TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 334, Number 1, November 1992

SUBGROUP CONDITIONS FOR GROUPS ACTING FREELY ON PRODUCTS OF SPHERES

JUDITH H. SILVERMAN

ABSTRACT. Let d and h be integers such that either $d \geq 2$ and $h = 2^d - 1$, or $d = 4$ and $h = 5$. Suppose that the group $\mathscr{G}$ contains an elementary-abelian 2-subgroup E_d of rank d with an element σ of order h in its normalizer. We show that if $\mathscr{G}$ admits a free and $\mathbf{F}_2$-cohomologically trivial action on $(S^n)^d$, then some nontrivial power of σ centralizes E_d.

The cohomology ring $H^*(E_d; \mathbf{F}_2) \simeq \mathbf{F}_2[y_1, \dots, y_d]$ is a module over the Steenrod algebra $\mathscr{A}(2)$. Let $\theta \in \mathbf{F}_2[y_1, \dots, y_d]$, and let $c \geq d-2$ be an integer. We show that θ divides $Sq^{2^i}(\theta)$ in the polynomial ring for $0 \leq i \leq c \Leftrightarrow \theta = \tau^{2^{c-d+3}}\pi$, where τ divides $Sq^{2^i}(\tau)$ for $0 \leq i \leq d-3$ and π is a product of linear forms.

PART I. PRELIMINARIES

1. INTRODUCTION

Suppose that the group $\mathscr{G}$ acts freely and $\mathbf{F}_2$-cohomologically trivially on a finite complex $X \sim_2 (S^n)^d$ (that is, X has the mod-2 cohomology of the Cartesian product $(S^n)^d$). A theorem due to Carlsson [Car 80] states that all elementary-abelian 2-subgroups of $\mathscr{G}$ have rank $\leq d$. The purpose of this paper is to find constraints on the normalizers of any rank-d elementary-abelian 2-subgroups E_d of $\mathscr{G}$. Note that if σ is an element of the normalizer $N_G(E_d)$, then the group generated by σ and E_d is a semidirect product $\langle\sigma\rangle \ltimes_\tau E_d$ over some homomorphism $\tau: \langle\sigma\rangle \to \mathrm{Aut}(E_d)$; E_d sits inside this group as a normal subgroup. Since $E_d \simeq (\mathbf{F}_2)^d$ as abelian groups, one may think of τ as a degree-d representation of $\langle\sigma\rangle$ over $\mathbf{F}_2$; if no nontrivial power of σ is in the centralizer of E_d, then the representation τ is faithful. We have the following:

Theorems III.5 and III.11 (Main Theorem). *Let d and h be integers such that either $d \geq 2$ and $h = 2^d - 1$, or $d = 4$ and $h = 5$. Suppose that the group $\mathscr{G}$ contains a semidirect product $G \simeq \mathbf{Z}/(h) \ltimes_\tau E_d$, where E_d is an elementary-abelian 2-group and τ is a faithful irreducible degree-d representation of $\mathbf{Z}/(h)$ over $\mathbf{F}_2$. Then $\mathscr{G}$ does not admit free, $\mathbf{F}_2$-cohomologically trivial actions on any finite complex $X \sim_2 (S^n)^d$ for any value of n (if $(d, h) = (4, 5)$, one requires that n not be of the form $2^l \cdot 5 - 1$).*

Received by the editors September 28, 1990.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 55M35, 55S10.
Key words and phrases. Steenrod algebra, free group actions.

If $(d, h) = (2, 3)$ or $(3, 7)$, then in fact $\mathscr{G}$ admits no such actions on any $X \sim_2 (S^n)^l$ for any $l \geq d$; see [Oli78 and Car81] for simple proofs of these theorems for the case $(d, h) = (2, 3)$ and the cases $(d, h) = (2, 3)$ and $(d, h) = (3, 7)$, respectively.

I thank Gunnar Carlsson for suggesting this question and for many helpful conversations. I am also grateful to the referee for pointing out that the groups $\mathbf{Z}/(2^d - 1) \ltimes_\tau E_d$ occur in the finite simple groups $PSL_2(\mathbf{F}_{2^d})$ as normalizers of the 2-Sylow subgroup, and consequently that there are an infinite number of *simple* groups of rank d not acting freely on $X \sim_2 (S^n)^d$.

2. Notation

From now on, we write k for the field of two elements $\mathbf{F}_2$. Let $L \supseteq K \supseteq k$ be field extensions, and let $\mathscr{C} = L[z_1, \dots, z_d]$ be a graded polynomial algebra over L on generators of degree 1. We denote the module of homogeneous elements of degree m by $\mathscr{C}_{(m)}$. Henceforth, all polynomials under discussion will be assumed to be homogeneous. The degree of a homogeneous polynomial ϕ is denoted by $\deg(\phi)$, and its degree as a polynomial in the single variable z_i by $\deg_i(\phi)$. Let $\mathrm{Mon}(\mathscr{C}) \subset \mathscr{C}$ be the set of monomials of $\mathscr{C}$ with coefficient 1. Any polynomial $0 \neq \phi \in \mathscr{C}$ is uniquely a sum $\phi = \sum\{f_\mu \mu | \mu \in \mathrm{Mon}(\phi)\}$ where $0 \neq f_\mu \in L$ and $\mathrm{Mon}(\phi) \subset \mathrm{Mon}(\mathscr{C})$. The elements of $\mathrm{Mon}(\phi)$ are the *monomials* of ϕ. We write $\partial/\partial z_i$ for the familiar derivations of $L[z_1, \dots, z_t]$. Since $\mathrm{char}(L) = 2$, we have the following useful characterizations of the squares of $L[z_1, \dots, z_t]$:

$$\text{(1)} \quad \phi \in \mathscr{C} \text{ is a square} \Leftrightarrow \partial(\phi)/\partial z_i = 0 \quad \textit{for } 1 \leq i \leq d \Leftrightarrow \mu \text{ is a square for all } \mu \in \mathrm{Mon}(\phi).$$

Let $\mathscr{R}$ be a graded K-subalgebra of $\mathscr{C}$ and $\mathrm{Mat}_n(\mathscr{R})$ the ring of $(n \times n)$-matrices over $\mathscr{R}$. We denote the determinant of a matrix $\mathscr{A} \in \mathrm{Mat}_n(\mathscr{R})$ by $\delta(\mathscr{A})$. A matrix $\mathscr{A} \in \mathrm{Mat}_n(\mathscr{R})$ is *diagonalizable over* k if the matrix $\mathscr{E}^{-1}\mathscr{A}\mathscr{E}$ is diagonal for some invertible matrix $\mathscr{E} \in \mathrm{Mat}_n(k)$, or equivalently, if $k^n \subset \mathscr{R}^n$ has a k-basis consisting of eigenvectors of $\mathscr{A}$ viewed as a linear transformation on $\mathscr{R}^n$.

It is also convenient to introduce the following notation:

Notation. Let $\{\phi_1, \dots, \phi_s\}$ be polynomials of $\mathscr{R}$. Then $\mathscr{I}\{\phi_1, \dots, \phi_s\}$ is the $\mathscr{R}$-ideal generated by the ϕ_i, $\mathscr{A}\{\phi_1, \dots, \phi_s\}$ is the subalgebra they generate, and $\mathscr{V}\{\phi_1, \dots, \phi_s\} \subset \mathscr{R}$ is the K-vector subspace they span.

Definition I.1. A set of (homogeneous) elements $\mathscr{S} = \{\phi_1, \dots, \phi_s\} \subset \mathscr{R}_{\geq 1}$ is an *independent set of* s *elements* if for each i, ϕ_i is not a 0-divisor in $\mathscr{R}/\mathscr{I}_{i-1}$, where $\mathscr{I}_0 = 0$ and $\mathscr{I}_j = \mathscr{I}\{\phi_1, \dots, \phi_{j-1}\}$ for $1 \leq j \leq s-1$. If $\deg(\phi_1) = \deg(\phi_2) = \cdots = \deg(\phi_s) = m$, then $\mathscr{S}$ is a *level independent set of degree* m.

It is proven in [Ser65a], where independent sets are referred to as $\mathscr{R}$-suites, that the above condition is independent of the order of the ϕ_i's. In particular, if $\rho\phi_i \in \mathscr{I}\{\phi_j | j \neq i\}$ for some $\rho \in \mathscr{R}$, then in fact the coefficient $\rho \in \mathscr{I}\{\phi_j | j \neq i\}$. The following consequence will be used repeatedly:

Fact I.2. 1. *Let* $\mathscr{S} = \{\phi_1, \dots, \phi_s\} \subset \mathscr{R}$ *be an independent set, and suppose that* $\sum_{i=1}^s \alpha_i \phi_i = 0$ *for some* $\alpha_1, \dots, \alpha_s \in \mathscr{R}$. *If for some* i *we have* $\deg(\alpha_i) < \deg(\phi_j)$ *for all* $j \neq i$, *then* $\alpha_i = 0$.

2. *Let* $\mathcal{T} = \{\psi_1, \dots, \psi_s\} \subset \mathcal{R}$ *be a level independent set of degree* m, *and suppose that* $\mathcal{M} \in \mathrm{Mat}(\mathcal{R}_{(n)})$ *is a matrix for which* $\mathcal{M}(\psi_1, \dots, \psi_s)^T = 0$ *or* $(\psi_1, \dots, \psi_s)\mathcal{M} = 0$. *Then either* $\mathcal{M} = 0$ *or* $n \geq m$. *In particular, if* $\sum_{i=1}^{s} \beta_i \psi_i = 0$ *for some* $\beta_1, \dots, \beta_s \in \mathcal{R}$ *of degree* n, *then either* $n \geq m$ *or* $\beta_i = 0$ *for all* i.

Definition I.3. We say a set of (homogeneous) elements $\mathcal{S} = \{\phi_1, \dots, \phi_s\} \subset \mathcal{R}$ is an *s-element homogeneous system of parameters* (*h.s.o.p.*) if $\mathcal{R}$ is a finitely-generated module over $\mathcal{A}\{\phi_1, \dots, \phi_s\}$. If $\deg(\phi_1) = \deg(\phi_2) = \cdots = \deg(\phi_s) = m$, we say $\mathcal{S}$ is a *level system of parameters* (*l.s.o.p.*) *of degree* m.

From [Ser65a], we have

Proposition I.4. *Let* $\mathcal{R} \subset \mathcal{C} = L[z_1, \dots, z_d]$ *be a* K*-subalgebra such that* $\mathcal{C}$ *is finitely generated as an* $\mathcal{R}$*-module. Then*

1. *no independent set of* $\mathcal{R}$ *has more than* d *elements,*
2. *for* $1 \leq s \leq d$, *any* s*-element independent set* (*resp. h.s.o.p.*) *of* $\mathcal{R}$ *is an* s*-element independent set* (*resp. h.s.o.p.*) *of* $\mathcal{C}$, *and*
3. *the* d*-element independent sets of* $\mathcal{R}$ *are precisely the* d*-element h.s.o.p.'s of* $\mathcal{R}$.

3. Cohomology of a twisted product

Let $\mathcal{G}$ be a group, $E_d \subset \mathcal{G}$ an elementary-abelian 2-subgroup of rank d, and $N_{\mathcal{G}}(E_d)$ the normalizer of E_d in $\mathcal{G}$, acting on E_d by conjugation. Suppose that $N_{\mathcal{G}}(E_d)$ contains an element η of odd order h, no nontrivial power of which acts trivially on E_d. Let $H = \langle \eta \rangle$, and define G to be $\langle \eta, E_d \rangle$, the group generated by η and E_d.

Notation. We say $G = \langle \eta, E_d \rangle$ is *of type* I if $d \geq 2$ and $h = 2^d - 1$, and *of type* II if $d = 4$ and $h = 5$.

The main theorem states that if G is of type I (resp. II), then the larger group $\mathcal{G}$ admits no free, k-cohomologically trivial action on any space $X \sim_2 (S^n)^d$, for any n (resp. for any n not of the form $2^l \cdot 5 - 1$). The method of proof is to show that even the subgroup G admits no such actions. In fact, $\mathcal{G}$ itself drops out of the picture and all computations take place within the cohomology of the subgroup G. Much of the discussion holds for all groups of the form $\langle \eta, E_d \rangle$, with no restrictions on d and h except those implicit in the condition on η. We will only restrict to groups of types I and II where necessary.

Following the approach of [Car81], we consider the cohomology algebra $H^*(G)$ of G, defined to be the cohomology (with k-coefficients) of the classifying space BG of G. As mentioned above, the group G may be regarded as a semidirect product $H \ltimes_\tau E_d$ for a suitable irreducible faithful representation $\tau: H \to Gl_d(k)$. There is a well-known isomorphism of graded k-algebras

$$H^*(E_d) \simeq k[y_1, \dots, y_d],$$

where $k[y_1, \dots, y_d]$ is the polynomial algebra on d generators $y_1, \dots, y_d$ of degree 1. The representation τ induces an action of H on $k[y_1, \dots, y_d]$, determined by multiplicity by its restriction ρ to $H^1(E_d) \simeq k[y_1, \dots, y_d]_{(1)}$, which is isomorphic to k^d as a k-vector space. The matrix of $\rho(\eta)$ is the transpose of the matrix corresponding to $\tau(\eta)$. It follows easily from the Hochschild-Serre spectral sequence for group extensions that

$$H^*(H \ltimes_\tau E_d) \simeq (k[y_1, \dots, y_d])^H,$$

the ring of invariants under the action of H [Car81]. In the next section we discuss Carlsson's method for working with this invariant subalgebra, which is difficult to study directly.

4. Representation theory

Let h be an odd number and let d be the order of 2 in $\mathbf{Z}/(h)$. Then the field extensions $k(\zeta)$ and $k(\omega)$ of k obtained by adjoining a primitive hth root of unity and a primitive (2^d-1)th root of unity respectively are isomorphic to each other and to the field of 2^d elements. We denote this field by $\hat{k}$. Note that ω is a generator of the multiplicative group of units $\hat{k}^\times$. The Galois group Γ of the extension $\hat{k}/k$ is a cyclic group of order d, generated by the Frobenius map $z \mapsto z^\gamma = z^2$.

Now let $H = \langle\eta\rangle$ be a cyclic group of order h acting irreducibly, as in the previous section, on $k[y_1, \dots, y_d]$. This action extends by $\hat{k}$-linearity to $\hat{k} \otimes k[y_1, \dots, y_d] \simeq \hat{k}[y_1, \dots, y_d]$, and the dimension-$d$ representation on $\hat{k}[y_1, \dots, y_d]_{(1)} \simeq \hat{k}^d$ is diagonalizable, as the larger field $\hat{k}$ contains the hth roots of unity. More precisely, one can show that there is an additive basis $\{x_0, \dots, x_{d-1}\}$ for $\hat{k}[y_1, \dots, y_d]_{(1)}$—hence a multiplicative basis for $\hat{k}[y_1, \dots, y_d]$—consisting of eigenvectors of the H-action, such that

$$\eta(x_i) = \zeta^{2^i} x_i \quad \text{for } 0 \le i \le d-1$$

for some appropriate primitive hth root ζ of unity (see e.g. [CS]). Henceforth we regard ζ as fixed, and choose the primitive (2^d-1)th root ω so that $\zeta = \omega^{(2^d-1)/h}$. All monomials in the $\{x_0, \dots, x_{d-1}\}$ are eigenvectors of H. It is convenient to extend the action of the Galois group Γ of $\hat{k}/k$ to all of $\hat{k}[x_0, \dots, x_{d-1}] = \hat{k}[y_1, \dots, y_d]$ via

$$c^\gamma = c^2, \quad c \in \hat{k}; \qquad x_i^\gamma = x_{i+1}, \quad 0 \le i \le d-1,$$

where the subscripts are read, here and throughout, as integers modulo d. One can check that the inclusion

$$\iota\colon k[y_1, \dots, y_d] \to \hat{k}[x_0, \dots, x_{d-1}]$$

maps $k[y_1, \dots, y_d]$ isomorphically onto $(\hat{k}[x_0, \dots, x_{d-1}])^\Gamma$, the invariant subalgebra. In particular, the 2^d-1 linear elements of $(\hat{k}[x_0, \dots, x_{d-1}])^\Gamma$ are determined by the coefficient of x_0; they are given by

$$l_i \stackrel{\text{def}}{=} \omega^i x_0 + \omega^{2i} x_1 + \cdots + \omega^{2^{d-1}i} x_{d-1} = \sum_{j=0}^{d-1} \omega^{2^j i} x_j, \qquad 0 \le i \le d-1.$$

From now on, we use the following abbreviations:

$$\mathscr{L} = k[y_1, \dots, y_d]_{(1)}, \quad \widehat{\mathscr{L}} = \hat{k}[x_0, \dots, x_{d-1}]^H_{(1)} = \iota(\mathscr{L}),$$
$$\mathrm{Mon}(Y) = \mathrm{Mon}(k[y_1, \dots, y_d]), \quad \mathrm{Mon}(X) = \mathrm{Mon}(\hat{k}[x_0, \dots, x_{d-1}]),$$

and write $\mathrm{Mon}(X)^H$ for the elements of $\mathrm{Mon}(X)$ which are fixed by the action of H on $\hat{k}[x_0, \dots, x_{d-1}]$.

