ISRAEL JOURNAL OF MATHEMATICS **121** (2001), 173–198

DIVISION ALGEBRAS WITH A PROJECTIVE BASIS

BY

ELI ALJADEFF

Department of Mathematics, Technion — Israel Institute of Technology
Haifa 32000, Israel
e-mail: aljadeff@techunix.technion.ac.il

AND

DARRELL HAILE

Department of Mathematics, Indiana University,
Bloomington, IN 47405, USA
e-mail: haile@indiana.edu

ABSTRACT

Let k be any field and G a finite group. Given a cohomology class $\alpha \in H^2(G, k^*)$, where G acts trivially on k^*, one constructs the twisted group algebra $k^\alpha G$. Unlike the group algebra kG, the twisted group algebra may be a division algebra (e.g. symbol algebras, where $G \cong Z_n \times Z_n$). This paper has two main results: First we prove that if $D = k^\alpha G$ is a division algebra central over k (equivalently, D has a projective k-basis) then G is nilpotent and G', the commutator subgroup of G, is cyclic. Next we show that unless $\mathrm{char}(k) = 0$ and $\sqrt{-1} \notin k$, the division algebra $D = k^\alpha G$ is a product of cyclic algebras. Furthermore, if D_p is a p-primary factor of D, then D_p is a product of cyclic algebras where all but possibly one are symbol algebras. If $\mathrm{char}(k) = 0$ and $\sqrt{-1} \notin k$, the same result holds for D_p, p odd. If $p = 2$ we show that D_2 is a product of quaternion algebras with (possibly) a crossed product algebra $(L/k, \beta)$, $\mathrm{Gal}(L/k) \cong Z_2 \times Z_{2^n}$.

Received January 6, 1999

0. Introduction

Let k be a field. Recall that a **Schur algebra** over k is a k-central simple algebra which is a homomorphic image of a group algebra kG for some finite group G. Equivalently a k-central simple algebra A is Schur over k if A^*, the group of units of A, contains a finite group (say Γ) that spans A as a k-vector space. Let $[A] \in \mathrm{Br}(k)$ be the class in the Brauer group of k which is represented by A and let $S(k)$ be the subgroup of $\mathrm{Br}(k)$ generated by (and in fact consisting of) classes represented by Schur algebras. This is the Schur subgroup of $\mathrm{Br}(k)$. See [Y]. This construction has a projective version which was introduced by Lorenz and Opolka in 1978 ([LO]). They considered twisted group algebras $k^\alpha G$ rather than group algebras, where $\alpha \in H^2(G, k^*)$ (k^* with the trivial G-structure). A **projective Schur algebra** over k is a k-central simple algebra which is a homomorphic image of $k^\alpha G$ for some finite group G and some $\alpha \in H^2(G, k^*)$. It is not difficult to see that a k-central simple algebra A is projective Schur if and only if A^* contains a subgroup Γ which spans A over k and is finite modulo the center (i.e. $| k^*\Gamma/k^* | < \infty$). Clearly, a projective Schur algebra A determines an element, $[A]$, in $\mathrm{Br}(k)$ and we may consider the subgroup they generate in $\mathrm{Br}(k)$. This is $\mathrm{PS}(k)$, the projective Schur group of the field k. For the structure of projective Schur algebras and the projective Schur group see [LO], [NV], [AS2], [AS3]. The special situation where a projective Schur algebra is a division algebra (projective Schur division algebra) has been studied in [AS1] and [Sh]. The main result in [AS1] is that every projective Schur division algebra is isomorphic to a "radical abelian algebra" which is a special type of abelian crossed product $(K/k, H, \alpha)$. The main tool in the proof was Amitsur's classification of finite groups contained in the group of units of division algebras (see [A]). In [Sh] the focus is on the type of finite groups of the form $k^*\Gamma/k^*$ where $\Gamma \subset D^*$, D being an arbitrary division algebra over k. Equivalently, the groups $k^*\Gamma/k^*$ are the finite groups that occur as groups of inner automorphisms of D.

One of the main motivations for introducing projective Schur algebras and the projective Schur group is that symbol algebras are examples. Recall that a k-central simple algebra B of dimension n^2 is a symbol algebra if k contains ζ_n (a primitive n-th root of unity) and B is generated by elements x, y that satisfy $x^n \in k^*, y^n \in k^*, yx = \zeta_n xy$. Let Γ be the subgroup in B^* generated by x and y. It is clear that $k^*\Gamma/k^*$ (and by abuse of notation Γ/k^*) $\cong Z_n \times Z_n$. Furthermore, Γ spans B as a vector space over k and so B is a projective Schur algebra. In fact it is evident from the construction that such an algebra is not only a homomorphic image of, but isomorphic to, a twisted group algebra over

k. In this situation we will say that the algebra B has a **projective basis**. That is, we say the algebra B has a projective basis if it contains a basis Θ over k, consisting of invertible elements and such that $k^*\Theta/k^*$ is a subgroup of B^*/k^*.

As mentioned above, symbol algebras have projective bases but, as we'll see, these are not the only examples. In particular, in section 2 we exhibit a twisted group division algebra D over a field k, where $\exp(D) = p^r$, $r \geq 2$ but k contains no primitive p^r roots of unity.

The object of this paper is to analyze division algebras over k which have a projective basis or equivalently division algebras over k which are k-isomorphic to a twisted group algebra $k^\alpha G$ for some finite group G. Note that the order of G must be an exact square. Here are the main results:

THEOREM 1: *If $k^\alpha G$ is a division algebra with center k then the commutator subgroup of G is cyclic.*

Remarks: (1) If $\mathrm{Char}(k) = p > 0$, the result is in [AS1], Main Lemma.

(2) The group G is a finite group of inner automorphisms of $D = k^\alpha G$ and hence it must satisfy the conditions in [Sh].

THEOREM 2: *If $k^\alpha G$ is a division algebra with center k then G is nilpotent. Furthermore, if $P_1, P_2, \ldots, P_m$ are the Sylow-p subgroups of G and if $\alpha_i = \mathrm{res}^G_{P_i} \alpha_i$ for $i = 1, \ldots, m$ then $k^\alpha G \cong k^{\alpha_1} P_1 \otimes_k \cdots \otimes k^{\alpha_m} P_m$.*

This theorem reduces the analysis to p-groups. In that case we have the following results:

THEOREM 3: *If G is a p-group and $D = k^\alpha G$ is a division algebra with center k and (p, k) satisfies one of the following conditions:*

(1) p is odd, or

(2) $p = 2$ and $\sqrt{-1} \in k$,

then D is the tensor product of cyclic algebras (with projective bases) where all but possibly one are symbol algebras.

The remaining cases are considered in the following result.

THEOREM 4: *Let $p = 2$ and assume $\sqrt{-1} \notin k$. If G is a 2-group and $D = k^\alpha G$ is a division algebra with center k. Then:*

(1) If $\mathrm{char}(k) > 0$, then $D \cong D_1 \otimes_k \cdots \otimes D_n$ where all D_i, $i = 1, \ldots, n$ are quaternion algebras.

(2) If $\mathrm{char}(k) = 0$, then either

(i) $D \cong D_1 \otimes_k \cdots \otimes D_n$ where all D_i are quaternion algebras, or

(ii) $D \cong D_1 \otimes_k \cdots \otimes D_n$ *where* $D_i, i = 1, \ldots, n-1$ *are quaternion algebras and* D_n *is isomorphic to a crossed product* $(K/k, H = \mathrm{Gal}(K/k))$ *where* $H \cong Z_{2^r} \times Z_2$ *and* $r \geq 1$. *Furthermore,* D_n *has a projective basis as well.*

In section 1 we analyze the structure of the group G whenever $k^\alpha G$ is a division algebra k-central and prove Theorems 1 and 2. In sections 2 and 3 we analyze the algebras in the case where G is a p-group and prove Theorems 3 and 4.

1. The structure of G

Let $D = k^\alpha G$ be a twisted group division algebra with center k and let $f\colon G \times G \to k^*$ be a 2-cocycle representing α. Consider the group extension

$$\alpha = [f]\colon 1 \to k^* \to \Gamma \xrightarrow{\pi} G \to 1.$$

Clearly the group Γ is contained in the units of D and it spans D as a vector space over k. We often write $D = k(\Gamma)$. For every $\sigma \in G$ we choose an element u_σ in Γ such that $\pi(u_\sigma) = \sigma$. We call Γ the set of **group-like** elements in D^*. Furthermore, we say that an element in $\pi^{-1}(\sigma)$ is of **weight** $\sigma \in G$. If H is a subgroup of G, we let $k^\alpha H$ denote the twisted group algebra obtained by restricting α to H.

We start with a lemma which will be used several times in the paper.

LEMMA A: *Let* $k^\alpha G$ *be a twisted group division algebra with center* k. *Let* N *be a normal subgroup of* G *and let* $A = k^\alpha N$ *be the corresponding subalgebra in* $k^\alpha G$. *Then the center* $K = Z(A)$ *is a Galois extension of* k. *Furthermore, if* $N \geq G'$, *then* K/k *is abelian.*

Proof: We observe that group-like elements u_σ, $\sigma \in G$ act on A by conjugation and therefore they act on its center K. Clearly, this action induces an action of G/N on K. Finally, $K^{G/N} = k$ since $K^{G/N} \subset Z(k^\alpha G) = k$. ∎

Observe that the group Γ is center by finite, so by a theorem of Schur the commutator subgroup Γ' is finite. It is easy to see that the weights of the elements in Γ' are in G' and, moreover, $(\Gamma'/k^* =)\ k^*\Gamma'/k^* = G'$. It follows that $k(\Gamma')$, the subalgebra generated by Γ', is a division algebra isomorphic to the twisted group algebra $k^\alpha G'$. Note that since Γ' is finite, the cohomology class $\mathrm{res}(\alpha) \in H^2(G', k^*)$ can be represented by a 2-cocycle f_0 which takes finite values in k^*, that is for every σ, τ in G', $f_0(\sigma, \tau) \in \mu \subset k^*$, where μ denotes the group of roots of unity in k. We say that a cohomology class is of **finite type** if it has a representative which takes finite values in k^*. We remark that the center of $k(\Gamma')$ is a field K which may be a proper extension of k.

We want to analyze $k(\Gamma')$ and so we first consider twisted group algebras $k^\alpha G$ where the class α is of finite type and where the center may be a proper extension of k.

THEOREM 1.1: *Let $k^\alpha G$ be a twisted group division algebra and assume α is of finite type. Then:*

(1) *If $p \neq 2$, the sylow p-subgroup of G is cyclic.*
(2) *The sylow-2 subgroup of G is isomorphic to a subgroup of the dihedral group D_{2^n}, some n.*

Let us postpone the proof of the theorem and show that for a p-group G satisfying (1) or (2) one can find a field k and a finite class α such that $k^\alpha G$ is a division algebra.

