) *If $N_\tau$ is the norm of $L/K$, we have* $N_\tau(1 - c_1a) = (c_1 - c_2)^3$.

*Proof:* (a) We start with some calculations involving the $c_i$. (2) yields

$$(4) \qquad b = \frac{1 - c_1a}{c_2 + c_3a}.$$

Applying $\tau$ to (2) yields

$$c_1b + c_2a^{-1}b^{-1} + c_3a^{-1} = 1,$$

and, plugging in (4), yields

$$\frac{c_1(1 - c_1a)}{c_2 + c_3a} + \frac{c_2(c_2 + c_3a)}{a(1 - c_1a)} + \frac{c_3}{a} = 1;$$

clearing denominators yields

$$(5) \quad c_1(1 - c_1a)^2a + c_2(c_2 + c_3a)^2 + c_3(c_2 + c_3a)(1 - c_1a) = a(c_2 + c_3a)(1 - c_1a),$$

which yields a cubic equation

$$(c_1^3 + c_1c_3)a^3 + c'a^2 + c''a + (c_2^3 + c_2c_3) = 0,$$

where we do not care about the middle two coefficients $c', c''$. Anyway,

$$\frac{c_2^3 + c_2c_3}{c_1^3 + c_1c_3} = -N_\tau(a) = -1,$$

so $c_2^3 + c_2c_3 = -c_1^3 - c_1c_3$, yielding

$$0 = c_1^3 + c_2^3 + c_1c_3 + c_2c_3 = (c_1 + c_2)(c_1^2 - c_1c_2 + c_2^2 + c_3). \tag{6}$$

Note that $c_1 + c_2 \neq 0$ (for example by (3), or by a short argument using (7) and (8) below). Thus (6) yields

$$c_3 = -c_1^2 - c_2^2 + c_1c_2,$$

which is (a).

(b) Note that $\mathrm{tr}(a) = \mathrm{tr}(b) = \mathrm{tr}((ab)^{-1})$ and $\mathrm{tr}(a^{-1}) = \mathrm{tr}(b^{-1}) = \mathrm{tr}(ab)$.

Taking traces in (2) thus yields

$$(c_1 + c_2)\,\mathrm{tr}(a) + c_3\,\mathrm{tr}(a^{-1}) = 3; \tag{7}$$

dividing through by $ab$ in (2) and taking traces yields

$$(c_1 + c_2)\,\mathrm{tr}(a^{-1}) + 3c_3 = \mathrm{tr}(a). \tag{8}$$

Solving for $\mathrm{tr}(a)$ and $\mathrm{tr}(a^{-1})$ in terms of Cramer's rule, noting by (a) that the denominator is

$$(c_1 + c_2)^2 - (-c_3) = 3c_1c_2,$$

we have

$$\mathrm{tr}(a) = \frac{c_1 + c_2 + c_3^2}{c_1c_2};$$

$$\mathrm{tr}(a^{-1}) = \frac{-(c_1 + c_2)c_3 + 1}{c_1c_2}.$$

(Strictly speaking, this solution degenerates in characteristic 3. However we could also have obtained the (same) solution by computing $c'$ and $c''$ in (5), a slightly longer calculation which however is characteristic-free.)

Thus, we compute

$$\begin{aligned}
N_\tau(1-c_1a) &= 1 - c_1\,\mathrm{tr}(a) + c_1^2\,\mathrm{tr}(a^{-1}) - c_1^3 \\
&= \frac{c_1c_2 - c_1^2 - c_1c_2 - c_1c_3^2 - c_1^3c_3 - c_1^2c_2c_3 + c_1^2 - c_1^4c_2}{c_1c_2} \\
&= \frac{c_1(-c_3^2 - c_1^2c_3 - c_1c_2c_3 - c_1^3c_2)}{c_1c_2} \\
&= \frac{c_3(c_1^2 + c_2^2 - c_1c_2) - c_1^2c_3 - c_1c_2c_3 - c_1^3c_2}{c_2} \\
&= \frac{c_2^2c_3 - 2c_1c_2c_3 - c_1^3c_2}{c_2} \\
&= c_2(-c_1^2 - c_2^2 + c_1c_2) - 2c_1(-c_1^2 - c_2^2 + c_1c_2) - c_1^3 \\
&= (c_1 - c_2)^3. \qquad \blacksquare
\end{aligned}$$