5. Invariant theory

To discuss the H-invariants of $\hat{k}[x_0, \dots, x_{d-1}]$, we introduce some terminology.

Notation. As in [CS], we refer to monomials of the form $x_i^{2^j}$ as "atoms." Every monomial $\mu \in \hat{k}[x_0, \dots, x_{d-1}]$ can be expressed uniquely as a product of distinct atoms, which we call the *atoms of* μ. Campbell and Selick define the weight function $w: \mathrm{Mon}(X) \to \mathbf{Z}/(2^d - 1)$ by declaring the weight of each atom $x_i^{2^j}$ to be $w(x_i^{2^j}) = 2^{i+j}$, and requiring that w be multiplicative. Evidently one has $w(\prod_{i=0}^{d-1} x_i^{e_i}) = \sum_{i=0}^{d-1} 2^i e_i$. We now define the *weight vector* $W(\mu)$ of a monomial with atomic decomposition $\mu = \prod_{l=1}^{n(\mu)} x_{i_l}^{2^{j_l}}$ to be the d-tuplet $(\beta_0(\mu), \dots, \beta_{d-1}(\mu))$, where $\beta_t(\mu)$ is the number of atoms of μ with weight 2^t (cf. [Woo86]). Clearly $w(\mu) \equiv \sum_{t=0}^{d-1} \beta_t(\mu) 2^t \pmod{2^d - 1}$. For $\phi = \sum c_\mu \mu$ a polynomial, $w \in \mathbf{Z}/(2^d - 1)$, and $W = (\beta_0, \dots, \beta_{d-1}) \in \mathbf{N}^d$, we define $\phi_w = \sum \{c_\mu \mu | w(\mu) = w\}$ and $\phi_W = \sum \{c_\mu \mu | W(\mu) = W\}$. If $\phi = \phi_W$, we say ϕ is *weight-vector pure* of weight-vector W; similarly, ϕ is *weight-pure* of weight w of $\phi = \phi_w$.

We now describe the H-invariant subalgebra of $\hat{k} \otimes k[y_1, \dots, y_d]$ in the basis $\{x_0, \dots, x_{d-1}\}$.

Lemma I.5 [Car81]. *Let* $\mu = x_0^{e_0} \cdots x_{d-1}^{e_{d-1}}$. *Then* μ *is an* H*-eigenvector with eigenvalue* $\zeta^{w(\mu)}$. *In particular,* μ *is* H*-invariant* $\Leftrightarrow w(\mu) = 0$. *A polynomial* $\phi \in \hat{k}[x_0, \dots, x_{d-1}]$ *is* H*-invariant* $\Leftrightarrow$ *each of its monomials is* H*-invariant; the invariant subalgebra* $\hat{k}[x_0, \dots, x_{d-1}]^H$ *is the subalgebra generated by the invariant monomials* $\mathrm{Mon}(X)^H$.

Let $n \in \mathbf{N}$. As usual, we write $\alpha(n)$ for the number of 1's in the dyadic representation of n. Let

$$\nu \stackrel{\text{def}}{=} \min\{\alpha(n) | n \equiv 0 \pmod{h}\}$$

be the minimum number of 1's in the dyadic representation of any multiple of h. Since $2^d - 1 \equiv 0 \pmod{h}$, we have $\nu \leq d$. In fact, it is not hard to see that $\nu = \alpha(n)$ for some multiple n of h with $1 \leq n \leq 2^d - 1$. From Lemma I.5 it follows that:

Corollary I.6 (cf. [Car81]). 1. *Any* H*-invariant monomial is composed of at least* ν *atoms. In particular, we have* $\hat{k}[x_0, \dots, x_{d-1}]^H_{(j)} = 0$ *for* $j < \nu$.

2. *In degree* ν, *we have* $\hat{k}[x_0, \dots, x_{d-1}]^H_{(\nu)} \neq 0$.

Proof. Let $\mu \in \mathrm{Mon}(X)^H$. As the integer $\sum_{t=0}^{d-1} \beta_t(\mu) 2^t \equiv w(\mu) \pmod{2^d - 1}$, we have that $\sum_{t=0}^{d-1} \beta_t(\mu) 2^t$ is a multiple of h by Lemma I.5, and thus

$$\nu \leq \alpha\left(\sum_{t=0}^{d-1} \beta_t(\mu) 2^t\right) \leq \sum_{t=0}^{d-1} \alpha(\beta_t(\mu) 2^t) = \sum_{t=0}^{d-1} \alpha(\beta_t(\mu)) \leq \sum_{t=0}^{d-1} \beta_t(\mu),$$

the last term being the number of atoms of μ. This proves this first statement. Now let n, $1 \le n \le 2^d - 1$, be a multiple of h such that $\nu = \alpha(n)$; write $n = \sum_{t=0}^{d-1} \varepsilon_i 2^i$ with $\varepsilon_i \in \{0, 1\}$. Then the monomial $x_0^{\varepsilon_0} \cdots x_{d-1}^{\varepsilon_{d-1}}$ is H-invariant and has degree ν. □

Suppose now that $\mu \in \mathrm{Mon}(X)^H$ is the square of some monomial $\lambda \in \mathrm{Mon}(X)$. Then $\beta_{t-1}(\lambda) = \beta_t(\mu)$ for all t, where again the subscripts are read modulo d, so that

$$w(\lambda) = \sum_{t=0}^{d-1} \beta_t(\lambda) 2^t = 2^{-1} \sum_{t=0}^{d-1} \beta_t(\mu) 2^t = 2^{-1} w(\mu).$$

Since 2 is a unit in $\mathbf{Z}/(2^d - 1)$, this means that $w(\lambda) = 0$, so that $\lambda \in \mathrm{Mon}(X)^H$. In view of the previous lemma and equation (1), we have

Lemma I.7 (cf. [Car81]). *Suppose* $\theta \in (\hat{k}[x_0, \ldots, x_{d-1}])^H$ *satisfies* $\theta = \psi^2$ *for some* $\psi \in \hat{k}[x_0, \ldots, x_{d-1}]$. *Then* $\psi \in (\hat{k}[x_0, \ldots, x_{d-1}])^H$; θ *is a square in* $(\hat{k}[x_0, \ldots, x_{d-1}])^H$.

6. Steenrod algebra

Recall that the cohomology ring of any group is naturally an algebra over the mod-2 Steenrod algebra $\mathscr{A}(2)$. In particular, $k[y_1, \ldots, y_d] \simeq H^*(E_d)$ and $(k[y_1, \ldots, y_d])^H \simeq H^*(H \ltimes_\tau E_d)$ are $\mathscr{A}(2)$-algebras. The action of $\mathscr{A}(2)$ on $k[y_1, \ldots, y_d]$ is determined by the Cartan formula and the requirements

$$Sq^1(y_j) = y_j^2; \qquad Sq^i(y_j) = 0 \quad \text{for } i \ge 1;$$

the action on $H^*(H \ltimes_\tau E_d)$ agrees with the restriction of this action to the invariant subalgebra $(k[y_1, \ldots, y_d])^H$. We now recall a few pertinent facts about $\mathscr{A}(2)$ and its action on $k[y_1, \ldots, y_d]$. Let $\phi \in k[y_1, \ldots, y_d]$ and $a \in \mathbf{N}$.

Fact I.8. 1. *The algebra* $\mathscr{A}(2)$ *is generated by the* Sq^{2^i}; *in particular,* Sq^a *may be expressed in terms of* $\{Sq^{2^i} | 2^i \le a\}$.

2. *We have*

$$Sq^{2^i}(\phi^{2^j}) = \begin{cases} (Sq^{2^{i-j}}\phi)^{2^j}, & i \ge j, \\ 0, & i < j. \end{cases}$$

3. Sq^{2^i} *acts as a derivation on* (2^i)*th powers.*
4. $Sq^a(\phi) = 0$ *for* $a > \deg(\phi)$.

As in [Car81], we recall the definition of the Milnor primitives

$$Q_1 = Sq^1, \qquad Q_{i+1} = [Sq^{2^i}, Q_i],$$

and define $Q_0 : k[y_1, \ldots, y_d] \to k[y_1, \ldots, y_d]$ by the requirements that $Q_0(y_j) = y_j$ and that Q_0 be a derivation.

Proposition I.9 [AW80].

1. $Q_i = \sum_{j=1}^d y_j^{2^i} \partial/\partial y_j$ *for* $i \ge 0$; *in particular,* Q_i *is a derivation for all* i.
2. *For* $i \ge d$, *there exist polynomials* $\phi_{ij} \in k[y_1, \ldots, y_d]$, $0 \le j \le d-1$, *such that* $Q_i = \sum_{j=0}^{d-1} \phi_{ij} Q_j$.
3. $Q_0(z) = 0$ *when* $\deg(z)$ *is even*; $Q_0(z) = z$ *when* $\deg(z)$ *is odd.*

Proposition I.10 [AW80]. *If $\theta \in k[y_1, \dots, y_d]$ (resp. $(k[y_1, \dots, y_d])^H$) satisfies $Q_i(\theta) = 0$ for $0 \le j \le d-1$, then θ is the square of an element in $k[y_1, \dots, y_d]$ (resp. $(k[y_1, \dots, y_d])^H$).*

Following [Car81], we extend the action of $\mathscr{A}(2)$ by $\hat{k}$-linearity to all of $\hat{k}[x_0, \dots, x_{d-1}]$. The new action still satisfies the Cartan formula and the condition that $Sq^a(f) = 0$ for $a > \deg(f)$, but it is no longer true that $Sq^a(f) = f^2$ whenever $\deg(f) = a$. Carlsson characterizes the new action as follows:

Proposition I.11 [Car81]. *With the notation as above, the action of $\mathscr{A}(2)$ on $\hat{k}[x_0, \dots, x_{d-1}]$ is determined by $\hat{k}$-linearity, the Cartan formula, and the condition that $Sq^1(x_j) = x_{j-1}^2$.*

It is straightforward to verify inductively that $Q_j(x_i) = x_{i-j}^{2^j}$ for $j \ge 1$. The Q_j being derivations, we have that

$$Q_j = \sum_{i=0}^{d-1} x_{i-j}^{2^j} \frac{\partial}{\partial x_i}. \tag{2}$$

We summarize the statements "$Q_j = \sum_{i=0}^{d-1} x_{i-j}^{2^j} \partial/\partial x_i$, $0 \le j \le d-1$" in matrix notation as follows:

$$\begin{pmatrix} x_0 & x_1 & \dots & x_{d-1} \\ x_{d-1}^2 & x_0^2 & \dots & x_{d-2}^2 \\ \vdots & \vdots & \vdots & \vdots \\ x_1^{2^{d-1}} & x_2^{2^{d-1}} & \dots & x_0^{2^{d-1}} \end{pmatrix} \begin{pmatrix} \frac{\partial(\theta)}{\partial x_0} \\ \frac{\partial(\theta)}{\partial x_1} \\ \vdots \\ \frac{\partial(\theta)}{\partial x_{d-1}} \end{pmatrix} = \begin{pmatrix} Q_0(\theta) \\ Q_1(\theta) \\ \vdots \\ Q_{d-1}(\theta) \end{pmatrix} \quad \text{for } \theta \in \hat{k}[x_0, \dots, x_{d-1}]. \tag{3}$$

Note that if μ is a monomial, then $x_{i-j}^{2^j}(\partial\mu/\partial x_i) = \mu(x_{i-j}^{2^j}/x_i)$ accordingly as x_i is or is not an atom of μ. As $w(x_{i-j}^{2^j}) = 2^i = w(x_i)$, we see that $W(Q_j(\mu)) = W(\mu)$ provided $Q_j(\mu) \ne 0$. Likewise, of course, $w(Q_j(\mu)) = w(\mu)$.

Suppose now that $\mathscr{R}$ is a k- or $\hat{k}$-algebra having an $\mathscr{A}(2)$-action, e.g. $\mathscr{R} = k[y_1, \dots, y_d]$, $\hat{k}[x_0, \dots, x_{d-1}]$, or their H-invariant subalgebras. Recall from §2 the definition of independent sets, h.s.o.p.'s and l.s.o.p.'s of $\mathscr{R}$.

Definition I.12. Let $\mathscr{S} = \{\phi_1, \dots, \phi_s\} \subset \mathscr{R}$ be an independent set or an h.s.o.p. $\mathscr{S}$ is *$\mathscr{A}(2)$-invariant* (resp. *Q-invariant*) if the ideal $\mathscr{I}\{\phi_1, \dots, \phi_s\}$ is closed under the action of $\mathscr{A}(2)$ (resp. of the Q_i, $1 \le i < \infty$).

Note that $\mathscr{S}$ as above is Q-invariant if the ideal $\mathscr{I}\{\phi_1, \dots, \phi_s\}$ is closed under Q_i for $1 \le i \le d-1$. As $k[y_1, \dots, y_d]$ is finitely generated over the algebra $(k[y_1, \dots, y_d])^H$, one may easily see that any $\mathscr{A}(2)$-invariant l.s.o.p. of $(k[y_1, \dots, y_d])^H$ is also an $\mathscr{A}(2)$-invariant l.s.o.p. of $k[y_1, \dots, y_d]$, and maps via $\imath$ to an $\mathscr{A}(2)$-invariant l.s.o.p. of $\hat{k}[x_0, \dots, x_{d-1}]$; similarly for Q-invariant l.s.o.p.'s.

7. Outline of the argument

We now outline the proof of the main theorem. In [Car81], Carlsson proves the following.

Theorem I.13 [Car80, Car81]. *Suppose $G = H \ltimes_\tau E_d$ acts freely and $\mathbf{Z}/(2)$-cohomologically trivially on a finite complex $X \sim_2 (S^n)^l$. Then $H^*(G) = (k[y_1, \ldots, y_d])^H$ contains an l-element $\mathscr{A}(2)$-invariant l.s.o.p. in degree $n+1$.*

This l.s.o.p. arises as follows: suppose that G acts on X as in Theorem I.13. Consider the Serre spectral sequence for the fibration $X \to EG \times_G X \to BG$, where EG denotes a contractible space on which G acts freely, and BG the classifying space of G. Let $y_j \in H^n(X)$ be the generators of the exterior algebra $H^*(X) \simeq H^*((S^n)^l)$, and let $\theta_j \in H^{n+1}(BG) \simeq H^{n+1}(G)$ be their transgressions in the spectral sequence. Then Carlsson shows that the set $\{\theta_1, \ldots, \theta_l\}$ forms an $\mathscr{A}(2)$-invariant l.s.o.p. for $H^*(G)$ in degree $n+1$.

To prove the main theorem using Theorem I.13, our approach will be to show that the algebras $(k[y_1, \ldots, y_d])^H$ possess no $\mathscr{A}(2)$-invariant l.s.o.p.'s with d elements in the relevant degrees.

