DECOMPOSING SYMMETRIC POWERS OF MODULAR REPRESENTATIONS OF ELEMENTARY ABELIAN $p$-GROUPS

JONATHAN ELMER

Abstract. Let $G$ be a elementary abelian $p$-group of order $q = p^n$. Let $V$ be a faithful indecomposable modular representation of $G$ with dimension 2. We consider representations of the form $S^d(S^m(V^*))$. In particular we prove that $S^d(S^m(V^*))$ is projective whenever $d + m \geq q$, and either $d < p$ and $m < q$ or $m < p$ and $d < q$. More generally we show that if $d + m \geq q$ and $d < q$, $m < q$, then each summand of $S^d(S^m(V^*))$ is induced from a subgroup of $G$, and that if $m < q$ then modulo induced modules, the sequence $S^d(S^m(V^*))_{i \geq 0}$ is periodic with period $q$. Our results generalise results of Almkvist and Fossum [1] for modular representations of cyclic groups of prime order. We also give some applications to invariant theory.

1. Introduction

Let $G$ be a finite group and let $V$ and $W$ be finite-dimensional representations of $G$ over a field $k$, which in this article will always mean a left $kG$-module. Let $v_1, v_2, \ldots, v_n$ and $w_1, w_2, \ldots, w_m$ be bases of $V$ and $W$ over $k$. Then the tensor product $V \otimes W$ of $V$ and $W$ is the $k$-vector space spanned by elements of the form $v_i \otimes w_j$, where scalar multiplication satisfies $\lambda(v_i \otimes w_j) = (\lambda v_i) \otimes w_j = v_i \otimes (\lambda w_j)$ for all $\lambda \in k$. There is a linear action of $G$ on the space defined by $g(v \otimes w) = gv \otimes w + v \otimes gw$. We can take the tensor product of $V$ with itself, and iterate the construction $d$ times to obtain, for any natural number $d$, a module $T^d(V) = V \otimes \cdots \otimes V$, called the $d$th tensor power of $V$. Formally, the $d$th symmetric power $S^d(V)$ of $V$ is defined to be the quotient of $T^d(V)$ by the subspace generated by elements of the form $v_1 \otimes \cdots \otimes v_d - v_{\sigma(1)} \otimes \cdots \otimes v_{\sigma(d)}$ where $\sigma \in \Sigma_d$, the symmetric group on $\{1, 2, \ldots, d\}$.

Let $V$ be a representation of $G$ over $k$ and denote by $V^*$ the $k$-vector space dual to $V$. We define an action of $G$ on $V^*$ by $g \phi(v) = \phi(g^{-1}v)$, which makes $V^*$ into a left $kG$-module. One also sometimes considers the subspace of $T^d(V)$ fixed by the natural action of $\Sigma_d$. This is called the $d$th divided power, $D^d(V)$ of $V$. If $d!$ is invertible in $k$ then the $kG$-modules $D^d(V)$ and $S^d(V)$ are naturally isomorphic. More generally they are related by $S^d(V^*) \cong D^d(V)^*$.

Symmetric powers of modules have a natural interpretation as the homogeneous components of the action of $G$ on a polynomial ring. In more detail, let $V$ be a finite-dimensional $kG$-module and let $V^*$ denote its dual. Define a basis $x_1, x_2, \ldots, x_m$ of $V^*$. The action of $G$ on $V^*$ induces an action on the graded polynomial algebra $k[x_1, x_2, \ldots, x_m]$ by degree-preserving algebra automorphisms. Then for $d \geq 1$, the $d$th symmetric power $S^d(V^*)$ is the homogeneous component of the finite-dimensional $kG$-module $k[x_1, x_2, \ldots, x_m]$ of degree $d$. Since the action of $G$ on the set of constants is trivial, we set $S^0(V^*) = k$. Provided $k$ is infinite, $S(V^*) = \cdots$
Theorem 1.1 (Almkvist and Fossum). Let \( G = C_p \) be a cyclic group of prime order \( p \) and let \( \mathbb{k} \) be a field of characteristic \( p \). Let \( V \) be the unique indecomposable representation of \( G \) over \( \mathbb{k} \) with dimension 2 (with action given by a Jordan block of size two).

(i) (Projectivity) Suppose \( m, d < p \) and \( m + d \geq p \). Then \( S^d(S^m(V)) \) is projective.

(ii) (Periodicity) For any \( m, d < p \) and any \( r \) we have a \( kG \)-isomorphism \( S^{m+d}(S^m(V)) \cong S^d(S^m(V)) + \text{ projective modules} \).

(iii) (Reciprocity) We have a \( kG \)-isomorphism \( S^d(S^m(V)) \cong S^m(S^d(V)) \).

Of course, in determining the indecomposable summands of any modular representation of \( C_p \), one is helped enormously by the fact that we have a classification of indecomposable representations. Indeed, the modules \( S^d(V) \) for \( 0 \leq d < p \), form a complete set of isomorphism classes of indecomposable modular representations for \( C_p \). Furthermore, each has a \( C_p \)-fixed subspace of dimension 1, and so the number of indecomposable summands in a given representation is equal to the dimension of the subspace fixed by \( C_p \).

For representations of elementary abelian \( p \)-groups, neither of these helpful results hold. In fact, if \( G \) is an elementary abelian \( p \)-group of order \( p^n \), then unless \( n = 1 \) or \( p = n = 2 \), the representation type of \( G \) is “wild”; essentially this means that there is no hope of classifying the indecomposable representations up to isomorphism.

We now state our main results. Let \( k \) be any field of characteristic \( p \). Let \( E \) be a subgroup of the additive group of \( k \) with order \( q = p^n \). Then \( E \) acts naturally on a 2-dimensional \( k \)-vector space \( V \) as left-multiplication by the matrices

\[
\begin{bmatrix}
1 & \alpha \\
0 & 1
\end{bmatrix},
\]

where \( \alpha \in E \). Note that, since every elementary abelian subgroup of \( GL_2(k) \) is conjugate to a subgroup of the upper triangular unipotent group, every indecomposable representation of an elementary abelian \( p \)-group of dimension 2 is isomorphic to one of the above form.

Theorem 1.2. Suppose \( d + m \geq q, m < p \) and \( d < q \). Then the \( kE \)-module \( S^d(S^m(V)^*) \) is projective.
Note that the modules $S^m(V)$ for $m < p$ are self-dual, so the above generalises the projectivity part of Theorem 1.1. This is also true of the following result:

**Theorem 1.3.** Suppose $d + m \geq q$, $m < q$ and $d < p$. Then the $kE$-module $S^d(S^m(V)^*)$ is projective.

Note that the modules $S^m(V)$ are not in general self-dual for $p \leq m < q$. Therefore the following result is not equivalent to the above; nevertheless, it may be proved in a similar fashion:

**Theorem 1.4.** Suppose $d + m \geq q$, $m < q$ and $d < p$. Then the $kE$-module $S^d(S^m(V))$ is projective.

We also obtain the following result, which generalises the periodicity part of 1.1.

**Theorem 1.5.** Let $E$ be an elementary abelian group of order $q$ and $V$ a $2$-dimensional indecomposable $kE$-module. Let $m < p$ and $d < q$. Then for any $l$ we have an isomorphism of $kE$-modules

$$S^{d+l}(S^m(V)^*) \cong S^d(S^m(V)^*) \oplus \text{projective modules}.$$ 

2. Relative projectivity and the relative stable module category

In this section, we fix a prime $p > 0$ and let $G$ be a finite group of order divisible by $p$. Let $k$ be a field of characteristic $p$ and let $\mathcal{X}$ be a set of subgroups of $G$. Now let $M$ be a $kG$-module. $M$ is said to be projective relative to $\mathcal{X}$ if the following holds: let $\phi : M \to Y$ be a $kG$-homomorphism and $j : \mathcal{X} \to Y$ a surjective $kG$-homomorphism which splits on restriction to any subgroup of $H \in \mathcal{X}$. Then there exists a $kG$-homomorphism $\psi$ making the following diagram commute.

$$\begin{array}{ccc}
X & \xrightarrow{j} & Y \\
\downarrow{\phi} & & \downarrow{0} \\
M & \xrightarrow{\psi} & Y
\end{array}$$

Dually, one says that $M$ is injective relative to $\mathcal{X}$ if the following holds: given an injective $kG$-homomorphism $i : X \to Y$ which splits on restriction to each $H \in \mathcal{X}$ and a $kG$-homomorphism $\phi : X \to M$, there exists a $kG$-homomorphism $\psi$ making the following diagram commute.

$$\begin{array}{ccc}
0 & \xrightarrow{i} & X \\
\downarrow{\phi} & & \downarrow{M} \\
Y & \xrightarrow{\psi} & M
\end{array}$$

These notions are equivalent to the usual definitions of projective and injective $kG$-modules when we take $\mathcal{X} = \{1\}$. We will say a $kG$-homomorphism is $\mathcal{X}$-split if it splits on restriction to each $H \in \mathcal{X}$. Note that, since a $kG$-module is projective relative to $H$ if and only if it is also projective relative to the set of all subgroups of $H$, we usually assume $\mathcal{X}$ is closed under taking subgroups.

