ISRAEL JOURNAL OF MATHEMATICS 146 (2005), 317–335

PROJECTIVE BASES OF DIVISION ALGEBRAS AND GROUPS OF CENTRAL TYPE

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

AND

MICHAEL NATAPOV

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

ABSTRACT

Let k be a field. For each finite group G and two-cocyle f in $Z^2(G, k^\times)$ (with trivial action), one can form the twisted group algebra $k^fG = \bigoplus_{\sigma\in G} kx_\sigma$ where $x_\sigma x_\tau = f(\sigma,\tau)x_{\sigma\tau}$ for all $\sigma, \tau \in G$. Our main result is a short list of p-groups containing all the p-groups G for which there is a field k and a cocycle such that the resulting twisted group algebra is a k-central division algebra. We also complete the proof (presented in all but one case in a previous paper by Aljadeff and Haile) that every k-central division algebra that is a twisted group algebra is isomorphic to a tensor product of cyclic algebras.

Received December 31, 2003

1. Introduction

Let k be a field. For each finite group G and two-cocyle f in $Z^2(G, k^\times)$ (with trivial action), one can form the twisted group algebra $k^fG = \bigoplus_{\sigma\in G} kx_\sigma$ where $x_\sigma x_\tau = f(\sigma,\tau)x_{\sigma\tau}$ for all $\sigma,\tau \in G$. The resulting k-algebra depends (up to k-isomorphism) only on the class α (say) of f in $H^2(G, k^\times)$, and so we denote the algebra $k^\alpha G$. One can characterize twisted group algebras in a more elementary way: They are precisely the k-algebras that possess a "projective" basis, that is a basis $\{a_1, a_2, \ldots, a_n\}$ such that for every pair i, j there is an m such that $a_i a_j = k_{ij} a_m$ for some $k_{ij} \in k^\times$.

If α is trivial then $k^\alpha G$ is the group algebra of G over k, which is semisimple if the characteristic of k does not divide $|G|$, but not simple if G is not trivial. If α is not trivial, however, the algebra $k^\alpha G$ may be simple. For example if k contains ω, a primitive n-th root of unity, and $a, b \in k^\times$, then the symbol algebra $(a, b)_\omega$ (that is, the k-algebra generated by two elements x, y subject to $x^n = a$, $y^n = b$, and $yx = \omega xy$) is a k-central simple algebra and the elements $x^i y^j$, for $0 \le i, j \le n-1$ form a projective basis and so $(a, b)_\omega \cong k^\alpha(Z_n \times Z_n)$ for some cocycle α, where Z_n denotes the cyclic group of order n.

In this paper we continue the investigation, begun in [1], of those twisted group algebras over a field k that are in fact k-central division algebras. Our main result is a short list of p-groups containing all the p-groups G for which there is a field k and a cocycle α such that $k^\alpha G$ is a k-central division algebra. In a subsequent paper the third author will prove, among other things, that the groups that can occur (proved to be nilpotent in [1]) are precisely the products of the groups on this list and so the classification of such groups will be complete. In [1] it was shown that if $k^\alpha G$ is a k-central division algebra, then $k^\alpha G$ is isomorphic to a tensor product of cyclic algebras, except possibly in the case where G is a 2–group and k does not contain $\sqrt{-1}$. In the last section of this paper we remove that exception, and hence show that every k-central division algebra of the form $k^\alpha G$ is a tensor product of cyclics.

One of the motivations for this study comes from the theory of group representations. To describe this we will let $k = \mathbb{C}$ and Γ a finite group. It is well known that if $\phi\colon \Gamma \to GL(V)$ is an irreducible representation, then the degree of the representation, that is the dimension of the vector space V over $\mathbb{C}$, is not greater than the square root of $[\Gamma : Z(\Gamma)]$, where $Z(\Gamma)$ denotes the center of Γ. The group Γ is said to be of **central type** if it admits an irreducible representation of degree equal to the square root of $[\Gamma : Z(\Gamma)]$. For example, the dihedral group of order 8 admits an irreducible representation of degree 2 and

so is of central type. Using the classification of finite simple groups, Howlett and Isaacs proved that if Γ is of central type then it is solvable ([3, Theorem 7.3]).

Now recall that a **projective representation** of a group G is a function $\phi\colon G \to GL(V)$ such that its composition with the canonical projection from $GL(V)$ to $PGL(V)$ is a group homomorphism. Given a projective representation ϕ, the map $f\colon G\times G \to \mathbb{C}$ given by $f(\sigma,\tau) = \phi(\sigma)\phi(\tau)(\phi(\sigma\tau)^{-1})$ is a two-cocycle and so represents a class α in $H^2(G,\mathbb{C}^\times)$. This map endows V with the structure of $\mathbb{C}^\alpha G$-module.

Now assume we have a group Γ such that $\Gamma/Z \cong G$, where Z is the center of Γ. The group extension $1 \to Z \to \Gamma \to G \to 1$ gives rise to a two-cocycle $g\colon G\times G \to Z$. If $\phi\colon \Gamma \to GL(V)$ is an irreducible representation, then it induces a projective representation of $G = \Gamma/Z$ and so V becomes a module for $\mathbb{C}^\alpha G$, where α is the cocycle class arising from the two-cocycle $\phi \circ g$. In particular, if the dimension of V is the square root of $[\Gamma : Z] = |G|$, then the algebra $\mathbb{C}^\alpha G$ is isomorphic to $M_n(\mathbb{C})$ where n is the order of G. Thus if Γ is of central type, then the algebra $\mathbb{C}^\alpha G$ is a central simple $\mathbb{C}$-algebra, for some cocycle class α. By abuse of language, we also call such groups G central type, that is groups G for which there is a cocycle α with $\mathbb{C}^\alpha G$ central simple over $\mathbb{C}$ (and hence isomorphic to $M_n(\mathbb{C})$). In fact one can show that a group G is of central type in this new sense if and only if G is isomorphic to a quotient $\Gamma/Z(\Gamma)$ where Γ is of central type in the classical sense. Note that the result of Howlett and Isaacs holds for groups of central type in this new sense.

Returning to our original setting of a twisted group algebra $k^\alpha G$, we see that if $k^\alpha G$ is k-central division algebra (or more generally k-central simple), and k is a subfield of the complex numbers, then G is a group of central type. It is therefore natural to examine such algebras.

2. Main results

Let G be a finite group and α a cocycle class on G. If $A = k^\alpha G = \bigoplus kx_\sigma$ is the twisted group algebra, we let Γ denote the subgroup of $A^\times$ generated by $\{x_\sigma | \sigma \in G\}$ and $k^\times$. The group Γ spans A as a vector space over k. We will often write $A = k(\Gamma)$. We have $\Gamma/k^\times \cong G$ and we will denote this map by π. We will refer to the elements of Γ as the **grouplike** elements of A and if u in Γ maps to σ in G, then we say the **weight** of u is σ. For each element σ in G conjugation by u_σ (an element of weight σ) is a k-algebra automorphism of A and this automorphism is independent of which grouplike element of weight σ is

used. This results in a group homomorphism from G to the group of k-algebra automorphisms of A.

The group Γ is center-by-finite, so by a theorem of Schur ([5, Theorem 9.8, Chapter 2]), its commutator subgroup Γ' is finite. It is easy to see that $k^\times\Gamma'/k^\times \cong G'$. It follows that $k(\Gamma')$ is a subalgebra of A isomorphic to the twisted group algebra $k^\alpha G'$. Because Γ' is finite there is a representative f of α which takes finite values on G', that is for all $\sigma, \tau \in G'$, $f(\sigma,\tau) \in \mu \subseteq k^\times$, where μ denotes the group of roots of unity in k. Moreover, by ([5, Lemma of Chapter 2, section 9]), if G is a p-group, then the values of f on G' are p-power roots of unity. We say that a cohomology class is of **finite type** if it can be represented by a two cocycle which takes finite values in k.

Now assume $k^\alpha G$ is a k-central division algebra. By [1, Theorems 1 and 2] the commutator subgroup G' is cyclic. Moreover, G is nilpotent and $k^\alpha G$ is isomorphic to $k^{\alpha_1}P_1 \otimes k^{\alpha_2}P_2 \otimes \cdots \otimes k^{\alpha_m}P_m$, where $P_1, P_2, \ldots, P_m$ are the Sylow p-subgroups of G and α_i is the restriction of α to P_i. From here on we will consider the case where G is a p-group.