It is not difficult to build an example with a cyclic p-group. For instance, assume k contains ζ_{p^r}, a primitive p^r root of unity, but does not contain $\zeta_{p^{r+1}}$ where $r \geq 1$ if p is odd and $r \geq 2$ if $p = 2$. Consider the field extension $K = k(x)$ where $x^{p^n} = \zeta_{p^r}$. Then one checks that $K \cong k^\alpha G$ where $G = C_{p^n}$ cyclic of order p^n and that the class α is finite. Note that if $p = 2$ and $i \notin k^*$ then the statement above may be false (e.g. $k = R$ the real numbers).

Next we build examples of twisted group algebras $k^\alpha G$ where G is isomorphic to a subgroup of D_{2^n} namely cyclic, Klein 4-group and dihedral. The cyclic case was considered above and the Hamilton quaternions is an example for the Klein 4 group. So let us assume $G \cong D_{2^n}$, $n \geq 3$. Consider the group extension

$$\alpha\colon 1 \to Z_2 = < q > \to Q_{2^{n+1}} \to D_{2^n} \to 1$$

where $Q_{2^{n+1}}$ denotes the quaternion group of order 2^{n+1}. Clearly α is non-split. Furthermore, α is non-split upon restriction to any non-trivial subgroup of D_{2^n}. We specialize $q = -1 \in Q$ (rationals) and build a twisted group algebra $D = Q^\alpha D_{2^n}$. We denote by $\Gamma \leq D$ the image of $Q_{2^{n+1}}$ under this specialization. Clearly α is of finite type. We claim D is a division algebra. In fact we are to show that D is the quaternion algebra $(-1,-1)$ over a certain field extension of Q of degree 2^{n-2}. Let $< \sigma >$ be the unique maximal cyclic subgroup (of order 2^{n-1}) of G and let τ be an involution in G such that $\tau\sigma\tau = \sigma^{-1}$. Let u_σ and u_τ be group-like elements in $\Gamma \leq D$ of weight σ and τ, respectively. A straigtforward calculation shows that the elements $u_\sigma + u_\tau u_\sigma u_\tau^{-1}$, $u_\sigma^2 + u_\tau u_\sigma^2 u_\tau^{-1}, \ldots, u_\sigma^{2^{n-3}} + u_\tau u_\sigma^{2^{n-3}} u_\tau^{-1}$ are in the center of D. Moreover, by the definition of the 2-cocycle one checks that for $0 \le i \le 2^{n-3}$, we have

$$u_\sigma^{2^i} + u_\tau u_\sigma^{2^i} u_\tau^{-1} = \sqrt{2+\sqrt{2+\sqrt{2+\sqrt{2+\sqrt{2}}}}}\ (i \text{ times})$$

and $L = k(u_\sigma + u_\tau u_\sigma u_\tau^{-1},\ u_\sigma^2 + u_\tau u_\sigma^2 u_\tau^{-1}, \ldots,\ u_\sigma^{2^{n-3}} + u_\tau u_\sigma^{2^{n-3}} u_\tau^{-1})$ is a field extension of degee 2^{n-2} over k. On the other hand, $(u_\sigma^{2^{n-2}})^2 = u_\tau^2 = -1$ and $(u_\sigma^{2^{n-2}})u_\tau = -u_\tau(u_\sigma^{2^{n-2}})$ and so D is isomorphic to the Hamilton quaternions $(-1,-1)$ over the field L. Finally, L is a real field and so D is a division algebra.

We proceed to the proof of Theorem 1.1:

CASE 1: $p \neq 2$. We show that if P is a sylow p-subgroup of G, then P contains no rank 2 elementary abelian group $(Z_p \times Z_p)$. This will imply that P is cyclic. Assume the converse and so let $P \supseteq P_0 \cong Z_p \times Z_p$ generated by σ and τ. As usual $u_\sigma., u_\tau$ are group-like elements in $k^\alpha G$ of weights σ and τ, respectively. The restriction of α to P_0 may be represented by the equations $u_\sigma^p = a$, $u_\tau^p = b$, $u_\sigma u_\tau = \zeta u_\tau u_\sigma$ and since α is a class of finite type we can assume that a, b, ζ are roots of unty in k. In particular, the subgroup of D^* generated by u_σ and u_τ is finite. From the equations above it follows that ζ is a p-th root of unity.

CASE 1.1: $\zeta = 1$. Then $K = k^\alpha Z_p \times Z_p$ is commutative. By replacing u_σ and u_τ by powers relatively prime to p, we may assume u_σ and u_τ are p-power roots of unity. But then one of two is a power of the other. If $u_\sigma = u_\tau^m$, then writing $m = ps+r$, where $0 \le r < p$, gives that u_σ is a k^* multiple of u_τ^r, a contradiction.

CASE 1.2: $\zeta =$ a primitive p-th root of unity. In this case $k^\alpha Z_p \times Z_p$ is a symbol algebra (a,b) where a and b are roots of unity. Replacing the algebra by a power prime to p we may assume a and b are p-power roots of unity. But that forces $a = b = \zeta$, because otherwise a or b is a p-th power in k and so (a,b) is split. But for p odd the symbol algebra (ζ,ζ) is split, so we have a contradiction.

This completes the proof of part (1) of Theorem 1.1.

CASE 2: $p = 2$. We need the following lemma.

LEMMA 1.2: *Let G be a 2-group, $k^\alpha G$ a division algebra where α is a class of finite type. Then:*

(i) *G contains no elementary abelian group isomorphic to $Z_2 \times Z_2 \times Z_2$.*

(ii) *G contains no group isomorphic to $Z_2 \times Z_4$.*

(iii) *G contains no group isomorphic to Q_8, the quaternion group of order* 8.

Assuming the Lemma, part (2) of Theorem 1.1 now follows since a finite 2-group not containing any of these 3 types of groups must be isomorphic to a subgroup of D_{2^n} for some n. (See [AGO].)

Proof of Lemma 1.2: (i) Assume G contains $Z_2 \times Z_2 \times Z_2$ and let σ, τ, ν be generators. Let u_σ, u_τ, u_ν be group-like elements in $k^\alpha G$ with weights σ, τ, ν respectively. Since the class α is of finite type the following relations are satisfied:

$$u_\sigma^2 = a, \quad u_\tau^2 = b, \quad u_\nu^2 = c, \quad u_\sigma u_\tau = \zeta_1 u_\tau u_\sigma, u_\sigma u_\nu = \zeta_2 u_\nu u_\sigma, u_\tau u_\nu = \zeta_3 u_\nu u_\tau$$

where a, b, c are roots of unity in k^* and $\zeta_1, \zeta_2, \zeta_3 \in \{1, -1\}$. If one of the ζ's (say ζ_1) is 1, we get that $k^\alpha < \sigma, \tau >$ is a field. This yields a contradiction as in case 1.1 above. If $\zeta_1 = \zeta_2 = \zeta_3 = -1$ we consider the elements $u_\sigma u_\tau$ and u_ν. They generate a field and again we get a contradiction.

(ii) Assume $\sigma, \tau \in G$ generate a subgroup $\cong Z_2 \times Z_4$. Then $u_\sigma^2 = a$, $u_\tau^4 = b$ and $u_\sigma u_\tau = \zeta u_\tau u_\sigma$ where a, b, ζ are roots of unity in k. Observe that $\zeta \in \{1, -1\}$, so u_σ and u_τ^2 generate a commutative subalgebra $\cong k^\alpha Z_2 \times Z_2$ which is not possible.

(iii) To show that G contains no subgroup isomorphic to Q_8, recall that $M(Q_8)$, the multiplicator of Q_8, vanishes. Applying the universal coefficient theorem for Q_8 gives

$$0 \to \mathrm{Ext}_Z^1((Q_8)_{ab}, k^*) \overset{\inf}{\to} H^2(Q_8, k^*) \to \mathrm{Hom}(M(Q_8), k^*) = 0 \to 0$$

where $(Q_8)_{ab} = Q_8/Q_8'$ is the abelianization of Q_8 and inf denotes the inflation map induced by the natural map $Q_8 \to (Q_8)_{ab}$. It follows that every cohomology class (regardless whether the class is finite or not) is trivial upon restriction to the commutator subgroup $Q_8' = Z(Q_8) = Z_2$ and therefore the twisted group algebra $k^\alpha G$ contains a non-trivial group algebra isomorphic to kZ_2. This shows that $k^\alpha G$ is not a division algebra. This completes the proof of Lemma 1.2 and also of Theorem 1.1. ∎

Remark 1.3: The argument above shows that if $k^\alpha G$ is a twisted group division algebra (where α is not necessarily of finite type) then the group G contains no quaternion group of order 8. On the other hand, it is easy to see that if α is not of finite type one can construct examples of twisted group division algebras $k^\alpha G$ where G contains any given abelian group (e.g. products of symbol algebras).

We are now heading toward the proofs of Theorems 1 and 2 of the introduction. Resuming our original notation we let $D = k^\alpha G$ be a k-central division algebra

(α arbitrary). Recall that the restriction of α to G' is of finite type so we can invoke Theorem 1.1 and conclude that the sylow p-subgroups of G' must be cyclic in the odd case or a subgroup of a dihedral 2-group in the even case.

We begin with the following result.

PROPOSITION 1.4: *Let $D = k^\alpha G$ be as above.*

(1) *The double commutator G'' is a 2-group.*
(2) *The sylow 2-subgroup of G' is characteristic in G.*

Proof: First note that (2) follows from (1) for if G'' is a 2-group, then G'_2, the sylow 2-subgroup of G', is normal in G'. This of course implies that G'_2 is characteristic in G' and therefore characteristic in G. To prove (1) we show that $G'' \cap P = \{1\}$ for every sylow $p \neq 2$ subgroup P of G'. If p is an odd prime, Theorem 1.1 says that P is cyclic and consequently $M(G')_p \leq M(P) = 0$ where A_p denotes the p-primary component of the abelian group A. It follows that the inflation map (in the universal coefficient theorem)

$$0 \to \mathrm{Ext}^1_Z((G')_{ab}, k^*)_p \overset{\inf}{\to} H^2(G', k^*)_p \to \mathrm{Hom}(M(G'), k^*)_p = 0 \to 0$$

is an isomorphism. This means that the p-component of any cohomology class $\alpha \in H^2(G', k^*)$ is trivial on G'' and therefore trivial on $G'' \cap P$. On the other hand, it is clear that the p' component of α vanishes on $G'' \cap P$, so $\mathrm{res}^G_{G'' \cap P}(\alpha) = 0$. This shows that the group algebra $k[G'' \cap P] \subset D$, which is impossible unless $G'' \cap P = \{1\}$. ∎

We know G'_2 is either cyclic or the Klein group of order 4 or dihedral of order 2^n, $n \geq 3$. We will eventually show that G'_2 is in fact cyclic. The previous proposition allows us to eliminate the dihedral case:

COROLLARY 1.5: *G'_2 is not isomorphic to the dihedral group of order 2^n, $n \geq 3$.*

Proof: Assume $G'_2 \cong D_{2^n}, n \geq 3$. Let $C_{2^{n-1}} \leq G'_2$ be the unique cyclic subgroup of order 2^{n-1}. Clearly $C_{2^{n-1}}$ is characteristic in G'_2 and by Proposition 1.4 it is characteristic in G' and in G. But $\mathrm{Aut}(C_{2^{n-1}})$ is abelian and so the map induced by conjugation $G \to \mathrm{Aut}(C_{2^{n-1}})$ factors through G/G'. This shows that the action of G' is trivial on $C_{2^{n-1}}$, contradicting our assumption on G'_2. ∎

PROPOSITION 1.6: *If G'_2 is cyclic, then G' is cyclic. If G'_2 is isomorphic to the Klein group, then we have the following:*

(a) *$G' \cong G'_2 \times C$ where C is cyclic of odd order. In particular G' is abelian.*
(b) *The center of $k^\alpha G'$ is the field $K = k^\alpha C$ and $k^\alpha G' \cong (-1,-1)_K$.*

(c) *3 does not divide the order of* G'.

