Annals of Mathematics, **162** (2005), 823–883

The classification of torsion endo-trivial modules

By Jon F. Carlson* and Jacques Thévenaz

1. Introduction

This paper settles a problem raised at the end of the seventies by J.L. Alperin [Al1], E.C. Dade [Da] and J.F. Carlson [Ca1], namely the classification of torsion endo-trivial modules for a finite p-group over a field of characteristic p. Our results also imply, at least when p is odd, the complete classification of torsion endo-permutation modules.

We refer to [CaTh] and [BoTh] for an overview of the problem and its importance in the representation theory of finite groups. Let us only mention that the classification of endo-trivial modules is the crucial step for understanding the more general class of endo-permutation modules, and that endo-permutation modules play an important role in module theory, in particular as source modules, in block theory where they appear in the description of source algebras, and in both derived equivalences and stable equivalence of block algebras, for which many new developments have appeared recently.

Let G be a finite p-group and k be a field of characteristic p. Recall that a (finitely generated) kG-module M is called endo-trivial if $\mathrm{End}_k(M) \cong k \oplus F$ as kG-modules, where F is a free module. Typical examples of endo-trivial modules are the Heller translates $\Omega^n(k)$ of the trivial module. Any endo-trivial kG-module M is a direct sum $M = M_0 \oplus L$, where M_0 is an indecomposable endo-trivial kG-module and L is free. Conversely, by adding a free module to an endo-trivial module, we always obtain an endo-trivial module. This defines an equivalence relation among endo-trivial modules and each equivalence class contains exactly one indecomposable module up to isomorphism. The set $T(G)$ of all equivalence classes of endo-trivial kG-modules is a group with multiplication induced by tensor product, called simply the group of endo-trivial kG-modules. Since scalar extension of the coefficient field induces an injective map between the groups of endo-trivial modules, we can replace k by its algebraic closure. So we assume that k is algebraically closed. We refer to [CaTh] for more details about $T(G)$.

*The first author was partly supported by a grant from NSF.

Dade [Da] proved that if A is a noncyclic abelian p-group then $T(A) \cong \mathbb{Z}$, generated by the class of $\Omega^1(k)$. For any p-group G, Puig [Pu] proved that the abelian group $T(G)$ is finitely generated (but we do not use this here since it is actually a consequence of our main results). The torsion-free rank of $T(G)$ has been determined recently by Alperin [Al2] and the remaining problem lies in the structure of the torsion subgroup $T_t(G)$.

Let us first recall some important known cases (see [CaTh]). If $G = 1$ or $G = C_2$, then $T(G) = 0$. If $G = C_{p^n}$ is cyclic of order p^n, with $n \geq 1$ if p is odd and $n \geq 2$ if $p = 2$, then $T(C_{p^n}) \cong \mathbb{Z}/2\mathbb{Z}$ (generated by the class of $\Omega^1(k)$). If $G = Q_{2^n}$ is a quaternion group of order $2^n \geq 8$, then $T(Q_{2^n}) = T_t(Q_{2^n}) \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. If $G = \mathrm{SD}_{2^n}$ is a semi-dihedral group of order $2^n \geq 16$, then $T(\mathrm{SD}_{2^n}) \cong \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ and so $T_t(\mathrm{SD}_{2^n}) \cong \mathbb{Z}/2\mathbb{Z}$. Our first main result asserts that these are the only cases where nontrivial torsion occurs.

THEOREM 1.1. *Suppose that G is a finite p-group which is not cyclic, quaternion, or semi-dihedral. Then $T_t(G) = \{0\}$.*

As explained in [CaTh], the computation of the torsion subgroup $T_t(G)$ is tightly connected to the problem of detecting nonzero elements of $T(G)$ on restriction to a suitable class of subgroups. A detection theorem was proved in [CaTh] and it was conjectured that the detecting family should actually only consist of elementary abelian subgroups of rank at most 2 and, in addition when $p = 2$, cyclic groups of order 4 and quaternion subgroups Q_8 of order 8. This conjecture is correct and the largest part of the present paper is concerned with the proof of this conjecture.

It is in fact only for the cases of cyclic, quaternion, and semi-dihedral groups that one needs to include cyclic groups C_p or C_4 and quaternion subgroups Q_8 in the detecting family. For all the other cases, we are going to prove the following.

THEOREM 1.2. *Suppose that G is a finite p-group which is not cyclic, quaternion, or semi-dihedral. Then the restriction homomorphism*

$$\prod_E \mathrm{Res}^G_E : T(G) \longrightarrow \prod_E T(E) \cong \prod_E \mathbb{Z}$$

is injective, where E runs through the set of all elementary abelian subgroups of rank 2.

In order to explain the right-hand side isomorphism, recall that $T(E) \cong \mathbb{Z}$ by Dade's theorem [Da]. Notice that Theorem 1.1 follows immediately from Theorem 1.2.

In the case of the theorem, $T(G)$ is free abelian and the method of Alperin [Al2] describes its rank by restricting drastically the list of elementary abelian subgroups which are actually needed on the right-hand side (see also [BoTh] for another approach). However, for a complete classification of all endo-trivial modules, there is still an open problem. Alperin's method shows that $T(G)$ is a full lattice in a free abelian group A by showing that some explicit subgroup $S(G)$ of the same rank satisfies $S(G) \subseteq T(G) \subseteq A$. But there is still the problem of describing explicitly the finite group $T(G)/S(G) \subseteq A/S(G)$. However, this additional problem only occurs if G contains maximal elementary subgroups of rank 2 (see [Al2] or [BoTh] for details). In all other cases the rank of $T(G)$ is one and we have the following result.

COROLLARY 1.3. *Suppose that G is a finite p-group for which every maximal elementary abelian subgroup has rank at least 3. Then $T(G) \cong \mathbb{Z}$, generated by the class of the module $\Omega^1(k)$.*

For the proof of Theorem 1.2, we first use the results of [CaTh] which provide a reduction to the case of extraspecial and almost extraspecial p-groups. These are the difficult cases for which we need to prove that the groups can be eliminated from the detecting family. When p is odd, this was already done in [CaTh] for extraspecial p-groups of exponent p^2 and almost extraspecial p-groups. So we are left with the remaining cases and we have to prove the following theorem, which is in fact the main result we prove in the present paper.

THEOREM 1.4. *Suppose the following*:

(a) *If $p = 2$, G is an extraspecial or almost extraspecial 2-group and G is not isomorphic to Q_8.*

(b) *If p is odd, G is an extraspecial p-group of exponent p.*

Then the restriction homomorphism

$$\prod_H \mathrm{Res}^G_H : T(G) \longrightarrow \prod_H T(H)$$

is injective, where H runs through the set of all maximal subgroups of G.

As mentioned earlier, the classification of endo-trivial modules has immediate consequences for the more general class of endo-permutation modules. The second goal of the present paper is to describe the consequences of the main results for the classification of torsion endo-permutation modules. We prove a detection theorem for the Dade group of all endo-permutation modules and also a detection theorem for the torsion subgroup of the Dade group. For odd p, this yields a complete description of this torsion subgroup, by the results of [BoTh].

THEOREM 1.5. *If p is odd and G is a finite p-group, the torsion subgroup of the Dade group of all endo-permutation kG-modules is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^s$, where s is the number of conjugacy classes of nontrivial cyclic subgroups of G.*

One set of s generators is described in [BoTh]. Since an element of order 2 corresponds to a self-dual module, we obtain in particular the following corollary.

COROLLARY 1.6. *If p is odd and G is a finite p-group, then an indecomposable endo-permutation kG-module M with vertex G is self-dual if and only if the class of M in the Dade group is a torsion element of this group.*

This is an interesting result in view of the fact that many invariants lying in the Dade group (e.g. sources of simple modules) are either known or expected to lie in the torsion subgroup, while it is not at all clear why the modules should be self-dual.

When $p = 2$, the situation is more complicated but we obtain that any torsion element of the Dade group has order 2 or 4. Moreover, the detection result is efficient in some cases, but examples also show that it is not always sufficient to determine completely this torsion subgroup.

Theorem 1.4 is the result whose proof requires most of the work. The result has to be treated separately when $p = 2$ or when p is odd. However, the strategy is similar and many of the same methods are of use for the proof in both cases. After a preliminary Section 2 and two sections about the cohomology of extraspecial groups, the proof of Theorem 1.4 occupies Sections 5–11. We use a large amount of group cohomology, including some very recent results, as well as the theory of support varieties of modules. The crucial role of Serre's theorem on products of Bocksteins appears once again and we actually need a bound for the number of terms in this product that was recently obtained by Yalçin [Ya] for (almost) extraspecial groups. Also, the module-theoretic counterpart of Serre's theorem described in [Ca2] plays a crucial role. All these results allow us to find an upper bound for the dimension of an indecomposable endo-trivial module which is trivial on restriction to proper subgroups. For the purposes of the present paper, we shall call such a module a *critical* module. The main goal is to prove that there are no nontrivial critical modules for extraspecial and almost extraspecial 2-groups, except Q_8, and also none for extraspecial p-groups of exponent p (with p odd).

The existence of a bound for the dimension of a critical module had been known for more than 20 years and was used by Puig [Pu] in his proof of the finite generation of $T(G)$. The new aspect is that we are now able to control this bound for (almost) extraspecial groups. One of the differences between the case where $p = 2$ and the case where p is odd lies in the fact that the cohomology of extraspecial 2-groups is entirely known, so that a reasonable bound can be computed, while for odd p some more estimates are necessary. Another difference is due to the fact that we have three families of groups to consider when $p = 2$, but only one when p is odd, because the other two were already dealt with in [CaTh].

The other main idea in the proof of Theorem 1.4 is the following. Under the assumption that there exists a nontrivial critical module M, we can construct many others using the action of $\mathrm{Out}(G)$ (which is an orthogonal or symplectic group since G is (almost) extraspecial), and then construct a very large critical module by taking tensor products. The dimension of this large module exceeds the upper bound mentioned above and we have a contradiction. It is this part in which the theory of varieties associated to modules plays an essential role. We use it to analyze a suitable quotient module $\overline{M}$ which turns out to be periodic as a module over the elementary abelian group $\overline{G} = G/\Phi(G)$.

Once Theorem 1.4 is proved, the proof of Theorem 1.2 requires much less machinery and appears in Section 12. It is very easy if p is odd and, if $p = 2$, it is essentially an inductive argument using a group-theoretical lemma. Theorem 1.1 also follows easily.

The paper ends with two sections about the Dade group of all endo-permutation modules, where we prove the results mentioned above.

We wish to thank numerous people who have shared ideas and opinions in the course of the writing of this paper. Special thanks are due to Cédric Bonnafé, Roger Carter, Ian Leary, Gunter Malle, and Jan Saxl. The first author also wishes to thank the Humboldt Foundation for supporting his stay in Germany while this paper was being written.

2. Preliminaries

Recall that G denotes a finite p-group, and k an algebraically closed field of characteristic p. In this section we write down some of the facts about modules and support varieties that we will need in later developments. All kG-modules are assumed to be finitely generated.

Recall that every projective kG-module is free, because G is a p-group, and that injective and projective modules coincide. Moreover, an indecomposable kG-module M is free if and only if $t_1^G \cdot M \neq 0$, where $t_1^G = \sum_{g\in G} g$ (a generator of the socle of kG). More generally, if M is a kG-module and if $m_1, \dots, m_r \in M$ are such that $t_1^G m_1, \dots, t_1^G m_r$ are linearly independent, then $m_1, \dots, m_r$ generate a free submodule F of M of rank r. Moreover F is a direct summand of M because F is also injective.

Suppose that M is a kG-module. If $P \xrightarrow{\theta} M$ is a projective cover of M then we let $\Omega(M)$ denote the kernel of θ. We can iterate the process and define inductively $\Omega^n(M) = \Omega(\Omega^{n-1}(M))$, for $n > 1$. Suppose that $M \xrightarrow{\mu} Q$ is an injective hull of M. Recall that Q is a projective as well as injective module. Then we let $\Omega^{-1}(M)$ be the cokernel of μ. Again we have inductively that $\Omega^{-n}(M) = \Omega^{-1}(\Omega^{-n+1}(M))$ for $n > 1$. The modules $\Omega^n(M)$ are well defined up to isomorphism and they have no nonzero projective submodules. In general we write $M = \Omega^0(M) \oplus P$ where P is projective and $\Omega^0(M)$ has no projective summands.

The basic calculus of the syzygy modules $\Omega^n(M)$ is expressed in the following.

Lemma 2.1. *Suppose that M and N are kG-modules. Then $\Omega^m(M) \otimes \Omega^n(N) \cong \Omega^{m+n}(M \otimes N) \oplus (\text{free})$.*

Here $M \otimes N$ is meant to be the tensor product $M \otimes_k N$ over k, with the action of the group G defined diagonally, $g(m \otimes n) = gm \otimes gn$. The proof of the lemma is a consequence of the facts that $M \otimes_k -$ and $- \otimes_k N$ preserve exact sequences and that $M \otimes N$ is projective whenever either M or N is a projective module.

The cohomology ring $\mathrm{H}^*(G,k)$ is a finitely generated k-algebra and for any kG-modules M and N, $\mathrm{Ext}^*_{kG}(M,N)$ is a finitely generated module over $\mathrm{H}^*(G,k) \cong \mathrm{Ext}^*_{kG}(k,k)$. We let $V_G(k)$ denote the maximal ideal spectrum of $\mathrm{H}^*(G,k)$. For any kG-module M, let $J(M)$ be the annihilator in $\mathrm{H}^*(G,k)$ of the cohomology ring $\mathrm{Ext}^*_{kG}(M,M)$. Let $V_G(M) = V_G(J(M))$ be the closed subset of $V_G(k)$ consisting of all maximal ideals that contain $J(M)$. So $V_G(M)$ is a homogeneous affine variety. We need some of the properties of support varieties in essential ways in the course of our proofs. See the general references [Be], [Ev] for more explanations and details.

Theorem 2.2. *Let L, M and N be kG-modules.*

(1) $V_G(M) = \{0\}$ *if and only if M is projective.*

(2) *If $0 \to L \to M \to N \to 0$ is exact then the variety of any one of L, M or N is contained in the union of the varieties of the other two. Moreover, if $V_G(L) \cap V_G(N) = \{0\}$, then the sequence splits.*

(3) $V_G(M \otimes N) = V_G(M) \cap V_G(N)$.

(4) $V_G(\Omega^n(M)) = V_G(M) = V_G(M^*)$ *where $M^* = \mathrm{Hom}_k(M,k)$ is the k-dual of M.*

(5) *If $V_G(M) = V_1 \cup V_2$ where V_1 and V_2 are nonzero closed subsets of $V_G(k)$ and $V_1 \cap V_2 = \{0\}$, then $M \cong M_1 \oplus M_2$ where $V_G(M_1) = V_1$ and $V_G(M_2) = V_2$.*

(6) *A nonprojective module M is periodic* (*i.e. for some $n > 0$, $\Omega^n(M) \cong \Omega^0(M)$*) *if and only if its variety $V_G(M)$ is a union of lines through the origin in $V_G(k)$.*

(7) *Let $\zeta \in \mathrm{Ext}^n_{kG}(k,k) = \mathrm{H}^n(G,k)$ be represented by the* (*unique*) *cocycle $\zeta : \Omega^n(k) \longrightarrow k$ and let $L = \mathrm{Ker}(\zeta)$, so that there is an exact sequence*

$$0 \longrightarrow L \longrightarrow \Omega^n(k) \xrightarrow{\zeta} k \longrightarrow 0\,.$$

Then $V_G(L) = V_G(\zeta)$, the variety of the ideal generated by ζ, consisting of all maximal ideals containing ζ.

We are particularly interested in the case in which the group G is an elementary abelian group. First assume that $p = 2$ and $G = \langle x_1, \dots, x_n\rangle \cong (C_2)^n$. Then $\mathrm{H}^*(G,k) \cong k[\zeta_1, \dots, \zeta_n]$ is a polynomial ring in n variables. Here the elements $\zeta_1, \dots, \zeta_n$ are in degree 1 and by proper choice of generators we can assume that $\mathrm{res}_{G,\langle x_i\rangle}(\zeta_j) = \delta_{ij} \cdot \gamma_i$ where $\gamma_i \in \mathrm{H}^1(\langle x_i\rangle, k)$ is a generator for the cohomology ring of $\langle x_i\rangle$. Indeed if we assume that the generators are chosen correctly, then for any $\alpha = (\alpha_1, \dots, \alpha_n) \in k^n$, $u_\alpha = 1 + \sum_{i=1}^n \alpha_i(x_i - 1) \in kG$, $U = \langle u_\alpha\rangle$, we have that

$$\mathrm{res}_{G,U}(f(\zeta_1, \dots, \zeta_n)) = f(\alpha_1, \dots, \alpha_n)\gamma_\alpha^t$$

where f is a homogeneous polynomial of degree t and $\gamma_\alpha \in \mathrm{H}^1(U,k)$ is a generator of the cohomology ring of U.

Now suppose that p is an odd prime and let $G = \langle x_1, \dots, x_n\rangle \cong (C_p)^n$. Then

$$\mathrm{H}^*(G,k) \cong k[\zeta_1, \dots, \zeta_n] \otimes \Lambda(\eta_1, \dots, \eta_n)\,,$$

where Λ is an exterior algebra generated by the elements $\eta_1, \dots, \eta_n$ in degree 1 and the polynomial generators $\zeta_1, \dots, \zeta_n$ are in degree 2. We can assume that each ζ_j is the Bockstein of the element η_j and that the elements can be chosen so that $\mathrm{res}_{G,\langle x_i\rangle}(\zeta_j) = \delta_{ij} \cdot \gamma_i$ where $\gamma_i \in \mathrm{H}^2(\langle x_i\rangle, k)$ is a generator for the cohomology ring of $\langle x_i\rangle$. Similarly, assuming that the generators are chosen correctly, for any $\alpha = (\alpha_1, \dots, \alpha_n) \in k^n$, $u_\alpha = 1 + \sum_{i=1}^n \alpha_i(x_i - 1) \in kG$, $U = \langle u_\alpha\rangle$, we have that

$$\mathrm{res}_{G,U}(f(\zeta_1, \dots, \zeta_n)) = f(\alpha_1^p, \dots, \alpha_n^p)\gamma_\alpha^t$$

where f is a homogeneous polynomial of degree t and $\gamma_\alpha \in \mathrm{H}^1(U,k)$ is a generator of the cohomology ring of U.

Associated to a kG-module M we can define a rank variety

$$V_G^r(M) = \Big\{\alpha \in k^n \mid M{\downarrow}_{\langle u_\alpha\rangle} \text{ is not a free } \langle u_\alpha\rangle\text{-module } \Big\} \cup \{0\}$$

where u_α is given as above and where $M{\downarrow}_{\langle u_\alpha\rangle}$ denotes the restriction of M to the subalgebra $k\langle u_\alpha\rangle$ of kG. Then we have the following result for any p.

THEOREM 2.3. *Let M be any kG-module. If $p = 2$ then, $V_G^r(M) = V_G(M)$ as subsets of k^n. If $p > 2$ then the map $V_G(M) \longrightarrow V_G^r(M)$ given by $\alpha \mapsto \alpha^p = (\alpha_1^p, \ldots, \alpha_n^p)$ is an inseparable isogeny (both injective and surjective). In particular, for $\alpha \neq 0$, $\alpha^p \in V_G(M)$ ($\alpha \in V_G(M)$ if $p = 2$) if and only if $M{\downarrow}_{\langle u_\alpha \rangle}$ is not a free $k\langle u_\alpha \rangle$-module.*

We should emphasize that if v is a unit in kG such that

$$v \equiv u_\alpha \mod(\mathrm{Rad}(kG)^2)$$

then $M{\downarrow}_{\langle v \rangle}$ is a free $k\langle v \rangle$-module if and only if $\alpha^p \notin V_G(M)$ ($\alpha \notin V_G(M)$ if $p = 2$). So for example the element $x_1x_2x_3$ fails to act freely on M if and only if $(1, 1, 1, 0, \ldots, 0) \in V_G(M)$.

3. Extraspecial groups in characteristic 2

In this section and the next, we are interested in the structure and cohomology of extraspecial and almost extraspecial p-groups. These are precisely the p-groups G with the property that G has a *unique* normal subgroup Z of order p such that G/Z is elementary abelian. Note that the dihedral group D_8 of order 8 and, more generally, the Sylow p-subgroup of $\mathrm{GL}(3, p)$ are extraspecial p-groups. The quaternion group Q_8 of order 8 and the cyclic group C_{p^2} of order p^2 also have the required property. Indeed, for $p = 2$ any extraspecial or almost extraspecial group is constructed from copies of D_8, Q_8 and C_4 by taking central products. In this section we concentrate on the case $p = 2$ and look more deeply into the structure of the extraspecial and almost extraspecial group and their cohomology.

Suppose that G_1 and G_2 are 2-groups with the property that each has a unique normal subgroup of order 2. Let $\langle z_i \rangle \in G_i$ be the subgroups. Then the central product $G_1 * G_2$ is defined by

$$G_1 * G_2 = (G_1 \times G_2)/\langle (z_1, z_2) \rangle.$$

It is not difficult to check that $D_8 * D_8 \cong Q_8 * Q_8$ and that $D_8 * C_4 \cong Q_8 * C_4$. Moreover, $C_4 * C_4$ has a central elementary abelian subgroup of order 4 and hence is not of interest to us (it is neither extraspecial nor almost extraspecial). We are left with three types. They are:

Type 1. $G = D_8 * D_8 * \cdots * D_8$ of order 2^{2n+1} where n is the number of factors in the central product.

Type 2. $G = D_8 * \cdots * D_8 * Q_8$ of order 2^{2n+1} where n is the number of factors in the central product.

Type 3. $G = D_8 * \cdots * D_8 * C_4$ of order 2^{2n+2} where n is the number of factors isomorphic to D_8.

The groups of type 1 and 2 are the extraspecial groups (see [Go1]) while the groups of type 3 are what we call the almost extraspecial groups.

The groups are also characterized by an associated quadratic form in the following way. Each group is a central extension

$$0 \longrightarrow Z \longrightarrow G \xrightarrow{\mu} E \longrightarrow 0$$

where $Z = \langle z \rangle$ is the unique central normal subgroup of order 2 and $E \cong \mathbb{F}_2^m$ is elementary abelian. Recall that a quadratic form on E (as a vector space over $\mathbb{F}_2$) is a map $q : E \longrightarrow \mathbb{F}_2$ with the property that

$$q(x+y) = q(x) + q(y) + b(x,y)$$

where $b : E \times E \longrightarrow \mathbb{F}_2$ is a symmetric bilinear form. Here the quadratic form q expresses the class of the extension as given in the above sequence. That is, if $\tilde{x}$, $\tilde{y}$ are elements of G and if $\mu(\tilde{x}) = x$ and $\mu(\tilde{y}) = y$, then

$$\tilde{x}^2 = z^{q(x)} \text{ and } [\tilde{x}, \tilde{y}] = z^{b(x,y)}.$$

Notice here that we are writing the operation in G as multiplication. Given the structure of the groups, it is not difficult to write down the associated quadratic forms. With respect to a choice of basis, E can be identified with $\mathbb{F}_2^m$ and in the sequel we make this identification. Thus we write $x = (x_1, \ldots, x_m)$ for the elements of E.

LEMMA 3.1. *Let G be an extraspecial or almost extraspecial group of order 2^{m+1}. Then the quadratic form q associated to G is given on $x = (x_1, \ldots, x_m) \in \mathbb{F}_2^m = E$ as follows.*

For type 1, $q(x) = x_1x_2 + \cdots + x_{2n-1}x_{2n} \quad (m = 2n)$.

For type 2, $q(x) = x_1x_2 + \cdots + x_{2n-3}x_{2n-2} + x_{2n-1}^2 + x_{2n-1}x_{2n} + x_{2n}^2 \quad (m = 2n)$.

For type 3, $q(x) = x_1x_2 + \cdots + x_{2n-1}x_{2n} + x_{2n+1}^2 \quad (m = 2n+1)$.

Now on the k-vector space $V = k^m$ of dimension m, let q, b denote the same forms but with the field of coefficients expanded from $\mathbb{F}_2$ to k. Let $F : k \to k$ be the Frobenius homomorphism, $F(a) = a^2$. If $\nu = (x_1, \ldots, x_m) \in V$, let F act on ν by $F(\nu) = (x_1^2, x_2^2, \ldots, x_m^2)$. Recall that a subspace $W \subseteq V$ is isotropic if $q(w) = 0$ for all $w \in W$. The following is not difficult:

LEMMA 3.2. *Let h be the codimension in V of a maximal isotropic subspace of V. The values of h for the quadratic forms associated to the above groups are:*

$h = n$ *for* G *of type* 1 $(m = 2n)$,

$h = n + 1$ *for* G *of type* 2 $(m = 2n)$ *or type* 3 $(m = 2n + 1)$.