As in [1] the analysis breaks up naturally into two different cases, having to do with the prime 2. We will distinguish these cases as follows. In *case one* either the prime p is odd or $p = 2$ and k contains $\sqrt{-1}$. In *case two* we assume $p = 2$ and k does not contain $\sqrt{-1}$.

Now assume we are in case one. Let G be a p-group and α a cocycle such that $D = k^\alpha G$ is a k-central division algebra. Because G' is cyclic the algebra $k^\alpha G'$ is a field extension and because the restriction of α to G' is of finite type, this extension is p-cyclotomic, that is there is a p-power root of unity ζ such that $k^\alpha G' = k(\zeta)$. In particular if the field k contains all p-power roots of unity, then G is abelian. In that case the structure of G is well known — it is an abelian group of **symmetric type**, that is of the form $H \times H$ where H is an abelian p-group. On the other hand k must contain a primitive p-th root of unity, because otherwise the degree of $k^\alpha G'$ over k is not a power of p. So we will assume k contains a primitive p^s-root of unity ($s \geq 1$), but does not contain a primitive p^{s+1}-root of unity.

We can now state our main result in case one.

THEOREM 1: *Let k be a field. Let p be a prime. If $p = 2$ assume k contains $\sqrt{-1}$. Let s be the largest positive integer such that $k \supseteq \mu_{p^s}$ (so $s \geq 1$ and $s \geq 2$ if $p = 2$). If G is a p-group such that there is a class $\alpha \in H^2(G, k^\times)$ with $k^\alpha G$ a k-central division algebra, then one of the following occurs:*

(1) *G is abelian of symmetric type and $\exp(G) \leq p^s$.*

(2) *There is an integer* $n > s$ *such that* $G \cong H_1 \times H_2$ *where* H_1 *is the semidirect product*

$$H_1 = Z_{p^n} \rtimes Z_{p^n} =< \pi, \sigma | \pi^{p^n} = \sigma^{p^n} = 1 \text{ and } \sigma\pi\sigma^{-1} = \pi^{p^s+1} >$$

and H_2 *is abelian of symmetric type and* $\exp(H_2) \leq p^s$.

Here is the result in case two.

THEOREM 2: *Let* k *be a field,* k *not containing* $\sqrt{-1}$. *If* G *is a 2-group such that there is a class* $\alpha \in H^2(G, k^\times)$ *with* $k^\alpha G$ *a* k*-central division algebra, then one of the following occurs:*

(1) G *is an elementary abelian 2–group of symmetric type.*

(2) *There is an integer* n *such that* $G \cong H_1 \times H_2$, *where* H_1 *is the semidirect product*

$Z_{2^{n+1}} \rtimes (Z_{2^n} \times Z_2)$ *given by generators and relations as follows:*

$$H_1 =< \pi, \sigma, \tau | \pi^{2^{n+1}} = \sigma^{2^n} = \tau^2 = 1 \text{ and } \sigma\pi = \pi^3\sigma, \tau\pi = \pi^{-1}\tau >$$

and H_2 *is an elementary abelian 2-group of symmetric type.*

Combining Theorems 1 and 2, we get the promised list of groups:

COROLLARY 3: *Let* p *be a prime and let* G *be a* p*-group. If there is a field* k *and a cocycle* $\alpha \in H^2(G, k^\times)$ *such that* $k^\alpha G$ *is a* k*-central division algebra, then* $G \cong G_1 \times G_2$ *where* G_1 *is one of the following groups:*

(1) *Abelian of symmetric type,*

(2) $Z_{p^n} \rtimes Z_{p^n} =< \pi, \sigma | \pi^{p^n} = \sigma^{p^n} = 1 \text{ and } \sigma\pi\sigma^{-1} = \pi^{p^s+1} >$ *where* $n > s \geq 1$ *and* $s \geq 2$ *if* $p = 2$,

(3) $Z_{2^{n+1}} \rtimes (Z_{2^n} \times Z_2) =< \pi, \sigma, \tau | \pi^{2^{n+1}} = \sigma^{2^n} = \tau^2 = 1 \text{ and } \sigma\pi = \pi^3\sigma, \tau\pi\tau^{-1} = \pi^{-1} >$ *where* $n \geq 1$,

and G_2 *is abelian of symmetric type such that* $\exp(G_2) \leq \exp(G_1)/|G_1'|$.

3. Structure of the group in case one

In this section we will prove Theorem 1. We begin by recalling the notation and set-up of the proof of Theorem 3 in [1].

Let G be a finite nonabelian p-group and α a cocycle class on G such that $D = k^\alpha G$ is a k-central division algebra. Since we are in case one, we are assuming p is odd or $p = 2$ and $\sqrt{-1} \in k$.

Consider the nonempty family

$$\{H \leq G | H \supset G' \text{ and } k^\alpha H/k \text{ is a } p\text{-cyclotomic field extension}\}.$$

Let N be a maximal subgroup in this set and let $|N| = p^r$. We have $r \geq 1$. The subgroup N is normal with abelian quotient and by [1, Proposition 2.6] the extension $k^\alpha N/k$ is cyclic. Let K_N denote this extension (so $K_N = k^\alpha N$). The field K_N is normalized by every grouplike element of D. The next result ([1, Theorem 2.1]) establishes a connection between the structure of G and p^s — the number of p-power roots of unity in k.

THEOREM 4: *Let $\sigma \in G$ and $u_\sigma \in D$ of weight σ. If u_σ centralizes K_N, then the order of u_σ modulo $K_N^\times$ (equivalently, the order of σ modulo N) divides p^s.*

Let $G/N \cong Z_{p^{n_1}} \times Z_{p^{n_2}} \times \cdots \times Z_{p^{n_m}}$. The group G maps onto the Galois group $Gal(K_N/k)$ (because the elements of the fixed field K_N^G commute with every element in D). The group N is in the kernel of this map. It follows that at least one cyclic component of G/N must map onto $Gal(K_N/k)$. So we may assume $Z_{p^{n_1}}$ maps onto $Gal(K_N/k)$. It follows that $n_1 = r + e$ for some $e \geq 0$. The next lemma ([1, Lemma 2.2] is a consequence of Theorem 4.

LEMMA 5: *Let $G/N \cong Z_{p^{r+e}} \times Z_{p^{n_2}} \times \cdots \times Z_{p^{n_m}}$ and let p^s be the number of p-power roots of unity in k. Then $e \leq s$ and $n_i \leq s$ for all $i = 2, \ldots, m$.*

Let $\sigma, \tau_2, \tau_3, \ldots, \tau_m$ be elements of G such that $\overline{\sigma}, \overline{\tau_2}, \overline{\tau_3}, \ldots, \overline{\tau_m}$ generate the cyclic components of G/N. Consider the subalgebra

$$D_0 = k^\alpha < N, \tau_2, \tau_3, \ldots, \tau_m >$$

and let L denote its center. The element σ has order p^{r+e} modulo the subgroup $< N, \tau_2, \tau_3, \ldots, \tau_m >$ and so if $u_\sigma \in D$ has weight σ then the order of u_σ modulo $D_0^\times$ is also p^{r+e}. Conjugation by u_σ preserves D_0 and so also preserves L.

The following statements follow from Lemmas 2.3–2.7 in [1].

- The action of u_σ on L induces an isomorphism of the cyclic group of order p^{r+e} generated by $u_\sigma D_0^\times$ with $Gal(L/k)$.
- The field L is generated by grouplike elements, that is there is a subgroup U of G such that $L = k^\alpha U$. The subgroup U is cyclic and normal in G.
- The element σ in G has order p^{r+e} and so the subalgebra $D_1 = k^\alpha < U, \sigma >$ is a cyclic crossed product over k.
- The subgroup $< U, \sigma >$ is normal in G.

Using the Factorization Lemma in [1] it now follows that the subalgebra $k^\alpha < U, \sigma >$ can be factored from $k^\alpha G$. More precisely, there is a two-cocycle β on $G/ < U, \sigma >$ such that

$$k^\alpha G \cong k^\alpha < U, \sigma > \otimes k^\beta G/ < U, \sigma > .$$

Our first new result in this paper is an improved version of the factorization lemma which will imply that not only the algebra, but the group G itself factors, that is $G \cong < U, \sigma > \times G/ < U, \sigma >$. The crucial fact, which we prove in the next lemma, is that for each $z \in G$, the action of z on $k^\alpha < U, \sigma >$ is realizable by an element of $< U, \sigma >$.