Notation. For G as above and integers l and m, write $P(G, l, m)$ for the following statement: Any $\mathscr{A}(2)$-invariant l.s.o.p. of $(k[y_1, \ldots, y_d])^H$ of degree m with l elements consists entirely of squares.

Some results of [Car81] can be paraphrased to say:

Proposition I.14. *Let $m = 2^t n$, where n is odd. Suppose $P(G, l, 2^i n)$ is true for $1 \le i \le t$. Then in fact $(k[y_1, \ldots, y_d])^H$ has no $\mathscr{A}(2)$-invariant l.s.o.p.'s with l elements in degree m.*

Proposition I.14 is proven by showing, first, that $(k[y_1, \ldots, y_d])^H$ has no $\mathscr{A}(2)$-invariant l.s.o.p.'s in odd degrees, and second, that the square roots of an $\mathscr{A}(2)$-invariant l.s.o.p. consisting entirely of squares themselves form an $\mathscr{A}(2)$-invariant l.s.o.p. In what follows, we demonstrate that if G is a group of type I (resp. II), then $P(G, d, m)$ is true for all m (resp. for all m not of the form $2^t \cdot 5$). This together with Theorem I.13 and Proposition I.14 proves the main theorem.

The idea behind the proof that $P(G, d, m)$ holds is as follows. Let $\mathscr{S} = \{\theta_1, \ldots, \theta_d\}$ be a d-element $\mathscr{A}(2)$-invariant l.s.o.p. for $(k[y_1, \ldots, y_d])^H$ in degree m, with m as in the main theorem. Carlsson observed that $\mathscr{A}(2)$-invariance allows us to write, for all $j = 1, 2, \ldots, d$ and $t = 0, 1, \ldots, d-1$,

$$Q_t(\theta_j) = \sum_{k=1}^{d} q(t)_{jk} \theta_k \tag{4}$$

for some $q(t)_{jk} \in k[y_1, \ldots, y_d]^H_{(2^t-1)}$. Let $\mathscr{Q}(t)$, $0 \le t \le d-1$, be the matrices $(q(t)_{jk}) \in \mathrm{Mat}_d((k[y_1, \ldots, y_d])^H)$. The goal is to prove that $\mathscr{Q}(t) = 0$ for all $0 \le t \le d-1$; this will imply, by Proposition I.10, that each element of $\mathscr{S}$ is a square. When G is of type I, this is accomplished fairly simply by studying the elements $q(t)_{jk}$. When G is of type II, the argument goes as follows: note that any k-basis for the k-linear span $\mathscr{V}\{\theta_1, \ldots, \theta_d\}$ is itself an H-invariant $\mathscr{A}(2)$-invariant l.s.o.p., since the ideal and subalgebra it generates are the same as those generated by $\{\theta_1, \ldots, \theta_d\}$. Thus to each basis $\mathscr{S}'$ of $\mathscr{V}\{\theta_1, \ldots, \theta_d\}$ we may associate the matrices $\mathscr{Q}_{\mathscr{S}'}(t)$ as above. Our approach is to show that $\mathscr{V}\{\theta_1, \ldots, \theta_d\}$ has a basis $\mathscr{S}'$ for which the associated matrices are diagonal, and then, by studying the possible eigenvectors of such matrices, to verify that these diagonal matrices are in fact 0.

In Part II we prove some propositions concerning the action of $\mathscr{A}(2)$ on our polynomial algebras and the diagonalization of matrices, which we use in Part III to prove the main theorem. In fact, when the group G is of type I, the proof that $P(G, d, m)$ holds relies only on the results of §8; the rest of the results in Part II, while interesting in their own right, are for our purposes necessary only for the discussion of groups of type II.

PART II. TECHNICAL RESULTS

8. JOINT KERNELS OF THE Q_i. I

Proposition I.10 says that a polynomial $\phi \in k[y_1, \dots, y_d]$ is a square if $Q_i(\phi) = 0$ for $0 \le i \le d-1$. In this section, we discuss certain polynomials ψ which vanish under some, but not all, of the Q's. Namely:

Definition II.1. For $1 \le s \le d-1$, let

$$K_s = \{\phi \in k[y_1, \dots, y_d]_{(2^{s+1}-1)} | Q_t(\phi) = 0 \text{ for } 1 \le t \le s\},$$
$$K_s^H = K_s \cap (k[y_1, \dots, y_d])^H.$$

In order to discuss K_s and K_s^H, we introduce the following notation:

Definition II.2. For $1 \le s \le d-1$, let

$$\mathscr{T}_s = \{\{y_{i_0}, \dots, y_{i_s}\} \mid i_t \ne i_{t'} \text{ for } t \ne t'\},$$
$$\widehat{\mathscr{T}_s} = \{\{x_{i_0}, \dots, x_{i_s}\} \mid i_t \ne i_{t'} \text{ for } t \ne t'\},$$
$$\widehat{\mathscr{T}_s}^H = \left\{\hat{\tau} \in \widehat{\mathscr{T}_s} \mid \sum_{j=0}^{s} 2^{i_j} \equiv 0 \ (\mathrm{mod}\ h)\right\}.$$

Note that $\widehat{\mathscr{T}_s}^H = \varnothing$ for $1 \le s \le \nu-2$, where $\nu = \min\{\alpha(m) | m \equiv 0 \ (\mathrm{mod}\ h)\}$ as in §5. Moreover, if $I = \{i_0, \dots, i_s\} \subset \{i_0, \dots, i_{d-1}\}$, then the set $\tau = \{x_{i_j} | i_j \in I\}$ belongs to $\widehat{\mathscr{T}_s}^H \Leftrightarrow \tau' = \{x_{i_k} | i_k \notin I\}$ belongs to $\widehat{\mathscr{T}}^H_{d-s-2}$, since

$$\sum_{i_j \in I} 2^{i_j} + \sum_{i_k \notin I} 2^{i_k} = \sum_{i=0}^{d-1} 2^i = 2^d - 1 \equiv 0 \quad (\mathrm{mod}\ h).$$

In particular, $\widehat{\mathscr{T}_t}^H = 0$ for $d - \nu \le t \le d-2$.

Definition II.3. Let $\tau = (\lambda_0, \dots, \lambda_s) \in \mathscr{T}_s$ or $\widehat{\mathscr{T}_s}$. Then $\mathscr{D}_Q(\tau)$ is the matrix

$$D_{\mathscr{Q}}(\tau) \overset{\text{def}}{=} \begin{pmatrix} \lambda_0 & \lambda_1 & \dots & \lambda_s \\ Q_1(\lambda_0) & Q_1(\lambda_1) & \dots & Q_1(\lambda_s) \\ \vdots & \vdots & \vdots & \vdots \\ Q_s(\lambda_0) & Q_s(\lambda_1) & \dots & Q_s(\lambda_s) \end{pmatrix},$$

and $\delta_Q(\tau)$ is the determinant $\delta(\mathscr{D}_Q(\tau))$.

Example. For $\hat{\tau} = \{x_{i_0}, \dots, x_{i_s}\} \in \widehat{\mathscr{T}_s}$, we have

$$\mathscr{D}_Q(x_{i_0}, \dots, x_{i_s}) = \begin{pmatrix} x_{i_0} & x_{i_1} & \dots & x_{i_s} \\ x_{i_0-1}^2 & x_{i_1-1}^2 & \dots & x_{i_s-1}^2 \\ \vdots & \vdots & \vdots & \vdots \\ x_{i_0-s}^{2^s} & x_{i_1-s}^{2^s} & \dots & x_{i_s-s}^{2^s} \end{pmatrix}.$$

Note that the weight function is constant along each column of $\mathscr{D}_Q(\hat{\tau})$. Therefore the polynomial $\delta_Q(\hat{\tau})$ is weight-vector pure of weight-vector $W(\hat{\tau}) = (a_0, \dots, a_{d-1})$, where $a_l = 1$ if $i_j = l$ for some j, and $a_l = 0$ otherwise. Clearly $W(\hat{\tau}_1) \neq W(\hat{\tau}_2)$ if $\tau_1 \neq \tau_2$. The polynomial $\delta_Q(\hat{\tau})$ is also of course weight-pure of weight $w = \sum_{j=0}^{s} w(x_{i_j}) = \sum_{j=0}^{s} 2^{i_j}$. In particular,

$$\delta_Q(\hat{\tau}) \in (\hat{k}[x_0, \dots, x_{d-1}])^H \Leftrightarrow \hat{\tau} \in \widehat{\mathscr{T}_s}^H. \tag{5}$$

Example. For $\tau = \{y_{i_0}, \dots, y_{i_s}\} \in \mathscr{T}_s$, the definition gives

$$\mathscr{D}_Q(y_{i_0}, \dots, y_{i_s}) = \begin{pmatrix} y_{i_0} & y_{i_1} & \dots & y_{i_s} \\ y_{i_0}^2 & y_{i_1}^2 & \dots & h_{i_s}^2 \\ \vdots & \vdots & \vdots & \vdots \\ y_{i_0}^{2^s} & y_{i_1}^{2^s} & \dots & y_{i_s}^{2^s} \end{pmatrix}.$$

It is well known that the determinant of this matrix is given by the product of all the nonzero linear forms in the $y_{i_0}, \dots, y_{i_s}$:

$$\delta_Q(y_{i_0}, \dots, y_{i_s}) = \prod \{\phi \mid \phi \in k[y_{i_0}, \dots, y_{i_s}]_{(1)}\}. \tag{6}$$

In [Woo86], Wood gives the following description of K_s:

Proposition II.4. *K_s is the linear span $\mathscr{V}\{\delta_Q(\tau) \mid \tau \in \mathscr{T}_s\}$.*

In §14, we will need the following corollary.

Corollary II.5. *Suppose $\phi \in K_s$. Then $Q_{s+1}(\phi) = \phi^2$.*

Proof. As Q_{s+1} and the squaring map are additive homomorphisms, it suffices to prove the corollary for $\phi = \delta_Q(\tau)$, where $\tau = (\lambda_0, \dots, \lambda_s) \in \mathscr{T}_s$. Applying the derivation Q_{s+1} one row at a time, we find that

(7)

$$Q_{s+1}(\delta_Q(\tau)) = \begin{vmatrix} Q_{s+1}(y_{i_0}) & \dots & Q_{s+1}(y_{i_s}) \\ Q_1(y_{i_0}) & \dots & Q_1(y_{i_s}) \\ \vdots & \vdots & \vdots \\ Q_s(y_{i_0}) & \dots & Q_s(y_{i_s}) \end{vmatrix} + \begin{vmatrix} y_{i_0} & \dots & y_{i_s} \\ Q_{s+1}(Q_1(y_{i_0})) & \dots & Q_{s+1}(Q_1(y_{i_s})) \\ \vdots & \vdots & \vdots \\ Q_s(y_{i_0}) & \dots & Q_s(y_{i_s}) \end{vmatrix}$$

$$+ \dots + \begin{vmatrix} y_{i_0} & \dots & y_{i_s} \\ Q_1(y_{i_0}) & \dots & Q_1(y_{i_s}) \\ \vdots & \vdots & \vdots \\ Q_{s+1}(Q_s(y_{i_0})) & \dots & Q_{s+1}(Q_s(y_{i_s})) \end{vmatrix}.$$

For $i \geq 2$, the ith matrix has ith row identically zero, so that its determinant vanishes. We see that

$$(8) \qquad Q_{s+1}(\delta_Q(\tau)) = \begin{vmatrix} y_{i_0}^{2^{s+1}} & \cdots & y_{i_s}^{2^{s+1}} \\ y_{i_0}^{2} & \cdots & y_{i_s}^{2} \\ \vdots & \vdots & \vdots \\ y_{i_0}^{2^s} & \cdots & y_{i_s}^{2^s} \end{vmatrix} = \begin{vmatrix} y_{i_0}^{2} & \cdots & y_{i_s}^{2} \\ \vdots & \vdots & \vdots \\ y_{i_0}^{2^s} & \cdots & y_{i_s}^{2^s} \\ y_{i_0}^{2^{s+1}} & \cdots & y_{i_s}^{2^{s+1}} \end{vmatrix} = \delta_Q(\tau)^2,$$

the equalities holding because in characteristic 2, squaring is a homomorphism and the order of a matrix's rows does not affect the value of the determinant. □

In order to study the invariant subspace K_s^H, we work in the larger field.

Definition II.6. For $1 \leq s \leq d-1$, let

$$\widehat{K}_s = \{\psi \in \hat{k}[x_0, \ldots, x_{d-1}]_{(2^{s+1}-1)} \mid Q_t(\psi) = 0 \text{ for } 1 \leq t \leq s\},$$
$$\widehat{K}_s^H = \widehat{K}_s \cap (\hat{k}[x_0, \ldots, x_{d-1}])^H.$$

One can easily check, along the lines of the previous proof, that

$$(9) \qquad \mathscr{V}\{\mathscr{D}_Q(\hat{\tau}) | \hat{\tau} \in \widehat{\mathscr{T}_s}\} \subset \widehat{K}_s.$$

In fact, the inclusion is an equality as we proceed to show. We need the following lemma.

Lemma II.7. *Let* $\tau = \{y_{i_0}, \ldots, y_{i_s}\} \in \mathscr{T}_s$. *Then* $\iota\delta_Q(\tau) \in \mathscr{V}\{\mathscr{D}_Q(\hat{\tau}) \mid \hat{\tau} \in \widehat{\mathscr{T}_s}\} \subset \widehat{K}_s$.

Proof. Write $y_{i_l} = \sum_{j=0}^{d-1} \zeta^{a_l 2^j} x_j$ for suitable a_l as in §4. Then

$$(10) \qquad \iota\delta_Q(\tau) = \begin{vmatrix} \sum_{j=0}^{d-1} \zeta^{a_0 2^j} x_j & \cdots & \sum_{j=0}^{d-1} \zeta^{a_s 2^j} x_j \\ \left(\sum_{j=0}^{d-1} \zeta^{a_0 2^j} x_j\right)^2 & \cdots & \left(\sum_{j=0}^{d-1} \zeta^{a_s 2^j} x_j\right)^2 \\ \vdots & \vdots & \vdots \\ \left(\sum_{j=0}^{d-1} \zeta^{a_0 2^j} x_j\right)^{2^s} & \cdots & \left(\sum_{j=0}^{d-1} \zeta^{a_s 2^j} x_j\right)^{2^s} \end{vmatrix}.$$

I claim that each column of the above matrix is a linear combination of the column vectors $(x_i, x_{i-1}^2, \ldots, x_{i-s}^{2^s})^T$; indeed, the jth column

$$\begin{pmatrix} \sum_{i=0}^{d-1} \zeta^{a_j 2^i} x_i \\ \left(\sum_{i=0}^{d-1} \zeta^{a_j 2^i} x_i\right)^2 \\ \vdots \\ \left(\sum_{i=0}^{d-1} \zeta^{a_j 2^i} x_i\right)^{2^s} \end{pmatrix} = \sum_{i=0}^{d-1} \zeta^{a_j 2^i} \begin{pmatrix} x_i \\ x_{i-1}^2 \\ \vdots \\ x_{i-s}^{2^s} \end{pmatrix}.$$

We can therefore express $\iota\delta_Q(\tau)$ as a linear combination of determinants of matrices with columns of the form $(x_i, x_{i-1}^2, \ldots, x_{i-s}^{2^s})^T$, and we may of course assume that the columns of each such matrix are distinct from each other. This says exactly that $\iota\delta_Q(\tau) \in \mathscr{V}\{\mathscr{D}_Q(\hat{\tau}) | \hat{\tau} \in \widehat{\mathscr{T}_s}\}$. □

The following corollary will be useful in the next section. Recall from §4 the notation $\mathscr{L}$ and $\widehat{\mathscr{L}}$.

Corollary II.8. *Let* $\tau_x = \{x_0, \dots, x_{d-1}\}$ *and* $\tau_y = \{y_1, \dots, y_d\}$. *Then* $\delta_Q(\tau_x) = \iota\delta_Q(\tau_y) = \prod\{\hat{l}_i | \hat{l}_i \in \widehat{\mathscr{L}}\}$.