(d) *The field extension* K/k *is abelian of degree prime to 6.*

Proof: Assume G'_2 cyclic. We then claim the sylow p-subgroups in G' for different primes p commute with each other. Indeed, take $x, y \in G'$ of orders p^s and q^t respectively where p and q are different primes. Consider the equality $xyx^{-1} = zy$ where $z \in G'_2$ (by Proposition 1.4). We assume (w.l.o.g.) that $q \neq 2$. Raising this equation to the q^t power we get $1 = (xyx^{-1})^{q^t} = zz^yz^{y^2}\cdots z^{q^t-1}$ where $z^{y^i} = y^izy^{-i}$. It follows that if the action of y on G'_2 is trivial (and in particular y centralizes z), z itself must be trivial (i.e. x and y commute). But we are assuming G'_2 cyclic and so its automorphism group is a 2-group, so we have proved the claim. By Proposition 1.4, G'_2 is normal in G' and by what we have just proved it is central and the quotient group $G'/Z(G')$ is abelian. Hence G' is nilpotent and so, in fact, cyclic.

Now assume $G'_2 = Z_2 \times Z_2$. Because the automorphism group of $Z_2 \times Z_2$ is S_3, the argument just given shows that every sylow p-subgroup commutes with every sylow q-subgroup as long as p and q are distinct and we are not in the situation where one of two is 2 and the other is 3. In particular, it follows (just as above) that G' is abelian and has the desired decomposition unless some generator y of a (cyclic) sylow 3-subgroup operates non-trivially (by conjugation) on G'_2, so we may assume we are in that case. We will show that this case leads to a contradiction. Since $G'_2 \leq G'$ the restriction of α on G'_2 is finite and therefore the twisted group algebra $k^\alpha G'_2$ is isomorphic to the Hamilton quaternions $(-1,-1)$. We are going to show that the existence of an element y as above will force k to contain a primitive third root of one. If so, then the algebra $(-1,-1)$ is split, so we will be done.

To see this let u_y be an element in $k^\alpha G'$ of weight y. It normalizes $k^\alpha G'_2$ and so there is an element $w \in k^\alpha G'_2$ (of order 3 modulo k^*) such that u_yw^{-1} centralizes $k^\alpha G'_2$ (and in particular it centralizes w). It follows that u_yw^{-1} is in the center of the subalgebra $D_0 = < k^\alpha G'_2, u_yw^{-1} >$. Furthermore, since u_y and w commute $\mathrm{ord}(u_yw^{-1}) = \mathrm{ord}(u_y) = 3^t, t \geq 1$ where ord here is the order modulo k^*. It follows that $k(u_yw^{-1})$ is a field extension of degree 3^t. We wish to show that $k(u_yw^{-1})/k$ is a Galois extension. Take any v element in G' of order prime to 6 and let u_v be an element of weight v. Let P_3 be a sylow 3-subgroup of G'. Recall that v centralizes G'_2 and P_3 and therefore the commutator of u_v and u_z, where $z \in < G'_2, P_3 >$, must be a root of unity ζ in k. Clearly, $\gcd(\mathrm{ord}(v), 6) = 1$ implies $\zeta = 1$. It follows that D_0 is centralized by all elements u_v where $v \in G'$ of order prime to 6. But the subgroup $< G'_2, P_3 >$ is normal in G' of index prime to 3. It follows that all the sylow 3-subgroups of G' lie in $< G_2', P_3 >$, as does the unique sylow 2-subgroup, and so $u_y w^{-1}$ commutes with all elements of weights a power of 2 or 3. We conclude that the field $k(u_y w^{-1})$ lies in the center of $k^\alpha G'$. By Lemma A the extension $Z(k^\alpha G')$ is Galois over k and the Galois group is abelian. Therefore $k(u_y w^{-1})/k$ is a Galois extension of degree 3^t and $(u_y w^{-1})^{3^t} \in k$. It follows that $k(u_y w^{-1})$ contains $k(\zeta)$, where ζ is a primitive 3^t-root of unity. But then k must contain a primitive third root of unity, because otherwise 2 will divide the degree of the extension $k(\zeta)/k$.

Statement (b) follows from part (a) and the fact that $k^\alpha G_2'$ is isomorphic to the Hamilton quaternions $(-1,-1)$.

For part (c), if 3 divides the order of G', then let G_3' denote the three part of G'. The ring $k^\alpha G_3'$ is a subfield of K and so is abelian over k by Lemma A. But G_3' is cyclic, so $k^\alpha G_3' = k(y)$ for some element y of order a power of 3 modulo k^*. As we saw above this forces k to contain a primitive third root of one, and so $(-1,-1)$ is split over K.

Part (d) is now clear. ∎

PROPOSITION 1.7: *The group G is nilpotent.*

Proof: We first <u>claim</u> that if p is a prime then every p-element of G commutes with every p'-element of G'. Let $g \in G \setminus G'$ be a p-element. Let $q \neq p$ be a prime dividing the order of G' and let G_q' denote the q-primary component of the abelian group G'. Observe that G_q' is characteristic in G' and therefore normal in G. It follows that the only way that the proposition can fail is in case that $p = 3$, $q = 2$ and G_2' is the Klein group. We claim that in this case $K = Z(k^\alpha G')$ must contain ζ_3, a primitive 3rd root of unity, and therefore by Proposition 1.6 (b) the algebra $k^\alpha G'$ is split. Let u_g be an element whose weight g is of order 3^e, $e \geq 1$ (and so of order 3^e modulo G' since 3 does not divide the order of G' by part (c) of Proposition 1.6). Clearly u_g normalizes $k^\alpha G'$ and therefore it normalizes the center K. Moreover, by Proposition 1.6 (d), u_g centralizes K. The argument now is similar to the one above. Indeed, by the Skolem–Noether theorem there is an element $x \in k^\alpha G'$ such that $w = u_g x^{-1}$ centralizes $k^\alpha G'$ and in particular it commutes with x. Note that w has order a power of 3 modulo K^*. Consider the subalgebra $B = k^\alpha < G', g >$ of $k^\alpha G$ and let $L = Z(k^\alpha < G', g >)$. Clearly $K(w) \subseteq L$. Thus

$$\begin{aligned} 4 &\leq \dim_L(k^\alpha < G', g >) \leq \dim_{K(w)}(k^\alpha < G', g >) \\ &= \dim_{K(w)}(< k^\alpha G', w >) \leq \dim_K k^\alpha G' = 4 \end{aligned}$$

by Proposition 1.6. This shows that $K(w) = L$. Next, by the twisted group construction

$$3^e \dim_k k^\alpha G' = \dim_k(k^\alpha < G', g >) = \dim_{K(w)}(k^\alpha < G', g >) \dim_K K(w) \dim_k K$$

and so $\dim_K K(w) = 3^e$, $e \geq 1$.

Now $L = K(w)$ is an ablelian extension of k by Lemma A and so $K(w)/K$ is abelian of degree 3^e and we have seen that w has order a power of 3 modulo K^*. As before it follows that K contains ζ_3. This finishes the proof of the claim.

Now let p divide the order of G and let P be a sylow p-subgroup of G. We want to show that P is normal in G. Let $g \in G$ and let $x \in P$. Then $gxg^{-1} = cx$ where $c \in G'$. By Proposition 1.6, G' is abelian so we may write $c = c_1c_2$ where $c_1 \in G'$ is a p-element and c_2 is a p'-element. By the first part of the proof x commutes with c_2 and so the three elements c_2, c_1x, gxg^{-1} all commute. Moreover, $c_1x \in P$ because $x \in P$ and $c_1 \in G'_p$ which is contained in every sylow p-subgroup of G. In particular, c_1x is a p-element. But gxg^{-1} is also a p-element and so $c_2 = (c_1x)^{-1}gxg^{-1}$ is a p-element. Hence $c_2 = 1$ and so $gxg^{-1} = c_1x \in P$. This proves G is nilpotent. ∎

In order to complete the proof of Theorem 2, we let $P_1, \ldots, P_m$ be the sylow subgroups of G and let $\alpha_i = \mathrm{res}^G_{P_i}(\alpha)$ for $i = 1, \ldots, m$. Denote by ϕ_i the k-algebra embedding of $k^{\alpha_i}P_i$ in $k^\alpha G$. Clearly the $\{\mathrm{Im}(\phi_i)_{i=1,\ldots,m}\}$ generate $k^\alpha G$ and by [AS4, Lemmas 2.1 and 2.2] $\mathrm{Im}(\phi_i)$ centralizes $\mathrm{Im}(\phi_j)$ for $i \neq j$. Thus the embeddings ϕ_i induce a surjective homomorphism

$$\phi\colon k^{\alpha_1}P_1 \otimes_k k^{\alpha_2}P_2 \otimes \cdots \otimes k^{\alpha_m}P_m \to k^\alpha G.$$

A dimension argument shows that ϕ is an isomorphism.

We have now finished the proof of Theorem 2. To complete the proof of Theorem 1, we need to show that $G_2' \neq Z_2 \times Z_2$. By the nilpotency of G we have $(G_2)' = G_2'$. Moreover, it is clear from the isomorphism ϕ that the twisted group algebra $k^\alpha G_2$ is a k-central division algebra. We therefore see that it is sufficient to prove the following: Let G be a 2-group and let $k^\alpha G$ be a twisted group division algebra with center k. Then $G' \neq Z_2 \times Z_2$.

So suppose $k^\alpha G$ is a division algebra with center k and $G' = \{1, \sigma, \tau, \sigma\tau\} \cong Z_2 \times Z_2$. We know then that $D = k^\alpha G'$ is isomorphic to the symbol algebra $(-1,-1)$ over k, so in the usual notation for the quaternions we may assume $u_\sigma = i$ and $u_\tau = j$. Because G is a 2-group, some non-identity element of G' lies in the center of G. We will assume that σ is in the center of G. It follows that conjugation by a given element of G either fixes all of G' or fixes σ and switches

τ and $\sigma\tau$. If $g \in G$, the automorphism $\mathrm{Inn}(u_g)$ preserves D and so is inner on D. That is, there is an element $r \in D$ such that $\mathrm{Inn}(u_g) = \mathrm{Inn}(r)$ on D. The discussion above implies that $\mathrm{Inn}(r)(i)$ is a k-multiple of i and that $\mathrm{Inn}(r)(j)$ is a k-multiple of either j or ij. Letting $r = a + bi + cj + dij$ where a, b, c, d are in k and computing, we easily see that r must be a k-multiple of one of the following eight elements: $\{1, i, j, ij, 1+i, 1-i, j+ij, j-ij\}$.

