Invariant Theory and the Koszul Complex Representations of $\mathbb{Z}/p$ in Characteristic p Applications

Larry Smith

YALE UNIVERSITY
NEW HAVEN, CT, USA
AND
AG-Invariantentheorie
GÖTTINGEN, GERMANY

SUMMARY : *We study the ring of invariants* $\mathbb{F}[V]^{\mathbb{Z}/p}$*, and its derived functors* $H^i(\mathbb{Z}/p;\mathbb{F}[V])$*, of the cyclic group* $\mathbb{Z}/p$ *of prime order* p *over a field* $\mathbb{F}$ *of characteristic* p*. We verify a formula of Ellingsrud and Skjelbred* [13] *for the homological codimension, show the quotient algebra* $\mathbb{F}[V]^{\mathbb{Z}/p}/\mathrm{Im}(\mathrm{Tr}^{\mathbb{Z}/p})$ *is Cohen-Macaulay, and that the ideal generated by the elements in the image of the transfer homomorphism,* $\mathrm{Im}(\mathrm{Tr}^{\mathbb{Z}/p}) \subset \mathbb{F}[V]^{\mathbb{Z}/p}$*, is primary of height* $n-1$ *when* V *is an* n*-dimensional irreducible representation of* $\mathbb{Z}/p$*. Using our cohomological computations and a previous result* [34] *about permutation representations we are able to obtain an upper bound for the degree of homogeneous forms in a minimal algebra generating set for* $\mathbb{F}[V]^{\mathbb{Z}/p}$*.*

The final work on this manuscript was done at Yale University, and I would like to thank the Yale Mathematics department for providing me with an office, library facilities, and atmosphere supportive to my research efforts.

MATHEMATICS SUBJECT CLASSIFICATION : 13A50 Invariant Theory

This note is a continuation of [33]. We will first be concerned with the rings of invariants of the irreducible representations of the cyclic group $\mathbb{Z}/p$ of prime order p over a field $\mathbb{F}$ of characteristic p. Specifically, for $2 \le n \le p$ the matrix (a single Jordan block)

$$\mathbf{J}_n = \begin{bmatrix} 1 & 1 & & & & \\ 0 & 1 & 1 & & & \\ 0 & \ddots & \ddots & 0 & & \\ & & & 1 & 1 & \\ & & & & 1 & \end{bmatrix} \in \mathrm{GL}(n, \mathbb{F}) \qquad 2 \le n \le p,$$

where $\mathbb{F}$ is a field of characteristic p is of order p and implements a faithful representation $\varrho_n : \mathbb{Z}/p \hookrightarrow \mathrm{GL}(n, \mathbb{F})$. Being a single Jordan block it is irreducible, and $\varrho_2, \ldots, \varrho_p$ is a complete list of irreducible representations of $\mathbb{Z}/p$ over $\mathbb{F}$. Since $\mathbf{J}_n$ is defined over the Galois field $\mathbb{F}_p$ with p elements, and $\mathbb{F}_p$ is a splitting field for $\mathbb{Z}/p$, we may, and will, suppose that $\mathbb{F} = \mathbb{F}_p$. Any finite dimensional representation of $\mathbb{Z}/p$ over $\mathbb{F}$ is a finite direct sum [1] of copies of these.

We set $V_n = \mathbb{F}^n$ and denote by $\mathbb{F}[V_n]$ the graded algebra of homogeneous polynomial functions on V_n (see e.g., [30] Section 1.1).Via $\mathbf{J}_n$, or ϱ_n, the group $\mathbb{Z}/p$ acts on $\mathbb{F}[V_n]$ and there is the ring of invariants $\mathbb{F}[V_n]^{\mathbb{Z}/p}$, which has been the subject of numerous [2] investigations [4], [5], [19], [13], [33], and [9] amongst others. In this note we are concerned with the **depth**, or **homological codimension** hom–codim$(\mathbb{F}[V_n]^{\mathbb{Z}/p})$ and the **transfer homomorphism** ([30] Section 4.2)

$$\mathrm{Tr}^{\mathbb{Z}/p} : \mathbb{F}[V_n] \longrightarrow \mathbb{F}[V_n]^{\mathbb{Z}/p},$$

which in this case is defined by $\mathrm{Tr}^{\mathbb{Z}/p} = \mathbf{J}_n^0 + \mathbf{J}_n^1 + \cdots + \mathbf{J}_n^{p-1}$. The transfer homomorphism along with $\partial := 1 - \mathbf{J}_n$ appears in the standard cocomplex

$$0 \longrightarrow \mathbb{F}[V_n] \xrightarrow{\partial} \mathbb{F}[V_n] \xrightarrow{\mathrm{Tr}^{\mathbb{Z}/p}} \mathbb{F}[V_n] \xrightarrow{\partial} \mathbb{F}[V_n] - \cdots$$

used to compute $H^*(\mathbb{Z}/p, \mathbb{F}[V_n])$, which in turn intervenes via the methods of [33] or [13] for studying hom–codim$(\mathbb{F}[V_n]^{\mathbb{Z}/p})$. From this cocomplex one sees ([10] or [14])

$$\begin{aligned} H^0(\mathbb{Z}/p; \mathbb{F}[V_n]) &= \mathbb{F}[V_n]^{\mathbb{Z}/p} \\ H^1(\mathbb{Z}/p; \mathbb{F}[V_n]) &= \ker(\mathrm{Tr}^{\mathbb{Z}/p})/\mathrm{Im}(\partial) \\ H^2(\mathbb{Z}/p; \mathbb{F}[V_n]) &= \mathbb{F}[V_n]^{\mathbb{Z}/p}/Im(\mathrm{Tr}^{\mathbb{Z}/p}) \end{aligned}$$

and $H^{i+2}(\mathbb{Z}/p; \mathbb{F}[V_n]) = H^i(\mathbb{Z}/p; \mathbb{F}[V_n])$ for all $i > 0$. To make effective use of the tools of [33] requires a knowledge of the cohomology $H^i(\mathbb{Z}/p; \mathbb{F}[V_n])$ for $i > 0$ as a module over a suitable subalgebra, such as $\mathbf{D}_*(n)$, the Dickson algebra, of $\mathbb{F}[V_n]^{\mathbb{Z}/p}$.

Let us abbreviate $H^i(\mathbb{Z}/p; \mathbb{F}[V_n])$ to $H^{\mathrm{ev}}(n)$ for $i > 0$ and i even, and $H^{\mathrm{od}}(n)$ for i odd. Although not profusely published, nor well known, it is not hard to see that $H^{\mathrm{od}}(n)$ and $H^{\mathrm{ev}}(n)$ have the same Poincaré series as graded vector spaces. This is a special case of Herbrand's Lemma (see e.g., [21] Theorem 5.2 or [28] VIII Proposition 8) and follows from the two exact sequences

$$\begin{aligned} 0 \longrightarrow \mathbb{F}[V_n]^{\mathbb{Z}/p} \longrightarrow \mathbb{F}[V_n] &\xrightarrow{\partial} \mathbb{F}[V_n] \longrightarrow \mathrm{coker}(\partial) \longrightarrow 0 \\ 0 \longrightarrow H^{\mathrm{od}}(n) \longrightarrow \mathrm{coker}(\partial) &\xrightarrow{\mathrm{Tr}^{\mathbb{Z}/p}} \mathbb{F}[V_n]^{\mathbb{Z}/p} \longrightarrow H^{\mathrm{ev}}(n) \longrightarrow 0 \end{aligned}$$

by taking Euler characteristics. Somewhat more suprising is the identity for Poincaré series of graded vector spaces

$$\sum_{s=0}^{n} (-1)^s P\left(\mathrm{Tor}^s_{\mathbf{D}_*(n)}\left(\mathbb{F}, H^{\mathrm{od}}(n)\right), t\right) = \sum_{s=0}^{n} (-1)^s P\left(\mathrm{Tor}^s_{\mathbf{D}_*(n)}\left(\mathbb{F}, H^{\mathrm{ev}}(n)\right), t\right).$$

[1] But do **not** jump the conclusion that anything analagous holds for the rings of invariants! See e.g. [34].

[2] Indeed, the study of these rings appears to be addictive.

This follows from Smoke's [35] formula (section 3) for the multiplicity symbols: this amounts to saying that $H^{\mathrm{od}}(n)$ and $H^{\mathrm{ev}}(n)$ are equal in the Grothendieck group of finitely generated modules over $\mathbf{D}_*(n)$. In this note we will show that in fact $H^{\mathrm{od}}(n)$ and $H^{\mathrm{ev}}(n)$ also have the same homological dimension as modules over $\mathbf{D}_*(n)$. This has led the author to pose the following:

PROBLEM: Let A be a graded, connected, commutative algebra over the field $\mathbb{F}$ of characteristic p and $\mathbb{Z}/p \hookrightarrow \mathrm{Aut}_*(A)$ a representation of $\mathbb{Z}/p$ by graded automorphisms of A. Are $H^1(\mathbb{Z}/p\,;A)$ and $H^2(\mathbb{Z}/p\,;A)$ isomorphic as modules over $A^{\mathbb{Z}/p}$?, or at least, over a suitable subalgebra $S \subseteq A^{\mathbb{Z}/p}$?

In [33] Proposition 4.3 we showed this to be the case when $\mathbb{Z}/p$ acts on $A = \mathbb{F}[V]$ via a permutation representation on a basis for V.

As a final comment on this problem we note that $\mathrm{Tr}^{\mathbb{Z}/p} = \partial^{p-1} \in \mathbb{F}(\mathbb{Z}/p)$, where $\mathbb{F}(\mathbb{Z}/p)$ denotes the group ring of $\mathbb{Z}/p$ over $\mathbb{F}$. Since $\partial^p = 0$ one has $\mathrm{Im}(\partial^{p-i}) \subseteq \ker(\partial^i)$ for $i = 1, \ldots, p-1$, and one might wonder if the modules $\ker(\partial^i)/\mathrm{Im}(\partial^{p-i})$ are all isomorphic for $i = 1, \ldots, p-1$.