Proof. As in equation (6), $\delta_Q(\tau_y) = \prod\{l_i | l_i \in \mathscr{L}\}$, so $\iota\delta_Q(\tau_y) = \prod\{\hat{l}_i | \hat{l}_i \in \widehat{\mathscr{L}}\}$. Since $\hat{\mathscr{T}}_d = \{\tau_x\}$, the lemma says that $0 \neq \iota\delta_Q(\tau_y) = c\delta_Q(\tau_x)$ for some $c \in \hat{k}$. As both $\iota\delta_Q(\tau_y)$ and $\delta_Q(\tau_x)$ are Γ-invariant, we see that $c = 1$. □

Lemma II.7 and Corollary II.8 actually give all that is needed of the structure of $\widehat{K}_s$, but for the sake of completeness we prove

Proposition II.9. $\widehat{K}_s = \mathscr{V}\{\mathscr{D}_Q(\hat{\tau}) \mid \hat{\tau} \in \widehat{\mathscr{T}_s}\}$.

Proof. By equation (9), we must show only that $\widehat{K}_s \subset \mathscr{V}\{\mathscr{D}_Q(\hat{\tau}) \mid \hat{\tau} \in \widehat{\mathscr{T}_s}\}$. Let $\phi \in \widehat{K}_s$ and let $W_1, \dots, W_n$ be the weight vectors corresponding to elements of $\mathrm{Mon}(\phi)$ as in §5. Since the Q_j preserve the weight-vector classes, it is evident that $Q_j(\phi_{W_i}) = 0$ for each $0 \leq j \leq s$ and $1 \leq i \leq n$. W.l.o.g., then, we may assume that ϕ is pure of weight vector W. In this case, let $\psi = \sum_{\gamma' \in \Gamma} \phi^{\gamma'}$. Now $\psi^{\gamma'} = \psi$ for all $\gamma' \in \Gamma$, so $\psi \in \iota k[y_1, \dots, y_d]$; clearly $\psi \in \iota K_s$. By Lemma II.7, $\psi \in \mathscr{V}\{\mathscr{D}_Q(\hat{\tau}) \mid \hat{\tau} \in \widehat{\mathscr{T}_s}\}$; say $\psi = \sum_{i=1}^m c_i\delta_Q(\hat{\tau}_i)$. Restricting to the weight-vector class W, we find that

$$\phi = \psi_W = \left(\sum_{i=1}^m c_i\delta_Q(\hat{\tau}_i)\right)_W = \sum_{i=1}^m c_i(\delta_Q(\hat{\tau}_i))_W.$$

But from the example following Definition II.3, $(\delta_Q(\hat{\tau}_i))_W = \delta_Q(\hat{\tau}_i)$ if $W(\hat{\tau}_i) = W$, and 0 else. We conclude that $W = W(\hat{\tau}_{i_0})$ for some i_0, and that $\phi = c_{i_0}\delta_Q(\hat{\tau}_{i_0}) \in \mathscr{V}\{\mathscr{D}_Q(\hat{\tau}) | \hat{\tau} \in \widehat{\mathscr{T}_s}\}$. □

Corollary II.10. $\widehat{K}_s^H = \mathscr{V}\{\delta_Q(\hat{\tau}) \mid \hat{\tau} \in \widehat{\mathscr{T}_s^H}\}$.

Proof. Since the polynomials $\delta_Q(\hat{\tau})$ are weight-vector pure with distinct weight-vectors, a linear combination of these is pure of weight $0 \Leftrightarrow$ each summand is pure of weight 0, and hence comes from $\widehat{\mathscr{T}_s^H}$. □

From Corollary II.10 and the remarks following Definition II.2, we see that $\widehat{K}_s^H$, and therefore K_s^H, is trivial unless h has a multiple of the form $\sum_{j=0}^s 2^{i_j}$, where $0 \leq i_j \leq d-1$ and the i_j are distinct. In particular:

Corollary II.11. $\widehat{K}_s^H = 0$, *and therefore* $K_s^H = 0$, *for* $s < \nu - 1$ *and* $s > d - \nu - 1$.

Corollary II.11 gives enough information about the action of $\mathscr{A}(2)$ on $(k[y_1, \dots, y_d])^H$ to prove that $P(G, d, m)$ holds for all m when G is of type I; the proof in that case may be found in §15. In the next four sections we obtain additional information about $k[y_1, \dots, y_d]$ and this action, and about the diagonalization of matrices with entries in a polynomial ring, which will be needed in the discussion of groups of type II.

9. Joint kernels of the Q_i. II

Having seen the concise description of K_s and $\widehat{K}_s$ in §8, one might ask how to characterize elements of dimensions other than $2^{s+1} - 1$ which lie in the joint kernel of the Q_i, $1 \leq i \leq s$. It follows from Wood's proof of Proposition II.4 that:

Lemma II.12. *Suppose* $\phi \in k[y_1, \dots, y_d]_{(m)}$ *(resp.* $\hat{k}[x_0, \dots, x_{d-1}]_{(m)}$*) satisfies* $Q_i(\phi) = 0$ *for* $1 \le i \le s$, *where* $m < 2^{s+1} - 1$. *Then* m *is even and* ϕ *is a square.*

The following is a partial characterization of the joint kernel in dimensions greater than $2^{s+1} - 1$:

Let $\phi \in \hat{k}[x_0, \dots, x_{d-1}]_{(m)}$, where $m \ge 2^{s+1} - 1$, and suppose ϕ satisfies $Q_i(\phi) = 0$ for $1 \le i \le s$. Let $\mu \in \mathrm{Mon}(\phi)$. Then either μ is a square or μ is of the form

$$\mu = (x_{i_0} x_{i_1-1}^{2^1} x_{i_2-2}^{2^2} \cdots x_{i_s-s}^{2^s}) x_{i_{s+1}} x_{i_{s+2}} \cdots x_{i_r} \lambda^2,$$

where $\lambda \in \mathrm{Mon}(X)$, $r \ge 0$, and the indices $i_0, \dots, i_r$ are distinct.
Note that when $m = 2^{s+1} - 1$, the statement is exactly that

$$\mu \in \mathrm{Mon}(\delta_Q(x_{i_0}, \dots, x_{i_s})),$$

which is consistent with Proposition II.9. An analogous statement holds in the smaller polynomial algebra $k[y_1, \dots, y_d]$, where $x_{i_j-j}^{2^j}$ is replaced by $y_{i_j}^{2^j}$.

We prove the statement for $s = 1$, which is the only case needed in this paper. The other cases may be proven inductively, with a good deal of bookkeeping.

Lemma II.13. *Let* $\phi \in \mathrm{Ker}(Q_1)$, *and let* $\mu \in \mathrm{Mon}(\phi)$. *Then either* μ *is a square, or* μ *is of the form* $\mu = (x_{i_0} x_{i_1-1}^2) x_{i_2} \cdots x_{i_r} \lambda^2$ *where* $\lambda \in \mathrm{Mon}(X)$, $r \ge 0$, *and the indices* $i_0, \dots, i_r$ *are distinct.*

Proof. If μ is a square, then there is nothing to prove. If not, write $\phi = \sum_{j=0}^n c_{\mu_j} \mu_j$, where the μ_j are the monomials of ϕ; w.l.o.g. $\mu = \mu_0$. As $Q_1(\phi) = 0$, we must have $c_0 Q_1(\mu_0) = \sum_{j=1}^n Q_1(\mu_j)$. Recall from §6 that

$$Q_1(\mu_0) = \sum_{j=0}^{d-1} x_{j-1}^2 \frac{\partial(\mu_0)}{\partial x_j} = \sum_J \left\{ \frac{x_{j-1}^2}{x_j} \mu_0 \right\}, \tag{11}$$

where $J = \{ j \in \mathbf{Z}/(d) \mid \deg_j(\mu_0) \equiv 1 \pmod 2 \}$. Now $J \ne \varnothing$, as μ_0 is not a square. Let $j_0 \in J$. Since the monomials $(x_{j-1}^2 / x_j)\mu_0$ of equation (11) are obviously distinct, there can be no cancellation in the right-hand summation, so that we have $x_{j_0-1}^2 \mu_0 / x_{j_0} \in \mathrm{Mon}(Q_1(\mu_0)) = \mathrm{Mon}(\sum_{j=1}^n c_{\mu_j} Q_1(\mu_j))$. This means

$$\frac{x_{j_0-1}^2}{x_{j_0}} \mu_0 = \frac{x_{j_1-1}^2}{x_{j_1}} \mu_1$$

for some $j_1 \ne j_0$ and some $\mu_1 \in \mathrm{Mon}(\phi)$, $\mu_1 \ne \mu_0$, with $\deg_{j_1}(\mu_1) \equiv 1 \pmod 2$. Now

$$\mu_0 = \frac{x_{j_1-1}^2}{x_{j_0-1}^2} \frac{x_{j_0}}{x_{j_1}} \mu_1,$$

from which we see that $\deg_{j_1-1}(\mu_0) \ge 2$ and $\deg_{j_1}(\mu_0) \equiv \deg_{j_1}(\mu_1) - 1 \equiv 0 \pmod 2$. Since by assumption $\deg_{j_0}(\mu_0) \equiv 1 \pmod 2$, we see that

$$\chi \overset{\text{def}}{=} \frac{\mu_0}{x_{j_1-1}^2 x_{j_0}}$$

has $\deg_{j_0}(\chi) \equiv \deg_{j_1}(\chi) \equiv 0 \pmod 2$. Thus χ is of the form $x_{i_2} \cdots x_{i_r} \lambda^2$ for some $\lambda \in \mathrm{Mon}(X)$ and some $x_{i_2}, \dots, x_{i_r}$ distinct from each other and from x_{j_0} and x_{j_1}. As $\mu_0 = x_{j_1-1}^2 x_{j_0} \chi$, this proves the lemma. □

10. Linear forms and 2^t-powers

We now digress to introduce some notation concerning linear forms and 2^t-powers of polynomials, both of which play a large role in what is to follow. Let $\mathscr{L}_1, \dots, \mathscr{L}_r \subset \mathscr{L}$ be the distinct orbits of the H-action on $\mathscr{L}$, and set $\pi_j = \prod_{\lambda_i \in \mathscr{L}_j} \lambda_i$, for $1 \leq j \leq r$.

Definition II.14. A polynomial $\pi \in k[y_1, \dots, y_d]$ is a *product over orbits of* H *on* $\mathscr{L}$ if $\pi = \prod_{j=1}^r \pi_j^{a_j}$ for suitable a_j. If l of the integers a_j are odd, then π is an *l-orbit nonsquare.*

Putting hats on everything in sight, we make a similar definition for polynomials of $\hat{k}[x_0, \dots, x_d]$.

Clearly any nontrivial H-invariant product of linear factors in $k[y_1, \dots, y_d]$ (resp. $(\hat{k}[x_0, \dots, x_{d-1}])^H$) is a product over orbits of H on $\mathscr{L}$ (resp. $\widehat{\mathscr{L}}$); the degrees of such products are multiples of h. From now on, we reserve the letters π and ρ for products of linear factors.

In what follows, $\mathscr{C}$ stands for either $k[y_1, \dots, y_d]$ or $\hat{k}[x_0, \dots, x_{d-1}]$, and t is a positive integer. We say a polynomial $\psi \in \mathscr{C}$ is a (2^t)th power if $\psi = \xi^{2^t}$ for some $\xi \in \mathscr{C}$. Any polynomial $\phi \in \mathscr{C}$ can be written, uniquely up to scalars, as $\phi = \psi\chi$, where ψ is a (2^t)th power and χ has no factors of multiplicity 2^t. Furthermore, there exists up to scalars a unique (2^t)th power polynomial $\xi \in \mathscr{C}$ of least degree such that $\phi \mid \xi$. We make the following definition:

Definition II.15. Let t, ϕ, ψ, χ, and ξ be as above. We write $\phi^{[t]}$ for χ and $\phi^{\{t\}}$ for ξ, and define $\phi^{\langle t\rangle}$ by $\phi^{\langle t\rangle} \cdot \phi = \phi^{\{t\}}$.

To illustrate this notation, we list a few facts which will be useful later.

Fact II.16. *Let* $\phi \in \mathscr{C}$, *and suppose that* $\beta \in \mathscr{C}$ *is a* (2^t)*th power polynomial such that* $\phi \mid \beta$. *Then* $\phi^{\{t\}} \mid \beta$, *so that* $\beta = \phi^{\{t\}}\alpha^{2^t}$ *for some* $\alpha \in \mathscr{C}$.

Lemma II.17. *Suppose* t *is a positive integer and* $1 \neq \pi \in \mathscr{C}^H$ *is an* H*-invariant product of linear factors, not a* (2^t)*th power, such that* $\deg(\pi) \equiv 0 \pmod{2^t}$. *Then* $\deg(\pi) \geq 2^t h$ *and* $\deg(\pi^{\langle t\rangle}) \geq 2^t h$.

Proof. In fact $0 \neq \deg(\pi) \equiv 0 \pmod{2^t h}$, by the remark following Definition II.14. Since $\phi^{\{t\}}$ is a (2^t)th power and an H-invariant product of linear factors, we have $\deg(\phi^{\{t\}}) \equiv 0 \pmod{2^t h}$, so that $0 \neq \deg(\phi^{\langle t\rangle}) = \deg(\phi^{\{t\}}) - \deg(\phi) \equiv 0 \pmod{2^t h}$. □

11. Eigenvectors of Steenrod operations

In this section, $\mathscr{C}$ stands for $k[y_1, \dots, y_d]$, $\hat{k}[x_0, \dots, x_{d-1}]$, or their H-invariant subalgebras.

Definition II.18. Let $\Psi \in \mathscr{A}(2)$ be a Steenrod operation of degree j, and let $\theta \in \mathscr{C}$ be a polynomial. If θ divides $\Psi(\theta)$ in the polynomial algebra $\mathscr{C}$, we say that θ is a Ψ-eigenvector with eigenvalue $\lambda_{\Psi,\theta} = \Psi(\theta)/\theta \in \mathscr{C}_{(j)}$.

Definition II.19. If $\theta \in \mathscr{C}$ is a Sq^{2^i}-eigenvector for all $0 \leq i < \infty$ (resp. a Q_i-eigenvector for $0 \leq i < \infty$), we say θ is an $\mathscr{A}(2)$-eigenvector (resp. a Q-eigenvector).

From Proposition I.9 it is evident that θ is a Q-eigenvector if it is a Q_i-eigenvector for $0 \leq i \leq d-1$; from Fact I.8, θ is an $\mathscr{A}(2)$-eigenvector if it is a Sq^{2^i}-eigenvector for all i such that $2^i \leq \deg(\theta)$. Proposition I.10 may be restated as follows: Let $\theta \in k[y_1, \dots, y_d]$ be a Q-eigenvector with $\lambda_{Q_i,\theta} = 0$ for $0 \leq i \leq d-1$. Then θ is a square.

The following is a corollary to a theorem of Serre:

Proposition II.20 [Ser65b]. *$\theta \in k[y_1, \dots, y_d]$ is an $A(2)$-eigenvector $\Leftrightarrow \theta = \prod_{l_i \in \mathscr{L}} l_i^{a_i}$ is a product of linear forms.*

Products of Γ-invariant linear forms of $\hat{k}[x_0, \dots, x_{d-1}]$ are therefore eigenvectors for the action of $\mathscr{A}(2)$ on $\hat{k}[x_0, \dots, x_{d-1}]$.

The next two propositions describe, respectively, Q-eigenvectors of the algebra $\hat{k}[x_0, \dots, x_{d-1}]$ whose eigenvalues are not necessarily 0, and polynomials of $\hat{k}[x_0, \dots, x_{d-1}]$ which are Sq^{2^i}-eigenvectors for $i \leq$ some integer c.