Moreover 2^h is the index in G of a maximal elementary abelian subgroup.

We are now prepared to state the theorem of Quillen on the cohomology. See [BeCa] for one treatment.

THEOREM 3.3 ([Qu]). *Let G be an extraspecial or almost extraspecial group of order 2^{m+1}. If $\nu = (x_1, \dots, x_m)$, then*

$$\mathrm{H}^*(G,k) = k[x_1,\dots,x_m]/(q(\nu), b(\nu,F(\nu)),\dots,b(\nu,F^{h-1}(\nu))) \ \otimes k[\delta]$$

where δ is an element of degree 2^h that restricts to a nonzero element of Z. Moreover the elements $q(\nu), b(\nu,F(\nu)),\dots,b(\nu,F^{h-1}(\nu))$ form a regular sequence in $k[x_1,\dots,x_m]$ and $\mathrm{H}^*(G,k)$ is a Cohen-Macaulay ring.

The following will be vital for the proof of our main results.

THEOREM 3.4. *Let G be an extraspecial or almost extraspecial 2-group. Define $t = t_G$ to be the natural number given as follows. If G is of type 1 of order 2^{2n+1}, let*

$$t_G = \begin{cases} 2^{n-1}+1 & \text{for } n \le 4\,, \\ 2^{n-1}+2^{n-4} & \text{for } n \ge 4\,. \end{cases}$$

If G is of type 2 of order 2^{2n+1} or of type 3 of order 2^{2n+2}, then let

$$t_G = \begin{cases} 3 & \text{for } n = 1\,, \\ 2^{n}+2^{n-2} & \text{for } n \ge 2\,. \end{cases}$$

Then there exist nonzero elements $\zeta_1,\dots,\zeta_t \in \mathrm{H}^1(G,\mathbb{F}_2)$ such that $\zeta_1\dots\zeta_t = 0$. Moreover, in the isomorphism $\mathrm{H}^1(G,\mathbb{F}_2) \cong \mathrm{Hom}(G,\mathbb{F}_2)$, each ζ_i corresponds to a homomorphism whose kernel is a maximal subgroup of G and is the centralizer of a noncentral involution in G.

Proof. The proof is contained in the paper [Ya]. For the groups of type 1, t_G is actually equal to the cohomological length, that is, the least number of nonzero elements in $\mathrm{H}^1(G,\mathbb{F}_2)$ such that the product of those elements is zero (see [Ya, Th. 1.3]).

Now, suppose that G has type 2 or 3. Then t_G in our theorem is equal to the cardinality $s(G)$ of a representing set in G (see [Ya, Props. 6.2 and 6.3]). A representing set for G is a collection of elements of G that contains at least one noncentral element from each elementary abelian subgroup of G. But now Proposition 1.1 of [Ya] shows that the cohomological length is at most $s(G)$.

The point of the last statement is that the centralizer of any maximal elementary abelian subgroup of G is contained in the centralizers of some elements in a representing set. Because the cohomology ring $\mathrm{H}^*(G,\mathbb{F}_2)$ is Cohen-Macaulay (see Theorem 3.3), any element whose restriction to the centralizer of every maximal elementary abelian subgroup of G vanishes, is the zero element (see Theorem 3.4 in [Ya]). Hence if we choose the elements ζ_i to correspond to the centralizers of the elements in a representing set as in the last statement, then their product is zero as desired. □

The next theorem will be very important to the proof of the general case. It is part of the effort to get an explicit upper bound on the dimensions of critical modules.

THEOREM 3.5. *Let G be an extraspecial or almost extraspecial group of order 2^{m+3} and let H be the centralizer of a noncentral involution in G. Then $H \cong C_2 \times U$ where U is an extraspecial or almost extraspecial group of order 2^{m+1} of the same type as G. Assume that $m \geq 2$ and, if $m = 2$, that $U \not\cong D_8$. Then for $2 \leq r \leq t_G$,*

$$\operatorname{Dim} \mathrm{H}^r(H,k) \leq \binom{m+r}{r} - \binom{m+r-2}{r-2}.$$

Proof. The structure of the centralizer H can be verified directly from what we know of G. For one thing it can be checked that all noncentral involutions in G are conjugate by an element in the automorphism group of G and hence their centralizers are all isomorphic.

Throughout the proof we use the notation in Theorem 3.3, for the cohomology of the group U, so that $\mathrm{H}^*(U,k)$ is generated by $x_1,\dots,x_m$ and δ, with $\deg(\delta) = 2^h$ (where h is the value associated to the group U as in Lemma 3.2). We know that

$$\mathrm{H}^*(H,k) \cong \mathrm{H}^*(U,k) \otimes \mathrm{H}^*(C_2,k)$$

and moreover we know that $\mathrm{H}^*(C_2,k) \cong k[y]$ is a polynomial ring in one variable y in degree 1. We want to focus on the polynomial ring S generated by $x_1,\dots,x_m,y$. We have a homomorphism from S to $\mathrm{H}^*(H,k)$ whose kernel contains the elements $q(\nu)$ and $\beta(\nu,F(\nu))$ where $\nu = (x_1,\dots,x_m)$. Let Q denote the image of S in $\mathrm{H}^*(H,k)$. For this argument, let $S^{\#} = S/(q(\nu))$ and let $S^{\#\#} = S/(q(\nu),\beta(\nu,F(\nu)))$. If R denotes any of these graded rings, we let R_r denote the homogeneous part of R in degree exactly r. Note that $R_r = 0$ if $r < 0$.

First notice that $\operatorname{Dim} S_r = \binom{m+r}{m} = \binom{m+r}{r}$. Because $q(\nu)$ and $\beta(\nu,F(\nu))$ are two terms of a regular sequence of elements in S we must have that

$$\operatorname{Dim} S^{\#}_r = \operatorname{Dim} S_r - \operatorname{Dim} S_{r-2}$$

and

$$\operatorname{Dim} S^{\#\#}_r = \operatorname{Dim} S^{\#}_r - \operatorname{Dim} S^{\#}_{r-3}$$

for all $r \geq 2$. Moreover $\operatorname{Dim} S_r \geq \operatorname{Dim} S^{\#\#}_r \geq \operatorname{Dim} Q_r$ for all values of r.

By Theorem 3.4, $t_G \leq 2t_U$ (with equality in most cases) and moreover, by Lemma 3.2, we see that $t_U < 2^h$ in all cases. The choice that $r \leq t_G$ now means that

$$r \leq t_G \leq 2t_U < 2 \cdot 2^h = 2 \cdot \deg(\delta)$$

and this implies that we must have either $\operatorname{Dim} \mathrm{H}^r(H,k) = \operatorname{Dim} Q_r$, if $r < \deg(\delta)$, or $\operatorname{Dim} \mathrm{H}^r(H,k) = \operatorname{Dim} Q_r + \operatorname{Dim}(\delta \cdot Q_{r-\deg(\delta)})$, if $\deg(\delta) \le r < 2\deg(\delta)$. Notice also that $\deg(\delta) = 2^h \ge 4$ in all cases because we assumed that $m \ge 2$ and $U \not\cong D_8$ (if $U \cong D_8$, then $h = 1$ and $\deg(\delta) = 2$). Hence we have that

$$\begin{aligned}
\operatorname{Dim} \mathrm{H}^r(H,k) &\le \operatorname{Dim} Q_r + \operatorname{Dim} Q_{r-\deg(\zeta)} \\
&\le \operatorname{Dim} S^{\#}_r - \operatorname{Dim} S^{\#}_{r-3} + \operatorname{Dim} S^{\#}_{r-\deg(\zeta)} - \operatorname{Dim} S^{\#}_{r-\deg(\zeta)-3} \\
&\le \operatorname{Dim} S^{\#}_r - \operatorname{Dim} S^{\#}_{r-3} + \operatorname{Dim} S^{\#}_{r-\deg(\zeta)} \\
&\le \operatorname{Dim} S^{\#}_r = \binom{m+r}{r} - \binom{m+r-2}{r-2}.
\end{aligned}$$

The last inequality follows from the facts that $r - \deg(\delta) \le r - 3$ and that $\operatorname{Dim} S^{\#}_s$ is an increasing function of s. □

Corollary 3.6. *Suppose that G and H are as in the theorem. If $2 \le r \le t_G$, then*

$$\sum_{i=0}^{r} \operatorname{Dim} \Omega^i(k_H){\uparrow}_H^G \le \binom{m+r-1}{m}|G| + 2.$$

Proof. For any i we have an exact sequence

$$0 \longrightarrow \Omega^{i+1}(k_H) \longrightarrow P_i \longrightarrow \Omega^i(k_H) \longrightarrow 0$$

where P_i is the degree i term in a minimal kH-projective resolution of the trivial kH-module k_H. Recall that $\operatorname{Dim} P_i = \operatorname{Dim} \mathrm{H}^i(H,k) \cdot |H|$. Then by the theorem, for $r = 2s+1$,

$$\begin{aligned}
\sum_{i=0}^{r} \operatorname{Dim} \Omega^i(k_H) &= \sum_{j=0}^{s} \left(\operatorname{Dim} \Omega^{2j+1}(k_H) + \operatorname{Dim} \Omega^{2j}(k_H) \right) = \sum_{j=0}^{s} \operatorname{Dim} P_{2j} \\
&\le \operatorname{Dim} P_0 + \sum_{j=1}^{s} \left[\binom{m+2j}{2j} - \binom{m+2j-2}{2j-2} \right] |H| \\
&= |H| + \left[\binom{m+2s}{2s} - \binom{m}{0} \right] |H| \\
&= \binom{m+r-1}{r-1}|H| = \binom{m+r-1}{m}|H|.
\end{aligned}$$

On the other hand if $r = 2s$ is even, then we use the fact that $\operatorname{Dim} P_1 = \binom{m+1}{1}|G|$ and we obtain similarly

$$\begin{aligned}
\sum_{i=0}^{r} \operatorname{Dim} \Omega^i(k_H) &= \operatorname{Dim} k + \operatorname{Dim} P_1 + \sum_{j=2}^{s} \operatorname{Dim} P_{2j-1} \\
&\le 1 + \binom{m+2s-1}{2s-1}|H| = 1 + \binom{m+r-1}{m}|H|.
\end{aligned}$$

In both cases, inducing from H to G, the dimension of $\Omega^i(k_H)\uparrow_H^G$ is doubled and the result follows. □

4. Extraspecial groups in odd characteristic

Our aim in this section is to get results similar to those of the last section for extraspecial p-groups in the case that the prime p is not 2. As in the characteristic 2 case, for any positive integer n there are two isomorphism types of extraspecial groups of order p^{2n+1} and one isomorphism type of almost extraspecial group of order p^{2n+2}. For each n, one of the two nonisomorphic groups of order p^{2n+1} has exponent p^2 and the other one has exponent p. In the earlier paper [CaTh] we showed that Theorem 1.4 holds for extraspecial groups of exponent p^2 and almost extraspecial groups (i.e. for these groups there are no nontrivial critical modules). As a consequence, the only groups of interest to us are the extraspecial groups of order p^{2n+1} and exponent p.

Up to isomorphism, there is exactly one extraspecial group G_1 of order p^3 and exponent p. It is generated by elements x, y and z, which satisfy the relations that z is in the center of G_1, $z^p = x^p = y^p = 1$ and $[x, y] = z$. It is isomorphic to the Sylow p-subgroup of the general linear group $\mathrm{GL}(3, p)$. For $n > 1$, the extraspecial group of order p^{2n+1} is a central product

$$G_n = G_1 \ * \ G_1 \ * \ \dots \ * \ G_1$$

of n copies of G_1 as in the last section. That is, G_n is the quotient group obtained by taking the direct product of n copies of G_1 and then identifying the centers (see [Go1]). The center of G_n is a cyclic subgroup $Z = \langle z \rangle$ of order p and G_n/Z is an elementary abelian p-group of order p^{2n}.

We need an analogue to Theorem 3.4 for our case.

THEOREM 4.1. *For $G = G_1$, let $t_G = 2(p+1)$, while for $G = G_n$, $n > 1$, let $t_G = (p^2 + p - 1)p^{n-2}$. Then there exist nonzero elements $\eta_1, \dots, \eta_t \in \mathrm{H}^1(G, \mathbb{F}_p)$ such that $\beta(\eta_1) \dots \beta(\eta_t) = 0$ where $t = t_G$. Moreover, in the isomorphism $\mathrm{H}^1(G, \mathbb{F}_p) \cong \mathrm{Hom}(G, \mathbb{F}_p)$, each η_i corresponds to a homomorphism whose kernel is a maximal subgroup of G and is the centralizer of a noncentral element of order p in G.*

Proof. The proof of the theorem is contained in the paper by Yalçin as Theorem 1.2 of [Ya]. In this case the dimension of $\mathrm{H}^1(G, \mathbb{F}_p,)$ is the same as that of $\mathrm{Hom}(G, \mathbb{F}_p)$ which is $2n$. □

As in the last section we are going to need estimates on the dimensions of the cohomology groups $\mathrm{H}^r(G_n, k)$ where k is a field of characteristic p. We begin with the case of the extraspecial group $G = G_1$ of order p^3. Ian Leary [Le1] has given a complete description of the cohomology ring $\mathrm{H}^*(G, k)$ except that he did not fully compute the Poincaré series, which is something that we need. The calculation is, of course, implicit in his work, and he did calculate it in the special case that $p = 3$ [Le2]. Note that our results agree with his in that situation.

THEOREM 4.2. *The Poincaré series for the cohomology ring of the group $G = G_1$ is given by the rational function*

$$\sum_{n=0}^{\infty} \operatorname{Dim} \mathrm{H}^n(G,k)\ t^n = \frac{1+t+2t^2+2t^3+t^4+t^5+\cdots+t^{2p-1}}{(1-t)(1-t^{2p})}.$$

Proof. We will not repeat the long list of relations given by Leary (Theorem 6 of [Le1]). However we will use exactly the notation of that paper and the interested reader can follow the computation. The strategy is first to ignore the contribution of the regular element z in degree $2p$. This element is a nondivisor of zero as it restricts nontrivially to the center of G. We also know that it is regular from the given relation and from the fact that it is represented on the E_2 of the spectral sequence, by an element in $E_2^{0,2p}$ which survives to the E_∞ page of the spectral sequence. Consequently, the Poincaré series $f(t)$ of $\mathrm{H}^*(G,k)$ is obtained by multiplying $1/(1-t^{2p})$ times the Poincaré series of the subalgebra A generated by all of the given generators other than z.

Next we consider the subalgebra A as a module over the subring R generated by x and x'. Note that x and x' are in degree 2 and satisfy the relation $x^p x' - x x'^p = 0$ in degree $2p+2$. So the Poincaré series for R is $f_1 = (1-t^{2p+2})/(1-t^2)^2$. This is also the series for the R-submodule M_1 generated by the element 1 in degree 0. The first thing that needs to be established from the relations is that the R-generators are the elements of the sequence

$$S = [1, y, y', Y, Y', X, X', yY', XY', XX', d_4, c_4, d_5, \ldots, c_{p-1}, d_p]$$

of length $2p+3$. Let M_i be the R-submodule generated by the first i elements of the sequence, and let f_i be the Poincaré series for M_i/M_{i-1}. Then the desired Poincaré series for A is $f_1 + f_2 + \cdots + f_{2p+3}$. Note that f_1 has been calculated.

- For f_2, we note that $xy' = x'y$ and $x^p y' = x'^p y$. So $x'(x^{p-1} - x'^{p-1})y = 0$. Therefore $f_2 = t(1-t^{2p})/(1-t^2)^2$.
- Since $xy' = x'y \in M_2$, we have that $f_3 = t/(1-t^2)$.
- Similarly to the calculation for f_2, we have that $f_4 = t^2(1-t^{2p})/(1-t^2)^2$ and $f_6 = t^3(1-t^{2p})/(1-t^2)^2$.
- For f_5, note that $x^2 Y' = xx'Y \in M_4$ and $xx'Y' \in M_4$. Therefore $f_5 = t^3 + t^2/(1-t^2)$.

- The calculation for f_7 is similar to that for f_3 and we get that $f_7 = t^3/(1-t^2)$.
- For $i := 8, \ldots, 2p+3$, it should be checked that $xS_i, x'S_i \in M_{i-1}$ where S_i is the i^{th} element of the sequence S. Consequently, $f_i = t^{j_i}$, where j_i is the degree of S_i. Note that $j_8 = 3$ while $j_i = i-4$ for $i \geq 9$.

Finally it is necessary to verify that

$$f_1 + f_2 + \cdots + f_{2p+3} = (1 + t + 2t^2 + 2t^3 + t^4 + \cdots + t^{2p-1})/(1-t)$$

by routine but tedious calculation. □

We need to derive two facts from the above theorem. The first is an upper bound which is not optimal but will be sufficient for our purposes.

COROLLARY 4.3. *For* $G = G_1$,

$$\operatorname{Dim} \mathrm{H}^r(G,k) \leq 2(r+1) = 2\binom{r+1}{1}.$$

Moreover, $\operatorname{Dim} \mathrm{H}^r(G,k) = 2r$ *if* $1 \leq r \leq 3$ *and* $\operatorname{Dim} \mathrm{H}^r(G,k) = r+3$ *if* $4 \leq r \leq 2p-1$.

Proof. Consider the series expansion

$$g(t) = \frac{1 + t + 2t^2 + 2t^3 + t^4 + \cdots + t^{2p-1}}{1-t} = \sum_{r=0}^{\infty} a_r t^r\,.$$

A routine computation yields the value of the coefficients $a_0 = 1$, $a_r = 2r$ if $1 \leq r \leq 3$, $a_r = r+3$ if $4 \leq r \leq 2p-1$, and $a_r = 2p+2$ if $r \geq 2p-1$. The Poincaré series for the cohomology ring of G_1 is obtained by multiplying $g(t)$ with $\frac{1}{1-t^{2p}} = \sum_{i=0}^{\infty} t^{2ip}$. Therefore $\operatorname{Dim} \mathrm{H}^r(G,k) = a_r$ for $r \leq 2p-1$ and this proves the second statement of the lemma. Moreover, for arbitrary r, writing $r = j + q(2p)$ with $0 \leq j < 2p$, we have that

$$\operatorname{Dim} \mathrm{H}^r(G,k) = a_j + qa_{2p} \leq (j+3) + q(2p+2) \leq 2(r+1)\,. \qquad \square$$

COROLLARY 4.4. *For* $G = G_1$, $\operatorname{Dim} \Omega^{2p}(k) = p^3(p+1)+1$.

Proof. If P_j is the j-th term of a minimal projective resolution of k, we have $\operatorname{Dim}(P_j) = \operatorname{Dim} \mathrm{H}^j(G,k)\,|G|$ and so $\operatorname{Dim} \Omega^{j+1}(k) = \operatorname{Dim} \mathrm{H}^j(G,k)|G| - \operatorname{Dim} \Omega^j(k)$. Using this relation and the dimensions given in the previous corollary, we obtain $\operatorname{Dim} \Omega^2(k) = p^3+1$ and then by induction $\operatorname{Dim} \Omega^{2j-1}(k) = (j+1)p^3 - 1$ and $\operatorname{Dim} \Omega^{2j}(k) = (j+1)p^3 + 1$ for $2 \leq j \leq p$. □

In the rest of the section, we require the following well known combinatorial identity.

LEMMA 4.5. *For all integers $c, i, j \geq 0$,*

$$\sum_{a+b=c} \binom{a+i}{i}\binom{b+j}{j} = \binom{c+i+j+1}{i+j+1}.$$

Proof. Recall that if P is a polynomial ring in n variables, then the number of monomials of degree r is $\binom{r+n-1}{n-1}$. Now the tensor product of a polynomial ring in $i+1$ variables with a polynomial ring in $j+1$ variables yields a polynomial ring in $i+j+2$ variables. The identity follows by counting the number of monomials of degree c. $\square$

We also need to know the dimension of the cohomology groups of elementary abelian groups.

LEMMA 4.6. *Let p be an odd prime and let E be an elementary abelian p-group of rank m. Then* $\operatorname{Dim} \mathrm{H}^r(E,k) = \binom{r+m-1}{m-1}$.

Proof. Recall that $\mathrm{H}^*(E,k) \cong k[\zeta_1, \ldots, \zeta_m] \otimes \Lambda(\eta_1, \ldots, \eta_m)$ where $\zeta_1, \ldots, \zeta_m$ are in degree 2 and $\eta_1, \ldots, \eta_m$ are in degree 1. A basis of $\mathrm{H}^r(E,k)$ consists of the elements $\zeta_1^{a_1} \ldots, \zeta_m^{a_m} \eta_1^{e_1}, \ldots, \eta_m^{e_m}$ where $0 \leq a_i \leq r/2$, $0 \leq e_i \leq 1$ and $\sum_{i=1}^m (2a_i + e_i) = r$. This basis is in bijection with the set of monomials of degree r in $k[x_1, \ldots, x_m]$ by mapping the above basis element to $x_1^{2a_1+e_1} \ldots x_m^{2a_m+e_m}$. Now the number of monomials of degree r is $\binom{r+m-1}{m-1}$. $\square$

Our main result in this section gives estimates for the dimensions of the cohomology of the centralizers of p-elements.

THEOREM 4.7. *Let $G = G_n$ be an extraspecial group of order p^{2n+1} and exponent p. Let H be the centralizer of a noncentral element of order p in G. Then $H \cong C_p \times G_{n-1}$. Moreover,*

$$\operatorname{Dim} \mathrm{H}^m(H,k) \leq 2\binom{m+2n-2}{2n-2}.$$

Proof. As with the characteristic 2 case, the structure of the centralizer H can be verified directly from what we know of G. All noncentral elements of order p in G are conjugate by an element in the automorphism group of G and hence their centralizers are isomorphic.

Next we need to approximate the dimensions of the cohomology groups of the group G_{n-1} for $n \geq 1$. The estimate in Corollary 4.3 will serve in the case that $n = 2$. Let N be a normal subgroup of G_{n-1} such that $N \cong G_1$. We can take N to be the first factor in the central product that expresses G_{n-1}. Then $G_{n-1}/N \cong C_p^{2(n-2)}$, an elementary abelian group of order $p^{2(n-2)}$. The Lyndon-Hochschild-Serre spectral sequence of the extension of G_{n-1}/N by N

has E_2 term

$$E_2^{r,s} = \mathrm{H}^r(G_{n-1}/N, \mathrm{H}^s(N,k)) \Rightarrow \mathrm{H}^{r+s}(G_{n-1},k).$$

As k-vector spaces, it is true that $E_2^{r,s} \cong \mathrm{H}^r(G_{n-1}/N,k) \otimes \mathrm{H}^s(N,k)$ because N commutes with the other factors of the central product. So we have that

$$\begin{aligned} \operatorname{Dim} \mathrm{H}^m(G_{n-1},k) &\leq \sum_{r+s=m} \operatorname{Dim}(E_2^{r,s}) \\ &= \sum_{r+s=m} \operatorname{Dim} \mathrm{H}^r(G_{n-1}/N,k)\ \operatorname{Dim} \mathrm{H}^s(N,k) \\ &\leq \sum_{r+s=m} \binom{r+2(n-2)-1}{2(n-2)-1} 2 \binom{s+1}{1} = 2\binom{m+2n-3}{2n-3}, \end{aligned}$$

using Lemma 4.6, Corollary 4.3 and the combinatorial identity of Lemma 4.5.

Now $\mathrm{H}^m(H,k) \cong \bigoplus_{r+s=m} \mathrm{H}^r(G_{n-1},k) \otimes \mathrm{H}^s(C_p,k)$. Therefore,

$$\begin{aligned} \operatorname{Dim} \mathrm{H}^m(H,k) &= \sum_{r+s=m} \operatorname{Dim} \mathrm{H}^r(G_{n-1},k) \cdot \operatorname{Dim} \mathrm{H}^s(C_p,k) \\ &\leq \sum_{r+s=m} 2\binom{r+2n-3}{2n-3}\binom{s}{0} = 2\binom{m+2n-2}{2n-2}, \end{aligned}$$

again by Corollary 4.3 and Lemma 4.5. □

Corollary 4.8. *Suppose that G and H are as in the theorem. If $r \geq 1$, then*

$$\sum_{i=0}^{r} \operatorname{Dim} \Omega^i(k_H)\!\uparrow_H^G \leq 2p^{2n+1}\binom{r+2n-2}{2n-1}.$$

Proof. Suppose that $\cdots \to P_1 \to P_0 \to k \to 0$ is a minimal kH-projective resolution of the trivial module k. Then we know that $\operatorname{Dim} \Omega^0(k) + \operatorname{Dim} \Omega^1(k) = \operatorname{Dim} P_0$. For $j \geq 2$, $\Omega^j(k_H)$ is a submodule of P_{j-1}. The dimension of P_j is precisely $|H| \operatorname{Dim} \mathrm{H}^j(H,k)$ and the dimension of $\Omega^j(k_H)\!\uparrow_H^G$ is p times the dimension of $\Omega^j(k_H)$. So from the theorem we have that

$$\begin{aligned} \sum_{i=0}^{r} \operatorname{Dim} \Omega^i(k_H)\!\uparrow_H^G &\leq p|H| \sum_{i=0}^{r-1} \operatorname{Dim} \mathrm{H}^i(H,k) \\ &\leq p^{2n+1} \sum_{i=0}^{r-1} 2\binom{i+2n-2}{2n-2}\binom{r-1-i}{0} \\ &= 2p^{2n+1}\binom{r+2n-2}{2n-1}, \end{aligned}$$

by the identity 4.5. □

5. New endo-trivial modules from old endo-trivial modules

Here we start the proof of Theorem 1.4. Suppose that G is an extraspecial or almost extraspecial p-group and that $G \ncong Q_8$. Let $Z = \langle z \rangle$ be the Frattini subgroup of G, of order p, with elementary abelian quotient $\overline{G} = G/Z$ of rank m. Let $x_1, \ldots, x_m \in G$ such that $\overline{G} = \langle \overline{x}_1, \ldots, \overline{x}_m \rangle$. Recall that Z is the unique normal subgroup of order p. Moreover every maximal subgroup of G contains Z and G is not elementary abelian. Some of the results in this section hold more generally if G has a Frattini subgroup Z of order p, but we leave this generalization to the reader.