Section 1 contains the cohomological computations that are applied in later sections, first for irreducible representations, and then for general finite dimensional representations, to verify a formula for hom–codim($\mathbb{F}[V]^{\mathbb{Z}/p}$) from [13] and to prove that $\mathrm{Im}(\mathrm{Tr}^{\mathbb{Z}/p}) \subset \mathbb{F}[V_n]^{\mathbb{Z}/p}$ is a primary ideal of height $n-1$ when V_n is irreducible. In Section 4 we establish for a general finite dimensional $\mathbb{Z}/p$-representation an upper bound for the degree of an algebra generator of $\mathbb{F}[V]^{\mathbb{Z}/p}$ in a minimal generating set. The proof of the depth formula uses [33] and the transfer computation uses [18]. The degree bound depends on results in [34] for permutation representations, some computations from [29], and some elmentary properties of Dade bases [25] shared by Jordan bases, as explained here.

§1. Some Cohomology Computations

We adhere to the notations introduced above, so in particular V_n is the irreducible n-dimensional representation of $\mathbb{Z}/p$ over the Galois field $\mathbb{F} = \mathbb{F}_p$ with p-elements; whence $2 \le n \le p$. Let $x_1, \ldots, x_n$ be the standard basis for V_n, i.e., the basis in which the representation of $\mathbb{Z}/p$ on V_n is implemented by the matrix $\mathbf{J}_n$, and denote by $z_1, \ldots, z_n \in V_n^*$ the dual basis for the dual vector space V_n^* of V_n. For two consecutive values of n the cohomology modules $H^{\mathrm{ev/od}}(n)$ are related, since there is the short exact sequence

$$0 \longrightarrow \mathbb{F}[z_1, \ldots, z_n] \xrightarrow{\cdot z_n} \mathbb{F}[z_1, \ldots, z_n] \longrightarrow \mathbb{F}[z_1, \ldots, z_{n-1}] \longrightarrow 0$$

where $\cdot z_n$ denotes multiplication by the fixed vector z_n: this yields an exact hexagon

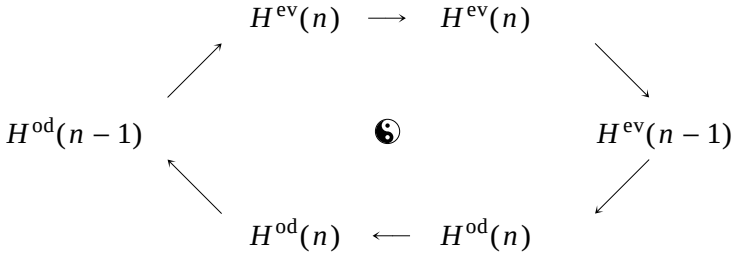


DIAGRAM 1.1: Exact Hexagon

The cohomology $H^{\mathrm{ev/od}}(n)$ are modules over $\mathbb{F}[V_n]^{\mathbb{Z}/p}$. The following lemma will help us to prove several results about $H^{\mathrm{ev/od}}(n)$ when $2 \le n \le p$ by downward induction on n starting with the case $n = p$ and results of [33].

LEMMA 1.1: *The map*

$$\cdot z_n : H^{\mathrm{ev/od}}(n) \longrightarrow H^{\mathrm{ev/od}}(n)$$

is the zero map.

PROOF: We are going to need a couple of formulae. We begin with the list

$$\begin{pmatrix} * \\ * \end{pmatrix} \qquad \begin{aligned} \partial(z_1) &= -z_2 \\ \partial(z_2) &= -z_3 \\ \ddots &= \ddots \\ \partial(z_{n-1}) &= -z_n \\ \partial(z_n) &= 0 \end{aligned}$$

from which we obtain

$$\mathrm{Tr}^{\mathbb{Z}/p}(z_1) = \partial^{p-1}(z_1) = (-1)^{p-1} z_n = z_n$$

and therefore $z_n \in \mathrm{Im}(\mathrm{Tr}^{\mathbb{Z}/p})$. From [13] we recall the formula (Lemma 1.1 (ii))

$$(**) \qquad f \cdot \mathrm{Tr}^{\mathbb{Z}/p}(h) - \mathrm{Tr}^{\mathbb{Z}/p}(f) \cdot h \in \mathrm{Im}(\partial)$$

where $f, h \in \mathbb{F}[V_n]$ are arbitrary.

We divide the proof of the lemma into two cases:

Case H^{ev}: we then have

$z_n \in \mathrm{Im}(\mathrm{Tr}^{\mathbb{Z}/p})$,

$H^{\mathrm{ev}}(n) = \mathbb{F}[V]^{\mathbb{Z}/p}/\mathrm{Im}(\mathrm{Tr}^{\mathbb{Z}/p})$

from which it is immediate that

$$\cdot z_n : H^{\mathrm{ev}}(n) \circlearrowright$$

is the zero map.

Case H^{od}: we have

$$H^{\mathrm{od}}(n) = \ker(\mathrm{Tr}^{\mathbb{Z}/p})/\mathrm{Im}(\partial)$$

so if $h \in \ker(\mathrm{Tr}^{\mathbb{Z}/p})$ we obtain from the formual (**) and $\begin{pmatrix} * \\ * \end{pmatrix}$

$$-z_n \cdot h = -\mathrm{Tr}^{\mathbb{Z}/p}(z_1) \cdot h \in \mathrm{Im}(\partial)$$

so

$$\cdot z_n : H^{\mathrm{od}}(n) \circlearrowright$$

is also the zero map. □

From Lemma 1.1 it follows that the hexagon ☯ splits into short exact sequences, namely:

LEMMA 1.2: *For $2 \le n \le p$ there are exact sequences*

$$0 \longrightarrow H(n) \xrightarrow{i^*} H(n-1) \xrightarrow{\delta} H(n) \longrightarrow 0$$

where i^* has degree 0 amd δ degree -1. □

PROPOSITION 1.3: *For $2 \le n \le p$ the element $\mathbf{d}_{n,n-1} \in \mathbf{D}_*(n)$ is a regular element on $H(n)$.*

PROOF: For $n = p$ this follows from [34] Theorem 2, or [33] the discussion preceeding Proposition 4.1. We proceed by downward induction from p and assume the result established for n. Consider the exact sequence of Lemma 1.2

$$0 \longrightarrow H(n) \xrightarrow{i^*} H(n-1) \xrightarrow{\delta} H(n) \longrightarrow 0.$$

Since $\mathbf{d}_{n,n-1} \in \mathbf{D}_*(n)$ is regular on $H(n)$, $H(n)$ is a free module over $\mathbb{F}[\mathbf{d}_{n,n-1}]$. As modules over $\mathbb{F}[\mathbf{d}_{n,n-1}]$ the preceeding sequence must then split, and $H(n-1)$ is also a free module over $\mathbb{F}[\mathbf{d}_{n,n-1}]$. This of course is equivalent to $\mathbf{d}_{n,n-1}$ being regular on $H(n-1)$. □

PROPOSITION 1.4: *For $2 \le n \le p$ the elements $\mathbf{d}_{n,n-2}, \ldots, \mathbf{d}_{n,0} \in \mathbf{D}_*(n)$ act nilpotently on $H(n)$.*

PROOF: For $n = p$ the elements $\mathbf{d}_{n,n-2}, \ldots, \mathbf{d}_{n,0}$ act trivially on $H(p)$ by [34] Theorem 2, and as in Proposition 1.3 we again proceed by downward induction. From the exact sequence

$$0 \longrightarrow H(n) \xrightarrow{i^*} H(n-1) \xrightarrow{\delta} H(n) \longrightarrow 0$$

of Lemma 1.2 we see that regarded as a $\mathbf{D}_*(n)$-module the elements $\mathbf{d}_{n,n-2}, \ldots, \mathbf{d}_{n,0} \in \mathbf{D}_*(n)$ act nilpotently on $H(n-1)$ also.

Next, note that the $\mathbf{D}_*(n)$-module structure on $H(n-1)$ arises via the change of rings map $i^* : \mathbf{D}_*(n) \longrightarrow \mathbf{D}_*(n-1)$ induced by the inclusion $V_{n-1} \hookrightarrow V_n$. The map i^* satisfies ([30] Section 8.1)

$$i^*(\mathbf{d}_{n,i}) = \begin{cases} 0 & \text{for } i = 0 \\ \mathbf{d}_{n-1,i-1}^p & \text{for } i = 1, \ldots, n-1. \end{cases}$$

Therefore the nilpotence of $\mathbf{d}_{n,n-2}, \ldots, \mathbf{d}_{n,0} \in \mathbf{D}_*(n)$ entails that of $\mathbf{d}_{n-1,n-3}, \ldots, \mathbf{d}_{n-1,0} \in \mathbf{D}_*(n-1)$. □

Combining Propositions 1.3 and 1.2 leads to:

THEOREM 1.5: *For* $2 \leq n \leq p$ $\text{hom–dim}_{\mathbf{D}_*(n)}\big(H(n)\big) = n-1$.