Proposition II.21. 1. *$\theta \in \hat{k}[x_0, \dots, x_{d-1}]$ is a Q-eigenvector $\Leftrightarrow \theta = \psi^2\pi$, where $\psi \in \hat{k}[x_0, \dots, x_{d-1}]$ is a polynomial and π is a square-free product of Γ-invariant linear forms.*

2. *$\theta \in (\hat{k}[x_0, \dots, x_{d-1}])^H$ is a Q-eigenvector $\Leftrightarrow \theta = \psi^2\pi$, where $\psi \in (\hat{k}[x_0, \dots, x_{d-1}])^H$ and π is a product over orbits of H on $\widehat{\mathscr{L}}$.*

Proof. One direction of these implications is an immediate consequence of the remark following Proposition II.20 and the fact that the Q_i's are derivations. Suppose now that $\theta \in \hat{k}[x_0, \dots, x_{d-1}]$ is a Q-eigenvector with $\deg(\theta) > 1$. Then by equation (3) we have

$$\begin{pmatrix} x_0 & x_1 & \cdots & x_{d-1} \\ x_{d-1}^2 & x_0^2 & \cdots & x_{d-2}^2 \\ \vdots & \vdots & \vdots & \vdots \\ x_1^{2^{d-1}} & x_2^{2^{d-1}} & \cdots & x_0^{2^{d-1}} \end{pmatrix} \begin{pmatrix} \frac{\partial(\theta)}{\partial x_0} \\ \frac{\partial(\theta)}{\partial x_1} \\ \vdots \\ \frac{\partial(\theta)}{\partial x_{d-1}} \end{pmatrix} = \begin{pmatrix} Q_0(\theta) \\ Q_1(\theta) \\ \vdots \\ Q_{d-1}(\theta) \end{pmatrix} = \begin{pmatrix} \lambda_0\theta \\ \lambda_1\theta \\ \vdots \\ \lambda_{d-1}\theta \end{pmatrix}$$

for appropriate $\lambda_i \in \hat{k}[x_0, \dots, x_{d-1}]_{(2^i-1)}$. In the notation of §14, the matrix on the left is $\mathscr{D}_Q(\tau_x)$. By Corollary II.8, its determinant is $\delta_Q(\tau_x) = \prod_{\hat{l}_i \in \widehat{\mathscr{L}}} \hat{l}_i$, which is invertible in the field of fractions $\hat{k}(x_0, \dots, x_{d-1})$ of $\hat{k}[x_0, \dots, x_{d-1}]$. We now use Kramer's Rule to solve for $\{\partial(\theta)/\partial x_j\}_{j=0}^{d-1}$ in terms of $\{\lambda_i\theta\}_{i=0}^{d-1}$. Let $\mathscr{X}_j$ be the matrix obtained by replacing the jth column of $\mathscr{D}_Q(\tau_x)$ with the vector $(\lambda_0\theta, \lambda_1\theta, \dots, \lambda_{d-1}\theta)^T$; by Kramer's Rule, we have

$$\frac{\partial(\theta)}{\partial x_j} = \frac{\delta(\mathscr{X}_j)}{\delta_Q(\tau_x)}.$$

The determinant $\delta(\mathscr{X}_j)$ is a homogeneous polynomial of degree $2^d - 1 + \deg(\theta) - 1 = 2^d + \deg(\theta) - 2$. Since each coefficient of the jth column of $\mathscr{X}_j$ is a multiple of θ, we find by expanding $\delta(\mathscr{X}_j)$ along the jth column that $\delta(\mathscr{X}_j)$ is itself a multiple of θ: $\delta(\mathscr{X}_j) = \theta\delta_j$ for some polynomial δ_j of degree $2^d - 2$. Thus we have

$$\frac{\partial(\theta)}{\partial x_j} = \frac{\theta\delta_j}{\delta_Q(\tau_x)}$$

for all $1 \leq j \leq d$.

If $\partial(\theta)/\partial x_j = 0$ for all j, then θ is a square by equation (1) of §2, and part 1 of the proposition is true. Suppose then that $\partial(\theta)/\partial x_j \neq 0$ for some j. Since $\partial(\theta)/\partial x_j$ belongs to the ring $\hat{k}[x_0, \dots, x_{d-1}]$, each factor $\hat{l}_i$ of the denominator $\delta_Q(\tau_x)$ must divide the numerator $\theta\delta_j$. For degree reasons $\delta_Q(\tau_x)$ cannot divide δ_j, so we see that $\delta_Q(\tau_x)$ and θ must have a common factor. Therefore θ has a Γ-invariant linear factor; say $\theta = \hat{l}\theta'$ for $\hat{l} \in \widehat{\mathscr{L}}$, $\theta' \in \hat{k}[x_0, \dots, x_{d-1}]$, $\deg(\theta') = \deg(\theta) - 1$. I claim now that θ' is also a Q-eigenvector. Indeed, for $0 \le i \le d-1$, we have $0 \equiv Q_i(\theta) = Q_i(\hat{l})\theta' + \hat{l}Q_i(\theta') \pmod{\hat{l}\theta'}$, as θ is a Q-eigenvector. But $\hat{l}$, being linear and Γ-invariant, is itself a Q-eigenvector, so that $Q_i(\hat{l})\theta' \equiv 0 \pmod{\hat{l}\theta'}$. Consequently, for $0 \le i \le d-1$ we have that $\hat{l}\theta' | \hat{l}Q_i(\theta')$, and so $\theta' | Q_i(\theta')$. Part 1 of the proposition now follows easily by induction on $\deg(\theta)$.

If $\theta \in (\hat{k}[x_0, \dots, x_{d-1}])^H$, then one sees that the set of linear factors $\{\hat{l}_{i_j}\}$ of π is closed under the action of H, so that $\{\hat{l}_{i_j}\}$ is a union of H-orbits and π is H-invariant. It follows that ψ is also H-invariant. This proves part 2. □

In this paper, we will be concerned with Q-eigenvectors that lie in the subalgebra $k[y_1, \dots, y_d] \subset \hat{k}[x_0, \dots, x_{d-1}]$. The following description of such Q-eigenvectors follows immediately from the proposition; alternatively, it may be proven by exactly the same argument, with $\mathscr{D}_Q(\tau_y)$ and $\delta_Q(\tau_y)$ replacing $\mathscr{D}_Q(\tau_x)$ and $\delta_Q(\tau_x)$.

Proposition II.22. 1. *$\theta \in k[y_1, \dots, y_d]$ is a Q-eigenvector $\Leftrightarrow \theta = \psi^2\pi$, where $\psi \in k[y_1, \dots, y_d]$ is a polynomial and π is a square-free product of linear forms.*

2. *$\theta \in (k[y_1, \dots, y_d])^H$ is a Q-eigenvector $\Leftrightarrow \theta = \psi^2\pi$, where $\psi \in (k[y_1, \dots, y_d])^H$ and π is a product over orbits of H on $\mathscr{L}$.*

Proposition II.22, applied repeatedly, yields the following characterization of simultaneous eigenvectors of $Sq^{2^1}, \dots, Sq^{2^c}$ in $k[y_1, \dots, y_d]$:

Proposition II.23. *Let $c \ge d-2$.*

1. *A polynomial $\sigma \in k[y_1, \dots, y_d]$ is a Sq^{2^i}-eigenvector for $0 \le i \le c \Leftrightarrow \sigma = \tau^{2^{c-d+3}}\pi$, where τ is a Sq^{2^i}-eigenvector for $0 \le i \le d-3$ and π is a product of linear forms.*

2. *A polynomial $\sigma \in (k[y_1, \dots, y_d])^H$ is a Sq^{2^i}-eigenvector for $0 \le i \le c \Leftrightarrow \sigma = \tau^{2^{c-d+3}}\pi$, where τ is an H-invariant Sq^{2^i}-eigenvector for $0 \le i \le d-3$ and π is a product over orbits of H on $\mathscr{L}$.*

Proof. We prove only part 1; part 2 follows exactly as did part 2 of Proposition II.21. To begin the inductive proof, suppose that $c = d-2$. Then from the definition of the Q_j as commutators of the Sq^{2^i}, we have that σ is a Q-eigenvector. By Proposition II.21, $\sigma = \chi^2\rho$ for some polynomial χ and product ρ of linear forms. We now show inductively that $\chi \mid Sq^{2^i}(\chi)$ for $0 \le i \le d-3$. Using the Cartan relations and Fact I.8, we write

$$(12) \qquad Sq^{2^{i+1}}(\chi^2\rho) = \sum_{j=0}^{2^{i+1}} Sq^j(\chi^2)Sq^{2^{i+1}-j}(\rho) = \sum_{j=0}^{2^i}(Sq^j\chi)^2 Sq^{2^{i+1}-2j}(\rho).$$

By hypothesis, $\sigma = \chi^2\rho \mid Sq^{2^{i+1}}(\chi^2\rho)$ for $0 \le i \le d-3$. When $i = 0$, we find that

$$\chi^2\rho \mid Sq^2(\chi^2\rho) = \chi^2 Sq^1(\rho) + (Sq^1\chi)^2\rho, \tag{13}$$

from which it follows that $\chi^2 \mid (Sq^1\chi)^2$, so that $\chi \mid Sq^1(\chi)$.

Now assume that $\chi \mid Sq^{2^l}(\chi)$ for $l < i \le d-3$. By Fact I.8, we have $\chi \mid Sq^j(\chi)$ for $j \le 2^i - 1$. Since ρ is an eigenvector for $\mathscr{A}(2)$ by Proposition II.20, we have

$$\chi^2\rho \mid (Sq^j\chi)^2 Sq^{2^{i+1}-2j}(\rho) \tag{14}$$

for $j \le 2^i - 1$. From equation (12) and the hypothesis on σ, we find that

$$0 \equiv Sq^{2^{i+1}}(\chi^2\rho) \equiv (Sq^{2^i}(\chi))^2\rho \pmod{\chi^2\rho}, \tag{15}$$

and hence that $\chi \mid Sq^{2^i}(\chi)$. This completes the inductive step of the proof that $\chi \mid Sq^{2^i}(\chi)$ for $0 \le i \le d-3$, and proves the proposition for $c = d-2$.

To prove the proposition for $c_0 > d-2$, we assume that it holds for $d-2 \le c \le c_0 - 1$. Suppose then that $\sigma \mid Sq^{2^i}(\sigma)$ for $0 \le i \le c_0$. By the proposition for $c = d-2$, we have $\sigma = \chi^2\rho$ for some polynomial χ and product ρ of linear forms. The above argument with $c_0 - 1$ replacing $d-3$ shows that χ is a Sq^{2^i}-eigenvector for $0 \le i \le c_0 - 1$. By the inductive hypothesis, $\chi = \tau^{2^{c_0-d}}\psi$, where τ is a Sq^{2^i}-eigenvector for $0 \le i \le d-3$ and ψ is a product of linear forms. This means that our original polynomial $\sigma = \tau^{2^{c-d+1}}\psi^2\rho$. As $\psi^2\rho$ is the product of linear forms, we may take $\pi = \psi^2\rho$, proving Proposition II.23. □

12. Independent sets of eigenvectors

We now prove a proposition about independent sets consisting of simultaneous eigenvectors for the first few Steenrod squares.

Proposition II.24. *Let l be an integer ≥ 1, and suppose that $\{\phi_1, \dots, \phi_s\} \subset k[y_1, \dots, y_d]$ is an independent set such that each $\phi_i = \psi_i^{2^l}\pi_i$ for some polynomial ψ_i and product π_i of linear forms. Suppose moreover that*

$$\sum_{i=1}^{s} \beta_i\phi_i = \omega^{2^l} \tag{16}$$

for some homogeneous polynomials $\beta_1, \dots, \beta_s$ and ω. If

$$\deg(\beta_{i_1}) + 2^{d+l-2} - 2^{l-1} < \deg(\phi_{i_2}) \quad \text{for all } 1 \le i_1, i_2 \le m, \tag{17}$$

then $\beta_i\phi_i$ is a 2^l-power for $1 \le i \le s$.

Proof. We prove the proposition one l at a time. Suppose to begin with that $l = 1$. As in §11, the ϕ_i's are all Q-eigenvectors, so for $1 \le i \le s$ and $0 \le j \le d-1$ we can define elements $\lambda_{j,i} \in k[y_1, \dots, y_d]_{(2^j-1)}$ by $Q_j(\phi_i) = \lambda_{j,i}\phi_i$.

For each j, $1 \leq j \leq d-1$, applying Q_j to equation (16) gives

$$\begin{aligned}0 &= \sum_{i=1}^{s} Q_j(\beta_i\phi_i) \\ &= \sum_{i=1}^{s} Q_j(\beta_i)\phi_i + \sum_{i=1}^{s} \beta_i Q_j(\phi_i) \\ &= \sum_{i=1}^{s}(Q_j(\beta_i) + \lambda_{j,i}\beta_i)\phi_i.\end{aligned}$$

This is a relation between the ϕ_i, the degrees of whose coefficients satisfy

$$\deg(Q_j(\beta_{i_1}) + \lambda_{j,i_1}\beta_{i_1}) \leq 2^{d-1} - 1 + \deg(\beta_{i_1}) < \deg(\phi_{i_2}),$$

for all $1 \leq i_1, i_2 \leq s$, by assumption. As the $\phi_1, \dots, \phi_s$ form an independent set, this relation must be trivial by Fact I.2; that is,

$$(18) \qquad 0 = (Q_j(\beta_i) + \lambda_{i,j}\beta_i)\phi_i = Q_j(\beta_i\phi_i), \qquad 1 \leq i \leq m,\ 0 \leq j \leq d-1.$$

By Proposition I.10, we conclude that $\beta_i\phi_i$ is a square for all i. This proves the proposition in the case $l = 1$.

To prove the proposition for general l, suppose inductively that it holds for all numbers $\leq l-1$, and that β_i, ϕ_i, and ω satisfy the hypotheses of the proposition for the case of l. Then the proposition for the case of 1 says that $\beta_i\phi_i$ is a square for $1 \leq i \leq s$, so that, as in §10, there exist polynomials $\{\beta_i'\}_{i=1}^s$ such that $\beta_i\phi_i = (\beta_i')^2\phi_i^{\{1\}} = (\beta_i')^2\psi_i^{2^l}\pi_i^{\{1\}}$. Now by construction, $\pi_i^{\{1\}}$ is a square; say $\pi_i^{\{1\}} = (\pi_i')^2$. The prime factors of $(\pi_i')^2$, being the factors of $\pi_i^{(1)}$, are linear forms. Set $\phi_i' = \psi_i^{2^{l-1}}\pi_i'$; then $(\phi_i')^2 = \phi_i^{\{1\}}$ and $(\beta_i'\phi_i')^2 = \beta_i\phi_i$.

We now verify that the conditions of the proposition for the case of $l-1$ are satisfied with ϕ_i replaced by ϕ_i' and β_i by β_i'. Square roots are unique in characteristic 2, so from the last equality we have $\omega^{2^{l-1}} = \sum_{i=1}^s \beta_i'\phi_i'$. It remains to check the degree condition. But for each i_1 and i_2, we have $\deg(\beta_{i_1}') \leq \frac{1}{2}\deg(\beta_{i_1})$ and $\deg(\phi_{i_2}') \geq \frac{1}{2}\deg(\phi_{i_2})$, so that the inequality

$$\deg(\beta_{i_1}') + 2^{d+(l-3)} - 2^{l-2} < \deg(\phi_{i_2}'), \qquad 1 \leq i_1, i_2 \leq m,$$

follows from equation (17). The proposition for the case of $l-1$ then gives that $\beta_i'\phi_i'$ is a 2^{l-1}-power for all i. But $(\beta_i'\phi_i')^2 = \beta_i\phi_i$, and consequently $\beta_i\phi_i$ is a 2^l-power for $1 \leq i \leq s$. This completes the induction step and proves the proposition. □

Corollary II.25. *Suppose $\phi_1, \dots, \phi_s$, ω, and $\beta_1, \dots, \beta_s$ are as in the proposition. Then for each i, either $\beta_i = 0$ or $\deg(\beta_i) \geq \deg(\pi_i^{\langle l\rangle})$.*

Proof. By the proposition, $\beta_i\phi_i$ is a 2^l-power, so $\pi_i^{\langle l\rangle}$ divides β_i as in §10. □

13. Diagonalization

In this section, we prove that a matrix over $k[y_1, \dots, y_d]$ satisfying a certain simple condition is diagonalizable. The argument is due to John Conway.