Before we proceed to considering $D$, let us derive more information about $K$ in a special case. Assume $F$ has $\delta$, a primitive cube root of 1, and so is of characteristic prime to 3. We will show $K$ is purely transcendental over $F$, and find a concrete transcendence base. Set

$$\begin{aligned}
z_0 &= x_1 + x_2 + x_3, \\
z_1 &= x_1 + \delta x_2 + \delta^2 x_3
\end{aligned}$$

and

$$z_2 = x_1 + \delta^2 x_2 + \delta x_3.$$

The fixed field $K' = L'^{\tau}$ has transcendence basis $z_0, z_1^3, z_2/(z_1)^2$ by, e.g., [Fi]. Since $K = L^{\tau}$ are the elements in $K'$ of degree 0, it follows that $K$ has transcendence basis $X = z_0^3/z_1^3$ and $Y = z_0z_2/(z_1)^2$.

Since $L/K$ has degree 3, $L$ has transcendence basis $A = z_0/z_1$ and $Y$. Note that $Y$ is $\tau$ fixed and that $\tau(A) = \delta A$.

We need to write $a$ and $b$ in terms of $A$ and $Y$. To do this, we first write the $z_i$ in terms of the $x_j$. By inverting the matrix we compute that:

$$\begin{aligned}
x_1 &= \frac{1}{3}(z_0 + z_1 + z_2), \\
x_2 &= \frac{1}{3}(z_0 + \delta^2 z_1 + \delta z_2), \\
x_3 &= \frac{1}{3}(z_0 + \delta z_1 + \delta^2 z_2).
\end{aligned} \tag{9}$$

Then

$$a = x_1/x_2 = \frac{z_0 + z_1 + z_2}{z_0 + \delta^2 z_1 + \delta z_2} = \frac{z_0/z_1 + 1 + z_2/z_1}{z_0/z_1 + \delta^2 + \delta z_2/z_1}$$
$$= \frac{A + 1 + Y/A}{A + \delta^2 + \delta Y/A} = \frac{A^2 + A + Y}{A^2 + \delta^2 A + \delta Y}.$$

Applying $\tau$ we have:

$$b = \frac{\delta^2 A^2 + \delta A + Y}{\delta^2 A^2 + A + \delta Y}.$$

Since the $c_i$ are in $K$, they can be written in terms of $X$ and $Y$. To achieve this, we substitute using (9) and derive that (after factoring)

$$d = 27\delta \frac{(X + \delta^2 Y + \delta Y^2)(\delta X + \delta^2 XY + Y^2)}{(X + X^2 - 3XY + Y^3)^2},$$
$$n_1 = 27 \frac{XY}{X + X^2 - 3XY + Y^3},$$
$$n_2 = \frac{X(Y-1)(Y^2 - X)(Y - X)}{(X + X^2 - 3XY + Y^3)^2}$$

and

$$n_3 = -\delta^2 \frac{(X + \delta Y + \delta^2 Y^2)(\delta^2 X + \delta XY + Y^2)}{(X + X^2 - 3XY + Y^3)^2}.$$

Of course, $c_1 = n_1/d$, $c_2 = n_2/d$, and $c_3 = n_3/d$.