PROOF: By Proposition 1.4 the elements

$$\mathbf{d}_{n,n-2}, \ldots, \mathbf{d}_{n,0} \in \mathbf{D}_*(n)$$

act nilpotently on $\mathbf{D}_*(n)$. Therefore for large $\ell \in \mathbb{N}$ the elements

$$\mathbf{d}_{n,n-2}^{\ell}, \ldots, \mathbf{d}_{n,0}^{\ell} \in \mathbf{D}_*(n)$$

act trivially. Consider the subalgebra $S := \mathbb{F}[\mathbf{d}_{n,n-1}, \mathbf{d}_{n,n-2}^{\ell}, \ldots, \mathbf{d}_{n,0}^{\ell}] \subseteq \mathbf{D}_*(n)$. Then $\mathbf{D}_*(n)$ is a free S-module of finite rank, so

$$\text{hom–dim}_{\mathbf{D}_*(n)}\big(H(n)\big) = \text{hom–dim}_S\big(H(n)\big).$$

Since, in addition $H(n)$ is a free $\mathbb{F}[\mathbf{d}_{n,n-1}]$-module by Proposition 1.3, a simple Koszul complex computation shows

$$\text{Tor}_S\big(\mathbb{F}, H(n)\big) \cong \Big(\mathbb{F} \otimes_S H(n)\Big) \otimes E[s^{-1}(\mathbf{d}_{n,n-2}^{\ell}), \ldots, s^{-1}(\mathbf{d}_{n,0}^{\ell})]$$

so

$$\begin{gathered} \text{Tor}_S^{-(n-1)}\big(\mathbb{F}, H(n)\big) \ni s^{-1}(\mathbf{d}_{n,n-2}^{\ell}) \cdots s^{-1}\mathbf{d}_{n,0}^{\ell} \neq 0 \\ \text{Tor}_S^{-n}\big(\mathbb{F}, H(n)\big) = 0 \end{gathered}$$

from which the result follows. □

COROLLARY 1.6: *For* $2 \leq n \leq p$, $\text{hom–codim}_{\mathbf{D}_*(n)}\big(H(n)\big) = 1$.

PROOF: This follows from Theorem 1.5 and the Auslander-Buchsbaum formula [8] Theorem 1.3.3. □

§2. Invariants of Irreducible $\mathbb{Z}/p$-representations

Using the results of the previous section and the spectral sequence of [33] leads to a proof of one of the results of [13].

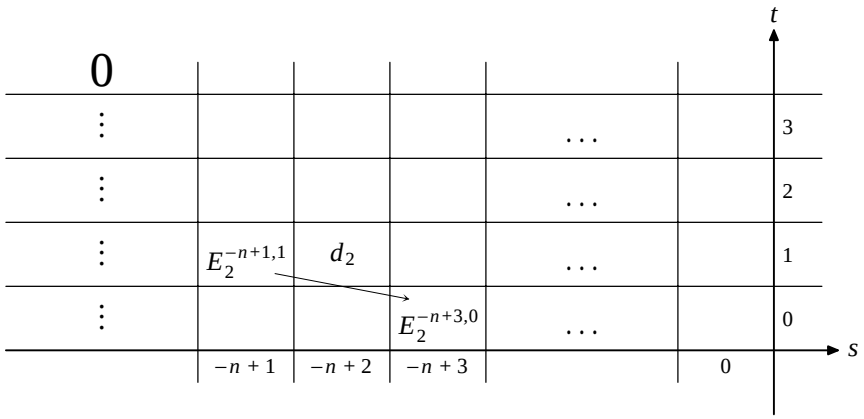
PROPOSITION 2.1 (Ellingsrud and Skjelbred): *Let* $p \geq 5$ *be an odd prime,* $\mathbb{F} = \mathbb{F}_p$, *and* $\rho_n : \mathbb{Z}/p \hookrightarrow \text{GL}(n, \mathbb{F})$ *the representation implemented by the Jordan block* $\mathbf{J}_n$, $3 \leq n \leq p$. *Then*

$$\text{hom–codim}(\mathbb{F}[V]^{\mathbb{Z}/p}) = 3.$$

PROOF: Consider the spectral sequence $\{E_r, d_r\}$ of [33] with

$$E_r \Rightarrow H^*\left(\mathbb{Z}/p\,, \mathbb{F}[V]_{\mathrm{GL}(n,\mathbb{F})}\right)$$
$$E_2^{s,t} = \mathrm{Tor}^s_{\mathbf{D}_*(n)}\left(\mathbb{F}, H^t(\mathbb{Z}/p\,; \mathbb{F}[V])\right).$$

From Theorem 1.5 the E_2-term of this spectral sequence has the form



where the term $E_2^{-(n-1),1} \neq 0$. The total degree of this term is $1 + (-(n-1)) = 2 - n$ which is negative. Hence $E_\infty^{-(n-1),1} = 0$. The only nonzero differential either starting or ending at $E_2^{-(n-1),1}$ is the indicated one, namely

$$d_2 : E_2^{-(n-1),1} \longrightarrow E_2^{-(n-3),0},$$

which must therefore be an isomorphism. Hence

$$0 \neq E_2^{-(n-3),0} = \mathrm{Tor}^{-(n-3)}_{\mathbf{D}_*(n)}(\mathbb{F}, \mathbb{F}[V]^{\mathbb{Z}/p})$$

and therefore

$$\text{hom–dim}_{\mathbf{D}_*(n)}(\mathbb{F}[V]^{\mathbb{Z}/p}) \geq n - 3.$$

On the otherhand, the picture also shows that $E_2^{-(n-2),0}$ must be zero since it too has negative total degree and no nonzero differential can either arrive or terminate at it. Therefore

$$0 = E_2^{-(n-2),0} = \mathrm{Tor}^{-(n-2)}_{\mathbf{D}_*(n)}(\mathbb{F}, \mathbb{F}[V]^{\mathbb{Z}/p})$$

so

$$\text{hom–dim}_{\mathbf{D}_*(n)}(\mathbb{F}[V]^{\mathbb{Z}/p}) \leq n - 3.$$

Combining these two inequalities gives

$$\text{hom–dim}_{\mathbf{D}_*(n)}(\mathbb{F}[V]^{\mathbb{Z}/p}) = n - 3.$$

and the result follows from the Auslander-Buchsbaum equality, loc.cit., . □

REMARK: The analagous result for $p = 3$ follows from the fact that rings invariants in three or less variables are always Cohen-Macaulay [31].

We can also apply our cohomological computations from Section 1 to study the ideal $\mathrm{Im}(\mathrm{Tr}^{\mathbb{Z}/p}) \subset \mathbb{F}[V]^{\mathbb{Z}/p}$ when V is an irreducible $\mathbb{Z}/p$-representation over $\mathbb{F}$. Specifically (see also [18] Proposition 2.9)

PROPOSITION 2.2: *Let p be an odd prime and V an irreducible representation of $\mathbb{Z}/p$ over the field $\mathbb{F}$ of characteristic p. Then $\mathrm{Im}(\mathrm{Tr}^{\mathbb{Z}/p}) \subset \mathbb{F}[V]^{\mathbb{Z}/p}$ is a primary ideal of height $\dim_{\mathbb{F}}(V) - 1$.*

PROOF: There is no loss in generality in supposing that V is the representation over $\mathbb{F} = \mathbb{F}_p$ implemented by the Jordan block $\mathbf{J}_n \in \mathrm{GL}(n, \mathbb{F})$ where $2 \leq n \leq p$. By [18] the transfer variety, $X_{\mathbb{Z}/p}$, i.e., the variety defined by the extended ideal $\left(\mathrm{Im}(\mathrm{Tr}^{\mathbb{Z}/p})\right)^e \subset \mathbb{F}[V]$, is the fixed point set $V^{\mathbb{Z}/p}$. If $x_1, \ldots, x_n \in V$ is a Jordan basis with dual basis $z_1, \ldots, z_n \in V^*$ this means

$$X_{\mathbb{Z}/p} = V^{\mathbb{Z}/p} = \mathrm{Span}_{\mathbb{F}}\{x_1\} = \bigcap_{i=2}^{n} \ker(z_i),$$

so by Hilbert's Nullstellensatz

$$\sqrt{\left(\mathrm{Im}(\mathrm{Tr}^{\mathbb{Z}/p})\right)^e} = (z_2, \ldots, z_n) \subset \mathbb{F}[V].$$

This is a prime ideal in $\mathbb{F}[V]$ and hence so is

$$(z_2, \ldots, z_n) \cap \mathbb{F}[V]^{\mathbb{Z}/p} = \sqrt{\left(\mathrm{Im}(\mathrm{Tr}^{\mathbb{Z}/p})\right)^e} = \sqrt{\left(\mathrm{Im}(\mathrm{Tr}^{\mathbb{Z}/p})\right)} \subset \mathbb{F}[V]^{\mathbb{Z}/p}.$$

Therefore $\mathrm{Im}\left(\mathrm{Tr}^{\mathbb{Z}/p}\right) \subset \mathbb{F}[V]^{\mathbb{Z}/p}$ has a unique minimal associated prime ideal, say $\mathfrak{p}$. The ideal $\mathfrak{p}$ is invariant under the action of the Steenrod algebra P^* (see e.g., [30] Chapter 11 Section 5). This ideal has height $n-1$, hence $\mathfrak{p} \cap \mathbf{D}_*(n)$ is also a prime ideal of height $n-1$ and P^*-invariant. By [30] Theorem 11.4.6 the only height $n-1$, P^*-invariant, ideal in $\mathbf{D}_*(n)$ is $(\mathbf{d}_{n,0}, \ldots, \mathbf{d}_{n,n-2})$, and the only height n, P^*-invariant, ideal is the maximal ideal. If $\mathrm{Im}(\mathrm{Tr}^{\mathbb{Z}/p})$ has an embedded prime ideal in $\mathbb{F}[V]^{\mathbb{Z}/p}$, say $\tilde{\mathfrak{p}}$, then $\tilde{\mathfrak{p}}$ has height n and is P^*-invariant [23] and [22]. Then $\tilde{\mathfrak{p}} \cap \mathbf{D}_*(n)$ must be the maximal ideal of $\mathbf{D}_*(n)$ so by lying over [30] Lemma 5.4.1 $\tilde{\mathfrak{p}}$ is the maximal ideal of $\mathbb{F}[V]^{\mathbb{Z}/p}$.