LEMMA 6: *For each $z \in G$ there is an element $y \in < U, \sigma >$ such that the action of z on $k^\alpha < U, \sigma >$ is the same as the action of y on $k^\alpha < U, \sigma >$.*

Proof: Recall that $L = k^\alpha U$ is a cyclic extension of k of degree p^{r+e} and U is a cyclic group. Let π be a generator of U. Let u_σ and u_π be elements of weight σ and π, respectively. Let $h = \sigma\pi\sigma^{-1}\pi^{-1}$ and let $u_h = u_\sigma u_\pi u_\sigma^{-1} u_\pi^{-1}$. Then $u_\sigma u_\pi u_\sigma^{-1} = u_h u_\pi$, so u_h lies in L and is a primitive p^{r+e}-root of unity.

Now let $z \in G$ and let u_z be an element of weight z. Let $\lambda = z\sigma z^{-1}\sigma^{-1}$ and let $u_\lambda = u_z u_\sigma u_z^{-1} u_\sigma^{-1} \in \Gamma'$, the commutator subgroup of the group of grouplike elements of $k^\alpha G$. In the proof of Lemma 2.7 of [1] it was shown that $\lambda \in < h >$. In particular $u_\lambda \in L$.

Let $D_1 = k^\alpha < U, \sigma >$. The division algebra D_1 is generated as a k-algebra by u_π and u_σ and the subgroup $< U, \sigma >$ is generated by π and σ. We need to prove that conjugation by u_z is realizable by conjugation by an element of the form $u_\pi^i u_\sigma^j$, that is

$$u_z d u_z^{-1} = u_\pi^i u_\sigma^j d (u_\pi^i u_\sigma^j)^{-1}$$

for all $d \in D_1$. First, because conjugation by u_σ generates the Galois group of L over k, there is an integer j_0 such that $u_z u_\pi u_z^{-1} = u_\sigma^{j_0} u_\pi u_\sigma^{-j_0}$.

Secondly, we have $u_z u_\sigma u_z^{-1} = u_\lambda u_\sigma$. As we saw above $u_\lambda \in \Gamma'$. It follows [5, Lemma of Chapter 2, section 9] that u_λ is a p-power root of unity. Because $\lambda \in < h >$ and u_h is also a p-power root of unity, it follows that $u_\lambda = u_h^{-i_0}$ for some integer i_0. Hence

$$u_\pi^{i_0} u_\sigma u_\pi^{-i_0} = u_h^{-i_0} u_\sigma = u_\lambda u_\sigma = u_z u_\sigma u_z^{-1}.$$

Thus $u_\pi^{i_0} u_\sigma^{j_0}$ and u_z act in same way on D_1. ∎

Theorem 1 will now be a consequence of the next result, a version of the factorization lemma of [1]. We will need the result more than once, so we state it in suitable generality. If H is any normal subgroup of a group G, then the action of G on $k^\alpha G$ preserves the subalgebra $k^\alpha H$. If $k^\alpha H$ is simple with center k, then this action is necessarily inner (but not necessarily given by the action of an element of H).

THEOREM 7: *Let $k^\alpha G$ be a twisted group division algebra with center k and let H be a normal subgroup of G such that the subalgebra $k^\alpha H$ is k-central. Suppose for all $z \in G$, there is an element $h \in H$ such that the action of z on $k^\alpha H$ is the same as the action of h on $k^\alpha H$. Let $E = \{\sigma \in G |\ \sigma$ acts trivially on $k^\alpha H\}$. Then we have the following:*

(1) *$G = HE$ and $H \cap E = 1$, so $G \cong H \times E$.*

(2) *The subalgebra $k^\alpha E$ has center k and $k^\alpha G$ is canonically isomorphic to $k^\alpha H \otimes k^\alpha E$.*

Proof: (1) We have $H \cap E = 1$ because the center of $k^\alpha H$ is k. Now let $z \in G$. By our assumption there is an element $h \in H$ such that the action of z on $k^\alpha H$ is the same as the action of h. But then $h^{-1}z \in E$, so $z \in HE$.

(2) By the definition of E, the subalgebra $k^\alpha E$ centralizes the subalgebra $k^\alpha H$. Because $G = HE$, we have $k^\alpha G = (k^\alpha H)(k^\alpha E)$. Therefore, there is a canonical homomorphism from $k^\alpha H \otimes_k k^\alpha E$ onto $k^\alpha G$. By dimension count this map is an isomorphism. It follows that the center of $k^\alpha E$ is k. ∎

COROLLARY 8: *Let G, U, σ be as described above. Let*

$$E = \{\gamma \in G |\ \gamma \text{ acts trivially on } k^\alpha < U, \sigma >\}.$$

Then G is canonically isomorphic to $< U, \sigma > \times E$. Moreover, $k^\alpha E$ is k-central and $k^\alpha G$ is canonically isomorphic to $k^\alpha < U, \sigma > \otimes_k k^\alpha E$.

We want to arrange things so that the subgroup E of the corollary is abelian. To do that we need to be more careful about our choice of generators for the cyclic components of G/N.

LEMMA 9: *Let G and N be as described above. There exist elements $\sigma, \tau_2, \tau_3, \ldots, \tau_m$ in G such that:*

(1) *$G/N \cong < \overline{\sigma} > \times < \overline{\tau_2} > \times < \overline{\tau_3} > \times \cdots \times < \overline{\tau_m} >$.*

(2) *The action of σ on K_N generates the Galois group $Gal(K_N/k)$.*

(3) *For all i the action of τ_i on K_N does <u>not</u> generate $Gal(K_N/k)$.*

Proof: As observed after Theorem 4, one of the components of G/N must map onto $Gal(K_N/k)$ and so must have order at least p^r. We can therefore choose an element σ such that $< \overline{\sigma} >$ is a cyclic component of G/N, the action of σ on K_N generates the Galois group, and such that the order of $\overline{\sigma}$ in G/N is as small as possible. With that choice of σ let $\tau_2, \tau_3, \ldots, \tau_m \in G$ be chosen so that $G/N \cong < \overline{\sigma} > \times < \overline{\tau_2} > \times < \overline{\tau_3} > \times \cdots \times < \overline{\tau_m} >$. Suppose for some i the

action of τ_i also generates $Gal(K_N/k)$. Then there is a positive integer c such that $\gamma_i = \sigma^c\tau_i$ acts trivially on K_N. Since the order of $\overline{\sigma}$ is less than or equal to the order of $\overline{\tau_i}$, it follows that $\overline{\gamma_i}$ and $\overline{\tau_i}$ have the same order. Moreover, if we replace τ_i by γ_i and keep the remaining generators, we still obtain a cyclic decomposition of G/N. By continuing in this way for every τ_j such that the action generates the Galois group of K_N, we obtain a set of generators of the desired kind. ∎

We now repeat the constructions following Lemma 5 with this special set of generators. In particular, we have the cyclic normal subgroup U such that $L = k^\alpha U$. By Corollary 8 we have $G \cong < U, \sigma > \times E$ and $k^\alpha G \cong k^\alpha < U, \sigma > \otimes k^\alpha E$.

PROPOSITION 10: *With the choice of generators as in the previous lemma, the subgroup E is abelian.*

Proof: We first claim that $G' \cap U \neq \{1\}$. We have $G' \subseteq N$ and N is cyclic. Let H be the unique subgroup of order p in N. Then $H \subseteq G'$. By our choice of generators the action of no τ_i generates the Galois group of $K_N = k^\alpha N$. In other words, for all i, the action of τ_i lies in the subgroup of $Gal(K_N/k)$ generated by the action of σ^p. It follows that for all i, the action of τ_i fixes elementwise the subfield $k^\alpha H$. Hence $k^\alpha H$ lies in the center of the algebra $k^\alpha < N, \tau_2, \ldots, \tau_m >$. But this center is $L = k^\alpha U$, so $H \subseteq U$ and $G' \cap U \neq \{1\}$. This proves the claim.