We next turn to describing the Brauer group element $[D] \in \mathrm{Br}(K)$, where we assume $F$ is algebraically closed of characteristic 0. Since $K = F(X, Y)$ we can think of $K$ as the function field of the affine space $\mathbb{A}^2$ contained in projective space $\mathbb{P}^2$. An element of $\mathrm{Br}(K)$ is then described by its ramification on $\mathbb{P}^2$. In particular, we wish to describe the ramification locus of our element $[D]$. We claim:

THEOREM 3.2: *$D$ ramifies along the single curve in $\mathbb{P}^2$ whose affine equation in $\mathbb{A}^2$ is $X + X^2 - 3XY + Y^3 = 0$.*

*Proof:* $F[A, Y]/F[X, Y]$ is an integral extension. Thus any curve $C \subset \mathrm{Spec}(F[X, Y])$ lies under a curve $C' \subset \mathrm{Spec}(F[A, Y])$. Moreover, the degree of the function field extension $F(C')/F(C)$ is prime to the order of any ramification of $[D]$ or $[D']$. It follows from e.g. [Se] p. 187 ex. 2 that $[D]$ ramifies at such a $C$ if and only if $[D']$ ramifies at the $C'$ lying over $C$. Since $D'$ is the symbol algebra $(a, b)_n$, $D'$ ramifies precisely along the three curves $A^2 + A + Y = 0$,

$A^2 + \delta^2 A + \delta Y = 0$ and $A^2 + \delta A + \delta^2 Y = 0$. These three curves are all $\tau$ conjugate and so lie over the single curve in $\mathrm{Spec}(F[X,Y])$ given by the norm. We compute this norm to be $X + X^2 - 3XY + Y^3$.

To finish 3.2 we must show $D$ does not ramify at infinity. The line at infinity is a prime of $F[X^{-1}, Y]$ which is integral in $F[A^{-1}, Y]$. Thus we must show that $D'$ does not ramify at infinity, which is immediate. ∎

This ramification information is enough to know that $D$ is cyclic, by a result of Tim Ford ([Fo]).

COROLLARY 3.3: *Suppose $F$ is of characteristic 0 and contains an algebraically closed field. Then any 3-accessible algebra is cyclic.*

*Proof:* By 1.11 it suffices to assume $F$ is algebraically closed of characteristic 0, and show the generic 3-accessible algebra over $F$ is cyclic. That is, to show $D$ above is cyclic. The curve given by $X + X^2 - 3XY + Y^3$ is easily seen to be a nodal cubic with node at $(1,1)$. Since $D$ ramifies only along a nodal cubic, $D$ is cyclic by ([Fo]). By 1.11 we get the result. ∎

Of course, it is of interest to remove the assumption in 3.3 that $F$ contains an algebraically closed field of characteristic 0. To do this we give an independent, elementary argument inspired by K-theory.

Recall that $L = F(a,b)$ is the function field in two variables and $\tau$: $L \cong L$ is defined by $\tau(a) = b$ and $\tau(b) = a^{-1}b^{-1}$. $K$ is the fixed subfield under $\tau$. The division algebra $D/K$ we need to show cyclic has the property that $D \otimes_K L$ is the symbol algebra $(a,b)_n$. The degree $n$ of $D$ is prime to 3 so it suffices to show that the underlying division algebra of $\mathrm{cor}_{L/K}((a,b)_n)$ is cyclic. That is, that $\mathrm{cor}_{L/K}((a,b)_n)$ is a symbol algebra over $K$ of degree $n$.

The computation of $\mathrm{cor}_{L/K}(a,b)$ is tricky, since the Rosset–Tate ([RT]) method is very complicated even in this case, and we do it by means of a related reduction. Note for arbitrary $c \in K$ that

$$\mathrm{cor}_{L/K}(a,c) \sim (N_\tau(a), c) = (1,c) \sim 1$$

by the projection rule, and likewise

$$\mathrm{cor}_{L/K}(b,c) \sim \mathrm{cor}_{L/K}(c,b) \sim 1.$$

Also we need the fact that $(u,v) \sim (u/v, u+v)$, seen easily from

$$\left(\frac{u}{u+v}, \frac{v}{u+v}\right) = 1.$$

Let $c_1, c_2, c_3$ in $K$ be as in (2).