Let M be an endo-trivial kG-module whose class in $T(G)$ lies in the kernel of the restriction to proper subgroups. This means that $M{\downarrow}^G_H \cong k \oplus (\text{free})$ for every maximal subgroup H of G. For the purpose of the proof of Theorem 1.4 (Sections 5–11), we make the following definition:

Definition 5.1. We say that a kG-module M is *critical* if it is an indecomposable endo-trivial module such that $M{\downarrow}^G_H \cong k \oplus (\text{free})$ for every maximal subgroup H of G.

Actually, the last condition implies that the module M is endo-trivial because its restriction to every elementary abelian subgroup is isomorphic to $k \oplus (\text{free})$, hence endo-trivial (see Lemma 2.9 of [CaTh]). In fact M is a torsion endo-trivial module by a theorem of Puig [Pu], but we do not need this fact in our arguments. By factoring out all free summands of an endo-trivial module M, one can always assume that M is indecomposable and this is why we do so. We shall often omit to mention this indecomposability condition, to the effect that we shall usually only prove that a module satisfies the condition on restriction to maximal subgroups in order to deduce that it is critical. Since our aim is to prove that the kernel above is trivial, we have to show that any critical kG-module M is isomorphic to k as a kG-module. We will often assume, by contradiction, the existence of a nontrivial critical kG-module.

In this section, we prove several results concerning the structure of a critical module M and the construction of new modules with the same property. For some of the results, we only need to assume that $M{\downarrow}^G_H \cong k \oplus (\text{free})$ for a single subgroup H of G.

For any critical kG-module M, and more generally for any kG-module M such that $M{\downarrow}^G_Z \cong k \oplus (\text{free})$, we let $M' = \{m \in M \mid (z-1)^{p-1}m = 0\}$ and we set

$$\overline{M} = M/M' .$$

We let $^{-} : M \longrightarrow \overline{M}$ be the quotient map. Since $(z-1)\overline{M} = 0$, the module $\overline{M}$ can be viewed as a $k\overline{G}$-module. A large part of this paper is devoted to an analysis of the properties of the module $\overline{M}$.

LEMMA 5.2. *Let M be a kG-module. Suppose that $M{\downarrow}_Z^G \cong k \oplus (\text{free})$.*

(a) *The module M has two filtrations*

$$\begin{array}{ccccccccccc} & & K_1 & \subset & K_2 & \subset & \dots & \subset & K_{p-1} & \subset & K_p = M \\ & & \cup & & \cup & & & & \cup & & \\ \{0\} & \subset & I_{p-1} & \subset & I_{p-2} & \subset & \dots & \subset & I_1 & & \end{array}$$

where $K_i = \{m \in M \mid (z-1)^i m = 0\}$ is the kernel of multiplication by $(z-1)^i$ (in particular $K_{p-1} = M'$) and $I_i = (z-1)^i M$ is the image of multiplication by $(z-1)^i$.

(b) *$K_i/I_{p-i} \cong k$ for any $i = 1, \dots, p-1$. Moreover $K_{p-1}/I_{p-1} \cong k \oplus (I_1/I_{p-1})$.*

(c) *The module $I_1 = (z-1)M$ is free as a module over the ring $kZ/(z-1)^{p-1}$. Moreover, $I_i/I_{i+1} \cong \overline{M}$ for any $i = 1, \dots, p-1$.*

(d) *The module M/K_1 is isomorphic to I_1. In particular it is free as a module over the ring $kZ/(z-1)^{p-1}$ and $K_{i+1}/K_i \cong \overline{M}$ for any $i = 1, \dots, p-1$.*

(e) $\mathrm{Dim}(M) = p\,\mathrm{Dim}(\overline{M}) + 1$.

Proof. (a) Note that K_i and I_i are submodules because z is central in kG. We have $I_{p-i} \subset K_i$ because $(z-1)^p = 0$. The filtrations are clear.

(b) In order to prove (b), it suffices to restrict to the subgroup Z. But we have $M{\downarrow}_Z^G = k \oplus F$ for some free kZ-module F, and therefore

$$K_i = k \oplus (z-1)^{p-i} F\,, \quad I_{p-i} = (z-1)^{p-i} F\,.$$

Moreover it is clear that $K_{p-1}/I_{p-1} = K_1/I_{p-1} \oplus (I_1/I_{p-1}) \cong k \oplus (I_1/I_{p-1})$.

(c) Multiplication by $(z-1)^i$ induces a map

$$M \longrightarrow (z-1)^i M/(z-1)^{i+1} M = I_i/I_{i+1}$$

and we claim that its kernel is M'. Again, in order to prove this, it suffices to restrict to the subgroup Z and consider the decomposition $M{\downarrow}_Z^G = k \oplus F$ as above. Then the kernel is $k \oplus (z-1)F = M'$. It is also clear that

$$(z-1)M = (z-1)F \cong F/(z-1)^{p-1} F$$

and this is free over the ring $kZ/(z-1)^{p-1}$.

(d) Multiplication by $(z-1)$ induces an isomorphism $M/K_1 \cong I_1$.

(e) Since $M{\downarrow}_Z^G = k \oplus F$, we have that $\mathrm{Dim}(\overline{M}) = \mathrm{Dim}(F/(z-1)F) = \mathrm{Dim}(F)/p$ and $\mathrm{Dim}(M) = p\,\mathrm{Dim}(\overline{M}) + 1$. □

LEMMA 5.3. *Let M be a kG-module. Suppose that there is a maximal subgroup H of G such that $M{\downarrow}_H^G \cong k \oplus (\text{free})$.*

(a) $M \cong k \oplus (\text{free})$ *as a* kG*-module if and only if* $\overline{M}$ *is a free* $k\overline{G}$*-module. More precisely,* M *has a free summand with* r *generators as a* kG*-module if and only if* $\overline{M}$ *has a free summand with* r *generators as a* $k\overline{G}$*-module. In particular, if* M *is indecomposable, then* $\overline{M}$ *has no projective summands.*

(b) $M \not\cong k \oplus (\text{free})$ *as a* kG*-module if and only if* $\overline{M}$ *is a periodic* $k\overline{G}$*-module.*

Proof. (a) It is easy to see that if M has a free summand $L \cong (kG)^r$ as a kG-module then $\overline{M}$ has a free summand $L/(z-1)L \cong (k\overline{G})^r$ as a $k\overline{G}$-module.

The converse is essentially contained in Lemma 3.3 of [CaTh] and we recall the argument. Assume that $M = N \oplus L$ where L is free and N has no free summands. Then $t_1^G \cdot N = 0$ where

$$t_1^G = \sum_{g \in G} g = (z-1)^{p-1} \prod_{i=1}^{m} (x_i - 1)^{p-1} ,$$

x_i being a lift in G of the generator $\overline{x}_i$ of $\overline{G}$. Let $X = \prod_{i=1}^{m}(x_i - 1)^{p-1}$. If $\overline{N}$ has a free submodule then $X \cdot \overline{N} \neq 0$, since $\overline{X} = t_1^{\overline{G}}$. But if $X \cdot \overline{N} \neq 0$ then, via the isomorphism $\overline{N} \cong (z-1)^{p-1}N$ of Lemma 5.2, we would obtain $(z-1)^{p-1}X \cdot N = t_1^G \cdot N \neq 0$, which is a contradiction.

(b) The hypothesis on $M{\downarrow}_H^G$ implies that $\overline{M}$ is free on restriction to H/Z. But $\overline{H} = H/Z$ is a maximal subgroup of $\overline{G} = G/Z$, so $\overline{G}/\overline{H}$ is a cyclic group of order p. Tensoring with $\overline{M}$ the exact sequence

$$0 \longrightarrow k \longrightarrow k[\overline{G}/\overline{H}] \longrightarrow k[\overline{G}/\overline{H}] \longrightarrow k \longrightarrow 0 ,$$

we obtain an exact sequence with $\overline{M}$ at both ends and free $k\overline{G}$-modules in the middle, because $k[\overline{G}/\overline{H}] \otimes \overline{M} \cong \overline{M}{\downarrow}_{\overline{H}}^{\overline{G}}{\uparrow}_{\overline{H}}^{\overline{G}}$. If now $M \not\cong k \oplus (\text{free})$, then $\overline{M}$ is not zero and is not free as a $k\overline{G}$-module, by part (a), so $\overline{M}$ is periodic. If conversely $\overline{M}$ is periodic, then $\overline{M}$ is not free and $M \not\cong k \oplus (\text{free})$ by part (a). $\square$

LEMMA 5.4. *Suppose that* $p = 2$ *and that* M *is a nontrivial critical* kG*-module. Then the number of generators of* M *is the same as the number of generators of* $\overline{M}$ *and is equal to* $4\,\mathrm{Dim}(\overline{M})/|G|$. *Moreover* $\mathrm{Dim}(\Omega(M)) = \mathrm{Dim}(\Omega^{-1}(M)) = \mathrm{Dim}(M) - 2$.

Proof. Let H be a maximal subgroup of G. Since $M{\downarrow}_H^G \cong k \oplus (\text{free})$, we know that $\overline{M}$ is free as a module over $k\overline{H}$. Thus, the number of generators of $\overline{M}$ as a $k\overline{H}$-module is $\mathrm{Dim}(\overline{M})/|\overline{H}|$. Our first claim is that G acts trivially on $\overline{M}/\mathrm{Rad}(k\overline{H})\overline{M}$. Thus, the number of generators of $\overline{M}$ as a $k\overline{G}$-module is also $\mathrm{Dim}(\overline{M}/\mathrm{Rad}(k\overline{H})\overline{M}) = \mathrm{Dim}(\overline{M})/|\overline{H}|$. In order to prove the claim, we note that the group G/H acts on $\overline{M}/\mathrm{Rad}(k\overline{H})\overline{M}$. If there were a free summand generated by the class of an element $\overline{m}$, then $\overline{m}$ would generate a free summand of $\overline{M}$ as a module over $k\overline{G}$, contrary to part (c) of the previous lemma. Since the group G/H has order 2, the only possibility is that G/H acts trivially on $\overline{M}/\mathrm{Rad}(k\overline{H})\overline{M}$.

Now our second claim is that, given a set of generators of $\overline{M}$, some lifts of those generators in M will generate M. If we asume this, it follows that the number of generators of M is $\mathrm{Dim}(\overline{M})/|\overline{H}| = 4\,\mathrm{Dim}(\overline{M})/|G|$. If $r = 4\,\mathrm{Dim}(\overline{M})/|G|$, then the projective cover of M is the free module $(kG)^r$. Using Lemma 5.2 we obtain

$$\begin{aligned}\mathrm{Dim}(\Omega(M)) &= \mathrm{Dim}((kG)^r) - \mathrm{Dim}(M)\\ &= 4\,\mathrm{Dim}(\overline{M}) - 2\,\mathrm{Dim}(\overline{M}) - 1 = \mathrm{Dim}(M) - 2\end{aligned}$$

as desired. Finally, since the dual module M^* also satisfies the assumptions of the lemma, we have that

$$\begin{aligned}\mathrm{Dim}(\Omega^{-1}(M)) &= \mathrm{Dim}(\Omega^{-1}(M)^*)\\ &= \mathrm{Dim}(\Omega(M^*)) = \mathrm{Dim}(M^*) - 2 = \mathrm{Dim}(M) - 2\end{aligned}$$

and this completes the proof.

We are left with the proof of the second claim. Let L be the submodule of M generated by some lifts in M of the generators of $\overline{M}$. Assume by contradiction that $L \neq M$. Since $M{\downarrow}^G_H = k \oplus F$ for some free kH-module F, we have $\overline{M}{\downarrow}^{\overline{G}}_{\overline{H}} = F/(z-1)F$ and so we can choose the lifts of the generators of $\overline{M}$ so that $L{\downarrow}^G_H = F$. Now for any other maximal subgroup H' of G, we have $M{\downarrow}^G_{H'} = k \oplus F'$ for some free kH'-module F'. The subgroup $H \cap H'$ is nontrivial because it contains Z and there are two decompositions

$$M{\downarrow}^G_{H\cap H'} = T{\downarrow}^H_{H\cap H'} \oplus F{\downarrow}^H_{H\cap H'} = T'{\downarrow}^{H'}_{H\cap H'} \oplus F'{\downarrow}^{H'}_{H\cap H'}$$

where T, respectively T', denotes a trivial one-dimensional module for kH, respectively kH'. By comparing the fixed points $M^{H\cap H'}$ and the relative traces $t_1^{H\cap H'} \cdot M$ in both decompositions, we see that $T'{\downarrow}^{H'}_{H\cap H'}$ cannot be contained in $F{\downarrow}^H_{H\cap H'}$ and therefore

$$M{\downarrow}^G_{H\cap H'} = T'{\downarrow}^{H'}_{H\cap H'} \oplus F{\downarrow}^H_{H\cap H'}$$

(see Lemma 8.2 in [CaTh] for details). Since F is the restriction of a kG-submodule, this is a decomposition of M as a kH'-module, namely

$$M{\downarrow}^G_{H'} = T' \oplus L{\downarrow}^G_{H'}\,.$$

By the Krull-Schmidt theorem, we deduce that $L{\downarrow}^G_{H'}$ is free. Since this holds for any maximal subgroup H' and since G is not elementary abelian, Chouinard's theorem (see [Be] or [Ev]) implies that L is free as a kG-module and so $M \cong k \oplus L$. But M is indecomposable and nontrivial by assumption. This contradiction completes the proof of the claim. $\square$

For our next theorem, we first need a technical lemma.

Lemma 5.5. *Let W be a kG-module satisfying the following two conditions*:

(a) *$W/(z-1)W = U_1 \oplus U_2$ where U_1 and U_2 are $k\overline{G}$-submodules such that the varieties satisfy $V_{\overline{G}}(U_1) \cap V_{\overline{G}}(U_2) = \{0\}$.*

(b) *For some $r \leq p$, there is $(z-1)^r W = 0$ and W is free as a module over the ring $kZ/(z-1)^r$.*

Then $W = W_1 \oplus W_2$ where W_1 and W_2 are kG-submodules of W such that $W_i/(z-1)W_i \cong U_i$ for $i = 1, 2$.

Proof. We use induction on r. There is nothing to prove if $r = 1$ so we assume $r \geq 2$. By induction, $W/(z-1)^{r-1}W = V_1 \oplus V_2$ where V_1 and V_2 are kG-submodules of $W/(z-1)^{r-1}W$ such that $V_i/(z-1)V_i \cong U_i$ for $i = 1, 2$. Now, since W is free as a module over $kZ/(z-1)^r$, multiplication by $(z-1)$ induces an isomorphism $W/(z-1)^{r-1}W \cong (z-1)W$ and we write L_i for the image of V_i. So $(z-1)W = L_1 \oplus L_2$.

Let $\pi : W \to W/(z-1)W = U_1 \oplus U_2$ be the canonical surjection. Passing to the quotient by L_1, we obtain a short exact sequence

$$0 \longrightarrow L_2 \longrightarrow W/L_1 \xrightarrow{\widetilde{\pi}} U_1 \oplus U_2 \longrightarrow 0$$

where $\widetilde{\pi}$ is induced by π. Let $K = \{x \in W/L_1 \mid (z-1)x = 0\}$. We claim that $\widetilde{\pi}(K) = U_1$. Let $x \in K$ and let $w \in W$ be a lift of x. Then $(z-1)w \in L_1$. Since multiplication by $(z-1)$ induces an isomorphism $W/(z-1)^{r-1}W \cong (z-1)W$, the class of w in $W/(z-1)^{r-1}W$ is in V_1. It follows that $\pi(w) \in U_1$, hence $\widetilde{\pi}(x) \in U_1$, proving the claim.

Therefore we obtain a short exact sequence

$$0 \longrightarrow (z-1)^{r-2}L_2 \longrightarrow K \xrightarrow{\widetilde{\pi}} U_1 \longrightarrow 0$$

because $L_2 \cap \mathrm{Ker}(z-1) = (z-1)^{r-2}L_2$. This is a sequence of $k\overline{G}$-modules since $(z-1)K = 0$ by construction. Now multiplication by $(z-1)^{r-1}$ induces an isomorphism $W/(z-1)W \cong (z-1)^{r-1}W$ mapping U_2 onto $(z-1)^{r-2}L_2$. By applying our assumption on the varieties of U_1 and U_2 we deduce that the sequence splits (see Theorem 2.2). Let σ be a section of $\widetilde{\pi} : K \to U_1$ and let W_1 be the inverse image of $\sigma(U_1)$ in W, so that $W_1/L_1 = \sigma(U_1)$. We have obtained a short exact sequence

$$0 \longrightarrow L_1 \longrightarrow W_1 \xrightarrow{\pi} U_1 \longrightarrow 0\,.$$

We can construct similarly a submodule W_2 and a short exact sequence

$$0 \longrightarrow L_2 \longrightarrow W_2 \xrightarrow{\pi} U_2 \longrightarrow 0\,.$$

Then $\pi(W_1 \cap W_2) = 0$, so that $W_1 \cap W_2 \subseteq \mathrm{Ker}(\pi) = L_1 \oplus L_2$. But since $W_i \cap \mathrm{Ker}(\pi) = L_i$, we obtain $W_1 \cap W_2 = 0$. For reasons of dimensions (or by a direct argument), the direct sum $W_1 \oplus W_2$ must be the whole of W. □

THEOREM 5.6. *Let M be a critical kG-module and suppose that $\overline{M} = \overline{M}_1 \oplus \overline{M}_2$ where $\overline{M}_1$ and $\overline{M}_2$ are $k\overline{G}$-submodules. Suppose that the varieties satisfy*

$$V_{\overline{G}}(\overline{M}_1) \cap V_{\overline{G}}(\overline{M}_2) = \{0\}.$$

Then there exist critical kG-modules N_1 and N_2 such that $\overline{N}_i \cong \overline{M}_i$ for $1 \leq i \leq 2$.

Proof. As before, let $M' = \{m \in M \mid (z-1)^{p-1}m = 0\}$. Let $M_1 \subseteq M$ be the inverse image of $\overline{M}_1$ under the quotient map $M \longrightarrow M/M' = \overline{M}$. Let M_2 be the inverse image of $\overline{M}_2$. Then $M' = M_1 \cap M_2$ and $M_1/M' \cong \overline{M}_1$, $M_2/M' = \overline{M}_2$.

By Lemma 5.2, $(z-1)M$ is free over $kZ/(z-1)^{p-1}$ and

$$(z-1)M/(z-1)^2M \cong M/M' = \overline{M} = \overline{M}_1 \oplus \overline{M}_2\,.$$

Therefore Lemma 5.5 applies and we have $(z-1)M = W_1 \oplus W_2$ such that $W_i/(z-1)W_i \cong \overline{M}_i$ for $i = 1, 2$. Now define $N_1 = M_1/W_2$ and $N_2 = M_2/W_1$. If $r_i = \mathrm{Dim}(\overline{M}_i)$, then $\mathrm{Dim}(\overline{M}) = r_1 + r_2$ and by Lemma 5.2 we obtain $\mathrm{Dim}(M) = pr_1 + pr_2 + 1$ and $\mathrm{Dim}((z-1)M) = (p-1)r_1 + (p-1)r_2$. Therefore we have $\mathrm{Dim}(M_1) = pr_1 + (p-1)r_2 + 1$ and $\mathrm{Dim}(M_2) = (p-1)r_1 + pr_2 + 1$. Also $\mathrm{Dim}(W_i) = (p-1)r_i$; hence $\mathrm{Dim}(N_i) = pr_i + 1$ for $i = 1, 2$.

We claim that $N_1{\downarrow}_H^G \cong k \oplus (\text{free})$ for every maximal subgroup H of G (and similarly for N_2). Let $H = \langle z, y_1, \ldots, y_{m-1}\rangle$ where $\overline{y}_1, \ldots, \overline{y}_{m-1}$ are generators of $\overline{H} = H/Z$. The assumption on $M{\downarrow}_H^G$ implies that $\overline{M}$ is free as a $k\overline{H}$-module. Therefore $\overline{M}_1$ and $\overline{M}_2$ must be free as $k\overline{H}$-modules. Let $Y = \displaystyle\prod_{i=1}^{m-1}(y_i - 1)^{p-1}$ so that $\overline{Y} = t_1^{\overline{H}}$ and $Y(z-1)^{p-1} = t_1^H$. Then we get

$$\mathrm{Dim}(\overline{M}_1) = |\overline{H}| \cdot \mathrm{Dim}(\overline{Y} \cdot \overline{M}_1)\,.$$

Now $(z-1)^{p-1}N_1 \cong (z-1)^{p-1}M_1$ because $N_1 = M_1/W_2$ and $(z-1)^{p-1}W_2 = 0$. Therefore

$$t_1^H \cdot N_1 = Y(z-1)^{p-1}N_1 \cong Y(z-1)^{p-1}M_1 \cong Y \cdot \overline{M}_1 = \overline{Y} \cdot \overline{M}_1\,.$$

It follows that

$$|H|\,\mathrm{Dim}(t_1^H \cdot N_1) = p \cdot |\overline{H}| \cdot \mathrm{Dim}(\overline{Y} \cdot \overline{M}_1) = p \cdot \mathrm{Dim}(\overline{M}_1) = pr_1 = \mathrm{Dim}(N_1) - 1\,.$$

Therefore $N_1{\downarrow}_H^G$ has a free submodule of dimension $\mathrm{Dim}(N_1) - 1$. The only way this can happen is if $N_1{\downarrow}_H^G \cong k \oplus (\text{free})$.

Now we prove that $\overline{N}_1 \cong \overline{M}_1$ (and similarly for N_2). We have to compute the submodule $N_1' = \{x \in N_1 \mid (z-1)^{p-1}x = 0\}$. But $N_1 = M_1/W_2$ and we have $W_2 \subseteq M' \subseteq M_1$ and $(z-1)^{p-1}M' = 0$. Therefore $M'/W_2 \subseteq N_1'$ and $\overline{N}_1 = N_1/N_1'$ is a quotient of $N_1/(M'/W_2) \cong M_1/M' = \overline{M}_1$. In order to prove that this is not a proper quotient, it suffices to prove that $\overline{N}_1$ and $\overline{M}_1$ have the same dimension. But by the previous part of the proof, we know that $N_1{\downarrow}^G_H \cong k \oplus (\text{free})$ for every maximal subgroup H. By Lemma 5.2 this implies

$$\mathrm{Dim}(\overline{N}_1) = \frac{\mathrm{Dim}(N_1) - 1}{p} = r_1 = \mathrm{Dim}(\overline{M}_1)\,,$$

as was to be shown.

Finally we conclude that N_1 is critical. Indeed, since $\overline{M}$ has no free summand as a $k\overline{G}$-module, $\overline{N}_1$ cannot have a free summand and therefore N_1 has no free summand as a kG-module by Lemma 5.3. This implies that N_1 is critical since we know that $N_1{\downarrow}^G_H \cong k \oplus (\text{free})$ for every maximal subgroup H. □

THEOREM 5.7. *Let M_1 and M_2 be critical kG-modules and suppose that the varieties satisfy*

$$V_{\overline{G}}(\overline{M}_1) \cap V_{\overline{G}}(\overline{M}_2) = \{0\}.$$

Then $M_1 \otimes M_2 \cong M \oplus (\text{free})$ where M is a critical kG-module such that $\overline{M} \cong \overline{M}_1 \oplus \overline{M}_2$.