Consider the quotient algebra $\mathbb{F}[V]^{\mathbb{Z}/p}/\mathrm{Im}(\mathrm{Tr}^{\mathbb{Z}/p}) = H^{\mathrm{ev}}(n)$. The associated primes of (0) in H^{ev} are the quotients of the associated primes of $\mathrm{Im}(\mathrm{Tr}^{\mathbb{Z}/p})$ in $\mathbb{F}[V]^{\mathbb{Z}/p}$ by $\mathrm{Im}(\mathrm{Tr}^{\mathbb{Z}/p})$. The preceeding argument therefore shows: if $\mathrm{Im}(\mathrm{Tr}^{\mathbb{Z}/p})$ has an embedded prime in $\mathbb{F}[V]^{\mathbb{Z}/p}$, then $(0) \subset H^{\mathrm{ev}}(n)$ has the maximal ideal as an associated prime ideal. By [3] Theorem 2.3.22 this means that every element in $H^{\mathrm{ev}}(n)$ of positive degree is a zero divisor, contrary to Proposition 1.3. Therefore $\mathrm{Im}(\mathrm{Tr}^{\mathbb{Z}/p}) \subset \mathbb{F}[V]^{\mathbb{Z}/p}$ cannot have any embedded prime ideals, and since it has a unique minimal associated prime ideal it must be primary. □

REMARK: Representations of $\mathbb{Z}/2$ in characteristic 2 are permutation representations, so $\mathrm{Im}(\mathrm{Tr}^{\mathbb{Z}/2})$ is quite explicitly described in [34].

§3. Invariants of General $\mathbb{Z}/p$-representations

In this section we apply the results of the preceeding sections to general finite dimensional representations $\rho : \mathbb{Z}/p \hookrightarrow \mathrm{GL}(n, \mathbb{F})$ of $\mathbb{Z}/p$ over a field of characteristic p. Again, since $\mathbb{F}_p$ is a splitting field for $\mathbb{Z}/p$, we may assume that $\mathbb{F} = \mathbb{F}_p$. It will be convenient to fix some notations for this section.

NOTATION: $\rho : \mathbb{Z}/p \hookrightarrow \mathrm{GL}(n, \mathbb{F})$ will denote a fixed faithful representation of $\mathbb{Z}/p$ over the Galois field $\mathbb{F} = \mathbb{F}_p$, p an odd prime. $V = \mathbb{F}^n$ and $V = V_{n_1} \oplus \cdots \oplus V_{n_k}$ will be a fixed decomposition of V into irreducible representations of dimensions $n_1, \ldots, n_k$. Each fixed point set $V^*_{n_i}$ is 1-dimensional and $\ell_i \in (V^*_{n_i})^{\mathbb{Z}/p}$ is a fixed nonzero linear form for $i = 1, \ldots, k$. N.b., $1 \leq n_i \leq p$, $i = 1, \ldots, k$ and $\mathbb{Z}/p$ acts on V_{n_i} in an appropriate choice of basis via the Jordan block $\mathbf{J}_{n_i} \in \mathrm{GL}(n_i, \mathbb{F})$.

We first need to adapt Lemma 1.1 to this more general context.

LEMMA 3.1: *With the preceeding notations the maps*

$$\cdot \ell_i : H^j(\mathbb{Z}/p; \mathbb{F}[V]) \longrightarrow H^j(\mathbb{Z}/p; \mathbb{F}[V]) \qquad j > 0$$

are trivial for $i = 1, \ldots, k$.

PROOF: Let $z_1(i), \dots, z_{n_i}(i) = \ell_i$ be the dual Jordan basis for $V^*_{n_i}$. The formula $\begin{pmatrix} * \\ * \end{pmatrix}$ from the proof of Lemma 1.1 shows that

$$\ell_i \in \mathrm{Im}(\mathrm{Tr}^{\mathbb{Z}/p}) \subset \mathbb{F}[V]^{\mathbb{Z}/p}$$

and the formula (**) shows

$$\ell_i \cdot h \in \mathrm{Im}(\partial) \qquad \forall\ h \in \ker(\mathrm{Tr}^{\mathbb{Z}/p}).$$

The result then follows as in the proof of Lemma 1.1. □

PROPOSITION 3.2: *With the preceeding notations any two distinct elements of the collection $\ell_1, \dots, \ell_k \in \mathbb{F}[V]^{\mathbb{Z}/p}$ are a regular sequence but no three are.*

PROOF: We may as well suppose that k is at least two. Consider the Koszul complex

$$\mathscr{L} = \mathbb{F}[V] \otimes E[s^{-1}\ell_1, \dots, s^{-1}\ell_k]$$
$$\partial(f \otimes 1) = 0, \quad \partial(1 \otimes s^{-1}\ell_i) = \ell_i \otimes 1 \qquad i = 1, \dots, k.$$

As in [33] Section 2 we have the cohomology $H^*\big(\mathbb{Z}/p; (\mathscr{L}, \partial)\big)$ of $\mathbb{Z}/p$ with coefficients in the complex $(\mathscr{L}, \partial)$, from which we obtain (loc.cit.) a spectral sequence

$$E_r \Rightarrow H^*(\mathbb{Z}/p; \mathbb{F}[V_{n_1-1} \oplus \cdots \oplus V_{n_k-1}])$$
$$E_2^{s,t} = \mathrm{Tor}^s_{\mathbb{F}[\ell_1, \dots, \ell_k]}\big(\mathbb{F}, H^t(\mathbb{Z}/p; \mathbb{F}[V])\big).$$

Here we have identified

$$\mathbb{F}[V]/(\ell_1, \dots, \ell_k)$$

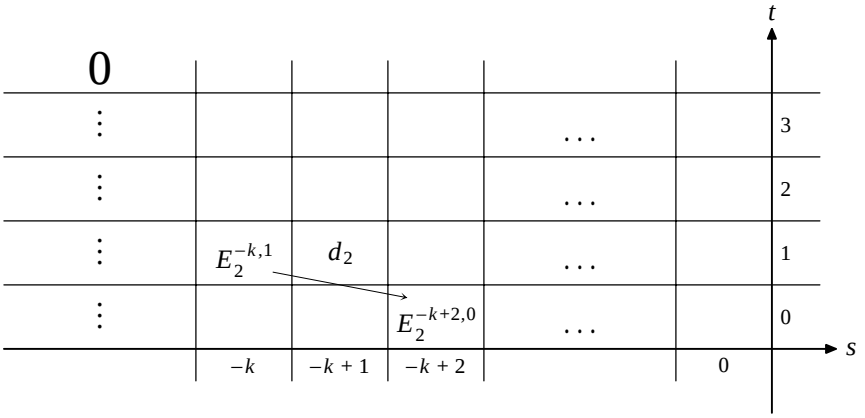
via the obvious isomorphism with

$$\mathbb{F}[V_{n_1-1} \oplus \cdots \oplus V_{n_k-1}].$$

Since $\ell_1, \dots, \ell_k$ act trivially on $H^t(\mathbb{Z}/p; \mathbb{F}[V])$ for $t > 0$ (Lemma 3.1) it follows that

$$E_2^{*,t} = \mathrm{Tor}^*_{\mathbb{F}[\ell_1, \dots, \ell_k]}\big(\mathbb{F}, H^t(\mathbb{Z}/p; \mathbb{F}[V])\big) \cong H^t(\mathbb{Z}/p; \mathbb{F}[V]) \otimes E[s^{-1}\ell_1, \dots, s^{-1}\ell_k].$$

In particular $E_2^{-k,1} \neq 0$ since it contains the nonzero element $1 \otimes s^{-1}\ell_1 \cdots s^{-1}\ell_k$. The total degree of $E_2^{-k,1}$ is negative and $E_\infty^{-k,1} = 0$ since the target of the spectral sequence is zero in negative gradings. As the following picture



shows, the only possible nonzero differential that can either originate or terminate at $E_2^{-k,1}$ is $d_2 : E_2^{-k,1} \longrightarrow E_2^{-k+2,0}$, which must therefore be an isomorphism, so

$$0 \neq E_2^{-k+2,0} = \mathrm{Tor}^{-k+2}_{\mathbb{F}[\ell_1, \dots, \ell_k]}\big(\mathbb{F}, \mathbb{F}[V]^{\mathbb{Z}/p}\big).$$

In a similar manner we see that

$$0 = E_2^{-k+1,0} = \mathrm{Tor}^{-k+1}_{\mathbb{F}[\ell_1, \dots, \ell_k]}\big(\mathbb{F}, \mathbb{F}[V]^{\mathbb{Z}/p}\big),$$

and hence $\hom\text{–}\dim_{\mathbb{F}[\ell_1, \dots, \ell_k]}(\mathbb{F}[V]^{\mathbb{Z}/p}) = k - 2$. The Auslander-Buchsbaum equality, loc.cit., then implies $\hom\text{–}\mathrm{codim}_{\mathbb{F}[\ell_1, \dots, \ell_k]}(\mathbb{F}[V]^{\mathbb{Z}/p}) = 2$, so at most two of $\ell_1, \dots, \ell_k$ can form a regular sequence. The proof of [30] Proposition 6.7.9 shows that indeed any two distinct ones do so. □

NOTATION: For $i > 0$, $H^i(\mathbb{Z}/p;\mathbb{F}[V])$ will be denoted by $H^{\mathrm{ev}}(n_1,\ldots,n_k)$ when i is even, and by $H^{\mathrm{od}}(n_1,\ldots,n_k)$ when i is odd, while if the parity of i is unimportant $H(n_1,\ldots,n_k)$ denotes either of the two.

The subgroup

$$\mathrm{GL}(n_1,\mathbb{F})\times\cdots\times\mathrm{GL}(n_k,\mathbb{F}) \subseteq \mathrm{GL}(n,\mathbb{F})$$

consisting of the block matrices

$$\begin{bmatrix} \mathbf{T}_1 & & \\ 0 & \ddots & 0 \\ & & \mathbf{T}_k \end{bmatrix} \qquad \mathbf{T}_i \in \mathrm{GL}(n_i,\mathbb{F}) \qquad i = 1,\ldots,k$$

has as ring of invariants the tensor product

$$\mathbf{D}_*(n_1)\otimes\cdots\otimes\mathbf{D}_*(n_k) =: \mathbf{D}_*(n_1,\ldots,n_k)$$

of Dickson algebras, and $H(n_1,\ldots,n_k)$ is a module over $\mathbf{D}(n_1,\ldots,n_k)$.