Now suppose E is not abelian. Then $k^\alpha E' \neq k$ is a p-cyclotomic subfield of $k^\alpha E$. Because $k^\alpha G \cong k^\alpha < U, \sigma > \otimes k^\alpha E$ we see that $k^\alpha(G' \cap U) \otimes k^\alpha E'$ is a subfield of $k^\alpha G$. But $k^\alpha(G' \cap U)$ is also p-cyclotomic and by the claim $k^\alpha(G' \cap U) \neq k$. Hence each of the fields $k^\alpha(G' \cap U)$ and $k^\alpha E'$ contains a primitive p^{s+1}-root of unity and so their tensor product is not a field, a contradiction. It follows that E is abelian. ∎

We can now finish the proof of Theorem 1. Using the special generators we have $G \cong < U, \sigma > \times E$ and E is abelian. Because $k^\alpha E$ is a k-central division algebra, the group E is of symmetric type ([1, Theorem 1.1]) and $k^\alpha E$ is a tensor product of symbol algebras. Because k does not contain a primitive p^{s+1}-root of unity, the symbol algebras have degree dividing p^s and so the exponent of E is bounded by p^s.

Finally, we analyze $< U, \sigma >$. Let $n = r + e$, so the order of U is p^n. As before we let π be a generator of U and choose elements u_σ and u_π of weights σ and π respectively. Let $h = \sigma\pi\sigma^{-1}\pi^{-1}$ and let $u_h = u_\sigma u_\pi u_\sigma^{-1} u_\pi^{-1}$. Because $h \in U$, there is an element $x \in k^\times$ and an integer m such that $u_h = x u_\pi^m$. Hence $u_\sigma u_\pi u_\sigma^{-1} = u_h u_\pi = x u_\pi^{m+1}$, and so $\sigma\pi\sigma^{-1} = \pi^{m+1}$. It follows that $< \pi^m >$ is

the commutator subgroup of $< U, \sigma >$. Let $m = cp^t$, where c is prime to p and $1 \leq t \leq n$.

We claim that $t = s$: Recall that $u_h = \zeta$ is a primitive p^n-root of unity. Because $u_\pi^{p^n} \in k^\times$, we have $(u_\pi^{cp^t})^{p^{n-t}} = x^{-p^{n-t}}\zeta^{p^{n-t}} \in k^\times$ and therefore $t \leq s$. On the other hand $\zeta^{p^{n-s}} \in k^\times$, hence $(u_\pi^{p^t})^{p^{n-s}} \in k^\times$. Therefore $t \geq s$. This proves the claim.

In summary, $< U, \sigma >$ is generated by σ and π and $\sigma\pi\sigma^{-1} = \pi^{cp^s+1}$. It now follows easily that $< U, \sigma >$ is isomorphic to the semidirect product:

$$Z_{p^n} \rtimes Z_{p^n} =< \pi, \sigma | \pi^{p^n} = \sigma^{p^n} = 1 \text{ and } \sigma\pi\sigma^{-1} = \pi^{p^s+1} > .$$

This finishes the proof of Theorem 1. ∎

4. Structure of the group in case two

In this section we prove Theorem 2. Let k be a field not containing $\sqrt{-1}$. Let G be a 2-group and α a cocycle on G such that $D = k^\alpha G$ is a k-central division algebra. The discussion at the beginning of section three still applies. In particular, G' is cyclic and $k^\alpha G'$ is a 2-cyclotomic extension of k. If θ generates G', then there is an element u_θ in $k^\alpha G'$ of weight θ such that $u_\theta^{|G'|} = -1$. As before we let N be a subgroup of G maximal subject to the properties: N contains G' and $K_N = k^\alpha N$ is a 2-cyclotomic extension of k. Let $|N| = 2^{r+1}, r \geq 0$. Then N is normal in G and K_N/k is a Galois extension. Unlike the case where p is odd, in the present case the Galois group of K_N/k may be noncyclic. In general, $Gal(K_N/k) \cong Z_{2^r} \times Z_2$ which is cyclic precisely when $r = 0$.

The canonical homomorphism from G to the group of k-algebra automorphisms of $k^\alpha G$ induces a surjective homomorphism η: $G/N \to Gal(K_N/k)$. Let $G/N \cong Z_{2^{s_1}} \times Z_{2^{s_2}} \times \cdots \times Z_{2^{s_t}}$. There must be two components, say $Z_{2^{s_1}} \times Z_{2^{s_2}}$, such that $\eta(Z_{2^{s_1}} \times Z_{2^{s_2}}) = Gal(K_N/k)$. Of course if $r = 0$ only one component is needed. We may assume that $s_1 \geq r$ and $s_2 \geq 1$, so that $G/N \cong Z_{2^{r+e}} \times Z_{2^{1+f}} \times Z_{2^{s_1}} \times \cdots \times Z_{2^{s_m}}$ where $e, f \geq 0, m \geq 0, s_i \geq 1$. By [1, Proposition 3.2], $e, f \leq 1$ and $s_i = 1$ for all i. Moreover, by [1, Lemma 3.3], we can choose generators $\overline{\sigma}, \overline{\tau}, \overline{\gamma_1}, \ldots, \overline{\gamma_m}$ such that

$$G/N \cong < \overline{\sigma} > \times < \overline{\tau} > \times < \overline{\gamma_1} > \times \cdots \times < \overline{\gamma_m} >$$

and such that for all i, γ_i centralizes K_N.

For each i let $u_{\gamma_i} \in k^\alpha G$ be an element of weight γ_i. Because for all i, $u_{\gamma_i}^2 \in K_N$ and γ_i acts trivially on K_N, we must have the multiplicative commutator

$(u_{\gamma_i}, u_{\gamma_j}) = \pm 1$ for all i, j. In particular, γ_i and γ_j commute for all i, j. Our first new step is to rewrite the generators $\overline{\sigma}, \overline{\tau}, \overline{\gamma_1}, \ldots, \overline{\gamma_m}$ so that for each i, $(u_{\gamma_i}, u_{\gamma_j}) = 1$ for all but at most one j.

LEMMA 11: *There are elements $\gamma_1, \gamma_2, \ldots, \gamma_m$ in G such that $G/N \cong Z_{2^{r+e}} \times Z_{2^{1+f}} \times Z_2 \times \cdots \times Z_2 \cong < \overline{\sigma} > \times < \overline{\tau} > \times < \overline{\gamma_1} > \times \cdots \times < \overline{\gamma_m} >$ and such that either $u_{\gamma_i}, u_{\gamma_j}$ commute for all i, j, or $(u_{\gamma_1}, u_{\gamma_2}) = -1$ and $u_{\gamma_1}, u_{\gamma_2}$ commute with all u_{γ_j} for $j > 2$.*

Proof: If there exist i, j such that u_{γ_i} and u_{γ_j} do not commute, we set, without loss of generality, $i = 1$ and $j = 2$. Now let $3 \leq t \leq m$. If $(u_{\gamma_1}, u_{\gamma_t}) = -1$ we let $\gamma_t' = \gamma_t \gamma_2$. Then $(u_{\gamma_1}, u_{\gamma_t'}) = (u_{\gamma_1}, u_{\gamma_t} u_{\gamma_2}) = 1$. If, on the other hand, $(u_{\gamma_1}, u_{\gamma_t}) = 1$, we let $\gamma_t' = \gamma_t$. Next, if $(u_{\gamma_2}, u_{\gamma_t}) = -1$, we set $\gamma_t'' = \gamma_t' \gamma_1$. Otherwise we set $\gamma_t'' = \gamma_t'$. Then $(u_{\gamma_2}, u_{\gamma_t''}) = (u_{\gamma_1}, u_{\gamma_t''}) = 1$. Replacing γ_t by γ_t'' results in another complete set of cyclic generators for G/N and the γ_t'' acts trivially on K_N. Continuing this process will create a set of generators of the desired type. ∎

PROPOSITION 12: *There exist $\gamma_1, \gamma_2, \ldots, \gamma_m$ in G such that*

$$G/N \cong Z_{2^{r+e}} \times Z_{2^{1+f}} \times Z_{2^{s_1}} \times \cdots \times Z_{2^{s_m}}$$
$$\cong < \overline{\sigma} > \times < \overline{\tau} > \times < \overline{\gamma_1} > \times \cdots \times < \overline{\gamma_m} >$$

and such that $(u_{\gamma_{2t-1}}, u_{\gamma_{2t}}) = \pm 1$ for all t, $2 \leq 2t \leq m$ and all other commutators between u_γ's are trivial. In particular, if m is odd, then u_{γ_m} commutes with u_{γ_i} for all i.