Proof. Let $r_j = \mathrm{Dim}(\overline{M}_j)$ for $j = 1, 2$. Thus $\mathrm{Dim}(M_j) = pr_j + 1$. Consider the filtration of M_1 as in Lemma 5.2

$$\{0\} \subset (z-1)^{p-1}M_1 \subset K_1 \subset \cdots \subset K_{p-1} \subset K_p = M_1\,,$$

where $K_i = \{m \in M_1 \mid (z-1)^i m = 0\}$. This induces a filtration on $M_1 \otimes M_2$

$$\{0\} \subset (z-1)^{p-1}M_1 \otimes M_2 \subset K_1 \otimes M_2 \subset \cdots \subset K_{p-1} \otimes M_2 \subset M_1 \otimes M_2\,,$$

with all quotients but one isomorphic to $\overline{M}_1 \otimes M_2$. We need to prove the following.

LEMMA 5.8. *$\overline{M}_1 \otimes M_2 = F \oplus L$ where $L \cong \overline{M}_1$ and F is a free kG-module of dimension pr_1r_2 such that $(z-1)^{p-1}F = \overline{M}_1 \otimes (z-1)^{p-1}M_2$.*

Proof. By hypothesis $V_{\overline{G}}(\overline{M}_1) \cap V_{\overline{G}}(\overline{M}_2) = \{0\}$ and hence $\overline{M}_1 \otimes \overline{M}_2$ is projective as a $k\overline{G}$-module. Choose elements $m_1, \ldots, m_r \in \overline{M}_1 \otimes M_2$ such that $\overline{m}_1, \ldots, \overline{m}_r$ is a free $k\overline{G}$-basis for $\overline{M}_1 \otimes \overline{M}_2$. Here $\overline{m}_i = m_i + (\overline{M}_1 \otimes M_2')$ denotes the class of m_i in $\overline{M}_1 \otimes \overline{M}_2 = (\overline{M}_1 \otimes M_2)/(\overline{M}_1 \otimes M_2')$.

As before, let $X = \displaystyle\prod_{i=1}^{m}(x_i - 1)^{p-1}$ so that $\overline{X} = t_1^{\overline{G}}$ and $X(z-1)^{p-1} = t_1^G$. Then $\overline{X}\overline{m}_1, \ldots, \overline{X}\overline{m}_r$ are linearly independent in $\overline{M}_1 \otimes \overline{M}_2$. Since z acts trivially on $\overline{M}_1$, multiplication by $(z-1)^{p-1}$ induces an isomorphism $\overline{M}_1 \otimes \overline{M}_2 \cong \overline{M}_1 \otimes (z-1)^{p-1} M_2$ and it follows that $X(z-1)^{p-1}m_1, \dots, X(z-1)^{p-1}m_r$ are linearly independent in $\overline{M}_1 \otimes (z-1)^{p-1}M_2$. Therefore $t_1^G m_1, \dots, t_1^G m_r$ are linearly independent in $\overline{M}_1 \otimes M_2$. So the kG-submodule F of $\overline{M}_1 \otimes M_2$ generated by $m_1, \dots, m_r$ is a free kG-module. Moreover we have $(z-1)^{p-1}F = \overline{M}_1 \otimes (z-1)^{p-1}M_2$.

Consider now the exact sequence of $k\overline{G}$-modules

$$0 \longrightarrow \overline{M}_1 \otimes (z-1)^{p-1}M_2 \longrightarrow \overline{M}_1 \otimes (M_2)^Z \longrightarrow \overline{M}_1 \otimes k \longrightarrow 0\,,$$

where $(M_2)^Z = \{x \in M_2 \mid (z-1)x = 0\}$. Since the kernel is free over $k\overline{G}$, the sequence splits and we have $\overline{M}_1 \otimes (M_2)^Z \cong (z-1)^{p-1}F \oplus L$ where L is a submodule isomorphic to $\overline{M}_1$. If we had $F \cap L \neq 0$, then we would have $\mathrm{Soc}(F) \cap L \neq 0$; hence $(z-1)^{p-1}F \cap L \neq 0$, a contradiction. Therefore $F \cap L = 0$ and $\overline{M}_1 \otimes M_2$ contains a submodule $F \oplus L$.

We now show that $F \oplus L = \overline{M}_1 \otimes M_2$ by proving that both modules have the same dimension. We have $\mathrm{Dim}(F) = p \cdot \mathrm{Dim}(\overline{M}_1 \otimes \overline{M}_2) = pr_1r_2$ and therefore

$$\mathrm{Dim}(F \oplus L) = pr_1r_2 + r_1 = r_1(pr_2+1) = \mathrm{Dim}(\overline{M}_1)\,\mathrm{Dim}(M_2)\,,$$

as was to be shown. □

Now, continuing with the proof of the theorem, we note that each quotient $(K_{i+1} \otimes M_2)/(K_i \otimes M_2)$ is isomorphic to $\overline{M}_1 \otimes M_2$, hence contains a free submodule $\overline{F_i}$ of dimension pr_1r_2 by the lemma. Now remember that projective modules are also injective and, as a result, if a projective module is a direct summand of a section of a module V, then it is a direct summand of V. Thus we can lift the free module $\overline{F_i}$ and obtain a free submodule F_i of $M_1 \otimes M_2$ mapping isomorphically onto $\overline{F_i}$ under the quotient map $M_1 \otimes M_2 \to (M_1 \otimes M_2)/(K_i \otimes M_2)$. Similarly, $(z-1)^{p-1}M_1 \otimes M_2$ is isomorphic to $\overline{M}_1 \otimes M_2$, hence contains a free submodule F_0 of dimension pr_1r_2 by the lemma. Therefore we have

$$M_1 \otimes M_2 = M \oplus F$$

where $F = F_0 \oplus \cdots \oplus F_{p-1}$ is free of dimension $p^2r_1r_2$ and M is a submodule of dimension $(pr_1+1)(pr_2+1) - p^2r_1r_2 = p(r_1+r_2)+1$.

Since, for any maximal subgroup H of G, we have $M_j{\downarrow}_H^G \cong k \oplus (\text{free})$ for $j = 1, 2$, the same holds for $M_1 \otimes M_2$ and hence $M{\downarrow}_H^G \cong k \oplus (\text{free})$. We are going to prove that $\overline{M} \cong \overline{M}_1 \oplus \overline{M}_2$. This will imply that M is critical. Indeed $\overline{M}_j$ has no $k\overline{G}$-free summand, because M_j is critical $(j = 1, 2)$, so $\overline{M}_1 \oplus \overline{M}_2$ has no $k\overline{G}$-free summand and therefore M has no kG-free summand by Lemma 5.2. This forces the endo-trivial module M to be indecomposable.

Instead of working with $\overline{M}$, we consider the isomorphic module $(z-1)^{p-1}M$ and our goal now is to prove that $(z-1)^{p-1}M \cong \overline{M}_1 \oplus \overline{M}_2$.

We work with the submodule $K_1 \otimes M_2$ of our filtration and we first analyze its submodule $K_1 \otimes K_1'$, where $K_1' = \{m \in M_2 \mid (z-1)m = 0\}$ is the analog of K_1 for M_2. Notice that $K_1 \otimes K_1'$ is a $k\overline{G}$-module with a filtration

$$\begin{aligned}(z-1)^{p-1}M_1 \otimes (z-1)^{p-1}M_2 \subset \big((z-1)^{p-1}M_1 \otimes K_1'\big)& \\ +\big(K_1 \otimes (z-1)^{p-1}M_2\big) &\subset K_1 \otimes K_1' .\end{aligned}$$

In the filtration, the bottom submodule is free over $k\overline{G}$ and is equal to $(z-1)^{p-1}F_0$ by the lemma. The middle quotient of this filtration is the direct sum of

$$\begin{aligned}&((z-1)^{p-1}M_1 \otimes K_1')/((z-1)^{p-1}M_1 \otimes (z-1)^{p-1}M_2) \\ &\qquad \cong (z-1)^{p-1}M_1 \otimes k \cong \overline{M}_1\end{aligned}$$

and

$$\begin{aligned}&(K_1 \otimes (z-1)^{p-1}M_2)/((z-1)^{p-1}M_1 \otimes (z-1)^{p-1}M_2) \\ &\qquad \cong k \otimes (z-1)^{p-1}M_2 \cong \overline{M}_2 .\end{aligned}$$

This direct sum can be lifted in $K_1 \otimes K_1'$, because the submodule $(z-1)^{p-1}F_0 = (z-1)^{p-1}M_1 \otimes (z-1)^{p-1}M_2$ is $k\overline{G}$-free and so the sequence

$$0 \longrightarrow (z-1)^{p-1}F_0 \longrightarrow K_1 \otimes K_1' \longrightarrow (K_1 \otimes K_1')/(z-1)^{p-1}F_0 \longrightarrow 0$$

splits. Therefore $K_1 \otimes K_1'$ contains a submodule $V_1 \oplus V_2$ with $V_j \cong \overline{M}_j$ and $(V_1 \oplus V_2) \cap (z-1)^{p-1}F_0 = 0$. It follows that $(V_1 \oplus V_2) \cap \mathrm{Soc}(F_0) = 0$ and so $(V_1 \oplus V_2) \cap F_0 = 0$.

We now have $V_1 \oplus V_2 \oplus F_0 \subset K_1 \otimes M_2$ and therefore $V_1 \oplus V_2 \oplus F_0$ intersects trivially $F_1 \oplus \cdots \oplus F_{p-1}$ because this free module has been lifted from quotients of $(M_1 \otimes M_2)/(K_1 \otimes M_2)$. This shows that $M_1 \otimes M_2$ contains the submodule $V_1 \oplus V_2 \oplus F_0 \oplus F_1 \oplus \cdots \oplus F_{p-1} = V_1 \oplus V_2 \oplus F$. Therefore $V_1 \oplus V_2$ is isomorphic to a submodule of M.

Now we show that $V_1 \oplus V_2 \subset (z-1)^{p-1}(M_1 \otimes M_2)$. Since z acts trivially on K_1', we have $(z-1)^{p-1}(M_1 \otimes K_1') = (z-1)^{p-1}M_1 \otimes K_1'$ and this contains V_1 by construction of V_1. Similarly $V_2 \subset K_1 \otimes (z-1)^{p-1}M_2 = (z-1)^{p-1}(K_1 \otimes M_2)$. Passing to the quotient by F, we deduce that $V_1 \oplus V_2$ is isomorphic to a submodule of

$$(z-1)^{p-1}\big((M_1 \otimes M_2)/F\big) = (z-1)^{p-1}\big((M \oplus F)/F\big) \cong (z-1)^{p-1}M .$$

In order to prove that this submodule is the whole of $(z-1)^{p-1}M$, it suffices to prove that they have the same dimension. But $V_j \cong \overline{M}_j$ has dimension r_j (for $j = 1, 2$) and we know that $\mathrm{Dim}(M) = p(r_1 + r_2) + 1$. Therefore $\mathrm{Dim}(\overline{M}) = r_1 + r_2$ and we are done. This shows that $(z-1)^{p-1}M \cong V_1 \oplus V_2$ and completes the proof of the theorem. □

Theorem 5.6 and Theorem 5.7 provide the basic tools for constructing a large critical module from any given finite set of such modules, as follows.

THEOREM 5.9. *For every $i = 1, \dots, t$, let M_i be a nontrivial critical kG-module. Let ℓ_i be a line in the variety of the periodic $k\overline{G}$-module $\overline{M}_i$ and assume that $\ell_i \neq \ell_j$ for $i \neq j$. Then there exists a nontrivial critical kG-module M such that $V_{\overline{G}}(\overline{M}) = \bigcup_{i=1}^{t} \ell_i$. Moreover,* $\mathrm{Dim}(M) \geq t|G|/2 + 1$ *if $p = 2$ and* $\mathrm{Dim}(M) \geq t|G| + 1$ *if p is odd.*

Proof. Recall that $\overline{M}_i$ is periodic by Lemma 5.3, and hence $V_{\overline{G}}(\overline{M}_i)$ is a union of lines. By Theorem 2.2, $\overline{M}_i = L_i \oplus N_i$ such that $V_{\overline{G}}(L_i) = \ell_i$ and the variety of N_i is the union of the other lines (if any; otherwise simply set $L_i = \overline{M}_i$). By Theorem 5.6, there exists a critical kG-module U_i such that $\overline{U}_i = L_i$.

Now by Theorem 5.7 and the assumption that the lines ℓ_i are distinct, we obtain a critical kG-module M such that

$$U_1 \otimes U_2 \otimes \cdots \otimes U_t = M \oplus (\text{free})$$

and $\overline{M} = \overline{U}_1 \oplus \overline{U}_2 \oplus \cdots \oplus \overline{U}_t$ so that $V_{\overline{G}}(\overline{M}) = \bigcup_{i=1}^{t} \ell_i$.

Since $U_i{\downarrow}_H^G \cong k \oplus (\text{free})$ where H is a maximal subgroup of G, $\mathrm{Dim}(U_i) - 1$ is a multiple of $|H|$ and therefore $\mathrm{Dim}(\overline{U}_i)$ is a multiple of $|H|/p = |G|/p^2$. It follows that $\mathrm{Dim}(\overline{M}) \geq t|G|/p^2$ and $\mathrm{Dim}(M) \geq t|G|/p + 1$. We can do better if p is odd because U_i is an endo-trivial module and so $\mathrm{Dim}(U_i) \equiv \pm 1 \pmod{|G|}$ by Lemma 2.10 in [CaTh]. A plus sign is forced here and therefore $\mathrm{Dim}(U_i) - 1$ is a multiple of $|G|$. The same argument then yields $\mathrm{Dim}(M) \geq t|G| + 1$. $\square$

Remark. By a theorem of Puig [Pu], the torsion subgroup $T_t(G)$ is finite. Therefore, there are actually finitely many possible choices for the modules M_i in the last theorem. It then follows from the theorem that one can construct an indecomposable torsion endo-trivial module M such that $V_{\overline{G}}(\overline{M})$ contains $V_{\overline{G}}(\overline{N})$ for any torsion endo-trivial module N. Moreover, $\mathrm{Dim}(M) \geq t|G|/2+1$, respectively $t|G|+1$, where t is the number of components of $V_{\overline{G}}(\overline{M})$. However, in view of the main theorem of this paper, it will turn out that $T_t(G) = 0$ and so $M \cong k$.

6. Lower bounds on dimensions of critical modules

In this section we prove a theorem that is essential to the general cases of our main result. Basically it says that, if an extraspecial group or an almost extraspecial group has a nontrivial critical module, then it has one of large dimension. For the proof, we need a few lemmas.

Lemma 6.1. *Suppose that M is a nontrivial critical kG-module and let ℓ be a line in $V_{\overline{G}}(\overline{M})$. Then ℓ is not contained in any $\mathbb{F}_p$-rational subspace of $V_{\overline{G}}(k)$.*

Proof. Note that $V_{\overline{G}}(k) = k^m$ where $|G| = p^{m+1}$. An $\mathbb{F}_p$-rational subspace (i.e. a subspace defined by a linear equation with $\mathbb{F}_p$-coefficients) corresponds to a maximal subgroup $\overline{H} \subseteq \overline{G}$. That is, the $\mathbb{F}_p$-rational subspaces of $V_{\overline{G}}(k)$ are precisely the subspaces of the form $\mathrm{res}^*_{\overline{G},\overline{H}}(V_{\overline{H}}(k))$. If ℓ were in $\mathrm{res}^*_{\overline{G},\overline{H}}(V_{\overline{H}}(k))$ then it would have to be the case that $V_{\overline{H}}(\overline{M}{\downarrow}^{\overline{G}}_{\overline{H}}) \neq \{0\}$ and hence $\overline{M}{\downarrow}^{\overline{G}}_{\overline{H}}$ would not be free as a $k\overline{H}$-module. By Lemma 5.3, this would contradict the hypothesis that $M{\downarrow}^G_H \cong k \oplus (\text{free})$ where H is the inverse image of $\overline{H}$ in G. □

Recall that a p'-group is a group of order prime to p.

Lemma 6.2. *Suppose that ℓ is a line through the origin in $V_{\overline{G}}(k) = k^m$ and suppose that ℓ is not contained in any $\mathbb{F}_p$-rational subspace of k^m. Then the stabilizer S of ℓ for the action of $\mathrm{GL}_m(\mathbb{F}_p)$ on k^m is a cyclic p'-subgroup.*

Proof. Suppose that $y \in \mathrm{GL}_m(\mathbb{F}_p)$ stabilizes ℓ and that v is a point on ℓ. Then v is an eigenvector of y with eigenvalue λ. That is, simply, $y \cdot v = \lambda v$. So the line ℓ is a kS-submodule for the action of S on k^m, corresponding to a homomorphism $\rho : S \longrightarrow \mathrm{GL}(\ell) \cong k^*$ mapping $y \in S$ to the eigenvalue λ.

We claim that ρ is injective on the stabilizer S. For suppose that $\rho(y) = \lambda = 1$. Then, viewing y as a matrix, we have that $(y - I_m)v = 0$. If y is not the identity then some row $(a_1, a_2, \ldots, a_m)$ of $y - I_m$ is not zero. But then v is in the subspace defined by the equation $a_1x_1 + a_2x_2 + \cdots + a_mx_m = 0$. Because the coefficients of y are in $\mathbb{F}_p$ we have a contradiction.

Now S is isomorphic to a finite subgroup of k^* and therefore it must consist of roots of unity. Thus it is a cyclic p'-group and we are done. □

Recall that for any automorphism α of G, the conjugate module N^α is defined to be the k-vector space N with the action of G given by $g \cdot n = \alpha(g)n$ for $g \in G$ and $n \in N$. If α is an inner automorphism of G, then $N^\alpha \cong N$ and it follows that the group $\mathrm{Out}(G)$ of outer automorphisms of G acts on the set of isomorphism classes of kG-modules. We shall also write N^y for a conjugate module defined by an outer automorphism $y \in \mathrm{Out}(G)$.

Since G is extraspecial or almost extraspecial, we control $\mathrm{Out}(G)$ in the following sense. Recall that if $p = 2$, there is an associated quadratic form on the $\mathbb{F}_2$-vector space $G/Z(G)$ (see Lemma 3.1). If p is odd, there is a symplectic form b on the $\mathbb{F}_p$-vector space $G/Z(G)$ defined by $[\tilde{x}, \tilde{y}] = z^{b(x,y)}$, where $x, y \in G/Z(G)$, $\tilde{x}, \tilde{y} \in G$ are elements of G that lift x and y, and z is a generator of $Z(G)$.

LEMMA 6.3. *Let G be an extraspecial or almost extraspecial p-group. Let $\mathrm{Out}_0(G)$ be the subgroup of $\mathrm{Out}(G)$ consisting of outer automorphisms fixing the center $Z(G)$ pointwise.*

(a) *If p is odd and G is extraspecial of exponent p, then $\mathrm{Out}_0(G)$ is isomorphic to the symplectic group O_G associated to the symplectic form corresponding to G.*

(b) *If $p = 2$, $\mathrm{Out}_0(G)$ is isomorphic to the orthogonal group O_G associated to the quadratic form corresponding to G.*

Proof. When G is extraspecial, this is one of the main results in Winter's paper [Wi]. If G is almost extraspecial, the arguments given in Sections 3F and 4 of [Wi] extend and yield the same result. Alternatively, this appears explicitly in Exercise 5 of Chapter 8 of [As]. $\square$

THEOREM 6.4. *Suppose that there exists a nontrivial critical kG-module N.*

(a) *If p is odd, there exists a critical kG-module M such that*

$$\mathrm{Dim}(M) > |G| \cdot \frac{|O_G|}{|C|}$$

where O_G is the symplectic group associated to G and C is a cyclic p'-subgroup of O_G of maximal order.

(b) *If $p = 2$, there exists a critical kG-module M such that*

$$\mathrm{Dim}(M) > \frac{|G|}{2} \cdot \frac{|O_G|}{|C|}$$

where O_G is the orthogonal group associated to G and C is an odd order cyclic subgroup of O_G of maximal order.

Proof. Let ℓ be a line in $V_{\overline{G}}(\overline{N})$. Notice that if $y \in O_G$ then N^y is also a nontrivial kG-module such that $N^y{\downarrow}_H^G \cong k \oplus (\text{free})$. But then $y(\ell)$ is in the variety $V_{\overline{G}}(\overline{N^y})$. If B denotes the stabilizer of ℓ in O_G, we obtain a family of modules N^y indexed by the set of cosets O_G/B. So by Theorem 5.9, there exists a critical kG-module M such that $V_{\overline{G}}(\overline{M}) = \bigcup_{y \in O_G/B} y(\ell)$. Moreover, $\mathrm{Dim}\, M > \dfrac{|O_G|}{|B|} \cdot \dfrac{|G|}{2}$ if $p = 2$ and $\mathrm{Dim}\, M > \dfrac{|O_G|}{|B|} \cdot |G|$ if p is odd.

By Lemma 6.1, the line ℓ is not contained in any $\mathbb{F}_p$-rational subspace of $V_{\overline{G}}(k) = k^m$. Thus by Lemma 6.2, the group $B = S \cap O_G$ is cyclic of order prime to p. If C is of maximal order among cyclic p'-subgroups of O_G, we deduce the lower bound of the statement. $\square$

For use in the following sections, we need to have some estimates of the orders of the orthogonal and symplectic groups and their cyclic p'-subgroups.

PROPOSITION 6.5. *Let G be an extraspecial or almost extraspecial p-group. Let O_G be the orthogonal or symplectic group associated to G.*

1. *If p is odd and G is extraspecial of exponent p and order p^{2n+1}, then $O_G = \mathrm{Sp}(2n, \mathbb{F}_p)$ and*
$$|O_G| = p^{n^2} \prod_{i=1}^{n} (p^{2i} - 1)\,.$$
2. *If $p = 2$ and $G \cong D_8 * \cdots * D_8$ is extraspecial of order 2^{2n+1} (type 1), then $O_G = O^+(2n, \mathbb{F}_2)$ and*
$$|O_G| = 2 \cdot 2^{n(n-1)}(2^n - 1) \prod_{i=1}^{n-1} (2^{2i} - 1)\,.$$
3. *If $p = 2$ and $G \cong D_8 * \cdots * D_8 * Q_8$ is extraspecial of order 2^{2n+1} (type 2), then $O_G = O^-(2n, \mathbb{F}_2)$ and*
$$|O_G| = 2 \cdot 2^{n(n-1)}(2^n + 1) \prod_{i=1}^{n-1} (2^{2i} - 1)\,.$$
4. *If $p = 2$ and $G \cong D_8 * \cdots * D_8 * C_4$ is almost extraspecial of order 2^{2n+2} (type 3), then $O_G = \mathrm{Sp}(2n, \mathbb{F}_2)$ and*
$$|O_G| = 2^{n^2} \prod_{i=1}^{n} (2^{2i} - 1)\,.$$

Moreover, if C is any cyclic p'-subgroup of O_G, then $|C| \leq (p+1)^n$.

Proof. In the first three cases, we have $O_G = \mathrm{Sp}(2n, \mathbb{F}_p)$, respectively $O_G = O^{\pm}(2n, \mathbb{F}_2)$, essentially by definition (see also [Wi]). In the third case, we obtain $O_G = O(2n+1, \mathbb{F}_2) \cong \mathrm{Sp}(2n, \mathbb{F}_2)$ (see Theorem 11.9 of Taylor's book [Ta]) where orders of the four groups appear on pages 70 and 141. The list can also be found in any of a number of text books on Chevalley groups or finite simple groups (e.g. Gorenstein's book [Go2]). The types of the groups of Lie type in the four cases listed are $C_n(p)$, $D_n(2)$, ${}^2D_n(2)$ and $C_n(2)$, respectively. In the first case the corresponding simple group is $O_G/\{\pm 1\}$. In the next two cases the corresponding simple group has index 2 in O_G, while the group is simple in the fourth case.

For the statement about the cyclic p'-subgroups, note first that elements of order prime to p are semi-simple, hence contained in a maximal torus. Now, for a Chevalley group of rank n over the field $\mathbb{F}_q$, the order of a maximal torus is equal to
$$|\det(w^{-1}F - 1)| \;=\; |\det(F - w)|$$

where $F(x) = x^q$ is the Frobenius morphism, w is an element of the corresponding Weyl group, and where F and w act on the cocharacter group of a fixed maximal torus of the corresponding algebraic group (see Proposition 3.3.5 in Carter's book [Cart]). Since w has finite order, we obtain a product $\prod_{i=1}^{n}(q-\zeta_i)$ for suitable roots of unity ζ_i (the eigenvalues of w). In our case, $q = p$ and the rank n is the same as the integer n of the statement. Therefore if C is any cyclic p'-subgroup of O_G, we get

$$|C| \leq |\det(F - w)| = \Big|\prod_{i=1}^{n}(p - \zeta_i)\Big| \leq \prod_{i=1}^{n}(p+1) = (p+1)^n ,$$

as was to be shown. □

7. Upper bounds on dimensions of critical modules

Throughout the section we assume that G is a p-group and that k is an algebraically closed field of characteristic p.