Let $M$ be a left $kG$-module and $H$ a subgroup of $G$. We write $M^G$ for the set of $G$-fixed points in $M$. There is a natural map $M^H \to M^G$ defined as follows. Let $S$
be a set of left coset representatives of $H$ in $G$. Then for $v \in M^H$ we define

\[ \text{Tr}^G_H(v) = \sum_{\sigma \in S} \sigma v. \]

This is called the transfer or trace map. Given $kG$-modules and $M$ and $N$, there is a natural left action of $G$ on $\text{Hom}_k(M, N)$ defined by

\[ (\sigma \cdot \alpha)v = \sigma \alpha(\sigma^{-1}v). \]

We write $(M, N)$ for $\text{Hom}_k(M, N)$, so that $(M, N)^G = \text{Hom}_G(M, N)$. If $H$ is a subgroup of $G$, we have a map $\text{res}^G_H : (M, N)^G \to (M, N)^H$ obtained by restricting homomorphisms. Then the map $\text{Tr}^G_H : (M, N)^H \to (M, N)^G$ is defined as

\[ \text{Tr}^G_H(\alpha)(v) = \sum_{\sigma \in S} \sigma \alpha(\sigma^{-1}v). \]

We note the following properties of transfer:

**Lemma 2.1.**

1. Let $\alpha \in (M, N)^H$ and $\beta \in (M, M)^G$. Then $\text{Tr}^G_H(\alpha) \circ \beta = \text{Tr}(\alpha \circ \text{res}^G_H(\beta))$.
2. Let $\alpha \in (N, N)^G$ and $\beta \in (M, N)^H$. Then $\alpha \circ \text{Tr}^G_H(\beta) = \text{Tr}(\text{res}^G_H(\alpha) \circ \beta)$.

**Proof.** See [3, Lemma 3.6.3(i), (ii)]. \qed

The transfer is related to relative projectivity in the following way.

**Proposition 2.2.** Let $G$ be a finite group of order divisible by $p$, $\mathcal{X}$ a set of subgroups of $G$ and $M$ a $kG$-module. Then the following are equivalent:

1. $M$ is projective relative to $\mathcal{X}$;
2. Every $\mathcal{X}$-split epimorphism of $kG$-modules $\phi : N \to M$ splits;
3. $M$ is injective relative to $\mathcal{X}$;
4. Every $\mathcal{X}$-split monomorphism of $kG$-modules $\phi : M \to N$ splits;
5. $M$ is a direct summand of $\bigoplus_{H \in \mathcal{X}} M \downarrow^G_H$;
6. $M$ is a direct summand of a direct sum of modules induced from subgroups in $\mathcal{X}$;
7. There exists a set of homomorphisms $\{\beta_H : H \in \mathcal{X}\}$ such that $\beta_H \in (M, M)^H$ and $\sum_{H \in \mathcal{X}} \text{Tr}^G_H(\beta_H) = \text{Id}_M$.

The last of these is called Higman’s criterion.

**Proof.** The proof when $H$ is a single subgroup of $G$ can be found in [3, Proposition 3.6.4]. This can easily be generalised. \qed

Note that (vi) tells us that $M$ is projective relative to $\mathcal{X}$ if and only if $M$ decomposes as a direct sum of modules, each of which is projective to some single $H \in \mathcal{X}$. The following corollary now follows immediately from [3, Corollary 3.6.7].

**Corollary 2.3.** Suppose $M$ and $N$ are $kG$-modules and $N$ is projective relative to $\mathcal{X}$. Then $M \otimes N$ is projective relative to $\mathcal{X}$.

Let $M$ and $N$ be $kG$-modules and let $\mathcal{X}$ be a set of subgroups of $G$. Let $(M, N)^G_{\mathcal{X}}$ denote the linear subspace of $(M, N)^G$ consisting of homomorphisms which factor through some $kG$-module which is projective relative to $\mathcal{X}$. We consider the quotient

\[ (M, N)^G_{\mathcal{X}} = (M, N)^G / (M, N)^G_{\mathcal{X}}. \]

One can define a category in which the objects are the $kG$-modules and $(M, N)^G_{\mathcal{X}}$ is the set of morphisms between $kG$-modules $M$ and $N$. This is called the $\mathcal{X}$-relative stable module category, or $\mathcal{X} \text{Stmod}_{kG}$ for short. It reduces to the usual stable module category when we take $\mathcal{X} = \{1\}$. If $M$ and $N$ are $G$-modules, we shall write $M \simeq_{\mathcal{X}} N$ to say that $M$ and $N$ are equivalent in $\mathcal{X} \text{Stmod}_{kG}$. In other words,
$M \cong_K N$ means that there exist modules $P$ and $Q$ which are projective relative to $X$ such that $M \oplus P \cong N \oplus Q$ in $\mathcal{K}G$-mod.

The question of whether a homomorphism factors through a relatively projective module is also related to the transfer.

**Lemma 2.4.** Let $M$, $N$ be $\mathcal{K}G$-modules, $\mathcal{X}$ a collection of subgroups of $G$, and $\alpha \in (M, N)^G$. Then the following are equivalent:

1. $\alpha$ factors through $\oplus_{H \in \mathcal{X}} M \downarrow_H$.
2. $\alpha$ factors through some module which is projective relative to $\mathcal{X}$.
3. There exist homomorphisms $\{\beta_H \in (M, N)^H : H \in \mathcal{X}\}$ such that $\alpha = \sum_{H \in \mathcal{X}} Tr_H^G(\beta_H)$.

**Proof.** This is easily deduced from [3, Proposition 3.6.6]. $\square$

We will need the following result in the proof of our main theorem.

**Proposition 2.5.** Let $G$ be a finite group, $\mathcal{X}$ a set of subgroups of $G$ which is closed under taking subgroups, and $\mathcal{Y}$ a non-empty subset of $\mathcal{X}$. Let $M$ and $N$ be $\mathcal{K}G$-modules and suppose that either $M$ or $N$ is projective relative to $\mathcal{X}$. Suppose $\alpha \in (M, N)^G$ has the property that $\text{res}_H^G(\alpha)$ factors through a module which is projective relative to the set $H \cap \mathcal{Y} := \{K \in \mathcal{Y} : K \subseteq H\}$, for every $H \in \mathcal{X}$. Then $\alpha$ factors through a module which is projective relative to $\mathcal{Y}$.

**Proof.** We give the proof when $M$ is projective relative to $\mathcal{X}$; the proof when $N$ is projective relative to $\mathcal{X}$ is similar. By Lemma 2.4 we can write, for each $H \in \mathcal{X}$

$$\text{res}_H^G(\alpha) = \sum_{K \in H \cap \mathcal{Y}} Tr_K^H(\beta_{H,K})$$

where $\beta_{H,K} \in (M, N)^K$. Since $M$ is projective relative to $\mathcal{X}$ we can write

$$\text{Id}_M = \sum_{H \in \mathcal{X}} Tr_H^G(\mu_H)$$

for some set of homomorphisms $\{\mu_H \in (M, N)^H : H \in \mathcal{X}\}$. Now we have

$$\alpha = \alpha \circ \text{Id}_M = \alpha \circ (\sum_{H \in \mathcal{X}} Tr_H^G(\mu_H))$$

$$= \sum_{H \in \mathcal{X}} Tr_H^G(\text{res}_H^G(\alpha) \circ \mu_H)$$

by Lemma 2.4(2),

$$= \sum_{H \in \mathcal{X}} Tr_H^G(\sum_{K \in H \cap \mathcal{Y}} Tr_K^H(\beta_{H,K} \circ \mu_H))$$

$$= \sum_{H \in \mathcal{X}} \sum_{K \in H \cap \mathcal{Y}} Tr_K^H(\beta_{H,K} \circ \text{res}_K^H(\mu_H))$$

$$= \sum_{H \in \mathcal{X}} \{ \sum_{K \in H \cap \mathcal{Y}} Tr_K^H(\beta_{H,K} \circ \text{res}_K^H(\mu_H)) \} \in (M, N)^G_{\mathcal{Y}}$$

as required. $\square$

**Corollary 2.6.** Suppose $M$ and $N$ are $G$-modules, at least one of which is projective relative to $\mathcal{X}$, $\alpha \in (M, N)^G$ is injective, and $X \in \mathcal{K}G$-mod has the property that, for each $H \in \mathcal{X}$, the equivalence class of $X \downarrow_H$ in the stable category of $\mathcal{K}H$-modules relative to $H \cap \mathcal{Y}$ is $\text{coker}\text{res}_H^G(\alpha)$. Then the equivalence class of $X$ in the stable category of $\mathcal{K}G$-modules relative to $\mathcal{X}$ is $\text{coker}(\alpha)$.

**Remark 2.7.** For the same reasons, if $\alpha \in (M, N)^G$ is surjective and $X \downarrow_H \cong_{H \cap \mathcal{Y}} \text{ker}(\text{res}_H^G(\alpha))$ for all $H \in \mathcal{X}$, then $X \cong_{\mathcal{Y}} \text{ker}(\alpha)$. We will not use this result.
We end this section with an elementary result which will be useful in section 7.

**Lemma 2.8.** Let $M$ be a $\mathbb{k}G$-module which is projective relative to a set $X$ of subgroups of $G$. Then $M^G = \sum_{H \in X} \text{Tr}^G_H(M^H)$.