Now let $x, y \in G$. The commutator $(x, y) = xyx^{-1}y^{-1}$ lies in $<\sigma, \tau>$. We claim that in fact $(x, y) \in <\sigma>$. If so we will have a contradiction. To prove the claim we choose $r, s \in D$ such that $\mathrm{Inn}(x) = \mathrm{Inn}(r)$ and $\mathrm{Inn}(y) = \mathrm{Inn}(s)$ on D. Then $r^{-1}u_x$ and $s^{-1}u_y$ centralize D in $k^\alpha G$. Moreover, $\mathrm{Inn}(r)$ fixes r, so u_x and r commute. Similarly, u_y and s commute. We compute the commutator $(r^{-1}u_x, s^{-1}u_y)$ in $k^\alpha G$. We obtain

$$(r^{-1}u_x, s^{-1}u_y) = (r^{-1}u_x)(s^{-1}u_y)u_x^{-1}ru_y^{-1}s$$

$$= (srs^{-1}r^{-1})(u_xu_yu_x^{-1}u_y^{-1}) = (r, s)(u_x, u_y)$$

which lies in D because $r, s \in D$ and $(x, y) \in G'$. But the commutator $(r^{-1}u_x, s^{-1}u_y)$ centralizes D. Hence $(r^{-1}u_x, s^{-1}u_y)$ lies in k. On the other hand, we have seen that r and s must be k-multiples of the elements $\{1, i, j, ij, 1+i, 1-i, j+ij, j-ij\}$. Computing once more one sees that (r, s) is a k-multiple of 1 or i. Hence $(u_x, u_y) = (r, s)^{-1}(r^{-1}u_x, s^{-1}u_y)$ is also a k-multiple of 1 or i and so $(x, y) \in <\sigma>$.

This finishes the proof of Theorem 1. ∎

2. Structure of the algebra

In this section and the next we analyze the division algebra $k^\alpha G$ and prove Theorems 3 and 4.

By Theorem 2 we may assume that G is a p-group. Furthermore, we know by Theorem 1 that G' is cyclic. It follows that the twisted group algebra $k^\alpha G'$ is a field extension of k and since the restriction of α to G' is of finite type this extension is cyclotomic, in fact it is p-cyclotomic. (In this paper, an extension L/k is **cyclotomic** if $L = k(\zeta)$ (rather than $L \subseteq k(\zeta)$), where ζ is a root of unity; it is **p-cyclotomic** if ζ is a p-power root of unity.)

Question: How many p-th power roots of unity must k have? By [AS4, Theorem 1.7], if $k^\alpha G \neq k$ (as we assume from now on) the field k must contain a primitive p-th root of unity. On the other hand, if k contains μ_p, the group of all p-power roots of unity, then $G' = 1$. But then the group G is abelian, so the algebra

$k^\alpha G$ is a product of symbol algebras (see [AS4], proof of Theorem 1.1), and so Theorems 3 and 4 hold. So we will assume that k contains ζ_{p^s}, a primitive p^s, $s \geq 1$ root of unity, but does not contain a primitive p^{s+1} root.

Consider the non-empty family

$$\Pi = \{G' \leq H \leq G\colon K_H = k^\alpha H/k \text{ is a } p\text{-cyclotomic field extension}\}$$

and let N be a maximal element. Let $\mathrm{ord}(N) = p^r$, $r \geq 1$. Since N is normal in G, the field K_N is normalized by any group-like element u_σ, $\sigma \in G$. The next result is a refinement of Theorem 1.1 in [AS5]. It establishes a connection between the structure of G and the number of p-power roots of unity in k.

THEOREM 2.1: *If u_σ centralizes K_N, then its order modulo K_N^* (or equivalently, the order of σ modulo N) divides p^s, the number of p-th power roots of unity in k.*

Remark: The proof is similar to the proof of Theorem 1.1 in [AS5] Theorem 1.1. Since the result is key for the rest of the paper we include a proof.

Proof: Assume the theorem is false. Then there is an element u_σ that centralizes K_N and $\mathrm{ord}(\sigma) = p^{s+1}$ modulo N. Consider the subalgebra $k^\alpha < N, \sigma >$ of $k^\alpha G$. Clearly it is a commutative algebra (u_σ centralizes the field K_N) and hence it is a field. Next, observe that $G' \subseteq < N, \sigma >$ and hence, by Lemma A, $k^\alpha < N, \sigma >$ is an abelian extension of k. This implies that the field generated by u_σ over k is also an abelian extension of k. Let us analyze the extension $k(u_\sigma)/k$. Assume $u_\sigma^{p^{s+1+t}} = b \in k^*$, $t \geq 0$. A theorem of Schinzel ([S, Theorem 2], [K, p. 235]) says that if $k(u_\sigma)/k$ is an abelian extension then $b^{p^s} = c^{p^{s+1+t}}$ for some $c \in k^*$. It follows that $u_\sigma^{p^s} = \zeta' c$ where ζ' is a p^{s+1+t} root of unity. To get a contradiction recall that the order of u_σ modulo K_N^* is p^{s+1}. This implies that $k^\alpha < N, \sigma^{p^s} >$ is a proper field extension of K_N^* and, in particular, the subgroup $< N, \sigma^{p^s} >$ of G strictly contains N. But $k^\alpha < N, \sigma^{p^s} > = K_N(\zeta')$ is a cyclotomic p-extension of k. This contradicts the maximality of N in Π. ∎

We will treat the case where $p = 2$ and $\sqrt{-1} \notin k$ in the last section. We therefore assume for the rest of this section that one of the following conditions holds:

(1) p is odd, or
(2) $\sqrt{-1} \in k$.

By construction, the extension K_N/k is p-cyclotomic of degree $p^r, r \geq 1$ (we can assume that $r \neq 0$, for otherwise G is abelian and $k^\alpha G$ is a product of symbol algebras). By the assumption just stated, the extension K_N/k is cyclic.

Let $G/N \cong Z_{p^{n_1}} \times Z_{p^{n_2}} \times \cdots \times Z_{p^{n_h}}$. Since N is normal in G, conjugation by group-like elements u_σ induces a map η: $G/N \to \mathrm{Gal}(K_N/k)$. As argued in Lemma A, $K_N^{G/N} = k$ (so η is surjective). It follows that at least one of the cyclic components in the decomposition of G/N is of order p^r and it is mapped onto $\mathrm{Gal}(K_N/k)$. So without loss of generality we assume that $n_1 \geq r$. We write $n_1 = r + \epsilon$ with $\epsilon \geq 0$ and $G/N \cong Z_{p^{r+\epsilon}} \times Z_{p^{n_2}} \times \cdots \times Z_{p^{n_h}}$. We denote this isomorphism by ϕ.

LEMMA 2.2: *With the notation above we have $\epsilon \leq s$ and $n_i \leq s$ for every $i = 2, \ldots, n$.*

Proof: Let $\sigma, \tau_2, \ldots, \tau_h$ be elements in G whose images in G/N generate the respective components of G/N as in the decomposition above. We know that the element σ is mapped to a generator of the Galois group $\mathrm{Gal}(K_N/k)$. This implies that σ^{p^r} acts trivially on K_N and, by Theorem 2.1, its order modulo N divides the number of roots of unity in k. This shows that $\epsilon \leq s$. Next, take one of the τ_i's. It normalizes the field K_N so there is a power $t(i)$ such that the actions of $\sigma^{t(i)}$ and τ_i agree on K_N. This means that $\tau_i\sigma^{-t(i)}$ acts trivially on K_N. Again by Theorem 2.1 we conclude that its order modulo N is bounded by the number of p-th power roots in k. Finally, we observe that the order of $\tau_i\sigma^{-t(i)}$ bounds the order of τ_i modulo N. This completes the proof of the lemma. ∎

Consider the family of subgroups

$$M = \{N \leq H \leq < N, \tau_2, \ldots, \tau_h > : K_H = k^\alpha H \text{ is a field}\}.$$

Let H_0 be a maximal element in M. As in the proof of Lemma A it follows that $k^\alpha H_0$ is a Galois extension of k and that the G action on $k^\alpha H_0$ (which is defined by conjugation of group-like elements) induces a homomorphism of G/H_0 onto $\mathrm{Gal}(k^\alpha H_0/k)$.

Let $S = < N, \tau_2, \ldots, \tau_h >$. Let $D_0 = k^\alpha S$ and L be its center. Recall that σ is an element in G which generates the component $Z_{p^{r+\epsilon}}$ modulo N. Clearly, by the construction of S, σ is of order $p^{r+\epsilon}$ modulo S, or equivalently, $\mathrm{ord}(u_\sigma) = p^{r+\epsilon}$ modulo D_0^*. Conjugation by u_σ in $k^\alpha G$ normalizes D_0 and therefore normalizes L.

LEMMA 2.3: *The action of u_σ on L induces an isomorphism of the cyclic group of order $p^{r+\epsilon}$ generated by $u_\sigma D_0^*$ with* $\mathrm{Gal}(L/k)$.

Proof: Conjugation by u_σ induces a homomorphism η from the cyclic group of order $p^{r+\epsilon}$ generated by $u_\sigma D_0^*$ into $\mathrm{Gal}(L/k)$. We show that η is an isomorphism.