Proof: By induction. ∎

Remark: In the special case $r = 0$, we will adopt the following notation: we will write $G/N \cong Z_{2^{1+g}} \times Z_{2^{s_1}} \times \cdots \times Z_{2^{s_m}} \cong < \overline{\sigma} > \times < \overline{\gamma_1} > \times \cdots \times < \overline{\gamma_m} >$, where $m \geq 0$, $g \geq 0$, $s_i \leq 1$. As in the general case $g \leq 1$ and $s_i = 1$ for all i. Moreover, we may assume that $\gamma_1, \ldots, \gamma_m$ satisfy the conditions of Proposition 12.

Now consider the division algebra $D_0 = k^\alpha < N, \gamma_1, \ldots, \gamma_m >$. Let L denote its center. We have $L \supseteq K_N$. The group G acts on D_0, hence on L, and this induces an action of $G/ < N, \gamma_1, \ldots, \gamma_m > \cong Z_{2^{r+e}} \times Z_{2^{1+f}}$ on L. Furthermore, $L^{G/<N, \gamma_1, \ldots, \gamma_m>} = k$ because k is the center of $k^\alpha G$.

Let u_σ, u_τ be elements of weight σ, τ, respectively. Let B be the subalgebra of $k^\alpha G$ generated by L, u_σ, u_τ. As in the previous section we would like to show

that for each $z \in G$ there is a grouplike element y in B such that the action of z on B is given by conjugation by y. Unfortunately, this is not always true. There are two ideas which overcome this problem. The first, which is used in the cases where $|N| = 2$ or $N \cong Z_2 \times Z_2$, is to enlarge the subalgebra by adjoining a suitable pair $\{u_{\gamma_i}, u_{\gamma_{i+1}}\}$ to it. The second idea, which works in the remaining cases, is to change the subalgebra by changing the generators σ and τ. In each case we will show that the action of G on the new subalgebra is indeed given by conjugation by grouplike elements in the subalgebra itself.

CASE (1.1): $r = 0, g = 0$. Then $N = G'$ has order 2. Let π be a generator of N. Then $u_\pi^2 = -1$. Computing dimensions, we have $\dim(D/k) = |G| = 2^{m+2}$. Because the dimension of D over k is a square, we see that m, the number of γ's, is even. Because we assume G is not abelian, we have $m \geq 2$.

We *claim* $(u_{\gamma_{2j-1}}, u_{\gamma_{2j}}) = -1$ for all $1 \leq j \leq m/2$. If not, by Proposition 12, $u_\pi, u_{\gamma_{2j-1}}, u_{\gamma_{2j}} \in L$. Hence $\dim(L/k) \geq 2^3$, but $G/ < N, \gamma_1, \ldots, \gamma_m >$, which is of order 2, maps onto $Gal(L/k)$, a contradiction. This proves the claim.

We want to summarize the current situation. We will then use only these facts to complete the argument. This will be useful in case 2.1.1 because we will reduce that case to the case we are now considering. At this point we have the following situation: The commutator subgroup G' has order 2. If π is a generator of G' then we may choose an element u_π of weight π such that $u_\pi^2 = -1$. The group $< u_\sigma >$ acts as the Galois group of $k(u_\pi)$ over k and so $k < u_\pi, u_\sigma >$ is a crossed-product algebra with center k. The number of γ's (cyclic generators for $G/ < \pi, \sigma >$) is even and chosen so that for all i, the element γ_i acts trivially on $k(u_\pi)$ and $u_{\gamma_i}^2 \in k(u_\pi)$. Furthermore, $(u_{\gamma_{2j-1}}, u_{\gamma_{2j}}) = -1$ for all $1 \leq j \leq m/2$ and $(u_{\gamma_i}, u_{\gamma_j}) = 1$ for any other choice of indices. We will proceed using only these facts.

We *claim* we can rewrite the cyclic generators $\gamma_1, \ldots, \gamma_m$ so that $(\sigma, \gamma_1) = \pi$ and $(\sigma, \gamma_j) = 1$ for all $j > 1$. First we observe that $(\sigma, \gamma_i) = \pi$ for *some* i, because $(\gamma_j, \gamma_t) = (\gamma_j, \pi) = (\sigma, \pi) = 1$ for all $1 \leq j, t \leq m$. So by possibly reordering the generators, we may assume $(\sigma, \gamma_1) = \pi$. Next, suppose for some $j \geq 3$ we have $(\sigma, \gamma_j) = \pi$ (we will deal with $j = 2$ at the end). Then we may assume, without loss of generality, that j is odd. Then $(u_{\gamma_j}, u_{\gamma_{j+1}}) = -1$. Let $\gamma_j' = \gamma_j \gamma_1$. Then we obtain $(\sigma, \gamma_j') = 1$. But now $(u_{\gamma_j'}, u_{\gamma_2}) = -1$ and, if we set $\gamma_2' = \gamma_2 \gamma_{j+1}$, then $(u_{\gamma_j'}, u_{\gamma_2'}) = 1$. If we replace γ_2 by γ_2' and γ_j by γ_j', then the new elements $\gamma_1, \gamma_2', \gamma_3, \ldots, \gamma_j', \ldots, \gamma_m$ still give a cyclic decomposition and still satisfy Proposition 12. We repeat this process for all γ_j, $j > 2$ that do not commute with σ. So starting over we may assume the generators $\gamma_1, \ldots, \gamma_m$

satisfy $(\sigma, \gamma_1) = \pi$ and $(\sigma, \gamma_j) = 1$ for all $j > 2$. Finally, if $(\sigma, \gamma_2) = \pi$, we replace γ_2 by $\gamma_2' = \gamma_2\gamma_1$ to get $(\sigma, \gamma_2') = 1$. The new set of generators $\gamma_1, \gamma_2', \gamma_3, \ldots, \gamma_m$ has the desired properties. ∎

Now consider the subalgebra $D_1 = k^\alpha < \pi, \sigma, \gamma_1, \gamma_2 >$. We want to show that D_1 is a crossed-product algebra with center k. Let $u_\pi, u_\sigma, u_{\gamma_1}, u_{\gamma_2}$ be elements of weights $\pi, \sigma, \gamma_1, \gamma_2$ respectively. Let $T = k^\alpha < \pi, \gamma_1 >= k(u_\pi, u_{\gamma_1})$. Because γ_1 acts trivially on $K_N = k(u_\pi)$, the subalgebra T is a field, and because $< \pi >= G'$, this field is a Galois extension of k. Recall that $(u_{\gamma_1}, u_{\gamma_2}) = -1$ and $u_{\gamma_1}^2 \in K_N = k(u_\pi)$. Thus $u_{\gamma_1}^4 \in k$, but $u_{\gamma_1}^2 \notin k$, because $(\sigma, \gamma_1) = \pi \neq 1$. Hence $u_{\gamma_1}^2 = cu_\pi$ for some $c \in k^\times$. It follows that T/k has degree 4 and the Galois group of T/k is $Z_2 \times Z_2$ ([1, Proposition 2.6]).

We *claim* that $< \sigma, \gamma_2 >$ is isomorphic to $Z_2 \times Z_2$ and that the action of this group on T is the Galois action. It will follow that D_1 is a crossed-product algebra with center k. The element σ acts on T and so $u_\sigma u_{\gamma_1} u_\sigma^{-1} = xu_{\gamma_1}$, for some $x \in k(u_\pi)$. Hence $u_\sigma u_{\gamma_1}^2 u_\sigma^{-1} = x^2 u_{\gamma_1}^2$. It follows that $-cu_\pi = x^2 cu_\pi$ and so $x = \pm u_\pi$. Replacing σ by $\sigma\gamma_2$ if necessary we may assume $x = u_\pi$. Thus conjugation by u_σ and u_{γ_2} induces the Galois action on $k(u_{\gamma_1}) = k(u_\pi, u_{\gamma_1})$:

$$u_\sigma u_{\gamma_1} u_\sigma^{-1} = u_\pi u_{\gamma_1} = c^{-1} u_{\gamma_1}^3,$$
$$u_{\gamma_2} u_{\gamma_1} u_{\gamma_2}^{-1} = -u_{\gamma_1}.$$

Moreover, $u_\sigma^2 \in k(u_\pi)$ and σ induces the Galois action on $k(u_\pi)$, so $u_\sigma^2 \in k$. Also $\gamma_2^2 \in N$, so $u_{\gamma_2}^2 \in k(u_\pi)$ and $u_{\gamma_2}^4 \in k$. Since $(\sigma, \gamma_2) = 1$ it follows easily that $u_{\gamma_2}^2 \in k$. Hence σ and γ_2 have order 2 and we have proved the claim.