**Proof.** It suffices to prove $M^G \subseteq \sum_{H \in X} \text{Tr}^G_H(M^H)$, the reverse inclusion being clear. As $M$ is projective relative to $X$, there exists a set of homomorphisms $\{\beta_H \in (M, M)^H, H \in X\}$ such that $\text{Id}_M = \sum_{H \in X} \text{Tr}^G_H(\beta_H)$. Now let $v \in M^G$. As $v \in M^H$ for all $H \in X$, we have $\beta_H(v) \in M^H$ for all $H \in X$, and

$$\text{Tr}^G_H(\beta_H)(v) = \sum_{\sigma \in S} \sigma \beta_H(\sigma^{-1} v) = \sum_{\sigma \in S} \sigma \beta_H(v) = \text{Tr}^G_H(\beta_H(v))$$

where $S$ is a left-transversal of $H$ in $G$. Therefore

$$v = \text{Id}_M(v) = \sum_{H \in X} \text{Tr}^G_H(\beta_H)(v) = \sum_{H \in X} \text{Tr}^G_H(\beta_H(v)) \subseteq \sum_{H \in X} \text{Tr}^G_H M^H$$

as required. \(\square\)

3. Main results

This section is about decomposing symmetric powers of representations of elementary abelian $p$-groups. We will begin by describing a partial decomposition which holds for arbitrary $p$-groups. This decomposition plays a role in, for instance [12] and [6]. Let $G$ be any finite $p$-group, and let $V$ be any finite-dimensional indecomposable $\mathbb{k}G$-module. It is well-known that one may choose a basis $\{x_0, x_1, \ldots, x_m\}$ with respect to which the action of $G$ is lower-triangular, that is to say, preserves the flag of subspaces $\langle x_m \rangle \subset \langle x_{m-1}, x_m \rangle \subset \ldots \subset \langle x_0, x_1, \ldots, x_m \rangle$.

For any $x \in V$ we set

$$N_G(x) = \prod_{y \in Gx} y$$

where $Gx$ denotes the orbit of $x$ under $G$.

Now let $e$ denote the degree of $N_G(x_0)$ when viewed as a polynomial in $x_0$ alone, and let $B$ be the set of all polynomials in $x_0, x_1, \ldots, x_m$ whose degree as a polynomial in $x_0$ alone is strictly less than $e$. Since $G$ fixes the subspace $\langle x_1, x_2, \ldots, x_m \rangle$, $B$ is a $\mathbb{k}G$-submodule of $S(V)$. Further, given any $f \in S(V)$ we may perform successive long division, writing uniquely $f = N_G(x_0) f' + b$ with $f' \in S(V)$ and $b \in B$.

Iterating this process shows there is an isomorphism of $\mathbb{k}G$-modules

$$S(V) \cong \mathbb{k}[N_G(x_0)]S(V) \oplus B.$$

or, taking the grading into account

$$S^d(V) = N_G(x_0)^a S^{d'}(V) \oplus B_d$$

where $B_d$ denotes those elements of $B$ with total degree equal to $d$, and $a$ and $d'$ are the quotient and remainder when $d$ is divided by $e$ respectively.

**Remark 3.1.** Suppose $W$ is a direct summand of $S^d(V)$, and $f \in S^e(V)^G$. Then $fW$ is a submodule of $S^{d+e}(V)$ in general. One way of viewing the above is to say that $N_G(x_0)W$ is always a direct summand of $S^{d+e}(V)$. We sometimes say that $W$ is propogated by the invariant $N_G(x_0)$. Note that if $W$ is projective, then since projective modules are injective we have that $fW$ is a direct summand of $S^{d+e}(V)$ for any $f \in S^e(V)^G$ - in other words, the projective direct summands are propogated by every invariant.
From this point onwards we let $E \leq (k,+)$ be an elementary abelian subgroup of order $q = p^n$. Let $V$ be a faithful $kE$-module with dimension 2 and choose a basis $X, Y$ of $V$ such that $\alpha \in E$ acts via left multiplication by the matrix $\begin{bmatrix} 1 & \alpha \\ 0 & 1 \end{bmatrix}$.

Notice that in order for this to be a faithful module, we must have $|E| \leq |k|$, and therefore any indecomposable $kE$-module is absolutely indecomposable. For any $k \leq n$, we denote by $X_k$ the set of subgroups of $E$ with order at most $p^k$.

The following result is taken from [3]:

**Proposition 3.2.** The ring of invariants $S(V)^E$ is a polynomial algebra generated by $X$ and $N_E(Y)$.

**Corollary 3.3.**
1. The Hilbert Series of $S(V)^E$ is $\frac{1}{(1-t)(1-t^q)}$.
2. For any $m < q$, the representations $S^m(V)$ and $(S^m(V))^*$ are indecomposable.
3. The representations $S^{q-1}(V)$ and $(S^{q-1}(V))^*$ are projective.

**Proof.** (a) follows immediately, since $N_E(Y)$ is an invariant of degree $q$. It follows that the fixed point space of $S^m(V)$ for $m < q$ is one-dimensional, generated by $X^m$, which establishes the first part of (b), and since a module is indecomposable if and only if its dual is too, also the second part. Finally, since $\dim(S^{q-1}(V)) = q$ and $\dim((S^{q-1}(V))^*) = 1$, and since projective modules for $p$-groups are self-dual, we obtain (c).

The following periodicity result is the special case $m = 1$ of Theorem 1.5. The case $E = \mathbb{F}_q$ is a special case of the main result of [2]. This result can be proved in similar fashion to loc. cit., but instead we give a short self-contained proof. We adopt the convention that if $l$ is a natural number and $V$ a representation of $E$, then $lV$ denotes the direct sum of $l$ copies of $V$ with diagonal action.

**Proposition 3.4.** Let $r$ be any non-negative integer and $m < q$. Then we have $S^{r+m}(V) \cong r(kE) \oplus S^m(V)$.

**Proof.** Let $P$ denote the projective module $S^{q-1}(V)$, and let $B = \oplus_{i=0}^{q-2} S^i(V)$. We form the graded submodule $T = \bigoplus_{d \geq 0} T_d$ of $S(V)$ defined as $T = S(V)^E P \oplus k[N_E(Y)]B$, with grading induced from that on $S(V)$. By Remark 3.1, $T$ is a direct summand of $S(V)$. Clearly $T^{q+m} \cong l(kE) \oplus S^m(V)$. Now by Proposition 3.2, the Hilbert Series of $S(V)^E$ is $\frac{1}{(1-t)(1-t^q)}$. Clearly the Hilbert series of $k[N_E(Y)]$ is $\frac{1}{1-t^q}$. As the dimension of $B$ in degree $k$ is $k+1$ if $k \leq q-2$ and zero otherwise, we have

$$H(B,t) = 1 + 2t + 3t^2 + \ldots + (q-1)t^{q-2} = \frac{d}{dt} \left( \frac{1 - t^q}{1 - t} \right) = \frac{-qt^{q-1}}{1-t} + \frac{1-t^q}{(1-t)^2}.$$  

Finally, as $P$ has dimension $q$ and lies in degree $q-1$, we have $H(P,t) = qt^{q-1}$. Therefore

$$H(T,t) = qt^{q-1} \frac{1}{(1-t)(1-t^q)} + \frac{1}{1-t^q} \left( \frac{-qt^{q-1}}{1-t} + \frac{1-t^q}{(1-t)^2} \right) = \frac{1}{(1-t)^2} = H(S(V),t).$$

Therefore $T = S(V)$ as required.

We are interested mainly in symmetric powers of the modules $S^m(V)$ and $(S^m(V))^*$. We set up some notation. For any $i \leq m$ set $a_i = X^{m-i}Y^i$. Then the set
$a_0, a_1, \ldots, a_m$ forms a basis of $S^m(V)$, and the action of $\alpha \in E$ on this basis is given by

$$\alpha \cdot a_i = \sum_{j=0}^{i} \binom{i}{j} \alpha^j a_{i-j}. \quad (3)$$

Notice that this does not depend on $m$; we have an inclusion $S^m(V) \subset S^{m+1}(V)$ for any $m \geq 0$. Now let $x_0, x_1, \ldots, x_m$ be the corresponding dual basis of $S^m(V)^*$; the action here is given by

$$\alpha \cdot x_i = \sum_{j=0}^{m-i} \binom{m}{j} (-\alpha)^j x_{i+j}. \quad (4)$$

Note in particular that $x_m \in (S^m(V)^*)^E$ and $S^m(V)^*/\langle x_m \rangle \cong S^{m-1}(V)^*$. This follows because $x_m = S^{m-1}(V)^\perp$.

Applying the decomposition described earlier in this chapter, we can write, for any $m < q$

$$S^d(S^m(V)^*) = B_{d,m} \oplus N_E(x_0)S^{d-q}(S^m(V)^*). \quad (5)$$

where $B_{d,m}$ is the degree $d$ part of graded direct summand of $S(S^m(V)^*)$ consisting of polynomials whose degree as a polynomial in $x_0$ alone is strictly less than $q$. Note that if $d < q$ then $B_{d,m} = S^d(S^m(V)^*)$. More generally, if $d \geq q$ then $S^d(S^m(V)^*)$ has a direct summand $N_E(x_0)S^{d-q}(S^m(V)^*)$ isomorphic to $S^{d-q}(S^m(V)^*)$, and the isomorphism class of $B_{d,m}$ is $[S^d(S^m(V)^*) - S^{d-q}(S^m(V)^*)]$ as an element of the Green ring. The next lemma, which is inspired somewhat by [II, III.2], is key to everything that follows:

**Lemma 3.5.** Let $m, d$ be natural numbers with $m < q$. Then there is a short exact sequence of $kE$-modules

$$0 \rightarrow B_{d-1,m} \xrightarrow{\alpha_{d,m}} B_{d,m} \xrightarrow{\beta_{d,m}} B_{d,m-1} \rightarrow 0. \quad (6)$$

Here $\alpha_{d,m}$ is multiplication by the invariant $x_m$ and $\beta_{d,m}$ is induced by the projection $S^m(V)^*/x_m = S^{m-1}(V)^*$.