PROPOSITION 3.3: *With the preceeding notations, the k elements in $\mathbf{D}_*(n_1,\ldots,n_k)$*

$$\begin{aligned}
&\mathbf{d}_{n_1,n_1-1}\otimes 1\otimes\cdots\otimes 1\\
&1\otimes\cdots\otimes\mathbf{d}_{n_m,n_m-1}\otimes 1\otimes\cdots\otimes 1\\
&1\otimes\cdots\otimes 1\otimes\mathbf{d}_{n_k,n_k-1}
\end{aligned}$$

form a regular sequence on $H(n_1,\ldots,n_k)$, and the remaining Dickson polynomials

$$\begin{aligned}
&\mathbf{d}_{n_1,n_1-j_1}\otimes 1\otimes\cdots\otimes 1, && j_1 = 0,\ldots,n_1-2\\
&1\otimes\cdots\otimes\mathbf{d}_{n_m,n_m-j_m}\otimes 1\otimes\cdots\otimes 1, && j_m = 0,\ldots,n_m-2\\
&1\otimes\cdots\otimes 1\otimes\mathbf{d}_{n_k,n_k-j_k}, && j_k = 0,\ldots,n_k-2
\end{aligned}$$

act nilpotently.

PROOF: From Lemma 3.1 we have an exact sequence

$$0\longrightarrow H(n_1,\ldots,n_m,\ldots,n_k)\longrightarrow H(n_1,\ldots,n_m-1,\ldots,n_k)\longrightarrow H(n_1,\ldots,n_m,\ldots,n_k)\longrightarrow 0.$$

By Proposition 4.4 of [33] the desired conclusion holds for $n_1 = n_2 = \cdots = n_k = p$, since in this case $\rho:\mathbb{Z}/p\hookrightarrow\mathrm{GL}(n,\mathbb{F})$ is conjugate to a permutation representation. The result follows by downward induction from this case. □

COROLLARY 3.4: *With the preceeding notations we have*

$$\text{hom–dim}_{\mathbf{D}_*(n_1,\ldots,n_k)}\big(H(n_1,\ldots,n_k)\big) = n-k.$$

PROOF: The proof is completely analagous to that of Theorem 1.5. □

COROLLARY 3.5: *With the preceeding notations the Dickson polynomials $\mathbf{d}_{n,n-1},\ldots,\mathbf{d}_{n,n-k}\in\mathbf{D}_*(n)$ are a regular sequence on $H(n_1,\ldots,n_k)$, and $\mathbf{d}_{n,n-k+1},\ldots,\mathbf{d}_{n,0}\in\mathbf{D}_*(n)$ act nilpotently.*

PROOF: This follows from Proposition 3.4, the Auslander-Buchsbaum equality (loc. cit.), and the main result of [7]. □

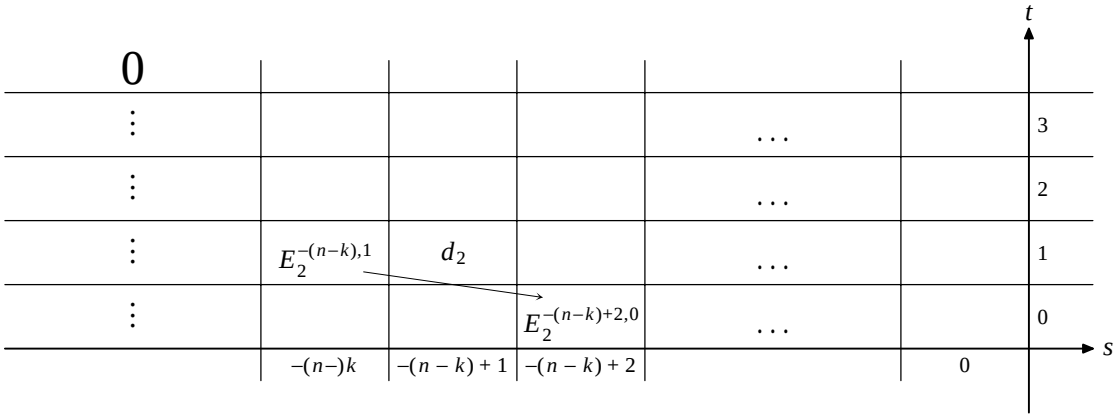
THEOREM 3.6 (Ellingsrud-Skjelbred [13]): *Let p be an odd prime and $\rho:\mathbb{Z}/p\hookrightarrow\mathrm{GL}(n,\mathbb{F})$ a faithful representation of the cyclic group $\mathbb{Z}/p$ over the field $\mathbb{F}$ of characteristic p. Then*

$$\text{hom–codim}(\mathbb{F}[V]^{\mathbb{Z}/p}) = 2 + \dim_{\mathbb{F}}(V^{\mathbb{Z}/p}).$$

PROOF: Write $V = V_{n_1} \oplus \cdots \oplus V_{n_k}$ as a sum of indecomposable representations of $\mathbb{Z}/p$. We consider the spectral sequence $\{E_r, d_r\}$ of [33] Proposition 2.2 with

$$E_r \Rightarrow H^*(\mathbb{Z}/p; \mathbb{F}[V]_{\mathrm{GL}(n_1;\mathbb{F})\times\cdots\times\mathrm{GL}(n_k;\mathbb{F})})$$
$$E_2^{s,t} = \mathrm{Tor}^s_{\mathbf{D}_*(n_1,\ldots,n_k)}\left(\mathbb{F}, H^t(\mathbb{Z}/p, \mathbb{F}[V])\right).$$

From Corollary 3.4 we have that $E_2^{-(n-k),1} = \mathrm{Tor}^{-(n-k)}_{\mathbf{D}_*(n_1,\ldots,n_k)}\left(\mathbb{F}, H^1(\mathbb{Z}/p; \mathbb{F}[V])\right) \neq 0$. The total degree of this term is $1 + k - n$, which is negative. The target of the spectral sequence $H^*(\mathbb{Z}/p; \mathbb{F}[V]_{\mathrm{GL}(n_1;\mathbb{F})\times\cdots\times\mathrm{GL}(n_k;\mathbb{F})})$ is zero in negative degrees, and, as the following picture



shows, the only possible nonzero differential either originating or terminating at $E_2^{-(n-k),1}$ is $d_2 : E_2^{-(n-k),1} \longrightarrow E_2^{-(n-k)+2,0}$, so we must have

$$0 \neq E_2^{-(n-k)+2,0} = \mathrm{Tor}^{-(n-k)+2}_{\mathbf{D}_*(n_1,\ldots,n_k)}\left(\mathbb{F}, \mathbb{F}[V]^{\mathbb{Z}/p}\right).$$

The same picture shows

$$0 = E_2^{-(n-k)+1,0} = \mathrm{Tor}^{-(n-k)+1}_{\mathbf{D}_*(n_1,\ldots,n_k)}\left(\mathbb{F}, \mathbb{F}[V]^{\mathbb{Z}/p}\right).$$

Hence

$$\mathrm{hom\text{–}dim}_{\mathbf{D}_*(n_1,\ldots,n_k)}\left(\mathbb{F}[V]^{\mathbb{Z}/p}\right) = n - k - 2$$

whence the result follows from the Auslander-Buchsbaum (loc.cit.) equality. □

REMARK: For $n = sp + r$ where $r < p$ the Jordan block matrix

$$\mathbf{J}_n = \begin{bmatrix} 1 & 1 & & & & \\ 0 & 1 & 1 & & & \\ 0 & \ddots & \ddots & 0 & & \\ & & & 1 & 1 & \\ & & & & 1 & \end{bmatrix} \in \mathrm{GL}(n, \mathbb{F}) \qquad 2 \leq n \leq p,$$

implements a representation of the cyclic group $\mathbb{Z}/p^{s+1}$ of order p^{s+1} and a completely analagous analysis of the corresponding representations can be made.

PROPOSITION 3.7: *If p is a prime and $\rho : \mathbb{Z}/p \hookrightarrow \mathrm{GL}(n, \mathbb{F})$ a faithful representation of the cyclic group $\mathbb{Z}/p$ over a field $\mathbb{F}$ of characteristic p, then the quotient algebra $\mathbb{F}[V]^{\mathbb{Z}/p}/\mathrm{Im}(\mathrm{Tr}^{\mathbb{Z}/p})$ is Cohen-Macaulay of Krull dimension $\dim_{\mathbb{F}}(V^{\mathbb{Z}/p})$.*

PROOF: For $p = 2$ this is shown in [34] Theorem 1, so we suppose p is odd, and without loss of generality that $\mathbb{F} = \mathbb{F}_p$. Let

$$V = V_{n_1} \oplus \cdots \oplus V_{n_k}$$

be a decomposition of V into irreducible $\mathbb{Z}/p$-representations. We know from [18] that

$$ht(\mathrm{Im}(\mathrm{Tr}^{\mathbb{Z}/p})) = n - k$$

so for the Krull dimension of the quotient algebra we have

$$\dim\left(\mathbb{F}[V]^{\mathbb{Z}/p}/\mathrm{Im}(\mathrm{Tr}^{\mathbb{Z}/p})\right) = k.$$

By Proposition 3.3 we know the k elements

$$\left\{1\otimes\cdots\otimes 1\otimes \mathbf{d}_{n_i,n_i-1}1\otimes\cdots\otimes 1 \mid i = 1,\ldots,k\right\}$$

are a regular sequence on $H^{\mathrm{ev}}(n_1,\ldots,n_k) = \mathbb{F}[V]^{\mathbb{Z}/p}/\mathrm{Im}(\mathrm{Tr}^{\mathbb{Z}/p})$, so

$$\text{hom–codim}_{\mathbf{D}_*(n_1,\ldots,n_k)}\left(\mathbb{F}[V]^{\mathbb{Z}/p}/\mathrm{Im}(\mathrm{Tr}^{\mathbb{Z}/p})\right) \geq k.$$

Since

$$\mathbf{D}_*(n_1,\ldots,n_k)/\mathrm{Im}(\mathrm{Tr}^{\mathbb{Z}/p}) \cap \mathbf{D}_*(n_1,\ldots,n_k) \subset \mathbb{F}[V]^{\mathbb{Z}/p}/\mathrm{Im}(\mathrm{Tr}^{\mathbb{Z}/p})$$

is a finite extension it follows from [3] (or the **non**preprint [32] which is available on request)) that

$$\text{hom–codim}\left(\mathbb{F}[V]^{\mathbb{Z}/p}/\mathrm{Im}(\mathrm{Tr}^{\mathbb{Z}/p})\right) \geq k.$$

Combining this with the general inequality [8] or [32]

$$k = \dim\left(\mathbb{F}[V]^{\mathbb{Z}/p}/\mathrm{Im}(\mathrm{Tr}^{\mathbb{Z}/p})\right) \geq \text{hom–codim}\left(\mathbb{F}[V]^{\mathbb{Z}/p}/\mathrm{Im}(\mathrm{Tr}^{\mathbb{Z}/p})\right)$$

yields the desired conclusion. □

§4. Degree Bounds

In this section we combine the cohomological computations of Section 1 with results of [34] on permutation representations to provide an upper bound on the degrees of algebra generators for rings of invariants of $\mathbb{Z}/p$ in characteristic p.