Definition II.26. Let $\mathscr{R}$ be a ring and suppose $A = (a_{ij}) \in \mathrm{Mat}_n(\mathscr{R})$. Then $A^{[2]}$ denotes the component-wise square of A; $A^{[2]} = (a_{ij}^2)$.

Proposition II.27. *Suppose $A \in \mathrm{Mat}_n(k[y_1, \dots, y_d])$ satisfies $A^{[2]} = A^2$. Then A is diagonalizable over k; that is, $k^n \subset k[y_1, \dots, y_d]^n$ has a basis consisting of eigenvectors of A.*

Proof. Let $\mathscr{C} = \overline{k[y_1, \dots, y_d]}$, the algebraic closure of $k[y_1, \dots, y_d]$. Let $\sigma: \mathscr{C} \to \mathscr{C}$ be the Frobenius automorphism given by $z \mapsto z^\sigma = z^2$; this automorphism acts in the obvious way on $\mathrm{Mat}_n(\mathscr{C})$. Then the fixed field $\mathscr{C}^\sigma = k$, and the hypothesis on A is that $A^\sigma = A^2$. Regarded as an element of $\mathrm{Mat}_n(\mathscr{C})$ acting on $\mathscr{C}^n$, A can be put in Jordan-canonical form. In particular, $\mathscr{C}^n$ has a basis consisting of higher-order eigenvectors of A, that is, of vectors v satisfying $(A + \lambda Id)^\delta v = 0$ for a suitable $\lambda \in \mathscr{C}$ and integer δ, where Id is the identity matrix of $\mathrm{Mat}_n(\mathscr{C})$. I claim that any σ-invariant higher-order eigenvector v of A is in fact an eigenvector: note that the hypothesis on A implies that $(A + \lambda Id)^{\sigma^i} = (A + \lambda Id)^{2^i}$ for all $i \geq 0$, since $\lambda^\sigma = \lambda^2$ and A commutes with Id. Let d be the smallest integer for which $(A + \lambda Id)^{2^d} v = 0$; suppose $d \geq 1$. Then

$$0 = (A + \lambda Id)^{2^d} v = ((A + \lambda Id)^{2^{d-1}})^2 v = ((A + \lambda Id)^{2^{d-1}} v)^\sigma;$$

σ being injective, we have $(A + \lambda Id)^{2^{d-1}} v = 0$, contradicting the choice of d. So $d = 0$; that is, v is an eigenvector. Therefore to prove the proposition, it will suffice to construct a basis of higher-order eigenvectors all of which lie in $k^n = (\mathscr{C}^n)^\sigma$.

Let $\lambda \in \mathscr{C}$ be an eigenvalue of A and $v \in \mathscr{C}^n$ a higher-order eigenvector for which $(A + \lambda Id)^{2^t} v = 0$, where $t \geq 0$. Let $v^{\sigma^{m+1}}$ be the first σ-image of v to be $\mathscr{C}$-linearly dependent on its predecessors, so that $v^{\sigma^{m+1}} = \sum_{i=0}^m c_i v^{\sigma^i}$ (say) and the elements $v, v^\sigma, \dots, v^{\sigma^m}$ are linearly independent. Now $(A + \lambda Id)^{2^{t+i}} v^{\sigma^i} = [(A + \lambda Id)^{2^t} v]^{\sigma^i} = 0$; thus the vectors $v, v^\sigma, \dots, v^{\sigma^m}$—and hence their linear combinations—are all higher-order eigenvectors belonging to λ. I claim that this linear span $\mathscr{V}\{v, v^\sigma, \dots, v^{\sigma^m}\}$ contains a nonzero σ-invariant element: by linear independence, the equality

$$\sum_{i=0}^m a_i v^{\sigma^i} = \left(\sum_{i=0}^m a_i v^{\sigma^i}\right)^\sigma = \sum_{i=0}^{m-1} a_i^\sigma v^{\sigma^{i+1}} + a_m^\sigma \sum_{i=0}^m c_i v^{\sigma^i}$$

holds when the scalars $a_0, \dots, a_m$ satisfy the equations

(1) $$a_m^2 c_0 = a_0,$$

(2) $$a_{i-1}^2 + a_m^2 c_i = a_i, \qquad 1 \leq i \leq m.$$

Starting with (1) and using (2) to express $a_0, \dots, a_m$ in terms of a_m and $c_0, \dots, c_m$, we find that $a_i = \sum_{j=0}^i (a_m^2 c_j)^{2^{i-j}}$ and in particular,

$$a_m = \sum_{j=0}^m (a_m^2 c_j)^{2^{m-j}}.$$

Conversely, any root of the polynomial

$$f(x) = \sum_{j=0}^m c_j^{2^{m-j}} x^{2^{m-j+1}} + x$$

gives rise to solutions $a_0, \ldots, a_m$ to (1) and (2). Since by their definition the $c_0, \ldots, c_m$ are not all 0, $f(x)$ has a nontrivial root a_m in algebraically-closed $\mathscr{C}$, which yields a vector $v_1 = \sum_{i=0}^m a_i v^{\sigma^i}$ satisfying $v_1^\sigma = v_1$. By the linear independence of the v^{σ^i}, $0 \le i \le m$, we have $v_1 \neq 0$. This proves the claim.

We now proceed to construct inductively a basis of σ-invariant eigenvectors for A. Suppose $v_1, \ldots, v_{l-1}$ is a linearly independent set of such eigenvectors, with $l \le d$. Choosing a higher-order λ_l-eigenvector w not in $\mathscr{V}\{v_1, \ldots, v_{l-1}\}$, as we may since $\mathscr{C}^n$ is spanned by higher-order eigenvectors, we repeat the above process modulo $\mathscr{V}\{v_1, \ldots, v_{l-1}\}$. This gives a vector

$$0 \neq \overline{u} \in \mathscr{C}^n/\mathscr{V}\{v_1, \ldots, v_{l-1}\}$$

satisfying $\overline{u}^\sigma = \overline{u}$; say $\overline{u} = u + \mathscr{V}\{v_1, \ldots, v_{l-1}\}$ where $u \in \mathscr{V}\{w, w^\sigma, w^{\sigma^2}, \ldots\}$ satisfies $u^\sigma = u + \sum_{j=1}^{l-1} \mu_j v_j$. As we saw above, $(A + \lambda_l Id)^{2^e} u = 0$ for some e; applying σ to this equation, we find

$$0 = (A + \lambda_l Id)^{2^{e+1}} \left(u + \sum_{j=1}^{l-1} \mu_j v_j \right) = \sum_{j=1}^{l-1} (\lambda_j + \lambda_l)^{2^{e+1}} \mu_j v_j,$$

so that for each j, either $\mu_j = 0$ or $\lambda_j = \lambda_l$.

If $\mu_j = 0$ for all j, we have $u^\sigma = u$, so we may take $v_l = u$ and proceed with the induction. If $\mu_{j_k} \neq 0$ for $k = 1, 2, \ldots, t$, we must have $\lambda_{j_1} = \cdots = \lambda_{j_t} = \lambda_l$. Let $\{\rho_{j_k} | 1 \le k \le t\}$ be solutions of $x^2 + x = \mu_{j_k}$ in the algebraically-closed field $\mathscr{C}$, and set $r = \sum_{k=1}^t \rho_{j_k} v_{j_k}$. It is easy to check that r is a higher-order λ_l-eigenvector and that $(u + r)^\sigma = u + r$ $(\notin \mathscr{V}\{v_1, \ldots, v_{l-1}\})$. We may now take $v_l = u + r$ and proceed with the induction.

We conclude that A has a basis of eigenvectors in $(\mathscr{C}^n)^\sigma = k^\sigma$. This proves the proposition. □

Let $G = H \ltimes_\tau E_d$ as in previous sections; recall that H acts on the algebra $k[y_1, \ldots, y_d] = H^*(E_d)$ with invariant subalgebra $H^*(G)$. The action extends to $\mathrm{Mat}_n(k[y_1, \ldots, y_d])$ by $\eta(a_{jk}) = (\eta a_{jk})$, and $\mathrm{Mat}_n(k[y_1, \ldots, y_d])^H = \mathrm{Mat}_n((k[y_1, \ldots, y_d])^H)$.

Corollary II.28. *Suppose that $A \in \mathrm{Mat}_n((k[y_1, \ldots, y_d])^H)$ satisfies $A^2 = A^{[2]}$. Then A is diagonalizable and its eigenvalues are H-invariant.*

Proof. Let $E \in \mathrm{Mat}_{n\times n}(k)$ be the matrix taking the standard basis of k^n to the basis $\{v_j\}_{j=1}^d$ given in the proposition, so that $A = E^{-1}\Delta E$ for $\Delta = \mathrm{diag}\{\lambda_1, \ldots, \lambda_d\}$. As H fixes A, we have

$$E^{-1}\Delta E = A = \eta A = (\eta E^{-1})(\eta\Delta)(\eta E) = E^{-1}(\eta\Delta)E,$$

the last equality holding because H acts trivially on

$$\mathrm{Mat}_n(k) \subset \mathrm{Mat}_n(k[y_1, \ldots, y_d]).$$

So $\eta\Delta = \Delta$, proving the corollary. □

Part III. Proof of the main theorem

14. Q-invariant independent sets. I

Let $G = H \ltimes_\tau E_d$ be a semidirect product as before. Recall from §7 the notation $P(G, l, m)$, representing the statement that any $\mathscr{A}(2)$-invariant l.s.o.p.

of the cohomology algebra $H^*(G) \simeq (k[y_1, \dots, y_d])^H$ in degree m consists entirely of squares. In this section, we prove some results about Q- and $\mathscr{A}(2)$-invariant independent sets which will imply that $P(G, d, m)$ holds for all m when G is of type I; from this the main theorem for groups $\mathscr{G}$ with subgroups of this form will follow as in §7. The rest of part 3 is devoted to proving that $P(G, d, m)$ holds for all m not of the form $2^t \cdot 5$ when G is of type II, thus completing the proof of the main theorem.

We begin by introducing some notation. Let $G = H \ltimes_\tau E_d$, and suppose that $\mathscr{S} = \{\theta_1, \dots, \theta_s\} \subset (k[y_1, \dots, y_d])^H$ is a level Q-invariant independent set of degree m. Define b by $2^b - 1 < m \le 2^{b+1} - 1$. For $1 \le t \le b$, we may define elements $q(t)_{jk} \in k[y_1, \dots, y_d]^H_{(2^t-1)}$ by

$$(19) \qquad Q_t(\theta_j) = \sum_{j=1}^{d} q(t)_{jk}\theta_k$$

as in §7; as $m > 2^b - 1$ by assumption, these elements are uniquely defined by Fact I.2. Let $\mathscr{Q}(t) \in \mathrm{Mat}_s k[y_1, \dots, y_d]^H_{(2^t-1)}$ be the matrices $\mathscr{Q}(t) = (q(t)_{jk})$, $1 \le t \le b$. Writing Θ to represent $(\theta_1, \dots, \theta_s) \in (k[y_1, \dots, y_d])^{\times d}$, we summarize the equations in (19) with the matrix equation $\Theta\mathscr{Q}(t) = (\theta_1, \dots, \theta_d)\mathscr{Q}(t) = Q_t(\Theta)$. In this notation, we have

$$Q_tQ_u(\Theta) = Q_t(\Theta\mathscr{Q}(u)) = \Theta Q_t(\mathscr{Q}(u)) + \Theta(\mathscr{Q}(t)\mathscr{Q}(u))$$

for $1 \le t, u \le b$. As the Q_t are commuting derivations, we have $Q_uQ_t(\Theta) = Q_tQ_u(\Theta)$, so that

$$(20) \qquad \Theta Q_u(\mathscr{Q}(t)) + \Theta(\mathscr{Q}(u)\mathscr{Q}(t)) = \Theta Q_t(\mathscr{Q}(u)) + \Theta(\mathscr{Q}(t)\mathscr{Q}(u)).$$

This is a matrix equation in Θ with coefficients of degree $2^t - 1 + 2^u - 1$. For t, u such that $2^t + 2^u - 2 < m$, Fact I.2 gives

$$(21) \qquad Q_u(\mathscr{Q}(t)) + Q_t(\mathscr{Q}(u)) = [\mathscr{Q}(t), \mathscr{Q}(u)].$$

We obtain another equation involving $\mathscr{Q}(u)$ from the fact that $Q_uQ_u = 0$:

$$\begin{aligned} 0 = Q_uQ_u(\Theta) &= Q_u(\Theta\mathscr{Q}(u)) \\ &= \Theta\mathscr{Q}(u)\mathscr{Q}(u) + \Theta(Q_u\mathscr{Q}(u)) \\ &= \Theta\mathscr{Q}(u)^2 + \Theta(Q_u\mathscr{Q}(u)). \end{aligned}$$

If $2(2^u - 1) < m$, then as before Fact I.2 applies to give

$$(22) \qquad (\mathscr{Q}(u))^2 + Q_u(\mathscr{Q}(u)) = 0.$$

In the next two propositions, we use equations (21) and (22) to prove that the elements of Q-invariant (resp. $\mathscr{A}(2)$-invariant) independent sets are eigenvectors for the first few Q_i (resp. Sq^{2^i}). Recall from §5 the definition of ν.

Proposition III.1. *Let $G = H \ltimes_\tau E_d$, and suppose that $\mathscr{S} = \{\theta_1, \dots, \theta_s\}$ is a level independent set for $(k[y_1, \dots, y_d])^H$ in degree m. If $m > 2^\nu - 2$ and $\mathscr{S}$ is invariant under Q_i for $0 \le i \le \nu - 1$, then $Q_i(\xi) = 0$ for all ξ in the linear span $\mathscr{V}\{\theta_1, \dots, \theta_s\}$ and all i, $1 \le i \le \nu - 1$. If in addition $m > 2^{\nu+1} - 2$ and $\mathscr{S}$ is invariant under Q_ν, then $\mathscr{V}\{\theta_1, \dots, \theta_s\}$ has a basis $\theta'_1, \dots, \theta'_s$ such that for $1 \le j \le s$, $Q_\nu(\theta'_j) = \lambda_j\theta'_j$ for suitable $\lambda_j \in k[y_1, \dots, y_d]^H_{(2^\nu-1)}$.*

Proof. Suppose to begin with that $m > 2^\nu - 2$ and $\mathscr{S}$ is invariant under Q_i, $0 \le i \le \nu - 1$. The matrices $\mathscr{Q}(t)$ discussed above are defined for $1 \le t \le \nu - 1$.

We have $\mathscr{Q}(1) = 0$, since its coefficients lie in $k[y_1, \dots, y_d]^H_{(1)}$, which is 0 by Corollary I.6. We prove inductively that $\mathscr{Q}(i) = 0$ for $1 \le i \le \nu - 1$.

Suppose that the matrices $\mathscr{Q}(t) = 0$ for $t < i$, where $i \le \nu - 1$. From equation (21), we have

$$(23) \qquad 0 = Q_t(\mathscr{Q}(i)), \qquad 1 \le t < i.$$

This means that $0 = Q_t(q(i)_{jk})$ for all $t = 1, \dots, i-1$ and $j, k = 1, \dots, s$. As $\deg(q(i)_{jk}) = 2^i - 1$, we have $q(i)_{jk} \in K^H_{i-1}$, in the notation of §8. But $i - 1 \le \nu - 2$, so $K^H_{i-1} = 0$ by Corollary II.11; therefore $\mathscr{Q}(i) = 0$. This completes the inductive step. We now have that $\mathscr{Q}(i) = 0$ for $1 \le i \le \nu - 1$, so that $Q_i(\theta_j) = 0$ for $0 \le i \le \nu - 1$ and $1 \le j \le s$. This proves the first claim of the proposition.