**Proof.** We have a short exact sequence

$$0 \rightarrow S^{d-1}(S^m(V)^*) \xrightarrow{\alpha_{d,m}} S^d(S^m(V)^*) \xrightarrow{\beta_{d,m}} S^d(S^{m-1}(V)^*) \rightarrow 0,$$

with $\alpha_{d,m}$ multiplication by the invariant $x_m$ and $\beta_{d,m}$ the projection $S^m(V)^*/x_m = S^{m-1}(V)^*$. As $\alpha_{d,m}$ does not affect the $x_0$-degree and $\beta_{d,m}$ can only decrease it, this restricts to a short exact sequence as claimed. \qed

We showed a little earlier that the module $S^{q-1}(V)^*$ is projective, and thus isomorphic to $kE$. In particular this implies that this module is a permutation module. Let $\{X_0, X_1, \ldots, X_q\}$ be a permutation basis; if $E = F_q$ then one can take $X_i = \sigma^i \cdot x_0$ where $\sigma \in k$ generates the cyclic group $F_q^\times$, see [II, Proposition 3.4] for details. It follows that each direct summand of $S^d(S^{q-1}(V)^*)$ is also a permutation module, and has a basis $\{\sigma \cdot m : \sigma \in E\}$ where $m$ is some monomial of degree $d$. The summand with this basis has isomorphism type $k[\sigma E]$ where $E'$ is the stabiliser of $m$.

**Proposition 3.6.** Given $d > 0$ we write $d = r p^k$ where $k \leq n$ is the maximal such that $p^k$ divides $d$. Then we have

(i) If $k < n$, $S^d(kE) \cong \chi_{X_0}$. 0.

(ii) If $k = n$ then $S^d(kE) \cong \chi_{X_{n-1}} k$. 
(iii) For any $k$ we have more generally

$$S^d(\mathbb{K}_E) \simeq x_{k-1} \bigoplus_{E' \leq E, |E'| = p^k} \frac{1}{p^{n-k}} \binom{p^{n-k} + r - 1}{r} \mathbb{K}_E^{E'}.$$ 

Proof. Clearly if the monomial $m$ has stabiliser $E'$ then $m$ can be written as a product of monomials of the form $\prod_{\sigma \in E'} (\sigma m')$. In particular, we must have that $E'$ divides $\deg(m)$. This establishes (i). On the other hand, if $d = rp^n$ then there is a unique monomial with stabiliser $E$, namely $\prod_{\sigma \in E} x_{\sigma}$. This establishes (ii).

Now let $E'$ be a subgroup of $E$ with order $p^k$. Define a power series $P(E', t) = \sum_{d \geq 0} M_{E'}^d t^d$ where $M_{E'}^d$ is the number of monomials of degree $d$ fixed by $E'$. Then we have

$$P(E', t) = \frac{1}{(1 - tp^k)^{p^{n-k}}}$$

by the generalised binomial theorem. Therefore the number of summands of $S^d(\mathbb{K}_E)$ with isomorphism type $\mathbb{K}_E^{E'}$ is $\frac{1}{p^{n-k}} \binom{p^{n-k} + r - 1}{r}$, as each one spans a submodule of dimension $p^{n-k}$. As there are no trivial summands and all other summands are induced from smaller subgroups, we have proved (iii). \qed

Corollary 3.7. For all $d > 0$, $B_{d,q-1}$ is projective relative to the set of proper subgroups of $E$. Furthermore, if $d = rp^k$ with $r$ coprime to $p$ and $k < n$, then $B_{d,q-1}$ is projective relative to the set of subgroups of $E$ with order $\leq p^k$.

Remark 3.8. Proposition 3 follows easily using a simple induction argument. By Corollary 3.7 $B_{d,q-1}$ is projective for all $1 \leq d < p$. Therefore, the first and second terms in the exact sequence \text{9} are projective when $m = q - 1$ and $d - 1 \geq 1$. This implies in turn that the last term is also projective, which shows that $B_{d,q-2}$ is projective for $2 \leq d < p$. Continuing in this fashion produces the desired result.

Our most general results are most easily stated in terms of the modules $B_{d,m}$ defined earlier. We note that taking symmetric powers commutes in general with restriction to a subgroup. Further, let $E'$ be a proper subgroup of $E$, with order $p^k$. When $m < p^k$ we will write $B_{d,m}(E')$ for the submodule of $S^d(S^m(V \downarrow_{E'}))$ consisting of polynomials whose $x_0$-degree is strictly less than $p^k$. Note that this is not the same thing as $B_{d,m} \downarrow_{E'}$; rather, we have in the Green ring

\begin{equation}
B_{d,m} \downarrow_{E'} = S^d(S^m(V)^*) \downarrow_{E'} - S^{d-q}(S^m(V)^*) \downarrow_{E'}
= B_{d,m}(E') + B_{d-p^k,m}(E') + \ldots + B_{d-q+p^k,m}(E')
\end{equation}

if $d \geq q$ and

$$B_{d,m} \downarrow_{E'} = S^d(S^m(V)^*) \downarrow_{E'}$$

$$= B_{d,m}(E') + B_{d-p^k,m}(E') + \ldots + B_{d,m}(E')$$

where $d'$ is the remainder when $d$ is divided by $p^k$ otherwise.

Proposition 3.9. Let $d, m$ be a pair of positive integers with $m < q$ and $m + d \geq q$. Then the following hold:

(i) $B_{d,m}$ is projective relative to the set of proper subgroups of $E$. 
(ii) Assuming \( n \geq 2 \), let \( s \) and \( r \) be the quotients when \( d \) and \( m \) respectively are divided by \( p^{n-1} \), with \( d' \) and \( m' \) the corresponding remainders. Then we have

\[
B_{d,m} \simeq_{X_{n-2}} \bigoplus_{E' \leq E: |E'| = p^{n-1}} \frac{1}{p} \left[ \left( \frac{r+s}{r} \right) - \left( \frac{r+s-p}{r} \right) \right] B_{d',m'}(E') \uparrow_{E'}^E
\]

provided \( \frac{1}{p} \left[ \left( \frac{r+s}{r} \right) - \left( \frac{r+s-p}{r} \right) \right] \) is an integer, and

\[B_{d,m}(E) \simeq_{X_{n-2}} 0\]

otherwise.

Proof. The proof is double induction. The first induction is on \( n \), the rank of \( E \). For the \( n = 1 \) case, only the first statement needs to be checked. This states that \( B_{d,m} \) is projective provided \( m + d \geq p \) and \( m < p \). In this case, \( E \) is a cyclic group and the proposition reduces to Theorem 1.1 more precisely, to (a) when \( d < p \) and to (b) when \( d \geq p \).

Now assume \( n > 1 \), and that the proposition has been proven for all elementary abelian groups of order \( p^n \), in particular for all proper subgroups of \( E \). The proof for each \( n \) is by downward induction on \( m \), starting at \( q - 1 \). When \( m = q - 1 \) we have \( r = p - 1 \) and \( m' = p^{n-1} - 1 \). There are two cases to consider. First, if \( d' \neq 0 \) then for every subgroup \( E' \leq E \) with order \( p^{n-1} \), \( B_{d',m'}(E') \) is projective relative to \( X_{n-2} \) by induction. Therefore the Proposition simply claims that \( B_{d,q-1} \) is projective relative to \( X_{n-2} \) in this case. The condition \( d' \neq 0 \) means precisely that \( d \) is not divisible by \( p^{n-1} \), and we showed in this case that \( S^d(S^{q-1}(V)^*) \) is projective relative to \( X_{n-2} \) in Corollary 3.7(i). Moreover, if \( d > q \) then the same is true of \( S^{d-q}(S^{q-1}(V)^*) \) and so we get that

\[B_{d,m} = S^d(S^{q-1}(V)^*) - S^{d-q}(S^{q-1}(V)^*) \simeq_{X_{n-2}} 0\]

as required. Now assume that \( d \) is divisible by \( p^{n-1} \), i.e. \( d' = 0 \). In that case, \( B_{d',m'}(E') = S^0(S^{q-1}(V \downarrow_{E'})^*) \) is \( k \). Furthermore since \( d \geq p^{n-1} \) we have \( s \geq 1 \), hence \( r + s \geq p \). So by Lemma 3.10

\[\left( \frac{r+s}{r} \right) = \left( \frac{r+s-p}{r} \right) \mod p\]

and we have to show that,

\[B_{d,q-1} \simeq_{X_{n-2}} \bigoplus_{E' \leq E: |E'| = p^{n-1}} \frac{1}{p} \left[ \left( \frac{r+s}{r} \right) - \left( \frac{r+s-p}{r} \right) \right] \uparrow_{E'}^E \]

Now by Corollary 3.7(iii), we have

\[S^d(S^{q-1}(V)^*) \simeq_{X_{n-2}} \frac{1}{p} \left( \frac{r+s}{r} \right) \uparrow_{E'}^E \]

and if \( d > q \) then \( d - q = (s-p)p^{n-1} \) so

\[S^{d-q}(S^{q-1}(V)^*) \simeq_{X_{n-2}} \frac{1}{p} \left( \frac{r+s-p}{r} \right) \uparrow_{E'}^E \]

from which the result follows. This concludes the proof for \( m = q - 1 \).