To set the stage we suppose that $\mathbb{F}$ is a field of characteristic p and $\rho : \mathbb{Z}/p \hookrightarrow \mathrm{GL}(n,\mathbb{F})$ a faithful representation. If

$$V = V_{n_1}\oplus\cdots\oplus V_{n_k} \qquad \dim_{\mathbb{F}}(V_{n_i}) = n_i, \text{ for } i = 1,\ldots,k$$

is a decomposition of V into irreducible $\mathbb{Z}/p$-representations, and $z_1(i),\ldots,z_{n_i}(i)$ is a Jordan basis for $V^*_{n_i}$ for $i = 1,\ldots,k$, then $\left\{z_i(j) \mid i = 1,\ldots,n_i,\ j = 1,\ldots,k\right\}$ is a **Dade basis** for V^*. This means that the top Chern classes $\left\{c_{\mathrm{top}}\left(z_i(j)\right) \mid i = 1,\ldots,n_i,\ j = 1,\ldots,k\right\}$ are a system of parameters for $\mathbb{F}[V]$, and since they are invariant, also for $\mathbb{F}[V]^{\mathbb{Z}/p}$. This may be verified directly from [30] Proposition 5.3.7 (see also [25]).

A Jordan block of dimension m contributes 1 linear top Chern class (that of the fixed basis vector) and $m-1$ Chern classes of degree p (those of the remaining basis vectors, whose $\mathbb{Z}/p$-orbits have p elements) to a system of parameters. Let

$$D_*(n_1,\ldots,n_k) := \mathbb{F}\left[c_{\mathrm{top}}\left(z_i(j)\right) \mid i = 1,\ldots,n_i,\ j = 1,\ldots,k\right].$$

This is a subalgebra of $\mathbb{F}[V]^{\mathbb{Z}/p}$ which we will refer to as the **Dade subalgebra** associated to the Dade basis (in this case a Jordan basis) $\left\{(z_i(j) \mid i = 1,\ldots,n_i,\ j = 1,\ldots,k\right\}$. Note that as an algebra $D_*(n_1,\ldots,n_k)$ is a polynomial algebra on linear forms and forms of degree p. Since $\mathbb{F}[V]$ is Cohen-Macaulay a short computation with Poincaré series shows that $\mathbb{F}[V]$ is generated as a $D_*(n_1,\ldots,n_k)$-module by forms of degree at most $(n-k)\cdot(p-1)$. The transfer homomorphism $\mathrm{Tr}^{\mathbb{Z}/p} : \mathbb{F}[V] \longrightarrow \mathbb{F}[V]^{\mathbb{Z}/p}$ is a map of $D_*(n_1,\ldots,n_k)$-modules, and therefore we have shown:

LEMMA 4.1: *Let $\rho : \mathbb{Z}/p \hookrightarrow \mathrm{GL}(n, \mathbb{F})$ be a faithful representation of $\mathbb{Z}/p$ over a field $\mathbb{F}$ of characteristic p, $V = \mathbb{F}^n$, and $D_* \subseteq \mathbb{F}[V]^{\mathbb{Z}/p}$ the Dade subalgebra associated to a Jordan basis for V^*. Then $\mathrm{Im}(\mathrm{Tr}^{\mathbb{Z}/p}) \subset \mathbb{F}[V]^{\mathbb{Z}/p}$ is generated as a D_*-module, and hence also as an ideal, by forms of degree at most $(n-k)\cdot(p-1)$, where $k = \dim_{\mathbb{F}}(V^{\mathbb{Z}/p})$ is the number of Jordan blocks.* □

Recall from Lemma 3.1 we have an exact sequence

$$(\divideontimes) \qquad 0 \longrightarrow H(n_1, \ldots, n_m, \ldots, n_k) \xrightarrow{i^*} H(n_1, \ldots, n_m - 1, \ldots, n_k) \xrightarrow{\delta} H(n_1, \ldots, n_m, \ldots, n_k) \longrightarrow 0,$$

where $n_1, \ldots, n_k$ are the dimensions of the Jordan blocks in a decomposition of V into irreducible $\mathbb{Z}/p$-representations. The map i^* has degree 0 and the map δ degree -1. Recall we also have an exact sequence

$$(\circledast) \qquad 0 \longrightarrow \mathrm{Im}(\mathrm{Tr}^{\mathbb{Z}/p}) \longrightarrow \mathbb{F}[V]^{\mathbb{Z}/p} \longrightarrow H^{\mathrm{ev}}(n_1, \ldots, n_k) \longrightarrow 0$$

of D_*-modules, and know from [34] and [33] Proposition 4.4 that

$$H(\underbrace{p, \ldots, p}_{k}) \cong \mathbb{F}[c_{\mathrm{top}}(z_1(j)) \mid j = 1, \ldots, k].$$

Hence $H(\underbrace{p, \ldots, p}_{k})$ has a single generator of degree 0 as a D_*-module. By downward induction from this case we therefore obtain:

LEMMA 4.2: *Let $\rho : \mathbb{Z}/p \hookrightarrow \mathrm{GL}(n, \mathbb{F})$ be a faithful representation of $\mathbb{Z}/p$ over a field $\mathbb{F}$ of characteristic p, $V = \mathbb{F}^n$, and $D_* \subseteq \mathbb{F}[V]^{\mathbb{Z}/p}$ the Dade subalgebra associated to a Jordan basis $\left\{(z_i(j) \mid i = 1, \ldots, n_i,\ j = 1, \ldots, k\right\}$ for V^*. Then $H(n_1, \ldots, n_k)$ is generated as a D_*-module by elements of degree at most $k\cdot(p-1)$, and hence as an algebra by forms of degree at most $\max\left(p, k\cdot(p-1)\right)$.* □

From these two lemmas we obtain our first degree bound.

THEOREM 4.3: *Let $\rho : \mathbb{Z}/p \hookrightarrow \mathrm{GL}(n, \mathbb{F})$ be a faithful representation of $\mathbb{Z}/p$ over a field $\mathbb{F}$ of characteristic p, $V = \mathbb{F}^n$, and $D_* \subseteq \mathbb{F}[V]^{\mathbb{Z}/p}$ the Dade subalgebra associated to a Jordan basis $\left\{(z_i(j) \mid i = 1, \ldots, n_i,\ j = 1, \ldots, k\right\}$ for V^*. Then $\mathbb{F}[V]^{\mathbb{Z}/p}$ is generated by forms of degree at most $(n-k)\cdot(p-1)$ as D_*-module and hence by forms of degree at most $\max\left(p, (n-k)\cdot(p-1)\right)$ as $\mathbb{F}$-algebra.*

PROOF: We can certainly assume that none of the Jordan blocks are trivial, so for a Jordan block of dimension m we always have $m \geq 2$ with the dimension of the fixed point set being 1. Therefore

$$\begin{aligned}(n-k)\cdot(p-1) &= (n_1-1)\cdot(p-1) + \cdots + (n_k-1)\cdot(p-1)\\ &\geq (p-1) + \cdots + (p-1) = k(p-1)\end{aligned}$$

and the result follows from the exact sequence $(\circledast)$ and the Lemmas 4.1 and 4.2. □

The discussion provides a strategy for computing a set of algebra generators for $\mathbb{F}[V]^{\mathbb{Z}/p}$, namely, first by hook or by crook, compute the invariants up to degree $k\cdot(p-1)$, where k is the number of Jordan blocks, and then the image of the transfer through dimension $(n-k)\cdot(p-1)$. Among a vector space basis for this will be a set of algebra generators. Again, similar results may be obtained for $\mathbb{Z}/p^s$, $s \in \mathbb{N}$, by working with Jordan blocks of size $(s+1)\cdot p + r$, where $0 \leq r < p$.

Here are some examples to illustrate how sharp the bound of 4.3 is in comparison to other known upper bounds.

EXAMPLE 1: Permutation Representations:
We suppose that X is a finite $\mathbb{Z}/p$-set, and for simplicity, this is no loss of generality, that $\mathbb{Z}/p$ acts freely on X. Then $|X| = kp$, for some $k \in \mathbb{N}$, and the upper bound given by the preceeding theorem is $k \cdot (p-1)^2$ (since the dimension of the corresponding linear representation is kp and that of the fixed point set k). For $p = 2$ this gives k as upper bound, which is sharp by [26] and [27]. By comparison Göbel's bound for permutation representations [16] gives $\binom{kp}{2}$ which generally is larger than $k \cdot (p-1)^2$.

EXAMPLE 2: A single Jordan block:
In this case $2 \le n \le p$ and, apart from some low dimensional cases, Theorem 4.3 gives $(n-1) \cdot (p-1)$ as an upper bound for algebra generators. For example, in the well studied example of the submaximal Jordan block (i.e., $n = p-1$) (see e.g., [4], [5], [1], [2], [19], and [13], to name just a few references) where $p = 5$ and $n = 4$, we get 12 as an upper bound. Moreover, the generators in degrees above 4 all lie in the image of the transfer. However, we will see shortly that this bound can be reduced to 8 if we exercise a bit more care in how we choose a system of parameters in the proof of Lemma 4.1.