We will need the following results. Recall that a nonzero element ζ of $\mathrm{H}^1(G, \mathbb{F}_p)$ corresponds to a maximal subgroup of G in the sense that there is a unique maximal subgroup H of G such that $\mathrm{res}_{G,H}(\zeta) = 0$. When p is odd, we also need the Bockstein map $\beta : \mathrm{H}^1(G, \mathbb{F}_p) \longrightarrow \mathrm{H}^2(G, \mathbb{F}_p)$ (see [Be] or [Ev]).

THEOREM 7.1. *Suppose that G is a p-group which is not elementary abelian. Suppose that $\eta_1, \dots, \eta_t$ are nonzero elements in $\mathrm{H}^1(G, \mathbb{F}_p)$ and have the property that*

$$\begin{aligned} \eta_1 \dots \eta_t = 0 \qquad & \textit{if } p = 2, \\ \beta(\eta_1) \dots \beta(\eta_t) = 0 \qquad & \textit{if } p \textit{ is odd.} \end{aligned}$$

(a) *Assume that $p = 2$. For each i, let H_i be the maximal subgroup of G corresponding to η_i. Then there is a projective module P such that $k \oplus \Omega^{1-t}(k) \oplus P$ has a filtration*

$$\{0\} = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_t \cong k \oplus \Omega^{1-t}(k) \oplus P$$

where $L_i/L_{i-1} \cong (\Omega^{1-i}(k))\uparrow_{H_i}^{G}$ for each $i = 1, \dots, t$.

(b) *Assume that p is odd. For each i, let K_i be the maximal subgroup of G corresponding to η_i and set $H_{2i} = H_{2i-1} = K_i$. Then there is a projective module P such that $k \oplus \Omega^{1-2t}(k) \oplus P$ has a filtration*

$$\{0\} = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_{2t} \cong k \oplus \Omega^{1-2t}(k) \oplus P$$

where $L_i/L_{i-1} \cong (\Omega^{1-i}(k))\uparrow_{H_i}^{G}$ for each $i = 1, \dots, 2t$.

Proof. This is the essence of Lemma 3.10 of [Ca2]. That lemma is stated for $\mathbb{Z}G$-modules but this does not really matter since we can tensor the whole thing with k. Because the emphasis of our theorem is different from that of the results of [Ca2] we give a brief sketch of the proof here. However, all of the ideas as well as the details are given in the paper [Ca2].

(a) We first give the proof when $p = 2$ and then indicate how to modify the arguments for odd p. Each of the cohomology elements η_i corresponds to an exact sequence

$$0 \longrightarrow \mathbb{F}_2 \longrightarrow \mathbb{F}_2{\uparrow}_{H_i}^G \longrightarrow \mathbb{F}_2 \longrightarrow 0\,.$$

Now we splice all of these together and tensor with k to get a sequence of the form

$$0 \longrightarrow k \longrightarrow k{\uparrow}_{H_t}^G \longrightarrow \ldots \longrightarrow k{\uparrow}_{H_2}^G \longrightarrow k{\uparrow}_{H_1}^G \longrightarrow k \longrightarrow 0\,,$$

which represents the element $\eta_1 \ldots \eta_t = 0$ in $\mathrm{H}^t(G,k)$. Note that we are using the same notation η_i for the element of $\mathrm{H}^1(G,\mathbb{F}_2)$ and its image under the change of rings in $\mathrm{H}^1(G,k)$. Now we consider the complex $\mathcal{C}$ obtained by truncating the ends off of the sequence. That is, $\mathcal{C}_i = k{\uparrow}_{H_{i+1}}^G$ for $i = 0,\ldots,t-1$ and $\mathcal{C}_i = 0$ otherwise. We see that the homology of $\mathcal{C}$ is a result of the truncations. That is, $\mathrm{H}_i(\mathcal{C}) = k$ if either $i = 0$ or $i = t-1$ and $\mathrm{H}_i(\mathcal{C}) = 0$ otherwise.

The next step is to collapse the complex $\mathcal{C}$ into a single module. This is accomplished exactly as in the paragraphs preceding Proposition 3.7 of [Ca2]. That is, we tensor, over k, the complex $\mathcal{C}$ with a projective resolution of the trivial module k. This gives us a projective resolution of the complex $\mathcal{C}$ and it has the same homology as $\mathcal{C}$. Thus, in degrees above t, it is exact and is the projective resolution of a module U, which we can take to be the image of the t^{th} boundary map of the total complex. The only problem with U is that it is in the wrong degree. So we take $W = \Omega^{-t}(U)$. This is the module that we want.

There are now two things to note about W. First because the terms of the complex $\mathcal{C}$ are induced from the maximal subgroup $H_1,\ldots,H_t$, the module W has a filtration by the modules $k{\uparrow}_{H_i}^G$ suitably translated by Ω, exactly as described in the statement of the theorem. That is, the projective resolution of the complex $\mathcal{C}$ as constructed above is filtered by the projective resolutions of the terms of the complex, suitably translated. See the proof of Proposition 3.8 of [Ca2] for this part.

Next we note that the module W is isomorphic to $k \oplus \Omega^{1-t}(k) \oplus P$ for some projective module P. This is because the original sequence that represented $\eta_1 \ldots \eta_t$ splits and hence the projective resolution of the complex is, in high degrees, a projective resolution of the homology groups of the complex, suitably translated. See Proposition 3.8 of [Ca2] for this part. This proves the theorem if $p = 2$.

(b) If p is odd, the cohomology element η_i has to be replaced by its Bockstein $\beta(\eta_i)$ which corresponds to an exact sequence

$$0 \longrightarrow \mathbb{F}_p \longrightarrow \mathbb{F}_p{\uparrow}_{K_i}^G \longrightarrow \mathbb{F}_p{\uparrow}_{K_i}^G \longrightarrow \mathbb{F}_p \longrightarrow 0\,.$$

Again we splice all of these together and tensor with k. Using our numbering of the subgroups H_i, we obtain a sequence of the form

$$0 \longrightarrow k \longrightarrow k{\uparrow}_{H_{2t}}^G \longrightarrow \ldots \longrightarrow k{\uparrow}_{H_2}^G \longrightarrow k{\uparrow}_{H_1}^G \longrightarrow k \longrightarrow 0\,,$$

which represents the element $\beta(\eta_1)\ldots\beta(\eta_t) = 0$ in $\mathrm{H}^{2t}(G,k)$. The complex $\mathcal{C}$ is obtained by truncating the ends off of the sequence and the rest of the argument is the same, except that the integer t has to be replaced by $2t$ throughout. □

The upper bounds wanted for the dimensions of our critical modules is contained in the following.

Theorem 7.2. *Suppose that G is a p-group which is not elementary abelian. Suppose that $\eta_1,\ldots,\eta_t \in \mathrm{H}^1(G,\mathbb{F}_p)$ are nonzero and have the property that*

$$\begin{aligned} \eta_1\ldots\eta_t &= 0 \qquad \textit{if } p=2,\\ \beta(\eta_1)\ldots\beta(\eta_t) &= 0 \qquad \textit{if } p \textit{ is odd.}\end{aligned}$$

Let $r = t$ if $p = 2$ and $r = 2t$ if p is odd. Let $H_1,\ldots,H_r$ be the maximal subgroups of G as in the previous theorem. Suppose that M is an indecomposable kG-module with the property that $M{\downarrow}_{H_i}^G \cong k \oplus (\text{free})$ for every i. Then for any s,

$$\mathrm{Dim}\ \Omega^s(M) + \mathrm{Dim}\ \Omega^{s-r+1}(M) \leq \sum_{i=1}^{r} \mathrm{Dim}\ (\Omega^{s+1-i}(k){\uparrow}_{H_i}^G)\,.$$

Proof. Let P be a projective module such that $W = k \oplus \Omega^{1-r}(k) \oplus P$ has a filtration as in the last theorem. Then tensoring W and all of the factors in the filtration with $\Omega^s(M)$ we get that

$$\begin{aligned}\{0\} = L_0 \otimes \Omega^s(M) &\subseteq L_1 \otimes \Omega^s(M) \subseteq \cdots \subseteq L_r \otimes \Omega^s(M)\\ &\cong W \otimes \Omega^s(M) \cong \Omega^s(M) \oplus \Omega^{s+1-r}(M) \oplus (\text{free}).\end{aligned}$$

Then we have

$$\begin{aligned}(L_i \otimes \Omega^s(M))/(L_{i-1} \otimes \Omega^s(M)) &\cong (L_i/(L_{i-1}) \otimes \Omega^s(M)\\ &\cong \Omega^{1-i}(k){\uparrow}_{H_i}^G \otimes \Omega^s(M)\\ &\cong \Omega^{1-i}(\Omega^s(M{\downarrow}_{H_i}^G)){\uparrow}_{H_i}^G \oplus Q\\ &\cong \Omega^{s+1-i}(k){\uparrow}_{H_i}^G \oplus Q'\end{aligned}$$

for some projective modules Q and Q'. Now the important thing to remember is that kG is a self injective algebra and hence projective modules are also injective. As a result, if a projective module is a direct summand of a section of a module V, then it is a direct summand of V. The consequence of this is that (after stripping away the unnecessary projective modules Q') we can get that, for some projective module R, the module $\Omega^s(M) \oplus \Omega^{s+1-r}(M) \oplus R$ has a filtration

$$\{0\} = X_0 \subseteq X_1 \subseteq \cdots \subseteq X_r \cong \Omega^s(M) \oplus \Omega^{s+1-r}(M) \oplus R$$

where $X_i/X_{i-1} \cong \Omega^{s+1-i}(k){\uparrow}_{H_i}^G$. The statement about dimensions follows immediately. □

8. Special cases of 2-groups of small order

In this section we consider some special cases of 2-groups that we need to treat separately, for they are not covered by the general argument of Section 10. For each of the groups we show Theorem 1.4 directly. We discuss the groups of order 8, the almost extraspecial group $D_8 * C_4$ of order 16 and the extraspecial group $D_8 * D_8$ of order 32 (type 1).

Let us start with the groups of order 8. First Q_8 is excluded by assumption (and there is actually a nontrivial critical kQ_8-module of dimension 5; see [CaTh]). For $G = D_8$ the structure of $T(D_8)$ is known (see [CaTh]) and every nontrivial endo-trivial kD_8-module is nontrivial on restriction to one of the two elementary abelian 2-subgroups of D_8. Thus the only critical module is the trivial one. Alternatively, we can also prove the result in the following way.

Proposition 8.1. *Let $G = D_8$. Then there exists no nontrivial critical kG-module.*

Proof. Let M be a critical kG-module. By Theorem 3.4, the number of cohomology classes whose product vanishes is equal to $t_G = 2$. Applying Theorem 7.2 with $s = 1$, we get

$$\mathrm{Dim}\ \Omega^1(M) + \mathrm{Dim}\ M \leq \mathrm{Dim}\ \Omega^1(k_{H_1}){\uparrow}_{H_1}^G + \mathrm{Dim}\, k{\uparrow}_{H_2}^G$$

for some maximal subgroups H_1 and H_2. Since H_i has order 4, $\Omega^1(k_{H_i})$ has dimension 3 and we obtain

$$\mathrm{Dim}\ \Omega^1(M) + \mathrm{Dim}\ M \leq 6 + 2 = 8\,.$$

By Lemma 5.4, $\mathrm{Dim}\ \Omega^1(M) = \mathrm{Dim}\ M - 2$. So $\mathrm{Dim}\ M \leq 5$. This part of the argument is essentially the same as the one appearing in Theorem 5.3 of [CaTh].

If we assume now that there exists a nontrivial critical kG-module, then by Theorem 6.4, there exists a nontrivial critical kG-module M of dimension

$$\operatorname{Dim} M > \frac{|G|}{2} \cdot \frac{|O_G|}{|C|} = 4 \cdot 2 = 8\,,$$

since $|O_G| = 2$ by Proposition 6.5. This contradicts the previous upper bound. □

We turn now to the group $G = D_8 * D_8$ of order 32.

PROPOSITION 8.2. *Let $G = D_8 * D_8$. Then there exists no nontrivial critical kG-module.*

Proof. Let M be a critical kG-module. By Theorem 3.4, the number of cohomology classes whose product vanishes is equal to $t_G = 3$. Applying now Theorem 7.2 with $s = 1$, we get

$$\operatorname{Dim}\ \Omega^1(M) + \operatorname{Dim}\ \Omega^{-1}(M) \le \operatorname{Dim}\ \Omega^1(k){\uparrow}_{H_1}^G + \operatorname{Dim} k{\uparrow}_{H_2}^G + \operatorname{Dim}\ \Omega^{-1}(k){\uparrow}_{H_3}^G$$

for some maximal subgroups H_1, H_2, and H_3. Since H_i has order 16, $\Omega^{\pm 1}(k_{H_i})$ has dimension 15 and we obtain

$$\operatorname{Dim}\ \Omega^1(M) + \operatorname{Dim}\ \Omega^{-1}(M) \le 30 + 2 + 30 = 62\,,$$

so that $\operatorname{Dim}\ \Omega^1(M) \le 62$.

If we assume now that there exists a nontrivial critical kG-module, then by Theorem 6.4, there exists a nontrivial critical kG-module M of dimension

$$\operatorname{Dim} M > \frac{|G|}{2} \cdot \frac{|O_G|}{|C|} \ge 16 \cdot \frac{72}{9} = 128\,,$$

by Proposition 6.5. So $\operatorname{Dim}\ \Omega^1(M) > 126$ by Lemma 5.4, a contradiction. □

In the last case, G is the almost extraspecial group $D_8 * C_4$ of order 16. The method of the previous cases does not work because the orthogonal group O_G is too small. Instead of using the action of O_G, we shall give an argument using the action of a Galois group.

LEMMA 8.3. *Let $G = D_8 * C_4$. If M is a critical kG-module, then* $\operatorname{Dim}\ M \le 17$.

Proof. By Theorem 3.4, the number of cohomology classes whose product vanishes is equal to $t_G = 3$. Applying now Theorem 7.2 with $s = 1$, we get

$$\operatorname{Dim}\ \Omega^1(M) + \operatorname{Dim}\ \Omega^{-1}(M) \le \operatorname{Dim}\ \Omega^1(k){\uparrow}_{H_1}^G + \operatorname{Dim} k{\uparrow}_{H_2}^G + \operatorname{Dim}\ \Omega^{-1}(k){\uparrow}_{H_3}^G$$

for some maximal subgroups H_1, H_2, and H_3. Since H_i has order 8, $\Omega^{\pm 1}(k)$ has dimension 7 and we obtain

$$\operatorname{Dim}\ \Omega^1(M) + \operatorname{Dim}\ \Omega^{-1}(M) \le 14 + 2 + 14 = 30\,.$$

By Lemma 5.4, $\mathrm{Dim}\ \Omega^1(M) = \mathrm{Dim}\ \Omega^{-1}(M) = \mathrm{Dim}\ M - 2$. So $\mathrm{Dim}\ \Omega^1(M) \leq 15$ and $\mathrm{Dim}\ M \leq 17$. □

PROPOSITION 8.4. *Let $G = D_8 * C_4$. Then there exists no nontrivial critical kG-module.*

Proof. Suppose that there is such a module N. We need to look at $V_{\overline{G}}(\overline{N}) \subseteq V_{\overline{G}}(k) \cong k^3$. Suppose that $p = (\alpha, \beta, \gamma)$ is a point in $V_{\overline{G}}(\overline{N})$. By dividing by α we may assume that $\alpha = 1$, so that $p = (1, \beta, \gamma) \in V_{\overline{G}}(\overline{N})$. Notice that $p \notin \mathrm{res}^*_{G,H}(V_{\overline{H}}(\overline{N}_H))$ for any maximal subgroup H since $\overline{N}_H$ is a free $k\overline{H}$-module. Therefore p is not in any $\mathbb{F}_2$-rational subspace of k^3, and hence β and γ cannot both be in the field with four elements (otherwise $1, \beta, \gamma$ would be linearly dependent over $\mathbb{F}_2$). It follows that if $F : k^3 \longrightarrow k^3$ is the Frobenius map, $F(a, b, c) = (a^2, b^2, c^2)$, then p, $F(p)$ and $F^2(p)$ lie on different lines in $V_G(k)$.

Next we need to notice that using the Frobenius homomorphism we can create a new module from N, by letting it act on the coefficients of the action of the elements of G on N. That is, if the module N is defined by a representation $G \longrightarrow \mathrm{GL}(N)$, and if we consider the homomorphism $F : \mathrm{GL}(N) \longrightarrow \mathrm{GL}(N)$ that takes a matrix (a_{ij}) to (a_{ij}^2), we let N^F be the module defined by the composition. It is not difficult to see that N^F is also critical. Moreover, $F(p)$ is a point in $V_{\overline{G}}(\overline{N^F})$. It follows that the lines through p, $F(p)$, and $F^2(p)$ are all lines in the variety of the quotient module $\overline{L}$ for some nontrivial critical module L. Thus by Theorem 5.9, kG has a nontrivial critical module of dimension at least 25. This contradicts Lemma 8.3. □

9. The groups of order p^3 for odd p

When the prime p is odd, there is one special case in the proof of Theorem 1.4 that must be handled with extra care. This involves the groups of order p^3. The problem is that the general estimates of the dimensions of critical modules used later are not sufficient to handle this case. The result that we want is the following.

PROPOSITION 9.1. *Let $G = G_1$, an extraspecial group of order p^3 and exponent p, for p an odd prime. Then there exists no nontrivial critical kG-module.*

The proof proceeds in several steps. Throughout assume that a nontrivial critical kG-module exists and use Theorem 6.4 to obtain one of large dimension, as follows.

LEMMA 9.2. *If a nontrivial critical kG-module exists, then there exists a critical kG-module M whose dimension is at least equal to $(p-1)p^4+1$. Moreover* $\operatorname{Dim}\Omega(M) \geq (p-1)p^4 - 1$ *and* $\operatorname{Dim}\Omega^{-1}(M) \geq (p-1)p^4-1$.

Proof. By Theorem 6.4 there exists a critical module M whose dimension is at least $|G|\ |\mathrm{Sp}(2,\mathbb{F}_p)|/|C|$ where C is a cyclic p'-subgroup of the symplectic group $\mathrm{Sp}(2,\mathbb{F}_p)$ of maximal order. Now $\mathrm{Sp}(2,\mathbb{F}_p) = \mathrm{SL}(2,\mathbb{F}_p)$ has order $p(p^2-1)$ and its cyclic p'-subgroup of maximal order has order $p+1$. So the dimension of M must be greater than $(p-1)p^4$ and must be congruent to 1 modulo p.

Now to compute the dimension of $\Omega(M)$, we notice from the proof of Theorem 6.4 that the variety of the module $\overline{M}$ is the union of at least $p(p-1)$ distinct lines in $V_{\overline{G}}(k) = k^2$. So $\overline{M} = \overline{U}_1 \oplus \cdots \oplus \overline{U}_t$ where, for each i, $V_{\overline{G}}(\overline{U}_i)$ is a single line and $t > p(p-1)$. Now, as in the proof of Theorem 5.9, $\operatorname{Dim}\overline{U}_i = r_i p^2$ for some r_i (we use here the fact that U_i is endo-trivial and p is odd). Because $\overline{U}_i$ is not a free $k\overline{G}$-module (and, in fact, has no free submodules) and because a projective cover of $\overline{U}_i$ has dimension $p^2 \operatorname{Dim}\overline{U}_i/\mathrm{Rad}(\overline{U}_i)$, we must have $\operatorname{Dim}\overline{U}_i/\mathrm{Rad}(\overline{U}_i) > r_i$. Therefore $\overline{U}_i$ is minimally generated by at least r_i+1 generators and the number of generators of $\overline{M}$ is at least

$$m = \sum_{i=1}^{t}(r_i+1) = \left(\sum_{i=1}^{t} r_i\right) + t\,.$$

Now $\overline{M}/\mathrm{Rad}(\overline{M})$ is a quotient of $M/\mathrm{Rad}(M)$, so the minimal number of generators of M is at least m. As a result, the number of copies of kG appearing in the projective cover of M must be at least m. Now the dimension of M is $p^3(\sum_{i=1}^t r_i)+1$ and so the dimension of $\Omega(M)$ is at least

$$p^3 m - \operatorname{Dim}(M) = p^3\left(\left(\sum_{i=1}^{t} r_i\right)+t\right) - p^3\left(\sum_{i=1}^{t} r_i\right) - 1 = tp^3 - 1 \geq (p-1)p^4 - 1\,.$$

By applying the same argument to the dual module M^* (which also satisfies the properties we need), we obtain

$$\operatorname{Dim}\Omega^{-1}(M) = \operatorname{Dim}\Omega^{-1}(M)^* = \operatorname{Dim}\Omega(M^*) \geq (p-1)p^4 - 1\,.$$

This proves the lemma. □

LEMMA 9.3.

$$\operatorname{Dim}\Omega^{2p}(M) + \operatorname{Dim}\Omega^{-1}(M) \leq p^3(p^2+p+1).$$

Proof. From any one of the papers [Le1], [Ya], [BeCa] we have that there exist $\eta_1, \ldots \eta_{p+1} \in \mathrm{H}^1(G,k)$ such that $\beta(\eta_1)\ldots\beta(\eta_{p+1}) = 0$. In Leary [Le1] the relation is given as $x^p x' - x x'^p = 0$. Now applying Theorem 7.2 with $t = p+1$

(hence $r = 2t = 2(p+1)$) and choosing $s = 2p$ in that theorem, we get

$$\operatorname{Dim}\Omega^{2p}(M) + \operatorname{Dim}\Omega^{-1}(M) \leq \sum_{i=1}^{2p+2} \operatorname{Dim}(\Omega^{2p+1-i}(k)\uparrow_{H_i}^{G}),$$

where H_i is a maximal subgroup of G corresponding to the appropriate η_j. In our case, every H_i is an elementary abelian group of order p^2, and hence the dimensions on the right-hand side of the inequality are independent of the particular η_j. Because $\operatorname{Dim}\mathrm{H}^j(H_i,k) = j+1$ (see Lemma 4.6), we have that (for $H_i = H$)

$$\operatorname{Dim}\Omega^{2j-1}(k_H) + \operatorname{Dim}\Omega^{2j}(k_H) = p^2 \operatorname{Dim}\mathrm{H}^{2j-1}(H,k) = p^2(2j).$$

Induction to G multiplies the dimensions by p. Consequently the right-hand side of the above inequality has the form

$$\begin{aligned}
&\sum_{i=1}^{2p+2} \operatorname{Dim}(\Omega^{2p+1-i}(k)\uparrow_{H_i}^{G}) \\
&\qquad = p\operatorname{Dim}\Omega^{-1}(k_H) + p\operatorname{Dim}k + p\sum_{j=1}^{p}\big(\operatorname{Dim}\Omega^{2j-1}(k_H) + \operatorname{Dim}\Omega^{2j}(k_H)\big) \\
&\qquad = p\big(p^2 - 1 + 1 + \sum_{j=1}^{p} 2p^2 j\,\big) \\
&\qquad = p^3 + 2p^3(p)(p+1)/2 = p^3(1+p^2+p)
\end{aligned}$$

as desired. □

At this point we should notice that the two lemmas above are not sufficient to give us the contradiction wanted. We need some further analysis of the dimension of $\Omega^{2p}(M)$. For this purpose we recall that there exists an element $\zeta \in \mathrm{H}^{2p}(G,k)$ which has the property that its restriction $\operatorname{res}_{G,Z}(\zeta)$ is not zero where $Z = \langle z\rangle$ is the center of G. In Leary's paper [Le1], the element that he calls z will do. The element ζ can also be obtained by applying the Evens norm map to an element in the degree 2 cohomology of a maximal elementary abelian subgroup whose restriction to Z is not trivial.

The element ζ can be represented by a unique cocycle $\zeta : \Omega^{2p}(k) \longrightarrow k$. Hence we have an exact sequence

$$0 \longrightarrow L \longrightarrow \Omega^{2p}(k) \xrightarrow{\ \zeta\ } k \longrightarrow 0$$

where L is the kernel of ζ. Now by Theorem 2.2, $V_G(L) = V_G(\zeta)$, the variety of the ideal generated by ζ. In particular, the restriction $L\downarrow_Z^G$ is free as a kZ-module. This fact can also be derived from the observation that the above sequence is split as a sequence of kZ-modules because the restriction of ζ to Z is not zero and $\Omega^{2p}(k)\downarrow_Z^G \cong k \oplus (\text{free})$.

Let $\overline{L} = L/(z-1)L \cong (z-1)^{p-1}L$. Then $\overline{L}$ is a $k\overline{G}$-module where $\overline{G} = G/Z$.

LEMMA 9.4. *The $k\overline{G}$-module $\overline{L}$ has no projective submodules, and moreover,*

$$V_{\overline{G}}(\overline{L}) \subseteq \bigcup res^*_{\overline{G},\overline{E}} V_{\overline{E}}(k)$$

where the union is over the set of all subgroups $\overline{E} = E/Z$ where E is a maximal subgroup of G.