Now fix \( m < q - 1 \) and assume the claim has been proven for all pairs of the form \( (d, m + 1) \) such that \( m + 1 < q \) and \( m + 1 + d \geq q \). We will prove the claim for all pairs of the form \( (d, m) \) where \( m + d \geq q \). So we fix such a \( d \) and consider the short exact sequence

\[
0 \rightarrow B_{d-1,m+1} \overset{\alpha_{d,m+1}}{\rightarrow} B_{d,m+1} \overset{\beta_{d,m+1}}{\rightarrow} B_{d,m} \rightarrow 0.
\]
By induction, the first two terms in the sequence are projective relative to the set of proper subgroups of $E$. We have to describe the decomposition of $B_{d,m} = \text{coker}(\alpha_{d,m+1})$ up to the addition of modules which are projective relative to $X_{n-2}$; applying Corollary 3.3 to $\mathcal{X} = X_{n-1}$ and $\mathcal{Y} = X_{n-2}$ shows that it is enough to check the formula gives the correct decomposition whenever we restrict to any subgroup of order $p^{n-1}$. Let $E'$ be such a subgroup. Then we have two cases check: firstly if $d > q$ then we have in the Green ring

$$B_{d,m} \downarrow E' = \mathcal{S}^d(\mathcal{S}^m(V \downarrow E')^*) - \mathcal{S}^{d-q}(\mathcal{S}^m(V \downarrow E')^*)$$

$$= \mathcal{S}^{p^{n-1}+d}(\mathcal{S}^{p^{n-1}+m'}(V \downarrow E')^*) - \mathcal{S}^{p^{n-1}(s-p)+d'}(\mathcal{S}^{p^{n-1}+m'}(V \downarrow E')^*)$$

$$= \mathcal{S}^{p^{n-1}+d'}((\mathcal{S}^m(V \downarrow E')^*) - \mathcal{S}^{p^{n-1}(s-p)+d'}(\mathcal{S}^m(V \downarrow E')^*)$$

where we used Proposition 3.4 in the last step. We now evaluate the above using the well-known formula for symmetric powers of direct sums $\mathcal{S}^m(V \oplus W) = \bigoplus_{i=0}^{m} \mathcal{S}^i(V) \otimes \mathcal{S}^{m-i}(W)$, to obtain

$$\sum_{i_1+i_2+\ldots+i_r=p^{n-1}s+d'} \mathcal{S}^{i_1}(\mathcal{S}^m(V \downarrow E')^*) \otimes \mathcal{S}^{i_2}(\mathcal{S}^m(V \downarrow E')^*) \otimes \ldots \otimes \mathcal{S}^{i_r}(\mathcal{S}^m(V \downarrow E')^*)$$

We now work in the stable module category relative to $X_{n-2}$. Using Corollary 3.3 and Proposition 3.7(i) we see that $\mathcal{S}^i(\mathcal{S}^m(V \downarrow E')^*) \simeq \mathcal{X}_{n-2,0}$ unless $i$ is divisible by $p^{n-1}$, in which case it is equivalent to the trivial module. We can therefore rewrite the above as

$$\sum_{j=0}^{\lfloor s/p \rfloor} \sum_{s-j \leq i_1 + \ldots + i_r \leq s-j} \mathcal{S}^{p^{n-1}i_1}(\mathcal{S}^m(V \downarrow E')^*) \otimes \mathcal{S}^{p^{n-1}i_2}(\mathcal{S}^m(V \downarrow E')^*) \otimes \ldots \otimes \mathcal{S}^{p^{n-1}i_r}(\mathcal{S}^m(V \downarrow E')^*)$$

$$= \sum_{j=0}^{\lfloor s/p \rfloor} \mathcal{P}(s-j,0) \mathcal{S}^{p^{n-1}+d'}(\mathcal{S}^m(V \downarrow E')^*) - \sum_{j=0}^{\lfloor s-p \rfloor} \mathcal{P}(s-p-j,0) \mathcal{S}^{p^{n-1}+d'}(\mathcal{S}^m(V \downarrow E')^*)$$

where $\mathcal{P}(a,b)$ denotes the number of distinct ways of writing the positive integer $a$ as a sum of exactly $b$ positive integers. Now observe that for each $j$ we have

$$\mathcal{S}^{p^{n-1}+d'}(\mathcal{S}^m(V \downarrow E')^*) = \sum_{l=0}^{j} \mathcal{B}_{lp^{n-1}+d',m'}(E')$$

by definition. Since $|E'| = p^{n-1}$, and $m' < p^{n-1}$, (ii) of the inductive hypothesis (on $n$) implies that $\mathcal{B}_{lp^{n-1}+d',m'}$ is projective relative to $X_{n-2}$, provided that $lp^{n-1} + d' + m' \geq p^{n-1}$. In particular this holds whenever $l \geq 1$, and additionally when $l = 0$ in the case that $m' + d' \geq p^{n-1}$. In the latter case we have now shown that

$$B_{d,m} \downarrow E' \simeq \mathcal{X}_{n-2,0}$$

Otherwise, we have shown that

$$B_{d,m} \downarrow E' \simeq \mathcal{X}_{n-2} \sum_{j=0}^{s} \mathcal{P}(s-j,0) \mathcal{B}_{d',m'}(E') - \sum_{j=0}^{s-p} \mathcal{P}(s-p-j,0) \mathcal{B}_{d',m'}(E')$$

$$= \left( \left( \frac{r+s}{r} \right) - \left( \frac{r+s-p}{r} \right) \right) \mathcal{B}_{d',m'}(E')$$

$$B_{d,m} \downarrow E' \simeq \mathcal{X}_{n-2} 0.$$
using the well-known combinatorial identity \( \sum_{i=0}^{a} \binom{a+b}{b} = \binom{a+b}{a} \).

If \( d < q \), then \( s < p \). Almost the same argument applies, but without any negative terms involved. Adopting the convention that binomial coefficients in which the bottom term exceeds the top are zero, we can still say that

\[
B_{d',m'} \downarrow_{E'} \cong \chi_{n-2} \left( \binom{r + s}{r} - \binom{r + s - p}{r} \right) B_{d',m'}(E')
\]

if \( m' + d' < p^{n-1} \), and \( B_{d',m'} \downarrow_{E'} \cong \chi_{n-2} 0 \) otherwise.

If \( m' + d' \geq p^{n-1} \), then since any \( kE \)-module which is projective relative to \( \chi_{n-2} \) remains so when restricted to a subgroup of order \( p^{n-1} \), the proposition follows immediately. So assume \( m' + d' < p^{n-1} \). Since \( m + d \geq q \) we have

\[
q \leq m + d = (r + s)p^{n-1} + m' + d'.
\]

\[
\Rightarrow (r + s)p^{n-1} \geq q - m' - d' > p^n - p^{n-1} = p^{n-1}(p - 1)
\]

and therefore \( r + s \geq p \). Since \( m < q \) we get \( r < p \) and therefore by Lemma 3.10

\[
\binom{r + s}{r} = \binom{r + s - p}{r} \mod p.
\]

We must therefore verify the formula (3).

We check that for any pair \( E', E'' \) of subgroups of \( E \) with order \( p^{n-1} \) we have

\[
(B_{d',m'}(E'') \uparrow_{E''} \downarrow_{E}) \downarrow_{E'} = \begin{cases} 
B_{d',m'}(E'') \uparrow_{E''} \downarrow_{E} & \text{if } E' = E'' \\
B_{d',m'}(E'') \uparrow_{E''} \downarrow_{E' \cap E''} \uparrow_{E' \cap E''} & \text{otherwise}
\end{cases}
\]

using the Mackey formula (remembering that \( E \) is abelian, so that a set of \( E' - E' \) double coset representatives is just a set of \( E' \)-coset representatives, and a set of \( E'' - E' \) double coset representatives can be chosen consisting only of the trivial element, since \( E = E'E'' \)), and therefore we have

\[
\bigoplus_{E' \leq E; |E'| = p^{n-1}} \frac{1}{p} \left[ \binom{r + s}{r} - \binom{r + s - p}{r} \right] B_{d',m'}(E'') \uparrow_{E''} \downarrow_{E'} \cong \chi_{n-2} \left( \binom{r + s}{r} - \binom{r + s - p}{r} \right) B_{d',m'}(E') \equiv B_{d,m} \downarrow_{E'}
\]

as required.

In the above proof we used the following number-theoretic lemma:

**Lemma 3.10.** Let \( r, s \) be integers and let \( p \) be a prime. Suppose that \( r < p \) and \( r + s \geq p \). Then

\[
\binom{r + s}{r} = \binom{r + s - p}{r} \mod p
\]

where the latter is interpreted as zero if \( s < p \).

**Proof.** If \( s < p \) then since \( s + r \geq p \) we have

\[
\binom{r + s}{r} = \frac{(r + s)(r + s - 1) \cdots (p) \cdots (s + 1)}{r(r - 1) \cdots 2 \cdot 1} = 0 \mod p.
\]

While if \( s \geq p \) we have

\[
\binom{r + s - p}{r} = \frac{(r + s - p)(r + s - 1 - p) \cdots (s + 1) \cdots (s - p)}{r(r - 1) \cdots 2 \cdot 1} = \frac{(r + s)(r + s - 1) \cdots (s + 1) - 0}{r(r - 1) \cdots 2 \cdot 1} \mod p.
\]

\( \square \)

**Theorem 3.11.** Let \( (d, m) \) be a pair of positive integers, with \( m < p^k < q \) and \( m + d \geq q \). Then \( B_{d,m} \) is projective relative to \( \chi_{k-1} \).
Remark 3.12. When $k = 1$ and $d < q$ we obtain Theorem 1.2. When $k = 1$ and $d \geq q$ we obtain Theorem 1.5.