LEMMA 3.4: *We have*

$$\mathrm{cor}_{L/K}(a,b) \sim \left(-\frac{c_3}{c_1c_2}, N_\tau\left(\frac{1-c_1a}{c_2}\right)\right) \otimes (c_2,c_1)^{\otimes 3}.$$

*Proof:* For the purposes of this proof, we will write $A \asymp B$ to mean $A, B$ are two central simple algebras over $L$ with equal corestrictions in $\mathrm{Br}(K)$. We have:

$$1 \sim (c_1a, c_2b + c_3ab) = (c_1a, (c_2 + c_3a)b),$$

so

$$(a,b) \sim (c_2 + c_3a, c_1a) \otimes (b, c_1) \asymp (c_2 + c_3a, c_1a).$$

Noting that

$$-\frac{c_3}{c_1c_2}c_1a + \frac{1}{c_2}(c_2 + c_3a) = 1,$$

we have

$$\left(-\frac{c_3}{c_1c_2}c_1a, \frac{1}{c_2}(c_2 + c_3a)\right) \sim 1$$

implying

$$\begin{aligned}(c_2 + c_3a, c_1a) &\sim \left(-\frac{c_3}{c_1c_2}, \frac{1}{c_2}(c_2 + c_3a)\right) \otimes \left(c_1, \frac{1}{c_2}\right) \otimes \left(a, \frac{1}{c_2}\right) \\ &\asymp \left(-\frac{c_3}{c_1c_2}, \frac{1}{c_2}(c_2 + c_3a)\right) \otimes (c_2, c_1).\end{aligned}$$

Noting by (4) that

$$c_2 + c_3a = \frac{1-c_1a}{b},$$

we have

$$\begin{aligned}\mathrm{cor}_{L/K}(c_2 + c_3a, c_1a) &\sim \mathrm{cor}_{L/K}\left(-\frac{c_3}{c_1c_2}, \frac{1-c_1a}{bc_2}\right) \otimes \mathrm{cor}_{L/K}(c_2, c_1) \\ &\sim \mathrm{cor}_{L/K}\left(-\frac{c_3}{c_1c_2}, \frac{1-c_1a}{c_2}\right) \otimes \mathrm{cor}_{L/K}(c_2, c_1).\end{aligned}$$

We conclude by means of the projection formula. ∎

THEOREM 3.5: *$D$ is a symbol, for $q = 3$ and $n$ relatively prime to 6. In fact*

$$D^{\otimes 2} \sim \left(\frac{c_2}{c_1}, c_3\right).$$

*Proof:* In view of 3.1 and 3.4 we have

$$D^{\otimes 3} \sim \operatorname{cor}_{L/F}(a,b) \sim \left(-\frac{c_3}{c_1c_2}, \frac{(c_1-c_2)^3}{c_2^3}\right) \otimes (c_2,c_1)^{\otimes 3}, \tag{10}$$

or equivalently (since 3 is prime to $n$),

$$D \sim \left(-\frac{c_3}{c_1c_2}, \frac{(c_1-c_2)}{c_2}\right) \otimes (c_2,c_1).$$

But this is

$$\left(-\frac{c_3}{c_1c_2}, c_1-c_2\right) \otimes \left(c_2, \frac{-c_3}{c_1c_2}\right) \otimes (c_2,c_1) \sim \left(-\frac{c_3}{c_1c_2}, c_1-c_2\right) \otimes (c_2,-c_3). \tag{11}$$

On the other hand,

$$(c_1c_2, c_3) \sim \left(\frac{c_1c_2}{c_3}, c_1c_2+c_3\right) = \left(\frac{c_1c_2}{c_3}, -(c_1-c_2)^2\right). \tag{12}$$

Substituting (12) into the square of (11) yields

$$D^{\otimes 2} \sim (-(c_1c_2)^{-1}, c_3) \otimes (c_2^2, c_3) \sim \left(\frac{c_2}{c_1}, c_3\right).$$

Indeed, since $n$ is odd, the minus sign is irrelevant, and furthermore we see $D$ is a tensor power of $D^{\otimes 2}$ and thus is a symbol. ∎

COROLLARY 3.6: *Suppose $F$ is a field of characteristic prime to $n$, containing a primitive $n$ root of 1. Assume $D$ is a 3-accessible algebra over $F$. Then $D$ is cyclic.*

*Proof:* By 1.11 again it suffices to prove the generic $D$ is cyclic. This is 3.5. ∎

From our description of the $c_i$ we can write down the symbol algebra in 3.5 in terms of $X$ and $Y$. It is interesting that this is a different description of $D$ than that which arises from Ford's result.