We want to apply the factorization theorem, Theorem 7, to the subgroup $H =< \pi, \sigma, \gamma_1, \gamma_2 >$. It only remains to show that every $z \in G$ acts on D_1 as a grouplike element of D_1. It is sufficient to check this for $z \in \{\gamma_3, \ldots, \gamma_m\}$. So let $z = \gamma_i$, with $i > 2$. Because $(\sigma, z) = 1$, it follows that $u_z u_\sigma u_z^{-1} = \pm u_\sigma$. Moreover, u_z centralizes u_π, u_{γ_1},and u_{γ_2}, so the action of z on D_1 is the same as the action of either the identity or u_π. Thus the factorization theorem applies and we get $G \cong < \pi, \sigma, \gamma_1, \gamma_2 > \times E$ where $E \cong Z_2 \times \cdots \times Z_2$, an elementary abelian 2-group of order 2^{m-2}. Moreover, it is clear that $< \pi, \sigma, \gamma_1, \gamma_2 >$ is the semidirect product given in the statement of Theorem 2.

CASE (1.2): $r = 0, g = 1$. Then $|Z_{2^{1+g}}| = 4$. We will show that this case is not possible. We have:

$$4 = |G/ < N, \gamma_1, \ldots, \gamma_m > | \geq \dim(L/k) \geq \dim(K_N/k) = 2.$$

Hence $\dim(L/k) = 2$ or 4. Suppose $\dim(L/k) = 2$. If $z \in G$ maps to the unique element of order 2 in $Z_{2^{1+g}}$, then z acts trivially on L. Let u_z be an element of weight z. By the Skolem–Noether theorem there is an element $x \in D_0$ such that $x^{-1}u_z$ centralizes D_0. Now let L_1 denote the center of the subalgebra $D_1 = k^\alpha < N, \gamma_1, \ldots, \gamma_m, z >$. Then $L_1 \supseteq L$ and $L_1 \ni x^{-1}u_z$, so $\dim(L_1/k) \geq 4$. But $L_1^{G/<N,\gamma_1,\ldots,\gamma_m,z>} = k$ and $|G/ < N, \gamma_1, \ldots, \gamma_m, z > | = 2$, so $\dim(L_1/k) = 2$, a contradiction.

Now suppose $\dim(L/k) = 4$. By [1, Proposition 2.6] the Galois group of L over k is $Z_2 \times Z_2$. But by its choice the component $Z_4 = Z_{2^{1+g}}$ maps onto $Gal(L/k)$, a contradiction.

CASE (2.1): *$r > 0$ and $|Z_{2^{r+e}} \times Z_{2^{1+f}}| = 2^{r+1}$.* We have

$$2^{r+1} = |G/ < N, \gamma_1, \ldots, \gamma_m > | \geq \dim(L/k) \geq \dim(K_N/k) = 2^{r+1}.$$

Hence $L = K_N$. In this case the dimension of D over k is 2^{2r+2+m}, so m is even. We *claim* that N is either cyclic or $Z_2 \times Z_2$. Suppose N is not isomorphic to $Z_2 \times Z_2$. If N is also not cyclic then N contains a subgroup isomorphic to either $Z_2 \times Z_4$ or $Z_2 \times Z_2 \times Z_2$. If N contains a subgroup isomorphic to $Z_2 \times Z_2 \times Z_2$, then $L = K_N$ will contain three quadratic extensions no one of which is contained in the field generated by the other two. It follows that the Galois group of L/K maps onto $Z_2 \times Z_2 \times Z_2$, a contradiction. If N contains $Z_2 \times Z_4$, then L contains a subfield $F = k^\alpha Z_4$, which by [1, Proposition 2.6] is Galois over k with $Gal(F/k) = Z_2 \times Z_2$. But L will also contain $k^\alpha Z_2$ from the other factor of N and this quadratic extension will not be a subfield of F. Again it follows that the Galois group of L over k maps onto $Z_2 \times Z_2 \times Z_2$, a contradiction. This proves the claim.

CASE (2.1.1): *$N = Z_2 \times Z_2$.* We want to reduce this case to case (1.1). Let $N =< \pi_1, \pi_2 >$ and let $G' =< \pi_1 >$. Then we may choose a grouplike element u_{π_1} of weight π_1 such that $u_{\pi_1}^2 = -1$. The group $< u_\sigma, u_\tau >$ acts as the Galois group on K_N. By possibly changing the generators $\overline{\sigma}, \overline{\tau}$ of $G/ < N, \gamma_1, \ldots, \gamma_m >$, we may assume the action is as follows:

$$u_\sigma u_{\pi_1} u_\sigma^{-1} = -u_{\pi_1}, \quad u_\tau u_{\pi_1} u_\tau^{-1} = u_{\pi_1}$$

and

$$u_\sigma u_{\pi_2} u_\sigma^{-1} = u_{\pi_2}, \quad u_\tau u_{\pi_2} u_\tau^{-1} = -u_{\pi_2}.$$

Now rename $\pi = \pi_1$, $\gamma_{m+1} = \pi_2$, and $\gamma_{m+2} = \tau$. We *claim* that with this notation we are (after a possible alteration of the γ_i's as described in (2) below) in the situation of case (1.1). We need to show several things:

(1) $\sigma^2 = 1$: We have $u_\sigma^2 \in K_N$, hence $u_\sigma^2 \in (K_N)^\sigma = k(u_{\pi_2})$. If $u_\sigma^2 \notin k$, then $u_\tau u_\sigma^2 u_\tau^{-1} = -u_\sigma^2$. But $u_\tau u_\sigma u_\tau^{-1} = x u_\sigma$ for some $x \in K_{G'} = k(u_{\pi_1})$. Note that $x^2 \in k$, so $\sigma(x) = \pm x$. Then

$$-u_\sigma^2 = u_\tau u_\sigma^2 u_\tau^{-1} = (x u_\sigma)^2 = x\sigma(x) u_\sigma^2.$$

If $x \in k$, then $x\sigma(x) = x^2 = -1$, a contradiction because by assumption $\sqrt{-1} \notin k$. If $x \notin k$, then $x\sigma(x) = -x^2 = -1$, a contradiciton because $k^\alpha G$ is a division algebra. Hence $u_\sigma^2 \in k$, so $\sigma^2 = 1$.

It follows that $k^\alpha < \pi_1, \sigma >$ is a crossed product subalgebra of $k^\alpha G$ normalized by G.

(2) We can select γ_i, for $1 \leq i \leq m$ so that u_τ commutes with u_{γ_i}: Let $1 \leq i \leq m$. There is an element $x \in k(u_{\pi_1})$ such that $u_\tau u_{\gamma_i} u_\tau^{-1} = x u_{\gamma_i}$. Then $x^2 \in k$ and, since γ_i acts trivially on K_N, we have

$$u_{\gamma_i} = u_\tau^2 u_{\gamma_i} u_\tau^{-2} = x^2 u_{\gamma_i}.$$

Hence $x^2 = 1$. If $x = 1$, then $(u_\tau, u_{\gamma_i}) = 1$. If $x = -1$ we may replace γ_i by $\gamma_i' = \gamma_i \pi_2$ to get $(u_\tau, u_{\gamma_i'}) = 1$. Because u_{γ_i} commutes with u_{π_2}, the new γ_i''s still satisfy the conditions of Proposition 12, that is $(u_{\gamma_{2t-1}}, u_{\gamma_{2t}}) = \pm 1$ for all t, $2 \leq 2t \leq m$ and all other commutators between u_γ's are trivial.

(3) We have $(u_\tau, u_{\gamma_i}) = (u_{\pi_2}, u_{\gamma_i}) = 1$ for all $1 \leq i \leq m$ and $(u_\tau, u_{\pi_2}) = -1$. Furthermore, $(u_\tau, u_{\pi_1}) = (u_{\pi_2}, u_{\pi_1}) = 1$ and $u_{\pi_2}^2, u_\tau^2 \in k(u_{\pi_1})$. These statements are clear.

So now if we rename $\pi = \pi_1$, $\gamma_{m+1} = \pi_2$, and $\gamma_{m+2} = \tau$, we have the conditions of case (1.1) and can complete the argument as in that case.