The dominant factor in the upperbound estimate of Theorem 4.3 is the degree bound contained in Lemma 4.1 for the ideal generators of $\mathrm{Im}(\mathrm{Tr}^{\mathbb{Z}/p})$, which in turn depends on the obvious upperbound for the degree of module generators of $\mathbb{F}[V]$ as a module over the Dade subalgebra $D_*(n_1, \ldots, n_k) \subseteq \mathbb{F}[V]^{\mathbb{Z}/p}$. But, as the proof shows, we are free to replace $D_*(n_1, \ldots, n_k)$ by any subalgebra $\mathscr{S}_* \subseteq \mathbb{F}[V]^{\mathbb{Z}/p}$ that contains a system of parameters. So if we can find a ***better*** system of parameters, then the proof of Theorem 4.3 will give a better estimate. Finding such a better system of paramaters is facilitated by computations in [17] and [29].

We begin by considering the irreducible representation of $\mathbb{Z}/p$ over $\mathbb{F} = \mathbb{F}_p$, V_n, of dimension n, $2 \le n \le p$.

LEMMA 4.4: *Let V_n be the irreducible representation of $\mathbb{Z}/p$ over the field $\mathbb{F}$ of characteristic $p > 2$, implemented by the matrix $\mathbf{J}_n \in \mathrm{GL}(n, \mathbb{F})$, and $z_1, \ldots, z_n \in V^*$ the dual to the Jordan basis for V. Then the quadratic forms*

$$Q_i = z_i^2 + 2 \cdot \left[\sum_{j=1}^{n-i} (-1)^j z_{i-j} z_{i+j} \right] \qquad \tfrac{n+1}{2} \le i < n$$

are invariant, i.e., $Q_{\frac{n+1}{2}}, \ldots, Q_{n-1} \in \mathbb{F}[V_n]^{\mathbb{Z}/p}$. (N.b. The condition on i is what assures that the indices in the sum stay in the range $1, \ldots, n$.)

PROOF: By direct computation we have

$$\partial(Q_i) = -2 z_i z_{i+1} + 2 \left[\sum_{j=1}^{n-i-1} (-1)^{j+1} \left(z_{i-j+1} z_{i-j} + z_{i-j} z_{i+j+1} \right) \right] + 2(-1)^{n-i} z_{2i-n+1} z_n ,$$

which upon rearranging terms gives

$$\begin{aligned} \partial(Q_i) = {} & -2 z_i z_{i+1} + 2 z_i z_{i+1} + \\ & 2 z_{i-1} z_{i+2} - 2 z_{i-1} z_{i+2} + \\ & \ddots \\ & 2(-1)^{n-i+1} z_{2i-n+i} z_n + 2(-1)^{n-i} z_{2i-n+1} z_n \\ & = 0 \end{aligned}$$

and the result follows. □

The number of invariant quadratic forms found in Lemma 4.4 will be denoted by $b(n)$. One finds by counting that

$$b(n) = \begin{cases} \frac{n}{2} - 1 & \text{if } n \text{ is even} \\ \frac{n-1}{2} & \text{if } n \text{ is odd.} \end{cases}$$

According to [29] Theorem 3.2 there are elements of degree $p-1$, $f_2, \ldots, f_{n-b(n)-1} \in \mathbb{F}[V_n]$, lying in the image of the transfer, and having leading monomials

$$z_2^{p-1}, \ldots, z_{n-b(n)-1}^{p-1}$$

respectively, with respect to the lexicographic order of monomials. (N.b. The indexing in [29] is *inverse* to that employed here, i.e., if $x_1, \ldots, x_n$ are the *variables* from [29], the $z_i = x_{n-i+1}$ for $i = 1, \ldots, n$. So the use of *reverse* lexicographic ordering in [29] turns into lexicographic ordering here.)

LEMMA 4.5: *Let V_n be the irredicible representation of $\mathbb{Z}/p$ over $\mathbb{F} = \mathbb{F}_p$ of dimension n, $2 \leq n \leq p$. Then, the invariants*

$$c_{top}(z_1), f_2, \ldots, f_{n-b(n)-1}, Q_{n-b(n)}, \ldots, Q_{n-1}, z_n \in \mathbb{F}[V_n]^{\mathbb{Z}/p}$$

form a system of parameters.

PROOF: If we look at the ideal of leading terms, $\mathcal{J}$, of the polynomials

$$c_{top}(z_1), f_2, \ldots, f_{n-b(n)-1}, Q_{n-b(n)}, \ldots, Q_{n-1}, z_n \in \mathbb{F}[V_n]^{\mathbb{Z}/p},$$

we see that it contains

$$z_1^p, z_2^{p-1}, \ldots, z_{n-b(n)-1}^{p-1}, z_{n-b(n)}^2, \ldots, z_{n-1}^2, z_n,$$

so the quotient algebra $\mathbb{F}[V]/\mathcal{J}$ is finite dimensional, since

$$\mathbb{F}[z_1, \ldots, z_n] \Big/ \left(z_1^p, z_2^{p-1}, \ldots, z_{n-b(n)-1}^{p-1}, z_{n-b(n)}^2, \ldots, z_{n-1}^2, z_n, \right)$$

already is. By Gröbner basis theory [11], Chapter 5 Section 3 Proposition 4, the quotient algebra

$$\mathbb{F}[V] \Big/ \left(c_{top}(z_1), f_2, \ldots, f_{n-b(n)-1}, Q_{n-b(n)}, \ldots, Q_{n-1}, z_n \right)$$

is also finite dimensional, and the result follows. □

Let $\mathcal{C}$ be the subalgebra generated by

$$c_{top}(z_1), f_2, \ldots, f_{n-b(n)-1}, Q_{n-b(n)}, \ldots, Q_{n-1}, z_n \in \mathbb{F}[V_n]^{\mathbb{Z}/p}$$

A short Poincaré series computation shows that $\mathbb{F}[V]$ is generated as a module over $\mathcal{C}$ by forms of degree at most

$$(\bigstar) \qquad \mathbf{b}_p(n) := \begin{cases} \frac{n}{2}(p-1) & \text{if } n \text{ is even} \\ 1 + \frac{n-1}{2}(p-1) & \text{if } n \text{ is odd.} \end{cases}$$

Hence using the system of parameters

$$c_{top}(z_1), f_2, \ldots, f_{n-b(n)-1}, Q_{n-b(n)}, \ldots, Q_{n-1}, z_n \in \mathbb{F}[V_n]^{\mathbb{Z}/p}$$

in the proof of 4.3 leads to:

THEOREM 4.6: *Let $\rho : \mathbb{Z}/p \hookrightarrow \mathrm{GL}(n, \mathbb{F})$ be a faithful irreducible representation of $\mathbb{Z}/p$ over a field $\mathbb{F}$ of characteristic p, $2 \leq n \leq p$. Set $V = \mathbb{F}^n$. Then $\mathbb{F}[V]^{\mathbb{Z}/p}$ is generated by forms of degree at most*

$$\max\left(p, \begin{cases} \frac{n}{2}(p-1) & \textit{if } n \textit{ is even} \\ 1 + \frac{n-1}{2}(p-1) & \textit{if } n \textit{ is odd} \end{cases} \right). \quad \square$$

This result is indeed sharp, as comparison with the results of [2], [12], [29], and the references to be found there, show. It extends to all finite dimensional $\mathbb{Z}/p$ representations in the same way that the results of Section 3 follow from those of Section 2. The proof is left to the reader.

COROLLARY 4.7: *Let $\rho : \mathbb{Z}/p \hookrightarrow \mathrm{GL}(n, \mathbb{F})$ be a representation of the group $\mathbb{Z}/p$ of prime order p over the field $\mathbb{F}$ of characteristic p. Let $V = V_{n_1} \oplus \cdots \oplus V_{n_k}$ be a decomposition of V as $\mathbb{Z}/p$-module into a sum of irreducible $\mathbb{Z}/p$-modules. Then $\mathbb{F}[V]^{\mathbb{Z}/p}$ is generated as an algebra by forms of degree at most*

$$\max\left(p, \sum_{i=1}^{k} \mathbf{b}_p(n_i)\right),$$

where $\mathbf{b}_p(n)$ is given by formula (★). □

§5. Closing Comments

Recall that the Dickson algebra $\mathbf{D}_*(n)$ over the Galois field $\mathbb{F}_q$ with $q = p^\nu$ elements has a fractal property:

$$\Phi\big(\mathbf{D}_*(n)\big) = \big(\Phi(\mathbb{F}[V])\big)^{\mathrm{GL}(n,\mathbb{F}_q)}$$

where $V = \mathbb{F}_q^n$ and $\Phi : \mathbb{F}_q[V] \circlearrowright$ is the Frobenius homomorphism $f \longmapsto f^q$. From Proposition 3.3 and Corollary 3.5 we obtain the following partial answer to the question posed in the introduction:

PROPOSITION 5.1: *Let $\rho : \mathbb{Z}/p \longrightarrow \mathrm{GL}(n, \mathbb{F}_p)$ be a representation of the cyclic group of prime order over the Galois field $\mathbb{F} = \mathbb{F}_q$. Then there exists an integer $s > 0$ such that $H^1(\mathbb{Z}/p; \mathbb{F}[V]) \cong H^2(\mathbb{Z}/p; \mathbb{F}[V])$ as modules over $\Phi^s\big(\mathbf{D}_*(n)\big)$.* □

The bound of Theorem 4.6 can be used to start an iterative procedure that leads to a bound for all finite p groups, and hence for all finite groups.

PROPOSITION 5.2: *Fix an odd prime p, and let $\mathbb{F}$ be a field of characteristic p. There is an integer valued function $\mathbf{m}_p(n, a)$ of two integer variables $n, a \in \mathbb{N}$, such that: for any finite p group P of order p^a and any faithful representation $\rho : P \hookrightarrow \mathrm{GL}(n, \mathbb{F})$ the ring of invariants $\mathbb{F}[V]^P$ is generated as an algebra by forms of degree at most $\mathbf{m}_p(n, a)$.*

The proof of the theorem will yield a rate of growth for $\mathbf{m}_p(n, a)$ that is far too large to be of any pratical use (ca. $(n!)^{a-1}$). However, since the proof is not hard, here are the details.