## 4. The q = 6 case, via K theory

Combining the results of Section 3 and [RS] yields that 6-accessible algebras are cyclic. Indeed, let $M$ be an accessible module. If $M$ is not faithful, then an accessible $(6, M)$ algebra is equivalent to an accessible algebra for $q = 3$ or $q = 2$. Thus we can assume $M$ is faithful over the cyclic group of order 6. Exactly as previously, we can assume $n$ is a prime power.

As in Section 1, $M = P/nP$ for $P = \mathbb{Z}[\theta]$ where $\theta$ is primitive with $\theta^6 = 1$. That is, $P = \mathbb{Z}[x]/(x^2 - x + 1)$. Let $\eta$ be a generator of the cyclic group of order 6. If $L = F(P)$, we can write $L = F(x, y)$ where $\eta(x) = y$ and $\eta(y) = y/x$. We change notation by setting $a = x$ and $b = y/x$. In these terms $\eta(a) = ab$, $\eta(ab) = \eta^2(a) = b$, $\eta(b) = \eta^3(a) = a^{-1}$, and $\eta^2(b) = \eta^4(a) = a^{-1}b^{-1}$. If $\tau = \eta^2$, then $\tau$ acts on $L$ exactly as in the previous section. Set $L_1$ to be the $\tau$ invariant subfield.

As before let $K$ be the $\eta$-invariant subfield of $L$. The 6-accessible generic algebra $D/K$ has the property $D \otimes_K L = (a, b)_n$. Thus the results of the previous section apply to $D \otimes_K L_1$, yielding $(D \otimes_K L_1)^{\otimes 2} \sim (c_1/c_2, c_3)_n$.

THEOREM 4.1: *Every 6-accessible algebra is cyclic.*

*Proof:* Once again it suffices by 1.11 to show the generic 6-accessible algebra is cyclic. Let $D_1 = (c_1/c_2, c_3)_{L_1, n}$. $\eta^3$ is the nontrivial automorphism of $L_1/K$. We need to compute the action of $\eta^3$ on the $c_i$. Applying $\eta^3$ to equation (2) of Section 3. We have:

$$\eta^3(c_1)a^{-1} + \eta^3(c_2)b^{-1} + \eta^3(c_3)a^{-1}b^{-1} = 1.$$

Multiplying by $\dfrac{ab}{\eta^3(c_3)}$ yields

$$\eta^3\left(\frac{c_1}{c_3}\right)b + \eta^3\left(\frac{c_2}{c_3}\right)a + 1 = \eta^3\left(\frac{1}{c_3}\right)ab.$$

Comparing with (2) and applying $\eta^3$ shows

$$\eta^3(c_1) = -\frac{c_2}{c_3}; \quad \eta^3(c_2) = -\frac{c_1}{c_3}; \quad \eta^3(c_3) = \frac{1}{c_3}.$$

It follows that $D$ is a dihedral algebra and so is cyclic by [RS]. ∎

In case $n$ is prime, the results of this paper yield the following, perhaps suggestive theorem.

THEOREM 4.2: *Suppose $D/F$ has a maximal subfield whose splitting field has solvable Galois group over $F$ and let $n$ be the degree of $D$. Assume $F$ has characteristic 0 and contains a primitive $n$ root of 1. If $n \leq 7$ and is prime, then $D$ is cyclic.*

*Proof:* It is known that $D$ is cyclic except for degrees 5 and 7. But in these cases the Galois group has to be a transitive solvable subgroup of the symmetric group $S_n$, and for $n$ prime these are known to be semidirect products of $C_n$ and $C_q$ for $q$ dividing $n-1$, e.g. [Ti1] p.372 or [BAI] p.254 ex.14. These algebras are accessible and so are covered by this paper. ∎

Another way of using the results of this paper is to bound the size of a prime to $p$ extension inducing cyclicity.