CASE (2.1.2): The group N is cyclic. Let π denote a generator of N. Then π has order 2^{r+1}. The subgroup $< \pi, \sigma, \tau >$ is normal in G and the subalgebra $k^\alpha < \pi, \sigma, \tau >$ is a crossed product algebra $(L, Gal(L/k)$.

Now let $z \in \{\gamma_1, \ldots, \gamma_m\}$, say $z = \gamma_i$. Let u_z be an element of weight z. We have $u_z^2 \in K_N$, hence $u_z^2 = a u_\pi^t$, where $a \in k^\times$ and t is an integer. We <u>*claim*</u> t is even. If not, then $< z >$ is a normal cyclic subgroup of G of order 2^{r+2}. But $k(u_z)/k$ is an abelian field extension with Galois group $Z_{2^{r+1}} \times Z_2$, by [1, Proposition 2.6]. It follows that $G/ < z >= G/ < \pi, z >$ maps onto $Z_{2^{r+1}} \times Z_2$. But $G/ < \pi, z > \cong Z_{2^r} \times Z_2 \times \cdots \times Z_2$, a contradiction. This proves the claim. Hence we can write $u_z^2 = a u_\pi^{2s}$ for some integer s, and so $z^2 = \pi^{2s}$. Replacing z by $z\pi^{-s}$ we may assume z has order 2 in G. Repeating this argument for all i, we get a new set of generators for $G/ < \pi, \sigma, \tau >$ which are of order two in G, rather than in G/N.

By the argument of case (1.1), we see that $(u_{\gamma_{2j-1}}, u_{\gamma_{2j}}) = -1$ for all $1 \leq j \leq m/2$. It follows that there exists $w = \gamma_{i\pm 1}$ such that $(u_z, u_w) = -1$. Because z has order 2, we have $u_z u_\sigma u_z^{-1} = x u_\sigma$, where $x = \pm 1$. If $x = 1$ then u_z acts trivially on u_σ. If $x = -1$ we let $\sigma' = \sigma w$ and let $u_{\sigma'} = u_\sigma u_w$. Then it follows that $u_z u_{\sigma'} u_z^{-1} = u_{\sigma'}$. Similarly, we can adjust τ to τ' so that $u_z u_{\tau'} u_z^{-1} = u_{\tau'}$. So we now have the following:

1. $< \overline{\sigma'}, \overline{\tau'}, \overline{\gamma_1}, \ldots, \overline{\gamma_m} > = < \overline{\sigma}, \overline{\tau}, \overline{\gamma_1}, \ldots, \overline{\gamma_m} >$.
2. $< \overline{\sigma'}, \overline{\tau'} >$ acts as the Galois group of L.
3. u_z acts trivially on $k(u_{\sigma'}, u_{\tau'}, u_\pi)$.
4. The action of u_{γ_j} for $j \neq i$ is unaffected, that is $u_{\gamma_j} u_{\sigma'} u_{\gamma_j}^{-1} = u_{\gamma_j} u_\sigma u_{\gamma_j}^{-1}$ and $u_{\gamma_j} u_{\tau'} u_{\gamma_j}^{-1} = u_{\gamma_j} u_\tau u_{\gamma_j}^{-1}$.

Continuing in this way for each element of $\{\gamma_1, \ldots, \gamma_m\}$, we can obtain new elements σ, τ generating the Galois group of L/k such that for every i, the element γ_i acts trivially on $k^\alpha < \pi, \sigma, \tau >$. In particular, we now have that G decomposes into the direct product $< \pi, \sigma, \tau > \times < \gamma_1, \ldots, \gamma_m >$ and that $< \gamma_1, \ldots, \gamma_m >$ is an elementary abelian 2-group. To finish the theorem in this case we need to identify the group $< \pi, \sigma, \tau >$.

Recall that $< \overline{\sigma}, \overline{\tau} >$ is isomorphic to the Galois group of $k(u_\pi)$ over k. Because u_π is a primitive 2^{r+2}-root of unity, we can compute this Galois group explicitly: it is generated by automorphisms ϕ and ψ where $\phi(u_\pi) = u_\pi^3$ and $\psi(u_\pi) = u_\pi^{-1}$. The automorphims ϕ has order 2^r and ψ has order 2. Hence by possibly changing the generators σ and τ, we may assume that $\sigma\pi\sigma^{-1} = \pi^3$ and $\tau\pi\tau^{-1} = \pi^{-1}$. This change will not affect the properties listed in the previous paragraph. In particular, we know that $\sigma^{2^r} \in N$ and $\tau^2 \in N$. We *claim* that in fact σ has order 2^r and τ has order 2 in G. If so, we will have the desired decomposition of G. Recall that $K_N = L$. It follows that $u_\sigma^{2^r} \in L^\sigma$. If $u_\sigma^{2^r} \notin k$, then $u_\sigma^{2^r} = a u_\pi^{2^r}$ for some $a \in k^\times$, because otherwise u_σ would generate a field extension of k of degree $\geq 2^{r+2}$, which is impossible. Hence u_σ commutes with $u_\pi^{2^r}$. But $u_\sigma u_\pi u_\sigma^{-1} = u_\pi^3$, so $u_\sigma u_\pi^{2^r} u_\sigma^{-1} = (u_\pi^{2^r})^3 = -u_\pi^{2^r}$, because $u_\pi^{2^r}$ is a primitive 4-th root of unity. Therefore $u_\sigma^{2^r} \in k$, so σ has order 2^r in G. A similar argument shows τ has order 2. This proves the claim and we have finished this case.

CASE (2.2): $r > 0$ *and* $|Z_{2^{r+e}} \times Z_{2^{1+f}}| = 2^{r+2}$. It follows that either $e = 1$, $f = 0$ or $e = 0, f = 1$. We have:

$$2^{r+2} = |G/ < N, \gamma_1, \ldots, \gamma_m > | \geq \dim(L/k) \geq \dim(K_N/k) = 2^{r+1}.$$

Hence $\dim(L/k) = 2^{r+1}$ or 2^{r+2}. We will show the first case is not possible. If

$\dim(L/k) = 2^{r+1}$, we argue as in case (1.2): There is an element $z \in G$ that maps to either the unique element of order 2 in $Z_{2^{r+1}}$ (when $e = 1$) or to the unique element of order 2 in $Z_{2^{1+f}}$ (when $f = 1$). Then z acts trivially on L. Let u_z be an element of weight z. By the Skolem–Noether theorem there is an element $x \in D_0$ such that $x^{-1}u_z$ centralizes D_0. Now let L_1 denote the center of the subalgebra $D_1 = k^\alpha < N, \gamma_1, \ldots, \gamma_m, z >$. Then $L_1 \supseteq L$ and $L_1 \ni x^{-1}u_z$, so $\dim(L_1/k) \geq 2^{r+2}$. But $L_1^{G/<N,\gamma_1,\ldots,\gamma_m,z>} = k$ and $|G/ < N, \gamma_1, \ldots, \gamma_m, z > | = 2^{r+1}$, so $\dim(L_1/k) = 2^{r+1}$, a contradiction.

Hence $\dim(L/k) = 2^{r+2}$ and $G/ < N, \gamma_1, \ldots, \gamma_m >$ is isomorphic to the Galois group of L/k. The dimension of D over k is 2^{2r+3+m}, so m is odd. By Proposition 12, if u_{γ_m} has weight γ_m, then u_{γ_m} centralizes D_0. It follows that $L = K_N(u_{\gamma_m})$. Let $U =< N, \gamma_m >$. The group U is cyclic: If not, then just as at the beginning of case (2.1) one can show that the $Gal(L/k) \cong Z_{2^{r+e}} \times Z_{2^{1+f}}$ maps onto $Z_2 \times Z_2 \times Z_2$, a contradiction. This case now follows the pattern of case (2.1.2) (where U plays the role of the group N of that case) and so we will merely outline the argument. Let π be a generator of U, so π has order 2^{r+2}. We have $G/ < \pi, \sigma, \tau > \cong < \overline{\gamma_1}, \ldots, \overline{\gamma_{m-1}} >$. The subgroup $< \pi, \sigma, \tau >$ is normal in G and the subalgebra $k^\alpha < \pi, \sigma, \tau >$ is a crossed product algebra $(L, Gal(L/k))$.