Arguing as in the proof of Lemma A we see that $L^{u_\sigma} = k$, where L^{u_σ} is the subfield of L fixed by u_σ. This proves η is surjective onto $\mathrm{Gal}(L/k)$ and, in particular, L/k is a cyclic extension. In order to prove η is injective we assume L/k is an extension of dimension p^d. We want to show that $d = r + \epsilon$. By the discussion above we see that $d \leq r + \epsilon$. Assume $e = r + \epsilon - d > 0$ and consider the element $u_\sigma^{p^d}$. It is of order p^e modulo D_0^* and it fixes L. We claim that the subalgebra Σ generated by D_0 and $u_\sigma^{p^d}$ has a center Δ which is of dimension $p^f > p^d$. Note that this contradicts $\mathrm{ord}(u_\sigma) = p^d$ modulo Σ^* and $\Delta^{u_\sigma} = k$. To prove the claim note that since $u_\sigma^{p^d}$ normalizes D_0 and centralizes L so (by the Skolem–Noether theorem) there is an element z in D_0 such that $zxz^{-1} = u_\sigma^{p^d} x u_\sigma^{-p^d}$ for every $x \in D_0$. This shows that $u_\sigma^{p^d} z^{-1}$ centralizes D_0 and, in particular, it centralizes z. It follows that $u_\sigma^{p^d}$ commutes with z. Since the order of $u_\sigma^{p^d}$ modulo D_0^* is precisely p^e, we obtain that the order of $u_\sigma^{p^d} z^{-1}$modulo D_0^* is also p^e. By assumption $e > 0$, so $u_\sigma^{p^d} z^{-1}$is not in D_0 and, in particular, it is not in L. On the other hand, it centralizes D_0 and therefore it is in the center of the algebra $\Sigma =< D_0, u_\sigma^{p^d} z^{-1} >=< D_0, u_\sigma^{p^d} >$. But clearly, L is also contained in the center of Σ and so the subfield generated by L and $u_\sigma^{p^d} z^{-1}$ is contained in Δ. This proves the claim and completes the proof of the lemma. ∎

Let us pause for a moment and sketch the remaining steps in the proof of Theorem 3. We will show that the subalgebra $(L/k, \sigma)$ generated by L and u_σ is a cyclic crossed-product over k and moreover it is of the form $k^\alpha Q$ for some normal subgroup Q of G. This will enable us to decompose $D = k^\alpha G \cong (L/k, \sigma) \otimes_k B$ where B is isomorphic to a twisted group algebra of the form $k^\beta G/Q$. Induction on the order of G shows that D may be decomposed into a product of cyclic algebras. But more than that, we will show that the group G/Q is abelian and therefore, using the proof of Theorem 1.1 of [AS4], one shows that the algebra B is isomorphic to a product of symbol algebras.

LEMMA 2.4: *The field L is spanned by group-like elements. More precisely, there is a normal subgroup U of G such that $L = K_U = k^\alpha U$.*

Proof: By the maximality of H_0 the action of S/H_0 on K_{H_0} is faithful and therefore the algebra $k^\alpha S$ is isomorphic to a crossed-product algebra $(K_{H_0}, S/H_0)$. It follows that the center L is precisely the fixed field $K_{H_0}^{S/H_0} = K_{H_0}^S$. Thus, in order to show that L is spanned by group-like elements we need to show that if $w = x_1 u_{\theta_1} + x_2 u_{\theta_2} + \cdots + x_n u_{\theta_n}$ ($x_i \in k^*$ and u_{θ_i} is a group like element of weight $\theta_i \in H_0$) is an element in $L = K_{H_0}^S$, then $u_{\theta_i} \in L$ for every $i = 1, \ldots, n$. In fact it is sufficient to show that if $w \in K_{H_0}^\tau$ (the fixed field by τ, and τ arbitrary in

S) then $u_{\theta_i} \in K_{H_0}^{\tau}$ for every $i = 1, \ldots, n$. To see this recall that the extension K_{H_0}/k is abelian ($H_0 \geq G'$) and therefore every group-like element u_θ, $\theta \in H_0$ generates a subextension $k(u_\theta)/k$ which is abelian. Therefore $k(u_\theta)$ is normalized by every element of S. Take an element $\tau \in S$. By Lemma 2.2 and the definitions of K_{H_0} and S, we have that $\mathrm{ord}(u_\tau) \leq p^s$ modulo $K_{H_0}^*$, where p^s is the number of p-th power roots of unity in k. It follows that the orders of the automorphisms in $\mathrm{Gal}(K_{H_0}/k)$ and in $\mathrm{Gal}(k(u_\theta)/k)$ which are induced by conjugation with u_τ are of p-power and bounded by p^s. It follows that $u_\tau u_\theta u_\tau^{-1} = \zeta u_\theta$ where $\zeta = \zeta(\theta)$ is a p^s root of unity and hence $\zeta \in k^*$. Assume now $w \in K_{H_0}^{\tau}$. Then we have

$$\begin{aligned} w = u_\tau w u_\tau^{-1} &= u_\tau(x_1 u_{\theta_1} + x_2 u_{\theta_2} + \cdots + x_n u_{\theta_n}) u_\tau^{-1} \\ &= x_1 \zeta(\theta_1) u_{\theta_1} + x_2 \zeta(\theta_2) u_{\theta_2} + \cdots + x_n \zeta(\theta_n) u_{\theta_n}. \end{aligned}$$

But the group-like elements $\{u_{\theta_i}\}_{\theta_i \in G}$ are linearly independent over k and therefore $\zeta(\theta_i) = 1$ for $i = 1, \ldots, n$. This completes the proof of the lemma. ∎

Having shown that the field L is isomorphic to a twisted group algebra $k^\alpha U$, for some subgroup U in G, we proceed to show the subalgebra $(L/k, \sigma)$ generated by L and u_σ is a cyclic crossed-product over k.

LEMMA 2.5: *The subalgebra $k^\alpha < U, \sigma >$ is a cyclic crossed-product algebra, k-central, of index $p^{r+\epsilon}$. Furthermore, L is a maximal subfield and $k^\alpha < U, \sigma > = (L/k, C = < u_\sigma L^* >)$.*

Proof: By Lemma 2.3, conjugation of L by u_σ induces an isomorphism of the cyclic group $< u_\sigma D_0^* >$ with $\mathrm{Gal}(L/k)$. So, all we have to show is that $\mathrm{ord}(u_\sigma L^*) = \mathrm{ord}(\mathrm{Gal}(L/k)) = p^{r+\epsilon}$. We claim $\mathrm{ord}(u_\sigma k^*) = p^{r+\epsilon}$ (in fact this is also necessary). Indeed, recall that σ is an element in G which generates modulo N the first component in the decomposition $G/N \cong Z_{p^{r+\epsilon}} \times Z_{p^{n_2}} \times \cdots \times Z_{p^{n_h}}$. Furthermore, by the discussion preceding Lemma 2.2 conjugation by u_σ induces a homomorphism from the group $< \sigma N >$ onto $\mathrm{Gal}(K_N/k)$. It follows that $u_\sigma^{p^{r+\epsilon}} \in K_N^\sigma = k$, as desired. ∎

As explained above we wish to factor the subalgebra $D_1 = k^\alpha < U; \sigma >$ from $k^\alpha G$. This will use a refinement of the factorization lemma ([AS4], Lemma 2.3) which we prove below. To apply it we need two results, the first of which will be used for a different purpose in the last section.

PROPOSITION 2.6: *Let H be a cyclic group of order p^n, p a prime, $n \geq 1$. If $k^\alpha H$ is a field and the extension $k^\alpha H/k$ is abelian, then:*

(1) $k \supseteq \mu_p$.

(2) *If p is odd, then the extension $k^\alpha H/k$ is cyclic.*

(3) *If $p = 2$ and $k \supseteq \mu_4$, then $k^\alpha H/k$ is cyclic.*

(4) *If $p = 2$ and $k \not\supseteq \mu_4$, then $\mathrm{Gal}(k^\alpha H/k)$ is isomorphic to $Z_2 \times Z_{2^{n-1}}$.*

Proof: We have $k^\alpha H = k(\theta)$ where $\theta^{p^n} = \beta \in k$ and the extension $k(\theta)/k$ has degree p^n. It follows that $x^{p^n} - \beta$ is the minimal polynomial of θ over k. To prove (1) note that, because $k(\theta)/k$ is Galois, we must have all the roots of $x^{p^n} - \beta$ in $k(\theta)$ and so $k(\theta) \supseteq \mu_{p^n} \supseteq \mu_p$. But $[k(\mu_p) : k]$ divides $p-1$. Hence $[k(\mu_p) : k] = 1$.

As we have just seen for arbitrary p the field $k(\theta)$ contains μ_{p^n}. We claim that $k(\theta^p)$ contains μ_{p^n}. Let $\omega \in k(\theta)$ be a primitive p^n-th root of one. Since $\omega\theta$ is a root of $x^{p^n} - \beta$ there is an automorphism σ of $k(\theta)$ over k such that $\sigma(\theta) = \omega\theta$. Hence $\sigma(\theta^p) = \omega^p\theta^p$. Because $k(\theta)/k$ is assumed abelian, the extension $k(\theta^p)/k$ is Galois. Moreover, $k(\theta^p) = k^\alpha(H^p)$ and so $[k(\theta^p) : k] = p^{n-1}$. In particular, the minimal polynomial of θ^p over k is $x^{p^{n-1}} - \beta$ and so $k(\theta^p) \supseteq \mu_{p^{n-1}}$. In particular, $\omega^p \in k(\theta^p)$. Hence both θ^p and $\sigma(\theta)^p$ are in $k(\theta^p)$. It follows that there is an element $\rho \in k(\theta^p)$ and an integer m, $0 < m < p$, such that $\sigma(\theta) = \rho\theta^m$. Hence $\rho\theta^m = \omega\theta$, so $k(\theta^p) \ni \rho = \omega\theta^{1-m}$. We claim $m = 1$. If not, there is an integer t, $0 < t < p$, such that $(1-m)t = ps + 1$ for some integer s. Then $k(\theta^p) \ni \rho^t = \omega^t\theta^{ps+1}$ and so $k(\theta^p) \ni \omega^t\theta$. But ω^t is a primitive p^n-th root of unity, so there is an element $\tau \in \mathrm{Gal}(k(\theta)/k)$ such that $\tau(\omega^t\theta) = \theta$. Since τ preserves $k(\theta^p)$, we obtain $\theta \in k(\theta^p)$, a contradiction. Hence $m = 1$, so $\omega = \rho \in k(\theta^p)$. This proves the claim.

We observe that the claim shows that for all i, $1 \le i \le n$, $k(\theta^{p^i}) \supseteq \mu_{p^{n-i+1}}$.

We now proceed to prove parts (2) and (3) in the case where $n \le 2$. If $n = 1$ then both parts are clear. Assume $n = 2$. Then $k^\alpha H = k(\theta)$ where $\theta^{p^2} = \beta \in k$ and $[k(\theta) : k] = p^2$. We have seen that $k(\theta^p) \ni \omega$, a primitive p^2-root of unity. Moreover, $k \supseteq \mu_p$ and so $\omega^p \in k$. There is an automorphism σ of $k(\theta)$ over k that satisfies $\sigma(\theta) = \omega\theta$. It suffices to show σ has order p^2. If not, then $\sigma^p = 1$, so $\theta = \sigma^p(\theta) = N_{k(\theta^p)/k}(\omega)\theta$, where $N_{k(\theta^p)/k}$ denotes the norm map from $k(\theta^p)$ to k. Hence $N_{k(\theta^p)/k}(\omega) = 1$. Therefore it suffices to show that $N_{k(\theta^p)/k}(\omega) \neq 1$. If $\omega \in k$, then $N_{k(\theta^p)/k}(\omega) = \omega^p \neq 1$. In particular, this takes care of part (3). If $\omega \notin k$ (so p is odd), then $\omega \in k(\theta^p)$ and $[k(\theta^p) : k] = p$, so $k(\omega) = k(\theta^p)$. It follows that the minimal polynomial of ω over k is $x^p - \omega^p$ and so $N_{k(\theta^p)/k}(\omega) = (-1)^p(-w^p) = w^p \neq 1$.