Notice that every maximal subgroup of G is elementary abelian and the union in the lemma is over all subgroups of order p in $\overline{G}$. Thus the right-hand side of the containment is the union of all of the $\mathbb{F}_p$-rational lines in $V_{\overline{G}}(k) \cong k^2$. It can be proved that the two sides are actually equal, but we do not need to know this.

Proof. If $\overline{L}$ had a $k\overline{G}$-projective submodule then L and hence also $\Omega^{2p}(k)$ would have projective kG-submodules. That is, if $t_1^{\overline{G}}\overline{L} \neq 0$ then also $t_1^G L \neq 0$. But clearly this is impossible.

Now suppose that $\ell \subseteq V_{\overline{G}}(k)$ is a line that is not $\mathbb{F}_p$-rational. Let N be a $k\overline{G}$-module such that $V_{\overline{G}}(N) = \ell$ (e.g. take $N = k\overline{G}/(\sigma - 1)$ where $\langle\sigma\rangle$ is a cyclic shifted subgroup corresponding to the line ℓ). Then the restriction $N{\downarrow}^{\overline{G}}_{\overline{E}}$ is a free $k\overline{E}$-module for any maximal subgroup E of G. So, viewing N as a kG-module by inflation, we have that $V_E(N{\downarrow}^G_E)$ is the line determined by the center Z, because Z acts trivially on $N{\downarrow}^G_E$. Therefore N is periodic as a kG-module and we must have that $V_G(N) = \mathrm{res}^*_{G,Z}(V_Z(k))$, the line determined by the center Z. Because L is free on restriction to Z we know that $V_G(L) \cap V_G(N) = \{0\}$ and hence $L \otimes N$ is a free kG-module. Now Z acts trivially on N and hence $(z-1)(L \otimes N) = ((z-1)L) \otimes N$. Thus, $\overline{L \otimes N} \cong \overline{L} \otimes N$ is a free $k\overline{G}$-module. It follows from Theorem 2.2 that $V_{\overline{G}}(\overline{L}) \cap V_{\overline{G}}(N) = \{0\}$. Hence the line ℓ is not in $V_{\overline{G}}(\overline{L})$ and this holds for all lines in $V_{\overline{G}}(k)$ which are not $\mathbb{F}_p$-rational. Thus the variety $V_{\overline{G}}(\overline{L})$ must be contained in the union of the $\mathbb{F}_p$-rational lines. □

LEMMA 9.5. *If M is a critical kG-module, $V_{\overline{G}}(\overline{M}) \cap V_{\overline{G}}(\overline{L}) = \{0\}$ and $M \otimes L \cong L \oplus$ (free).*

Proof. We first show that $\overline{M} \otimes L$ is a free kG-module. That is, L is free as a kZ-module and $\overline{\overline{M} \otimes L} \cong \overline{M} \otimes \overline{L}$. But from Lemmas 9.4 and 6.1 we have that $V_{\overline{G}}(\overline{M}) \cap V_{\overline{G}}(\overline{L}) = \{0\}$. Hence $\overline{M} \otimes \overline{L}$ is free as a $k\overline{G}$-module. Thus $\overline{M} \otimes L$ is free as a kG-module.

It follows that $M \otimes L$ has a filtration

$$0 \subseteq ((z-1)^{p-1}M) \otimes L \subseteq \cdots \subseteq ((z-1)M) \otimes L \subseteq M' \otimes L \subseteq M \otimes L$$

where $M' = \{m \in M | (z-1)^{p-1}m = 0\}$. All of the factors are isomorphic to $\overline{M} \otimes L$ and hence are projective, except for the factor

$$(M' \otimes L)/((z-1)M \otimes L) \cong (M'/(z-1)M) \otimes L \cong k \otimes L \cong L\,.$$

The lemma follows from the fact that free modules are also injective and hence any free composition factor is a direct summand. □

Now tensoring the sequence given above with M we get an exact sequence

$$0 \longrightarrow M \otimes L \longrightarrow M \otimes \Omega^{2p}(k) \xrightarrow{1\otimes\zeta} M \longrightarrow 0\,.$$

Any projective submodule of $M \otimes L$ is also a direct summand of the middle term and can be factored out. So we have an exact sequence of the form

$$0 \longrightarrow L \longrightarrow \Omega^{2p}(M) \oplus P \longrightarrow M \longrightarrow 0\,,$$

for some projective module P. It remains to prove the following.

Lemma 9.6. *In the preceding exact sequence, the projective module P is zero.*

Proof. Because the module L is free as a kZ-module the sequence is split as a sequence of kZ-modules. So multiplication by $z-1$ is an exact functor on this sequence. Hence we have a sequence

$$0 \longrightarrow (z-1)^{p-1}L \longrightarrow (z-1)^{p-1}\Omega^{2p}(M) \oplus (z-1)^{p-1}P \longrightarrow (z-1)^{p-1}M \longrightarrow 0\,;$$

that is,

$$0 \longrightarrow \overline{L} \longrightarrow \overline{\Omega^{2p}(M)} \oplus \overline{P} \longrightarrow \overline{M} \longrightarrow 0\,,$$

which is a sequence of $k\overline{G}$-modules. Because $V_{\overline{G}}(\overline{L}) \cap V_{\overline{G}}(\overline{M}) = \{0\}$ by the previous lemma, we must have that the sequence splits. Thus,

$$\overline{L} \oplus \overline{M} \cong \overline{\Omega^{2p}(M)} \oplus \overline{P}\,.$$

But $\overline{L} \oplus \overline{M}$ has no projective $k\overline{G}$-submodules by Lemma 9.4. Hence $\overline{P} = \{0\}$ and therefore also $P = \{0\}$. □

Proof of Proposition 9.1. By Lemma 9.6, $\operatorname{Dim}\Omega^{2p}(M) = \operatorname{Dim} L + \operatorname{Dim} M$. By Lemma 4.4, $\operatorname{Dim}\Omega^{2p}(k) = p^3(p+1)+1$, and so $\operatorname{Dim} L = p^3(p+1)$ by definition of L. Now by Lemma 9.2, $\operatorname{Dim} M \geq p^4(p-1)+1$ and $\operatorname{Dim}\Omega^{-1}(M) \geq p^4(p-1)-1$. Hence we have that

$$\begin{aligned}\operatorname{Dim}\Omega^{2p}(M) + \operatorname{Dim}\Omega^{-1}(M) &\geq p^3(p+1) + p^4(p-1) + 1 + p^4(p-1) - 1 \\ &= p^3(2p^2 - p + 1)\,.\end{aligned}$$

This inequality, however, is a contradiction to Lemma 9.3 since we are assuming that $p \geq 3$.

10. The general case in characteristic 2

We are now prepared to prove the general case by induction and complete the proof of the detection Theorem 1.4 when $p = 2$. Throughout, k has characteristic 2. Let G be an extraspecial or almost extraspecial group of order 2^{m+1}. The theorem that we are trying to prove is the following. It is equivalent to Theorem 1.4.

THEOREM 10.1. *If G is an extraspecial or almost extraspecial 2-group and if G is not isomorphic to Q_8, then there are no nontrivial critical kG-modules.*

Three cases have to be treated separately, namely the groups of order at most 16 as well as $D_8 * D_8$. But these cases have been dealt with in Section 8. Therefore we can now assume that $m \geq 4$ and that $m > 4$ for the groups of type 1. This allows us to use Corollary 3.6.

The strategy of the proof is expressed in the following.

PROPOSITION 10.2. *Let G be an extraspecial or almost extraspecial group of order 2^{m+1}, with $m = 2n$. Assume that $m \geq 4$ and $m > 4$ if G is of type 1. Let t_G be the number of cohomology classes whose product vanishes, as described in Theorem 3.4, and let*

$$\sigma_G = \binom{t_G + m - 4}{m - 2}|G| + 2 \qquad \text{and} \qquad \tau_G = \frac{|G|}{2} \cdot \frac{|O_G|}{3^n}.$$

If $\tau_G > \sigma_G$ then there exists no nontrivial critical kG-module.

Proof. Let $t = t_G$. In view of Theorem 3.4, there exist nonzero elements $\eta_1, \ldots, \eta_t \in \mathrm{H}^1(G, \mathbb{F}_2)$ such that $\eta_1 \ldots \eta_t = 0$ and each η_i corresponds to a maximal subgroup H_i. Moreover each subgroup H_i is the centralizer of a noncentral involution in G and by Theorem 3.5, $H_i \cong C_2 \times U$ where U has the same type as G. So $H_i \cong H_1$ for each i.

Suppose that M is a critical kG-module. Then by Theorem 7.2 with $t = t_G$ and $s = t - 1$, we have

$$\mathrm{Dim}\ M \leq \mathrm{Dim}\ \Omega^{t-1}(M) + \mathrm{Dim}\ M \leq \sum_{i=1}^{t} \mathrm{Dim}\ (\Omega^{t-i}(k)\uparrow_{H_i}^{G}).$$

Since all the subgroups H_i are isomorphic to H_1, we obtain

$$\mathrm{Dim}\ M \leq \sum_{j=0}^{t-1} \mathrm{Dim}\ (\Omega^{j}(k)\uparrow_{H_1}^{G}).$$

Now by Corollary 3.6, which applies in view of our assumption on m (with m, in the corollary, replaced by $m-2$ and $r = t_G - 1$), we obtain

$$\sum_{j=0}^{t-1} \mathrm{Dim}\ (\Omega^j(k)\uparrow_{H_1}^G) \leq |G| \cdot \binom{m-2+t_G-1-1}{m-2} + 2 = \sigma_G\,.$$

It follows that $\mathrm{Dim}\, M \leq \sigma_G$.

If there exists a nontrivial critical kG-module, then by Theorem 6.4, there exists a nontrivial critical kG-module M of dimension

$$\mathrm{Dim}\ \ M > \frac{|G|}{2} \cdot \frac{|O_G|}{|C|} \ \geq\ \frac{|G|}{2} \cdot \frac{|O_G|}{3^n} = \tau_G > \sigma_G\,.$$

This contradicts the upper-bound obtained above. □

We have now reduced the problem to the proof that $\tau_G > \sigma_G$ for all the groups G as above. This is a purely numerical problem which only requires estimating the numbers τ_G and σ_G. We start with a lemma which will be useful for estimating σ_G.

LEMMA 10.3. *Let t and m be integers with $t \geq 4$ and $m \geq 6$. Then*

$$\frac{\dbinom{2t+m-2}{m}}{\dbinom{t+m-4}{m-2}} < 2^{m-3}\, t^2\,.$$

Proof. Expanding the left-hand side and eliminating the common factor $(m-2)!$, we get the following expression. Notice that we can bound each of the first $m-5$ fractions by 2 (using $m \geq 6$), the next three by 3 (using $t \geq 4$), and bound $1/m(m-1)$ by $1/30$. Thus we get the following.

$$\frac{2t+m-2}{t+m-4} \cdot \frac{2t+m-3}{t+m-5} \cdot \ldots \cdot \frac{2t+4}{t+2} \cdot \frac{2t+3}{t+1} \cdot \frac{2t+2}{t} \cdot \frac{2t+1}{t-1} \cdot \frac{2t}{m} \cdot \frac{2t-1}{m-1}$$
$$< 2^{m-5}\, 3^3\, \frac{4t^2}{30} < 2^{m-3} t^2\,.$$

□

For the proof that $\tau_G > \sigma_G$, we proceed with cases.

10.1. *Groups of type* 1. Let $G_n = D_8 * \cdots * D_8$ be the central product of n copies of D_8, with $n \geq 3$. Remember that the cases $n = 1$ and $n = 2$ were treated in Propositions 8.1 and 8.2. For convenience, we write $G = G_n$ and let $\sigma_n = \sigma_{G_n}$ and $\tau_n = \tau_{G_n}$. We prove that $\sigma_n < \tau_n$ by induction, starting with two cases.

If $n = 3$, then $t = t_G = 5$ by Theorem 3.4 and we have that

$$\tau_3 = 2^6 \cdot \frac{2^7 \cdot 7 \cdot 3 \cdot 15}{3^3} > 2^{13} \cdot 11\,,$$

$$\sigma_3 = \binom{5+6-4}{6-2} \cdot 2^7 + 2 = 35 \cdot 2^7 + 2 < 2^{13} \cdot 11 < \tau_3 .$$

If $n = 4$, then $t = t_G = 9$ by Theorem 3.4 and

$$\tau_4 = 2^8 \cdot \frac{2^{13} \cdot 15 \cdot 3 \cdot 15 \cdot 63}{3^4} = 2^{21} \cdot 525 ,$$
$$\sigma_4 = \binom{9+8-4}{8-2} \cdot 2^9 + 2 = 1716 \cdot 2^9 + 2 < \tau_4 .$$

For $n \geq 4$, we have $t_{G_{n+1}} = 2t_{G_n}$ by Theorem 3.4, and this allows for an inductive argument. We assume that $\sigma_n < \tau_n$ and we prove that $\sigma_{n+1} < \tau_{n+1}$. The course of our proof is to show that

$$\frac{\sigma_{n+1} - 2}{\sigma_n - 2} < 2^{4n} < \frac{\tau_{n+1}}{\tau_n}$$

from which we get $\sigma_{n+1} - 2 < 2^{4n}\sigma_n - 2^{4n+1} < 2^{4n}\tau_n - 2 < \tau_{n+1} - 2$ and we are done. So we are left with the proof of the two inequalities above.

From the value of τ_n given by Proposition 6.5, we obtain

$$\frac{\tau_{n+1}}{\tau_n} = \frac{|G_{n+1}|}{|G_n|} \cdot \frac{2^{(n+1)n+1}}{2^{n(n-1)+1}} \cdot \frac{2^{n+1}-1}{2^n - 1} \cdot \frac{2^{2n}-1}{3}$$
$$> 2^2 \cdot 2^{2n} \cdot 2 \cdot \frac{2^{2n}-1}{4} = 2^{4n+1} - 2^{2n+1} > 2^{4n} .$$

On the other hand, setting $m = 2n$ and $t_{G_n} = t_n = 2^{n-1} + 2^{n-4}$ (Theorem 3.4), we obtain by Lemma 10.3

$$\frac{\sigma_{n+1} - 2}{\sigma_n - 2} = \frac{|G_{n+1}|}{|G_n|} \cdot \frac{\binom{2t_n + m - 2}{m}}{\binom{t_n + m - 4}{m-2}}$$
$$< 4 \cdot 2^{m-3} \cdot t_n^2 = 2^{2n-1}(2^{n-1} + 2^{n-4})^2 < 2^{2n-1}\, 2^{2n} < 2^{4n} .$$

10.2. *Groups of type* 2. Let $G_n = D_8 * \cdots * D_8 * Q_8$ be the central product of $n-1$ copies of D_8 and one of Q_8, with $n \geq 2$. Let $G = G_n$, $\sigma_n = \sigma_{G_n}$, $\tau_n = \tau_{G_n}$, and $t_n = t_{G_n} = 2^n + 2^{n-2}$ (see Theorem 3.4).

We start with the case $n = 2$, for which we need to replace τ_2 by the slightly larger value

$$\tau_2' = \frac{|G_2|}{2} \cdot \frac{|O_G|}{|C|}$$

where C is a cyclic subgroup of O_G of maximal odd order. By Corollary 12.43 of Taylor's book [Ta], O_G has a simple subgroup of index 2 isomorphic to $\mathrm{PSL}(2, \mathbb{F}_4)$ (that is, A_5, and in fact O_G is isomorphic to the symmetric group S_5). Therefore $|C| = 5$ and we get $\tau_2' = 384$. On the other hand $t_2 = 5$ and we have

$$\sigma_2 = \binom{5+4-4}{4-2} \cdot 2^5 + 2 = 322 < \tau_2' .$$

The argument of Proposition 10.2 goes through with τ_2' instead of τ_2.

Now we prove that $\sigma_n < \tau_n$ by induction, starting with $n = 3$:

$$\begin{aligned} \tau_3 &= 2^6 \cdot \frac{2^7 \cdot 9 \cdot 3 \cdot 15}{3^3} = 2^{13} \cdot 15 , \\ \sigma_3 &= \binom{10+6-4}{6-2} \cdot 2^7 + 2 = 495 \cdot 2^7 + 2 < \tau_3 . \end{aligned}$$

If now $n \geq 3$ the course of our proof is to show that

$$\frac{\sigma_{n+1} - 2}{\sigma_n - 2} < 2^{4n} - 2^{2n} < \frac{\tau_{n+1}}{\tau_n}$$

from which we conclude the proof as in the previous case. Here is the computation:

$$\begin{aligned} \frac{\tau_{n+1}}{\tau_n} &= \frac{|G_{n+1}|}{|G_n|} \cdot \frac{2^{(n+1)n+1}}{2^{n(n-1)+1}} \cdot \frac{2^{n+1}+1}{2^n+1} \cdot \frac{2^{2n}-1}{3} \\ &> 2^2 \cdot 2^{2n} \cdot 1 \cdot \frac{2^{2n}-1}{4} = 2^{4n} - 2^{2n} . \end{aligned}$$

On the other hand, we obtain by Lemma 10.3

$$\begin{aligned} \frac{\sigma_{n+1} - 2}{\sigma_n - 2} &= \frac{|G_{n+1}|}{|G_n|} \cdot \frac{\binom{2t_n + m - 2}{m}}{\binom{t_n + m - 4}{m-2}} \\ &< 4 \cdot 2^{m-3} \cdot t_n^2 = 2^{2n-1}(2^n + 2^{n-2})^2 \\ &= 2^{4n-1} + 2^{4n-2} + 2^{4n-5} + 2^{2n} - 2^{2n} < 2^{4n} - 2^{2n} . \end{aligned}$$

10.3. *Groups of type* 3. Let $G_n = D_8 * \cdots * D_8 * C_4$ be the central product of n copies of D_8 and one of C_4. Let $G = G_n$, $\sigma_n = \sigma_{G_n}$, $\tau_n = \tau_{G_n}$, and $t_n = t_{G_n} = 2^n + 2^{n-2}$ (see Theorem 3.4). Note that $m = 2n + 1$ for type 3.

We prove that $\sigma_n < \tau_n$ by induction, starting with $n = 2$. Remember that the case in which $n = 1$ was treated in Proposition 8.4. First we have that

$$\begin{aligned} \tau_2 &= 2^5 \cdot \frac{2^4 \cdot 3 \cdot 15}{3^2} = 2560 , \\ \sigma_2 &= \binom{5+5-4}{5-2} \cdot 2^6 + 2 = 1282 < \tau_2 . \end{aligned}$$

If now $n \geq 2$ we show that

$$\frac{\sigma_{n+1} - 2}{\sigma_n - 2} < 2^{4n+2} < \frac{\tau_{n+1}}{\tau_n}$$

from which we make our conclusions as in the previous cases. Here is the computation. First note that

$$\begin{aligned}\frac{\tau_{n+1}}{\tau_n} &= \frac{|G_{n+1}|}{|G_n|} \cdot \frac{2^{(n+1)^2}}{2^{n^2}} \cdot \frac{2^{2(n+1)}-1}{3} \\ &> 2^2 \cdot 2^{2n+1} \cdot \frac{2^{2n+1}}{4} = 2^{4n+2}.\end{aligned}$$

On the other hand, we obtain by Lemma 10.3

$$\begin{aligned}\frac{\sigma_{n+1}-2}{\sigma_n-2} &= \frac{|G_{n+1}|}{|G_n|} \cdot \frac{\binom{2t_n+m-2}{m}}{\binom{t_n+m-4}{m-2}} \\ &< 4 \cdot 2^{m-3} \cdot t_n^2 = 2^{2n}(2^n+2^{n-2})^2 < 2^{2n}\,2^{2(n+1)} = 2^{4n+2}.\end{aligned}$$

This completes the proof of Theorem 10.1 and hence also the proof of Theorem 1.4 when $p = 2$.

11. The general case in odd characteristic

In this section we complete the proof of Theorem 1.4 for odd p. We assume throughout that the field k has characteristic p and that $G = G_n$ is an extraspecial group of order p^{2n+1} and exponent p. Our aim is to prove the following.

THEOREM 11.1. *If $G = G_n$, then there are no nontrivial critical kG-modules.*

If $n = 1$, the result follows from Section 9. Thus we can assume $n \geq 2$. The proof follows the same basic pattern as in the last section. We define σ_n and τ_n such that σ_n is an upper bound for the dimension of any critical module and τ_n is a lower bound for the dimension of some nontrivial critical module if nontrivial critical modules exist. Then we prove that $\sigma_n < \tau_n$. First we give the definitions.

For $n \geq 2$ let

$$\sigma_n = 2|G_n|\binom{t_n+2n-3}{2n-1}$$

where $t_n = 2(p^2+p-1)p^{n-2}$. Let τ_n be given by the rule

$$\tau_n = \frac{|G_n|\ |\mathrm{Sp}(2n,\mathbb{F}_p)|}{c_n}$$

where $c_n = (p+1)^n$ except in the case in which $p = 3$ and $n = 2$. In that case let $c_n = p^2+1 = 10$. Then we have the following.

PROPOSITION 11.2. *If $n \geq 2$ and $\tau_n > \sigma_n$, then there exists no nontrivial critical kG_n-module.*

Proof. Let $t = t_n/2 = (p^2 + p - 1)p^{n-2}$. By Theorem 4.1, we know that there exist nonzero elements $\eta_1, \dots, \eta_t \in \mathrm{H}^1(G, \mathbb{F}_2)$ such that $\beta(\eta_1) \dots \beta(\eta_t) = 0$ and each η_i corresponds to a maximal subgroup H_i. Moreover each subgroup H_i is the centralizer of a noncentral element of order p in G and by Theorem 4.7, $H_i \cong C_p \times G_{n-1}$. So $H_i \cong H_1$ for each i.

If M is a critical kG_n-module, then by Theorem 7.2 with $r = 2t = t_n$ and $s = t_n - 1$,

$$\mathrm{Dim}\ M \leq \mathrm{Dim}\ \Omega^{t_n - 1}(M) + \mathrm{Dim}\ M \leq \sum_{i=1}^{t_n} \mathrm{Dim}\ (\Omega^{t_n - i}(k){\uparrow}_{H_i}^G)\,.$$

Since all the subgroups H_i are isomorphic to H_1, we obtain

$$\mathrm{Dim}\ M \leq \sum_{j=0}^{t_n - 1} \mathrm{Dim}\ (\Omega^j(k){\uparrow}_{H_1}^G)\,.$$

By Corollary 4.8,

$$\sum_{j=0}^{t_n - 1} \mathrm{Dim}\ (\Omega^j(k){\uparrow}_{H_1}^G) \leq 2|G| \cdot \binom{t_n - 1 + 2n - 2}{2n - 1} = \sigma_n\,.$$

It follows that $\mathrm{Dim}\, M \leq \sigma_n$.

On the other hand, if we assume that there exists a nontrivial critical kG_n-module, then by Theorem 6.4, there exists a nontrivial critical kG-module M of dimension

$$\mathrm{Dim}\ M > |G| \cdot \frac{|O_G|}{|C|}$$

where C is a cyclic p'-subgroup in $\mathrm{Sp}(2n, \mathbb{F}_p)$ of maximal order. In the case that $p = 3$ and $n = 2$, we know from character tables or from direct analysis on $\mathrm{Sp}(4, \mathbb{F}_3)$ that C has order at most 10. In all other cases we know by Proposition 6.5 that the order of C is at most $(p + 1)^n$. So in either case, $\mathrm{Dim}\, M > \tau_n$. Hence if $\sigma_n < \tau_n$ then we have a contradiction. □

So it remains to prove that $\tau_n > \sigma_n$. We will proceed by induction beginning with the following.

LEMMA 11.3. $\tau_2 > \sigma_2$.

Proof. If $p = 3$, then $\sigma_2 = 860,706$ while $\tau_2 = 1,259,712$, and so the lemma holds in that case (note that it is here that we need the special choice made for τ_2). So suppose that $p \geq 5$. Then

$$\begin{aligned}\frac{\sigma_2}{p^{11}} &= \frac{1}{p^{11}} 2p^5 \binom{2(p^2+p-1)+1}{3} \\ &= \frac{2}{3!}(2+\frac{2}{p}-\frac{1}{p^2})(2+\frac{2}{p}-\frac{2}{p^2})(2+\frac{2}{p}-\frac{3}{p^2}) < \frac{1}{3} 3\cdot 3\cdot 3 = 9\,.\end{aligned}$$

On the other hand,

$$\frac{\tau_2}{p^{11}} = \frac{p^5}{p^{11}} \frac{p^4(p^2-1)(p^4-1)}{(p+1)^2} = p^2 \frac{(1-\frac{1}{p^2})(1-\frac{1}{p^4})}{(1+\frac{1}{p})^2} > p^2 \frac{(\frac{4}{5})^2}{(\frac{4}{3})^2} = 9\frac{p^2}{25} > 9$$

by the fact that $p \geq 5$ and hence $1+1/p < 4/3$ and $1-1/p \geq 4/5$. So again $\tau_2 > \sigma_2$. □

LEMMA 11.4. *For $n \geq 2$, $\dfrac{\sigma_{n+1}}{\sigma_n} < \dfrac{\tau_{n+1}}{\tau_n}$.*

Proof. Notice first that a special computation is needed if $p = 3$ and $n = 2$. In that case, by direct calculation, we have that $\sigma_3 = 49,157,255,862$ while $\tau_3 = 313,380,128,880$. It is then easy to check the lemma in this particular case.