NOTATION: If A is a graded, connected, commutative Noetherean algebra over $\mathbb{F}$ then $\beta(A)$ denotes the maximal degree of a generator in a minimal algebra generating set for A. This is just the degree of the Poincaré series $P(QA, t)$, where $QA = \mathbb{F} \otimes_A \bar{A}$ and $\bar{A}$ is the augmentation ideal of A. (See e.g., [30] Chapter 4.)

LEMMA 5.3: *Let A be a graded, connected, commutative, Noetherean algebra over the field $\mathbb{F}$ and $\rho : G \hookrightarrow \mathrm{Aut}_*(A)$ a faithful representation of the group G by grading preserving automorphisms of A. Let W_i denote the graded vector space with $W_i = A_i$ and all other homogeneous components 0. Then the natural map $\varphi_i : S(W_i) \longrightarrow A$ is G equivariant, where $S(W)$ denotes the symmetric algebra on W, and, the induced map*

$$\bigotimes_{i=1}^{\beta(A^G)} \varphi_i^G : \bigotimes_{i=1}^{\beta(A^G)} S(W_i) \longrightarrow A$$

is an epimorphism.

PROOF: A^G is finitely generated by [30] Theorem 2.3.1. Let $\beta = \beta(A^G)$. Since A^G is generated by homogeneous elements of degree at most β it will be enough to show that

$$\varphi_i^G : S(W_i)_i^G \longrightarrow A_i$$

is an epimorphism for $i \leq \beta$. By the definition of the symmetric algebra functor $S(\text{—})$ we have

an inclusion $W_i \subseteq S(W_i)_i$ and by definition of φ_i the triangle

$$\begin{array}{ccc} W_i & \hookrightarrow & A \\ \downarrow & \nearrow & \\ S(W_i) & & \end{array}$$

commutes. Recall, per definition $W_i = A_i$, so taking homogeneous components of degree i and passing to fixed point sets gives

$$\begin{array}{ccc} W_i^G & = & A_i^G \\ \downarrow & \nearrow & \\ S(W_i)_i^G & & \end{array}$$

from which the lemma follows. □

LEMMA 5.4: *Let A be a graded, connected, commutative, Noetherean algebra over the field $\mathbb{F}$ and $\rho : \mathbb{Z}/p \hookrightarrow \mathrm{Aut}_*(A)$ a faithful representation of the group $\mathbb{Z}/p$ by grading preserving automorphisms of A. Then $\beta(A^G) \leq \max\left(d_i \mid i \leq \beta(A)\right) \cdot p$ where $d_i = \dim_{\mathbb{F}}(A_i)$.*

PROOF: This follows from Lemma 5.3 and Theorem 4.3. □

PROOF OF THEOREM 5.2: By induction on $a \in \mathbb{N}$. For $a = 1$ this is contained in Theorem 4.3. Assume the result has been established for $a - 1$ and that P has order p^a. Choose a maximal normal subgroup $Q \lhd P$ of index p, so $P/Q \cong \mathbb{Z}/p$. Then $\mathbb{F}[V]^P = \left(\mathbb{F}[V]^Q\right)^{\mathbb{Z}/p}$. From the induction hypothesis we then have $\beta(A^Q) \leq \mathbf{m}_p(n, a-1)$. Since $\mathbb{F}[V]_b^Q \subseteq \mathbb{F}[V]_b$, $b \in \mathbb{N}$, we certainly have

$$\dim_{\mathbb{F}}(\mathbb{F}[V]_b^Q) \leq \dim_{\mathbb{F}}(\mathbb{F}[V]_b) = \binom{n+b-1}{n-1} \qquad b \in \mathbb{N},$$

so if we apply Lemma 5.4 to the action of $\mathbb{Z}/p$ on $\mathbb{F}[V]^Q$ we obtain

$$\beta(\mathbb{F}[V]^P) \leq \max\left(\binom{n+b-1}{n-1} \mid b \leq \beta\left(\mathbb{F}[V]^Q\right)\right) \cdot p \leq \binom{n+\mathbf{m}_p(n,a-1)-1}{n-1} \cdot p$$

and the result follows. □

References

[1] G. Almkvist, *Invariants, Mostly Old,* Pac. J. of Math. 86 (1980), 1–13.

[2] G. Almkvist, *Invariants of* $\mathbf{Z}/p\mathbf{Z}$ *in Characteristic p,* In: Invariant Theory (Proceedings of the 1982 Montecatini Conference), Lecture Notes in Math.996, 109–117, Springer-Verlag, Heidelberg, Berlin, 1983.

[3] S. Balcerzyk and T. Józefiak, *Commutative Noetherean and Krull Rings,* PWN, Polish Scientific Publishers, Warsaw, 1989.

[4] M.-J. Bertin, *Anneaux d'invariants d'anneaux de polynômes en caractéristique p,* C. R. Acad. Sci. Paris t. 264 (Série A) (1967), 653–656.

[5] M. -J. Bertin, *Anneaux d'invariants d'anneaux de polynômes en caractéristique p,* C. R. Acad. Sci. Paris t. 277 (Série A) (1973), 691–694.

[6] D. Bourguiba, *Profondeur et algèbre de Steenrod,* Thèse, Uni. de Tunis II, (1997).

[7] D. Bourguiba and S. Zarati, *Depth and Steenrod Operations,* Inventiones Math., 128 (1997), 589–602.

[8] W. Bruns and J. Herzog, *Cohen-Macaulay Rings,* Cambridge Studies in Advanced Math 39, Math. Proc. of the Camb. Phil. Soc. , Cambridge, 1993.

[9] H. E. A. Campbell, I. P. Hughes, G. Kemper, *Depth of Modular Invariant Rings,* preprint, Kingston 1997.

[10] H. Cartan and S. Eilenberg, *Homological Algebra,* Princeton Univ. Press, Princeton, 1956.

[11] D. Cox, J. Little and D. O'Shea, *Ideals, Varieties, and Algorithms,* Springer-Verlag, Heidelberg, Berlin, 1992.

[12] L.E.J. Dickson, *On Invariants and the Theory of Numbers,* The Madison Colliquium, AMS 1913, Dover reprint Corp. NY 1966.

[13] G. Ellingsrud and T. Skjelbred, *Profondeur d'anneaux d'invariants en caractéristique p,* Comp. Math. 41 (1980), 233–244.

[14] L. Evens, *The Cohomology of Groups,* Claerndon Press, Oxford, 1991.

[15] R. M. Fossum and P. A. Griffith, *Complete Local Factorial Rings which are not Cohen-Macaulay in Characteristic p,* Ann. Scient. Éc. Norm. Sup. 4^e série, t. 8 (1975), 189–200.

[16] M. Göbel, *Computing Bases for Permutation Invariant Polynomials,* J. of Symbolic Computation 19 (1995), 285 – 291.

[17] K. Kuhnigk, *Das Transferhomomorphismus für Ringen von Invarianten,* Diplomarbeit, Universität Göttingen, 1997.

[18] K. Kuhnigk and L. Smith, *Feshbach's Transfer theorem and Applications,* Preprint, AG-Invariant Theory, 1998.

[19] R. M. Fossum and P. A. Griffith, *Complete Local Factorial Rings which are not Cohen-Macaulay in Characteristic p,* Ann. Scient. Éc. Norm. Sup. 4^e série, t. 8 (1975), 189–200.

[20] G. Kemper *On the Cohen-Macaulay Property for Modular Invariant Rings,* Preprint, IWR Heidelberg, 1997.

[21] S. Lang, *Rapport sur la Cohomologie des Groupes,* Benjamin, Princeton, 1967.

[22] M.D. Neusel, *Integral Extensions of Unstable Algebras over the Steenrod Algebra,* Forum. Math. (to appear).

[23] M. D. Neusel and L. Smith, *The Lasker-Noether Theorem for* $\mathcal{P}^*$*-invariant ideals,* Forum Math. 10 (1998), 1–18.

[24] V. Reiner, *On Göbel's Bound for Invariants of Permutation Groups,* Arch. der Math. 65 (1995), 475 – 480.

[25] V. Reiner and L. Smith, *Systems of Parameters for Rings of Invariants,* Preprint, Göttingen, 1996.

[26] D. R. Richman, *Invariants of Finite Groups over Fields of Characteristic p,* Adv. in Math. 124 (1996), 25–48.

[27] D. R. Richman, *Explicit Generators of the Invariants of Finite Groups,* Adv. in Math. 124 (1996), 49–76.

[28] J.-P. Serre, Corps Loceaux, Herman, Paris, 1962.

[29] R.J. Shank, *S.A.G.B.I Bases for Rings of Formal Modular Invariants,* Comm. Math.Helv. 73 (1998), 546–565.

[30] L. Smith, *Polynomial Invariants of Finite Groups,* A.K. Peters, Ltd., Wellesley, MA, 1995, second printing 1997.

[31] L. Smith, *Some Rings of Invariants that are Cohen-Macaulay,* Canad. Math. Bull. 39 (1996), 238 – 240.

[32] L. Smith *Folklore . . . ,* NonPreprint , AG-Invariantentheorie, 1996.

[33] L. Smith, *Homological Codimension of Modular Rings of Invariants and the Koszul Complex*, J. of Math of Kyoto Univ. 38 (1998), 727 – 747.

[34] L. Smith, *Modular Vector Invariants of Cyclic Permutation Groups*, Canad. Math. Bull. 42 (1), (1999) 125 – 128.

[35] W. Smoke, *Dimension and Multiplicity for Graded Algebras*, J. of Algebra 21 (1972), 149–173.

Larry Smith
Yale University

New Haven, CT, USA

and

Göttingen, Germany

LARRY@SUNRISE.UNI-MATH.GWDG.DE