We now prove parts (2) and (3) in the case where $n > 2$. We proceed by induction on n. As we have seen $k(\theta^p) = k^\alpha H^p$ is an abelian extension of k and so is cyclic by the induction hypothesis. We also know that $k(\theta^p) \supseteq \mu_{p^n}$ and $k(\theta^{p^2}) \supseteq \mu_{p^{n-1}}$. Let $\omega \in k(\theta^p)$ be a primitive p^n-th root of one. Just as in the previous argument, there is an automorphism σ of $k(\theta)$ over k that satisfies $\sigma(\theta) = \omega\theta$. We would like to show σ has order p^n. If not then $\sigma^{p^{n-1}} = 1$, so $\theta = \sigma^{p^{n-1}}(\theta) = N_{k(\theta^p)/k}(\omega)\theta$, where $N_{k(\theta^p)/k}$ denotes the norm map from $k(\theta^p)$ to k. So it suffices to show $N_{k(\theta^p)/k}(\omega) \neq 1$. Now $\sigma(\theta^p) = \omega^p\theta^p$ and so σ restricted to $k(\theta^p)$ generates the Galois group of $k(\theta^p)$ over k. In particular, $\sigma^{p^{n-1}}(\theta^p) = \theta^p$ and so $N_{k(\theta^p)/k}(\omega^p) = 1$. Similarly, $N_{k(\theta^{p^2})/k}(\omega^{p^2}) = 1$. But $\sigma^{p^{n-2}}(\theta^p) \neq \theta^p$ and so $\gamma = N_{k(\theta^{p^2})/k}(\omega^p) \neq 1$. It follows that γ is a primitive p-th root of one. Therefore we have $\gamma = \omega^p\sigma(\omega^p)\cdots\sigma^{p^{n-2}-2}(\omega^p)\sigma^{p^{n-2}-1}(\omega^p)$ and so $\delta = \omega\sigma(\omega)\cdots\sigma^{p^{n-2}-2}(\omega)\sigma^{p^{n-2}-1}(\omega)$ is a primitive p^2-root of unity. Hence

$$\begin{aligned} N_{k(\theta^p)/k}(\omega) &= \omega\sigma(\omega)\cdots\sigma^{p^{n-1}-2}(\omega)\sigma^{p^{n-1}-1}(\omega) \\ &= \delta\sigma^{p^{n-2}}(\delta)\sigma^{2p^{n-2}}(\delta)\sigma^{3p^{n-2}}(\delta)\cdots\sigma^{(p-1)p^{n-2}}(\delta). \end{aligned}$$

But $\sigma^{p^{n-2}}$ fixes δ: If $p = 2$ this is true by assumption. If p is odd, $\delta \in k(\theta^{p^{n-1}})$ and so $\sigma^{p^{n-2}}$ fixes δ because $n \geq 3$. Hence $N_{k(\theta^p)/k}(\omega) = \delta^p \neq 1$.

Finally we prove (4). Assume $p = 2$ and $k \not\supseteq \mu_4$. If $n = 1$ the result is clear, so assume $n \geq 2$. Let i be a primitive 4-th root of 1. Then we have seen that $k(\theta^{2^{n-1}}) \ni i$ and so $k(\theta^{2^{n-1}}) = k(i)$. It follows that $\theta^{2^{n-1}} = ci$ for some $c \in k$ and so that $\theta^{2^n} = -c^2$. Hence the element $y = (1+i)\theta^{2^{n-2}}$ satisfies $y^2 = 2i\theta^{2^{n-1}} = -2c \in k$. It follows that $k(y)/k$ is a quadratic extension not equal to $k(\theta^{2^{n-1}})$, so $k(\theta)/k$ is not cyclic. But by assumption $k(\theta)/k$ is abelian and by part (3) the extension $k(\theta)/k(i)$ is cyclic. It follows that $\mathrm{Gal}(k^\alpha H/k)$ is isomorphic to $Z_2 \times Z_{2^{n-1}}$. ∎

LEMMA 2.7: *With the notation above, the subgroup $< U, \sigma >$ is normal in G or equivalently the crossed product $D_1 = (L/k, C)$ is normalized by any group-like element u_z, $z \in G$.*

Proof: First note that u_z normalizes $D_0 = k^\alpha S$ ($S \geq G'$) and so it normalizes its center L. So the lemma will be proved if we show that $u_z u_\sigma u_z^{-1} u_\sigma^{-1} \in L^*$. To see this recall that $L = k^\alpha U$ is a cyclic extension of k of degree $p^{r+\epsilon}$. It follows that the group U is cyclic (otherwise U contains $Z_p \times Z_p$ and so the extension L/k contains two different subfields of degree p over k). Let π be a generator of U. Since the action of $< u_\sigma k^* >$ on L is faithful, it follows that $u_\sigma u_\pi u_\sigma^{-1} = \zeta u_\pi$ where $\zeta = \zeta_{p^{r+\epsilon}}$ is a primitive $p^{r+\epsilon}$ root of unity which is obviously in L. But more than that: ζ is a group-like element u_h where $h \in G'$ and $\mathrm{ord}(h) = \max\{1, p^{r+\epsilon-s}\}$. (Recall that k contains a primitive p^s root of unity but does not contain a primitive p^{s+1} root of unity.)

CLAIM: *Let* $u_\lambda = u_z u_\sigma u_z^{-1} u_\sigma^{-1}$ *where* $\lambda \in G'$. *Then* $\mathrm{ord}(\lambda) \le \mathrm{ord}(h)$. *This shows that* $\lambda \in < h >$ *and* $u_\lambda \in L$.

Proof of the claim: Consider the action of u_z on the field $K_N = k^\alpha N (N \ge G')$ by conjugation. Since conjugation by u_σ generates $\mathrm{Gal}(K_N/k)$ (paragraph preceding Lemma 2.2), there is a power $d = d(z)$ of u_σ such that $u_\sigma^{-d} u_z$ centralizes K_N. Consequently, $k^\alpha < N, \sigma^{-d} z >= K_N(u_\sigma^{-d} u_z)$ is a field extension of k. Furthermore, it is an abelian extension and so is the subextension $k(u_\sigma^{-d} u_z)/k$. By Proposition 2.6, $k(u_\sigma^{-d} u_z)/k$ is cyclic.

SUBCLAIM: $\deg(k(u_\sigma^{-d} u_z)/k) \le \max\{p^s, p^{r+\epsilon}\}$. Indeed, we observe that the group G/N is mapped onto the group $\mathrm{Gal}(K_N(u_\sigma^{-d} u_z)/k)$ and therefore onto $\mathrm{Gal}(k(u_\sigma^{-d} u_z)/k)$. On the other hand, $\exp(G/N) \le \max\{p^s, p^{r+\epsilon}\}$ and the subclaim follows.

Finally, $(u_\sigma^{-d} u_z) u_\sigma (u_\sigma^{-d} u_z)^{-1} u_\sigma^{-1} = u_\sigma^{-d} u_\lambda u_\sigma^d$. Thus $\mathrm{ord}(u_\sigma^{-d} u_\lambda u_\sigma^d) = \mathrm{ord}(u_\lambda) \le \max\{p^s, p^{r+\epsilon}\}$ and, since all p^s roots of unity are contained in k, $\mathrm{ord}(\lambda) \le \max\{1, p^{r+\epsilon-s}\}$. This completes the proof of the claim and also of the lemma. ∎

As mentioned above, for the last step in the proof of Theorem 3 we need the following factorization lemma.

FACTORIZATION LEMMA: *Let* $k^\alpha G$ *be a non-modular (that is,* $\mathrm{ord}(G) \in k^*$*) twisted group division algebra over* k. *Let* H *be a normal subgroup of* G *and assume the subalgebra* $k^\alpha H$ *is* k*-central. Then* $k^\alpha G \cong k^\alpha H \otimes_k k^\beta E$ *where* $k^\beta E$ *is a (*k*-central) twisted group algebra with finite group* E *and* $\beta \in H^2(E, k^*)$.

Proof: We may assume of course that H is a proper subgroup of G. Let u_s be a group-like element whose weight s is in G but not in H. The group H is normal in G so u_s normalizes $k^\alpha H$. Since the latter is simple over k, the Skolem–Noether Theorem implies that there exists an element $e(s)$ in the units of $k^\alpha H$ such that $e(s)^{-1} u_s$ centralizes $k^\alpha H$. Clearly, u_s and $e(s)$ commute in $k^\alpha G$, and since u_s is of finite order modulo k^*, $e(s)$ and therefore $e(s)^{-1} u_s$ is of finite order modulo k^*. Let Γ be the group of group-like elements in $k^\alpha G$ and consider the subgroups Φ of $(k^\alpha H)^* \Gamma (\Gamma$ normalizes $(k^\alpha H)^*)$ that centralize $k^\alpha H$. Since $k^\alpha H$ is k-central, $\Phi \cap k^\alpha H = k^*, \Phi/k^* \le (k^\alpha H)^* \Gamma/(k^\alpha H)^*$ which is a quotient of $\Gamma/k^* \cong G$ and moreover a quotient of G/H. Thus a maximal such Φ exists. We wish to show that $k^\alpha G = (k^\alpha H)(k(\Phi))$. If not, there is an element $s \in G$ such that u_s is not in $(k^\alpha H) k(\Phi)$. In particular, $s \notin H$, so repeating the argument above we get an element $e(s)^{-1}u_s \in (k^\alpha H)^*\Gamma$ which centralizes $k^\alpha H$ and lies outside Φ. Then we can strictly enlarge the subgroup Φ to $< \Phi, e(s)^{-1}u_s >$, contradicting the maximality of Φ.