Suppose now that in addition $m > 2^\nu - 2$ and $\mathscr{S}$ is invariant under Q_ν. Applying equation (21) as before, we find that $q(\nu)_{jk} \in K^H_{\nu-1}$. Though we can no longer conclude that $q(\nu)_{jk} = 0$, we do know from Corollary II.5 that $Q_\nu(q(\nu)_{jk}) = (q(\nu)_{jk})^2$ for all j, k. This means

$$(24) \qquad Q_\nu(\mathscr{Q}(\nu)) = \mathscr{Q}(\nu)^{[2]},$$

in the notation of §13. On the other hand, from equation (22) we have

$$(25) \qquad Q_\nu\mathscr{Q}(\nu) = \mathscr{Q}(\nu)^2.$$

The last two equations say that $\mathscr{Q}(\nu)^2 = \mathscr{Q}(\nu)^{[2]}$, so that $\mathscr{Q}(\nu)$ satisfies the conditions of Proposition II.27 and its corollary, as a matrix with coefficients in $k[y_1, \dots, y_d] \supset (k[y_1, \dots, y_d])^H$. Therefore its action on $\mathscr{V}\{\theta_1, \dots, \theta_s\}$ is diagonalizable, and the diagonalized matrix is H-invariant. The eigenvectors $\theta'_1, \dots, \theta'_s$ forming the new basis for $\mathscr{V}\{\theta_1, \dots, \theta_s\}$ are H-invariant and are killed by $Q_1, \dots, Q_{\nu-1}$ as above. □

Before looking at the implication of Proposition III.1 for groups of type I, we prove an analogous result describing independent sets which are invariant not under the first few Q_i's but under the first few Sq^{2^i}'s. Proposition III.2 will play a role later on in the discussion of groups of type II.

Proposition III.2. *Let $G = H \ltimes_\tau E_d$, and suppose that $\mathscr{S} = \{\theta_1, \dots, \theta_s\} \subset (k[y_1, \dots, y_d])^H$ is a level independent set in degree $m > 2^{t+1}$ where t is defined by $2^{t-1} < \nu \le 2^t$. Suppose $\mathscr{S}$ is invariant under Sq^{2^i} for $0 \le i \le t$. Then $Sq^{2^i}(\xi) = 0$ for all ξ in the linear span $\mathscr{V}\{\theta_1, \dots, \theta_s\}$ and all i, $0 \le i \le t-1$. Moreover, $\mathscr{V}\{\theta_1, \dots, \theta_s\}$ has a basis $\theta'_1, \dots, \theta'_s$ such that for $1 \le j \le s$, $Sq^{2^t}(\theta'_j) = \mu_j\theta'_j$ for suitable $\mu_j \in k[y_1, \dots, y_d]^H_{(2^t)}$.*

Proof. This time we define elements $p(i)_{jk} \in k[y_1, \dots, y_d]^H_{(2^i)}$ by $Sq^{2^i}(\theta_j) = \sum_{k=1}^s p(i)_{jk}\theta_k$, and let $\mathscr{P}(i)$ be the matrices $(p(i)_{jk})$; as before, these matrices are well-defined provided $0 \le i \le t$. By Corollary I.6, $\mathscr{P}(i) = 0$ for $0 \le i \le t-1$, so from Fact I.8 we have $Sq^a(\Theta) = 0$ for $1 \le a \le 2^t - 1$. It then follows from the Adem relations that

$$\begin{aligned} 0 &= Sq^{2^t}Sq^{2^t}(\Theta) = Sq^{2^t}(\Theta\mathscr{P}(t)) \\ &= (\Theta\mathscr{P}(t))\mathscr{P}(t) + \Theta(Sq^{2^t}\mathscr{P}(t)) = \Theta(\mathscr{P}(t)^2 + \mathscr{P}(t)^{[2]}). \end{aligned}$$

As $2^{t+1} < m$, we conclude from this matrix equation that $0 = \mathscr{P}(t)^2 + P(t)^{[2]}$. The rest follows as in the proof of Proposition III.1. □

Propositions III.1 and III.2 give information about level Q- and $\mathscr{A}(2)$-invariant independent sets of sufficiently high degree. The following special case of a result from [Car81] provides an estimate for the degrees of those level Q-invariant independent sets which contain d elements, that is, of Q-invariant l.s.o.p.'s.

Proposition III.3 [Car81]. *Suppose $\mathscr{S} = \{\theta_1, \dots, \theta_s\}$ is a Q-invariant l.s.o.p. of $(k[y_1, \dots, y_d])^H$ of degree m. Then $2h \mid m$.*

Using this estimate and Proposition III.1, we proceed to prove the main theorem for groups $\mathscr{G}$ containing subgroups of type I.

15. Main theorem, Part I

In view of Propositions III.1 and III.3, we have the following:

Proposition III.4. *Suppose $G = H \ltimes_\tau E_d$ is of type* I. *Then the algebra $H^*(G) \simeq (k[y_1, \dots, y_d])^H$ has no d-element $\mathscr{A}(2)$-invariant l.s.o.p.'s.*

Proof. By Proposition I.14, it suffices to prove that $P(G, d, m)$ holds for all even m, i.e. that any d-element $\mathscr{A}(2)$-invariant l.s.o.p. of even degree m consists entirely of squares. Suppose that $\mathscr{S} = \{\theta_1, \dots, \theta_d\}$ is such an l.s.o.p. As its degree is even, we have $Q_0(\theta_j) = 0$ for $1 \le j \le d$. Moreover, $m > h = 2^d - 1$ by Proposition III.3, and as G is of type I, $\nu = d$. It follows from Proposition III.1 that $Q_i(\theta_j) = 0$ for $1 \le i \le d-1$ and $1 \le j \le d$. By Proposition I.10, θ_j is a square for $1 \le j \le d$. This proves the proposition. □

We can now prove

Theorem III.5 (Main Theorem, Part I). *Suppose the group $\mathscr{G}$ contains a subgroup $G = H \ltimes_\tau E_d$ of type* I. *Then $\mathscr{G}$ does not act freely and k-cohomologically trivially on any finite complex $X \sim_2 (S^n)^d$, for any n.*

Proof. Immediate from Theorem I.13 and Proposition III.4. □

16. Q-invariant independent sets, Part II

Let $G = H \ltimes_\tau E_4$ be a group of type II, and let $\mathscr{S} = \{\theta_1, \dots, \theta_s\}$ be a Q-invariant l.s.o.p. of $(k[y_1, \dots, y_4])^H$ in degree m. Proposition III.1 says that the linear span $\mathscr{V}\{\theta_1, \dots, \theta_s\}$ has a basis $\mathscr{S}' = \{\theta'_1, \dots, \theta'_s\}$ consisting of eigenvectors for Q_i, $0 \le i \le 2$, provided $m > 6$. In the next few sections we show, first, that if $m > 14$, then the θ'_j are in fact eigenvectors for Q_3 as well, and are therefore Q-eigenvectors; and second, that if in addition $\mathscr{S}$ is actually a $\mathscr{A}(2)$-invariant l.s.o.p. and $m \ne 5 \cdot 2^t$ for any t, then these eigenvectors must in fact be squares.

Suppose then that $m > 14$, and that $\mathscr{S}$ is a Q-invariant l.s.o.p. in degree m; let $\mathscr{S}'$ be as above. Let $\mathscr{Q}(u)$, $0 \le u \le 3$, be the matrices for the Q_u in the basis $\{\theta'_1, \dots, \theta'_s\}$ as in §14. Then $\mathscr{Q}(1) = 0$ and $\mathscr{Q}(2)$ is diagonal. The degree conditions for equations (21) and (22) of §14 are now satisfied for

$t = 1, 2$ and $u = 3$, and these equations give

$$Q_1(\mathscr{Q}(3)) = 0, \tag{26}$$

$$Q_2(\mathscr{Q}(3)) + Q_3(\mathscr{Q}(2)) = [\mathscr{Q}(2), \mathscr{Q}(3)], \tag{27}$$

$$Q_3(\mathscr{Q}(3)) = \mathscr{Q}(3)^2. \tag{28}$$

We use these equations first to restrict the monomials that can appear in the off-diagonal elements of $\mathscr{Q}(3)$, and then to show that these elements are in fact 0. This will mean that $\mathscr{Q}(3)$ is diagonal and the θ'_j's are Q-eigenvectors.

Taking the (i, j)th coordinate of the matrices in equation (27) gives, for $i \neq j$,

$$Q_2(q(3)_{ij}) = (q(2)_{ii} + q(2)_{jj})q(3)_{ij}, \tag{29}$$

as $\mathscr{Q}(2)$ is diagonal. If $q(2)_{ii} + q(2)_{jj} = 0$, then $Q_2(q(3)_{ij}) = Q_1(q(3)_{ij}) = 0$, so $q(3)_{ij} \in K_2^H$, in the notation of §8. But $K_2^H = 0$ by Corollary II.11, and therefore $q(3)_{ij} = 0$.

We now consider the case $q(2)_{ii} + q(2)_{jj} \neq 0$, and check that $q(3)_{ij} = 0$ here as well. We do so by showing that $\mathrm{Mon}(q(3)_{ij}) = \varnothing$.

Equation (26) and its analogue $Q_1(\mathscr{Q}(2)) = 0$ say that $Q_1(q(2)_{ij}) = Q_1(q(3)_{ij}) = 0$ for all $1 \le i, j \le 4$. Thus by Lemma II.13 each monomial of $q(2)_{ij}$ and $q(3)_{ij}$ is of the form $(x_{i_0} x_{i_1 - 1}^2) x_{i_2} \cdots x_{i_r} \lambda^2$ for suitable x_{i_k} and λ. These monomials must all be H-invariant, since the polynomials $q(2)_{ij}$ and $q(3)_{ij}$ are.

Notation. For typographical convenience, we write $(a_0\, a_1 \cdots a_{d-1})$ to represent the monomial $x_0^{a_0} \cdots x_{d-1}^{a_{d-1}}$.

One may easily check that the only possible monomials of $q(2)_{ij}$ are $(2\ 0\ 0\ 1)$ and its conjugates under Γ, and the only possibilities for $\mathrm{Mon}(q(3)_{ij})$ are

$$(6\ 0\ 1\ 0), \quad (4\ 3\ 0\ 0), \quad (4\ 0\ 2\ 1), \quad (3\ 2\ 2\ 0) \tag{30}$$

and their conjugates under Γ.

Notation. Henceforth, we write $p(2)_{ij}$ for $q(2)_{ii} + q(2)_{jj}$.

From the above paragraph, we have $p(2)_{ij} = \sum_{n=0}^{3} c^{\gamma^n} (2\ 0\ 0\ 1)^{\gamma^n}$ for some $c \neq 0$. Equation (29) becomes

$$Q_2(q(3)_{ij}) = p(2)_{ij} q(3)_{ij}. \tag{31}$$

We now ask which monomials may appear in equation (31). Any monomial of $Q_2(q(3)_{ij})$ must be conjugate to one of

$$(10\ 0\ 0\ 0), \quad (4\ 2\ 0\ 4), \quad \text{and} \quad (2\ 2\ 6\ 0),$$

and any monomial of $p(2)_{ij} q(3)_{ij}$ is conjugate to a product of $(2\ 0\ 0\ 1)$ with one of the monomials of equation (30). One may check that the monomial $(8\ 0\ 1\ 1) = (2\ 0\ 0\ 1)(6\ 0\ 1\ 0)$ is conjugate to such a product in exactly one way. Writing λ for the coefficient of $(6\ 0\ 1\ 0)$ in $q(3)_{ij}$, we see that the coefficient of $(8\ 0\ 1\ 1)$ on the left side of equation (30) is λc and its coefficient on the right side is 0; as $c \neq 0$, we conclude that $\lambda = 0$. That is, $(6\ 0\ 1\ 0)$, and likewise its conjugates, does not appear in $q(3)_{ij}$ after all. The same argument using $(5\ 5\ 0\ 0) = (1\ 2\ 0\ 0)(4\ 3\ 0\ 0)$ in place of $(8\ 0\ 1\ 1)$ shows that $(4\ 3\ 0\ 0)$ and its conjugates do not appear either, in any off-diagonal element $q(3)_{ij}$.

It remains to eliminate the monomials $(4\ 0\ 2\ 1)$ and $(3\ 2\ 2\ 0)$ and their conjugates. We do so using equation (28). Looking at the i, j-coordinate, we find that

$$Q_3(q(3)_{ij}) = \sum_{k=1}^{4} q(3)_{ik} q(3)_{kj}. \tag{32}$$

Recall that

$$\mathrm{Mon}(q(3)_{ab}) \subset \begin{cases} \{(4\ 0\ 2\ 1)^\gamma, (3\ 2\ 2\ 0)^\gamma | \gamma \in \Gamma\}, & a \neq b, \\ \{(4\ 0\ 2\ 1)^\gamma, (3\ 2\ 2\ 0)^\gamma, (6\ 0\ 1\ 0)^\gamma, (0\ 0\ 4\ 3)^\gamma | \gamma \in \Gamma\}, & a = b. \end{cases}$$

One may easily check that the monomial $(2\ 10\ 2\ 0) = Q_3(3\ 2\ 2\ 0)$ does not appear in the right-hand side of equation (32) at all. It follows that its coefficient in $Q_3(q(3)_{ij})$, which is its coefficient in $q(3)_{ij}$, vanishes, and hence that $(3\ 2\ 2\ 0) \notin \mathrm{Mon}(q(3)_{ij}) \subset \{(4\ 0\ 2\ 1)^\gamma | \gamma \in \Gamma\}$. Referring again to equation (31), we find by studying the coefficient of, say, $(2\ 2\ 6\ 0)$, that the coefficients of $(4\ 0\ 2\ 1)$ and its conjugates in $q(3)_{ij}$ must vanish as well. Thus we have that $q(3)_{ij} = 0$ whenever $p(2)_{ij} \neq 0$. We have already seen that $q(3)_{ij} = 0$ whenever $p(2)_{ij} = 0$ and $i \neq j$, and therefore we conclude that $\mathscr{Q}(3)$ is diagonal as asserted.

Thus the θ'_j are all Q-eigenvectors. From Corollary II.22, we have that $\theta'_j = \phi_j^2 \rho_j$ for all j, where $\phi_j \in (k[y_1, \ldots, y_4])^H$ and ρ_j is a product over orbits of H on $\mathscr{L}$.

Suppose now that m is even. Because h is odd, each ρ_j must be a product over an even number of orbits. Now there are only three orbits of G on $\mathscr{L}$, and as the θ_j form an independent sequence, they have no common factors and the orbits associated to them must be distinct. Without loss of generality, then, $\theta'_j = \phi_j^2$ for $j \leq s-1$, and $\theta'_s = \phi_s^2 \rho$ where ρ is either 1 or a 2-orbit nonsquare.

We have proven

Proposition III.6. *Suppose $(k[y_1, \ldots, y_4])^H$ has a Q-invariant independent sequence $\mathscr{S} = \{\theta_1, \ldots, \theta_s\}$ in degree $m > 14$. Then there is a basis $\mathscr{S}' = \{\theta'_1, \ldots, \theta'_s\}$ of $\mathscr{V}\{\theta_1, \ldots, \theta_s\}$ such that $\theta'_j = \phi_j^2 \rho_j$ for $1 \leq j \leq s$, where ρ_j is a (possibly trivial) product over orbits of H on $\mathscr{L}$. If m is even, then w.l.o.g. $\theta'_j = \phi_j^2$ for $1 \leq j \leq s-1$, and $\theta'_s = \phi_s^2 \rho$ where ρ is either 1 or a 2-orbit nonsquare.*

The rest of Part III will be devoted to demonstrating that if $\mathscr{S}$ is a $\mathscr{A}(2)$-invariant l.s.o.p. and m is not of the form $2^t \cdot 5$, then the second possibility cannot in fact occur. This will prove $P(G, d, m)$ for such m and groups G of type II.

17. $\mathscr{A}(2)$-INVARIANT L.S.O.P.'S

In this section, we prove a proposition which will later be used as the inductive step in a description of the $\mathscr{A}(2)$-invariant l.s.o.p.'s in $H^*(G)$ for G of type II.