THEOREM 4.3:

(a) *Let $D/F$ be a division algebra of degree 5 where $F$ contains a primitive 5th root of 1. Then there is a field $K/F$ of degree prime to 5 and less than or equal to 6 such that $D \otimes_F K$ is cyclic.*

(b) *Let $D/F$ be a division algebra of degree 7 where $F$ contains a primitive 7th root of 1. Then there is a field $K/F$ of degree prime to 7 and less than or equal to 5! such that $D \otimes_F K$ is cyclic.*

*Proof:* We will prove (a) as (b) is exactly the same. Let $L$ be a maximal subfield of $D$ with Galois closure $\bar{L}$ and Galois group $G = \mathrm{Gal}(\bar{L}/F) \subset S_5$. Let $H' \subset S_5$ be the subgroup $C_5 \rtimes C_4$ where $C_4$ acts on $C_5$ faithfully. Choose $H'$ such that $H = H' \cap G$ has a subgroup of order 5. Set $K = (\bar{L})^H$. Since

$$\frac{|G|}{|H|} = \frac{|GH'|}{|H'|}$$

the result follows. ∎

## References

[B] K. Brown, *Cohomology of Groups*, Springer-Verlag, New York–Heidelberg–Berlin, 1982.

[CTS] J.-L. Colliot-Thélène and J.-J. Sansuc, *La R-équivalence sur les tores*, Annales Scientifiques de l'École Normale Supérieure **4** (1977), 175–230.

[DI] F. DeMeyer and E. Ingraham, *Separable algebras over commutative rings*, Lecture Notes in Mathematics **181**, Springer-Verlag, Berlin–Heidelberg–New York, 1971.

[D] P. K. Draxl, *Skew Fields*, Cambridge University Press, Cambridge, 1983.

[Fi] E. Fischer, *Die Isomorphie der Invariantenkorper der endlichen Abel'schen Gruppen linearen transformationen*, Gott. Nachr. (1915), 77–80.

[Fo] T. Ford, *Division algebras that ramify only along a singular plane cubic curve*, New York Journal of Mathematics **1** (1995), 178–183, http://nyjm.albany.edu:8000/j/v1/ford.html.

[BAI] N. Jacobson, *Basic Algebra I*, Freeman, San Francisco, 1974.

[KO] M. A. Knus and M. Ojanguren, *Théorie de la Descente et Algèbres d'Azumaya*, Lecture Notes in Mathematics **389**, Springer-Verlag, Berlin, 1974.

[MT] P. Mammone and J.-P. Tignol, *Dihedral algebras are cyclic*, Proceedings of the American Mathematical Society **101** (1987), 217–218.

[Mi] J. S. Milne, *Etale Cohomology*, Princeton University Press, Princeton, 1980.

[OS] M. Orzech and C. Small, *The Brauer groups of commutative rings*, Marcel Dekker, New York, 1975.

[RT] S. Rosset and J. Tate, *A reciprocity law for generalized traces*, Commentarii Mathematici Helvetici **58** (1983), 38–47.

[RS] L. H. Rowen and D. Saltman, *Dihedral algebras are cyclic*, Proceedings of the American Mathematical Society **84** (1981), 162–164.

[S] D. J. Saltman, *Generic Galois extensions and problems in field theory*, Advances in Mathematics **43** (1982), 250–283.

[S2] D. J. Saltman, *Azumaya algebras with involution*, Journal of Algebra **52** (1978), 526–539.

[Se] J.-P. Serre, *Local Fields*, Springer-Verlag, New York, 1979.

[Ti1] J.-P. Tignol, *Galois' Theory of Algebraic Equations*, Longman Scientific and Technical, Essex, England, 1988.

[Ti2] J.-P. Tignol, *Metacyclic division algebras of degree 5*, in *Ring Theory 1989* (L. H. Rowen, ed.), Israel Mathematical Conference Proceedings, Weizmann Science Press of Israel, Jerusalem, 1989.