More generally, we calculate that

$$\begin{aligned}\frac{\tau_{n+1}}{\tau_n} &= \frac{|G_{n+1}|}{|G_n|}\frac{p^{(n+1)^2}}{p^{n^2}}\frac{(p^2-1)\dots(p^{2n+2}-1)/(p+1)^{n+1}}{(p^2-1)\dots(p^{2n}-1)/(p+1)^n} \\ &= p^2\cdot p^{2n+1}\cdot(p^{2n+2}-1)/(p+1) > \frac{1}{2}p^{4n+4}.\end{aligned}$$

The above estimate is that, since $p \geq 3$, we have $1/(p+1) > 1/(\sqrt{2}p)$ and $p^{2n+2}-1 > p^{2n+2}/\sqrt{2}$.

At the same time, setting $t = t_n$ and noting that $t_{n+1} = pt_n$, we have

$$\begin{aligned}\frac{\sigma_{n+1}}{\sigma_n} &= \frac{2p^{2n+3}}{2p^{2n+1}}\frac{\binom{tp+2n-1}{2n+1}}{\binom{t+2n-3}{2n-1}} \\ &= \frac{p^2}{(2n+1)(2n)}(tp+2n-1)(tp+2n-2)\frac{(tp+2n-3)}{(t+2n-3)}\cdots\frac{tp}{t}\frac{(tp-1)}{(t-1)}\,.\end{aligned}$$

Now we note that $(tp+b)/(t+b) \leq tp/t = p$ for all $b \geq 0$. Also $(tp-1)/(t-1) < \frac{3}{2}p$ because $t \geq 3$. Moreover,

$$\begin{aligned}tp+2n-1 &= 2(p^2+p-1)p^{n-2}p+2n-1 \\ &= 2p^{n+1}\left(1+\frac{1}{p}-\frac{1}{p^2}+\frac{2n-1}{2p^{n+1}}\right) \\ &< 2p^{n+1}(2) = 4p^{n+1}.\end{aligned}$$

So we have that

$$\frac{\sigma_{n+1}}{\sigma_n} < \frac{p^2}{(2n+1)(2n)}(4p^{n+1})(4p^{n+1})(p^{2n-2})(\frac{3}{2}p)$$
$$= \frac{16\cdot 3/2}{(2n+1)(2n)}p^{4n+3} \le \frac{24}{20}p^{4n+3} < \frac{1}{2}p^{4n+4}\,.$$

Finally $\dfrac{\sigma_{n+1}}{\sigma_n} < \dfrac{1}{2}p^{4n+4} < \dfrac{\tau_{n+1}}{\tau_n}$, as required. □

Proof of Theorem 11.1. Remember the case in which $n = 1$ was treated in Proposition 9.1. We have shown that $\tau_2 > \sigma_2$ and that $\tau_{n+1}/\tau_n > \sigma_{n+1}/\sigma_n$ for all $n \ge 2$. So, by induction, assume that $\tau_n > \sigma_n$. We get that $\tau_{n+1} = (\tau_{n+1}/\tau_n)\tau_n > (\sigma_{n+1}/\sigma_n)\sigma_n = \sigma_{n+1}$. Therefore, $\tau_n > \sigma_n$ for all n. The theorem follows from Proposition 11.2.

The proof of Theorem 1.4 is now complete in all cases.

12. The detection theorem and the vanishing theorem

Having now settled Theorem 1.4, we can move to the main detection theorem (Theorem 1.2) and the vanishing theorem (Theorem 1.1). Recall that they assert that if G is not cyclic, quaternion or semi-dihedral, then $T(G)$ is detected on restriction to all elementary abelian subgroups E of rank 2, and that the torsion subgroup of $T(G)$ is trivial.

Let us first prove a general version of the detection theorem.

THEOREM 12.1. *For any p-group G, the restriction homomorphism*

$$\prod_H \mathrm{Res}^G_H\ : T(G) \longrightarrow \prod_H T(H)$$

is injective, where H runs through the set of all subgroups of G which are elementary abelian of rank 2, *cyclic of order p with p odd, cyclic of order* 4, *and quaternion of order* 8.

Proof. First note that that there is nothing to prove if G is cyclic of order 1 or 2, because $T(G) = \{0\}$. There is also nothing to prove if G is in the detecting family of the statement. So we can assume that G is not elementary abelian of rank 2, C_p, C_4, or Q_8. By an obvious induction argument, it suffices to prove that

$$\prod_H \mathrm{Res}^G_H\ : T(G) \longrightarrow \prod_H T(H)$$

is injective, where H runs through the set of all maximal subgroups of G.

If $G = C_{p^n}$ is cyclic (with $n \ge 2$ for p odd and $n \ge 3$ if $p = 2$), then $\mathrm{Res}^{C_{p^n}}_{C_{p^{n-1}}} : T(C_{p^n}) \longrightarrow T(C_{p^{n-1}})$ is an isomorphism (both groups are isomorphic to $\mathbb{Z}/2\mathbb{Z}$ generated by the class of $\Omega^1(k)$). If G is extraspecial or almost extraspecial, the result follows from the main theorem of this paper (Theorem 1.4) if either $p = 2$ or p is odd and G has exponent p. If p is odd and G has exponent p^2 (extraspecial or almost extraspecial), then the result was proved in Section 4 of [CaTh].

So we can assume that G is neither cyclic, nor elementary abelian of rank 2, nor extraspecial, nor almost extraspecial. In that case, the result was proved as Theorem 3.2 of [CaTh]. □

This theorem provides a direct proof of the following result, which was first proved by Puig [Pu] using an argument of commutative algebra.

COROLLARY 12.2. *The abelian group $T(G)$ is finitely generated.*

As observed by Puig, this easily implies the finite generation of the Dade group of all endo-permutation modules (see Corollary 2.4 in Puig [Pu]).

Proof. $T(H)$ is finitely generated whenever H is in the detecting family. Now a subgroup of a finitely generated group is finitely generated. □

Theorem 12.1 is the intermediate statement which we need for our inductive proof of Theorem 1.2. We first need to prove the result in two special cases.

PROPOSITION 12.3. *Suppose that $G \cong Q_8 \times C_2$ or $G \cong D_8 * C_4$. Then $T(G)$ is detected on restriction to all elementary abelian subgroups E of rank* 2.

Proof. Suppose that M is a nontrivial endo-trivial module such that $M{\downarrow}^G_E \cong k \oplus (\text{free})$ for every elementary abelian subgroup E of rank 2. Assume that M has minimal dimension among such modules. On restriction to a maximal subgroup of the form $C_4 \times C_2$, we must have that $M{\downarrow}^G_{C_4\times C_2} \cong k \oplus (\text{free})$, because $T(C_4\times C_2) \longrightarrow T(E)$ is an isomorphism for $E = C_2\times C_2 \subset C_4\times C_2$. It follows that $\mathrm{Dim}(M) \equiv 1 \pmod 8$. It also follows that $M{\downarrow}^G_{C_4} \cong k \oplus (\text{free})$ for any cyclic subgroup C_4, because C_4 is contained in a maximal subgroup of the form $C_4\times C_2$.

Since M is nontrivial, it must be detected on some restriction (Theorem 12.1). So there exists a quaternion subgroup $H \cong Q_8$ in G such that $M{\downarrow}^G_H$ is nontrivial. Then $M{\downarrow}^G_H \cong \Omega^2(k_H) \oplus (\text{free})$, because $\Omega^2(k_H)$ is the only indecomposable endo-trivial kH-module other than k_H itself whose dimension is congruent to 1 modulo 8 (see [CaTh, §6]).

Let z be the generator of the center of H (which is also central in G). We consider the variety $V_{\overline{G}}(\overline{M}) \subseteq V_{\overline{G}}(k) \cong k^3$ where, as in Section 5, $\overline{G} = G/\langle z\rangle$ and $\overline{M} \cong (z-1)M$. On restriction to H, we have $V_{\overline{H}}(\overline{M}) = V_{\overline{H}}(\overline{\Omega^2(k_H)})$ and $\overline{\Omega^2(k_H)}$ is a periodic $k\overline{H}$-module by Lemma 5.3. Since $\Omega^2(k_H)$ is invariant under Galois automorphisms, so is $\overline{\Omega^2(k_H)}$, and therefore $V_{\overline{H}}(\overline{M})$ is a union of lines permuted by Galois automorphisms. But these lines are not $\mathbb{F}_2$-rational (by Lemma 6.1 applied to the kH-module $\Omega^2(k_H)$, which is critical), hence not fixed by Galois automorphisms. It follows that there are at least two lines in $V_{\overline{H}}(\overline{M})$ (and in fact exactly two, which are $\mathbb{F}_4$-rational, because this is the only possibility for the 4-dimensional module $\overline{\Omega^2(k_H)}$). Now $V_{\overline{G}}(\overline{M})$ also contains at least two lines since it contains $\mathrm{res}^*_{\overline{G},\overline{H}}(V_{\overline{H}}(\overline{M}))$. So $\overline{M} \cong \overline{M_1} \oplus \overline{M_2}$ where $V_{\overline{G}}(\overline{M_1})$ is one of the two lines. Now following the procedure of Theorem 5.6 we can construct a nontrivial endo-trivial kG-module N_1 such that $\overline{N_1} = \overline{M_1}$. Moreover N_1 is trivial on restriction to every elementary abelian subgroup. But $\mathrm{Dim}(N_1) < \mathrm{Dim}(M)$, contrary to the choice of M. □

We also need a group-theoretical lemma.

LEMMA 12.4. *Let G be a semi-direct product $G = Q_{2^n} \rtimes C_2$ for some $n \geq 3$ and some action of C_2 on Q_{2^n}. Then one of the following properties holds*:

(a) *G contains a semi-dihedral subgroup S such that $S \supseteq Q_8 \subseteq Q_{2^n}$.*

(b) *G contains a subgroup $Q_8 * C_4$ with $Q_8 \subseteq Q_{2^n}$.*

(c) *G contains a subgroup $Q_8 \times C_2$ with $Q_8 \subseteq Q_{2^n}$.*

Proof. Let u be a generator of C_2. We use induction on n and first consider the case $n = 3$. If the action of u on $Q_8/Z(Q_8)$ is nontrivial, then we can choose two generators x and y of Q_8 such that $uxu^{-1} = y$. In that case G is semi-dihedral and we are in case (a). If now u acts trivially on $Q_8/Z(Q_8)$, then u fixes each of the three cyclic subgroups of order 4 of Q_8. If u acts trivially on Q_8, then $G = Q_8 \times C_2$ and we are in case (c). Otherwise it easy to see that u must invert two of the cyclic subgroups of order 4 and fix pointwise the third one, say $\langle x \rangle$. But then the actions of u and x coincide, so that ux^{-1} acts trivially and $G = Q_8 * C_4$, which is case (b).

Assume now that $n \geq 4$. Let x and y be generators of Q_{2^n} with $x^{2^{n-1}} = 1$, $y^2 = x^{2^{n-2}}$ and $yxy^{-1} = x^{-1}$. All elements of the form $x^b y$ have order 4 (where $0 \leq b \leq 2^{n-1}$). Conjugation by u must satisfy $uxu^{-1} = x^a$ for some odd integer a and $uyu^{-1} = x^b y$ for some b. Since $u^2 = 1$, we must have the following congruences modulo 2^{n-1}:

$$a \equiv \pm 1\,, 2^{n-2} \pm 1 \qquad \text{and} \qquad (a+1)b \equiv 0\,.$$

If $a \equiv -1$ and b is odd, we can replace x by x^b and we get a standard presentation of the semi-dihedral group $\mathrm{SD}_{2^{n+1}}$, so we are in case (a). Otherwise b must be even, because this is forced by the condition $(a+1)b \equiv 0$ if $a \not\equiv -1$. Therefore conjugation by u stabilizes the subgroup $Q_{2^{n-1}}$ generated by x^2 and y. The result now follows by induction applied to the group $Q_{2^{n-1}} \rtimes \langle u \rangle$. □

Now we come to the detection theorem (Theorem 1.2 of the introduction).

THEOREM 12.5. *Suppose that G is a p-group which is not cyclic, quaternion, or semi-dihedral. Then $T(G)$ is detected on restriction to all elementary abelian subgroups E of rank* 2.

Proof. We use induction on the order of G. First recall that the result is known if G is abelian or dihedral (see [CaTh]); so we assume that G is neither abelian nor dihedral.

Let M be an endo-trivial module such that $\mathrm{Res}^G_E[M]=0$ for every elementary abelian subgroup E of rank 2, where $[M]$ denotes the class of M in $T(G)$. It suffices to prove that $\mathrm{Res}^G_H[M]=0$ for every maximal subgroup H of G, because then $[M]=0$ by Theorem 12.1. For every maximal subgroup H which is not cyclic, quaternion, or semi-dihedral, $M{\downarrow}^G_H$ satisfies the same assumption as M, so that $\mathrm{Res}^G_H[M]=0$ by induction. Now, we are left with the cases where the maximal subgroup H is cyclic, quaternion, or semi-dihedral.

Assume first that $H\cong C_{p^n}$ is cyclic. By a well-known result of group theory (see Theorem 4.4 in Chapter 5 of [Go1]), G is either abelian, or isomorphic to a group P to be described below, or in addition when $p=2$, isomorphic to $D_{2^{n+1}}$, $Q_{2^{n+1}}$, or $\mathrm{SD}_{2^{n+1}}$. The cases of the cyclic group $C_{p^{n+1}}$, the quaternion group $Q_{2^{n+1}}$, or the semi-dihedral group $\mathrm{SD}_{2^{n+1}}$, are excluded by our hypothesis. The cases of an abelian group or a dihedral group $D_{2^{n+1}}$ have already been dealt with. So we are left with the case $G=P=H\rtimes C_p$, with respect to the action $uxu^{-1}=x^{1+p^{n-1}}$, where x is a generator of H and u is a generator of C_p. This case occurs if $n\geq 2$ when p is odd and $n\geq 3$ when $p=2$. Now G also contains a maximal subgroup $K=\langle x^p\rangle\times\langle u\rangle\cong C_{p^{n-1}}\times C_p$ and we already know that $\mathrm{Res}^G_K[M]=0$. Therefore

$$\mathrm{Res}^G_{C_{p^{n-1}}}[M]=\mathrm{Res}^K_{C_{p^{n-1}}}\ \mathrm{Res}^G_K[M]=0\,.$$

But we also have $\mathrm{Res}^G_{C_{p^{n-1}}}=\mathrm{Res}^H_{C_{p^{n-1}}}\ \mathrm{Res}^G_H$ and

$$\mathrm{Res}^H_{C_{p^{n-1}}}:T(H)\longrightarrow T(C_{p^{n-1}})$$

is an isomorphism since both $T(H)$ and $T(C_{p^{n-1}})$ are cyclic of order 2 generated by the class of $\Omega^1(k)$ (because $n\geq 2$ and $n\geq 3$ if $p=2$). It follows that $\mathrm{Res}^G_H[M]=0$.

Assume now that $H\cong\mathrm{SD}_{2^n}$ is semi-dihedral. We know that the torsion subgroup $T_t(H)$ is cyclic of order 2 generated by the class of an endo-trivial module whose dimension is congruent to 1 modulo 2^{n-1} (see [CaTh, §7]). This class cannot be in the image of Res^G_H, because all endo-trivial modules for G have dimension congruent to ±1 modulo 2^n, by Lemma 2.10 in [CaTh]. It follows that the image of Res^G_H is contained in $\langle\,[\Omega^1_H(k)]\,\rangle\cong\mathbb{Z}$, because $T(H)=T_t(H)\oplus\langle\,[\Omega^1_H(k)]\,\rangle$. But now the restriction map

$$\mathrm{Res}^H_E\ :\langle\,[\Omega^1_H(k)]\,\rangle\longrightarrow T(E)=\langle\,[\Omega^1_E(k)]\,\rangle$$

is an isomorphism where E is an elementary abelian subgroup of rank 2. Since $\operatorname{Res}^H_E \operatorname{Res}^G_H[M] = 0$, we must have $\operatorname{Res}^G_H[M] = 0$ as required. Note that the same argument shows that $\operatorname{Res}^G_S[M] = 0$ for any semi-dihedral subgroup S of G.

Assume finally that $H \cong Q_{2^n}$ is quaternion. Since G is neither cyclic nor quaternion, its 2-rank cannot be 1 (see Chapter 5 of [Go1]) and so there exists an element of order 2 outside H. Therefore $G \cong Q_{2^n} \rtimes C_2$ for some action of C_2 on Q_{2^n}. By Lemma 12.4, G contains a subgroup R which is isomorphic to $Q_8 * C_4$, $Q_8 \times C_2$, or semi-dihedral, and such that $R \supseteq Q_8 \subseteq H$. In the first two cases we have $\operatorname{Res}^G_R[M] = 0$ by Proposition 12.3 and in the third we have $\operatorname{Res}^G_R[M] = 0$ by the argument above. It follows that

$$\operatorname{Res}^H_{Q_8} \operatorname{Res}^G_H[M] = \operatorname{Res}^G_{Q_8}[M] = \operatorname{Res}^R_{Q_8} \operatorname{Res}^G_R[M] = 0\,.$$

We know that $T(H) \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, where $\mathbb{Z}/4\mathbb{Z}$ is generated by the class of $\Omega^1_H(k)$ and $\mathbb{Z}/2\mathbb{Z}$ is generated by the class of an endo-trivial module of dimension $2^{n-1}+1$ (see [CaTh, §6]). Again this class cannot be in the image of Res^G_H, because all endo-trivial modules for G have dimension congruent to ± 1 modulo 2^n. Thus the image of Res^G_H is contained in $\mathbb{Z}/4\mathbb{Z} = \langle\, [\Omega^1_H(k)]\,\rangle$. But now the restriction map

$$\operatorname{Res}^H_{Q_8} : \langle\, [\Omega^1_H(k)]\,\rangle \longrightarrow \langle\, [\Omega^1_{Q_8}(k)]\,\rangle$$

is an isomorphism. Since $\operatorname{Res}^H_{Q_8} \operatorname{Res}^G_H[M] = 0$, we must have $\operatorname{Res}^G_H[M] = 0$ as required. □

We immediately deduce the vanishing theorem (Theorem 1.1 of the introduction).

Corollary 12.6. *If G is not cyclic, quaternion or semi-dihedral, then the torsion subgroup of $T(G)$ is trivial.*

Proof. By the theorem, we know that $T(G)$ is embedded in a product of copies of $T(E) \cong \mathbb{Z}$, where E is elementary abelian of rank 2. □

We can now prove Corollary 1.3 of the introduction.

Corollary 12.7. *Suppose that G is a finite p-group for which every maximal elementary subgroup has rank at least 3. Then $T(G) \cong \mathbb{Z}$, generated by the class of the module $\Omega^1(k)$.*

Proof. The assumption implies that G cannot be cyclic, quaternion or semi-dihedral. Therefore, by the theorem, $T(G)$ is detected on restriction to elementary abelian subgroups of rank 2. The rest of the proof follows Alperin [Al2] and we recall the argument (also used in [BoTh]). The partially ordered set of all elementary abelian subgroups of rank at least 2 is connected, in view of the assumption and by a well-known result of the theory of

p-groups. For any such subgroup H, the restriction map $T(H) \longrightarrow T(E) \cong \mathbb{Z}$ to an elementary abelian subgroup of rank 2 is an isomorphism. It follows that all restrictions to such rank 2 subgroups E are equal. □

13. The Dade group

In this section, we prove detection theorems for the Dade group $D(G)$ of all endo-permutation modules and we determine its torsion subgroup when p is odd. We refer to [BoTh] for details about $D(G)$. Let us only mention that the torsion-free rank of $D(G)$ has been determined in [BoTh] so that we are particularly interested in the torsion subgroup $D_t(G)$. We first state an easy consequence of Theorem 12.1.

THEOREM 13.1. *Let G be a finite p-group.*

(a) *The product of all restriction-deflation maps*

$$\prod_{K/H} \mathrm{Def}^K_{K/H}\ \mathrm{Res}^G_K\ :\ D(G) \longrightarrow \prod_{K/H} D(K/H)$$

is injective, where K/H runs through the set of all sections of G which are elementary abelian of rank 2, cyclic of order p with p odd, cyclic of order 4, or quaternion of order 8.

(b) *For the torsion subgroup, the product of all restriction-deflation maps*

$$\prod_{K/H} \mathrm{Def}^K_{K/H}\ \mathrm{Res}^G_K\ :\ D_t(G) \longrightarrow \prod_{K/H} D_t(K/H)$$

is injective, where K/H runs through the set of all sections of G which are cyclic of order p if p is odd, quaternion of order 8 or cyclic of order 4 if $p = 2$.

Proof. The argument is exactly the same as the one given in Theorem 1.6 of [BoTh] or in Theorem 10.1 of [CaTh]. □

We now deduce Corollary 1.6 of the introduction.

COROLLARY 13.2. *Let G be a finite p-group.*

(a) *If p is odd, any nontrivial torsion element in $D(G)$ has order 2. In other words, for any indecomposable endo-permutation kG-module M with vertex G, the class of M is a torsion element if and only if M is self-dual.*

(b) *If $p = 2$, any nontrivial torsion element in $D(G)$ has order 2 or 4.*

Proof. The nontrivial elements of $D(C_p)$ have order 2, while those of $D(Q_8)$ and $D(C_4)$ have order 2 or 4. Moreover, an element of order 2 corresponds to a self-dual module by definition of the group law. □

If p is odd, the detection theorem above allows for a complete description of the torsion subgroup of $D(G)$ (Theorem 1.5 of the introduction), by the partial results already obtained in [BoTh].

THEOREM 13.3. *If p is odd and G is a finite p-group, the torsion subgroup of $D(G)$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^s$, where s is the number of conjugacy classes of nontrivial cyclic subgroups of G.*

Note that explicit generators are described in [BoTh].

Proof. Theorem 6.2 in [BoTh] asserts that a certain quotient $\overline{D_t(G)}$ of the torsion subgroup $D_t(G)$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^s$, where s is as above. So we only have to prove that $\overline{D_t(G)} = D_t(G)$. But by definition, $\overline{D_t(G)} = D_t(G)/\operatorname{Ker}(\psi)$, where ψ is the product of all restriction-deflation maps

$$\psi = \prod_{K/H} \operatorname{Def}^K_{K/H} \operatorname{Res}^G_K \,:\, D_t(G) \longrightarrow \prod_{K/H} D_t(K/H)$$

where K/H runs through the set of all sections of G which are cyclic of order p. Now ψ is injective by Theorem 13.1 and the result follows. □

Our purpose now is to improve Theorem 13.1 by restricting the kind of section needed on the right-hand side. However, we will also change the target by including all groups having torsion endo-trivial modules, namely cyclic, quaternion, and semi-dihedral groups.

If $S = \langle x \rangle$ is cyclic of order p^n, then

$$D(S) = D_t(S) \cong \prod_{i=1}^{n} T_t(S/\langle x^{p^i} \rangle)\,,$$

and we let $\pi_S : D_t(S) \to T_t(S)$ denote the projection onto the factor indexed by $i = n$. The situation is easier if S is a quaternion or semi-dihedral group, since $D_t(S) = T_t(S)$ by [CaTh, §10]. In this case, we write $\pi_S : D_t(S) \to T_t(S)$ for the identity map.

THEOREM 13.4. *Let G be a finite p-group. If p is odd, let $\mathcal{X}$ be the class of all subgroups H of G such that $N_G(H)/H$ is cyclic. If $p = 2$, let $\mathcal{X}$ be the class of all subgroups H of G such that $N_G(H)/H$ is cyclic of order ≥ 4, quaternion of order ≥ 8, or semi-dihedral of order ≥ 16. Let $[\mathcal{X}/G]$ be a system* *of representatives of conjugacy classes of subgroups in $\mathcal{X}$. Then the map*

$$\prod_{H\in[\mathcal{X}/G]} \pi_{N_G(H)/H}\ \mathrm{Def}^{N_G(H)}_{N_G(H)/H}\ \mathrm{Res}^G_{N_G(H)} :$$
$$D_t(G) \longrightarrow \prod_{H\in[\mathcal{X}/G]} T_t(N_G(H)/H)$$

is injective.