Lemma III.7. *Let G be a group of type* II, *and let $l \geq 1$ be an integer. Suppose $\mathscr{S} = \{\theta_1, \ldots, \theta_4\} \subset (k[y_1, \ldots, y_d])^H$ is a $\mathscr{A}(2)$-invariant l.s.o.p. of degree m. Suppose that the $\theta_j = \psi_j^{2^l}$ are 2^l-powers, $1 \leq j \leq 3$, and $\theta_4 = \sigma^{2^l}\pi$ is a 2^l-power times a 2-orbit nonsquare. Then for i such that $0 \leq i \leq 2$ and $2^{l+i} + 2^{l+2} - 2^{l-1} < m$, the ideal $\mathscr{I}\{\theta_1, \theta_2, \theta_3\}$ is invariant under $Sq^{2^{l+i}}$ (equivalently, the ideal $\mathscr{I}\{\psi_1, \psi_2, \psi_3\}$ is invariant under Sq^{2^i}).*

Proof. Suppose that i satisfies the conditions of the lemma. Since the ideal $\mathscr{I}\{\theta_1, \ldots, \theta_4\}$ is $\mathscr{A}(2)$-invariant, there exist elements

$$a(l+i)_{jk} \in k[y_1, \ldots, y_4]^H_{(2^{l+i})}, \qquad 1 \leq j \leq 3,$$

such that

$$(Sq^{2^i}\psi_j)^{2^l} = Sq^{2^{i+l}}\theta_j = \sum_{k=1}^{4} a(l+i)_{jk}\theta_k. \tag{33}$$

We verify now that Proposition II.24 and its corollary apply to this situation. Indeed, we have

$$\deg(a(l+i)_{jk}) + 2^{l+(4-2)} - 2^{l-1} = 2^{l+i} + 2^{l+2} - 2^{l-1} < m,$$

and in addition, $\deg(\pi^{\langle l \rangle}) \geq 2^l \cdot 5$ by Lemma II.17, so that $\deg(a(l+i)_{jk}) \leq 2^{l+2} < \deg(\pi^{\langle l \rangle})$. Proposition II.24 and Corollary II.25 then give, for $1 \leq j \leq 3$,

(34)

$$a(l+i)_{jk} = \begin{cases} (\alpha(l+i)_{jk})^{2^l} \text{ for some } \alpha(l+i)_{jk} \in k[y_1, \ldots, y_4]^H_{(2^i)}, & 1 \leq k \leq 3, \\ 0, \quad k = 4. \end{cases}$$

In view of equation (33), equation (34) means that the ideal $\mathscr{I}(\theta_2, \theta_2, \theta_3)$ is invariant under $Sq^{2^{l+i}}$ for $0 \leq i \leq 2$. Taking (2^l)th roots of equation (33) now gives

$$Sq^{2^i}\psi_j = \sum_{k=1}^{3} \alpha(l+i)_{jk}\psi_k,$$

so that the ideal $\mathscr{I}(\psi_1, \psi_2, \psi_3)$ is invariant under Sq^{2^i}. □

Proposition III.8. *Let G be a group of type* II, *and let $l \geq 1$ be an integer. Suppose $\mathscr{S} = \{\theta_1, \ldots, \theta_4\} \subset (k[y_1, \ldots, y_4])^H$ is a $\mathscr{A}(2)$-invariant l.s.o.p. of degree m such that the $\theta_j = \psi_j^{2^l}$ are 2^l-powers, $1 \leq j \leq 3$, and $\theta_4 = \sigma^{2^l}\pi$ is a 2^l-power times a 2-orbit nonsquare. If $m > 14 \cdot 2^l$, then in fact $\theta_j = \phi_j^{2^{l+1}}$ is a 2^{l+1}-power, $1 \leq j \leq 3$, and $\theta_4 = \tau^{2^{l+1}}\rho$ is a 2^{l+1}-power times a 2-orbit nonsquare.*

Proof. We begin by showing that θ_j is a 2^{l+1}-power, $1 \leq j \leq 3$. We may assume that π has no factors of multiplicity $\geq 2^l$. Now for $0 \leq i \leq 2$ we have

$$2^{l+i} + 2^{l+2} - 2^{l-1} \leq 2^{l+3} - 2^{l-1} < m,$$

so that by Lemma III.7, the ideal $\mathscr{I}\{\psi_1, \psi_2, \psi_3\}$ is invariant under Sq^{2^i} for $0 \leq i \leq 2$. The ideal is therefore invariant under Q_i for $0 \leq i \leq 3$. Now the ψ_j, being (2^l)th roots of an independent set, themselves form an independent set, the degree of which is $m/2^l > 14$ by hypothesis. Thus by Proposition

III.6, there exists a basis $\{\psi_1', \psi_2', \psi_3'\}$ for $\mathscr{V}(\psi_1, \psi_2, \psi_3)$ such that each ψ_j' is of the form $\psi_j' = \xi_j^2 \rho_j$ for some ξ_j and some square-free product ρ_j over H-orbits on $\mathscr{L}$. Now there are only three products of H-orbits on $\mathscr{L}$, and two of these divide θ_4 by assumption. Since the θ_j's form an independent set, they have no common factors, and so w.l.o.g. $\rho_1 = \rho_2 = 1$ and ρ_3 is either 1 or a product over a single orbit, hence of odd order h. But since $\psi_1' = \xi_1^2$ is a square, the common degree of the ψ_j' is even, which means that $\deg(\rho_3)$ must be even. Thus $\rho_3 = 1$ as well, so that all three of the ψ_j' are squares. Therefore the original ψ_j's, which are linear combinations of the ψ_j''s, are themselves squares; say $\psi_j = \phi_j^2$. We conclude that for $1 \le j \le 3$, $\theta_j = \psi_j^{2^l} = \phi_j^{2^{l+1}}$ is a 2^{l+1}-power, as asserted.

It remains to show that $\theta_4 = \sigma^{2^l}\pi$ actually factors as $\theta_4 = \tau^{2^{l+1}}\rho$ with ρ a 2-orbit nonsquare. To begin with, I claim that σ^{2^l} divides $Sq^{2^s}(\sigma^{2^l})$ for $0 \le s \le l+2$. This is proved by induction on s. The cases $s < l$ are trivial, as Sq^{2^s} acts trivially on 2^{s+1}-powers by Fact I.8. Suppose now that σ^{2^l} divides $Sq^{2^q}(\sigma^{2^l})$ for $q < s$. Since the Steenrod algebra $\mathscr{A}(2)$ is generated by $\{Sq^{2^q}\}_{q=0}^{\infty}$, we have in fact that σ^{2^l} divides $Sq^r(\sigma^{2^l})$ for $1 \le r \le 2^s - 1$. Bearing in mind that π is an eigenvector for $\mathscr{A}(2)$, define the polynomials $\{\lambda_r\}_{r=0}^{2^s-1}$ and $\{\mu_r\}_{r=0}^{2^s} \subset \hat{k}[x_0, \dots, x_{d-1}]^H_{(r)}$ by

$$Sq^r(\sigma^{2^l}) = \lambda_r \sigma^{2^l} \quad \text{and} \quad Sq^r(\pi) = \mu_r \pi. \tag{35}$$

Since the ideal generated by $\mathscr{S}$ is $\mathscr{A}(2)$-invariant, we can also define elements $a(s)_k \in \hat{k}[x_0, \dots, x_{d-1}]^H_{(2^s)}$ by $Sq^{2^s}(\theta_4) = \sum_{k=1}^4 a(s)_k \theta_k$. Using the Cartan relations, we now write

$$\begin{aligned}\sum_{k=1}^{4} a(s)_k \theta_k = Sq^{2^s}\theta_4 &= \sum_{r=0}^{2^s} Sq^r(\sigma^{2^l}) Sq^{2^s - r}(\pi) \\ &= \sum_{r=0}^{2^s-1} (\lambda_r \mu_{2^s - r} \sigma^{2^l}\pi) + Sq^{2^s}(\sigma^{2^l})\pi.\end{aligned}$$

Collecting terms with a factor of π, we find that

$$\kappa\pi \overset{\text{def}}{=} \left[a(s)_4 \sigma^{2^l} + \sum_{r=0}^{2^s-1} \lambda_r \mu_{2^s-r}\sigma^{2^l} + Sq^{2^s}(\sigma^{2^l}) \right] \pi = \sum_{k=1}^{3} a(s)_k \theta_k, \tag{36}$$

where κ is defined to be the coefficient of π in equation (36). Multiplying through by σ^{2^l}, we find that

$$\kappa\theta_4 + \sum_{k=1}^{3} a(s)_k \sigma^{2^l}\theta_k = 0. \tag{37}$$

Equation (37) gives a relation between the θ_j's whose coefficients are of degree

$$\deg(\kappa) = 2^s + \deg(\sigma^{2^l}) = 2^s + m - \deg(\pi).$$

But $\deg(\pi) \ge 2^l \cdot 5 > 2^{l+2} \ge 2^s$ by Lemma II.17, and thus we have $\deg(\kappa) < m = \deg(\theta)$. As the θ's form an independent set, Fact I.2 implies that the coefficients, and in particular κ, must vanish. Viewing equation (36), in which κ was defined, modulo σ^{2^l}, we find that σ^{2^l} divides $Sq^{2^s}(\sigma^{2^l})$. This completes the induction step and proves the claim.

Now for $0 \leq \beta \leq 2$ we have $\sigma^{2^l} \mid Sq^{2^{l+\beta}}(\sigma^{2^l}) = (Sq^{2^\beta}(\sigma))^{2^l}$, the equality holding as in Fact I.8. Taking (2^l)th roots, we find that σ divides $Sq^{2^\beta}(\sigma)$ for $0 \leq \beta \leq 2$. From this it follows that σ divides $Q_\beta(\sigma)$ for $0 \leq \beta \leq 3$, so that by Corollary II.22, we have that $\sigma = \tau^2\pi_0$ for some polynomial τ and some product π_0 of linear factors. Thus $\theta_4 = \sigma^{2^l}\pi = \tau^{2^{l+1}}\pi_0^{2^l}\pi$. We take $\pi' = \pi_0^{2^l}\pi$ to prove the proposition. □

18. Main theorem, Part II

In this section, we use Proposition III.8 to complete the proof of the main theorem.

Proposition III.9. *Let $H \simeq \mathbf{Z}/(5)$, and let $G = H \ltimes_\tau E_4$ be a group of type* II.

1. *If m is an integer not of the form $2^t \cdot 5$, then $P(G, 4, m)$ is true.*
2. *If $m = 2^t \cdot 5$ for some $t \geq 2$ and $\mathcal{S} = \{\theta_1, \dots, \theta_4\}$ is a 4-element l.s.o.p. of $H^*(G)$ in degree m, then either θ_j is a square for all i, or else the linear span $\mathcal{V}\{\theta_1, \dots, \theta_4\}$ has a basis $\phi_1, \dots, \phi_d$ such that*

$$\phi_j = \psi_j^{2^{t-1}}, \quad 1 \leq j \leq 3; \qquad \phi_4 = \psi_4^{2^{t-1}}\rho,$$

where ρ is a 2-orbit nonsquare and the elements $\psi_1, \dots, \psi_3 \in k[y_1, \dots, y_4]^H_{(10)}$ satisfy the conditions $Sq^1(\psi_j) = 0$ and $\psi_j \mid Sq^2(\psi_j)$, and generate an ideal invariant under Sq^4.

Proof. Note that by Proposition III.3, the proposition is trivially true if m is not a multiple of 10. Now fix $m = 10n \geq 20$, and let $\mathcal{S} = \{\theta_1, \dots, \theta_4\}$ be an $\mathcal{A}(2)$-invariant l.s.o.p. of $(k[y_1, \dots, y_4])^H$. By Proposition III.6, the linear span $\mathcal{V}\{\theta_1, \dots, \theta_4\}$ has a basis $\theta'_1, \dots, \theta'_4$ such that $\theta'_j = \phi_j^2$ for $1 \leq j \leq 3$ and $\theta'_4 = \phi_4^2\rho$ where ρ is either 1 or a 2-orbit nonsquare. If $\rho = 1$, then $\theta'_1, \dots, \theta'_4$ are all squares, and consequently the $\theta_1, \dots, \theta_4$ are all squares as well, being linear combinations in characteristic 2 of the θ'_j's.

Suppose then that ρ is a 2-orbit nonsquare. We now apply Proposition III.8 as long as the degree condition is satisfied. If l is defined by

$$14 \cdot 2^{l-1} < m \leq 14 \cdot 2^l, \tag{38}$$

we find that $\mathcal{V}\{\theta_j, \dots, \theta_4\}$ has a basis $\phi_1, \dots, \phi_d$ such that $\phi_j = \psi_j^{2^l}$ for $1 \leq j \leq 3$ and $\phi_4 = \psi_4^{2^l}\sigma$ for some polynomials $\psi_j \in (k[y_1, \dots, y_4])^H$ and some 2-orbit nonsquare σ. Now $m = 2^l \deg(\psi_1)$ is divisible by 2^l, and m is divisible by 5 by Proposition III.3, so we may write $m = 2^l \cdot 5c$ for some integer c. From equation (38), we have $\frac{7}{5} < c \leq \frac{14}{5}$, so that $c = 2$ and $m = 2^{l+1} \cdot 5$.

If in fact m is not of the form $2^t \cdot 5$, then the above argument shows that to assume that $\rho \neq 1$ leads to a contradiction. Thus $P(G, d, m)$ holds for m not of this form. If, on the other hand, $m = 2^{l+1} \cdot 5 \geq 20$, we apply first Lemma III.7 and then Proposition III.2 to the situation of the previous paragraph to see that indeed the ψ_j have the properties claimed. □

Corollary III.10. *Let G be a group of type* II, *and let m be an integer not of the form $2^t \cdot 5$. Then $H^*(G) \simeq (k[y_1, \dots, y_4])^H$ has no $\mathscr{A}(2)$-invariant l.s.o.p.'s in degree m.*

Proof. Follows in view of Proposition I.14. □

Finally, we have

Theorem III.11 (Main Theorem, Part II). *Suppose that the group $\mathscr{G}$ contains a subgroup $G \simeq \mathbf{Z}/(5) \ltimes_\tau E_4$ of type* II, *and let m be an integer such that $m \neq 2^t \cdot 5$ for all t. Then $\mathscr{G}$ does not act freely and k-cohomologically trivially on any finite complex $X \sim_2 (S^{m-1})^4$.*

Proof. Immediate from Theorem I.13 and Proposition III.10. □

References

[AB88] A. Adem and W. Browder, *The free rank of symmetry of* $(S^n)^k$, Invent Math. **92** (1988), 431–440.

[AW80] J. F. Adams and C. W. Wilkerson, *Finite H-spaces and algebras over the Steenrod algebra*, Ann. of Math. **111** (1980), 95–143.

[Car80] G. Carlsson, *On the non-existence of free actions of elementary abelian groups on products of spheres*, Amer. J. Math. **102** (1980), 1147–1157.

[Car81] ——, *Some restrictions on finite groups acting freely on* $(S^n)^k$, Trans. Amer. Math. Soc. **264** (1981), 449–457.

[CS] H. E. A. Campbell and P. S. Selick, *Polynomial algebras over the Steenrod algebra*, Comment. Math. Helv. **65** (1990), 171–180.

[Oli78] R. Oliver, *Free compact group actions on products of spheres*, Proc. Aarhus Sympos. on Algebraic Topology, Springer-Verlag, 1978, pp. 539–548.

[Ser65a] J.-P. Serre, *Algèbre locale. Multiplicités*, Springer-Verlag, 1965.

[Ser65b] ——, *Sur la dimension cohomologique des groupes finis*, Topology **3** (1965), 412–420.

[Woo86] R. M. W. Wood, *Splitting* $\Sigma(\mathbf{C}P^\infty \times \cdots \times \mathbf{C}P^\infty)$ *and the action of Steenrod squares* Sq^i *on the polynomial ring* $\mathbf{F}_2[x_1, \dots, x_n]$, Algebraic Topology, Barcelona, Lecture Notes in Math., Vol. 1298, Springer, Berlin and New York, 1986, pp. 237–255.

Department of Mathematics, University of Michigan, Ann Arbor, Michigan 48109
E-mail address: judith.silverman@math.lsa.umich.edu