Proof. The proof is by backwards induction on $k$, the case $k = n$ having been covered in Proposition 3.9. Let $k \leq l \leq n$ and assume that $B_{d,m}$ is projective relative to $X_l$ for all pairs $d, m$ with $d + m > q$ and $m < p^{l+1}$. Now suppose $m < p^l$ and $m + d > q$; we will show that $B_{d,m}$ is projective relative to $X_{l-1}$. As $m < p^{l+1}$, we have that $B_{d,m}$ is projective relative to $X_l$. So by Proposition 2.2(iv), $B_{d,m}$ is a direct summand of

$$
\bigoplus_{E' \in X_l} (B_{d,m} \downarrow E') \uparrow E',
$$

where $a$ is the largest integer such that $a \leq (p^{n-l} - 1)$ and $d - ap^l \geq 0$. Note that therefore

$$
m + d - ap^l \geq m + d - p^l(p^{n-l} - 1) = m + d - p^n + p^l \geq p^l,
$$

therefore for each $E'$ the modules $B_{d,m}(E'), B_{d-p^l,m}(E'), \ldots, B_{d-2p^l,m}(E')$ are projective relative to $X_{l-1}$ by Proposition 3.9 applied to $E'$, from which the result follows.

\[\square\]

4. SOME ELEMENTARY NUMBER THEORY

In this section, we prove some number-theoretic results which will be needed in the sequel. Throughout, we fix a prime power $q = p^n$ and consider a pair of non-negative integers $(d, m)$ with $m < q$ and $d < q$. For any $0 \leq i \leq n$, we write $d_i$ (resp. $m_i$) for the remainder when $d$ (resp. $m$) is divided by $p^{n-i}$. We define

$$
k = \min\{i \geq 0 : m_i + d_i < p^{n-i}\}.
$$

We will refer to this as the $p$-depth of the pair $(d, m)$. With $k$ as above, we write $s$ and $r$ for the quotients when $d$ and $m$ respectively are divided by $p^{n-k}$. Thus we have $m = rp^{n-k} + m_k$ and $d = sp^{n-k} + d_k$. Notice that since $m < p^n$ we must have $r < p^k$, and similarly $s < p^k$ Consider the $p$-adic expansions of $r$ and $s$

$$
s = s_0 + s_1 p + \ldots + s_{k-1} p^{k-1} = r_0 + r_1 p + \ldots + r_{k-1} p^{k-1}.
$$

Lemma 4.1. $r_0 + s_0 \geq 2$ and for $1 \leq i < k$ we have $r_i + s_i \geq 1$.

Proof. By definition we have

$$
m = (r_0 + r_1 p + \ldots + r_{k-1} p^{k-1})p^{n-k} + m_k.
$$

Now let $1 \leq i \leq k$. One way to rearrange (12) is

$$
m = (r_0 + r_1 p + \ldots + r_{i-1} p^{i-1})p^{n-k} + m_k + (r_i + r_{i+1} p + \ldots + r_{k-1} p^{k-1})p^{n-k+i}.
$$

Since each of $r_0, r_1, \ldots, r_{i-1}$ are $\leq p - 1$, we have $(r_0 + r_1 p + \ldots + r_{i-1} p^{i-1}) \leq p^i - 1$, and therefore

$$
(r_0 + r_1 p + \ldots + r_{i-1} p^{i-1})p^{n-k} + m_k < (p^i - 1)p^{n-k} + p^{n-k} = p^{n-k+i}.
$$

By uniqueness of division with remainder, $m_{k-i} = (r_0 + r_1 p + \ldots + r_{i-1} p^{i-1})p^{n-k} + m_k$. A similar argument shows that, $d_{k-i} = (s_0 + s_1 p + \ldots + s_{i-1} p^{i-1})p^{n-k} + d_k$.

By definition of $p$-depth, $m_k + d_k < p^{n-k}$ and $m_{k-i} + d_{k-i} \geq p^{n-k+i}$ for all $1 \leq i \leq k$. It follows that, when $1 \leq i \leq k$,

$$
(r_0 + s_0) + (r_1 + s_1) p + \ldots + (r_{i-1} + s_{i-1}) p^{i-1})p^{n-k} \geq (m_{k-i} - m_k - d_k) > p^{n-k+i} - p^{n-k}.
$$

This could also be written as

$$
(r_{i-1} + s_{i-1})p^{n-k+i-1} > p^{n-k}(p^i - 1)(r_{i-2} + s_{i-2})p^{n-k+i-2} - \cdots - (r_1 + s_1)p^{n-k+1} - (r_0 + s_0)p^{n-k}.
$$
\[ \geq p^n - k (p^i - 1) - 2(p-1)p^{n-k+i-2} - \ldots - 2(p-1)p^{n-k+1} - 2(p-1)p^{n-k} \]
\[ = p^{n-k+i} - 2p^{n-k+i-1} + p^{n-k} \]

since \( r_j, s_j \leq p - 1 \) for all \( j \). Dividing both sides by \( p^{n-k+i-1} \) now shows that \( r_{i-1} + s_{i-1} \geq p - 2 + \frac{1}{p} \). Setting \( i = 1 \) shows that \( r_0 + s_0 > p - 2 + 1 = p - 1 \), i.e. \( r_0 + s_0 \geq p \), whilst if \( i \geq 2 \) we get \( r_{i-1} + s_{i-1} > p - 2 \), i.e. \( r_{i-1} + s_{i-1} \geq p - 1 \) as required.

We obtain the following

**Corollary 4.2.** Let \( m, d \) be a pair with p-depth equal to \( k \). Then
\[ \left( \frac{r + s}{r} \right) = 0 \mod p^k. \]

**Proof.** Write \( r = r_0 + r_1 p + \ldots r_{k-1} p^{k-1} \) and \( s = s_0 + s_1 p + \ldots s_{k-1} p^{k-1} \). By a well-known theorem of Kummer (see [9], the maximum power of \( p \) which divides \( \left( \frac{r + s}{r} \right) \) is equal to the number of “carries” when \( r \) and \( s \) are added in base \( p \). It follows from Lemma 4.1 that this number is at least \( k \).

There is also a partial converse:

**Lemma 4.3.** Suppose \( m, d \) are positive integers such that \( m < q \), \( d < q \). Then
\[ \left( \frac{m + d}{m} \right) \text{ is divisible by } q \text{ if and only if the } p \text{-depth of } (d, m) \text{ is } n. \]

**Proof.** Write \( m = r_0 + r_1 p + \ldots r_{n-1} p^{n-1} \) and \( d = s_0 + s_1 p + \ldots s_{n-1} p^{n-1} \) (this notation is consistent, and \( m \) and \( d \) are the quotients when \( m \) and \( d \) respectively are divided by \( p^{n-n} = 1 \)). If the p-depth of \( (d, m) \) is \( n \), then \( \left( \frac{m + d}{m} \right) \) is divisible by \( p^n \) by the preceding Corollary. Conversely, suppose that \( \left( \frac{m + d}{m} \right) \) is divisible by \( p^n \). This means that there are \( n \) carries in the \( p \)-adic addition of \( m \) and \( d \), i.e.
\[ r_0 + s_0 \geq p \text{ and } r_i + s_i \geq p - 1 \text{ for all } i = 1, \ldots, n - 1. \]

As before, write \( m_k \) and \( d_k \) for the remainders when \( m \) and \( d \) are divided by \( p^{n-k} \). Thus for all \( k = 0, \ldots, n - 1 \) we have
\[ m_k = r_0 + r_1 p + \ldots + r_{n-k-1} p^{n-k-1}, \quad d_k = s_0 + s_1 p + \ldots + s_{n-k-1} p^{n-k-1}. \]

Now \( m_{n-1} + d_{n-1} = r_0 + s_0 \geq p \). Assume that \( m_k + d_k \geq p^{n-k} \) where \( k \geq 1 \). Then we have
\[ m_{k-1} + d_{k-1} = m_k + d_k + p^{n-k} (r_{n-k} + s_{n-k}) \geq p^{n-k} + p^{n-k} (p - 1) = p^{n-k+1}. \]

Therefore by backwards induction on \( k \), \( m_k + d_k \geq p^{n-k} \) for all \( k = 0 \ldots n - 1 \). As \( m < q, d < q \) we have \( m_n = d_n = 0 \) and so \( m_n + d_n < p^0 = 1 \), therefore the p-depth of \( (d, m) \) is \( n \) as required.

It is interesting to note that this does not extend to divisibility by \( p^k \) for \( k < n \).

For example, take \( m = 5, d = 5 \) and \( q = 8 \). Observe that
\[ \left( \frac{m + d}{d} \right) = \left( \frac{10}{5} \right) = 252 \]
is divisible by 4, but \( m_1 = 1, d_1 = 1 \) are the remainders when \( m \) and \( d \) are divided by 4, so that \( m_1 + d_1 < 4 \) and the p-depth of \( (d, m) \) is only 1. We will see the consequences of this in the next section.
5. Decomposing $S^d(S^m(V)^*)$

It is clear that, for the modules $S^d(S^m(V)^*)$ with $m, d < q$, Theorem 8.11 does not give the strongest possible result in all cases. For instance, Theorem 1.3 is stronger in the case $d < p$, in the sense that it provides a set of smaller subgroups of $E$ relative to which $S^d(S^m(V)^*)$ is projective. The aim of this section is to following result, which contains both Theorem 1.3 and Theorem 1.2 as special cases.

Theorem 5.1. Suppose $(d, m)$ is pair of integers such that $m < q$, $d < q$ and the $p$-depth of $(d, m)$ is at least $k$. Then $S^d(S^m(V)^*)$ is projective with respect to the set of subgroups of $E$ with index $p^k$.