In order to complete the proof of the lemma, let $\beta \in H^2(\Phi/k^*, k^*)$ be the class determined by the following central extension:

$$\beta\colon 1 \to k^* \to \Phi \to \Phi/k^* \to 1.$$

This gives surjective homomorphisms

$$\eta\colon k^\beta(\Phi/k^*) \to k(\Phi) \quad \text{and} \quad 1 \otimes \eta\colon (k^\alpha H) \otimes_k k^\beta(\Phi/k^*) \to (k^\alpha H)k(\Phi) = k^\alpha G.$$

Because Φ/k^* is the quotient of G/H, a dimension argument shows that $\Phi \cong G/H$ and $1 \otimes \eta$ is an isomorphism. This completes the proof of the lemma. ∎

We now complete the proof of Theorem 3:

By Lemma 2.7 the subgroup $< U, \sigma >$ is normal in G and by Lemma 2.5 the twisted group algebra $k^\alpha < U, \sigma > = (L/k, C =< u_\sigma L^* >)$ is k-central. The factorization lemma then implies that there exists a finite group E and $\beta \in H^2(E, k^*)$ such that $k^\alpha G \cong k^\alpha < U, \sigma > \otimes_k k^\beta E$. It remains to show that E is abelian and then, by the proof of ([AS4], Theorem 1.1), $k^\beta E$ is a product of symbol algebras. Assume the converse and let $E' \neq \{1\}$ be the commutator. By Theorem 1, E' is cyclic. Moreover, the algebra $k^\beta E'$ (as well as $k^\alpha G'$) is a non-trivial cyclotomic p-extension of k. It follows that the subalgebra $k^\alpha G' \otimes_k k^\beta E'$ is commutative and hence a field. This is of course impossible, since it contains a finite non-cyclic group of units. ∎

We now want to exhibit a twisted group division algebra D over a field k, where $\exp(D) = p^r$, $r \geq 2$ but k contains no primitive p^r roots of unity. Let p be an odd prime and assume k contains a primitive p^s, $s \geq 1$ root of unity but not a primitive p^{s+1} root. Consider the polynomial $X^{p^r} - a$, where $a \in k^*$ and $r > s$. Assume it is irreducible over k and let x be a root. The field extension $K = k(x)$ may be abelian and, if it is, it must be cyclic. Assuming that this is the case we denote by H the *Galois* group and by σ a generator. Since K/k is cyclic, it follows (using a theorem of Schinzel, see [S, Theorem 2]) that $a^{p^s} = b^{p^r}$ for some $b \in k^*$. So if we take the p^{r+s} roots of this equality we get $x = a^{1/p^r} = \zeta b^{1/p^s}$, where ζ is a p^{r+s} root of unity. We claim that ζ is a primitive p^{r+s} root of unity. To see this we raise the above equality to the p^s power and get $x^{p^s} = \zeta^{p^s} b$. Now if ζ is a p^{r+s-1} root of unity, then ζ^{p^s} is a p^{r-1} root and the extension $k(x^{p^s}) = k(\zeta^{p^s})$ is cyclotomic over k and of dimension $\leq p^{r-1-s}$. But $\dim k(x)/k(x^{p^s}) \leq p^s$, so we get $\dim k(x)/k \leq p^{r-1}$. This contradicts our original assumption on the polynomial $X^{p^r} - a$. Having shown that ζ is a primitive p^{r+s} root of unity, we have that ζ^{p^s} is a primitive p^r root of unity and from the equality above it follows that modulo k^* all the p^r roots of unity are powers of x. Let $\Delta = (K/k, \sigma)$ be the crossed-product algebra where the 2-*cocycle* is given by $u_\sigma^{p^r} = c \in k^*$. From the discussion above it is clear now that the group $G = < x, u_\sigma > /k^*$ is of order p^{2r} and that Δ has a projective basis over k. Note that the group G is not abelian. One can easily construct such crossed products Δ which are division algebras. It should be emphasized that Δ is not (in general) a product of symbol algebras. Indeed, choosing a suitable field k and an element $c \in k^*$ we can construct Δ as above and of exponent $\geq p^{s+1}$. Since k contains no primitive p^{s+1} root of unity Δ is not (Brauer equivalent to) a product of symbol algebras.

3. Structure of the algebra, case II

In this section we analyze the twisted group algebra $D = k^\alpha G$ where G is a 2-group, and $\sqrt{-1} \notin k$. By Theorem 1, G' is cyclic and hence the subalgebra $k^\alpha G'$ is a 2-cyclotomic extension of k. We assume G' is not trivial, for then G is abelian and the result follows from Theorem 1.1 [AS4]. Let $\mathrm{ord}(G') = 2^{r_0} < \mathrm{ord}(G) = 2^n$. Following the argument in the previous section we let N be a maximal subgroup of G that contains G' and the subalgebra $K_N = k^\alpha N$ is a 2-cyclotomic extension of k. Assume $\mathrm{ord}(N) = 2^{r+1}$, $r \geq 0$. Note that in this case the group N may be cyclic (in which case we may have a group-like element u_θ where θ is a generator of N, that satisfies $u_\theta^{2^{r+1}} = -1$) or non-cyclic (e.g. $N = < z > \times < w >$ and $u_z^2 = -1$ and $u_w^2 = 2$, say over the field Q). In any case, $\mathrm{Gal}(K_N/k) \cong Z_{2^r} \times Z_2$, which is non-cyclic unless $r = 0$. We first show that $r = 0$ when k has positive characteristic.

PROPOSITION 3.1: *If k has positive characteristic, then* $\mathrm{ord}(N) \leq 2$.

Proof: First note that in positive characteristic any 2-cyclotomic extension is necessarily cyclic: If w is a primitive 2^t root of unity then the Galois group of $k(w)$ over k imbeds in the Galois group of $F(w)$ over F, where F is the prime field of k. Now assume $\mathrm{ord}(N) = 2^n$. Because the $k^\alpha N/k$ is cyclic, the group N must also be cyclic. But then by Proposition 2.6, since k does not contain $\sqrt{-1}$, the only case in which $k^\alpha N/k$ is cylic is where $\mathrm{ord}(N) \leq 2$. ∎

As in the previous section, conjugation by u_g, $g \in G$, induces a surjective homomorphism η: $G/N \to \mathrm{Gal}(K_N/k)$. Let $G/N \cong Z_{2^{s_1}} \times Z_{2^{s_2}} \times \cdots \times Z_{2^{s_n}}$ $=< \bar{\tau}_1, \bar{\tau}_2, \ldots, \bar{\tau}_n >$, $\tau_i \in G$. It follows that there are two components (one of which may be trivial), say $Z_{2^{s_1}} \times Z_{2^{s_2}}$, such that $\eta(Z_{2^{s_1}} \times Z_{2^{s_2}}) = \mathrm{Gal}(K_N/k)$. (Of course it follows from the previous proposition that in positive characteristic only one component is needed.) We may assume that $s_1 \geq r$ and $s_2 \geq 1$ and after remembering that

$$G/N \cong Z_{2^{r+e}} \times Z_{2^{1+f}} \times Z_{2^{s_1}} \times \cdots \times Z_{2^{s_m}} =< \overline{\sigma}_1, \overline{\sigma}_2, \overline{\gamma}_1, \ldots, \overline{\gamma}_m >,$$

$\sigma_i, \gamma_j \in G$, $m \geq 0$, e, $f \geq 0$, $s_i \geq 1$.

PROPOSITION 3.2: *$e, f \leq 1$ and $s_i = 1$ for $i = 1, \ldots, m$.*

Proof: Assume first e or f is ≥ 2. Then there is an element $u_x, x \in G$ whose order modulo K_N is 4 and it centralizes K_N, contradicting Theorem 2.1 (since $\sqrt{-1} \notin k$). The same argument shows that $s_i \leq 1$ if u_{γ_i} centralizes K_N. So let us assume that u_{γ_i} acts non-trivially on K_N. Since the map η: $G/N \to \mathrm{Gal}(K_N/k)$ is surjective, there is an element $y = y(i) \in G$ such that $\overline{y} \in Z_{2^{r+e}} \times Z_{2^{1+f}}$ and such that $u_y^{-1}u_{\gamma_i}$ centralizes K_N. Again, by Theorem 2.1, $u_y^{-1}u_{\gamma_i}$ is of order at most 2 modulo K_N and therefore $\mathrm{ord}(u_{\gamma_i}) \leq 2$. The proposition is now proved. ∎

In fact we can obtain more from this argument: If u_{γ_i} acts non-trivially on K_N then the element u_y, defined above, is also of order 2 modulo K_N ($\mathrm{ord}(u_y) > 2$ modulo K_N would imply $\mathrm{ord}(u_y^{-1}u_{\gamma_i}) > 2$ modulo K_N). This implies that either e or f is 0, for if $e = f = 1$, the element u_y would centralize K_N. This proves (i) and (ii) and consequently (iii) of the following lemma.

LEMMA 3.3: *Assume u_{γ_i}, some i, does not centralize K_N. Then:*

(i) *Either e or f is 0. In particular, $2^{r+1} \leq \mathrm{ord}(Z_{2^{r+e}} \times Z_{2^{1+f}}) \leq 2^{r+2}$.*

(ii) *If u_y, $y \in G$, is a group-like element such that $\overline{y} \in Z_{2^{r+e}} \times Z_{2^{1+f}}$ and $u_y^{-1}u_{\gamma_i}$ centralizes K_N, then u_y is of order 2 modulo K_N^*.*

(iii) *There are elements $\gamma_1, \gamma_2, \ldots, \gamma_m$ such that*

$$G/N \cong Z_{2^{r+e}} \times Z_{2^{1+f}} \times Z_{2^{s_1}} \times \cdots \times Z_{2^{s_m}} = < \overline{\sigma}_1, \overline{\sigma}_2, \overline{\gamma}_1, \ldots, \overline{\gamma}_m >$$

and such that for all i, u_{γ_i} centralizes K_N. ∎

Denote by Γ the group of group-like elements in $k^\alpha G$. Using Lemma 3.3 we may assume that G/N decomposes as in (iii). We consider two cases:

CASE (1): $\mathrm{ord}(Z_{2^{r+e}} \times Z_{2^{1+f}}) \leq 2^{r+2}$, CASE (2): $\operatorname{ord}(Z_{2^{r+e}} \times Z_{2^{1+f}}) = 2^{r+3}$.

Note that Case (1) includes the case of positive characteristic and in that case $r + e = 0$.

CASE (1): Consider the division algebra $D_0 = k^\alpha < N, \gamma_1, \ldots, \gamma_m >$. As in section 2, conjugation by elements of Γ induces an action of $G/ < N, \gamma_1, \ldots, \gamma_m > \cong Z_{2^{r+e}} \times Z_{2^{1+f}}$ on $L = Z(D_0)$. Furthermore, $L^{G/<N,\gamma_1,\ldots,\gamma_m>} = k$ since $k = Z(k^\alpha G)$. But, by construction, $K_N \subseteq L$ (the elements u_{γ_i}, $i = 1, \ldots, m$ centralize K_N) and so $\dim(L/k) \geq 2^{r+1}$. We claim $\dim(L/k) = \operatorname{ord}(G/ < N, \gamma_1, \ldots, \gamma_m >)$. If not, there is an element $z \in G$, z not in $< N, \gamma_1, \ldots, \gamma_m >$, such that u_z centralizes L and its order modulo D_0^* is 2. Applying the argument of Lemma 2.3 we obtain a division algebra $D_1 = k^\alpha < N, \gamma_1, \ldots, \gamma_m, z >$ with center L_1, of dimension at least 2^{r+2} over k and such that $L_1^{G/<N,\gamma_1,\ldots,\gamma_m,z>} = k$. But this is impossible since by the assumption of Case (1), $\operatorname{ord}(G/ < N, \gamma_1, \ldots, \gamma_m, z >) \leq 2^{r+1}$. This proves the claim.

Following the steps as in the previous section we consider the subalgebra $L(u_{\sigma_1}, u_{\sigma_2}) \leq k^\alpha G$. By what we have just done,

$$\operatorname{Gal}(L/k) = G/ < N, \gamma_1, \ldots, \gamma_m >$$

and $L(u_{\sigma_1}, u_{\sigma_2})$ is isomorphic to a crossed-product algebra $(L/k, \operatorname{Gal}(L/k))$. In particular, in the case of positive characteristic we see that L/k is a cyclic extension of degree at most 4.