Now let $z \in \{\gamma_1, \ldots, \gamma_{m-1}\}$, say $z = \gamma_i$. Let u_z be an element of weight z. We have $u_z^2 \in K_N$, hence $u_z^2 = au_\pi^t$, where $a \in k^\times$ and t is an integer. Because u_π^2 generates K_N over k, the integer t is even. Hence we can write $u_z^2 = au_\pi^{2s}$ for some integer s, and so $z^2 = \pi^{2s}$. Replacing z by $z\pi^{-s}$ we may assume z has order 2 in G. Repeating this argument for all i, we get a new set of generators for $G/ < \pi, \sigma, \tau >$ which are of order two in G, rather than in G/N.

The argument of case (2.1.2) now shows that just as in that case we can, by suitably adjusting σ and τ, assume that for every i, the element γ_i acts trivially on $k^\alpha < \pi, \sigma, \tau >$. In particular, we have that G decomposes into the direct product $< \pi, \sigma, \tau > \times < \gamma_1, \ldots, \gamma_{m-1} >$ and that $< \gamma_1, \ldots, \gamma_{m-1} >$ is an elementary abelian 2-group. We are left with the computation of the group $< \pi, \sigma, \tau >$. Because the order of π is 2^{r+2}, we can write $u_\pi^{2^{r+2}} = b$, for some $b \in k^\times$. The polynomial $x^{2^{r+2}} - b$ is irreducible over k and, because $\sqrt{-1} \notin k$, by a theorem of Schinzel [4, Theorem 2], there is an element $c \in k^\times$, such that $b^2 = c^{2^{r+2}}$. If $b = c^{2^{r+1}}$, then $x^{2^{r+2}} - b$ is reducible, so we have $b = -c^{2^{r+1}}$ and $u_\pi^{2^{r+2}} = -c^{2^{r+1}}$. It is now straightforward to verify that the Galois group of $k(u_\pi)$ over k is generated by automorphisms ϕ and ψ where $\phi(u_\pi) = u_\pi^3/c$ and $\psi(u_\pi) = cu_\pi^{-1}$. Moreover, ϕ has order 2^{r+1} and ψ has order 2. We may assume

that σ acts on $k(u_\pi)$ as ϕ and τ acts as ψ. In particular, we have $\sigma\pi\sigma^{-1} = \pi^3$ and $\tau\pi\tau^{-1} = \pi^{-1}$. We are left with computing the orders of σ and τ. For σ, note that the order of u_σ modulo $K_N \subseteq L$ is 2^{r+1} and so $u_\sigma^{2^{r+1}} = au_\pi^i$ for some $a \in k^\times$ and $0 \leq i \leq 2^{r+1}$. Clearly $u_\sigma^{2^{r+1}} \in L^\sigma$, so $au_\pi^i = u_\sigma a u_\pi^i u_\sigma^{-1} = a(u_\pi^3/c)^i$. Hence $u_\pi^{2i} = c^i \in k^\times$. It follows that $i = 0$ or $i = 2^{r+1}$. If $i = 2^{r+1}$, then $u_\pi^{2^{r+2}} = c^{2^{r+1}}$, a contradiction. Hence $i = 0$ and so σ has order 2^{r+1}. The argument for τ is similar. We thus have the desired presentation of G.

CASE (2.3): *$r > 0$ and $|Z_{2^{r+e}} \times Z_{2^{1+f}}| = 2^{r+3}$.* In this case $e = f = 1$. This is impossible by the discussion of Case (2) of [1].

This completes the proof of Theorem 2.

5. Decomposition into cyclic algebras

In this section we prove the following result:

THEOREM 13: *Let G be a 2-group and let k be a field not containing $\sqrt{-1}$. If $D = k^\alpha G$ is a k-central division algebra, then D is isomorphic to a tensor product of cyclic algebras.*

Proof: By [1, Theorem 4], either D is a tensor product of quaternion algebras or $D \cong D_1 \otimes \cdots \otimes D_n$, where $D_1, D_2, \ldots, D_{n-1}$ are quaternion algebras and $D_n \cong k^\alpha(Z_{2^{r+1}} \rtimes (Z_{2^r} \times Z_2))$. We will in fact show that D_n is isomorphic to a tensor product of two cyclic algebras, one of which is quaternion. We consider two cases:

CASE 1: $r = 1$. In this case, D_n is precisely the algebra denoted D_1 in case (1.1) of section 4. We will use the notation of that case. We have $D_1 \cong k^\alpha H$, where $H = Z_4 \rtimes (Z_2 \times Z_2) =< \gamma_1, \gamma_2, \sigma | \gamma_1^4 = \gamma_2^2 = \sigma^2 = 1$ and $\sigma\gamma_1\sigma^{-1} = \gamma_1^3, \gamma_2\gamma_1\gamma_2^{-1} = \gamma_1 >$ and the cocycle α is defined by

$$u_{\gamma_1}^4 = -c^2, \quad u_\sigma u_{\gamma_1} u_\sigma^{-1} = c^{-1}u_{\gamma_1}^3, \quad u_{\gamma_2} u_{\gamma_1} u_{\gamma_2}^{-1} = -u_{\gamma_1}$$

and

$$u_\sigma^2 = s, \quad u_{\gamma_2}^2 = t$$

for some c, s, t in k. The commutator (u_σ, u_{γ_2}) must be a 2-power root of unity and $u_{\gamma_2}^2 = t \in k$, so we also get $(u_\sigma, u_{\gamma_2}) = \pm 1$. We may set $u_{\sigma\gamma_2} = u_\sigma u_{\gamma_2}$.

Now we compute $u_\sigma u_{\gamma_1}^2 u_\sigma^{-1} = (u_\sigma u_{\gamma_1} u_\sigma^{-1})^2 = c^{-2}u_{\gamma_1}^6 = -u_{\gamma_1}^2$. It follows that the k-subalgebra B generated by $c^{-1}u_{\gamma_1}^2$ and u_σ is the quaternion algebra $(-1, s)$. But then $D_n \cong B \otimes C_{D_n}(B)$ where $C_{D_n}(B)$ is the centralizer of B

in D_n. By dimension count $C_{D_n}(B)$ is another quaternion algebra and we are done in this case.

CASE 2: $r > 1$. We are now in the situation of case (2.2) of section 4 (where the r of that case is replaced by $r-1$). Using the notation of that case, we can present our group as

$$H = Z_{2^{r+1}} \rtimes (Z_{2^r} \times Z_2))$$
$$=< \pi, \sigma, \tau | \pi^{2^{r+1}} = \sigma^{2^r} = \tau^2 = 1 \text{ and } \sigma\pi\sigma^{-1} = \pi^3, \tau\pi\tau^{-1} = \pi^{-1} > .$$

The cocycle is given by the relations

$$u_\pi^{2^{r+1}} = -c^{2^r}, \quad u_\sigma u_\pi u_\sigma^{-1} = c^{-1}u_\pi^3, \quad u_\tau u_\pi u_\tau^{-1} = cu_\pi^{-1}$$

and

$$u_\sigma^{2^r} = s, \quad u_\tau^2 = t, \quad (u_\sigma, u_\tau) = \pm 1, \quad u_\sigma u_\tau = u_{\sigma\tau}$$

for some c, s, t in k.

Now consider the subfield $L = k(u_\pi)^\tau$. It is a Galois extension with Galois group isomorphic to the cyclic subgroup generated by σ. The element u_σ acts on L by conjugation and this action is the Galois action because $L^\sigma = L^{H/<\pi,\tau>} \subsetneq Z(K^\alpha H) = k$. It follows that the subalgebra generated by L and u_σ is the cyclic crossed product algebra $B = (L, \sigma, s)$. We can decompose $D_n \cong B \otimes C_{D_n}(B)$ as before. Once again, by dimension count the centralizer $C_{D_n}(B)$ is a quaternion algebra, so D_n is a product of cyclics. ∎

Adding this result to [1, Theorems 3 and 4] we obtain the following corollary.

COROLLARY 14: *If G is a finite group and $D = k^\alpha G$ is a k-central division algebra, then D is isomorphic to a tensor product of cyclic algebras.*

References

[1] E. Aljadeff and D. Haile, *Division algebras with a projective basis*, Israel Journal of Mathematics **121** (2001), 173–198.

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

[3] R. Howlett and I. Isaacs, *On groups of central type*, Mathematische Zeitschrift **179** (1982), 555–569.

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

[5] M. Suzuki, *Group Theory I*, Springer-Verlag, New York, 1982.