Proof. Let φ denote the map in the statement and let $a \in \mathrm{Ker}(\varphi)$, so that $\pi_{N_G(H)/H}\ \mathrm{DefRes}^G_{N_G(H)/H}(a) = 0$ for every $H \in \mathcal{X}$, where we write for simplicity $\mathrm{DefRes}^G_{K/H} = \mathrm{Def}^K_{K/H}\ \mathrm{Res}^G_K$ for every section K/H. By Theorem 13.1 above, it suffices to prove that $\mathrm{DefRes}^G_{K/H}(a) = 0$ for every section K/H isomorphic to C_p, C_4 or Q_8. We are going to show that $\mathrm{DefRes}^G_{N_G(H)/H}(a) = 0$ and the result will follow from this since $\mathrm{DefRes}^G_{K/H} = \mathrm{Res}^{N_G(H)/H}_{K/H}\ \mathrm{DefRes}^G_{N_G(H)/H}$. For simplicity of notation, we write now $L = N_G(H)$.

We use induction on the index $|G : H|$. If H has index p, there is nothing to prove because $L = G$, $\pi_{G/H} = \mathrm{id}$, and

$$\mathrm{DefRes}^G_{G/H}(a) = \pi_{G/H}\ \mathrm{DefRes}^G_{G/H}(a) = 0\,,$$

by assumption if p is odd and by the fact that $D(G/H) = \{0\}$ if $p = 2$. Let F be a subgroup such that $H < F \le L$. By induction, $\mathrm{DefRes}^G_{N_G(F)/F}(a) = 0$ and consequently $\mathrm{DefRes}^G_{N_L(F)/F}(a) = 0$. This holds for every such F and therefore

$$\mathrm{DefRes}^G_{L/H}(a) \in \bigcap_{H<F\le L} \mathrm{Ker}(\mathrm{DefRes}^{L/H}_{N_L(F)/F})\ =\ T(L/H)\,.$$

The last equality is a well-known characterization of $T(L/H)$ as a subgroup of $D(L/H)$ (see Lemma 2.1 in [CaTh] and note that this characterization is also at the heart of the proof of Theorem 13.1). Since a was chosen to be a torsion element in $D(G)$, we have proved that $\mathrm{DefRes}^G_{L/H}(a) \in T_t(L/H)$.

If L/H is not cyclic, quaternion, or semi-dihedral, then $T_t(L/H) = \{0\}$ by Theorem 1.1 and so $\mathrm{DefRes}^G_{L/H}(a) = 0$. The same holds if L/H is cyclic of order 2. If L/H is quaternion or semi-dihedral, then $\pi_{L/H}$ is the identity map and $\pi_{L/H}\ \mathrm{DefRes}^G_{L/H}(a) = 0$ by assumption, so $\mathrm{DefRes}^G_{L/H}(a) = 0$. If L/H is cyclic of order ≥ 3, then $\pi_{L/H} : D_t(L/H) \to T_t(L/H)$ restricts to the identity on $T_t(L/H)$. Since $\pi_{L/H}\ \mathrm{DefRes}^G_{L/H}(a) = 0$ by assumption, we obtain again $\mathrm{DefRes}^G_{L/H}(a) = 0$. □

In order to illustrate the efficiency of Theorem 13.4 compared to Theorem 13.1, suppose that G is abelian. Then there are numerous sections of G isomorphic to C_p or C_4 and the map in Theorem 13.1 is an injection in a much larger group, whereas the map in Theorem 13.4 hits exactly every cyclic quotient of G and is an isomorphism (Dade's theorem).

If G is a dihedral 2-group, there are many sections of G isomorphic to C_4, but $N_G(H)/H$ is never cyclic of order ≥ 4, quaternion, or semi-dihedral, so that $\mathcal{X}$ is empty and $D_t(G) = \{0\}$, a result also obtained in [CaTh, §10].

Theorem 13.4 allows us to handle also a case where the structure of $D_t(G)$ was not previously known.

Proposition 13.5. *Suppose that G is an extraspecial 2-group of type 1, that is, a central product of copies of D_8. Then $D_t(G) = \{0\}$.*

Proof. We claim that $\mathcal{X}$ is empty and so $D_t(G) = \{0\}$. If H is a subgroup of G containing $Z(G)$, then H is a normal subgroup, G/H is elementary abelian, and $H \notin \mathcal{X}$. If H does not contain $Z(G)$, then for any $g \in N_G(H)$, we have that $[g,h] \in H \cap Z(G) = \{1\}$. Thus $N_G(H) = C_G(H)$ and in particular H is abelian, actually elementary abelian, since the square of every element of H belongs to $H \cap Z(G) = \{1\}$. Using the quadratic form on $G/Z(G)$, it is not hard to prove that if n is the number of copies of D_8 in the central product and if $H = (C_2)^k$, then $C_G(H) = H \times L$ where L is a central product of $n-k$ copies of D_8 (possibly $n-k = 0$ and $L = Z(G)$). Therefore $N_G(H)/H$ is extraspecial and $H \notin \mathcal{X}$. This proves that $\mathcal{X}$ is empty. □

14. Two examples

Theorem 13.4 is not sufficient to determine $D_t(G)$ in all cases when $p = 2$. This seems to be in contrast to the case of an odd prime, for which the solution of the detection conjecture for $T(G)$ allows for a complete description of $D_t(G)$ (Theorem 1.5).

Our purpose is to illustrate the situation with the extraspecial groups of type 2 and the almost extraspecial groups (type 3). For simplicity, we shall only deal with the smallest of the groups, namely $D_8 * Q_8$ and $D_8 * C_4$, but our results can easily be generalized to the other groups of types 2 and 3.

If follows from Theorem 13.4 that the product of all restriction-deflation maps

$$\prod_{H \in [\mathcal{X}/G]} \mathrm{Def}^{N_G(H)}_{N_G(H)/H} \ \mathrm{Res}^G_{N_G(H)} : D_t(G) \longrightarrow \prod_{H \in [\mathcal{X}/G]} D_t(N_G(H)/H)$$

is injective. In the opposite direction, there is the sum of all maps obtained by composing inflation maps $\mathrm{Inf}^{N_G(H)}_{N_G(H)/H}$ and tensor induction $\mathrm{Ten}^G_{N_G(H)}$, namely

$$\sum_{H \in [\mathcal{X}/G]} \mathrm{Ten}^G_{N_G(H)} \ \mathrm{Inf}^{N_G(H)}_{N_G(H)/H} : \bigoplus_{H \in [\mathcal{X}/G]} D_t(N_G(H)/H) \longrightarrow D_t(G)\,.$$

We let $D^0_t(G)$ be the image of this map. The question of the surjectivity of this map does not seem to be easy and this is why we have to introduce the subgroup $D^0_t(G)$. In similar situations for odd primes, or for the Dade group tensored with $\mathbb{Q}$, we can prove the surjectivity of the map (see Sections 4 and 6 of [BoTh]), so it seems natural to conjecture that $D_t^0(G) = D_t(G)$. In our two examples, we shall be able to compute $D_t^0(G)$ but it is not easy to know if $D_t(G)$ is larger or not.

In order to compute the image by restriction-deflation of elements of $D_t^0(G)$, we need a technical formula which is derived from the results of [BoTh]. There is a general formula describing the restriction-deflation of an element of the form $\mathrm{Ten}_K^G \mathrm{Inf}_{K/H}^K(x)$, but for simplicity we only consider two very special cases. The Frobenius map $\lambda \mapsto \lambda^{p^n}$ is an endomorphism of k and we let

$$\gamma_{p^n} : D(G) \longrightarrow D(G)$$

be the group homomorphism induced by the Frobenius map, as defined in Section 3 of [BoTh].

LEMMA 14.1. *Let G be a p-group and let K and H be subgroups of G such that H is a normal subgroup of K.*

(a) *Let P and R be subgroups of G such that R is a normal subgroup of P. Assume that K and P satisfy $KP = G$ (a single double coset). Assume further that the inclusions $P \cap K \to K$ and $P \cap K \to P$ induce isomorphisms*

$$(P \cap K)/(R \cap H) \xrightarrow{\sim} K/H \qquad \text{and} \qquad (P \cap K)/(R \cap H) \xrightarrow{\sim} P/R$$

respectively. Then the following maps from $D(K/H)$ to $D(P/R)$ are equal:

$$\mathrm{Def}_{P/R}^P \ \mathrm{Res}_P^G \ \mathrm{Ten}_K^G \ \mathrm{Inf}_{K/H}^K = \gamma_{|R:R\cap H|} \ \mathrm{Iso}_{(P\cap K)/(R\cap H)}^{P/R} \ (\mathrm{Iso}_{(P\cap K)/(R\cap H)}^{K/H})^{-1} ,$$

where the two latter maps are induced by the isomorphisms $(P\cap K)/(R\cap H) \xrightarrow{\sim} P/R$ and $(P \cap K)/(R \cap H) \xrightarrow{\sim} K/H$ respectively.

(b) *Let L be a normal subgroup of K. Then the following maps from $D(K/H)$ to $D(K/L)$ are equal:*

$$\mathrm{Def}_{K/L}^K \ \mathrm{Inf}_{K/H}^K = \mathrm{Inf}_{K/HL}^{K/L} \ \mathrm{Def}_{K/HL}^{K/H} .$$

Proof. (a) Since there is a single double coset, the Mackey formula implies that

$$\mathrm{Def}_{P/R}^P \ \mathrm{Res}_P^G \ \mathrm{Ten}_K^G \ \mathrm{Inf}_{K/H}^K = \mathrm{Def}_{P/R}^P \ \mathrm{Ten}_{P\cap K}^P \ \mathrm{Res}_{P\cap K}^K \ \mathrm{Inf}_{K/H}^K .$$

Now Proposition 3.10 in [BoTh] asserts that

$$\mathrm{Def}_{P/R}^P \ \mathrm{Ten}_Q^P = \gamma_{|R:Q\cap R|} \ \mathrm{Ten}_{QR/R}^{P/R} \ \mathrm{Iso}_{Q/Q\cap R}^{QR/R} \ \mathrm{Def}_{Q/Q\cap R}^Q .$$

Applying this with $Q = P \cap K$, we have that $QR = P$ and $Q \cap R = R \cap H$, because of the assumed isomorphism $(P \cap K)/(R \cap H) \xrightarrow{\sim} P/R$, and therefore

$$\mathrm{Def}_{P/R}^P \ \mathrm{Ten}_{P\cap K}^P = \gamma_{|R:R\cap H|} \ \mathrm{Iso}_{P\cap K/R\cap H}^{P/R} \ \mathrm{Def}_{P\cap K/R\cap H}^{P\cap K} .$$

Composing on the right with $\mathrm{Res}^K_{P\cap K}\ \mathrm{Inf}^K_{K/H}$, it is easy to see that

$$\mathrm{Def}^{P\cap K}_{P\cap K/R\cap H}\ \mathrm{Res}^K_{P\cap K}\ \mathrm{Inf}^K_{K/H} = (\mathrm{Iso}^{K/H}_{P\cap K/R\cap H})^{-1}\ ,$$

using either the definitions of the maps or the methods of Corollary 3.9 in [BoTh]. It follows that

$$\mathrm{Def}^P_{P/R}\ \mathrm{Ten}^P_{P\cap K}\ \mathrm{Res}^K_{P\cap K}\ \mathrm{Inf}^K_{K/H} = \gamma_{|R:R\cap H|}\ \mathrm{Iso}^{P/R}_{P\cap K/R\cap H}\ (\mathrm{Iso}^{K/H}_{P\cap K/R\cap H})^{-1}\ ,$$

and the result follows.

(b) This follows either from the definitions of the maps or from the methods of Corollary 3.9 in [BoTh]. □

Now we can start with our first example $D_8 * C_4$. Let S_1, S_2, S_3 be representatives of the three conjugacy classes of noncentral subgroups of order 2 (the two classes in D_8 and the product of a generator of C_4 with an element of order 4 in D_8).

PROPOSITION 14.2. *Let $G = D_8 * C_4$ be the almost extraspecial group of order* 16. *Then $D^0_t(G)$ is cyclic of order* 2, *generated by the class of the module* $\mathrm{Ten}^G_{S_1\times C_4}\ \mathrm{Inf}^{S_1\times C_4}_{S_1\times C_4/S_1}(\Omega^1_{S_1\times C_4/S_1}(k))$.

Proof. We have that $N_G(S_i) = S_i \times C_4$ and so $N_G(S_i)/S_i \cong C_4$ and S_i is in the class $\mathcal{X}$ of Theorem 13.4. These are the only subgroups in $\mathcal{X}$ (because every other nontrivial subgroup H contains the Frattini subgroup and G/H is elementary abelian). Therefore Theorem 13.4 yields an injective map

$$\prod_{i=1}^{3} \mathrm{Def}^{S_i\times C_4}_{S_i\times C_4/S_i}\ \mathrm{Res}^G_{S_i\times C_4} : D_t(G) \longrightarrow \prod_{i=1}^{3} D_t(S_i \times C_4/S_i) \cong (\mathbb{Z}/2\mathbb{Z})^3\ ,$$

each factor $D_t(S_i \times C_4/S_i) \cong D_t(C_4)$ being cyclic of order 2 generated by the class of $\Omega^1_{S_i\times C_4/S_i}(k)$. Now by definition $D^0_t(G)$ is generated by the three elements

$$\mathrm{Ten}^G_{S_i\times C_4}\ \mathrm{Inf}^{S_i\times C_4}_{S_i\times C_4/S_i}(\Omega^1_{S_i\times C_4/S_i}(k)) \quad (1 \le i \le 3)\ .$$

We claim that they are all equal and have order 2. This will complete the proof of the proposition.

In order to prove the claim, we show that the image of any of these three elements by the injective map above is equal to the "diagonal element"

$$(\Omega^1_{S_1\times C_4/S_1}(k)\ ,\ \Omega^1_{S_2\times C_4/S_2}(k)\ ,\ \Omega^1_{S_3\times C_4/S_3}(k)\ )\ .$$

This follows from a straightforward application of Lemma 14.1. If $i \neq j$, we obtain

$$\begin{aligned}
&\mathrm{Def}^{S_j\times C_4}_{S_j\times C_4/S_j}\ \mathrm{Res}^G_{S_j\times C_4}\ \mathrm{Ten}^G_{S_i\times C_4}\ \mathrm{Inf}^{S_i\times C_4}_{S_i\times C_4/S_i}(\Omega^1_{S_i\times C_4/S_i}(k))\\
&\quad = \gamma_{|S_j:1|}\ \mathrm{Iso}^{S_j\times C_4/S_j}_{C_4/1}\ (\mathrm{Iso}^{S_i\times C_4/S_i}_{C_4/1})^{-1}(\Omega^1_{S_i\times C_4/S_i}(k))\\
&\quad = \gamma_2(\Omega^1_{S_j\times C_4/S_j}(k)) = \Omega^1_{S_j\times C_4/S_j}(k)\ ,
\end{aligned}$$

using the fact that $\Omega^1(k)$ is defined over the prime field $\mathbb{F}_2$ and hence is fixed by the Frobenius map γ_2. In the case $i = j$, we have for any $k[S_i \times C_4]$-module M,

$$\mathrm{Res}^G_{S_i\times C_4}\ \mathrm{Ten}^G_{S_i\times C_4}(M) = M \otimes {}^gM\,,$$

where g is a representative of the nontrivial class of $G/S_i \times C_4$ and ${}^gM$ denotes the conjugate module. Therefore, ignoring inflation for simplicity, we obtain

$$\begin{aligned}
&\mathrm{Def}^{S_i\times C_4}_{S_i\times C_4/S_i}\ \mathrm{Res}^G_{S_i\times C_4}\ \mathrm{Ten}^G_{S_i\times C_4}\ \mathrm{Inf}^{S_i\times C_4}_{S_i\times C_4/S_i}(\Omega^1_{S_i\times C_4/S_i}(k))\\
&\quad= \mathrm{Def}^{S_i\times C_4}_{S_i\times C_4/S_i}\ \big(\Omega^1_{S_i\times C_4/S_i}(k)\otimes {}^g(\Omega^1_{S_i\times C_4/S_i}(k))\big)\\
&\quad= \mathrm{Def}^{S_i\times C_4}_{S_i\times C_4/S_i}\ \big(\Omega^1_{S_i\times C_4/S_i}(k)\big)\otimes \mathrm{Def}^{S_i\times C_4}_{S_i\times C_4/S_i}\ \big(\Omega^1_{S_i\times C_4/gS_ig^{-1}}(k)\big)\\
&\quad= \Omega^1_{S_i\times C_4/S_i}(k)\otimes \mathrm{Def}^{S_i\times C_4}_{S_i\times C_4/S_i}(\Omega^1_{S_i\times C_4/gS_ig^{-1}}(k))\,.
\end{aligned}$$

But the second factor is trivial because, by part (b) of Lemma 14.1 with $K = S_i \times C_4$, we have

$$\mathrm{Def}^K_{K/S_i}\ \mathrm{Inf}^K_{K/gS_ig^{-1}} = \mathrm{Inf}^{K/S_i}_{K/S_i(gS_ig^{-1})}\ \mathrm{Def}^{K/gS_ig^{-1}}_{K/S_i(gS_ig^{-1})}$$

and a deflation of the class of $\Omega^1(k)$ is trivial (see Lemma 1.3 of [BoTh]). $\square$

In this example, we see that $D_t(G)$ embeds in three copies of $\mathbb{Z}/2\mathbb{Z}$ and that $D^0_t(G) \cong \mathbb{Z}/2\mathbb{Z}$. So in order to prove the conjectural equality $D^0_t(G) = D_t(G)$, we would have to improve Theorem 13.4 by showing the injectivity of the restriction-deflation map to a single section $S_i \times C_4/S_i$. In this specific example, we have been able to do this by a rather delicate argument not given here.

The methods are similar with our second example $D_8 * Q_8$, but another complication occurs. Recall that $D_t(Q_8)$ is generated by the class of $\Omega^1_{Q_8}(k)$, which has order 4, and the class of a certain 5-dimensional module M, which has order 2 (see [CaTh, §6]). Moreover M is defined over the field $\mathbb{F}_4$ (so we assume here that k contains $\mathbb{F}_4$) and M is not invariant under the Galois automorphism γ_2. Actually $\gamma_2(M) \cong \Omega^2(M)$, another 5-dimensional module, and $\Omega^2(k)$, M, $\Omega^2(M)$ are the three elements of order 2 in $D_t(Q_8) \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

Let $S_1, \ldots, S_5$ be representatives of the five conjugacy classes of noncentral subgroups of order 2 (the two classes in D_8 and the product of an element of order 4 in D_8 with one of the three possible elements of order 4 in Q_8).

PROPOSITION 14.3. *Let $G = D_8 * Q_8$ be the extraspecial group of order* 32 (*type* 2). *Then*

$$D^0_t(G) \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$$

generated by the class of the module

$$\mathrm{Ten}^G_{N_G(S_1)}\ \mathrm{Inf}^{N_G(S_1)}_{N_G(S_1)/S_1}(\Omega^1_{N_G(S_1)/S_1}(k)) \qquad (\textit{order } 4)$$

and by the class

$$\mathrm{Ten}^{G}_{N_G(S_1)}\,\mathrm{Inf}^{N_G(S_1)}_{N_G(S_1)/S_1}(M_{N_G(S_1)/S_1}) \qquad (\textit{order } 2),$$

where $M_{N_G(S_1)/S_1}$ *is the module* M *viewed as a module for the group* $N_G(S_1)/S_1$*, which is isomorphic to* Q_8.

Proof. We have that $N_G(S_i) = S_i \times C$ (for some subgroup C isomorphic to Q_8) and so $N_G(S_i)/S_i \cong Q_8$ and S_i is in the class $\mathcal{X}$ of Theorem 13.4. These are the only subgroups in $\mathcal{X}$, because every other nontrivial subgroup H contains the Frattini subgroup and G/H is elementary abelian. Therefore, by Theorem 13.4, the map

$$\prod_{i=1}^{5} \mathrm{Def}^{N_G(S_i)}_{N_G(S_i)/S_i}\ \mathrm{Res}^{G}_{N_G(S_i)} : D_t(G) \longrightarrow \prod_{i=1}^{5} D_t(N_G(S_i)/S_i) \cong (D_t(Q_8))^5$$

is injective. Now by definition $D^0_t(G)$ is generated by the classes of the modules

$$\mathrm{Ten}^{G}_{N_G(S_i)}\,\mathrm{Inf}^{N_G(S_i)}_{N_G(S_i)/S_i}(X) \quad (1 \le i \le 5)\,,$$

where X is either $\Omega^1(k)$ or M (viewed in $D_t(N_G(S_i)/S_i)$).

If $X = \Omega^1(k)$, we always obtain the same element, independently of i, mapping to the diagonal element consisting of $\Omega^1(k)$ in each component under the injective map above. The proof of this follows exactly the same argument as the one used in the proof of Proposition 14.2, with the following minor modification. For every pair S_i, S_j with $i \neq j$, the group generated by S_i and S_j is isomorphic to D_8. Its centralizer C is isomorphic to Q_8, and we have $N_G(S_i) = S_i \times C$ and $N_G(S_j) = S_j \times C$. It follows that we can use Lemma 14.1 (with $P/Q = N_G(S_i)/S_i$, $K/H = N_G(S_j)/S_j$, $P \cap K = C$). The rest of the argument is similar to that used in Proposition 14.2.

If now $X = M$, we again use Lemma 14.1, but the computation changes because of the presence of the Galois automorphism γ_2 which does not fix the class of M. Moreover, for each i, we need to fix a choice of isomorphism $N_G(S_i)/S_i \cong Q_8$ in order to be able to make a consistent computation. We skip the details and only give the result. It turns out that, under the injective map above, the image of $\mathrm{Ten}^{G}_{N_G(S_i)}\,\mathrm{Inf}^{N_G(S_i)}_{N_G(S_i)/S_i}(M)$ is the 5-tuple (M, M, M, M, M), again independent of i. It follows that we obtain just one extra generator of $D^0_t(G)$, of order 2. □

In this example, $D_t(G)$ is sandwiched between $D^0_t(G) \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ and $(\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z})^5$. The question of the equality $D_t(G) = D^0_t(G)$ remains open.

University of Georgia, Athens, GA
E-mail address: jfc@sloth.math.uga.edu

École Polytechnique Fédérale de lausanne, Lausanne, Switzerland
E-mail address: jacques.thevenaz@epfl.ch

References

[Al1] J. L. Alperin, Invertible modules for groups, *Notices Amer. Math. Soc.* **24** (1977), A–64.

[Al2] ———, A construction of endo-permutation modules, *J. Group Theory* **4** (2001), 3–10.

[As] M. Aschbacher, *Finite Group Theory*, Cambridge Univ. Press, Cambridge, 1986.

[Be] D. J. Benson, *Representations and Cohomology* I, II, Cambridge Univ. Press, Cambridge, 1991.

[BeCa] D. J. Benson and J. F. Carlson, The cohomology of extraspecial groups, *Bull. London Math. Soc.* **24** (1992), 209–235.

[BoTh] S. Bouc and J. Thévenaz, The group of endo-permutation modules, *Invent. Math.* **139** (2000), 275–349.

[Ca1] J. F. Carlson, Endo-trivial modules over (p, p)-groups, *Illinois J. Math.* **24** (1980), 287–295.

[Ca2] ———, Cohomology and induction from elementary abelian subgroups, *Quarterly J. Math.* **51** (2000), 169–181.

[CaTh] J. F. Carlson and J. Thévenaz, Torsion endo-trivial modules, *Algebr. Represent. Theory* **3** (2000), 303–335.

[Cart] R. W. Carter, *Finite Groups of Lie Type: Conjugacy Classes and Complex Characters*, John Wiley and Sons, New York, 1985.

[Da] E. C. Dade, Endo-permutation modules over p-groups, I, II, *Ann. of Math.* **107** (1978), 459–494, **108** (1978), 317–346.

[Ev] L. Evens, *The Cohomology of Groups*, Oxford University Press, New York, 1991.

[Go1] D. Gorenstein, *Finite Groups*, Harper & Row, New York, 1968.

[Go2] ———, *Finite Simple Groups*, Plenum Press, New York, 1982.

[Le1] I. J. Leary, The mod-p cohomology rings of some p-groups, *Math. Soc. Cambridge Philos. Soc.* **112** (1992), 63–75.

[Le2] ———, A differential in the Lyndon-Hochschild-Serre spectral sequence, *J. Pure Appl. Algebra* **88** (1993), 155–168.

[Pu] L. Puig, Affirmative answer to a question of Feit, *J. Algebra* **131** (1990), 513–526.

[Qu] D. Quillen, The mod 2 cohomology rings of extra-special 2-groups and the spinor groups, *Math. Ann.* **194** (1971), 197–212.

[Ta] D. E. Taylor, *The Geometry of the Classical Groups*, Heldermann Verlag, Berlin, 1992.

[Wi] D. L. Winter, The automorphism group of an extraspecial p-group, *Rocky Mountain J. Math.* **2** (1972), 159–168.

[Ya] E. Yalçin, Set covering and Serre's theorem on the cohomology algebra of a p-group, *J. Algebra* **245** (2001), 50–67.

(Received March 3, 2003)