Proof. The proof is by induction on $k$. Note that the case $k = 1$ is covered by Proposition 5.9 and the case $k = 0$ is vacuous. Let $(d, m)$ have $p$-depth equal to $k$ and suppose that $S^d(S^m(V)^*)$ is projective relative to $X_{n-1}$ where $l > k$. We will show that $S^d(S^m(V)^*)$ is projective relative to $X_{n-l-1}$. By hypothesis, $S^d(S^m(V)^*)$ is a direct summand of

$$\bigoplus_{E'\in X_{n-l}} (S^d(S^m(V)^*) \downarrow_{E'}) \uparrow_{E'}^E.$$ 

Write $m_l$ for the remainder when $m$ is divided by $p^n - l$ and $r$ for the corresponding quotient (note this is not the same notation as in the previous chapter, where $r$ denoted the quotient when $m$ is divided by $p^k$). Similarly define $d_l$ and $s$. Then for each $E' < E$ with index $p^l$ we have

$$S^d(S^m(V)^*) \downarrow_{E'} = S^{d_l + sp^n - l}(S^{m_l + rp^n - l}(V)^*) \downarrow_{E'} \cong X_{n-l-1} \begin{pmatrix} r + s & \vspace{1cm} \\
 & & \\
 & & \\
 & & \\
 & & \\
 & & \end{pmatrix} S^{d_l}(S^{m_l}(V)^*) \downarrow_{E'}$$

by the same argument as in the proof of Proposition 5.9. As $d_l + m_l \geq p^n - l$, Proposition 5.9 applied to $E'$ implies that $S^{d_l}(S^{m_l}(V)^*) \downarrow_{E'}$ is projective relative to $X_{n-l-1}$. The result follows. \qed

Remark 5.2. Lemma 4.3 now implies that $S^d(S^m(V)^*)$ is projective whenever $(d + m)/m$ is divisible by $q$, i.e. whenever the dimension of $S^d(S^m(V)^*)$ allows it. The author thanks Alex Fink for raising this question. On the other hand, it’s not true that $S^d(S^m(V)^*)$ is projective relative to the set of all subgroups of index $p^k$ whenever $(d + m)/m$ is divisible by $p^n - k$ and $d + m \geq q$; for a counterexample take $q = 8$, $m = d = 5$. We have observed that $S^5(S^5(V)^*)$ has dimension divisible by 4, but the $p$-depth of (5, 5) with respect to 8 is only 1. By Proposition 5.9(ii), we have

$$S^5(S^5(V)^*) \cong X_1 \bigoplus_{E' < E, |E'| = 4} 2S^1(S^1(V)^*) \downarrow_{E'} \uparrow_{E'}^E.$$

As $S^1(S^1(V)^*) \downarrow_{E'} = S^1(V)^* \downarrow_{E'}$ is not projective relative to the set of cyclic subgroups of $E'$ for any $E'$ with order 4, we get that $S^5(S^5(V)^*)$ is not projective relative to $X_1$.

Over the course of the last three sections, we have proved results generalising the projectivity and periodicity results (Theorem 1.1 (i) and (ii)) of Almkvist and Fossum. We have said nothing concerning their reciprocity result (iii). It is clear that we cannot have $S^d(S^m(V)^*) \cong S^m(S^d(V)^*)$ for arbitrary $d$ and $m$; one only has to look at the case $q = 4$, $m = 1$, $d = 2$ for a counterexample. One can easily show (using Proposition 5.9 and Theorem 1.1) that $S^d(S^m(V)^*) \cong S^m(S^d(V)^*)$ if
Proof. The inclusion basis for the dual $k$ of polynomial functions $\sigma f$ $X$ $E$ and its kernel may contain elements outside of the image of $\alpha$. For a counterexample, take $q = 8$, $m = 5$ and $d = 6$. Then

$$S^d(S^5(V)^*) \simeq \mathcal{X}_1 \bigoplus_{E' < E, |E'| = 4} 2S^2(V)^* \not\simeq \mathcal{X}_1 \bigoplus_{E' < E, |E'| = 4} 2S^2(V)^* \simeq \mathcal{X}_1 S^6(S^5(V)^*)$$

and so $S^6(S^5(V)^*) \not\simeq S^5(S^6(V)^*)$.

6. DECOMPOSING $S^d(S^m(V))$

Computational experiments with MAGMA [4] suggest that there is far less uniformity in the summands which make up $S^d(S^m(V))$. However, there are some things which can be said. The aim of this section is to prove Theorem 1.4.

Lemma 6.1. Let $m < q$ and let $d < p$. Then there is a short exact sequence

$$0 \to S^d(S^{m-1}(V)) \xrightarrow{\alpha_d, m} S^d(S^m(V)) \xrightarrow{\beta_d, m} S^{d-1}(S^m(V)) \to 0. \tag{13}$$

Proof. The inclusion $S^{m-1}(V) \subset S^m(V)$ induces, for any $d \geq 0$, an injective $kE$-homomorphism $\alpha_d, m : S^d(S^{m-1}(V)) \to S^d(S^m(V))$. We define a mapping $\beta_d, m : S^d(S^m(V)) \to S^{d-1}(S^m(V))$ by setting $\beta_d, m(f) = \frac{\partial f}{\partial m}$ for any $f = f(a_0, a_1, \ldots, a_m)$ of degree $d$. Clearly $\beta_d, m$ is a linear map which decreases degrees by one; we claim it is a $kE$-homomorphism. The key fact here is that, for any $\alpha \in E$ we have $\alpha \cdot a_m = a_m + g_\alpha$ for some linear expression $g_\alpha \in k[a_0, a_1, \ldots, a_m]$. Now let $f = f(a_0, a_1, \ldots, a_m) \in S^d(S^m(V))$. We can decompose $f$ as a sum of terms of the form $a_m^k f_k$ where $f_k \in k[a_0, a_1, \ldots, a_{m-1}]$ has degree $d - k$. Now

$$\beta_d, m(\alpha \cdot (a_m^k f_k)) = \beta_d, m((a_m + g_\alpha)^k (\alpha \cdot f_k)) = k(a_m + g_\alpha)^{k-1}(\alpha \cdot f_k)$$

since $\alpha \cdot f_k \in k[a_0, a_1, \ldots, a_{m-1}]$, while

$$\alpha \cdot (\beta_d, m(a_m^k f_k)) = \alpha \cdot (ka_m^{k-1} f_k) = k(a_m + g_\alpha)^{k-1}(\alpha \cdot f_k)$$

also.

If $d < p$ then the map $\beta_d, m$ is surjective, and its kernel consists of those polynomials in $S^d(S^m(V))$ not involving $a_m$ - that is, the image of $\alpha_d, m$. This gives us an exact sequence as desired. \hfill $\square$

Proposition 1.4 now follows by another downward induction argument: as $S^{q-1}(V)$ is projective, it follows from Proposition 4.7 that $S^d(S^{q-1}(V))$ is projective for $1 \leq d < p$. Therefore, in the exact sequence (13) with $m = q - 1$ and $2 \leq d < p$, the second and last terms are projective. It follows that for $2 \leq d < p$, the module $S^d(S^{q-2}(V))$ is also projective. Continuing in this fashion produces the desired result.

Remark 6.2. Note that if $d \geq p$ then the map $\beta_d, m$ described above is not surjective, and its kernel may contain elements outside of the image of $\alpha_d, m$; for instance, $X_m^p \in \ker(\beta_p, m)$ for any $m$. For this reason, we cannot take this approach any further.

7. APPLICATIONS TO INVARIANT THEORY OF FINITE GROUPS

In this section let $G$ be a finite group and $V$ a finite-dimensional $kG$-module, with $k$ an infinite field of arbitrary characteristic. We denote by $k[V]$ the $k$-algebra of polynomial functions $V \to k$. This itself becomes a $kG$-module with the action given by $(\sigma f)(v) = f(\sigma^{-1}v)$ for $f \in k[V], v \in V$ and $\sigma \in G$. If $X_1, X_2, \ldots, X_n$ is a basis for the dual $kG$-module $V^*$ then

$$k[V] = k[X_1, X_2, X_3, \ldots, X_n] = S(V^*)$$
where the action on $S(V^*)$ is extended from that on $V^*$ by algebra automorphisms. The set of $G$-fixed points $k[V]^G$ is again a $k$-algebra, the algebra of invariants. This is the central object of study in invariant theory.

It is difficult in general to describe $k[V]^G$ by generators and relations. There are, however, many ways to construct elements of $k[V]^G$. Two of these we have already met: given $f \in k[V]$ we defined $N_G(f) = \prod_{\sigma \in G} (\sigma f)$. This is known as the norm of $f$. We have in addition

$$
Tr^G(f) = \sum_{\sigma \in G} (\sigma f),
$$

the trace or transfer of $f$. This gives us a degree-preserving $k[V]^G$-homomorphism $k[V] \to k[V]^G$, whose image is an ideal of $k[V]^G$. There is also a relative version: given a subgroup $H \leq G$ we define a $k[V]^G$-homomorphism

$$
Tr_H^G : k[V]^H \to k[V]^G
$$

$$
Tr_H^G(f) = \sum_{\sigma \in S} \sigma f
$$

where $S$ denotes a left-transversal of $H$ in $G$. This definition is clearly independent of the choice of $S$. We denote by $I^G_H$ its image, which is an ideal in $k[V]^G$. More generally, given a set $X$ of subgroups of $G$, we set $I^G_X = \sum_{H \in X} I^G_H$.

If $|G|$ is not divisible by $\text{char}(k)$ then $Tr^G$ is surjective. This has many nice consequences; in particular, it implies that $k[V]^G$ is a direct summand of $k[V]$ as a $kG$-module, and hence that $k[V]^G$ is Cohen-Macaulay. Totaro [15] has shown that more generally that $k[V]^G/I^G_P$ is Cohen-Macaulay, where $<P$ denotes the set of proper subgroups of a (any) Sylow-$p$-subgroup of $G$, generalising earlier work of Fleischmann [8], where $I^G_P$ is replaced by its radical.