We want to apply the factorization lemma from section 2 to factor the algebra $L(u_{\sigma_1}, u_{\sigma_2})$ off from $k^\alpha G$. We therefore need to show two things:

(i) The field generated by L is a twisted group algebra $k^\alpha U$ for some subgroup U of G.

(ii) The subgroup $< U, \sigma_1, \sigma_2 >$ is normal in G.

It will then follow (see the argument at the end of Theorem 3) that $k^\alpha G \cong k^\alpha < U, \sigma_1, \sigma_2 > \bigotimes_k k^\beta(\Phi/k^*)$, where Φ/k^* is a finite abelian group and $k^\beta(\Phi/k^*)$ is a product of quaternion algebras.

In the present situation (ii) follows at once because $G' \leq N \leq L^*$. Let us show (i). The argument is the same as in Lemma 2.4. Indeed, we build a maximal field of the form $K_{H_0} = k^\alpha H_0$ where $N \leq H_0 \leq < N, \gamma_1, \ldots, \gamma_m >$ and show that $K_{H_0}^{\gamma_i}$, the invariant subfield of K_{H_0} under the action of γ_i, is spanned by group-like elements. For this (as in Section 2) it is sufficient to show that for every $z \in H_0$, $u_{\gamma_i} u_z u_{\gamma_i}^{-1} = \lambda u_z$ where $\lambda \in k^*$. To see this we consider the field extension $k(u_z)/k$. Clearly it is abelian, since K_{H_0}/k is abelian. Furthermore, $k(u_z)$ is normalized by the action of G (which is induced by conjugation with group-like elements). Next, note that $\exp(< N, \gamma_1, \ldots, \gamma_m > /H_0) = 2$ and so every u_{γ_i} induces an automorphism of $k(u_z)$ of order at most 2. Now $\gamma_i z \gamma^{-1} z^{-1} \in G'$ and so $u_{\gamma_i} u_z u_{\gamma_i}^{-1} = \lambda u_z$, where $\lambda \in K_{G'} \subseteq K_N$. But u_{γ_i} centralizes K_N and u_{γ_i} induces an automorphism of $k(u_z)$ of order at most 2, so $\lambda \in \{+1, -1\} \subset k^*$.

The proof now proceeds exactly as in section 2 and so we obtain Theorem 4 in Case (1). Note that, in particular, we have seen that this case includes the case of positive characteristic and that in positive characteristic L/k is a cyclic extension of degree at most 4. But in fact we can now see that degree 4 cannot occur in positive characteristic: By the argument above L is a twisted group algebra $k^\alpha U$. Since L/k is cyclic, the group U must be cyclic and so $L = k(u)$, where $u^4 \in k$. But since k does not contain $\sqrt{-1}$, this is impossible by Proposition 2.6. We therefore have the full part one of the theorem.

We consider now Case (2), that is $\mathrm{ord}(Z_{2^{r+e}} \times Z_{2^{1+f}}) = 2^{r+3}$, so $e = f = 1$. We let $D_0 = k^\alpha < N, \gamma_1, \ldots, \gamma_m >$ and $L = Z(D_0)$. Again, by Lemma 3.3, we have that $K_N \subseteq L$ and, since $L^{Z_{2^{r+1}} \times Z_4} = k$, we have that $2^{r+1} \leq \dim_k(L) \leq 2^{r+3}$. Arguing as in Case (1) one shows that $\dim_k(L) \neq 2^{r+2}$ and if $\dim_k(L) = 2^{r+3}$ then the subalgebra $L(u_{\sigma_1}, u_{\sigma_2}) \subseteq k^\alpha G$ gives a crossed-product algebra $(L/k, \mathrm{Gal}(L/k))$ with $\mathrm{Gal}(L/k) \cong Z_{2^{r+1}} \times Z_4$ and that this algebra can be factored from $k^\alpha G$. Hence we have Theorem 4 in this case, if we can show that $r = 0$. We will do so after we consider the other cases.

Now assume $\dim_k(L) = 2^{r+1}$ and hence $L = K_N$. Consider the field $L(u_{\gamma_{i_0}})/k$, some $i_0 = 1, \ldots, m$. Clearly, the subgroup $S = < \bar{\sigma}_1, \bar{\sigma}_2 > \cong Z_{2^{r+1}} \times Z_4$ of G/N acts on $L(u_{\gamma_{i_0}})/k$. Note that $\dim_k(L(u_{\gamma_{i_0}})) = 2^{r+2}$. *Assume* $L(u_{\gamma_{i_0}})^S = k$. Then we can multiply, if necessary, each u_{γ_j}, $j \neq i$ by a group-like element u_w, $w = w(j) \in S$ and get group-like elements $u_{\gamma_j'} = u_{w(j)} u_{\gamma_j}$, $j = 1, \ldots, m$ that centralize $L(u_{\gamma_{i_0}})$. It follows that

$$L' = Z(D_0') = Z(k^\alpha < N, \gamma_1', \ldots, \gamma_m' >)) \supseteq L(u_{\gamma_{i_0}})$$

and therefore $\dim_k(L') \geq \dim_k(L(u_{\gamma_{i_0}})) = 2^{r+2}$. Then just as above $\dim_k(L')$ must equal 2^{r+3} and the algebra $L'(u_{\sigma_1}, u_{\sigma_2})$ is a crossed-product algebra $(L', \mathrm{Gal}(L', k))$ with $\mathrm{Gal}(L', k) \cong Z_{2^{r+1}} \times Z_4$ that can be factored from $k^\alpha G$. Again we need to show $r = 0$ and will do so after we consider the next case.

Finally, we consider the case where $L(u_{\gamma_{i_0}})^S \neq k$. Then $(L(u_{\gamma_{i_0}})^S : k) \geq 2$. Recall that $L^S = k$ and $(L(u_{\gamma_{i_0}}) : L) = 2$. Consider the maps $S \xrightarrow{\phi} \mathrm{Gal}(L(u_{\gamma_{i_0}})/k) \xrightarrow{\nu} \mathrm{Gal}(L/k)$. We know that ϕ is not surjective onto $\mathrm{Gal}(L(u_{\gamma_{i_0}})/k)$ but its composition with ν is surjective onto $\mathrm{Gal}(L/k)$. It follows that $\mathrm{im}(\phi)$ is mapped isomorphically onto $\mathrm{Gal}(L/k)$ by ν and so

$$\ker(S \to \mathrm{Gal}(L(u_{\gamma_{i_0}})/k) = \ker(S \to \mathrm{Gal}(L/k)).$$

Let u_x be a group-like element, where x is in S but not in N. Furthermore, assume that u_x centralizes $L = K_N$ (such an element does exist since $\mathrm{ord}(S/N) = 2^{r+3}$ and $\dim_k(L) = 2^{r+1}$). The equality of the kernels above says that u_x and $u_{\gamma_{i_0}}$ commute. Repeating this argument for all γ_i, we see that we can assume that u_x commutes with $u_{\gamma_i}, i = 1, \ldots, m$. Consider the twisted group algebra $D_1 = k^\alpha < N, \gamma_1, \ldots, \gamma_m, x >$. By the discussion above $k^\alpha < N, x >$ is contained in L_1, the center of D_1, and therefore $\dim_k(L_1) \geq \dim_k(k^\alpha < N, x >) \geq 2^{r+2}$. This case then proceeds just as the two previous ones.

At this point we have shown that if the characteristic of k is zero, then either D is a tensor product of quaternion algebras or $D \cong D_1 \otimes_k \cdots \otimes D_n$ where D_i, $i = 1, \ldots, n-1$ are quaternion algebras and D_n is isomorphic to a crossed product $(K/k, H = \mathrm{Gal}(K/k))$ where $H \cong Z_{2^r} \times Z_{2^s}$ and $r \geq 1$ and $1 \leq s \leq 2$. We claim in fact $H \cong Z_{2^r} \times Z_{2^4}$ with $r \geq 2$ does not occur. This will finish the theorem. To see this recall that we have shown that the field extension K is a twisted group algebra $K = k^\alpha U$. It follows that U must be a cyclic group: If not, U contains $Z_2 \times Z_2 \times Z_2$ or $Z_2 \times Z_4$. If U contains $Z_2 \times Z_2 \times Z_2$, then K will contain three quadratic extensions no one of which is contained in the field generated by the others. It follows that the Galois group of K/k maps onto $Z_2 \times Z_2 \times Z_2$, a contradiction. If U contains $Z_2 \times Z_4$, then K contains a subfield $F = k^\alpha(Z_4)$ which, by Proposition 2.6, will be Galois with group $Z_2 \times Z_2$. But K will also contain $k^\alpha(Z_2)$ from the other factor of U and this quadratic will not be a subfield of F. Again it follows that the Galois group of K/k maps onto $Z_2 \times Z_2 \times Z_2$, a contradiction. So U must be cyclic. But then, by Proposition 2.6, we know H is of the form $Z_{2^r} \times Z_2$. This proves the claim.

This finishes the proof of Theorem 4. ∎

References

[A] S. Amitsur, *Finite subgroups of division rings*, Transactions of the American Mathematical Society **80** (1955), 361–386.

[AGO] E. Aljadeff, Y. Ginosar and U. Onn, *Projective representations and relative semisimplicity*, Journal of Algebra, to appear.

[AS1] E. Aljadeff and J. Sonn, *Projective Schur division algebras are abelian crossed products*, Journal of Algebra **163** (1994), 795–805.

[AS2] E. Aljadeff and J. Sonn, *Projective Schur algebras have abelian splitting fields*, Journal of Algebra **175** (1995), 179–187.

[AS3] E. Aljadeff and J. Sonn, *On the projective Schur group of a field*, Journal of Algebra **178** (1995), 530–540.

[AS4] E. Aljadeff and J. Sonn, *Projective Schur algebras of nilpotent type are Brauer equivalent to radical algebras*, Journal of Algebra **220** (1999), 401–414.

[AS5] E. Aljadeff and J. Sonn, *Exponent reduction for radical abelian algebras*, Journal of Algebra **223** (2000), 527–534.

[K] G. Karpilovsky, *Field Theory*, Dekker, New York, 1988.

[LO] F. Lorenz and H. Opolka, *Einfache Algebren und projektive Darstellungen uber Zahlkopern*, Mathematische Zeitschrift **162** (1978), 175–182.

[NV] P. Nelis and F. Van Oystaeyen, *The projective Schur subgroup of the Brauer group and root groups of finite groups*, Journal of Algebra **137** (1991), 501–518.

[S] A. Schinzel, *Abelian binomials, power residues, and exponential congruences*, Acta Arithmetica **32** (1977), 245–274.

[Sh] M. Shirvani, *The finite inner automorphism groups of division rings*, Mathematical Proceedings of the Cambridge Philosophical Society **118** (1995), 207–213.

[Y] T. Yamada, *The Schur Subgroup of the Brauer Group*, Springer-Verlag, New York/Berlin, 1970.