The results of this paper allow us to say something about generating sets for rings of invariants of elementary abelian $p$-groups. In the proposition below, we let $E$ be an elementary abelian $p$-group of order $q$, and let $W$ be a 2 dimensional indecomposable faithful representation of $E$ over an infinite field $k$ of characteristic $p$. Recall that $E$ can be identified with a subgroup of $(k,+)$, and we can assume the action of $E$ on $W$ is given as left multiplication by $\begin{bmatrix} 1 & \alpha \\ 0 & 1 \end{bmatrix}$. Suppose $V \cong S^{m_1}(W) \oplus \ldots \oplus S^{m_r}(W)$ for some set of integers $m_1,m_2,\ldots,m_r$ with $m_i < q$ for all $i$. Let $k$ be the smallest integer such that $m_i < p^k$ for all $i$. Let $x_{0,1},x_{1,1},\ldots,x_{m_r,r}$ be the basis of $V^*$ such that the action of $\sigma$ on $\{x_{0,1},\ldots,x_{m_r,i}\}$ is given by the formula (3) for all $i$, and let

$$
N_i = N_E(x_{0,i}) = \prod_{\alpha \in E} \alpha(x_{0,i}).
$$

If $f \in k[V]$ then we shall say that $f$ is of multidegree $(d_1,d_2,\ldots,d_r)$ if $f$ has degree $d_i$ in $x_{0,i},\ldots,x_{m_i,i}$ for all $i$. As $k$ is infinite we have a decomposition

$$
k[V]_{d_1,d_2,\ldots,d_r} \cong k[S^{m_1}(W)]_{d_1} \otimes k[S^{m_2}(W)]_{d_2} \otimes \ldots \otimes k[S^{m_r}(W)]_{d_r}.
$$

Further, for each $i$ where $d_i \geq q$ we have $k[S^{m_i}(W)]_{d_i} \cong S^{d_i-q}(S^{m_i}(W)^*) \cong N_{d_i}^* S^{d_i}(S^{m_i}(W)^*) \oplus B_{d_i,m_i}$, where $d_i'$ and $a_i$ are the remainder and quotient when $d_i$ is divided by $q$ and $B_{d_i,m_i}$ is the set of polynomials in $S^{d_i}(S^{m_i}(W)^*)$ whose degree in $x_{0,i}$ is $<q$. Notice that, by Theorem 3.11 $B_{d_i,m_i}$ is projective relative to $X_{k-1}$, if $d_i \geq q - m_i$.

**Proposition 7.1.** $k[V]^E$ has a generating set consisting of

(i) The orbit products $N_i$, $i = 1,\ldots,r$;

(ii) Certain invariants of multidegree $(d_1,d_2,\ldots,d_r)$, where $d_i < q - m_i$, for all $i$. 


(iii) Certain invariants of the form $\text{Tr}_H^E(f)$ for $f \in k[V]$, where $H \in X_{k-1}$.

Proof. Let $f \in k[V]^E_{d_1, d_2, d_3, \ldots, d_r}$. If $d_i < q - m_i$ for all $i$ there is nothing to prove. If for some $i$ we have $q - m_i \leq d_i < q$ then

$$(k[V]_{d_1, d_2, d_3, \ldots, d_r} = k[S^{m_1}(W)]_{d_1} \otimes k[S^{m_2}(W)]_{d_2} \otimes \cdots k[S^{m_r}(W)]_{d_r})$$

is projective relative to $X_{k-1}$ by the above discussion and Corollary 2.8. Then by Lemma 2.8 we have $f \in I_{R_{k-1}}^E$. This completes the proof in case $d_i < q$ for all $i$. So now assume that $d_i \geq q$. The proof is now by induction on the total degree of $f$ (the case of total degree $< q$ being settled already). We can write

$$f = N_i^a f' + b$$

for some unique $f' \in k[V]_{d_1, d_2, \ldots, d_i}$ and $b \in k[V]_{d_1, d_2, \ldots, d_i}$, whose degree in $x_{i+1}$ is $< q$, where $a_i$ and $d'_i$ are the quotient and remainder, respectively, when $d_i$ is divided by $q$. Furthermore for any $\alpha \in k$ we have

$$f = \alpha f = N_i^a (\alpha f') + \alpha b$$

so the uniqueness of division with remainder implies that $f'$ and $b$ are invariant. By induction, $f'$ belongs to the subalgebra of $k[V]^E$ generated by the claimed generating set and $b$ is a fixed point in

$$k[S^{m_1}(W)]_{d_1} \otimes \cdots \otimes k[S^{m_r}(W)]_{d_r}$$

which, by Corollary 2.8 and Theorem 3.11 is projective relative to $X_{k-1}$. Then by Lemma 2.8 we have $b \in I_{R_{k-1}}^E$ and Theorem 3.11 is projective relative to $X_{k-1}$. This completes the proof.

In the special case where $E$ is a cyclic group of order $p$, the fact that $k[V]^E$ has a generating set of the form above was conjectured by Shank [13, 14]. In fact, Shank’s conjecture goes further to describe more precisely the invariants labelled by (ii) in the generating set. Recall that there are exactly $p$ indecomposable representations of $E$ over $k$. For each $1 \leq m < p$, let $V_m$ denote the unique indecomposable $kE$-module of dimension $m$, on which a generator $\sigma$ of $E$ acts as left-multiplication by a Jordan block of length $m$. One easily sees that $S^m(V_2)^* \cong S^m(V_2) \cong V_{m+1}$ for $1 \leq m < p$. If we take instead $k = \mathbb{Q}$, then the matrix representing $\sigma$ has infinite order, and we get a representation of $\mathbb{Z}$. Each invariant of the second kind is then obtained from an invariant in $Q[V]^Z$ by reduction modulo $p$. Shank calls these integral invariants.

Shank’s conjecture (including the statement about integral invariants) was recently proved by Wehlau [15]. Of course, the classification of indecomposable modules for cyclic groups in the modular case implies that this applies to arbitrary representations of a cyclic group of order $p$ over $k$. Our generalisation does not apply to arbitrary representations of an elementary abelian $p$-group.

Acknowledgments. Special thanks go to Professor David Benson a number of invaluable conversations.

References

[1] Gert Almkvist and Robert Fossum. Decomposition of exterior and symmetric powers of indecomposable $\mathbb{Z}/p\mathbb{Z}$-modules in characteristic $p$ and relations to invariants. In Séminaire d’Algèbre Paul Dubreil, 30ème année (Paris, 1976–1977), volume 641 of Lecture Notes in Math., pages 1–111. Springer, Berlin, 1978.

[2] J. Alperin and L. G. Kovacs. Periodicity of Weyl modules for $SL(2,q)$. J. Algebra, 74(1):52–54, 1982.

[3] D. J. Benson. Representations and cohomology. I, volume 30 of Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge, second edition, 1998. Basic representation theory of finite groups and associative algebras.
[4] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[5] H. E. A. Campbell, R. J. Shank, and D. L. Wehlau. Rings of invariants for modular representations of elementary abelian $p$-groups. *Transform. Groups*, 18(1):1–22, 2013.

[6] Jonathan Elmer. Depth and detection in modular invariant theory. *J. Algebra*, 322(5):1653–1666, 2009.

[7] Jonathan Elmer and Martin Kohls. Zero-separating invariants for linear algebraic groups. To appear in *J. Edin. Math. Soc*. Preprint available from http://arxiv.org/abs/1402.6608, 2013.

[8] Peter Fleischmann. Relative trace ideals and Cohen-Macaulay quotients of modular invariant rings. In *Computational methods for representations of groups and algebras* (Essen, 1997), volume 173 of *Progr. Math.*, pages 211–233. Birkhäuser, Basel, 1999.

[9] Andrew Granville. Arithmetic properties of binomial coefficients. I. Binomial coefficients modulo prime powers. In *Organic mathematics (Burnaby, BC, 1995)*, volume 20 of *CMS Conf. Proc.*, pages 253–276. Amer. Math. Soc., Providence, RI, 1997.

[10] Frank Himstedt and Peter Symonds. Exterior and symmetric powers of modules for cyclic $2$-groups. *J. Algebra*, 410:393–420, 2014.

[11] Ian Hughes and Gregor Kemper. Symmetric powers of modular representations, Hilbert series and degree bounds. *Comm. Algebra*, 28(4):2059–2088, 2000.

[12] Dikran B. Karagueuzian and Peter Symonds. The module structure of a group action on a polynomial ring: a finiteness theorem. *J. Amer. Math. Soc.*, 20(4):931–967 (electronic), 2007.

[13] R. J. Shank. Classical covariants and modular invariants. In *Invariant theory in all characteristics*, volume 35 of *CRM Proc. Lecture Notes*, pages 241–249. Amer. Math. Soc., Providence, RI, 2004.

[14] R. James Shank, S.A.G.B.I. bases for rings of formal modular seminvariants [semi-invariants]. *Comment. Math. Helv.*, 73(4):548–565, 1998.

[15] Burt Totaro. *Group cohomology and algebraic cycles*, volume 204 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 2014.

[16] David L. Wehlau. Invariants for the modular cyclic group of prime order via classical invariant theory. *J. Eur. Math. Soc. (JEMS)*, 15(3):775–803, 2013.

University of Aberdeen, King’s College, Aberdeen, AB24 3UE

E-mail address: j.elmer@abdn.ac.uk